STRUČNI ČLANAK

UDK: 343.85:004.7
343.98(497.5)
Primljeno: siječanj 2013.

MIROSLAV BAČA*, JASMIN ĆOSIĆ**

Prevencija računalnog kriminaliteta

Sažetak

Vremena kriminala kakvog smo poznavali prije par godina danas su prošlost. Materijalna šteta koju je moguće počiniti "kliktanjem miša" ili "tipkanjem po tipkovnici" danas je nerazmjerno veća u odnosu na prijetnju pištoljem, trgovinu ljudima ili prodaju narkotika, i reda je stotina milijardi dolara. I ne samo to, počinitelji djela iz prošlosti mogli su biti gotovo sve osobe bez obzira na spol, dob, rasu, stupanj obrazovanosti. Danas to više nije slučaj. Počinitelji današnjih kriminalnih djela daleko su obrazovaniji, stručniji i na neki način predstavljaju elitistički dio (ako ga se tako uopće može nazvati) kriminalnog miljea. Kako se stoga ponašati, odnosno, kako se boriti protiv tako sofisticiranog načina činjenja kriminala? Je li to uopće moguće? Problema je puno, neki od odgovora bit će naznačeni kroz ovaj rad, međutim, oni ne predstavljaju niti "kuharicu" u prevenciji, niti način "borbe" već samo informiranje te naznake kako bi se trebalo postupati. Zašto? Zato što je promjenjivost oblika kao i prilagodljivost ovog novog načina kriminala toliko velika da ju je nemoguće prevenirati u punom smislu te riječi.

Ključne riječi: *računalni kriminalitet, prevencija, digitalni dokaz, računalni podatak, računalni sustav, računalni program, spam, malware, socijalna mreža, phishing, krađa identiteta, računalna forenzika.*

UVOD

Svi smo se tijekom života susreli s pričama o osobama koje su tijekom odrastanja imale cijeli niz životnih stranputica, koje nisu bile naš uzor, kako niti u svom vladanju tako niti u ponašanju. Svi smo bili svjedocima da je barem jedna od tih osoba odabrala zanimanje policajca, na silno zgražanje i čuđenje okoline misleći da takva osoba ne može biti dobar policajac odnosno da ne može biti dobar čuvar zakona. Koji bi bio rezultat? Rezultat bi bio zapanjujući, takva osoba bi iz pozicije čuvara zakona znala gotovo sve što se događa,

* prof. dr. sc. Miroslav Bača, Centar za biometriju, Fakultet organizacije i informatike Varaždin, Sveučilište u Zagrebu; stalni sudski vještak za biometriju, informatiku i telekomunikacije.
** Jasmin Ćosić, Ministarstvo unutarnjih poslova Unsko-sanske županije, Bosna i Hercegovina.

bila bi upoznata sa svim modusima postupanja kao i s načinima skrivanja. Takva osoba postala bi čuvarom zakona u punom smislu te riječi. Danas su nam potrebni takvi čuvari zakona. Zašto? Iz jednostavnog razloga što poznaju način rada i razmišljanja onih koje treba spriječiti u kršenju zakona.

Danas gotovo i ne postoji kazneno djelo koje u sebi "ne posjeduje" nekakav digitalni uređaj. Samim time u tome djelu postoje *digitalni dokazi*. U 85% od svih kriminalističkih istraživanja koje provodi FBI pojavljuju se digitalni dokazi, čak u 65% slučajeva ti dokazi su ključni.

Što ti digitalni dokazi nose? Kako ih protumačiti? Je li to djelo samim time i djelo koje se može klasificirati u domenu računalnog kriminaliteta? Ovo su zasada pitanja za daljnju raspravu, ali za potrebe ovog rada pretpostavimo da se pod ukupnosti računalnog kriminaliteta smatraju sva djela u kojima je uređaj na kojem se nalazi digitalni dokaz korišten za počinjenje kaznenog djela, odnosno koji je cilj kaznenog djela. Iako mnogi autori nespretno pokušavaju definirati računalni kriminalitet kao ukupnost počinjenih kaznenih djela kojima se neovlašteno utječe na korištenje, cjelovitost i dostupnost računalnih sustava, odnosno tajnost podataka bez obzira na štetu, to i nije baš točno. *Računalni kriminalitet* u današnjem obliku predstavlja ukupnost svih kaznenih djela u kojima su sredstva informacijsko-komunikacijske tehnologije korištena kao sredstvo ili kao cilj počinjenja kaznenog djela. U ovakvu definiciju ulaze i "klasična" kaznena djela u kojima se koristi suvremena informatičko-komunikacijska tehnologija. Limitirati pojam računalnog kriminaliteta isključivo na informacijski, odnosno računalni sustav – ne bi odgovaralo realnim uvjetima te bi pokazalo nepoznavanje problematike. Veliki broj autora koji danas piše o toj temi u naravi se nikada nije susreo s radom na takvim kaznenim djelima te stoga i ne čudi način na koji se takva djela obrađuju. U svrhu ovog rada računalnim kriminalom će se smatrati svaka kriminalna djelatnost koja se čini uz pomoć informacijsko-komunikacijske tehnologije (bilo da se radi o računalu, serveru, PDA-uređaju, mobilnom telefonu, pametnom telefonu, igraćoj konzoli, aparatu za kockanje, GPS-uređaju, uređaju za snimanje zvuka, digitalnom fotoaparatu, bilo kojemu ugrađenom sustavu ili nekom mrežnom uređaju i sl.). U tom smislu dalje će se obraditi prevencija djela vezanih za kaznena djela koja se kolokvijalno mogu nazvati kaznenim *djelima u virtualnom prostoru*[1].

1. KAZNENA DJELA

Računalni kriminal nije uvijek bio kršenje formalnog prava. Tek od 1979. godine Ministarstvo pravosuđa SAD-a je definiralo računalni kriminal kao bilo koji nelegalni akt za čije počinjenje je upotrijebljeno računalo ili računalna tehnologija. Potrebu za ovim je nametnula činjenica, da je samo krajem 70-ih godina već bilo nekoliko stotina (preko 500) kaznenih djela učinjenih upotrebom računala.

