ДРАГАН М. РАНЂЕЛОВИЋ*
БОЈАНА ЦАРЕВИЋ
Криминалистичко Полицијска академија
Београд

УДК: 343.85:[343.533::004](73)
Прегледни рад
Примљен: 11.03.2012
Одобрен: 06.04.2012

УЛОГА ЦЕНТРА ЗА ЖАЛБЕ НА ИНТЕРНЕТ КРИМИНАЛ У ЗАШТИТИ ЉУДСКИХ ПРАВА У САД**

Сажетак: У Сједињеним Америчким Државама (САД) постоји Центар за жалбе на интернет криминал (*Internet Crime Complaint Center* – IC3), који даје извештаје који се прослеђују савезним, државним и локалним органима јавног реда и мира како би се спровела активна истрага. Извештаји служе и да би се подигла свест о том проблему и да би се грађани ближе информисали, а даје и слику о распрострањености и утицају интернет превара, при чему се мора водити рачуна приликом доношења закључака о „типичним" жртвама или починиоцима тих кривичних дела. Свако ко користи интернет је потенцијална жртва, па IC3 прима пријаве оба пола, мушкараца и жена, у распону старости од десет до сто година. Способност да се предвиди жртва је ограничена, нарочито без познавања других сродних фактора ризика (на пример, броја корисника интернета као и њихово искуство и способност). Зато се многе организације слажу да су образовање и свест о томе главни алати за заштиту појединца а незаобилазни су и место и улога полиције како у превенцији, тако и у спречавању таквог криминала, познатог под именом „високотехнолошки криминал".

Кључне речи: интернет, киберкриминал, људска права, политика безбедности

* dragan.randjelovic@kpa.edu.rs
** This work was supported by the Ministry of education and scientific Republic of Serbia-Projects, III44007, TR34019.

Увод

У Сједињеним Америчким Државама је, у децембру 2003, Центар за интернет преваре и жалбе (*Internet Fraud Complaint Center* – IFCC) преименован у Центар за жалбе на интернет криминал (*Internet Crime Complaint Center* – IC3)[1] Од 1. јануара до 31. децембра 2008. године на IC3 сајт је стигло 275.284 поднесака жалби. У питању су били различити типови превара, аукцијске преваре, питања неиспоручене робе, преваре путем кредитних картица, али и жалбе на компјутерске упаде, спам (нежељена е-пошта), као и дечју порнографију. Све те жалбе су прослеђене савезним, државним и локалним органима јавног реда и мира како би се спровела активна истрага, подигла свест о том проблему, и грађани ближе информисали. У анализу су укључени и следећи подаци:

1) пријаве које се односе на неиспоручену робу или неплаћање по испоруци (чине 32,9% жалби), преваре путем интернет аукција (25,5%), преваре путем кредитне или дебитне картице (9,0%); преваре које се остварују путем стеченог поверења на интернету, (тзв. превара „нигеријско писмо") такође спадају у седам најчешће пријављиваних случајева у току године;
2) 77,4% починилаца је мушког пола, а половина је боравила у једној од следећих држава: Калифорнија, Њујорк, Флорида, Тексас, Дистрикт Колумбија и Вашингтон; већина пријављених починилаца (66,1%) била је из Сједињених Држава, али је значајан број и из Велике Британије, Нигерије, Канаде, Кине и Јужне Африке;
3) 55,4% подносилаца жалби били су мушкарци, скоро половина узраста од 30 и 50 година, већином из САД (92,4%);
4) мушкарци су изгубили више новца него жена (на 1,69 долара мушкарца 1 долар жена);
5) имејл (74,0%) и веб-странице (28,9%) су два примарна механизма којима се остварује контакт.

Преглед

Центар за жалбе на интернет криминал (IC3), који је почео са радом 8. маја 2000, основан је као партнерски пројекат Националног центара за привредни криминал (*National White Collar Crime Center* – N*W*3C)[2] и Федералног истражног бироа (ФИБ)[3], да послужи као станица која би примала, обрађивала и прослеђивала кривичне пријаве. У вре-

[1] http://www.ic3.gov
[2] http://www.nw3c.org/
[3] http://www.fbi.gov/

мену када се киберкриминал брзо шири јавља се велика потреба за таквим центром. *IC3* је намењен и наставља да служи извршавању закона заједнице, укључујући и савезне, државне и локалне агенције. Од свог оснивања, IC3 прима притужбе различитог типа: *Comer Daglas* (2006), *Council of Europe* (2008), *Defler Frank* (2008), *Elliott*, *J. E.* (2002), *Gershwin, L.K*. (2008), *Preston Gralla* (2007), *Steling William* (2006), *Vacca John R.* (2007), *Vacca John R.*, *Scott R. Ellis* (2005), преваре на мрежи (све врсте), питања права интелектуалне својине, упади у компјутере (хаковање), економска шпијунажа (крађа пословне тајне), дечија порнографија, међународно прање новца, крађа идентитета итд. Списак кривичних дела стално расте.

