Centar Informacijske Sigurnosti

Profiliranje cyber kriminalaca

siječanj 2012

CIS-DOC-2012-01-038

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Cyber kriminal[1] prisutan je od samih začetaka Interneta, ali tek je u zadnjem desetljeću prepoznato da se radi o ozbiljnom problemu te mu je posvećeno više pažnje. Stalni porast štete koju nanosi doveo je do toga da se danas na cyber kriminal gleda jednako kao i na sve ostale tipove zločina, a problemu suzbijanja i rješavanja pristupa se korištenjem klasičnih kriminoloških metoda.

Jedna od preuzetih metoda je profiliranje kriminalaca, postupak kojim se nastoji otkriti nešto o psihološkim osobinama kriminalaca – osobnosti, navikama, znanjima. Popularizaciji ovog pristupa doprinijele su i brojne kriminalističke serije i filmovi, poput filma „Kad jaganjci utihnu“ iz devedesetih u kojem agentica FBI-a Clarice Starling i zatvorenik Hannibal Lecter zajedno rade profil serijskog ubojice. Moderne kriminalističke serije gotovo isključivo se temelje na forenzici i profiliranju kriminalaca, a u zadnje vrijeme nerijetko se bave upravo cyber kriminalom.

Profiliranje se paralelno provodi na dva načina, induktivni i deduktivni. Induktivni način uključuje izradu profila kriminalaca iz poznatih statističkih podataka (obrazaca ponašanja, demografskih osobina), dok se deduktivni zasniva na forenzičkim dokazima i tragovima sa mjesta zločina. Iako je osnovni princip isti, prilagodba metoda profiliranja na cyber kriminal ipak nije tako jednostavna. Mnogi su čimbenici specifični i otežavajući u odnosu na klasičan zločin, primjerice drugačiji tip i način prikupljanja dokaza, anonimnost na Internetu, počinitelji iz drugih država i zakonske prepreke. Koliko su zakonske i geografske prepreke velik problem jasno je vidljivo na primjeru brojnih tužbi američkih kompanija protiv švedske stranice *thepiratebay*.[2]

Profiliranje cyber kriminalaca provodi se s istim primarnim ciljem kao i kod ostalih zločina – da se pospješi pronalaženje počinitelja određenog zločina. Psihološki profili mogu biti od velike pomoći pri sužavanju liste osumnjičenih koja, posebice u cyber zločinima, može biti iznimno velika, te je cijena pronalaska počinitelja često veća od počinjene štete. Međutim, za očekivati je ipak da će korist od profiliranja ipak biti nešto niža nego kod ostalih tipova zločina. Razlog tomu je što se počinitelji klasičnih zločina često po nekoj osobini znatno izdvajaju od ostatka populacije, dok se cyber kriminalci mnogo bolje „uklapaju“ i teško je pronaći njima specifične osobine.

[1] Kriminalna aktivnost počinjena korištenjem računala i Interneta.

[2] Brojne američke kompanije slale su zahtjeve thepiratebay-u, švedskom hostu magnet linkova i .torrent datoteka, za uklanjanje određenih datoteka koje omogućuju djeljenje određenog zaštićenog sadržaja. Budući da na stranicama nije bio zaštićen sam sadržaj, već samo .torrent datoteke, prema švedskom zakonu nije bilo počinjenog prekršaja.

2. Postojeće metode profiliranja kriminalaca i primjena na cyber kriminal

Kao što je u uvodnom poglavlju spomenuto, metode profiliranja kriminalaca moraju se malo prilagoditi kako bi bile primjenjive na cyber kriminal. To se prvenstveno odnosi na deduktivne metode, dok su induktivne gotovo izravno primjenjive.

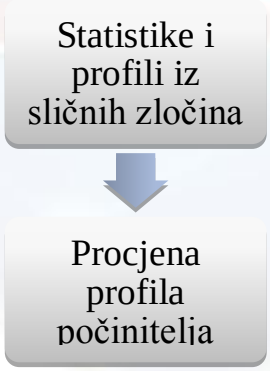
2.1. Induktivno profiliranje

Induktivno profiliranje (Slika 1) temelji se na premisi da počinitelje sličnih zločina vežu neke zajedničke osobine. Proučavaju se postojeće statistike i generalizira primjenom informacija iz profila vezanih za slične zločine kako bi se mogao stvoriti najvjerojatniji profil. Kao izvor informacija mogu poslužiti službeni dokumenti poput policijskih dosjea, ali i članci iz novina i ostalih medija.

Sam naziv, „induktivne“, dolazi od induktivne statistike i induktivne logike, dvije grane matematike koje su osnova induktivnog profiliranja. Induktivna statistika zaključuje o nekoj populaciji na temelju proučenog slučajnog uzorka. Slično je i sa induktivnom logikom, gdje se iz određenih premisa generalizira i donosi logičan i vjerojatan, ali ne i nužno posve točan zaključak.

Najveća prednost induktivnog profiliranja svakako je jednostavnost. Nije potrebno nikakvo forenzičko znanje, iskustvo u proučavanju ponašanja kriminalaca ili kriminoloških istraga, već samo poznavanje statistike i što veći uzorak na kojem se temelji. Vrijeme potrebno za izradu profila je tipično vrlo kratko, a u posljednje se vrijeme primjenjuju i računalne neuronske mreže kako bi se proces djelomično automatizirao.

Za primjenu u cyber kriminalu nije potrebna praktički nikakva modifikacija. Primjerice, koriste se statistički podaci kako bi se otkrilo koje su trenutno najpopularnije i najčešće metode napada. Također, određuje se i koje su najvjerojatnije mete, te se ti podaci koriste kako bi se pospješila obrana protiv ovih oblika napada. Zapravo se radi o pokušaju predikcije budućih napada temeljenom na dostupnim statističkim podacima i vjerojatnosti.