[1] Gotovo je nemoguće kvalitetno prevesti sve pojmove koji su nužni za razumijevanje ove problematike na hrvatski jezik, tako se i u slobodnom prijevodu virtualni prostor na engleskom govornom području nalazi pod pojmovima *cyberspace* odnosno *Internet space*.

Usvajanjem **Konvencije o kibernetičkom kriminalu**[2] Republika Hrvatska preuzela je obavezu i modificiranja Kaznenog zakona, te je početkom ove godine stupio na snagu novi Kazneni zakon (KZ)[3], ali na žalost s nekim starim boljkama, barem što se tiče informatičkih opisa, odnosno kaznenih djela iz te domene. Tako se u članku 87. KZ-a nalaze definicije računalnog sustava, računalnog podatka te računalnog programa. U Kaznenom zakonu (čl. 87. st. 17.) je navedeno kako je **računalni sustav** "svaka naprava ili skupina međusobno povezanih naprava, od kojih jedna ili više njih na osnovi programa automatski obrađuje podatke". Ova definicija bila bi odlična za opisivanje uređaja koji na temelju bušene kartice odrađuju određenu aktivnost (poput strojeva za pletenje i slično) ali opisuje li ova definicija računalo odnosno računalni sustav? Odgovor je "ne"! Je li ovom definicijom moguće opisati mobilni telefon, usmjerivač ili neki drugi segment informacijsko-komunikacijske infrastrukture? Odgovor je ponovno "ne"! Druga je definicija u KZ-u (čl. 87. st.18.) **računalnog podatka**. Ako se oprosti semantičko nerazumijevanje autora u smislu razlikovanja podatka, poruke i informacije ostaje nejasno i što se pod time mislilo? I kakav je to oblik prikladan za obradu u računalnom sustavu kada u prijašnjoj definiciji to nije spomenuto? Informatički je netočno *podatkom* zvati *informaciju* jer je informacija po svojoj definiciji rezultat obrade podataka koji primatelju daje neku novinu odnosno znanje, dok je podatak jednostavna činjenica koja ima neko značenje, ali primatelju ne daje nikakvo novo znanje. I za sam uvod definicija, ponovno netočna, **računalnog programa** (KZ čl. 87. st. 19.), koja kaže kako je to "skup računalnih podataka koji su u stanju prouzročiti da računalni sustav izvrši određenu funkciju". Računalni program bi se najjednostavnije mogao opisati skupom naredbi odnosno uputa koje digitalnom uređaju kažu što treba učiniti i kako. Ovdje se namjerno koristi pojam digitalnog uređaja. Naime, svi današnji uređaji koji se pokušavaju opisati (računala, mobitel, ugrađeni sustavi …) u svojoj su naravi digitalni jer obrađuju isključivo dva stanja, i stvaraju nešto što se naziva digitalni dokaz. Stoga je korektnije ove uređaje zvati digitalnim uređajima.

U članku 147. stavku 2. KZ-a, kod kaznenog djela uvrede, spominje se počinjenje ovog kaznenog djela između ostalog *putem računalnog sustava ili mreže*. Ista je situacija i kod kaznenog djela sramoćenja (čl. 148. st. 2. KZ-a) i kod kaznenog djela klevete (čl. 149. st. 2. KZ-a) kao i kod kaznenog djela javnog objavljivanja presude za kaznena djela protiv časti i ugleda (čl. 151. st. 1. KZ-a). U članku 165. stavku 1. KZ-a, kazneno djelo upoznavanja djece s pornografijom, govori se o počinjenju kaznenog djela "posredstvom računalnog sustava, mreže ili medija za pohranu podataka …". Posebno je zanimljivo kazneno djelo iz članka 178. KZ-a, povreda privatnosti djeteta, koji u stavku 2. daje mogućnost počinjenja djela putem računalnog sustava ili mreže.

U Glavi XXV. Kaznena djela protiv računalnih sustava, programa i podataka, dan je popis djela koja se dovode u svezu s računalnim kriminalom. Ono što se prvo da zami-

---

[2] Sam naziv *kibernetički kriminal* nespretno je preveden jer se pod pojmom kibernetski podrazumijevaju opće zakonitosti procesa upravljanja, reguliranja, dobivanja, pohranjivanja, prijenosa i pretvorbe informacija u sustavima neovisno o njihovoj prirodi, što znači da to može biti biološki sustav, društveni sustav ili pak tehnički sustav. *Cyber* je pojam koji se kolokvijalno može opisati kao sinonim za sve računalne mreže odnosno načine prijenosa računalnih podataka na daljinu te se odnosi kako na interent mreže tako i na intranet mreže i ostale vrste mreža koje su danas u upotrebi.

[3] Kazneni zakon. (NN 125/11., 144/12.)

jetiti da u ovoj glavi nema pojma mreže – znači li to da je zakonodavac ispustio opisati računalni sustav kao mrežu ili se mreža iz drugih djela opisanih u ovom Zakonu može tumačiti drugačije od računalne?

Članak 266. KZ-a bavi se neovlaštenim pristupom računalnom sustavu odnosno računalnim podacima ali se nigdje ne govori o tome što se smatra neovlaštenim pristupom. U idućem članku postoji još malo veća konfuzija jer se u članku 267. KZ-a govori o ometanju rada računalnog sustava, te se kaže: tko onemogući ili oteža rad ili korištenje, računalnog sustava, računalnih podataka ili programa ili računalne komunikacije. Ovdje se sada uvode novi pojmovi poput *računalne komunikacije*, a i nije u potpunosti jasno što se smatra pod pojmom *otežati*.

