

MOTIVI I PROFILI IZVRŠILACA

Srđan Mesarović spec.bezbednosti IS i e-poslovanja,
SŠ "Dr Đorđe Natošević"
Trg Slobode 2a, Inđija srki@vets.edu.yu

Abstrakt: *U ovom radu je sistematizovan materijal vezan za kompjuterski kriminal, motive i profile počinioca uz kratku statistiku razvoja kriminala i sa osvrtom na, za sada, neuspešnu borbu pravosuđa i sajber kriminalaca.*

Abstract: In this work has been sistematised the material connected to computer crime, motives, and profiles of perpetrators with the short statistics of the development of crime and looking back on, for now, an unsuccessful fight of the legal system with cyber criminals.

UVOD

Prošle, 2005. godine, po prvi put u istoriji, zarada od kompjuterskog kriminala premašila je onu ostvarenu prodajom ilegalnih droga. Prema komentaru Valeri McNiven, savetniku američkog ministarstva finansija "Kompjuterski kriminal napreduje takvom brzinom da ga snage zakona ne mogu stići".

Kompjuterski kriminal rapidno evoluirao i iz domena kompjuterskih zanesenjaka sve više prelazi u domen organizovanih kriminalnih grupa iz okoline ili sa drugog kraja sveta. Danas, 85% malware-a kreirano je sa ciljem sticanja profita, a samo 5% počinilaca je otkriveno i osuđeno.

Pored boljeg razumevanja kako kompjuterski kriminalci razmišljaju i deluju, ljudski faktor takođe treba da što bolje sagleda potencijalnu umešanost i bliske okoline u neželjene događaje. Organizacije bi trebalo bolje da sagledaju ceo svoj sigurnosni program i to ne samo sa tehničkog aspekta nego i na nivou sumnjivog ponašanja zapslenih.

Kompjuterski kriminal

Definisanje kompjuterskog kriminala je izuzetno teško, što proizilazi iz više razloga:¹

- reč je o *relativno novom obliku kriminalnog ponašanja*, koji se još nije u potpunosti izdiferencirao u odnosu na druge vidove kriminala;
- kompjuterski kriminal ispoljava *veliku fenomenološku raznovrsnost*, koja se teško može obuhvatiti jednom definicijom, bez obzira na njenu širinu i konačno;
- *retka su zakonodavstva koja poznaju kompjuterske delikte kao posebna krivična dela*, tako da se u ovom slučaju, nauka ne može u određivanju pojma kompjuterskog kriminala, oslanjati u većoj meri na pozitivnu krivičnopravnu legislativu.

Zbog specifičnosti računarskog kriminala, jednostavno nije moguće dati jedinstvenu definiciju.

Ekspertska grupa OECD dala je sledeću definiciju: "Kompjuterski kriminal predstavlja svako ilegalno, neetičko ili neautorizovano ponašanje koje uključuje automatsku obradu podataka ili njihov prenos."²

Sveobuhvatnu i opšteprihvaćenu definiciju u domaćoj literaturi dao je profesor Đorđe Ignjatović, određujući kompjuterski kriminal kao poseban oblik inkriminiranih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i softvera) pojavljuje ili kao sredstvo izvršenja ili kao objekt krivičnog dela, ukoliko se delo na drugi način, ili prema drugom objektu, uopšte ne bi moglo izvršiti ili bi ono imalo bitno drugačije karakteristike.

Poslednjih nekoliko godina broj krivičnih dela koji uključuju upotrebu računara i Interneta drastično se uvećao.

Kako u svemu ovome postoji i tehnološka priroda, postoje i jedinstveni izazovi u otkrivanju počinilaca. Na primer, kompjuterski kriminalci često koriste određene programe kojima prikrivaju sopstveni identitet, pa čak i ako budu otkriveni, često nastaje problem u njegovom izvođenju pred sud iz razloga što pravosuđe u državi u kojoj je počinjeno pomenuti kriminalno akt, uopšte ne poznaje kompjuterski kriminal kao jedno od kriminalnih dela. Kao rezultat svega, da bi kompjuterski kriminalac bio uhvaćen, pored tehnički obučanih inspektora koji moraju sarađivati sa stranim kolegama, veoma je važno i napraviti psihološki profil počinilaca i otkriti njihov motiv.

¹ Stamenković B., Đukić O., *Kompjuterski kriminal – opasnost na našem pragu*, 2001., <http://Arhiva.glas-javnosti.co.yu./arhiva/2001/09/22/srpski/D01092106.shtml>

² Đurić-Lulić A., op.cit.

Generalne karakteristike počinitelja

Računarski kriminal sa sobom donosi i novi profil kriminalca, hakera, koji uglavnom predstavlja mladu, ambicioznu osobu željnu znanja i napredovanja, ali koja često, upravo ostvarajući svoje želje, narušava bezbednost računarskih sistema. Ljudi a ne računari izvršavaju kriminalna dela i to uvek sa nekim razlogom. Različite vrste kriminala privlače različite tipove kriminalaca. FBI kategoriše kompjuterske kriminalce u tri različite kategorije: (*hakere*) *krakere*, *kriminalce* i *vandale*. Puni opis FBI matrice kompjuterskih kriminalaca i kriminala dat je u literaturi [5].

