

NAJČEŠĆE METODE NAPADA CYBER KRIMINALACA I KAKO SE ODBRANITI

Srđan Nikić, dipl. ing.
Privredni sud u Pančevu
nikic.srdjan@pa.pr.sud.rs

Sažetak: Razvoj Informaciono-komunikacionih tehnologija doveo je do poboljšanja poslovanja savremenog društva (e-poslovanje). Međutim razvoj tih istih tehnologija stvorio je, a i dalje stvara, sve više mogućnosti cyber-kriminalcima da na lak način upadnu u sistem pojedinca ili kompanije i da načine neku štetu. U radu je opisan razvoj i rast upotrebe Interneta u novom veku, definicijom cyber kriminala, oblici zloupotreba i prevara izazvani razvojem IKT, tehnologije koje su najviše napadane kao i neke od metode kojima su napadnute i mere zaštite od takvih napada.

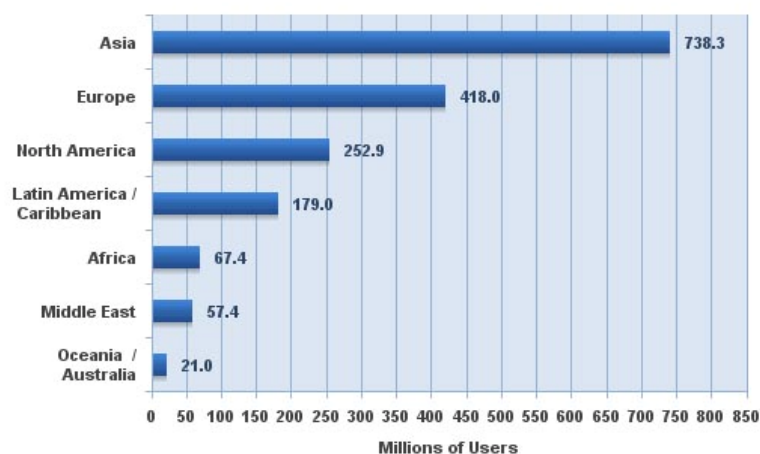
Ključne reči: cyber-kriminal, tipovi napada, trojanci, mere zaštite

1) Uvod

Razvoj računara i komunikaciono-računarskih mreža doneo je otvaranje mogućnosti za napredak u svim oblastima naših života, pre svega poslovne sfere a zatim i edukacione i sportske, a na kraju i socijalne sfere tj sfere zabave.

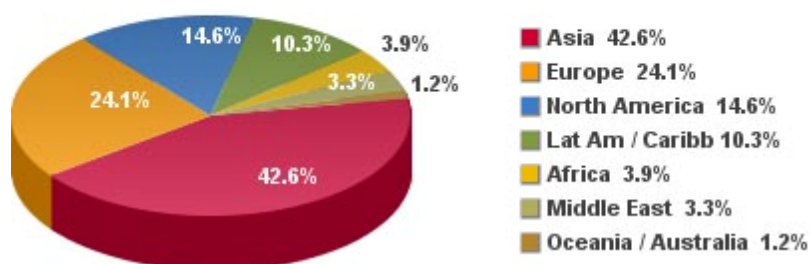
Međutim, nažalost, globalne računarske mreže stvorile su mogućnosti i za nove oblike kriminala. Velika „zavisnost“ od računara i računarskih mreža omogućila je dobro tehnički potkovanim pojedincima, grupama ili organizovanim grupama da u velikoj meri utiče na dešavanja u cyber-svetu. Odbrana od ovakvih pojedinaca ili grupa je redovno ažurirana zaštita računara i računarskih sistema od takvih napada, svest o postojanju istih i njihovo prijavljivanje od strane svi korisnika tih sistema, ako i adekvatno kažnjavanje uhvaćenih cyber-kriminalca. Ali te cyber-kriminalce upravo je teško otkriti u činjenju nelegalnih dela, zatim identifikovati i uhvatiti, kao i očuvati dokaze o njihovom nelegalnom delu. Globalna računarska mreža (Internet) je zbog ogromnog broja korisnika idealno skrovište za takve kriminalce.

Internet Users in the World by Geographic Regions

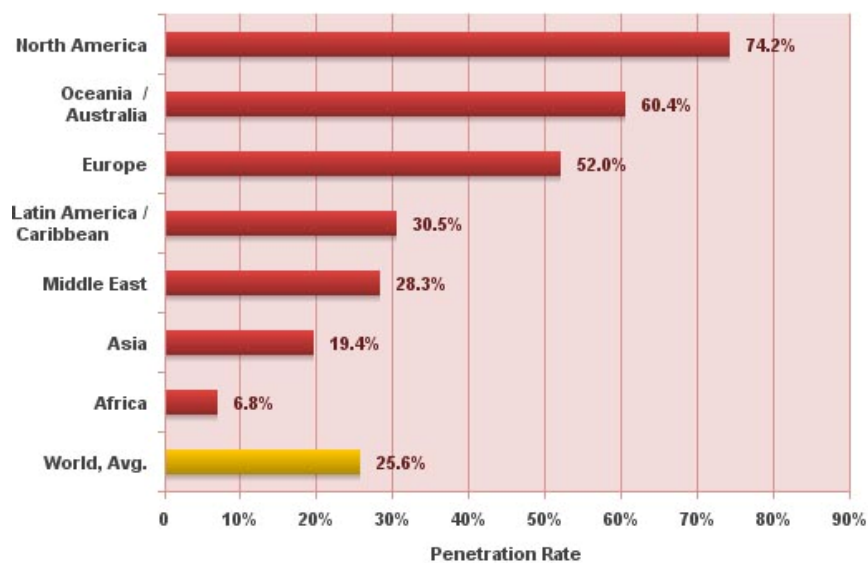


Slika 1. Broj korisnika Interneta po kontinentima (u milionima)¹

Procenat korisnika Interneta po kontinentima



Slika 2. Procenat korisnika Interneta po kontinentima
Procenat populacije koji koristi Internet
po kontinentima