Članak 269. KZ-a donosi još jedan pojam, a to je: *nejavni prijenos računalnih podataka*. Postavlja se pitanje, kakav je to nejavni prijenos? Što ako osoba slučajno dođe u posjed podataka putem javne komunikacijske infrastrukture? Isti stavak govori i o *elektromagnetskim emisijama računalnog sustava* koje prenose te podatke. Nije jasno, u smislu primjene informacijsko-komunikacijskih tehnologija kakve veze ima elektromagnetska emisija s računalnim podacima. Ako se zakonodavac htio pozabaviti s načinima prikupljanja podataka te kao jedan od načina izdvojiti elektromagnetsko "prisluškivanje", onda ovaj stavak treba kvalitetnije opisati.

Članak 270. KZ-a govori o računalnom krivotvorenju, a članak 271. KZ-a o računalnoj prijevari. Iz opisa danih u ovim člancima nije razvidno koja je razlika između njih, odnosno – kada se govori o računalnom krivotvorenju, a kada o računalnoj prijevari. Temeljna razlika leži u opisu djela jer se kod računalnog krivotvorenja govori o "tko neovlašteno izradi, unese, izmijeni, izbriše ili učini neupotrebljivim računalne podatke ili programe koji imaju vrijednost za pravne odnose …", dok se u računalnoj prijevari govori o "tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, koristi, izmijeni, izbriše ili na drugi način učini neupotrebljivim …". Vidljiva je sličnost i teško je odlučiti kada će biti krivotvorenje, a kada krivotvorenje postaje prijevara.

Općenito gledajući, zakonodavac nije dovoljno kvalitetno opisao djela koja se mogu dogoditi niti je ostavio mogućnost boljeg i svrsishodnijeg načina pristupanja ovoj problematici[4].

2. STANJE U REPUBLICI HRVATSKOJ

Prema statističkim pokazateljima Ministarstva unutarnjih poslova RH[5], koje djela iz domene računalnog kriminaliteta stavlja unutar gospodarskog kriminala[6], broj ovih djela je svake godine sve veći i veći. Prvi podaci vezano za problematiku računalnog kriminala javljaju se u službenoj statistici MUP-a 2008. godine. Od tada pa do danas ta je statistika

[4] Prema mišljenju autora jedno od kvalitetnijih zakonodavnih rješenja je US Federal Statutes, Title 15 Commerce and Trade.

[5] Podaci dostupni na stranici *mup.hr*.

[6] Očigledno se radi o povijesnom nasljeđu kada su se ova djela nalazila isključivo u gospodarskom kriminalitetu i krajnje je vrijeme da MUP RH promijeni svoju nomenklaturu te preskoči tridesetak godina prošlosti i požuri u sadašnjost jer u protivnome neće biti u mogućnosti kvalitetno analizirati situaciju i kretanje kriminaliteta.

varirala kako je to prikazano u tablici 1. Prema iskazanoj statistici vidljivo je da postoji veliki nerazmjer po broju prijavljenih kaznenih djela prema pojedinim člancima. Tako na primjer, kazneno djelo računalne prijevare 2008. godine je po broju prijavljenih imalo 346 kaznenih djela, da bi iduće godine to isto djelo doživjelo blagi pad, a 2010. bi se tri puta povećao broj tih kaznenih djela. Godine 2011. zabilježena je blaga stagnacija iako se i dalje bilježi dvostruko veći broj kaznenih djela negoli 2009. godine. Veliki se nerazmjer vidi i kod kaznenog djela računalnog krivotvorenja kod kojeg je 2008. godine bilo prijavljeno184 kaznenih djela da bi 2009. taj broj bio gotovo deset puta manji, svega 19 kaznenih djela, a 2011. godine 89 kaznenih djela.

Postavlja se pitanje, jesu li ti statistički podaci dovoljno kvalitetno prikupljeni i iskazani, jesu li djela pravilno okarakterizirana, ili se jednostavno dogodio propust u nomenklaturi i zbrajanju pojedinih kaznenih djela? Također je zanimljiva statistika otkrivanja kaznenih djela iz domene računalnog kriminaliteta. Prema statistici MUP-a RH proizlazi da je ona gotovo stopostotna, a postavlja se pitanje je li ona i uistinu takva i može li uopće i biti takva – jer prema dostupnim informacijama otkrivenost ovih djela u svijetu i zemljama Europske unije daleko je manja i izražava se jednoznamenkastim postocima.

Ovo sve posebno čudi ako se uzmu u obzir kretanja računalnog kriminala u svijetu koji je u konstantnom porastu (što je i logično s obzirom na dostupnost tehnologije, uređaja kao i komunikacijskih kanala).

Kazneno djelo		**Prijavljeno**	**Razriješeno**	**Naknadno otkriveno**
Dječja pornografija na računalnom sustavu ili mreži	2008.	101	100	75
	2009.	35	33	24
	2010.	63	53	38
	2011.	50	50	25
	Σ	**249**	**236**	**162**
Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka	2008.	22	22	-
	2009.	8	7	-
	2010.	9	9	-
	2011.	40	39	-
	Σ	**79**	**77**	**-**
Računalno krivotvorenje	2008.	184	183	-
	2009.	19	20	-
	2010.	27	27	-
	2011.	89	86	-
	Σ	**319**	**316**	**-**
Računalna prijevara	2008.	346	320	-
	2009.	305	278	-
	2010.	903	886	-
	2011.	684	638	-
	Σ	**2 238**	**2 122**	**-**
Ukupno	2008.	653	605	75
	2009.	367	338	24
	2010.	1002	975	38
	2011.	863	868	25
	Σ	**2 885**	**2 786**	**162**

Tablica 1: Prikaz kretanja broja kaznenih djela (podaci preuzeti s www.mup.hr)