Slika 1. *Blok dijagram induktivnog profiliranja kriminalaca*
Izvor: *CIS*

2.2. Deduktivno profiliranje

Deduktivnim metodama koriste se podaci dobiveni iz forenzičke analize, proučavanja žrtve, samog mjesta zločina, fotografija i sličnih dokaza, kako bi se što točnije opisalo ponašanje počinitelja najprije na mjestu zločina, a zatim i dobile neke općenite informacije o osobnosti, ponašanju i motivima.

Naziv „deduktivno“, kao i u slučaju induktivnog profiliranja, dolazi zbog logike na kojoj se temelji, u ovom slučaju deduktivne. Na temelju određenih premisa dolazi se do zaključka koji nužno

slijedi iz tih premisa, te je sigurno točan ako su premise točne. Naravno, kod deduktivnog profiliranja nije moguće doći do zaključka za koji se može jamčiti da je točan.

Ovakav je pristup obično vrlo spor. Potrebno je čekati da se izvuku svi dokazi, detaljno prouči mjesto zločina i sam zločin te provedu sve potrebne istrage, a zatim proučiti sve prikupljeno i na temelju toga polako graditi profil počinitelja, što je često iterativan proces.

Svi čimbenici koji se koriste u deduktivnom profiliranju – mjesto zločina, žrtva, forenzički dokazi – – u slučaju cyber kriminala su specifični i uvelike se razlikuju od ostalih, klasičnih zločina. Dok je u slučaju klasičnog zločina tipično najvažnije dobro proučiti žrtvu (eng. *victimology*), kod cyber kriminala odabir žrtve često je slučajan, a u najboljem slučaju može dati dosta nepouzdan odgovor o kojem se osnovnom tipu cyber kriminalca radi. Samo „mjesto zločina“ je virtualno i ne može dati neke odgovore koji se u slučaju klasičnog zločina mogu dobiti iz mjesta zločina (npr. živi li počinitelj blizu mjesta zločina, po čemu je odabrano mjesto specifično). Dokazi prik

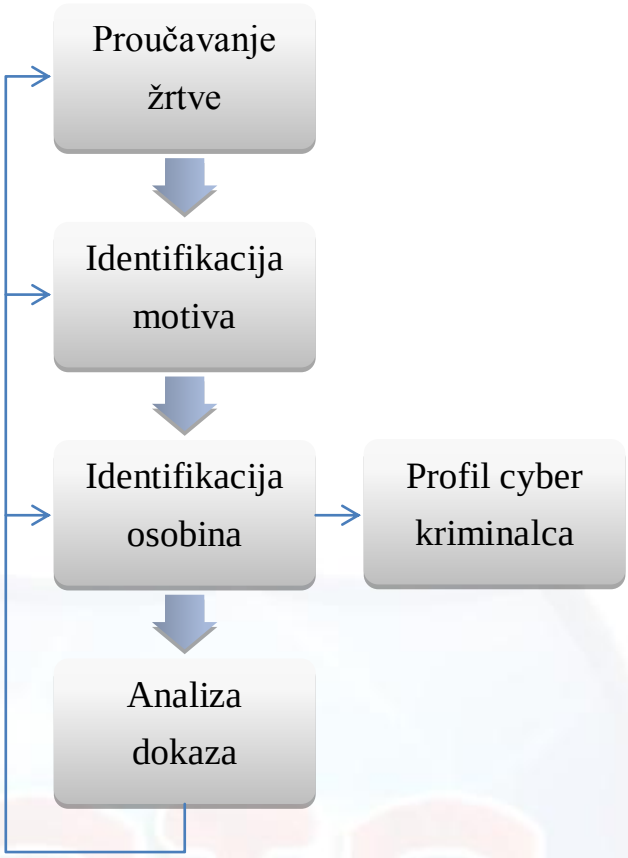
Kod deduktivnog profiliranja cyber kriminalaca često se koriste sljedeća četiri koraka:

1. Proučavanje žrtve, koja u slučaju cyber kriminala može biti pojedinac ili organizacija. Važno je odrediti što je sve u vezi žrtve moglo privući napadača.
2. Identifikacija motiva napadača, proces usko povezan s prethodnim korakom. O motivima će biti više govora u idućem poglavlju.
3. Identifikacija osobina napadača. Postoji više predloženih primjera klasifikacije cyber kriminalaca s obzirom na motive, ali zbog tehnološkog razvoja te promjena u ponašanju i metodama napada potrebno ih je stalno prilagođavati.
4. Analiza dokaza prikupljenih digitalnom forenzikom[3].

Kao i kod profiliranja ostalih tipova kriminalaca, deduktivno profiliranje cyber kriminalaca također je iterativan proces u kojem nova saznanja iz svakog od četiri koraka mogu donijeti do drugačijeg tumačenja nekih zaključaka ranije izvučenih iz ostalih koraka.

Slika 2 prikazuje bok dijagram kojim je opisan proces iterativnog deduktivnog profiliranja cyber kriminalaca kroz opisana četiri koraka.

[3] Grana forenzike koja se bavi proučavanjem i izvlačenjem podataka iz digitalnih uređaja.



