Кривична дела високотехнолошког криминала

Драган Прља
Звонимир Ивановић
Марио Рељановић

ИНСТИТУТ ЗА УПОРЕДНО ПРАВО

Др Драган Прља

Др Звонимир Ивановић Др Марио Рељановић

КРИВИЧНА ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

Издавач
ИНСТИТУТ ЗА УПОРЕДНО ПРАВО БЕОГРАД

Рецензенти
Проф. др Божидар Бановић
Проф. Др Бранислав Симоновић
Др Јован Ћирић

Уредник
Др Јован Ћирић

Тираж
300

ISBN 978-86-80059-75-4

ДР ДРАГАН ПРЉА
ДР ЗВОНИМИР ИВАНОВИЋ
ДР МАРИО РЕЉАНОВИЋ

КРИВИЧНА ДЕЛА
ВИСОКОТЕХНОШКОГ КРИМИНАЛА

БЕОГРАД
2011

Реч на почетку

У почетку беше реч, интернет је дошао тек много касније. (Иако ми се наметало да кажем „на крају беше интернет“, то нисам рекао, просто да не бих слутио то „на крају“) У сваком случају, после арапских фејс-бук револуција, данас је свима јасно да интернет више није тек само играчка за бубуљичаве пубертетлије. Чак и они који о компјутерима и интернету имају тек површна и половична знања, схватају да је (кривично)правна проблематика употребе и злоупотребе компјутера и интернета од изузетног глобалног значаја. Драган Прља, Марио Рељановић и Звонимир Ивановић одавно то знају врло добро, те су се зато и прихватили посла у вези са писањем књиге о високотехнолошком криминалитету и свакодневној пракси и проблемима у борби против ове нове врсте криминалитета.

Ако постоји нешто што симболизује данашњи нови свет и нове технологије, ако постоји нешто што нам показује како и колико је данашњи свет мали и свакоме на дохват руке, онда су то управо компјутери и интернет. Можете се не померати из места у којем живите, можете, шта више бити приковани за болесничку постељу, непокретни практично, а опет можете обићи читав свет и оставити за собом бројне и добре и лоше трагове, те направити велике штете, чак веће него да сте по том свету путовали на уобичајени начин, било којим данас познатим превозним средством.

Када је на пример реч о порнографији, педофилији, о којој, између осталих ствари, Прља, Рељановић и Ивановић овде пишу, ствар је јасна: не морате путовати у Бразил, нити на Тајланд – педофилијом се можете бавити и овде и одавде и можете се сасвим лако умрежити са другима, себи сличнима, да бисте се бавили овом патолошком делатношћу. Обашка што путем интернета можете преварити и „навући“ девојчице и дечаке из читавог света, да се уплету у вашу мрежу и да их искористите за многе понекад безопасне, али и врло опасне ствари. О свему томе има речи у овој књизи, као и о неким занимљивим контролисаним експериментима, када је педофилија у питању.

Аутори нам овде говоре и о кривичним делима против интелектуалне својине, али и о кривичним делима против имовине, а ту је превара, тзв. нигеријска превара у првом плану. Данас се о тој тзв. нигеријској превари зна веома много, али, када се тек била појавила, људи су били и необавештени и неопрезни и неприпремљени. Готово да нема човека који колико-толико барата компјутером и интернетом, а да се није сусрео са тим да неко покуша да га превари на овај или онај начин. Тако сам и ја на пример, пре неколико месеци, добио један е-маил у којем ме један мој пријатељ, пишући ми писмо на енглеском језику, обавештава да се налази у Шпанији, да су га опљачкали, да је остао без пасоша и платних картица

и да му је хитно потребно да му пошаљем 5.000 евра. Ја наравно нисам насео. Знао сам да се тај мој пријатељ тада не налази у Шпанији, осим тога, зашто би ми тај мој пријатељ писао на енглеском, а не на српском језику и поврх свега, 5.000 евра су за мене стварно паре које нису баш за бацање. Али, питам се шта би било да је порука била послата на српском и да су уместо 5.000 евра, тражили само 50 евра и да се ја нисам баш тога дана претходно чуо са мојим пријатељем, па сам знао да није у Шпанији? Шта би тада било, да ли бих насео?

Аутори ове занимљиве књиге, пишу и о кривичним делима против привреде, о фалсификовању и злоупотребама платних картица, о крађи идентитеа, о тзв. фишингу и фармингу, који су се први пут појавили још 1996.године. Једноставно речено, платни промет се данас у све већој мери одвија преко интернета и све се више плаћа кредитним (дебитним) картицама и ето проблема, ето нових изазова. О свему томе, као и о још много чему другом, о прању новца, о неовлашћеној употреби туђег имена, прочитаћете у овој књизи.

У књизи се анализирају и кривична дела против опште сигурности људи и имовине, наравно кривична дела против безбедности рачунарских података, затим против уставног уређења, а ту је пре свега реч о шпијунажи, као и о кривичним делима против човечности и других добара заштићених међународним правом, а ту се првенствено ради о расној и другој дискриминацији.

Све у свему, ово је једна врло занимљива област где се сусрећу они који су се иначе сусретали још једино у своје време у КСТ-у или Бона Фидесу, студенти електротехнике или математике са студентима права. Све до недавно је изгледало да електротехника и математика (информатика) са правима и немају много додирних тачака, а онда се појавио интернет. Компјутери и интернет су ипак исувише озбиљне ствари да се њима не би бавили и правници, а опет, са друге стране и право је систем, понекад прегломазан и несистематизован, али ипак систем који би бар по дефолту (ето једног типичног компјутерашког израза) требало да буде логички математичан.

Ово је дакле област, ово је дакле правничка књига, која ће, за разлику од других правничких књига, подједнако занимати и правнике и инжењере. Чини се да боља препорука од тога и није потребна. У ствари, ја ове речи и нисам написао зато да бих ову књигу препоручивао, то њој и није потребно, већ зато да бих се ауторима Драгану Прљи, Марију Рељановићу и Звонимиру Ивановићу захвалио што су библиотеку, издавачку делатност Института за упоредно право, обогатили овом вредном и занимљивом књигом.

Др Јован Ћирић

1. КРИВИЧНА ДЕЛА ПРОТИВ ПОЛНЕ СЛОБОДЕ

1.1 Приказивање порнографског материјала и искоришћавање деце за порнографију

Конвенција о ВТК као кривично дело Дечије порнографије[1] (политички и етички коректнији термин је материјал који приказује злостављање деце) инкриминише: а. производњу дечије порнографије са циљем њеног дистрибуирања кроз рачунарски систем;

б. нуђење или на други начин чињење доступним дечије порнографије путем рачунарског система;

в. дистрибуцију или емитовање дечије порнографије путем рачунарског система;

г. набављање дечије порнографије за себе или другога, путем рачунарског система;

д. поседовање дечије порнографије на рачунарском систему или на медијуму за пренос рачунарских података.

Европска конвенција о високотехнолошком криминалу (ВТК)[2], тежи да помогне хармонизацији правних система држава чланица и да утиче на то ову појаву све чланице схвате са достојном озбиљношћу. Конвенција садржи и неке одредбе које су шире од свих упоредних решења у националним законодавствима[3]. Тако је старосна граница које се особе сматрају децом постављена на 18 година, уз могућност да државе, стављањем резерве на овај члан Конвенције, исту смање на 16 година старости[4]. Затим, инкриминисани су садржаји у којима се појављују особе за које се може основано претпоставити да су млађе од 18 година, или се

---

[1] Највеће и најзначајније измене везане за кривична дела према Закону о изменама и допунама Кривичног законика од 31.08.2009. године су настале изменама у чл. 185, 185а и б, 225, 317, 387.

[2] CETS 185 и додатни протокол CETS 189 доступни на: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm и http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=189&CL=ENG последњи пут приступљено 29.08.2011.год.

[3] Комлен Николић, Л. и др. Сузбијање вискотехнолошког криминала, Удружење јавних тужилаца и заменика јавних тужилаца, АЕЦИД 2010, Београд. Стр. 45.

[4] У претходном периоду ово је направило проблем у пракси, обзиром да је до измена 2009.год. у чл.185 стајало да се као пасивни субјекат овог дела јавља дете а не малолетник, па су, беспотребно одређене, изузетно битне, категорије жртава избачене из инкриминације, обзиром на њихово дефинисање у нашим законима (Закон о малолетним учиниоцима кривичних дела и кривично правној заштити малолетних лица – ЗОМ "Службени Гласник РС", бр. 85/05 и Кривични законик – КЗ,"Службени Гласник РС" бр. 85/2005, 88/2005, 107/2005, 72/2009 и 111/2009).

представљају као такве, као и други графички садржаји (цртежи, цртани филмови и сл.) у којима се представљају особе млађе од прописане границе у порнографском контексту. Конвенција оставља могућност стављања резерви, свакој држави чланици, на оваква, можемо рећи, врло иновативна решења.

Постоје најразличитији, доста разматрани проблеми, у оквиру овог кривичног дела. Један од таквих је контроверза око инкриминације самог акта поседовања материјала дечије порнографије и интеграција фиктивних фотографија. Први случај код инкриминисања поседа (државине) везује се за објашњење о чињеници да само поседовање или држање подстиче потражњу и да доводи до наставка даље продукције оваквог материјала. Ова веза између поседовања и продукције је главно објашњење, али се ипак оставља државама могућност стављања резерве на ову одредбу Конвенције. Са друге стране, заштита се пружа и на ширем плану, обухватајући и производњу фотографија или колажа од делова имица (фотографија) и употребе 3Д програма, дакле, креирање потпуно нових фотографија (чиме се не задире у слободе и права било ког детета), дајући као разлог за ову фиктивну дечију порнографију (њено инкримиинисање) то што се овако креиране фотографије могу користити као мамац за децу да пристану на сексуалне акте или ради повећања потражње за дечијом порнографијом. У смислу потпунијег разматрања овог кривичног дела неопходно је консултовати и текст Конвенције о заштити деце од сексуалне експлоатације и сексуалног злостављања[5] коју је Србија ратификовала.

У нашем законодавству кривично дело има четири облика. Први (у ставу 1) чини лице које малолетнику прода, прикаже или јавним излагањем, или на други начин, учини доступним текстове, слике, аудио – визуелне или друге предмете порнографске садржине или му прикаже порнографску представу. За ову алтернативно постављену радњу извршења кривичног дела предвиђена је новчана казна или затвор до шест месеци.

У ставу 2 инкриминисан је други облик а то је искоришћавање малолетника за производњу слика аудио-визуелних или других предмета порнографске садржине или за порнографску представу а предвиђена је казна затвора од шест месеци до пет година. Ради се о искоришћавању малолетника у специфичне сврхе – злоупотребу детета које, често, није ни свесно чињенице да је искоришћено или у које се сврхе искоришћава.

Трећи облик чини оно лице које прва два облика изврши према детету, учинилац овог облика ће се казнити за дело из става 1. затвором од шест месеци до три године, а за дело из става 2. затвором од једне до осам година

Четврти облик предвиђен је ставом 4 и чини га радња лица које прибавља за себе или другог, поседује, продаје, приказује, јавно излаже или електронски или на други начин чини доступним слике, аудио-визуелне или друге предмете порнографске садржине настале искоришћавањем малолетног лица, казниће се затвором од три месеца до три године[6]. Ово кривично дело може бити извршено

[5] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CL=ENG, доступна 27.04. 2010.год.

[6] Што се тиче примене нпр. мере из чл.504е или других специјалних истражних мера ово дело представља један од веома интересантних примера. Наиме теоријски примена ових мера би према

само према пунолетном лицу, јер би се у супротном радило о извршењу овог дела али из става 1. У погледу виности потребан је умишљај[7]. У ставу 5 предвиђено је да ће се предмети о којима је реч одузимају.

Законик не даје дефиницију порнографског материјала. Иначе, растурање порнографског материјала до XVIII века није ни инкриминисано[8]. *Конвенција о заштити деце од сексуалне експлоатације и сексуалног злостављања у чл. 20.* даје дефиницију[9] и она је код нас законом о њеном потврђивању уведена у правни систем. Ово дело је свршено предузимањем ма које од алтернативно постављених радњи извршења, а у погледу виности потребан је умишљај.

Прописивањем овог кривичног дела и великог броја кажњивих радњи законодавац је имао намеру да заштити психофизички и полни интегритет деце. Кривични законик у члану 112. дефинише појмове (8) Дететом се сматра лице које није навршило четрнаест година. (9) Малолетником се сматра лице које је навршило четрнаест година, а није навршило осамнаест година. (10) Малолетним лицем сматра се лице које није навршило осамнаест година[10].

За доказивање кривичног дела потребно је, на несумњив начин, утврдити време и место извршења кривичног дела, начин извршења - која од радњи извршења је спроведена и према ком лицу, а за одређене облике овог дела потребно је утврдити да се ради о малолетном лицу, односно о детету. Ово су индиције које се могу назрети већ при обезбеђењу лица места или приликом вршења увиђаја, а даљим мерама које ће се предузимати и потврдити или оповргнути. Такође је потребно утврдити у ком облику је наведени порнографски садржај манифестован, да ли се ради о фотографијама (имиџима), аудио визуелним записима, као и начин на који је учињен доступним. То је неопходно и документовати прилозима са логова сервера односно рачунарског система. Такође,

---

ЗКП дошла у обзир за други и трећи облик у другом случају, а не за први и четврти, као и други у првом случају.

[7] Герке, М и др., Op.cit., стр.147.

[8] Амброз Паре је у XVI веку објавио уџбеник о акушерству у којем је до детаља описао начине на које жена себе може довести до сексуалног климакса. За ову књигу он је гоњен и претила му је смртна казна, а сама књига је забрањена. Никола Вене је публиковао 1675.год. илустрован рад у којем је веродостојно описао мушке и женске гениталије. Сви примерци овог рада су одузети и уништени од стране власти. Први судски поступак за растурање порнографије вођен је у Енглеској 1727.год. у којем је оптужени био (и осуђени) Едмунд Керл. Књиге за које је гоњен биле су под називима „Купидоново уље“, „Венера у манастиру“ итд. Кажњен је са 33 фунте и једну годину надзора.

[9] Која је специфично одређена у сврху потребе објашњавања овог кривичног дела – опет политички некоректно, али део је конвенције па је и даље у ширем оптицају, и подразумева сваки материјал који визуелно одсликава или описује дете (и малолетника) укључено у стварне или симуловане сексуално експлицитне радње или било које одсликавање (описивање) дечије полне органеза примарно сексуалне сврхе.

[10] Према старом решењу кривично-правном регулативом у Републици Србији малолетници изнад 14 година старости нису били обухваћени кривично правном заштитом. Такође, прибављање и поседовање материјала који представља дечију порнографију у рачунарском систему није било предвиђено као кажњиво. Иначе и Закон о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица у чл. 3. даје истоветне категоризације и поред тога посебно категоризује специфичну категорију млађих пунолетних лица до 21 године, на један специфичан начин их сврставајући тако у категорију лица на која се могу применити одредбе овог закона и тиме им дајући посебан положај у кривичноправном систему.

значајно је, на несумњив начин, утврдити везу лица са материјалом који је инкриминисан у овом кривичном делу. Посебно је важно истаћи чињеницу да се у случају овог кривичног дела ради о малолетним лицима што захтева посебну пажњу у поступању имајући у виду њихове године, специфично психофизичко стање и процес развоја и сазревања, било да се ради о малолетном лицу као извршиоцу кривичног дела или таквом лицу као оштећеном или сведоку[11]. Посебан проблем се може појавити у случајевима који би били парадоксални, код којих се као извршиоци и жртве јављају малолетници који су у вези, услед, одређених, ниских побуда. Посебно интересантан је случај тзв. секстинга[12]. У оваквим случајевима мора се водити рачуна о сврси кажњавања оваквог понашања као и ресоцијализационом смислу покретања вођења поступка и изрицања санкције[13]. Изузетно је у оквирима расветљавања дела, која имају конотацију присутну овом кривичном делу, значајна међународна полицијска сарадња. Видећемо да је у последње време интензивирана активност на остваривању сарадње у овим правцима[14].

Што се процесног дела тиче и поступка према лицима чије жртве су малолетна лица и деца он има својих специфичности. Веће, којим председава судија који је стекао посебна знања из области права детета и кривичноправне заштите малолетних лица, суди пунолетним учиниоцима следећих кривичних дела прописаних Кривичним закоником, ако је оштећени у кривичном поступку малолетно лице: Приказивање порнографског материјала и искоришћавање деце за порнографију (члан 185)[15]. Јавни тужилац који је стекао посебна знања из области

[11] Герке, М и др., Op.cit., стр.148

[12] Секстинг је кованица која означава слање, примање или прослеђивање сексуално експлицитне или сугерирајуће слике нагих или скоро нагих фотографија путем ММС или пушмејла (и и мејла) које оваквим путем сазнаје треће лице. Овај значајан моменат подразумева лица која су између себе разменила овакве фотографије а инкриминише се прослеђивање трећој особи. Ми би у таквом случају имали парадоксалну ситуацију у којој би кажњиво било и само размењивање ових порука између два малолетна лица. У овом смислу значајно је навести резултате истраживања Кокс Комуникација http://www.cox.com/takecharge/safe_teens_2009/media/2009_teen_survey_internet_and_wireless_safety.pdf последњи пут приступљено 01.09.2010.год. Према истом 65% секстера су мушкарци, а 35% девојчице, секстери ће најпрре бити старији малолетници 61% (16-18) насупрот 39% (13-16). У погелду употребе високотехнолошких средстава интересантно је да 81% малолетника поседује или користи мобилни телефон са приступом Интернету, а 89% поседује профил на некој социјалној мрежи.

[13] Мора се избећи кажњавање малолетника у оној мери којој би се на њихову ресоцијализацију могло утицати до те мере да она нема сврху, на пример изрицањем значајно дугих казни.

[14] Нарочито је интересантна декларација коју је 19.04.2010.год, усвојио европски парламент којом се позива на стварање Система раног упозоравања у области дечије порнографије. За више о овоме видети на: http://www.smile29.eu/doc/DS29_EN. pdf Такође је значајно поменути и да у оквирима ИНТЕРПОЛ – а постоје базе података са фотографијама познате и непознате злостављање деце, као и база података – црне листе сајтова на којима се размењују порно садржаји са децом као субјектима на тим садржајима.

[15] Поред описаног дела у питању су и: Тешко убиство (члан 114); Навођење на самоубиство и помагање у самоубиству (члан 119); Тешка телесна повреда (члан 121);Отмица (члан 134); Силовање (члан 178); Обљуба над немоћним лицем (члан 179); Обљуба са дететом (члан 180); Обљуба злоупотребом положаја (члан 181); Недозвољене полне радње (члан 182); Подвођење и омогућавање вршења полног односа (члан 183); Посредовање у вршењу проституције (члан 184); ; Ванбрачна заједница са малолетником (члан 190); Одузимање малолетног лица (члан 191); Промена породичног стања (члан 192); Запуштање и злостављање малолетног лица (члан 193.); Насиље у

права детета и кривичноправне заштите малолетних лица покреће и поступак против пунолетних учинилаца других кривичних дела прописаних Кривичним закоником, сагласно одредбама овог дела закона, ако оцени да је то потребно ради посебне заштите личности малолетних лица као оштећених у кривичном поступку. Кривични поступак против окривљених за описана кривична дела спроводи се према одредбама Законика о кривичном поступку. Истрагу спроводи истражни судија који је стекао посебна знања из области права детета и кривичноправне заштите малолетних лица. У истрази кривичних дела на штету малолетних лица учествују специјализовани службеници органа унутрашњих послова који су стекли посебна знања из области права детета и кривичноправне заштите малолетних лица, кад се поједине радње поверавају овим органима.

Кад воде поступак за кривична дела учињена на штету малолетних лица, јавни тужилац, истражни судија и судије у већу ће се односити према оштећеном водећи рачуна о његовом узрасту, својствима личности, образовању и приликама у којима живи, посебно настојећи да се избегну могуће штетне последице поступка по његову личност и развој. Саслушање малолетних лица обавиће се уз помоћ психолога, педагога или другог стручног лица.

Ако се као сведок саслушава малолетно лице које је оштећено кривичним делом наведеним у члану 150. ЗОМ, саслушање се може спровести највише два пута, а изузетно и више пута ако је то неопходно ради остварења сврхе кривичног поступка[16]. У случају да се малолетно лице саслушава више од два пута, судија је дужан да посебно води рачуна о заштити личности и развоја малолетног лица.

породици (члан 194); Недавање издржавања (члан 195); Родоскрвњење (члан 197); Разбојничка крађа (члан 205); Разбојништво (члан 206); Изнуда (члан 214); Омогућавање уживања опојних дрога (члан 247); Ратни злочин против цивилног становништва (члан 372); Трговина људима (члан 388);Трговина децом ради усвојења (члан 389); Заснивање ропског односа и превоз лица у ропском односу (члан 390).

[16] Предлог новог Законика о кривичном поступку уводи нову категорију *Посебно осетљивог сведока.* Материјални услов за одређивање статуса посебно осетљивог сведока може се поделити на два подсистема. Први представљају одређене особине саме личности сведока, док се други односи на специфичности извршеног кривичног дела. Наиме, године живота сведока, његово искуство које је стекао у животу, начин на који је живео до вермена када је извршено кривично дело, родна одређеност и здравствено стање могу утицати на то да се таквом сведоку додели статус посебно осетљивог сведока. Уз то се додају и специфичности кривичног дела које је извршено а под којима се подразумева природа дела, начин на који је извршено као и последице које су настале услед извршења кривичног дела. Не треба занемарити и друге околности које су карактеристичне за сваки конкретан случај. Управо ови елементи – материјалног услова од великог значаја су за тактику обезбеђења личних доказа, те је ова категорија самим увођењем у законодавство допринела у приступу државних органа овој категорији сведока, а са друге стране, узимање исказа од оваквих категорија сведока подигло на виши ниво. Формални услов: за добијање наведеног статуса неопходна је иницијатива односно захтев, који могу органу који води поступак поднети странке или сам сведок. Такође, орган поступка може по службеној дужности сведоку одредити статус посебно осетљивог сведока. Орган који води поступак може донети решење којим се одређује постављање пуномоћника посебно осетљивом сведоку ако оцени да је то неопходно како би се заштитио његов интерес. У том случају јавни тужилац или председник суда у обавези је да постави пуномоћника сходно редоследу списка адвоката достављеног суду од стране надлежне адвокатске коморе за одређивање бранилаца по службеној дужности. *Испитивање посебно осетљивог сведока* Испитивање посебно осетљивог сведока може се спровести искључиво посредстом органа који води поступак, што ће рећи – суда. Том приликом, орган који води поступак мора посебно водити рачуна о пажљивом односу према сведоку са тежњом да у сваком случају не наступе потенцијалне

Уколико, с обзиром на особености кривичног дела и својства личности малолетног лица, оцени да је то потребно, судија ће наредити да се малолетно лице саслушава употребом техничких средстава за пренос слике и звука, а саслушање се спроводи без присуства странака и других учесника поступка, у просторији у којој се сведок налази, тако да му странке, и лица која на то имају право, питања постављају посредством судије, психолога, педагога, социјалног радника или другог стручног лица.

Малолетна лица, као сведоци-оштећени, могу се саслушати и у свом стану или другој просторији, односно овлашћеној установи-организацији, стручно оспособљеној за испитивање малолетних лица. При испитивању сведока-оштећеног, државни органи могу наредити примену мере саслушања употребом видео линка.

Када је малолетно лице саслушавано у претходно поменутим случајевима, на главном претресу ће се увек прочитати записник о његовом исказу, односно пустити снимак саслушања.

последице кривичног поступка, које негативно могу утицати на личност сведока као и његово телесно или душевно стање. Ако орган који води поступак тако одлучи, за потребе испитивање сведока може бити затражена стручна помоћ психолога или социјалног радника као и другог стручног лица. У овом смислу стручна помоћ има сврху олакшања давања исказа како сведоку тако и узимања исказа суду, дакле, двосмерну.

Посебна категорија сведока су деца, која могу да буду сведоци и сведоци – оштећени, код којих постоји могућност конфабулације, хипертрофије догађаја и других девијација. Управо због тога је и неопходна стручна помоћ приликом испитивања ове категорије сведока.

Посебно осетљив сведок се може испитати и помоћу посебних аудио видео техничких средстава који служе за пренос слике и звука. Спровођењем такве одлуке органа који води поступак, сведок се испитује док се налази у сам просторији без присуства странака и других учесника у поступку. Иако овакве околности олакшавају поступак саслушања резултат у криминалистичком смислу није у потпуности адекватан. Наиме, давање исказа овим путем лишава нас директног контакта ин виво са лицем које одговара на питања или неометано излаже, није могуће у криминалистичком смислу (или шта више у форензичком – смислу форензичког интервјуа) видети сваки покрет лица, сваку његову микроекспресију, могуће илустраторе или амблеме покрета и сл. Додуше, могуће је овакав исказ снимити аудио – видео техником, што је у овом случају лакше, а што омогућава и каснију обраду оваквог материјала, увећавање делова и регистровање делова исказа и неких од побројаних елемената форензичког интервјуа, нпр. микроекспресије. Ово би изискивало да суд накнадно поново прегледа овакве материјале и тада их додатно анализира, али обзиром на оптерећеност судова, то је ипак у домену фантастике.

Посебно осетљиви сведок може се испитати и у свом стану или другој просторији односно у овлашћеној институцији која је стручно оспособљена за испитивање посебно осетљивих лица. У том случају може се такође донети одлука од стране органа надлежног за вођење поступка о употреби поменутих техничких средстава, но и у овом случају постоји слична проблематика горе описаној.

Оно што је веома важно за заштиту личности посебно осетљивог сведока је чињеница да он не може бити суочен са окривљеним, осим у случају да то сам захтева. То је веома важна мера превенције секундарне виктимизације жртава, нарочито, када су у питању кривична дела против полне слободе, против човечности и других добара заштићених међународним правом, али и друга тешка кривична дела.

Изузетно је битно напоменути да у случају доношења решења од стране органа који води поступак којим се одлучује о ангажовању при испитивању посебно осетљивог сведока лица са посебним стручним квалификацијама или коришћењу посебних техничких средстава или одређивању околности које се односе на место испитивања сведока, жалба није дозвољена.

Ако се као сведок саслушава малолетно лице које је услед природе кривичног дела, последица или других околности, посебно осетљиво, односно налази се у посебно тешком душевном стању, забрањено је вршити суочење између њега и окривљеног.

Малолетно лице као оштећени мора имати пуномоћника од првог саслушања окривљеног. У случају да малолетно лице нема пуномоћника, њега ће решењем из реда адвоката који су стекли посебна знања из области права детета и кривичноправне заштите малолетних лица поставити председник суда. Трошкови заступања падају на терет буџетских средстава суда.

Ако препознавање окривљеног врши оштећено малолетно лице, суд ће поступати посебно обазриво, а такво препознавање ће се, у свим фазама поступка, вршити на начин који у потпуности онемогућава да окривљени види ово лице. Кривични поступак за кривична дела из члана 150. ЗОМ је хитан.

1.2 Навођење малолетног лица на присуствовање полним радњама

Законодавац прописује основни облик на следећи начин: „Ко наведе малолетника да присуствује силовању, обљуби или са њом изједначеним чином или другој полној радњи, (затвор од шест месеци до пет година и новчана казна).“ [17] Дакле радња је навођење на присуствовање – што подразумева наговарање, неке облике психичке сугестије одређеног лица према малолетнику у сврху његовог навођења на присуствовање одређеном догађају (слиовању, обљуби или изједначеном чину, као и другој полној радњи). Дакле, могуће је и да, приликом вршења, на пример, кривичног дела недозвољених полних радњи присутно дете и малолетник квалификује постојање овог кривичног дела поред првог. Ставом 2. одређује се тежи облик: уколико је дело учињено употребом силе или претње, или према детету, (затвор од једне до осам година). Овде је квалификујућа околност кривичног дела употреба силе или претње, дакле и могућност постојања психичке принуде према малолетнику као средство извршења кривичног дела. Извршилац овог кривичног дела може бити свако лице, али, по природи ствари, посебну тежину носи околност уколико је у питању лице које је у сродничком односу са малолетником. Радња кривичног дела свршена је самим присуствовањем оваквом чину малолетног лица. Посебан случај овде везан је за ситуацију „посредног присуства“ када се путем Интернет конекције оваква активност прикаже малолетнику или детету. Код доказивања ових кривичних дела значајна пажња мора се усмерити на постојање доказа о сексуалним радњама којима је малолетник присуствовао, као и о траговима који се могу повезати са његовим праћењем таквог материјала. Овакви трагови у случајевима аудио визуелних записа остају на рачунару малолетника и серверима, посредством којих су приказивани, када је у питању ВТК. Из тог разлога је јако значајно спровести увиђај апсолутно поштујући правила lege artis, а такође и прегледање и претресање рачунара и података похрањених у њима. Питање радње навођења малолетника у датом случају мора

[17] Законом о изменама и допунама Кривичног законика од 31.08.2009. године у члану 55. Закона о изменама и допунама Кривичног законика После члана 185. додати су и члан 185а и 185б.

бити, такође, недвосмислено утврђено, обзиром да представља квалификаторну околност па је неопходно добровољно присуствовање од принудног присуствовања и утврдити ниво, начин и степен навођења на присуствовање, односно начин и средства принуде. Нарочито је интересантан случај постојања порнографских сајтова на којима постоје ограничења за малолетна лица, а који немају никаквих других заштита, осим постављања питања старости посетиоца, а које је веома лако заобићи.

1.3 Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу

Први основни облик гласи: „Ко у намери извршења кривичног дела из чл. 178. став 4 (кривично дело „Силовање“)[18], 179. став 3 (кривично дело „Обљуба над немоћним лицем“), 180. ст. 1. и 2 (Обљуба са дететом), 181. ст. 2. и 3 (кривично дело „Обљуба злоупотребом положаја), 182. став 1 (кривично дело „Недозвољене полне радње“), 183. став 2 (кривично дело „Подвођење и омогућавање полног односа“), 184. став 3 (кривично дело „Посредовање у вршењу проституције“), 185. став 2. и 185а овог законика, користећи рачунарску мрежу или комуникацију другим техничким средствима договори са малолетником састанак и појави се на договореном месту ради састанка, казниће се затвором од шест месеци до пет година и новчаном казном. Ставом 2 прописује се и тежи облик: „Ко дело из става 1. овог члана изврши према детету, казниће се затвором од једне до осам година.”

Чланом 185б. санкционисано је искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу или детету. Данас радња овог кривичног дела подразумева постојање намере извршиоца да коришћењем рачунарске мреже или комуникација другим техничким средствима договори састанак[19] са малолетником, и да се појави на договореном месту ради састанка. У оквиру борбе против ВТК најинтензивнија сарадња у последње време везана је за ова кривична дела[20].

---

[18] У току 2009. године догодио се и један случај у коме је пунолетно лице, које је, представљајући се као малолетник од 17 година, контактирало са малолетним лицем (старости 13 година) преко социјалне мреже *Facebook* и, након тога, извршило над тим лицем кривично дело силовања из чл.178. КЗ РС

[19] Познат је случај из фебруара 2009. године када је Александар Нешковић (43) ухапшен због сумње да је сексуално злостављао малолетну девојчицу коју је пре тога намамио лажно се представљајући на Интернету као шеснаестогодишњи Филип. Приликом његовог хапшења, полиција је у његовој кући пронашла лаптоп и мобилни телефон са више од 100 фотографија малолетних лица оба пола. www.facebooksrbija.com/uhapsen-pedofil-sa-fejsbuka/informacije/135.html, доступно 10.01.2010.год.

[20] Компанија *Landslide* бавила се израдом и одржавањем Интернет портала чије услуге су се плаћале кредитним картицама. Априла 1999. године, поштански службеници су пријавили полицији случај у којем се преко овог сајта рекламира дечија порнографија. Овлашћена службена лица су у сарадњи са стручњацима из Мајкрософта приступили садржају Интернет портала и открили знатку количину дечије порнографије до које се могло приступити плаћањем преко кредитне картице компанији *Landslide.* Августа исте године, заплењен је сав материјал и ухапшени су њени власници

У борби против Интернет педофилије ангажован је велики број људи, постоје посебне полицијске јединице које периодично откривају извршиоце ових кривичних и њихове организације. Бројна удружења грађана се баве овим проблемом и помажу жртвама, а често и сами хакери помажу државним органима у откривању оваквих група. У супротстављању овој појави неопходно је организовати веома широк фронт са учешћем свих релевантних актера у најразличитијим улогама, једино то може дати адекватан резултат[21]. Током 2008. године у САД су три велика Интернет провајдера Sprint Nextel, Time Warner Cable i Verizon, постигли договор о блокирању приступа сајтовима са дечијом

Томас и Џенис Риди. Јануара 2000. године Томас Риди бива проглашен кривим за дистрибуцију дечије порнографије и осуђен на укупно 1335 година казне затвора која је након уложене жалбе смањена на 180 година. Џенис Риди је осуђена на 14 година. Приликом истраге, Томасу Риду је наложено да остави активан портал компаније како би се он искористио у даљој истрази против дечије порнографије. Августа 2001. информације прикупљене из компаније *Landslide* искоришћени су за покретање операције „Лавина“. Подаци о начину рада Интернет портала као и о корисницима који су плаћали кредитним картицама услуге и преко електронске поште поручивали дечји порнографски материјал, користили су за постављање Интернет клопки са циљем да се прикупе докази против *Landslide* корисника. Као резултат, ухапшено је преко 1000 осумњичених лица кроз 144 истраге спроведене у 37 држава унутар САД-а. Дубља истрага је довела и до лица ван територије САД-а. ФБИ је својим страним колегама проследио те информације, које су поред осталог чинила имена 7272 лица у Великој Британији и 2329 у Канади. Даље истраге су довеле до нових хапшења широм света. Операција „Руда“ (енг. *Operation Ore*), је, такође, повезана са истрагом против компаније *Landslide*. Операцију је спровела Британска полиција на основу информација које су проистекле операцијом „Лавина“. Примењене су сличне методе, а резултат је био драматичан: 7250 осумњичених лица, 4283 претраге домова осумњичених, 3744 ухапшених, 1848 оптужених, 1451 признања, 493 изречене опомене, 879 истрага проистеклих новим информацијама, 140 деце склоњено из сумњивих и опасних ситуација и на крају, чак 39 самоубистава. Иако је операција „Руда“ открила значајан број педофила, дистрибутера и корисника дечије порнографије, касније се испоставило да је било доста пропуста у истрагама које су резултирале погрешним оптужбама и растуреним породицама. Највећи пропуст је био што нису детаљно проверене информације до којих се дошло преко кредитних картица које су коришћене у плаћању преко Интернета. Испоставило се да је већи број тих картица украден, као и да њихова употреба није водила до дечије порнографије већ до неких других, безазлених садржаја. Више о овоме у Ћировић, Д. Јанковић, Н. Лађевић, М. „Cyber podzemlje u Srbiji“, *Репортер,* 16.11.2005. страна 12.

[21] Амерички служба FBI (*Federal Biro of Investigation Eng.*), на основу података о мрежи Интернет педофила у САД, коју је открило Одељење за борбу против високотехнолошког криминала Министарства унутрашњих послова Републике Србије, поднело је кривичну пријаву против свештеника - педофила из америчке државе Њу Џерси. Правосудни органи САД су прихватили оперативни полицијски материјал о мрежи педофила коју је доставио МУП Републике Србије. У фебруару 2009. године МУП РС започео је сопствену истрагу, која је довела до хапшења осумњиченог. Откривено је да ово лице своје активности обављало у оквиру неколико педофилских група, као и да је имао регистровано неколико лажних налога електронске поште и налога у тзв. „собама за четовање“, да се на Интернету лажно представљао као 13 - годишња девојчица или као женска особа и мајка од 25 година. Приликом претресања његове куће, пронађен је педофилски материјал на чије је постојање указивао МУП Србије, као и други докази. Овде се мора указати и на чињеницу да се у актуелном КЗ дефинитивно не садржи кривично дело крађе идентитета а које је изузетно неопходно у актуелним околностима у свету, а да је лажно представљање предвиђено чл.329. КЗ потпуно анахроно. Анахроност долази од субјеката који су предмет овог кривичног дела – службена лица и војна лица.

порнографијом и улагању суме од 1,1 милиона долара ради проналажења и брисања са мреже педофилских материјала[22].

Према наводима групе аутора „Тужилаштво интензивно сарађује и са међународним организацијама у циљу сузбијања дечије порнографије и откривања извршилаца ових кривичних дела. Установљена је интензивна сарадња са Националним централним бироом (НЦБ) ИНТЕРПОЛА у Београду, на основу чијих обавештења су преко активности других организационих јединица МУП РС, откривани корисници Интернета у Србији а преко чијих рачунара и коришћених ИП адреса[23] је вршено преузимање и размена педофилских материјала. Тако је у оквиру операција „Мађ“, „Муосис“ и „Дуга“ идентификовано више лица која су се бавила овом врстом криминалних активности“[24]. Логичан наставак ових акција је спровођење акције под називом „Армагедон“, истог типа.

Извршиоци кривичних дела данас радије користе причаонице (енгл. chat room), новинске групе (енгл. newsgroup) и друге услуге различитих Интернет сервиса, посебно у околностима све значајнијих web 2.0 апликација, него што жртве траже на местима као што су школе или дечија игралишта. Посебно је

[22] “Three US ISPs agree to block child pornography sites”, Tech Connect Magazine, Internet, http://www.tcmagazine.info/comments.php?id=20354&catid=6&highlight=child+pornography, 7.05.2009. О оваквим активностима постоје иницијативе и у ЕУ, али је исто тако гласна и иницијатива за заштиту у таквим случајевима људских права прописаних Европском конвенцијом о људским правима, конкретно чл. 8. 9 и 10. Конвенције и то : права на заштиту приватног живота и слободе мисли, савести и вероисповести односно слободе изражавања. такође овде се имплицира и право лица која су инвалиди на приступ садржајима које једино могу примити, или путем којих једино могу остварити комуникацију.

[23] IP (интернет протокол) (енгл. *Internet Protocol*) Техничка протокол адреса рачунара у мрежној комуникацији, то је протокол трећег слоја ОСИ референтног модела (слоја мреже). Садржи информације о *адресирању*, чиме се постиже да сваки мрежни уређај (рачунар, сервер, радна станица, интерфејс рутера) који је повезан на интернет има јединствену адресу и може се лако идентификовати у целој интернет мрежи, а исто тако садржи контролне информације које омогућују пакетима да буду прослеђени (рутирани) на основу познатих IP адреса. Овај протокол је документован у RFC 791 и представља са TCP протоколом језгро интернет протокола, TCP/IP стек протокола (енгл. *Transmission Control Protocol/Internet Protocol*). Више о томе на: http://sr.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB последњи пут приступљено 04.09.2011.год.

[24] Комлен Николић, Л. и др. *Op.cit.*. стр, До сада су пред Окружним судом (Вишим судом – од 2010.год.) у Београду вођени поступци против извршилаца овог кривичног дела, а ова лица су осуђивана на вишегодишње затворске казне. Тако је неправоснажном пресудом К бр. 1930/05 осуђен ЈС на казну затвора у трајању од дванаест година затвора због четири кривична дела Искоришћавање малолетних лица за порнографију из чл. 111а. ст. 2 у вези ст. 1 КЗ РС у стицају са кривичним делом Обљуба или противприродни блуд са лицем које није навршило 14 година из чл. 106 ст. 1 КЗ РС. Ово лице је преко Интернета растурало фотографске снимке малолетних лица порнографског садржаја која нису навршила 14 година, мушког и женског пола као и беба на којима је приказано вршење обљубе, сексуалног злостављања и противприродног блуда, али и 211 фотографија коју је сам сачинио док је злостављао малолетну девојчицу, Други, не тако драстичан пример је неправоснажна пресуда К бр, 1207/05 којом је БН осуђен на три године затвора, јер је у временском периоду између 12.3.2005. године и 18.6.2005. године у Београду, у два наврата продао и покушао да прода фотографске, филмске и друге снимке малолетних лица порнографског садржаја која нису навршила 14 година, тако што је преко Интернета оглашавао продају оваквог материјала преко Интернета, а затим ступао у контакт са саинтересованим лицима и уговарао продају по цени од 100 до 150 евра

значајно указати и на околност да малолетници, деца и њихови родитељи осетно доприносе оваквој ситуацији. У Истраживању Кокс комуникација[25] указано је да се од скоро хиљаду испитаних тинејџера, њих 58% се, у последњих месец дана, упустило у ажурирање својих профила у социјалним мрежама, а 63% је поставило своју приватну фотографију или видео запис[26] на социјалној мрежи. Извршиоци кривичних дела користе то што на Интернету могу сексуално да узнемиравају децу у условима који им гарантују висок ниво анонимности али и приступачности младима. Користећи предности савремених информационих технологија они на различитим Интернет сервисима креирају већи број профила помоћу којих задобијају поверење деце, без физичког контакта, а затим сексуално узнемиравају и на различите начине увлаче у своје замке.

Једна од највећих опасности које прете деци када се налазе у On-Line простору на Интернету јесу тзв. „причаонице“[27] (Engl. Chat Room). Овакав вид комуникације одвија се текстуалним порукама преко ИРЦ (IRC) сервиса (Engl. Internet Relay Chat) који функционишу на тај начин што се више сервера међусобно повезује ради размене текстуалних порука или се врши Web базирана размена текстуалних порука. IRC сервиси омогућују истовремену размену текстуалних порука и зато су веома популарни, посебно међу малолетницима. Деца и малолетници користе услуге ових сервиса како би се упознали са новим пријатељима или размењивали поруке са већ постојећим познаницима. Ови сервиси представљају неку врсту „психичког игралишта“, „шопинг центра“ или „кафића“ где деца и млади размењују поруке различите природе, од оних везаних за израду домаћих задатака до оних везаних за забављање, моду и сл. Посебно је значајно да у условима све популарније примене web 2.0 апликација у социјалним мрежама и ово постају стандардне и неизбежне апликације ових окружења. Психологија размене интимних информација[28] са потпуним странцима је заступљена и овде. Иако су многи Интернет сервиси ове врсте конципирани тако да се на њима врши мониторинг, од стране модератора[29], у причаоницама, ради искључивања, између осталог, могућности да деца буду угрожена наведеним радњама, на многима од њих оваква заштита није довољно ефикасна или уопште и не постоји. Ово је неопходно посебно посебно образложити у окружењу социјалних мрежа, наиме тамо оваквих администратора у чету – причаоници, нема. Очекује се да корисници сами одређују свој круг пријатеља и целокупна

[25] Доступно на: http://www.cox.com/takecharge/safe_teens_2009/media/2009_teen_survey_internet_and_wireless_safety.pdf последњи пут приступљено 01.09.2010.год.

[26] У истраживању се ишло и даље, давањем структуре података који су објављени на социјалним мрежама: 4% испитаника објавило је адресу, 9% места на која често излазе, 14% број мобилног телефона, 14% веома личних видео записа, 15% видео записе пријатеља, 41% град у којем живе, 45% назив школе коју похађају, 49% фотографије пријатеља и 62% испитаника је објавило неке фотографије којима откривају своје лице у одређеном обиму.

[27] Виртуелни простори у којима се може пријављивати под псеудонимом, без страха да се учесницима у комуникацији (текстуалној, али савремени сервиси нуде најразличитије облике комуникације, обједињујући до сада невиђене) открије стваран идентитет у тренутку комуникације.

[28] Феномен је веома специфичан, просто је, много лакше, поверити се потпуном странцу, ово је, често, могуће за одрасле, а посебно специфично за малолетнике и децу.

[29] Лица које представља „надзорно тело“ у оваквом окружењу.

концепција се заснива на пристанку корисника, чак и вери у истинитост изјава које корисници дају. Ово последње веома је значајно за присуп корисника социјалној мрежи где се од корисника тражи да буде искрен приликом постављања профила а да за тако нешто нема довољно адекватне провере.

Преко Интернет сервиса педофили траже рањиву децу како би задобили њихово поверење и сексуално их узнемиравали, или како би са њима касније ступили у физички контакт ради вршења кривичних дела. На сервисима причаоница (chat room) одрасла особа може да успостави директан контакт да дететом, које већ учествује у комуникацији са осталим члановима, тако што ће се лажно представити као дете које има одређена интересовања и након тога чекати да оствари контакт са дететом супротног пола, сличног интересовања и др[30]. Као што је речено, он ће највероватније направити неколицину профила и користити сваки чак и за намаљивање малолетника

Однос између приступа информацијама и идентификације читача може се искористити за описивање начина на који педофили уређују Интернет приступ својим збиркама, уједно и за доказивање кривичног дела у погледу физичког присуства одређених фотографија и видео записа. Највећи проблем у овим случајевима је установљавање везе између извршиоца, датог рачунара и одређених материјала.

Власници информација су заинтересовани за контролисање приступа приватном материјалу. Иако се може прихватити да неидентификовани читалац приступи информацијама које су приступачне широј јавности, неидентификовани приступ приватним информацијама не би био прихватљив. Педофили су обезбеђивали Интернет приступ својим колекцијама употребом[31]:

- неидентификованог отвореног приступа: конструисањем WWW страница без "логовања" посетиоца и дистрибуцијом информација Интернет групама којима се може приступити путем јавних сервера;
- идентификованог отвореног приступа: конструисањем WWW страница или FTP сајтова са могућношћу "логовања" читаоца;
- ограниченог приступа: конструисањем WWW страница или FTP сајтова са лозинкама које су дистрибуиране у оквиру ИРЦ и дистрибуцијом информација групама којима се могло приступити само путем сервиса који су вршили контролу приступа;
- овлашћеног приступа: конструисањем WWW страница или FTP сајтова са приступом идентификованом кориснику и саопштавањем локација сајтова појединцима путем електронске поште или ИРЦ коришћењем техника енкрипције;
- неовлашћеног приступа: претпостављало се да је онемогућен. Иако није примећен неовлашћени приступ, примећене су многе поруке и линкови у оквиру ИРЦ који пружају савете о обезбеђењу фајлова. Сматра се да педофили штите своје збирке коришћењем процеса енкрипције и стратегија релокације (на пример, чувањем осетљивих материјала на забаченим Интернет локацијама,

[30] O'Connell, R.: A typology of cybersexploitation and on-line grooming practices, Cyberspace Research Unit, University of Central Lancashire, Велика Британија, 2003, стр.4.

[31] Forde P. и Patterson A. Трендови & проблеми у криминалу и кривичном правосуђу, Криминолошки институт Аустралије, бр.97. новембар 1998. issn 0817-8542, isbn 0 642 24082 5 стр.7.

посебно је интересантно размотрити заштиту специфичних оперативних система нпр. иОС, везани за ифон и ипед – Iphone, Ipad научници су доказали да је ове системе веома лако „отворити“[32]).

У Републици Србији постоји више оваквих сервиса а говорно подручје бивших југословенских република, због сличности језика, такође је створило он лајн (*On-line)* простор на Интернету где су деца са територије Републике Србије у опасности да постану жртве сексуалног узнемиравања.

На неколико Интернет сервиса где се може приступити ИРЦ каналима у оквиру којих се користи српски језик, користећи корисничка имена из којих се може наслутити да се ради о деци до 12 до 14 година старости (навођењем надимка и године рођења или старосне доби) у временском раздобљу од 2 часа дневно у периоду од 5 дана праћена је комуникација лица која су се, различитим надимцима, јављала ради успостављања контакта. У циљу истраживања појаве покушали смо спровођење контролисаног ограниченог криминалистичког експеримента[33]. Опсервациони процес је био ограничен на Интернет странице на којима се користи српски језик, у оквиру тог подручја коришћена су само она средства која су у широј употреби (претраживачи, читачи, итд.), коришћено је реално Интернет окружење приступачно јавности. Намера је била да се опсервира јавна активност педофила. Коришћен је Интернет сајт са контролисаним приступом ИРЦ једног српског провајдера (назив из разумљивих разлога није објављен). Само су сервери са приступом широј јавности коришћени за опсервацију група.

За сврхе ове опсервације педофилски материјал и педофилска активност је дефинисана као материјал који се налази на Интернет страницама који сам прокламује емоционални или сексуални интерес за децу (на пример, фотографије или видео стриминг или видео клипови) а педофилска активност је одређена као било какво навођење на опсцене или ласцивне комуникације очигледно малолетног лица или детета (на пример навођењем погрдних речи и сл.). У том контексту, педофили су дефинисани као лица повезана са педофилским материјалима.

Изабрани су неутрални ИРЦ канали, без одређених тема тј. „универзални“ канали[34]. Праћено је на који ће начин и колико ће ових лица покушати да врши сексуално узнемиравање деце након што им буде саопштен узраст детета, и након

---

[32] У питању су веома проблематични елементи и слабости овог система ова и друге информације шире се могу пронаћи на: http://www.sit.fraunhofer.de/Images/sc_iPhone%20Passwords_tcm501-80443.pdf последњи пут приступљено 10.02.2011.год.а додатне расправе се могу наћи и на: http://www.net-security.org/secworld.php?id=10570&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29 последњи пут приступљено истог дана.

[33] Према професору Симоновићу, у Криминалистици на стр.327. – Криминалистички (истражни) експеримент. – Криминалистички (истражни) експеримент представља свесно, планско и вишекратно варирање нових околности приликом њиховог увођења у спорни чињенични склоп испитиваног кривичног догађаја како би се утврдили услови, узроци, механизам развоја кривичног догађаја као и закономерности настанка последица и трагова с циљем провере постојећих и прибављања нових доказа. Увођењем нових околности у чињенични склоп утврђују се последице које оне производе и на основу тога доносе релевантни закључци о испитиваном догађају.

[34] У питању су канали који се постављају са намером за слободно разговарање (испразне разговоре) „читчетовање“, зато се и постављају без теме.

што сами кажу које је њихово годиште. Спроведеном анализом утврђено је да на ИРЦ каналима у Републици Србији постоји одређени број корисника старосне доби од 18 година до 36 година, који, и поред очигледне напомене да се ради о малолетном саговорнику-детету узраста од 11 до 14 година, настављају даљу комуникацију чија садржина, недвосмислено и очигледно, представља сексуално узнемиравање детета.

У периоду од 2006. до 2010. године од стране различитих полицијских служби широм територије Републике Србије откривено је више случајева кривичних дела из чл. 185. под називом „Приказивање порнографског материјала и искоришћавање деце за порнографију“ у оквиру којих је Интернет служио као средство за дистрибуцију недозвољене садржине или као средство за комуникацију са децом. У једном од ових случајева материјал чија је садржина материјал који садржи облике дечије порнографије, од стране извршиоца кривичног дела размењиван је са страним држављанима, док се у другим случајевима радило о постављању и чињењу доступним садржаја који представља дечију порнографију на серверима Интернет страница, које су се налазиле на територији Републике Србије.

Значајна штета као резултат злоупотребе савремених информационих технологија јавља се услед великог броја начина извршења таквих злоупотреба. Ове злоупотребе могу да се састоје од једне активности или их, у исто време, може бити и више[35]. Многа деца и малолетници сматрају сервисе причаоница (*chat room)* на Интернету местом на ком се могу слободно изражавати, без бојазни од родитељског надзора и забрана[36]. Повећавање броја социјалних мрежа на Интернету омогућило је људима лакшу међусобну комуникацију, посебно уколико имају иста интересовања. Поред тога што омогућавају креирање различитих садржаја и размену новости и информација, они пружају и могућност за стварање штетног и незаконитог садржаја, и одраслим људима пружају могућност да дођу у контакт са адолесцентима и децом, да задобију њихово поверење како би их злостављали[37]. За описане активности није неопходно да и физички дође до злостављања деце, ово је нарочито својствено web 2.0 апликацијама а, посебно, социјалним мрежама. Обзиром на савремено сексуално понашање малолетника, довољно је да неки педофил постане пријатељ малолетнику на социјалној мрежи, након чега му се отвара велики број употребљивих фотографија, за њихове карактеристичне збирке. Веома значајна је и околност да у случајевима клауд компјутинга можемо препознати нове проблеме у овој области, наиме извршилац се може сакрити иза неког од псеудонима (и иза тога спуфовати своју ИП адресу или на друге сличне начине прикрити свој идентитет), и похрањивати најразличитије материјале на некој локацији у оквирима клауд компјутинга. Такође, у једном перфектном правном систему у којем се захтева да се контактира

[35] Quayle E., Loof, L. Palmer, T.: Child pornography and sexual exploitation of children online, ECPAT International, ECPAT International, Тајланд, 2009, p. 43.

[36] Dixon, N.: „Catching ‘Cyber Predators’: the Sexual Offences (Protection of Children) Amendment Bill 2002 (Qld)“, Research Brief No 2002/35, Queensland Parliamentary Library, Аустралија, 2002, p. 3.

[37] Quayle E., Loof, L. Palmer, T.:Op.cit., p. 9.

одређени власник датог материјала и упозорава на његов нелегитиман садржај, те се од њега тражи да га повуче са исте локације ово може бити проблем[38].

Лица која користе ове сервисе на Интернету имају корисничка имена, тј. надимке, којима се међусобно препознају у комуникацији и, на основу тога, позивају на разговор. Дете које се осећа несигурно, које сматра да није довољно интересантно свом окружењу или је одбачено од стране својих вршњака, или има проблеме са родитељима (а што може бити опис сваког тинејџера), може да уђе у комуникацију на овом Интернет сервису. То ће моћи урадити без бриге да ће бити откривено, под окриљем надимка који му омогућава да представе себе онако како то он, или она, жели. Лица која сексуално узнемиравају децу на овим сервисима, након што открију да је дете рањиво или да је раније било злостављано, користе његов страх и, често, користе претње – како би успоставили и држали контролу над њим, а затим континуирано вршили узнемиравање или, у најгорим случајевима, континуирано физичко злостављање над дететом уколико су успели да ступе са њим у контакт. Неки малолетници који имају проблеме, често се и заљубљују у лик који на оваквим сервисима формирају педофили (нпр. романтични студент или ученик који жели да им помогне) и одају своје најинтимније жеље и тајне којима педофила доводе у супериоран положај и омогућавају му да након што прикупи детаље о њиховом животу, исте користи вршећи уцене ради задовољавања својих потреба. Не треба заборавити да их у неким земљама карактеришу као сексуалне предаторе, што само појачава конотацију коју желимо да прикажемо. Интернет је повећао проблеме везане за дечију порнографију због све веће количине илегалног материјала, све лакше дистрибуције и лакоће приступа таквом материјалу[39]. ИРЦ канали су још једно у низу средстава које педофили користе како би дошли у контакт са децом ради сексуалног узнемиравања и вршења других кривичних дела.

Анализом неколико профила који су отворени на овим Интернет сервисима (из чијих се назива јасно може наслутити да се ради о деци због начина на који су креирани пошто се састоје од имена и годишта рођења или имена и узраста) који су отварани на ИРЦ каналима у Републици Србији (који су у посматраном периоду имали од 600 до 1000 корисника), утврђено је да педофили користе наведене техничке могућности како би тражили рањиву децу у *On line* простору, укључујући ту и децу која имају недостатак самопоуздања везаног за физички изглед или друштвене односе[40]. Овим профилима они су навођени да помисле да комуницирају са децом узраста од 11 до 14 година која имају проблеме у комуникацији са родитељима и случајни су посетиоци ИРЦ канала.

---

[38] У датом случају у Француској где се захтева реаговање на овакав начин дошло је до првобитне погрешне примене закона по којој је хост фирма за одређени облик клауд компјутинга кажњавана за оно што постују њени клијенти. Овако погрешну примену закона констатовао је Касациони суд у Француској и укинуо дату пресуду. Више о овоме на адреси: http://www.01net.com/www.01net.com/editorial/528466/dailymotion-et-fuzz-reconnus-hebergeurs-par-la-cour-de-cassation/ последњи пут приступљено 25.02.2011.год.

[39] Wortley, R. Smallbone, S.: Child Pornography on the Internet, Problem-Oriented Guides for Police Problem Specific Guides Series No. 41, U.S. Department of Justice-Office of Community Oriented Policing Services, САД, 2006., p. 9.

[40] Експеримент који је спроведен од стране Ивановића, Урошевића и Вуковића у склопу другог пројекта, до сада није још објављен али је у процедури објављивања.

Након што су се распитивали за место где дете живи, разлоге његовог посећивања наведених канала, и других питања о његовом идентитету (са ким живи, са ким се дружи и др.) лицима која су се јављала ради остваривања комуникације постављано је питање везано за узраст. Углавном се радило о лицима старосне доби од 20 до 36 година. У даљој комуникацији, контакт је остваривaн са лицима која су, након што су написала да су пунолетна, изразила жељу да наставе комуникацију. Приликом комуникације уочено је да су педофили научили многе „трикове“, које у ове сврхе користе на *IRC* каналима. Да би дошли до података о жртви они су формирали у више случајева различите „ликове“ како би из различитих перспектива пришли жртвама и сазнали што више података. Приликом комуникације они најчешће формирају већи број различитих „ликова“[41] за које сматрају да највише одговарају жртви, и након одређеног времена покушавају да уђу у интимнију комуникацију, упркос чињеници да знају да се очигледно ради о детету (у комуникацији је навођено да је дете болесно, да је остало кући и да не иде у школу због температуре, да је искористило прилику да користи Интернет док родитељи нису код куће и сл). Када успешно успоставе комуникацију ова лица се распитују за разлог посећивања и отварања профила, годиште, место становања, школу, емотивни статус (најчешћа питања се односе на то да ли жртва има или нема дечка), распитују се за родитеље и њихово присуство, проблеме са родитељима које дете има и сл. Врло често ради провере искрености жртве преко осталих профила постављају слична или иста питања да би се уверили да ли жртва прича истину. Када сазнају које су особине жртве и њена интересовања, кроз њено испитивање преко различитих профила које држе под својом контролом, за даљу комуникацију педофили бирају најпогоднији профил и постепено формирају лик по жељама жртве (најчешће млађег лица које има заједничка интересовања, а у неколико случајева формирали су и лик девојчице сличног узраста). Сада је апсолутно јасно откуда им назив сексуални предатори, алузија је на грабљивице које „плету своје мреже“ око жртава прикупљајући сваку информацију о слабости жртве са намером да је у некој блиској будућности експлоатишу.

Након што пронађу „најпогоднији“ профил и начин комуникације педофили убеђују жртве да причају о свом тзв. „сексуалном животу“. Питањима наводе жртву да им причају да ли су имале сексуално искуство, шта од одеће на себи имају обучено (нпр. „које гаћице носиш“), „да ли мастурбираш“, колико су физички развијене и слично. По упућивању одговора на неко од наведених питања у коме дете наводи да му није јасно питање креће много агресивнија комуникација у којој се помињу много вулгарнији изрази и, конкретни, предлози за комуникацију у вези полног односа или недозвољених полних радњи. Када уоче да жртва има проблем у вези начина комуникације покушавају да јој се приближе под изговором како такав начин комуникације није чудан, да то „није срамота“ и наводе да су и они имали слична искуства у тим годинама, како би их навели да се ради о нормалној појави. У ову сврху могу користити и део своје колекције фотографија и видео записа о сексуалним активностима малолетника са одраслим

[41] По једном профилу детета и до пет различитих профила, који га контактирају, а иза којих, очигледно, стоји једно лице, убеђено да дете, које користи профил није свесно да се ради о унакрсним питањима постављаних од исте особе преко више лажних профила.

особама. По сазнању да жртва не жели да комуницира на такав начин пребацују се на друге профиле, које је она прихватила у жељи да наставе комуникацију и прикупе друге информације. Најчешће формирају профиле у којима наводе да су истог пола као жртва и да имају слична интересовања. У неколико случајева се дешавало да настављају вулгарну комуникацију, након што сазнају да жртва комуницира са другим профилом који они контролишу и да на том профилу комуникацију обављају на интимнији начин (нпр. уколико се представе као вршњакиња, након што сазнају шта дете има на себи започињу ласцивне приче).

У току разговора, педофили се, врло често, распитују и за интересовања детета, његове проблеме, породичну ситуацију, његово кретање, круг људи са којима се дружи, профилима које има на одређеним Интернет сервисима за он лајн комуникацију и сл. Врло често се распитују и за Интернет сервисе на којима постоји могућност аудио-визуелне комуникације као што су нпр. MSN или SKYPE, као и за профиле на социјалним мрежама као што је нпр. Facebook (фејсбук). Интернет сервис Facebook сматра се једним од најпопуларнијих друштвених мрежа на Интернету[42]. Након што добију ове податке преко наведених Интернет сервиса се тражи интимија комуникација. Као што је већ наведено, веома је лако искористити пријатељство или различита средства на социјалним мрежама, како би се дошло до интимних фотографија и других личних података о многим малолетницима на социјалној мрежи. Неретко покушавају и да договоре стварни састанак којима се деца могу довести у опасност да над њима буде извршено кривично дело.

На неколико профила уочено је да сексуално узнемиравање креће одмах након успостављања комуникације питањима о доњем вешу, начину мастурбирања, физичком изгледу и полној развијености и сл. Описано је одговарајуће класичном типичном профилу педофила сексуалног предатора. На највећем броју профила сексуално узнемиравање лица су започињала након неколико минута, иако су у комуникацији сазнали да се ради о детету које не жели да комуницира на такав начин, и коме није јасно о чему се прича.

[42] Athanasopoulos, E. Makridakis A. Antonatos, S. Antoniades, D. Ioannidis, S. Anagnostakis, K. G. Markatos, E. P. Antisocial Networks: Turning a Social Network into a Botnet, Section: Network Security, Lecture Notes In Computer Science, Berlin, Germany, p.146-160.

2. ГРУПА ДЕЛА ПРОТИВ ИНТЕЛЕКТУАЛНЕ СВОЈИНЕ

Прописивањем ових кривичних дела употпуњена је заштита у нашем правном систему која се пружа у погледу заштите права интелектуалне својине. Као што се види из претходног текста елаборирано је о прекршајима и привредним преступима којима се, такође, штите ова права а на овом месту говорићемо о кривичним делима којима се инкриминишу радње које представљају по законодавцу најтежа дела. Група кривичних дела против интелектуалне својине први пут је предвиђена у нашем законодавству у глави двадесет Кривичног законика Републике Србије из 2005. године па су тада и предвиђена по први пут и два кривична дела која за објект заштите имају патентно право и право на дизајн. То су кривично дело "Повреда проналазачког права" предвиђено чланом 201. Кривичног законика Србије и кривично дело "Неовлашћеног коришћења туђег дизајна" предвиђено чланом 202. Кривичног законика Србије. У ранијим законским решењима није постојала група кривичних дела против интелектуалне својине, већ је постојало само једно кривично дело "Неовлашћено коришћење ауторског и другог сродног права" у оквиру групе кривичних дела против имовине. Кривичним закоником из 2005. године кривично дело повреде проналазачког права и кривично дело неовлашћеног коришћења туђег дизајна сврстана су у групу кривичних дела против интелектуалне својине док је инкриминисање повреде осталих права индустријске својине: права жига, права географских ознака порекла и права заштите топографије интегрисаних кола извршено у оквиру кривичног дела "Неовлашћене употребе туђе фирме" у члану 233. Кривичног законика Републике Србије.

На кривична дела против интелектуалне својине, па тако и на кривично дело повреде проналазачког права и кривично дело неовлашћеног коришћења туђег дизајна примењује се и Закон о организацији и надлежности државних органа за борбу против вискотехнолошког криминала. Домен примене овог закона је дефинисан у члану 3 где је изричито речено да се он примењује на: "кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара "[43]

[43] Члан 3. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала.

2. 1 Повреда моралних права аутора и интерпретатора

Први облик чини лице које под својим именом, или именом другог, у целини, или делимично, објави, стави у промет примерке туђег ауторског дела или интерпретације, или на други начин јавно саопшти туђе ауторско дело или интерпретацију (новчана казна или затвор до три године). Дакле, радња овог дела је постављена алтернативно и састоји се из делимичног, или у целости, објављивања или стављања у промет примерака туђег ауторског дела или интерпретације или на други начин јавног саопштавања ауторских дела или интерпретација чији извршилац није аутор. То подразумева продају, размену, растурање, поклањање и све друге сличне делатности. Објављивање се може састојати из продаје дигиталних или других копија ауторског дела или интерппретације, али и у омогућавању другим лицима да овакве предмете кривичног дела преузму са одређених Интернет страница, чиме се покрива последњи облик – на други начин јавно саопштавање туђег ауторског дела или интерпретације.

Други облик врши онај ко без дозволе аутора измени или преради туђе ауторско дело или измени туђу снимљену интерпретацију (новчана казна или затвор до једне године). Посебан проблем у оваквим случајевима је питање када је извршена измена или прерађивање туђег ауторског дела или интерпретације. У питању су правила lege artis која се морају консултовати у сваком појединачном случају. Није исто када се изводи нпр. џез нумера одређеног ауторског дела јер тада такво извођење или интерппретација представљају посебно ауторско дело и посебан облик интерпретације, па је очигледно да је у сваком посебном случају неопходно разлучити на који начин је дело настало и интерпретирано. Претходно описани облици се гоне по предлогу оштећеног. Битна карактеристика је да извршилац има свест о томе да је у питању туђе ауторско дело или интерпретација, као и да свесно објављује под туђим или својим именом. У суштини неопходно је да постоје елементи обмане или лажног приказивања да је интерпретација или ауторско дело дело лица које објављује или неког трећег а не оштећеног.

Трећи облик чини оно лице које ставља у промет примерке туђег ауторског дела или интерпретације на начин којим се вређа част или углед аутора или извођача (новчана казна или затвор до шест месеци), овај облик се гони по приватној тужби. Предмети коришћени у свим описаним облицима ће се одузети.

Морална права аутора су једна од компоненти ауторског права, поред имовинских права. Морална права аутора представљају групу права коју аутор поседује у односу на његово ауторско дело. У ова права спадају:

- *Право патернитета:* Аутор има искључиво право да му се призна ауторство на његовом делу.
- *Право на назначење имена:* Аутор има искључиво право да његово име, псеудоним или знак буду назначени на сваком примерку дела, односно наведени приликом сваког јавног саопштавања дела.

- *Право објављивања:* Аутор има искључиво право да објави своје дело и да одреди начин на који ће се оно објавити. До објављивања дела само аутор има искључиво право да јавно даје обавештења о садржини дела или да описује своје дело.
- *Право на заштиту интегритета дела:* Аутор има искључиво право да штити интегритет свог дела, и то нарочито: да се супротставља изменама свог дела од стране неовлашћених лица; да се супротставља јавном саопштавању свог дела у измењеној или непотпуној форми; да даје дозволу за прераду свог дела.
- *Право на супротстављање недостојном искоришћавању дела:* Аутор има искључиво право да се супротставља искоришћавању свог дела на начин који угрожава или може угрозити његову част или углед.[44]

Морална права се дакле односе на неимовинску компоненту која се може повезати са ауторством на неком делу. У складу са овиме, кривично дело „Повреда моралних права аутора и интерпретатора“ се инкриминише као:
- Објављивање или јавно саопштавање на други начин примерака туђег ауторског дела или интерпретације у целини или делимично, под именом које није име аутора;
- Измена или прерада туђег ауторског дела или снимљене интерпретације без дозволе аутора;
- Стављање у промет примерака туђег ауторског дела или интерпретације на начин којим се вређа част или углед аутора или извођача.[45]

Како се у пракси ово дело може довести у везу са делима ВТК?

Развој технологија електронске технологије и комуникације олакшао је више него икада у прошлости злоупотребе које се дотичу ауторских права. Ако се ово кривично дело разматра у својим појавним облицима, може се доћи до неколико закључака.

Када је реч о објављивању или другом начину јавног саопштавања ауторског дела, требало би пре свега имати у виду хиперпродукцију електронских часописа, текстова, форума и блогова. У тој „поплави“ текстова који се објављују на вишемилиона интернет сајтова и доступни су практично сваком кориснику интернета (мада су неки и ограничени према чланству које се плаћа) практично је немогуће контролисати објављивање оваквих садржаја. Ово је идеална подлога за вишеструко објављивање туђих дела под именом извршиоца, или чак неким трећим именом. Како се материјална корист није битан елемент (реч је о кршењу моралних права аутора), свако објављивање текстова за које онај који их објављује нема дозволу аутора, односно носиоца ауторских права, конституише ово кривично дело.

[44] Чланови 14-18. Закона о ауторским и сродним правима, Сл. гласник РС 104/09.
[45] Члан 198. Кривичног законика.

Посебан, у последње време све чешћи, начин повреде моралних права аутора настаје кроз активности интернет сајтова специјализованих за писање стручних, школских и факултетских, радова. Осим што је овако нешто забрањено актима факултета и универзитета, „аутори“ оваквих текстова се баве хиперпродукцијом истих из потпуно различитих области, па логично не поседују довољна знања да би написали квалитетне радове које продају. Отуда овакве радове углавном чине потпуни плагијати и/или компилације већ објављених текстова у штампаном или електронском облику, наравно без навођења аутора. *Плагијат*, као облик неовлашћеног коришћења туђих стручних и научних радова, посебно је распрострањен облик злоупотребе који може довести до конституисања радње извршења овог кривичног дела. У пракси су познати плагијати не само када је реч о семинарским и завршним радовима, већ и о магистарским, мастер радовима и докторатима, као и плагирање целих ауторских истраживања – монографија, и сл. Отуда су многи универзитети и комерцијалне компаније развиле посебан софтвер који открива плагирање у радовима студената.

2.2 Неовлашћено искоришћавање ауторског дела или предмета сродног права[46]

[46] Неовлашћено искоришћавање ауторског дела или предмета сродног права из чл. 199. ст. 3. у вези са ст.1 и 2. Кривичног законика у вези са чл.33. КЗ; По оптужници Посебног тужилаштва КТ ВТК.бр.42/08, пресудом Окружног суда у Београду К1.втк.бр.19/08 од 10.10.2008.год., због Интернет пиратерије, оглашени су кривим Ж.Ј. (36) и С.М. (35) Пресудом бр.**К1 ВТК број 19/08** којом су окривљени осуђени на условну казну затвора у трајању од шест месеци са роком проверавања од две године из Краљева. Они су, у периоду од 21.06.2005.године, па све до дана 03.06.2008.године, када су лишени слободе, на територији Општине Краљево, по претходном договору, у намери да себи прибаве имовинску корист, путем бежичне Интернет мреже (wireless), за новчану надокнаду неовлашћено стављали у промет преко 500 (петстотина) примерака разноврсних ауторских дела, различитих носилаца ауторских права на тај начин што су током 2005.године па надаље, на основу заједничких финасијских улагања, изградили и пустили у експлоатацију Wireless - бежичну Интернет мрежу која је функционисала нерегистровано под неформалним називом „eXcalibur Wireless“ (Екскалибур Вајрлес), што су чинили у оквиру пословног простора - привредног друштва „EXCALIBUR COM D.O.O.“ током ког периода су у наведеном простору примали новчане уплате корисника Интернета и FTP сервиса којима је након извршених уплата било омогућено да на своје кућне рачунаре преузимају неовлашћено умножене примерке разноврсних ауторских дела - у виду фонограма, видеограма, рачунарских програма и других мултимедијалних садржаја које су окривљени, ради стављања у промет, неовлашћено држали похрањене на hard (тврдим) дисковима File Transfer Protocol сервера тј. сервера са протоколом за размену фајлова, који се физички налазио у кући првоокривљеног на адреси његовог пребивалишта, на који је првоокривљени претходно путем сателитског Интернета - из етра download-овао (преузимао) наведене садржаје којима су крајњи корисници приступали са својих рачунара, уз уношење приступног имена и корисничке шифре - преко MAC (Media Access Control) адресе и приступне тачке на којој су регистровани у приступној бази корисника (на месту где се налази антена која прима најачи сигнал њихове бежичне мреже), а потом download-овали (преузимали) понуђене садржаје – неовлашћено стављене у промет примерке ауторских дела, у виду филмова, рачунарских игрица, музике и других мултимедијалних садржаја. Кривично дело - *Неовлашћено искоришћавање ауторског дела или предмета сродног права* из чл. 199. ст. 3. у вези са ст. 2. Кривичног законика. По оптужници Посебног тужилаштва КТ ВТК.бр.70/08, пресудом Окружног суда у Београду К1.втк.бр.44/08 од 28.11.2008.год., због Интернет пиратерије, оглашен је кривим М.С. (30) из Београда што је, у периоду од 01.01.2005. године до 03.09.2008. године, у Београду, на адреси свог пребивалишта, у намери прибављања имовинске користи, неовлашћено умножавао и стављао у промет различита видеограмска и фонограмска ауторска дела већег броја ошт. носилаца ауторских права, у виду оптичких дискова у „DVD“ и „DivX“ формату на тај начин што је неовлашћено набављене копије ауторских дела претходно наснимавао на оптичке, као и тврде дискове својих рачунара након чега је њихову продају, са каталогом од око 15.000 (*петнаестхиљада*) појединачних наслова и ценовником, оглашавао путем своје електронске адресе поштанског сервиса yahoo.com коју је слао заинтересованим лицима која су се оглашавала на разним Интернет форумима да би потом, након пристизања наруџбина, умножавао копије ауторских дела, паковао их и тако припремљене лично достављао купцима, што је чинио све до интервенције овлашћених службених лица Одељења за борбу против високотехнолошког криминала, СБПОК-а, УКП, МУП-а Републике Србије која су након обављеног претреса стана и других просторија на напред наведеној адреси, од осумњиченог уз потврду привремено одузели два рачунара, 10.327 (*десетхиљадатристотинедвадестиседам*) комада неовлашћено умножених оптичких дискова са неовлашћено умноженим ауторским делима у виду филмова, телевизијских серија, музике, стрипова и других мултимедијалних садржаја, који су се налазили у омотима на којима су руком били уписани редни бројеви из каталога који је окривљени достављао заинтересованим лицима, као и и интерну евиденција у виду три каталога са списковима наручених филмова, подацима наручилаца за 2005, 2006. и 2007. годину и обрачуном зараде за наведени период.