3. PREGLED NAJČEŠĆIH ZLOUPORABA

3.1. Spam

U posljednje vrijeme varijanta *DDoS* napada, takozvani *Spamming*, predstavlja vrlo veliki problem. Naime, ova vrsta napada koristi sustav elektroničke pošte kao cilj napada, te se kroz njega šalje veliki broj istih ili različitih poruka s ciljem da ciljno računalo prestane s radom. Međutim ne dolazi samo do prestanka rada računalnih sustava zbog namjere. Naime, mnoge marketinške i reklamne agencije koristeći usluge osoba/organizacija čija je osnovna djelatnost pronalaženje *e-mail* adresa (bilo putem novinskih grupa, web-servisa, informacijskih servisa i sl.), reklamiraju i izvješćuju veliki broj korisnika o svojim proizvodima i uslugama. S obzirom na količinu, odnosno na veliki broj takvih poruka, može doći do prestanka rada računalnog sustava. Bez obzira je li do prekida rada računalnog sustava došlo s namjerom ili bez nje, radi se o nekoj vrsti nedopuštene aktivnosti te kršenju određenih prava i sloboda osobe/korisnika (dolaze nam poruke koje ne želimo primati[7], a ujedno nas i ometaju u svakodnevnom radu sa sustavima elektroničke pošte).

---

[7] Da spam poruke ne pogađaju isključivo korisnike elektroničke pošte na računalu, već i korisnike mobilnih telefonskih uređaja najbolje opisuje članak objavljen u poslovnom dnevnom listu Dnevnik od 28. svibnja 2004. godine pod naslovom: *"Zbog SMS spama kažnjena navodno hrvatska tvrtka Fast Way Holding",* članak glasi: "Tvrtke koje su masovno varale korisnike svojim SMS porukama kažnjene su s rekordnih 450 tisuća funti. Britanski Neovisni odbor za nadgledanje standarda telefonskih informacijskih servisa (ICSTIS), neprofitno tijelo koje regulira tzv. primium telefonske usluge, kaznio je tvrtke koje su masovno varale korisnike svojim SMS porukama. Svaka od šest kažnjenih tvrtki dobila je uplatnicu na 75 tisuća funti zbog kršenja pravila o radu, ukupno rekordnih 450 tisuća funti (gotovo pet milijuna kuna). Pozivi bez nagrade. Zaposlenici tih tvrtki kontaktirali su tisuće brojeva mobitela i zemaljskih linija, obavještavajući ljude da su osvojili tisuću ili dvije funti i da samo moraju nazvati određeni broj telefona, kako bi se prijavili za nagradu. Zvanje tog broja, međutim, košta i do 20 kuna po minuti, a nagrada koja ih je čekala na kraju tog dugog i skupog poziva ili uopće nije postojala ili nije ni izdaleka bila adekvatna ni slična obećanoj. Najčešća nagrada bila je putovanje za jednu osobu na neku od jeftinijih destinacija masovnog turizma i još k tome bremenito ograničenjima. ICSTIS je u prva dva mjeseca ove godine zabilježio više od 300 žalbi, nakon čega je proveo istragu. Slučaj je prijavljen policiji. Među kažnjenim tvrtkama nalazi se i Fast Way Holding Ltd., za koju britanski mediji kažu da je iz Hrvatske. No, provjerom u registru hrvatskih tvrtki, s takvim imenom nije nađena nijedna. Svih šest kažnjenih tvrtki, navodi se u priopćenju, ima sjedište izvan Velike Britanije, ali su povezane s istim britanskim agentom, tvrtkom Smile Telecom, koja tvrdi da nije odgovorna za njihove prevarantske sheme jer je samo pružala administrativne usluge. Osim novčanih kazni, svih šest tvrtki dobilo je zabranu rada u Britaniji. ICSTIS, s kojim smo kontaktirali, priopćio je i kako je cijeli slučaj prijavio nadležnom tijelu, OFCOM-u, kao i policiji te će nastaviti svoju istragu da bi pokušali izboriti kompenzaciju za prevarene ljude." U istom se listu na toj stranici može pronaći i članak koji govori o načinu stjecanja brojeva mobitela: "Brojevi mobitela mogu se doznati putem Interneta. I posljednjih dana korisnici mobilnih mreža u Hrvatskoj izloženi su brojnim spam SMS porukama koje ih ovoga puta obavještavaju o navodno osvojenim novčanim nagradama. Kao i u nedavnom slučaju flert SMS-ova, i ovaj put je riječ o spam SMS porukama koje nisu poslane iz hrvatskih mreža. Tako su na zaslone mobilnih uređaja počele stizati poruke sljedećeg sadržaja: 'Vaš mobilni broj dobio je nagradu u vrijednosti 5.000 kuna. Nazovite s fiksnog telefona kroz 24 sata i zatražite svoju nagradu na broj 0088213884254.' Poruke se šalju iz mreža raznih stranih operatera i nije ih moguće kontrolirati, jer je riječ o porukama kojima se neprestano mijenja broj s kojih se odašilju. Tako se čini da one stižu iz mreža Velike Britanije, Indije ili pak Surinamskih otoka, ali dosad nije bilo moguće utvrditi njihovo podrijetlo. No, riječ je o govornim automatima s dodatnom vrijednošću smještenim u različitim stranim zemljama. Njihovi vlasnici, osim

Prema nekim podacima danas se gotovo tri od četiri poslane elektroničke poruke smatraju neželjenima odnosno spamom, dok prema stručnjacima SECUNIA-e[8] svega pet posto elektroničkih poruka nije spam. Glede geografskog podneblja, prema podacima SophosLabsa najviše spama dolazi iz SAD-a, čak 28,4%, drugo mjesto drži Južna Koreja s 5,2% globalnog spama, a zatim u poretku dolaze Kina, Rusija i Brazil. Prema nekim podacima 1994. godine spam je poslan milijunima ljudi u svijetu, u 2005. godini dnevno je poslano preko 30 milijardi spam poruka, dok je u 2007. godini poslano čak *90 milijardi spamova svaki dan, danas je ta cifra mnogo veća*. Borba protiv spama je veoma teška i izrazito mukotrpna. Najčešće se koriste razni anti-spam filtri (statičko, heurističko filtriranje, kao i filtriranje temeljeno za sadržaju e-maila). Reputacija je metoda borbe bazirana na *black listama*, *white listama*, te *grey listama* (crne, bijele i sive liste). Crne liste su IP adrese već poznatih servera s kojih dolazi spam, adrese zombija, odnosno poznatih spamera. Bijele liste su liste servera u koje imamo povjerenja (postoje li uopće takve), dok sive liste koristi MTA (engl. *Mail Transfer Agent*) s namjerom da privremeno odbijaju e-mail poruke od pošiljatelja kojeg ne prepoznaju. Ako poruka nije spam, poslužitelj s kojega poruka dolazi ponovno će poslati poruku, nakon čega će poruka biti prihvaćena. Siva lista zasniva se na tome da *spameri ne ponavljaju slanje poruke*.

