

KOMPJUTERSKI KRIMINAL,

ZLOČIN i PREVENCIJA

Zornić Džemail

Abstract: Najnovije i očekivane promene u tehnologiji koje proizilaze iz konvergencije računarstva i telekomunikacija uopšte zaista oduzimaju dah, a već su imali značajan uticaj na mnoge aspekte života: bankarstvo, berza, kontrola vazdušnog saobraćaja, telefon, električna energija, zdravstvo, socijalna zaštita i obrazovanje su u velikoj meri zavisile i zavise od informacionih tehnologija i telekomunikacija uopšte.

Društvo se zaista kreće prema tački u kojoj je moguće potvrditi da sve zavisi od informacionih tehnologija i softvera.

Ovaj eksponencijalni rast i povećanje svojih kapaciteta i pristupačnost u kombinaciji sa smanjenjem troškova, donelo je revolucionarne promene u svakom aspektu ljudske civilizacije, uključujući i kriminalne radnje.

Povećanje kapaciteta za informacione sisteme ujedno donosi i povećanje ranjivosti i zloupotrebe tih i takvih sistema. Novoj vrsti kriminala, što je bilo počinjenih pomoću računara, ili su na drugi način povezane sa njima, široko je preraslo u visokotehnološki kriminal.

Šta je kompjuterski kriminal ?

Cyber kriminal u užem smislu – predstavlja svako nezakonito ponašanje usmereno na elektronske operacije sigurnosti kompjuterskih sistema i podataka koji se u njima obrađuju;

Cyber kriminal u širem smislu – kao svako nezakonito ponašanje vezano za ili u odnosu na kompjuterski sistem i mrežu, uključujući i takav kriminal kakvo je nezakonito posedovanje, nuđenje i distribuiranje informacija preko kompjuterskih sistema i mreža.

U skladu sa **Preporukom Saveta Evrope** i listom OECD-a iz 1989. godine. Oblici kompjuterskog kriminaliteta su:

1. Neautorizovani pristup kompjuterskom sistemu ili mreži kršenjem mera sigurnosti (haking);
2. Oštećenje kompjuterskih podataka ili programa;
3. Kompjuterske sabotaze;
4. Neovlašćeno presretanje komunikacija od i u kompjuterskim sistemima i mrežama;
5. Kompjuterska špijunaža. Svaki od ovih oblika može se ukrštati sa svakim jer gotovo da ne postoji “čisti” oblik.

Tako haking, pored neovlašćenog ulaska u kompjuterske sisteme i mreže, često obuhvata i uništenje podataka ili kompjutersku špijunažu (kao što je to slučaj sa upadima na veb sajtove i uništenje ili “prepravljjanje” podataka na njima ili haking i trgovina pasvordima).

Izmena kompjuterskih podataka i programa uključuje i “lansiranje” kompjuterskih crva i virusa što je najčešće praćeno zaustavljanjem rada kompjuterskog sistema, uništenjem

podataka. U mrežama crvi i virusi se u većini slučajeva “razmenjuju” elektronskom poštom, a ne retko to čine i hakeri prilikom neovlašćenog pristupa.¹

Tipovi kompjuterskog kriminala:

1. Krađa elektronskih usluga
2. Komunikacija u cilju krivične zavere
3. Piraterija
4. Elektronsko pranje novca
5. Vandalizam i terorizam na Internetu
6. Prodaja i investicija laži
7. Ilegalno presretanje komunikacionih kanala
8. Transfer sredstava za on line prevare

Krađa elektronskih usluga:

Odnosi se na to da kriminalne grupe ili pojedinci preuzimaju signal i prodaju krajnjem kupcu kao svoju uslugu ili preprodaju trećim licima na on line tržištu. Naime, najčešće su to telefonski impulsi, provajding usluge pristupa Internetu, kablovski Internet itd...

Komunikacija u cilju krivične zavere:

Baš kao što legitimne organizacije koriste informacione tehnologije i računarske mreže za vođenje evidenciju, upravljanje i komunikaciju, tako su ove mogućnosti uticale na smanjenje troškova i lakšu komunikaciju i bolju logistiku i kriminalnim grupama koje se bave nedozvoljenim ili kriminalnim delatnostima.