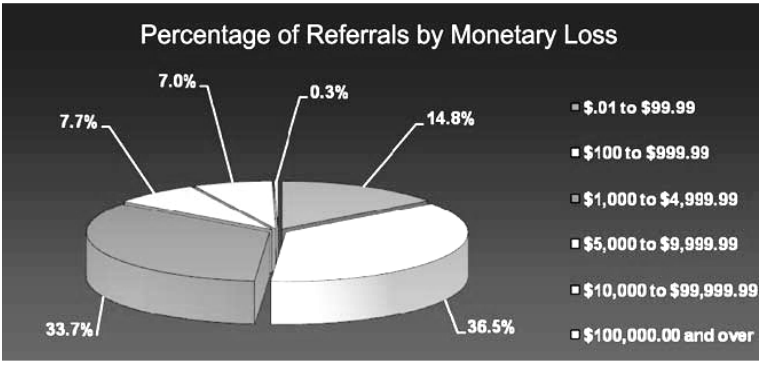
IC3 жртвама киберкриминала пружа згодан и за употребу једноставан механизам пријављивања кривичних дела. За спровођење закона, како на савезном, тако и на државном и локалном нивоу, IC3 има централни механизам за упућивање жалби. Поред значајне сарадње са полицијом и другим агенцијама, приоритетни циљ IC3 је да успостави ефикасну сарадњу и са индустријским сектором. Таквом сарадњом са обавештајним службама и могућношћу употребе стручних ресурса, *IC3* постаје способан да одигра кључну улогу у идентификовању и борби против високотехнолошког криминала. Године 2008. *IC3* је уочио повећање процента неколико злочина који се односе искључиво на интернет, као што су пецање, обмана, и жалбе на спам. „IC3 2008 Извештај о интернет криминалу" представља осмогодишњу компилацију информација о примљеним жалбама и акцијама за спровођење закона које је IC3 предузео. Резултати дају преглед кључних карактеристика: 1) жалбе, 2) починиоци, 3) подносиоци, 4) интеракције између починилаца и жалбе и 5) успех спровођења законске регулативе од стране *IC3*. Резултати тог извештај требало би да побољшају опште знање о обиму и распрострањености интернет криминала. Тај извештај не обухвата све жртве интернет криминала и превара, јер је изведен искључиво од пријава које су људи поднели IC3.[4] Резултати које он садржи заснивају се на информацијама које је *IC3* добио у форми кривичних пријава које јавност путем интернета доставља на www.ic3.gov. Међутим, ти подаци представљају

[4] Жалбе упућене *IC3*, које се односе на интернет криминал, подносе се *online* на www.ic3.gov. Подносиоцима жалби који немају приступ интернету дата је и могућност да жалбу доставе путем телефона. После пријема, жалбе се прегледају, категоришу и прослеђују одређеним агенцијама које се брину за одржавање јавног реда и мира. Такав приступ интернет криминалу, поред тога што помаже да се велики број пријава реши и починиоци законски санкционишу, помаже и у смислу подизања свести појединца, али и друштва, о интернет криминалу, а статистичка обрада података помаже да се прате обим и евентуални раст жалби, што опет умногоме може да помогне превенцији те врсте криминала. http://www.ic3.gov/default.aspx, 10. 7. 2011.

издвојене примере који се састоје од кривичних пријава које су прослеђене органима гоњења. Иако је првенствени задатак *IC3* да служи као средство за пријем, елаборацију и подношење кривичних пријава у погледу киберкриминала, наведене су и кривичне пријаве које се тичу традиционалних начина ступања у контакт (нпр. телефон и пошта). На основу информација из поднетих кривичних пријава, већи број кривичних пријава се односи на интернет или услугу путем интернета. Кривичне пријаве су прослеђене органима гоњења и/или радним групама у оквиру правосудних органа на основу места становања учиниоца (учинилаца) кривичног дела и жртве (жртава) напада.

Карактеристике кривичних пријава

Током 2008. године, кривично дело које се далеко највише пријављивало било је неиспоручивање робе и/или неплаћање. Обухватало је 32,9% поднетих кривичних пријава.[5]



Слика 1: *Проценат предвиђених монетарних губитака*

Поред тога, током 2008. године, превара путем аукција чинила је 25,5% кривичних пријава (28,6% мање него у 2007. години), а преваре путем кредитних и дебитних картица чиниле су 9% кривичних пријава. Кривичне пријаве због превара на поверење, као што су „понзи шема", компјутерска превара и превара са чековима, чиниле су 19,5% свих поднетих кривичних пријава. Друге категорије кривичних пријава, као што су нигеријска превара[6], крађа идентитета, превара према финансијским

[5] У односу на 2007. годину, то представља 32,1% повећања нивоа случајева неиспоручивања робе и/или неплаћања који су пријављени *IC3*. http://www.ic3.gov/default.aspx, 10. 7. 2011.

[6] Један од најраспрострањенијих облика кривичних дела преваре, који се врши уз помоћ рачунара, је превара позната као нигеријска превара или „превара 419". Она представља специфичан начин извршења кривичног дела преваре, који је настао захваљујући гло-

институцијама и кривичне пријаве због претњи, чиниле су, заједно, мање од 9,7% свих кривичних пријава. Статистика у оквиру категорија кривичних пријава мора се посматрати као кратак приказ који може да дâ погрешну слику због перцепције клијената и због начина на који они карактеришу своје страдање у оквиру широког опсега категорија кривичних пријава. Важно је знати и да је *IC3* активно тражио подршку од многих кључних учесника у трговини путем интернета. У оквиру тих напора многе од компанија, као што је *eBay*[7], обезбедиле су својим клијентима линкове са веб-сајтом *IC3*.

