CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Pregled sigurnosnih incidenata u 2008. godini

CCERT-PUBDOC-2009-02-254

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Računalni kriminal, iz godine u godinu, postaje sve sofisticiraniji i efikasniji. Napadi su sve više usmjereniji prema manjim konkretnim metama, a sve sa ciljem skupljanja osjetljivih podataka. Krađa osjetljivih informacija i dalje je glavni uzrok nastajanja sigurnosnih incidenata. Naravno, ne smije se zanemariti ni faktor ljudske znatiželje kad napadači ispituju dokud sežu njihove granice prilikom napada na tuđi sustav, bez ikakve konkretne namjere.

Računalne tehnologije svakodnevno napreduju i dolazi do razvoja novih tehnologija namijenjenih međusobnoj kolaboraciji i povećanju produktivnosti. Tu se prvenstveno misli na nove generacije uređaja, te porast korištenja web 2.0 stranica. Nepoštovanje sigurnosnih standarda od početka razvoja ovih novih tehnologija zadaju nove glavobolje sigurnosnim stručnjacima. Ovi trendovi počeli su se pokazivati već u 2008. godini, a stručnjaci predviđaju da će njihov udio u budućnosti biti još veći. Veći broj različitih tehnologija za napadača znači veći izbor načina pomoću kojih može napasti određeni sustav pa je važno razvijati nove tehnologije sa posebnom pažnjom na sigurnosni aspekt.

Iako su neželjeni programi (eng. malware) do sada uglavnom bili problem Microsoft operacijskih sustava i programa, u 2008. godini to postaje problem i ostalih operacijskih sustava kao što su Mac OS X Leopard, te razne distribucije Linux operacijskih sustava. Istodobno, zlonamjerni programi postaju i problem aplikacija i operacijskih sustava na mobilnim telefonima. S obzirom na rastuću popularnost Google Android operacijskog sustava i uređaja poput iPhonea i iPod Toucha stručnjaci predviđaju ne samo nastavak ovog trenda, već i njegov značajniji porast.

Zlonamjerni programi pisani prije desetak godina bili su napravljeni iz jednostavnog razloga – kako bi se zarazilo tuđe računalo. Današnji napadi su organizirani i osmišljeni u svrhu krađe informacija sa računala tvrtke, a sve zbog postizanja dodatne zarade. Broj globalnih sigurnosnih incidentata je došao do te razine da se, kako stručnjaci Sophos-a navode, svakih 4.5 sekundi otkrije nova zaražena web stranica. To nas dovodi do brojke od nekih 20 000 sigurnosnih napada dnevno. Potreba za povećanom sigurnosnom zaštitom ne samo da postaje dio naše budućnost, već postaje i pravilo.

2. Web prijetnje

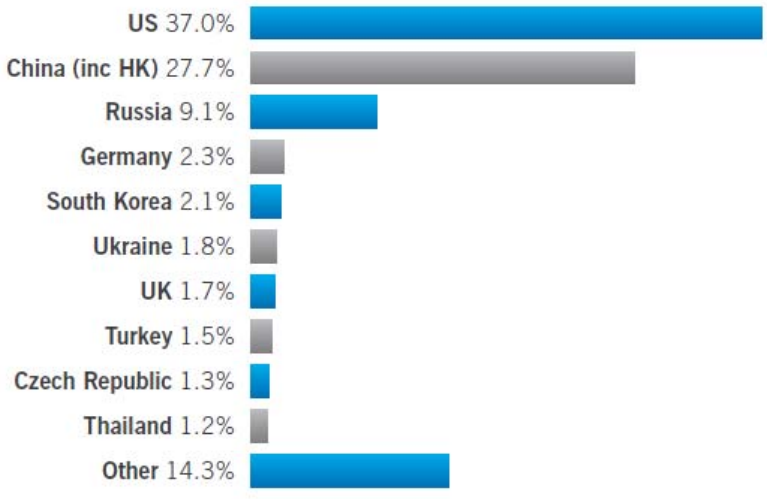
U 2008. godini, kao i prijašnjih godina, nastavio se povećani trend širenja zlćudnih programa pute web stranica. Time je web, kao medij za širenje zlćudnog koda, istisnuo poruke elektroničke pošte koje su u prijašnjim godinama bile najzastupljenije. Zlonamjerni napadači iskorištavaju sigurnosne propuste kod legitimnih web stranica kako bi ubacili zlćudni kod koji onda pokušava zaraziti svakog korisnika koji posjeti ranjivu stranicu. Upravo je veliki broj posjetitelja - potencijalnih žrtava – razlog zašto je web toliko popularan kao meta zlonamjernih napadača.