Kompjuterski kriminalci predstavljaju različite tipove ličnosti koje možemo pronaći u svim društvenim slojevima. Pa ipak, uvek postoji bar mala doza razlika ljudske ličnosti koja čini razliku između kriminalca i ne-kriminalca. Vidljivi motivi nisu dovoljni da se neko definiše kao kriminalac. U slučaju kompjuterski kriminalaca, takođe je potrebno i razumevanje mrežnih tehnologija na visokom nivou. Može biti jednostavno upotrebljavati Internet, slati elektronsku poštu ali neovlašćeno pristupiti drugom računaru ili mreži zahteva više od opšteg informatičkog znanja. Potrebno je mnogo vremena da bi se dostigao takav nivo znanja da bi se počinilo delo kompjuterskog kriminala i neopaženo nestati „sa lica mesta“ što objašnjava činjenicu da su kompjuterski kriminalci po pravilu specijalizovani za jedan oblik kriminalnih radnji.

Profil savremenog kompjuterskog kriminalca se često veoma brzo menja. Ako mislite da haker sedi na pragu fakulteta ili u nekom podrumu, razmislite opet. Prema rečima Dona Pipkina, autora knjige "Zaustavljanje hakera" hakeri su poslednjih godina izuzetno napredovali. Postoje napadi koji su vidljivi kao što su distribucija virusa ili napad na web stranice. Ovi napadi su najčešće izvršeni kao stvar dokazivanja pred drugima da su oni sposobni da to učine. Postoji i mnoštvo drugih napada, koji nisu vidljivi i odnose se na narušavanje integriteta i tajnosti informacije koje se žele sačuvati kao što su podaci o platnim karticama ili tajni podaci manjih i većih kompanija. Ovakvi tipovi napada su neprimetni onoliko koliko je to moguće da bi se došlo do željenih informacija.

Motivi

Ne može se govoriti o jedinstvenom profilu počinitelja kompjuterskog kriminala, jer se oni svrstavaju u različite kategorije prema pojavnim oblicima dela koja čine, ali i prema motivima, koji ih pokreću u vršenju kriminalnih aktivnosti. Postoje dve tipične grupe kompjuterskih kriminalaca i to:

- Amateri – povremeno se upuštaju u kriminal. Uglavnom čine kompjuterske krađe, pronevere i sabotaze,
- Profesionalci – kriminal im je često jedino zanimanje. U organizacionom smislu nastupaju pojedinačno, u grupama ili kao članovi organizacija.

Uopšteno bi se svi počinioци ovih dela mogli podeliti na *zlonamerne*, koji mogu da deluju radi ostvarenja imovinske koristi, ili samo u cilju nanošenja štete, kao i na učinioce koji nisu motivisani ni ostvarenjem koristi, niti prouzrokovanjem štetnih posledica, već jednostavno traže zadovoljstvo u neovlašćenom prodiranju u neki dobro obezbeđen informacioni sistem. Reč je o tzv. "*hakerima*" (eng. *hackers*), koji koristeći svoje računarsko znanje, uz pomoć modema upadaju u tuđe kompjuterske sisteme. Hakerski rečnih definiše hakera kao osobu koja uživa u korišćenju programabilnih sistema i ima eliku želju da proširi njihove mogućnosti za razliku od većine korisnika koji teže tome da nauče dovoljan minimum. Ovi počinioци predstavljaju svojevrsne *kompjuterske entuzijaste*, koji provaljujući u dobro čuvane informatičke sisteme izivljavaju svoju strast za

avanturama po tzv. "informacionim autostradama" u specifičnom kibernetičkom prostoru (eng. *cyber-space*)³.

Postoji i posebna vrsta hakera kojima posao kojim se bave predstavlja zabavu. Obično se odnosi na mlade ljude koji su tek učli u svet hakera. Većina njih isprobava mnoge načine hakovanja u cilju prepoznavanja koji način funkcioniše, a koji ne. "Scamps" su tzv. šaljivi hakeri koji ne čine ništa više od neovlašćenih ulazaka u web sajtove i postavljanja određenih poruka ili fotografija iz razloga većeg respekta među hakerima. Takođe, među njima ima i onih koji osećaju uzbuđenje u pokušajima da prođu u obezbeđen sistem čak i bez namere da načine štetu. Iz njihovog gledišta, ovi motivi su zanemarljivo štetni, međutim čest proboj sistema na ovaj način predstavlja izazov za ozbiljnije hakere i daleko štetnija kriminalna dela.

U WWW društvu danas treba dodati individue koje iz političkih i socijalnih razloga šire *online* grafite menjajući *web* stranoce svojih protivnika.