Slika 3. Procenat populacije koji koristi Internet po kontinentima²

¹ www.internetworldstats.com

² www.internetworldstats.com

Statistika populacije i korisnika Interneta u svetu					
Svetska regija	Populacija	Korisnici Interneta	Procenat populacije koji koristi Internet	Udeo u korišćenju Interneta	Procenat rasta korisnika Interneta (2000-2009)
Afrika	991.002.342	67.371.700	6,8 %	3,9 %	1392,4 %
Azija	3.808.070.503	738.257.230	19,4 %	42,6 %	545,9 %
Evropa	803.850.858	105.096.093	52,0 %	24,1 %	297,8 %
Srednji Istok	202.687.005	57.425.046	28,3 %	3,3 %	1648,2 %
Severna Amerika	340.831.831	252.908.000	74,2 %	14,6 %	134,0 %
Latinska Amerika i Karibi	586.662.468	179.031.479	30,5 %	10,3 %	890,8 %
Austaralija i Okeanija	34.700.201	20.970.409	60,4 %	1,2 %	175,2 %
Svet ukupno	6.767.805.208	1.733.993.741	25,6 %	100 %	380,5 %

Tabela 1. Statistika populacije i korisnika Interneta u svetu³

Prema istim izvorima u Srbiji⁴ je situacija da od 7.379.339 stanovnika, njih 3.300.000 što čini 44,7% populacije njih, što je, ako uporedimo sa podacima iz tabele 1, veći procenat nego prosek svetske populacije koja koristi Internet za čak 20%, a opet nešto manji nego što je to Evropski prosek. Upotreba Interneta za razliku od 2000. godine porasla je za čitavih 725,8%. Zanimljivo je reći da prema podacima iz 2007. godine u Srbiji je svega 1.400.000 stanovnika koristilo Internet što je tada činilo 18,7% populacije Srbije i bili smo čak ispod prosečnog broja korisnika Interneta u svetu u odnosu na populaciju.

2) Cyber kriminal

Kompjuterski (Cyber) kriminal predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog dela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivično-pravnom smislu relevantna posledica. Cyber-kriminal je takođe protivpravna povreda imovine kod koje se računarski podaci sa predumišljajem menjaju, razaraju ili se koriste zajedno sa hardverom.⁵

Tako u isto vreme računari, kao i cela informaciono-komunikaciona mreža, mogu biti i meta napadača, ali i oruđe tj. alat napadača, da bi kasnije bili i dokaz u forenzičko-istražnom postupku.

³ www.internetworldstats.com

⁴ U istraživanjima je uzeta Srbija bez Kosova

⁵ APIS Security consulting, Kompjuterski kriminalitet, <http://www.apisgroup.org/sec.html?id=29>

Još 2000. godine Ujedinjene nacije su na svom Desetom kongresu za suzbijanje kriminala i postupanju prema prestupnicima podelile cyber-kriminal na dve sub-kategorije:

1. **Cyber-kriminal u užem smislu** – svako nezakonito ponašanje usmereno na elektronske operacije sigurnosti kompjuterskih sistema i podataka koji se u njima obrađuju
2. **Cyber-kriminal u širem smislu** – 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

Istim dokumentom su definisani i konkretni oblici ovog kriminaliteta u skladu sa Preporukom Saveta Evrope i listom OECD-a te u dela cyber kriminala u užem smislu spadaju:

- 1) neautorizovani pristup kompjuterskom sistemu ili mreži kršenjem mera sigurnosti;
- 2) oštećenje kompjuterskih podataka ili programa;
- 3) kompjuterske sabotaze;
- 4) neovlašćeno presretanje komunikacija od i u kompjuterskim sistemima i mrežama;
- 5) kompjuterska špijunaža.

Od dela cyber kriminala u širem smislu najčešće se pojavljuju:

- 1) kompjuterski falsifikati;
- 2) kompjuterske krađe;
- 3) tehničke manipulacije uređajima ili elektronskim komponentama uređaja;
- 4) zloupotrebe sistema plaćanja kao što su manipulacije i krađe elektronskih kreditnih kartica ili korišćenje lažnih šifri u nezakonitim finansijskim aktivnostima.

Njima se u novije vreme dodaju i dela podržana računarima. Ova dela obuhvataju “rasturanje” materijala ili samo njihovo posedovanje pri čemu se mreža koristi za postizanje boljih rezultata kriminala ili pokušaja izbegavanje pravde. U ova dela se ubrajaju razni nezakoniti i štetni sadržaji, kršenje autorskih i srodnih prava, piraterija, prodaja zabranjene robe (oružja, kradene robe, lekova) ili pružanje nedozvoljenih usluga (kockanje, prostitucija). Najviše pažnje u ovoj grupi dela privlači dečija pornografija i distribucija raznih materijala Internetom⁶.

3) Najčešći tipovi napada i tehnologije koje se zloupotrebljavaju

Nove tehnologije u mnogome olakšavaju da posao koji obavljamo se uradi brže i bolje radeći ga preko mreže, kao i da lakše komuniciramo sa drugima i da se eventualno i zabavimo. Međutim iste te tehnologije ujedno olakšavaju posao i „cyber-kriminalcima“, ljudima koji koriste globalnu mrežu za ilegalne svrhe. Oni na različite načine, i iz različitih pobuda pokušavaju da upadnu u sisteme kompanija, personalne računare, u našu svakodnevicu. Za ovakve „poslice“ cyber-kriminalci koriste različita sredstva i metode, a

⁶ Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders, www.un.org

njihova inovativnost iz dana u dana sa razvojem tehnologija sve je veća. Tehnologije koje napadači najčešće zloupotrebljavaju su:

1. Dostupnost „žrtava“

Iako je Internet nastao još 80 tih godina prošlog veka (pre toga je 1969 napravljen ARPAnet), svoju ekspanziju je doživeo tek u prvoj deceniji novog stoleća. Kao što možemo da vidimo u statističkim podacima broj Internet korisnika iz dana u dan sve je veći. Poznato je da i broj IPv4 adresa polako nestaje i da će se uskoro preći na IPv6 adrese. Zahvaljujući Internet provajderima, globalna mreža postaje dostupna svima i u svaki čas (broadband). Dostupnost Internetu za korisnike ima brojne koristi: poslovne, komunikacijske, zabavne... međutim kao što smo rekli ta dostupnost koristi i cyber-napadačima. Brza internet konekcija 24/7 pruža mnogo veću mogućnost cyber-kriminalcima da vam za kratko vreme upadnu u računar i ukradu podatke, da vam sruše sistem, da vam ubace maliciozni kod, bilo to virus, trojanac, crv, spyware ili malware.