Postoje dokazi gde se informacioni sistemi koristi u cilju prodaje i distribucije droge, kockanje, pranje novca i trgovinu oružjem.

Piraterija:

Digitalna tehnologija omogućava savršenu reprodukciju i lako širenje štampe, grafičkih rešenja, zvuka i multimedijalnih sadržaja. Ovo je proizvelo iskušenje da se reprodukuje materijal zaštićen autorskim pravima za ličnu upotrebu ili za prodaju po višestruko nižoj ceni.

Elektronsko pranje novca:

Za veoma kratko vreme elektronski transfer sredstava je pomogao u prikrivanje i kretanje prihoda od nedozvoljene, kriminalne delatnosti. Savremene Informacione tehnologije olakšavaju da kriminalni tragovi sakriju poreklo i odredište za prenos tih sredstava. Na ovaj način prljavi novac dolazi u regularne, legalne tokove.

Vandalizam i terorizam na Internetu:

U Svim društvima u kojima računari igraju važnu ulogu u svakodnevnom životu su ranjivi na napade od ljudi koji su motivisani: radoznalošću, gnevom, patnjom, interesom itd. Ovi ljudi mogu da prouzrokuju sitne neprijatnosti u najboljem slučaju a imaju potencijala i da nanese ozbiljnu štetu.

¹ <http://www.bos.rs/cepit/idrustvo/sk/tipovisajberkriminala.php>

Prodaja i investicija laži:

Kako elektronska trgovina ili e-trgovine postaje sve više i više popularna, primena digitalne tehnologije za lažne kriminalce znači lakšu manipulaciju, manje troškove, veće mogućnosti skrivanja i jednostavno veće mogućnosti prevare.

Korišćenje lažnih telefona za prevaru, lažnih naloga, lažne prodaje, lažne investicije su samo neki od načina sticanja dobiti i prodaju laži.

Cyberspace sada obiluje širokim spektrom mogućnosti investiranja, od tradicionalnih hartija od vrednosti, kao što je akcija i obveznica pa do više egzotičnih mogućnosti kao što su uzgoj kokosa, prodaja turističkih aranžmana, posredovanje u trgovini nekretninama itd .

Fraudsters² sada imaju pristup milionima ljudi širom sveta, a trenutno ima minimalne cene.

Ilegalno presretanje komunikacionih kanala:

Razvoj u oblasti telekomunikacija, kao i prenos podataka preko mreže ima za rezultat veću brzinu i kapacitet, ali i veće ranjivosti. Sada je lakše nego ikada za neovlašćena lica da dobiju pristup poverljivim informacijama.

Elektromagnetni signal koje emituje računar, sada lako mogu biti presretnuti i zloupotrebjeni.

Da dodamo još i to da postojeći zakoni ne sprečavaju praćenje signala sa dislociranog, udaljenog računara.

Pod ovim okolnostima informacija je sve više i više ugrožene i dostupna neovlašćenim korisnicima.

Zavisno od vrste učinjenog dela Kompjuterski kriminal može biti :

1. Politički
2. ekonomski
3. Kriminal u proizvodnji
4. Kriminal u distribuciji
5. Kriminal u logistici
6. Privatni(povreda privatnosti)

Metode za izvršenje:

1. Neovlašćenog pristupa
2. E-pošta bombardovanja
3. Date diddling
4. Salama napad
5. Krađe Internet vreme
6. Logička bomba
7. Virus / crv napada
8. Trojanac napada
9. Denial of service napada
10. Distribuirano uskraćivanje usluga napada
11. E-pošta Varka

² http://en.wikipedia.org/wiki/Internet_fraud#Example_one

12. Intelektualnu svojinu kriminal
13. Cyber špijuniranje

Neovlašćenog pristupa (krekovanje, nije hakerisanje):

Neovlašćeni pristup je takođe poznat kao pojava ili pukotina za razliku hakerisanje, i ona omogućava hakeru, prestupniku, kriminalcu da pristupi sistemu bez dozvole korisnika ili bez odgovarajućeg odobrenja ovlašćenog lica.