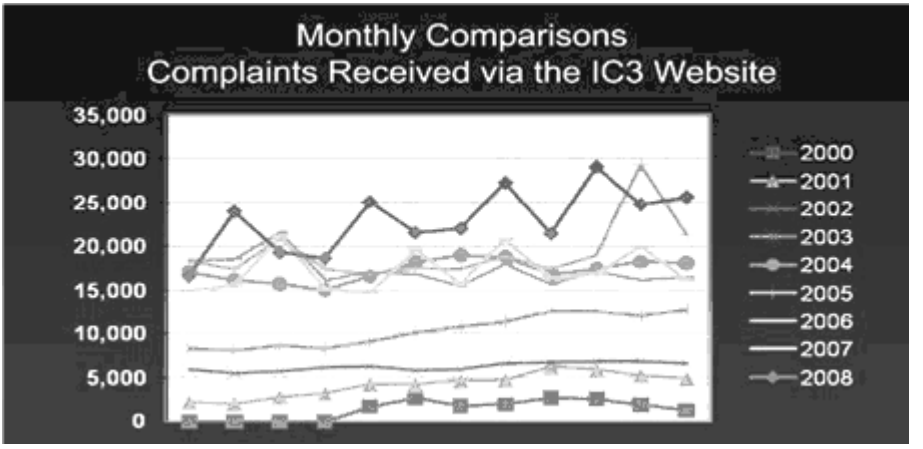
Директан резултат је повећан број поднетих пријава због кривичних дела која су описана као преваре путем аукције. Путем својих пословних односа са органима гоњења и радним групама при правосудним органима, *IC3* непрекидно прослеђује кривичне пријаве одговарајућим агенцијама. Кривичне пријаве које су достављене *IC3* односиле су се на преваре на поверење, преваре са инвестицијама, пословне преваре и друге неспецификоване преваре. Кривичне пријаве због крађе идентитета подносе се, како другим органима, тако и Федералној комисији за трговину (*Federal Trade Commission – FTC*). Кривичне пријаве против нигеријске преваре (западноафричке краткорочне позајмице на име аванса) или преваре 419 прослеђене су Тајној служби Уједињених нација, а кривичне пријаве због сексуалне експлоатације деце прослеђене су Националном центру за несталу и експлоатисану децу (*National Center for Missing and Exploited Children*). У поређењу са 2007. годином, извештај за 2008. годину (*2008 Internet Crime Report*) наводи нешто већи ниво поднетих кривичних пријава свих врста, осим за превару путем аукције Кључна област интересовања у погледу превара путем интернета је просечан новчани губитак који су претрпели подносиоци кривичне пријаве који су се обратили *IC3*. Те информације су важне јер чине основ за генералну процену просечних губитака услед превара на интернету. За приказ информација о просечним губицима[8], нуде се два облика

балној улози интернета као средства за комуникацију, електронско пословање и сл., као и све већој употреби савремених информационих технологија од стране великог броја крајњих корисника широм света. Први појавни облици те преваре подразумевали су лажне пословне понуде које су извршиоци кривичних дела нудили жртвама. Данас начини њеног извршења имају различиту форму: помоћу лажних електронских порука о добицима на играма на срећу, лажних порука везаних за добротворне прилоге, порука у вези са „љубавним понудама" и др. Урошевић, В., *Нигеријска превара у Републици Србији*, МУП РС.

[7] „With more than 90 million active users globally, eBay is the world's largest online marketplace, where practically anyone can buy and sell practically anything."
http://www.ebayinc.com/who., 11. 7. 2011.

[8] Од 72.940 кривичних пријава за преваре које је *IC3* обрадио током 2008. године, код 63.382 постојала је жртва која је пријавила новчани губитак. Могуће је да су подносиоци

просека: средња вредност и медијална. Средња вредност представља облик упросечавања који је опште познат у јавности: укупан износ у доларима подељен укупним бројем подносилаца кривичних пријава. Будући да средња вредност може бити осетљива на број кривичних пријава које се односе или на изузетно велики или на изузетно мали износ губитака, даје се и медијална. Она представља 50. перцентил, или средњу тачку свих износа губитака за све поднете тужбе. Медијална је мање осетљива на екстремне случајеве, било да се ради о високим, било да се ради о ниским трошковима.



Слика 2: *Графикон месечних жалби пристиглих на сајт IC3*

који нису пријавили губитак, пријавили инцидент пре него што су постали жртве преваре (тј. примили су понуду за лажну пословну инвестицију путем интернета или имејла) или су, већ, повратили новац од инцидента пре подношења пријаве (нпр. нема одговорности у случају преваре путем кредитних/дебитних картица). Укупни губици од свих пријављених случајева преваре у 2008. години били су 264,6 милиона долара. Ти губици су били већи него у 2007. години (према извештају, 239,1 милиона долара). Од кривичних пријава са пријављеним новчаним губицима, средња вредност губитака била је 4.174,5 долара, а медијана је била 931 долар. Скоро петнаест процената (14,8%) ових кривичних пријава односило се на губитке мање од 100 долара, а (36,5%) је пријавило губитак од 100 до 1.000 долара. Другим речима, преко половине тих случајева односило се на новчане губитке мање од 1.000 долара. Скоро трећина (33,7%) кривичних пријава пријавила је губитке од 1.000 до 5.000 долара, а само је за 15% Центар за пријављивање интернет криминала (*Internet Crime Complaint Center*) навео губитак већи од 5.000 долара. Највећи губитак у доларима по инциденту био је пријављен за превару путем чекова (медијана губитака 3.000 долара). Жртве преваре на поверење (медијана губитака 2.000 долара) и нигеријске преваре (медијана губитака 1.650 долара) су биле друга категорија високих губитака у доларима. Најнижи губитак у доларима био је везан за превару путем кредитних/дебитних картица (медијана губитака 223,5 долара).
http://www.ic3.gov/default.aspx, 10. 4. 2011.