Slika 2. *Blok dijagram iterativnog procesa deduktivnog profiliranja cyber kriminalaca*
Izvor: *CIS*

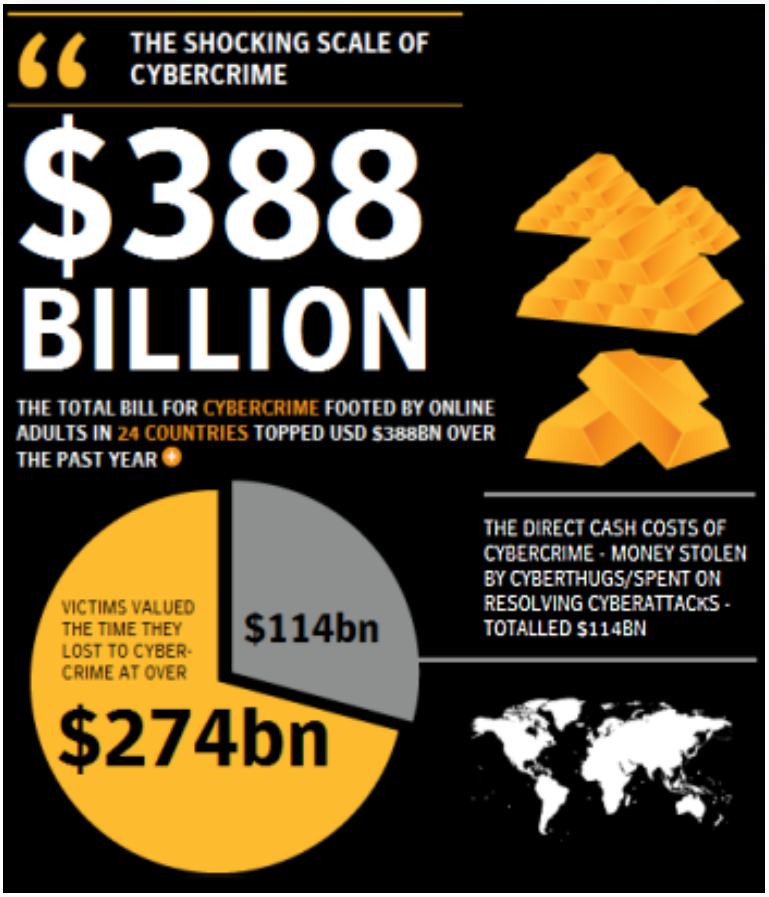
3. Šteta uzrokovana cyber kriminalom

Kako bi se shvatilo zašto je bilo potrebno intenzivirati i unaprijediti metode borbe protiv cyber kriminala potrebno je sagledati neke statističke vrijednosti. One su opisane u nastavku ovog poglavlja.

3.1. Istraživanje Symantec-a 2011. godine

Prošle je godine Symantec, jedna od najvećih svjetskih kompanija u području računalne sigurnosti, proveo opsežno istraživanje pod nazivom "Norton Cybercrime Report 2011", o šteti nastaloj kao posljedici cyber kriminala. Istraživanje je uključivalo ljude u dobi od 18 do 64 godine iz 24 različite zemlje, te su procjene globalnih vrijednosti dobivene ekstrapolacijom dobivenih rezultata.

Ukupan globalni trošak uzrokovan cyber kriminalom iznosi oko 114 milijardi američkih dolara godišnje. To uključuje izravno izazvanu štetu te trošak borbe protiv počinitelja. Štetu zbog izgubljenog vremena žrtve cyber napada su procijenile na još više nego dvostruko - 274 milijarde, što znači da je **ukupna procjena štete 388 milijardi američkih dolara godišnje**. Za usporedbu, ukupan trošak izazvan trgovinom svih vrsta droge UNODC (eng. *United Nations Office on Drugs and Crime)* procjenjuje na 411 milijardi američkih dolara. Slika 3. **Dio prezentacije Symantec-a nakon provedenog istraživanja** Izvor: **symantec.com** prikazuje dio prezentacije o rezultatima istraživanja koji se odnosi na ukupan trošak cyber kriminala.



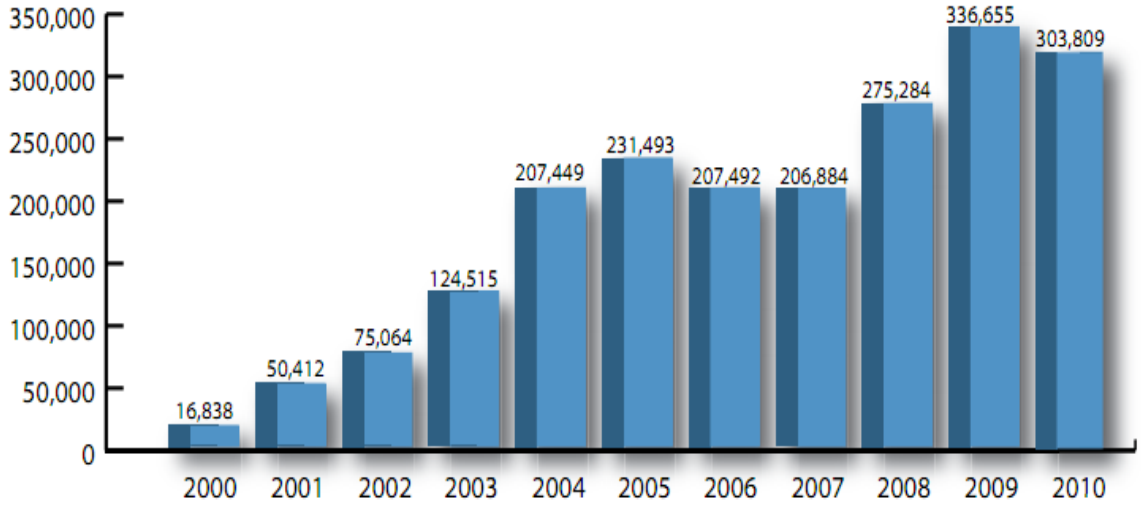
Slika 3. *Dio prezentacije Symantec-a nakon provedenog istraživanja*
Izvor: *symantec.com*

Napravljene su još mnoge statistike, poput broja žrtava cyber kriminala, najčešćih tipova žrtava i najčešćih vrsta kriminala, a potpune je rezultate moguće pronaći na web stranici Symantec-a, http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/.