2. Bežične mreže

Bežično umrežavanje je još jedna tehnologija u ekspanziji, kako kod poslovnih korisnika tj. poslovnih mreža tako i za privatne korisnike. Bežični hot-spotovi postali su obavezni inventar na svim javnim mestima, kako u hotelima, na aerodromima i u parkovima, tako i u svakom modernom kafiću. Bežična tehnologija omogućava korisnicima pokretnost, i vezu sa Internetom na gotovo svakom koraku. Međutim ova tehnologija omogućava cyber-kriminalcima da lako i bez traga upadnu u vašu mrežu i sistem, jer gotovo svako sa lap-topom može presresti signal vašeg bežičnog rutera ako barem ne probate da ga zaštitite. Za ovakav vid upada kreiran je i poseban softver (kao na primer Wi-fi Hack). Novi bežični pristupni uređaji, za razliku od starih, po defaultu koriste enkripciju, međutim treba se postarati da se koristi bezbednija enkripcija kao što je WPA/WPA2 ili 802.11i pre nego WEP enkripcija, koju je lakše provaliti. Takođe trebala bi se primenjivati i enkripcija aplikacija koje koriste bežičnu mrežu (SSH ili TLS/HTTPS), a može se čak i zaštititi saobraćaj koji se obavlja preko te bežične mreže(VPN-om ili Ipsec-om)

3. World Wide Web (WWW)

Iako WWW ne spada u novije tehnologije, i dalje spada među omiljene tehnologije za eksploataciju cyber-kriminalcima, jer svako ko se poveže na Internet uglavnom koristi Web pretraživače. Dok se nekad WWW bazirao uglavnom na tekstu i bio bezbedan za korišćenje, danas WWW koriste podprograme (Java i ActiveX kontrole), kako bi se korisnicima omogućilo bogato multimedijalno iskustvo. Međutim te podprograme napadači mogu da iskoriste kako bi izvršili svoje maliciozne programe na vašem računaru. Zato je važno vršiti redovan update kako operativnih sistema tako i antivirusnih sistema.

4. E-mail poruke

E-mail poruke su postale nezaobilazan deo naše svakodnevice i predstavljaju jedan od najlakših načina komunikacije. Gotovo svaki građanin ima svoju e-mail

adresu. Baš zbog tolike rasprostranjenosti upotrebe e-mail poruka, kao i zbog nekih karakteristika lakih za zloupotrebu, e-mail poruke predstavljaju jedan od omiljenih sredstava cyber-kriminalaca. Koristeći lažne adrese oni mogu nam slati spam ili phishing poruke, pretnje, dečju pornografiju, ili neki drugi vid nelegalne korespodencije i ostati neakžnjeni zbog toga.

5. Unificirane komunikacije

Velike kompanije sve više i više koriste ovaj vid tehnologije, dobijajući prednost u tome što mogu da objedine više vidova komunikacije: e-mail, telefoniju, IM servis, konferencijske veze. VoIP (Voice over IP) tehnologija sve češće zamenjuje tradicionalne telefonske servise. Međutim, isto kao što su vaši podaci ranjivi isto tako su ranjivi i VoIP paketi jer se lako mogu presresti.

6. Prenosivi mediji

Bilo koji od prenosivih medija (flopi diskovi, CD/DVD diskovi, USB fleš diskovima ili bilo koji drugi prenosivi mediji) predstavljaju pravu „Meku“ cyber-kriminalcima. Preko njih se lako šire maliciozni kodovi, a zahvaljujući tome cyber-kriminalci lako mogu pristupiti vašim podacima, prekopirati i obrisati ih. Kako bi sprečili zloupotrbu prenosivih medija, mnoge banke i kompanije dozvoljavaju upotrebu samo kompanijskih prenosnih uređaja, koji se mogu koristiti samo i isključivo unutar kompanije. Takođe se može u Grupnim polisama ili u registru onemogućiti upotreba USB i IEEE 1394 portova.

7. E-commerce i online banking

Iako u našoj zemlji su ljudi još pomalo skeptični, ova tehnologija ulazi polako na sporedna vrata. Sve više i više korisnika (kako pravnih tako i fizičkih lica) završava poslove preko Interneta. Prednosti su brojne: od brzine korespodencije i ne gubljenja vremena do povezivanja sa ostalim pravnim i fizičkim licima, kao i dobrim marketingom za svoj proizvod. Ali baš zato što se ovde radi uglavnom o novcu, cyber-kriminalci vole ovu tehnologiju. Oni lako mogu doći do pozicije da upravljaju vašim novcem. Najčešći oblici zloupotreba ove tehnologije su: Prezare, krađe, pronevere, nelojalna konkurencija, manipulacije sa elektronskim novcem itd.