Prema izvješću stručnjaka tvrtke Sophos, web stranice mnogih poznatih svjetskih tvrtki i organizacija bile su žrtve zlonamjernih napada u protekloj godini. Neki od značajnijih primjera su web stranice tvrtki Adobe[6] i Trend Micro[7], zatim službene stranice na kojima su se prodavale karte za Europsko prvenstvo u nogometu[8], stranice časopisa BusinessWeek[10] te američke stranice tvrtke Sony[9]. Većina napada izvedena je umetanjem SQL (eng. Structured Query Language) koda (eng. SQL injection) što pokazuje još jedan trend primijećen od strane Sophosovih stručnjaka.

Umetanje zlćudnog koda na legitimne web stranice efektivan je način širenja zlćudnih programa. Posjetitelji takvih stranica obično nemaju nikakve sumnje u njihovu sigurnost i ispravnost jer su to stranice koje redovito posjećuju. Sigurnosne aplikacije koje filtriraju URL (eng. Uniform Resource Locator) i IP (eng. Internet Protocol) adrese također su nemoćne u sprječavanju ovakvih napada. Kompromitiranje legitimnih stranica napadačima omogućuje vrlo precizno odabiranje korisničkih grupa koje žele zaraziti. Tako primjerice mogu napasti stranice fakulteta ukoliko su je ciljna skupina studenti, ili stranice nekog poslovnog časopisa ukoliko žele kompromitirati tvrtke i druge poslovne subjekte.

Prema podacima koje je objavila tvrtka Cisco, 87% svih web prijetnji dolazi od strane web stranica sa zlćudnim kodom. Također, prema podacima tvrtke White Hat Security, više od 79% zlćudnih web stranica su kompromitirane legitimne web stranice. Razlog ovom trendu može se pronaći upravo u zanemarivanju sigurnosti kao važnog čimbenika u izradi svake web stranice.

Statistički podaci prikazani na slici 2.1 prikazuju kako je gotovo trećina svih zlćudnih web stranica locirana u SAD-u, Kini ili Rusiji. Iako se ove tri države najviše ističu, ne treba zanemariti utjecaj ostalih država. Prema Sophos-ovom istraživanju postoji cijeli niz država (oko 150) u kojima su locirane zlćudne web stranice. Među web stranicama uključenima u istraživanje, njih čak 85% bile su legitimne stranice kompromitirane od strane zlonamjernih napadača.



Slika 2.1. Top 10 država sa najvećim brojem zlćudnih stranica

Broj zlćudnih stranica lociranih u SAD-u bilježi značajan porast u usporedbi sa 2007. godinom kada se 23.4%

svih otkrivenih zloćudnih stranica nalazilo u toj državi. Kina je u 2007. godini bila država u kojoj se nalazilo najviše zloćudnih web stranica (čak 51.4%), no u 2008. je zabilježen značajan pad na 27.7%. Češka je nova država na ovoj nepopularnoj listi sa nešto više od 1% svih otkrivenih zloćudnih stranica, dok su sa nje ispale Poljska, Francuska i Kanada koje su 2007. zauzimale šesto, osmo i deveto mjesto.

2.1. Vrste napada

Neki od najpopularnijih napada kod zlonamjernih napadača u 2008. godini su napadi umetanjem SQL koda, XSS (eng. Cross Site Scripting) napadi te XSRF napadi. Zabilježeni su slučajevi kod kojih su napadači kod XSS napada, te napada umetanjem SQL koda koristili tzv. iFrame ranjivost. Riječ je o oznaci HTML (eng. HyperText Markup Language) jezika koja omogućava ubacivanje zloćudnog koda sa drugog poslužitelja u kompromitiranu web stranicu.

Nedovoljna provjera podataka koje korisnik unosi razlog su brojnim napadima umetanjem zloćudnog SQL koda. Oporavak nakon ovakve vrste napada može biti težak i kompliciran, a zabilježeni su i brojni slučajevi u kojima su web stranice ponovno napadnute nekoliko sati nakon.

Također, uočen je trend izrade automatiziranih alata za otkrivanje i iskorištavanje ranjivosti web aplikacija od strane zlonamjernih korisnika. Takvi alati koriste se tražilicama (poput Google-a) za otkrivanje ranjivih stranica te onda automatski iskorištavaju ranjivosti i provode napade. Ciljevi tih alata nisu specifične, već nasumične web stranice koje posjeduju poznate ranjivosti.

Otkriven je i značajan broj web stranica koje su u potpunosti izradili zlonamjerni napadači, obično postavljenih putem besplatnih servisa za pohranu web stranica (eng. free web hosting services). Takve stranice onda se najčešće reklamiraju na forumima i blogovima putem nekih automatiziranih alata. Prilikom posjete takvih stranica od korisnika se obično traži instalacija nekog lažnog programskog dodatka (npr. lažnog Flash Player-a).