Ово кривично дело је веома широко дефинисано. Првим ставом прописан је први облик који чини лице које неовлашћено објави, сними, умножи или на други начин јавно саопшти у целини или делимично ауторско дело, интерпретацију, фонограм, видеограм, емисију, рачунарски програм или базу података (казна затвора до три године) при чему за постојање кривичног дела није од значаја број копија[47]. Други облик постоји када лице стави у промет, или у намери стављања у промет, неовлашћено држи умножене или неовлашћено стављене у промет примерке ауторског дела, интерпретације, фонограма, видеограма, емисије, рачунарског програма или базе података (иста казна као за претходни облик). Стављање у промет подразумева чињење доступним јавности примерака туђег ауторског дела, а под тим треба подразумевати продају, размену, растурање, поклањање и све друге делатности којима се остварује суштина неовлашћеног чињења доступним[48]. Држање у намери стављања у промет подразумева држање у количини, на местима и на начин који подразумева нуђење на продају или представља логичну степеницу (иманентно је) у активности стављања у промет. Трећим ставом је прописан тежи облик који постоји уколико је лице учинило претходна два облика у намери прибављања имовинске користи за себе или другог (прописана казна затвора од три месеца до пет година). Четврти став предвиђа посебан облик овог дела, по којем ће се лице које произведе, увезе, стави у промет, прода, да у закуп, рекламира у циљу продаје или давања у закуп или држи у комерцијалне сврхе уређаје или средства чија је основна или претежна намена уклањање, заобилажење или осујећивање технолошких мера намењених спречавању повреда ауторских и сродних права, или које такве уређаје користи у циљу повреде ауторског или сродног права, казнити новчаном казном или казном затвора до три године[49]. Овим последњим ставом инкриминисане су припремне радње за извршење свих осталих облика овог кривичног дела али и других кривичних дела из ове групе.

Ово кривично дело најзаступљеније је у последње време, глобално гледано, а, нарочито, у Србији. Многи су покушаји објашњења у погледу заступљености и распрострањености овог кривичног дела, од којих су неки доступност различитих софтвера којима се веома лако и веома брзо преносе дигитални садржаји путем

---

[47] Али наведено јесте значајно са аспекта надлежности за поступање у овом кривичном делу у смислу члана 3. Закона о организацији и надлежности државних органа у борби против високотехнолошког криминала. У надлежност СБПОК – а и Посебног Тужиоца за ВТК, као и већа за ВТК Вишег суда у Београду спадају само они случајеви са преко 2000 примерака умножених ауторских дела или када је настала штета од преко 1.000.000 динара. У питању су измене чл.3. Закона о организацији и надлежности државних органа у борби против ВТК.

[48] Герке, М и др., *Приручник за истрагу кривичних дела у области ВТК, Савет Европе, 2008.*, str.133.

[49] Током 2008. године Тужилаштву за борбу против високотехнолошког криминала је поднето 319 кривичних пријава против 332 лица због извршења укупно 379 кривичних дела која се односе на повреду интелектуалне својине, а укупно су одузета 131.232 оптичка диска и 50 техничких уређаја. Имајући у виду описано стање криминала, на основу договора са истражним одељењем Окружног суда у Београду, да се у циљу што ефикаснијег решавања ових предмета примењује поступак за кажњавање и изрицање пресуде од стране истражног судије, сагласно члану 455. Законика о кривичном поступку. Ова врста поступка примењује се онда када је то оправдано, а у обзир се нарочито узима ранија осуђиваност осумњичених лица и мотиви за извршење кривичног дела. Наведено према Комлен Николић Л. и др. *Op.cit...*

Интернета од торент клијената до П2П преноса. Чињеници заступљености погодују многи фактори од оних на страни сиромашних земаља у транзицији и немогућности да њихово становништво одговори скупим захтевима ималаца права, до стратешке неуједначености на глобалном нивоу у погледу различитих облика заштите медија, путем којих се преносе дигитални садржаји.

Неретко извршиоци на својим Интернет страницама нуде и више десетина хиљада наслова а да се, у ствари, њих пронађе свега пар стотина копија. У преткривичном поступку је потребно сачинити потврду о предметима који су одузети од окривљеног. У њој морају бити наведени наслови свих филмова, програма или музичких дела, која су стављена у промет, формат и медијум на ком се налазе, као и одређени носиоци права који су овом приликом оштећени. Пописивање је неопходно како би била извршена идентификација овлашћених носилаца права који су оштећени извршењем кривичног дела[50]. Ово ствара тешкоће и одузима много времена полицијским службеницима, нарочито када се број наслова мери десетинама хиљада и представља главни разлог због кога се број уличних продаваца пиратских дискова не смањује. Идентификација носилаца права оптерећује и тужиоце, па је ради убрзавања преткривичног поступка, Тужилаштво за борбу против високотехнолошког криминала направило базу података са насловима филмова, музичких дела и софтвера, као и овлашћеним дистрибутерима истог садржаја[51].

Ово дело може бити извршено и без прибављања имовинске користи. Према ставу 3. овог члана, уколико се учини у намери прибављања имовинске користи за себе или другога, постоји тежи облик овог дела. Овако дефинисано, дело обухвата и широк појам коришћења високих технологија за тзв. пиратерију, односно неауторизовано пласирање – најчешће продају или размену, ауторских дела (књига, филмова, музичких нумера, рачунарских програма, и сл.). Ово кривично дело је једно од најраспрострањенијих у многим државама, а посебан замах је добило развојем како рачунара тако и интернет веза и комуникације – данас се практично неограничен број ауторских дела може без дозволе аутора понудити сваком кориснику интернета – дакле, постоји и неограничен број потенцијалних корисника нелегалног производа.

„Пирати“ за своје деловање злоупотребљавају компаније које нуде услуге чувања (енгл. хост) датотека на својим серверима, попут Rapidshare, Megaupload (Рапидшер, Мегааплоад) и др. Пре постављања (енгл. *upload*) оригинални фајл се подели на више мањих делова коришћењем неких од програма за дељење попут „Winзип“, „АРЈ“„Филесплиттер“ (Filesplitter) или „ХјСплит“ (eng. HjSplit), који се потом заштићују шифром. Мали фајлови добијени на овај начин обично немају оригиналан назив филма или програма, због чега је нелегалан садржај тешко

[50] Исто је резултат става Врховног суда Републике Србије, изнет у пресуди Кзз.бр.10/06 од 16.03.2006.године, према којем, радња извршења кривичног дела Неовлашћено искоришћавање ауторског дела лии предмета сродног права из чл.199.КЗ-а описана у пресуди, мора бити ближе одређена објектом дела односно, називом ауторског дела и субјектом ауторског права

[51] Наведено према Комлен Николић Л. и др. *Op.cit...*

открити. Линкови који воде ка овим фајловима се налазе на веб сајтовима и форумима специјализованим за размену пиратских садржаја. Наведене компаније остављају могућност својим корисницима да у сваком тренутку пријаве злоупотребу, што пирате не одвраћа да и даље постављају нелегалне садржаје, због чега се сервери ових компанија данас сматрају главним изворима пиратерије на Интернету.

Још један веома популаран начин размене фајлова који се злоупотребљава за пиратерију представљају торенти, програми који се базирају на „П2П“ (енг. *peer to peer*) технологији, којом се остварује директна веза између два рачунара ради размене података између корисника. Успоставља се веза између корисника који имају одређену датотеку на свом рачунару тзв. „сејачи“ (енг. *seeders*) и клијената који траже исту тзв. „пијавице“ (енг. *leechers*), а на овај начин се најчешће размењују различити садржаји: велике видео датотеке, музичка дела и софтвер. Како би иницирао преузимање фајла (енг. *download*) „личер“ покреће торент, програм који остварује везу са централним сервером – „трекером“ (енг. *tracker*) на коме се налазе подаци о „сидерима“. Након тога клијент успоставља више симултаних „П2П“ конекција са „сидерима“ и почиње да преузима тражени фајл са више локација одједном. Карактеристика овог процеса је да корисник који преузима фајлове, у исто време постаје „сидер“, односно дели те исте фајлове са другим корисницима[52]. Судови извршиоцима кривичних дела против интелектуалне својине најчешће изричу условне казне затвора[5354].

---

[52] "BitTorrent (protocol)", Wikipedia, http://en.wikipedia.org/wiki/BitTorrent_(protocol), 10.05.2009.

[53] Мада је у 2008. години Посебно одељење Окружног суда у Београду осудило двојицу извршилаца на затворске казне и то окривљеног ЖД пресудом К1 16/08 на казну затвора у трајању од шест месеци, а окривљног МЈ пресудом К1 17/08 на казну затвора у трајању од једанаест месеци. Ова лица су била вишеструки повратници, а раније су осуђивани искључиво због извршених кривичних дела против интелктуалне својине.

[54] Примери из судске праксе: 1) Дело *Неовлашћено искоришћавање ауторског дела или предмета сродног права* из чл. 199. ст. 3. у вези са ст.1 и 2. Кривичног законика у вези са чл.33. КЗ.

По оптужници Посебног тужилаштва КТ ВТК.бр.42/08, пресудом Окружног суда у Београду К1.втк.бр.19/08 од 10.10.2008. године, због Интернет пиратерије, оглашени су кривим Ж.Ј. (36) и С.М. (35) Пресудом су окривљени осуђени на условну казну затвора у трајању од шест месеци са роком проверавања од две године из Краљева. Они су, у периоду од 21.06.2005. године, па све до дана 03.06.2008. године, када су лишени слободе, на територији Општине Краљево, по претходном договору, у намери да себи прибаве имовинску корист, путем бежичне интернет мреже (*вирелесс*), за новчану надокнаду неовлашћено стављали у промет преко 500 (петстотина) примерака разноврсних ауторских дела, различитих носилаца ауторских права на тај начин што су током 2005. године па надаље, на основу заједничких финасијских улагања, изградили и пустили у експлоатацију Вирелесс - бежичну Интернет мрежу која је функционисала нерегистровано под неформалним називом „еXcalibur Wireless“ (Екскалибур Вајрлес), што су чинили у оквиру пословног простора – привредног друштва „ЕХЦАЛИБУР ЦОМ Д.О.О.“ током ког периода су у наведеном простору примали новчане уплате корисника Интернета и ФТП сервиса којима је након извршених уплата било омогућено да на своје кућне рачунаре преузимају неовлашћено умножене примерке разноврсних ауторских дела – у виду фонограма, видеограма, рачунарских програма и других мултимедијалних садржаја које су окривљени, ради стављања у промет, неовлашћено држали похрањене на хард (тврдим) дисковима File Transfer Protocol сервера тј. сервера са

Ваља приметити да КЗ говори о неовлашћеном објављивању, снимању, умножавању или јавном саопштавању на други начин – ова формулација је језички помало неспретно уобличена, јер се снимање или умножавање немогу сматрати јавним саопштавањем. Намера законодавца је, међутим, јасна. Реч је о делу које инкриминише сваку радњу која се може сматрати функционално повезаном са радњом објављивања, односно чињења доступним ширем кругу јавности. Тако би се радњом извршења могло сматрати и израђивање ДВД-ова са сврхом уличне продаје, тајно (тј. свако неовлашћено) снимање биоскопских пројекција филмова, али и њихово потоње стављање у промет, односно чињење сотупним кроз нпр. постављање на одређене интернет сајтове. Да ли се ово врши у комерцијалне сврхе – да би се остварила зарада (како КЗ каже, „имовинска корист“) или не, потпуно је ирелевантно са становишта постојања овог кривичног дела али има утицаја на одређивање да ли је у питању основни или тежи његов облик.

- Други облик дела се односи на стављање у промет, или држање ради стављања у промет примерака ауторског дела, интерпретације, фонограма, видеограма, емисије, рачунарског програма или базе података, неовлашћено умножених или

протоколом за размену фајлова, који се физички налазио у кући првоокривљеног на адреси његовог пребивалишта, на који је првоокривљени претходно путем сателитског Интернета – из етра downлоад-овао (преузимао) наведене садржаје којима су крајњи корисници приступали са својих рачунара, уз уношење приступног имена и корисничке шифре – преко MAC (*Media access control*) адресе и приступне тачке на којој су регистровани у приступној бази корисника (на месту где се налази антена која прима најачи сигнал њихове бежичне мреже), а потом downлоад-овали (преузимали) понуђене садржаје – неовлашћено стављене у промет примерке ауторских дела, у виду филмова, рачунарских игрица, музике и других мултимедијалних садржаја.

2) Дело - *Неовлашћено искоришћавање ауторског дела или предмета сродног права* из чл. 199. ст. 3. у вези са ст. 2. Кривичног законика. По оптужници Посебног тужилаштва КТ ВТК.бр.70/08, пресудом Окружног суда у Београду К1.втк.бр.44/08 од 28.11.2008. године, због интернет пиратерије, оглашен је кривим М.С. (30) из Београда што је, у периоду од 01.01.2005. године до 03.09.2008. године, у Београду, на адреси свог пребивалишта, у намери прибављања имовинске користи, неовлашћено умножавао и стављао у промет различита видеограмска и фонограмска ауторска дела већег броја ошт. носилаца ауторских права, у виду оптичких дискова у „ДВД“ и „ДивХ“ формату на тај начин што је неовлашћено набављене копије ауторских дела претходно наснимавао на оптичке, као и тврде дискове својих рачунара након чега је њихову продају, са каталогом од око 15.000 (*петнаестхиљада*) појединачних наслова и ценовником, оглашавао путем своје електронске адресе поштанског сервиса уахоо.цом коју је слао заинтересованим лицима која су се оглашавала на разним Интернет форумима да би потом, након пристизања наруџбина, умножавао копије ауторских дела, паковао их и тако припремљене лично достављао купцима, што је чинио све до интервенције овлашћених службених лица Одељења за борбу против високотехнолошког криминала, СБПОК-а, УКП, МУП-а Републике Србије која су након обављеног претреса стана и других просторија на напред наведеној адреси, од осумњиченог уз потврду привремено одузели два рачунара, 10.327 (*десетхиљадатристотинедвадестиседам*) комада неовлашћено умножених оптичких дискова са неовлашћено умноженим ауторским делима у виду филмова, телевизијских серија, музике, стрипова и других мултимедијалних садржаја, који су се налазили у омотима на којима су руком били уписани редни бројеви из каталога који је окривљени достављао заинтересованим лицима, као и и интерну евиденција у виду три каталога са списковима наручених филмова, подацима наручилаца за 2005, 2006. и 2007. годину и обрачуном зараде за наведени период.

неовлашћено стављених у промет. Као и код претходног дела, уколико се то учини у намери прибављања имовинске користи за себе или другога, постоји тежи облик овог дела. Развој интернет комуникације је омогућио велики број различитих начина „дељења“ фајлова на светској електронској мрежи. Због тога се мора нагласити да је ово дело подједнако вазано за неовлашћено „дељење“ које се ради без икакве надокнаде, као и за оне врсте чињења доступним ових ауторских дела за накнаду (продајом дискова, чланством на интернет сајтовима за download, и сл.).

На овом месту би требало напоменути још једну важњу чињеницу – поседовање, односно држање оваквог материјала, кажњиво је само уколико се може доказати да оно служи његовом стављању у промет. Ако би могли направити паралелу са другом врстом кривичног дела, „поседовање ради личне употребе“, као ни радња прибављања, нису кажњиве. У надлежност МУП РС – СБПОК, Одељења за борбу против ВТК и Посебног Тужиоца за ВТК, као и одељења за ВТК Вишег суда у Београду спадају само они случајеви са преко 2000 примерака умножених ауторских дела или када је настала штета од преко 1.000.000 динара. У питању су измене чл.3. Закона о организацији и надлежности државних органа у борби против ВТК.

- Коначно, према члану 199. КЗ-а кривично дело представља и производња, увоз, стављање у промет, продаја, давање у закуп, рекламирање у циљу продаје или давања у закуп или држање у комерцијалне сврхе уређаја или средстава чија је основна или претежна намена уклањање, заобилажење или осујећивање технолошких мера намењених спречавању повреда ауторских и сродних права. Као радња извршења одређено је и само коришћење таквих уређаја или средстава у циљу повреде ауторског или сродног права. Иако је одредба сама по себи јасна, може бити веома дискутабилно који су то „уређаји“[55] који су погодни за извршење овог кривичног дела, будући да се оно може извршити и са оним апаратима који су уобичајено присутни код сваког просечног корисника – рачунар, скенер, интернет модем, штампач, оптички дискови, и сл.[56]

Што се доказивања тиче веома је значајно успоставити везу између лица које је извршилац и предмета који су *corpora delicti* овог кривичног дела. Веза се може установити нпр. упоређивањем дигиталних карактеристика времена настанка, времена преноса на одређене носиоце – медије, конкретног ауторског

[55] При томе мислимо да би појам „уређаја“ требало схватати у смислу члана 6. Европске конвенције о високотехнолошком криминалу (Закон о потврђивању Конвенције о високотехнолошком криминалу, Сл.гласник РС – Међународни уговори 19/2009).

[56] Овај проблем је донекле решен када је реч о оптичким дисковима као носачима ауторских дела за чије објављивање починилац дела нема дозволу, доношењем Закона о оптичким дисковима (Сл.гласник РС 52/11), којим су регулисани, између осталог, и услови прозводње оптичких дискова, комерцијално умножавање оптичких дискова (снимање материјала заштићеног ауторским правом или сродним правима са постојећих носача на оптичке дискове, у циљу њиховог стављања у промет или њиховог извоза), као и услови и поступак за добијање лиценце за прозводњу и промет оптичких дискова.

дела. Све описане радње облика овог кривичног дела може извршити било ко, али неопходно је да то чини неовлашћено. Дакле, извршилац може бити свако лице. или видео записом са јавног саопштавања или интерпретације туђег ауторског дела. Битна карактеристика је да извршилац има свест о томе да је у питању туђе ауторско дело или интерпретација, као и да свесно објављује под туђим или својим именом. У суштини неопходно је да постоје елементи обмане или лажног приказивања да је интерпретација или ауторско дело дело лица које објављује или неког трећег а не оштећеног.

У практичном поступању значајно је уочити разлике између легалног и „пиратског“ издања музичког диска, неке од њих би биле:

1.) Различита слика и графичка обрада спољног омота кутије и самог диска

2.) “Пиратски” диск нема: шифру стампера, ознаке кодова (има рељефно оштећење на месту СИД кода - Source Identification Code, идентификациони код за аутентичност диска, такође, може имати али и не мора RID код - Recorder Identification Code) листу песама на диску[57]

3.) Ознака заштитног знака - жига - лога није иста као на оригиналу LBR код мастера: означава погон у којем је израђен.

Докази за кривично дело се могу прибавити прикупљањем и утврђивањем одређених чињеница, на пример:

1) Непостојање уговора или другог правног основа за коришћење ауторских права

2) Привремено одузети музички или видео оптички дискови у производњи, магацинима готових производа и више продајних објеката

3) Стампери

4) Пописне листе и каталози наслова

5) Интерне евиденције шефа производње

6) Уговори између СОКОЈ-а и власника ауторских права представљају тзв. компаративне доказе

7) Решење Завода за интелектуалну својину о издавању дозволе СОКОЈ-у за обављање делатности колективног остваривања ауторских имовинских права

8) Фотодокументација и видео запис

9) Вештачење музичких и видео оптичких дискова (упоређење са референтним оптичким диском неспорно произведеним на машини откривеној у производном погону)

10) Подаци садржани на хард дисковима персоналних рачунара, у власништву или државини учинилаца

11) Подаци садржани на оптичким дисковима

12) Музички компакт дискови на којима се неовлашћено налазе ознаке туђег заштитног знака, жига - лога

13) Папирни омоти на којима се налазе исте ознаке

14) Решења Завода за интелектуалну својину о заштити заштитног знака, жига - лога

[57] За боје и заштите које дискови различитих капацитета и технологија носе видети http://en.wikipedia.org/wiki/Rainbow_Books доступан 28.06.2010.год. и http://en.wikipedia.org/wiki/IFPI последњи пут приступљени истог датума

15) Слике и графичке припреме за штампу заштитних знакова, жигова - лога

16) Фотодокументација и видео запис

17) Код калупа : означава погон у којем је произведен

Идентификациона обележја оргиналног производа су:

- име дискографске или издавачке куће,
- име извођача или састава тј. групе, назив продуцента и носилаца права дистрибуције
- јасно отиснути логотипи и заштићени знакови, праћени и холограмским заштитама
- каталошки број
- копија логотипа ауторског удружења
- упозорење о заштићеним ауторским правима
- ознаке © і ® са датумом и именом дискографске куће
- земља производње (роба произведена у ЕУ наводи ЕУ као место производње)
- у случају CD-а и DVD-а обично је наведен SID код, којег данас користе 80% произвођача оптичких дискова
- понекад је истакнут потпун попис назива песама или снимака
- омоти морају бити јасно отиснути на квалитетном папиру

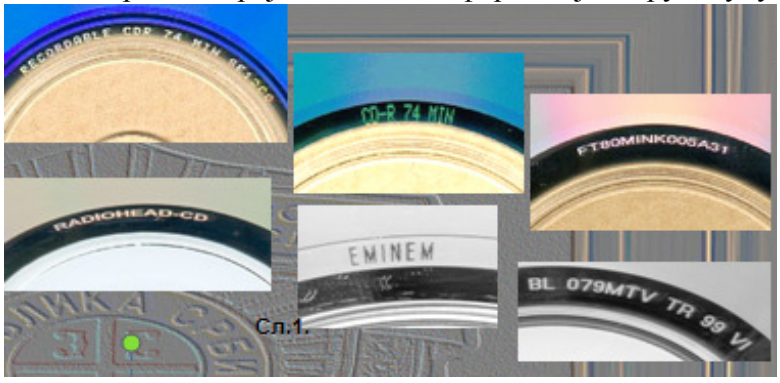
Такође и: сви тонски записи морају бити означени датумом заштите ауторских права и објављивања, горе наведено се обично налази и на носачу звука и на омоту диска

© Copyright – означава власника ауторских права на снимку на наведени датум, а ознака ® Publication– означава датум објављивања звучног снимка.

Кривотворење (фалсификовање) дискова:

Кривотворине (фалсификати) се копирају и пакују тако да наликују оригиналу, у практичном поступању је веома битно, на омоту проверити следеће: оштрину изгледа насловне фотографије, контраст боја, квалитет папира, квалитет дубине штампе, постојање холограмских заштитних ознака, фотокопије на папиру у боји, штампање на само једној страни папира, уклоњен логотип, непостојање каталошког броја, квалитет реза или облика омота, постојање парадоксалних ситуација: познати извођач, непозната дискографска кућа, веома често, висок квалитет репродукције звука.

Матрични бројеви: неке информације с руба унутрашњег појаса (близу средишта диска) често садрже слова CD-R и дужину трајања диска, као што је приказано у горњем реду на слици (то није уобичајено на DVD-R – овима).



Сл.1.

У доњем реду на илустрацији

Илустрација 7-1

приказани су CD – ови који пружају и информације о садржају на диску, што није случај са CD-R – овима. Матрични појас CD-R – а обично не носи никаква обележја, или садржи само неки алфанумерички код. На матричном појасу се не могу појавити обележја као што су логотип дискографске куће или каталошки број. CD-R – ови нису обележени LBR кодовима, јер нису подвргнути процесу мастеринга као индустријски CD – ови. CD-R – ови обично нису обележени кодовима калупа. Међутим, у неким земљама су произвођачи законски обавезни на сваком калупу навести и код калупа, тако да се и калупи за CD-R – ове кодирају, тако да такви дискови носе код који је додељен произвођачу у земљи у којој се производи CD-R. Обично је очитавана страна CD-R – а обојена (најчешће зеленом или плавом бојом), а приметан је „ефекат дуге“, за разлику уобичајеног сребрнастог завршног слоја који се налази на CD – у, што је приказано на горњој слици у црвеном оквиру. Велики део изложеног се може користити и у случају кривичног дела Неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима из члана 200. КЗ.

Пирати за своје деловање злоупотребљавају компаније које нуде услуге чувања (енгл. *hosting*) датотека на својим серверима, попут *Rapidshare, Megaupload* и др. Пре постављања (енгл. уплоад) оригинални фајл се подели на више мањих делова коришћењем неких од програма за дељење попут „Winzip“, „ARJ“,„Filesplitter“ или „HjSplit“, који се потом заштићују шифром. Мали фајлови добијени на овај начин обично немају оригиналан назив филма или програма, због чега је нелегалан садржај тешко открити. Линкови који воде ка овим фајловима се налазе на веб сајтовима и форумима специјализованим за размену пиратских садржаја. Наведене компаније остављају могућност својим корисницима да у сваком тренутку пријаве злоупотребу, што пирате не одвраћа да и даље постављају нелегалне садржаје, због чега се сервери ових компанија данас сматрају главним изворима пиратерије на Интернету.

Још један веома популаран начин размене фајлова који се злоупотребљава за пиратерију представљају торенти, програми који се базирају на „П2П“ (енгл. *peer to peer*) технологији, којом се остварује директна веза између два рачунара ради размене података између корисника. Успоставља се веза између корисника који имају одређену датотеку на свом рачунару тзв. „сејачи“ (енгл. *seeders*) и клијената који траже исту тзв. „пијавице“ (*leechers*), а на овај начин се најчешће размењују различити садржаји: велике видео датотеке, музичка дела и софтвер. Како би иницирао преузимање фајла (енгл. *download*) „личер - пијавица“ покреће торент, програм који остварује везу са централним сервером – „трекером“ (енгл. *tracker*) на коме се налазе подаци о „сидерима“. Након тога клијент успоставља више симултаних „П2П“ конекција са „сидерима“ и почиње да преузима тражени фајл са више локација одједном. Карактеристика овог процеса је да корисник који преузима фајлове, у исто време постаје „сидер“, односно дели те исте фајлове са другим корисницима[58]. Судови у пракси у Србији извршиоцима кривичних дела против интелектуалне својине најчешће изричу условне казне затвора[59].

---

[58] “BitTorrent (protocol)”, Wikipedia, Internet, http://en.wikipedia.org/wiki/BitTorrent_(protocol), 10.05.2009.

[59] Мада је у 2008. години Посебно одељење Окружног суда у Београду осудило двојицу извршилаца на затворске казне и то окривљеног ЖД пресудом К1 16/08 на казну затвора у трајању од шест

Из упоредноправне праксе можемо издвојити пример када је суд у Шведској осудио четворицу власника чувене странице пајратбеј „The Pirate Bay“ на казне затвора од по годину дана, с тим што им је наложено да плате одштету од три и по милиона долара компанијама као што су Warner Brothers, Sony i EMI.[60] На наведеној страници се незаконито размењују музика, филмови и рачунарске игрице, а има око 22 милиона корисника.[61] Што се грађанско правне заштите тиче најинтересантнији пример је цивилна тужба холандског удружења за борбу против пиратерије BREIN[62] против администратора и власника највећег сајта за размену торент датотека Mininova. Смисао тужбе је био да власници плате казне веће од 5 милиона ЕУР –а али су тужени у овом случају применили једну меру којом су одговорили захтевима тужилаца. Наиме, одбијен је приступ свим неауторизованим садржајима на серверу и тако онемогућила пиратска размена. Посебан случај је ФТЦ (Federal trade commision) у САД који је изрекао санкције Comcast – у за појачавање и преусмеравање саобраћаја преко BitTorrent[63]. Овакво санкционисање је ипак оглашено незаконитим Одлуком Федералног апелационог суда. Наиме, доследно спроводећи став ВСС о коме је већ разматрано, сви државни органи гоњења и суђења, дужни су да у својим писменим актима наведу све наслове ауторских дела при чему, тужилаштво и суд и податке који се односе на оштећене субјекте ауторских права, у виду набрајања њихових имена или назива носилаца права. У појединим (све чешћим) случајевима „пиратерије“, који подразумевају количине заплењених оптичких дискова од 2.000 до 15.000 комада, диспозитиви оптужних аката и пресуда знају да броје по 50 и више страна, а време неопходно за утврђивање ових информација мере се данима. Мишљења смо да је у таквој ситуацији нужно изнаћи неко разумно решење, с обзиром на непримерено трошење времена и материјалних ресурса.

Одређени аутори[64], решење нуде у инкорпорирању у процесни закон одредби чл. 22. „новог“ ЗКП-а[65] којим дефинише значење израза „спис, писмено, пошиљка и други документи“[66], на који начин би преписи оптужних аката тужилаштва и одлука суда, осим евентуално изворника, могли бити у целости, или само делом - и у електронској форми. У том смислу ова одредба морала би претрпети одређене измене, утолико што би се у самом тексту на крају реченице,

---

месеци, а окривљног МЈ пресудом К1 17/08 на казну затвора у трајању од једанаест месеци. Ова лица су била вишеструки повратници, а раније су осуђивани искључиво због извршених кривичних дела против интелктуалне својине.

[60] „Osuđeni osnivači Pirate Bay-a“, BBC Serbian, Internet, http://www.bbc.co.uk/serbian/news/2009/04/090417_swedennetpiracy.shtml последњи пуп приступљено 24.07.2010.год.

[61] Кнежевић Ћосић, В. „Шведски пирати на нафтној платформи праве пиратску државу“, *Борба*, 23.04.2009. Internet, http://www.borba.rs/content/view/5127/36/, 10.05.2009.

[62] www.torrentfreak.com/mininova-deletes-all-infringing-torrents-and-goes-legal-091126/ доступан 09.05.2010.

[63] http://www.nytimes.com/2010/05/06/technology/06broadband.html?ref=technology доступно 10.05. 2010.год.

[64] Комлен Николић Л. и др. *Op.cit.*., стр.144

[65] Који неће ни отпочети са применом.

[66] Спис, писмено, пошиљка и други документи могу бити и у електронском облику и бити садржани у одговарајућим носиоцима података, као што су ЦД, други дискови, магнетне траке и било који други носиоци података, што се односи и на доказе и исправе садржане у списима.

иза речи „садржане у списима“ , унеле речи „као и на преписе оптужних аката и одлука суда, или њихових делове, осим изворника који морају бити и у писменој форми“. Овакво решење увело би, према овим ауторима, „на велика врата“ примену електронског потписа и електронског сертификата, што подразумева озбиљну припрему за њихову примену. Једини проблем јесте што овај Законик неће заживети, али би Законодавни орган ово морао узети у обзир приликом израде новог ЗКП или код измена и допуна постојећег.

2.3 Неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима

Први облик врши онај ко неовлашћено уклони или измени електронску информацију о ауторском или сродном праву, или стави у промет, увезе, извезе, емитује или на други начин јавно саопшти ауторско дело или предмет сроднoправне заштите са којег је електронска информација о правима неовлашћено уклоњена или измењена (новчана казна и затвор до три године). Предмети о којима је реч одузеће се и уништити. Објекат кривичног дела јесте електронска информација о правима интелектуалне својине, у смислу носиоца права на експлоатацију и друга пратећа права. Већ код разматрања објекта јасно је да је неизбежна импликација ВТК. Ова електронска информација је облик заштите права интелектуалне својине којом се покушава спречити крађа права интелектуалне својине, у смислу комерцијалне дистрибуције али и других аспеката, са одређених медија и носилаца датих података, предмета правне заштите. Извршилац овог кривичног дела може бити свако лице које има средства или знања, којима се ова заштита, умишљајно, може уклонити, или изменити, односно свако ко може јавно саопштити предмет права интелектуалне својине са којег је електронска информација о правима неовлашћено уклоњена или измењена.

Као што се може приметити, дело се може извршити на два начина: један подразумева уклањање електронске „заштите“ на ауторском делу, а други коришћење таквог дела са скинутом информацијом о ауторском или сродном праву. Другим речима, дело је извршено већ након што неко нпр. уклони заштиту са оригиналног ДВД-а на којем се налази неко ауторско дело – ништа више није потребно да би се конституисало, тј. да би био оптужен за његово извршење. Други облик, који је изричито постављен у тексту члана 200. КЗ као алтернативна радња извршења (а не кумулативна) постоји када се ДВД „откључан“ на претходно описан начин проследи, прода, прибави или на било који начин дистрибуира или користи. Значајно је и то да имовинска корист не представља релевантан мотив за постојање овог дела – оно ће постојати увек када се изврше описане радње, без обзира да ли је намера починиоца била да га стави у промет или користи на било који начин.

У погледу доказивања неопходно је утврдити време и место радње извршења, као и начин на који је дело извршено. Овде треба обратити посебну пажњу на средства којима је дело извршено јер се, путем компарације карактеристика датих уређаја и њихових отисака и утисака, могу непосредно

доказати присуства истих. У претходном делу указано је на неколико елемената заштите постојећим на неким медијима за складиштење података. Веза ових уређаја са лицима која се сматрају извршиоцима указује на њихово учешће у кривичном делу. Код овог кривичног дела за први облик веома је значајно утврдити постојање одређене заштите ауторског и сродног права, у облику електронске информације, као и везу одређеног лица са уклањањем ове информације, и његово својство као и да се уклањање врши неовлашћено. Веома је битно и утврдити носиоца права заштите како би се могла одредити установа која је оштећена. Начин утврђивања постојања повреде зависи од њеног обима, као и метода и техничких средстава која су том приликом коришћена. Код другог облика значајно је утврдити везу између радњи и лица које их врши како би установили везу са протурањем незаконито креираних дела уништавањем или изменом електронске информације о ауторским правима. У сваком случају веома је значајно евидентирати локације средства и просторе који су коришћени у вршењу дела. Као што је напоменуто у доказном и техничко форензичком смислу могу се користити околности и чињенице наведене раније у тексту код кривичног дела неовлашћеног искоришћавања ауторског дела или предмета сродног права из члана 199.

2.4 Повреда проналазачког права

Поред ауторских права у групу права интелектуалне својине спадају и права индустријске својине. Најважнија права индустријске својине су патентно право, право на дизајн, право на жиг право географске ознаке порекла и право заштите типографије интегрисаних кола. Први облик чини лице које неовлашћено производи, увози, извози, нуди ради стављања у промет, ставља у промет, складишти или користи у привредном промету производ или поступак заштићен патентом (новчана казна или затвор до три године).Радња извршења овог кривичног дела је алтернативно ппрописана што значи да је довољно да се изврши само нека од наведених радњи како би постојало извршење овог кривичног дела. Овај став треба тумачити тако да је за постојање овог кривичног дела неопходно код увоза, извоза и складиштења да се на основу околности датог случаја утврди да су производи или поступак заштићен патентом намењени стављању у промет. Предпоставља се да је делатност која представља радњу извршења овог кривичног дела предузета неовлашћено, односно без дозволе носиоца патента. Носилац патента је проналазач - физичко лице које је створило проналазак или његов правни следбеник. Објект радње код овог кривичног дела је производ или поступак заштићен патентом, који је као такав дефинисан Законом о патентима.[67] Према члану 5. Закона о патентима предмет проналаска који се штити патентом може бити производ (као нпр. уређај, супстанца, композиција, биолошки материјал) или поступак, а може се односити и на: 1) производ који се састоји од биолошког материјала или који садржи биолошки материјал; 2) поступак којим је биолошки материјал произведен, обрађен или коришћен; 3) биолошки материјал који је

[67] Закон о патентима, Сл. лист СЦГ 32/2004.

изолован из природне средине или је произведен техничким поступком, чак иако је претходно постојао у природи. Чланом 5 Закона о патентима дефинисано је да се не сматрају проналасцима у смислу тог закона, нарочито: 1) открића, научне теорије и математичке методе; 2) естетске креације; 3) планови, правила и поступци за обављање интелектуалних делатности, за играње игара или за обављање послова; 4) програми рачунара и 5) приказивање информација.

Законом о патентима чланом 52. дефинисана је садржина искључивих права носилаца патента: 1) да користи у производњи заштићени проналазак; 2) да ставља у промет предмет проналска заштићен патентом; 3 да располаже патентом.

У остваривању свог искључивог права на економско искоришћавање заштићеног проналаска, носилац патента има право да спречи свако треће лице које нема његову сагласност: 1) да производи, нуди, ставља у промет или употребљава производ који је израђен према заштићеном проналаску или да увози или складишти тај производ у наведене сврхе; 2) да примењује поступак који је заштићен патентом; 3) да нуди поступак који је заштићен патентом; 4) да производи, нуди, ставља у промет, употребљава, увози или складишти за те сврхе производ директно добијен поступком који је заштићен патентом; 5) да нуди и испоручује производе који чине битне елементе проналаска лицима која нису овлашћена за коришћење тог проналаска, ако је понуђачу или испоручиоцу познато или му је из околности случаја морало бити познато да је тај производ намењен за примену туђег проналаска.

Тежи облик постоји уколико је основним обликом прибављена имовинска корист или проузрокована штета у износу који прелази милион динара (затвор од једне до осам година).

Први привилеговани облик чини лице које неовлашћено објави или на други начин учини доступним (подразумевајући ту и увоз и извоз, понуду на продају, коришћење или замену, па чак и само складиштење) суштину туђег пријављеног проналаска пре него што је овај проналазак објављен на начин утврђен законом (новчана казна или затвор до две године). И у случају овог посебног облика кривичног дела повреде проналазачког права неопходно је да се делатност која представља радњу извршења предузме неовлашћено. Субјективна страна овог кривичног дела подразумева умишљај који поред осталих обележја кривичног дела треба да обухвати и свест о две околности, првој, да се радња извршења предузима неовлашћено и другој, да се радња извршења предузима пре него што је проналазак објављен на начин утврђен законом.[68] Други, тежи, облик чини онај ко неовлашћено поднесе пријаву патента или у пријави не наведе или лажно наведе проналазача (затвор од шест месеци до пет година). Овим обликом се штити правна сигурност у правном промету, покушава се давањем на значају овом делу подићи ниво заштите проналазака и патената. Такође, овим посебним обликом кривичног дела повреде проналазачког права штите се, пре свега, морална права проналазача, за разлику од основног облика овог кривичног дела којим се штите имовинска права проналазача. Последица извршења овог посебног облика кривичног дела повреде проналазачког права је да проналазач у том својству буде

[68] Наташа Делић, *Повреда проналазачког права и неовлашћено коришћење туђег дизајна (чл. 201. и 202 КЗС)*, Привреда и право, бр. 1-4, 2006, стр. 55.

наведен у пријави за признање патента, списима, регистрима, исправама и публикацијама о његовом проналаску, на начин предвиђен законом.[69] И у овим случајевима као и у претходном делу предмети се одузимају и уништавају. Што се доказних аспеката тиче у овом кривичном делу неопходно је доказати власништво над патентом или проналазком одређеног лица и повезати незаконите радње извршилаца описане у претходним реченицама временски и просторно у односу на заштиту права интелектуалне својине и других сродних права. У вези промета важи све изнето у претходним кривичним делима.

Код кривичног дела повреде проналазачког права заштитни објект овог кривичног дела је патент као субјективно и искључиво право које се, уколико су испуњени законом прописани услови, признаје на проналазак из било које области технике и у себи обухвата једно морално и више имовинских права носиоца патента.[70]

Треба истаћи да се заштита права код патената поред подношења кривичне пријаве за дело повреде проналазачког права, може остваривати и подношењем: тужбе за утврђивањем својства проналазача, тужбом због повреде права, тужбом за утврђивање права на заштиту, мерама инспекцијских и других органа на основу Закона о посебним овлашћењима ради ефикасне заштите права интелектуалне својине,[71] итд.

2.5 Неовлашћено коришћење туђег дизајна

Основни облик врши оно лице које на свом производу у промету неовлашћено употреби, у целости или делимично, туђи пријављени, односно заштићени дизајн производа (новчана казном или затвор до три године).
Под неовлашћеном употребом треба подразумевати производњу индустријског или занатског предмета за тржиште, на основу примене заштићеног дизајна, као и: употребу таквог производа у привредној делатности, складиштење таквог производа ради његовог стављања у промет, понуду таквог производа ради стављања у промет, стављање у промет таквог производа, увоз таквог производа и извоз таквог производа.

Заштитни објект кривичног дела неовлашћеног коришћења туђег дизајна је право на дизајн. Индустријским дизајном се сматра тродимензионални или дводимензионални изглед целог производа, или његовог дела, који је одређен његовим визуелним карактеристикама, посебно линијама, контурама, бојама, обликом, текстуром и/или материјалима од којих је производ сачињен, или којима

---

[69] *Ibidem*, стр. 57.
[70] Наташа Делић, *Повреда проналазачког права и неовлашћено коришћење туђег дизајна (чл. 201. и 202 КЗС)*, Привреда и право, бр. 1-4, 2006, стр. 49.
[71] Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, Сл. гласник РС 46/2006 и 104/2009.

је украшен, као и њиховом комбинацијом.[72] На овај начин се штите пре свега имовинска права аутора дизајна, односно његово право да ужива економску корист од искоришћавања заштићеног дизајна.

Блажи облик постоји онда када неко неовлашћено објави или на други начин учини доступним јавности предмет пријаве туђег дизајна, пре него што је објављен на начин утврђен законом (новчана казна или затвор до једне године). Управо код превара о којима ће бити речи касније може се видети да се извршиоци у циљу искоришћавања лаковерности или неопрезност грађана када им се неки званични орган обрати, користе веома лако околности да се не сумња у званичне дизајне и логое нпр. ФБИ. Битна карактеристика овог посебног кривичног дела неовлашћеног коришћења туђег дизајна је неовлашћено објављивање пре него што је дизајн објављен на начин утврђен законом. Законом предвиђен начин објављивања дизајна врши се у службеном гласилу надлежног органа након спроведеног поступка у коме аутор дизајна подноси пријаву за признање права на дизајн са свим неопходним елементима и доказима, а надлежни орган признато право на дизајн, са прописаним подацима, уписује у Регистар дизајна, а носиоцу дизајна издаје исправу о дизајну. Према томе, посебан облик кривичног дела неовлашћеног коришћења туђег дизајна постоји када је предмет пријаве туђег дизајна неовлашћено објављен, или се на други начин учини доступан јавности након подношења пријаве за признање права на дизајн надлежном органу, а пре него што је предмет пријаве дизајна на основу признатог права на дизајн објављен у службеном гласилу надлежног органа. Да би постојала кривица извршиоца овог кривичног дела неопходно је да се утврди постојање умишљаја који поред других битних обележја бића кривичног дела треба да обухвати и свест о томе да се радња извршења предузима неовлашћено и пре него што је предмет пријаве туђег дизајна објављен на начин предвиђен законом.[73] Код овог кривичног дела веома је значајно третирање заштићених дизајнова производа, наиме, у оваквој проблематици од значаја је питање схватања различитости заштићеног дизајна производа о чему је неопходно консултовати правила *lege artis* односне области у којој је дизајн ради. У оперативне сврхе неопходно је стриктно се држати евидетираних заштићених дизајнова производа и ангажовати стручно лице ради давања мишљења и налаза о разлици предметних објеката кривичног дела. Веома је битно да се у оваквим случајевима припадници полиције и органа гоњења понашају уздржано и да делају на бази мишљења стручних лица у датој области.

У Србији од 2008. године Министарству унутрашњих послова регистрован је свега један случај повреде проналазачког права и три случаја неовлашћеног коришћења туђег дизајна, док је у истом периоду регистровано чак 777 кривичних дела неовлашћеног искоришћавања ауторског дела (одузето 211.440

[72] Закон о правној заштити индустројског дизајна, Сл. гласник РС 104/2009.

[73] Наташа Делић, *Повреда проналазачког права и неовлашћено коришћење туђег дизајна (чл. 201. и 202 КЗС)*, Привреда и право, бр. 1-4, 2006, стр. 61.

фалсификованих књига и брошура, 4.886 техничких уређаја, 316.538 компакт дискова, итд.).[74]

[74] Пиратерија: на цени ноте и рецепти, Вечерње новости, 5.7.2011, интернет адреса: http://www.naslovi.net/2011-07-05/vecernje-novosti/piraterija-na-ceni-note-i , 11.09.2011.

3. КРИВИЧНА ДЕЛА ПРОТИВ ИМОВИНЕ

Као што је већ поменуто изменама Закона о организацији и надлежностима државних органа у борби против ВТК уврштена су, неправедно и непрактично изостављена, дела против имовине[75]. У оквиру ове групе најинтересантнија су следећа дела.

[75] Код којих се, да подсетимо, као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара.

3.1 Превара Члан 208. Кривичног законика[76]

Кривично дело Преваре чини лице које, у намери да себи или другом прибави противправну имовинску корист, доведе у заблуду некога лажним приказивањем или прикривањем чињеница или га одржава у заблуди и тиме га наведе да овај на штету своје или туђе имовине нешто учини или не учини, а запрећена је новчана казна или затвор до три године. Привилегован облик постоји када је извршилац имао само намеру да другог оштети, за шта је запрећена новчана казна или затвор до шест месеци. Превара има и два квалификована облика[77] када прибављена имовинска корист, или износ штете проузрокован основним

[76] Продужено кривично дело Превара из чл. 208. ст.1. у вези са чл. 33. и чл. 61. Кривичног законика. По оптужном предлогу Посебног тужилаштва КТ ВТК.бр.55/07, пресудом Окружног суда у Београду, због преваре почињене путем Интернета, оглашени су кривим Ј.Ш. (30) и његова девојка Т.Д. (29) из Новог Сада што су, у тачно неутврђеном периоду, од јануара до 15. јула 2007. године у Новом Саду, у намери да себи прибаве противправну имовинску корист, заједнички - лажним приказивањем чињеница да су представници Агенције "Exit apartments" која пружа услуге смештаја посетиоцима интернационалног музичког фестивала *"Exit 07",* са местом одржавања у Новом Саду, у трајању од 12.-16. јула 2007.године, користећи рачунар, рачунарске мреже и рачунарске податке, као и њихове производе у материјалном и електронском облику, довели у заблуду више британских држављана, укупно њих 29 (двадесетидевет) и, тиме их навели да им на штету своје имовине, а на име плаћања уговорених услуга смештаја, уплате на назначени рачун „Erste bank" укупно 314.960,00 динара што су учинили на тај начин, што је окр. Ј.Ш. претходно, у Новом Саду, закључио са *„Ерсте банком"* уговор о отварању девизног текућег рачуна, код Интернет сервис провајдера *„Neobee.net"* поднео Захтев за регистрацију интернационалног поддомена www.exitapartments.com на којем је потом његов познаник, користећи услуге web hostinga Интернет - провајдера *„Eunet",* израдио и поставио Интернет страницу израђену по детаљним упутствима првоокривљеног, а на којој су окривљени, њеним посетиоцима, на енглеском језику, нудили услуге дневног смештаја по цени од 30 до 60 еура, у једнособним и трособним апартманима хотела „Gymnas" у Новом Саду, са којим окривљени никада нису имали пословни однос и сарадњу те које су услуге, према датим упутствима на Интернет страници www.exitapartments.com, посетиоци сајта могли не само да резервишу, већ авансно и да плате - полажући депозит у висини од 30% од цене аранжмана на наведени рачун *„Ерсте банке",* што су чинили тзв. S.W.I.F.T.-ом, при чему су ошт. британски и ирски држављани, пре обављених плаћања односно, пре полагања депозита и доласка на фестивал *"Exit 07"* обављали комуникацију са другоокривљеном, позивањем њеног броја мобилног телефона +381964/668.... објављеног на страници и путем назначених електронских адреса info@exitapartments.com и exitapartments@neobee.net, која им се у тим приликама лажно представљала као менаџер за односе са јавношћу агенције „Exitapartments" из Новог Сада, одговарајући им на питања у вези плаћања, квалитета апартмана, положаја апартмана у односу на место одржавања Фестивала и сл., да би им након извршених уплата саопштавала место сусрета у Новом Саду одакле би требало да буду превежени до својих апартмана - где би уследило плаћање до пуног износа цене пруженог смештаја, па су, тако, и поред постигнутих договора, избегавали било какве контакте са оштећенима након њиховог доласка у Нови Сад , задржавајући на описан начин прибављену имовинску корист, с тим, што су од неколико ошт. британских држављана, осим уплаћеног депозита, добили у Новом Саду и готов новац у износу од 710 евра, на тај начин, што су се, по претходном договору, дана 10. 07. 2007. године у кафићу "Олива" у Булевару Ослобођења бр.133 у Новом Саду, сусрели са ошт. британским држављанима, на ком месту другоокривљеној, на име наводне доплате за смештај, предају готов новац у наведеном износу, а она њима печатом оверени Уговор и посетницу са натписом *„Agency for rent apartments",* да би их након тога, по инструкцијама окривљених, такси возило превезло до хотела „Путник" у Новом Саду где би схватили да су преварени.

[77] Код којих је могућа примена специјалних истражних мера и метода, јер спадају у групу дела из чл.504а. ЗКП, као и спровођење посебног поступка, чак и без постојања околности да је извршено од стране организоване криминалне групе.

облицима, прелази четристопедесет хиљада динара, за шта је прописана казна затвора од једне до осам година, односно када овај износ прелази милион и петсто хиљада динара, за шта је прописана казна затвора од две до десет година.

Радња кривичног дела је навођење неког лица да учини или не учини нешто што је штетно за његову или туђу имовину. Навођење представља стварање или учвршћивање, већ постојеће, одлуке код другог, да предузме неку активност, односно, да се уздржи од тога и, оно мора бити усмерено на имовину. Услов за постојање овог кривичног дела јесте да је оштећени под утицајем погрешно створене представе о некој чињеници нешто учинио, или пропустио да учини, и тиме нанео штету својој или туђој имовини. За доказивање овог дела неопходно је утврдити и намеру извршиоца кривичног дела, која се састоји у прибављању себи или другом противправне имовинске користи или, за привилеговани облик, само наношење штете другоме. Извршилац кривичног дела може бити свако лице, које мора поступати са умишљајем[78].

Специфичност облицима овог дела која им даје конотацију за област ВТК представља веза рачунара, рачунарских система и мрежа у вршењу оваквих превара. Интернет представља нову област деловања извршилаца кривичних дела који на преваран начин остварују имовинску корист, појава ове глобалне мреже даје ново оружје у рукама криминалаца за вршење класичних облика кривичних дела, дајући нова средства за прикривање извршилаца, за олакшавање варања, за прикривање преваре. Појава Интернета створила је неограничене могућности за вршење различитих кривичних дела чинећи доступним огроман број потенцијалних жртава и, скоро сасвим, елиминисала трошкове неопходне за организовање овог кривичног дела.

Извршиоци се служе погодношћу којом им Интернет пружа, скоро потпуну, анонимност, као и чињеницом да је дигиталне финансијске токове, који обично воде преко више држава, веома тешко пратити и утврдити крајњу дестинацију средстава. Социјални профили оштећених се веома разликују, а жртва преваре извршене путем Интернета може постати, готово, свако, због чега је неопходно увек бити на опрезу, јер извршиоци оваквих кривичних дела усавршавају начине обављања својих криминалних активности, прилагођавајући се најразличитијим условима и новостима на свом „тржишту“ и мењају циљне групе свог деловања, у зависности од сопствених потреба и могућности. Групе ових криминалаца су веома добро организоване, специјализоване су за одређене регионе, а да би Интернет преваре биле успешне, служе за најразличитијим методама за прибављање података о потенцијалним жртвама и склапање њиховог социолошког профила. Најбољи извор информација представљају сами оштећени, који посетом лажним рекламним сајтовима, или одговором на посебну врсту рекламних и мејл порука тзв. спам, остављају своје личне податке, а на основу прикупљених материјала се прави механизам преваре. У овом смислу значај оштећених али и њиховог страха и осећаја стида препознали су у САД и зато увели на сајту ИЦЗ[79] могућност пријављивања он лајн, без страха да ће неко открити њихов идентитет, или да ће бити осрамоћени. Са друге стране, они на овај начин остварују скоро

[78] Лазаревић, Љ, *Коментар кривичног законика Републике Србије,* Савремена администрација, Београд, 2006, стр. 585.

[79] http://www.ic3.gov/доступан 20.05.2010.год.

тренутни увид у разноврсност и променљивост овог облика криминалитета, па је лако и обавештавати ширу јавност о појавним облицима превара, и тиме остваривати ширу превенцију[80].

Листа ФТЦ[81] (Федералне комисије за трговину) од класичних 12 превара садржи:

- лажне пословне прилике
- ланчана писма
- преваре са радом у кући
- здравствене и дијететске преваре
- лаке прилике за зараду
- бесплатна роба
- прилике за инвестиције
- преварне масовне електронске поруке
- пакети за дескрембловање кабловске телевизије
- гарантовани кредити или зајмови
- промотивне понуде наградних путовања
- преваре у вези побољшања кредитних способности

Лажне пословне прилике са собом носе понуде и обећања прилика за прављење веће количине новца, уз веома мало труда. Уобичајено садрже бомбастичне крилатице као на пример: будите свој шеф, одредите себи време за рад, радите само неколико часова недељно, радите од куће. Обично ове врсте превара у предмету често садрже: остварите регуларни приход кроз он лајн аукције; Обогатите се, кликните; оставите свој рачунар да зарађује новац за Вас; искористите Интернет да зарадите; eBay Insider Secrets Revealed 6228. Ове преваре, у ствари, представљају пирамидалне шеме за преваре, пре или касније ова превара се открије и жртве се повлаче, па и превара престаје. За овакве преваре се обично каже да изгледају превише добро да би биле истините[82].

Ланчана писма. Код ове врсте превара које су познате и на нашим просторима али не у виртуелном окружењу, већ у реалности, бар на нашим просторима иде се на сујеверје, које је веома присутно у народу и рачуна се на вероватне, компулсивне, потезе преварених. Нарочито су значајне нове врсте оваквих превара присутне у окружењу социјалних мрежа. Овакве преваре са собом носе каратеристике и елементе других кривичних дела нпр. носе са собом црве увезане у линк који нуде у поруци или уношење неког злонамерног програма обавезног за читање дате поруке и сл.

Преваре еликсира живота и здравља као и дијеталне преваре користе несигурност људи у сопствено тело и здравствене околности. Оваква стања жртава их чине веома подложним и сугестибилнима за овакве преваре. И остали облици слично изгледају – увек је то превише лепо да би било стварно.

---

[80] Једна од скоријих активности САД у том смислу је и упозорење ИЦ3 доступно на Интернет адреси: http://www.ic3.gov/media/2011/110901.aspx последњи пут приступљено 08.09.2011.год.

[81] http://www.ftc.gov/opa/1998/07/dozen.shtm доступна 26.09.2009.год.

[82] Чак је и један Интернет сајт постављен под називом: www.lookstoogoodtobetrue.com услободном преводу изгледао би на на српском : www.изгледасувишедобродабибилоистинито.com

3.1.1 Интернет преваре – типологије ИЦЗ[83]

Методологија и основ класификовања у оквирима ИЦЗ су, са научног становишта, дискутабилни, али је прагматичност решења и њихова применљивост у супротстављању преварама основни разлог због којег се типологија о којој је реч наводи овде. Прва, од оних које се наводе за 2007 у извештају ИЦЗ, без неког већег значаја према редоследу, је превара кућних љубимаца[84]. Ова превара за објекат напада има и продавце и купце, преваранти дају оглас у новинама и он лајн у коме продају кућне љубимце. Купци затим шаљу новац, често у цену зарачунавају и трошкове доставе, након чега чекају и доставу љубимца којег су „купили“, али он, наравно, не стиже. Имамо и облик у којем се љубимци поклањају па се, накнадно, тражи новац за вакцину, или слично значајно средство, које бивши власник мора да дâ љубимцу. Познате су и методе које користе велики ланци продавница играчака и љубимаца у свету, када се деци допушта да се у просторијама фирме играју у посебно одређеним игралиштима са играчкама и љубимцима на продају па, чак, им се даје и да на недељу дана однесу љубимце кућама (само покушајте да замислите да се после недељу дана одвојите од љубимца, а после замислите како то да учините вашем детету) и сл. Када су мете продавци, преваранти се договарају о куповини љубимца а, након чега, шаљу чекове без покрића (или неки други недозвољени облик плаћања) који гласе на већи износ од оног који би се морао платити, уз објашњење, да вишак иде на име оног ко ће се старати о љубимцу, привремено, док га купац не преузме. Тада преварант продавцу даје упутства како да продавац трансферише средства, која су вишак привременом „стараоцу“, након чега, жртва шаље свој, потпуно легалан, новац на рачун или адресу преваранта. Док жртве схвате или добију обавештење од банке о превари, преваранти су већ увелико потрошили новац. За овакве случајеве веома је значајно утврдити токове новца и повезати у том смислу извршиоца и жртву, па чак и у случајевима да је новац потрошен. Тада дело постоји а иманентан је и имовинско правни захтев према учиниоцу, посебно је могуће искористити и тактичку могућност коју нуди институт одлагања кривичног гоњења од стране Јавног тужилаштва у чл. 236 ЗКП тач.1. и 7. у случајевима ако осумњичени прихвати извршење обавезе 1. да отклои штетну последицу насталу извршењем дела или накнади причињену штету, односно да изврпи обавезу установљену правоснажном одлуком суда.

Уцене или изнуде[85], ови облици превара[86] су веома чести у последње време, појавни облици су веома различити – најчешће се ради о неком DDoS напада[87] или

---

[83] Назив је скраћеница од Internet Crime Complaint Center (IC3) Интернет центра за притужбе и пријаве и представља заједнички пројекат Националног центра за борбу против криминала белог ооковратника (National White Collar Crime Center (NW3C))и ФБИ (Federal Bureau of Investigation (FBI)) доступан на http://www.ic3.gov/media/IC3-flyer.pdf последњи пут приступљено

[84] http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf доступан 15.12.2009.год. Ово је једна од варијација преваре са исплатом одређених износа унапред.

[85] Оба облика представљају друга имовинска дела али су овде наведени из разлога везаности за материју која се излаже и извор који се користи. Дакле треба их посматрати као дела из чл. 214 и 215 КЗ РС.

[86] Два су МО извршилаца – тзв. блеф напад – код којих извршилац иде на блефирање, где нема правог интереса за реалним нападом, док је други унапред припремљен и квалитетно испланиран,

о претњи да ће се о неком лицу објавити нешто што може шкодити угледу тог лица или њему блиског лица. У сваком од поменутих примера у намери прибављања противправне имовинске користи од жртве се захтева да учини нешто на штету своје или туђе имовине како не би трпела последице, у ову групу превара на Интернету могла би се уврстити једна појава која се назива сајбер ухођењем, неки говоре и о застрашивању[88]. Ово дело код нас није предвиђено у оригиналном облику али уколико садржи елементе преваре може се третирати као дело из чл. 208. КЗ Превара прикривених купаца (или превара трансфера средстава)[89] је она код које су такође у употреби чекови без покрића или фалсификовани чекови. Жртве се овде доводе у заблуду да их ангажује неки прикривени инвеститор како би за његов рачун а у своје име куповали или обилазили ресторане и дегустирали храну како би пружили своје оцене искустава као потрошача. Након првог контакта и давања сагласности следе новчане трансакције сличне претходно поменутим у случају кућних љубимаца, средство плаћања које је прослеђено жртви садржи номинални износ који је преко оног потребног за овакве услуге, при чему се од жртве тражи да тај вишак уплати трећем лицу од сопствених средстава а да за остатак обави договорено. Понекада преваранти овде злоупотребљавају обележја веома познатих фирми као што су МекДоналдс, Пепси, Гап, ФедЕкс и слично, чиме врше и друге облике кривичних дела. Једна од варијација овде је облик цимерске преваре у којој је преварант цимер који на исти начин као и претходне шаље новац и тражи да се вишак проследи негде другде, слична је варијација и превара за рентирање станова а и продаје некретнина (с тим да су овде много веће своте новца у питању). Превара усвојења (преваре у добротворне сврхе)[90]. Овај облик превара често стиже нежељеним и мејлом и веома често као облик спам –а[91], у суштини преварант апелује и циља на оне који су више осетљиви на туђу муку и који су веома осетљиви на добротворне позиве. Пошиљаоци оваквих порука се лажно представљају као представници неких

наравно овде говоримо чак и о плаћеним „револверашима“ хакерима који не презају ни од чега. Њима се плаћа да изврше „посао“ по сваку цену у шта су урачунати и ризици. Један од примера је Archiveus Trojan који копира садржај датотеке Моји документи у шифровану архиву а потом обрише датотеку са оригиналима, остављајући поруку да је неопходно укуцати 30-цифарну шифру коју можете добити куповином у онлајн апотеци на одређеној Интернет адреси.

[87] Посебно је опасно, што се мора напоменути, да извршиоци ову врсту напада нуде на Интернету у виду хакерске услуге, која се продаје или програма који врши овакве нападе (ransomware). Када су у питању ови програми они преузимају какве важне датотеке и шифрирају их и склањају на неко власницима недоступно место након чега упућују захтев за откупнином власнику. Цене се крећу од 10-20$ за сат времена напада до 40$ за два сата константног напада, док цео дан вреди око 100$. У неким случајевима веома професионално се нуде маркетиншки коректно попусти и до 20% за првих 100 купаца. Неки од програма коришћених за ransomware су Delf.ck, Gpcode.AK, TROJ.RANSOM.A

[88] http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf p.20. доступна 09.04.2010.

[89] *Ibid*

[90] *Ibid*.

[91] Што се тиче термина сматра се да порекло води из једног скеча чувене енглеске групе комичара Monty Pyton flying circus, више о томе на
http://en.wikipedia.org/wiki/Spam_(electronic)#Origin_of_the_term доступном 20.03.2010.год.
Негативни ефекти спама су: троши време онога ко га прима и чита, уколико нема заштиту; заштита од спама некад може обухватити и фајлове који нису спам; он користи капацитете конекције и заузима базе података; за креирање веће количине спама користе се зомби мреже; често се користи за дистрибуцију злоћудних програма.

добротворних организација (на пример УНИЦЕФ или УНЕСЦО, а специфично за Британију БААФ (British Association for Adoption and Fostering – BAAF), регистрована организација за адоптивно и тазбинско сродство) и у њихово име а, у ствари, за свој рачун траже уплате одређених средстава. Оно чиме преварант заокупљује пажњу жртве је носећа прича, обично, о неком убогом детету – сирочету или напуштеном од стране родитеља у циљу убеђивања исте да поднесе захтев за усвојење, након чега се од жртве тражи да плати трошкове процесирања захтева. Једна друга варијација је да мејл садржи број рачуна родитеља детета које је у питању, уз шта се објашњава да је тај једини живи родитељ оболео од неке смртоносне болести и да му није остало много, уз шта је овај родитељ енормно богат и требало би да том детету остави већу суму новца након смрти, при чему се често користи лого БААФ у циљу мамљења новца за захтев и формуларе. У Србији је било случајева везаних за преваре овог облика у смислу трансфера новчаних средстава намењених особама у иностранству – у земљама Африке. Романтичне преваре[92] за предмет напада имају особе које користе мреже за судare на слепо и социјалне мреже. Након контакта, овим путем, преварант тежи задобијању поверења жртве кроз различите облике изјава о наклоности или изливима љубави, често преваранти живе далеко од жртве (у већини случајева у другој земљи), након чега преварант изражава незадрживу жељу да се са жртвом физички сретне. Уколико жртва пристане онда креће зачкољица – преварант нема довољно новца да допутује на место које је договорено за сусрет и захтева од жртве да пошаље новац како би могао да допутује да би се видели. Након пријема новца превара се развија на различите начине, тада се дају најразличитија објашњења типа преварант је због плејаде непредвидивих догађаја у међувремену (или чешће у току путовања, услед, на пример несреће на путу) напрасно упућен у болницу и неопходно је да се покрију трошкови лечења, брат преваранта је отет па је неопходно да се прикупе средства за ослобађање и сл[93]. У свакој даљој секвенци догађаја преварант тражи још новца док жртва не пресуши или престане да верује обмани. Преваре које укључују логое и обележја ФБИ[94]. Преваре овог типа садрже у себи и елементе изнуде, јер постоји озбиљна претња која стоји иза оваквих облика мејлова, претња иманентне принуде од стране ФБИ обзиром да се користе различите методе обмане, обично позивају на постојећу финансијску истрагу у току тако да су грађани којима је овакав захтев упућен у страху од могућих последица непружања информација неопходних за овакву истрагу. Шта више жртве се доводе и у заблуду, не само да ће оваквим облицима сарадње представљати добре кооперативне грађане, већ и да ће добро профитирати. Преварни извор за средства којима би лице било награђено, у описаним случајевима, има најразличитије порекло. Неки од ових мејлова су издати у име неких од стварних званичника ФБИ (заменика директора Johna S. Pistolea, или самог директора Roberta Muellera[95] како би се додала, још званичнија, и озбиљнија нота) па се иде и до граница којима се оштећени обмањују да ће, уколико не пруже

[92] *Ibid*.

[93] Више о овоме можете пронаћи на http://www.prevara.info/index.php?option=com_content&task=view&id=283&Itemid=7 доступном 14.01.2010.год.

[94] http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf доступан 15.12.2009.

[95] *Ibid*. str.11.

податке, и они постати предмет истраге о тероризму, или да ће бити новчано кажњени и сл. У овом смислу треба назначити да на овај начин ни једна полицијска организација[96] не би контактирала појединце а камо ли ФБИ, нарочито у погледу финансијских личних података грађана кроз различите облике незахтеваних или нежељених мејлова[97]. Изузетно карактеристично за ове облике мејлова јесте граматичка и писмена неподударност и кардиналне граматичке грешке. У 2008. год. веома чест је био облик превара различитих техника социјалног инжењеринга фокусиран на близак лични контакт комбинован са рачунарским упадом[98]. Превара почиње остваривањем неовлашћеног упада и остваривањем неовлашћеног приступа и мејл налогу одређеног лица, након чега се користи за слање спам мејлова контактима оштећеног власника мејл налога, након чега постављају у описаним спам порукама превару која је слична нигеријским – „419" преварама, од којих је један од многих сценарија да је лице које је у питању на путу у Нигерији опљачкано и да му је неопходна нека сума новца како би могао да се врати. У оваквој ситуацији сви прави пријатељи би притекли у помоћ, али не без провере, но... Уколико се и деси да неко од пријатеља поверује и пошаље, наравно, уследиће нови захтеви за новцем и то док не пресуши извор или жртва не схвати превару. Варијација претходних превара је превара прекомерне исплате[99] код које се захтева да се преплаћени део исплате (извршене лажним или чеком без покрића) пошаље назад исплатиоцу од новца жртве. Један од веома честих облика су и Он лајн аукцијске преваре[100] (познате и као преваре распродаја) често се одређују као лажне продаје или аукције на Интернету предмета, ствари и робе кроз или преко аукцијских сајтова који су непостојећи или лажни, или преко реалних аукцијских сајтова али без намере да се роба (ствар предмет) испоручи. Посебан облик у овом моменту је румунска акукцијска превара[101] Често извршиоци отварају налог на и бају (или неком другом сајту) и врше неколико значајних трансакција, како би остварили добар чланski рејтинг[102] чиме би привукли могуће

[96] Веома је интересантан случај превараната који су поставили сајтове за продају лекова на црно како би изнуђивали новац од купаца са тих сајтова лажно се представљајући као агенти ФДА (Food and Drugs Administration (FDA)), што говори о перфидности креативности у приступима и веома великој прилагодљивости извршилаца, више о овоме на:
http://www.sophos.com/blogs/gc/g/2010/01/04/bogus-fda-agents-scam-online-drug-purchasers/ доступан 10.01.2010.год

[97] За овакве случајеве неопходно је донети прописе којима се регулишу системи опт ин или опт аут у случајевима незахтеваних информација, као и употребе личних података без знања корисника. У ЕУ је то решено Директивом о приватности и електронским комуникацијама „Directive 2002-22-EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services", Official Journal of the European Communities, L108/51-77, од 24.04.2002.

[98] http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf доступан 15.12.2009.

[99] *Ibid*

[100] www.ic3.gov/media/initiatives/econbrief.pdf а и на www.ifccfbi.gov доступан 25.12.2009.год.

[101] Ово је ништа друго до посебан облик за који је везана вероватно организована група која води порекло из Румуније, карактеристике су да се продавац издаје као особа из САД, али она обично упућује на лице које њен сарадник у некој европској земљи, користећи MoneyGram за пренос новца, због необавезности постојања потпуне идентификације лица које преузима новац, нема потребе ни за МТЦН money transfer control number (MTCN) бројем нити за тајним одговором на питање пошиљаоца.

[102] Овај рејтинг није замишљен као начин превенције специфичних одређених преварних радњи, он представља субјективне утиске искустава корисника сумирана на једном месту. У

жртве. Оног тренутка када га остваре почињу са продајом скупе робе за своје жртве. Посебан облик аукцијских превара су тзв. „напумпај и одбаци“ (pump and dump) преваре. Овај облик превара је облик који злоупотребљава правила берзе и комбинује берзанско пословање са класичним уличним варањем. Ова превара користи обрнуту психологију панике, користећи позитивне вибрације масовним облицима спама[103] позивајући Интернет кориснике да купују одређену врсту акција на берзи, које су са великим потенцијалом услед неког неочекиваног догађаја. Од посебне вредности су тзв. лажне преваре, код којих је основна карактеристика давање бомбастичног и веома продорног наслова у новинама или медијима уопште, типа „Самсунг продаје бренднејм рачунаре са руткитом“[104] а који је усмерен на наношење комерцијалне штете неком од произвођача и дистрибутера. Веома интересантна је превара лажних акредитива[105], У циљу остваривања преваре најразличитијих неповерљивих купаца на Интернету, нарочито у случајевима Интернет аукција, преваранти нуде или предлажу увођење треће стране, такозване акредитивне службе[106] како би оштећеног или жртву намамили да им исплати одређену суму новца која би служила наводној куповини. Жртва у овом случају није свесна да је извршилац спуфовао (фалсификовао) легитимну акредитивну службу, и зато и шаље новац лажном акредитивном службенику и тада је новац већ изгубљен[107]. Све описано представља облике превара инвестирања, које се јављају у једном од подтипова у облику пирамидалних превара, добро познатих у Србији деведесетих година. У 2009. год. интересантна је превара „плаћених убица“[108] која представља подтип изнуђивачких или уцењивачких превара. Жртва прима електронску пошту од члана организације нпр. “Ishmael Ghost Islamic Group” који тврди да је послат да убије примаоца

одређеним случајевима извршиоци преузму идентитет неког од добрих продаваца у циљу вршења преваре, зато треба обратити пажњу на постојање скоријих продаја и трансакција које је продавац вршио и на њихов бонитет.

[103] Уобичајено је да се оваква порука шири путем инфициране мреже ботова. Један од примера је Prime Time stores напад из 2005.год. Тада је извештај са берзе о овој фирми стигао у облику ПДФ датотеке, која је тада лакше пролазила филтере мејл сервера.

[104] Само неколико дана пре овог наслова владала је грозница у објављивању вести према којој Самсунг дистрибуира рачунаре са крајмвером, да би дошло до демантија на сајту: http://sunbeltblog.blogspot.com/2011/03/samsung-laptops-do-not-have-keylogger.html последњи пут приступљено 01.04.2011.год.