2006. godine Američko udruženje za zaštitu potrošača (NLC) napravilo je istraživanje za otkrivanje najčešćih Internet prevara. Lista 10 najčešćih Internet prevara izgledala bi ovako:

Mesto na listi	Naziv prevare	% žalbi u odnosu na sve druge žalbe	Prosečan gubitak po prevari
1.	On-line aukcije	34 %	1.331 \$
2.	Prodaja on-line	33 %	1.197 \$
3.	Plaćanje lažnim čekovima	11 %	4.053 \$
4.	„Nigerijske prevare“	7 %	3.741 \$
5.	Lažne lutije	4 %	1.750 \$
6.	Lažni zajmovi	3 %	1.515 \$
7.	Phishing	2 %	/
8.	Nagradne igre	1 %	2.447 \$

9.	Internet pristupni servisi	1 %	920 \$
10.	Investicije	1 %	4.759 \$

Tabela 2. Lista 10 najčešćih Internet prevara⁷

Prema zvaničnim podacima za 2007. godinu, šteta naneta kompjuterskim kriminalom u USA iznosi negde oko 66 miliona dolara⁸. Međutim veruje se da je cifra štete nanete kompjuterskim kriminalom znatno veća, jer mnoge kompanije, među kojima su i one najveće, nisu prijavile štetu organima vlasti iz više razloga, pre svega misleći da će im to doneti negativan publicitet, zatim da će konkurentske firme to znati iskoristiti, zato što ne veruju da organi vlasti mogu bilo šta da urade po tom pitanju kao i iz mnogih drugih razloga. Vrlo često korporacije sami angažuju vrsne stručnjake iz oblasti digitalne forenzike, kako bi izvršili unutrašnju (korporacijsku) analizu napada, odnosno nanete štete.

Američki institut za informacionu bezbednost (Computer security institute (CSI); www.gocsi.com) i ove godine, kao i ranijih, sproveo je istraživanje o najčešćim bezbednosnim incidentima, kao i o štetama prouzrokovane tim incidentima. U istraživanju su učestvovali stručnjaci za bezbednost IKT iz raznih malih i velikih kompanija, vladinih agencija, finansijskih, obrazovanih i medicinskih institucija itd. Neka od najvažnijih i najinteresantnijih zaključaka su⁹:

Prosečan gubitak po incidentu



Slika 4. Prosečan gubitak kompanije/ustanove po incidentu

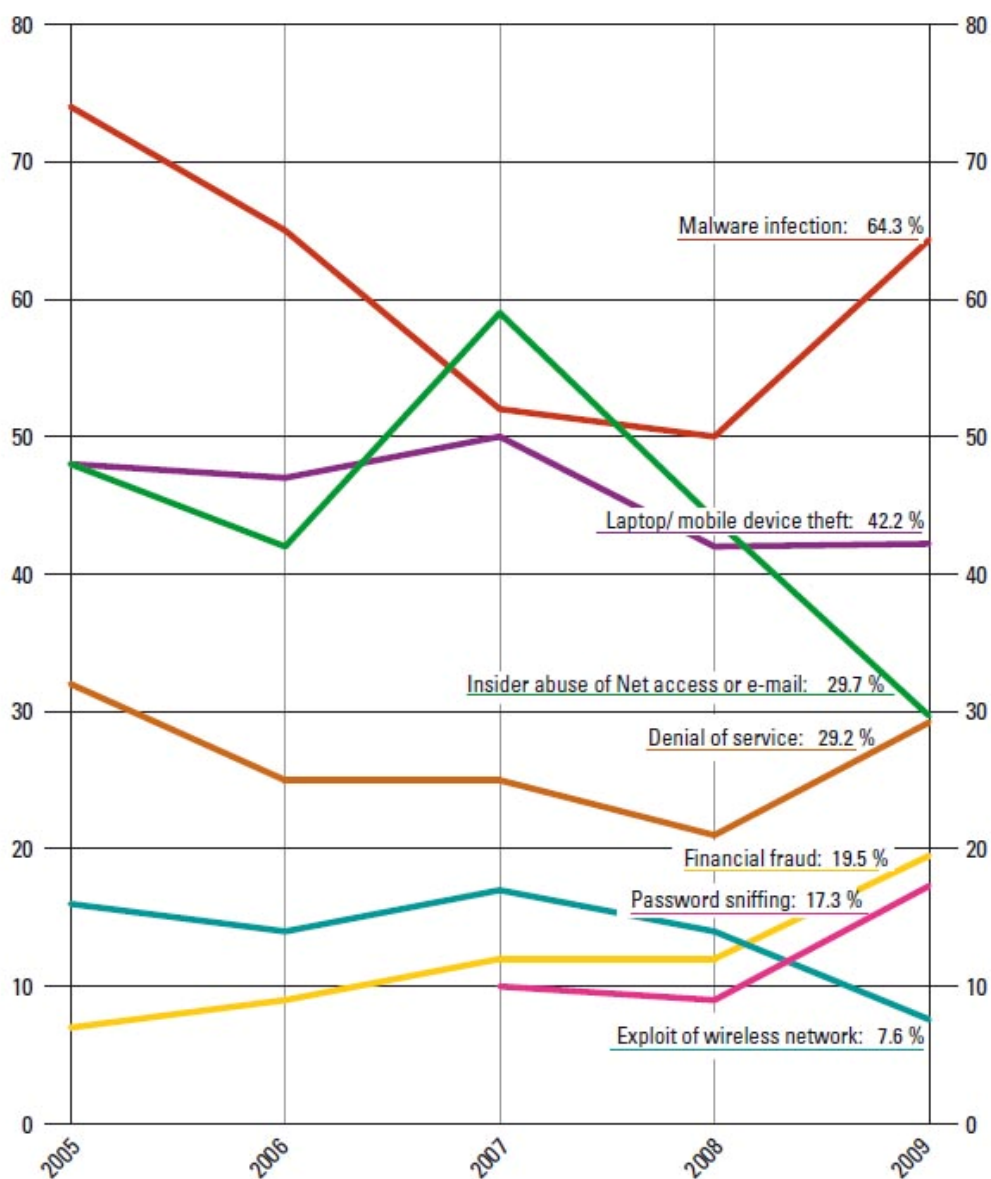
Kao što možemo videti na slici 4. prosečni gubici po incidentu su se smanjili za skoro 20%, sa 289.000\$ na 234.000\$. Ovde treba reći da su na vrhu ove skale troškova zloupotreba wirellessa (770.000\$), krađa identifikacionih podataka kao i podataka o zdravstvenom osiguranju (710.000\$) i naravno finansijske prevare (450.000\$). Treba reći i da su ispitanici prijavili veliku upotrebu takozvane „Return of investment“ kao bezbednosne mere zaštite, tj. uložili su u bezbednost svojih informaciono –komunikativnih sistema manje sredstava nego što bi izgubili da to nisu učinili. Napredak u bezbednosti IK sistema možemo uočiti ako kažemo da je 2001. godine prosečan gubitak kompanije/ustanove po incidentu prelazio višemilionske cifre.