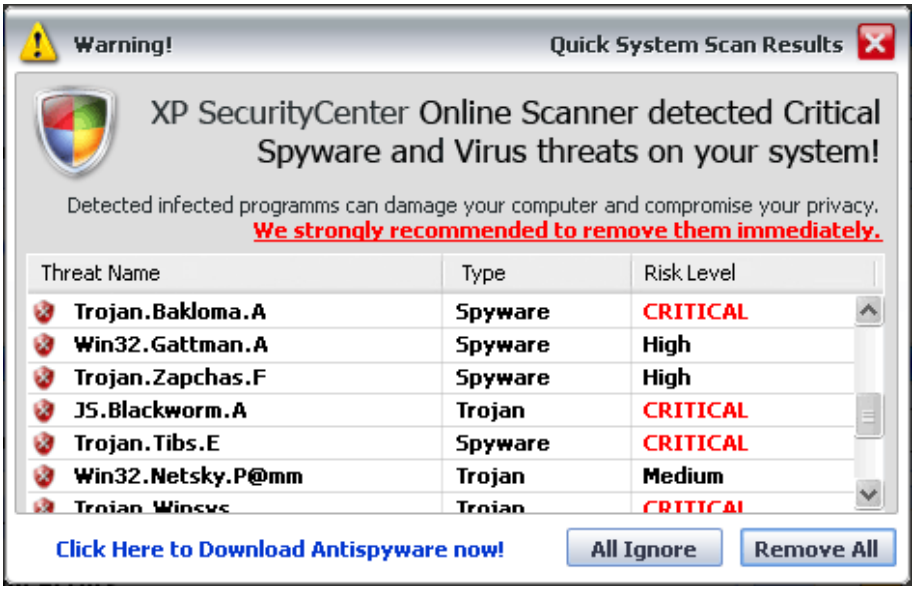
Slika 2.2. Pokušaj instalacije lažnog dodatka

2.2. Primjeri napada

Jedan od značajnijih primjera napada na Internetu je napad na web stranicu poslovnog časopisa BusinessWeek u rujnu 2008. godine. Radilo se o napadu umetanjem SQL koda kod kojeg je na web stranicu ovog uglednog časopisa umetnut trojanski konj Mal/Badsrc-C. Ovaj slučaj je posebno odjeknuo u javnosti budući da se stranica BusinessWeek-a nalazi među 1000 najposjećenijih stranica na webu.

Drugi primjer dogodio se na japanskim i engleskim stranicama antivirusne kompanije Trend Micro. U ovom napadu iskorištena je upravo iFrame ranjivost spomenuta u prethodnom poglavlju. Svi korisnici ranjive stranice bili su preusmjeravani na zloćudnu stranicu i izloženi napadu trojanskog konja.

Još jedan od napada zabilježen je na američkim stranicama tvrtke Sony. Radilo se o stranici koja predstavlja nove igrice za PlayStation, igraću konzolu tvrtke Sony. Korisnicima ranjive stranice ponuđen je lažni antivirusni proizvod koji je sadržavao maliciozni program i javljao korisniku lažne poruke o infekciji.



Slika 2.3. Reklamiranje lažnog antivirusnog proizvoda

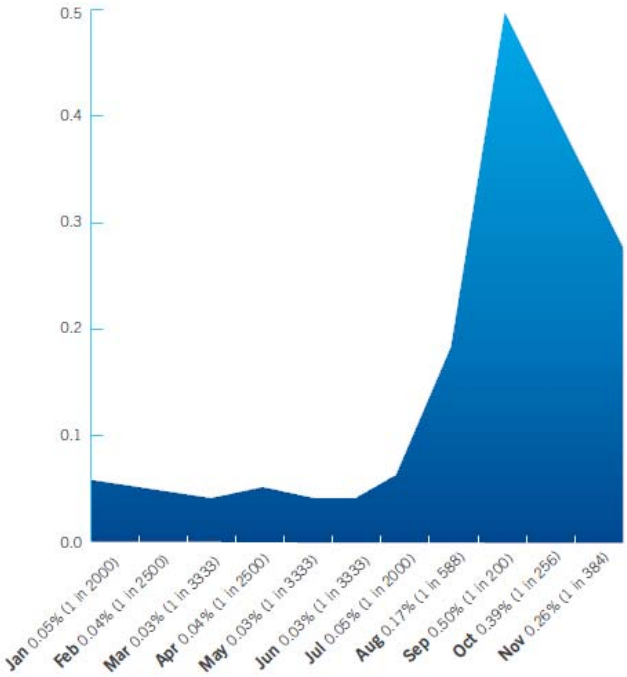
3. Napadi putem poruka elektroničke pošte

Broj napada putem poruka elektroničke pošte u 2008. godini doživio je značajan porast, iako je posljednjih nekoliko godina zabilježen trend pada ove vrsta napada. Kao što se može vidjeti u tablici 3.1., od 2005. godine kada je svaka 44. poruka elektroničke pošte sadržavala zloćudni program u privitku, frekvencija ovakvih napada pala je na svaku 714. poruku početkom 2008. godine.