[105] *Ibid.*

[106] The escrow service представља средство за превенцију превара – то су, по дефиницији, независна трећа лица која примају новац купаца и омогућавају и обезбеђују за продавце доставу купљене робе, и притом предају новац продавцу тек оног тренутка када су добили обавештење да је купац примио робу. Овај облик пословања сличан је документарном акредитиву, који се користи као средство обезбеђења купопродаје робе на удаљеним локацијама.

[107] Приликом обављања трансакције пре него што искористите акредитивну службу прво је неопходно на http://www.networksolutions.com (или неком другом бесплатном сајту) проверити да ли је валидан домен; затим захтевати листу Интернет трговаца који користе ову акредитивну службу, па уколико је листа краћа од 10 не обавезно покушати извршити трансакцију, уколико их има више проверити и ове фирме кроз претходно поменути сајт (почните са дна или средине листе), уколико је било који контакт акредитивне службе исти као и продавчев то је знак упозорења; неопходно је пазити на ситуације у којима овакве акредитивне службе као званичне мејл адресе користе бесплатне провајдере као hotmail, gmail, yahoo.

[108] http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf стр.11 доступна 09.04.2010.год.

поруке и његову породицу. Као разлог овог смакнућа пошиљалац наводи наводни злочин против члана ове братије који је жртва учинила. У изненадном обрту који је уследио када је неки члан братства указао пошиљаоцу ове поруке да познаје неког од рођака из седмог колена примаоца ове поруке и тој информацији следећег захтева за помиловање жртве од стране тог члана братства, неопходно је да жртва плати свој и живот својих ближњих (800 долара које ће послати преко Western Union –а или Money Gram –а у Велику Британију за миграцију Исламских патриота из САД) дајући му обично 72 часа да то уради. Превара Астролошког читања - жртва прима спам или искачућу поруку о бесплатном астролошком очитавању информација, жртва мора дати податке о датуму и месту свог рођења. Након бесплатног текста о судбини по основу астролошких карактеристика, од жртве се тражи одређена новчана сума за пуну наталну карту уз обећавање постојања нечег позитивног као догађаја садржаног у овој карти, жртва плаћа новац али наравно не добија ништа, а у већини случајева астролог је недоступан за пријем мејлова. Превара економске стимулације[109] користећи ситуацију велике економске кризе и информације о пакетима економске помоћи у САД као и говоре и исечке тих говора председника Обаме, одређени број америчких грађана варан је путем нежељених телефонских позива са снимцима говора који личе на Обамине којима их позива на приступање одређеним сајтовима www.nevergiveitback.com или www.myfedmoney.com у циљу добијања економске стимулативне помоћи. Наравно, да би се добила ова помоћ, неопходно је унети многе личне податке и платити трошкове обраде ових информација 28 долара, након чега нема никакве економске помоћи. Сличан систем користе и преваре за сајтове о пословима, где жртве дају мноштво личних података, при чему се обећавају послови код куће, слање посебних софтвера за обављање тих послова, плаћање на сат, или плате од неколико хиљада долара недељно. Овакви сајтови су веома убедљиви, толико да су многе жртве уновчавале преварне чекове или примале непостојеће или постојеће новчане дознаке са потребом даљег трансфера већих сума новца и сл. Друга подврста ове преваре је да се оглашавају оваква лица жртве као незапослени али, да би се огласили, извршиоци од жртава траже податке о њиховим рачунима и претходним примањима, шта више, траже копије последњих чекова плата, након чега користе овакве податке за даље криминалне активности. Лажни антивирус програми и искачући рекламни садржаји којима се тест скенирањем на рачунару жртве наводно проналазе вируси и тројанци и за које се препоручује баш неки софтвер којим се они могу скинути, а уколико жртва кликне на тај линк њој се на рачунар даунлоадује злоћудни (малициозни) код у облику тројанаца, вируса или килогера. Посебно се наглашава проблематика стручних превараната, као једна врста инсајдерске преваре код које запослени у одређеној добростојећој фирми злоупотребљава ресурсе фирме како би варао жртве, али и саму фирму. Проблем код ове преваре је проток времена од извршења дела до његовог откривања од стране оштећених[110].

---

109 *Ibid.*

110 Тзв. АЦХ (ACH) преваре. У периоду јануар 2008. Decembar 2009. 1,843 случаја стручних превара из 106 земаља обрађено је од стране сертификованих стручњака у овом пољу, тренд се не смањује ни у 2010.год. Више на: http://www.govinfosecurity.com/articles.php?art_id=2601 последњи пут приступљено 04.06.2010.год

Од бројних врста Интернет превара, издвојићемо нигеријско писмо, које представља синоним за лажне е-маил поруке, различитог квалитета у којима се потенцијална жртва обавештења о околности: - да јој је нека блиска особа у иностранству и да се налази у невољи, због чега је неопходно послати јој одређен новчани износ; - о наследству за које је потребно платити таксе; - писмом у коме се тражи помоћ за трансфер новчаног износа за који „помоћник“ – жртва, добија велику провизију; - повољна понуда за атрактиван посао; - понуда за склапање брака[111].

Као веома специфичан облик преваре са међународним прерогативима и који наноси штету у милионима долара, нигеријска превара заслужује посебну пажњу и посебну анализу. Обзиром да на простору Западне Африке функционише велики број организованих криминалних група специјализованих за вршење превара, као и да је њихово поље деловања фокусирано на Интернет, као глобално распрострањено средство за комуникацију. Електронско банкарство и електронско пословање, додатно су олакшали извршење кривичних дела преваре која се врше злоупотребом рачунара. Услуга електронског трансфера новца преко система за пренос новца на даљину (нпр. *Western Union-a* или *MoneyGram-a)* у комбинацији са лаковерношћу жртава и значајном убедљивошћу извршилаца омогућили су им прибављање противправне имовинске користи од оштећених лица широм света, скоро потпуно некажњено.

Грађани Републике Србије који користе Интернет изложени су ризику који је настао као последица деловања ових криминалних група. Државне институције, јавне установе и предузећа са наше територије такође су изложене ризику.

На нашој територији Нигеријским преварама оштећено је више физичких и правних лица, а кривична дела су извршена са подручја Нигерије, Сенегала и Бенина. Материјално оштећење у овим случајевима износило је укупно 60.000 америчких долара[112]. Међународна полицијска сарадња са државама из којих су извршена ова кривична дела, до данас није довела до значајнијих резултата. Превентивна улога полиције и других државних органа, као и медија, од кључног је значаја када је спречавање Нигеријских превара на територији Републике Србије у питању.

Нигеријска превара, или превара позната под називом „Превара 419“ појавила се у раним 80-тим годинама, са наглим економским развојем Републике Нигерије, који се заснивао на употреби нафтних ресурса. Неколико незапослених студената са нигеријског универзитета почело је да употребљава методе ове преваре како би довели у заблуду пословне људе са Запада који су били заинтересовани за „тајанствене“ послове у Нигеријском нафтном сектору, а касније су те методе почели да употребљавају и на широј популацији. Извршиоци ових превара су раних 80-тих и средином 90-тих извршили преваре над разним компанијама шаљући поруке путем писама, факсом или телексом. Са све већом употребом електронских порука и рачунарских програма који су имали могућност да шаљу велики број порука на различите електронске адресе (*Енгл. e-mail*

---

111 Упореди са Урошевић, В.: „Нигеријске преваре у Републици Србији“, часопис Безбедност, број 3/09, стр. 147.

112 Урошевић, В.: „Нигеријске преваре у Републици Србији“, часопис Безбедност, број 3/09, стр.145-157.

harvesting software), омогућено је да, у почетку, слање електронских порука буде врло јефтино, а касније и бесплатно. У току прве деценије 21-ог века „Превара 419“ постала је веома популаран начин извршења кривичних дела преваре у Африци, Азији и Источној Европи, а у последње време и у Северној Америци, Западној Европи (углавном Великој Британији) и Аустралији.

„Превара 419“, као израз за Нигеријску превару, добила је назив по члану број 419 Нигеријског кривичног закона (који је део поглавља 38) под називом „Прибављање имовине помоћу преварних радњи: Превара“ који дефинише ово кривично дело[113]. Америчко друштво за дијалектику је утврдило да се израз „Превара 419“ користи од 1992. године.

Под нигеријском преваром подразумева се метода вршења кривичног дела преваре уз помоћ рачунара, и најчешће почиње писмом или електронском поруком која је тако осмишљена да изгледа као да је намерно послата примаоцу поруке. Радња извршења Нигеријске преваре углавном почиње убеђивањем „жртве“ преваре да учествује у подели одређених новчаних фондова ако унапред уплати одређени новчани износ који је у највећем броју случајева неупоредиво мањи од оног износа који би требала да добије као корист од тог фонда[114]. Методи који се у овим случајевима користе почивају на социјалном инжењерингу.

Електронском поруком (најчешће *спам* поруком) од примаоца поруке се тражи помоћ за трансфер великих новчаних износа, за који ће након обављеног трансфера добити одређени проценат као надокнаду. У оваквим порукама се нпр. наводи да је:

- Реч о великој суми новца, која је позната само пошиљаоцу поруке, и да он чека да буде исплаћена као резултат одређених банкарских малверзација и сл.
- Пошиљалац поруке члан нигеријске владе или нигеријске војске који покушава да изнесе већу количину новца из Нигерије, али да му је за то потребна помоћ из иностранства.
- Пошиљалац поруке спреман да новац подели са оним ко му помогне да изврши трансфер одређене суме новца (нпр. прање новца).
- Тајност посла апсолутна потреба, пошто би корумпирани званичници Нигерије присвојили новац за себе уколико би сазнали да он постоји[115].

3.1.2 Начин извршења нигеријске преваре

---

[113] Chawki, M.: Nigeria Tackles Advance Fee Fraud, Journal of Information, Law & Technology, University of Warwick, 2009, p. 2. Наведено према Урошевић, В.: „Нигеријске преваре у Републици Србији“, часопис Безбедност, број 3/09, стр.145-157.

[114] Smith, R. Holmes, M. Kaufmann, P.: Nigerian Advance Fee Fraud, Trends and Issues in crime and criminal justice, Australian Institute of Criminology, 1999, p.1. Наведено према Урошевић, В.: „Нигеријске преваре у Републици Србији“, часопис Безбедност, број 3/09, стр.145-157.

[115] Buchanan, J. Grant, A.: Investigating and Prosecuting Nigerian Fraud, United states attorneys bulletin, САД, 2001, p. 40. Наведено према Урошевић, В.: „Нигеријске преваре у Републици Србији“, часопис Безбедност, број 3/09, стр.145-157.

Извршиоци кривичног дела преваре шаљу електронске поруке корисницима Интернета, са намером да понуде неки примамљив посао у нади да ће жртва преваре на крају уплатити одређени износ новца на име његове реализације (нпр. разне измишљене надокнаде за ангажовање стручних лица или адвокате, за издавање потребних дозвола за реализацију посла, уплате административних такси и друго). Ове електронске поруке или писма насловљена су уопштено на сваког примаоца поруке, и из њих се не може видети коме се пошиљалац обраћа, али је њихов контекст такав да прималац поруке лако може помислити да се порука односи управо на њега. Оне углавном почињу реченицама као што су: "*From the desk of Mr. [Name]...*" (из канцеларије господина ...), *"Your assistance is needed..."* (Ваша помоћ је неопходна), и другим сличним реченицама којима се примаоцу поруке придаје на важности и значају, и којима се методом социјалног инжењеринга будућа „жртва“ преваре наводи да помисли да је њена помоћ неопходна да би се одређена радња извршила (нпр. трансфер новца, уручивање наследства и др.).[116] Детаљи у вези порука могу да се разликују, али садржина самог писма које стиже жртвама преваре најчешће се односи на то да особа која је наводни пошиљалац поруке није у могућности да сама изврши одређене радње, те да јој је зато потребна помоћ примаоца поруке. Такав је случај са Нигеријским писмима у којима се као пошиљалац наводи особа која је запослена у владином сектору или у некој банци, и која је сазнала за огромну количину новца или злата, коме не може прићи директно, обично зато што он или она нема право да то учини, па јој је потребна друга особа преко које ће се извршити трансфер тог новца. Особе које се наводе у овим порукама, најчешће стварно постоје, али су њихови идентитети украдени без њиховог знања и користе се од стране извршилаца кривичних дела како би се прикрио њихов прави идентитет, или како би се снагом ауторитета одређених лица улило поверење жртвама преваре и придобило њихово поверење. Карактер, личне особине и сл., лица са којима жртве преваре, наводно, комуницирају измишљени су од стране извршилаца кривичних дела а током комуникације њихове особине се прилагођавају профилу жртве преваре ради задобијања њених симпатија и њеног поверења. Често се дешава да се поруке шаљу у име измишљених ликова као што су нпр. деца или супруге афричких или индонезијских лидера и диктатора који поседују одређено крадено благо, запослено лице у банци које познаје неку јако болесну богату особу која нема рођаке, или богатог странца који је ставио новац у депозит пре него што је погинуо у авионској несрећи (неостављајући за собом наследника или тестамент) итд.

У тим порукама помињу се суме новца које се крећу и до неколико милијарди америчких долара, затим злато, „прљав“ новац на банковним рачунима, „крвави дијаманти“, серије чекова и др. Суме новца укључују милионе долара које

---

116 Социјални инжињеринг је акт манипулације којим се људи наводе да одају поверљиве информације о себи. Ова техника заснива се на ометању пажње одређеног лица у циљу прикупљања информација, које оно, иначе, не би одало, а како би се ти подаци касније злоупотребили (ради одавања корисничких имена, лозинки или, нпр. података о платним картицама). Све методе социјалног инжињеринга заснивају се на специфичним правилностима у процесу доношења одлука познатијем као „погрешна когниција“ (грешке у когнитивном процесу мишљења, наравно подстакнуте активностима извршилаца) која представља образац неправилног просуђивања људи који се појављују у одређеним, специфичним ситуацијама. Неки говоре о „багу у људском уму“.

ће наводни инвеститори на крају посла поделити са жртвом преваре, а проценат зараде који се обећава креће се и до 40 % од суме новца која је предмет „посла“. Већина прималаца ових електронских порука на те поруке најчешће не одговара (пошто знају да се ради о врсти преваре), а Интернет сервис провајдери их приликом филтрирања на својим серверима најчешће одвајају, и пре него што дођу до крајњих корисника, помоћу „црних листа“ у оквиру којих се за анализу и елиминацију користе ажурирани спискови ИП адреса са којих ове електронске поруке најчешће пристижу. Мали проценат корисника ипак прима овакве поруке, које пролазе кроз филтере Интернет сервис провајдера, и ступа у контакт са извршиоцима кривичних дела. То је довољно да „идејни творци“ ових превара шаљу милионе електронских порука, пошто рачунају да ће један мањи проценат корисника ипак ступити у контакт са њима, након што их прочита. Овде је modus извршилаца такав да циљају на неодређене жртве у броју и карактеристикама. Дакле, у питању је клопка или замка неодређене жртве, без неких специфичних карактеристика, насупрот томе постоје и циљане клопке чији modus је карактерисчан за друге облике кривичних дела као нпр. код циљаног (спир) фишинга.

Оштећена лица се методама социјалног инжењеринга при комуникацији наводе да уплате један мали проценат од укупне суме новца која је предмет „посла“. Уплату тих новчаних износа извршиоци кривичних дела траже како би се нпр. надокнадили одређени трошкови које сноси неко измишљено лице (нпр. трошкови подмићивања, накнаде у банкама, трошкови адвоката и др) да би дошло до предметног новца, од којег је један део жртви преваре обећан као надокнада. Ове новчане уплате које се траже од жртава преваре представљају онај део новца за који ће жртва, након што открије да је преварена, бити оштећена, док живи у убеђењу да ће зарадити огромне суме новца које извршиоци кривичних дела обећавају у комуникацији. Уједно, та сума новца представља и противправну имовинску корист коју извршиоци ових кривичних дела остварују извршењем кривичног дела преваре.

У преваре су, често, умешани и службеници државних органа Нигерије, а дешава се и да се ради контакта остављају и подаци одређених државних званичника, који учествују у најтежим преварама овог типа. Поред извршилаца ових кривичних дела из Нигерије, саизвршиоци и помагачи се налазе и у другим државама широм планете. Примећено је и да се овим врстама преваре баве и извршиоци кривичних дела преваре из Сенегала, Гане, Обале Слоноваче, Тога, Бенина, Буркина Фасо и других држава Афричког континента. Жртва преваре која покуша да пронађе позадину овакве преваре, често, на крају сама може да дође до закључка да су сви делови приче изузетно добро осмишљени и професионално повезани[117]. Извршиоци кривичних дела чак успевају и да преваре чланове богатих инвеститорских група или других пословних окружења, те да им на тај начин причине огромну материјалну штету и наруше углед код пословних партнера. Највећи број извршилаца ових кривичних дела припада мањим организованим криминалним групама, али се понекад дешава да функционишу и самостално. Уколико извршиоци кривичних дела нису добро организовани, онда не могу да изврше преваре већих размера и оштете веће и богатије компаније, али су јако

[117] Ово је добро описао Глени, М. Мекмафија, Самиздат, Б92. 2008. Београд

опасни за средњу класу грађана и мала предузећа. Овакве преваре резултирају и остваривањем мање противправне имовинске користи, али су њихове размере такође јако велике када се у обзир узме број лица којима је причињена материјална штета.

Ако жртва преваре пристане на понуђени „посао“, извршиоци кривичних дела јој шаљу један или више фалсификованих докумената са лажним печатима, потписима, лажном садржином и сл.. Извршиоци који врше ове преваре често користе лажне податке и крађу идентитета, те тако врло често при представљању користе фотографије других лица које су прикупили са Интернета како би се лажно представили оштећенима.

Након што оштећени уплати одређени новчани износ према инструкцијама извршилаца кривичних дела следи одлагање новчаних трансакција везаних за исплату обећане суме новца. Пошто се исплата не одвија по напред уговореном плану, извршиоци кривичног дела се (и даље се лажно представљајући) правдају изговорима као што су: „За реализацију посла нам је потребан новац да подмитимо службеника банке. Можете ли Ви да нам пошаљете зајам?“ или „Како би вам било дозвољено да будете странка у трансакцији, потребно је да уплатите Нигеријској банци износ од 100.000 долара“ и др. Стално се појављују нови трошкови за оштећеног на име реализације посла и траже нова одлагања, стално се обећава „експресна“ исплата новца, уз убеђивање жртве преваре да ће јој се улагање у договорени посао вишеструко исплатити. Невероватно је колико људи пада на овакве варке.

Психолошки притисак на жртву преваре додатан је када се „Нигеријска страна“ тј. извршиоци кривичног дела, у циљу плаћања одређене надокнаде, жале на то да морају нпр. да продају ствари које им припадају као што су личне ствари, кућа и др. како би реализовали неки посао, или се указује на разлику у животном стандарду становника Афричког континента и на „развијеном Западу“, на који начин се изазива грижа савест и самилост код жртве преваре. Притисак се на жртве додатно се врши и навођењем да је тајност „посла“ јако потребна, пошто би корумпирани званичници присвојили новац за себе уколико би сазнали да он постоји[118]. Један од аспеката који треба имати у оваквим случајевима је и „алавост“ жртве, са којом извршиоци и рачунају. Овакав притисак, понекад, жртва преваре додатно врши и сама над собом, нпр. у случају када извршиоцима кривичног дела преда новац са намером да оствари зараду, након чега има осећај да мора да заврши посао који је започела да би макар повратила уложени новац. Неке жртве чак верују и да ће надмудрити извршиоце кривичних дела ако наставе комуникацију, те да ће их открити и натерати да им врате новац. Жртве на ову идеју долазе и због тога што извршиоци кривичних дела, знајући за то, намерно при писању текста себе представљају као неуке и наивне, па се чини да их људи, веома лако, могу преварити зато што су образованији и сл.

Кључна чињеница при оваквим преварама је да се обећани трансфер новца према жртви преваре неће никада ни десити, пошто новац (или друге материјалне вредности и драгоцености као нпр. злато или дијаманти) у стварности не постоје.

---

[118] Buchanan, J. Grant, A.: Investigating and Prosecuting Nigerian Fraud, United states attorneys bullet in, САД, 2001, p. 40. Наведено према Урошевић, В.: „Нигеријске преваре у Републици Србији“, часопис Безбедност, број 3/09, стр.145-157.

Извршиоци кривичних дела се ослањају на чињеницу да ће, за време које прође, док жртва схвати да је преварена, новчани трансфер који је она извршила на њихове рачуне бити реализован, те да оштећени неће стићи на време да блокира трансфер. Новац који жртва шаље извршиоци кривичног дела преузимају обично преко електронских трансакција на такав начин да их је немогуће открити и ухватити (ангажују помагаче који са фалсификованом документацијом, ангажују муле (мазге) за новац, које отварају рачуне уз малу новчану надокнаду, без знања о чему се заправо ради, са којих подижу новац, након чега га предају извршиоцу кривичног дела). Извршиоци кривичног дела најчешће траже да им се новац исплати преко Western Union-a и MoneyGram-a, и при том жртви преваре шаљу инструкције за уплату. Разлог за то је брзина исплате новца, која смањује могућност откривања од стране полиције. Овакав начин слања новца је иреверзибилан, није могуће ући му у траг, а потребни су само подаци који су довољни за исплату (идентификатор трансакције у облику броја и лозинка), тако да омогућују велику анонимност лицу које преузима новац.

У најекстремнијим случајевима жртва преваре не схвата да је преварена ни након што се трансфер новца реализује. Верзије Нигеријске преваре су тако осмишљене да се стварају чак и лажни уговори по којима се новац, који жртва преваре уплаћује на име реализације неког посла, сматра легалним пословним улагањем, тако да жртва није убеђена да ради било шта илегално, и не сумња да може доћи до злоупотребе њеног поверења. Због постојања уговора, који представља вешто укомпоновано средство социјалног инжењеринга, жртва преваре је убеђена и да је правно заштићена. У случају да оштећени и посумња у истинитост приче, извршиоци кривичних дела ће понудити и да се лично упознају са жртвом преваре, инсистираће на томе да је повежу са „стручним људима“ као што су нпр. брокери, банкари и др., који могу да потврде истинитост њихових навода и сл. На такав начин жртва преваре уплаћује новац без осећаја да је учинила било шта на своју штету. У оваквом емоционалном стању жртве, извршилац кривичног дела може тражити још новчаних зајмова и исплату одређене суме новца унапред, уз већ поменуте фиктивне уговоре, држећи оштећеног константно у заблуди. Овакви случајеви, често, се и не пријављују пошто жртва преваре не схвата да је оштећена, а, понекад, не жели да призна ту чињеницу или пријављивање одлаже све док, након дужег времена, сама не схвати да је преварена. Наравно, и оваква писана акта могу бити веома значајна приликом доказивања кривичног дела, а посебно уколико су она размењивана путем електронске поште са жртвом.

Електронске поруке, као што су спам-ови са оваквом садржином, најчешће се шаљу из Интернет кафеа који су опремљени са сателитским Интернетом. Количина електронских порука које се шаљу путем спам-а из Нигерије забринуле су многе државне органе широм света. Поред тога што успоравају рад рачунара корисника на Интернету, ове поруке подижу и цену коштања употребе Интернета крајњим корисницима пошто Интернет сервис провајдери морају додатно да улажу у своју опрему како би их заштитили од нежељене електронске поште овог типа[119].

[119] Longe, B. Chiemeke, C.: Cyber Crime and Criminality in Nigeria – What Roles are Internet Access Points in Playing?, European Journal of Social Sciences, 2008., p. 138. Наведено према

Код нас је Законом о електросним комуникацијама чл.118. и 119. увео обавезу оператера да својим корисницима омогуће филтрирање шкодљивих и незатражених порука. Адресе прималаца и садржај електронских порука се копира и преноси на *Webmail* са уређаја за складиштење, као што су нпр. меморијске картице, а потом се шаљу преко Интернета. Области у Нигерији као што су Лагос или Фестак имају много Интернет кафеа који су отворени управо у ове сврхе. Радно време многих Интернет кафеа је од 22,30 часова па до 07,00 часова, тако да извршиоци кривичних дела у њима могу раде без страха да ће их службеници државних органа открити. У овим Интернет кафеима корисницима Интернета не траже се лична документа на увид, не постоји видео надзор и сл., тако да и када логови са ИП адресама укажу на то да је извршилац са тог места слао електронске поруке, његов проналазак није могућ због недостатка информација. Државним органима је веома тешко да идентификују и пронађу лица која се баве рачунарским преварама. Чињеница је да извршиоци ових кривичних дела користе информационе технологије да би сакрили свој идентитет и физичку локацију, како би осујетили напоре полицијских служби да их открију[120].

У Нигерији постоје и многа предузећа која уз новчану надокнаду обезбеђују лажна документа која се користе у Нигеријским преварама.[121] При извршењу кривичних дела дешава се да извршиоци траже бројеве банковних рачуна оштећених, копије личних докумената и сл. Ове информације извршиоци најчешће траже да би видели колико је жртва преваре озбиљна и спремна за „посао“ који су јој понудили. У неким случајевима се дешавало и да се прикупљени подаци од жртава преваре користе од стране извршилаца да би се нпр. са њихових банковних рачуна украо новац, на њих трансферисао новац који је добијен извршењем кривичних дела како би тај новац након тога подигли за себе и сл.

Са жртвама кривичних дела извршиоци Нигеријских превара комуницирају и преко мобилних телефона, користећи припејд *SIM* картице, тако да уколико сумњају да их неко прислушкује, исте лако могу да баце и потом купе нове ради даље комуникације.

У најекстремнијим случајевима Нигеријских превара жртве преваре се од стране извршилаца кривичних дела позивају на пословне састанке, и то обично на места одакле се киднапују, присилно им се отуђује лична имовина, врше се уцене њихових породица, па се дешава да их чак и убијају уколико не плате откуп.

Урошевић, В.: „Нигеријске преваре у Републици Србији“, часопис Безбедност, број 3/09, стр.145-157.

[120] Chawki, M.: Anonymity in Cyberspace: Finding the Balance between Privacy and Security, Revista da Faculdade de Direito Milton Campos, Nova Lima, Бразил, 2006, стр. 5. Наведено према Урошевић, В.: „Нигеријске преваре у Републици Србији“, часопис Безбедност, број 3/09, стр.145-157.

[121] Након једне преваре која је укључивала лажни потпис нигеријског председника Olusegun Obasanjo у лето 2005. године, нигеријске власти извршиле су претресе на тржници у делу Лагоса под називом *Oluwole*. Заплењене су хиљаде нигеријских и других пасоша, 10.000 бланко British Airways карата, 10.000 налога за исплату новца из САД, царинска документација, лажна уверења универзитета, 500 рачунара са скенираном документацијом који су служили за прављење фаслификоване документације и др. Извор: http://web.archive.org/web/20051029165224 /http://news.yahoo.com/s/latimests/20051020/ts_latimes/iwilleatyourdollars, дана 07.09.2009. године.

Како би извршили кривично дело преваре овог типа извршиоци најчешће користе фалсификовану документацију како би преузели новац који им је оштећени уплатио, бежичне трансфере новца за пренос противправно стечених новчаних средстава, техничка средства која им омогућују анонимну комуникацију, *Web*-базирану електронску пошту, електронске налоге који су претходно преузети од правих корисника, факс машине за слање факс порука при размени документације са жртвама преваре, услуге телекомуникационих сервиса за директну комуникацију са жртвом преваре, постављају лажне Интернет странице на Интернету којима оштећене доводе у заблуду да комуницирају и сарађују са представницима легалних и легитимних институција, уговарају пословне састанке са оштећенима (приликом комуникације извршиоци кривичних дела обећавају специјалне аранжмане као што је нпр. улазак у Нигерију „без визе“ и слично, након чега се жртве ових кривичних дела које дођу у контакт са извршиоцима киднапују, захтева се откуп и сл.) и др. [122]

Колико су Интернет преваре присутне и у Србији говори нам примери двоје наших грађана, који су на овакав начин оштећени за више хиљада евра, с тим што организатори преваре још увек нису откривени. Оштећени су електронском поштом примили обавештење да су у иностранству добили милионске новчане награде. Након што су одговорили на иницијалне поруке, оштећенима су послата детаљнија обавештења о начину подизања добитка, обрасци уговора које је требало попунити, упутства за отварање рачуна у иностранству на који ће награда бити уплаћена, чак и активациони кодови за рачуне на којима се налази новац, подаци о људима који су наводно већ обијали награде на овакав начин, али и износ „таксе“ и број рачуна на који је неопходно извршити уплату, како би награда била исплаћена. Када би оштећени уплатили тражене износе, њихова новчана средства су преусмеравана на више других рачуна у иностранству, што је праћење оваквог новчаног тока учинило немогућим.

Посебан начин за стицање противправне имовинске користи представља и креирање лажних веб сајтова намењених куповини робе. Пред Посебним одељењем Окружног суда у Београду за борбу против високотехнолошког криминала у току је кривични поступак против шесторо лица која су током 2003. године направила сајт *www.escroweurope.net* доводећи изгледом, садржином и адресом наведене Интернет странице оштећене у заблуду да комуницирају са легалним „*escrow*“[123] сервисом који пружа услугу посредовања приликом обављања робно - новчаних трансакција на Интернету, које се реализују тек након испоруке предмета купопродаје. Окривљени су објављивали огласе неистинитог садржаја и лажним приказивањем чињеница да као продавци поседују одређену робу коју ће након извршеног плаћања испоручити купцу односно, да ће као наводни купци наручену и испоручену робу продавцу платити, доводили и одржавали у заблуди већи број оштећених америчких држављана и тиме их

[122] Dyrud, M.: „I brought You a good news An analysis of Nigerian 419 Letters, Proceedings of 2005 Annual Association for Business Communication, Convention Association for Business Communication, САД, 2005, стр. 4. Наведено према Урошевић, В.: „Нигеријске преваре у Републици Србији“, часопис Безбедност, број 3/09, стр.145-157.

[123] Који функционише по принципу документарног акредитива. Ово представља варијацију облика акредитивне преваре описане мало раније у тексту.

наводили да им на штету своје имовине путем специјализованих сервисних служби *„DHL“*, *„FedEx“*, или *„UPS“* пошаљу одређену робу односно, да им као купци плате робу коју окривљени као наводни продавци нису ни поседовали, што су оштећени чинили путем сервиса за трансакцију новца *„Western Union“,* или употребом кредитних картица. Вредност ствари и новца који су окривљени прибавили на овакав начин износи више десетина хиљада евра[124].

3.1.3 Извршиоци

Коришћење Интернет сервиса и програма на Интернету, за прикривање ИП адреса такође је веома распрострањено. Ови сервиси извршоцима омогућују анонимно слање електронских порука, без остављања трага о правој ИП адреси извршиоца кривичног дела, на тај начин што целокупан Интернет саобраћај према одређеним Интернет адресама и страницама иде преко сервиса који потом као траг оставља своју ИП адресу, а адреса правог корисника се налази на серверу ових сервиса.

Прикривање идентитета врши се на много различитих начина, а већина случајева прикривања везана је за сакривање идентитета лица које је осмислило превару и лица које злоупотребљава податке о „жртвама“ преваре.

Пошто се ради о простору где се време реакције мора сводити на секунде, кључна је брза и ефикасна реакција. Шанса за проналазак доказа у оваквом окружењу зависи од саме конфигурације умрежених рачунара који се појављују у комуникацији као рачунарски сервери, улазне капије, рутери и др. лог фајлови су главни извор проналаска трагова и доказа о извршеном кривичном делу. У зависности од броја корисника и процеса који су у току, број ових лог фајлова у све је већем порасту, тако да поједини Интернет сервис провајдери у само једном дану стварају лог фајлове величине неколико стотина мегабита.

Прве информације о илегалној активности најчешће не воде до правог идентитета лица, већ је прикупљају подаци са више локација, често и широм света, преко ИНТЕРПОЛ-а. На међународном нивоу у полицијској и правосудној сарадњи још није постигнут довољно висок квалитет сарадње потребан за овакве врсте истрага. Разлози томе нису само у спорости правних система већ и у потреби обавештајне заштите држава.

Након сазнања да је извршено ове врсте преваре и да је дошло до злоупотребе података који су од стране извршилаца кривичних дела прикупљени на напред описане начине полицијски службеници прикупљају доказе и трагове у виду електронских података о оствареној комуникацији која се одвијала између извршилаца кривичних дела и оштећених, као и податке о финансијским трансакцијама које је оштећени извршио према инструкцијама које је добио од извршилаца. Врше се провере лог фајлова у потрази за ИП адресом, како би се лоцирао сервис преко кога је извршилац кривичног дела слао електронске поруке оштећеном, као и преглед целокупне електронске поште коју је оштећени примио,

[124] Урошевић, В.: „Нигеријске преваре у Републици Србији“, часопис Безбедност, број 3/09, стр.145-157.

како би се уочили пропусти направљени од стране извршиоца који могу указати на постојање кривичног дела (нпр. у случају да је извршилац поставио лажни Интернет линк неке институције, провером места хостовања правог Интернет сајта институције и лажног сајта може се уочити да се ради о превари) и места одакле је извршена превара. Након изоловања ИП адресе и времена слања електронских порука из лог фајлова преко ИНТЕРПОЛ-а се, у зависности од државе са чије је територије извршено кривично дело, врше провере у вези корисника коме је она била додељена у тренутку вршења кривичног дела.

Како би се детекција електронских порука свела на што мањи ниво, данас извршиоци кривичних дела данас шаљу мање количине спам порука са рачунара заражених рачунарским вирусима, како би се обезбедило што дуже функционисање њиховог слања. Неки комерцијални спам сервиси укључују *botnet* мреже за слање ових порука, које помажу да се избегну анти - спам мере на рачунарима корисника и заштите на серверима Интернет провајдера, које функционишу на тај начин што се блокирају ИП адресе које су постављене на „црне листе“. Данас постоји велики број ИП адреса са којих је вршено слање ових порука и које су идентификоване као носиоци спам активности. „Црне листе“ се врло често ажурирају, па извршиоци кривичних дела који користе слање оваквих порука за прибављање података морају да ангажују *botnet* мреже како би избегли блокирање њиховог пријема. Овакав начин слања *спам* порука додатно отежава рад полицијских служби МУП-а Републике Србије, пошто корисници Интернета на територији Републике Србије и не сумњају да поруке које им стижу могу бити штетне. Из наведеног разлога сматра се да постоји и велика „тамна бројка“ када су Нигеријске преваре у питању пошто оштећена лица или нису свесна да су преварена, или их је срамота да пријаве да су оштећени због своје околине. Оштећени се често плаше да пријаве овакве случајеве пошто их извршиоци кривичних дела убеђују да су сами криви за то што посао није могао да се реализује, прете им да ће их тужити и сл. Са друге стране резултати емпиријског истраживања, објављени у одбрањеној дисертацији једног од аутора овог рада, дају нам простора за даље везивање спама за неке друге облике ВТК. И основна верзија анкете и делфи верзија[125] дају (37,5% односно 46.15% делфи) значајан проценат експерата који сматрају спам увертиром за фишинг. 18,75% односно 23.08% у делфи верзији сматрало их је да је спам део напада социјалног инжењеринга и 43,75% односно 23,08% у делфи верзији изнело је да је спам носилац злонамерних програма. У делфи верзији анкете за одговор да је спам полазна основа за све облике ВТК било њих 7.69%.

Такође у другом анкетном питању у емпиријском истраживању испитаници су се у погледу односа опасности спама и осталих облика ВТК одредили на следећи начин. 40% испитаника определило се за одговор као и сам фишинг, а у делфи верзији за овај одговор се определило њих 18.18%. 18,75% испитаника сматра га опасним као и социјални инжењеринг док се у делфи верзији анкете определило њих 36,36%, а у основној верзији анкете 25% сматра га опасним као

[125] Делфи верзија анкете урађена је са стручњацима у првој линији одбране у Србији и неколико значајних личности у области ВТК, док је основна верзија анкете за испитанике имала припаднике ЈТ и полиције који раде у овој области, као и учеснике неколико скупова везаних за ВТК проблематику.

вирусе док се у делфи верзији анкете за овај одговор определило њих 9,09%, на крају у основној верзији анкете за опасност исту као и код свих злонамерних програма определило се 16,25% испитаника а у делфи 36,36%.

Постоје категорије превара електронском поштом које се могу превентирати следећим активностима:

- филтрирањем спама
- не веровати непознатим електронским порукама
- односити се према сумњивим порукама са дужном пажњом и опрезним
- не пратити мишем на линкове у електронским порукама
- инсталирати антивирусне и фајервол програме и ажурирати их редовно
- конфигурисати клијент електронске поште безбедно

Како препознати поруку која носи превару у себи? Нежељене (незатражене и шкодљиве према класификацији Закона о електронским комуникацијама) комерцијалне електронске поруке или „СПАМ“ представљају почетну позицију сваке преваре електронском поштом. Изумом електронске поште преварантима је отворен неслућен простор за малверзације, у савременим условима. Наиме, веома је лако у овом моменту након слања великог броја порука на личне адресе корисника (десетинама хиљада а у појединим случајевима и милионима) од којих је довољно да један посто буде преварено на оно што је преварант уложио исто представља вишеструку зараду. Савремени облици превара се веома угледају на класичне примере у прошлости у вези оваквих активности.

3. 2 Изнуда

Први облик овог дела чини оно лице које, у намери да себи или другом прибави противправну имовинску корист, силом или претњом принуди другог да нешто учини или не учини на штету своје или туђе имовине, (затвором од једне до осам година). Тежи облик овог дела постоји уколико је делом прибављена имовинска корист у износу који прелази четиристо педесет хиљада динара (затвор од две до десет година). Још тежи облик постоји ако је делом прибављена имовинска корист у износу који прелази милион и петсто хиљада динара, (затвор од три до дванаест година). Још тежи облици постоје у случајевима бављења вршењем претходно описаних дела или када је дело извршено од стране групе (затвор од пет до петнаест година). Најтежи облик постоји уколико је дело из ст. 1. до 3. овог члана извршено од стране организоване криминалне групе, (затвор од најмање пет година). Последња два облика спадају у дела за која се сматра да су дела организованог криминала и у њиховом расветљавању могу се примењивати специјалне истражне мере и методе.

Ова кривична дела код нас била су заступљена у неколико случајева различитих облика примене неких тројанаца или вируса, или код случајева ки логера или снимача шифара (пасворд снупера) код различитих сајтова приватних фирми и покушаја код неких он лајн игрица или социјалних мрежа у случајевима крађа идентитета на њима. У сваком случају о овим примерима је већ разматрано на различитим местима у овом раду.

4. ГРУПА КРИВИЧНИХ ДЕЛА ПРОТИВ ПРИВРЕДЕ

4.1 Фалсификовање и злоупотреба платних картица [126]

Прописивањем овог кривичног дела законодавац је имао намеру да заштити платне картице као средство у платном промету са истом функцијом као новац.

Радња кривичног дела је прописана алтернативно као прављење лажне платне картице, преиначавање праве платне картице у намери да се употреби као права или употреба лажне платне картице. Прављење подразумева израду потпуно нове лажне платне картице коришћењем одређених уређаја и процеса, а преиначење значи преправљање праве платне картице. У већини случајева у пракси се јавља прављење потпуно нових а веома су ретки случајеви преиначења. Употреба подразумева стављање таквих картица у промет и њихово коришћење нпр, на банкоматима, продавницама или плаћањем преко Интернета. У погледу виности потребан је умишљај, а дело је свршено када је лажна платна картица направљена, или је права преиначена у намери употребе или када је употребљена. Извршилац може бити свако лице, али, по природи ствари, лице које прави или преиначава праву платну картицу мора поседовати одређена знања и техничке уређаје за то. Став 4. овог члана санкционише неовлашћену употребу туђе картице или личних података власника картице и шифара које иду уз исте, чиме се омогућава инкриминација фишинга. Оно што представља проблем јесте да овде није санкционисано и прибављање ових података. Став 5. инкриминише набављање лажне платне картице у намери њене употребе као праве или прибављање података у намери да се исти искористе за прављење лажне платне картице[127].

За доказивање овог кривичног дела потребно је утврдити време и место извршења, да ли је картица која је употребљена лажна, на који начин је направљена и уз помоћ којих техничких уређаја. Посебно је потребно обратити пажњу на могуће радње саучесништва[128], јер ово кривично дело и његове радње, као и начин његовог извршења може обухватати више лица са различитим задужењима у оквиру криминалне групе – прибављање бланко картица, прибављање уређаја, прибављање кодова, израда самих лажних платних или преиначење правих платних картица, каснија употреба у промету или дистрибуција у циљу употребе у промету итд. У овом случају постоји квалификовани облик. Када је извршено кривично дело из ст. 1. неопходно је утврдити намеру учиниоца да преиначену платну картицу употреби као праву.

---

126 Изменама и допунама кривичног законика у члану 85 предвиђене су измене члана Члан 225 Фалсификовање и злоупотреба платних картица.

127 Герке, М и др., *Op.cit.*., стр.149. о овоме је код нас писао и Урошевић, В.: „Злоупотребе платних картица и рачунарске преваре“, часопис Правни Информатор, Београд, 2009. година

128 Уз ово дело од значаја је и чл.227. КЗ (2) Ко прави, набавља, продаје или даје другом на употребу средства за прављење лажних платних картица или лажних знакова за вредност, казниће се новчаном казном или затвором до три године.

Потребно је, уколико је могуће, утврдити и време и место употребе оваквих картица, као и висину штете причињене њиховом употребом. Исто се документује изводима из банке чији је банкомат или ПОС терминал обавио трансакцију, односно сервис или терминал који је остварио web banking трансакцију. Када су извршена кривична дела из ст. 2. и 3. потребно је утврдити да ли је и у ком износу прибављена противправна имовинска корист. Код кривичног дела из ст. 4. потребно је утврдити начин прибављања и коришћења такве картице и да ли је извршилац поступао неовлашћено. За кривично дело из ст. 5, потребно је утврдити на који начин је набављена лажна платна картица, да ли је набављена у намери употребе, као и који подаци су набављени, на који начин, круг лица, да ли су набављени у намери прављења лажних платних картица, и на који начин, од стране кога и где су такве картице имале бити направљене.[129] У овом смислу веома је значајно утврдити и карактеристике пластике картица коришћених у трансакцијама, као и начин наношења на магнетне траке бланко картица и карактеристике дигиталних трагова овог процеса.

Повећање броја кривичних дела ове врсте, ипак, није у сразмери са повећањем броја платних картица, с обзиром на то да је у нашој земљи установљен веома добар правно институционални оквир за спречавање оваквих злоупотреба, који чине Форум за превенцију злоупотребе платних картица при Привредној комори Србије, полицијски и правосудни органи. Треба напоменути и да банке имају своје центре који 24 часа врше мониторинг промета платним картицама, док је при Народној Банци Србије формиран Национални центар за платне картице.

Како смо већ напоменули, за извршење ових кривичних дела потребна је добра организација, а радња кривичног дела се одвија у неколико фаза. До злоупотребе платних картица долази тако што извршиоци прво набављају податке са картица служећи се разним преварним методама (скимовање, крађа пин кодова, либанска уста)[130], затим исте податке продају преко Интернета „крајњим корисницима“ који праве фалсификоване картице наносећи украдени запис на тзв. „беле“ картице. Значајно је утврђивати и везе и односе у организацији оваквих извршилаца ради каснијег документовања о субординационим и другим односима чланова организоване групе. Овакве картице се углавном не користе у земљама у којима су подаци украдени, па су, у пракси, извршиоци ових кривичних дела најчешће странци. Фалсификоване картице се најчешће користе на банкоматима.

Постоји неколико начина којима се могу прибавити подаци са платних и кредитних картица. Неки од њих су фишинг, фарминг, скиминг[131], либанска уста[132], употребом хакерских алата (злоћудних програма) и сл.

---

129 Герке, М и др., Op.cit. стр.150.

130 Посебни методи укључују нове облике техничких средстава, као на пример, постављање мобилних телефона са висококвалитетним облицима снимања видео записа, прикривено лажним металним оквиром, на оквир АТМ апарата, у низу са више батерија како би се обезбедило дуготрајно и вишеструко праћење и картица које се уносе и пратећих пинова. Све ово се чини снимањем активности корисника кји нису свесни да их неко прати. Ово је могуће вршити и онлајн, чак и видео стримингом, са инстантном корисношћу. Варијација описаног је тзв. шиминг (shimming), која подразумева стављање малог пластичног електричног кола у уста банкомата које онда скимује податке и путем вајерлес технологије преноси извршиоцу податке.

131 Очитавање дигиталних карактеристика картице и њихово снимање, за каснију употребу.

Поред организованих криминалних група које су концентрисане у појединим државама или областима и које имају јасно организовану структуру, постоје и многе криминалне групе које се формирају око појединих заједничких интереса и потом трају неко време, од неколико месеци па до неколико година. Овакве групе се формирају у зависности од потребе и интереса њених чланова. Као најлакши метод за комуникацију ове групе су изабрале форуме и Интернет сајтове са ограниченим приступом како би се приликом вршења илегалних активности заштитили од кривичног прогона, а у исто време обезбедили и место где ће моћи да размењују искуства, купују и продају податке, средства за извршење кривичних дела и др. Распрострањеност платних картица, могућност њихове примене и доступност најмодернијих информационих технологија, учинила их је изузетно атрактивним за велики број криминалаца и криминалних група широм света. Посебно су постала рањива тржишта на којима се платне картице тек уводе у платни промет, где нема довољно искуства у електронском пословању и где не постоји систем за спречавање оваквих злоупотреба, као и државе где је стандард веома висок, и где је развијен систем он лајн банкарства и трговине.

Платне картице је данас могуће користити за подизање готовине на банкоматима, шалтерима банака, за плаћање робе и услуга на продајним местима опремљеним ПОС (*engl.* Point of sale.) терминалима или импринтерима, за плаћање у електронској трговини, као и за плаћање робе наручене поштом и телефоном. Плаћање помоћу платних картица се може извршити преко Интернета без одласка до банке или до трговца, из куће, како у земљи, тако и у иностранству. Управо на Интернету постоји највећа опасност да електронски подаци са платних картица буду компромитовани[133]. Видећемо да и у физичком окружењу прети велика опасност – преварантима је довољно да им физички предате картицу и да док Вам одвраћају пажњу различитим триковима провуку вашу картицу кроз неки од својих уређаја и сниме податке са магнетне траке (о кориснику, рачуну и картици). Постоје различити системи који служе као заштита – од најновијег Mastercard – овог давањем привремених генерисаних бројева на самој картици до Jitter технологије[134] која користи стоп – старт или џитер покрете па ако се на банкоматима налази скиминг уређај спречава снимање корисне информације због оваквих покрета. Виши ниво заштите представља нови EMB чип уграђен у мастеркард (MasterCard®) који у сваком тренутку даје приликом комуникације са идентификационим сервером динамички елемент идентификације[135]. Даљи облици усавршавања плаћања иду ка мобилним плаћањима (путем целуларних или сателитских телефонских апарата, вајерлес телефона), или токенизацијом, или енкрипцијом оба краја комуникационе конекције (end-to-end encryption).

---

[132] У отвор за картицу банкомата се поставља штипаљка која заглављује картицу. Тада оштећеном прилази „случајни пролазник“ који нуди помоћ и предлаже оштећеном да поново укуца пин код. По одласку оштећеног криминалац вади картицу из банкомата и наставља да је користи.

[133] Урошевић, В.: *Злоупотреба платних картица и рачунарксе преваре*, Правни информатор 9/2009, Београд, стр.4.

[134] http://www.bankinfosecurity.com/articles.php?art_id=2667&rf=2010-06-21-eb доступан 21.06.2010.

[135] http://www.bankinfosecurity.com/articles.php?art_id=3351&rf=2011-02-19-eb доступан 05.03.2011. год.

Специјализовани Интернет сајтови и форуми на Интернету веома често представљају погодно место за нуђење рачунарских вируса на продају, као и других услуга, међу којима су и софтверски алати намењени прибављању података о платним картицама, електронски туторијали намењени за обуку лица који хоће да прибаве податке о платним картицама, па чак и информације о платним картицама као што су бројеви платних картица, ЦВВ2 бројеви (CVV2 – Card Verification Value 2 – троцифрени број који се налази на полеђини картице)[136], тип платне картице, валидност платне картице и имена и презимена корисника, као и други подаци о пребивалишту власника платне картице, електронска адреса власника, поштански број, својство на основу кога се корисник налази у бази неке електронске продавнице, датум када је извршена куповина, ИП адреса корисника коју је исти користио приликом куповине, тип коришћеног Интернет претраживача, као и податке о томе да ли је корисник, тј. клијент још увек активни клијент електронске продавнице. На оваквим форумима нуде се само иницијални подаци понуђача, које не представљају ништа више сем иницијалног контакта (ИЦQ, МСН, електронска адреса, број телефона или неки други контакт). Након размене података са заинтересованим лицима, која ни понуђача ни заинтересовано лице не обавезује, корисници се упућују на сигурније Интернет сајтове и форуме (где је приступ заштићен помоћу шифри) и где им се нуде озбиљнији послови.

Најчешће је за куповину преко Интернета купцу данас потребно да има електронске податке о платној картици као што је број картице, валидност (датум од када картица важи) и ЦВВ2 број. До ових података о платним картицама извршиоци кривичних дела преко Интернета долазе на неколико раније помињаних начина, а најраспрострањенији су:

1. Слање нежељених порука (енгл. *Spam*)
2. Пецање (*Phishing* енгл.)[137]
3. Фарминг (*Pharming* енгл.)
4. Крађа података о платним картицама из базе података електронских продавница

Основни облици фалсификовања и злоупотреба платних картица су:

- злоупотреба украдених или утајених (изгубљених) платних картица,
- злоупотреба неуручених платних картица,
- неовлашћена употреба туђе платне картице,

---

136 Card Verification Value (CVV or CV2), Card Verification Value Code (CVVC), Card Verification Code (CVC), Verification Code (V-Code or V Code), ili Card Code Verification (CCV). Постоји неколико шифара (кодова) прва од њих је ЦВЦ1 или ЦВВ1, она је унета на магнетну траку картице и користи се за плаћање када је и власник присутан ради упоређивања података из идентификационих докумената. Други код и најчешће цитирани, а који се у 99% користи у горе описаним преварама је CVV2 или CVC2 (у зависности од типа катрице), често се назива и идентификујућим кодом картице CCID – Sredit card ID користи се у случајевима плаћања на даљину – обично путем Интернета у случјавима "цард нот пресент" трансакција. Неке нове картице тзв. чип картице или Цонтацтлесс могу имати сопствене електронски самогенеришуће кодове као нпр. iCVV или Динамички CVV.

137 У одређеним случајевима постоје и такозвани TAM (temporary account number, eng.) Привремени број рачуна) за обезбеђење одређене онлајн куповине путем картице. Наравно чак је и њих могуће прибавити комбинацијама социјалног инжењеринга и малвера управо фишингом и фармингом.

- прављење и коришћење лажних платних картица,
- прибављање података за прављење лажне платне картице,
- злоупотребе и преваре од стране акцептаната (трговаца),
- злоупотребе од стране корисника.

Кардерски форуми постали су веома популарни као место и начин за размену знања и вештина потребних за вршење ових кривичних дела, као и за продају података о платним картицама који су на овај начин прибављени[138]. Сваког дана стотине информација везаних за украдене, лажне и друге платне картице продаје се и купује од стране криминалаца који се баве извршењем кривичних дела из ове области на кардерским форумима. Специјализовани форуми повезују кардере и купце једне са другима. Они прво купују тест податке, испробавају им функционалност и, уколико су задовољни, купују већу количину оваквих података, ради даљег вршења кривичних дела. Ови подаци се касније користе за преваре везане за класичне видове злоупотреба као што су скидање новчаних износа на банкоматима помоћу лажних платних картица или куповину робе, као и за све друге видове превара типа „card not present“ на Интернету.

Оваквих форума има много, али су и полицијске службе многих држава успеле да прате рад неких од њих, као и да инфилтрирају полицијске службенике у ову виртуелну средину у циљу праћења активности њихових чланова. Овакве активности полицијских служби су у неколико случајева резултирале проналаском и хапшењем оснивача и чланова кардерских форума. Један од оваквих форума био је и *Shadow Crew*. Овај форум био је у функцији од августа 2002. године до октобра 2004. године. На њему су корисницима нуђени подаци и информације везане за куповину или продају дигиталних личних или банковних података (SSN – бројеви социјалног осигурања држављана САД, дампови картица, CVV2 бројеви), као и фалсификована документа потребна за вршење кривичних дела из области привредног криминала. Корисници су добијали одређене привилегије кроз активно учешће и доприносе туторијалима у оквиру дискусионих група. На форуму је садржај нуђен на енглеском и руском језику, и углавном је био усмерен на кориснике из САД и Источне Европе. Корисници из САД су се углавном бавили хаковањем, а чланови из Русије и Румуније су били експерти за производњу лажних платних картица и њихову злоупотребу[139].

У септембру месецу 2008. године америчка служба ФБИ објавила је и да је завршена двогодишња тајна операција везана за „Dark Market“ кардерски форум. Ова акција резултирала је хапшењем 56 лица, и тиме је спречена превара чија је

---

[138] Можемо указати на информације добијене од стране господина Клауса Бајерлеа да су још новембра 2007.год. у циљаном претраживању Интернета у оквиру његове јединице откривени: понуде за украдене информације о кредитним картицама у „шопу“ а затим, праћењем хакерског форума "www.hacksector.cc" остварено: поред правних садржаја путем рачунара пронађено пуно илегалних садржаја као што су: Пијаца (размена корисничких података, између осталог) Шопинг центар (куповина информација о кредитној картици и власницима). Хијерархијска структура на сајту извршилаца: • Први ниво - Приступ за свакога, • Други ниво - приступ трајање чланства и број порука, • Трећи ниво - приступ личним позив главног администратора. Сајт је имао око 33 000 регистрованих корисника у питању су, углавном, млади људи и омладина, у земљама немачког говорног подручја. Други кључни подаци су: у оптицају је било 700.000 порука, на 70.000 различитих тема.

[139] http://en.wikipedia.org/wiki/ShadowCrew: dostupno na dan 16.04.2010.

вредност била већа од 70 милиона америчких долара. Акција је реализована у сарадњи са полицијским службама и међународним полицијским организацијама широм света. Извршиоци кривичних дела из различитих држава широм света су на овом кардерском форуму, који је представљао својеврсну међународну, транснационалну криминалну мрежу у виртуелном простору Интернета, били укључени у куповину и продају информација везаних за податке са платних картица, података за логовање (корисничка имена и лозинке), као и опреме потребне за вршење кривичних дела из области привредног криминала. На врхунцу свог рада овај форум је имао преко 2.500 чланова[140].

Агенција ФБИ је ову операцију извршила уз помоћ многих домаћих и међународних полицијских служби међу којима су Computer Crime and Intellectual Property Section of the U.S. Department of Justice, Serious Organised Crime Agency из Велике Британије, Turkish National Police – KOM Department iz Turske, Bundeskriminalamt (Немачка Савезна Криминалистичка полиција у Висбадену - Нем. Wiesbadden), и Die Landskriminalmat Badden – Wurtemberg (Државна Полиција покрајине Баден Виртемберг у Немачкој)[141]. Многи случајеви инфилтрације полицијских служби у кардерске форуме учинили су криминалце из ове области веома опрезним, па су мере заштите све јаче. А парадокс је да се у Србији многе специјалне истражне мере и методе не могу применити у области сузбијања ВТК. То је у Хрватској веома лако и елегантно решено.

4.1.1 Утицај кардерских форума на злоупотребу платних (и кредитних) картица

Извршиоци кривичних дела која се врше преко Интернета личне, финансијске и друге податке потребне за извршење кривичних дела прибављају најчешће коришћењем *phishing* алата, слањем нежељених порука (Спам) и коришћењем SQL инјекција за прибављање података из база података[142] електронских продавница у иностранству. Електронски подаци који су од интереса за извршиоце кривичних дела су најчешће везани за платне картице, а након крађе они их, преко Интернета најчешће користе за наручивање робе преко електронских

---

[140] Интервјуом са Клаусом Бајерлеом утврђено је и да је БКА дана 22.11.2007 открила: тендер за продају савезне Немачке личне карте, на одређеним сајтовима постављане су везе за преузимање Тројанаца, новији филмови, музички албуми и софтвер, а такође омогућавани и приступи онлајн сервисима као што је ПејПал, Т-Онлине и други. У марту 2008: спроведена је национална операција претраге, откривено је да су: Администратори, Супер Модератори и Ко-Администратори: Мо ... 18-годишњи из Баден-Виртемберга... 22 године, из покрајине Северна Рајна-Вестфалија, Ф. .. 17 година стари студент из Рајинланд-Пфалз Фи ...16 година студент из Рајинланд-Пфалз, Ст .. 18 године, из Хамбург Да ... 16 година студент из Северна Рајна-Вестфалија ЦХ ... 15-годишњи студент из Хамбурга и сл. Акција је укључила 13 одељења у Немачкој спроведене су претраге у 6 провинција обезбеђено је, између осталог, скоро 20 ПЦ и нотебоок рачунара, око 1.000 ЦД-Р, више екстерних хард дискова, одређена количина наркотика, роба прибављена преварама.

[141] http://www.fbi.gov/pressrel/pressrel08/darkmarket101608.htm: последњи пут приступљено 16.04.2010.

[142] У питању су програмски пакети који се убацују (инјектују) користећи слабости браузера и буквално музу податке који се преко SQL програмског језика већ налазе у програмираној страници. На овај начин извршиоци прибављају већ делимично обрађене податке и спремне за даље коришћење о постојећим трансакцијама и претходним корисницима онлајн продавнице.

продавница, најчешће на територији Републике Србије, али и у иностранству. Извршиоци кривичних дела су, на основу праксе Одељења за борбу против високотехнолошког криминала[143], углавном млађи пунолетници, док се као саизвршиоци јављају и старија пунолетна лица, нарочито у улози лица која преузимају робу за одређени проценат (тзв. *Money mules*).

Електронске продавнице, преко својих Интернет страница, на нашој територији, углавном, за наручивање робе захтевају неке основне податке као што су: број телефона, име, презиме и адреса лица које ће преузети робу, електронска адреса и слично. Приликом уноса наруџбине траже се број платне картице и ЦВВ2 број, као и лични подаци власника. Овакав начин електронског пословања довео је до пораста броја злоупотреба везаних за нелегално прибављање личних и других података.

Велики број база података које се данас користе у пословне сврхе имају неку форму Интернет интерфејса, и на тај начин дозвољавају интерним и/или спољним корисницима да лако могу да им приђу кроз комерцијалне софтвере за претраживање. Врло се често дешава да се базе података у којима се налазе лични подаци о корисницима услуга, међу које спадају и електронски подаци о платним картицама, компромитују управо овим путем, пошто нису довољно заштићене.

Већина Интернет страница електронских продавница је направљена на PHP или SQL базираним софтверским платформама[144]. Главни циљ ових Интернет страница је обезбеђивање производа и услуга клијентима. Ови Интернет сајтови углавном су интерактивни, и засновани на принципу поштовања жеља корисника и одговора на њихове упите. Постоји много начина како се преузима контрола над Интернет сајтовима и како се компромитују базе података, ради прибављања личних података клијената. Најчешћи и најопаснији су напади SQL инјекцијама. SQL инјекцијама се у систем базе података убацује мали део података или програмски код који истражује слабости у заштити саме базе података, да би се оне, затим, несметано злоупотребиле ради компромитовања и крађе података о платним картицама.

У циљу лакшег разумевања проблематике и њеног утицаја не само на кривична дела из чл. 225. КЗ већ и друга кривична дела а посебно за случајеве фишинга неопходно је размотрити неколике случајеве из праксе. Године 2008. од стране једног предузећа са територије Републике Србије, које води успешну електронску продавницу на Интернету, поднета је кривична пријава за кривично дело Фалсификовање и злоупотреба платних картица из чл. 225 КЗ и Рачунарска превара из чл. 301 КЗ због злоупотребе електронских података, са више платних картица, као и крађе и злоупотребе идентитета[145] аустралијских држављана

---

143 Упоредити са Ивановић, З. Урошевић, В. *Улога интернета код ангажовања посредника у преузимању противправно прибављене робе и новца извршењем кривичних дела високотехнолошког криминала*, Гласник права, Крагујевац, бр.1. 2010.стр. 83-95

144 Више о материји на: http://en.wikipedia.org/wiki/SQL последњи пут приступљено 10.07.2010.год.

145 Ова разлика није значајна у теорији у Србији, али је увелико актуелна у свету, наиме код нас постоји кривично дело преваре, које супсумпцијом инкорпорира акт злоупотребе идентитета, док крађе идентитета осим у кривичном делу лажног представљања (Члан 329) нема. Неколико елемената крађе идентитета садржи дело Фалсификовање и злоупотреба платних картица из члана 225. где се у ст.4. говори о делу извршеном неовлашћеном употребом туђе картице или поверљивих

власника ових платних картица, у сврху куповине техничке робе. Проверама је утврђено да је извршилац наведених кривичних дела електронске податке о платних картица и идентитету њихових власника прибавио употребом SQL инјекција, које је користио за нападе на слабо заштићене SQL базе података које су се налазиле на SQL серверима електронских продавница са подручја Аустралије. Поред података о бројевима платних картица, CVV2 бројевима, типу платне картице, валидности платне картице и имена и презимена корисника, извршилац кривичног дела прибавио је и друге податке као што су: пребивалиште власника платне картице, електронска адреса власника, поштански број, својство на основу кога се корисник налази у бази електронске продавнице, датум када је извршена куповина, ИП адреса корисника коју је исти користио приликом куповине, тип коришћеног Интернет претраживача, као и податке о томе да ли је корисник, тј. клијент још увек активни клијент електронске продавнице. Извршилац је био у могућности и да сазна укупан број платних картица чији се подаци налазе у самој SQL бази електронске продавнице.

У току 2009. године од стране више предузећа са територије Републике Србије које своје пословање врше и преко електронских продавница подношене су кривичне пријаве за кривична дела Фалсификовање и злоупотреба платних картица из чл. 225 КЗ и Рачунарска превара из чл. 301 КЗ против неидентификованог извршиоца због покушаја злоупотребе електронских података са више десетина платних картица, као и крађе и злоупотребе идентитета страних држављана који су власници ових платних картица, у циљу куповине техничке и друге скупоцене робе. У једном случају утврђено је да је један од извршилаца преко Интернета прибавио податке о више десетина електронских адреса корисника Western Union банке, направио лажну страницу Western Union банке која је била постављена на сервер под његовом контролом, а затим слао СПАМ поруке корисницима банке у којима је од њих тражено да преко лажног линка постављеног у поруци посете наводне странице Western Union банке ради ажурирања њихових података у бази. Уносом својих података на лажној страници банке клијенти су податке о платним картицама несвесно слали директно у руке извршиоцу кривичног дела који их је злоупотребио.

У овим случајевима су, поред података о бројевима платних картица, CVV2 бројева, типова платне картице, валидности платне картице и имена и презимена корисника извршиоци кривичних дела прибављали и друге податке као што су пребивалиште власника платне картице, електронска адреса власника, поштански број, својство на основу кога се корисник налази у бази електронске продавнице, датум када је извршена куповина, ИП адреса корисника коју је користио приликом куповине, тип коришћеног Интернет претраживача и др.

Анализом ових случајева уочено је да је активност извршилаца кривичних дела који су злоупотребили платне картице на Интернету у великој мери зависила од њиховог искуства везаног за учешће на кардерским форумима. Они су се, у комуникацији са другим извршиоцима кривичних дела, опредељивали за то који ће *modus operandi* применити при прибављању података о платним картицама

података који јединствено уређују ту картицу у платном промету. У ст.5. наводи се и ко набави лажну платну картицу у намери да је употреби као праву или ко прибавља податке у намери да их искористи за прављење лажне платне картице.

страних држављана. У ове сврхе они су, преко кардерских форума, ступали у комуникацију са извршиоцима кривичних дела из иностранства који су им давали тзв. туторијале, савете и сл[146]. Преко ових форума извршиоци су прибављали и електронске адресе клијената банака, на које су потом слали СПАМ поруке са линковима који воде на фишинг сајтове чије су странице постављене на сервере, који су под контролом извршиоца кривичног дела. Извршиоци кривичних дела користили су и услуге „специјализованих" сервиса на Интернету преко којих су слали СПАМ поруке. Преко Интернет сервиса, за које су сазнали преко кардерских форума, су такође слали и SQL инјекције којима су прибављали податке из SQL база података електронских продавница. Такође, је уочено и да преко кардерских форума стицали знања о томе како да украду податке о идентитету лица. Крађа идентитета настављала се употребом прикупљених података за извршење кривичних дела која су у највећем броју случајева везана за стицање противправне имовинске користи лицима која злоупотребљавају украдени идентитет[147].

У току 2008., 2009. и 2010. године на територији Републике Србије откривено је осам случајева рачунарских превара и злоупотреба платних картица на Интернету, у оквиру којих су покушане и извршене злоупотребе података са више стотина платних картица, а прибављена имовинска корист износила је преко пет милиона динара. Идентификовано је дванаест лица која су се бавила овим кривичним делима и против њих су поднете кривичне пријаве надлежном тужилаштву. Злоупотребљаване су углавном платне картице страних банака издавалаца са територије Сједињених Америчких Држава, Немачке и Аустралије а за прибављање података коришћене су технике СПАМ-а, фишинга и SQL инјекција, о чему си извршиоци знања стицали највећим делом преко активног учешћа у кардерским форумима.

Сваког дана стотине информација везаних за украдене, лажне и друге платне картице продаје се и купује од стране криминалаца који се баве извршењем кривичних дела из ове области. Специјализовани кардерски форуми повезују извршиоце кривичних дела и купце и пружају им амбијент у коме, без постојања граница могу да размењују знања, вештине и податке, да планирају заједничке акције и на тај начин угрозе фрагилну структуру савремених финансијских токова везаних за електронско пословање.

---

146 Између осталих у питању су и продаје онлајн програма који служе у ову сврху, међу којима и keylogger - i. Њихова цена на црном тржишту у најпростијој верзији је према Cybercrime: current threats and trends, Discussion paper, 2008. COE p.10., dostupan na adresi: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567%20study1-d-provisional%20_13%20Mar%2008_en.pdf 16.04.2010.god. 40 $, webmoney Trojan – 500$, snatch Trojan који има карактеристике и функционалности руткита а краде шифре - 600$.

147 Милошевић М., Урошевић В.: *Крађа идентитета злоупотребом информационих технологија*, Безбедност у постмодерном амбијенту, Зборник радова књига VI, Центар за стратешка истраживања националне безбедности, Београд, 2009, стр. 53-64. А упоредити и са: Урошевић, В. Уљанов, С.: „Утицај кардерских форума на експанзију и глобализацију злоупотребе платних картица на Интернету", у: Журнал за криминалистику и право НБП, Криминалистичко-полицијска академија, Vol. XV, No. 2, 2010, Београд, 2010, стр. 13-24.

Ова претња по безбедност финансијског система, као једног од основних претпоставки за сигурност савременог информационог друштва све је већа, па је и заштита од њих од кључног значаја.

Кардерски форуми су, због начина функционисања, веома опасни у овом контексту, па је потребно веће ангажовање полицијских служби на откривању њиховог присуства и проналажењу њихових оснивача и чланова. У случајевима злоупотребе платних картица на Интернету на територији Републике Србије, како је наведено, примећена је значајна активност извршилаца кривичних дела са наше територије на кардерским форумима.

У последњих пет година ниво професионалности оваквих напада је у великом порасту, рапидно се повећава број малициозних софтвера, а стално се мењају и циљеви напада. У наредних пет година очекује се и пораст броја нових трендова, као и усавршавање старих метода крађе података о платним картицама и начина њихове злоупотребе. У складу са познатим параметрима могуће је очекивати следеће трендове:

- Високотехнолошки криминал ће по обиму постајати све више налик класичном криминалу.
- Појачаће се веза између високотехнолошког, организованог и привредног криминала.
- Рад Offshore компанија које подржавају он лајн банкарске сервисе и виртуелне кладионице који су на граници са илегалним активностима увек ће представљати идеалну прилику за прање новца насталог на основу илегалних активности.
- Упркос труду међународних организација, извршиоци кривичних дела из области високотехнолошког криминала ће, и даље, бити веома спретни у истраживању слабости и пропуста у међународним стандардима који се примењују у борби против високотехнолошког криминала. Увек ће проналазити начине да врше прање новца преко међународних он лајн компанија намењених искључиво у те сврхе.
- Заштићени кардерски форуми биће све затворенији за пријем нових чланова па ће инфилтрација од стране полицијских службеника, као и обезбеђивање доказа о њиховој активности бити све тежа.
- Анонимност која се постиже употребом украдених података о идентитету биће све учесталија.
- Употреба Интернет сервиса намењених прикривању техничких трагова о логовању биће све распрострањенија.

4.2 Фишинг и крађа идентитета

4.2.1 Кратка историја феноменологије фишинга

Термин се први пут јавља 1996. год.[148] када је група хакера украла корисничка имена и лозинке рачуна АОЛ путем мејл (поруке електронске поште) „удице“ на коју су се корисници АОЛ упецали. Пре 2003. год. фишери су користили пецање, преко електронске поште, за недозвољено прибављање података, фактички преварно изнуђивање података – од њихових мета. Недостаци које су ови фишери имали у свом раду до 2003. год. су подразумевали и граматичке грешке садржане у оваквим мејловима, који су били веома карактеристични, и лако препознатљиви, те и нису представљали неки већи проблем или претњу[149]. Ове околности од 2003. год. мењају свој ток драстично и пецање постаје много софистицираније и укључује много квалитетнију анализу мета и подразумева коришћење многих програмских оруђа и алатки у циљу прикривања и лажног приказивања чињеница ради преварног изнуђивања података и информација. Почело се са регистрацијом домена који личе на оне којима жртве верују, па се тако јављају слични домени чувеним, као на пример, www.wcitybank.com или www.societegenerali.com но овде није крај (хомографски или хомоглифски напади). Преваранти на различите начине прибављају и званичне логое ових фирми и прикривају лажне садржаје својих лажних страница приближно сличним или оваквим садржајима све у циљу обмане корисника. Циљ је наравно да се прибаве подаци који су идентификациони за одређене рачуне финансијских институција, али и ИСП-а, као и сваки други садржаји чији идентификациони капацитет омогућава прибављање недозвољене имовинске користи или могућност злоупотребе идентитета у циљу наношења штете другоме (бројеви социјалног осигурања – веома значајни на територији САД, бројеви кредитних картица и пратећи ПИН бројеви, као и друге поверљиве информације). Овде се могу убројати

148 http://www.websense.com/site/docs/whitepapers/en/Phishing%20and%20Pharming%202006%20White paper%20(3).pdf

149 У Србији се овакви фишинг мејлови јављају у скорије време, највероватније услед доступности и шире употребе гугл преводиоца. Оне изгледају овако: From: isaac george <georgei60@yahoo.com> Date: 2010/4/19 Subject: ХИТНО МОЛИМ ВАС. To: Најдражи, Ја сам Isaac George , адвокат. Преминуо клијент мина, по имену Господин Андрев Паркер из ваше земље, који су у даљем тексту ће бити наведена као мој клијент, чији је живот и да његове целе породице истекао, а на одмор у љетовалишта у Пхукет на Тајланду 26. децембар 2004 у цунамију природне катастрофе. обратили су се и да помогне у репатриатинг новца иза мог клијента пре него што се одузети или проглашена некористан од стране банке где се ово депозит у вредности од $ 12.5миллион долара је уложио. Ова банка има мене издала обавештење да контактирате најближи рођак, или рачуна ће бити конфискована, јер је влада лист / мандату / овлашћује све банке да замрзне или заплени било који налог који није погодан у дугом временском периоду, ово је усмерена ка капитал лет за привреду.Мој предлог вам је да тражи свој пристанак да вам представити као следећи-на-рода и корисника моје зове клијент, тако да је приход од овај налог може бити плаћени за вас. Ово ће бити исплаћена или дели у овим процентима, 60% до 40% мене и за вас. Сви правни документи да направите резервну копију захтева и поред мог клијента-на-рода ће бити обезбеђен. Оно што тражим је ваш искрен сарадњу како би смо видели кроз ову трансакцију.Ово ће бити извршен у оквиру легитимне аранжман који ће вас заштитити од било које кршење лав.Иф овог посла предлог вређа своје моралне вредности, да ли да прихватите моје извињење, али ако не, онда контактирајте ме на једном показују свој интерес, од мене дајући хитно следе у наставку: ХИТНО МОЛИМ ВАС.1. Ваше име и презиме 2. Ваш број телефона 3. Ваша контакт адреса. 4.. Ваша доба и занимања. Ваш хитне одговор ће бити веома очекиване и поштовати. Назовите ме на мој приватни телефон +229 96 86 47 50 за више информација. С поштовањем, Barrister Isaac George.