Prema razlogu bavljenja hakovanjem, mogli bi ih podeliti u tri osnovne grupe:

- Kreativci – ovoj grupi pripada većinski deo hakerske populacije i čine je pojedinci avanturističkog duha, koji hakiranje shvataju kao istraživanje, stručno usavršavanje, intelektualni izazov, zabavu, bez ikakvih zlih namera i negativnih posledica. Ova grupa može biti čak i vrlo korisna ako se sa njom uspostavi korektna saradnja, jer su u stanju da otkriju mnoge slabosti u sistemu zaštite. Često ih velike organizacije unajmljuju u cilju testiranja sopstvenog sigurnosnog sistema. Nažalost, njihovo uspešno probijanje sistema zaštite često dovodi do velike ekonomske štete ili oštećenja sistema;
- Destruktivci - ovoj grupi pripadaju oni kojima hakovanje predstavlja mogućnost namernog uništavanja i izmene sadržaja napadnutih sistema, posebno korišćenjem virusa ali i direktnim delovanjem. Ova grupa hakera se često naziva krakeri (*cracker*), zbog svojih malicioznih osobina;
- Kriminalci - čine ih pojedinci čiji je osnovni motiv hakovanja ostvarivanje protivpravne imovinske koristi. Krađu tuđe industrijske i nacionalne tajne, krađu novac, uništavaju datoteke, OS ili menjaju podatke Web stranica ili baza podataka. Napadači koriste različite tehnike za slabljenje sistema. Pogađanje lozinki, socijalni inženjering, mapiranje (sekvencijalno pozivanje telefonskih brojeva tražeći odziv modema), virusi i trojanski konji su samo neki primeri takvih tehnika. Zavisno od tipa organizacije počinioци mogu biti špijuni, organizovani kriminalci ili male grupe krakera, samostalne ili povezane sa međunarodnim organizacijama.

Zlonamerni učinioci kompjuterskih delikata su najčešće motivisani *koristoljubljem*, a smatra se da podaci iz prakse ukazuju na određeni skup osobina koje čine njihov kriminalni profil. Oko 80% ovih delinkvenata čini delo po prvi put; 70% je zaposleno više od pet godina u oštećenom preduzeću; njihovo starosno doba je u proseku između 19 i 30 godina; pretežno su muškog pola; veoma su inteligentni; imaju uglavnom više godina radnog iskustva i važe kao savesni radnici koji prilikom obavljanja radnih zadataka ne prouzrokuju nikakve probleme; često su tehnički kvalifikovaniji nego što to zahteva radno mesto na koje su raspoređeni; ovi učinioci sebe po pravilu ne smatraju kradljivcima ili uopšte kriminalcima, već samo pozajmljivačima, a kod njih je ponekad, naročito ukoliko su meta njihovog delovanja veoma bogate i finansijski moćne multinacionalne privredne korporacije prisutan i tzv. "*sindrom Robina Huda*", kada oni sebe doživljavaju kao svojevrsne "borce za pravedniju raspodelu bogatstva".⁴

Redovno se radi se o mladim osobama, prosečne starosti dvadeset i pet godina, koji u najvećem broju slučajeva nisu ranije dolazili u sukob sa zakonom; u pogledu formalnog obrazovanja ne postoji pravilo, obzirom da se znanje za rukovanje kompjuterom relativno lako stiče i bez pohađanja određenih škola ili fakulteta; u pogledu ličnih osobina, radi se o inteligentnim osobama, potpuno

³ Škulić M., op.cit.

⁴ Škulić M., op.cit.

otvorenim za praćenje tehnološkog napretka, dok su na intimnom planu vrlo često neostvareni i kompjuter za njih predstavlja centar njihovog života.

Jedna od najnezgodnijih grupa koja ima za cilj ne koristoljublje već želju da naprave što veću štetu su oni koji to čine iz besa ili osvete kao što su npr. ostavljeni ljubavnici ili supružnici, otpušteni radnici, prevareni biznismeni. Bes može predstavljati razlog za bilo koji oblik počinjenog kriminalnog dela. Oslobođanje adrenalina kao efekat ima privremen prekid razumnog i racionalnog razmišljanja. Svi koji osećaju da im je naneta nepravda, mogu biti pripadnici pomenute grupe počinilaca. Ozbiljnost načinjene štete direktno zavisi od ličnog osećaja povređenosti. Jedino što je sigurno, dela učinjena iz besa po pravilu su loše zamišljena i neprofesionalno izvedena.

Jedan od veoma čestih motiva, naročito izražen kod tinejdžera su hakovanja s ciljem dokazivanja među svojim vršnjacima.

Takođe, postoje i politički motivi gde počinioци obično sve pripisuju svojim ideološkim protivnicima, levici ili desnici. Mrežu uglavnom koriste retko i to pre svega u propagandne svrhe ali mogu i oštetiti ceo sistem suprotstavljene strane ili jednostavno povećati sopstveni uticaj ili uticaj stranke eksponiranjem celog slučaja u štampi.

Poslednjih godina sve su rašireniji slučajevi seksualnog uznemiravanja i trgovine belim robljem kao i pedofilijom putem Interneta. Pasivni pedofili sa Interneta skidaju slike dečije pornografije. Grubo kršenje dečijih prava preuzimanjem ovakvih fotografija je ono što dečju pornografiju čini nelegalnom. Seksualno motivisani kompjuterski kriminalci obuhvataju kako pasivna tako i aktivne pedofile kao i serijske silovatelje. Kako god, aktivni pedofili se ne zaustavljaju samo na fantaziranju i koriste chat sobe kako bi postali prijatelji sa decom da bi nakon toga i ugovaranja sastanka izvršili silovanje ili se odlučiti za drugu opciju. Ta druga opcija predstavlja postepeno uvlačenje dece u imaginarnu dugotrajnu seksualnu vezu. Oba slučaja dovode do visokih kazni otkrivenih počinilaca. Serijski silovatelji imaju želju isključivo da se susretnu sa žrtvom na mračnim i usamljenim mestima, a mrežu koriste kao podršku zločinu iz realnog sveta. Neki kriminalci takođe pripadaju ovoj kategoriji.