3.2. Malware

Maliciozni računalni programi poznati su pod raznim imenima (virusi[9], crvi, trojanci i sl.), a zajednički naziv im je *malware*, nastali su u posljednjih par desetljeća prošlog stoljeća, iako problemi koje oni izazivaju su uvijek trenutni te izazivaju štetu u realnom vremenu. Analiziranje malicioznih računalnih programa može predstavljati važan alat za progon počinitelja računalnog kriminala, a poznavanje takvih alata kao i samih malicioznih računalnih programa može pomoći istražiteljima i osobama koje su zadužene za sigurnost računalnih sustava u prepoznavanju njihovih učinaka. Kada se govori o *malwareu* govori se o "zločinačkoj organizaciji" koja ujedinjuje viruse, crve, trojance i druge zloćudne i nedobronamjerne aplikacije u svrhu ostvarivanja počiniteljima protupravne koristi koja je u većini slučajeva materijalne prirode (iako može imati i neke druge oblike poput uznemiravanja).

Osnovne osobine današnjeg *malwarea* su sljedeće:

• **Modularnost.** Svi se suvremeni maliciozni programi izrađuju kroz module tako da su pojedini moduli lako zamjenjivi, pri čemu se isključivo poboljšavaju mogućnosti samih

metodom slučajnog uzorka, do brojeva mobitela hrvatskih korisnika dolaze i preko Interneta, jer mnogi mladi korisnici downloadaju besplatne ikone, sličice i melodije ostavljajući brojeve svojih mobilnih uređaja. Jedini lijek je ne nasjedati, nego odmah izbrisati poruku jer je moguće da stigne mnoštvo takvih spam poruka koje zatrpavaju inbox i sprječavaju dolazak regularnih SMS poruka."

[8] SECUNIA je lider u svijetu IT sigurnosti i testiranja ranjivosti IS-a.

[9] U studenome 1983. godine dr. Fredrick Cohen učinio je demonstraciju samokopirajućeg računalnog programa serijom eksperimenata na *VAX* i *UNIX* računalima na Lehigh University Pennsylvania, *USA*. Tijekom tih eksperimenata Leonard Adleman, Cohenov kolega prvi put je taj računalni program nazvao *"virus"*. Više o tome može se vidjeti na internetskoj adresi: *http://sunset.usc.edu/news/boehm-NAE.html* te na internetskoj adresi: *http//www.cknow.com/vtutor/vthistory.htm.*

programa. Na taj se način osigurava nesmetano širenje putem Interenta, a modularnim pristupom onemogućuje se potencijalne programe za borbu protiv *malwarea.*

• **Prodornost i razornost.** Jednom kada inficira domaćina *malware* preuzima potpunu inicijativu i dominaciju nad inficiranim domaćinom, kao i na mrežnim vezama. Onemogućuje *firewall,* kao i osvježavanje antivirusnih zapisa te eliminira "konkurentski" *malware.* U pravilu se pokušava ostvariti i dohodak za autore *malwarea* (iako je sve to samo manji dio ukupnih zlodjela).

• **Financije.** *Malware* je vrlo unosan oblik prihoda, ne radi se o zabavi niti o zabavnim sadržajima, ako je moguće provoditi i intelektualnu eksploataciju žrtve. Kako se pri tome "zarađuje" veliki novac ne čudi činjenica da u tom poslu vrlo često dolazi i do ubojstava.

• **Uključenje na zahtjev.** Kako bi maksimalizirali svoj učinak počinitelji "unajmljuju" takozvane zombi servere za DDoS napade ili za spam. Servisi ovakvog tipa donedavno su bili gotovo javni (*www.shadowcrew.com*) te je koncept "podzemnog" elektroničkog tržišta dobio sasvim novu dimenziju. Naravno da je i pravosuđe moralo krenuti u konkretniju borbu s tim oblikom zlouporaba informacijskog infrastrukturnog prostora (detalji na *http://www.usdoj.gov/opa/pr/2004/October/04_crm_726.htm*).

• **Homogenost.** Ne treba biti informatički stručnjak da se zaključi kako operacijski sustavi tvrtke Microsoft i njihov Internet Explorer dominiraju tržištem.

• **Kontaminacija.** Jednom kada se *malware* "naseli" on započinje s kontaminiranjem.

• **Konkurentnost.** *Malware* može biti, i više puta jest, jedini način borbe protiv drugog *malwarea.*

• **Neprimjetnost.** Može se širiti zavaravanjem ili iskorištavanjem drugih slabih točaka.