и подаци који представљају идентификационе елементе за логовање на као и сам Интернет месиџинг (ИМ). Такође, ту можемо убројати и експлоатацију рањивости Интернет сајтова, и П2П (пир ту пир) мрежа, али и механизама за претраге на Интернету у циљу „скидања“ (даунлоадовања). Поред описаног, ту спада и активирање програма килогера или скринлогера или преварно редиректовање (преусмеравање) Интернет претраживача (npr. Google)[150] на садржаје фишинг сајтова. Ови напади су усмерени и на пословне кориснике, и фирме (чак и на мултинационалне компаније) слањем фишинг порука како би припадници и запослени у њима, заварани вером у сопствену ИТ заштиту фирме, постали жртве у погледу сопствених идентификационих података у фирми. Циљ је овде много виши, нарочито, у случајевима финансијских привредних друштава и предузећа где је крајњи циљ да се упадом у систем фирме прибаве подаци о комитентима и њихове идентификационе ознаке у циљу злоупотребе у неком од горе описаних случајева. 2003. год. Пуштен је у оптицај имејл црв Мимаил који је за мету имао PayPal, у децембру 2003. год. APWG упозорава[151] на пораст фишинг порука за преко 400% преко викенда, у јануару 2004. мете напада пецароша биле су: Одељење Државне Безбедности (Department of Homeland security), Poreska Управа САД (IRS) и Федерална компанија за осигурање депозита (Federal Deposit insurance Comp). У фебруару 2004. год. преваранти се логују на реалном сајту користећи украдене информационе податке, у априлу 2004. хакери почињу да примењују замену УРЛ[152] фишинг сајта са УРЛ –ом приказаном у адресној линији претраживача корисника коју желе лажно приказати. У јуну 2004. год. фишери користе податке о украденим картицама и прибављају одређене количине противправне материјалне користи. Јун 2004.год. Гартнер Инц. (Gartner Inc.) објављује да је пецање коштало индустрију и потрошаче 2,4 милијарде долара у

---

150 Један од путева је и Гугл бомбардовање, он подразумева покушај да се утиче на рангирање рејтинга неког сајта у резултатима повратног процеса гугл претраживачке машинерије. Алгоритам ће рангирати сајт према количини екстерних линкова који на исти указују. У суштини систем је такав да што више сајтова објави линкове ка одређеном сајту већи ће рејтинг имати сајт и пре ће се појавити у резултатима претраге. Подаци о критеријумима за претрагу. У опцијама за претрагу сервиса типа Google, Yahoo и др. могу се пронаћи критеријуми за претрагу одређеној садржаја ради проналаска Интернет страница које одговарају критеријуму претраге. Ови подаци говоре о намери корисника да дође до одређеног садржаја на Интернету, а нарочито уколико је у ова поља уношено више критеријума тј. речи за претрагу (нпр. „fishing+farming").

151 Доступно на: 1H2008: HU http://www.apwg.org/reports/APWG_GlobalPhishingSurvey1H2008.pdf последњи пут приступљено 30.06.2010.год.

152 УРЛ (или Uniform Resource Locator (URL)) је подгрупа УРИ (Uniform Resource Identifier (URI)) која одређује или показује где су одређени ресурси неопходни за покретање сајта и механизме њиховог преузимања.URL представља све што се може пронаћи на Интернету (Интернет странице, слике, текстови итд). Састоји се од протокола (http), места хостовања (интернет адреса где се налази одређени садржај), броја порта, пута слања (локација одређеног садржаја на Интернет страници), критеријума претраге и идентификатора фрагмента претраге (нпр. download). Подаци о укуцаним URL-има у претрагама Интернет претраживача говоре о директном претраживању одређеног, познатог садржаја од стране корисника рачунара, пошто се за разлику од претрага помоћу одређених појмова нпр. у опцији за претраге Google-а, ради о начиину претраге и приласка тачно одређеном Интернет сајту. У Google бази података налазе се подаци о унетим URL-има у опцији за уношење Интернет адреса код претраживача и, то говори, о намери корисника да директно приђе одређеној Интернет страници.

2003. год. У јулу 2004. фишери први пут користе АИМ (America online instant messaging programme). У октобру 2004. год. преваранти отварају наизглед легитимне лажне сајтове за он лајн апотеке, банке и предузећа за обезбеђење и залоге како би прибавили на преваран начин податке о кредитним и дебитним картицама и ПИН бројеве власника. Јануара 2005. Корисницима и беја (еВау) шаљу се велике количине порука са захтевом за валидацију својих корисничких података, користећи отети или „запоседнути" домен. Фишери у фебруару 2005. Нападају Пеј Пал (PayPal) и неколико чувених банака, док се у априлу овакви напади интензивирају претећи да укину одређене привилегије појединим корисницима овог система. У јулу 2005. Администрација Националне кредитне уније САД (National Credit Union Administration (NCUA)) бива искоришћена за покушаје фишинга особа које имају рачуне у било којој Федералној кредитној унији.

У савременим околностима у Србији „преваранти шаљу електронске, углавном спам поруке ширем кругу потенцијалних жртава у којима наводе да је њихов даљи рођак, за кога нису ни знали, умро - али да је оставио велико наследство које могу да преузму само рођаци пошто преминули није имао директног наследника. Они жртву доводе у заблуду да постоји могућност да она добије наследство па јој нуде и услуге сређивања документације у вези наследства и, при том, константно захтевају од ње да шаље новац како би се измирили трошкове за отварање рачуна, адвокатске услуге, таксе, дозволе. Често се представљају и као чланови породице неког богатог политичара које прогони тамошња власт. Пошаљу и фотографије деце да би све било уверљивије. Обећавају „куле и градове", али је потребно да им потенцијална жртва пошаље новац како би се успешно реализовали њихови планови, а заузврат нуде проценат од укупне суме новца коју желе да извуку из државе. Преваранти користе софтвере и писма преводе на српски језик како би читава прича била убедљивија. Грађани најчешће постају жртве због саосећања, наивности или из похлепе, што су уједно и најчешћи мотиви због којих шаљу новац. Саветујем да се такве поруке не отварају и да се не успоставља никаква комуникација са пошиљаоцима.

Грађани преко различитих сервиса на интернету шаљу своје CV како би конкурисали за неку врсту посла. Ти подаци су понекад доступни и ширем кругу корисника интернета. Преваранти понуде шаљу електронским путем и лажно се представљају као послодавци. При томе, жртве не проверавају да ли су електронске адресе и бројеви телефона са којих их контактирају потенцијални послодавци из европске земље у којој наводно нуде запослење, или можда из неке афричке државе. Жртве иду директно на линк који је остављен у огласу, а који води на лажну интернет презентацију коју су поставили преваранти. Најлакша провера је да се на „Гуглу" откуцају име фирме и земљу из које је, посете праву Интернет презентацију и упореде бројеве телефона, електронске адресе и контакте послодаваца. Преваранти методом „фишинга" или ширењем рачунарских вируса преузимају лозинке и отимају мејл адресе корисника. Читањем мејлова сазнају доста о тој особи. Ако, рецимо, сазнају да је неко отпутовао у иностранство не либе се да са његове интернет адресе, након што преузму контролу над њом, познаницима жртве пошаљу поруке. Лажно се представе као да су власници тог налога, тврде да су покрадени и да треба да се на одређени рачун уплати новац да

би допутовали кући. У таквим случајевима треба обавезно позвати пријатеља и проверити све наведено у фишинг мејлу“[153].

Путем комбиновања добрих социјално инжењерисаних прича са техничким триковима поменутим у претходним редовима могу се направити чуда и преварити и најопрезнији међу нама. Чињеница да је контекстуална информација погрешна јесте и једина могућа одбрана за све који бивају жртве фишинга, зато је треба добро проучити. И наше емпиријско истраживање указује да експерти најугроженијим сматрају клијенте банака (84.6%), а по 7,7% одговора испитаника обухватило је виши менаџмент (банака, пословних привредних друштава) и државне службенике, док је један експлицитан одговор фокусирао следеће групу: неедукована лица на важним местима, непознаваоце функција лажне он лајн куповине ради прикупљања података код даљих дела крађе идентитета.

4.2.2 Утврђивање појма

Према ОЕБС – овом документу са министарског састанка у Сеулу јуна 2008. год.[154] каже се да извршиоци на располагању имају и користе веома широк спектар средстава за вршење крађа идентитета. Неки од ових метода подразумевају употребу и активирање злоћудних програма. Поједини од њих подразумевају фишинг[155] нападе, код којих се жртве маме слањем обмањујућих електронских писама или коришћењем посебно дизајнираних веб сајтова да Интернет корисници одају своје поверљиве податке о финансијским и другим добрима. Понеки подразумевају и коришћење фишинг[156] електронских порука, које се нашироко и масовно дистрибуирају кроз спам, често, са намером инсталирања злоћудних програма на своје мете. Друга дефиниција појма фишинга је: “метод мамљења (или мамаца за) наивних корисника Интернета како би од њих, различитим методама и техникама, упецали приватне податке о личним или идентификационим карактеристикама”[157]. Неки га дефинишу и као: „облик социјалног инжењеринга познат и под називом фишинг, покушај да се на преваран начин прибави легитимни кориснички пакет – корисничко име и шифра, његови поверљиви или осетљиви

---

153 http://www.blic.rs/Vesti/Hronika/196854/Ostao-bez-imovine-zbog-prevaranta-iz-Afrike последњи пут приступљено 05.07.2010

154 OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, може se pronaći na sajtu OECD. Материјал припремљен за 72. састанак овог тела.

155 Сматра се да је термин креиран 1996.год. када су Хакери преварно прибављали шифре и корисничка имена на серверу АОЛ (America online), крадући корисничке рачуне, том приликом, овом провајдеру. Ове крађе датирају од раније 1990.год. али су тада преварно коришћени бројеви кредитних картица, а касније средином деведесетих када су противмере овог провајдера почеле да дају неке резултате 1996.год. почињу са крађом корисничких рачуна.

156 Поједини теоретичари за објашњење назива phishing користе следећу логику – у питању је сложеница од phreaking и fishing као облик дефинисања комплексног појма фрикера – старе врсте хакера и пецања. Овај појам тежи да објасни и природу ове врсте преваре и њен дубљи основ.

157 OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, може се пронаћи на сајту ОЕЦД. Материјал припремљен за 72. састанак овог тела, стр.17.

подаци путем фалсификовања имитирањем и другим техникама и средствима електронских комуникација као да потичу од поузданих јавних организација, аутоматским путем. Овакве комуникације се обављају веома често путем електронске поште, које упућују адресате на преварне сајтове који купе ове податке од корисника када их услед оваквих мејлова унесу на превару. Подаци које овим путем преваранти најчешће прибављају се односе на банковне рачуне (нарочито оне за веб банкинг) дебитне и кредитне платне картице, различите шифре и национални идентификациони бројеви"[158]. Фишинг се у одређеним земљама чланицама ОЕБС идентификује са крађом идентитета а у одређеним разликује. Ипак, као што се може приметити фишинг представља најчешће коришћену методу или технику при крађи идентитета. Треба прецизирати да се овакви напади не смеју посматрати у савременим околностима као напади усамљених тинејџера или као безазлени акти. Како истраживање Кристофера Абада указује, у којем је он надзирао четове у четрумовима посећиваним од стране фишера, генерално напади се не дешавају насумично и од стране усамљених лица – управо супротно, ово јесу координирани добро организовани, специјализацијски оријентисани напади са организованом поделом рада, који омогућавају различитим типовима извршилаца координирано садејство[159]. Фишинг подразумева процес варања адресата одређене поруке којим се од њега захтева да подели осетљиве информације са непознатим трећим лицем[160]. Према Википедији мрежна крађа идентитета представља покушај крађе података корисника Интернета путем фалсификоване веб странице[161]. Фишинг представља најчешћи вид прибављања поверљивих података. Овај облик прибављања података подразумева скуп активности којима неовлашћена лица коришћењем лажних електронских порука преко електронске поште и лажних Интернет страница кориснике Интернета наводе на откривање поверљивих података као што су нпр. јединствени матични број грађана, корисничко име и лозинка, PIN (Personal Indentification Number engl.) број картице, број кредитне картице и других личних или пословних података. Према налазима пројекта под називом „сајбер криминалитет" у оквирима Савета Европе[162] фишинг напади комбинују технике социјалног инжењеринга са техничким модалитетима како би прибавили податке жртава. Шта више, Абад је препознао следеће групе у оквиру дате поделе рада – мејлере, СПАМ-ере, прикупљаче и кешере[163]. APWG (Anti

---

158 Jakobsson M., Myers S. Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft, 2007 by John Wiley & Sons, Inc. Hoboken, New Jersey, стр.2.

159 Jakobsson M., Myers S. Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft, 2007 by John Wiley & Sons, Inc. Hoboken, New Jersey, стр.3.

160 Threatsaurus,the a-z of computer and data security threats, p.61. Sophos. Доступан у дигиталном облику на: http://www.sophos.com/sophos/docs/eng/papers/sophos-a-to-z-computer-and-data-security-threats.pdf последњи пут приступљено 23.08.2011.год

161 http://sr.wikipedia.org/sr/Фишинг доступна 29.08.2011.год.

162 Cybercrime current threats and trends COE, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study1-d-provisional%20_13%20mar%2008.pdf последњи пут приступљено 01.09.2011.год. p.19.

163 Мејлери су спамери и хакери са способношћу слања велике количине преварних мејлова, обучно путем ботнетова, Колектори су хакери који постављају преварне сајтове на које се жртве пецају тако што им уносе поверљиве податке у току упита на датом сајту, они овакве активности предузимају најчешће преко компромитованих рачунара на Интернету (преко зомби мрежа или

phishing working group)[164] је препознала неколико модалитета фишинга (подела заснована на коришћеним средствима у сврху остваривања преваре): у Бразилу – путем пласирања преко сајтова генеричке забаве злоћудних програма – килогера; примамљујући сајтови који садрже злоћудне програме су класика; постоји велики раст алтернативних начина придобијања и обмањивања жртава у циљу преварног узимања личних података; фишинг заснован на инјектовању тројанаца килогера (креираних да потајно купи податке од крајњих корисника о њиховим рачунима корисничким именима и шифрама); фишинг заснован на тројанцима редиректорима (изменама и сечењем по датотекама хоста - домаћина или коришћењем редирекције ДНС –а кроз модификовање букмаркова домаћина, чиме се дешава да браузери не отварају легитимне сајтове, већ се усмеравају на фалсификоване); фишинг или фарминг (човек између – алудирање на између две ватре) посреднички напад (тип који пресреће комуникације између две стране у сврху преусмеравања – редирекције корисника на преварне локације); друге врсте напада, нпр. погрешног уноса – када корисник погрешно откуца у адресној линији браузера неку адресу, коју је фишер унапред регистровао са таквом грешком у циљу преусмеравања саобраћаја на свој инфицирани сајт (хомографски напад).

Обично се таква лажна страна нуди путем посебно припремљеног имејла или чет поруке. Пошиљалац тако наводи жртву, да телефоном или на лажној веб страници чија је хипервеза дата у поруци, пошиљаоцу открије поверљиве информације. Те информације он користи за разне сврхе али најчешће за крађу новца са банковног рачуна или за провалу у имејл рачун жртве. У савременој литератури израз фишинг подразумева коришћење лажних електронских порука како би се прибавиле личне или пословне информације од корисника Интернета или извршила крађа идентитета. У припремном документу ОЕБС – а разликују се два типа фишинг напада (ова класификација заснована је на средствима која се користе при извођењу напада) они који користе злоћудне програме и они који користе СПАМ. Први подразумевају софтверски код или прогам убачен у оперативни систем у циљу наношења штете систему, или системима, или у циљу подређивања система да врши оно што његов корисник није намеравао да он ради[165]. Фишинг представља још један од веома честих видова прибављања поверљивих личних, финансијских и других података у последњих неколико година. Овај облик прибављања података подразумева скуп активности којима неовлашћена лица коришћењем лажних електронских порука преко електронске поште и лажних Интернет страница финансијских институција кориснике Интернета наводе на откривање поверљивих података као што су нпр. јединствени матични број грађана, корисничко име и лозинка, ПИН (*Personal Indentification*

ботнетова), често се дешава да колектори плаћају мејлерима да их у датим преварним мејловима „рекламирају“, у ствари, упућују на њихов сајт. Кешери су лица која прибављањем ових поверљивих података исте користе за наплату. Различити су начини на које они функционишу – од прављења фалсификованих кредитних и дебитних картица за директно дизање новца са АТМ машина до куповине робе и услуга путем коришћења ових података на нету. Они обично плаћају колекторима за дате информације или се уговара проценат са овима.

164 Више о организацији на http://www.antiphishing.org/

165 OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, може се пронаћи на сајту ОЕЦД. Материјал припремљен за 72. састанак овог тела, p.16.

Number енгл.) број картице, број кредитне картице и слично. При фишинг нападима користи се комбинација социјалног инжењеринга и техничких могућности које пружају савремене информационе технологије[166]. За реализацију оваквих напада користе се електронске поруке, као што су:

- Лажна упозорења банака или других финансијских организација да ће доћи до гашења рачуна клијента, уколико он не изврши унос, односно ажурирање одређених података,
- Лажне поруке администратора у којима се траже кориснички подаци нпр. лозинка, корисничко име и сл.
- Поруке које се позивају на безбедност и захтевају од корисника откривање личних информација (кориснички рачун, лозинку итд.) или захтевају инсталацију неког програма ради отклањања откривеног безбедносног пропуста,
- Поруке којима се обавештава корисник да је добио на лутрији, због чега треба да достави одређене податке како би могао подићи неки добитак.

Да би се жртве преварили и навеле да унесу своје податке у техникама „пецања“ често се користе линкови који по називу личе на праве адресе банака или пословних организација, али се, заправо, налазе на сасвим другој ИП (*engl. Internet Protocol*) адреси и хостоване су на серверима широм света, док изглед Интернет презентације у потпуности одговара правој Интернет страници.

У принципу, основни начин функционисања „пецања“ је следећи: на електронску пошту корисника одређене институције шаље се електронска порука у којој се, нпр. наводи да се база података институције преуређује и да је потребно да прималац поруке оде на линк који се налази у поруци преко Интернета. Линк је лажан, тј. води на лажну страницу у којој се нуди да се прималац поруке улогује, да унесе своје личне податке као што су име и презиме, адреса, телефон, број картице са валидношћу, CVV2 број, број рачуна, лозинка и друго. Свест корисника Интернета о „пецању“ сваким даном је на све вишем нивоу, па су и извршиоци кривичних дела приморани да употребе нове технике. Уместо слања електронских порука којима се корисници убеђују да посете неку Интернет страницу на адреси из лажне поруке, данас се користе вируси типа trojan keylogger, mouse loggers и screen grabers како би се од жртава преваре преузимали осетљиве податке. Наше истраживање указало је и на то експерти, према сопственом искуству, сматрају актуелне нападе превише наивним, и да ретко ко може да се „навуче“ на овакве преваре. 23.1% испитаника је сматрало да су напади релативно наивни, обзиром на генералне карактеристике, затим, 15.4% учесника анкете их је квалификовало као суптилно перфидне а највећи проценат се определио за карактеризацију: изузетно опасни, нарочито, спир фишинг – 46.3% . Један екстензивнији одговор имплицирао изузетну опасност а, нарочито, старијим лицима код којих њихов „понос и искуство“ доводе у дубљу заблуду, наивни због постојања разлике у URL.

Фишинг технике[167] су постале све софистицираније данас, према документу ОЕБС –а[168] од 2008. год. главне форме или облици су:

---

166 The Phishing Guide Understanding & Preventing Phishing Attacks, NGSSoftware LTD, United Kingdom Sutton, 2006. p. 3.

167 Furnell, S.M. Problem of categorising cybercrime and cybercriminals 2nd Australian Information Warfare and Security conference 2001.p.4.

- фарминг, (неки га одређују и као warkitting) по ОЕБС – у: „овај тип напада, који је веома сличан фишингу, користи исти тип лажних идентификатора као и у класичним фишинг нападима и у исто време усмерава кориснике са легитимних сајтова на преварне који су реплике оригинала“

- СМиСх(ш)инг (Smishing): „код овог облика корисници целуларних (код нас одомаћеног термина „мобилних“) телефона примају СМС поруке у којима одређена фирма потврђује да је корисника уписала на листу својих услуга и уједно га обавештава да ће му наплатити одређени износ уколико не откаже овакве услуге на њиховом сајту“

- СПАМ представља још један вектор за слање масивних фишинг погодака, данас је СПАМ постао веома опасан прерастајући из неинвазивних пропагандних порука у потенцијално опасне поруке са садржајима који могу резултирати чак и крађом идентитета. Спам често дистрибуира злоћудне програме, или усмерава адресате на инфициране сајтове.

- фишинг копљем (усмерени, циљани, фишинг): За разлику од уобичајеног циљани фишинг се не врши масовним мејл порукама, већ конкретизацијом једне или неколико добро бираних жртава (које су, обично, високо рангирани функционери фирми, државних органа или сл). Пошиљалац глуми или се лажно представља као администратор или слично лице у безбедносном рачунарском сектору одређеног предузећа (или, чак, неко друго – примаоцу познато лице) и обраћа се неком од запослених како би измамио корисничка имена и шифре за приступ рачунару или рачунарској мрежи тог предузећа. Најчешће су жртве овог облика фишинга веома добро биране – то су виши службеници у фирмама, којима су доступне разне поверљиве информације. Обично се наводи да је ово високо прецизиран облик СПАМ-а[169]. Прецизност која је овде у питању односи се, како на адресата, тако и на садржину поруке која се шаље. Овај облик фишинга може изгледати као да долази од шефа или колеге са посла који би морао слати мејлове свим запосленима у фирми. Поред захтева за шифрама и корисничким именима може садржати, чак, и тројанца. „Циљани (Spear) фишинг“ фишинг је, за разлику од класичних облика фишинга који је усмерен генерално на потенцијалне жртве, много прецизнији, пошто се усмерава на одређену групу жртава или на појединца[170]. Извршиоци кривичних дела који врше класичне фишинг нападе шаљу стотине лажних електронских порука неодређеном броју људи. У „Циљаном (*Spear*)“ фишинг нападу шаљу се усмерене поруке на адресе тачно одређених, циљаних корисника. Овакве електронске поруке најчешће садрже личне податке као што су име или презиме корисника, који представља циљ напада, неке детаље о послу којим се бави и сл. Овакве електронске поруке су најчешће оригиналне, и разликују се од масовних порука које се приликом класичног фишинга шаљу на адресе корисника. Видећемо да се у емпиријском истраживању једног од аутора

---

168 OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, може се пронаћи на сајту ОЕЦД. Материјал припремљен за 72. састанак овог тела, p.16.

169 http://www.microsoft.com/protect/terms/socialengineering.aspx доступан 07.12.2009.год.

170 Као што би риболовац користио копље да улови само једну, одређену рибу из неког јата, тако и извршилац кривичног дела користи циљани (реч spear на енглеском језику значи копље) фишинг да нападне тачно одређене кориснике Интернета.

овог дела спир фишинг (циљани или усмерени фишинг) сматра савременим обликом фишинга (огромна већина 75% испитаника) и то као усавршеног прецизираног и перфиднијег облика фишинга. 16.7% сматра га посебним обликом фишинга не разликујући његову специјалност и 8,3% испитаника сматра га савременим обликом фишинга без даљих категоризовања појма.

Један од примера оваквог напада су поруке у којима се запосленима у неком предузећу шаљу поруке у којима се налазе и подаци о неком стварном и актуелном послу у који су укључени. Пошто је то нов начин преваре запослени, примаоци овакве поруке, врло лако могу да претпоставе да се ради о сасвим регуларној поруци, да кликну на линк који се налази у поруци. То је практично тренутак када корисник бива „погођен копљем“, тј. тренутак када долази у ситуацију да ода пословне податке без свог добровољног пристанка и знања. Пошто порука изгледа као да је пристигла од легитимног пошиљаоца тражење поверљивих информација као што су корисничка имена, лозинке, бројеви рачуна, платних картица и других захтеваних података могу изгледати уобичајено, тако да жртва у њих лакше поверује него код класичних облика фишинга. Оваквим порукама често претходи и крађа идентитета лица у чије се преварна порука наводно шаље како би се жртве обмануле. Због начина на који функционишу, многи Интернет сервиси постали су погодан „амбијент“ за крађу и злоупотребу идентитета. Крађа идентитета почиње са присвајањем личних података о неком лицу, без пристанка и знања тог лица, путем обмањивања, крађе или преваре. Прикупљене информације могу да буду искоришћене одмах након крађе, да се складиште и чувају ради коришћења или да се препродају другоме уз новчану надокнаду. Крађа идентитета наставља се употребом прикупљених података за извршење кривичних дела која су у највећем броју случајева везана за стицање противправне имовинске користи лицима која злоупотребљавају украдени идентитет.

У јануару месецу 2010. године испоставило се да је циљани фишинг веома актуелан и опасан вид преваре. Тада су широм света извршени успешни „Циљани фишинг“ напади на нафтне компаније у САД којима су прибављене информације о истраживањима о налазиштима нафте у протеклих неколико година. Врло убрзо по овом догађају отпочело се са помињањем појма сајбер ратовање.

Циљани фишинг је, за разлику од класичних облика фишинга усмерен генерално на потенцијалне жртве и много је прецизнији, пошто се усмерава на одређеног појединца или групу жртава.

Некада циљане фишинг електронске поруке садрже и рачунарске фајлове који се могу сачувати на рачунару. Веома често пропратни текст везан за разлог слања фајла је толико убедљив и често изгледа као да га је послао послодавац или неко други, подједнако важан за примаоца поруке. Међутим, овакви фајлови често садрже злоћудне програме, који када их корисник преузме прикупљају приватне податке корисника и шаљу их назад извршиоцу кривичног дела.

За разлику од класичних облика фишинга, усмерени или циљани фишинг је теже открити пошто извршиоци кривичних дела улажу додатне напоре да превару учине што убедљивијом. Корисници би практично требали да уложе много напора и да имају много техничких знања и информација везаних за безбедност како би установили да се ради о овој врсти преваре. Такође је потребно и да повежу податке о електронској поруци са лажним Интернет сајтом како би установили да се ради о

превари. Корист која се добија употребом ове врсте фишинга је, такође, и знатно већа. При вршењу Циљаног фишинга користе се технике, којима се електронска порука приказује на тај начин да изгледа као да се ради о оригиналној поруци која се иначе шаље запосленима или члановима одређене компаније, владиних институција, различитих организација или група.

Да би успешно извршили овакве напада извршиоци кривичних дела морају да имају почетне информације о жртвама које желе да преваре, како би их методама социјалног инжењеринга убедили да су електронске поруке које су им пристигле заиста упућене од стране правог пошиљаоца. Овакве информације извршиоци кривичних дела добијају или неовлашћеним упадима у компанијске мреже или комбиновањем података добијених о запосленима преко различитих Интернет сајтова, блогова или социјалних мрежа, типа Facebook или Twitter, или, чак, прибављене путем техника социјалног инжењеринга.

Након што прибаве овакве информације, које су им довољне да нападну жртву, они користе најразличитије врсте изговора: да се ради о хитним и неодложним стварима, због којих је на такав начин потребно да жртве дају своје пословне или личне податке и сл.

Од жртава се често тражи да посете линк из електронске поруке који води ка лажној, али веома добро урађеној Интернет страници, где се од њих тражи унос лозинки, бројева рачуна, приступних шифри, података о платни картицама и др. Путем оваквих порука и линкова шире се и злоћудни програми. Из ових разлога запослени данас, посебно, треба да воде рачуна о томе да приликом читања електронских порука не посећују Интернет линкове, који се користе као референца одређене компаније, пошто се извршиоци кривичних дела служе овом могућношћу да методом социјалног инжењеринга наведу лице да посети Интернет страницу коју су сами креирали да би их убедили да се заиста ради о легитимним компанијама, њиховим правим представницима и сл.

Овакви напади се користе у различите сврхе, а као пример се могу навести откривени напади из јануара 2010. године када је циљаним фишингом прослеђен велики број порука ка војној информационој инфраструктури у САД. Извршен је покушај ширења рачунарског вируса типа тројанца под називом „Зевс“ преко електронских адреса корисника домена „.mil“ (војни домени) и „.gov“ (владине институције) из САД.

Још један пример ове врсте је крађа, односно превара, у вези квота за продукцију CO_2. Извршиоци кривичних дела су поруке са лажним линковима слали компанијама у Европи, Новом Зеланду и Јапану, а поруке су изгледале као да долазе од немачких власти које се баве трговином овим квотама. Примаоцима поруке је навођено да њихове компаније морају да промене и ажурирају њихове налоге у оквиру којих се налазе и подаци о квотама и трансакцијама везаним за квоте.

Уколико би радници ових компанија посетили линк из поруке и оставили податке, извршиоци кривичних дела су могли да преузму квоте и преместе их на своја два рачуна које су отворили наменски за ову сврху.

Нови појавни облици фишинга какав је циљани фишинг, због брзине и обима прибављања података о циљаним корисницима представљају изузетно негативну појаву. Спектар злоупотребе података добијених на овај начин везан је за цео свет, а циљане преваре „Циљаним (Spear)“ фишингом полако преузимају примат када је

активност криминалаца и криминалних група које се баве високотехнолошким криминалом у питању, због веће прецизности коју им омогућава при вршењу превара.

Емпиријско истраживање, раније описано у докторској дисертацији једног од аутра овог рада, је дало и следеће резултате: у погледу разликовања фишинга од циљаног или усмереног 83.3% испитаника определило се за видно постојање разлике, док се њих 16.7% одредило да ову разлику не види.

У веома кратком временском року овим видом фишинга изазиване су велике последице како у компанијама, тако и у државном сектору, и финансијским институцијама. Посебно је забрињавајућа експанзија употребе малициозних софтвера који се шире циљаним фишингом у сврхе војне и индустријске шпијунаже.

Постојање техничких могућности на Интернету којима се омогућава анонимност извршилаца (прикривање ИП адреса коришћењем proxy сервера, лажно представљање, ВоИП и др.), лоша међународна сарадња, мали број државних службеника који се баве овом проблематиком, слаба сарадња са Интернет провајдерима и лоша техничка опремљеност ових субјеката који се баве спречавањем кривичних дела на Интернету додатно су утицала на то да се овим кривичним делима баве и веома добро организоване међународне криминалне групе.

Заштита од ових видова напада је веома отежана посебно због употребе података који су о личности којој се порука шаље претходно прибављани ради довођења жртве у заблуду. Међутим, потребно је имати на уму да компаније, банке и агенције личне податке и информације, скоро, никада не траже путем електронских порука. При пријему оваквог садржаја треба проверавати телефонским путем да ли се заиста ради о правом пошиљаоцу (наравно не из електронске поруке за коју се претпоставља да је лажна, пошто је вероватно и број телефона у поруци такође остављен са намером да се жртва доведе у заблуду). Коришћење фишинг филтера који имају Интернет претраживачи такође је веома битно. Интернет линк никада не треба посећивати из електронске поруке него га треба унети у претраживач у поље за унос URL адресе ручно, па тек онда посетити страницу.

Овај вид фишинг напада данас је реалност и омогућио је нападе који су координирани и веома прецизни. Штета коју изазива компанијама и различитим организацијама много је веће, а несигурност коју изазива у окружењу које почива на фрагилној информационој структури такође је повећана. Превентивно упознавање службеника са овим видом напада нужан је како би се ефикасно спречавали овакви напади.

- неки овој подели додају и Вишинг, као крађу или превару у циљу злоупотребе ВоИП –а, и његових варијација (скајпа, Интернет месинџера итд.).

Постоји још једна подела[171] значајна за фишинг технике, то је подела на блендиране (мешане или насумичне) и циљане нападе. Ова подела је заснована на облику и начину избора међу техникама које ће се користити. Они су најчешће

[171] OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, може се пронаћи на сајту ОЕБС. Материјал припремљен за 72. састанак овог тела, p.16.

скривени. Мешане технике напада подразумевају софистицирање технологија и техника које се користе приликом напада како би се избегле савремене методе и средства одбране, шта више подразумева се да они користе већи број злоћудних програма. Пример за овај облик напада је када извршиоци уграде своје злоћудне програме у један легитиман сајт. Циљани напади могу бити скривени и самонајављујући. Они су резултат проактивних и одбрамбених мера које су дале резултате. Извршиоци из овог разлога прелазе на конкретније одређене циљеве (мете) јер се више не исплати лов у мутном, јер су масовни напади имали за циљ да прибаве онолико информација колико је то могуће. Овде се циља на одређену мету при чему овакви напади омогућавају учиниоцу да прође неопажено средства заштите (антивирусе и фајерволове (ватрене зидове))[172] и да задржи свој статус непримећен и користи систем жртве дуже време.

Обзиром на карактеристике ове врсте напада може се рећи да је фишинг веома софистицирана појава, која је великом успону, за нас је значајно да схватимо да се, као извршиоци, не јављају аматери, већ су у питању најчешће професионалци, организовни у групе са веома прецизним улогама и делатностима, као и да је веома могућа веза овог облика криминала са организованим криминалом.

Могуће је разликовати и следеће типове фишинг напада (али ову класификацију треба узети условно, јер актуелна софистицираност и рапидна еволуција ових техника утиче на порозност граница, које се могу, у датом тренутку, направити), у оквиру којих ће бити описане неке од техника наведене у књизи Фишинг и противмере[173]. Према овим ауторима постоје обмањујући фишинг напади, фишинг напади базирани на злоћудним (злонамерним) програмима (малверу); ки логери или скринлогери (неки говоре и о скринграберима), пресретачи сесија, напади системског реконфигурисања, крађе података, фишинг базиран на ДНС (домејн нејм серверима eng. domain name servers, неки га одређују као фарминг, говори се и о cybersquatting –u), фишинг инјектовања садржаја, фишинг типа човек у средини (или посреднички напад)**,** фишинг претраживачких програма. Обмањујући фишинг се обично сматра класичним фишинг нападом. Њихов најчешћи пратилац су мејлови. Типични сценарио је следећи: жртви стиже хрпа и мејл порука са позивом адресатима да хитно реагују[174] притиском на неки од понуђених линкова. Фишинг напади базирани на злоћудним програмима подразумевају ширење ових програма, путем социјалног инжењеринга или преко

---

172 Програми који користећи различите методе штите рачунар од нежељених садржаја.

173 Jakobsson M., Myers S. Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft, 2007 by John Wiley & Sons, Inc. Hoboken, New Jersey, стр.3

174 Примери ових позива су: упозорење по којем постоји проблем са адресатовим рачуном у одређеној финансијској или штедној институцији. Поруком га извршилац позива да посети сајт у циљу решавања овог проблема, користећи обмањујући и лажни линк до преварног сајта; упозорење да је адресатов рачун ризичан и позива га да се укључи у анти преварни програм; фиктивна профактура често веома луксузне или забрањене робе коју адресат није наручио, са могућношћу да се откаже наруџбина са посебним линком; преварно обавештење да је дошло до неауторизоване промене на рачуну адресата са линком за решавање проблема; Тврдња да је у одређеној финансијској институцији понуђена нека нова услуга и да се овом адресату нуди јединствена понуда да бесплатно добије ову услугу али ограниченог трајања.

експлоатације безбедносних рањивости програма и система[175]. Типичан социјални инжењеринг подразумева убеђивање корисника на отварање неког линка из и мејл поруке кликом на њега или даунлоадовањем неког фајла са вебсајта, са тврдњом да дати има неког додира са порнографским материјалом, ласцивним фотографијама неке познате личности или трачевима о њој[176]. Саобраћај се на одређеном сајту може усмерити на неки фиктивни, преварни, путем социјалног инжењеринга као на пример путем спама који на пример нуди неки примамљиви садржај или кроз инјекцију неког злоћудног садржаја у легитимни сајт искоришћавањем безбедносних слабости у виду међускриптне рањивости на датом сајту. Ки логери и скринлогери обично врше надзор над подацима који се уносе у ваш веб претраживач у одређене листе захтеваних идентификационих програмских модула, након чега их шаљу преварним фишинг сајтовима. Користе при томе различите технологије – објекте који су помоћни у вашем претраживачу а који региструју промене на УРЛ и логује (снима) информације када је УРЛ на сајту за прикупљање резервисаних креденцијала; или драјвер за праћење уноса извршених путем миша и тастатуре у садејству са праћењем активности корисника; или скрин логер који прати дешавања на монитору који види корисник и снима све што он ради. Након напада килогера и скринлогера се могу појавити и тзв. секундарне штете од нпр. преко 50 рачуна кредитне извештајне агенције који су компромитовани јер су били предмет напада преко порнографског спама, као директна консеквенца овако компромитованих рачуна појавило се негде око 310000 сетова персоналних информација који су злоупотребљени из базе података ове агенције. Пресретачи сесија су извршиоци следећег типа напада – надзор над активношћу жртве, најчешће се то врши преко злоћудних компоненти веб браузера. Оног тренутка када жртва користи свој рачун или започне трансакцију злоћудни програм пресреће овакву сесију и предузима злоћудне активности по успостављању сигурне везе и прихваћеног идетитета корисника рачуна. Овај напад се може извести на корисниковом рачунару преко малвера – злоћудних (злонамерних) програма али се може извести и са удаљених сервера преко напада човек између. Онда када је напад спроведен малвером пресретање сесије може изгледати потпуно исто као и да је корисник директно посетио оригинални сајт и као легитмна комуникација, започета од стране самог корисника.

Веб Тројанци су малициозни програми који „искачу“ преко логин прозора са намером да прикупе податке који се у њих уносе. У овом случају корисник верује да уноси своје персоналне идентификационе податке у прозор за легитимисање, али се та информација уноси локално на рачунару па се након тога трансмитује на неки други – извршиочев рачунар.

Веб базиране технике подразумевају и укључивање HTML прикривених линкова на популарним сајтовима; примену лажних или рекламних банера трећих

---

[175] У последње време (јануар 2008.год.) извршиоци користе у фишингу посебно израђени УРЛ како би убацили модификовани образац за логовање на банчине стране, где је ССЛ сертификат издат од стране Banca Fidearum S.p.A. у Италији, извршиоци су успели да инјектују IFRAME који учитава измењени образац са сервера на Тајвану.

[176] Нарочито је интересантно искоришћавање човечије жеље за сензационализмом или актуелним догађајима и њиховим моменталним конзумирањем – посебно преко Интернета – где се користе и бомбардовања претраживачких софтверских основица, али и спуфовани сајтови за „уважавање товара“.

лица у графичком облику да намаме жртве на инфициран сајт; коришћење веб багова (сакривених података на страници, као на пример графичке датотеке величине 0 бајта) за праћење потенцијалне жртве фишинг напада, коришћење невидљивих оквира – поп ап прозора за прикривање правих извора фишинг порука; увезивање злоћудног садржаја у видљиву веб страницу која онда експлоатише познате рањивости веб браузера инсталирајући софтвере фишера (нпр. килогере, скрингребере, бекдор програме и сл.).

Тровање датотеке домаћина (Hosts File Poisoning) уколико корисник у свој Интернет (браузер) претраживач унесе одређену адресу или стисне одређену запамћену локацију (претходно меморисану у Интернет претраживачу) рачунар онда мора превести ову адресу у бројне ознаке формата комбинације три пута по четири броја са тачкама између (111.111.111.111). Већина оперативних система има пречице датотека домаћина (хостова) за претраге домена домаћина пре него што то учини DNS (Domain Name System) ради убрзавања претрага и уопште рада. Уколико се оваква датотека измени онда првобитна претрага или задата адреса неће бити пронађена као таква већ се тиме омогућава прикривена претрага и прикривање резултата команде давањем обмањујућег резултата са малициозном намером. Уношењем информација поверљиве природе овим путем, које кориснику изгледа потпуно нормално и легитимно али оваква информација иде директно фишеру.

Напади реконфигурисања система – мењају (модификују) подешавања на корисниковом рачунару у циљу компромитовања информација. Један од типова ових напада је измена корисниковог ДНС сервера како би се лажне информације овог типа могле дистрибуирати и другим корисницима, други тип је реконфигурисање корисниковог оперативног система на начин да сва комуникација коју корисник врши буде пропуштана кроз прокси који се најчешће налази изван рачунара овог корисника, ово такође представља вид напада човек између. Сличан напад је напад под називом „бежични зли близанац“ код којег се фингира конектовање на непостојећи или постојећи злонамерни извор бежичног Интернета. Након оваквог конектовања сва активност овог корисника се надзире или се чак мењају Интернет странице које захтевају легитимисање корисника па на тај начин купе поверљиве податке од стране корисника.

Крађа података – оног тренутка када је злоћудни програм или код иницран на рачунару корисника он тада може директно красти поверљиве информације. Њих чине шифре, корисничка имена, активациони кључеви софтвера осетљиви и мејл, као и сваки други облик информације која је похрањена на рачунару жртве. Ово се веома лако може учинити филтрирањем података претрагом поверљивих уноса који се веома лако проналазе прављењем шаблона за претрагу оваквог типа података. Крађе података се нашироко користе код фишинг напада у циљу остваривања комерцијалне и индустријске шпијунаже, на основу (вишеструко потврђене и оправдане) тезе по којој се на приватним рачунарима запослених налазе веће количине поверљивих података њихових фирми (а које се обично чувају на веома добро заштићеним серверима чиме се вишеструко смањују трошкови извршиоца), а такође се овим путем може доћи и до поверљиве документације као што је пословна преписка и кореспонденција или документација заштићених дизајнова које могу јавно „исцурети“ чиме се наноси економска штета или брука жртви.

ДНС базирани фишинг - „фарминг“ подразумева у овом смислу било који облик фишинга код ког постоји примена било каквих измена интегритета процеса претраживања за именом (називом) домена. Као основна разлика са фишингом наводи се да фишери теже да искористе методе социјалног инжењеринга или методе прикривања и замагљивања пута до одређене дестинације (инфицираног веб сајта) док фарминг напади представљају манипулацију различитих компонената основних домена и система именовања хостова, за погрешно усмеравање на исте дестинације као код фишинга. Ово укључује тровање датотека иако домаћинова датотека по дефиницији не представља део ДНС-а. Следећи облик ДНС базираног фишинг напада подразумева тровање корисниковог ДНС кеша са нетачним информацијама које ће се користити у будућим сесијама корисниковог конектовања на Интернет да га усмере на неку другу локацију од жељене. У нашем истраживању 68,75% испитаника изјаснило се да је фарминг савршенији и софистициранији облик фишинга, док је 18,75% њих сматрало супротно, као и 100% учесника делфи верзије.

Фишинг инјекцијом садржаја означава убацивање злоћудног садржаја у легитиман сајт. Овако убачени злоћудни садржај може вршити усмеравања на друге преварне сајтове, инсталирати злоћудне програме на корисников рачунар или убацивати фрејмове или садржаје који ће преусмеравати садржаје на сервер фишера. Три су основна типа фишинга садржајном инјекцијом, који могу имати најразличитије варијације:

- може се компромитовати сервер кроз његове безбедносне рањивости и преко замене или додавања легитимног садржаја злоћудним

- Злоћудни садржај може бити убачен на одређени сајт путем међу скриптну рањивост (cross – script vulnerability, рањивост преклапања скрипти). Она представља рањивост у облику програмске грешке која претпоставља долазећи садржај из екстерног извора, као на пример, блог, корисничка оцена неког продукта, термин за претраживање или електронска порука базирана на вебу. Овакав садржај може имати облик злоћудне скрипте или другог садржаја, који није адекватно профилтриран и који се активира у претраживачу корисника, стартујући злоћудни садржај[177].

- могу се активирати на сајту кроз рањивост SQL инјекције. Ово представља начин изазивања даљинског извршавања команди у базама података кроз даљински сервер који може изазвати цурење података. Као и претходни случај у питању је резултат неадекватног филтрирања долазећих и одлазећих пакета података.

Фишинг типа човек између (посреднички напад) претпоставља позиционирање извршиоца између корисника и легитимног сајта, који користи брзину комуникација и злоупотребљава одређене безбедносне протоколе и временски проток од уноса до пријема информације. Поруке адресиране на легитимни сајт се пресрећу од стране фишера, који информације из оваквих комуникација архивира у циљу даљег злоупотребљавања, и трансферује даље легитимном сајту а потом пресреће и одговоре и прослеђује их кориснику. У овом

[177] Посебан случај је тројанац вирус под називом Silentbanker, који се појавио у јануару 2008.год. а чији је МО даунолоадовање најобичнијим сурфовањем, без знања корисника, функционише неприметно између комуницирања банке са корисником дајући потпуну слободу кориснику да оперише у баковној сесији веб банкинга, након чега му празни рачун.

облику не постоји препознавање напада, жртва и легитимни сајт (који се такође може одредити као жртва) су потпуно несвесни напада. Такође, овај напад се може користити и у пресретању сесија, са или без похрањивања било каквих информација[178].

Фишинг претраживачких сервиса је новији облик фишинг преваре који се састоји у креирању веб страница (сајтова) у вези лажних производа, прибављању индексирања од стране великих претраживача за такве сајтове, након чега пуким наручивањем таквих производа или логовањем на тај сајт од стране корисника прибављају њихове поверљиве информације.

Да би постигао оно што жели извршилац мора да учини свој мамац примамљивим и убедљивим. За овако нешто фишери користе многе трикове, одређени аутори[179] деле ове трикове у две групе: социјалне и техничке. Категорија социјалних подразумева приче, сценарија и методологије које се могу користити за креирање убедљивог контекста за социјални инжењеринг, за који је вероватно да ће „навући" жртву или је чак навести да веома ентузијастички ода потребне информације о својој личности и неком економском добру, фишеру. Техничка категорија садржи коришћење техничких трикова који утичу на програм за читање електронске поште[180] (а самим тим и примаоца и читаоца електронске поште) или браузер у циљу одржавања у заблуди корисника и омогућавања приказивања вештачког социјалног контекста крајњем кориснику.

У емпиријском истраживању у погледу питања у вези најчешће сретаних облика фишинга у пракси испитаници су се одредили за одговор: фишинг порукама на енглеском језику њих 92.3%. У новијим моментима се дешава да се, у овој области, користе он лајн преводиоци и аутоматизовани програми, који генеришу поруке које се аутоматски преводе на српски језик и тако шаљу на живе адресе у Србији али и шире, за шта је 7,7% испитаника одредило у нашој анкети. Веома је карактеристично да и за наше подручје у овој области има интересената, дакле, лако је закључити да постоји одређена економска исплативост за овакве извршиоце, као и да ће ово постати масовнија појава.

4.2.3 Метододика социјалног инжењеринга

Како би натерао жртву да кликне на линк у СПАМ поруци неопходно је да пружи одговарајући и вероватни разлог (или колоквијалним речником „навлакушу"), па самим тим и информације које иницијално пружа морају бити

---

178 Један од еклатантних примера напада се десио у мају 2007.год. када су корисници PayPal-a eBay-a били преварени моћном фишинг техником, када су њихови браузери (у овом случају ИЕ7) без реакције антифишинг филтера и Нортона 360, добили низ питања о приватним подацима приликом логовања на ове сајтове. У питању је био злоћудни програм који је браузеру дозвољавао одлазак на адресу која се УРЛ-ом преводила, али се овај програм качио на ИЕ7, као датотека екстензије .длл и у транзиту мењао садржаје и купио информације.

179 Jakobsson M., Myers S. Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft, 2007 by John Wiley & Sons, Inc. Hoboken, New Jersey, p.12.

180 Посебни екслузивитет јесу тзв. *pushmail* могућности везане за нове телекомуникационе смарт уређаје и директне приступе серверима маил боксева.

веома убедљиве. Сценарија за фишинг су готово непресушна, нека од најчешћих су следећа: Ажурирање безбедносних поставки, Непотпуна информација о рачуну, финансијског добитка или попуста, лажна ажурирања рачуна[181]...

4.2.4 Методика техничког аспекта

Најчешћи облици су: Искоришћавање легитимних фирми, логоа и фотографија (већина људи и није свесна како је лако нити има у виду из ког разлога би неко копирао слику, лого или сл.) спуфовања мејлова, сакривање УРЛ-а, енкодирање и поклапање, коришћење ботнетова и зомби нетова.

4.2.5 Методика фишинга

Могуће је проучавати методику поступања фишера из различитих углова. ***Класични фишинг напади***[182] могу се описати на следећи начин, преко корака, на основу којих је могуће претпоставити и слабе тачке жртава, које извршиоци користе али и моменте и слабе тачке извршилаца, када су они најрањивији а које могу искоритити органи гоњења:

Први корак[183]: фишер шаље својој потенцијалној жртви електронску пошту којом се представља као администратор банке или неке друге организације која може депоновати личне податке. Он код овог напада веома пажљиво бира: боје, графичке елементе, логое и речи (фразе и крилатице) компаније коју жели да имитира. Он мора имперсонирати поуздан извор поруке. Овде фишери користе оруђа спамера (чак и римејлере eng. *remailer*) за слање великог броја порука на огроман број „живих мејл адреса".

Други корак: потенцијална жртва чита поруку и „пеца се на мамац" пружајући нападачу приватне податке, кроз слање одговора са подацима или кликом на понуђени линк у ел. пошти, и уношењем података у формулар понуђен на сајту који је линкован, а који се чини сајтом фирме која је у питању.

---

181 Једна од интересантнијх скоријих је у оквирима социјалне мреже Фејсбук (eng. Facebook) веома вешто смишљена превара корисника ове мреже. Наиме у питању је тројанац (регистрован под именом Troj/Iframe-ET.) који се убацује у систем корисника уколико падне на превару. Превара стиже кориснику као порука следеће могуће садржине: ЛОЛ (Веома смешно енг.laughing out loud, laugh out loud, или lots of laughs) „ова девојка бива поседована након што јој полицајац прочита поруку о статусу" или „ова девојка има интересантан начин гутања банане" „матурска хаљина која је девојку која ју је носила коштала избацивања из школе": све поруке су веома вешто смишљене како би значајно брзо и без размишљања сваки корисник кликнуо на линк и примио тројанца. Више о овоме на: http://www.sophos.com/blogs/gc/g/2010/05/31/viral-clickjacking-like-worm-hits-facebook-users/ доступан 02.08.2011.год.

182 OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, може се пронаћи на сајту ОЕБС. Материјал припремљен за 72. састанак овог тела, p.18.

183 Неки теоретичари говоре и о нултом кораку о чему ће се елаборирати након приказа ове типологије.

Трећи корак: преко овог лажног сајта или ел. поште[184] сви приватни лични подаци се директно сливају код извршиоца.

Постоје многи нивои на којима се могу применити различите технике за превенцију или репресивно деловање на фишинг. Базични проток информација фишинг напада изгледа овако[185]:

Нулти корак (овај корак и представља припремне радње, па је боље описати га као нулти): Припрема фишера за напад. У различитим случајевима као на пример преварним нападима са искоришћавањем рођачких (или сличних) домена[186], неопходно је да се прво региструју ови домени. Фишери или креирају потпуно нове овакве домене, или трују неке постојеће (што је много чешћи случај) путем злоћудних програма или хакерисањем. Овакви сервери су подешени да примају информације од корисника преко веб базираног интерфејса или злоћудних програма инсталираних фишинг нападима. Тактички приступи (технике) извршилаца фишинга обухватају следеће: мејлови (електронске поруке) који личе на званичне или оригиналне; копије званичних адреса сајтова са минорним изменама УРЛ, примена сличних домена; HTML базирани мејл, како би се злоупотребила могућност читања УРЛ информације (посебно у скраћеним верзијама истог); стандардни прилози у облику вируса и тројанаца; креирање персонализованих или јединствених и мејл порука; лажно постовање на популарним местима за постављање порука и мејлинг листи и сл.

Превентивне мере: У одређеним случајевима се може спречити напад и пре него што се деси. Жртве (појединци или фирме) се могу припремити за нападе у случајевима редовног рада, како би се побољшала одговорност и смањили могући губици. Овакве припреме укључују:

Постављање мејл адресе на коју се корисници могу у најкраћем року пожалити у случајевима фишинг напада или спуфинга[187.] У оваквом случају омогућава се бржа реакција одбрамбених структура.

Надзирање мејлова који су „одскачући“. Већина фишера користи електронске адресе у гомилама, вештачки креираних од стране рачунара, од који су многе непостојеће, или користе адресе које припадају институцијама које су предмет напада. Бујица оваквих мејлова означава да је напад у току.

Надзирање броја позива и природе постављаних питања потрошачком сервису фирме. Уколико статистички врх показује максимум у одређеним питањима, као на пример промене шифара, може индицирати фишинг напад.

Надзор активности на рачунима корисника са циљем проналажења аномалија, као на пример, велики број логовања, промена шифри, трансфера и подизања новца и сл.

Надзор над применом и коришћењем логоа компанија и фирми, њихових жигова и дизајна. Често се користе јавне слике и логои који се могу преузети са

---

184 Према www.ngsconsulting.com do sada najuspešniji napadi su preko fišing i mejl poruka.

185 Jakobsson M., Myers S. Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft, 2007 by John Wiley & Sons, Inc. Hoboken, New Jersey, p.37.

186 У питању је термин којим се означава сличан домен по свим карактеристикама, понекада веома тешко разазнатљив од оригинала.

187 Постоји у оним случајевима када се адреса пошиљаоца фалсификује или прикрива у циљу коришћења у преварама, примени техника социјалног инжењеринга или фишингу.

Интернета, од стране фишера у циљу обмањивања жртава. Ово се често може регистровати на серверу кроз празан или неадекватни погрешни „усмеривач“ на лого или фотографију логоа. Тиме се може водити евиденција о корисницима и пратити активност на каснијој употреби ових логоа.

Установљавање и успостављање „тегли меда“[188] („хани потова“ енгл. honey pots) и вршење надзора за регистровање електронских порука које се наводно шаљу из институција које су могуће жртве.

Сазнавање момента отпочињања напада даје циљаној институцији (жртви) да примени противмере отпочне сопствену истрагу и иницира полицијску, постави праве људе на одговорна места у циљу адекватног и правовременог одговора

Први корак: Малициозни товар (у облику злоћудних програмских садржаја) стиже кроз неки облик пропагандног вектора. У нападу типа обмањујућег фишинг напада најчешће је то електронска пошта. Код случајева злоћудних програма или напада системског реконфигурисања, овај товар је најчешће злоћудни код, који представља прилог одређене електронске поште, или неочекивани део неког пакета даунлоадованог програма или једноставно искоришћавање рањивости одређених безбедносних протокола и програма. У случају ДНС тровања садржај је лажна ИП информација. Код фишинга претраживачких сервиса он је референцирање у претрагама преварних сајтова. И код крос скриптних напада у питању је злоћудни код похрањен на легитимном сајту или увезан у УРЛ-у или електронској пошти, зависно од врсте и типа напада.

Превентивне мере: Детектовања предстојећег напада. Код одређених облика напада фишер мора поставити домен како би примао податке прибављене фишингом. Један од облика превенције је превентивна циљана регистрација домена са циљем проналажења вероватно спуфованих домена. Овим се може смањити доступност већине преварних сајтова. Овај систем није лош, али има својих негативних карактеристика, које се могу веома брзо и лако искористити. Један пример је карактеристика ИЕ 8 код ког постоји пријављивање фишинг сајтова, оно се може веома лако злоупотребити на различите начине. Неке фирме нуде систем регистрационог надзора који би евидентирали регистровање потенцијалног маскираног домена, као и надзирали било какву активност са тог сајта у циљу долажења до лица које је регистровало исти[189]. Неки од предлога су укључивали и одређени грејс период до активирања сајта од регистрације нових домена, у ком би се легитимни носиоци Досадашњих домена могли жалити или ставити примедбе на нови регистровани домен. Ова мера може утицати на рођачке домене али не може утицати на лажно представљање имитирање легитимних сајтова од стране фишера.

Превенција „уваљивања фишинг товара“. Прва прилика по отпочињању напада је управо у превенцији убацивања „уваљивања“ товара, у облику нпр.

---

188 У надевању назива за ову противмеру покушало се са хиперболом која презентује начин лова на медведе у постављању замке у облику тегле меда на коју се, као мамац, лепи.

189 Гугл је покушао да иде корак даље по основу доменских називних кључева, за више о томе погледати на:
http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBUQFjAA&url=http%3A%2F%2Fcode.google.com%2Fapis%2Fmaps%2Ffaq.html&ei=4EWnTIDSHYHqOaH6hZwM&usg=AFQjCNGe8vV-geAqBc--lH9ads4VJLZBUw&sig2=t1 8B10O4Dm9twiVK9j_tpA доступан 02.09.2011.год.

Електронске поште или искоришћавања безбедносних рупа. Ово представља ометање првог корака тока фишинг напада.

Постављање фишинг сајта често подразумева прављење копије сајта који се имитира. Некада је могуће анализирање шаблона приступа у логовању на легитимном сајту и на тај начин регистровање фишерских активности даунлоадовања. Док се садржаји јавних сајтова не могу држати подаље од фишера ово може обезбедити време за реакцију на напад, рану анализу базирану на ИП адресама које се користе у циљу убрзавања истраге једном иницираног напада.

Неке службе покушавају претраживање мреже и идентификовање нових фишинг сајтова, пре него што се активирају. Често се као резултат ових јавља обарање фишинг сајта пре него што се он активира. Ипак у већини случајева фишинг сајтови остану недоступни претраживачким пауцима (како се ове службе називају, Web crawler, Web spider, Web scatter)[190], најчешће због неактивности фишинг сајтова, они и не морају бити активни дуже време, обзиром да се већина информација прибави у иницијалном периоду. У просеку фишинг сајтови су активни највише два дана, најчешће неколико сати, колико је ефективно време искоришћавања напада.

Противмера у кораку један може бити и филтрирање. Филтери електронске поште за спречавање спама (електронских порука – ђубрета, нежељене поште) често могу бити успешни и за борбу против фишинга. Ово се обично чини подешавањем анти спам филтера да препознају карактеристичне познате фишинг поруке и блокирају их, такође, статистички и хеуристички спам филтери могу делом бити ефектни у погледу фишинг напада, али ту се могу јавити проблеми уколико права порука има сличности са фишинг поруком, тада се може десити да се грешком блокира порука која није фишинг порука.

Обмањујуће фишинг поруке морају имитирати реалне поруке и користити елементе реалних, као, на пример, боје и логое фирми увезане у поруке – права употреба реалних логоа умногоме повећава ефикасност фишинга. Једна од могућих противмера је регистровање неауторизоване употребе логоа, са друге стране, фишери могу предузимати разне мере како би избегли просту компарацију фотографија или логоа, на пример, више ситних сличица које креирају већу слику која представља лого или примена транспарентне слике (транспарирање више делова једног истог имица како би се креирао нови) у креирању композитне слике. Како би се све ово избегло све слике (фотографије и други облици дигиталног имицовања) морају се потпуно рендеровати[191] пре анализирања. Посебан проблем би се могао јавити у случајевима примене ситних измена на логоима и ознакама порекла или дизајновима када се не користе идентични елементи већ се суштински мењају.

---

[190] Више о овоме доступно је на http://en.wikipedia.org/wiki/Web_crawler последњи пут приступљено 31.05.2010 год.

[191] Рендеровање представља процес генерисања фотографије – имица из модела путем рачунарског програма. Модел је опис тродимензионалног објекта у стриктно дефинисаном рачунарском језику или структури података. Имиц је дигитална фотографија или растер графичка фотографија. Више можете погледати на http://en.wikipedia.org/wiki/Rendering_%28computer_graphics%29 доступан 31.08.2011.год.

Аутентифицирање електронске поште. Фишинг поруке обично преварно изгледају да стижу из извора познатог кориснику. Најчешће се то ради на два начина: - фалсификовањем повратне адресе

- регистровањем тзв. рођачког домена (на пример, commerceflow-security.corn у циљу спуфовања реалног домена commerceflow.corn) и слање мејлова са тог домена.

Ова мера може имати веома великог утицаја на фишинг, наиме она омогућава сигурност да је мејл порука послата из извора који дефинитивно представља странку која је послала исти. Оног тренутка када се буде нашироко примењивала имаће потенцијал за превенцију фалсификовања повратних адреса и приморава фишера да открива праве адресе, или да региструју домене који изгледају исто као оригинали. Предности су да тада повратне адресе могу бити мање обмањујуће него фалсификоване, такође и регистрација оваквих домена може бити раније регистрована и фишеру се може лакше учи у траг преко поступка регистрације домена. Више врста ове идентификације постоји: Sender-ID and SPF – IETF Experimental Standards, Domain Key Identified Mail (DKIM), Mail Transfer Agent (MTA), а други тип ауторизације од наведених (који захтева поседовање посебних интерфејсова – код генерисања специфичних адреса или инфраструктуре – код токена) је да шаљу идентификационе и коришћење специфичних, аутоматски генерисаних мејлова за пошиљаоца са унапред утврђених и примаоцу познатих адреса, могуће и уз употребу токена или специјалних сертификата (издатих од примаоца). Криптографско потписивање и мејл поште (на пример S/MIME) може имати будућност у погледу заштите, обзиром на постојеће системе, јер уколико се буде масовно користило, а ограничиле оперативности непотписаних порука[192].

Противмера одбацивање рођачких домена, у недостатку масивизирања претходне аутентификације у првом кораку неопходно је да корисници подробно анализирају своје мејлове и реагују уколико примете преварну ситуацију.

Противмера безбедносно ажурирање софтвера, популарне закрпе, у циљу спречавања искоришћавања безбедносних слабости софтвера. Дистрибуција ових закрпа је посебан проблем, највише због тога што се широм дистрибуцијом достављају и хакерима информације о њима. Но и то се да решити.

Корак други: Корисник предузима активност која га чини рањивим у смислу компромитовања поверљивих информација. Код преварних фишинга у питању је притисак на дугме миша по линку фишера, код логера кључева корисник иде на легитимни сајт и уноси податке, код напада претраге имена домаћина корисник

---

[192] Веома је интересантна Национална Стратегија САД о поузданим идентитетима у сајбер простору (Strategy for Trusted Identities in Cyberspace) која подразумева примену смарт картица и дигиталних сертификата. Све о овоме прочитати на
http://www.msnbc.msn.com/id/37943900/ns/technology_and_science-security/
http://www.computerworld.com/s/article/9178537/White_House_seeks_comment_on_trusted_ID_plan?taxonomyId=145
http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=225701456&cid=RSSfeed_IWK_News
http://www.nextgov.com/nextgov/ng_20100628_8259.php?oref=topnews
http://www.govinfosecurity.com/articles.php?art_id=2694
http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace
http://www.dhs.gov/xlibrary/assets/ns_tic.pdf доступним 29.06.2010. год.

верује да иде на легитиман сајт, а у ствари иде на фиктивни, преварни, сајт, где уноси поверљиве информације.

Превенција или ометање активности корисника код корака два тока информација код фишинга подразумева ситуацију довођења корисника у ситуацију, и на локацију, у којој је његова заштићена информација компромитована. Тада он може предузети више мера:

Први корак је обука и образовање корисника, најчешће кроз инструисање на поштовање одређених правила, као, на пример, не праћење одређених линкова, бити сигуран да је коришћен SSL[193], као и верификација домена. Но у пракси се показало да то баш и није дало адекватних резултата[194].

Следећи је употреба персонализованих информација, као, на пример, пратеће фотографије, пуног имена и презимена корисника итд. Једна од интересантних варијација се може приказати кроз унапред уговорену (између примаоца и пошиљаоца) текстуалну идентификациону ознаку.

У једном примеру дата је комбинација текстуалних и фотографских техника – констатација где је рођено лице (You were born in Prague) уз фотографију новчића са ликом британске краљице. Иза овог аутентификационог прозора долази други (уколико је погођена идентификација) који садржи образложење према којем се корисник налази у сигурном окружењу и зашто. На сличан начин се може користити описан облик аутентификације и на сајтовима, приликом уношења корисничког имена а пре шифре, али ипак администратори сајта морају потврдити идентитет корисника пре давања званичних идентификационих обележја званичне фирме.

Следећи облик противмере је приказ варљивог садржаја у низовима (канонски). Осим у случајевима рођачких домена у свим осталим случајевима фишери врло често немају ни приближно легитиман назив домену са којег наводно шаљу поруке (код обмањујућих фишинг техника). У овом моменту линкови на које се корисник упућује могу бити приказани кориснику према наредби аутора – како он хоће да изгледају кориснику. Ово чини лаким фишинг обману о којој је реч, при чему се користе најразличитије рачунарске технике. Намерно сугестивно обојене линкове као на пример: http://kasperski.com а реално води на http://phisher.corn. Затим прикривене линкове, преусмеравајуће линкове (у овом случају се преусмерава на основу преводилаца унутар браузера), програмски прикривени линкови који постоје у случају дозвољавања јава апликацији да ради у току сесије, при чему, се могу користити њене слабости и када корисник мишем прелази преко линка да се програмски измени садржај линка, и слично. Једна могућа противмера је да се у и мејл клијенту или браузеру отварају садржаји на начин на који је могуће предвидљиво и јасно идентификовати потенцијално опасан садржај као сумњив, и већ уграђене алатке у мејл клијентима да се поруке виде само у простом формату,

---

193 Secure Socket Layer, више о томе на: http://www.webopedia.com/TERM/S/SSL.html последњи пут приступљено 10.09.2011.год.

194 Jakobsson M., Myers S. Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft, 2007 by John Wiley & Sons, Inc. Hoboken, New Jersey, p.44 . у свету на пример Гугл покушава преко домејн ки система, а са друге стране можемо видети и да и извршиоци – нарочито они организовани покушавају доскочити и системима аутентификације у два корака погледати на http://www.net-security.org/malware_news.php?id=1472 доступан 26.09.2010.

док се фотографије и други опасни садржаји блокирају док их корисник не отвори ручно, свестан ризика.

Следећа противмера је утицање на навигацију браузера се може користити у смислу чак и када корисник кликне на преварни линк може аутоматски бити постављена информативна порука упозорења од стране система. Најразличитији комерцијални програми нудее овакве алатке, користећи веб облаке (cloud – e) својих корисника за прикупљање и обраду информација о потенцијално опасним локацијама.

Противмера детекције неконзистентних информација ДНС –а, у случајевима ДНС заснованог фишинга (фарминга) фишери се ослањају на претходне контакте одређених корисника са одређеним доменом, па очекују да исти неће поново ићи на тај сајт, већ ће аутоматски кликнути на линк. У овом случају могуће је да корисник чува податке о свом претходном посећивању сајта независно од ДНС кеша и да тако примети несагласност са претходним. У овом случају је могућа и противмера која подразумева чишћење историје о крстарењу Интернетом, и посећеним доменима.

Противмера модификовања референцираних имица. Ова мера се може применити и на корак три и четири. Наиме могуће је да фишер даунлоадује намерно фотографију (имиџ) са легитимног сајта у циљу искоришћавања у сврхе фишинга. Фирма која је оштећена може регистровати овакав захтев за даунлоадовањем и истраживањем захтеваочевог поља покушати да спречи даље искоришћавање истог – прекидањем скидања или каснијом дистрибуцијом замењених слика сликама са упозорењем о фишинг нападу. Наравно, могуће је користити и програме за праћење дистрибуције одређених садржаја на Интернету датотеке типа doc. pdf. ppt и сл. екстензија, и на тај начин спровести праћење кретања одређених садржаја ради лакше реконструкције догађаја и лишења слободе свих учесника у овој криминалној активности. Овај поступак је могућ преко одређених сервиса нпр. www.readnotify.com.

Противмера превенције компромитовања навигације и података

Треба поменути да се ова противмера може користити и у кораку број четири. Код другог корака корисник радњом коју предузима постаје рањив на фишинг нападе, као на пример навигацијом на фишинг сајт (уз помоћ Интернет браузера – претраживача – често називаног и навигатором), док се код корака четири компромитују поверљиви подаци.

Прва противмера представља повећање размене података између апликација – као што су филтери СПАМ порука, и мејл клијенти и браузери (претраживачи). Информације сакупљене при обради порука могу помоћи у осујећивању покушаја преотимања информација фишингом. Оног тренутка када се примети сумњива порука свака апликација може добити ту информацију и у складу са њеним значајем поступати са њом другачије од аутентификоване. Сумњива порука може визуелно бити обележена, тада и скрипте могу бити забрањене, линкови се могу приказати са правим адресама и сл. Исто пружа многе нове начине за превенцију фишинга.

Корак три: Описано уношење информација у претходном кораку је, у ствари, део трећег корака када се од корисника тражи да се идентификује кроз корисничко име и шифру, најчешће то од њега захтева удаљени сервер или веб тројанац. Овај може бити легитимни сајт (код напада килогера) злоћудни сајт (у

случају преварно базираних фишинг напада) и легитимни сајт који је затрован малициозним кодом (у случају напада инјекције садржаја).

У овом кораку протока информација код фишинг напада постоји моменат у којем се од корисника тражи одређена информација и тада се компромитују поверљиви подаци. Превентивне мере овог корака иду ка елиминацији или превенцији овог момента. Прва противмера је филтрирање скрипти међу сајтовима. Скриптовање између сајтова представља напад инјекцијом садржаја, и он може бити изведен на два начина. Први подразумева инјекцију садржаја у легитиман сајт (Интернет страницу) у кораку један кроз смештање истог у легитимни сервер, као део утисака корисника, аукција, веб базиран и – мејл и сл. Други пут је укључивање злоћудног садржаја у URL који је део и – мејл поруке (електронске поште), на пример везивањем скрипте у претраживачком упиту, који ће бити приказан са резултатима претраге. Овакав садржај везан за URL биће прослеђен са корисника на легитимни сервер у кораку два и враћен као део момента о коме је горе елаборирано у погледу личних и поверљивих информација у кораку три. Као превенција описаних у кораку три неопходно је извести ометање протока информација фишинг напада. То се мора чинити филтрирањем садржаја информација, како би се одстраниле било какве скрипте. Следећа противмера је онемогућавање инјектованих скрипти, два су могућа пута[195] одбране од описаног, први подразумева филтере који „држе подаље“ и оне који „дозвољавају унутра“, први региструју малициозни садржај и блокирају га, док други детектују легитимни садржај и блокирају, било шта, што није препознато као исти. Први су се лоше показали у овом случају одбране и рањиви су на ове облике напада значајно у односу на друге. Неки аутори предлажу да се у Интернет претраживачима уведу посебни, виртуелни, дугмићи, који откривају да ли сајт на који се браузер конектује - има или нема скрипте. Овакве “етикете” би се могле користити у циљу спречавања уношења и активирања скрипти на сајту.

Корак четири: Жртва одаје своје поверљиве информације малициозном серверу, злоћудном програму који је активан локално на рачунару жртве, или програму који прати и прислушкује комуникацију и легитимну интеракцију.

Моменат који се може препознати за деловање у смислу превенције и дејствовања по иницијацији напада, а у вези овог корака, је моменат у којем би се овакав напад могао открити као злонамеран или преваран (па да сама жртва не проследи поверљиве информације) или да се овај проток информација на неки начин прекине или измени како би информације које су поверљиве природе имале неки облик или средство прикривености. Једна од противмера би се могла одредити као антифишинг алатка на статусној или некој другој линији Интернет претраживача. Оваква средства користе различите технике за утврђивање легитимитета сајта, укључујучи и базе података о познатим и пријављеним фишинг сајтовима, анализу УРЛ на сајту, анализу фотографија и делова фотографија, анализу текста на сајту, као и друге хеуристичке алатке за детектовање фишинга. Но, и ове алатке се могу, у некој догледној будућности злоупотребити, обзиром на брзину развоја технологија. Следећи облик обухвата блокирање трансмитовања података на одређене ИП адресе за које је потврђено да су повезане са фишингом,

[195] Jakobsson M., Myers S. Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft, 2007 by John Wiley & Sons, Inc. Hoboken, New Jersey, p.61.