Godina	Poruka sa zloćudnim privitkom
2005	svaka 44. poruka
2006	svaka 337. poruka
2007	svaka 909. poruka
2008	svaka 714. poruka

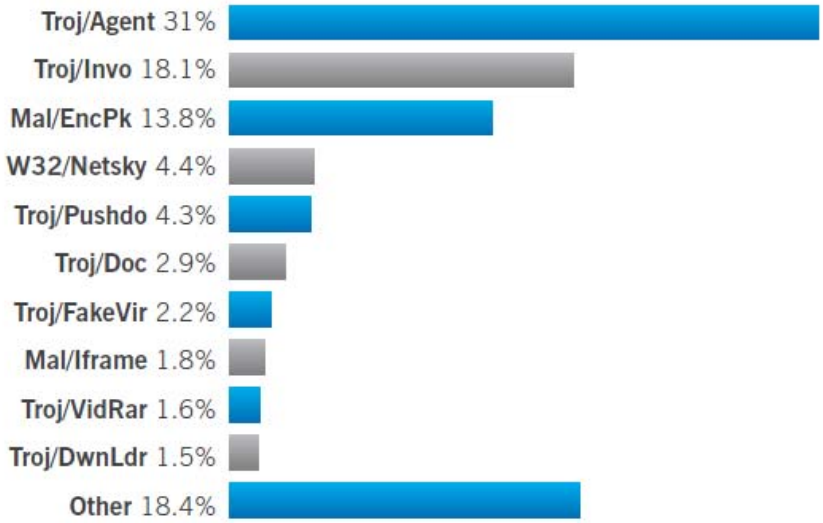
Tablica 3.1. Broj zaraženih poruka elektroničke pošte

Međutim, tijekom 2008. godine zabilježen je ponovni porast poruka sa zloćudnim privicima. Ovaj trend najbolje se može vidjeti na slici 3.1. koja prikazuje porast zloćudnih poruka kroz mjesece 2008. godine.



Slika 3.1. Porast zloćudnih poruka u 2008. godini

Stručnjaci iz tvrtke Sophos tvrde da su razlog ovog porasta tri značajnija napada koja su se dogodila krajem godine. Riječ je o dva napada koji su se širili putem obavijesti o neuspješnim dostavama putem tvrtki kao što su Fed-Ex i UPS, a sadržavale su trojanskog konja Invo-Zip, te o napadu porukama koje su reklamirale iPhone igrice, a širile trojanskog konja EncPk-CZ.

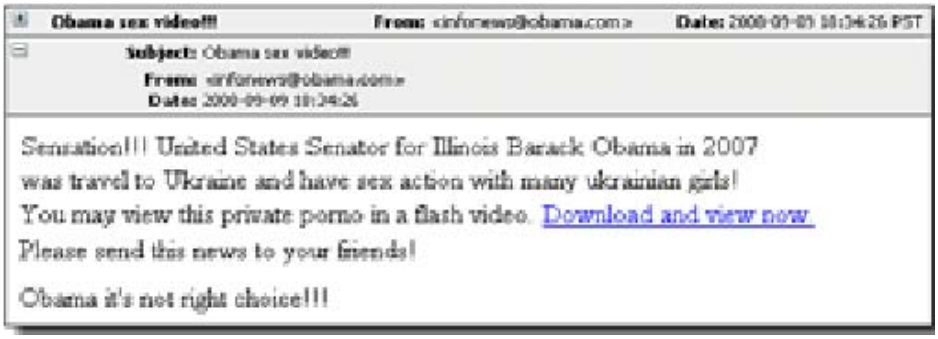


Slika 3.2. Top lista najzastupljenijih zloćudnih programa u porukama elektroničke pošte 2008.

Na slici 3.2. prikazana je lista trojanskih konja i drugih zloćudnih programa koji su bili najzastupljeniji u privicima elektroničke pošte u 2008. godini. Činjenica da je trojanski konj Pushdo u prvoj polovici 2008. bio zastupljen sa 31% u napadima porukama elektroničke pošte, a na kraju godine sa tek 4.3%, slikovito ilustrira koliko se značajan porast ove vrste napada dogodio u drugoj polovici godine.