3.3. Prijevare

Premetanje i prijevare s podacima napad je koji se ponekad naziva i *lažnim unosom podataka.* Samo se kažnjivo djelo čini promjenom podataka prije ili poslije unosa u računalni sustav. Uzmimo na primjer isplatu osobnih dohodaka na kraju obračunskog razdoblja od jednog mjeseca. Svaki zaposlenik svoju plaću ostvaruje shodno broju odrađenih radnih sati tijekom mjeseca. Ti se radni sati bilježe s pomoću kartica ili neke druge metode, te se potom unose u računalo. Svaka isplatna lista uz zaposlenikovo ime i prezime uključuje i njegov osobni identifikacijski broj, kako u sustavu isplate plaće ne bi došlo do zamjene zaposlenika. Vrlo jednostavnom zamjenom svega dviju vrijednosti moguće je jednom zaposleniku povećati plaću na štetu drugog zaposlenika, a da pri tome organizacija nije oštećena niti za jedan radni sat. Ovakav se oblik prijevare u pravilu primjenjuje na prekovremene radne sate i na zaposlenike koji obično rade prekovremeno. Zbog svoje jednostavnosti ova se vrsta napada ne prijavljuje jer se ne vidi, pa ju je vrlo teško otkriti. Za ovaj oblik napada može se reći da je rezerviran za specifične skupine počinitelja, jer ga može počiniti isključivo ovlašteni korisnik na računalnom sustavu, te stoga ovdje možemo govoriti o unutarnjim počiniteljima. Među počinitelje ovog oblika napada ubrajamo programere s detaljnim poznavanjem računalnog programa, zaposlenike ili bivše zaposlenike, programere financijskih sustava, računalne korisnike i računalne operatere.

Naravno da se u kontekstu određivanja napadača ne može reći da su ovi napadači jedini u stanju izvesti ove napade.

3.4. Zlouporabe u društvenim mrežama

Danas je veoma veliki problem u svijetu i zlouporaba društvenih mreža Facebook, Twitter, MySpace i sl. za razne kriminalne djelatnosti. Pored toga što su obični korisnici interneta i društvenih mreža meta kriminalaca, danas je veoma čest slučaj da su to i velike korporacije i tvrtke. Gubljenje vremena zaposlenika na društvenim mrežama u radno vrijeme pored pojma koji se označava *"krađa procesorskog vremena"*, utječe i na ranjivost računala odnosno računalnog sustava. Prema podacima SOPHOS-a, korporacije su žrtve *malwarea, spama, phishinga* – najviše kroz društvene mreže i posjećivanje profila koji su kreirani samo s tim ciljem.

Danas je *"socijalni inženjering"* opasnost broj jedan u svijetu. Footprinting, istraživanja, ispitivanja uposlenika poduzeća o običajima u poduzeću, otkrivanje nekakvih poslovnih tajni o poduzeću – postala je sasvim normalna pojava na socijalnim mrežama. Liste prijatelja na socijalnim mrežama mogu otkriti mnogo o korisnicima. U početku se čini ne baš mnogo, ali kako vrijeme odmiče, korisnici postaju ponosni vlasnici nekoliko stotina virtualnih prijatelja. Mnoge od njih niti ne znanju. Postaje se članom nekakvih korisnih (ali i beskorisnih) grupa. Problem nastaje kada se "prijeđe granica" i kada grupa postane zanimljiva službenoj provedbi zakona.

Stvari se dodatno kompliciraju i dobivaju novu dimenziju kada "on–line" postane "off–line". Tada se narušava i fizička sigurnost poduzeća, ali i osobna sigurnost i privatnost. Što to u biti znači? Korisnici socijalnih mreža najčešće pišu što rade, što im je na umu, gdje planiraju i kada planiraju na putovanja, tko su im prijatelji. Novu dimenziju svemu daje i multimedija, te objavljivanje fotografija, videouradaka, s privatnim podacima od imovine s kojom se raspolaže, članovima obitelji, pa do slika interijera kuće ili stana i druge pokretne ili nepokretne imovine? U ovome su mogućnost naravno vidjeli kriminalci, te počeli koristiti blagodati koje im je ponudila informacijsko-komunikacijska tehnologija (IKT) kako bi si olakšali posao. Otkrivanje i praćenje žrtvi postalo je trivijalno. Prate se društvene mreže, otkrije se eventualna žrtva, pronađu potrebni podaci, putem Googleovih servisa pronalazi se lokacija, uz pomoć ekstrakcije metapodataka iz same slike moguće je dobiti točnu zemljopisnu duljinu i širinu (koje mogu biti veoma svježe), te se time omogući izrada detaljnih skica i planova. On–line kriminalci su se već duže vrijeme počeli grupirati u skupine na društvenim mrežama i čak počeli dijeliti, razmjenjivati i prodavati ove informacije[10].

Veoma čest scenarij: *Čovjek je kupio novi SLK mercedes, naravno na Facebook je postavio fotografije načinjene iz svih mogućih perspektiva, skenirane račune koje je platio, mjesto gdje je parkiran, i onda je na zid (oglasna ploča Facebook stranice) napiše kako ga nažalost sada ne može voziti jer ide 15 dana na Mallorku na godišnji odmor*! Zar ovo ne zvuči kao "otvoreni" poziv na krađu automobila?

[10] Danas se na internetu sasvim "regularno" mogu okupiti mailing liste, e-mail adrese, baze podataka kadrovske evidencije, validni brojevi kreditnih kartica i sl. Tržište Rusije je najbogatije ovim "robama".

Cyberstalkeri[11] pronalaze svoje žrtve najviše putem socijalnih mreža, te im onda putem ovih mreža i zaraženih profila šalju *spam, malware*, uznemiravaju ih na razne načine. Najčešće provode istraživanja tko su žrtve, što rade, gdje žive, kakve su im navike i sl.

Kada ih se zainteresira, mogu prijeći granicu i početi s off–line napadima što dobiva sasvim novu dimenziju, uznemiravanja se mogu nastaviti telefonom, vandalizmima, tradicionalnom poštom i slično. Cilj je "izluditi žrtvu" i ostvariti planiranu korist.

Policija i sudovi već unazad nekoliko godina procesuiraju ovakve slučajeve, naravno tamo gdje im uspiju ući u trag. Danas postoji pojam SNA (*Social Networking Analysis*) koji označava alat koji se upotrebljava u kriminalističkim istraživanjima, s ciljem prikupljanja i analiziranja dokaza. Policija je već mnogo puta do sada procesuirala slučajeve gdje su ljudi na socijalne mreže postavljali razne neprimjerene sadržaje. Svjedoci smo nekoliko desetaka slučajeva najavljivanja ubojstava i samoubojstava na Facebooku koja su se zaista i dogodila. Danas policija ima pune ruke posla s maloljetnicima koji na socijalnim mrežama upražnjavaju reklamiranje alkohola, marihuane, teških droga i drugih zabranjenih stvari.