па исто представља покушај да се омете четврти корак информационог тока. Он се колоквијално назива постављање црних листа дестинације података (eng. *blacklisting*), но, поред свих напора, овај начин има мана јер се информациони ток може ипак одвијати и преко комуникационих канала ДНС (енгл. *Domain Name System* (DNS)) који служи за превођење адреса домаћина у ИП адресе. Следећа мера је покушај да се унос података измени, па се налазе алтернативни путеви, као, на пример, унос поверљивих података селекцијом или избором кликом миша на екрану[196], чиме се злоћудни програми за регистровање укуцаних информација на тастатури онемогућавају у извршењу и крађи тих података. Управо из овог разлога извршиоци су увели скринлогере и скрингребере. Други облик ове мере је када се од корисника захтева да одговори на одређене графички базиране питалице о шифри без уношења, или откривања другим путем, праве шифре. Овакве технике могу бити јако ефективне против краткорочних облика злоћудних програма за надзор активности и представљају мере које ће се засигурно даље развијати у борби против фишинга али и других облика сајбер криминалитета. Следећа мера је узајамна аутентификација. Код примене шифара у комуникацији веома чест случај је да је обема странама у комуникацији позната шифра одређеног корисника. Уместо директног уношења овог идентификационог елемента може се користити заједнички протокол аутентификације[197] за пружање доказа да обе стране поседују акредитиве а да, при том, ни једна од страна не трансмитује информације поверљиве природе у вези саме шифре. Један од облика ове мере је и да корисник приликом аутентификације приказује одређену фотографију (унапред уговорену са другом страном) која се чува на скривеном месту ван домашаја трећих лица. Следеће мере се могу користити и у четвртом и у шестом кораку. У питању су имплементирања поверљиве стазе или везе, а ова мера се може применити и у оперативним системима када може бити квалитетно превентивно средство за напада злоћудних програма везаних за Виндоуз апликације, као и експлоатације оперативних система, па чак и компромитованог хардвера . Ова мера се најчешће може користити против обмањујућих фишинг напада и ДНС фишинга. Два су начина када се могу користити ове мере у смислу 4 корака информационог протока, приликом логовања кроз резервисани простор на екрану или кроз унос који није могуће пресрести. Последње се може остварити кроз дигитално потписан криптографски сертификат који садржи идентификациона обележја захтеваоца, лого који се мора приказати и јавни кључ и спецификацију тражених података. Када оперативни систем буде обавештен о постојећем уносу података кроз поверљиву везу или стазу, кориснику се нуди да унесе алфанумеричку секвенцу познату као

---

196 Jakobsson M., Myers S. Op.cit., p. 53.

197 Има више врста ових протокола неки од њих су: SPEKE [према Jablon. D. P. Strong password-only authenticated key exchange. Submission to IEEE PI 363.2, September 1996,], PAK [према Brusilovsky A. Password authenticated diffie-hellman exchange (PAK). Internet Draft, October 200.5.], SRP [Wu, T. The secure remote password protocol. In Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, March 1998.], AMP prema Kwon T. Summary of AMP (authentication and key agreement via memorable passwords). Submission to IEEE 1363.2, August 2003.], SNAP1 [према MacKenzie P. and Swaminathan R.. Secure network authentication with password identification. Submission to IEEE 1363.2, July 1999.] and AuthA [према Bellare M. and Rogaway P.. The AuthA protocol for password-based authenticated key exchange. Contribution to IEEE P1363.2, March 2000.] .

безбедносну секвенцу (secure attention sequence), тек када систем утврди да постоји позитивна секвенца, могуће је унети корисничко име и шифру.

Корак пет: Поверљиве информације се достављају фишеру, зависно од напада путем малициозног или компромитованог сервера, евентуално злоћудног програма локално активног на рачунару жртве, као, на пример, килогера или тројанца (када се трансмитују и са рачунара саме жртве). Извршиоци могу веома закомпликовати даљи пут ове информације кроз постављање разних зомби рачунара, инстант поруке, чет канале и анонимне П2П механизме трансфера података, на пример торенте, такође је могуће информације кроз тајне или јавно тајне канале, као на пример стеганографске јавне кључеве, који се могу убацити у јавну комуникацију кроз на пример постове на www.naslovi.net. Што се тиче могуће превенције на овом кораку један од могућих путева је и онај који је влада Јужне Кореје покушала у скоријој будућности – кроз условљавање подизања оперативног система постојањем безбедносног софтвера, законом[198].

Корак шест: Корисничка информација се користи у циљу лажног представљања. Као један од начина превенције злоупотреба у кораку бр. 6. је да се овакве поверљиве информације учине мање вредним, јер извршиоци тада претварају компромитоване поверљиве информације у новчану вредност – незаконитим коришћењем. Најчешће се за превенцију користи мер*а аутентификације два фактора*[199] која подразумева пружање доказа о поседовању најмање два од три критеријума: о томе ко је корисник (биометријске податке), шта има као доказ (смарт картицу и сл.) или о томе шта зна (назив или корисничко име и шифру). Најчешће се напади дешавају у сегменту – шта знаш, па је могуће да се убацивањем новог сегмента – шта има? може решити проблем. Најчешће се као овакво средство у САД тренутно користи уређај за креирање једнократних шифри (ОТП one-time-passcode (OTP))[200]. Но и ови уређаји су у последње време под ударом па је боље користити токене или смарт картице[201]. Следећа противмера може бити рачунарски заснована аутентификација другог фактора (која се лако може јавити као алтернатива смарт картицама због скупоће). Она функционише на тај начин што се памти рачунар са којег корисник приступа на систем који поседује ову безбедносну меру и сваки следећи пут се мора идентификовати рачунар. Следећа мера је заштита шифара кроз додатно шифровање приликом употребе и трансмитовање само тако шифрованих на одређени сајт ради примене. Тако се може имати јединствена шифра за различите сајтове а да њено приказивање на сајтовима буде различито за сваки сајт због различите енкрипције. Овде се име сајта који представља дестинацију увезује енкрипцијом са шифрованом шифром и може само тако бити и коришћено. Следећа мера је потврђивање трансакције која је аналогна мерама које банке користе у физичком свету. Она се може вршити на разне

---

198 http://www.zdnet.com/blog/security/zombie-pc-prevention-bill-to-make-security-software-mandatory/8487 последњи пут приступљено 04.09.2011.год.

199 Jakobsson M., Myers S. *Op.cit.*. p. 58.

200 Мастеркард је у новим видовима облика заштите увео постојање дигиталног дисплеја на картицама, који служи креирању једнократних дигиталних шифара за обављање трансакција – нешто слично OTP или TAH (Transaction authentication number – TAN) броју, који се користи само за дату трансакцију и има веома кратку валидност од тренутка генерисања. Више о овоме на http://www.mastercard.com/za/personal/en/education/fraud_protection.html доступно 26.06.2011.

201 Jakobsson M., Myers S. *Op.cit.*. p. 59.

начине применом различитих метричких елемената као на пример ИП адресе или присуство аутентификационих елемената као, на пример, колачића, карактеристика дестинационог банчиног рачуна, међурачунске трансакционе анализе шаблона. Ова анализа би требала бити у оквирима фактора означеног раније као шта знаш. Веома јак облик аутентификације се може користити применом другог поузданог извора нпр. телефона – позивањем лица комитента банке у тренутку вршења трансакције на број који је он оставио банци у циљу потврде трансакције или путем смс-а на мобилни претплатнички број. Следећа мера је увођење примене или коришћења података који, су према унапред одређеној политици фирме, одређени као обавезни за примену, а који, приказани трећем лицу, бивају за њега неупотребљиви. Овако утврђена политика диктира ко и на који начин може користити податке, па из тог разлога бивају неупотребљиви другима. Пример је плаћање преко Интернета, сајт који служи за плаћање има неколико елемената од којих је за плаћање битан процесор за плаћање, док се сви дуги подаци посебно похрањују и чувају, тако да за сваки сегмент постоји посебан облик заштите. Крађа сваког сегмента посебно не даје могућности злоупотребе фишерима, већ само крађа укупних података, а који су шифровани, што опет бива средство одвраћања. Када се трансакција изврши у процесор плаћања стижу трансакциони детаљи и информације о кредитној или дебитној картици, након чега их он дешифрује и проверава поступање по унапред утврђеној политици. Овде је пример ТАН број – који представља идентификациони елемент дате трансакције, са унапред датим и дефинисаним учесницима.

Корак седам: преварант остварује недозвољену имовинску корист или на други начин врши превару искоришћавањем поверљиве информације. Као честе мере се користе у разним финансијским институцијама одложено наплаћивање или остваривање (извођење) трансакције одређених типова трансфера новчаних средстава. Уколико се идентификује преварно поступање или рачун трансфер се отказује и економска штета се може избећи. Од великог значаја за проналажење извршилаца је праћење новчаног тока и употребе украдених креденцијала (акредитива). Фишери често перу новац кроз вишеструке слојеве и примењују анонимне инструменте и средства као на пример eGold, али на крају последњи и крајњи корисник је фишер, па му је могуће ући у траг.

У нашем истраживању испитаници су предвидели најопаснији облик фишинга у будућности, па према резултатима 31,25% њих сматра покушај преотимања информација у мобилним социјалним мрежама, а 66.67% испитаника у делфи верзији анкете. Затим 18,75% испитаника сматра фишинг највиших руководилаца мултинационалних компанија најопаснијим обликом фишинга у будућности а 8,33% у делфи и 50% (8,33%) фишинг политичких лидера. 16,67% испитаника у делфи верзији навело је као будуће облике фарминг и циљани фишинг.

4.2.6 Правила и смернице о поступањима за превенцију фишинга (и других облика крађе идентитета)

- уколико нисте корисник услуга или купац производа (потрошач) компаније која вам шаље овакве поруке, игноришите их, а чак и уколико. Преваранти се

ослањају на онај мали број лица која јесу корисници услуга и купци производа одређене компаније, како би навукли ту неколицину у своје мреже.

- чак и ако јесте потрошач никада немојте директно одговарати на овакве мејлове путем давања осетљивих информација. Уместо овога верификујте аутентичност путем мејла или путем телефонских контаката и службеника ове компаније, како би сте били сигурни у легитимитет захтева.

- никада немојте ићи на веб сајт преко линка у мејлу. Уместо тога отворите нови прозор претраживача и прекопирајте или укуцајте (што је најсигурније) УРЛ за који знате да је легитиман, или искористите већ направљене пречице у вашем претраживачу (мање поуздана верзија).

- проверите стање рачуна своје картице одмах након пријема ове информације о фишингу, тражите трансакције које нисте очекивали, чак и мале трансакције могу бити знак невоље.

- уколико случајно и дате своје личне информације, у најкраћем року обавестите надлежне органе. Банке и кредитне организације ће са оштећенима радити на превенцији злоупотребе овако одатих информација.

- упознајте се са триковима које преваранти користе како би сте били обавештени о модусима и техникама и могли приметити преварне мејлове у циљу спречавања превара. Знање је моћно оружје против ових преварантских игара.

- будите обавештени и одржавајте систем ажурним са информацијама и подацима, трудите се да ваш систем буде обезбеђен свим актуелним критичним софтверским закрпама и безбедносним софтверским програмским пакетима (анти СПАМ, анти фишинг, анти спајвер и антивирус програмима).

Софос група даје следеће смернице:[202]

Никада не одговарајте на пошту којом се захтевају ваше личне финансијске информације

Пратите сигнале који индикују да је неки мејл налик фишингу

Посећујте сајтове ваших банака уношењем адреса у браузере а не преко линкова

Пратите редовно своје стање рачуна

Обезбедите информације да је веб сајт који посећујете безбедан

Будите опрезни са својим личним информацијама

Чувајте свој рачунар

Увек пријављујте сумњиве активности

У току 2009.год. Федерација потрошача Америке (Consumer Federation of America (CFA)) била је тешко критикована у погледу поступања у вези заштите потрошача од крађе идентитета. 2011.године, из тог разлога је у марту (11.) објавила најбољу праксу у погледу заштите у овој области[203]:

Погрешно представљање у вези заштите од крађе идентитета. Службе за борбу против крађе идентитета би требале избегавати тврдње којима погрешно наводе кориснике својих услуга како оне могу обезбедити потпуну заштиту од свих облика крађе идентитета, откривања свих инстанци крађе идентитета или спречити

---

202 Sophos, Treatsaurus, Locus citatus, pp.101-2.

203 http://www.net-security.org/secworld.php?id=10731&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29 последњи пут приступљено 14.03.2011.год.

или зауставити сваки покушај извршења крађе идентитета – тврдње које ни једна служба не може начинити.

Ове службе морају водити рачуна и бити изузетно пажљиве у случајевима употребе сведочења (задовољних корисника) и приказа статистике обраде, како не би довели до погрешних закључака приликом тумачења таквих приказа а све у сврху комерцијализације.

Најбоља пракса захтева од ових служби јасна одређења о трошковима, одустанку од коришћења ових услуга, политике повраћаја средстава за које услуга није плаћена, начина решавања приговора и друге значајне информације.

Ове службе морају подробно објаснити начин функционисања појединих сегмената њихових програма као и како исти могу помоћи потрошачима

Најбоља пракса указује на околност да службе за заштиту имају јасну и транспарентну политику приватности корисника, да користе разумне и адекватне облике заштите појединаца и њихових личних података, као и да буду опрезне приликом дељења таквих података са другима.

Ове службе које пружају услуге помоћи жртвама би требале подробно објаснити шта конкретно предузимају у правцу пружања те помоћи, као и све облике ограничења или искључења одговорности, које се у таквим случајевима могу применити.

Службе које нуде осигурање или гаранције морају их пружити у подробном и прецизном облику, на лако доступним местима нарочито о политици фирме, као и опште услове пословања којима се исти прописују, а посебно ограничења и искључења која се односе на посебне случајеве.

Мејл фронтиер (mail frontier)[204] даје веома интересантну класификацију фишинга (код које се сам феномен објашњава кроз врсту описивања начина напада, понашање нападача и жртве, објашњава суштину преваре):

1. *риба стрелац*, која има креативан начин напада и изводи га и изван воде и у њој, она је позната по својим неконвенционалним нападима жртава кроз резак млаз воде (као у облику стреле, откуда и назив). Објашњава се понашање преваранта и суштина преваре, оно на шта он циља кроз следеће: најављује жртви да постоји одређена врста проблема (да су учестали напади на ваш рачун, покушајима да се погоди шифра, па је неопходна ваша акција да потврдите шифру, у што краћем времену), прети се са наступањем одређених непогодности и штета по ваш рачун уколико ви не реагујете у што краћем року, након чега вам се нуди лако решење кликом на понуђени линк. Овде извршилац ужива у преношењу панике жртвама да се неко намерио на њих. Уз ово се пружају многи савети како открити овакву превару[205].

2. *Пешчана риба*, коју описују као ону која живи на дну океана лако се скрива у песку и прави мртва, за њу жртве не очекују да буде превише токсична, у чему лежи њен мамац. Оно што се чини безазленим код ње је веома опасно, обично вам се нуди да учините нешто за себе, као на пример, учланите се у службу за

---

[204] http://www.mailfrontier.com/docs/field_guide.pdf доступан 09.08.2011. У питању је илустровани водич за жртве фишинга, који је веома луцидно и квалитетно одрађен, пружају се и подкласификације и поделе према природним везама са алудирањем на билолошке класификације животиња (управо врста риба) са приказом сличности и разлика.

[205] *Ibid.* str.2.

заштиту кредитних картица, или да постанете почасни члан удружења потрошача који користе картице. Суштина преваре је да вас извршилац навуче да кликнете на линк на који не би смели, кроз причину да вам чини неку услугу, кроз коју ви на његову молбу остварујете нешто веома повољно по вас.

3. *Разрока (Волај) риба*. Иако изгледа да је приглупа, безазлена и потпуно легитимна, то је превара. Овакав маил (риба) вара корисника, тако што изгледа као да стварно потиче од банке или кредитне уније. Обично захтева класичне и стандардне податке за картице и рачуне, као што су ПИН бројеви, или други осетљиви подаци који могу пружити приступ вашем рачуну. Пример је „ми вршимо ажурирања на систему па је неопходно да се улогујете, како би смо то и вама учинили“ или „ваша дебитна картица је, према нашој евиденцији, истекла – молимо вас да се улогујете и продужите рок важења“. Овај облик рибе вас вара тако што вам нуди помоћ како би добила податке о вашем рачуну.

4. *Сабљарка* је веома позната по свом изузетно уско циљаном приступу својим лаковерним жртвама. Ови облици напада су карактеристични по усамљеним извршиоцима који се ретко јављају у групама. Веома су трансакционо оријентисани, обично користе „реалну активност“ на вашем рачуну како би измамили одговор, оно што најчешће карактерише овај облик напада је да постоји један од ваших идентификационих елемената, као на пример ваше име, и најчешће се шаље на вас директно и не представља део масовно дистрибуираних мејлова. Пример је када Вам се обраћа са тврдњом да вас чека депозит од 223 ЕУР или траже од Вас да реагујете због тога што сте изгубили на аукцији он лајн. Суштина преваре овде је да користе ваше корисничко име, чланско име или друге персоналне информације како би изгледало што веродостојније. Обично указује на одређену трансакцију и наводи вас да кликнете на одређени злоћудни УРЛ.

5. *Рибарица* свој пандан у животињском свету има у риби која живи на великим дубинама у којима нема довољно светла, при чему она користи трик светла плаве боје које јој виси директно испред уста, како би намамила друге рибе и осталу храну светлуцањем. Када плен примети светло и приђе ближе ова рибарица га прогута. Преведено на терен високотехнолошког криминала фишери овим обликом технике објављују да сте добитник велике награде на одређеном такмичењу, након чега од Вас захтевају Ваше осетљиве личне податке, како би сте били награђени. Превара се у суштини ослања на компететивну страну личности, потребу да се личност доказује, жељу за победом и признањем, или на жељу да се нешто добије без муке или без плаћања.

6. *Риба папагајка* је веома привлачна риба, светлуцавих и лепих боја, светлуцајући и поигравајући се са светлошћу њена спољашњост је веома примамљујућа. Суштина ове преваре је ослањање на одређене сезонске или догађаје од националног значаја, чиме се искоришћава емоционална и милосрдна околност (нпр. у САД дан празника захвалности, а код нас, на пример, задушнице). Овде извршиоци користе потребу и жељу да се помогне другим људима, шта више покушава се документовати да су и друге особе већ помогле.

7. *Хоботница* – њу карактерише изванредна способност да се маскира узимајући друге облике и боје. Овакав напад је карактеристичан по постављању многих мамаца у различитим областима за навлачење жртава, користећи се

различитим претходно описаним техникама других напада. Суштина ове преваре је комбинација претходних метода фишера.

8. *Риба коњског репа* у последње време ређе примењивана техника фишинг напада због изумирућих карактеристика. Овај облик напада карактерише веома лоша израда порука, са словним и граматичким грешкама у енглеском језику, обично није адресирана на одређену мету већ су у питању масовно дистрибуирани напади. Карактеришу је преварни трикови који су старије генерације, веома лаки за приметити, осим оних најлаковернијих корисника Интернета.

Спуфинг[206] или обмањивање различитих врста преставља превалентно понашање корисника на Интернету у овом моменту[207]. Под овим појмом подразумева се техника у којој се лице представља као неко други, мејлом (и мејл поруком – садржински и формалним елементима – појавним обликом) или веб сајтом (опет и садржински и формом). Обично се ово чини копирањем садржаја легитимног сајта на нови – креацију извршиоца, даљи МО овог облика ВТК се своди на приморавање или обмањивање жртве да кликне на хиперлинк дат у мејлу, или на сајту, уместо куцања у адресној линији браузера УРЛ-а жељеног сајта. Ово жртву води на преварни фалсификовани сајт, који вара жртву да ода неке своје личне и идентификационе информације, нарочито у финансијском смислу. Наравно, спуфинг се врши у циљу омогућавања средстава за вршење даљих кривичних дела – фишинга, крађе идентитета или превара. У контексту фишинга, фарминг се развио као алтернатива фишингу, јер је овај облик криминалитета много тежи за откривање него фишинг. Фармингом се корисници преусмеравају (редиректују) на лажне или фалсификоване сајтове у случајевима када покушавају да приступе легитимним сајтовима (на пример путем неког веб претраживача – Yahoo, Google search) или путем линкова у имејл порукама које упућују, на први поглед, на легитимне сајтове[208]. Један од најчешћих облика напада 2005. године био је у облику захтева за потврдом и валидацијом рачуна у одређеној банци у облику броја, корисничког имена и ПИН броја. Исти почиње електронском поштом (писмом - поруком) прикривеном под именом, логоом и другим идентификационим обележјима банке код које поседујете рачун са обавештењем кориснику (обично комитенту) да је неопходно да ажурира своје податке у погледу одређеног рачуна у тој банци или финансијској институцији. Уколико је пецање успело, корисник, кликом миша на линк понуђен у овој поруци, одлази на фалсификован сајт и уноси, у неком облику фингиране сигурне везе, и одаје своје податке о рачуну и ко зна чему још. Истог момента извршиоци имају на располагању те податке у сврху крађе новца са тог рачуна (чак и путем напада човек у средини – прикривени посредник) или, још перфидније, за каснији промет оваквих података на Интернету у пакету са већим бројем других.

---

206 Спуфинг или прикривено и лажно представљање (Spoofing).

207 Jakobsson M., Myers S. *Op.cit.*. p. 59.

208 Један о новијих је случај Министарства финансија САД који је 03.05.2010.год. са више разичитих сајтова преусмеравао (редиректовао) саобраћај на друге лажне сајтове који су покушавали инсталацију злоћудних програма. Методика напада је увезани Ифрјем на три сајта министарства који вуку скрипте са других сајтова. Злоћудни програм делује само на оне посетиоце који до тада нису посећивали ове сајтове. Доступно на: http://www.theregister.co.uk/2010/05/03/treasury _websites_attack/

У већини случајева код напада линковани прикривени или фалсификовани сајтови невероватно подсећају до најситнијих детаља на оригиналне. Ови злоћудни сајтови (односно, њихови креатори) користе обично иностране домене у покушају да закомпликују процедуралне сегменте неког могућег кривичног поступка или прогона, те да створе јурисдикционе проблеме (позитивног или негативног сукоба надлежности). Напад ове врсте представља варијацију тзв. „хомографског напада“ који користи рупе у начину на који неки популарни браузери (Интернет претраживачи) приказују имена домена који користе словне знакове или идеограме неенглеског говорног подручја. Веома је интересантно како се могу користити словне ознаке, на пример ћириличних и латиничних истих слова као на пример а ћирилицом Unicode карактер U+0430 и а латиницом Unicode карактер U+0061. У питању су подврсте хоморгафског напада које се називају хомоглифски напади[209]. У овим случајевима веома је тешко уочити разлику, а да би се то учинило мора се прочитати ознака карактера у типу кода којим је писан, а то захтева много времена и додатних програма, што је просечном кориснику, у принципу, веома велико трошење времена. Наравно, то отвара неслућене могућности злоупотребе, нарочито у светлу увођења фонетски различитих домена нпр. на ћириличном писму што је код нас сегмент планова eCEE агенде и eCEE агенде плус.

Већина фарминг напада користи облике УРЛ енкодирања као хомографске или хомоглифских напада, али и примењују заменице (колоквијално „дивље карте“ – (wild cards) карактере, који се у DOS – у користе као помоћни карактери за претраге) ? или * који мењају једно или више слова.

Који су облици заштите од оваквих мера криминалаца? Комбинација ефективног ватреног зида и неког антивирусног софтвера више није добитна. Неопходно је укључити што је више могуће средстава и уложити велику количину пажње у ономе шта се на Интернету ради, уз свакодневно ажурирање свих софтвера који се користе на Интернету (браузери, ИМ месинџери, ИРЦ клијенти и сл.). Као највреднији од свих резултата оперативних активности у расветљавању ових дела у борби са фишингом према резултатима емпиријског истраживања је: 37,5% порекло фишер поште, док се у делфи верзији анкете за овај одговор определило 45.45% испитаника, затим модус операнди стварања и дистрибуције поште 18,75% а у делфи верзији њих 27.27%. Највише испитаника у основној верзији анкете одредило је ХУМИНТ рад после напада као највреднији од свих оперативних изазова у смислу резултата који са собом може донети – њих 50% а у делфи њих18,18%.

Фишинг и фарминг напади долазе из различитих делова света, а према следећим табелама слободно можемо оценити да управо из најразвијенијих држава долази највећи део. Такође, одредиште превара је значајно везано за описане земље.

Веома је интересантно размотрити регионалну дистрибуцију по земљама света према држави домаћину сервера са којих потичу фишинг поруке, као и проучити дистрибуцију оригинарних локација фишинг превара – према

---

[209] Неки помињу и cybersquatting. Код истог реч је о креирању сајтова који имају сличне називе са популарним значајно посећиваним сајтовима банака или финансијских организација (нпр. www.kombank.com.sr). Постоје и други различити облици, као нпр. скраћени УРЛ трећих лица, прикривање и фалсификовање имена хоста.

националности извршилаца али и према крајњој дестинацији средстава прибављених преварама ове врсте. Геолоцирање фишинг хостова[210]:

Држава	Април	Март	Промена у % поена
САД	51%	50%	+1
Немачка	6%	7%	-1
Јужна Кореја	4%	4%	Без промене
Велика Британија	4%	4%	Без промене
Француска	3%	3%	Без промене (Бп)
Русија	3%	2%	+1
Кина	2%	2%	Бп
Холандија	2%	2%	Бп
Бразил	2%	Није било података	Бп

Геолоцирање фишинг превара[211]

Држава	Април	Март	Промена у % поена
САД	52%	51%	+1
Канада	6%	7%	-1
Немачка	5%	5%	Без промене
Јужна Кореја	5%	4%	+1
Велика Британија	3%	3%	Без промене
Бразил	3%	3%	Бп
Холандија	2%	Није било података	Бп
Русија	2%	3%	-1
Аустралија	1%	Није било података	Бп

У 2011.год. слика је мало другачија[212]:

САД	46.3%
ВБ	31.0%
Аустралија	5.1%
Немачка	2.1%

210 http://www.symantec.com/business/theme.jsp?themeid=state_of_spam доступан 30.05.2010.год.

211 *Ibid.*

212 http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_08-2011.en-us.pdf последњи пут приступљено 14.09.2011.

Канада	1.6%
Холандија	1.4%
Хонг Конг	1.3%
Јужна Африка	0.8%
Сингапур	0.8%
Индија	0.7%

Наше истраживање указало је да стручњаци у датој области (представници банака, полиције и приватног сектора) сматрају - њих 50% да је фишинг опаснији од осталих облика, друга половина испитаника сматрају га мање или исто опасним, као и друге облике ВТК.

4.2.7 Крађа идентитета

Према одређеним ауторима[213] ова дела комбинују карактеристике више помињаних облика: фишинг представља радње предузете у сврху принуђивања или навођења жртве да ода личне или поверљиве податке фишеру, са друге стране крађа идентитета обухвата активност која подразумева прибављање, трансфер или злоупотребу података везаних за личност а које имају употребну вредност у финансијском смислу. Можемо препознати као прелазну фазу крађе идентитета радње фишинга, фарминга, вишинга и, евентуално, СМишинга.

4.2.8 Дефинисање крађе идентитета

Крађа идентитета обухвата[214] такво кривично дело код којег се неко лице лажно представља (као друго лице – са идентификационим подацима тог другог лица) у намери прибављања противправне имовинске користи или друге личне користи. Жртва или пасивни субјект овог дела може бити физичко али и правно лице, као што и извршилац може бити појединац или више лица, која су делови организоване групе. Неретко се крађа идентитета користи као секундарно кривично дело како би се извршило примарно, појављује се као средство којим се врши главно дело, како би извршилац сакрио свој траг или га заметнуо. Примери за ово су преваре са кредитним картицама или у подношењу лажних докумената за добијање кредита на име лица чији је идентитет украден.

---

213 Newman, G. R. McNally, M. M. Identity theft literature review, доступан на Интернету дана 12.01.2010.год. http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf стр.1.

214 Teri Bidwell: *Hack Proofing Your Identity in the Information Age* Syngress Publishing, Inc, 2002. стр.3.

Шјолберг[215] наводи да се у основи под крађом идентитета сматра злоупотреба личних података другог лица са намером вршења преваре. У истом документу он наводи да се у новом законодавству Краљевине Норвешке (у Казненом Законику из 2009. год.) избегава термин крађа користећи супституциони термин „злоупотреба идентитета“. Овај Законик у чл. 202. наводи да дело постоји оно лице које неовлашћено држи средства идентификације другог лица или дететом другог лица или користи идентитет који се лако може заменити са другом особом у циљу:

прибављања противправне имовинске користи себи или другоме или

наношења штете или срамоте (или нелагодности) другом лицу.

Према закону о крађи идентитета (Identity Theft Assumption and Deterrence Act (the Identity Theft Act; U.S. Public Law 105-318) као иста се сматра: „сваки акт лица које свесно трансферује или неовлашћено користи, било које име или број, који се може користити, самостално или у спрези са неком другом информацијом, како би идентификовао одређену особу, у намери да изврши, помогне у извршењу или наведе на, неку незакониту активност која представља кршење федералног закона, или представља кривично дело према неком закону државе чланице“.

Чл. 18. У.С.Ц. § 1028 (a) (7) дефинише крађу идентитета као: „свесно трансферисање, поседовање или коришћење идентификационих средстава друге особе (другог лица) у намери вршења или помагања или подстрекавања на вршење или другој вези са незаконитим активностима којима се стичу околности за извршење неког кривичног дела прописаног федералним законом или законима држава САД“[216].

Овиме се описаним нормама покрива шири спектар активности везаних са средствима идентификовања.

Друга дефиниција коју даје Федерална трговинска комисија САД 15. У.С.Ц. § 1681a (q) (3) означава крађом идентитета: „коришћење идентификационе информације другог лица“. Основна разлика је: да ли се мисли на превару и да ли се дело везује, у својој основи, за превару. Управо ово ограничава инкриминацију и домет у реалном животу када извршилац користи информације у друге сврхе а не преварне. Потоња инкриминација обухвата коришћење информација али не и њихово прибављање, чиме, рецимо, фишинг и фарминг отпадају из примене ове норме.

Због начина на који функционише, овај Интернет сервис постао је погодан „амбијент“ за крађу и злоупотребу идентитета. Крађа идентитета почиње са присвајањем личних података о неком лицу, без пристанка и знања тог лица, путем обмањивања, крађе или преваре. Крађа идентитета наставља се употребом прикупљених података за извршење кривичних дела која су у највећем броју случајева везана за стицање противправне имовинске користи лицима која

---

[215] Материјал за 12 Конгрес УН у вези превенције криминала и кривичног правосуђа одржан у Бразилу 12-19.04.2010., на стр.6.

[216] Наведено према: Internet related Identity theft, a discussion paper, prepared by Gercke, M. као део Project Cybercrime, Council of Europe, ECD, Directorate General of Human Rights and Legal Affairs. Доступно на Интернету: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp дана 20.03.2010.год.

злоупотребљавају украдени идентитет[217]. Ове погодности и, веома често, користе педофили како би преузимали идентитет других лица и представљали се у њихово име ради анонимне комуникацији са децом. Према ОЕБС – овом документу са министарског састанка у Сеулу јуна 2008. год.[218] један од закључака био је да се, услед нејединствене дефиниције крађе идентитета, овај облик криминалне активности веома брзо и несметано развија и узима маха. Управо у овом документу покушало се са дефинисањем и то на следећи начин: „**крађа идентитета** постоји онда када једно лице прибавља, поседује или користи личне информације о физичком или правном лицу, на недозвољен начин, у намери да изврши превару или друго кривично дело или учини нешто друго у вези са тим кривичним делима“[219]. Каже се да извршиоци на располагању имају и користе веома широк спектар средстава за вршење крађа идентитета.

Прља и Рељановић се баве питањем одређивања појма крађе идентитета. Они у свом раду говоре о крађи лика и идентитета и други видовима (не)законитог понашања[220]. Они у свом раду одређују крађу идентитета као: “ преузимање “улоге” неког лица на Интернету, редовно у циљу стицања неке материјалне или друге користи“[221]. Категоризују га и као: најдрастичнији атак на приватност личности, јер се учинилац, након што је преваром или на други начин дошао до виталних података за преузимање нечијег идентитета (интернет и друге шифре, бројеви платних картица, и сл.) представља у његово име, закључује послове или остварује друштвене контакте, исправно примећујући и да тако може вршити кривична дела на овај начин, прикривен иза туђег идентитета. Пружајући и сопствену дефиницију по којој: крађа идентитета претпоставља претходно извршење неког другог кривичног дела (преваре, упада у туђи рачунар или рачунарски систем, постављање вируса или другог штетног софтвера). Ови аутори веома коректно примећују да постоје и други начини упада у приватан живот људи, које они карактеришу као “мање или више кажњиве”[222]:

• Коришћење туђих (јавних) података. Овде није реч о преузимању идентитета неке особе ради остваривања користи, већ о једноставном коришћењу јавно доступних података ради стварања фиктивног лица које се појављује на интернету, нпр. на форумима, социјалним сајтовима, сајтовима за четовање и упознавање, и сл. Ова активност се своди на размену туђих слика, резимеа, ставова, које је особа пронашла на интернету, како би се лакше упознала са неком трећом особом или остварила циљ социјализације на неки други начин. Иако се свакако

---

[217] Милошевић М., Урошевић В.: Крађа идентитета злоупотребом информационих технологија, Безбедност у постмодерном амбијенту, Зборник радова књига VI, Центар за стратешка истраживања националне безбедности, Београд, 2009, стр. 53-64.

[218] OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, може се пронаћи на сајту OECD. Материјал припремљен за 72. састанак овог тела.

[219] Furnell, S.M. Problem of categorising cybercrime and cybercriminals 2nd Australian Information Warfare and Security conference 2001.str.3.

[220] Прља, Д. Рељановић, М. *Високотехнолошки криминал – упоредна искуства, у* Страни Правни живот, бр.3/09, стр.161-184. Београд, на стр.169.

[221] *Ibid.*

[222] Неки од њих су заиста инкриминисани; о некима закони ћуте и као такви представљају само морално неприхватљиво понашање

може окарактерисати као неморална, ова врста активности (за сада) није кажњива нити у једној држави – осим уколико се не ради о силоватељу или педофилу, који на тај начин покушава да пронађе своју жртву, али је и тада реч о другим кривичним делима а коришћење туђих података се јавља само као једно од претходних средстава припреме за извршење.

• Коришћење електронских података о активности лица. Закони о заштити података о личности, који су стандард у правним системима развијених земаља, јасно одређују како одређени подаци до којих дођу различите институције, органи и други субјекти, могу бити употребљени. Међутим, као и код следећег примера уступања података о електронским адресама, могућа је злоупотреба прикупљених података о једном лицу. Коришћењем платне картице као средства плаћања, може се нпр. јасно видети шта је једна особа купила, у које време и на ком месту. Ако неко редовно купује одређену врсту производа, или користи неке услуге, може се (непријатно) изненадити – на његову кућну адресу ће стићи рекламни материјал одговарајуће садржине. Ако нпр. редовно купује храну за мачке, добиће понуде за куповину хране за мачке, уз пратећи асортиман других производа за животиње. Ако редовно резервише карте за позориште путем интернета, може добити понуду за колекцију кућних ДВД-ова сличне садржине, итд. Иако делује безазлено, можда чак и као безопасан маркетиншки трик, то заправо значи да су информације о плаћању те особе доступне некоме ко их даље "уступа" различитим компанијама. Треба се запитати: шта ће се десити ако подаци на овакав начин буду "цурели" и код других куповина, нпр. продаје он лајн аранжмана за летовање? Одговор је: онда ће неко ко зна Вашу кућну адресу знати и период када ће та кућа бити празна, док сте са породицом на летовању.

• "Продаја" е-маил адреса и спамовање. Постоји небројено програма чија је једина сврха слање што већег броја електронских порука, како на рачунаре (путем е-маил сервиса) тако на мобилне телефоне (путем смс сервиса). Ове поруке најчешће имају рекламни карактер, али понекад могу садржати и елементе преварних е-маил-ова (тзв. "Нигеријско писмо", и сл.) односно порука којима се отпочиње комуникација са лицем ради коначног циља извршења преваре. Заједнички назив за све ове поруке је "нежељена пошта" (енгл. спам). Друга страна спам-а јесте добијање нежељене поште зато што је неки од сајтова или других сервиса коме особа остави своју важећу е-маил адресу (приликом регистрације, или у неком сличном случају) уступа – бесплатно или за одређену накнаду – спискове тих адреса различитим компанијама, које затим шаљу огроман број (правих или лажних) реклама за најразличитије производе. Ту се заправо врши (незаконито) филтрирање – за разлику од аутоматског слања на адресе које можда нису активне или чак ни не постоје, овде се користе само постојеће, активне адресе и "обезбеђује" се пажња њиховог корисника. Иако је овакво "уступање" података сасвим сигурно кажњиво у већини земаља према прописима о заштити података о личности, практично је немогуће утврдити да ли је и на који начин неки од сајтова уступио нечију е-маил адресу. Против спам-а су могуће различите превентивне техничке мере – нпр. аутоматско филтрирање порука пре него што дођу до корисника или одбијање порука које долазе са одређених сервера који се користе у великој мери, или искључиво, за овакве активности. Аустралија је прва држава која је инкриминисала спам-овање. Ирска јој се недавно придружила, а обзиром на

трендове нарастања нежељене поште и на прогнозе да ће она у најскоријој будућности имати удео у укупном е-маил саобраћају преко 90%, што чини преко милијарду порука дневно[223], могуће је да ће и друге државе следити овај новозапочети тренд инкриминације.

• Коришћење опреме за надзор и обезбеђење. Опрема која је до пре неколико година била сувише софистицирана и скупа за општу употребу, масовном производњом је постала доступна великом кругу корисника. Иако не спада у оно што се обично подразумева "високом технологијом", њоме се може значајно умањити или чак и укинути право на приватност личности. Телевизијске куће свакодневно користе ове камере које су инсталиране на локацијама које су непознате пролазницима на улици. За разлику од саобраћајних камера, као и камера обезбеђења, које се фокусирају на један сегмент околине у којој се налазе, и које имају друштвено користан циљ и самим тим оправдање свог постојања, камере до којих се може доћи и преко многобројних интернет сајтова, као и оне које се користе у телевизијским програмима, омогућавају веће задирање у приватност људи него што имају корисну сврху. Наравно, особе на улици нису заштићене правом на приватност, али се могу запитати да ли је могуће да неко свакодневно прати њихово кретање путем ових јавних камера, као и да ли је могуће да снимци направљени овим камерама буду доступни практично сваком појединцу који за њих буде заинтересован. Чак и уколико овакви снимци не буду употребљени за вршење кривичних дела или других недозвољених радњи, чини се да преовладава мишљење да људи не желе да живе "у кући великог брата", у свету у коме сваког тренутка постоји могућност да буду снимљени и праћени. Један од проблематичних аспеката овакве ситуације се јасно показује и кроз контроверзни програм који је лансирала компанија Гоогле – Google Street View, који може показати слике из различитих улица већих градова широм света. Овај програм се заснива на реалним сликама улица „уживо", на којима се налазе људи, аутомобили и сл. Колико се дубоко на овај начин задире у право на приватност? Можда не најпрецизнији, али у сваком случају занимљив одговор може понудити госпођа из Велике Британије, која је покренула бракоразводну парницу након што је случајно на снимку једне од улица видела паркиран аутомобил свог мужа испред непознате куће, у време када је он наводно био на службеном путу[224].

Могуће је говорити о крађи идентификационих података – информација правних и физичких лица, али је могуће препознати и крађу виртуелних ликова – идентитета.

Многе земље чланице ОЕБС –а труде се да пруже потрошачима и обичним грађанима разне могућности за борбу против крађе идентитета. Шта више развијају се различита средства за то, од обука потрошача до размене информација, између приватног и јавног сектора, а, нарочито, у циљу гоњења учинилаца кривичних дела крађе идентитета. Ипак, ова сарадња је у многим државама чланицама ограничена. У том смислу, привредна друштва датих земаља схватила су значај и потребу за

---

[223] Извор: http://www.junk-o-meter.com/stats/index.php, 20.10.2009.

[224] Извор: Блиц онлине, Преко Гугла открила прељубу, http://www.blic.rs/zanimljivosti.php?id=86407, 20.10.2009. упоредити и са Прља, Д. Рељановић, М. *Високотехнолошки криминал – упоредна искуства, у* Страни Правни живот, бр.3/09, стр.161-184. Београд, на стр.170-172.

обезбеђивањем људског потенцијала и безбедносних стратегија, али се мора много више урадити на томе. Због тога је и наглашено у ОЕБС – овом документу[225] да се мора следити пример неколицине држава које су наметнуле обавезу прикупљачима података (као што су привредна друштва која се баве пружањем Интернет услуга (ИСП)) да објаве продоре и упаде у секторе идентитета и дела крађе идентитета, како оним грађанима и правним лицима која су жртве, тако и широј јавности. У многим државама ОЕБС –а се још разматра да ли је неопходно да се законом пропише ова активност или на други начин да се унесе у правни систем. Интересантно је да, у оквиру ЕУ, ИСП предузећа захтевају да, у оваквим случајевима, дејствују у име сопствених муштерија (уколико је њихова персонална информација злоупотребљена). Слично компанијама које издају кредитне картице, одговорност заштите се ограничено преноси на пружаоце услуга.

Анализа у оквирима ОЕБС –а довела је до постављања неколико постулата, који су есенцијални за борбу против крађе идентитета:

- Дефинисање – постоји неопходност постављања потпуне адекватне и свеобухватне дефиниције кривичног дела крађе идентитета Непостојање општеприхваћене дефиниције и инкриминације отежава међународну сарадњу у овој области, која је неопходност и императив, а не могућност.

- статус крађе идентитета у правним системима чланица ОЕБС специфичан је Већина није инкриминисала ово дело, ни као облик постојећих дела, нити као самостално дело.

- сарадња са приватним сектором мора бити приоритетна. Овај сектор има своје место у борби против криминалитета и државе чланице морају размотрити, поред пооштрења казнене политике, већег и значајнијег учешћа приватног сектора у овом смислу.

- стандарди у оквирима чланица ОЕБС морају бити јединствени и морају се поставити на националним нивоима у погледу правила за приватни сектор у вези захтева за безбедност података али и обавеза у случајевима упада и продора у такве безбедносне секторе, где се морају поставити правила по којима је приватни сектор обавезан да обавештава и државу и оштећена лица.

- статистика – везана за крађу идентитета (било да се она врши он лајн или оф лајн), у већини држава чланица ОЕБС не постоји, док се на другој страни у САД али и Великој Британији, томе придаје доста пажње, управо због могућности вођења квалитетне аналитичке делатности, ово се мора променити, мора се водити прецизна и тачна статистика и у то мора бити укључен и приватни сектор.

- мора се оформити и стратешки поставити метод пружања помоћи жртвама ових дела, морају се покренути програми заједничке помоћи жртвама, и у то се морају укључити сви релевантни субјекти

- у циљу испуњења претходно наведене помоћи законодавац мора дати адекватне правне лекове и друга правна средства жртвама крађе идентитета, како би повратили своја права, отуђена без њихове кривице на овај начин.

- сматра се да, у актуелном моменту, не постоји адекватна снага која би служила као средство одвраћања учинилаца кривичних дела (као облик превенције вршења кривичних дела) због недостатка средстава, људства и актуелних метода

---

[225] S.M. Furnell, *Op.cit.*. p.4.

рада, те се из тог разлога на развијању ових мора што пре и што преданије радити у свакој држави чланици.

- у том смислу се мора радити на проширивању знања, и образовања везаних за крађу идентитета који би покрили све значајније субјекте у борби против крађе идентитета – укључујући кориснике, потрошаче, владин сектор, привреду и индустрију.

Координација и кооперација је веома значајна, како у националним оквирима, тако и на међународном плану. Неопходно је централизовати у оквиру држава чланица одређене органе, који би преузели ову улогу на унутрашњем плану, а тиме, уједно, и спровели контролу и уједначили праксу на националном нивоу. Са друге стране, значајно је и остваривање даље сарадње са страним партнерима на истим нивоима, где постоје могућности истраживања сарадње у многим областима. Оне би могле обухватити: А. проширење и побољшање одвраћања од вршења делатности у циљу превенције. Б. Проширивање међународне сарадње и учешћа у кључним међународним институцијама и инструментима (што се показује и код нас скоријом ратификацијом Конвенције о ВТК) В. Побољшањем одговора на захтеве за помоћи у кривично правним стварима, Г. На други начин ојачати сарадњу са страним партнерима (на пример, на пољу образовања или обуке у ходу).

Многе државе у Европи су предузеле одређене кораке на пољу заштите својих потрошача од крађе идентитета. Ове мере подразумевају: кампање подизања свести потроша и корисника у погледу појаве крађе идентитета, иновирање или већ прихваћене измене легислативних оквира у пољу телекомуникација, високих технологија, као и заштите корисника. Такође, значајно је подржати развој партнерства у области јавни – приватни сектор, иницијативе производње везане за постављање на место техничких превенционих мера и одговора на претње.

Начини крађе идентитета могу бити различити, типолошки исти према начину, односно средству, прибављања информација могу бити електронски и физички.

- социјални инжењеринг, који се назива и претекстовање[226], је као што је поменуто, термин који се користи за велики број превара или преварних игара на срећу код којих се жртва вара кроз навођење на давање корисних приватних информација. Још један покушај објашњења овог појма је: оригинално скројени фишинг напади уз примену обмањујућих или лажних и прикривених електронских писама и исхакованих веб сајтова брендова банака електронских комерцијалиста (e-bay) и компанија кредитних картица (visa, master card, maestro, american express, itd) који су спроведени са циљем да се адресат наведе да ода идентификационе информације везане за неки од поменутих. Значајно је схватити социјални инжењеринг као методе преварних навођења жртава да буду доведене у ситуацију

[226] Према ОЕБС-у претекстовање је један од облика социјалног инжењеринга за прибављање осетљивих информација. На различитим нивоима претекстери контактирају финансијске институције или предузећа телефоније, лажно се представљајући, под маском легитмних корисника (или коминтената) и од ових захтевају податке тако злоупотребљених лица. Други облик претекстовања се састоји у коришћењу инсајдера у финансијским институција или путем преварног стварања фиктивних или стварних рачуна онлајн у име оштећеног корисника или коминтента. Видети у OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, може се проначи на сајту ОЕБС –а. Материјал припремљен за 72. састанак овог тела, p.16.

да одају, одређене, поверљиве податке особама, које нису позване да их сазнају. Претекстовање представља покушај погађања специфичног одговора на социјалну ситуацију коју је креирао одређени извршилац; на пример, неко вам даје лажну информацију у сврху прибављања забрањених или тајних података (службене или државне тајне) од вас. Ову лажну информацију можете примити кроз пошту, електронску пошту, или рачунарски чет програм, веб сајт, телефоном или чак лично од извршиоца. Пример је нигеријска 419 превара[227] електронском поштом, која се креира у намери откривања вашег броја банковног рачуна. У сваком случају од вас се тражи да одате податке и информације које уобичајено не би сте дали свакоме. У САД је 1999. год. усвојен Грејем Лич Блили (Gramm-Leach-Bliley Act)[228] закон којим се овакво понашање инкриминише и санкционише али само у погледу финансијских података[229]. У анализи ОЕБС –а[230] изнето је веровање да ове преваре нису тако честе у данашњем времену, са чим се не можемо сложити, пре можемо рећи да оне више нису тако успешне као што су некада биле, али њихов интензитет блендираним нападима није умањен. У нашем истраживању везу између фишинга и социјалног инжењеринга испитаници су видели као међусобно условљену – група од 50% испитаника, односно 77,78% испитаника у делфи верзији анкете. 31,25% испитаника сматра их независним друштвеним феноменима (11,11% у делфи), док их 18,75% посматра као два дела једног злочиначког подухвата исте криминалне групе.

- он лајн крађе, малопређашњи пример новчаника би се могао користити у објашњавању ове појаве – наиме, све оно што садржи један новчаник садржи и ваш персонални рачунар, све податке о одређеним финансијским трансакцијама, али и личне податке, па и одређене интимне податке, тако да се он може сматрати вашим личним новчаником без новца. Он садржи податке о корисничким именима, шифрама Интернет налога, али и свих других „тајних“ информација и података, шифара, бројеве електронских комерцијалних рачуна, и – мејл адреса (адреса електронске поште), рачунарских имена домена, ИП адреса. Описани тип крађа има два појавна облика, први представља напад на сервере који садрже личне информације или податке (као пример се могу навести сервери који омогућавају пружање услуга Интернет трговине или сервери државне управе). Поред крађе извршилац може остварити и друге врсте користи или штете нпр. изменом одређених података у бази датих сервера, као један пример, се наводи тинејџер – хакер, који је својој мајци услед свађе, изменио податке у полицијској евиденцији

---

[227] Позната и под називом нигеријско писмо, зато што није само електронска пошта та која је била угрожена овом преваром. Често преваранти нуде да поделе своје богатство са примаоцем, само ако им он незнатно помогне у остваривању преноса или повраћаја новца из неке забити. Ово се обично одређује као помоћ за неплаћене таксе, порезе, или сличне дажбине.

[228] http://www.ftc.gov/privacy/glbact/glbsub1.htm последњи пут приступљено 10.09.2011.год.

[229] Овим законом се дефинише лична идентификациона информација као било која информација, податак који се пружа финансијској институцији како би се прибавио производ или услуга од дате финансијске институције. Такође, дефинише и јавну свима доступну информацију као податак који је доступан у јавној федералној, државној или локалној евиденцији или било која друга информација за коју финансијска институција верује да је сме објавити.

[230] OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, може се пронаћи на сајту OECD. Материјал припремљен за 72. састанак овог тела, p.18.

возачких дозвола, где је у досијеу додао прекршаје који су довели до кажњавања. Други облик је преко директних напада на извор података који се шаљу на сервер, као и на податке који се памте на кућним рачунарима[231]. Поменути облик се спроводи пресретањем комуникација између корисника и његових контаката, наиме нападач скенира софтвер у употреби на рачунару – мети и проналази слабости, да би, вешто их користећи, дошао до најразличитијих података – броја кредитне или дебитне картице и пратећих ПИН – ова и сл. Описана ситуација се може догодити онда када банке шаљу изводе са рачуна или платних и кредитних картица, што је сада веома чест случај код нас. Ово се може десити и посредно, када нападач прави замку за кориснике који на Интернету „скидају" одређене програме и којима се уносе одређени злоћудни програми, познати под називом тројански коњи - тројанци. Овако се могу унети тројанци, који прате и памте шифре које корисник примењује у свакодневном раду, они се могу појавити и у облику стеганографских порука[232] прикривених злоћудних програма у облику слике (имиџа енг. *image*) може се догодити и да у електронској поруци постоји злоћудни линк који корисник кликне и учита злоћудни програм.

- ерозија приватности огледа се у различитим облицима шпијунаже Интернет активности корисника рачунара. Каже се да постоје легитимни случајеви шпијунирања овог типа, када је у питању родитељски надзор комуникација малолетника како не би посећивао порно сајтове али већина других случајева је нелегално и нелегитимно надзирање Интернет комуникација и обично се ови случајеви дешавају у сивој (несанкционисаној) зони. Један облик је шпијунирање активности запослених од стране послодавца, наспрам права приватности запослених и на послу[233]. Други облик је случај адвертајзинга – рекламирања када могули ове индустрије користе различите електронске методе за праћење навика потрошача приликом сурфовања Интернетом наспрам њихових легитимних захтева за приватношћу и анонимношћу. Посебно интересантан је социјални претраживач (као на пример, Yahoo! People Search (http://people.yahoo.com) или us search.com (www.ussearch.com)) или социјалне мреже (као нпр. Twitter.com ili facebook.com), где се могу пратити и навике и склоности лица, као и прибавити најразличитије информације о особи. Оваква пролиферација информација на Интернету је омогућила веома велике злоупотребе личних података о особама а што извршиоци једва чекају.

Која све то средства могу носити податке значајне за крађу идентитета:

---

231 Између осталог већ пријем различитих колачића, (cookies) као мајушних помоћних програмчића за преузимање података на Интернету омогућавају примену најразличитијих програмских пакета за снифовање или надзор над прометом података који долазе или одлазе са вашег целуларног (мобилног) телефона.

232 Најновији случај везан је за откривени круг руских шпијуна у САД који су комуницирали преко стеганографских техника и чија је комуникација била заштићена двадесетседмокарактерном шифром користећи ad hoc WiFi мреже. Приликом рачунарског претресања у Њу Џерсију пронађено је преко 100 текстуалних датотека (порука) у оквиру једне фотографије. Интересантно је да је шифра пронађена записана на парчету папира приликом претресања стана једног од 11 чланова групе. доступно на http://www.theregister.co.uk/2010/06/29/spy_ring_tech/ последњи пут приступљено 01.07.2010.

233 О оваквим случајевима већ се оглашавао и Суд за људска права у Стразбуру. Погледати одлуку

- информације о рачунима за трговце који похрањују ваше личне податке
- податке и информације о рачунима које похрањујете он лајн
- подаци о изводима из кредитног бироа о кредитној способности лица
- информације о корисничком налогу за приступ Интернету
- бројеви мобилног телефона или контактне листе запамћене на телефону
- он лајн поруке и четовање са лицима о којима не постоји потпуна информација о томе ко су
- он лајн куповина и потврде о куповини примљене и послате мејлом или похрањене на рачунару
- нешифроване информације послате Интернетом
- нешифровани фајлови (датотеке) похрањене у ПДА уређајима
- колачићи са веб сајтова
- услуге Интернет сајтова које захтевају од вас више информација него што је потребно

Овој подели у ОЕБС –у додају и скиминг[234] који подразумева меморисање (крађом, колоквијално: „скидање“) информација са магнетних трака платних (дебитних) и кредитних картица; овакви подаци се онда преносе на другу локацију где се рекодирају ради прављења фалсификованих картица.

Крађе идентитета на основу прибављених информација о личности могу се остварити на различите начине, најчешћи у 2007. год.[235] били су у оквиру три главне категорије: креирање нових рачуна (кредитних картица, текућих банковних рачуна, подизање кредита), злоупотреба постојећих рачуна (на којима нису издате кредитне и платне картице) и злоупотреба постојећих уз коришћење дебитних и кредитних картица. Могуће је вршити и класична кривична дела прибављањем оваквих података, па тако могу се креирати фалсификоване картице а могу се и злоупотребити подаци постојећих[236].

Најчешће пријављивани су: преваре са кредитним картицама (61%), крађе и преваре са текућих или штедних рачуна (33%); преваре у вези рачуна са телефонским услугама (11%); преваре у вези плаћања преко Интернета (5%), и мејл и других електронских рачуна (4%), Медицинског осигурања (3%) и остало (1%). У последње време дошло је до пораста некласичних кривичних дела која се врше помоћу извршења крађе идентитета – терористички акти, акти којима се омогућавају или прикрива трговина људима и илегалне миграције[237]. Али највећи пораст бележе дела за која крађа идентитета представља претходно дело у сврху прања новца, финансирања тероризма и друга дела организованог криминала.

---

234 OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, налази се на сајту ОЕБС. Материјал припремљен за 72. састанак овог тела, p.16.

235 www.ftc.gov/opa/2006/12/fyi0688.htm dostupan 06.05.2010.

236 Видећемо да се наш законодавац у чл.225. КЗ дефинитивно новим изменама определио за инкриминацију и података који се могу злоупотребити.

237 http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%284CA02151F94FFB778ADAEC2E6EA865329~ID+Theft+Booklet+-+Protecting+your+Identity.PDF/$file/ID+Theft+Booklet+-+Protecting+your+Identity.PDF доступан 06.05.2010.год.

4.2.9 Карактеристике крађе идентитета

У оквирима ОЕБС, већина чланица не препознаје крађу идентитета као посебно кривично дело, многе га разматрају као могуће будуће кривично дело. Наиме, комплексност активности које га чине, може бити један проблем, ово дело представља забрањено дело са вишеструким последицама, оно се врши различитим комплексним радњама, које отварају врата различитим правним категоризацијама концепта дефинисања овог дела. Неке државе га квалификују као посебно кривично дело, као грађански деликт или као припремну радњу за вршење других, тежих, кривичних дела као нпр. превара, крађа, терористичких аката или прања новца. Веома мали број држава чланица ОЕБС инкриминисала је ово дело, све остале га сматрају конститутивним елементом опште опасних радњи, и сматра се да је ово дело покривено широком лепезом правила која укључују неовлашћен приступ подацима, преваре, кривоклетства, фалсификовања, кршења ауторских права и др. Чињеница је да кривична дела крађе идентитета, често, бивају средства за вршење тежих кривичних дела и, у овим случајевима, она бивају конзумирана или, на други начин (па, чак, и другим облицима привидног идеалног стицаја), укључена у таква дела. Но, то не значи да би ова кривична дела, због тога, требало искључити из правног поретка. Управо због транзиције традиционалних форми крађе идентитета на електронско тржиште поставља се питање довољности легислативних оквира чланица ОЕБС – а за супротстављање овом облику криминала. Овде можемо дати преглед стања у области кривично правних категоризација крађе идентитета:

САД дефинишу крађу идентитета као посебно кривично дело, то чине федералним али и многим законима држава чланица федерације. По прописима САД она се постоји када неко: „свесно трансферише, поседује, користи без пристанка или овлашћења, средства за доказивање идентитета друге особе (лица), у намери да изврши, или у вези извршења, неке нелегалне активности, која представља кршење федералног прописа, или која представља дело прописано позитивним прописима државе чланице или локалне самоуправе“[238]. Од 2004. год. доношењем закона о повећању казни за крађу идентитета прописане су теже казне за основни облик, и прописани су тежи облици овог дела. Као један од значајних напредака наводи се да је Јединица за борбу против крађе идентитета прва на фронту у супротстављању овом облику криминала, као и да њени напори иду у правцима пружања подршке и помоћи свим државама у свету. Овде је веома значајно схватити концепт по којем је ово кривично дело веома комплексно са радњама и последицама, које могу превазилазити границе многих држава, чак са глобалним импликацијама, при чему се могу појавити проблеми неинкриминације овог дела у различитим правним системима али и немогућности сарадње између различитих држава у кривичним стварима. Управо из овог разлога се Јединица у САД појављује на челу групација које се супротстављају овој пошасти.

У Великој Британији крађа идентитета није сматрана кривичним делом све до 2007. год. када је UK Fraud Act 2006 инкриминисао превару, обухватајући и превару извршену „он лајн“. По овом акту превара се може извршити на три

[238] United States Code (U.S.C.), Title 18, Section 1028 (a) (7).

начина: 1. лажним представљањем, приказивањем чињеница, (перфидно у циљу остваривања имовинске користи, изазивања и наношења штете другоме), 2. путем намерног неизношења и прикривања чињеница и 3. злоупотребом положаја и односа подређености или зависности. Овај акт је тада увео у инкриминације радње као што су „несавесно прибављање услуга... уколико су плаћене" као на пример, превара кредитним или платним картицама преко Интернета; поседовање предмета и ствари са намером употребе у преварама (овде се под стварима или артиклима подразумевају програми или подаци у електронској форми); које се односе на крађу идентитета; или радње прибављања или креирања предмета и ствари за примену (или који се намеравају употребити) у вршењу превара, које се односе на стварање или прибављање злоћудних програма.

У Аустралији није самостално кривично дело, осим у Квинсленду[239] и Јужној Аустралији[240]. Ипак, стратешки и тактички у Аустралији се почело са борбом против пошасти крађе идентитета, од тренутка када је она одређена као један од приоритета Владе 2000. год. и васпостављањем резултата извештаја „цифара у ходу" (као приоритетних аката који се имају извршавати што пре) комитета парламента за економију, финансије и јавне администрације. Најзад 2004. год. Аустралијски комитет Јавног (Државног) Тужиоца[241] постигао је сагласност у покушајима за развој инкриминације кривичних дела која би обухватила крађу идентитета. Шта више, за ово је припремљен и материјал који је одобрен од стране истог и прослеђен надлежнима за укључивање у правни систем.

Канада је крајем 2007. год. увела крађу идентитета као посебан облик кривичног дела. Као разлог наведена је околност да постојећи кривични закон не покрива све елементе овог кривичног дела, наиме злоупотреба туђег идентитета је покривена законом кроз фалсификовање или лажно представљање али припремне радње за крађу идентитета, као што су прикупљање, поседовање и промет података за идентификацију не могу бити покривене постојећим кривичним делима, из тог разлога уведена су нова дела, од којих последњих три облика у марту 2009. Смисао инкриминације ових кривичних дела је попуњавање празнина у кривичном закону и потпуно покривање свих кривичних дела, која нису, силом прилика, могла бити обухваћена праћењем савремених трендова у криминалитету. За сва новопрописана кривична дела предвиђена је као максимална казна од пет година затвора.

Француска као чланица ЕУ је чинила напоре да у свој правни систем уведе кривично дело крађе идентитета, влада је 2005. год. поднела предлог закона Сенату (горњем дому француског парламента) да би у октобру 2006. год. Француски Министар правде повукао овај предлог уз образложење да је овај облик кривичног дела ипак адекватно покривен другим прописаним кривичним делима те да не постоји потреба за инкриминацијом новог облика.

Као интересантно објашњење за инкриминацију крађе идентитета Великој Британији је дала Служба за избегавање превара са кредитним картицама (UK Credit Industry Fraud Avoidance Service (CIFAS)) по којем „извршиоци добијају

---

[239] Queensland Criminal Code and Civil Liability Amendment Act 2007. Ступио на снагу у марту 2007.

[240] South Australia Criminal Law Consolidation ("Identity Theft") Amendment Act 2003. Ступио на снагу 2004, у септембру.

[241] Australian Standing Committee of Attorneys General (SCAG)

изванредну прилику да остваре већу добит а, нарочито, у случајевима када знају да их полиција највероватније неће гонити“[242]. У истом акту ове организације разматра се неколико иницијатива и смерница за боље разумевање природе овог дела, од интензивирања полицијских активности на расветљавању овог дела до пружања помоћи жртвама и признавања тог статуса, како би им се могла омогућити реституцију права и санирати повреде права које су том приликом учињене.

Препоруке за чланице ОЕБС су да се прихвати вишезначни приступ који укључује, на пример, легислативу у погледу обавештавања оштећених и јавних служби у погледу продора у секторе безбедности података (нарочито у погледу личних информација о идентитету), као и јавно – приватних иницијатива за адекватно решавање проблема крађе идентитета.

4.2.10 Основни елементи кривичног дела крађе идентитета

Прво је неопходно разјаснити концепт идентитета и личне (персоналне) информације. У савременом свету актуелне околности (доступност електронских и других високотехнолошких средстава) омогућавају веома брзу размену информација и комуникације, које се могу веома лако злоупотребити. Таква доступност, лакоћа коришћења олакшава и злоупотребу у најразличитијим димензијама. Компоненте идентификације лица се обично деле на правне, физичке и фактичке. У савременим околностима ове компоненте је веома лако отуђити, а начин на које оне функционишу на различитим медијима је веома различит, и круцијално је на њима одредити адекватна средства заштите. Ове идентификационе компоненте су, генерално, базиране на фиксираним и потврдивим атрибутима, који се најчешће званично воде у евиденцијама државних органа (садржане у документима као што су личне карте, пасоши, здравствене књижице, возачке дозволе, изводи из матичних књига итд.). Они су: име презиме (правне карактеристике), име родитеља, девојачко (или претходно) презиме родитеља, датум и место рођења (фактичке), јединствени матични број грађана, пол, висина тежина, код (формула) папиларних линија прстију или длана, физички опис (физичке карактеристике) итд. Поред ових, лица могу у правним односима са другим физичким и правним лицима добити и друге карактеристике, као што су (што је актуелно у свету високе технологије) корисничко име и шифра за приступ Интернету, такође и за приступ одређеном веб банкинг рачуну, евентуални ПИН (Персонални Идентификациони Број, eng. *Personal Identification Number*) број за такав рачун, веб страници, електронску пошту, или чак могу се идентификовати приликом приступа Интернету преко бројева Интернет протокола (путем којих сваки рачунар, или други уређај, посебно приступа Интернету) или чак МАК (MAC – Media access control) адреса.

У Јужној Кореји се покушало са отежавањем крађе информација о идентитету 2006. год. кроз побољшани систем идентификације корисника он лајн,

[242] OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, доступан на сајту ОЕБС. Материјал припремљен за 72. састанак овог тела, p.14.

који би повећао безбедност верификације корисника у сајбер простору. Број који се до тада користио је сличан нашем ЈМБГ, имао је тринаест цифара и садржао је податке о личним карактеристикама носиоца (датум рођења и сличне информације), и био је веома тешко измењив, а такође и подложан крађи и другим злоупотребама[243]. Он је замењен променљивим и рачунарски генерисаним бројем за идентификацију, што је у многоме олакшало верификације и идентификације корисника. Но, овај приступ носи са собом могућност случајних погађања броја.

Код одређивања простора за инкриминацију крађе идентитета неопходно је препознати неколико сегмената самог акта који се може дефинисати као преварно прибављање и коришћење идентификационих обележја (идентитета) другог лица[244]. Ово кривично дело се може извршити, како физичким методама или путем, без примене техничких и технолошких средстава, тако и помоћу свеприсутних Интернета, техничких и технолошких средстава и метода. Посебно, Интернет као медијум пружа невероватне могућности за вршење дела крађе идентитета, где су досадашњи случајеви приказали веома широк дијапазон коришћених метода и средстава од аутоматизованих напада, са једне стране, до комбинованих метода и средстава, која су сва усмерена на најслабије тачке жртве ка којој је напад усмерен (то могу бити корисник Интернета или његов рачунар – уређај). Оваква ситуација поставља велики број проблема и тешкоћа пред органе гоњења, како у смислу дигиталних форензичких техника, тако и оперативних и истражних техника и метода. Примери који се могу разложити у фазе напада се своде на:

- Извршилац убеђује (обично методама социјалног инжењеринга) жртву да открије поверљиве податке на одређеном сајту и користи их у криминалне сврхе.
- Извршилац прибавља податке о кредитним или дебитним картицама од жртве, које потом користи за наручивање или прибављање робе и услуга
- Извршилац прибавља податке о корисничком имену и лозинци на Интернет налогу и имејл клијенту и користи их да шаље имејл (електронску пошту) са нелегалним садржајем.

Можемо препознати две групе разлога за доступност идентификационих обележја лица широј јавности.

У овом тренутку на Интернету постоји велики број сервиса који са собом носе конотацију социјалних мрежа, а посебно се може указати на неке можда и перфидније облике одавања информација, као на пример социјалне игрице као што су, на пример, Second life[245]. У свим описаним долази до лаког или потпуно несвесног одавања или цурења података, који се могу везати за личност и носити идентификациона обележја. Такође, овде се креира култура дигиталних идентитета[246] у коју корисник преноси део сопствених социјалних интеракција а које извршиоци крађе идентитета, веома квалитетно, умеју искористити. Веома је

---

243 *Ibid*. p.15.

244 Peeters, Identity theft scandal in U.S.:Oportunity to improve Data Protection, MMR 2007, 415.

245 http://secondlife.com/ доступан 01.09.2011.год.

246 Internet related ID theft, Counsel Of Europe, str.7.доступно на Интернет страници http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf дана 29.03.2010. год.

лако искористити простор за истраживање података о одређеном лицу, кроз унакрсно упоређивање података прибављених нпр. постајањем контактом у некој од социјалних мрежа датог лица, или у оквиру описане социјалне игре, са претраживањем кроз неке од специјализованих претраживача лица као на пример http://people.yahoo.com/ или http://www.intelius.com који имају посебне линкове и приступ базама података претходно описаних социјалних игара и мрежа. Ако на све ово додамо и физичке оперативне активности уз примене метода социјалног инжењеринга резултат је неизбежан, врло брзо.

Друга група разлога блиско је везана за процес трансфера ових информација Органи који располажу овим информацијама веома олако их објављују на Интернету, шта више, понегде и уз комбинацију са другим идентификујућим подацима. Мада такво објављивање, осим у потоњим случајевима, не може довести самостално до злоупотреба – значајно је да, уз остале податке, који се могу прибавити на најразличитије начине, се то може лако десити. Као што можемо приметити, извршиоци теже укрштању више различитих извора, за овакве податке, а тренутно стање у електронском пословању и дешавањима на Интернету показује тенденцију, која иде на руку овим извршиоцима.

Свему овоме погодује и немогућност стопроцентног идентификовања сопствених контаката од стране жртве, нарочито лица са којима није у сталном контакту, што, са собом, носи много ризика. Ово се може приметити на социјалним мрежама, али још је перфидније, код инстант месинџера, где и нема екстензивних социјалних профила особе. Конкретно један од аутора овог рада је у тренутку конфигурисања једног од ИМ ICQ[247], десет секунди након инсталације, добио понуду за пријатељство од потпуно непознатих особа, чиме би се омогућио увид у многе сегменте приватних података. Слична ситуација поновила се и код skype ВоИП –а.

Крађа идентитета има и међународну димензију. Обично извршиоци и жртве нису у истим државама, што са собом повлачи питања јурисдикција, примену принципа nullum crimen nulla poena sine lege, као и проблеме надлежности институција за сарадњу, уколико нема потписа на Конвенцији о ВТК (на пример Русија).

Аутоматизација напада је још један од проблема који се јавља у случајевима крађе идентитета. Један од најозлоглашенијих примера је СПАМ, који се користи у најразличитије сврхе, од прибављања података о активним електронским поштама, до директног имплементирања у методама социјалног инжењеринга или фишинга за конкретне крађе идентификационих података.

Савет Европе је 2007. год. покушао да припреми платформу за израду легислативе о крађи идентитета, на глобалном нивоу, која би имала униформну димензију, јер се увидело да не постоји уједначеност ни у земљама чланицама ЕУ па ни у СЕ. Пружена је неутрална дефиниција „крађа или преузимање постојећег идентитета (постојећих идентификационих обележја лица, или значајног дела истих) са или без пристанка лица чија су, и без обзира да ли је власник жив или преминуо“[248]. Поред ове, у анализи су приказане и дефиниције које се фокусирају

[247] Исто се десило и са ИМ mail.ru

[248] Internet related ID theft, Counsel Of Europe, p.7. доступно на Интернет страници http://www.coe.int/t/dghl/coopera tion/economiccrime/cybercrime/Documents/Reports-

на чињеницу да феномен крађе идентитета укључује одређену сврху прибављања података, као и постављање одређених услова приликом прибављања следећих аката (за разлику од прве која фокусира сам акт прибављања идентификационих обележја).

Главне потешкоће долазе услед неконзистентне примене термина, у САД се разликује крађа идентитета и превара са идентитетом, док се у Великој Британији више примењују идентитетска превара[249]. Неразликовање фишинга од крађе података, преузимања рачуна (налога), или отмице налога, такође, је присутно у различитим стручним расправама, што иде у прилог аргументу да се мора утврдити свеприхваћена дефиниција.

Значајно је проучити како се у САД дефинише крађа идентитета, па тако 18 U.S.C. § 1028.(a)(7)[250] под насловом превара и везане активности у вези са идентификационим документима, аутентификационим средствима и информацијама под крађом идентитета подразумева:

„свесно трансферисање, поседовање или коришћење, без законског овлашћења, средства за идентификацију другог лица у намери извршења, помагања или навођења на извршење, или у вези са делом, које представља дело кажњиво дело по федералном или закону државе чланице САД, као и локалним прописима“

Овим делом се покрива широк дијапазон радњи везаних за идентификациона средства.

Друга дефиниција је дата Федералне комисије за трговину у глави 15 поглављу 41 подпоглављу III § 1681a (q) (3): „термин крађа идентитета означава превару извршену коришћењем идентификационих информација другог лица, која се може ажурирати терминолошки од стране ФТЦ (Federal trade commision), другим прописом“. Главна разлика је што, овај потоњи акт, везује крађу идентитета за преварне активности, што ограничава примену норме у случајевима када извршилац користи идентификационе информације у циљу вршења других дела а не преваре. Ова норма покрива само употребу информације а не и активности у прибављању ових информација. ФТЦ је донела детаљнији опис дела, па се према томе под крађом идентитета подразумева (а) „покушана или учињена превара уз бесправно коришћење идентификационих информација другог лица“ и (б) појам идентификационих информација подразумева свако име или број који се могу самостално, или у комбинацији са другим информацијама, користити у идентификовању одређеног лица, укључујући ту и:

1. Име број социјалног осигурања (веома значајан број у САД који се користи у скоро свим идентификујућим поступцима), датум рођења, или број возачке дозволе или идентификациони број, регистарски или лични број странца, број пасоша, ПИБ (порески идентификациони број)

2. Јединствене биометријске податке, као на пример формулу дактилоскопског фиша, идентификациони аудио запис гласа, видео запис ретине или ириса, као и сваку другу јединствену физичку репрезентацију

Presentations/567%20port%20id-d-identity%20theft%20paper%2022 %20nov%2007.pdf дана 29.03.2010. год.