Napadači su se u 2008. služili i drugim tehnikama za napadanje računala preko elektroničke pošte. Primjerice, zabilježen je značajan broj zlonamjernih poruka koje ne sadrže zloćudne privitke, već poveznice (eng. link) na zloćudne web stranice. Korisnike se atraktivnim ponudama ili vijestima pokušava navesti da posjete te zloćudne stranice i tako se zaraze nekim od zloćudnih programa.

Jedan od poznatijih primjera takvog napada dogodio se u rujnu prošle godine. Internetom se širila poruka elektroničke pošte u kojem se poticalo čitatelja da posjeti stranicu na kojoj može vidjeti pornografski uradak američkog predsjednika Barracka Obame. Umjesto reklamiranog sadržaja svaki posjetitelj stranice bio je zaražen zloćudnim programom Mal/Hupig-D.



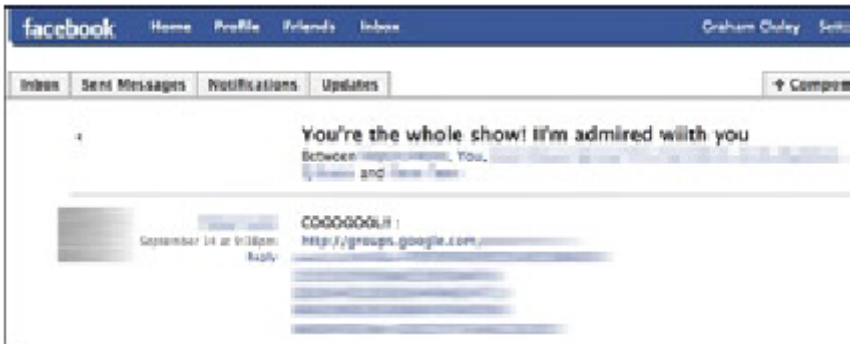
Slika 3.3. Lažna poruka elektroničke pošte

4. Zloćudni programi

Jedna od značajnijih metoda kojima su se služili kriminalci u 2008. godini,bila je oglašavanje lažnih antivirusnih proizvoda. Takva vrsta napada straši žrtvu jer ju uvjerava da njeno računalo ima nekakav sigurnosni problem i da je jedino rješenje u korištenu određenog antivirusnog alata. Najčešće se takvo programsko rješenje oglašava na web stranicama u obliku "pop-up" oglasa (mali prozori koji iskaču prilikom surfanja i sadrže reklamu). U takvim oglasima lažno se reklamira, odnosno predstavlja programsko rješenje za kojeg se navodi da ima odlične kritike te je jako efikasan u pronalaženju i uništavanju računalnih virusa i drugih zloćudnih programa. Često se prilikom kupovanja takvih proizvoda korisnicima kradu osobni i povjerljivi podaci poput adresa elektroničke pošte i brojeva kreditnih kartica. Stručnjaci iz tvrtke Sophos tvrde da su tijekom 2008. godine dnevno otkrivali i do 20 takvih lažnih web stranica koje reklamiraju antivirusne proizvode.

Zloćudni programi prilično su se brzo proširili i na prijenosne memorijske uređaje (USB prijenosne memorije i slično). Možda najbizarniji primjer ovakvog načina prijenosa zloćudnih programa koji se dogodio tijekom 2008. godine je onaj kada su astronauti iz NASA-e nepažnjom prenijeli računalni crv W32.Gammima.AG putem USB memorije na internacionalnu svemirsku postaju. Antivirusni program je, srećom, detektirao zlonamjerni program, ali su posljedice mogle biti katastrofalne.

Sve većom popularnošću društvenih mreža poput Facebook-a i MySpace-a bilo je za očekivati da će autori zloćudnih programa iskoristiti i ovaj fenomen za širenje svojih uradaka. Tako je u 2008. godini zabilježeno više slučajeva kompromitiranja profila korisnika ovih mreža kako bi se oni iskoristili za širenje zloćudnih programa. Tako su, primjerice, Facebook korisnici tijekom 2008. počeli dobivati poruke od osoba koje im se nalaze na listi prijatelja, a kojima su računi kompromitirani. U tim porukama ponovno se navodi čitatelja da posjeti zloćudne web stranice.