⁷ “The top 10 Internet Frauds”, National Fraud Information Center, <http://www.nclnet.org/>

⁸ Computer Security Institute, <http://www.gocsi.com>

⁹ Robert Richardson: „2009 CSI Computer Crime & Security Survey“, Computer Security Institute, <http://www.gocsi.com>

Najčešći tipovi napada

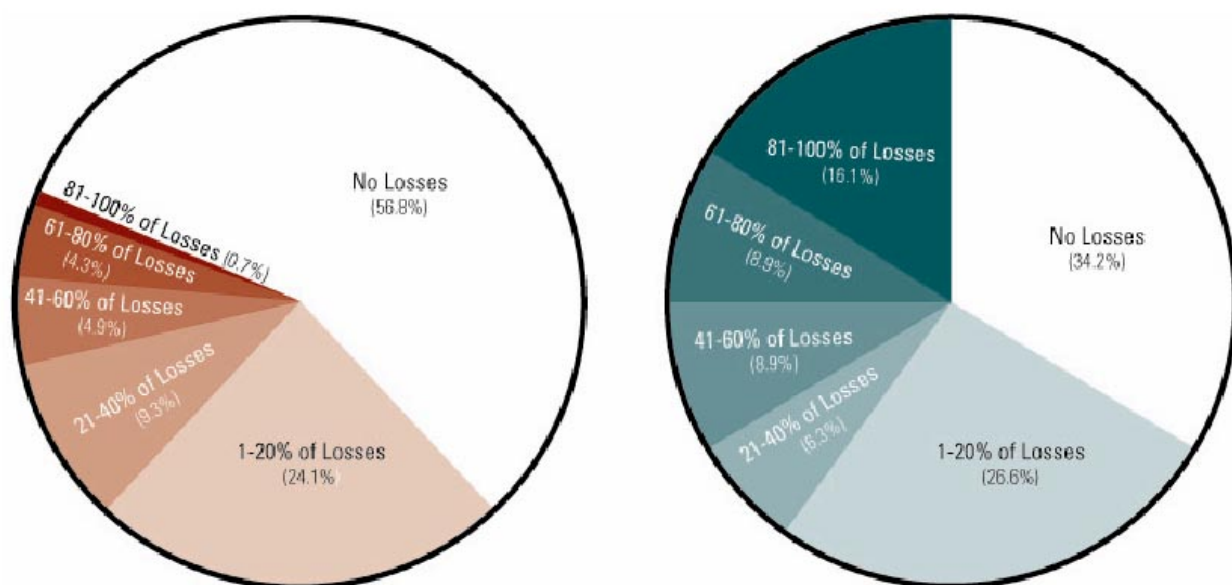


Slika 5. Najčešći bezbednosni incidenti po kompanijama/ustanovama

Kao što se sa slike 5. može videti incidenti koji su se imali najveći porast u odnosu na 2008. godinu su incidenti sa Malware-om, DoS incidenti, finansijske prevare i krađa šifri. Isto tako može se zaključiti da su incidenti sa zloupotrebom wirellessa kao i incidenti izazvani od strane insajdera u kompaniji/ustanovi u padu u odnosu na prethodnu godinu.

Zanimljiv je još i rezultat istraživanja koji pokazuje da su kompanije/ustanove prijavile čak 60% gubitaka usled slučajnih grešaka zaposlenih, grešaka koje su nastale neispravnim rukovanjem ili neznanjem korisnika (slika 6.)

Procenat gubitaka nastalih od insajdera sa namerom slučajnom greškom



Slika 6. Procenat gubitaka nastalih od zaposlenih u kompaniji/ustanovi

Kako bi smanjili rizik od napada i time smanjili gubitke u Vašoj kompaniji morate prvo spoznati koji rizici, pretnje i ranjivosti su mogući u Vašoj okolini. Sledeći korak je dobro ih proučiti i formulisati adekvatnu zaštitu i na kraju treba primenjivati tu zaštitu kada i ako do napada dodje, ali i pre i posle njega. Najčešće metode kojima cyber-kriminalci pokušavaju da probiju Vašu bezbednost su:

1. Krađa i zloupotreba šifara

Tehnologija u današnje vreme je isuviše napredovala, te tako šifre, koje predstavljaju samo niz karaktera, čak i one najsloženije, u nekom vremenskom roku mogu da se pronadju, procesuirajući ih sa nekim „cracking“ alatom kroz neki drugi računar. Metode cyber-kriminalaca da razbiju šifre su:

- Napad slučajnim pogađanjem – u nekim slučajevima šifre se mogu biti nasumičnim pogađanjem. Ponekad korisnici čak ni ne upisuju šifru, ponekad su to tipične reči: PASSWORD ili ADMIN, ime korisnika, adresa ili broj kancelarije u kojoj korisnik radi, ...
- Napadi „rečnikom“ – korisnici često upotrebljavaju uobičajne reči (GOD, LOVE, SEX) ili kratke (kraće od 8 karaktera) i lako pamtive reči iz rečnika koje cyber-kriminalci lako provale
- Napadi „brutalnom silom“ – kod napada „brutalnom silom“ koristi se svaka moguća kombinacija, i ukoliko je to moguće uvek će se doći do željene šifre. Ali u zavisnosti od složenosti šifre, brzine računara koji pokušava da otkrije tu šifru, kao i hash funkcije pitanje je koliko vremena će proteći dok ne dodje do probijanja šifre. Cyber kriminalcima obično treba da do te šifre dođu u što kraćem vremenskom periodu.