3.2. Izvješće centra za prijavu zločina na internetu 2010.

Centar za prijavu zločina na Internetu (eng. *Internet Crime Complaint Center,* IC3) objavljuje na svojim web stranicama godišnja izvješća o broju prijavljenih slučajeva u toj godini. U 2010. godini najveći je broj prijavljenih zločina bio vezan uz neplaćanje ili neisporučivanje robe naručene preko Interneta, prijevara u kojima je počinitelj glumio da je iz FBI-a te krađa indentiteta.

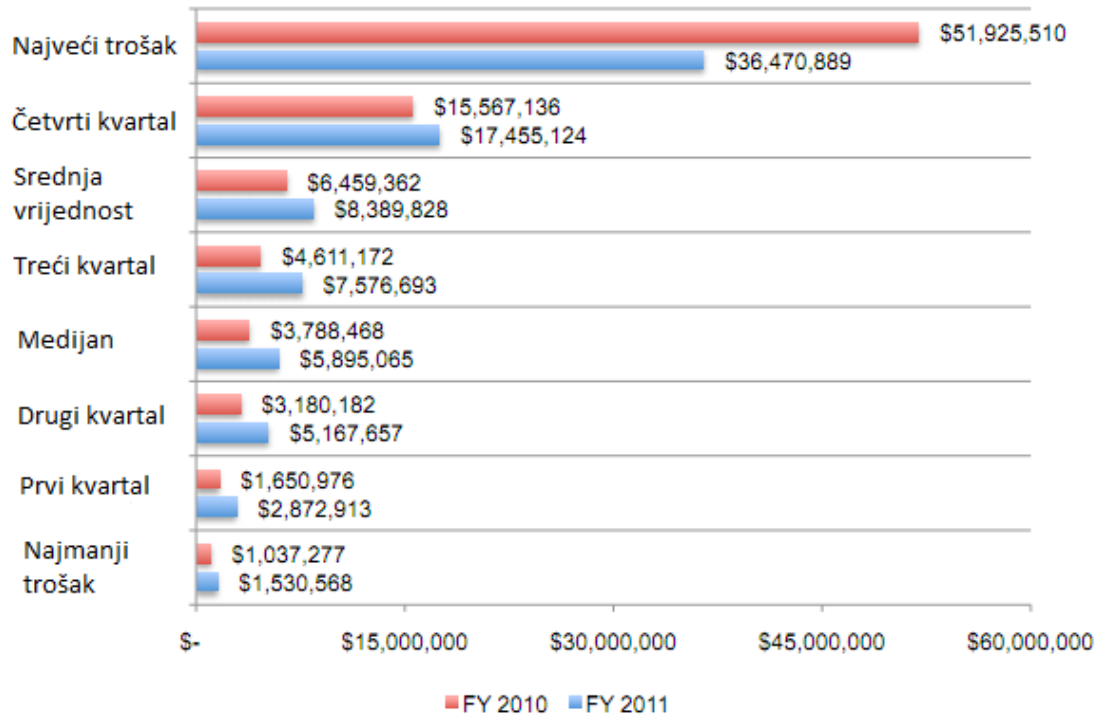
Slika 4 prikazuje graf s brojem prijava zaprimljenih u proteklih 11 godina.



Slika 4. *Broj prijava zločina na Internetu u proteklih 11 godina*
Izvor: *IC3.gov*

3.3. Istraživanje o troškovima cyber kriminala 2011.

U 2010. i 2011. godini provedena su istraživanja među 50 organizacija o šteti koju im je cyber kriminal nanio u toj godini. Medijan štete u 2011. godini iznosio je 5.9 milijuna američkih dolara, 55% više nego u 2010. kad je ta brojka iznosila 3.8 milijuna. Slika 5 prikazuje neke od statistika dobivenih ovim istraživanjem, te usporedbu sa 2010. godinom. Iz usporedbe se vidi da se šteta u 2011. povećala u sva četiri kvartala u odnosu na 2010. godinu. Jedina vrijednost koja je smenjena je najveća šteta u jednoj organizaciji, podatak koji sa stajališta ukupne procjene odnosa štete u 2011. i 2010. godini nije od velike važnosti.



Slika 5. *Statistike troškova organizacija koje su sudjelovale u istraživanju 2010. i 2011. godine*
Izvor: *acrsight.com*

4. Motivacija kriminalaca

U ovom će poglavlju biti opisani najčešći motivacijski čimbenici u cyber kriminalu. Zanimljivo je primjetiti da se zapravo radi o istim motivima kao i kod "klasičnog" kriminala, s izuzetkom da je zabava u cyber kriminalu mnogo češći motiv.. Razlog tomu je što većina cyber kriminalaca smatra da ih nikada neće uhvatiti i zbog toga imaju mnogo veći osjećaj sigurnosti u odnosu na „klasične“ kriminalce. U slučaju cyber zločina iz zabave taj je osjećaj sigurnosti najizraženiji jer počinitelji često ne razumiju ili ne smatraju da čine zločin.

4.1. Novac

Najčešći motiv za cyber kriminal je novac. Štoviše, novac je toliko čest i općenit motiv, prisutan u svim dobnim, spolnim i ekonomskim skupinama te ga je potrebno dodatno raščlaniti u nešto specifičnije slučajeve.

Najbezazleniji, ali i najčešći svakako je ilegalno preuzimanje zaštićenog materijala s Interneta, poput pjesama, filmova i raznih aplikacija. Profiliranje kod takvih zločina nije od koristi jer se i dalje radi o širokoj populaciji, a i broj slučajeva je prevelik. Međutim, profiliranje se može uspješno koristiti za određivanje profila osnivača stranica koje omogućuju ilegalnu distribuciju.