Ovo se obično obavlja bilo kao faking identity, ili provaljivanje pristupne šifre.

E-pošta bombardovanja:

Ovo zapravo znači slanje velikog broja e-mailova na žrtve gde dovodi do toga da e-mail nalog korisnika odnosno, u ovom slučaju žrtve pada (u slučaju pojedinačnih) ili server (u slučaju da korporacija).

Deadlining:

Ova vrsta napada uključuje promenu na sirovim podacima pre nego što je obrađeno sistem i ponovo ga menja posle obrade. Ovakav vid zloupotrebe podrazumeva instaliranje scripti u sirovom kodu koje imaju zadatak da kopiraju, izbrišu, pošalju, manipulišu gotovom podacima u završnoj fazi ili tek onda kada se proizvod ili usluga pusti na tržište.

Salama napad:

Ovo se generalno koristi kod počinioaca finansijskog kriminala. Ovde je Ključno da se napravi mala promena, tako da će u jednom slučaju otići, proći nezapaženo. Na primer, radnik banke naplaćuje pet dinara iz svakog naloga klijenata. Mali broj kupaca će verovatno primetiti ove male promene, ali većina korisnika neće primetiti tako male transakcije a kriminalac će imati značajnu zaradu.

Krade Internet vremena:

Ovo zapravo znači korišćenje od strane neovlašćenog lica na Internetu gde će njegov račun za internet sate platiti neko drugi.

Logička bomba:

Ovaj događaj zavisi od programa. Ovo implicira da je ovaj program kreiran da uradi nešto samo onda kada dođe do određenog događaja (npr. virusa Černobilj) ili jednostavno kada otvorite određeni targetirani fajl istog momenta se pokreće program koji ima zadatak da kopira vaše podatke ili uništi tabelu u vašoj bazi podataka. Najčešće se koristi za industrijsku špijunažu.

Virus / crv napad:

Virus je program, koji se prikači na drugoj datoteci ili sistemu i potom šalje u druge fajlove i na drugim računarima preko mreže. Oni obično utiču na računare bilo menjanjem ili brisanjem podataka iz njega.

Crvi sa druge strane ne ometa podataka. Oni se jednostavno množi dok ne popune ceo slobodni prostor na vašem računaru.

Trojanac:

Trojanac je program, koji izgleda kao da je nešto korisno ali se ispod skriva program koji prouzrokuje neke štete na računaru korisnika žrtve.

Denial of service:

Ovo uključuje poplava resursa računara sa mnogo zahteva nego što računar može da obradi.

To dovodi do kraha resursa, čime se onemogućava pristup ovlašćenim korisnicima sistema. Ovaj vid napada je veoma zastupljen i u najčešćem broju slučajeva sa koristi kod email-a i kod hostinga, odnosno kada napadač praktično blokira vašu veb stranicu i taj period zloupotrebljava na svoj način.

Distribuirano uskraćivanje usluga:

Ovo je uskraćivanje servisa napada u kojima su počinioci stacionirani u više od jedne lokacije. Veoma je teško kontrolisati ovakve napade. Najčešće je to dobro organizovana kriminalna grupa koja ima svoje saradnike u više zemalja ili čak u svakoj zemlji koja je njima interesantna.

E-pošta Varka:

predstavlja puno Lažnih e-poruka, koja izgleda kao da potiču iz jednog izvora, ali u stvari potiče iz sasvim drugog. Varka se sastoji u tome što Vi kada pogledate pošiljaoca ustvari vidite poznatu email adresu a u suštini je drugi pošiljalac koji je trenutno zamenio pošiljaoca, Naravno da je adresa iz vašeg address buka jer je tako siguran da ćete otvoriti email.

Intelektualna svojina:

Ovo je kriminal, koji podrazumeva neovlašćeno umnožavanje i distribucija softvera zaštićenih autorskim pravima. Npr. Softverska piraterija.