Карактеристике учиниоца кривичног дела

Једнако важно за приказивање распрострањености и монетарног утицаја преваре путем интернета је и пружање увида у демографију учинилаца кривичног дела преваре. У случајевима код којих је наведена локација, преко 75% учинилаца кривичних дела су биле особе мушког пола, а место боравка половине њих било је у некој од следећих савезних држава САД: Калифорнија, Флорида, Њујорк, Тексас, Дистрикт Колумбија и Вашингтон. Те локације спадају у најнасељеније у земљи.

У односу на број становника, Дистрикт Колумбија, Невада, Вашингтон, Монтана, Флорида и Делавер имају највећу стопу учинилаца кривичних дела преваре по глави становника у САД. Показало се да има учинилаца кривичног дела преваре и са местом боравка у Великој Британији, Нигерији, Канади, Румунији и Италији. Границе међу савезним државама и међународне границе немају значаја за интернет криминалце. Проблеми са јурисдикцијом могу да помогну њиховим криминалним напорима јер велики број жртава, велики број савезних држава и варирање губитака у доларима успоравају истрагу. Те статистике истичу анонимну природу интернета. У само 37,3% случајева наведен је пол учиниоца кривичног дела, а савезна држава боравка за домаће учиниоце кривичног дела наводи се само у 33,3% случаја. Велики број учинилаца кривичног дела остварио је контакт са подносиоцем кривичне пријаве или преко имејла или путем веб-сајта. У тим извештајима 77,4% учинилаца кривичног дела преваре биле су особе мушког пола, а 22,6% особе женског пола.

Карактеристике подносилаца кривичних пријава

Просечан подносилац кривичне пријаве је мушкарац старости између 40 и 49 година, са местом боравка у једној од најнастањенијих савезних држава: Калифорнија, Флорида, Тексас и Њујорк. Иако су Аљаска, Колорадо и Вашингтон имале мали број поднетих кривичних пријава (налазе се на 31, 11, и 45. месту), оне спадају у савезне државе са највећим бројем поднетих кривичних пријава по глави становника у САД. Већина кривичних пријава је била из САД, али је *IC3*, такође, добио известан број пријава и из Канаде, Велике Британије и Аустралије. У табели 4 дато је поређење разлика између губитака у доларима по инциденту и демографског порекла подносилаца кривичних пријава. Особе мушког пола су пријавиле веће губитке у доларима него особе

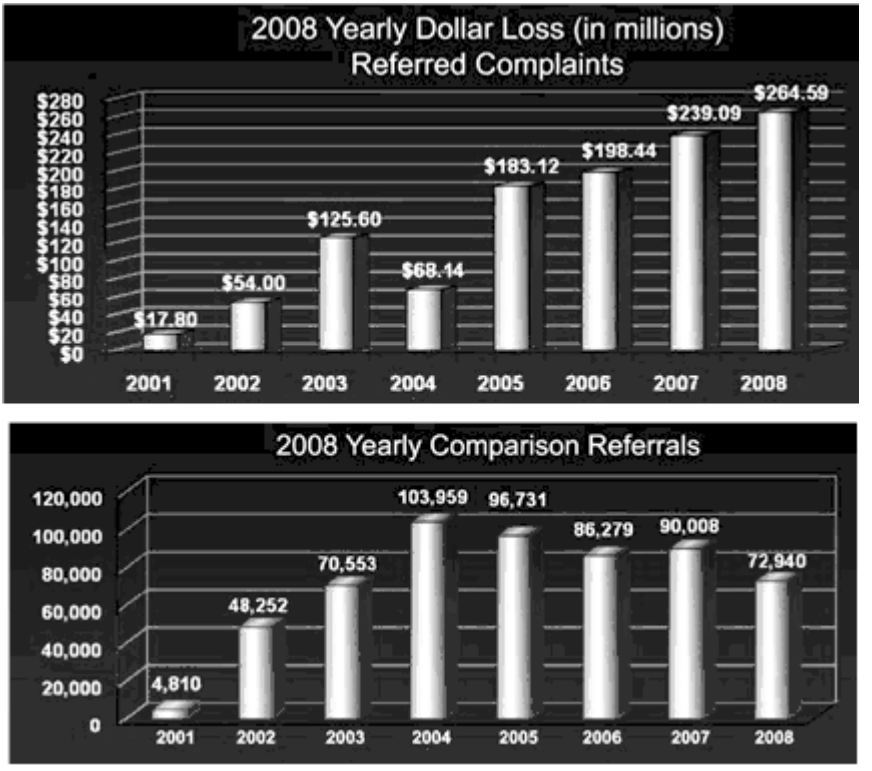
женског пола (на сваки долар 1,69 долара). Особе старости 40–49 година пријавиле су једнаке или веће износе губитака него друге групе.