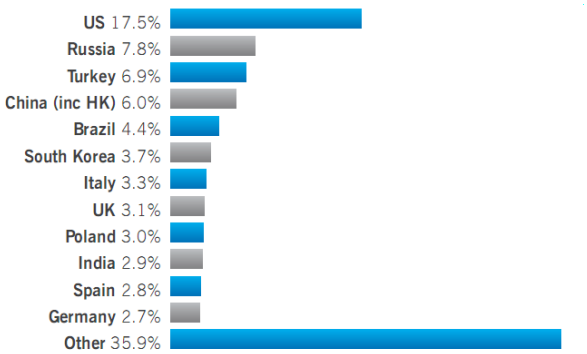


Slika 4.1. Lažna poruka na društvenoj mreži Facebook

U 2008. godini povećan je broj napada i na neke raširene i često korištene programe poput Adobe Reader-a te Flash Player-a, a ne kao do sada samo na operacijske sustave i Internet preglednike. Razlozi povećanja ovih napada može se pronaći u sve većoj integraciji spomenutih programa sa web preglednicima. Tako su, primjerice, PDF dokumenti i Flash video datoteke sastavni dio gotovo svake moderne web stranice. Također je primijećen i veći porast broja tzv. "rootkit" programa od čak 46%. Riječ je o zlonamjernim programima koji se integriraju duboko u operacijski sustav korisnika kako bi izbjegli detekciju od strane antivirusnih programa.

4. Spam

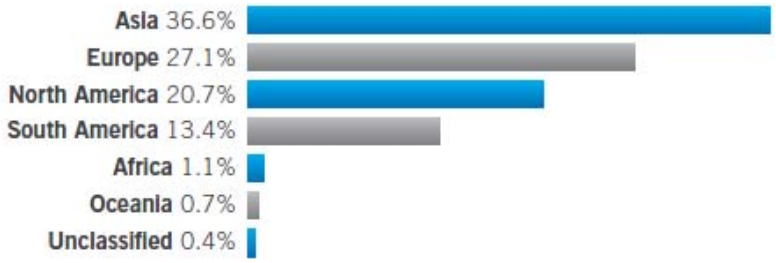
Baš kao i proteklih godina, i u 2008. spam (neželjena elektronička pošta) predstavlja veliki problem za poslovanje tvrtki, ali i druge subjekte na Internetu. Prema istraživanju stručnjaka iz tvrtke Sophos 97% svih poruka elektroničke pošte zapravo je spam. Spam je u protekloj godini poslan iz 240 različitih zemalja svijeta. Na slici 4.1. prikazani su udjeli pojedinih zemalja u ukupnom broju poslanih spam poruka.



Slika 4.1. Udio odaslanih spam poruka po zemlji podrijetla

Zemlja sa najvećim udjelom spam poruka (sa 17.5%) u 2008. godini je SAD, iako je u usporedbi s 2007. uočena tendencija pada tog udjela (u 2007. udio je bio 22.5%). Većina spam poruka i dalje sadrži zlоćudne privitke ili poveznice na zlonamjerne web stranice, a većina spam poruka šalje se sa tzv. "botnet"-ova, odnosno mreža povezanih računala koji su pod kontrolom zlonamjernih napadača.

Iako je SAD država iz koje se šalje najviše spam poruka, kontinenti na kojima je uočena najveća tendencija rasta spam-a su Azija i Europa. Kao što se može vidjeti na slici 4.2., spam poruke poslane na adrese u Aziji i Europi čine gotovo dvije trećine od svih ukupno dostavljenih.



Slika 4.2. Udio kontinenata u broju dostavljenih spam poruka

Novi putovi širenja neželjenih poruka uočeni u 2008. godini su oni putem blogova i raznih društvenih mreža. Autori neželjenih poruka izrađuju posebne automatizirane alate za ostavljanje poruka na ovakvim i sličnim stranicama najčešće u obliku komentara, osobnih poruka ili statusa. Mnogi od ovakvih napada povezani su sa krađom korisničkih podataka i upadima na profile korisnika.

Slika 4.3. Spam poruka na društvenoj mreži Twitter

Prema izvješću tvrtke Sophos čak 85% svim komentara na blogovima su spam poruke generirane automatiziranim alatima. Spam poruke na raznim društvenim mrežama usko su povezane uz prijevare i krađe korisničkih podataka, a čak su zabilježeni i slučajeva kada su napadači osobno imitirali osobe kojima su ukrali podatke kako bi bili što uvjerljiviji u širenju svojih zlonamjernih programa. Kako popularnost društvenih mreža i dalje raste stručnjaci predviđaju da će upravo prijevare na takvim stranicama i u budućnosti biti u značajnom porastu.

5. Mobilni telefoni

Svijet mobilnih telefona 2008. godine obilježili su izlazak 3G verzije Apple iPhone-a te novog operacijskog sustava tvrtke Google naziva Android. Nova verzija već popularnog uređaja tvrtke Apple te izlazak prvog telefona pogonjenog Google-ovom platformom Android dodatno su zahuktali tržište mobilne telefonije i privukli veliki broj novih korisnika.