Najređi ali i potencijalno najopasniji kompjuterski kriminalci su mentalno poremećene osobe. Oni koji pate od šizofrenije, depresije, manije, podeljene ličnosti i sl. su po pravilu odbačeni od društva i kao takvi, u sajber svetu, mogu pronaći mesto gde će njihova prava ličnost biti skrivena i gde će moći da žive van svojih fantazija. Ovi kriminalci mogu potencijalno biti vrlo teški za pronalaženje zbog njihove nelogične i nerazumljive motivacije kao i nepredvidljivih akcija. Ovo se posebno odnosi na visoko inteligentne osobe koje su se našle u ovoj kategoriji.

Generalni tipovi

Profilisanje kriminalaca je izuzetno važan aspekt istražnog postupka, bilo to su realnom ili sajber svetu. Istraživači i psiholozi su potrošili godine rada izučavajući način rada i pozadinu kriminalaca. Upotrebom statistike i komparativnih metoda, informacije prikupljene iz celog sveta su obrađene i iskorišćene u sačinjavanju profila kriminalaca. Naravno, najveći problem je u tome što mnogi kriminalci ne odgovaraju direktno postavljenim šablonima što drastično otežava ili usporava istragu. U nastavku teksta biće predstavljeni, koliko je to moguće, generalni tipovi kompjuterskih kriminalaca.

Kriminalci belih kragi (eng. White-collar criminals)

Obično se pretpostavlja da osobe sa niže društvene lestvice i lošeg materijalnog stanja čine kriminalna dela. Međutim, u stvarnosti, sasvim je logično da onaj ko ima mnogo novca, želi da ga ima još više. Kvalifikovani za mnoštvo različitih složenih kriminalnih dela i dovoljno obrazovani d aznaju šta pred zakonom može, a šta ne , da prođe, takvi kriminalci su daleko izgledniji počiniooci nego što mnogi u to žele da poveruju. Izraz „bele košulje“ je nastao od kancelarijskih službenika i njihove uobičajene odeće. Njihovi motivi su različiti, a ono što im je zajedničko je to da ih je veoma teško otkriti iz razloga što su po pravilu visoko obrazovani, znaju za „rupe“ u zakonu, imaju mnoštvo otvorenih bankarskih računa širom sveta, svojim poslom, stilom i načinom života skidaju svaku sumnju u očima običnog sveta, pametno isplaniraju svoje delo i uvek imaju rezervnu opciju ako ne krene sve po planu. Osnovni tipovi ovih kriminalaca su:

- Osvetoljubivi kriminalci Potencijalno nastaju usled otkaza na poslu, kaznenog odbijanja od plate i sl. Usled nekih od navedenih razloga, javlja se želja za osvetom kompaniji što je olakšano s obzirom da dovoljno dobro poznaju sistem rada kompanije i sve njene sigurnosne slabosti;
- Strpljivi kriminalci Problematici su zbog stanja njihovog uma i što to nije uočljivo odmah. Obično svoje delo sprovode u stvarnost dug niz godina. To se najčešće ogleda u sitnim krađama od po nekoliko \$ od stotina ili hiljada ljudi koje niko ne prijavljuje, a koje nakon nekoliko meseci ili godina predstavljaju značajnu sumu ukradenog novca;
- Očajni kriminalci Predstavljaju osobe koje se nalaze u finansijskoj krizi u koju su najčešće upale kockanjem ili svojim životnim stilom. Veoma ih je lako otkriti jer pritisnuti problemima veoma često prave nepromišljene poteze koji ih odaju. Najbolji pokazatelj je nagli rast sredstava na tekućem računu.

Kriminalci se javljaju u svim društvenim slojevima, a ono što je začuđujuće, zavidan deo ih pripada višim slojevima društva što iziskuje pažljivu proveru pojedinaca pri zapošljavanju ili već zaposlenih na odgovornim mestima.

Psihijatrijski slučajevi

Kao što je prethodno rečeno, veoma mali broj kriminalaca nema niti jasan motiv izvršenja određenog kriminalnog dela niti kontrolu nad svojim akcijama. Ovakav tip kriminalaca predstavlja psihijatrijske slučajeve. Ovoj grupi pripadaju takođe i pedofili, sajber lovci (eng. cyberstalkers) i sajber teroristi.

Problem kod ovih osoba je što često deluju kao normalne osobe pa samim tim predstavljaju osobe koje su veoma opasni kriminalci. Isto tako, njihov totalno nelogičan i nerazumljiv način razmišljanja je otežavajuća okolnost u otkrivanju ko su, gde su i kad će sledeći put napasti. Osnovni tipovi ovih kriminalaca su:

- Pedofili U stvarnom svetu, pedofil je onaj koji ima nenormalan seksualni nagon prema deci. U sajber svetu, postoji širi opseg žrtava. U globalu, postoje dve vrste pedofila, pasivni koji skidaju sa Intreneta i uživaju u slikama i video materijalima nage dece i aktivni

pedofili koji se preko chat soba zbližavaju sa decom što kasnije često dovodi do silovanja pa čak i ubistava čime se već prelazi u stavan svet.