Динамика подносилац кривичне пријаве – учинилац кривичног дела

Једна од компоненти преваре која се врши путем интернета, а која отежава гоњење, јесте то што учинилац и жртва могу да се налазе било где у свету. То је јединствена карактеристика која се не налази код „традиционалног" криминала. Због проблема са јурисдикцијом, често је потребна сарадња више органа да би се одређени случај решио, што указује на феномен који заиста „нема граница".[9] Други фактор који омета истрагу и гоњење починиоца интернет криминала је анонимност коју пружа сам интернет. Иако су подносиоци кривичних пријава у тим случајевима можда пријавили више начина ступања у контакт, веома мали број је пријавио контакт лицем у лице, а далеко највећи број пријавио је контакт са учиниоцима кривичног дела преко имејла (74,0%) или веб-странице (28,9%).

Према извештајима, остали су имали контакт са учиниоцем кривичног дела путем телефона (15%) или су се дописивали путем редовне поште (8,3%). Ретко када се извештавало о контакту оствареном преко соба за четовање (2,2%) и о директним сусретима (1,7%). Анонимна природа имејл адресе или веб-сајта пружа могућност учиниоцима кривичног дела да се једним притиском на тастер обрате великом броју жртава.

[9] Чак и у Калифорнији, одакле потиче највећи број пријављених случајева преваре, у само 30,6% свих пријављених случајева место боравка и учиниоца кривичног дела и подносиоца кривичне пријаве било је у истој савезној држави. Код осталих савезних држава је чак и мањи проценат сличности у погледу места боравка између подносиоца кривичне пријаве и учиниоца кривичног дела. Поред тога што указују на „вруће тачке" учинилаца кривичног дела (нпр. Калифорнија), чији циљ чине евентуалне жртве из целог света, модели понашања указују и на могућност да подносиоци кривичних пријава и учиниоци кривичног дела нису били ни у каквој вези пре инцидента. http://www.ic3.gov/default.aspx, 10. 4. 2011.



Слика 3: *Анализа од 2001. до 2008.*

Додатне информације о кривичним пријавама које добија *IC3*

Мада је *IC3* оријентисан ка пријему кривичних пријава у погледу интернет криминала, он добија кривичне пријаве које се односе и на друге врсте кривичних дела. Оне обухватају (али нису ограничене на) кривично дело насиља, пљачке, провале, претње и многе повреде закона. Углавном се људи који подносе те врсте кривичних пријава упућују да се одмах обрате локалним органима гоњења, да би се благовремено и ефикасно удовољило њиховим појединачним потребама. Уколико добије гаранције, особље *IC3* може, у име подносиоца кривичне пријаве, ступити у контакт са органима гоњења. *IC3* такође прима знатан број пријава за кривична дела која су везана за компјутер, а која, по својој природи, не представљају преваре. *IC3* рутински упућује кривичне пријаве које имају везу са компјутерима, али се не сматрају преварама путем интернета, органима и организацијама које се баве одређеним пов-

редама закона. На пример, уколико *IC3* прими информацију која се односи на претњу председнику САД, информација о добијеној кривичној пријави одмах се упућује Тајној служби САД. Кривичне пријаве у које се односе на спам и случајеве крађе идентитета упућују се Федералној комисији за трговину, федералним органима, органима савезних држава и локалним органима управе који имају јурисдикцију.

Преваре

У напору да упозори јавност и смањи број жртава превара, овај одељак описује основне карактеристике најучесталијих превара и, истовремено, указује на њихове варијације и начин на који се оне често преклапају са другим врстама кривичних дела. Једна од значајнијих превара коју је *IC3* идентификовао у току 2008. године била је коришћење противправних, нежељених имејлова у циљу крађе идентитета. Иако идеја коришћења спама за крађу информација о идентитету није нова, ти имејлови се, по свом изгледу, разликују од оних које шаље Федерални истражни биро (ФИБ). Њима се траже лични подаци, као што је број рачуна у банци, лажном тврдњом да су те информације потребне ФИБ ради истраге о предстојећој финансијској трансакцији. Та трансакција обично подразумева трансфер новчаних средстава из извора у страној земљи, често Нигерији, на рачун у банци који припада особи која је примила имејл. Примаоци тих имејлова се наводе да поверују да, сарађујући са том истрагом и пружајући неопходне информације, могу да помогну ФИБ да утврди да ли је та трансакција законита и олакшају њено извршење. Примаоци се наводе да верују да могу да извуку велику добит из те сарадње. Наводни извор средстава варира. На пример, у имејлу се може тврдити да прималац има право на неко наследство, или да је освојио добитак на некој непознатој лутрији. Милиони долара чекају да буду пребачени на рачун у банци примаоца имејла. Међутим, да би остварили право на тај новац, примаоци морају да дају обавештење о свом рачуну у банци, да би ФИБ могао да ради са службеницима стране банке на прописном обављању трансфера. Многи од тих имејлова садрже и елемент изнуђивања. Примаоцима се каже да ће, уколико не сарађују, бити судски гоњени, или ће сносити неку другу финансијску казну.