3G verzija Apple iPhone-a pobudila je mnogo zanimanja u poslovnim krugovima i među redovitim korisnicima Interneta upravo zbog novog i boljeg načina spajanja i jeftinije cijene. Planetarna popularnost iPhone-a već je donijela Apple-u mnogo profita, ali i brojne glavobolje kod implementacije sigurnosnih standarda i funkcija. Baš kao i kod drugih novih popularnih tehnologija, zlonamjerni napadači pokušavaju iskoristiti svaku mogućnost novih tehnologija kako bi ih iskoristili za svoje zlonamjerne aktivnosti. Iako je već otkriven jednostavan zloćudni program namijenjen iPhone-u, neki značajan napad na sigurnost ovog uređaja nije zabilježen. Broj korisnika iPhone-a svakodnevno raste, što znači da raste i broj potencijalnih meta za zlonamjerne napadače, pa se opasniji napadi na ovaj i druge slične uređaje u budućnosti svakako očekuju. Dosad je pronađeno nekoliko sigurnosnih propusta u Apple-ovom rješenju za slanje elektroničke pošte preko mobitela te u Safari Internet pregledniku. Važno je spomenuti i kako je Apple dobio mnogo kritika jer uočene propuste nije zakrpao istodobno sa propustima ekvivalentnih aplikacija za Mac OS operacijski sustav. Usprkos nađenim propustima nisu zabilježeni ozbiljniji gubici.

Slika 5.1. Izlazak novog, atraktivnog iPhone-a 3G

Operacijski sustav Android trebao bi ubrzati proces izlaska novih mobilnih uređaja i pojednostavniti izlazak novih programa namijenjenih tržištu mobilnih telefona. Otvorenost ovog novog sustava trebala bi biti njegova glavna prednost u odnosu na konkurente (npr. Symbian OS). Android dolazi sa paketom svih osnovnih funkcija i programa, a budući je zasnovan na modifikaciji Linux operacijskog sustava, trebao bi biti dovoljno otvoren za sve zainteresirane proizvođače programa (pogotovo uzevši u obzir da već na početku postoji prilično velika zajednica koja radi na njegovu razvoju). Na tržištu je protekle godine bio samo jedan mobilni uređaj koji je pokretan operacijskim sustavom Google Android - T-Mobile G1. Iako je fokus javnosti prilikom izlaska bio uglavnom na kozmetičkim razlikama novog operacijskog sustava u usporedbi sa sustavom koji pokreće iPhone, vrlo brzo je otkriven sigurnosni propust u Android-ovom web pregledniku. Kako Android nema striktnu sigurnosnu politiku prema nepoznatim programima, poput drugih operacijskih sustava za mobilne telefone (Symbian OS), zlonamjerni program može relativno lako i brzo proširiti.

Prema mišljenju stručnjaka, pisci prvih zlonamjernih programa za mobilne uređaje biti će uglavnom entuzijasti koji žele dospjeti na naslovnice, a ne isključivo financijski motivirane osobe. Međutim, kako popularnost ovih uređaja raste, kriminalci koje zanima (samo) financijska dobit također će postati vrlo zainteresirani za iskorištavanje ranjivosti ovih uređaje za širenje svojih zlonamjernih aktivnosti.

6. Curenje podataka

Baš kao i prethodnih godina, tvrtke i vlade još jednom su se pokazale manjkavima u zaštiti svojih povjerljivih podataka. Tako se curenje podataka (eng. data leakage) još jednom pokazalo kao kritični sigurnosni problem koji je i u 2008. godini punio novinske stupce. Moderan način poslovanja zahtijeva dostupnost velikog broja povjerljivih informacija unutar i izvan ureda, zajedno sa mogućnošću dijeljenja podataka među suradnicima i partnerima. Prema istraživanju "Utimaco Removable Media Survey" organizacije iz 2007. godine, čak 30% povjerljivih financijskih informacija, te informacija o kupcima čuvaju se na prijenosnim memorijskim uređajima (npr. USB memorijama). Ovaj podatak samo je jedan od pokazatelja koliko je situacija zabrinjavajuća i jedan od uzroka brojnih sigurnosnih incidenata koji su se dogodili u 2008.

Jedan od bizarnijih primjera curenja povjerljivih podataka je prodaja tvrdog diska sa podacima o korisnicima banaka NatWest i Royal Bank of Scotland, te kartične kuće American Express na Internetskom portalu E-Bay. Sporni tvrdi disk prodao je neoprezni zaposlenik tvrtke „Graphic Data“ koja je digitalizira povjerljive podatke nekih od najvećih britanskih financijskih institucija. Podaci, srećom, nisu završili u rukama kriminalaca, no i ovaj slučaj važno je upozorenje svim tvrtkama koje barataju sa tajnim i osjetljivim podacima.