249 *Ibid.*

250 http://www.law.cornell.edu/uscode/18/1028.html доступан 29.03.2010.

3. Јединствен електронски идентификациони број, адреса или рутерска шифра.

4. Телекомуникационе идентифицирајуће информације или приступног уређаја

Као што се може видети и ова норма везује крађу идентитета за превару, с тим што обухвата и радњу неовлашћеног коришћења информација везаних за идентитет.

Као једну врсту рекапитулације можемо констатовати да се одређене дефиниције фокусирају на акт прибављања информације[251]. Уколико сматрамо да је постојеће законодавство релативно добро обухватило актуелним инкриминацијама и крађу идентитета, могуће је увођењем новог дела приказати теже облике или прецизније обухватити сва могућа дела и појавне облике. Са друге стране, посматрајући 18 УСЦ § 1028 (а) (7) можемо приметити значајно другачији приступ проблематици. На основу овог дела могуће је гонити извршиоца и у случајевима када он није прибавио информације везане за идентитет, нити их је употребио у нелегалне сврхе. Инкриминација изискује само неки облик интеракције са подацима, (обухватајући трансфер или поседовање или употребу) у намери да се изврши, подстакне или помогне извршење дела. Управо овакав приступ иде даље од многих инкриминација пружајући адекватно обухватање свих појавних облика овог дела.

У сваком случају могуће је препознати неколико фаза, са специфичним активностима и радњама извршилаца, у извршењу овог дела:

Фаза прибављања информација везаних за идентитет лица

Фаза поседовања или трансферисања информација везаних за идентитет (такозване интеракције)

Фаза употребе информација везаних за идентитет у криминалне сврхе.

Овакво разликовање фаза у оквиру извршења дела омогућава да сагледамо и могуће појавне облике дела као и да фокусирамо инкриминације на прецизно утврђене радње или акте. Наиме, могуће је замислити различите облике крађе идентитета а који међусобно немају никаквих заједничких елемената осим везе са неком од описаних фаза.

Герке[252] је спровео анализу три елемента најпопуларнијих облика крађе идентитета разликујући манифестационе облике у њима: метод коришћен при извршењу (modus operandi, MO), мете напада и мотивацију извршилаца. При анализи MO наводе се следећи облици: физички метод – крађа делова рачунара

---

[251] Уколико извршилац прибавља информације које нису везане за идентитет коришћењем електронских комуникционих средстава и мера норме које покривају шпијунске активности у прибављању података или неовлашћени (нелегални) приступ у глобалу могу обухватити овакво дело. Постоје генерално два приступа у инкриминацији овог дела у свету, први обухвата уски приступ инкриминишући само акте прибављања тајних података. Пример је УСЦ § 1831. Други обухвата шири приступ инкриминације обухватајући и радње прибављања података похрањених у рачунару, чак када исте не садрже економске класификоване и тајне податке. Пример за ову групу је претходна верзија § 202а Казненог Законика Немачке.

[252] Internet related ID theft, Council Of Europe, str.7. доступно на Интернет страници http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf дана 29.03.2010. год.

(физичко противправно одузимање носилаца података)[253] који носе идентификационе информације; претраживање ђубрета ("dumpster diving"), или физичка крађа поште; Интернет претраживачи[254] и коришћење система за дељење датотека (file sharing systems) – иако је већином овај облик крив за пиратерију, веома је актуелно његово коришћење и за прибављање података о личности; напади инсајдера – извршилаца изнутра, лица која су инфилтрирана у одређене фирме, као и лица која су из фирми отпуштена аутсајдери – извршиоци споља (па то раде из разлога освете или за новац) али у ову категорију спадају и хакери; на крају имамо и нападе у облику социјалног инжењеринга.

Уколико посматрамо који су то подаци предмет крађе идентитета можемо навести податке о идентификационим бројевима, као на пример бр. социјалног осигурања у САД, код нас су у питању матични бројеви (мада се у овом облику они код нас нису до сада одузимали), бр. личних карата, пасоша, возачких дозвола; датум рођења, адреса и бр. телефона, корисничка имена и шифре нефинансијских налога или рачуна, као и корисничка имена и шифре финансијских рачуна.

Значајно је размотрити и мотивацију која стоји иза оваквих кривичних дела. Она варира управо као и сами методи које користе извршиоци у вршењу ових дела. У одређеним случајевима ова дела су неопходан услов за вршење даљих кривичних дела друге врсте и типа (не фокусирајући се при томе на податке, већ на њихову употребљивост у даљим криминалним активностима). Други облик мотивације везан је за прибављање финансијске користи на основу продаје идентификационих информација и на крају трећи облик (у досадашњој пракси) мотивације везује се за прикривање правог идентитета, коришћењем ових идентификационих обележја у различитим облицима и случајевима.

У смислу покривености, према изложеним законским инкриминацијама можемо закључити да, обзиром на варирајуће појавне облике (и њихово свакодневно ажурирање и мењање) традиционални облици кривичних дела не могу у потпуности покрити свако дело ове врсте. Шта више, у великој већини традиционалних инкриминисаних случајева свесно учешће оштећеног у извршењу дела – откривању личних података, бива основ који онемогућава подвођење под одређену законску норму (услед тзв. пристанка оштећеног). Дакле, у овим случајевима инкриминација не покрива ова дела, а видећемо да је тако у огромном броју случајева фишинга.

Једини конзистентан елемент у свим случајевима крађе идентитета су фазе у извршењу. Уколико посматрамо претходно помињано, могуће је извући из тих фаза два заједничка елемента. Први је идентитет (идентификациона обележја или информације) и он се дефиницијом чл. 15. УСЦ 1681 (q)(3), одређује кроз идентификујуће информације, а за дело се не захтева да је злоупотребљен целокупан „идентитет" од стране извршиоца. Неке информације по својој природи не представљају део идентитета лица, не представљају део његове правне

---

253 Рецимо и то да је 2007.год. већина истраживања показала да је око 15% свих пробоја података бива резултат овог облика – физичке крађе.

254 Код ових облика значајно је поменути да су у питању незаконита коришћења претраживача за прибављање података филтрирањем кроз ове претраживаче о питањима рачунарске безбедности, али и мете крађе идентитета. Пример је проналажење несигурних система за заштиту шифара у циљу прибављања информација о овим системима.

личности, али, обзиром да могу бити препознате као идентификујуће, јер се путем истих може доћи до личних идентификационих и других личних података, морају се таквим третирати[255]. Други је тзв. „синтетички идентитет“[256] могу их извршиоци користити генерисањем (вештачким креирањем), а што је много лакше, у смислу дигиталних комуникација. Неопходно је препознати да је могуће искористити предности познавања информатичких технологија, како би се у оквирима све присутније, е – владе остварили услови за издавање докумената без постојања реалних идентификационих елемената или комбиновањем података о постојећем лицу и фиктивних података[257].

Појам крађе идентитета се користи веома палијативно и непрецизно, томе кумују и различите дефиниције различитих законодаваца у свету. Првенствено се користи као термин који означава крађу – радњу прибављања и употребе идентификационих обележја другог лица (дакле обухватајући поседовање – држање и коришћење). Овај термин се користи и за означавање кривичних дела извршених употребом туђег идентитета применом туђих идентификационих обележја. У пракси кривично правног регулисања при покривању све три поменуте фазе то изгледа овако: у првој фази радње прибављања информација везаних за идентитет. Ова дела се, на пример, могу извршити фишинг нападима или применом малициозних (злоћудних) програма.

Друга фаза се карактерише интеракцијом са идентификационим информацијама и подацима пре њиховог искоришћавања у делу. Пример је продаја оваквих информација на црном тржишту прибављених од стране трећег лица.

Трећа фаза представља употребу идентификационих информација и података у извршењу кривичног дела. Пример јесу фалсификовање идентификационих докумената, навођење на оверавање неистинитог садржаја, прибављање докумената на основу фиктивних података.

Актуелна законодавна решења обухватају два приступа: јединствену инкриминацију[258] која обухвата радње прибављања, поседовања и употребе идентификационих информација (обележја, података) у криминалне сврхе; и индивидуализације инкриминисањем типичних радњи[259] везаних за прибављање

---

255 Ово ће нарочито бити случај код земаља код којих је један идентификациони елемент кључан и користи се у свим идентификационим поступцима (бр. пасоша, ЈМБГ, број Социјалног осигурања и сл.). У ову групу спадамо и ми.

256 Internet related ID theft, Council Of Europe, p.19. *locus citatum.*

257 О стварању новог идентитета преко података прибављених са социјалних мрежа и социјалним инжењерингом, а на основу истог и издавању возачке дозволе за лице рођено 1788.год. у Аустралији погледати: http://www.sophos.com/blogs/duck/g/2009/12/14/facebook-privacy-video/ доступан 09.04. 2010.

258 Карактеристичан пример су 18 УСЦ § 1028 (а)(7) и 18 УСЦ 1028А(а)(1) – покрива све три фазе. Једини недостатак у оквиру прве фазе огледа се у инсистирању законодавца на чињеници да трансфер података иницира извршилац, па у том случају фишинг и социјални инжењеринг могу бити изван ове инкриминације. У другој фази државини (поседовању) инсистира се на намери извршиоца да касније користи у криминалне сврхе податке, дакле не покрива саму државину већ државину са намером. Ова дела не покривају припремне радње за извршење кривичног дела крађе идентитета.

259 Пример је Конвенција о ВТК ETS 185. Својим одредбама и предвиђањем инкриминација не покрива крађу идентитета, као ни сва могућа дела незаконите употребе и манипулације са идентификационим подацима. Видимо да у првој фази немамо потпуно покривање свих могућих

идентификационих обележја као и радњи везаних за поседовање и употребу таквих информација.

У већини случајева учиниоци који врше ове забрањене активности за циљ имају вршење других кривичних дела, као што су кредитне преваре, преварно прибављање готовог новца, услуга, права по основу рада, као и било шта друго од користи што се може искористити на уштрб жртве.

4.2.11 Облици заштите

Заштита нарочито осетљивих података о личности заснована на приступу типа ААА (3А), он подразумева три елемента. Прво А је овера (authentication) — поступак утврђивања идентитета оног ко жели да приступи подацима, који се у систему налазе, односно, провера тог идентитета. У ту сврху користе се најчешће три начина утврђивања аутентичности. Први начин утврђивања аутентичности заснива се на услову: имати. Услов за утврђивање аутентичности јесте поседовање неког легитимационог средства, знака, предмета или уређаја. Други начин се заснива на услову: знати. Аутентичност се утврђује коришћењем информације која је, по дефиницији, позната само кориснику и лицу, или елементу система, који врши провере аутентичности. То су шифре, лозинке или ПИН кôд који се користи приликом пријаве. Трећи се заснива на услову: бити. Аутентичност се утврђује на основу физичких својстава, или понашања, која се означавају као биометријске функције. Друго А је ауторизација — подразумева дефинисање корисника или група корисника, које имају право приступа информационом систему, односно његовим деловима, односно, ниво података о личности до којег могу приступити конкретни овлашћени корисници и шта са тим подацима могу да раде (увид, копирање, измене или неке друге врсте обраде). Треће А је праћење (accountability) и представља најважнији елемент. Он подразумева заштиту нарочито осетљивих података о личности, тако уређену и организовану, да је у сваком тренутку, накнадно, могуће утврдити када су поједини подаци коришћени или обрађивани и ко је то урадио.

радњи које би представљале крађу идентитета, на пример нема инкриминације шпијунаже (крађе података који су означени као поверљиви државна тајна или сл.). Постоји расправа о домашају чл.3. Конвенције у овом погледу, али она представља горући проблем. Такође и у другој фази имамо сличну ситуацију (чл.2-5. ЦЕТС 185.) нарочито је знчајно да ни једним чалном не покрива растуће црне берзе за трговину идентификационим подацима. У тећој фази инкриминисана је превара са кредитним картицама (уколико је онлајн онда иде примена чл.8.) али други облици кривичних дела која се могу извршити уз помоћ овако прибављених података нису покривена инкриминацијама ЦЕТС 185 (нарочито у случају вршења крађе идентитета у циљу употребе идентификационих података за прикривање идентитета и лажно представљање). Чл.2. Конвенције одређује „приступ“ по којем исти не зависи од конкретног облика комуникације чиме се у овакву инкриминацију могу укључити и нови облици комуникације нпр. WLAN.

ЦЕТС 18518 УСЦ § 1028 (а)(7)Инкриминација фаза 1-3Само инкриминише одређене акте у фазама не покрива у потпуности све могуће радњеИма шири приступ и инкриминише екстензивно радње у све три фазеРелевантне рупе у погледу крађе идентитета нарочито у фазама 2 и 3немаИнкриминација припремних радњиСамо одређене радње покривенеНе покриваПримењивост на дела која не укључује ВТКнеда

У основи можемо разликовати три нивоа праћења. Први омогућава накнадно утврђивање чињеница о томе ко је унео, ажурирао, променио, односно избрисао неки податак и када. Други ниво подразумева и праћење приступа подацима, дакле, бележи и то ко и када је одређеном податку само приступио (увид, упознавање), при том га немењајући. Коначно, трећи ниво подразумева потпуно праћење у коме се бележи све: ко и када је приступио или мењао податак, и какав је податак био и у шта је промењен. Трећи ниво је очигледно као најзахтевнији, најскупљи, што га у нашим условима не чини баш прихватљивим. Ипак, бар у неким ситуацијама има места и његовој примени[260].

У одређеним случајевима учиниоци не користе податке жртава да би вршили преваре, већ да би их продали другима, који ће их преварно користити. Оваква секундарна активност обухвата преварне радње али и креирање нових преварних форми (фалсификовање) јавних или службених исправа (на пример, извода из матичних књига, возачких дозвола или пасоша)[261].

4.2.12 Типологија крађе идентитета и стадијуми

Подела на глобалном нивоу крађе идентитета се може свести на: физичку крађу идентитета, виртуелну и кредитну (условно јер можемо говорити и о дебитној)[262].

Постоје аутори који сматрају да крађа идентитета представља подкатегорију идентитетских превара[263] а веома је значајно приметити да се преваре картицама јављају у већини комбинованих дела крађе идентитета. Наравно, полицијске снаге на локалном нивоу не дају приоритет у погледу хитрог поступања у случајевима крађе идентитета, а на томе, дефинитивно, треба радити, са друге стране кривица за финансијски губитак ипак је резултат непоступања од стране издавалаца картица а не корисника. Треће, није редак случај да се од стране саме жртве веома касно (или дуже време) не сазна о постојању кривичног дела и висини оштећења, због неажурности у погледу бриге о сопственим средствима, а што је значајан моменат за извршиоца али и органе гоњења. Наиме, једном извршена крађа идентитета може се надаље максимално експлоатисати, вршити даље злоупотребе, препродавати информације и сл.

Одређени аутори[264] дају следећу типологију крађе идентитета:

1. искоришћавање слабости и недостатака у одређеним технолошким решењима и информационим системима[265].

---

260 Више о овоме у: Шабић, Р. Ревија за безбедност, бр. 6/09, Заштита нарочито осетљивих података о личности — нека отворена питања, стр.3-7.

261 OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, može se pronaći na sajtu OECD. Материјал припремљен за 72. састанак овог тела, стр.15.

262 Moore, R. Search and seizure of digital evidence, LFB Scholarly publishing inc, NY 2005. Str.46

263 *Ibid.*

264 *Ibid.*

265 Најбољи пример су преваре са кредитним и дебитним картицама, које су или фалсификоване или украдене па тако извршилац користи податке (личне идентификационе

2. Финансијске преваре

У једном истраживању о он лајн анонимности, Форд и Армстронг[266] тврде да је највећа вероватноћа да ће се оне услуге Интернета које дају највећи ниво анонимности користити у криминалне сврхе. Откривено је да су шифровани имејл и ИРЦ чет, она средства која пружају више нивое анонимности, омиљени међу лицима која су умешани у он лајн активности педофилије и хакерисања, док употребу WWW и FTP протокола, који дају слабије нивое анонимности озбиљни криминалци избегавају. Најчешћи тип крађа идентитета у пракси јесу преваре са кредитним картицама, неки их одређују као крађа идентитета – у ужем смислу, јер је код овог типа само једном могуће украсти идентитет, зато што је дело извршењем свршено и не може се поновити, јер ће у следећем моменту бити откривено или, просто, неће моћи бити изводљиво у пракси.

Са друге стране одређени аутори препознају три стадијума (нивоа): Први: Прибављање идентитета путем: крађе, хакерским активностима, преваром, различитим муљкама и смицалицама, и обманама разне врсте, силом, преусмеравањем или пресретањем и отварањем туђе поште, па понекада и легалним и доступним средствима (на пример информацијама о купопродаји доступним на Интернету).

Други: Злоупотреба информација о истоветности (или идентитету) у циљу остваривања какве имовинске користи (која иначе представља најчешћи облик мотивације), али и у циљу избегавања лишења слободе али и евидентирања или регистровања од стране других државних органа и агенција (као, на пример, пореске управе). Овде се могу као даље радње предузети следеће активности: преузимање рачуна, отварање нових рачуна на име лица жртве крађе идентитета, екстензивна злоупотреба кредитних и дебитних картица на име жртве, продаја идентификационих података на црном тржишту, прибављање додатних података везаних за истоветност одређене личности (као, на пример, вађење додатних докумената, легалним путем, на име жртве, уз додавање сопствених физичких обележја – као на пример пасош, возачка дозвола итд.), преваре у вези осигурања, попуњавање захтева за повраћајем већих сума новца по основу пореских олакшица, крађе рентакар возила и многе друге.

Трећи стадијум: откривање да је дело извршено. Док се код различитих врста злоупотреба платних и других картица, релативно брзо, разоткрива извршење овог дела, крађа идентитета у себи садржи црту прикривености и тежи да се што касније открије, што се већ из ових стадијума може закључити. У питању је период од неколико месеци до неколико година, у зависности од манифестација последица овог дела. У сваком случају искуство казује да је временски ток пропорционалан штети коју ће жртва претрпети.

На пријављивање кривичних дела крађе идентитета негативно утичу три околности:

информације и поверљиве податке), друге уобичајене мете овог облика су електронске базе података које садрже поверљиве личне и финансијске податке о потрошачима (у питању су обично институције које издају платне и дебитне картице).

266 Forde, P. and Armstrong, H. 2002, 'The Utilisation of Internet Anonymity by Cyber Criminals', Paper presented at the International Network Conference, 16-18 July, Sherwell Conference Centre, University of Plymouth, Plymouth.

1. Тешкоће везане за дефинисање појма и бића овог кривичног дела, а нарочито везивање са другим облицима кривичних дела (тзв. споредним или помоћним кривичним делима, акцесорна дела). Већина полицијских управа у свету нема механизме, којима би одвојила ова дела од основне крађе идентитета. Ово је, нарочито, омогућено непостојањем обуке полиције у погледу препознавања и евидентирања информација везаних за дела општег криминалитета, која могу продуцирати крађу идентитета.

2. Вишејурсдикциони и међународни карактер крађе идентитета. Поред различитих надлежности у погледу носећих кривичних дела за ово кривично дело, веома често, су проблем и непостојање међународне сарадње и велика удаљеност места извршења кривичног дела и наступања последица.

3. У зависности од типа крађе идентитета дешаваће се да оштећени пријављују одређене типове дела неким другим органима и организацијама а не полицији (банкама и другим финансијским организацијама, осигуравајућим друштвима). Обзиром и да пријавом овим организацијама и привредним друштвима, такође, може отпочети истрага о делу, постоји довољно јасна мотивација и за припаднике полиције да не узимају пријаве, које би коректније преузеле стручне службе ових организација и брже предузеле адекватне акције[267].

Смисао истраживања овог кривичног дела је сагледавање његове опортунистичке структуре, а што захтева два значајна корака:

1. Разматрање сегмената радњи које ово дело садржи – од којих се састоји, пажљиво дефинисање специфичних аката како би се што конкретније проучило, и

2. Препознавање прилика новог окружења у информационом добу, које су извршиоцима омогућиле и које ће, у будућности, омогућавати извршење ових дела.

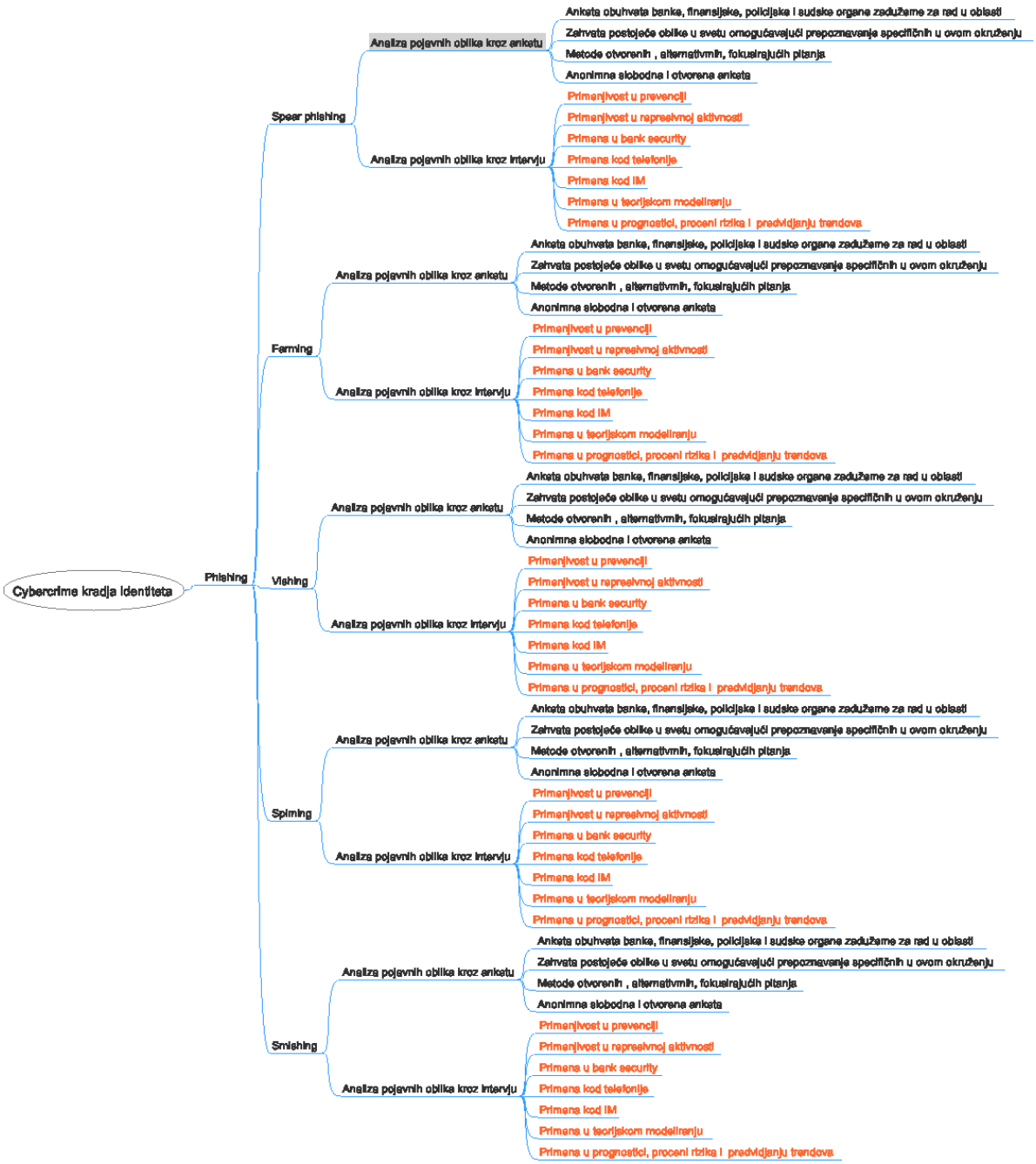
Препоручује се да се у будућности на основу истраживања, путем интервјуисања и анкета извршилаца и оперативаца класификују облици понашања и одлуке извршилаца при извршењу дела, што може представљати срж и основ развоја нових техника за супротстављање овим облицима криминалитета[268]. Наравно, овим путем се може доћи и до прогностичких елемената у погледу назирања будућих облика овог криминалитета (начина искоришћавања слабости система итд.).

На основу изнетог и резултата емпиријског истраживања можемо покушати да дамо следеће типологије у вези крађе идентитета и облика кривичних дела који се могу сматрати посебним облицима крађе идентитета. Исте су приказане на следећим дијаграмима.

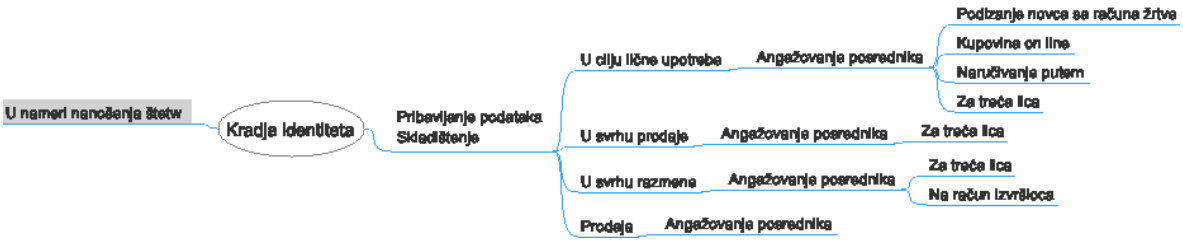
---

267 Newman, G. R. McNally M. M. Identity Theft Literature Review U.S. Department of Justice. 2005, Prepared for presentation and discussion at the National Institute of Justice Focus Group, p. VI уводног дела.

268 *Ibid.* VI-VII



Илустрација



Илустрација

4.3 Прање новца

Основни облик овог дела чини оно лице које изврши конверзију или пренос имовине, са знањем да та имовина потиче од кривичног дела, у намери да се прикрије или лажно прикаже незаконито порекло имовине, или прикрије или лажно прикаже чињенице о имовини са знањем да та имовина потиче од кривичног дела, или стекне, држи или користи имовину са знањем, у тренутку пријема, да та имовина потиче од кривичног дела, (затвор од шест месеци до пет година и новчана казна). Тежи облик постоји ако износ новца или имовине првог облика прелази милион и петсто хиљада динара (затвор од једне до десет година и новчана казна). Посебан облик постоји када неко учини претходне облике са имовином коју је сам прибавио извршењем кривичног дела, казниће се казнама прописаним за те облике. Најтежи облик чини онај ко прва два облика изврши у групи, (затвором од две до дванаест година и новчаном казном[269]. Још један посебан облик постоји када неко учини прва два облика, а могао је и био дужан да зна да новац или имовина представљају приход остварен кривичним делом (затвор до три године). Нарочит облик постоји када одговорно лице у правном лицу које учини прва два облика и други посебан, казниће се казном прописаном за то дело, ако је знало, односно могло и било дужно да зна да новац или имовина представљају приход остварен кривичним делом.

Веома је код доказивања овог дела значајно утврдити ниво и степен свести извршилаца о томе да имовина потиче из кривичног дела. Начини утврђивања оваквих околности могу варирати од потпуно индицијалних трагова до писаних и електронских извора који указују да је извршилац овог дела у потпуности упознат са околности вршења кривичног дела и да средства потичу из њих. Овде треба додати и обавезе банака и других финансијских институција да врше мониторинг и пријављују сумњиве трансакције, као и оне за које постоји обавеза пријављивања, а и обавезе сарадње са институцијама за спречавање прања новца и гоњење кривичних дела.

Ово дело је посебно интересантно у савременим облицима комуникације и обављања финансијских трансакција, скоро тренутно. У данашњем свету најлакши

[269] Код ових (основног, посебног и најтежег) облика изричито је наведено да се могу примењивати правила поступка за дела из чл.504а.

облик прикривања имовине и користи прибављене извршењем кривичног дела јесте путем уплата и, уопште, извршења различитих трансакција електронским путем, а, посебно, путем Интернет плаћања. Још једна интересантна могућност јесте она коју банке пружају својим ВИП клијентима, јер то омогућава обострану корист и клијенту и банци, када су у питању клијенти који обављају велики број трансакција и обрћу велике количине новца, онда дају и могућности привилегованих трансакција а нуде и услуге кореспондентних банака по сличним принципима. У оваквим околностима од значаја су сви трагови који остају као резултат ових трансакција, како код банке која је спровела трансакције, тако и код клијента. Првенствено, у питању су изводи које банка чува и у електронском и у физичком (папирном) облику, али и лог фајлови на серверима банке о обављању трансација и пореклу и адреси са које је захтев на сервер стигао, време и место извршења трансакција и износи. Од значаја су и начини логовања клијента, јачина његове шифре и корисничког имена, као и употреба токена идругих облика заштите при коришћењу погодности веб банкинга.

4.4 Неовлашћена употреба туђег пословног имена и друге посебне ознаке робе или услуга

Први облик постоји у оном случају када се лице, у намери да обмане купце или кориснике услуга послужи туђим пословним именом, туђом географском ознаком порекла, туђим жигом или туђом другом посебном ознаком робе или услуга или унесе поједина обележја ових ознака у своје пословно име, своју географску ознаку порекла, свој жиг или у своју другу посебну ознаку робе или услуга (новчана казна или затвор до три године).

Други, тежи облик, представља недозвољену трговину робе у основном облику. Он постоји у случају када неко, у сврху продаје, у већој количини или вредности, набавља, производи, прерађује, ставља у промет, даје у закуп или складишти робу из првог облика или се бави пружањем услуга неовлашћено користећи туђе ознаке, (затвор од шест месеци до пет година). Још тежи облик постоји ако је учинилац другог облика организовао мрежу препродаваца или посредника или је прибавио имовинску корист која прелази износ од милион и петсто хиљада динара (затвор од једне до осам година). Наравно предмети из овог кривичног дела се обавезно одузимају. Овај облик је за ВТК интересантан када се ова дела врше преко Интернета, и када се као објекат или средство извршења јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара.

У пракси први облик се најчешће врши у продајама на неким од сајтова који служе масовном сучељавању и омогућавању пласмана понуде и потражње за робом од којих је најпознатији нпр. ww.ebay.com а код нас http://www.limundo.com. Смисао ових кривичних дела је у превари корисника или потрошача, па је значајно напоменути да се на ову област односе сви прописи о заштити потрошача, и веома

је значајна улога удружења за заштиту потрошача, а такође је веома битна улога норми Закона о електронској трговини којима се ова област регулише. Код доказивања овог дела од значаја је утврђивање намере да се обману купци и потрошачи, управо активношћу која подразумева коришћење туђим пословним именом, туђом географском ознаком порекла, туђим жигом или туђом другом посебном ознаком робе или услуга или уношење појединих обележја ових ознака у своје пословно име, своју географску ознаку порекла, свој жиг или у своју другу посебну ознаку робе или услуга од стране извршиоца. Начини заштите сопственика ових ознака могу бити од великог значаја код доказивања овог кривичног дела. Наиме, управо коришћење посебних облика заштите може бити од значаја код доказивања у оним случајевима када је могуће да извршилац преузме у потпуности, нпр. са Интернета лого или сличну ознаку оштећеног са постојећом заштитом, нпр. у облику стеганографских симбола увезаних са тим логом или путем идентификационих обележја саме пдф датотеке могуће је испратити пут ове датотеке и присуство на рачунару извршиоца може бити доказ о вршењу дела.

5. КРИВИЧНА ДЕЛА ПРОТИВ ОПШТЕ СИГУРНОСТИ ЉУДИ И ИМОВИНЕ

5.1 Уништење и оштећење јавних уређаја

Ово кривично дело у основном облику чини лице које: уништи, оштети, измени, учини неупотребљивим или уклони јавни уређај за воду, топлоту, гас, електричну или другу енергију или уређаје система веза и на тај начин проузрокује поремећај у животу грађана или у функционисању привреде, казниће се затвором од три месеца до пет година. Други облик постоји када је дело учињено из нехата, учинилац ће се казнити новчаном казном или затвором до једне године. Ово кривично дело са аспекта ВТК значајно је у оном делу који представља облик којим се уништава, оштећује, мења, чини неупотребљивим или уклања јавни уређај за електричну или другу енергију или уређаје система везе и тиме проузрокује поремећај у животу грађана или у функционисању привреде. Значи, неопходно је да наступи последица већих размера, а у вези са проблематиком ВТК. Код овог дела значајно је утврдити постојање везе између радње извршиоца и последице која је наступила, а у смислу разликовања облика неопходно је утврдити и постојање умишљаја или нехата. Такође, основни услов је да је дело проузроковало поремећај у животу грађана или у функционисању привреде.

6. КРИВИЧНА ДЕЛА ПРОТИВ БЕЗБЕДНОСТИ РАЧУНАРСКИХ ПОДАТАКА

У објашњавању дела ове главе КЗ од изузетног је значаја објаснити и кривична дела одређена Конвенцијом о ВТК у оном облику како их она прописује јер смо је ратификовали. Прилком тумачења одредаба КЗ треба имати у виду и одредбе Конвенције, и због правила тумачења законских норми али и због могућих колизионих елемената ових аката. Прописивањем дела *Незаконито поступање са подацима* (измена и ометање података и ометање система)[270] на рачунару, Конвенција о ВТК, у смислу намерног потпуног или делимичног оштећења, брисања, уништења, промене садржине, или компресије[271] оригиналних података[272]. Ово дело можда на први поглед изгледа слично *незаконитом приступу*, али се мора схватити пре свега као њему комплементарно: нелегални приступ (у намери да се измене подаци) омогућава извршење самог дела[273]. И овде Конвенција оставља могућност сужавања домета инкриминације – државе могу измену података сматрати кривичним делом, само ако је причињена већа штета. Дакле интенција креатора Конвенције била је да се дело односи на рестриктивне облике неовлашћеног поступања са подацима (оштећења, брисања или прикривања...) када наступе теже последице, али се, ипак, оставља државама да саме ставе резерву у овом погледу. Поступци описани у делу нелегалног приступа, као што су „тројанци“ и „логичке бомбе“, за крајњи циљ имају неовлашћено поступање са подацима на рачунару, које укључује и њихово слање аутору штетног програма или неком трећем лицу - наручиоцу (ради даље злоупотребе, најчешће, ради стварања зомби рачунара чак, мрежа истих). Треба поменути да се не инкриминише оштећење и брисање података, као, на пример, штета изавана вирусима, већ се традиционалним облицима манипулације додају акти који доводе до сличних последица. Пример је измена података – уколико вирус насумично измени садржину документа штета може бити упоређена са брисањем датотеке.

Један од практичних проблема у погледу овог дела може бити чињеница по којој се може избрисати податак на начин којим је немогуће доказати постојање таквог податка у систему, пре брисања, анализом претходне локације на Хард диску (HD –у). У таквим случајевима је неопходна темељнија форензичка анализа

---

270 Ово дело је покривено чл. 298, 299, 301, 302, КЗ РС.

271 У Internet related identity theft, A discusion paper, Prepared by Marco Gercke, www.coe.int/cybercrime Одређује се као: „акт који утиче на доступност података ширем кругу лица која имају приступ медију на којем је похрањен податак у негативном смислу“.

272 Чл.4. Конвенције.

273 Значајно је указати да је могуће извршити ово дело, (као и дело упада у рачунарску мрежу или систем), уз постојање конкретизоване намере: наношења штете или угрожавања јавне безбедности; угрожавања државних рачунара, система, мрежа или података; изазивања сметњи или оштећивања критичних информационих структура; и наравно у сврху предузимања аката тероризма; више на http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p.15. последњи пут приступљено 26.04.2010.год.

целокупног система, што апострофира значај сарадње са форензичком обрадом предмета и лица места.

На дело измене података надовезује се *упад у рачунарску мрежу или систем*[274], који је дефинисан, као умишљајно, озбиљно и неовлашћено манипулисање рачунарским системом уношењем, трансмисијом, оштећивањем, брисањем, уништењем, изменом или компресовањем рачунарских података. Делом се инкриминише бланкетна диспозиција, наводећи низ радњи, покривајући сваку ситуацију која претпоставља онемогућавање рада или мењање рачунарског система или мреже. Подразумева се да у ово дело спада и физичко искључивање сервера, али и DoS („ускраћивање услуга"енгл. *Denial of Service*, мисли се на услуге одговарајуће рачунарске мреже због нелегалног упада у њене податке[275]) и вирус. Даје се простор државама чланицама и да ставе резерву у погледу примене ове одредбе Конвенције инкриминишући само нападе усмерене на најважније службе или случајеве са значајном штетом[276]. Тражи се умишљај и мора бити неовлашћено упадање[277] у рачунарску мрежу или систем како би ово дело постојало. У случајевима овог дела у циљу повећања и појачавања последица, све чешће су примене ботнетова, великих група заражених рачунара зомбија који врше снажан напад на рачунар. Ово чини расветљавање и доказивање овог дела изузетно тешким и компликованим, зато што је неопходно пратити трагове до ботова (рачунара који су злоупотребљени у оквиру ботнета[278]) чији корисници нису свесни своје улоге, а све у циљу прибављања доказа и трагова који могу довести до извршиоца.

---

[274] Чл.5. Ковенције, код нас везано за дела из чл.298-304. Али у односу на прикупљање ових података и чл.146 (од којих се ст.1. и 2. гоне по приватној тужби а ст.3. по сл. дужности)

[275] Овај облик напада подразумева напад са циљем да се одсече одређени рачунар преплављивањем истог захтевима за комуникацијом који долазе споља, на такав начин да рачунар није у могућности да одговори на легитимне корисникове захтеве за саобраћајем.

[276] Иако термин озбиљне има проблематичне импликације и значајно ограничава примену неопходно га је искористити да не би било одређених примедби држава чланица у погледу ширине ове одредбе. Инкриминација обухвата према http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p.14. приступ и злоупотребу (прибављање): рачунарског програма, рачунарских података, података о саобраћају као и садржини тог саобраћаја; заштићених или поверљивих, критичних али и других државних рачунарских података или програма; рачунарских података или програма неопходних за финансијске трансакције и друге незаконите активности; и у сврху вршења терористичких аката

[277] Термин је интерференција који користи писац Конвенције, али у овом случају имамо најбоље решење у духу нашег језика у упаду.

[278] Под ботнетовима се подразумева велики број компромитованих рачунара који активирају програме без сопствене контроле. Компромитовање се обично врши даљински управљаним програмом учитаним на рачунару жртве (са карактеристикама руткит тројанаца) који отвара задња врата (backdoor) на жртвиноммрачунару са командним местом (C&C command &control) који представља најчешће ИРЦ (Internet relay chat) сервер легално инсталиран на некој јачој конекцији. Ботнетови раде прикривено и не ометају рад корисника који их није свестан, до ммомента када се Ботхерд (креатор и командант ботнетова) не одлучи за напад. Тада милиони рачунара крећу да путем мреже фокусирају неку одређену мету задајући јој м илионе и милијарде захтева (ДДоС напада) или ботехерд изнуђује –прети оваквим нападима у циљу прибављања противправне имовинске користи, или их користи у сврху креирања СПАМ-а, као и убацивања и инсталације злоћудних програма (руткитова) па чак и спајвера у циљу крађе идентитета. Своју армију ботхерд одржава коришћењем коктела тројанаца, црва и вируса, чиме себи омогућава систем проверавања способности армије и повећања исте.

Конвенција о ВТК прописује *Незаконит приступ* (хакерисање)[279] (чл. 2.) информацијама садржаним на рачунару или рачунарском систему, у намери да се те информације присвоје, измене или униште[280]. За ово дело се, дакле, тражи *намера*, тако да је државама – потписницама остављена могућност да инкриминишу само посебне радње које доводе до илегалног приступа неком рачунару или мрежи[281]. Типичан пример оваквог дела је убацивање „тројанаца" у нечији рачунар[282].

Незаконит приступ без овлашћења, неретко, представља први акт комбинације радњи (као елемената комплексних кривичних дела) на пример фишинга[283] (неки га називају пецањем) или крађе идентитета[284]. Конвенција не инкриминише метод на који се биће овог дела остварује, већ остаје неутрална у погледу технологије која се користи, основно што се захтева је постојање умишљаја и неовлашћеност приступа. У сваком тренутку државе чланице имају право да ставе резерву на ову одредбу конвенције којим се, на пример, може ограничити домашај у погледу захтева за безбедносним мерама – да се захтева неки вид пренебрегавања истих, или да се захтева да је извршилац деловао стриктно у намери прибављања рачунарских података.

Проблематика овог дела је веома значајна, довољно је навести податак да се сваког месеца, према независним истраживањима оствари више од 130 милиона

---

279 Термин који користи у оквирима Конвенције СЕ и Извештаја је дат у негативној конотацији, али треба имати у виду да се у раним развојним годинама ИТ хакерисање сматрало „покушајем извлачења максимума (из софтвера и хардвера) чак и изнад максималних граница онога за шта је дизајниран", те је некада исто сматрано конструктивном активношћу.

280 Овај облик у КЗ РС покрива више кривичних дела и то: чл.298. (без постојања намере), чл.299. (уз предвиђену намеру, која је ипак конкретнија од понуђене у Конвенцији), чл. 300. (овај члан веома екстензивним тумачењем може представљати имплементацију чл.2. Конвенције)

281 Може изгледати чудно али овај облик инкриминације није свуда постојећи, на пример, Немачка је тек 2007.год. увела Казненим Законом (који се односи на само остваривање неовлашћеног приступа а без измене података). Са друге стране неке земље иду у потпуности до краја па рецимо Румунија (нпр.чл.42. Закона бр.161/2003 http://www.coe.int/t/dghl/cooperation/economiccrime/ cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Romania%20_April%202008 _.pdf) инкриминише и сам неовлашћени приступ рачунарском систему, док друге инкриминишу само неовлашћени приступ одређеном рачунарском систему који је заштићен (дакле који има заштиту од оваквих упада) или инкриминишу неовлашћени приступ који је резултирао неовлашћенимн прибављањем , изменом или уништењем података, као и приступ који је остварен у намери наношења штете другоме.

282 „Тројанци" (енг. trojans) се испољавају пре свега као форма ненасилног или прикривеног преузимања контроле над туђим рачунаром, чега власник рачунара најчешће није свестан. „Тројанац" не може сам да се активира, већ то чини корисник рачунара који је нападнут у убеђењу да инсталира ауторизован програм, или неку другу апликацију за рад на рачунару (отуд аналогија са тројанским коњем). Више о разликама и сличностима са другим терминима касније.

283 По приручнику за обуку судија у супростављању сајбер криминалу доступном на Интернет страници http://www.coe.int/t/dghl/cooperation/lisbonnetwork/meetings/Bureau/TrainingManualJudges_en.pdf дана 26.01.2010. појам фишинг (пецање) описује покушај да се на преваран начин прибаве осетљиве информације (подаци – као на пример шифре) лажно се представљајући као одређена особа од поверења или финансијска институција кроз наизглед официјелну електронски остварену комуникацију. О фишингу опширније у тексту.

284 Појам крађа идентитета, по претходно наведеном извору, је одређен као криминална радња преварног прибављања и коришћења туђег идентитета. О крађи идентитета опширније у тексту.

хакерских напада[285]. Јасно је да се хакерски напади могу лако аутоматизовати (кроз ботнетове и сл.) а што, са друге стране, бива велики хендикеп за органе гоњења у супротстављању овом облику криминала, јер аутоматизован одговор ових органа веома тешко може постојати, нарочито у глобалним оквирима. Други проблем који се истиче у Савету Европе везује се за примену социјалног инжењеринга[286] јер се манипулисањем крајњег корисника (кроз искоришћавање његовог корисничког имена и шифре) прикрива стварни извршилац, и наводе органи гоњења на погрешно лице. Веома је тешко разоткрити који је контекст у којем се одају одређене информације и да ли су се одале у овом погледу, а нарочито је тешко тако нешто открити од стране органа гоњења.

6.1 Оштећење рачунарских података и програма

Први облик овог дела чини оно лице које неовлашћено избрише, измени, оштети, прикрије или на други начин којим се рачунарски податак или програм чини неупотребљив за његову намену[287] (новчана казна или затвор до једне године).

Други, тежи, (квалификовани) облик постоји онда када је проузрокована штета у износу који прелази четиристо педесет хиљада динара (затвор од три месеца до три године). Још тежи облик постоји уколико штета прелази милион и петсто хиљада динара (затвор од три месеца до пет година). Уређаји и средства којима је учињено кривично дело одузеће се, ако су у својини учиниоца. Последица овог кривичног дела је чињење неупотребљивим програма или податка. Дело је свршено предузимањем било које од наведених радњи уз остварење ове последице. Уколико је више радњи предузето према једном објекту рачунарском податку ил програму остварује се биће само једног кривичног дела. Извршилац овог кривичног дела може бити свако лице, а у погледу виности потребан је умишљај[288].

Кривични законик у члану 112. тачка 17. дефинише појам рачунарског податка свако представљање чињеница, информација или концепта у облику који

---

[285] У последња 24 сата 2.828.016 у последњих 7 дана19,942,974 а у последњих 30 дана 130,916,103. Извор http://www.hackerwatch.org/ доступан 26.01.2010.

[286] Под којим се, у приручнику за обуку судија у супростављању сајбер криминалу, за ову прилику одређује манипулисање лицима у циљу на пример остваривања приступа одређеним рачуанрским системима.

[287] Лазаревић, Љ, *Op.cit.*. стр. 745.

[288] Герке, М и др., *Приручник за истрагу кривичних дела у области ВТК, Савет Европе, 2008.*, str.115. Видећемо и да по Немачком Казненом законику: Намерна измена података, на пример, уништење или чињење неупотребљивим података је према чл.303б. кажњиво као дело измене, оштећењаили уништења података, истина и не тако тешком запрећеном казном – новчаном казном. Јасно строже је постављена ситуација уколико наступи знатна штета као резултат такве измене података (уколико је сервер компаније блокиран преко унетог црва) према чл. 303б. кривично дело рачунарске саботаже. Податак прибављен интервјуом са начелником одељења за борбу против ВТК Бајернске полиције.

је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију., Тачка 18. Рачунарском мрежом одређује скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке. И рачунарски програм у члану 112. тачка 19. одређује као уређени скуп наредби који служе за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара. Намера законодавца је да прописивањем овог кривичног дела заштити интегритет рачунарских података од неовлашћених деловања. Законодавац у тачки 33. одређује да је рачунар сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке, а у тачки 34. рачунарски систем је сваки уређај или група међусобно повезаних или зависних уређаја од којих један или више њих, на основу програма, врши аутоматску обраду података.

Значајно је разумети да се под другим начинима чињења неупотребљивим подразумева и чињење недоступнима, па се на овај начин инкриминишу и случајеви дејствовања разних бекдор или тројанских програма којима се одређени програми прикривају на рачунару, као припремне радње, рецимо, за рачунарску изнуду. За правилну квалификацију овог кривичног дела неопходно је утврдити да ли је извршилац поступао неовлашћено, тачно време и место извршења кривичног дела, начин на који је дело извршено – да ли је у питању физички приступ рачунарском програму или податку, или је дело извршено у оквиру рачунарске мреже интерног карактера или путем Интернета, па, уколико је извршено путем другог рачунара, уз помоћ ког програма, као и последице које су настале, односно да ли је објекат дела учињен неупотребљивим. Потребно је утврдити и својство учиниоца кривичног дела, односно да ли се ради о службеном или одговорном лицу у оквиру неког правног лица, или о лицу које је било, на основу неког правом регулисаног односа, овлашћено да на било који утврђен начин манипулише рачунарским програмом или податком, да га ажурира или мења[289]. Како би чињенично стање било потпуно утврђено, неопходно је идентификовати и коју је опрему употребио учинилац приликом извршења кривичног дела и коме она припада, с обзиром на то да је предвиђено одузимање уређаја и средства којима је учињено кривично дело, ако су у својини учиниоца. Подаци, датотеке и програми који су објекат извршења овог кривичног дела служе оштећенима за свакодневно пословање, књиговодствену евиденцију, одржавање пословних контаката или су у њима садржани лични подаци који имају само сентименталну вредност. Оштећени најчешће сами покушавају да отклоне штету која им је нанета или ангажују лица која имају већи или мањи фонд знања из информационих технологија, као би повратили избрисане податке. Оваквим деловањем се готово увек уништавају непосредни докази, који би могли довести до извршиоца, а органима гоњења остају само посредни докази, који, у већини случајева, нису довољни за откривање и процесирање учинилаца.

Уобичајено брисање података у „корпу за отпатке“ је могуће релативно лако повратити, па се у том случају јављају недоумице. Подржавамо став који је изнела група аутора[290] по којем је за постојање кривичног дела Оштећење рачунарских података и програма довољно спровести овај уобичајен начин

289 Герке, М и др., *Op.cit.* стр..116.

290 Комлен Николић Л. и др. *Op. Cit*., стр.90.

брисања података, а да каснији повраћај података не може бити третиран као околност која елиминише постојање кривичног дела[291].

Најчешћи вид извршења овог кривичног дела представља рушење (дефејсинг) веб сајтова, што је свакодневна активност хакерских група. Објекат напада је обично само део сајта, најчешће насловна страна, која бива промењена тако да се на њој остави ауторски „потпис“ групе, порука или поздрав, што јесте (али не само и једино) најчешћи елемент или чак и сврха акције хактивиста. Извршиоце је веома тешко открити јер они користе алате за скривање, који онемогућавају утврђивање места са кога је напад дошао, односно идентификовање праве ИП адресе, коју је извршилац користио у време извршења кривичног дела. У одређеним случајевима учиниоци иду, намерно, са постизањем ове околности, с тим да је ове податке веома тешко прибавити (обзиром да се на пример налазе на серверима у иностранству) чак и у оним случајевима када их нису сакрили или користили лажне. Тада временски протек игра своју улогу на многе елементе дела, од уништења и оштећења трагова до бекства извршилаца из земље.

Кривична дела *Оштећење рачунарских података и програма* и *Рачунарска саботажа* су слична према начину извршења и последицама које могу оставити, због чега се мора бити веома опрезан приликом квалификације кривичног дела. У сваком конкретном случају, мора се ценити умишљај извршиоца кривичног дела, значај избрисаних или оштећених података за пословање и функционисање оштећеног, али и све друге околности, како би одређена противправна радња била квалификована као једно од ова два дела.

Ова кривична дела се разликују и према тежини проузрокованих последица. Код кривичног дела *Оштећење рачунарских података и програма* последице су лакше, отклоњиве, док су последице *Рачунарске саботаже* много теже и имају шири дијапазон последица и објеката и пасивних субјеката.

---

[291] О важности правилног обезбеђивања доказа након извршеног кривичног дела, нужности заштите података које користе привредни субјеки али и ограничавања права њиховом приступу, говори нам пример једног преткривичног поступка који је Тужилаштво за борбу против високотехнолошког криминала водило током 2007. године. Против Осумњичене Б.А. из Суботице је била поднета кривична пријава због основане смуње да је током 2007. године извршила кривично дело *Оштећење рачунарских података и програма* - чл. 298. Кривичног законика на штету свог предузећа и то тако што је, као стално запослени административни радник, избрисала фолдере и фајлове, који се односе на улазне и излазне фактуре и, који представљају основну документацију значајну за пословање предузећа, као и фајлове са подацима о пословним партнерима оштећеног. Након саслушања осумњичене, запослених у предузећу и прикупљања свих других потребних доказа није било могуће утврдити њену кривицу. Осумњичена је негирала да је обрисала податке, није било сведока, који би тако нашто потврдили, а испоставило се да рачунари оштећеног предузећа нису били заштићени приступном шифром и да је свако од запослених могао приступити рачунару осумњичене. Иако се радило о веома значајним подацима за функционисање предузећа, ово брисање није имало већих штетних последица по пословање привредног субјекта, јер је оштећено предузеће у овлашћеном сервису рачунарске опреме већ следећег дана извршило повраћај обрисаних података. Како је повраћај података био извршен пре подношења кривичне пријаве и обавештавања надлежних државних органа, сви валидни докази су били трајно уништени, због чега није било могуће повести кривични поступак, па је кривична пријава одбачена

6.2 Рачунарска саботажа

Први облик овог дела у више радњи врши онај ко унесе, уништи, избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм или уништи или оштети рачунар или други уређај за електронску обраду и пренос података, са намером да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте, казниће се затвором од шест месеци до пет година.

Последица овог кривичног дела је чињење неупотребљивим рачунарског податка или програма или уништење или оштећивање рачунара или другог уређаја за електронску обраду и пренос података. Извршилац овог кривичног дела може бити свако лице, а у погледу виности потребан је умишљај. Битно обележје овог кривичног дела јесте намера учиниоца да предузимањем радњи онемогући или омете поступак електронске обраде или преноса података од значаја за поменуте субјекте, те је ову намеру потребно утврдити и доказати, односно наведена последица не може настати као резултат случаја или непажње.

Намера законодавца је да прописивањем овог кривичног дела заштити рачунаре и друге уређаје намењене електронској обради и преносу података који су од посебног значаја за државне органе, јавне службе, установе, предузећа или друге субјекте. Ово кривично дело неће постојати уколико је извршено према другим рачунарима, односно, оним рачунарима који нису од значаја за наведене субјекте, што значи да, у сваком конкретном случају, треба утврдити да ли се ради о рачунарима, описаних органа и организација таквог значаја[292]. Непосредан заштитни објекат представљају рачунари и други уређаји намењени електронској обради и преносу података који су од посебног значаја за државне органе, јавне службе, установе, предузећа или друге субјекте.

Већ је речено да постоји сличност између дела *Оштећење рачунарских података и програма,* али једна од разлика је што код *Рачунарске саботаже* имамо и уношење података, као посебан облик извршења којим се у рачунар уноси податак што за последицу има чињење неупотребљивим рачунарског програма или података, односно уништење или оштећење рачунара. Такође постоји и разлика у односу на који субјекат и од каквог значаја за њега, и грађане уопште, су уређаји који су предмет дела.

Неопходно је утврдити својство учиниоца као и његов умишљај, у оквиру кога и поменуту намеру. Потребно је тачно утврдити време и место извршења кривичног дела, начин на који је дело извршено – да ли је у питању физички приступ рачунарском програму или податку, или је дело извршено у оквиру рачунарске мреже интерног карактера или путем Интернета, као и уколико је извршено путем другог рачунара, уз помоћ ког програма. Значајно је утврдити да ли је наступила последица - уништење или оштећење рачунарских података или програма, предузимањем неке од инкриминисаних радњи, а уколико последица није наступила, неопходно је утврдити све напред наведено ради каснијег

[292] Герке, М и др., *Op.cit.*.стр.117.

процесуирања, с обзиром на то да је могуће да се последица манифестује и касније у раду ових уређаја[293].

Напади на веб сајтове државних органа, институција и приватних предузећа, као и крађа података од значаја за рад наведених субјеката, најчешће су били предмет, до сада, вођених поступака за кривична дела *Оштећење рачунарских података и програма* и *Рачунарска саботажа*. Обичним обарањем веб сајта није долази до продора у рачунарске системе и њиховог оштећења, а функционисање нападнутих веб страница би биле успостављане после неколико сати[294]. Последице саботаже би биле теже и могле би се састојати у онемогућавању или знатном отежавању функционисања оштећеног субјекта за дужи временски период, пословним губицима и наношењу високе материјалне штете[295].

---

[293] Герке, М и др., *Op.cit.*.стр.118. Он на овом месту наводи и да је покушај извршења овог кривичног дела кажњив међутим у нашем законодавству не гони се за покушај овог дела, јер није стриктно наведено а дело не спада у ред најтежих, за која је могуће изрећи казну затвора од пет година, или тежу казну, када би према чл.30. КЗ био кажњив и покушај.

[294] Комлен Николић Л. и др. *Op. cit*., стр.93-94.

[295] Посебно је значајно навести последњи пример у светским догађањима око Иранског нуклеарног питања и ангажовања две земље савезнице – САД и Израела, око пројекта stuxnet црва, ово и представља школски пример рачунарске саботаже али усеби садржи више различитих интересантних аспеката. Суштински значајна за разматрање у овом раду је и сама припрема за извршење овог кривичног дела кроз прављење IR-1 симулатора центрифуга истог као оног нуклеарне централе у Натанцу, и опсежних активности на изналажењу нешкодљивог пута да се саботажа изврши и онеспособе иранске могућности и капацитети на овом пољу (целокупна операција симулација и припрема одиграла се у Израелу у Dimona nuclear arms development објекту у пустињи Негев). У том смислу значајан је податак и да су коришћени сви адекватни елементи овог реактора и софтверски елементи које производи компанија Сименс, спекулише се да је ово откривено у случају када су Сименсови научници у сарадњи са Idaho National Laboratory покушавали да превентирају неке сопствене системске слабости. Објекат напада је директно био СКАДА (Supervisory Control and Data Acquisition) систем Сименсовог софтвера, а у самом малверу функционисала је размена П2П која је била криптована по FIPS 140-2 стандарду. Ова саботажа је резултат дуготрајне операције сајбер ратовања и обавештајне активности под називом Myrtus, која је зелено светло према разним гласинама добила 2008.год. Директно је спровођена у активном смислу од јуна 2009. до маја 2010.год, у три наврата. Сама операција је била усмерена веома прецизно и промишљено на онемогућавање постизања квалитетног резултата у обогаћивању уранијума у Натанцу, чиме се ишло на повећање трошкова за Иранску страну, где је аутпут – резултат невредан за њих, као и где ј сам поступак скопчан са великим трошковима и безвредан и потуно нерентабилан. У физичком смислу као резултат се јавило неконтролисано експлодирање центрифуга (неколико стотина) у различитим периодима, и поред безбедносних механизама инжењера у Натанцу. Овај се пројекат јавио као алтернатива предлогу Израелске стране за бомбардовањем централе, која би резултовала многим негативним елементима – од могућих људских жртава до губитака технике. Недостатак у овом подухвату је био везан за креатора, који је сматарао да се након извршеног напада неће десити да јавност сазна резултат и ток целокупне акције, чак нападачи су у циљу диверзије пустили овај злонамерни или злоћудни програм у етар и на другим местима – Индији, Индонезији и др. Али управо тамо где није могао проузроковати такве штете, шта више био је потпуно безазлен. Значајно је поменути да је 111 Сименсових контролера који су садржали ове слабости задржани у луци у Дубаију док су чекали административне процедуре на путу за Иран. Екслузивитет је да је целокупна проблематика око ове Сименсове слабости чак и објављен на саветовању 2008.год. а презентација у којој је исто садржано волшебно је нестала са сајта врло брзо по саветовању. За више погледати на:http://www.net-security.org/secworld.php?id=10452&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29 и http://www.wired.com/dangerroom/2011/01/with-stuxnet-did-the-u-s-and-israel-create-a-new-cyberwar-era/ и

6.2.1 Безбедност у сајбер простору за електронску обраду података

Услед повећане зависности друштва од рачунара, високе технологије и мрежне повезаности у свакодневном животу, неопходно је признати постојеће рањивости ових система али и система за аутоматизовану обраду и анализу података. Овај корак је неопходан а за њим и корак за предузимање мера у циљу заштите од такве рањивости и побољшања системских решења у погледу тих рањивости.

Електронска обрада података (ЕОП) може се третирати као скупина елемената (сопствености, ствари) различитог сензибилитета у погледу одржавања три основна захтева: поверљивости, интегритета и доступности.

Безбедност ЕОП је подложна најразличитијим тумачењима. Првенствено посматрано питање заштите је обично везивано у контексту предузимања безбедносних мера према поверљивим информацијама и подацима за контекст државне безбедности. У новије време се доста води рачуна о питању личне приватности и нарочито у контексту локације на којој се могу гомилати веће количине приватних података и информација – кућном рачунару, базама података на хард диску. Такође се разматрају питања заштите података у финансијским, научним и апликацијама контроле поступака. Питања безбедности рачунарских инсталација су још једна значајна група питања обзиром на вредност улагања у тај сектор.

Безбедна ЕОП представља стање постигнуто у оном тренутку када аутоматизовани системи обраде података и услуга поседују адекватну и одговарајућу заштиту од намерних или случајних опасности по њихову поверљивост, интергритет или доступност.

Безбедност је најшире могуће схваћена као: примењени менаџмент ризика дефинисан као покушај да се постигне највиши могући однос толеранције ризика за најмању могућу цену. Циљ је да се умањи изложеност ризику одређене фирме до прихватљивог нивоа, а што се најчешће најефикасније постиже формалним проценама ризика. Ово укључује одређени број компонената као, на пример, одређивање битних елемената, елемената од посебног значаја, опасности али и рањивости истих; финансијски утицај сваке комбинације напада или опасности на поједине вредне елементе система; процену вероватноће понављања и

---

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&ref=general&src=me&pagewanted=all као и http://www.guardian.co.uk/world/2011/jan/16/stuxnet-cyberworm-us-strike-iran сви доступни 19.01.2011 Презентација о којој је реч је доступна на http://graphics8.nytimes.com/packages/pdf/science/NSTB.pdf последњи пут приступљено 19.01.2011. Упоредити чињенице и са http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf последњи пут приступљено: 16.02.2011.год.

Овај облик злоћудних програма је новост у светским размерама и представља програм који је напредна константна претња, који има следеће карактеристике – примењује најсофистицираније технике напада инфекције и растурања малвера. Дизајниран је да остане прикривен унутар мреже жртве или у домаћину дужи период – најчешће коришћењем јаких руткит техника, чишћења логова, и спорих и тихих канала за командовање и контролу.

фреквентности за сваки од упарених битних елемената система и његову рањивост и претећу опасност; као и одређивање и избор тактичких и стратешких концепата у одбрамбеном смислу, избор средстава одбране и примена принципа приоритета безбедносних мера. Овакве мере не морају бити само финансијски ефикасне већ морају обезбедити и правичан баланс између оних мера предузетих у смислу превенције опасности и искоришћавања рањивости, оних које их детектују (њихово понављање или дешавање) и оних које служе као реакција на појаву.

Предмет заштите су три групе ствари: софтвер (програми) и информације, сервиси обраде података (контрола лета, обавештајни и информациони системи полиције, системи електронских трансфера новца) опрема и просторије за електронску обраду података. Мере безбедности ЕОП се састоје од седам есенцијалних компоненти административне и организационе мере, безбедносне мере персонала, физичке мере безбедности, комуникациона – електронска безбедност, хардверска и софтверска сигурност, оперативна безбедност и планирање напада и могућих изненађења, непредвидивог.

Значајно је увести и појам: административне и организациона безбедност и мере. Она подразумева развој свеобухватне безбедносне политике и успостављање безбедносних процедура за примену принципа и смерница ове политике. Минимум безбедносних захтева подразумева (процедуре ће се разликовати у зависности од величине фирме и броја запослених али ово представља најминималније захтеве):

1. Развој поступака које ће осигурати идентификације ризика
2. Дефинисање индивидуалних безбедносних дужности и адекватну расподелу одговорности
3. Одређивање простора на којим није дозвољен приступ непозваним особама
4. Установљавање процедура безбедносне ауторизације
5. Препознавање екстерних и уговорних веза
6. Припрема планова за ванредне ситуације

Уз ово, значајно је и определити се за адекватног администратора система фирме која ће водити или обављати безбедносне послове.

Заједничка карактеристика готово свих извршених кривичних дела је била слаба заштита рачунара, рачунарских података и веб сајтова. Профил извршилаца као и мотиви за извршење кривичних дела су веома различити, од радника који су незадовољни условима рада и висином примања, окривљених, који су то схватали као добру забаву, до оних који су били политички мотивисани. Иако до сада није вођено много кривичних поступака, извесно је да су ова кривична дела у стварности веома честа али да оштећени због необавештености, или незнања, не пријављују њихово извршење[296].

---

[296] У упоредном праву је устаљена пракса да се извршиоцима изричу веома строге казне чак и за покушај саботаже. Почетком 2008. године у америчкој држави Њујорк осуђен на 30 месеци затвора програмер запослен у предузећу "Medco Health Solutions“ због подметања "логичке бомбе" у рачунарски систем компаније, што је могло да доведе до обарања и оштећења више од 70 сервера који су садржали информације као што су подаци о издатим рецептима, медицински подаци, финансијски извештаји, платни спискови итд. До брисања наведених података није дошло јер је злонамерни код на време откривен од стране запослених “Man gets record sentence for computer sabotage”, ZDNet News & Blogs, Internet, *http://news.zdnet.com /2100-1009_22-182571.html,* 07.05.2009.

Познато је да је потписивањем eCEE агенде и агенде + Влада Републике Србије преузела на себе многоструке обавезе, па је истим било предвиђено да, до краја јуна 2009. године, влада почне са вођењем електронских седница. Такође предвиђено је и да ће се наставити процес електронског умрежавања свих општина у Србији, у оквиру пројекта електронске државне управе. Преузете су одређене обавезе као што је увођење „E- сервиса“[297] за потребе грађана и привредних субјеката и то на свим нивоима (и органа централне власти и органа локалне самоуправе). Увођење информационо комуникационих технологија у државну управу и прелазак државне управе на електронски режим рада представља велики изазов, значајно унапређује квалитет рада државних органа, смањује трошкове управе, побољшава квалитет живота грађана и пружа нове могућности за утицај грађана на јавни живот. Од државног је интереса да информациони системи државних органа буду адекватно заштићени, а државни службеници буду добро обучени, јер оштећење или уништавање података садржаних у тим системима може имати значајне последице по безбедност државе и животе грађана. У оваквом случају, због њиховог значаја и озбиљности могућих последица ова дела би била предмет обраде припадника БИА или ВОА (или ВБА). Веома велики проблем у оваквим случајевима могу бити и сукоби надлежности поменутих организација, ови односи регулисани су посебним правилима, а значајну улогу у томе игра Биро за координацију служби безбедности.

Закон о војнобезбедносној агенцији (ВБА) и војнообавештајној агенцији (ВОА)[298] у члану 5. прописује надлежност ВБА. ВБА је надлежна за безбедносну и контраобавештајну заштиту Министарства одбране и Војске Србије, у оквиру које, обавља опште безбедносне, контраобавештајне и остале послове и задатке од значаја за одбрану Републике Србије, у складу са законом и прописима донетим на основу закона. Чланом 6. Прописују се Послови и задаци ВБА. У оквиру опште безбедносних послова, ВБА у Министарству одбране и Војсци Србије:

4) примењује и контролише примену мера заштите тајности података;
7) врши послове из области индустријске безбедности;
8) врши послове безбедности информационих система и рачунарских мрежа, система веза и криптозаштите;
9) учествује у безбедносној заштити других субјеката система одбране;

У оквиру контраобавештајних послова и задатака, ВБА:

---

297 Под овим сервисима се подразумева широк спектар јавних услуга, од питања која се тичу личног статуса грађана, пребивалишта и држављанства, преко сервиса у вези издавања дозвола, до пријављивања пореза и др. На пример eCEE агенда предвиђа у тач. 1.5.2. Успостављање јединственог електронског шалтера за спољнотрговинско пословање у складу са препорукама UN Economic Commission for Europe - UN Centre for Trade Facilitation and Electronic Business као рок одређује март 2010.год. а у тач.3.2.2. Увести сет основних електронских јавних сервиса за правна лица у тачки један на пример Реализација јединственог електронског шалтера за пореског обвезника рок је децембар 2012.год. или 3.2.3. Увести сет основних електронских јавних сервиса за грађане одговарајући циљеви Agende+:C.2.b међу којима нпр. Реализација електронских сервиса везаних за издавање личних докумената (лична карта, пасош и возачка дозвола) до нивоа који је лиминитран обавезним присуством грађана ради идентификације и узимања биометријских података са роком до децембра 2011.год.

298 Службени гласник РС бр.88/09

1) открива, прати и онемогућава обавештајно деловање, субверзивне и друге активности страних држава, страних организација, група или лица усмерених против Министарства одбране и Војске Србије;

2) открива, прати и онемогућава унутрашњи и међународни тероризам, екстремизам и друге облике организованог насиља усмерених против Министарства одбране и Војске Србије;

3) открива, истражује и документује кривична дела против уставног уређења и безбедности Републике Србије, кривична дела против човечности и других добара заштићених међународним правом, кривична дела организованог криминала, кривично дело прање новца, као и кривична дела корупције (злоупотреба службеног положаја, трговина утицајем, примање мита и давање мита) и ако нису резултат деловања организоване криминалне групе, унутар Министарства одбране и Војске Србије;

4) открива, истражује и документује кривична дела одавање пословне тајне од интереса за одбрану, неовлашћеног приступа заштићеном рачунару, рачунарској мрежи и електронској обради података, одавање службене тајне и одавање војне тајне;

5) планира, организује и спроводи контраобавештајну заштиту тајних података Министарства одбране и Војске Србије;

6) планира, организује и спроводи контраобавештајну заштиту Министарства одбране и Војске Србије;

7) прикупља, анализира, обрађује и процењује контраобавештајне податке из своје надлежности;

8) обавља и друге контраобавештајне послове и задатке.

Ако су активности и дела из става 2. тач. 1), 2), 3) и 4) овог члана усмерена према Министарству одбране и Војсци Србије од лица која нису припадници Војске Србије и запослени у Министарству одбране, ВБА своје активности и мере на плану њиховог откривања, праћења и онемогућавања, односно истраживања и документовања предузима уз обавезну сарадњу са Безбедносно – информативном агенцијом или полицијом, са којима заједно утврђује начин даљег поступања.

Поред послова из ст. 1. и 2. овог члана, ВБА:

1) планира, организује и спроводи унутрашњу контролу рада припадника ВБА;
2) ...
3) сарађује и размењује податке са службама, организацијама и институцијама које се баве пословима безбедности, као и са безбедносним службама других земаља;
4) обрађује, проверава, сређује, процењује и штити прикупљене податке и информације од неовлашћеног откривања, давања, мењања, коришћења, губитка или уништавања;
5) обезбеђује и штити своје снаге, припаднике и објекте од противправних радњи и претњи;
6) штити опрему и средства која користи у раду од неовлашћеног приступа;
7) обавља безбедносну проверу кандидата за пријем у радни однос у Министарство одбране и на службу у Војску Србије, као и других лица

која су од значаја за обављање послова из члана 5. овог закона у сарадњи са Безбедносно-информативном агенцијом и полицијом;

8) ...

9) обавља и друге послове из своје надлежности.

Истим законом прописују се и овлашћења ВБА чланом 9. По којем су државни органи, организације и службе, органи аутономних покрајина, јединице локалне самоуправе, организације које врше јавна овлашћења, Војска Србије и правна лица, дужни да овлашћеним службеним лицима ВБА омогуће увид у регистре, збирке података, електронске базе података и другу службену документацију, осим служби безбедности и полиције са којима се размена података врши у складу са законима којима су уређене службе безбедности и полиција.

Ако подаци из регистара и других збирки података представљају тајни податак, субјекти из става 1. овог члана, осим служби безбедности и полиције, дужни су да омогуће ВБА увид у ове регистре и збирке података, на основу писаног захтева директора ВБА, у складу са законом којим се уређује заштита тајних података.

Независно од одредаба из ст. 1. и 2. овог члана, ВБА остварује сарадњу и размењује податке са Безбедносно-информативном агенцијом и полицијом у складу са одредбама закона којима су уређене службе безбедности и полиција. Посебно је интересантна одредба члана 10. по којој је ВБА овлашћена да, у оквиру своје надлежности, тајно прикупља податке применом посебних поступака и мера. Ове мере детаљније се образлажу чланом 11. Њиме се образлаже да је ВБА овлашћена да прикупља податке применом посебних поступака и мера када се подаци не могу прикупити на други начин или је њихово прикупљање у вези са несразмерним ризиком по живот и здравље људи и имовину, односно, са несразмерним трошковима.

ВБА прикупљање података применом посебних поступака и мера врши превасходно у превентивне сврхе, односно са циљем да се предупреде претње које су усмерене према Министарству одбране и Војсци Србије.

У случају да постоји могућност избора између више посебних поступака и мера, примениће се мера којом се мање задире у Уставом зајамчена људска права и слободе.