Cyber Violation:

Uključuje uznemiravanje korisnika dok je na Internetu.

Metode prevencije:

1. Firewall . Česte promene lozinke
2. Bezbedno surfovanje
3. Česte provere virusa
4. E-mail filteri

Firewall:

To su programi koji štite korisnika od neautorizovanog pristupa, kod napada na mreži. Oni omogućavaju pristup samo poznatim korisnicima ili ljudima kojima korisnik dozvoli pristup.

Firewall je deo računarskog sistema ili mreže koja je dizajnirana da blokira neovlašćeni pristup, dok dozvoljava komunikaciju ovlašćenim licima. To je uređaj ili skup uređaja podešena da dozvoljava, ospori, šifrovanje, dešifrovanje, ili kontroliše sve (i van) računara saobraćaj između različitih oblasti bezbednosti na osnovu seta pravila i drugih kriterijumima.

Firewall se može implementirati bilo u hardver ili softver, ili kombinacija oba. Zidovi su često korišćeni za sprečavanje neovlašćenih korisnika Interneta da pristupaju privatnim mrežama povezani na Internet, a posebno intranet. Sve poruke koje ulaze ili napuštaju Intranet

prolaze kroz zaštitni zid, koji ispituje svaku poruku i blokira one koji ne ispunjavaju navedene kriterijume bezbednosti.

Česte promene lozinke:

Sa pojavom multi-korisničkih sistema, bezbednost je postala zavisna od lozinke. Stoga je potrebno postaviti sigurne lozinke koje se sastoje od kombinacija slova, brojeva i znakova. Menja ih često, i vodi računa o tome da lozinka nikad ne bude datum rođenja, adresa, posao, registarske oznaka automobila, broj telefona itd.

Bezbedno surfovanje:

To je praksa koja treba da prate sve korisnike na mreži.

Bezbedno surfovanje podrazumeva držanje one e-mail adresu privatne, a ne razgovor na otvorenim sistemima, koji nemaju adekvatne metode za zaštitu, u poseti sigurne lokacije. Prihvatanje podataka iz samo poznatih korisnika, preuzimanje pažljivo, Takođe, preuzimanje fajlova sa poznatih sajtova smanjuje rizik napada.

Česte provere virusa:

Često treba proveravati fajlove koje unosimo u računar, antivirus programima kao i anti spam programima i ostalim vidovima zaštite. Takođe, bilo spoljnih medija, kao što su disketa i CD-ROMovi uvek treba proveriti pre pokretanja bilo čega što se nalazi na ovim medijumima.

Filteri email:

E-mail filter za prerađu e-mail organizuju u skladu sa specificiranim kriterijumima. Najčešće se odnosi na ovu automatsku obradu dolazne poruke, ali termin se takođe odnosi na intervenciju ljudskoj inteligenciji pored anti-spam programa, kao i za odlazne i dolazne e-poruke.

E-mail softver za filtriranje ulaza. Za svoj izlaz, poruka može da prođe kroz nepromenjenu poruku za isporuku u poštansko sanduče korisnika, preusmeravanje poruka za isporuku i drugde, ili čak i bacanje poruku. Neke pošte filteri su u stanju da menjaju poruke u toku obrade.

Motivacija

Zajedničke koristi filtere za poštu uključuju uklanjanje neželjene pošte i računarskih virusa. Ređe se koristi da pregledaju odlazne e-maile na neke kompanije, da se zaštite zaposleni u skladu sa odgovarajućim zakonima. Korisnici takođe mogu da koriste filtriranje mail poruka prioriteta, i da ih poredi po folderima na osnovu predmet ili drugih kriterijumima.