- „Hibridni“ napadi – hibridni napadi su ustvari unapređena vrsta napada rečnikom. Isto se koriste određeni rečnici, ali i određeni koji određeno slovo zamenjuje karakterom ili brojem (npr. J0hn123)

Najbolje bi bilo kada bi pored autentifikacije šifrom koristili još neki vid autentifikacije (sigurnosni token, ID karticu, biometriju...). Međutim i sa dobrom sigurnosnom polisom i snažnim šiframa može se itekako otežati posao cyber-kriminalcima. Prvo se polisom mora ograničiti broj pokušaja ukucavanja šifara (npr. nakon trećeg neuspešnog pokušaja blokiraće se sistem), a zatim se treba izabrati snažna šifra svakom korisniku. Broj lične karte, pasoša, telefona, mobilnog telefona, ime Vaše majke, oca, deteta, ljubimca, čak ni devojачko prezime Vaše majke i rođendani nisu podobni za snažnu šifru, a korišćenje takve šifre od strane krajnjeg korisnika čine šifru beskorisnom. Dobru i snažnu šifru čini kombinacija velikih i malih slova, brojeva kao i specijalnih karaktera. Treba izbegavati reči iz rečnika, a šifra treba da bude dovoljno dugačka, ali oepť ne preduga kako bi je korisnik lakše zapamtio a ne zapisao jer ma koliko šifra bila jaka i snažna, ako korisnik je zapiše i drži na vidnom ili dostupnom mestu ona postaje dostupna cyber-kriminalcima. Vrlo često se umeto jedne reči upotrebljava i fraza sastavljena od više karaktera, brojeva i specijalnih karaktera.

Primer stvaranja dobre šifre, šifre koja će lako da se zapamti a opet teška za provaljivanje, bio bi:

Grad + Uzrečica + Sport + Godina + Broj



Bg + bre + biathlon + 2010 + 12

bgbrebiathlon201012

Kada tu šifru sredimo koristeći brojeve i specijalne karaktere dobijamo

BGBReb1@thl0NMMX!2.

Pored toga što je ne zapisujemo, dobru i snažnu šifru ne treba koristiti na više mesta, a naročito ne na javnim Internet nalogima koji nemaju baš uvek dobru zaštitu. Takođe ne treba koristiti nesigurne protokole, koji šifru šalju kao čisti tekst, šifre trebaju da putuju enkriptovane.

2. Trojanci

Trojanci predstavljaju specifičan malware čija je spoljna manifestacija obično zabavna i interesantna prosečnim korisnicima., koji omogućavaju cyber-kriminalcima udaljen pristup kompjuterskom sistemu, a da korisnici čak i ne primeti. On ne inficira ostale izvršne datoteke, jer se ne umnožava (replicira). Trojanci nisu virusi zato što se ne

umnožavaju, već stoje i čekaju da budu pokrenuti, direktnim aktiviranjem, ili uz pomoć drugog programa koji ga pozove. Svako danas može napraviti Trojanca i povezati ga sa nekom benignom aplikacijom. Ta aplikacija se zajedno sa Trojancom korisnicima dostavlja na razne načine: direktnim unosom, kada neovlašćeno lice sedne za računar i preko prenosnog medija ubaci Trojanca, kao attachment u e-mail poruci, kroz download softvera od strane korisnika, kroz Web izvršive aplikacije (ActiveX), kroz propuste u programskim kodovima Web pretraživača, Media plejerima, IM klijentima, kao i mnogim drugim aplikacijama. Vrste šteta koje Trojanci prave su takođe varijabilne: neovlašćeno skidanje, prepravljjanje ili brisanje podataka kao i e-mail poruka, instalacija softwarea prikrivanje drugih procesa. Međutim cilj većine Trojanaca je da omogući udaljenom korisniku pristup i punu kontrolu nad napadnutim računarom. Česti su i napadi koji iskorištavaju računar korisnika za napad na neki server, radi zloupotrebe ili kompjuterskog kriminala, što se pripisuje vlasniku sistema.

Postoji mnogo vrsta Trojanaca, ipak po svojim osobinama ističu se dva najpoznatija: SubSeven i NetBus.

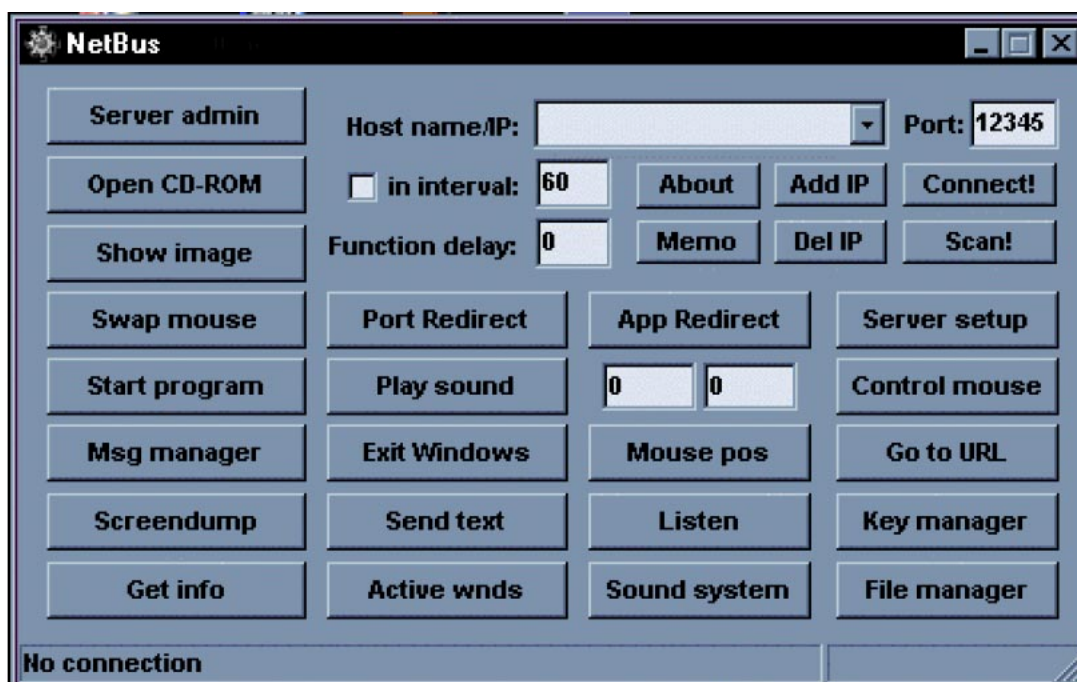
Subseven je jedan od najnaprednijih virusa naprednih karakteristika i sposobnosti. Na slici 7. možemo videti izgled Trojanca SubSeven zajedno sa nekim od mogućnosti koji pruža napadaču.