У неким случајевима, примаоци се наводе да поверују да ће, уколико не сарађују, бити подвргнути истрази због тероризма. Увек постоји покушај да се имејловима дâ привид законитости, тако што се изјављује

да они потичу од директора ФИБ, Роберта Милера (Robert Mueller), заменика директора, Џона Пистоле (John S. Pistole), неког другог лица са високим рангом, или од неке истражне јединице ФИБ. На пример, многи имејлови се позивају на Одељење за борбу против тероризма и монетарног криминала ФИБ – вероватно у покушају да подрже идеју да ће примаоци, уколико не поступе према захтеву, вероватно бити оптужени за терористичке активности.[10] Пошто је *IC3* недавно модификовао свој систем за сакупљање података, да би издвојио кривичне пријаве које се односе на ове врсте имејлова, *IC3* није у могућности да одреди количину те врсте кривичних пријава за 2008. годину. Међутим, летимичан поглед на неке недавне кривичне пријаве указује на популарност те методе међу крадљивцима идентитета. Друга превара која се обично пријављивала *IC3* током 2008. године комбиновала је технике упада путем компјутера са друштвеним инжењерингом уз истовремено лично обраћање у покушају да се изврши кривично дело преваре људи. Превара почиње тиме што учиниоци стичу неовлашћен приступ корисничком рачуну неког имејла. Пошто добију приступ на неки кориснички рачун, учиниоци преваре га преузимају и користе за слање нежељених имејлова на адресе жртава. Представљајући се као власници имејл рачуна, учиниоци преваре изјављују да се налазе заробљени у Нигерији (или некој другој земљи) и да им је неопходно потребна финансијска помоћ да би се извукли из кризе. У многим случајевима примаоцима имејла се каже да су им пријатељи опљачкани на улици и да им је сада потребно 1.000 долара за плаћање рачуна у хотелу и трошкова пута. Примаоци који одговоре на те имејлове тиме што, верујући да помажу пријатељу у невољи, пошаљу новац према упутству, често добијају нове имејлове којима се захтева више новца.

У покушају да убеде своје жртве, особе које се лажно представљају обећавају тим људима да ће им вратити новац када се буду у потпуности извукли из тешке ситуације. Као и лажни имејлови ФИБ, и ти су пуни словних и граматичких грешака, што је обично знак незаконитог дописа. Особе које добију такав имејл треба да буду опрезне и да се својим пријатељима обрате, не имејлом, већ на неки други начин и про-

[10] Корисници интернета, међутим, треба да знају да се ФБИ не обраћа грађанима САД у вези са личним финансијским питањима путем нежељених имејлова. Други непогрешиви знак незаконитости је тај да, скоро увек, ти имејлови садрже велики број словних и граматичких грешки. Те грешке су карактеристичне за многе нигеријске преваре (западноафричке, 419, краткорочне позајмице на име аванса). http://www.ic3.gov/default.aspx 10.04. 2011.

вере да ли се заиста ради о захтеву за помоћ.[11] Учиниоци преваре тада дају инструкције жртвама преваре да депонују новац и да уплаћени износ пошаљу телеграфским трансфером њима или некој трећој страни, обично уз неку вероватну причу којом тај износ објашњавају.

Уколико учиниоци преваре успеју у својој намери, жртве преваре поступају према њиховим инструкцијама да би тек касније сазнали да је инструмент плаћања који је учинилац преваре користио био незаконит. Жртве преваре тада сносе одговорност према својој банци због губитка који је произведен противправном трансакцијом. Постоји неколико облика преваре путем уплаћеног износа. У те преваре спадају и шеме тајног продавца и љубимца о којима се говори у одељку под тим насловом у извештају *IC3* за 2007. годину. Најчешћи облик те преваре који се пријављивао *IC3* током 2008. године био је облик преваре путем собног колеге. Код те преваре, жртве које траже собног колегу склапају споразум са заинтересованом страном (учиниоцима преваре). Учинилац преваре увек договара са жртвом преваре да плати чеком или налогом за плаћање. Затим следи познати редослед финансијских трансакција: жртве преваре примају неисправне чекове који су написани на већу вредност од оне која је првобитно договорена, депонују их на својим рачунима у банци, а затим, следећи инструкције учиниоца преваре, врше телеграфски трансфер више уплаћеног износа трећој страни пре него што оригиналан чек прође. Обично учиниоци преваре кажу својим жртвама да вишак износа треба да покрије трошкове селидбе и да разлику треба вратити њима или њиховом пословном партнеру (обично лажном испоручиоцу намештаја или компанији за селидбу). Прави статус чекова које шаљу учиниоци преваре обично не избија на површину док се не изврши и телеграфски трансфер уплаћеног износа и овај уновчи, а жртве преваре претрпе губитке.

МОГУЋНОСТИ INTERNET CRIME COMPLAINT CENTER (IC3)

Током претходне декаде коришћени су бројни методи да би се одржао корак са технолошким променама и разменом информација и сви су они, из разних разлога, постигли само делимичан успех. Верова-

[11] Током 2008. године *IC3* је често примао пријаве о преварама путем више уплаћеног износа. Код тих превара, учиниоци преваре преговарају о званичним или незваничним уговорима којима је предвиђено плаћање жртвама преваре. Жртве преваре, увек приме више уплаћени износ од оног који се дугује.