3.5. Phishing i krađa identiteta

Tehnika *phishing* je opisana prvi put davne 1987. godine u dokumentaciji i prezentaciji isporučenoj od strane međunarodne *HP User Group Interex*. U računalnom žargonu termin *phishing*, izvedenica od *fishing* što znači ribarenje ili pecanje, oblik je kriminalnog ponašanja, pri kome se uz upotrebu IKT-a, prikrivanjem pravog identiteta, pokušavaju ukrasti, odnosno prisvojiti osjetljivi osobni podaci trećih osoba, kao što su korisničko ime (*username*), šifra (*password*), broj kreditne kartice (*credit card number*), broj socijalnog osiguranja (*social number*), osobni identifikacijski broj i drugi osobni podaci. Prikrivanje ili *masquerading* se obavlja tako da se korisnik, obično prijevarom, preusmjerava na lažne web-stranice, na kojima se putem web-aplikacija, e-maila ali i neposrednim putem preko telefonske linije, traži izravan unos osjetljivih podataka. U literaturi možemo često sresti i pojam *Identity Theft* ili *Identity Fraud* koji se također mogu dovesti u svezu sa *phishingom*, a predstavljaju termine koji se upotrebljavaju za sve tipove kriminala, u kojima netko pokušava ukrasti personalne podatke i zlouporabiti ih, pribavljajući time sebi neku protupravnu ekonomsku korist.

Prvi konkretni napad ovom tehnikom na platni sustav zabilježen je u SAD-u ne tako davne 2001. godine, dok je već 2004. godine *phishing* bio prepoznatljiv kao dio gospodarskog kriminala. Štete koje su učinjene s ovom tehnologijom već su 2004. godine bile milijunske, a 1,2 milijuna korisnika u SAD-u bile su žrtve ove računalne pošasti s načinjenom štetom od 929 milijuna US $. Krajem 2007. godine Microsoft je objavio novo istraživanje koje upućuje na još brži – progresivan rast, sigurnosnih napada usmjerenih na krađu osjetljivih podataka (osobnih podataka). U *Security Intelligence Reportu* Microsoft je otkrio da je u prvih šest mjeseci 2007. godine otkriveno 31,6 milijuna slučajeva krađe osobnih podataka. U odnosu na protekli period (drugih šest mjeseci 2006. godine) to je čak za 150% više. U istoj studiji se navodi da je za nevjerojatnih 500% povećan broj "trojanaca", "droppersa" i "malicioznog koda" instaliranih kod krajnjih korisnika, a sve

[11] Prema studijama Guardiana, *cyberstalking* je postao češći oblik zlostavljanja od onog koje se događa u stvarnom životu.

s ciljem krađe passoworda, bilježenja aktivnosti na tastaturi – prikupljanja *key loggera*, s krajnjom svrhom ponovne zlouporabe podataka radi pribavljanja materijalne koristi.

U siječnju 2004. godine US Federal Trade Commission je podnio prvu tužbu protiv osumnjičenih osoba koje su se bavile *phishnigom*. Optuženik je bio kalifornijski tinejdžer, koji je, kako se tvrdi, kreirao web-stranicu koja je sličila na AOL website, i upotrebljavao je kako bi krao brojeve kreditnih kartica od prevarenih korisnika. I u ostatku "informatiziranog" svijeta je počela *anti-phishing* kampanja. U Brazilu je također uhvaćen jedan od najvećih prevaranata, koji je u dvije godine ukrao između 18 i 37 milijuna US $. U 2006. godini je japanska policija uhvatila 8 ljudi koji su protupravno stekli materijalnu korist u iznosu od 100 milijuna yena, što iznosi oko 870.000 US $. Sjedinjene Američke Države, odnosno država Kalifornija, nastavile su i najjaču *anti-phishing* kampanju protiv prevaranata i u svibnju 2005. godine predložile *Anti-phishing Act 2005*, po kojem su kazne za "ribare" bile i do 250.000 $ i do 5 godina zatvora. Ovim zakonom ova aktivnost je definitivno proglašena kriminalom. Velika Britanija je bila malo stroža i u svom aktu *Fraud Act 2006* predložila je do 10 godina zatvora za ove prijestupnike.

4. ISKUSTVA IZ PRAKSE

Prema osobnim iskustvima autora iz dugogodišnje prakse bavljenja borbom protiv računalnog kriminala, ali i bavljenja digitalnom forenzikom i prezentiranjem digitalnih dokaza pred sudovima u Hrvatskoj, Srbiji i Bosni i Hercegovini, najčešći uzroci zbog kojih su građani ali i korporacije bili žrtve računalnog kriminala sigurnosni su propusti i needuciranost u domeni IKT-a.

U jednom slučaju u susjednoj Bosni i Hercegovini 2011. godine žrtvi je skinuto s bankovnog računa 40.000 KN. U prvom razgovoru sa žrtvom, ona nikada nije učinila nikakva on–line plaćanja računa niti je educirana za rad s računalom i internetom. Nakon provedene istrage i učinjene forenzične analize računala, ispostavilo se da je jedan član obitelji žrtve često igrao on–line igrice, te obavljao plaćanja u iznosima nekoliko desetaka eura za članstvo na *gejmerskim* poslužiteljima. Kada je osoba obavljala plaćanja, to je radila iz istog *browsera* s otvorenim aktivnim tabom on–line igrice čime je otvorila mogućnost i postala žrtva XSS napada (*Cross site scripting*).