- Noćni lovci Nisu toliko štetni kao aktivni pedofili, često čekaju u senci i posmatraju svoju žrtvu. Na internetu žrtva ne može tako lako da se oslobodi nametljivosti sajber lovca niti da ga zamoli da prestane i odustane. Lovac je ovde u prednosti i ako je veoma pametan, znaće kako da uznemirava, ometa, izaziva bes, muči, kinji, proganja i na kraju izbegne način da bude uhvaćen. Postoje dva tipa slučajeva: lovac i žrtva se ne poznaju il lovac i žrtva se znaju ali je u pitanju davno raskinut odnos. U drugom slučaju cilj lovca je da se revanširaju za nešto što im je ta osoba davno učinila i često nema seksualne note u celom slučaju. Žrtva često biva zastrašivana putem telefona, elektronske pošte, hakovanjem računara i sl. Međutim, češći i opasniji slučaj je kad se lovac i žrtva ne poznaju.
- Serijske ubice Verovatno najopasnija vrsta sajber kriminalaca. Nepredvidljivi su i uvek imaju plan koga će napasti. Internet im uglavnom služi da odaberu i prate žrtvu. Postoje dva tipa ubica, onaj neorganizovan, asocijalan, sa niskim IQ i koga je lakše otkriti ali i veoma opasan s obzirom na kombinaciju želje za ubistvom i malom inteligencijom. Drugi tip ubice je organizovan, tačno zna šta želi, kako da do toga dođe i kako da pobjegne. Primer ovog tipa ubice je dr Hanibal Lektor u filmu „Kad jaganjci utihnu“.

Glumci (eng. Con Artist)

Predstavljaju verovatno najlukavije tipove sajber kriminalaca. Kao kameleoni menjaju svoj izgled i karakter prema situaciji sa ciljem obmanjivanja žrtve i sticanja novčane dobiti. Obično su veoma prijateljski nastrojeni, šarmantni i veoma ljubazni, a sve to sa ciljem skidanja eventualne sumnje u očima buduće žrtve. Osnovni motivi ovog tipa sajber kriminalaca su:

- pritisak za brzom zaradom - na bilo koji način;
- želja za iskorišćavanjem ljudi - izmišljenim pričama naterati žrtve da čine sve što on poželi;
- izazov;
- kažnjavanje žrtve – veruju da neke žrtve zaslužuju ono što im čini i da ih uči lekciju pljačkajući ih.

Tehnike koje glumci koriste su uglavnom veštačko prijateljstvo dok odabrana buduća žrtva ne prestane da sumnja u doskorašnjeg stranca, visoke kamate na štednju, vršenje pritiska u vidu ponude koje predstavljaju „životne šanse“ i zbog kojih će se žrtva kajati ako je ne prihvati kao i elokventnost gde uz sastavljenu priču i „poznavanje“ svake teme dovodi žrtvu u uverenje da je u pitanju obrazovan stručnjak koji zna o čemu priča pri čemu se žrtvi ne ostavlja ni malo vremena da eventualno postavi neko pitanje.

Hakeri

Hakeri najčešće izvode akcije iz razloga dokazivanja pred drugima, pomoći „kolegama“ ili da bi skrenuli pažnju javnosti na sebe. Ukupno gledano, motivi su različiti. Graboski i Smit grupisali su moguće motive hakera. Kompjuterski kriminal definišu kao neovlašćen pristup računarskom sistemu. Kao što su autori naveli, razloge koje navode hackeri treba uzeti sa rezervom s obzirom da za njih uvek postoji razlog. Razlozi, odnosno motivi za hakovanje su podeljeni u dve grupe zavisno od nivoa privlačenja pažnje i proistekle štete.

Motivi koji privlače manju pažnju::

- finansijska dobit;
- intelektualni izazov;
- moć;
- samodokazivanje;
- mladost, nerazumevanje učinjenog dela....

Motivi koji privlače veću pažnju:

- osveta;
- napad na sistem;
- terorizam;
- uzimanje pravde u sopstvene ruke
- “testiranje” sigurnosti sistema.

Kilger je takođe grupisao motive hakera pod skraćenicom MEECES, direktno aludirajući na FBI skraćenicu MICE-novac, ideologija, nagodba i ego (eng. *money, ideology, compromise and ego*). MEECES predstavlja skraćenicu za novac, zabavu, ego, mržnju, ulazak u socijalnu grupu i status (eng. *money, entertainment, ego, cause, entrance to social groups and status*). U oba slučaja, neopravdano je izostavljena radoznalost kao jedan od motiva. Kombinujući radove Kilgera odnosno, Graboskog i Smita mogu se izdvojiti šest osnovnih motiva. Dok motivi kao što su novac, zabava, ego pripadnost određenoj socijalnoj grupi i zadovoljenje “pravde” ne zaokupljaju toliku pažnju, najozbiljnije se treba pozabaviti mržnjom kao motivom koja obuhvata osvetu, napad na državni sistem i terorizam i kao takva, predstavlja najopasniji motiv.