Slučajevi u kojima je profiliranje od puno veće koristi su online prijevare (eng. *scam*), krađa poslovnih tajni od organizacija (od strane unajmljenog hakera ili samih zaposlenika) i slični.

4.2. Zabava

Ilegalno preuzimanje zaštićenog materijala također se može protumačiti kao djelovanje zbog zabave. No, kao što je već spomenuto, broj osoba koje (čak i svakodnevno) čine taj zločin je prevelik za neku realnu korist od profiliranja.

S druge strane, zabava je često motiv za hakiranje, najčešće kod mladih, koji žele vidjeti mogu li oni to učiniti. Pritom obično ne razmišljaju o mogućim posljedicama svog djelovanja i šteti koju mogu prouzročiti.

4.3. Prestiž i medijska pažnja

Iskusniji hakeri ponekad napadaju samo iz razloga da pokažu da mogu te da se dokažu pred sebi sličnima. Slično, ponekad je motiv želja za medijskom pažnjom.

4.4. Emocije

Emocije su također čest motiv kod cyber kriminala. Objašnjenje se može naći u tome da se ljudi u iznimno emotivnom stanju (npr. bijes, ljubomora) puno teže kontroliraju na Internetu nego u stvarnom svijetu jer smatraju da ih štiti anonimnost te da ih nitko neće uhvatiti. U skupine koje se zbog emocija upuštaju u cyber kriminal spadaju otpušteni radnici koji žele nauditi organizaciji, ostavljeni ljubavnici koji progone svoje bivše i mnogi drugi.

Postoji još nekoliko motiva koji spadaju pod emocije, ali imaju određene specifičnosti. Radi se o politici i religiji te će oni biti obrađeni odvojeno.

4.4.1. Politika

Političke rasprave na Internetu znaju dovesti do oštrih svađa među neistomišljenicima koje ponekad kulminiraju cyber kriminalom.

4.4.2. Religija

S religijom je gotovo ista situacija kao i u slučaju političkih motiva. Međutim, religijske svađe znaju biti i puno većih intenziteta te dovesti do ozbiljnijih napada, kako u cyber svijetu, tako i u stvarnom svijetu.

4.4.3. Seksualni motivi

Zločini pogonjeni seksualnim motivima su specifični jer često prelaze iz cyber kriminala u silovanja, pedofiliju i slične teške zločine. Velikom porastu zločina s ovim motivima svakako je doprinio razvoj društvenih mreža zadnjih godina. U smislu čisto cyber zločina, najčešći su maltretiranja, ucjene i dječja pornografija.

5. Klasifikacija cyber kriminalaca

Kod profiliranja kriminalaca korisno je napraviti osnovnu klasifikaciju u nekoliko relativno općenitih profila na temelju određenih čimbenika. U slučaju cyber kriminala za takvu je klasifikaciju logično odabrati računalne i hakerske sposobnosti napadača te motiv. Ovdje će biti opisana klasifikacija koju je predložio prof. Marcus Rogers sa Sveučilišta Purdue. Nazivi pojedine skupine su slobodan prijevod naziva koje je iznio prof. Rogers.

- **Početnici**

  Početnici (eng. *Novice, Newbies*) imaju malo znanja o računalima i vrlo ograničene programerske sposobnosti. Zbog toga se prilikom napada uobičajeno koriste nekim jednostavnim alatima koje pronađu na Internetu. Budući da ne razumiju detaljno kako ti alati funkcioniraju, postoji opasnost da nenamjerno počine štetu mnogo veću od planirane. Dominantni motivi su zabava i želja za medijskom pažnjom.

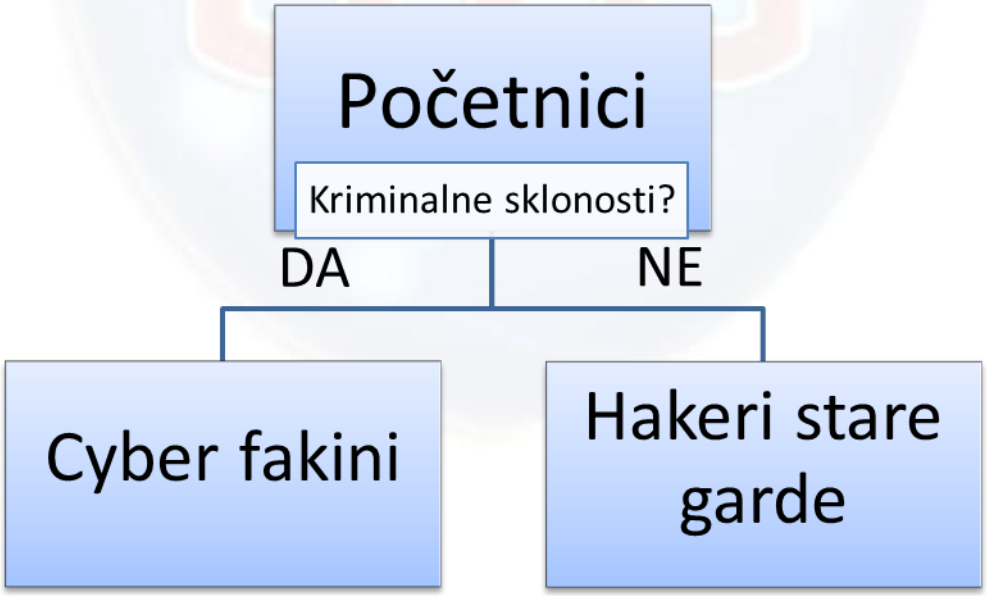
- **Cyber fakini**

  Drugu je skupinu Rogers nazvao "Cyber Punks", a u nedostatku boljih riječi u hrvatskom jeziku možemo ju prevesti kao "cyber frajeri" ili "cyber fakini". Oni imaju dovoljno programerskog znanja za razvoj vlastitog softvera te razumiju kako rade sustavi koje napadaju. Tipični motivi prisutni kod ove skupine su zabava i želja za dokazivanjem, ali ponekad sudjeluju i u prijevarama sa kreditnim karticama i sličnima nezakonitim radnjama isključiva radi novca. Često imaju izražen ego i vole se hvaliti nakon uspješnog napada. Najbliže odgovaraju stereotipnom hakeru jer često nisu društveni.