Metode

Mail filteri mogu biti instalirane od strane korisnika, bilo kao poseban program, ili kao deo e-pošte (e-mail client). U e-pošte programa, korisnici mogu lično, u delu "uputstvo" podesiti filtere koji automatski filtriraju mail poruke prema izabranim kriterijumima. Većina e-pošte programa sada imaju funkciju automatskog filtriranja neželjene pošte. Internet servis provajderi mogu instalirati filtere mail-u u njihovim agentima za prenos pošte, kao uslugu za sve svoje klijente. Korporacije ih često koriste kako bi zaštitili svoje službenike i njihovu imovinu informacionih tehnologija.

Prilagodavanje

Mail filteri imaju različit stepen konfigurisanja. Jedan od njih jeste da se ključne reči u telu poruke koriste, ili možda e-mail adresa pošiljaoca poruke. Neki napredniji filteri, posebno anti spam filteri, korišćenje statističkih tehnika, kao što su dokumenta klasifikacionih naivno Bibes klasifikatora. Filtriranje Slika se takođe može koristiti da biste koristili sliku kompleksne analize algoritama, gde algoritam otkrije skin tonove i specifične oblike tela obično u vezi sa odraslima slike (pornografske slike).

Studije slučaja:

Navešću nekoliko primeri sajber kriminala počinjene u poslednjih nekoliko godina:

Legija sudbine (Lod):

Članovi: Frenklin Darden zvanog levičar, Beograd donaciju zvani Urvile Robert Riggs zvani Prorok)

Uhapšen: Jul 21, 1989, Naplaćuje: 1989, Osuđeni: 1990. Godine.

Kriminal: kreiranje u BelSouth's Telephone (uključujući i 911) mreže - BellSouth imaju vlasnički softver i podatke, neovlašćenog upada, nelegalno posedovanje telefonskih brojeva kreditnih kartica sa namerom da prevare i zavere. Iz Vlade Memorandum o kazni: "BellSouth troše oko 1,5 miliona dolara u identifikovanju uljeza u svoj sistem i od tada proveo oko 3 miliona dolara više da dodatno obezbedi svoju mrežu".

Rečenice: Frenk Darden (24): 14 meseci, Adam je donaciju (22): 14 meseci Robert Riggs (22): 21 meseci. Kolektivno naloženo da plati \$ 233,000.00 na restituciju.

Majstori prevara (MO):

Članovi: Marko Abene zvani Phiber Optik i Il Duće, Elija Ladopoulos zvani kiselina Phreak, Pavle Stira zvani Škorpion, Džon Li zvani korumpiran i Džon Farrington, Hulio Fernandez zvani Odmetnik)

Uhapšen: 1992, Naplaćuje: Jul 1992, Osuđeni: Jul 1993

Kriminal: Više računara hakerisanje u vezi optužbi, uključujući zavere, prevare žice, neovlašćenog pristupa računarima, neovlašćeno posedovanje pristupnih uređaja, kao i presretanje elektronske komunikacije. Institucijama koje su uključene su jugozapadnom Bel, AK Sjeverna Amerika, Njujork Telefon, ITT, Informacije Amerika, TRU, trans unije, Pacifik Bel, Univerzitet Vašington, Njujork University, US Uest, učenje link, Tymnet, Martina Marietta Elektronika Informacije i raketa grupa, AT & T Banka Amerike, SAD i Agenciji za nacionalnu bezbjednost. Zločin je široko u javnost, i rezultiralo u najmanje jednoj knjizi se pismeno, chronicling događaja.

Rečenice: Marko Abene: 12 meseci + uslovno i 600 sati društveno-korisnog rada Džon Li: 6 meseci uslovno + Eli Ladopoulos: 6 meseci + uslovno Stira Pol: 6 meseci uslovno + Hulio Fernandez sarađivali i dobili kaznu.