Novac

Načini za nelegalnu zaradu uključuju malverizacije sa kreditnim karticama i bankomatima, pirateriju, krađe podataka, narušavanje pravilnog funkcionisanja telefonskih servisa, preprodaju email adresara...

Zabava

U pitanju je hakovanje iz čistog zadovoljstva koje može izazvati neželjene posledice.

Ego: intelektualna nadmoć

Kod hakera sa ovim motivom, cilj je ulaziti u što bolje obezbeđene i sofisticiranije sisteme. Tipični predstavnici ovih grupa su kreatori virusa. Simon Valor, koji je napisao viruse ResediB, Admirer i Gokar pravdao se da je to učinio samo da vidi da li je sposoban za to. Osuđen je na dve godine zatvora.

Sticanje statusa u određenim društvenim grupama

Stereotipna slika predstavlja hakera kao usamljenog kompjuterskog zanesenjak koji isteruje "svoju pravdu" čime se hakerska zajednica, koja definitivno postoji, lini veoma razjedinjenom. Neki hakeri iskreno veruju u članstvo u zajednici u kojoj su sa ciljem deljenja iskustva. Međutim, ono što je karakteristično za ovakve zajednice, to je da postoje podgrupe među kojima vlada veliki rivalitet. Možda je najilustrativniji primer Dejvida Smita, tvorca crva Melisa, koji je hakovanje koristio kako bi dobio viši status u *mainstream* društvu. Kao karakterističan slučaj, može se pomenuti i Adrian Lamo koji je upadao u računarske sisteme velikih korporacija, a zatim se nudio da ih popravi besplatno.

Zadovoljenje pravde

Hakeri mogu vršiti akcije i bez osećaja samozadovoljnosti. U stanju su svesno da čine štetu. Isto tako mogu se pravdati testiranjem sistema kao što je načinila grupa studenata provalivši u računarsku mrežu Univerziteta Oksford i zatim to iskustvo objavila u studentskom časopisu. Ima i onih koji istragu drugih hakera preuzimaju na sebe i pomažu službenim organima. Jedan takav slučaj je zabeležen u Turskoj gde je lokalni haker ponudio informacije koje su dovele do otkrivanja njegovog "kolege" u SAD koji je računar koristio za dečju pornografiju.⁵

Mržnja

Hakeri mogu, motivisani mržnjom prema nekoj korporaciji, kao što je bio slučaj sa Microsoft-om ili SCO, organizovati široko rasprostranjene i sinhronizovane napade na iste.

Isto tako mogu biti motivisani lično doživljenom nepravdom iskaljujući bes na pojedinca ili korporacije. Jedan od primera takvih napada je bio upad i narušavanje sistema za odvođenje otpadnih voda što je dovelo do toga da se iste izliju u vodovod. Počinilac je kažnjen sa dve godine zatvora.

Uopšte, hakovanje ima mogućnost da izazove štetu ili samo poveća nesreću koju je nešto drugo izazvalo. kao glavne mete ovih hakera su sistemi od ključnog značaja za državu: energija, komunikacije, zdravstvo, opasne materije i sl.

Vrste hakera

U današnje vreme postoji više tipova hakera ali je ustaljeno mišljenje o hakerima kao o osobama koje provode mnogo vremena uz računar izučavajući kako uopšte funkcionišu računarske mreže i kako pristupiti nečijem sistemu. Međutim, danas je reč „haker“ sve više vezana za pojam sajber kriminalca koji krši zakon putem računara i računarskih mreža.

Tipovi:

Hakeri stare škole	Predstavljaju profesionalce starije generacije koji često biva-ju unajmljeni od organizacija kako bi testirali njihovu mrežnu sigurnost. Često im predstavlja uvredu kad današnje hakere nazivaju tim imenom;
Unutrašnji hakeri	Predstavljaju uglavnom zaposlene radnike razočarane upra-vljanjem u organizaciji ili bivše zaposlene koji znaju za bez-bednosne propuste u organizaciji kao i procedure interne istrage;
Cyber punk	Poznati i kao šaljivdžije, često su neshvaćeni od okoline, bolje komuniciraju sa računarima nego sa ljudima i više su nego sposobni za pisanje malicioznih kodova. Krše zakon

⁵ *US v Steiger* 2003 WL 115261 (11th Cir. 2003); *US v Jarrett* 338 F. 3d 339 (Va., 2003)

	upadajući u sisteme gde mogu nenamerno naneti štetu. Uglavnom su akteri spam-ovanja, krađe podataka vezanih za platne kartice ili izmena izgleda web strana;
Profesionalni kriminalci i sajber teroristi	Definitivno su najopasniji, često su u pitanju bivši obaveštajci koji su dobro upoznati sa putevima trgovine umetničkim delima, sa industrijskom špijunažom i savršeno su obučeni da izvrše dobro koordinisanu akciju koja će izazvati štetu većih razmera. Oni kod kojih je ostalo još malo profesionalnog ponosa, izbegavaju rušenje sistema i zadovoljavaju se krađom obaveštajnih podataka;
Skript klinici	U pitanju su uglavnom tinejdžeri koji se žele predstaviti kao iskusni hakeri ali im nedostaje sposobnost i iskustvo. Koriste programe krekovane od strane drugih kako bi napravili štetu nad napadnutim sistemom. Skoro uvek budu otkriveni jer im cilj i jeste da skrenu pažnju na sebe.