Посебни поступци и мере тајног прикупљања података из надлежности ВБА (посебни поступци и мере) су према (члану 12.):

1) тајна сарадња са физичким лицима;
2) оперативни продор у организације, групе и институције;
3) тајно прибављање и откуп докумената и предмета;
4) тајни увид у евиденције личних и са њима повезаних података, у складу са законом;
5) тајно праћење и надзор лица на отвореном простору и јавним местима уз коришћење техничких средстава;
6) тајни електронски надзор телекомуникација и информационих система ради прикупљања података о телекомуникационом саобраћају и локацији корисника, без увида у њихов садржај;

7) тајно снимање и документовање разговора на отвореном и у затвореном простору уз коришћење техничких средстава;
8) тајни надзор садржине писама и других средстава комуницирања, укључујући и тајни надзор садржаја телекомуникација и информационих система;
9) тајни надзор и снимање унутрашњости објеката, затворених простора и предмета.

Примену посебних поступака и мера уређује министар одбране, на предлог директора ВБА, уз мишљење Савета за националну безбедност. Посебни поступци и мере из члана 12. тач. 1) до 6) овог закона предузимају се на основу налога директора ВБА или лица које он овласти. Неопходно је напоменути да је овај члан (13), посебно због овлашћења прописаног у чл.12. тач.6. као и неки други чланови овог закона на поступку утврђивања усклађености са Уставом Републике Србије. Овај поступак оцене уставности и законитости резултат је иницијативе Повереника за информације од јавног значаја и заштитника грађана.

Посебни поступци и мере из члана 12. тач. 7) до 9) овог закона предузимају се на основу писаног и образложеног налога Врховног касационог суда. Председник Врховног касационог суда одређује судије овлашћене за издавање ових налога. Писани предлог за примену посебних поступака и мера из члана 12. тач. 7) до 9) овог закона директор ВБА подноси Врховном касационом суду. Судија без одлагања, а најкасније у року од 24 сата, доноси акт поводом предлога за примену посебних поступака и мера и доставља га ВБА. Ако надлежни судија одбије да изда налог за примену посебних поступака и мера, о разлозима одбијања без одлагања обавестиће ВБА која о томе обавештава Биро за координацију служби безбедности.

Предлог из става 3. овог члана, односно налог из члана 13. став 1. овог закона садржи назив посебног поступка и мера које ће се примењивати, податке о лицу, групи и организацији према којима ће се примењивати посебан поступак и мере, разлоге због којих се посебан поступак и мере спроводе, као и место и рок трајања њихове примене.

Предлог и налог за примену посебног поступка и мера представљају тајну. Службена и друга лица која учествују у поступку одлучивања и предузимања посебног поступка и мера дужна су да чувају као тајну све податке које су при томе сазнала. Након добијања налога суда, директор ВБА издаје налог за примену посебног поступка и мера. Посебно је интересантно овлашћење предвиђено чланом 15. Када разлози хитности то захтевају, а посебно у случајевима унутрашњег и међународног тероризма, директор ВБА може да наложи почетак примене посебних поступака и мера из члана 12. тач. 7) до 9) овог закона, уз претходно прибављену сагласност надлежног судије из члана 14. став 2. овог закона.

Судија, на основу поднетог предлога за примену посебних поступака и мера, доноси акт о наставку примене одговарајућих мера, односно њиховој обустави у року од 24 сата од почетка њихове примене. Међутим уколико надлежни судија не одобри примену посебних поступака и мера у року од 24 сата у складу са ставом 2. овог члана, директор ВБА је дужан да одмах прекине њихову примену и наложи комисијско уништавање прикупљених података, а записник о томе достави надлежном суду.

Према члану 16. поштанска, телеграфска и друга јавна предузећа, привредна друштва и лица регистрована за послове телекомуникационих оператора, друге начине преношења информација и послове доставе поштанских пошиљки дужни су да обезбеде услове и да омогуће ВБА примену мера тајног прикупљања података и извршења посебних поступака и мера из члана 12. овог закона и мера из члана 18. став 3. овог закона. ВБА има право на добијање информација од телекомуникационих оператора о корисницима њихових услуга, обављеној комуникацији, локацији са које се обавља и других података од значаја за резултате примене посебних поступака и мера. И овај члан је обухваћен оценом уставности и законитости о којој је било речи.

Према члану 17. Посебни поступци и мере тајног прикупљања података из члана 12. тач. 1) до 6) овог закона могу се примењивати све док постоје разлози за њихову примену. Посебни поступци и мере тајног прикупљања података из члана 12. тач. 7) до 9) овог закона, по налогу надлежног судије из члана 14. став 2. овог закона, могу се примењивати шест месеци, а на основу новог предлога могу се продужити још једном, најдуже на шест месеци. Чланом 18. Регулисан је случај када се деси да подаци прикупљени применом посебних поступака и мера из члана 12. овог закона указују на припремање или извршење кривичног дела за које се гони по службеној дужности, тада ВБА о основама сумње обавештава надлежно јавно тужилаштво. Значајно је да ово обавештење не садржи податке о примењеним посебним поступцима и мерама. ВБА, на основу резултата примене посебних поступака и мера, надлежном тужилаштву може да предложи примену надзора и снимања телефонских и других разговора или комуникација другим техничким средствима и оптичка снимања лица и примену других мера за кривична дела организованог криминала, корупције и друга изузетно тешка кривична дела, под условима и на начин прописан законом којим се уређује кривични поступак.

У погледу даљег прецизирања надлежности чланом 19. ВБА је овлашћена да у обављању послова и задатака из своје надлежности примењује посебне поступке и мере из члана 12. и мере из члана 18. став 3. овог закона, према запосленима у Министарству одбране и припадницима Војске Србије. Када ВБА у вршењу послова и задатака из своје надлежности оцени да би посебне поступке и мере из члана 12. тач. 5) до 9) овог закона, као и мере из члана 18. став 3. овог закона требало применити и према другим физичким лицима, дужна је да о томе одмах обавести Безбедносно – информативну агенцију или полицију, са којом заједно утврђује начин даљег поступања. Ради отклањања недоумица члан 20. прописује и да Овлашћено службено лице ВБА има приступ свим местима ради инсталирања уређаја за примену посебних поступака и мера из члана 12. и мера из члана 18. став 3. овог закона, у складу са налогом надлежног суда. А још конкретније дефинише и чл. 21. по којем приликом примене посебних поступака и мера из члана 12. овог закона, ВБА је овлашћена да користи податке, документа и средства која служе за прикривање идентитета ВБА, идентитета њених припадника и физичких лица са којима је успостављена тајна сарадња. У обављању послова из своје надлежности, ВБА по потреби предузима и мере прикривања својине над стварима и правним лицима, као и саме сврхе прикупљања података. ВБА може уз накнаду тајно да користи услуге физичких и правних лица. Члан 23. прописује

овлашћења у откривању, истраживању и документовању кривичних дела ВБА. Овлашћено службено лице ВБА у откривању, истраживању и документовању кривичних дела из члана 6. став 2. тач. 3) и 4) и члана 6. став 3. овог закона има следећа овлашћења:

1) провера и утврђивање идентитета лица и идентификација предмета;
2) позивање;
3) тражење обавештења;
4) привремено одузимање предмета;
5) преглед простора, објеката и документације и противтерористички преглед;
6) опсервирање;
7) прикупљање, обрада и коришћење личних података;
8) полиграфско тестирање;
9) овлашћења полиције за вршење мера надзора и снимања телефонских и других разговора или комуникација другим техничким средствима и оптичка снимања лица и предузимање других мера и радњи, у складу са законом којим се уређује кривични поступак.

Када овлашћено службено лице ВБА у вршењу послова и задатака из своје надлежности оцени да би овлашћења требало применити према лицима која нису припадници Војске Србије и запослени у Министарству одбране, ВБА о томе одмах обавештава Безбедносно-информативну агенцију или полицију, са којима заједно утврђује начин даљег поступања.

Члан 24. опредељује надлежности ВОА. ВОА је надлежна за обављање обавештајних послова од значаја за одбрану који се односе на прикупљање, анализу, процену, заштиту и достављање података и информација о потенцијалним и реалним опасностима, активностима, плановима или намерама страних држава и њихових оружаних снага, међународних организација, група и појединаца. Подаци и информације су војног, војно-политичког, војно-економског карактера и други подаци и информације, који се односе на пролиферацију наоружања и војне опреме и претње тероризмом усмерени из иностранства према систему одбране Републике Србије.

Након овога, чланом 25. прописују се и послови и задаци ВОА. У оквиру своје надлежности ВОА:

1) прикупља и проверава податке и информације, обрађује их, анализира, процењује и доставља надлежним органима;
2) сарађује и размењује информације и податке са службама, организацијама и институцијама Републике Србије које се баве безбедносно-обавештајним пословима, као и са службама других земаља и организација у складу са утврђеном безбедносно-обавештајном политиком, међународним уговорима и преузетим обавезама;
3) чува прикупљене податке и информације у складу са законом, подзаконским актима и штити их од неовлашћеног откривања, давања, коришћења, губитка или уништавања;
4) планира, организује и спроводи безбедносну заштиту својих активности, лица, објеката и докумената;

5) организује безбедносну заштиту објеката Министарства одбране и Војске Србије у иностранству и лица која су од стране Министарства одбране и Војске Србије службено упућена у иностранство;

6) штити опрему и средства која користи у раду од неовлашћеног приступа;

7) прибавља, развија и користи информационе системе, системе веза и системе за пренос података, као и средства за заштиту информација;

8) организује обуку припадника ВОА, организује специјалистичке курсеве, врши истраживања, формира архиве и објављује сопствена издања;

9) планира, организује и спроводи унутрашњу контролу рада припадника ВОА;

10) захтева од надлежних служби безбедности безбедносне провере правних и физичких лица када је то неопходно за обављање послова из надлежности ВОА утврђених овим законом;

11) планира опремање и врши набавку ствари за своје потребе;

12) обавља и друге послове из своје надлежности.

Закон прописује посебно овлашћења ВОА, па члан 26. говори о прикупљању података. ВОА је у оквиру својих надлежности овлашћена да прикупља податке:

1) из јавних извора;
2) од физичких и правних лица;
3) разменом података са другим службама безбедности;
4) применом посебних поступака и мера.

За ВОА чланом 27. прописана је примена посебних поступака и мера за тајно прикупљање података. Посебни поступци и мере за тајно прикупљање података су:

- тајна сарадња са физичким и правним лицима ради прикупљања података и информација из члана 24. став 2. овог закона;
- тајно прибављање и откуп докумената и предмета;
- оперативни продор у организације, институције и групе;
- предузимање мера на прикривању идентитета и својине;
- оснивање правних лица и уређење њиховог рада на начин који их не доводи у везу са ВОА;
- прикривено коришћење имовине и услуга физичких и правних лица уз накнаду;
- коришћење посебних докумената и средстава којима се штити ВОА, њени припадници, просторије и средства.

Посебни поступци и мере из става 1. овог члана предузимају се на основу налога директора ВОА или лица које он овласти. Примену посебних поступака и мера из става 1. овог члана уређује министар одбране, на предлог директора ВОА, уз мишљење Савета за националну безбедност.

У примени посебних поступака и мера ВБА и ВОА не могу се користити легитимације посланика Народне скупштине, чланова Владе, Генералног секретаријата Владе, Генералног секретаријата председника Републике и службене легитимације судија, јавних тужилаца, припадника других служби безбедности Републике Србије, полиције и других овлашћених службених лица.

Закон о БИА[299] чланом 9. прописује да Агенција у обављању послова из своје надлежности примењује одговарајуће оперативне методе, мере и радње, као и одговарајућа оперативно-техничка средства којима се обезбеђује прикупљање података и обавештења ради отклањања и спречавања делатности усмерених на подривање или рушење Уставом утврђеног поретка Републике Србије, угрожавање безбедности у земљи и, у вези с тим, предузима друге потребне мере и радње на основу закона и прописа донетих у складу са законом.Одлуку о примени описаних мера и метода доноси директор Агенције или лице које он овласти.

Посебно овлашћење у вези прикупљања података прописано је чланом 10. Закона о БИА. У обављању послова из свог делокруга, припадници Агенције овлашћени су да од државних и других органа, правних и физичких лица траже и добију обавештења, податке и стручну помоћ од значаја за разјашњавање чињеница везаних за обављање послова из делокруга Агенције. На пружање помоћи, давање обавештења и података нико не може бити принуђен, а ускраћивање или одбијање помоћи, давања обавештења или података мора бити засновано на законом утврђеним разлозима.

Изузетно Закон о БИА чланом 13. прописује да Директор Агенције може, уколико је то потребно, из разлога безбедности Републике Србије, својим решењем, а на основу претходне одлуке суда, одредити да се према одређеним физичким и правним лицима предузму одређене мере којима се одступа од начела неповредивости тајне писама и других средстава општења, у поступку утврђеном овим законом. Чланом 14. Предвиђа се одступање од начела неповредивости тајности писама и других средстава општења, на предлог директора Агенције одобрава одлуком председник Врховног касационог суда Србије, односно судија тог суда који је одређен да по овим предлозима одлучује у случају одсуства председника тог суда (у даљем тексту: овлашћени судија), у року од 72 часа од подношења предлога. Одобрене мере могу се примењивати најдуже шест месеци, а на основу новог предлога могу се продужити још једанпут најдуже на још шест месеци. У случају неприхватања предлога, председник Врховног касационог суда Србије, односно овлашћени судија у образложењу одлуке наводи разлоге одбијања.

Кад разлози хитности то захтевају, а посебно у случајевима унутрашњег и међународног тероризма, одступање из члана 14. овог закона може својим решењем наложити директор Агенције, уз претходно прибављену писмену сагласност за почетак примене одговарајућих мера председника Врховног касационог суда Србије, односно овлашћеног судије.

У овом случају писмени предлог за примену одговарајућих мера доставља се у року од 24 часа од добијања сагласности. Одлука о наставку примене одговарајућих мера, односно о њиховој обустави доноси се у року од 72 часа од подношења предлога. Одлука о обустави одговарајућих мера мора бити писмено образложена.

[299] Службени гласник РС бр.: 42/02 , 111/09

6.3 Прављење и уношење рачунарских вируса

Први облик чини оно лице које направи рачунарски вирус у намери његовог уношења у туђ рачунар или рачунарску мрежу. За дело је предвиђена санкција новчана казна или затвор до шест месеци.

Други облик чини онај ко унесе рачунарски вирус у туђ рачунар или рачунарску мрежу и тиме проузрокује штету, казниће се новчаном казном или затвором до две године. предвиђено је да се уређај и средства којима је учињено кривично дело одузму.

Кривични законик у члану 112. став 3. тачка 20. дефинише рачунарски вирус као рачунарски програм или неки други скуп наредби унет у рачунар или рачунарску мрежу, који је направљен да сам себе умножава и делује на друге програме или податке у рачунару, или рачунарској мрежи, додавањем тог програма, или скупа наредби, једном или више рачунарских програма или података.

За успешно вођење кривичног поступка против извршилаца кривичног дела неопходно је прибавити следеће доказе: 1) утврдити време и место извршења кривичног дела, 2) прибавити рачунарски вирус, одузети алате и уређаје помоћу којих је вирус направљен, и где 3) установити начин на који је рачунарски вирус унет у туђ рачунар или мрежу (уношење у сопствени рачунар или мрежу не представља ово кривично дело) односно да ли је вирус унет физички у одређени рачунар или мрежу директним приступом том рачунару или мрежи, или је то учињено у оквиру мреже интерног карактера, уз помоћ другог рачунара, као дела мреже или путем Интернета, 4) утврдити наступање штете[300]. У овим пословима неопходно је и ангажовање стручног лица, за шта полиција има овлашћења по ЗКП – у (може наредити вештачење из разлога који не трпе одлагање за кривична дела за која је запрећена казна до 10 година затвора).

6.3.1 Разлика између типова злоћудних програма

Вирус[301] је мали програм написан са намером да измени начин рада рачунара, без дозволе или знања корисника тог рачунара. Друга дефиниција[302] је да је то програм који инфицира одређени изабрани систем, као на пример датотеку, и који се може ширити даље по систему, па чак и изван њега. Трећа дефиниција[303] је да је у питању паразитска апликација која се самореплицира. Услови које мора да испуни како би се сматрао вирусом су:

---

300 Герке, М и др., *Op.cit.*.стр.120.

301 Неки их називају и паразитским вирусима. Видети у: Threatsaurus,the a-z of computer and data security threats, p.57. Sophos. доступан у дигиталноим облику на: http://www.sophos.com/sophos/docs/eng/ papers/sophos-a-to-z-computer-and-data-security-threats.pdf последњи пут приступљено 23.04.2010.год

302 Kizza, J. M., Computer Network Security, 2005 Springer Science+Business Media, Inc, p.154.

303 http://www.sophos.com/blogs/chetw/g/2010/04/03/3-types-viruses-demystified доступан 06.04.2010.

- Мора се сам активирати, често убацује свој код (програмску секвенцу) на место путање за извршавање дугог програма.
- Мора се реплицирати. На пример, може заменити друге стартујуће програме копијама вирусом инфицираних фајлова. Они могу инфицирати кућне рачунаре као и мрежне сервере.
- Мора имати носиоца, како би се неко други у контакту са носиоцем могао инфицирати.

Неки вируси су програмирани да оштете рачунар преко програма за уништавање или програма који могу нанети штету, брисање датотека (фајлова)[304]. Други нису дизајнирани за ту сврху већ да би се, просто, самореплицирали и приказали њихово присуство у меморији путем текстуалних, видео или аудио порука. Чак и ови „бенигни“ вируси могу створити проблеме за кориснике рачунара. Обично они заузимају меморију намењену другим програмима а као резултат се јављају погрешна понашања и евентуални пад система. Већина вируса је везана за багове[305] а који могу довести до пада система. Према систематизацији Симантек корпорације постоји пет типова познатих вируса. Први тип је *вирус који инфицира фајлове (датотеке)*, овај вирус инфицира програмске датотеке, обично извршне (егзекутабилне,) програме као што су датотеке са екстензијама .com и .exe, онда они могу својим извршавањем инфицирати друге датотеке, када се стартују са флопија, ХД-а, флеша или са мреже. Већина ових вируса је резидентна (отпорна и егзистирајућа) у меморији рачунара[306]. Након инфицирања меморије, било који извршни фајл који се стартује такође бива инфициран. Примери овог типа вируса су Jerusalem и Cascade вирус. Други тип је *вирус бут сектора*[307] било ког медија, флопија, ХД-а ЦД, ДВД, или флеш меморије, многи ове типове вируса сматрају праисторијским[308]. Сви поменути имају мали сектор на својој меморијској површини који се активира када се исти „утакну“ у рачунар. Описани тип вируса се прикачи за овај сектор на диску и активира се када корисник покуша да дигне систем преко ових медија који су заражени. Ови вируси су увек резидентни у меморији, већина их је написана у DOS –у[309], али сви кућни рачунари су потенцијалне жртве ових вируса. Све што је потребно је да се покуша стартовање система са оваквих медија и да се тако зарази систем. У овако зараженом систему неопходно је да се незаштићен медиј укључи и он ће бити заражен. Primeri za ovaj

---

304 О овоме се може више прочитати и у Урошевић, В. Ивановић, З. Злоћудни програми у ур. Оливера Лазаревић, ФОРУМ БИСЕЦ 2010 Конференција о безбедности информација стр.64-71 Београд Метрополитан универзитет, ФИТ, 2010.

305 Баг – на енглеском bug – програмска грешка или недостатак, који изазива проблеме у раду система.

306 Неки говоре о посебним врстама оваквих вируса те да их одликују следеће особине: већа перфидност, лака и брза пренсивост, врло су тешки за одстрањивање и најштетнији су од осталих облика вируса. Могу се условно поделити на два подтипа: **транзитни**, који су активни само онда када се извршава убачени програм и **резидентни** врста која се сама качи кроз сурогатни програм и остаје активна, дуго времена, након извршења сурогат програма, примери су вируси бут сектора, као што је israeli вирус.

307 Бут сектор - Boot sector је системска област на диску, он представља скуп датотека које иницирају стартовање система.

308 http://www.sophos.com/blogs/chetw/g/2010/04/03/3-types-viruses-demystified доступан 06.04.2010.год. неопходно је поменути да су били јако активни у неко прошло време.

309 Ранији тип оперативних система персоналних рачунара.

tip su: Form, Disk Killer, Michelangelo, and Stoned. Трећа група су вируси **главног бут сектора** и они функционишу на исти начин као претходни осим што су објекат њиховог напада системски сектори. Разлика између ове две групе је локација депоновања вирусног кода. Ова група, по правилу, легалну копију стартних (бутабилних) датотека памте на неуобичајеној локацији, и као резултат се добија немогућност подизања система. *Мултипартитни вируси* јесу четврта категорија (познати су и као полипартитни), они инфицирају и бут сектор и програмске датотеке. Они су веома тешки за брисање и повраћај система који су напали. Ово из разлога непотпуности мера за чишћење оваквих вируса (ако обришемо и очистимо бут сектор, остаће у програмским датотекама и обратно). Примери су: One_Half, Emperor, Anthrax and Tequilla. *Макро вируси* су пета категорија и они нападају датотеке које нису извршне, већ оне које садрже податке, оне су најчешће и највише коштају оштећене (због ангажовања веће количине ресурса (времена и новца) на њиховом чишћењу). Почетком примене Микрософтовог Visual Basic у Office 97 истог произвођача ови вируси се могу убацивати у све типове датотека повезане са овим програмским пакетима, а и друге. Због лакоће њиховог креирања сада постоје велике количине овог типа вируса. Примери су: W97M.Melissa, WM.NiceDay and W97M.Groov.

Неопходно је указати да постоје и друге категоризације које се овде могу приказати. Неки говоре[310] о врстама средстава који вируси користе, те по овом основу, разликују оне који *стварају грешке*, (њих хакери шаљу јер су тешки за откривање, и брзо се крећу, шаљу их у облику извршних датотека). Сваки пут када се датотека изврши прави грешке. Ове грешке могу варирати од тешких логичких грешака, које узрокују потпуни пад система, до лаких логичких грешака, које дају просте моменталне трептаје на екрану. Помињу се и *програмски и уништивачи података*, они су веома озбиљни у наношењу штете описаним подацима, који се прикаче програмима, након чега их користе за узгајање, реплицирање али и као лансирну рампу за нападе на друге програме или податке. Једном када се прикаче програму нападају друге програме или податке са којим носилац дође у контакт, мењајући им садржај, брисањем или потпуним уништавањем садржине. *Обарач система* се користи за потпуно онеспособљавање система, више је начина на који се они могу користити, а један од њих је уништавање системских програма као што су оперативни системи, везивне програме или друге. Други систем је самопродукција, реплицирање, док се систем не загуши и падне. *Вируси крађе рачунарског времена* се користе или као легитимни корисник система или спречавањем легитимног корисника да оствари услуге на систему, стварањем бројних прекида у систему. Овај тип ефективно оставља програме да чекају унедоглед на сопствено извршење док извршилац користи њихове ресурсе. Код овог облика је веома тешко приметити упад. *Уништивачи хардвера* иако нису чести ове „убице вируси“ користе се да селективно уништавају системске справе кроз везивање вируса у микроинструкције (мик) као што су биос или драјвери за уређаје. Оног тренутка када су се везали за мик могу довести уређај у ситуацију да се сам уништи или оштети. На пример, блокирање миша или тастатуре, или паркирање глава ХД на секторе диска који га могу довести до оштећења. *Логичке*

[310] Kizza J. M., Computer network security, Cyber crimes and Hackers,, 2005 Springer Science+Business Media, Inc, pp.155-6.

или временске бомбе временски су темпиране, а користе се да се, након уласка у систем, у одређеном тренутку активирају и направе хаос. Већина окидача временски су темпирани, али је могуће да то буде и неки догађај. Микеланђело је један од примера. Један од веома значајних облика је *врата са замком* највероватније један од најчешће коришћених облика. Функционишу тако што хакери налазе пут уласка у систем кроз слабо брањене тачке и рупе у систему или скенерима истог. Веома често произвођачи програма, приликом тестирања, намерно остављају отворене рупе у системским кодовима из различитих разлога, најчешће недокументоване као тајне тачке како би се програми касније могли модификовати. Шта више, оне се користе за тестирање од стране програмера у току коришћења од стране легитимних корисника. Као што то обично и бива овакве рупе се користе и од стране злонамерних лица. *Снифери или трагачи* представља софтверски шаблон који претражује (њушка) у систему који представља мету, у потрази за шифрама и корисничким именима, специфичним информацијама идентитета које обично доводе до експлоатације система.

Тројански коњи (тројанци) су програми који се представљају као легитимне софтверске апликације а који, у ствари, врше прикривене активности и врше штетне функције. Они су датотеке које наизглед представљају неке пожељне елементе, али, у ствари, су злоћудни. Веома значајна разлика вируса и тројанаца је да се ови потоњи не реплицирају. Тројански коњи садрже злоћудни код који када се активира проузрокује губитак или чак крађу података. Како би се постигло ширење тројанских коња неопходно је да неки други програми буду активирани на вашем рачунару, на пример отварањем и мејл поруке, у ствари додатка исте (attachment) или даунлоадовањем или извршавањем одређених датотека са Интернета. Битно је схватити да тројанци немају носиоце, већ да се они могу шетати, са инфицираног сајта, користећи недостатке и мањкавости браузера улазе на рачунар и врше свој посао. Тројански коњ је нпр. Trojan.Vundo.

Постоје још и *PCW тројанци* –претражују машину у покушају да нађу фајлове у којима се чувају поверљиви подаци и да их пошаљу нападачу. *Trojan clickers* – тројанци који преусмеравају рачунар корисника на одређени веб сајт, било са циљем да изазову DDoS напад на тај сајт, било да се корисник приступом том сајту зарази неким другим тројанцем или вирусом. *Trojan dropper* – тројанац који врши прикривену инсталацију других тројанаца или програма[311]. Слично „тројанцима“ делују и „логичке бомбе“, штетни програми попут вируса, али без могућности самосталног извршавања, све док не добију команду од корисника нападнутог рачунара која се, најчешће, састоји у покретању одређеног програма.

Црви су програми који се реплицирају потпуно самостално, од система до система, не користећи никакве датотеке домаћине. Сматрају их подврстом вируса, одређују се уобичајено као злоћудни програми који су свесни мреже (network-aware malware)[312]. Они су самостални програми, који немају потребу коришћења других датотека. Ово и представља разлику са вирусима јер је њима потребан неки облик домаћина – датотеке. Иако црви постоје унутар других датотека, постоје разлике у начинима како вируси и црви користе датотеке домаћине. Уобичајено је да црв

311 http://www.singi.co.yu/podrska/crvi.htm, 07.05.2009.

312 http://www.sophos.com/blogs/chetw/g/2010/04/03/3-types-viruses-demystified доступан 06.04.2010.

емитује датотеку која има „макро“ црва унутар себе. Цео документ (датотека) ће путовати од система до система тако да цео документ мора бити сматран црвом. Пример је W32.Mydoom.AX@mm. У сваком случају када се говори о црвима мисли се на програме који се користећи ЛАН (или Интернет) реплицирају са једних на друге рачунаре. Значајно је да се могу јавити и црви тројанци[313].

Вирусна превара[314] представља облике порука, најчешће трансмитоване путем и мејла, у количинама нешто мало вишим од уобичајених количина ланчаних писама. Следећи су примери ових облика вирусних превара, који садрже ове фразе:

- If you receive an email titled [email virus hoax name here], do not open it! (уколико примите и мејл под насловом (назив и мејл преваре), немојте га отварати)
- Delete it immediately! (Одмах обришите!)
- It contains the [hoax name] virus. (Ово садржи (назив преваре) вирус)
- It will delete everything on your hard drive and [extreme and improbable danger specified here]. (Ово ће обрисати све на ХД вашег рачунара и још многе екстремне и невероватне опасности које се сете навести)
- This virus was announced today by [reputable organization name here]. (Овај вирус је објављен данас од стране (име неке организације са добром репутацијом))
- Forward this warning to everyone you know! (Пошаљите ово свима које знате)

Ове преваре су изузетно честе на све популарнијим социјалним мрежама као што су фејсбук, мајспејс, хајфајв итд. Наводи се да постоји велики број различитих облика превара које иду од преваре која вас упозорава на неки нови злоћудни програм који се појавио на Интернету, или од вас тражи да проследите надаље ову поруку, или од вас тражи помоћ за прибављање веће количине новца у некој страној земљи, па до позива да покупите награду коју сте остварили на лутрији[315].

Шта не представља вирус? Обзиром на публицитет који вируси имају, веома је лако окривити их за неке проблеме на рачунару. Из овог разлога можемо навести неколике ситуације чији настанак није условљен вирусима или другим злоћудним кодовима:

хардверски проблеми	Ни један вирус не може физички уништити или оштетити хардвер рачунара, као што су чипови, плоче, процесори, матичне плоче или монитори
Рачунар пишти при стартовању без приказивања било чега на дисплеју	Обично је резултат проблема на хардверу приликом дизања система.
Рачунар не региструје или не пријављује 640 KB уобичајене меморије	Ово може бити знак постојања вируса, али не у сваком случају, неки драјвери

313 *Ibidem.*

314 Поједини аутори разликују према типу следеће преваре: ланчана писма, варалице, неспоразумске, лажних аларма (узбуна), вирусне преваре и преваре страха. Више на: http://www.sophos.com/security/hoaxes/ последњи пут приступљено 01.06.2010.год.

315 http://www.microsoft.com/protect/terms/socialengineering.aspx доступан 07.12.2009.год. Неке од ових превара представљају средство или увертиру у фишинг.

	(програми за покретање одређених уређаја под Виндоуз системима) за мониторе или СЦСИ картице или дискове могу узимати део ове меморије.
Постојећа су два антивирус програма и један од њих пријављује проналазак вируса	Могуће је постојање вируса, али је вероватно и да други антивирус програм региструје први као вирус.
Микрософтов програм ворд вас упозорава да документ садржи макро	Обично не значи да има и вирус
Не можете отворити одређени документ	Не значи присуство вируса, покушајте отворити други или његову сигурносну копију

Постоје правила именовања вируса, на пример, Симантек/Нортон (Symantec/Norton) антивирус има своје услове и правила. Име вируса се састоји од префикса, имена и често и суфикса.

Префикс означава платформу на чијој се основи вирус репликује или тип вируса. DOS вируси не садрже префиксе. Име је име фамилије вируса, Суфикс не мора увек постојати, а означава варијанте у оквиру исте фамилије, и обично га чине бројеви који означавају величину вируса или мање често слова. Примери су: префикси: АОЛ – овакви вируси су карактеристични за окружење Америка он Лајн или Backdoor Бекдор (задња врата или тајни пролаз) ове претње могу омогућавати недозвољени приступ извршиоцима са Интернета приступ вашем систему, итд. Суфикси: @m – означава да је вирус или црв мејлер, везан за електронску пошту, @mm – означава масовну пошту, Worm – значи да је у питању црв а не вирус. У сваком случају видећемо да скоро сваки од безбедносних програма даје свој назив одређеним категоријама. Чак и без присуства тројанаца у рачунару, Виндоуз може да омогући другима да приступе диску преко Интернета. Реч је у ствари о једном сервису који се користи код умрежених рачунара, дакле, тамо где постоји локална мрежа, а који извршиоци злоупотребљавају за извођење својих злонамерних и противзаконских активности. Назив сервиса је NetBIOS и, преко њега, се размењу фајлови у локалној мрежи. Овако створен проблем је релативно лако решити простим искључивањем овог сервиса, али поред овако простих проблема постоје многи који нису тако лако решиви.

6.3.2 Злоћудни програми

Уколико разматрамо проблематику злоћудних програма (злонамерни, малвер, а мало раније поменути други назив крајмвер[316] - криминални програми,

[316] Неки аутори наводе да се овако инсталирани програми могу користити на најразличитије начине, од којих су интересантни: крађа личних података у преварне сврхе и/или препродају на секундарном тржишту, крађа пословних тајни или интелектуалне својине или уценом (или претњом изношења у јавност нечега понижавајућег), трансмисијом спама, превара клика којом се генерише приход симулирањем саобраћаја онлајн рекламама, програми за изнуду (Ransomware) који шифрују податке и омогућавају извршиоцима да изнуђују или уцењују жртве; примена консолидованих личних података за омогућавање других и даљих напада.

неки говоре и о термину Warez,) неопходно је поменути да се СПАМ у литератури[317] наводи и као подгрупа ових програма. Злоћудни програми представљају категорију нежељених (оно што је заједничко за све облике СПАМ –а је да је у питању нежељени, непознат и веома злонамеран програм за крајњег корисника) програма који се активирају на рачунару корисника и предузимају малициозне активности. Према другој дефиницији[318] то је програм који је убачен у рачунар, рачунарски систем,најчешће прикривено, без одобрења или сагласности, у намери да се њиме компромитује поверљивост, интегритет или доступност рачунарских програма, рачунара, рачунарског система, мреже, рачунарских података, података о садржини, саобраћају комуникација или на други начин ометање употребе истих од стране правог власника (корисника). Овај појам подразумева и, генерално, легалне, али проблематичне, програме као што су адвер[319] и спајвер[320] (шпијунске програме) као и програме који предузимају незаконите активности и програме без комерцијалне примене, на пример, вирусе. Интересантно је поменути и поделу која, у оквиру злоћудног кода, као највише категорије предвиђа следеће подврсте[321]: спајвер, аутономне злоћудне програме (који се даље деле на вирусе и црве) и руткит / бекдор програме (који као подврсту имају ауторутере). Једна подела која је овде од значаја је подела по којој се крајмвер састоји од две групе програма: програма везаних за социјални инжењеринг и програма који користе безбедносне недостатке (оперативних система и других тулс програма као, на пример, браузера или инстант месинџера). Прва подгрупа се даље може поделити на програме који се додају у прилогу (attachments) и програме који се колоквијално називају „носећим – на свињским леђима“ (“piggybacking”, који се преносе легалним софтверима, без знања произвођача тог софтвера). Друга подгрупа обухвата Интернет црве[322], искоришћавања недостатака браузера и хакерисање. Треба поменути да се креатори

---

317 The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond A Joint Report of the US Department of Homeland Security – SRI International Identity Theft Technology Council and the Anti-Phishing Working Group. October, 2006 доступан на адреси www.antiphishing.org/reports/APWG_ CrimewareReport.pdf 28.12.2009.год p.4. више о овоме код нас погледати у Урошевић, В. Ивановић, З. Злоћудни програми у ур. Оливера Лазаревић, ФОРУМ БИСЕЦ 2010 Конференција о безбедности информација стр.64-71 Београд Метрополитан универзитет, ФИТ, 2010.

318 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p.12.

319 Рекламни програми, према енциклопедији сајбер криминалитета то је сваки програмски пакет који се самостално активира, приказује или даунлоадује рекламни материјал након инсталације другог софтвера или иницијализације и коришћења одређене апликације. Мада у Threatsaurus,the a-z of computer and data security threats, p.53. Sophos. Dostupan u digitalnom obliku na http://www.sophos.com/sophos/docs/eng/papers/sophos-a-to-z-computer-and-data-security-threats.pdf последњи пут приступљено 23.04.2010.год. не убрајају адвер ми остајемо при овом ставу.

320 Програми који шпијунирају приватне информације корисника, према енциклопедији, у питању су програми који из најразличитијих разлога прикупљају информације са рачунара корисника који није упознат са истим. Према Threatsaurus,the a-z of computer and data security threats, p.75. locus citatus, спајвер представља програме који омогућавају другим лицима (адвертајзинг индустрији и хакерима) да прибављају осетљиве податке од корисника Интернета без њиховог пристанка.

321 Berk, V. H. Cybenko, G. V. and Gray R. S. Early detection of active worms, Chapter 6. p.149.

322 Conficker црв је један од примера Интернет црва који искоришћава рањивости Виндоус система неки од црва су веома заразни, реплицирају се огромном брзином и могу да захвате велики број рачунара, неки од њих праве „задња врата“ за ддаље експлоатисање инфицираних система

свих злоћудних програма максимално труде да изграде и презентацију својих програма. У последње време веома је интересантно да „криминални“ форуми пласирају велики број различитих злоћудних програма, тројанских DIY (енгл. Do it yourself, уради сам) [323] који омогућавају сваком да креира овакав програм самостално, а што омогућава креаторима оваквих програма да у року од неколико минута, од регистровања као непожељних њихових програма преко различитих безбедносних програма, створе нову верзију. Значајно је да се у крајмвер убрајају: килогери[324], скринлогери[325], преусмеравачи[326], отимачи сесија[327], веб тројанци[328], генератори трансакција[329], системски реконфигуратори[330] и крадљивци података[331]. Постоје и друге поделе[332].

---

[323] И не само криминални или „црни“ форуми – већ и на youtube –у у овом тренутку има истих садржаја доступно на http://www.youtube.com/watch?v=9g5IU3Th2wQ и http://www.youtube.com/watch?v=YX4P-KS-j6c&feature=related.

[324] Програми који се самостално инсталирају у веб претраживач или као драјвери који надзиру унос података и шаљу релевантне податке фишинг серверима. Могу се унети као: објекти за помоћ претраживача – браузера (који детектују УРЛ (или Uniform Resource Locator (URL) је подгрупа УРИ (Uniform Resource Identifier (URI)) која одређује или показује где су одређени ресурси неопходни за покретање сајта и механизме њиховог преузимања) измене и логују податке када је УРЛ везан за одређене карактеристичне податке који се намеравају одузети), драјвер који снима уносе на тастатури и уносе мишем уз надзор корисникових активности, скринлогери, који прате уносе на дисплеју – монитору; Његова цена на црном тржишту у најпростијој верзији је према Cybercrime: current threats and trends, Discussion paper, 2008. COE p.10., доступан на адреси http://www.coe.int/t/dghl/cooperation/economiccrime /cybercrime/cy_activity_Interface2008/567%20study1-d-provisional%2013%20Mar%2008_en.pdf 16.04.2010.год. 40 $, webmoney Trojan – 500$, snatch Trojan који има карактеристике и функционалности руткита а краде шифре - 600$.

[325] Ова група је веома карактеристична јер се развила као реакција на мере против претходне групе, према којима је уместо уноса путем тастатуре генерисана на дисплеју тастатура путем које се уносе подаци од стране корисника. Како би се и овакав облик уноса података искористио креирани су ови програми,

[326] У питању су преусмеравачи електронске или инстант месинџер поште, који пресрећу и преусмеравају уз то и шаљу копије порука на нежењене адресе а којима приступ има нападач. Често се користе у корпоративној и економској шпијунажи.

[327] Овај облик напада се састоји од надзора над активностима корисникових активности на Интернету најчешће кроз малициозну компоненту претраживача. Оног тренутка када се корисник улогује на свој рачун или иницираттрансакцију малициозни софтвер „отима“ сесију у циљу предузимања криминалних активности, користећи се овако прибављеним подацима на најразличитије начине. Могу се активирати локално на десктоп рачунарима али могу бити и део напада човек између (или у средини).

[328] Ово су малициозни програми који искачу (поп ап – искачући програми) у циљу прикупљања поверљивих података. Ови програми играју на карту варања корисника приказујући му се као легитимни прозори банке или сличне финансијске институције за унос таквих података.

[329] Представљају, за разлику од осталих, програме креиране за напад на рачунаре унутар трансакционог процесног центра (а не као што смо до сада видели на крајњег корисника), као на пример процесор картица. Они креирају фиктивне трансакције у корист нападача а које потичу из самог процесора трансакција, често се користе за пресретање и злоупотребу података о картицама (кредитним и дебитним).

[330] Напади системског реконфигурисања као на пример, напади претраге домаћиновог имена и прокси напади врше модификације на рачунарима корисника и компромитују податке и информације. Код првог случаја браузери су ти који су нападнути и интерфејс који врши превод са откуцаног нама видљивог и читљивог на језик ИП адреса (четири комбинације троцифрених бројева са тачкама), ови напади су много чешће локални него што су на Интернет ДНС (Domain Name

У приручнику ИТУ[333] начињен је искорак унапред у правцу инкриминације трансмисије злоћудних програма и њихове злоупотребе (ова матрица за инкриминације обухвата производњу, продају, нуђење на продају, дистрибуцију, поседовање, као и постојање намере – коју градира на неколико типова – да изврши кривично дело, да нанесе физичку повреду, изазивања измене у пружању или погрешне примене медицинске помоћи; изазивања опасности по јавно здравље или јавну безбедност, и на крају у намери спровођења терористичких аката). Овим кораком охрабрују се државе да уведу инкриминацију везану и за злоћудне програме, која може имати веома далекосежне последице.

Типични облик напада из групе социјалног инжењеринга је убеђивање корисника да отвори прилог неког мејла или да „скине“ неку датотеку уз често присутно објашњење да је у питању неки порнографски материјал или сочне фотографије неке филмске звезде, трача или сличног објашњења које би лако „навукло“ жртву. Такође, и неки програми који се могу даунлоадовати са Интернета као на пример игре или програми који омогућавају убрзавање репродуковања видео или музичких записа могу бити заражени оваквим садржајем. Посебна ситуација у овој режији догодила се у веома блиској прошлости, кроз коришћење фејсбук платформи као комбинација социјалног инжењеринга, фишинга и спајвера, када је веома перфидно и лукаво искоришћен аватар смајлија за уваљивање товара спајвера[334]. Ови злоћудни програми се могу дистрибуирати на различите друге начине начине: кроз експлоатисање безбедносних слабости и рањивости путем мултиплицирања црва или вируса, који експлоатише даље недостатке безбедносних елемената, у циљу инсталације злоћудних програма или чињења

System (DNS)). Постоји три типа ових напада – као помоћни објекти за претраживач (BHO Browser helper object, где је обично килогер или скринлогер садржај), програм апликација (замена инстант месинџер програма која узима корисничко име и шифру за ИМ), или као драјвер. Са друге стране други тип напада реконфигурације система је инсталација проксија кроз који ће нападач спровести Интернет саобраћај одређеног корисника (жртве) нападач на овај начин може надзирати поверљиве податке и информације за време док корисник истим барата са овлашћеним сајтом своје институције (ово је облик напада човек између – нападач посредник). Оно што је карактеристично за овај облик је да оног тренутка када се активира више не постоји потреба за инсталацијом било каквог другог резидентног програма јер је овај процес тиме завршен.

[331] Оног момента када је активан злоћудни код на рачунару корисника, могуће је директно красти податке са тог рачунара (шифре, корисничка имена за логовање, кључеве за активацију софтвера, приватну и осетљиву кореспонденцију, као и било коју другу врсту информација похрањену на рачунару корисника). Ово се може вршити и преко различитих облика крајмвера укљученог у корпоративну и уопште у економску шпијунажу.

[332] Санбелт Лабс (енг. SunbeltLabs) на свом сајту даје следеће категоризације Адвере, кукије, дајалере, софтвере ниског ризика, малвер, потенцијални ИТ ризик, оруђе за даљинско управљање, надзорни програми, вируси и црви. Свака од ових има подкатегорије, па на пример малвер има опште облике, бекдор (задња врата), руткит, експлиоте, савлађиваче безбедносних програма, тројанце и скидаче тројанаца – даунлоадере или Надзирући програми имају облике килогера, комерцијалних килогера, општи надзор, снимаче и ли крекере шифри, прислушкиваче система, повратнике шифара и сл. За више о овоме погледати на: http://www.sunbeltsecurity.com/BrowseCategories.aspx последњи пут приступљено 25.06.2010.

[333] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf pp.16-17

[334] http://www.net-security.org/malware_news.php?id=1637&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29 последњи пут приступљено 25.02.2011.год.

доступним злоћудних програма на сајту, који искоришћава друге безбедносне слабости. Тада се саобраћај у браузеру може усмерити на одређени сајт који је спуфован и који нуди неке веома примамљиве садржаје, а може се искористити у случају када се врши инјектовање злоћудног садржаја у легитиман сајт (тада се искоришћава скриптна слабост међу сајтовима)[335].

Када би покушали даље да класификујемо или дамо неку исцрпну типологију крајмвера то би било изузетно тешко, најпре, због рапидног развоја сајбер криминалитета али и због савремене порозности граница међу типовима (јер се све више може препознати мешање и комбиновање карактеристика различитих облика напада). Наравно, то не значи да не треба разматрати облике који су репрезентативни, из дидактичких разлога. Могуће је разликовати следеће стадијуме напада крајмвера[336]:

1. Дистрибуирање крајмвера – у зависности од конкретног облика напада дистрибуција се може извршити путем социјалног инжењеринга (у виду малициозних прилога електронске поште – имејла) или кроз искоришћавање безбедносних мана и недостатака (преко сервера код Интернет претраживача – браузера искоришћавање безбедносних рупа[337], уз помоћ црва – инфицираним рачунаром или хакерисањем), дистрибуција се може вршити и кроз прилоге електронске поште или поште инстант месинџера. Један од интересантних начина је „случајан губитак““, у близини мете, неког преносног уређаја за архивирање података - УСБ драјва или преносивог ХД са инфицираном садржином. Постоји и

---

[335] Веома је интересантан случај комбинације социјалног инжењеринга и увезивања злоћудних програма у искоришћавању људске слабости у виду помаме и глади за вестима и знатижеље. Неколико часова након убиства бивше председнице Пакистана, Беназир Буто креиран је сајт на ком је у оквиру сајта увезан злоћудан ЈавaСкрипт, који је посетиоцима сајта нуђен као нови видео кодек (програм који декодира видео сигнал у стримингу) који се мора скинути како би се могао видети аудио-визуелни запис убиства. Исти је представљао врсту тројанца. Други пример је чувена фирма Seagate која је у августу 2007.год. обавестила своје купце да су у њиховим ХД-овима типа Maxtor произведеним у Кини пронађена два тројанца који краду шифре и корисничка имена (укупно је пријављено 1800 дискова). У последње време нарочито се говори о новим напредним генерацијама злоћудним програмима, који у свом коду носе велики број могућности за свог креатора. Један од примера је Stuxnet који је имао мултипле мете и невероватне могућности, а који је креирало випе особа и у чијем је стварању учествовало најмање две обавештајне службе, најачих земаља у овој области Израела и САД. Овај вирус је са собом донео вишеструке могућности праћења зараженост мета и контроле учинка вируса. Више о томе на: http://www.nytimes.com/2011/02/13/science/13stuxnet.html?_r=1&ref=science последњи пут приступљено 16.02.2011. год.

[336] The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond A Joint Report of the US Department of Homeland Security – SRI International Identity Theft Technology Council and the Anti-Phishing Working Group. October, 2006 доступан на адреси www.antiphishing.org/reports/APWG_ CrimewareReport.pdf 28.12.2009.год страна 7.

[337] Веб сајтови који користе слабости браузера обично су домаћини (популарно: хостују) мноштву експлоататорских програма, чак иницирају оне који се везују за одређене браузере према регистровању браузера који жртва користи. Веб апликације се такође искоришћавају, њихове слабости нуде извршиоцима веома широк оквир за експлоатацију и различите врсте напада, као на пример SQL инјекције, Ајах инјекције, ПХП скрипте и сл. Један од облика се назива драјв бај (drive by) даунлоадовање, простим посећивањем одређених инфицираних сајтова браузером се (без обзира на његов тип или врсту) инфицира браузер и малициозни програм је у рачунару.

облик даунлоадовања легалног софтвера уз који је повезан и неки злоћудни[338]. Дистрибуција је могућа и путем хакерисања, али кроз афилијативни маркетинг (нуђење на продају одређене робе, уз понуду одређеног релативно јефтиног софтвера повезаног за дати облик маркетинга) чиме се „скидањем“ таквог програма исти дистрибуирају.[339] Постоји и могућност примене крајмвера у смислу прикупљања личних и поверљивих података, и њиховог даљег дистрибуирања, а понекада и за допуњавање већ украдених података (уколико поседује делимичне информације, да би се употпуниле – бр.л.к. А да би се добио и ЈМБГ или адреса становања и слично), такође и за друге податке нпр. податке о колегама са посла одређеног лица и сл.

2. Инфицирање рачунарског система[340] или платформе корисника[341]. Различити су облици инфекција о којима се у овом раду разматра на различитим местима, но, у одређеним случајевима, крајмвер је од ефемерног значаја, већ је управо инфекција та, која је основни циљ, у датом нападу. Овде инфекција није пролазна, или припремна, фаза за вршење крађе података или нападе реконфигурације система, овде је она циљ целокупне активности извршиоца.

3. Извршавање (активирање дистрибуираног) крајмвера или као део једнократног напада (у случају крађе идентитета) или као позадински сегмент неког напада (нпр. Руткит) или иницирајући инфицирану компоненту.

4. Поверљиви подаци се узимају директно са извора у случајевима напада крађе идентитета.

5. Поверљиве податке одаје сам корисник у случајевима социјалног инжењеринга, ки логера или веб тројанаца.

6. Нападач злоупотребљава поверљиве податке. Подаци могу доћи из неколико различитих извора у зависности од облика крајмвера, као што је горе наведено.

7. Легитимном серверу се пружају поверљиви адекватни подаци о идентитету и шифра корисника или од стране крајмвера (у нападима када су подаци компромитовани директно од стране крајмвера) или нападача директно (напада човек између),

8. На крају, постоје и случајеви примећени у скорије време, који подразумевају крајмвер фишинг који се крије иза лажних понуда на ажурирање

---

338 Посебна подврста су лажни антивирус програми, који се иницирају искоришћавањем слабости браузера, након чега раде лажну проверу на присуство злоћудних програма, којом приликом налазе већу количину истих, након чега инсистирају на преузимању сопствених програма за чишћење, кооји су у ствари малициозни.За више види у Threatsaurus,the a-z of computer and data security threats, p.51. Sophos. *Loc.cit.*

339 У питању су, рецимо, лажни антивирус програми.

340 Одређени аутори (The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond A Joint Report of the US Department of Homeland Security – SRI International Identity Theft Technology Council and the Anti-Phishing Working Group. October, 2006 доступан на адреси www.antiphishing.org /reports/APWG_ CrimewareReport.pdf 28.12.2009.год стр. 19.) говоре о нужним моментима, стадијумима или кључним тачкама информационе компромитације од којих су најзначајније тачка инфицирања и тачка компромитације информација. То су момнети које сви облици крајмвера имају.

341 Инфицирање система и платформи жртве врши се разним средствима: кроз инфициране веб странице, прилоге електронске поште, социјални инжењеринг и примену експлоататора оперативних система.

верзија програма и тзв. печеве (patches) или закрпе програма које се, једноставно, „морају“ скинути. Ове специфичне преварне активности које комбинују методе социјалног инжењеринга и преварне ефекте понуда закрпа фреквентних програма односе све више жртава[342].

За супротстављање крајмверу значајно је препознати одређене слабе тачке у методици извршилаца. Оне представљају, у ствари, простор за примену противмера. Неки аутори препознају као примарне слабе тачке[343](моменте) инфицирања и компромитације података, јер се у датим код сваког облика малвера могу применити противмере. Сваки други моменат базиран на неким другим карактеристикама или фази у методици поступања извршиоца може се одредити као секундарна слаба тачка[344].

Рачунарски вируси, тројанци, црви и други злоћудни програми служе за стицање противправне имовинске користи, на неколико основних начина и то:

- За крађу личних података ради вршења рачунарских превара, изнуда, уцена и др., или за њихову даљу продају на Интернету (као нпр. за фишинг нападе),
- За крађу података који представљају пословну тајну – такозвану пословну шпијунажу или за крађу интелектуалне својине, како би се касније извршило кривично дело изнуде, уцене и др. према оштећеним лицима и предузећима, или информације даље дистрибуирале уз накнаду,
- За *DDoS* нападе везане за *On-line* уцене и ометање или онеспособљавање пословне конкуренције,
- За слање нежељених електронских порука (*Енг. spam*),
- За слање рачунарских програма који енкриптују електронске податке на рачунарима оштећених лица а, потом, служе за изнуђивање оштећених лица како би им се противправно отуђио одређени новчани износ за враћање важних података тј. њихову декрипцију,
- За прибављање електронских података потребних за вршење нових напада рачунарским вирусима, као што су контакти из листе контаката налога за електронску пошту оштећених лица или даље нападе на оштећеног и његове пријатеље, познанике и пословне партнере, на основу већ прикупљених информација о њима.

Помоћу откривања свих облика злоћудних програма можемо увидети шаблоне функционисања извршилаца кривичних дела, препознати путеве и начине на које можемо покушати правце превенције. У овом смислу неопходно је ангажовање свих друштвених и државних капацитета, јер овакве пошасти представљају појаве, које угрожавају све темеље друштва и подривају све добре

---

342 Погледати пример за овај облик у случају инсталације напредне верзије програма адоуб (Adobe) на: http://news.cnet.com/8301-1009_3-20049199-83.html последњи пут приступљено 04.04.2011.год.

343 The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond A Joint Report of the US Department of Homeland Security – SRI International Identity Theft Technology Council and the Anti-Phishing Working Group. October, 2006. *Loc.cit*. p. 20

344 На пример код дистрибуције крајмвера – спам филтери могу остварити превенцију дистрибуције, или спречавање извршавања крајмвера системски програм који дозвољава иницијализацију само сертификованих програма и кодова, или на пример, утицај на могућност извршиоца да прими и користи поверљиве податке, коришћењем комбинација шифри и кључева за заштиту поверљивих података.

карактеристике и добробити Интернета. Само свеобухватно ангажовање свих актера у области може донети прави резултат у борби против високотехнолошког криминала.

У нашем правном систему први случај откривања овог кривичног дела десио се у мају 2010. год[345]. У упоредно правној судској пракси до сада је било више поступака против лица која су креирала и ширила рачунарске вирусе. Тако је током 2005. године у Немачком граду Вердену условно осуђен осамнаестогодишњи хакер Свен Јашан (Sven Jaschan) на казну затвора у трајању од 21 месеца, јер је написао и пустио на мрежу црв „Sasser" који је 2004. године за само недељу дана инфицирао скоро 20 милиона рачунара широм света[346]. Sasser је паралисао болнице у Хонг Хонгу, блокирао сваку трећу пошту на Тајвану, пореметио рад рачунарског система Британ ервејза, Британске обалске страже и Аустралијске железнице, а компанија Голдман сакс претрпела је огромну штету. Занимљиво је да је извршилац вирус креирао у априлу, када је био малолетан, међутим штетне последице изазвао је касније, када је постао пунолетан. Млади Немац је типични пример профила одређене групе извршилаца кривичних дела која се врше путем високих технологија. То су најчешће млади, талентовани програмери са средњошколским образовањем. Због сличних дигиталних злоупотреба на Интернету. Средњошколац из Јужне Кореје лишен је слободе после напада на сервере важних институција, а младић из Мађарске је успео да блокира званични сајт тадашњег председника Владе, Виктора Орбана. Значајно је поменути да се сви описани облици злоћудних или злонамерних програма могу сматрати средством извршења овог кривичног дела.

6.3.3. Правила и смернице о поступањима за превенцију заразе вирусима, тројанцима и црвима[347]

Посебно је значајно примењивати антивирус или програме за заштиту крајње тачке[348], блокирати уобичајене типове злоћудних носиоце програма, блокирати фајлове који имају више од једног типа наставака нпр. annakournikova.jpg.vbs, пријављивати се на неки од и мејл служби за упозоравање, примењивати заштитне зидове на свим рачунарима, редовно ажурирати рачунарске софтвере, правити редовно архиве (бекапове) својих датотека. Такође, битно је увести политику поступања у оквирима мрежног окружења (она може укључити: забрану преузимања (даунлоадовања) докумената (доц екстензија) и извршних датотека (exe, com, bat и сл.) директно са мреже; забрану отварања нетражених архива, програма, база података или документа; забрану коришћења скринсејвера

---

345 http://www.blic.rs/Vesti/Hronika/188170/Prva-krivicna-prijava-za-unosenje-racunarskog-virusa-u-Srbiji доступан 12.05. 2010.год. Посебно је значајно да је у овом случају ЦЕРТ тим Немачких банкарских организација одиграо значајну улогу у расветљавању овог дела и да је заједничком сарадњом Немачке и Српске полиције расветљено дело које има карактеристике и фишинг преваре. Извршилац је Србин, а дело је вршено на теиторији Србије и Немачке.

346 http://en.wikipedia.org/wiki/Sasser_(computer_worm) доступан 07.05.2010.

347 Sophos, Treatsaurus *loc.cit*, pp.98-100.

348 У питању је комплексна програмска машинерија која интегрише већи број заштитних програма: антивирусе, фајерволове, за контролу уређаја, контролу приступа мрежи, контролу апликација, заштиту у току времена иницијације програма, за шифрирање, превенцију цурења информација.

или рачунарских игрица које нису дошле уз оперативни систем; обавезно прослеђивати прилоге у мејловима и сваке преваре или упозорења одељењу за ИТ заштиту; неопходно је памтити све доц фајлове у ртф формату, јер доц могу садржати макро вирусе; сваки неочекивани мејл мора се третирати као сумњив; у случају сумње у инфицираност неопходно је обавестити ИТ безбедносно одељење.

Правила и смернице о поступањима за превенцију спама[349]

У случајевима превенције спама неопходно је: користити филтрирање поште у и мејл клијенту, никада не куповати од рекламираних фирми путем незахтеване поште, уколико је у питању непознати пошиљалац нежељене поште обавезно је обрисати такву пошту. Значајна смерница је да никада не треба одговарати на СПАМ поруке и не пратити мишем линкове у њима, не користити начин гледања са прегледањем фотографија у и мејл клијенту. Обавезно је користити бцц (bcc) поље у случајевима слања неке поште на више адреса и, такође, не објављивати сопствене мејл адресе на Интернету и давати их само особама којима верујете. Један од веома популарних корака је коришћење једне или две адресе као секундарних, и да, увек, на сајтовима буде искључено даље примање информација са истих.

[349] Sophos, Treatsaurus *loc.cit*, pp.103-4.

6.4 Рачунарска превара[350]

Конвенција о ВТК (ЦЕТС 185) предвиђа дело под називом Рачунарско фалсификовање[351] и односи се само на умишљајно, неовлашћено убацивање, измену, брисање или сакривање рачунарских података, које као последицу има измењен садржај тих података, без обзира да ли они на овај начин добијају другу сврху и смисао, или постају неупотребљиви, а са намером да се такви подаци касније користе као аутентични у правном саобраћају. Државама је остављена могућност да предвиде и посебну врсту намере да се учини превара да би постојало ово кривично дело.

Предмет рачунарског фалсификовања, као објекат напада, су само подаци а Конвенција захтева да се у погледу умишљајног елемента дела чији подаци су у питању, садрже две категорије докумената: јавне и приватне исправе. Фалсификовање је дефинисано као умишљајно, неовлашћено убацивање, брисање, измена или сакривање рачунарских података, као и свако друго мешање у рад рачунарског система, са циљем да се прибави противправна имовинска корист за себе или треће лице.

---

[350] Посебно тужилаштво поднело је истражном одељењу Окружног суда у Београду Предлог за предузимање одређених истражних радњи Кт. втк. бр. 58/08 против М.Д. (33) из Чачка, због основане сумње да је дана 22.06.2008.године, у просторијама спортске кладионице која се налази у у Чачку, власништво ошт. „LES FOLIES“ Д.О.О., у својству лица запосленог на пословима пријема и наплате спортских тикета, у намери да себи и другом прибави противправну имовинску корист, приликом уноса података у рачунар - изменила системско време на рачунару и то за уплате по тикетима Спортске прогнозе серијских бројева F1.... и F16... , уносећи уместо реалног времена, време када је исход утакмица по уплаћеним тикетима већ био познат, на који начин је утицала на резултат електронске обраде података у виду регистровања новчаног добитка по уплаћеним тикетима наведених серијских бројева – који је НН лицу, истог и наредног дана, исплаћен у износу противправно прибављене имовинске користи од укупно 120.438,00 динара. Посебно тужилаштво поднело је Предлог за предузимање одређених истражних радњи Кт. втк 17/08 против З.М. (31) из Крагујевца због постојања основане сумње да је, у тачно неутврђеном периоду 2006 - 2007. године, у Крагујевцу, у намери да себи и другом прибави имовинску корист, на свом кућном рачунару прво написао - израдио, а затим кладионицама на територији Републике Србије за одговарајућу месечну новчану надокнаду и дистрибуирао рачунарски програм под називом „ТРКЕ ПАСА“ - који власницима кладионица пружа рачунарски генерисано клађење уз одсуство финансијског ризика и сигуран добитак од извршених новчаних уплата од стране лица која се кладе и то тако што је претходно, користећи своја знања из области математике и информатике, направио рачунарски програм чији је саставни део чини 1.190 појединачних видео - записа, већ одражаних - по исходу познатих - различитих трка паса, као и један фрејм у JPEG формату са речима на одговарајућој позадини *„NOT RACE AT THE MOMENT“* („*У овом тренутку нема трка - преноса*“), који програм је написао на тај начин да према извршеним уплатама и изабраним бројевима паса који учествују у тркама - програм сам бира одговарајућу, већ одржану и унапред снимљену трку која власнику кладионице гарантује новчани добитак, при чему би на напред наведени начин одабрана трка путем постављених екрана у кладионицама била емитована лицима која се кладе, како би стекла уверење да на екранима посматрају трке које се емитују путем сателитске телевизије и одвијају у реалном времену односно, да посматрају трке у којима се унапред не зна победник утрке, или редослед паса који пролазе кроз циљ.

[351] Ово дело у КЗ посредно покрива чл.301, и делимично чл. 299.чак и чл.225.

Треба указати да је према приручнику за судије као пример за ово дело истакнут фишинг (пецање)[352]. Ово захтевање постојања намере у већини случајева компликује примену инкриминације у пракси, али код овог дела није такав случај. Код фишинга није проблем доказивање намере - само слање оваквих облика електронске поште даје нам простор за закључивање о постојању намере.

Конвенција ЦЕТС 185 предвиђа дело Рачунарске преваре[353] и оно представља кривично дело које чини лице, у намери да прибави имовинску корист себи или другоме, које неовлашћено нанесе штету другоме путем: а. било какве измене, уношења, брисања или сакривања рачунарских података,

б. било каквог утицаја на функционисање рачунарског система;

Циљ инкриминисања овог дела је да се спрече манипулације у току процесирања података предузете у намери остваривања утицаја на нелегални трансфер средстава.

Примери које за ово дело наводи приручник су превара платним или кредитним картицама (што је код нас регулисано чл. 225. КЗ) и аукцијске преваре (а оне су регулисане чл. 208. КЗ). Као предмет напада се све више јављају електронски фондови, депозитни новац, е злато, као нови предмети класичног кривичног дела преваре. Значајно је поменути да се код овог кривичног дела може указати на разлику са класичним схватањем преваре. Наиме схватање по којем лажно представљање у превари представља облик лажног приказивања чињеница или на други начин довођења у заблуду лица како би се нешто учинило или не у намери прибављања имовинске користи, и уопште појма заблуде овде је специфично. Просто у овом делу Рачунарски систем је извршилац (а не физичко лице, оно је деловало пре наступања последице) преваре па га морамо инкриминисати. У циљу спречавања остваривања оваквих превара у свету се предузимају најразличитије техничке мере, од којих је један од добрих пример плаћање преко PayPal –а али он изостаје за територију Србије, па нама остаје да будемо под отвореним ударом превараната.

У нашем законодавству први облик овог дела чини онај ко унесе нетачан податак, пропусти уношење тачног податка или на други начин прикрије или лажно прикаже податак и тиме утиче на резултат електронске обраде и преноса података, у намери да, себи или другом, прибави противправну имовинску корист и тиме другом проузрокује имовинску штету, казниће се новчаном казном или затвором до три године.

Квалификовани облици овог дела постоје када је прибављена имовинска корист која прелази износ од четиристо педесет хиљада динара, (затвор од једне до осам година), односно корист која прелази износ од милион и петсто хиљада динара (затвор од две до десет година). Ово дело постоји и у лакшем (привилегованом) облику када се учини само у намери да другог оштети (новчана казна или затвор до шест месеци).

---

[352] Веома је значајно дати дефиницију коју користи овај приручник, по којој је фишинг тип кривичног дела карактеристичан по покушају извршиоца да преварно прибави осетљиве податке и информације, као на пример шифре за приступ одређеном рачунарском систему, представљајући се као особа или фирма од поверења (нпр. финансијска институција) на начин који изгледа као њихова официјелна комуникација.

[353] Покрива га истоимено дело у чл.301. КЗ РС

Кривично дело *Рачунарска превара* се мора разликовати од кривичног дела *Превара* из члана 208. КЗ, из групе кривичних дела против имовине. *Превара* такође може бити извршена коришћењем рачунарске технологије, када извршилац у намери да себи или другом прибави противправну имовинску корист, оштећеног – лажним приказивањем неких чињеница или њиховим прикривањем, доведе или одржава у заблуди и, тиме га, наведе да овај нешто учини или не учини на штету своје или туђе имовине. Фокус кривичног дела рачунарске преваре јесу подаци и поступак обраде и преноса података, дакле синтаксички а не семантички, као што је то случај са преваром из чл. 208. КЗ где је фокус на одређеном лицу – жртви преваре. О кривичном делу *Превара* и начинима његовог извршења коришћењем информационих технологија попут нигеријског писма, већ је било образлагано.

Радња кривичног дела је алтернативно одређена, као уношење нетачног податка или пропуштање уношења тачног податка. Нетачан податак је онај податак који не одражава истинито оно на шта се односи. Уколико се дело врши нечињењем, пропуштање треба да се односи на неки важан податак. Важност податка је фактичко питање, које се разматра у сваком конкретном случају али, то може бити само онакав податак, који може утицати на електронску обраду података. Можемо говорити и о прикривању или лажном приказивању податка, на други начин, као облицима радње овог дела. Прикривање података значи физичко склањање или обмањивање о постојању одређених података, док је лажно приказивање података приказивање непостојећег као постојећег или неистинито приказивање постојећег. У сваком облику радње кривичног дела неопходно је да је таква радња подобна да се њоме утиче на резултат електронске обраде података и да она јесте разлог другачије електронске обраде.

Намера законодавца је да прописивањем овог кривичног дела заштити веродостојност и интегритет података, који се електронски обрађују или се врши њихово преношење електронским путем. Као неопходни елемент бића потребно је утврдити, у сваком конкретном случају, и намеру учиниоца да за себе или другог прибави противправну имовинску корист и да, тиме, другом проузрокује имовинску штету.

Извршилац овог кривичног дела може бити свако лице, а у погледу виности потребан је умишљај, квалификован намером. Дело је свршено када је предузета нека од радњи извршења, уз постојање описане намере и када је тиме другоме проузрокована имовинска штета, при чему, није неопходно да услед предузете радње буде и остварена противправна имовинска корист.

За правилну квалификацију кривичног дела *Рачунарска превара*[354] и његово успешно доказивање неопходно је утврдити време и место извршења кривичног дела, тачну радњу која је предузета, као и начин и средство којим је унет нетачан податак. У погледу унетих података потребно је установити њихову неистинитост, у чему се та неистинитост огледа, и како је, тиме, утицано на резултат електронске обраде и преноса података, затим уколико је у питању пропуштање уноса тачног

[354] У Немачкој употреба података у преварне сврхе, на пример, трансфера средстава са банкарског рачуна употребом хакерски прибављених података представља посебан облик преваре, у овом случају рачунарске преваре из чл. 263 Казненог законика Немачке. Описано је још једна смерница за поступање у овом правцу у Србији. Податак прибављен интервјуом једног од аутора са начелником Бајернске јединице за ВТК, уз помоћ НВО Ханс Зајдел фондације (*Hans Seidel Stiftung*).

податка, на који начин је то пропуштено, одн. на који други начин је прикривен или лажно приказан податак, а све у циљу утицања на резултат обраде и преноса. У вези овога потребно је утврдити начин уношења податка (или уколико је пропуштено његово уношење) да ли је то учињено путем физичког приступа уређају подобном за електронски пренос или обраду података или је то учињено путем мреже. Неопходно је утврдити који је софтвер био коришћен, као и колики је износ користи био обухваћен умишљајем учиниоца (одн. да ли је хтео да је прибави себи или неком другом), наравно и висину износа наступиле штете, па и у случајевима да корист и није остварена. За доказивање дела из става 4. потребно је утврдити врсту штете која је била обухваћену намером и њено наступање, као и постојање намере учиниоца да својим деловањем проузрокује такву штету. Потребно је утврдити којим је средствима извршено кривично дело и уколико је могуће, извршити њихово одузимање како би били обезбеђени сви неопходни докази[355].

Електронска обрада података и очување њеног интегритета и веродостојности су од изузетног значаја за сваку државу, нарочито због тога што електронско пословање постаје доминантан вид активности привредних субјеката и државних органа. Пословне трансакције које се обављају електронским путем нарочито су погодне за разне видове злоупотреба, а са растом њиховог обима повећава се број кривичних дела из те области, а последице постају све теже. Овим кривичним делом могу бити погођени сви привредни субјекти од великих корпорација и државних предузећа, банака, до најмањих попут књиговодствених фирми или спортских кладионица[356]. У овој области од значаја је и закон о електронској трговини[357].

---

[355] Герке, М и др., *Op.cit.*. стр..122.

[356] У досадашњој домаћој судској пракси било је неколико случајева процесуирања учинилаца овог кривичног дела, али све говори о томе да је Рачунарска превара све учесталије кривично дело. Тако је Тужилаштво за борбу против високотехнолошког криминала иницирало покретање истраге против осумњиченог ЧА због основане сумње да је током 2007. и 2008. године у два наврата користећи рачунар улазио у системе банака у Аустралији и Швајцарској и издавао лажне налоге за трансфер средстава, чиме је прибавио противправну имовинску корист у износу од 51.990 CHF, односно да је покушао да из једне швајцарске банке неовлашћено изврши трансфер средстава у износу од 19.000 USD, Како у нашој земљи постоји велики број спортских кладионица које имају разгранату мрежу пословница и чије пословање је незамисливо без рачунарских мрежа, неретко се дешавају злоупотребе оваквих система. Извршиоци на различите начине покушавају да утичу на резултат елктронске обраде података и да користећи софтверска решења фалсификују одигране тикете. Против М.Д. покренута истрага због основане сумње да је дана 22.06.2008.године, у просторијама спортске кладионице која се налази у у Чачку, власништво ошт. „ЛЕС ФОЛИЕС“ Д.О.О. у својству лица запосленог на пословима пријема и наплате спортских тикета, у намери да себи и другом прибави противправну имовинску корист, приликом уноса података у рачунар - изменила системско време на рачунару и то за уплате по тикетима Спортске прогнозе серијских бројева Ф1.... и Ф16... , уносећи уместо реалног времена, време када је исход утакмица по уплаћеним тикетима већ био познат, на који начин је утицала на резултат електронске обраде података у виду регистровања новчаног добитка по уплаћеним тикетима наведених серијских бројева – који је НН лицу, истог и наредног дана, исплаћен у износу противправно прибављене имовинске користи од укупно 120.438,00 динара.Тужилаштво је током 2008. године покренуло истрагу против једног од радника предузећа „Телеком“ због основане сумње да је периоду од 2003. до 2007. године оштетио предузеће за више од десет милиона динара, на тај начин што је лажно приказивао податке који се односе на тарифирање телефонског саобраћаја и на осамнаест телефонских прикључака омогућио бесплатно телефонирање у локалном, међуградском и

6.5 Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података[358]

Кроз дело Незаконито пресретање комуникације, Конвенција ВТК покушава да изједначи, по третману, електронске комуникације са телефонским комуникацијама и, на овај начин, уводи инкриминацију пресретања електронске

међународном саобраћају, као и у свим мрежама мобилне телефоније, Наведено према Комлен Николић, Л. *Op.cit...* стр.102. Сличан пример можемо наћи и у суседној Црној гори, када је током 2005. године црногорски Телеком оштећен за износ од 6.120.000 евра и ти тако што су двојица Будвана без лиценце коју издаје Агенција за телекомуникације Владе Републике Црне Горе и пријављене делатности, користили сервис „Воице овер ИП", пребацујући међународне телефонске позиве на локалну мрежу, наплаћујући ову услугу у иностранству више о томе на: „Рачунарска превара тешка шест милиона еура", Побједа Интернет, http://www.pobjeda.co.me/citanje. php?datum=2005-11-19&id=75425, 07.05.2009

[357] Службени Гласник РС бр. 41/09.