Mitnik, Kevine Dejvid (alijas: Glen slučaj):

Uhapšen: Februar 15, 1995

Naplaćuje: Septembar 26, 1996

Osuđeni: Mart 18, 1999

Kriminal: Od 26. septembra 1996 zapis sud: "dobijanje neovlašćenog pristupa računarima koje pripadaju brojnim softver računara i operativni sistemi proizvođača računara, mobilnih telefona proizvođača, Provajderi Internet servisa, kao i obrazovnim institucijama, i (b) krađa, umnožavanje i misap propriating vlasnički softver računara "iz" Siemens, kompanija Fujitsu, LG, Sun-cea, Novell i NEC-a. "

Rečenica: Pošto je bio zatvoren, pun čeka suđenje 4 godine, Kevina služio dodatnih 10 meseci i bio je uslovno pušten na uslovno - On ne može da koristi računar, mobilni telefon, ili bilo koji drugi Internet uređaja do 2003, kao ni profit od svog zločina na bilo koji način. Ukupno vreme provedeno u zatvoru za ovo delo bila 4 godine, 11 meseci i 6 dana.

Zaključak:

Svaki naš dom je pun raznih informacija u digitalnom obliku, većinu tih informacija svakodnevno dobijamo od prijatelja, kolega putem email-a ili pomoću ostalih socijalnim sajtova kao što su: facebook, twiter, my space itd., stoga, Svi smo potencijalne žrtve cyber kriminala.

Sve o našim životima je na neki način smešteno na našim računarima. Pod ovim okolnostima, krajnje vreme je da krajnje ozbiljno shvatimo ove stvari i na vreme se zaštitimo od njih a u tekstu sam naveo nekoliko načina preventive. Sajber Kriminal je problem svih nas.

Najbolji način zaštite od cyber kriminala jeste kvalitetna Informacija o vrstama, oblicima i naravno primarnoj zaštiti od najpre virusa a zatim i hakera i ostalih kriminalaca u cyber prostoru.

Cyber prostor u republici Srbiji nije ostao imun na mnoge oblik cyber kriminala. Za svega nekoliko godina "uspeli" smo da se popnemo visoko na rang listi opasnih i nesigurnih područja sa akterima kojima raste ugled u cyber podzemlju. Međutim, jedna grupa ovih počinilaca izgubila je predznak kriminalaca i svrstana je u heroje iako su njihove aktivnosti uveliko prevazilazile takve kvalifikacija. S druge strane, nespremnost pravosuđa i uspavanost prava olakšali su prelazak ovih pojedinaca u sferu "čistog" kriminala. To je ohrabrilo i mnoge druge koji su iz faze bojažljivih pokušaja prešli u drske i samosvesne kriminalce ubeđene da im niko ništa ne može.

Suočili smo se sa nekonzistentnošću sa drugim delima i sankcijama. Iako je ekspertski tim Saveta za državnu upravu Vlade Republike Srbije i UNDP-a u novembru 2002. godine izradio prvu verziju posebnog, lex specialis, Zakona o cyber kriminalu, ova verzija nije dalje otišla od nečije fioke. Poseban propust je što se u odredbe o organizovanom kriminalu nisu uvrstila i oblici cyber kriminala.

Svemu ovome treba dodati i problemi u radu pravosudnih i policijskih organa, uvreženog mišljenja o nedodirljivosti izvršilaca, nepostojanja saradnje sa međunarodnim organizacijama, telima i asocijacijama, kao i nacionalnim institucijama drugih zemalja, nepostojanja posebnih specijalizovanih jedinica za istragu, specijalizovanih sudova za presuđivanje i serioznosti u radu provajdera, neuspostavljanja saradnje između subjektima koji bi trebalo da se izbore sa ovom pojavom, ipak se mora konstatovati da je koliko toliko pomeren sa "mrtve tačke" i da treba očekivati da se to nastavi kao organizovani, sistematizovani i kontinuirani rad. Kako i koliko će se to realizovati videće se već sa prvim presudama i formiranjem javnog mnjenja.³

Literatura:

³ www.bos.rs

1. Cyber Crime (article), Silicon Times, Vol. 2, Issue 12, December 2002
2. Computer Vulnerabilities, Eric Knight, CISSP, Electronic Edition, March 2000, release 4
3. An Unofficial Guide to Ethical Hacking, Ankit Fadia, Macmillan India Ltd., 2001
4. The Little Black Book of Computer Viruses, Mark Ludwig, Electronic Edition, American Eagle Publications, 1996