Krakeri

Krakeri predstavljaju osobe koje su zadužene za kršenje autorskih prava nad programima ili muzičkim fajlovima tj. svemu onome što je potrebno regularno platiti. Često ih poistovećuju sa hakerima s obzirom da imaju slične poglede na svet i jedni i drugo pripadaju sajber kriminalcima. Međutim, postoji značajna razlika među njima. Krakeri sve čine u korist širokih narodnih masa koje odbijaju ili nemaju da plate korisnička prava dok su hakeri pre svega okrenuti sebi. Postoje tri tipa krakera: krakeri lozinki, krakeri izvršnih programa i hobisti od kojih su ovi poslednji najbezazleniji.

- Krakeri lozinki Okrenuti su kriptologiji i osnovna briga im je kako da razbiju određeni kriptografski algoritam. Izučavaju što je moguće više o slabostima u kriptografiji pokušavajući da stečeno znanje prime- ne na malom komadu šifrovanog materijala do kojeg su došli. Da bi uspeli u svojoj nameri, posegnuće za svakim metodom koji poznaju, koristeći trojance ili možda ići i direktnom silom tj. isprobavati sve moguće kombinacije;
- Krakeri izvršnih programa Veruju u sopstveni princip da su programi pravljeni da bi izvrša- vali zamisli ljudi pa da onda nema ničeg lošeg u tome da ih izmene i uklone njihovu limitiranost (npr. demo verzija) osim što će napraviti štetu njihovim kreatorima. Ovakve sposobnosti se stiču nakon višegodišnje programerske prakse;
- Hobisti Predstavljaju mešavinu prethodne dve pomenute grupe. Bave se krekovanjem čisto zbog sticanja znanja. Obično imaju dosta vremena utrošenog na učenje i povremeno se bave krekov- njem lozinki ili izvršnih programa. Većina od njih krekovanje vrši po potrebi „za javnost“ kako bi dokazali svoju umešnost.

Zablude o sajber kriminalcima

Holivud često sa simpatijama prikazuje sajber kriminalce kao borce za ljudska prava i protivnike surovih i beskompromisnih vlada i korporacija.

Za većinu pogrešnih shvatanja o sajber kriminalcima nema opravdanja. U celoj priči postoji samo delić istine i to: sajber kriminalci zaista moraju biti tehnički veoma

obrazovani i inteligentni kako bi ostali neuhvatljivi. Kao i u realnom svetu kriminala, među sajber kriminalcima daleko su više zastupljeni muškarci nego žene. Uglavnom ne odgovaraju tipičnim profilima kriminalaca što je otežavajuća okolnost koja izaziva lako bekstvo predstavnicima zakona. Zablude o sajber kriminalcima su:

Zabluda 1: Svi sajber kriminalci su zanesenjaci – pametni ali nedruštveni

Ovaj stav se može opisati slikom gde student nekog tehničkog fakulteta po ceo dan sedi pred monitorom i grozničavo kuca po tastaturi. Pri tome je tehnički savršeno opremljen i nema ni malo vremena za druženje sa vršnjacima. U današnje vreme, dostupnost računara i opreme dozvoljava skoro svakome da bude sajber kriminalac samo ako to želi. Potrebno je samo da se posveti tome, da bude društven, da ima harizmu, da bude slatkorečiv i da poznaje ljudsku psihu kao i način razmišljanja onih kojima treba da provali u sistem.

Zabluda 2: Svi tinejdžeri sa računarima su sajber kriminalci

Televizija je kriva za ovaj stereotip gde dečak sedi u podrumu i pomoću svog računara pristupa bez problema najčuvanim državnim i vojnim sistemima i radi sve ono što rade profesionalni teroristi. To što je sad daleko lakše biti haker nego ranije, ne znači da je povećan broj tinejdžera koji se time „zabavljaju“. Takvi incidenti se dešavaju jednom u milion slučajeva. U ostalim slučajevima se uspeh svodi na pristup određenim sajtovima odakle može besplatno da se skinu muzika ili filmovi.

Zabluda 3: Sajber kriminalci nisu „pravi“ kriminalci

Zanimljivo je da većina sajber kriminalaca veruje u ovu tvrdnju u čemu nalaze opravdanje za ono što čine. Popularnost chat-ovanja pod pseudonimima povećava uverenje da je sajber svet izdvojen od realnog sveta. Ovo omogućava kriminalcima da zanemare etiku i moral. Sajber lovci, pedofili, *OnLine* ucenjivači su sve češće pojave. Mnogi od njih traže žrtve preko Interneta bez mogućnosti da nekom slučajnom prolazniku „zapadnu za oko“ i postanu sumnjivi. Takođe, velik problem je i pojava sajber terorizma koji omogućava izvršenje terorističkih akata sa veoma velikim posledicama, a pri tome i zanemarljivom opasnošću po sajber teroriste..

Zabluda 4: Svi sajber kriminalci imaju iste karakteristike

Iako svi imaju slične karakteristike, ne mogu se svi svrstati u istu grupu. Svaka skupina predstavlja ličnosti za sebe bez obzira što je možda epilog njihovih dejstva gotovo identičan. Tek onda kad ljudi budu shvatili da ne postoji tipičan sajber kriminalac, moći će da preduzmu akcije na svaku grupu koje će dati efekta.