- **Hakeri stare garde**

  Treću skupinu čine hakeri stare garde (eng. *Old Guard Hackers*). Oni zapravo nemaju kriminalnih namjera, već nastoje što više unaprijediti svoja hakerska znanja. Drugim riječima, oni čine kriminalna djela jer "vježbaju".

  Postoji određena veza između prve tri skupine. Svi počinju kao početnici, a onda dolazi do grananja prema drugoj ili trećoj skupini, ovisno o kriminalnim sklonostima. Slika 6. **Blog dijagram odnosa između prve tri Rogersove skupine** Izvor: prikazuje blok dijagram odnosa između početnika, cyber fakina i hakera stare garde.



Slika 6. *Blog dijagram odnosa između prve tri Rogersove skupine*
Izvor: *CIS*

- **Koderi**

  Četvrta skupina su koderi, programerski vrlo vješti pojedinci koji sebe smatraju elitom. Pišu vlastite skripte i razvijaju alate, ali često bez namjere da ih sami upotrebljavaju. Umjesto

toga, objavljuju ih na Internetu kako bi dobili priznanje za svoj rad i znanja. Predstavljaju opasnost jer pišu i zloćudne programe.

- **Profesionalni cyber kriminalci**

  U petu skupinu, profesionalne cyber kriminalce, spadaju oni koji nude svoje usluge drugima u zamjenu za novac. Najčešće ih unajmljuju pojedinci i organizacije kako bi za njih špijunirali druge pojedince ili organizacije, ukrali im poslovne tajne ili na neki način onemogućili njihov rad. Imaju pristup najnovijoj opremi i iznimna programerska i računalna znanja. Motiv im je novac.

- **Cyber teroristi**

  Ova je skupina vrlo slična profesionalnim cyber kriminalcima, ali djeluje iz političkih ili religijskih motiva. Dobro su financirani i imaju pristup opremi, a svoje usluge nude i drugima.

- **Zaposlenici i bivši zaposlenici**

  Posljenju skupinu čine bivši i trenutni zaposlenici. Iako se na prvi pogled možda ne čini tako, posebice nakon do sada nabrojanih skupina, upravo su oni skupina koja izaziva najveću štetu. Prema nekim istraživanjima, odgovorni su za gotovo 70% ukupne štete počinjene cyber kriminalom.

  Imaju određenu razinu pristupa, što im olakšava krađu poslovnih informacija, te stoga predstavljaju najveći sigurnosni problem za organizacije. Koriste i znanja o sigurnosnom sustavu, kao i činjenicu da je sigurnosni sustav uvijek lakše probiti iznutra. Motiv im je u većini slučajeva novac, te ponekad emocije i osveta.

  S obzirom na korist od krađe može ih se podijeliti u dvije skupine. Prvu čine oni koji imaju veliku financijsku korist od počinjene krađe, a često su u dosluhu sa suparničkom organizacijom. U drugu skupinu spadaju mali lopovi, ponekad alkoholičari ili ovisnici, koji provode manje krađe kad im ponestane financijskih sredstava.

Tablica 1 prikazuje Rogersove kategorije cyber kriminalaca i njihove osnovne značajke.

Kategorija	Motivi	Vještine i znanja
Početnici	Zabava, učenje	Vrlo ograničene, koriste gotove dostupne alate
Cyber fakini	Dokazivanje, zabava, novac	Dobra programerska i računalna znanja, često pišu svoje alate
Hakeri stare garde	Učenje	Odlična programerska i računalna znanja
Koderi	Dokazivanje	Odlična programerska znanja, često pišu i zloćudne programe
Profesionalni cyber kriminalci	Novac	Odlična znanja, pristup modernoj opremi
Cyber teroristi	Politički i religijski motivi, novac	Vrlo dobra znanja, često pristup modernoj opremi
Zaposlenici	Novac, osveta	Variraju, imaju određenu razinu pristupa

Tablica 1. *Prikaz osnovnih Rogersovih kategorija cyber kriminalaca*

Izvor: *CIS*

6. Proces profiliranja

U nastavku će biti malo detaljnije opisan teorijski proces profiliranja cyber kriminalaca koji je ukratko opisan u drugom poglavlju.

6.1. Proučavanje žrtve i identifikacija motiva

Prvi korak u profiliranju cyber kriminalaca je identifikacija i proučavanje žrtve. Ako je moguće, potrebno je utvrditi što je sve u vezi žrtve moglo privući napadača. U cyber kriminalu ovaj proces ne daje toliko mnogo informacija kao u slučaju klasičnih zločina (npr. kod ubojstva, otmice ili krađe), ali je svejedno vrlo važan i može dati početne smjernice o kojoj bi se od osnovnih klasa cyber kriminalaca moglo raditi. Primjerice, ukoliko je žrtva velika organizacija kojoj su ukradene poslovne tajne, velika je vjerojatnost da se radi o zločinu nekog od sadašnjih ili bivših zaposlenika, a gotovo da se može eliminirati mogućnost da se radi o početniku.

Uvid u postupke žrtve u bliskoj prošlosti daje također vrijednu informaciju, npr. ako se radi o medijskom portalu, velika je vjerojatnost da je proteklih dana objavljen kontroverzni tekst koji je izazvao ljutnju kod jednog od čitatelja. U osnovi, proučavanje žrtve trebalo bi donijeti procjenu najvjerojatnijih motiva za zločin.