тно је најважнији био тај што су претходни напори углавном досезали до малих сегмената локалних или регионалних група органа гоњења са крајњим резултатом који је био ограничен на размену података. Брзина и једноставност којом учиниоци кривичних дела могу да прелазе границе широм света чине проблем још тежим. Остале препреке обухватају недоследну обуку и ограничену размену података после истраге. Јединица ФИБ за *IC3* користи аналитичке алате да од базе података о кривичним пријавама клијената *IC3* припреме оптужнице. Аналитичари ФИБ допунили су податке о кривичним пријавама клијената информацијама из отворених и затворених (органи гоњења) извора као и приватних делатности. ФИБ је омогућио приступ анализама и помоћ у случајевима свим органима гоњења у оквиру сваке пријаве *IC3* или на захтев неког органа гоњења. Заједно са корисним продуктивним алатима, *IC3* и *NW3C* нуде и тимове за анализу, обучавање и истраживање који би органима гоњења помогли у свему што им је неопходно у погледу припреме оптужнице, у шта спадају: претрага и компилација информација о случају, анализе које би вештаци извршили на добијеним подацима, ступање у контакт са другим органима који, такође, могу бити заинтересовани за сарадњу у истрази, пружању помоћи у обуци или директно у вршењу обуке, припреми дијаграма међусобне повезаности и писање извештаја о случају.

Заштита на интернету и *IC3* центар

Мада могућност конекције на интернет нуди огромне предности због могућности већег приступа информацијама, она је опасна због сајтова са ниским нивоом безбедности. (Ранђеловић, Јаћимовић, 2010; Ранђеловић, 2011). Интернет „пати" од очигледних проблема везаних за безбедност који, уколико се игноришу, могу да имају погубне последице за неприпремљене сајтове (видети више у: Forouzan, 2009). Предузећа су с правом забринута у погледу безбедности коришћења интернета и постављају следећа питања: 1) хоће ли хакери пореметити интерне системе?; 2) хоће ли важни подаци предузећа бити угрожени (промењени или прочитани) приликом преноса?; 3) хоће ли предузеће бити доведено у непријатну ситуацију? Све претходно речено представља ваљан разлог за бригу. Појављују се многа техничка решења која се односе на основне проблеме везане за безбедност интернета. Међутим, њихова је цена веома висока. Многа решења ограничавају функционалност да би повећала безбедност. Остала захтевају значајне уступке на рачун једно-

ставне употребе. Код осталих, особље које ради на традиционалним ресурсима троши време на њихову имплементацију и рад, а захтева се и трошење новца за куповину и одржавање опреме и софтвера.

Политика безбедности на интернету има за циљ доношење одлуке о томе како ће се предузеће заштитити. Углавном је потребно поделити ту политику на два дела: генералну политику и посебна правила (која су еквивалентна посебној политици система)[12]. Да би политика која се односи на интернет деловала, њен творац мора да разуме уступке који се чине. Такође, политика безбедности се мора синхронизовати са другим одговарајућим питањима политике предузећа.

Интернет је извор од виталне важности, који мења начин на који комуницирају и послују многа предузећа и појединци. Интернет, међутим, пати од знатних широко распрострањених проблема везаних за безбедност. Многе организације и предузећа претрпела су напад уљеза или покушај упада који је за последицу имао губитке у продуктивности или репутацији. У неким случајевима, предузећа су морала привремено да се дисконектују са интернета и инвестирају знатна средства у исправљање проблема са конфигурацијом система и мреже. Сајтови који нису свесни тих проблема, или им они нису познати, суочавају се са ризиком да их нападну уљези у мрежи. Чак се и сајтови који поштују праксу добре безбедности суочавају са новом рањивошћу софтвера и упорношћу уљеза. Основни проблем је што интернет није пројектован као безбедан.

Софтвер центар за спречавање високотехнолошког криминала

После две године интензивног истраживања, састанака циљних група, планирања и развоја пројеката, национални центар за спречавање привредног и високотехнолошког криминала, *NW3C*, сада нуди јединствени Систем за претраживање и истраживање кривичних пријава путем интернета (*Internet Complaint Search and Investigation System – ICSIS*)[13], приступачно софтверско решење коме се приступа путем безбедног веб-

[12] „Генерална политика одређује укупан приступ питању безбедности на интернету. Та правила дефинишу оно што је дозвољено и оно што није дозвољено. Правила се могу допунити процедурама и осталим смерницама." (Forouzan, 2009).

[13] „The Internet Complaint Search and Investigation System (ICSIS) is a Web-accessible software solution from the Internet Crime Complaint Center accessed via a secure", password-controlled website."

сајта заштићеног лозинком. Уз то обезбеђење, сваки орган са приступом интернету који добије одобрење *NW3C* може да користи тај алат, чиме се елиминише потреба за куповином новог софтвера или хардвера, осим десктоп или лаптоп компјутера са уобичајеним веб-претраживачем. *ICSIS* садржи карактеристику претраживања којом се може истовремено истраживати више токова података и користити *fuzzy* логика за побољшање компилационе анализе. Аналитички алати треће стране заједно са карактеристиком уноса/износа, (нпр. *I2 Analyst's Notebook link charts*)[14] уграђени су у ту апликацију ради визуелног представљања трендова и модела вршења кривичних дела у оквиру случајева и они обухватају цртање карата, статистичке и временске функције.[15] Резултати претраживања и случајеви могу се непрекидно размењивати између више истражитеља, појединаца или група, који су дефинисани као корисници, као што је радна група истражитеља. Корисници могу уносити коментаре, карактеристике или категорије. Остале карактеристике обухватају: обавештавање или линкове са другим отвореним истражитељима, аутоматско обавештавање када се отвори нова истрага, форуме за дискусију, подршку коју дају корисници, помоћ, повратне информације као и *I2 – Analyst Notebook ixviewer*, који омогућава графички приказ информација које су добијене преко *ICSIS*. Заједно са системом *ICSIS* ради Систем за управљање кривичним пријавама (*Complaint Management System – CMS*), пројекат развоја софтвера који одређује нивое приоритета органа међу неким групама прикупљених података или њиховим комбинацијама и прослеђује примљену кривичну пријаву надлежном органу.[16]

[14] I2 Analyst's Notebook, http://www.i2group.com/us.