U posljednje dvije godine zabilježeno je i nekoliko slučajeva gdje je ciljanim žrtvama poslan e-mail s web-stranicom koju su priredile osobe koje se bave *phishingom*, gdje se od korisnika tražila hitna promjena podataka za autentifikaciju (korisničko ime i zaporka), nakon čega su isti zlouporabljeni na način da je s računa skinuto nekoliko desetaka tisuća kuna i potrošeno na on–line klađenja, pa čak i u dobrotvorne svrhe i plaćanje avionskih karata u Australiji! I u ovom slučaju presudnu ulogu je imalo povjerenje korisnika i vjerovanje da je e-mail stigao od eBay korporacije.

U posljednje vrijeme je aktualna problematika "krađe identiteta", koja se događa na više načina i uz pomoć različitih metodologija. Najčešći načini su *socijalni inženjering* i *footprinting* gdje se na sve moguće načine pokušava pronaći što više informacija o potencijalnim žrtvama. Koriste se razni alati od "običnog" guglanja[12] pa do specijaliziranih alata

[12] Pojam *guglanje* je danas općeprihvaćen na internetu, a označava pretraživanje određenih sadržaja ili

kao što su servis *www.spokeo.com* koji je dizajniran kao *mash tehnologija,* da pronalazi informacije unutar socijalnih mreža. Obično se importira adresar iz Outlooka te pretražuje sve informacije o vlasnicima e-mail adresa koji se nalaze u adresaru. Slično rade i *www.pipl.com* i *www.cvgadget.com*! Špijunira se što rade prijatelji, čime se bave, kakvu glazbu slušaju, koliko novca troše i na što troše, što rade na Facebooku. Servis *www.rapleaf.com*, opisan kao *data and people lookup*, radi klasično špijuniranje odnosno otkrivanje podataka o ljudima kao eventualnim kupcima. Nakon što se prikupe svi podaci, pristupa se krađi identiteta zlouporabom prikupljenih podataka (datumi rođenja djece, registarske oznake vozila, ime kućnog ljubimca ili razrednice u gimnaziji), što su obično pitanja koja se postavljaju za *reset passworda*!

5. ZAKLJUČAK

Prevencija računalnog kriminaliteta, odnosno ukupnosti kaznenih djela, ponajprije iz Glave XXV. Kaznenog zakona, kao i drugih kažnjivih djela koja se mogu podvesti pod opću definiciju računalnog kriminala, trebala bi se provesti kroz sljedeće korake:

• Modifikacija Kaznenog zakona vezano za djela povezana s informacijsko-komunikacijskim tehnologijama kao i kvalitetnije i detaljnije pojašnjenje pojedinih definicija i samih kaznenih djela.

• Povećanje broja državnih odvjetnika koji bi se specijalizirali za borbu protiv ove vrste kriminala, te njihova edukacija.

• Povećanje broja policijskih službenika koji bi se specijalizirali za borbu protiv ove vrste kriminala, njihova edukacija i obuka kao i pribavljanje potrebne opreme.

• Povećanje svijesti kod građana i promicanje svijesti o novim kaznenim djelima kao i edukacija o postojećim kroz aktivniji rad policije i državnog odvjetništva.

• Prilikom edukacija angažirati priznate stručnjake iz područja računalnog kriminala i digitalne forenzike, te edukacije netehničkog osoblja obavljati na tehničkoj razini.

LITERATURA

1. Bača, M. (2004). *Uvod u računalnu sigurnost*. Narodne Novine: Zagreb.
2. Brown, C. L. (2009). *Computer evidence: Collection and Preservation*. Course Technology PTR.
3. Casey, E. (2011). *Digital evidence and computer crime.* Third edition. Waltham, MA: Academic Press.
4. Ćosić, J., Bača, M. (2010). *Kompjuterska forenzika-široki aspekt primjene*. Infoteh – naučno-stručni skup, Jahorina, Bosna i Hercegovina, 857.-860.
5. Ćosić, J., Bača, M., Ćosić, Z. (2012). *Knowledge Sharing and Reuse in Digital Forensic Domain a Review.* The Proceedings of the 4th International Conference on Information Technologies and Information Society ITIS 2012, Fakulteta za informacijske študije, Novo Mesto, Slovenia.
6. Ćosić, J., Ćosić, Z., Bača, M. (2011). *Modeling Digital Evidence Management Using Petri Net*. Computer Technology and Application, 2(7), 545.-549.

pojmova (pa i osoba) uz pomoć Googleovih algoritama za pretragu.

7. Ćosić, J., Ćosić, Z., Bača, M., (2011). *Chain of Digital Evidence Based Model of Digital Forensic Investigation Process*. International Journal of Computer Science & Information Security, 9(8), 18.-24.
8. Pregled sigurnosnih pokazatelja, Ministarstvo unutarnjih poslova Republike Hrvatske, *www.mup.hr.*
9. Sammes, A., Jankinson, B. (2000). *Forensic Computing: A Practitioner's Guide (Practitioner Series).* NewYork: Springer-Verlag.
10. Symantec (2011). *Cyber Crime Report 2011.* Mountain View, CA: Symantec Corporation World Headquarters.

Summary

Miroslav Bača, Jasmin Ćosić

Cyber Crime Prevention

Crime time as we have known a few years ago, are past now. Material damage that can be committed by mouse clicking or keyboard typing today is disproportionately higher in relation to the threat of a gun, trafficking or sale of narcotics. It is expressed in hundred billion dollars. And not only that, the perpetrators of the past could be almost all people, regardless of gender, age, race, level of education. Today this is no longer the case. The perpetrators of today's crimes are far more educated, professional and in some way represent the elitist part (if it is so can call) gangland. How, then, behave and how to fight against such sophisticated methods of committing crime? Is that even possible? Some of the answers will be outlined in this paper, however this paper do not represent any "cookbook" to prevent, or how the "battle", but just in these indications to be followed. Why? Because the variability of the shape and flexibility of this new way of crime is so great that it is impossible to prevent in the full sense of the word.

Key words: computer crime, prevention, computer evidence, computer data, computer system, computer program, spam, malware, social networking, phishing, identity theft, computer forensics.