Ako se radi o većem zločinu, uvijek je korisno pratiti članke i rasprave na Internetu koji se bave tim zločinom.

6.2. Identifikacija osobina napadača

Nakon što je detaljno proučena žrtva na temelju procjena motivacije vrši se i procjena mogućih kategorija cyber kriminalaca. Važno je primjetiti da se u ovom koraku (u prvoj iteraciji postupka) za procjenu profila počinitelja koristi isključivo čimbenik motivacije, dok se čimbenik vještine analizira odvojeno, u idućem koraku. To omogućuje procjenu iz dva različita aspekta, a u pravilu i od različitih stručnjaka. Naime, u procjeni iz motivacije uobičajeno su aktivniji psiholozi, dok se procjenom vještine počinitelja bave stručnjaci za računalnu sigurnost.

Uz to, u ovom se koraku pokušava i detaljnije pristupiti klasifikaciji (ako je to moguće). Primjerice, ako se odredi da je najvjerojatniji počinitelj cyber terorist koji je iz vjerskih razloga srušio određenu stranicu, analizira se iz koje bi države on mogao biti. Kombiniraju se i podaci iz induktivnog profiliranja, traže se prijašnji zločini počinjeni sa sličnim motivom.

6.3. Analiza dokaza prikupljenih digitalnom forenzikom

U ovom se koraku pokušava odrediti vještina počinitelja, druga kategorija (uz motivaciju) prema kojoj je napravljena osnovna klasifikacija cyber kriminalaca. Rezultate digitalne forenzike treba tumačiti računalni stručnjak koji može ocjeniti koliko je „pametan“ bio počinitelj, je li mogao nešto napraviti učinkovitije, je li mogao nanijeti i veću štetu. Na temelju takvih procjena i informacijama o vještini pojedinih kategorija cyber kriminalaca moguće je osvježiti ranije donesenu odluku koja se temeljila pretežito na motivaciji napadača.

Naravno, moguće je i da se dogodi da digitalna forenzika ne da nikakve korisne rezultate. Međutim, u postupku profiliranja čak i nedostatak dokaza nosi određenu informaciju, a to je da se vjerojatno radi o vrlo vještom počinitelju.

Nakon što je završena i ova faza, potrebno je vidjeti jesu li možda neki dokazi prikupljeni digitalno forenzikom odbacili ili potvrdili prije postavljenu hipotezu, te je li potrebno iznova pristupiti prvom ili drugom koraku. Ako su iscrpljene sve mogućnosti, daje se konačna procjena profila počinitelja.

7. Organizacije za profiliranje cyber kriminalaca i budućnost profiliranja kao kriminološke discipline

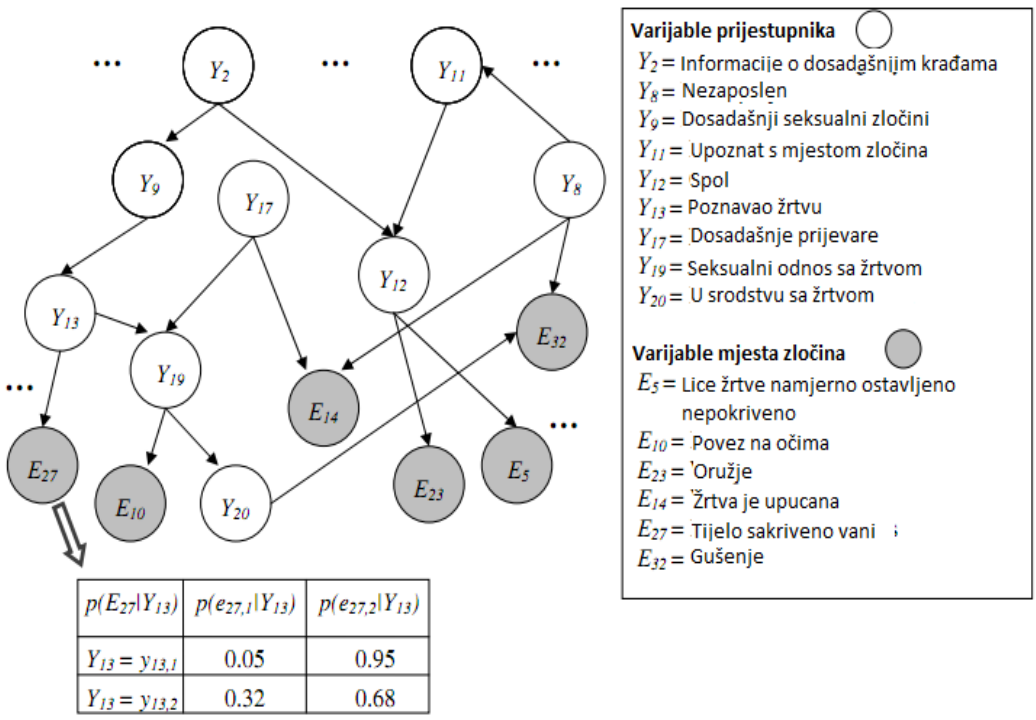
Do prije desetak godina cyber kriminal istraživao se jednako kao i ostali zločini, u policiji i organizacijama koje se bave istraživanjem i rješavanjem kriminala. Intenziviranjem borbe protiv cyber kriminala osnivaju se mnoge organizacije koje se bave isključivo problemom cyber kriminala. Ako se pokaže da profiliranje cyber kriminalaca daje dobre rezultate, logično je očekivati da će se u budućnosti početi pojavljivati i organizacije koje će se specijalizirati za taj problem. Danas se profiliranje, uz pomoć psihologa i računalnih stručnjaka, još uvijek provodi u organizacijama koje se bave spriječavanjem, otkrivanjem i rješavanjem cyber kriminala.