Slika 7. Izgled Trojanca SubSeven

Napadač uz pomoć SubSeven Trojanca može da: prekopira ceo adresar, izvrši IP skeniranje sa udaljene lokacije, host lookup, dobiti broj Windows Cdkey-a, preuzme ili špijunira sve Instant Message servise, kreira FTP root folder, rediriguje portove, preuzme ili obriše fascikle, kao i da napravi nove, preuzme menadžer procesa, preuzme dial-up konekciju(ako postoji) zajedno sa korisničkim imenom i šifrom, restartovanje servera kao i preuzimanje podataka sa njega (Adresa, ime, grad, kompanija, e-mail, ...) itd.

Netbus spada u jedne od starijih Trojanaca, međutim zbog brojnih mogućnosti i danas se mnogo upotrebljava. Na slici 8. možemo videti izgled Trojanca NetBus zajedno sa nekim od mogućnosti koji pruža napadaču.



Slika 8. Izgled Trojanca NetBus

Odlike NetBus Trojanca su: otvaranje CD/DVD uređaja (jednom ili u određenom intervalu), zamena f-ja miša (levi klik postaje desni i obrnuto), startovanje određene aplikacije, puštanje određenog zvuka (zbog starosti Trojanca u opciji je samo WAV fajl), pojačavanje i u tišavanje zvuka, gašenje računara, direkcija ka određenoj URL adresi, postavljanje (Upload), skidanje(download) i brisanje (delete) podataka sa/na računar „metu“. Međutim najopasnije opcije ovog Trojanca su: redirekcija podataka kao i aplikacija sa računara „mete“ na određeni port ili na drugi računar „metu“ pri čemu taj drugi računar kao napadača vidi samo prvi računar „metu“ a ne i pravog napadača.

Trojanci se obično sastoje od server i klijent dela, pri čemu je server program koji treba da se ubaci u računar „metu“. Najčešći metod ubacivanja Trojanca u neki računar je sa nekom drugom aplikacijom. Na primer napadači mogu uzeti neku bezazlenu igricu (kao primer uzecu kartasku igru Texas HoldEm poker):



Texas.exe

+



TrojanServer.exe

Aplikacija napadača lako i bezo će sjediniti ova dva fajla u jedan fajl razno.exe, koji se lako kasnije preimenuje u Texas.exe. Razlika između originalnog Texas.exe fajla i zaraženog Texas.exe fajla je samo u njihovim veličinama (i to ne znatno). Sada ostaje samo da postavi igricu na neki server. Kada korisnik skine fajl i pokrene ga, korisniku će

sve izgledati normalno, pokrenuće igru pokera koju je tražio, međutim u pozadini serverski deo Trojanca se instalira i ako je korisnik na Internetu šalje podatke napadaču o podacima korisnika koga je zarazio. Napadač kroz klijentski deo Trojanca pristupa zaraženom računaru kroz Serverski deo.

Na svu sreću današnji antivirus programi kao i razni malware skeneri otkrivaju gotovo sve vidove Trojanaca. Baš zato kao najbolja odbrana od Trojanaca je redovan update kako antivirus i „antimalware“ softvera, tako i svih ostalih aplikacija na sistemu kao i operativnog sistema jer programeri kad otkriju „rupu“ u kodu nastoje da je što pre zatvore i odmah šalju zakrpe kojima se to postiže. Takođe treba se vršiti redovno skeniranje sistema, čitave mreže, a za Trojance možda i najbitnije monitoring odlazećeg saobraćaja.

3. Iskorišćavanje podrazumevanih vrednosti

Nema ništa lakše i lepše jednom cyber-kriminalcu nego kad neki korisnik koristi podrazumevane vrednosti koje je dobio pri kupovini računara od proizvođača ili prodavca. Mnogi napadački softveri pretpostavljaju da su na računaru tj. u računarskom sistemu koji napadaju podrazumevane šifre i da je sistem podešen na podrazumevane vrednosti. Internet je prepun sajtova sa katalogima podrazumevanih korisničkih imena, pristupnih šifri, konvencija imena raznih proizvođača, ali isto tako i komponenta, servisa i konfiguracija.

Zaštitne mere od ovoga sigurno bi bile da se promene podrazumevane vrednosti šifara, da se isključe „gostinski“ nalozi kao i nalozi korisnika koji nisu više u kompaniji, da se isključe servisi koji se ne upotrebljavaju (npr. Telnet ili FTP). Takođe pokušajte da izbegnete instalaciju softvera u njihove standardne fascikle.

4. Čovek u sredini

Pri napadima „Čovek u sredini“, napadač uspeva da zavara korisnika da pristupa pravom serveru tj. servisu, a ustvari korisnik pristupa sistemu kojeg kontroliše napadač. „Čovek u sredini“ napad obično počinje sa phishing e-mailom, koji deluje bezazleno i koji sadrži URL adresu. Međutim ta URL adresa vodi korisnika na adresu na zloćudni sistem kontrolisan od napadača, koji ima isti interfejs kao i legitimni server tj. servis. Napadač time dobija podatke za logovanje korisnika na pravi server, a time i raspolaže i resursima korisnika na tom serveru bez njegovog znanja. Ovo je lakši metod napada „čovek u sredini“, teže metode podrazumevaju dupliranje MAC-a (Media Access Control), trovanje ARP-a (Address Resolution Protocol) kao i tabela rutiranja i DNS (Domain Name Server) pretrage, pravljenje novih lažnih routing tabela, napad na DNS server korisnika kao i servera kojem korisnik pristupa, rerutiranje proxija...