[358] Посебно тужилаштво поднело је истражном одељењу Окружног суда у Београду Предлог за предузимање одређених истражних радњи Кт.втк.бр. 56/07 против В.М. (31) из Београда због основане сумње да је... неовлашћено приступио рачунарској мрежи ошт. предузећа „Yunicom" са седиштем у Београду, на тај начин што је - путем интерне рачунарске мреже хотела у којем је боравио - конектовао свој рачунар на глобалну рачунарску мрежу - Интернет и приступајући са IP адресе број: 87.116...., која је у то време од стране Интернет провајдера „SBB" била додељена предузећу „Tourist gamesstari grad", прекршио мере заштите успостављене од стране ошт. предузећа „Yunicom" - уносећи у свој рачунар web - адресу број: 217.24..... додељену ошт. предузећу „Yunicom" за приступање web - mail серверу „World Client for MDaemon" преко којег су запослени из ошт. „Yunicom-а" остваривали поштански саобраћај, након чега је - знајући као бивши радник „Yunicom-а" адресе електронске поште и лозинке запослених лица, исте уносио и на свом рачунару неовлашћено прегледао садржај њихове електронске поште.

У саопштењу МУП РС од 15. децембра 2009. се прецизира да су кривичне пријаве поднете против Александра А., Милана М. и Ђорђа Д. из Крагујевца због постојања основане сумње да су извршили кривична дела неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података и фалсификовање исправе. Осумњичени су у дужем временском периоду "клонирали" сим картице за мобилне телефоне од којих је већина била власништво већ постојећих постпејд корисника, тако да је овом приликом нанета имовинска штета домаћим мобилним операторима у укупном износу од 62.800.405 динара. Овако "клониране" картице користиле су се за позивање високотарифних сервиса (хотлајн сервиси, сервиси за забаву и друго) који се налазе углавном у државама континента Африке, а неки и у Молдавији и Украјини, чиме је овим сервисима неосновано омогућена наплата по основу непостојећих услуга. С обзиром на то да су позиви упућивани са бројева који припадају наведеним мобилним операторима, стварни власници картица нису имали сазнања о томе да су наведени сервиси позивани све до момента пристизања рачуна, које су им доставили мобилни оператери са којима су закључили уговоре о постпејд услугама. Код осумњичених Милана М. и Александра А. пронађени су хардверски и софтверски алати за клонирање сим картица, као и датотеке клонираних сим картица са којих су позивани високотарифирани сервиси у иностранству. Випе о овоме на: http://www.glas-javnosti.rs/clanak/hronika/glas-javnosti-15-12-2009/ojadili-operatere-za-68-miliona-dinara dostupan 20.05.2010.

комуникације[359]. У питању је неовлашћено пресретање приватних података (конвенција говори о нејавним) који се преносе (трансмитују) између два рачунарска система, садржинских података о комуникацијама, али и о саобраћају[360] укључујући ту и електромагнетну емисију са рачунара, који носи овакве податке[361]. Јавне трансмисије података и други начини прибављања оваквих података изостају из ове инкриминације. Под нејавном комуникацијом се према Објашњавајућем извештају о Конвенцији[362] подразумева она ситуација у којој је природа поступка трансмисије поверљива. Приватна индивидуална комуникација (као на пример слање и примање електронске поште или даунлоадовање са Интернет странице) се уопштено може сматрати нејавном. Конвенција оставља могућност државама да, овако дефинисано дело, услове постојањем намере. Као и у претходном случају, ова чињеница је битна, пре свега, због могућности да неко без свог знања, или бар без икакве намере, дође у посед туђих података на рачунарској мрежи. Предмет заштите је интегритет нејавних комуникација.

Значајно је поменути да је примена овог дела веома ограничена из разлога што је инкриминација фокусирана на пресретање процеса трансфера, па тако не може бити проширена и на моменат када лице, које пресреће трансфер података похрањује исте на неком медијуму. Инкриминише се само поступак пресретања трансмисије података а не и њихово архивирање. Пример за пресретање дају нам „ки логери“ и „скрин логери“. Посебан проблем постоји у случајевима када се пресретање података не врши техничким средствима – јер се ово дело може дефинисати и као сваки облик прибављања података у поступку трансфера, али чл.3. не покрива акте социјалног инжењеринга[363], те се, према томе, овако остварена дела не могу убројати у дела која покрива чл. 3.

Први облик овог дела чини оно лице које се, кршећи мере заштите, неовлашћено укључи у рачунар или рачунарску мрежу, или неовлашћено приступи електронској обради података, казниће се новчаном казном или затвором до шест месеци. Радња првог облика састоји се у неовлашћеном укључивању у рачунар, кршењем мера заштите, или у неовлашћеном приступу ЕОП –у. Други, квалификовани, облик чини лице које употреби податак добијен на претходно описан начин, казниће се новчаном казном или затвором до две године. Као још тежи облик јавља се случај ако је услед дела дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже или

---

359 Овај облик дела у нашем законодавству је веома палијативно регулисан чл. 143. – гони се по приватној тужби (осим у ст.3. када то чини службено или војно лице), чл.301. КЗ, , чл.302. (уз постојање неког облика заштите), чл.304. (без заштите), посредно и 304а. евентуално чл.315. тек се неким подзаконским актима и предлозима закона покушава подробније и конкретније регулисати ова материја.

360 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p.16. доступан 01.06.2010.год.

361 Чл.3. Конвенције. Овде може бити речи и о бежичним уређајима, али и другим облицима анализе електромагнетне емисије коју рачунари одају о својим операцијама. Према неким изворима један од обавештајних извора података у хладном раду представљале су електромагнетне трансмисије рачунара, на основу којих се могла дешифровати садржина података који су у рачунарима у том тренутку обрађивани.

362 Explanatory report nr.60.

363 У случајевима када извршилац наведе различитим методама лице да му сâмо ода поверљиве податке.

су наступиле друге тешке последице, учинилац ће се казнити затвором до три године.

Објекат заштите овог кривичног дела су заштићени рачунари или рачунарске мреже, односно, подаци који се електронски обрађују. Последица кривичног дела је неовлашћено укључивање или приступ, односно, употреба тако добијеног податка. Ово кривично дело има веома интересантан савремени облик. Наиме, проблем крађе бежичне Интернет конекције може се подвести под ову инкриминацију. С обзиром да се савремени АДСЛ или кабловски Интернет пакети нуде уз модеме који садрже и бежичне WLAN предајнике, а уз дате постоји нашироко позната корисничка шифра и име за дате уређаје (нпр. админ, админ) неопходно је увести обавезу пружаоца услуга (провајдера) да едукује своје кориснике у овом правцу. Чак, и уколико власник не заштити овакву конекцију, различитим корисничким именом и шифром, како би спречио другог да је користи, ово кривично дело могуће је извршити било којим уређајем, који садржи пријемник и предајник бежичне конекције (смарт телефон, лап топ (ноутбук), али и десктоп рачунар са бежичном картицом, па чак и мултимедијални стерео уређај). Неопходно је да код извршиоца постоји свест да неовлашћено користи – укључује у рачунар, кршењем мера безбедности, или неовлашћено приступа ЕОП. Уколико власник посебно заштити ову конекцију[364], сваки уређај и програм, који се користи да би се оваква конекција преузела од стране лица које га контролише, учествује у извршењу кривичног дела. Уколико немамо заштиту а последица кривичног дела постоји, онда је реч о делу из чл. 304. КЗ РС. (али се оно гони по приватној тужби).

Облик крађе услуга вајерлес технологије и Интернет услуга дефинисан као Wardriving[365] кажњив је, рецимо, у Немачкој само у случајевима када је бежична (вајерлес) локална мрежа заштићена ВПА шифровањем (WPA encoding), док у свим осталим случајевима није[366]. Посебну тешкоћу можемо препознати у употреби различитих оруђа да се, овим путем, дође и до одређених података са рачунара (или, просто, пресретањем сесије на Интернету) оштећеног лица преко

---

[364] Посебно треба поменути на пример да се још у неким државама, поред наше, случајеви без постојања неког облика заштите не гоне по службеној дужности. Код нас је у питању кривично дело из чл.304. Такозвани недозвољени електронски приступ (пролаз) из чл. 202а Немачког Казненог законика који подразумева неовлашћено коришћење Интернет услуга путем недозвољеног приступа провајдеру (односно тачкама приступа). Интересантно је да се за ово кривично дело тражи да није нанета штета, јер би онда представљало неко друго дело. Чл.202б. се односи на пражњење фондова или пресретање поверљивих података, путем на пример Wardriving-а. Уз поменуто веома је значајно инкриминисање и припремних радњи за вршење ових дела, па на пример, прибављање програма, којима би се ова дела могла вршити, програмског тројанског оруђа „Шарк“ (ајкула) би представљало кажњиво дело. Подаци прибављени интервјуом са начелником Бајернске јединице за ВТК.

[365] Облици напада на бежичне (вајерлес) локалне мреже (WLAN) веома су широки простори за нападе на ове облике телекомуникација, неки од уобичајених су прислушкивање, анализа комуникацијског саобраћаја, манипулација подацима, напади на клијенте вајерлеса, противправно одузимање и злоупотреба бежичног интернета (wardriving), типовање (и буквално обележавање) оваквог места са којег се може бесправно користити ова услуга (war-chalking) новији облик овог случаја је у развијеним земљама примена техничких и превозних средстава – према којим се региструју буквално стотине оваквих места приликом летења на висинама од 500 – 800 m висине (warflying).

[366] Дакле, када је отворена мрежа, јавна и јавно отворено доступна, и када није злоупотребљена у било ком другом виду.

овакве крађе информација, као и остваривања тежег облика кривичног дела у употреби таквих података. У сваком од описаних случајева доказивање иде од утврђивања начина приступа, утврђивања и прецизирања уређаја, који је, том приликом, коришћен. Неопходно је установити тачан начин на који је извршено укључивање у рачунар или приступ електронској обради података, као и како је и на који начин тај податак употребљен. Такође, неопходно је прецизирање софтверског пакета, па све до индивидуализације и директног повезивања одређеног лица са овим средствима и његовог лоцирања на датом месту и у времену, када је дело извршено. У сваком конкретном случају потребно је прецизно утврдити које мере заштите су кршене и на који начин, што представља битно обележје овог кривичног дела. Посебно питање је питање прибављања информација (корисничких имена и шифара) за извршење овог кривичног дела, као и њихово даље препродавање и нуђење на продају. Ове радње нису инкриминисане као посебна кривична дела, а могу представљати посебне облике крађе идентитета. Нарочита пажња мора се обратити утврђивању постојања последице и њене тежине јер од тога зависи квалификовање дела.

Извршилац кривичног дела може бити свако лице, а у погледу виности потребан је умишљај. Извршилац мора имати свест да се врши неовлашћено укључење у рачунар или рачунарску мрежу, да се употребљава податак добијен на овакав начин и да, услед тога, могу наступити наведене последице[367]. Извршилац кривичног дела из става 2. може бити и лице које је извршило дело из става 1. али то може бити и свако друго лице које је дошло у посед података. Уколико је исто лице предузело радње из става 1. и 2. тада постоји кривична одговорност тог лица само за став 2. с обзиром на то да радње из става 1. представљају само припремне радње за извршење основног кривичног дела, у овом случају постоји случај конзумпције у оквирима привидног идеалног стицаја (супсидијаритет, конзумпција и као посебан облик конзумпције инклузија) [368]. С обзиром на то да приступ заштићеном рачунару и заобилажење постављених баријера не захтева претерано високо познавање функционисања рачунара и мрежа, као и да на Интернету постоје различити уређаји и програмски пакети, који нуде брзо и лако остваривање бића овог дела, можемо закључити да извршилац овог кривичног дела може бити скоро свако лице, које поседује омањи фонд стручних информатичких знања.

За квалификацију кривичног дела је потребно утврдити време, место и начин извршења кривичног дела и каква је овлашћења имао извршилац, јер само лице које није овлашћено да се укључи у рачунар или приступи електронској обради података може бити извршилац првог облика овог кривичног дела. Извршилац другог облика кривичног дела може бити свако лице, јер појам овлашћености приступа или укључивања не мора у себи садржавати и дозволу да се такав податак употреби. За доказивање тежег облика кривичног дела потребно је на неспоран начин утврдити да ли је услед радњи првог облика дела дошло до застоја, или озбиљног поремећаја, у функционисању електронске обраде и преноса података или мреже, у чему се огледа тај застој, или поремећај, функционисања или које су то друге тешке последице које су наступиле[369].

---

367 Лазаревић, Љ, *Op.cit.*., стр. 750.

368 Герке, М и др., *Op.cit.*., стр.125.

369 *Ibid.*

Осуде извршилаца оваквих кривичних дела на затворске казне у дугом трајању и изрицање високих новчаних казни не одвраћају хакере од изазова, који представља упад у добро чуване системе. Иако, до сада, није било потврђених упада у системе наших државних органа, институција од јавног значаја, државних предузећа и дугих предузећа која обављају делатности од општег значаја, не значи да овакви напади нису покушавани или да их неће бити. Искуство развијених земаља нам говори да не постоји нити један непробојан систем нити препрека коју хакери не могу да заобиђу.

Кривично дело из чл. 302. КЗ, према начину извршења, може бити слично кривичном делу ***Шпијунажа*** из члана 315. КЗ, које спада у групу Кривичних дела против уставног уређења и безбедности Републике Србије, уколико би у питању били војни, економски или службени подаци или докумената који су законом, другим прописом или одлуком надлежног органа, донетим на основу закона, проглашени тајним. Одавање таквих података могло би да проузрокује штетне последице за безбедност, одбрану или за политичке, војне или економске интересе земље. Због тога је важно да се у сваком конкретном случају утврди умишљај учиниоца кривичног дела, значај заштићеног рачунар или рачунарске мреже који су били предмет напада, као и природу података који би били прибављени на такав начин. Наравно, у оваквом случају ова дела би била предмет обраде припадника БИА или ВОА (или ВБА), а чија овлашћења и околности поступања по криминалитету су већ раније била објашњена.

6.6 Спречавање и ограничавање приступа јавној рачунарској мрежи

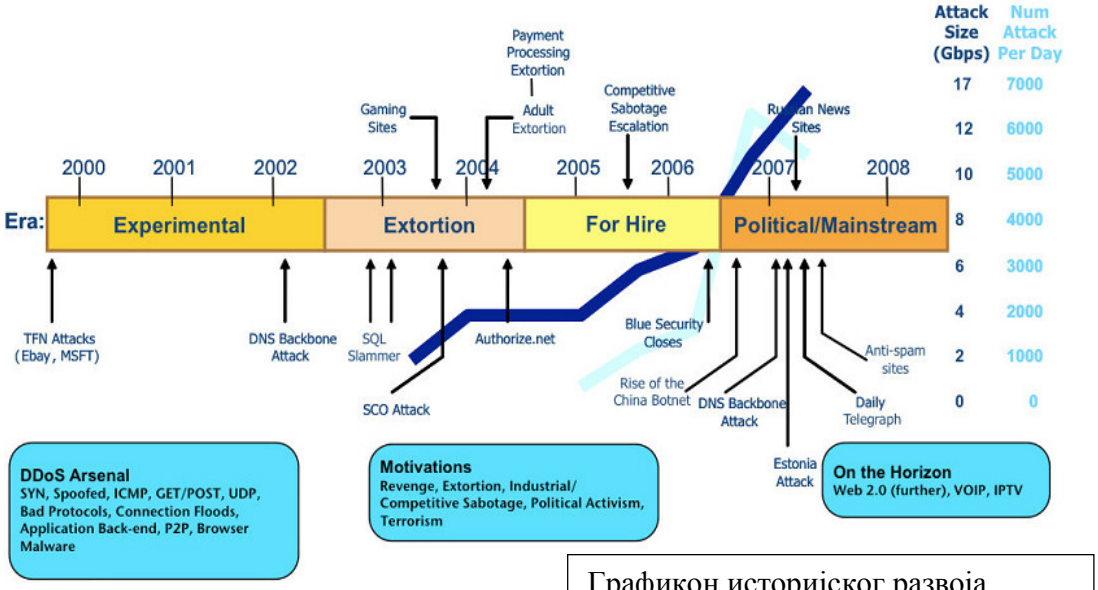
Први облик чини онај ко неовлашћено спречава или омета приступ јавној рачунарској мрежи (новчана казна или затвор до једне године). Квалификован облик постоји ако дело учини службено лице у вршењу службе (затвор до три године). Кривични законик у члану 112. тачка 18. дефинише јавну рачунарску мрежу као скуп међусобно повезаних рачунара који комуницирају размењујући податке. Спречавање приступа јавној мрежи представља потпуно онемогућавање другог лица да се користи јавном рачунарском мрежом, док се под ометањем подразумева свако отежавање приступа таквој мрежи. Извршилац овог кривичног дела мора поступати неовлашћено, а уколико је постојао правни основ онда не постоји ово кривично дело.

Објекат заштите овог кривичног дела представљају јавне рачунарске мреже, доступне неограниченом броју лица, а које грађани користе у свакодневном животу за информисање, обављање финансијских трансакција, електронску трговину или одржавање друштвених контаката. Дакле, није реч само о Интернету, као глобалној мрежи, већ и о другим врстама мрежа – интранет, ВПН и сл.

Извршилац овог кривичног дела може бити свако лице и мора поступати са умишљајем. Кривично дело је свршено кад је од стране неког лица предузета било која радња којом се спречава или омета приступ јавној рачунарској мрежи, као и

када дело изврши службено лице у оквиру вршења своје службене дужности, наравно, неовлашћено.

За квалификацију овог кривичног дела неопходно је утврдити следеће чињенице: непостојање овлашћења, односно непостојање правног основа за спречавање или ометање приступа, време и место извршења кривичног дела, начин на који је извршено спречавање или ометање, као и својство мреже, односно да ли је у питању јавна рачунарска мрежа. За доказивање другог облика кривичног дела, потребно је утврдити својство службеног лица извршиоца и радњу коју је он предузео. Веома је значајно обратити пажњу да ли је наведено кривично дело извршено у функцији неког другог кривичног дела или је праћено још неком радњом која, по својим елементима, представља биће неког другог кривичног дела, у ком случају се поставља питање њиховог међусобног односа и повезаности[370].



Графикон историјског развоја

Илустрација

Један од најчешћих начина спречавања или ограничавање приступа јавној мрежи представљају такозвани DoS (енгл. Denial of service) и DDoS (енгл. Distributed Denial of Service) напади. Историјски приказ развоја ових напада приказан је на графикону[371]. Организовању оваквих напада претходи стварање тзв. ботнета – мреже заражених рачунара, која настаје тако што се, помоћу одређеног малициозног софтвера, остварује контрола над великим бројем рачунара. Нападачи[372] претражују Интернет, проналазе рачунаре који нису адекватно заштићени и у њих убацују наведени софтвер. Број заражених рачунара може бити

370 *Ibid*.

371 Јасно се може видети правац трендова – 2000 – 2002.год. експериментални напади, затим 2003 – 2004.год. изнуде, 2005 – 2006.год. плаћенички напади и од 2007.год. политички и мејнстрим напади.

372 То могу бити власници ових ботнетова, ботхерди креатори злонамерних софтверских програма који су створили ботнет, али и друга лица која закупљују услуге ботхерда.

и неколико хиљада нпр. код DDOS напада. После преузимања контроле нападач издаје команду рачунарима у мрежи да на одређени сервер пошаљу велики број комуникационих захтева, чиме се саобраћај комуникационих портова, код рачунара жртве, загушује и тиме онемогућује приступ мрежи и услугама које она пружа. Историјски развој DDoS приказан је на графикону. Ту су приказани и могући мотивациони снопови извршилаца, као и историјски развој количинске квантификације напада у Гигабитима у секунди.

Нарочито опасну врсту представљају ПDOS напади (енгл. Permanent denial of service) који могу да трајно оштете хардвер на серверима са даљинским приступом. Напад се заснива на искоришћавању „firmware apdejta“[373] који се серверима шаље преко мреже или Интернета, а који је способан да превари хардвер и флешује (енгл. flash) било који део система, што би могло довести до трајног и потпуног хардверског пада[374].

Као што група аутора у монографији наводи[375], оваква активност може се одредити као рачунарска саботажа, приклањамо се овом мишљењу услед тежине последица које овакви напади могу имати. Лоше уписивање фирмвера или уписивање погрешног или неисправног фирмвера обично значи „клиничку смрт” за уређај и захтева посебне интервенције стручних сервисера[376]. Посебан облик у најновије време представљају TDoS[377] напади телекомуникациона одбијања пружања услуга у којима су извршиоци компромитовали рачуне корисника, након чега контактирају финансијске институције и мењају податке о датим корисницима добијајући на тај начин прикривену анонимност – потпуно нови дигитални идентитет. Ови напади су коришћени да друге жртве приморају путем безбројних позива упућених према одређеним лицима (телефонским бројевима или контактима) на промену бројева. Управо то су и биле жртве чији се дигитални идентитет крао, јер се на овај начин – променом дигиталног идентитета и недоступношћу на пружене бројеве телефона избегава могућност да финансијске компаније провере бонитет купаца или продаваца на неком од комерцијалних сајтова, као што је ибеј (eng. ebay).

6.7 Неовлашћено коришћење рачунара или рачунарске мреже

---

373 Термин фирмвер (енг. firmware) означава скуп програма, фабрички уграђених у хардверске уређаје и компоненте. Временом произвођачи опреме проналазе боља софтверска решења за функционисање тих уређаја. Поступак замене постојећег фирмвера новим назива се флешовање.

374 “Denial-of-service attack”, Wikipedia, Internet, http://en.wikipedia.org/wiki/Denial-of-service_attack, 07.05.2009

375 Комлен Николић, Л. *Op.cit.*. стр.108.

376 Živković, B. „Operacija visokog rizika“, Svet kompjutera, Internet, http://www.sk.co.yu/2004/09/skse01.html, 07.05.2009. Наведено према Комлен Николић, Л. и др. *Op.cit.*.

377 http://www.ic3.gov/media/2010/100621.aspx доступан 23.06.2010.год.

Конвенција ЦЕТС 185 предвиђа кривично дело под називом ***Злоупотреба уређаја***[378]**.** Озбиљност појаве различитих уређаја високих технологија који омогућавају корисницима остваривање разноликих злоупотреба овакве технологије бива предмет ове инкриминације. Вршење најразличитијих дела, која са собом носе веома вициозне и подмукле начине остваривања последице кривичних дела омогућава се оваквим уређајима. Овде лежи *ratio* инкриминације кривичног дела. Државе – потписнице преузимају на себе обавезу[379] да казне сваку намерну илегалну производњу, продају, поседовање, давање на употребу или набавку, као дистрибуцију и сваки други облик чињења доступним неовлашћеним лицима било ког „уређаја", под којим се подразумевају и рачунарски програми (дизајнирани или адаптирани примарно за сврху извршења неког дела из чл. 2. Конвенције), рачунарске шифре, шифре за приступ, као и било који други сличан облик података помоћу којих се могу извршити кривична дела наведена у претходним члановима Конвенције (2-5). Конвенција допушта државама да ставе резерву на овај члан, осим овог кривичног дела постоје и друге инкриминације, када је реч о продаји или другом облику дистрибуције лозинки или других рачунарских података помоћу којих се могу учинити наведена дела. На овај начин се „уређаји" можда и неправедно стављају у други план, али се и државама оставља да саме одреде домашај поменутог принципа по којем нема кажњавања без (јасно) инкриминисаног кривичног дела[380].

У прилог даљем разматрању ове проблематике је и чињеница да у ЕУ постоје тенденције у за инкриминацијом припремних радњи тежих кривичних дела ове врсте[381]. Значајно је изнети и да је овако широк круг радњи којима је дефинисано дело сличан ономе у ЕУ, али су тамо радње ограничене на уређаје који су креирани за превазилажење технолошких и техничких мера заштите[382]. Овако дефинисана проблематика у Конвенцији је веома вешто упакована и представља Комбинацију ограничења на уређаје којима је основна сврха извршење оваквих кривичних дела, уз комбиновање са психичким елементом „уз постојање намере да се исти користе за вршење дела из чл. 2-5 Конвенције".

Основни проблем који се може појавити у вези примене ове одредбе Конвенције је доказ да је интеракција остварена на Интернету, уз умишљај и постојање намере да ће исти бити коришћени у вршењу кривичних дела, јер само поседовање ових уређаја не садржи у себи и намеру која се тражи. Ово се, дакле, оставља свакој држави да сама регулише својим материјалним правом.

Другу групу инкриминисаних дела поједини аутори[383] с правом називају високотехнолошком варијантом класичних кривичних дела. Она по конвенцији бива група дела везана за рачунаре и обухвата два дела: фалсификовање и превару[384].

---

378 Ово дело регулише члан између осталог и 304а КЗ РС

379 Чл.6. Конвенције.

380 Комлен Николић, Л. Op. Cit. стр. 45.

381 Оквирна одлука Европске комисије ABI EG бр. L149, 02.06.2001.

382 Директива 29/2001 ЕЦ Европског Парламента и Савета 22.05.2001.

383 Комлен Николић, Л. и др. *Op.cit.*. Стр. 45.

384 Чланови 7. и 8. Конвенције.

У нашем законодавству у првом облику ово кривично дело чини оно лице које неовлашћено користи рачунарске услуге или рачунарску мрежу у намери да себи или другом прибави противправну имовинску корист. За ово дело запрећена је новчана казна или затвор до три месеца. Такође, је предвиђено да се гоњење за ово дело предузима се по приватној тужби. Радња кривичног дела је одређена као неовлашћено коришћење рачунарских услуга или рачунарске мреже. Ово је сувише широко постављена формулација, што може довести до значајних злоупотреба. За постојање овог кривичног дела је неопходно утврдити и намеру извршиоца да себи или другом прибави противправну имовинску корист. Извршилац може бити свако лице, а у погледу виности потребан је директан умишљај[385].

И у случају овог кривичног дела овлашћена службена лица дужна су да предузму радње из своје надлежности и да прикупе потребне доказе, уколико постоје основи сумње да је у вези радњи које спадају у ово кривично дело извршено и неко друго кривично дело за које се гоњење предузима по службеној дужности, у ком случају за то дело важе овлашћења и одредбе које се односе на подношење кривичне пријаве[386].

Поред описаног постоји и обавеза да се оштећеном и у случају дела које се не гони по службеној дужности учине доступним подаци о извршиоцу како би се могло остварити гоњење по приватној тужби. Веома је значајно да приметимо да се и код нас, као и Немачкој, не гони по службеној дужности ово дело. Такође, може се размотрити и случај у којем се користи бежична интернет локална мрежа WLAN са постојећом фабричком заштитом у којој је и корисничко име и шифра исто = admin. У овим познатим случајевима заштита постоји, али је позната скоро већини људи па се поставља питање њене сврхе, као и значаја. Мишљења смо да и у овом случају (ако извршилац искористи ову околност а оштећени није мењао фабричку шифру) постоји кривично дело из чл. 302. КЗ.

Посебан проблем је актуелни случај Гугла (Google) који је у склопу своје кампање Гугл стрит вјуа (eng. Google street view) и истоимене апликације на Интернету успео да сними одређене садржаје у 40 држава света. Снимање се односило на бежичне комуникације, уређаје и адресе, и заштићених и незаштићених извора, али чак и на делове садржине коминкација[387]. Значајно је да се ово дешава још од 2007. год. Ово дело би могло бити примењиво и на овај случај уколико је и код нас снимана комуникација у склопу описане кампање. Највећи комплекс проблема код овог кривичног дела постоји у његовој концепцији у нашем правном систему. Наиме, веома је тешко очекивати од обичног грађанина који није ни подучен а ни делимично упућен у ИТ технологије, од стране пружаоца услуга, како би заштитио сопствене уређаје од оваквих облика напада. Следећи проблем је околност по којој дати грађанин није ни стручно верзиран како би препознао постојање оваквог напада или приметио трагове које он за собом оставља. Оваква ситуација са собом носи даљу проблематику очувања испаривих

---

385 Лазаревић, Љ, *Op.cit.*., стр. 751

386 Герке, М и др., *Op.cit.*., стр.128.

387 Више на: http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html, и на: http://www.guardian.co.uk/tec hnology/2 010/may/15/google-admits-storing-private-data, оба последњи пут приступљена 08.06.2010.год.

(краткотрајних) података, којима се ово дело може доказати, питање ко, на који начин, како и када може захтевати примену мера којима се дати подаци могу обезбедити. На крају постоји и проблем трошкова које би појединац у датом случају имао од плаћања услуга које би пратиле описане мере до саме судске таксе која се у случају приватне тужбе мора платити (и евентуално ангажовање адвоката који је стручан у овој области).

У разматрање у оквиру ВТК могу ући и кривична дела из главе XVII Кривичног законика, уперена против части и угледа, а за која се гоњење, такође, предузима по приватној тужби

Интернет простор је изузетно окружење за вршење кривичних дела против части и угледа, односно кривичних дела *Увреда* – члан 170, *Клевета* – члан 171 и *Изношење личних и породичних прилика* – члан 172. кривичног законика, као и *Повреда угледа због расне, верске, националне или друге припадности* – члан 174. Свакодневно се на Интернету, неовлашћено, објављују различите експлицитне фотографије или видео записи јавних личности, као и пикантни детаљи из њиховог интимног живота. Такође, рачунарске мреже користе се и за вређање других, изношење неистинитих чињеница које могу штетити нечијем угледу или части. Ова кривична дела доживљавају своју експанзију и имају веома плодно тле у сајбер простору, како због веома великог потенцијалног аудиторијума, тако и због могућности несметане анонимности извршиоца. Са друге стране постоји и питање одговорности лица која своје експлицитне фотографије и друге облике записа са „осетљивим“ садржајима објављују на Интернету (па ма колико ограничена јавност у том смислу била).

Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података
члан 304а[388]

У ставу 1. овог члана начин извршења овог кривичног дела дефинисан је на следећи начин: „Ко поседује, прави, набавља, продаје или даје другом на употребу рачунаре, рачунарске системе, рачунарске податке и програме ради извршења кривичног дела из чл. 298. до 303. овог законика казниће се затвором од шест месеци до три године”. У ставу 2 предвиђено је да ће се предмети из става 1 овог члана одузети.

Прво кривично дело овог облика рачунарског криминала у Србији откривено и расветљено је дана 11. марта 2011.године. Званично саопштење МУП РС: Број: 100 /11, Служба за борбу против организованог криминала у сарадњи са Вишим јавним тужилаштвом у Београду, лишили су слободе Атилу Алађана (1984) из Суботице, због основа сумње да је извршио кривична дела прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података; прављење и уношење рачунарских вируса; рачунарска превара и прање новца.

Осумњичени Алађан је јуна 2010. године купио рачунарски вирус, потом га сачувао на закупљеном серверу а затим га је путем Интернет мреже унео у преко 1000 рачунара широм света, стварајући такозвану "ботнет" мрежу којом је управљао са свог сервера.

---

[388] Овај члан унет је чланом 119. Закона о изменама и допунама КЗ.

Користећи заражене рачунаре, осумњичени се регистровао на торент сајтовима и постављао фајлове са називима филмова, који у себи нису садржавали филм, већ рекламу која је упућивала на Интернет сајт који је креирао осумњичени, како би се преко њега преузимали софтверски садржај, лажно приказујући чињеницу да је садржај постављеног фајла филм. Овако нерегистровану услугу Алаћан је наплаћивао од једне канадске компаније коју је довео у заблуду и од ње за девет месеци наплатио преко свог девизног рачуна износ од преко 70.000 америчких долара, знајући да та средства потичу од недозвољене рачунарске мреже сачињене од заражених рачунара којима је осумњичени управљао.

Осумњичени је, уз кривичну пријаву, приведен надлеженом истражном судији Вишег суда у Београду.

На напред наведени начин законодавац је омогућио кривично правну заштиту платних картица, али и свих других одговарајућих предмета – објеката кривичних дела из групе о безбедности рачунарских података и створио правне оквире за ефикасно спречавање ових кривичних дела а, уједно, и елегантно инкриминисао припремне радње за вршење ових дела, а посебно за дела која у себи носе елементе крађе идентитета.

7. КРИВИЧНА ДЕЛА ПРОТИВ УСТАВНОГ УРЕЂЕЊА И БЕЗБЕДНОСТИ РЕПУБЛИКЕ СРБИЈЕ

Ова дела могу бити предмет разматрања у оквирима ВТК само ако се због начина извршења или употребљених средстава могу сматрати кривичним делима која спадају у оквире овог облика криминалитета.

7.1 Признавање капитулације или окупације

Грађанин Србије који потпише или призна капитулацију или прихвати или призна окупацију Србије или појединог њеног дела, казниће се затвором најмање десет година.

По правилу акт потписивања капитулације није акт који се може извршити путем активности на Интернету али је могуће документовати припремне радње код оваквог дела објављивањем појединих манифеста или других докумената на Интернету. Са друге стране признавање капитулације је овим путем могуће. У погледу извршења оваквих кривичних дела значајна карактеристика везује се за извршиоца. По правилу то може бити само одређено службено лице које је овлашћено да представља Републику Србију и у том смислу да је Уставом и законом овлашћено да предузима акте који производе одређена правна дејства у међународном јавномм праву.

7.2 Напад на уставно уређење

Ко силом или претњом употребе силе покуша да промени уставно уређење Србије или да сврге највише државне органе, казниће се затвором од три до петнаест година.

По природи ствари, није могуће да се преко Интернета силом покуша промена уставног уређења, али је могуће да се овим путем прети употребом силе у покушају свргавања највиших државних органа или у покушају промене уставног уређења. Код оваквог кривичног дела неопходно је у циљу доказивања утврдити сајтове на којима је оваква активност вршена, недвосмислено повезати извршиоца и рачунар, или сличан уређај, до којег води ИП адреса са које је комуникација вршена односно претње или припреме за промену уставног уређења вршене и свргавање државних органа планирано.

7.3 Позивање на насилну промену уставног уређења

Први облик чини онај ко, у намери угрожавања уставног уређења или безбедности Србије, позива или подстиче да се силом промени њено уставно уређење, сврgну највиши државни органи или представници тих органа, казниће се затвором од шест месеци до пет година.

Ко први облик учини уз помоћ из иностранства, казниће се затвором од једне до осам година.

Ко у намери растурања израђује или умножава материјал који је по свом садржају такав да позива или подстиче на вршење првог облика или ко упућује или пребацује на територију Србије такав материјал или држи већу количину тог материјала у намери да га он или неко други растура казниће се затвором од три месеца до три године.

Поред описаних околности у претходном члану на ово дело се може применити у циљу доказивања дела и околност документовања трансмисија различитим путевима, П2П или торент клијената, па чак и уз заштићене облике дељења ових материјала. Од великог значаја је у оваквим случајевима примена различитих форензичких алата, како оних који су комерцијални (ncase, Analyst notebook) тако и оних тзв. отворних извора (*open source*). Шта више у страној литератури се препоручују комбиновања различитих комерцијалних и отворених (свима доступних) софтверских апликација. Лог датотеке обе ове систематике служе и за међусобно контролисање прецизности ових апликација.

7.4 Шпијунажа

Ко тајне војне, економске или службене податке или документе саопшти, преда или учини доступним страној држави, страној организацији или лицу које им служи, казниће се затвором од три до петнаест година.

Ко за страну државу или организацију ствара обавештајну службу у Србији или њом руководи, казниће се затвором од пет до петнаест година.

Ко ступи у страну обавештајну службу, прикупља за њу податке или на други начин помаже њен рад, казниће се затвором од једне до десет година.

Ко прибавља тајне податке или документе у намери да их саопшти или преда страној држави, страној организацији или лицу које им служи, казниће се затвором од једне до осам година.

Ако су услед дела из ст. 1. и 2. овог члана наступиле тешке последице за безбедност, економску или војну моћ земље, учинилац ће се казнити затвором најмање десет година.

Тајним се сматрају они војни, економски или службени подаци или документи који су законом, другим прописом или одлуком надлежног органа донесеним на основу закона проглашени тајним, а чије би одавање проузроковало

или би могло да проузрокује штетне последице за безбедност, одбрану или за политичке, војне или економске интересе земље.

7.5 Одавање државне тајне

Ко неовлашћено непозваном лицу саопшти, преда или учини доступним податке или документе који су му поверени или до којих је на други начин дошао, а који представљају државну тајну, казниће се затвором од једне до десет година.

Ко другом лицу саопшти податке или документе за које зна да су државна тајна, а до којих је противправно дошао, казниће се затвором од шест месеци до пет година.

Ако је дело из става 1. овог члана извршено за време ратног стања, или ванредног стања или је довело до угрожавања безбедности, економске или војне моћи Србије, учинилац ће се казнити затвором од три до петнаест година.

Ако је дело из става 1. овог члана учињено из нехата, учинилац ће се казнити затвором од шест месеци до пет година.

Државном тајном сматрају се подаци или документи који су законом, другим прописом или одлуком надлежног органа донесеним на основу закона проглашени државном тајном и чије би одавање проузроковало или би могло да проузрокује штетне последице за безбедност, одбрану или за политичке, војне или економске интересе Србије.

Државном тајном, у смислу става 5. овог члана, не сматрају се подаци или документи који су управљени на тешке повреде основних права човека, или на угрожавање уставног уређења и безбедности Србије, као и подаци или документи који за циљ имају прикривање учињеног кривичног дела за које се по закону може изрећи затвор од пет година или тежа казна.

Посебно актуелна је ова проблематика у случају Wikileaks који је објавио поверљиве податке о комуникацијама дипломатских представништава САД у свету са централом. Услед актуелних истрага и поступака који се воде према извршиоцима ипак није могуће извести неке шире закључке о овако извршеним делима, па треба сачекати потпун завршетак свих процеса. Посебно треба имати у виду улоге цивилне контроле обавештајних служби и војске, у оваквим случајевима као и тзв. узбуњивача или пиштаљки (whistleblowers – a) обзиром да је поменути Wikileaks, до скора, имао ову улогу. У нашем правном систему ипак не би било већих проблема за гоњење ових НВО.

7.6 Изазивање националне, расне и верске мржње и нетрпељивости

Обзиром на обавезе везане за додатни протокол Конвенције о ВТК о коме је било речи, у Кривични законик уведене су инкриминације дела на која се протокол

односи. Радња извршења кривичних дела којима се шири говор мржње била је инкриминисана пре измена КЗ РС.

Први облик овог дела чини лице које изазива националну, расну или верску мржњу или нетрпељивост међу народима или етничким заједницама које живе у Србији. У другом ставу прописани су квалификовани облици кривичног дела и постоје када је оно учињено принудом, злостављањем, угрожавањем сигурности, излагањем порузи националних, етничких или верских симбола, оштећењем туђе ствари, скрнављењем споменика, спомен обележја или гробова. Ставом 3. прописан је најтежи облик када се дело из прва два облика врши злоупотребом службеног положаја или овлашћења или ако је услед тих дела дошло до нереда, насиља или других тешких последица за заједнички живот народа, националних мањина или етничких група у Србији.

Радња првог облика кривичног дела је одређена као изазивање мржње – стварање, до тада непостојеће, мржње, односно распиривање – развијање и продубљивање, већ постојећих осећања, а што се може постићи вређањем, исмевањем или потцењивањем националних, расних или верских осећања, излагањем порузи симбола, ниподаштавањем историјских, културних и других вредности[389]. Кривично дело постоји само уколико су побројане делатности усмерене на националну, верску или расну припадност, с тим што број лица према којима су радње предузете није од значаја – дело ће постојати ако је извршено и према само једном лицу.

Квалификаторне околности овог дела чине: начин извршења дела (а то може бити принудом, злостављањем, угрожавањем сигурности, скрнављењем споменика, спомен обележја или гробова, њиховим оштећењем) и својство извршиоца уз начин извршења, односно, постојање тежих последица као што су нереди или насиље.

Злоупотреба Интернета представља веома погодно средство за изазивање националне, расне и верске мржње. Извршиоци овог дела могу, уз мале трошкове, отворити веб сајт или да, потпуно бесплатно, направе блог, на којем, без икаквог ограничења, износе расистичке ставове, вређају или исмејавају друге народе и етничке заједнице, што за последицу може имати изазивање мржње или њено распиривање. Посредством Интернета овакви ставови могу доћи до неограниченог броја људи, што њихово деловање чини нарочито опасним. Кривично дело може извршити и само једно лице, али то, данас углавном, чине различита удружења и организације. Дефинисање и означавање организација које имају за циљ стварање националне, верске и расне мржње је веома тешко, а често се своди на питања дневне политике. При одређивању оваквих категорија, такође, се мора бити веома опрезан јер су веома танке и порозне границе између слободе изражавања сопственог мишљења и говора мржње.

У Србији постоји више организација и удружења грађана чије деловање и ставови које пропагирају може изазвати сумњу у погледу њихове легалности. Према подацима Министарства унутрашњих послова, на територији Србије у такве екстремистичке организације се убрајају „Национални строј“[390], „Крв и част“[391],

---

389 Лазаревић, Љ, Op.cit., str. 782.

390 http://nacionalnistroj.com/index.php доступан 20.05.2010.

391 http://www.bhserbia.org/uvod.htm доступан 20.05.2010.

„1389“[392], „Расни националисти-расоналисти“[393] и „Отачаствени покрет Образ“[394]. Скупштина Војводине је у децембру 2005. године усвојила закључак којим се од Владе Србије тражи забрана свих неонацистичких, расистичких и клерофашистичких група и организација на територији Србије. Уз то, од Владе Србије затражено је и да онемогући „оне активности „Омладинског покрета 64 жупаније“ које повређују интегритет Србије и вређају национална осећања грађана”. Усвојеним закључком затражена је и забрана скупова припадника свих војних формација из Другог светског рата које су сарађивале или биле део фашистичких окупационих снага, који представљају узнемиравање јавности, подстичу националне тензије и нису у складу са стремљењима Србије ка европским интеграцијама.

До сада није било забране нити једне организације због расистичких ставова или ширења верске и националне мржње, мада је Републичко јавно тужилаштво у октобру 2008. године упутило је иницијативу Уставном суду Србије за забрану рада и деловања организације „Национални строј“. Деловање сајтова националистичких организација и њихових форума се не може блокирати, јер су углавном регистровани на серверима у иностранству, а поједине државе не сматрају кажњивим оваква иступања, а уз то поједини сајтови омогућавају постављање странице са гаранцијом да је сервер анониман, што омогућује и анонимност ИП адресе. Ове организације најчешће своје сајтове постављају у САД, које због њихових законских одредби о слободи говора и изражавања одбијају да доставе податке о лицима која су их поставила или их администрирају[395].

С обзиром на деликатност овог проблема, потребно је бити веома опрезан приликом означавања неке организације као политичке или расистичке и у сваком конкретном случају утврдити околности које су пратиле извршење евентуалног кривичног дела, прикупити валидне доказе, али и утврдити умишљај учинилаца. Забрана рада неке организације може бити окарактерисана као ускраћивање политичких права и ограничавање слободе говора, па је потребно установити јасну разлику између политичких партија са екстремним ставовима од деловања организација, која могу имати негативну конотацију.

---

392 http://www.snp1389.rs/ доступан 20.05.2010.

393 http://srpskifront.com/ доступан 20.05.2010

394 http://www.obraz.rs/index1.htm доступан 20.05.2010.

395 Једна од најстаријих расистичких организација Кју клукс клан (енг. Ku Klux Klan), настала још у XIX веку и данас делује у САД, а своје ставове пропагира и преко Интернета. Ова организација заговара надмоћност „беле расе“ над осталим расама: црнцима и хиспано (Мексиканцима, Кубанцима, Уругвајцима и Порториканцима), као и антисемитизам, мржњу према католицима (ово се нарочито односи на имигранте из Пољске, Италије и Ирске) и хомофобију. Позната је по застрашивању и суровим егзекуцијама које су у прошлости спроводили њени чланови. Имала је велики број присталица, временом је њен значај опадао.“Ku Klux Klan”, Wikipedia, Internet, http://en.wikipedia.org/wiki/Ku_Klux_Klan, 20.05.2010. Актуелан сајт им је http://www.kkk.bz/ доступан 30.05.2010.

8. КРИВИЧНА ДЕЛА ПРОТИВ ЧОВЕЧНОСТИ И ДРУГИХ ДОБАРА ЗАШТИЋЕНИХ МЕЂУНАРОДНИМ ПРАВОМ

8.1 Расна и друга дискриминација[396]

Први облик у ставу 1 гласи „Ко на основу разлике у раси, боји коже, верској припадности, националности, етничком пореклу или неком другом личном својству крши основна људска права и слободе зајамчена општеприхваћеним правилима међународног права и ратификованим међународним уговорима од стране Србије, казниће се затвором од шест месеци до пет година.“. У ставу два је прописан други облик овог дела и састоји се у вршењу прогањања организација или појединаца због њиховог залагања за равноправност људи. У ставу 3 је прописан трећи облик који чини онај ко шири идеје о супериорности једне расе над другом или пропагира расну мржњу или подстиче на расну дискриминацију (затвор од три месеца до три године). У овом члану додати су и став 4 и став 5. Став 4 гласи: „Ко шири или на други начин учини јавно доступним текстове, слике или свако друго представљање идеја или теорија које заговарају или подстрекавају мржњу, дискриминацију или насиље, против било којег лица или групе лица, заснованих на раси, боји коже, верској припадности, националности, етничком пореклу или неком другом личном својству, казниће се затвором од три месеца до три године“. Ставом 5 је предвиђено следеће: „Ко јавно прети да ће, против лица или групе лице због припадности одређеној раси, боји коже, вери, националности, етничком пореклу или због неког другог личног својства, извршити кривично дело за које је запрећена казна затвора већа од четири године затвора, казниће се затвором од три месеца до три године.”

Наведеним кривично правним прописима, између осталог, инкриминишу се оне радње које су карактеристичне за говор мржње на Интернету, као што су јавно излагање порузи лица или групе због припадности одређеној раси, боји коже, вери, националности, етничког порекла или неког другог личног својства. Инкриминишу се и радње којима се изазива или распирује национална, расна или верска мржња или нетрпељивост међу народима или етничким заједницама које живе у Републици Србији. Предвиђено је као кажњиво и прогањање организација или појединаца због њиховог залагања за равноправност људи и ширење идеја о супериорности једне расе над другом, као и пропагирање расне мржње и подстицање на расну дискриминацију. Посебан значајна за спречавање говора мржње на Интернету је измена која је унета у чл. 387 у ставу 4 којом се прописује као кажњиво ширење и чињење јавно доступним текстова, слика или свако друго представљање идеја или теорија које заговарају или подстрекавају мржњу, дискриминацију или насиље, против било којег лица или групе лица, заснованих на раси, боји коже, верској припадности, националности, етничком пореклу или неком другом личном својству, казниће се затвором од три месеца до три

[396] Чланом 172. Закона о изменама и допунама кривичног законика од 31.08.2009. године извршене су измене и у члану 387.

године[397]. Такође се у ставу 5 овог члана санкционише јавна претња којом се наводи да ће се, против лица или групе лице због припадности одређеној раси, боји коже, вери, националности, етничком пореклу или због неког другог личног својства, извршити кривично дело за које је запрећена казна затвора већа од четири године затвора.

[397] Немци су 2009.год. отишли и даље у примени Конвенције о ВТК али и других аката који се односе на Тероризам и акте насиља, уводећи чл.89а, 89б и 91. Казненим Законником Немачке. Тиме се инкриминишу давања инструкција о прављењу бомби, експлозива, ватреног оружја нуклеарних и других радиоактивних направа, производња, продаја и чување као и сличне активности са овим предметима, похрњивање, примање и чињење доступним на други начин истих као и средства за вршење ових дела (чл.89а). Такође инкриминишу се и примања инструкција за вршење озбиљних и насилних напада којима се угрожава држава, установљавање и одржавање контакта са терористичким организацијама (чл.89б). Поред описаног сматра се кривичним делом и дисеминација – растурање писаних садржаја који садрже упутства за вршење насилних аката против државе.

З А К Љ У Ч А К

Овај текст је настао као резултат настојања да се одговори захтевима и потребама свакодневне праксе и обједини материјал неопходан за разумевање појединих сегмената борбе против криминалитета и практичних недоумица, које се могу јављати приликом поступања органа гоњења и суда у овој области. Наравно, поред ове основне циљане групе којој је намењен овај текст, он је занимљив и другим државним органима али и широј јавности. У последњем случају од значаја је чињеница да се, недвосмислено и јасно, омеђе границе надлежности и одговорности поступања државних субјеката и да иста логика буде доступна широј јавности. Не тако давно у наш правни систем уведене су одредбе којима се третирају прва дела ВТК, након чега су уследили и закони који се баве овом облашћу, али веома брзо дошло је, како до њихових измена, тако и до концепцијских и организационих измена у већини структура које се баве супротстављањем криминалитету. Оне и јесу биле израз вивидне и врло брзе еволуције ВТК у начинима обављања и вршења кривичних дела али и понашању извршилаца, њиховој стручној оспособљености, која је у овој области посебно значајна. Управо у овом циљу текст који је пред вама представља прво систематизовано обједињавање ресурса у области ВТК, без претензија да полаже право на апсолутну јединственост. Поред практичних кривично правних аспеката овај текст има и криминалистички значај, обзиром да је у приказаним делима објашњен значајан број криминалистичко тактичких и методичких поступања у циљу брзог, ефикасног, темељног и ефективног поступања органа гоњења у сврху расветљавања кривичних дела ВТК. Значајни аспекти дати су и у криминалистичким смерницама које суд има узети у обзир приликом утврђивања материјалне истине у предметима који за циљ обраде имају кривична дела ВТК. У смислу одржавања позитивних аспеката у доприносу потпуног утврђивања материјалне истине, овај текст даје значајне смернице и одбрани у циљу заштите слобода и права грађана оптуженог и окривљеног. У погледу садржаја везаних за дела описана у тексту неопходно је поменути да је коришћен материјал који је у датој материји доступан, уколико су дела постојећа у нашој пракси, а уколико нису коришћени су еклатантни примери из иностранства. Садржински нека дела су много више обрађена од других, а као разлог јавља се њихова актуелност у моментима док се овај рад синтетизовао. У тексту су приказана и кривична дела која би требало укомпоновати у наш правни поредак, обзиром на њихову сложеност и постојање потребе, а уз упоредно правни приказ њиховог статуса у релевантним правним системима. Указано је и на пропусте које је законодавац у нашем случају направио у датом временском моменту, као и на решења која је накнадно понудио изменама и допунама Закона о организацији и надлежности државних органа у погледу борбе против ВТК. На дато треба гледати као на оправдане облике еволуције материјалних, процесних и организационих прописа у овој области условљене проблематиком, преузетим међународним обавезама, али и уважавањем проблема насталих у судској пракси.

ВТК слови за један од најактуелнијих проблема у борби против криминалитета, о чему говоре и области које, према нашем позитивном законодавству обухвата. Стандардне границе између класичног, економског, еколошког или других облика криминалитета у зависности од класификационих основа све мање постоје а један од главних разлога јесте појава и развој ВТК. Приказана кривична дела која спадају у ВТК обухватају веома широк дијапазон различитих кривичних дела по значају, сложености, бројности објеката напада и пасивних субјеката, методима који се користе у извршавању кривичних дела. У овако представљеној проблематици неопходно је схватити да не могу само специјализовани субјекти бити једини носиоци борбе против ове области криминалитета. Значајно је препознати да у супротстављању могу учествовати све групе субјеката у супротстављању криминалу, од примарних до терцијарних субјеката (од оних којима је основна сврха и функција супротстављању криминалитету до оних којима то није ни споредна функција или сврха). У овој области од великог значаја је и подизање нивоа свести грађана о постојећим актуелним облицима кривичних дела па је и активност на превенцији свих органа од изузетног значаја. Тиме се на значају даје и, оним, крајњим корисницима могућим будућим жртвама, и постиже проактивно деловање ангажовањем заједнице и целокупног друштва и његових ресурса у супротстављању ВТК. Пружањем прилике сваком сегменту друштва да учествује у супротстављању овом облику криминалитета представља нов метод у борби против укупног криминалитета а који и јесте неминовност, обзиром да он и доноси нове облике и методе криминала и извршилаца. Овај текст представља један корак у том правцу.

Л И Т Е Р А Т У Р А

1. Quayle E., Loof, L. Palmer, T.: Child pornography and sexual exploitation of children online, ECPAT International, ECPAT International, Тајланд, 2009, p. 43.
2. Dixon, N.: „Catching 'Cyber Predators': the Sexual Offences (Protection of Children) Amendment Bill 2002 (Qld)", Research Brief No 2002/35, Queensland Parliamentary Library, Аустралија, 2002.
3. Wortley, R. Smallbone, S.: Child Pornography on the Internet, Problem-Oriented Guides for Police Problem Specific Guides Series No. 41, U.S. Department of Justice-Office of Community Oriented Policing Services, САД, 2006.
4. Athanasopoulos, E. Makridakis A. Antonatos, S. Antoniades, D. Ioannidis, S. Anagnostakis, K. G. Markatos, E. P. Antisocial Networks: Turning a Social Network into a Botnet, Section: Network Security, Lecture Notes In Computer Science, Berlin, Germany, p.146-160.
5. O'Connell, R.: A typology of cybersexploitation and on-line grooming practices, Cyberspace Research Unit, University of Central Lancashire, Велика Британија, 2003.
6. Forde P. и Patterson A. Трендови & проблеми у криминалу и кривичном правосуђу, Криминолошки институт Аустралије, бр.97. новембар 1998.
7. Ћировић, Д. Јанковић, Н. Лађевић, М. „Cyber podzemlje u Srbiji", *Репортер,* 16.11.2005. страна 12.
8. Герке, М. Ђокић, Д. Радуловић, С. Петровић З. Лазовић, В. Прах, Р. *Приручник за истрагу кривичних дела у области високотехнолошког криминала, Савет Европе, 2008.*
9. Комлен Николић, Л, Гвозденовић, Р. Радуловић, С. Милосављевић, А. Јерковић, Р. Живковић, В. Живановић, С. Рељановић, М. Алексић И.. Сузбијање вискотехнолошког криминала, Удружење јавних тужилаца и заменика јавних тужилаца, АЕЦИД 2010, Београд.
10. Кнежевић Ћосић, В. „Шведски пирати на нафтној платформи праве пиратску државу", *Борба*, 23.04.2009. Internet, http://www.borba.rs/content/view/5127/36/, 10.05.2009.
11. Наташа Делић, *Повреда проналазачког права и неовлашћено коришћење туђег дизајна (чл. 201. и 202 КЗС)*, Привреда и право, бр. 1-4, 2006,
12. Лазаревић, Љ, *Коментар кривичног законика Републике Србије,* Савремена администрација, Београд, 2006
13. Урошевић, В.: „Нигеријске преваре у Републици Србији", часопис Безбедност, број 3/09.
14. Chawki, M.: Nigeria Tackles Advance Fee Fraud, Journal of Information, Law & Technology, University of Warwick, 2009,
15. Smith, R. Holmes, M. Kaufmann, P.: Nigerian Advance Fee Fraud, Trends and Issues in crime and criminal justice, Australian Institute of Criminology, 1999,
16. Buchanan, J. Grant, A.: Investigating and Prosecuting Nigerian Fraud, United states attorneys bulletin, САД, 2001.
17. Глени, М. Мекмафија, Самиздат, Б92. 2008. Београд
18. Buchanan, J. Grant, A.: Investigating and Prosecuting Nigerian Fraud, United states attorneys bullet in, САД, 2001.

19. Longe, B. Chiemeke, C.: Cyber Crime and Criminality in Nigeria – What Roles are Internet Access Points in Playing?, European Journal of Social Sciences, 2008., p. 138.
20. Chawki, M.: Anonymity in Cyberspace: Finding the Balance between Privacy and Security, Revista da Faculdade de Direito Milton Campos, Nova Lima, Бразил, 2006.
21. Dyrud, M.: „I brought You a good news An analysis of Nigerian 419 Letters, Proceedings of 2005 Annual Association for Business Communication, Convention Association for Business Communication, САД, 2005.
22. Урошевић, В.: *Злоупотреба платних картица и рачунаркске преваре*, Правни информатор 9/2009, Београд,
23. Ивановић, З. Урошевић, В. *Улога интернета код ангажовања посредника у преузимању противправно прибављене робе и новца извршењем кривичних дела високотехнолошког криминала*, Гласник права, Крагујевац, бр.1. 2010.стр. 83-95
24. Милошевић М., Урошевић В.: *Крађа идентитета злоупотребом информационих технологија*, Безбедност у постмодерном амбијенту, Зборник радова књига VI, Центар за стратешка истраживања националне безбедности, Београд, 2009, стр. 53-64.
25. Урошевић, В. Уљанов, С.: „Утицај кардерских форума на експанзију и глобализацију злоупотребе платних картица на Интернету“, у: Журнал за криминалистику и право НБП, Криминалистичко-полицијска академија, Vol. XV, No. 2, 2010, Београд, 2010, стр. 13-24.
26. OECD Ministerial meeting on the future of the internet economy, Scoping paper on online Identity theft, Ministerial background report: DSTI/CP (2007)3/FINAL, може се пронаћи на сајту ОЕЦД. Материјал припремљен за 72. састанак овог тела, стр.17.
27. Jakobsson M., Myers S. Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft, 2007 by John Wiley & Sons, Inc. Hoboken, New Jersey.
28. The Phishing Guide Understanding & Preventing Phishing Attacks, NGSSoftware LTD, United Kingdom Sutton, 2006.
29. Furnell, S.M. Problem of categorising cybercrime and cybercriminals 2nd Australian Information Warfare and Security conference 2001.
30. Newman, G. R. McNally, M. M. Identity theft literature review, доступан на Интернету дана 12.01.2010.год. http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf стр.1.
31. Teri Bidwell: *Hack Proofing Your Identity in the Information Age* Syngress Publishing, Inc, 2002.
32. Internet related Identity theft, a discussion paper, prepared by Gercke, M. као део Project Cybercrime, Council of Europe, ECD, Directorate General of Human Rights and Legal Affairs. Доступно на Интернету: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp дана 20.03.2010.год.
33. Милошевић М., Урошевић В.: Крађа идентитета злоупотребом информационих технологија, Безбедност у постмодерном амбијенту,

Зборник радова књига VI, Центар за стратешка истраживања националне безбедности, Београд, 2009, стр. 53-64.
34. Прља, Д. Рељановић, М. *Високотехнолошки криминал – упоредна искуства, у* Страни Правни живот, бр.3/09, стр.161-184. Београд.
35. Peeters, M. Identity theft scandal in U.S.:Oportunity to improve Data Protection, MMR 2007.
36. Шабић, Р. Ревија за безбедност, бр. 6/09, Заштита нарочито осетљивих података о личности — нека отворена питања, стр.3-7.
37. Moore, R. Search and seizure of digital evidence, LFB Scholarly publishing inc, NY 2005. Str.46
38. Forde, P. and Armstrong, H. 2002, 'The Utilisation of Internet Anonymity by Cyber Criminals', Paper presented at the International Network Conference, 16-18 July, Sherwell Conference Centre, University of Plymouth, Plymouth.
39. Newman, G. R. McNally M. M. Identity Theft Literature Review U.S. Department of Justice. 2005, Prepared for presentation and discussion at the National Institute of Justice Focus Group, p. VI уводног дела.
40. Internet related identity theft, A discusion paper, Prepared by Marco Gercke, www.coe.int/cybercrime
41. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p.15. последњи пут приступљено 26.04.2010.год.
42. Урошевић, В. Ивановић, З. Злоћудни програми у ур. Оливера Лазаревић, ФОРУМ БИСЕЦ 2010 Конференција о безбедности информација стр.64-71 Београд Метрополитан универзитет, ФИТ, 2010.
43. Kizza J. M., Computer network security, Cyber crimes and Hackers,, 2005 Springer Science+Business Media, Inc, pp.155-6.
44. The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond A Joint Report of the US Department of Homeland Security – SRI International Identity Theft Technology Council and the Anti-Phishing Working Group. October, 2006 доступан на адреси www.antiphishing.org/reports/APWG_CrimewareReport.pdf
45. Berk, V. H. Cybenko, G. V. and Gray R. S. Early detection of active worms, Chapter 6.
46. http://www.youtube.com/watch?v=9g5IU3Th2wQ и http://www.youtube.com/watch?v=YX4P-KS-j6c&feature=related.
47. *The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond A Joint Report of the US Department of Homeland Security – SRI International Identity Theft Technology Council and the Anti-Phishing Working Group. October, 2006 доступан на адреси* www.antiphishing.org/reports/APWG_CrimewareReport.pdf *28.12.2009.год Živković, B. „Operacija visokog rizika“, Svet kompjutera, Internet,* http://www.sk.co.yu/2004/09/skse01.html

Интернет

48. http://conventions.coe.int/Treaty/en/Treaties/html/185.htm http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=189&CL=ENG
49. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CL=ENG,
50. http://www.cox.com/takecharge/safe_teens_2009/media/2009_teen_survey_internet _and_wireless_safety.pdf

51. http://www.smile29.eu/doc/DS29_EN. pdf
52. www.facebooksrbija.com/uhapsen-pedofil-sa-fejsbuka/informacije/135.html
53. "Three US ISPs agree to block child pornography sites", Tech Connect Magazine, Internet, http://www.tcmagazine.info/comments.php?id=20354&catid=6&highlight=child+pornography, http://sr.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB
54. http://www.cox.com/takecharge/safe_teens_2009/media/2009_teen_survey_internet_and_wireless_safety.pdf
55. http://www.sit.fraunhofer.de/Images/sc_iPhone%20Passwords_tcm501-80443.pdf
56. http://www.net-security.org/secworld.php?id=10570&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29 последњи пут приступљено истог дана.
57. http://www.01net.com/www.01net.com/editorial/528466/dailymotion-et-fuzz-reconnus-hebergeurs-par-la-cour-de-cassation/
58. http://en.wikipedia.org/wiki/Rainbow_Books доступан 28.06.2010.год. и http://en.wikipedia.org/wiki/IFPI последњи пут приступљени истог датума
59. "BitTorrent (protocol)", Wikipedia, Internet, http://en.wikipedia.org/wiki/BitTorrent_(protocol),
60. „Osuđeni osnivači Pirate Bay-a", BBC Serbian, Internet, http://www.bbc.co.uk/serbian/news/2009/04/090417_swedennetpiracy.shtml
61. www.torrentfreak.com/mininova-deletes-all-infringing-torrents-and-goes-legal-091126/ http://www.nytimes.com/2010/05/06/technology/06broadband.html?ref=technology
62. Пиратерија: на цени ноте и рецепти, Вечерње новости, 5.7.2011, интернет адреса: хттп://www.наслови.нет/2011-07-05/вецерње-новости/пиратерија-на-цени-ноте-и , 11.09.2011.
63. http://www.ic3.gov/
64. http://www.ic3.gov/media/2011/110901.aspx
65. http://www.ftc.gov/opa/1998/07/dozen.shtm
66. www.lookstoogoodtobetrue.com
67. http://www.ic3.gov/media/IC3-flyer.pdf
68. http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf
69. http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf
70. http://en.wikipedia.org/wiki/Spam_(electronic)#Origin_of_the_term
71. http://www.prevara.info/index.php?option=com_content&task=view&id=283&Itemid=7 http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf
72. http://www.sophos.com/blogs/gc/g/2010/01/04/bogus-fda-agents-scam-online-drug-purchasers/
73. http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf доступан 15.12.2009.
74. www.ic3.gov/media/initiatives/econbrief.pdf
75. www.ifccfbi.gov
76. http://sunbeltblog.blogspot.com/2011/03/samsung-laptops-do-not-have-keylogger.html http://www.networksolutions.com
77. http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

78. http://www.govinfosecurity.com/articles.php?art_id=2601
79. http://www.bankinfosecurity.com/articles.php?art_id=2667&rf=2010-06-21-eb
80. http://web.archive.org/web/20051029165224 /http://news.yahoo.com/s/latimests/20051020/ts_latimes/iwilleatyourdollars
81. http://www.bankinfosecurity.com/articles.php?art_id=3351&rf=2011-02-19-eb
82. http://en.wikipedia.org/wiki/ShadowCrew: dostupno na dan 16.04.2010. http://www.fbi.gov/pressrel/pressrel08/darkmarket101608.htm:
83. http://en.wikipedia.org/wiki/SQL.
84. Cybercrime: current threats and trends, Discussion paper, 2008. COE p.10., dostupan na adresi: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567%20study1-d-provisional%20_13%20Mar%2008_en.pdf http://www.websense.com/site/docs/whitepapers/en/Phishing%20and%20Pharming%202006%20Whitepaper%20(3).pdf
85. 1H2008: HU http://www.apwg.org/reports/APWG_GlobalPhishingSurvey1H2008.pdf http://www.blic.rs/Vesti/Hronika/196854/Ostao-bez-imovine-zbog-prevaranta-iz-Afrike
86. Threatsaurus,the a-z of computer and data security threats, p.61. Sophos. Доступан у дигиталном облику на: http://www.sophos.com/sophos/docs/eng/papers/sophos-a-to-z-computer-and-data-security-threats.pdf
87. http://sr.wikipedia.org/sr/Фишинг
88. Cybercrime current threats and trends COE, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study1-d-provisional%20_13%20mar%2008.pdf
89. http://www.antiphishing.org/
90. http://www.microsoft.com/protect/terms/socialengineering.aspx
91. http://www.sophos.com/blogs/gc/g/2010/05/31/viral-clickjacking-like-worm-hits-facebook-users/
92. www.ngsconsulting.com
93. http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBUQFjAA&url=http%3A%2F%2Fcode.google.com%2Fapis%2Fmaps%2Ffaq.html&ei=4EWnTIDSHYHqOaH6hZwM&usg=AFQjCNGe8vV-geAqBc--lH9ads4VJLZBUw&sig2=t1_8B10O4Dm9twiVK9j_tpA
94. http://en.wikipedia.org/wiki/Web_crawler.
95. http://en.wikipedia.org/wiki/Rendering_%28computer_graphics%29.
96. http://www.msnbc.msn.com/id/37943900/ns/technology_and_science-security/ http://www.computerworld.com/s/article/9178537/White_House_seeks_comment_on_trusted_ID_plan?taxonomyId=145 http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=225701456&cid=RSSfeed_IWK_News http://www.nextgov.com/nextgov/ng_20100628_8259.php?oref=topnews http://www.govinfosecurity.com/articles.php?art_id=2694 http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace http://www.dhs.gov/xlibrary/assets/ns_tic.pdf .
97. Secure Socket Layer, http://www.webopedia.com/TERM/S/SSL.html
98. http://www.zdnet.com/blog/security/zombie-pc-prevention-bill-to-make-security-software-mandatory/8487 .
99. http://www.mastercard.com/za/personal/en/education/fraud_protection.html
100. http://www.net-security.org/secworld.php?id=10731&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29
101. http://www.mailfrontier.com/docs/field_guide.pdf доступан 09.08.2011.
102. http://www.theregister.co.uk/2010/05/03/treasury_websites_attack/
103. http://www.symantec.com/business/theme.jsp?themeid=state_of_spam

104. http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_08-2011.en-us.pdf
105. http://www.junk-o-meter.com/stats/index.php.
106. Блиц онлине, Преко Гугла открила прељубу, http://www.blic.rs/zanimljivosti.php?id=86407, 20.10.2009. упоредити и са Прља, Д. Рељановић, М. *Високотехнолошки криминал – упоредна искуства, у* Страни Правни живот, бр.3/09, стр.161-184. Београд, на стр.170-172.
107. http://www.ftc.gov/privacy/glbact/glbsub1.htm
108. http://www.theregister.co.uk/2010/06/29/spy_ring_tech/
109. www.ftc.gov/opa/2006/12/fyi0688.htm.
110. http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%284CA02151F94FFB778ADAEC2E6EA865329~ID+Theft+Booklet +-+Protecting+your+Identity.PDF/$file/ID+Theft+Booklet+-+Protecting+your+ Identity.PDF.
111. Identity Theft Penalty Enhancement Act ("ITPEA") може се пронаћи на: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108. pdf.
112. www.consumer.gov/idtheft/pdf/penalty_enhance_act.pdf.
113. http://www.ag.gov.au/www/agd/agd.nsf/Page/Modelcriminalcode_IdentityCrimeDiscussion Paper-CopiesofSubmissionsReceived.
114. http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32347.html.
115. http://secondlife.com/ доступан 01.09.2011.год.
116. Internet related ID theft, Counsel Of Europe, str.7.доступно на Интернет страници
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf
http://www.law.cornell.edu/uscode/18/1028.html
117. http://www.sophos.com/blogs/duck/g/2009/12/14/facebook-privacy-video/
118. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf.
119. http://www.coe.int/t/dghl/cooperation/economiccrime/ cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Romania%20_April%202008_.pdf)
120. http://www.coe.int/t/dghl/cooperation/lisbonnetwork/meetings/Bureau/TrainingManualJudges_en.pdf
121. http://www.hackerwatch.org/
122. http://www.net-security.org/secworld.php?id=10452&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29
http://www.wired.com/dangerroom/2011/01/with-stuxnet-did-the-u-s-and-israel-create-a-new-cyberwar-era/
http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&ref=general&src=me&pagewanted=all
http://www.guardian.co.uk/world/2011/jan/16/stuxnet-cyberworm-us-strike-iran свидоступни 19.01.2011
123. http://graphics8.nytimes.com/packages/pdf/science/NSTB.pdf последњи пут приступљено 19.01.2011.
124. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
125. "Man gets record sentence for computer sabotage", ZDNet News & Blogs, Internet, *http://news.zdnet.com /2100-1009_22-182571.html* .

126. http://www.sophos.com/sophos/docs/eng/ papers/sophos-a-to-z-computer-and-data-security-threats.pdf
127. http://www.sophos.com/blogs/chetw/g/2010/04/03/3-types-viruses-demystified
128. http://www.symantec.com/business/resources/articles/index.jsp
129. http://www.sophos.com/blogs/chetw/g/2010/04/03/3-types-viruses-demystified
130. http://www.singi.co.yu/podrska/crvi.htm
131. http://www.sophos.com/blogs/chetw/g/2010/04/03/3-types-viruses-demystified
132. http://www.sophos.com/security/hoaxes/.
133. http://www.microsoft.com/protect/terms/socialengineering.aspx.
134. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf http://www.sophos.com/sophos/docs/eng/papers/sophos-a-to-z-computer-and-data-security-threats.pdf
135. http://www.sunbeltsecurity.com/BrowseCategories.aspx
136. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf
137. http://www.net-security.org/malware_news.php?id=1637&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29
138. http://www.nytimes.com/2011/02/13/science/13stuxnet.html?_r=1&ref=science
139. http://news.cnet.com/8301-1009_3-20049199-83.html
140. http://www.blic.rs/Vesti/Hronika/188170/Prva-krivicna-prijava-za-unosenje-racunarskog-virusa-u-Srbiji
141. http://en.wikipedia.org/wiki/Sasser_(computer_worm)
142. „Рачунарска превара тешка шест милиона еура“, Побједа Интернет, http://www.pobjeda.co.me/citanje. php?datum=2005-11-19&id=75425,
143. http://www.glas-javnosti.rs/clanak/hronika/glas-javnosti-15-12-2009/ojadili-operatere-za-68-miliona-dinara
144. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf
145. “Denial-of-service attack”, Wikipedia, Internet, http://en.wikipedia.org/wiki/Denial-of-service_attack
146. http://www.ic3.gov/media/2010/100621.aspx.
147. http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html,
148. http://www.guardian.co.uk/tec hnology/2 010/may/15/google-admits-storing-private-data http://nacionalnistroj.com/index.php.
149. http://www.bhserbia.org/uvod.htm.
150. http://www.snp1389.rs/
151. http://srpskifront.com/
152. http://www.obraz.rs/index1.htm.
153. “Ku Klux Klan”, Wikipedia, Internet, http://en.wikipedia.org/wiki/Ku_Klux_Klan,
154. http://www.kkk.bz

Садржај

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

343.533::004(497.11)

ПРЉА, Драган, 1959-
Кривична дела високотехнолошког криминала / Драган Прља, Звонимир Ивановић, Марио Рељановић. - Београд : Институт за упоредно право, 2011 (Београд : Горагораф). - 202 стр. ; 21 cm

Тираж 300. - Стр. 6-7: Реч на почетку / Јован Ћирић. - Напомене и библиографске референце уз текст. - Библиографија: стр. 194-200.

ISBN 978-86-80059-75-4
1. Ивановић, Звонимир, 1976- [аутор] 2. Рељановић, Марио, 1977- [аутор]
а) Рачунари - Злоупотреба - Србија
COBISS.SR-ID 187776268