[15] *Fuzzy* логика је као концепт много природнија него што се то у првом тренутку чини. Наиме, постоје ситуације у којима није могуће репрезентовати знање о систему на апсолутно прецизан начин. Да бисмо били у стању да репрезентујемо знање о таквим системима (а има их јако пуно), морамо да се одрекнемо класичне (бинарне) логике, у којој је нешто или тачно или нетачно (црно или бело) и да користимо *fuzzy* логику (све је нијанса сиве боје). У дискретним скуповима елемент или припада, или не припада одређеном скупу. Ако то представимо математички кажемо да је степен припадности скупу 1 (ако припада) или 0 (ако не припада). С друге стране, елементи у *fuzzy* скуповима могу делимично да припадају, што се математички може представити на следећи начин: 1 (100% припада), 0 (уопште не припада скупу), 0,7 (70% припада скупу). http://www.omega.com/techref/fuzzylogic.html.

[16] Упутство за самостално коришћење може се добити на: *https://members.* nw3c.org/services_databases.cfm, а и подршка Службе за помоћ стоји на располагању током редовног радног времена. *ICSIS* је алат који је *NW3* развио за потребе својих чланова за рад са подацима *IC3* и није био подвргнут провери од стране ФИБ.

Литература:

1. Vacca, J. R. (2007), *Practical Internet Security*, Pomeroy, Ohio.
2. Vacca, J. R., Scott, R. E. (2005), *Firewalls: Jumpstart for Network and Systems Administrators*, Digital Press, Florida.
3. Defler, F. (2008), *How Networks Work*, Digital Technologies and the New Media, Michigen.
4. Elliott, J. E. (2002), *Cyber Terrorism: A Threat to National Security*, Army War College, Pennsylvania-Carlisle Barracks.
5. Forouzan, B., (2009), *TCP/IP Protocol Suite (Mcgraw-Hill Forouzan Networking)*, New York.
6. Gershwin, L. K. (2008), *Cyber Threat Trends and US Network Security*, www.cia.gov.
7. Preston, G. (2007), *How to Internet Works*, Que Pub, Indianapolis.
8. Ranđelović, D., Jaćimović, S. (2010), *Policijska informatika*, Kriminalističko.policijska akademija, Beograd.
9. Ranđelović, D. (2011), *Poređenje komercijalnih i nekomercijalnih alata digitalne forenzike i njihova upotreba*, Naučno-tehnička informacija, Vojnotehnički institut, Beograd.
10. Steling, W. (2006), *Criptografi and Network security*, New Age International, New Delhi.
11. Comer, D. (2006), *The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works* (3rd Edition), The Internet Book.
12. Council of Europe (2008), *Cyberterrorism – The use of the Internet for terrorist purposes*, Council of Europe Publications.

Role of Internet Crime Complaint Center in Protection of Human Rights in US

Summary: The IC3 report describes many of the current Internet trends and models of crime. The data show that the examples of Internet crime on the rise seen in relation to data on the number of criminal charges, 275 284 in 2008. compared to 206 884 in 2007. year, 207 492 in 2006. years and 231 493 in 2005. year. Total losses of all reported cases of fraud were 264.6 million in 2008. against 239.1 million in 2007. year. Most frequently reported offense was non-delivery of goods / non-payment and fraud by credit / debit cards. Among individuals who reported losses from fraud, the highest median dollar losses were found in victims of check fraud ($ 3,000), confidence fraud victims ($ 2,000), and victims of Nigerian scams (west African, 419, short-term loans on behalf of the advance) (1,650 dollars). When comparing data for 2007. and 2008. one can see that the e-mail and web pages are still two primary mechanisms by which the contact is linked to fraud. Although this report may give a brief overview of the prevalence and effects of fraud on the Internet,

should be taken to avoid drawing conclusions about the ”typical” victims or perpetrators of these types of crimes. Anyone who uses the Internet can be compromised, and IC3 has received criminal reports from male and female from ten to a hundred years old. Applicants have criminal charges in all fifty states, in dozens of countries worldwide , and over them were committed offenses of fraud by working at home to identity theft.

Internet ”suffer” from the obvious problems related to security, which, if ignored, can have disastrous consequences for unprepared sites – Behrouz Forouzan (2009). Companies concerned about the safety of the Internet raise the following questions: 1) Will hackers disturb the internal systems?, 2) Will the companies important data be compromised (changed or read) the transfer? And 3) Will the company be brought into an unpleasant situation ? Appear in many technical solutions related to the basic problems related to Internet security. However, their price is very high – Randjelovic Dragan (2011). Many solutions limit the functionality to increase security. Internet security policy aims to make a decision about how to protect the company. It usually takes this policy divide into two parts: general policy and specific rules (which are equivalent to specific policies of the system) - Behrouz Forouzan (2009). The main problem is that the Internet is not designed to be very safe.

Key words: Internet, cyber crime, human rights, security policy