Najbolji vid zaštite je ne klikati na URL adrese sumnjive prirode. Takođe za ovakve napade pomaže i IDS (Intrusion Detection System) sistemi koji prate mrežni saobraćaj, kao i promene lokalnog sistema.

4) Mere zaštite

Pored ovih metoda napada, cyber-kriminalci koriste još mnoge druge. Međutim većina od njih prvo se informiše o korisnim podacima potencijalnih meta. Tačna informacija je postala jedna od moćnih oružja u današnjem cyber svetu. Tako napadači mogu saznati imena predsednika kao i nadređenih u Vašoj kompaniji, imena zaposlenih koji su u skorije vreme dobili otkaze (vrlo često se dešava da njihova korisnička imena i

šifre ostanu u sistemu još neko dogledno vreme), adresu i telefone kompanije, provajdera za Internet te kompanije, detaljne podatke o svim zaposlenim, ceo softver sistema kao i najslabije tačke u bezbednosnoj strukturi Vašeg sistema.

Možda i najbolja zaštita od napada ove vrste je dizanje svesti korisnika o informacionoj bezbednosti, o pretnjama i napadima koji dolaze cyber tehnologijom, kao i obuka istih o načinima zaštite kako ne bi došlo do neželjenih šteta. Međutim menadžmenti kompanija obično obučavaju zaposlene kako da upotrebljavaju beneficije nekog sistema i kako da ga koriste a i sami zaposleni nisu uvek voljni da učestvuju u takvim obukama. Treba ubediti menadžment da ulaganje u dobru politiku bezbednosti, dobru bezbednosnu opremu kao i obuku korisnika o informacionoj bezbednosti, predstavlja dobru investiciju, jer ti segmenti dovode do bolje zaštite informacionih sistema kompanije, a samim tim i do manjih šteta prouzrokovanih upadom u iste. Politika bezbednosti treba da sadrži sve metode korišćenja informacionog sistema u Vašoj kompaniji koji će omogućiti zaštitu informacija i imovine od svih pretnji, kako od eksternih tako i od internih. Politika bezbednosti treba da je jedinstvena i svojstvena za svaku kompaniju.

Kompanije često, bez razmišljanja, rado daju ključeve svoje bezbednosti drugim kompanijama, samo zato što su te druge kompanije ekspertske u toj oblasti i time se osećaju bezbedno. Sertifikaciona tela im kažu kome treba da veruju, ukidajući im time mogućnost da same odluče kome će i u šta verovati. Webmail servisi pružaju serversku enkripciju i dekripciju i ukidaju mogućnost da korisnici kontrolišu sopstvene enkripcione ključeve, a samim tim mogućnost enkripcije između samih korisnika. **Ne postoji kompanija niti proizvođač kome više možete verovati osim same Vaše kompanije.** Korporativni proizvođači uglavnom uvek gledaju samo da zaštite svoj profit i udeo na tržištu. Zato morate preispitati Vaše bezbednosne potrebe i prema njima izabrati proizvode koji će te potrebe zadovoljiti, nebitno od kog proizvođača oni bili.

Na kraju, čak i kad se najbolji plan bezbednosti informacionog sistema Vaše kompanije sprovede u delo, morate biti na oprezu jer sa razvojem novih tehnologija razvijaju se i opcije i mogućnosti da Vam neko upadne u system.

5) Zaključak

Da li je rešenje da se diskonektujemo sa globalne mreže, izbrišemo naše prisustvo na mreži i sakrijemo u svoje odaje? Ovakva opcija nije moguća, jer u današnjem modernom svetu, funkcionisanje bez globalne mreže je gotovo nemoguće, a upuštanje u svet informacija predstavlja put bez povratka. Ključ uspeha je u povećanom oprezu i konstantnoj budnosti. Upotrebite zdrav razum, kao što to činite i u pravom životu. Ne verujte strancima, ne idite na mesta „sumnjive“ prirode, ne dajte korisne i poverljive informacije. Preduzmete li neke mere predostrožnosti i dalje možete da iskorišćavate taj svet informacija a da pritom ne postanete nečija žrtva.

6) Literatura

- [1] Kassner Michael: “10 ways to avoid IT security breaches”, TechRepublic, <http://techrepublic.com.com/>
- [2] Perrin Chad: “10 things you should do to secure every general-purpose operating system”, TechRepublic, <http://techrepublic.com.com/>

- [3] Shinder Debra Littlejohn: "10 technologies that cybercriminals love to exploit", TechRepublic, <http://techrepublic.com.com/>
- [4] Steward James Michael: "Ten ways Hackers Breach Security", Global Knowledge, <http://www.globalknowledge.com/>
- [5] Richardson Robert: "14th Annual CSI Computer Crime and Security Survey", Computer Security Institute, <http://gocsi.com>
- [6] „An Introduction to Computer Security: The NIST Handbook“, National Institute of Standards and Technology Technology Administration, <http://www.nist.gov/index.html>
- [7] "Kompjuterski kriminalitet", APIS Security Consulting, <http://www.apisgroup.org/sec.html?id=29>
- [8] "The top 10 Internet Frauds", National Fraud Information Center, <http://www.nclnet.org/>
- [9] Statistički podaci o korisnicima Interneta, <http://www.internetworldstats.com/>

Abstract: Development of information and communication technology improve business and make it much easier (e-commerce). However at the same time it made, and still make, possibilities for cyber-criminals to brake in system of some user or company and to make some damage. In this work I described development growth of Internet in new century, definitions of cyber crime, types of abuses and frauds caused with that devolpment of ICT, technologies that have been attacked the most, some of methods that attackers used and how to protect from these attacks.

Key words: cyber criminal, types of attack, trojans, security issues