Profiliranje cyber kriminalaca još je uvijek vrlo mlada disciplina i veliki problem predstavlja činjenica da nije poznato kolika je korist od profiliranja cyber kriminalaca. Nije provedeno nijedno istraživanje koje bi prikupilo statistike o rezultatima i koristi profiliranja. Sve dok se do ne dogodi, ne može se reći sigurnošću koliko se isplati ulagati u ovu disciplinu. Sigurno je da postoji određena koristi, ali ovisno o tome kolika je potrebno je odlučiti hoće li profiliranje ostati na današnjoj razini, kao usputna pomoć kod traženja cyber kriminalaca, ili će se razviti u disciplinu koja će dati značajniji doprinos u globalnoj borbi protiv cyber kriminala.

Jedna od tehnika kojoj bi svakako trebalo dati više pažnje u budućnosti je primjena Baysovih i neuronskih mreža. Njima bi se profiliranje moglo djelomično automatizirati, a u kombinaciji sa iskusnim psiholozima mogle bi dati odlične rezultate. Postoji već niz radova na temu profiliranja kriminalaca pomoću navedenih metoda. Iako se istraživanja baziraju na korištenjem u „klasičnom“ kriminalu, moguće ih je primijeniti i za slučaj cyber kriminala.

Slika 7 prikazuje jednu Baysovu mrežu kakva se može koristiti za profiliranje ubojice. Na temelju infomacija prikupljenih na mjestu zločina i uz informacije iz rješenih prijašnjih sličnih zločina procjenjuju se varijable prijestupnika. Prema nekoliko provedenih testova, ovakva metoda pokazala se vrlo uspješnom u procjeni profila počinitelja.

Za slučaj cyber kriminala potrebno je pronaći drugi skup varijabli koje će što bolje opisivati zločin i počinitelja. Primjerice, umjesto varijeble oružje može se koristiti informacija o tipu napada.



$p(E_{27}\|Y_{13})$	$p(e_{27,1}\|Y_{13})$	$p(e_{27,2}\|Y_{13})$
$Y_{13} = y_{13,1}$	0.05	0.95
$Y_{13} = y_{13,2}$	0.32	0.68

Slika 7. *Baysova mreža za profiliranje ubojice*
Izvor: *Baumgartner et al. – Knowledge-Based Systems*

8. Zaključak

Rapidni porast cyber kriminala u posljednja dva desetljeća (između 50 i 100% godišnje) doveo je do toga da se danas godišnja šteta koju cyber kriminalci naprave može mjeriti u stotinama milijardi američkih dolara. Na cyber kriminal se počinje gledati kao i na ostale, „klasične“ tipove kriminala, iz kojih se preuzimaju neke tehnike suzbijanja i hvatanja počinitelja. Jedna od njih je i profiliranje kriminalaca, metoda kojom se iz prikupljenih tragova i statistika ranijih zločina nastoje što točnije odrediti neke psihološke osobine počinitelja.

U slučaju cyber kriminala postoje neke specifičnosti, prvenstveno tipovi dokaza i tragova te mjesto zločina. Osim toga, cyber kriminalci često nisu iz iste države kao žrtva, što donosi geografske, ali i velike zakonske prepreke. To otežava ili često čak potpuno onemogućuje profiliranje, a u slučaju male štete čini ga i financijski neisplativim.

Iako nije primjenjivo u mnogim slučajevima, korist od profiliranja cyber kriminalaca ipak je neupitna. U doba kad je cyber kriminal u rapidnom porastu potrebno je što više ovakvih metoda. Uz relativno mali trošak profiliranje povećava šanse za pronalaskom počinitelja ili čak spriječavanjem napada. Čak i s klasifikacijom cyber kriminalaca u nekoliko osnovnih skupina dobiva se puno informacija, te se u najmanju ruku može donijeti odluka o prioritetu rješavanja različitih slučajeva.

Velik potencijal u profiliranju kriminalaca imaju i neuronske i Bayesove mreže. Njihovo bi korištenje potencijalno moglo doprinijeti točnijem profiliranju te ubrzati i pojeftiniti cijeli proces.

9. Reference

[1] Hemamali Tennakoon, The need for a comprehensive methodology for profiling cyber-criminals
http://www.newsecuritylearning.com/index.php/feature/150-the-need-for-a-comprehensive-methodology-for-profiling-cyber-criminals, siječanj 2012.

[2] Ann Badnarz, Profiling cybercriminals: A promising but immature science
http://www.networkworld.com/supp/2004/cybercrime/112904profile.html, siječanj 2012.

[3] Deb Shinder, Profiling and categorizing cybercriminals
http://www.techrepublic.com/blog/security/profiling-and-categorizing-cybercriminals/4069, siječanj 2012.

[4] Kelly Jackson Higgins, The Art of Profiling Cyberiminals,
http://www.darkreading.com/insider-threat/167801100/security/vulnerabilities/232300211/the-art-of-profiling-cybercriminals.html, siječanj 2012.

[5] Norton Cybercrime Report 2011, http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/, siječanj 2012.

[6] Psychological Profiling,
http://www.sagepub.com/upm-data/23999_1___Psychological_Profiling.pdf, siječanj 2012.

[7] K. Baumgartner, S. Ferrari, G. Palermo, Constructing Bayesian networks for criminal profiling from limited dana
http://fred.mems.duke.edu/silvia.ferrari/downloadables/Ferrari/SamplePapers/KNOSYS1721.pdf, siječanj 2012.

[8] 2010. Internet Crime Report, http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf, siječanj 2012.

[9] Offender Profiling,
http://en.wikipedia.org/wiki/Offender_profiling, siječanj 2012.