Zaključak

Na nastajanje, širenje i intenzitet svih oblika kriminala značajan uticaj imaju određeni kriminogeni faktori, no kod kompjuterskog kriminala oni naročito dolaze do izražaja. Pored tehnološkog razvoja na intenzitet kompjuterskog kriminala utiču i koncentracija podataka, nove vrednosti, nove metode i tehnike izvršenja dela, širenje informatičke pismenosti itd. Takođe, počinioци ove vrste krivičnih dela imaju specifičnu motivaciju koju čine ne samo finansijski i ekonomski razlozi, već i tehnički sindrom, sindrom milosrđa, emotivni razlozi, ideologija i politika, i visok nivo znanja, a izvršenje dela za njih uglavnom predstavlja izazov ili igru, dok informativni mediji podstiču nedozvoljene radnje kompjuterskih kriminalaca glorifikujući ih. Ovoj tvrdnji ide u prilog činjenica da je veliki broj izvršilaca ovih krivičnih dela starosnog doba ispod 18 godina, u kom uzrastu je potreba za dokazivanjem i najveća, uz tendenciju stalnog pomeranja donje granice.

Poređenjem istraživanja koja su rađena u SAD i zemljama EU, došlo se do profila najčešćih počinilaca kompjuterskog kriminaliteta. U pitanju su mahom mlađe osobe, od 18 do 30 godina starosti, muškog pola, visokog koeficijenta inteligencije, ali i visokog stepena motivacije za ovu vrstu zloupotrebe. Tehnološki su veoma obrazovani, ranije neosuđivani, sa svega nekoliko godina radnog iskustva, bez problema na pret-

hodnim radnim mestima i uglavnom sa višom kvalifikacijom od one koju zahteva posao na koji su raspoređeni.

U socio-demografskom smislu u pitanju su pretežno mlađi i obrazovaniji ljudi, a u psihološkom, osobe koje su otvorene za nova iskustva, koje odlikuje maštovitost, ali često i stidljivost, povučenost i nedostatak samopouzdanja u realnom svetu.

Takođe ono što je veoma uznemiravajuće, u početnim danima hakovanja, hakeri su uspeali da postignu cilj u 80% slučajeva dok danas, sa daleko većim nivoom sigurnosti, taj procenat skoro da nije smanjen. Kao odgovor na takvu situaciju, FBI je borbu protiv kompjuterskog kriminala postavio na 3. mesto prioriteta. Prema podacima iz 2002. godine, šteta koju počinje sajber kriminalci, odnosno hakeri i njihovi maliciozni kodovi koštaju poreske obveznike širom sveta 13.2 milijardi dolara godišnje.

FBI procenjuje da se manje od 10% ukupnog kompjuterskog kriminala završava uspešnom istragom, a većina čak ne bude ni prijavljena. Oko 10% od tog broja bude suđeno, a samo 10% od tog broja bude stvarno kažnjeno. To znači da tipičan kompjuterski kriminalac ima verovatnoću da ostane nekažnjen preko 99%.

Kao i „pravi“ kriminalci, sajber kriminalci po pravilu opravdavaju svoja (ne)dela, a mnogi zbog svoje pozicije, inteligencije i sposobnosti sebe postavljaju iznad zakona.

Može se reći da hakovanje predstavlja neobičan način ujedinjenja društva „dobrih“ i „loših“ hakera. Nekad se maliciozno hakovanje naziva kreovanje kako bi se jasno izdvojilo od benignog i „dobrog“ hakovanja što daje slobodu da se hakerski napadi predstave kao legalna testiranja koji uključuju bezobzirnost i neprijatnost koju napad može izazvati i sve to skrivajući se iza maske „dobrog hakera“. Veoma je važno većinu hakerskih motiva prihvatiti uzdržano iz razloga što su loša namera i bezobzirnost srce svakog kriminalne sklonosti.

LITERATURA

1. Cyber crime, <http://library.thinkquest.org/04oct/00460/index.html>
2. Dr. Grover Maurice Godwin , *The Psychology of the Cyber-Stalker*, 2006
<http://www.investigativepsych.com/stalk.htm>
3. Green Kate, *Catching Cyber Criminals*, Technology Review, 3.8.2006
http://www.technologyreview.com/read_article.aspx?id=16520&ch=infotech
4. Horn Paul, *It's Time to Arrest Cyber Crime*, BusinessWeek Online, 2.2.2006
http://www.businessweek.com/technology/content/feb2006/tc20060202_832554.htm
5. Icové D., Segar K., VonStorch W., *Computer Crime, A Crimefighter's Handbook*, O'Reilly & Associates
6. Krone Tony, *High tech Crime Brief*, Australian Institute of Criminology, 2005
<http://www.aic.gov.au/publications/htcb/htcb006.html>
7. Pipkin Donald, *Does Cyber Crime Pay ?*, WebTalk Radio Show, avg.2002
<http://www.webtalkguys.com/article-pipkin.shtml>
8. What is a cyber stalker?
<http://www.angelfire.com/wv/StormMastiffs/cyberstalker.html>