Slika 6.1. Mnogi tajni podaci prodaju se na internetskim portalima poput E-Bay-a

Prema istraživanju "Chronology of Data Breaches" tvrtke Privacy Rights Clearinghouse od siječnja 2005. godine više od 230 milijuna povjerljivih zapisa bilo je kompromitirano u sigurnosnim incidentima vezanim uz curenje podataka. Da je situacija kritična pokazuje i podatak instituta Ponemon koja kaže da se na velikim, te aerodromima srednje veličine godišnje izgubi čak 600 000 prijenosnih računala od kojih se za polovicu

nikada ne javi vlasnik. Srećom, maleni dio ovako izgubljenih podataka završi u rukama kriminalaca. Međutim, posljedice takvog scenarija mogle bi biti katastrofalne za poslovanje tvrtke.

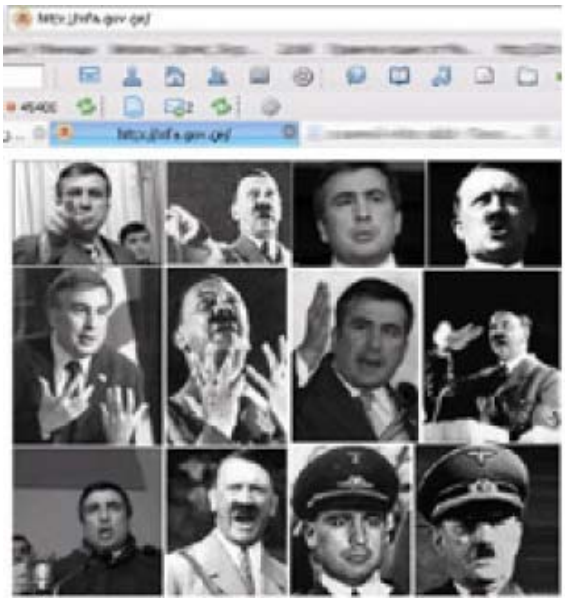
Stručnjaci iz Sophos-a predlažu dvije ključne sigurnosne mjere u zaštiti osjetljivih podataka. Prva mjera je enkripcija svih važnih i povjerljivih informacija koji se nalaze na prijenosnim računalima, te u porukama elektroničke pošte. Ukoliko su podaci kriptirani, oni su zaštićeni od krađe i otkrivanja čak i u slučaju kada svi drugi sigurnosni mehanizmi zakažu. Druga mjera je edukacija korisnika, odnosno zaposlenika tvrtki, oko korištenja povjerljivih informacija, kao bi ih oni pravilno tretirali. Treba naglasiti rizike i moguće posljedice riskantnog ponašanja, poput prijenosa nezaštićenih podataka na prijenosnim memorijama, te minimizirati mogućnost takvih sigurnosnih incidenata.

7. Međudržavni cyber kriminal

Države se međusobno špijuniraju zbog političkih, ekonomskih i vojnih razloga i bilo bi naivno za misliti da se između ostalih tehnika i računalna špijunaža ne koristi u tu svrhu. Još tijekom 2007. godine postalo je uobičajeno da se države međusobno optužuju za špijuniranje putem Interneta.

2008. godina je donijela još više izvještaja i potvrda o međudržavnom računalnom kriminalu. Iako je iznimno teško dokazati da je iza nekog računalnog kriminala (eng. cybercrime) država, bilo je nekoliko sigurnosnih incidenata od kojih možemo izdvojiti sljedeće:

- U travnju 2008. časopis Der Spiegel je napisao da je BND, Njemačka tajna služba, koristila špijunažu kako bi motrila industriju u Afganistanu. Povjerljivi dokumenti, lozinke i e-mail poruke redovno su kompromitirane od strane njemačkih špijuna.
- U svibnju 2008. Indijska vlada je potvrdila kako su kineski hakeri ciljano napadali njihova ministarstva i Indijski nacionalni informatički centar. Indijski nacionalni informatiči centar ima glavnu ulogu u davanju Internetskih usluga vladi i ministarstvima u Indiji.
- U svibnju 2008. i Belgija optužuje kineske hakere za međudržavnu *cyber* špijunažu. Belgijanci su tvrdili da iza svega stoji kineska vlada i da to nije prvi slučaj.
- Tijekom kolovoza 2008. godine, kako su rasle tenzije između Rusije i Južne Osetije u stvarnom svijetu, borba se nastavila i u cyber prostoru među ruskim i gruzijskim hakerima. Radilo se o nekoliko distribuiranih DoS (eng. Denial of Service) napada na web stranicu vlade Južne Osetije te kompromitiranja web stranice gruzijskog Ministarstva vanjskih poslova.
- U rujnu 2008. Seoul je optužio Sjevernu Koreju za krađu tajnih dokumenata od vojnih dužnosnika putem spyware programa. Napad je izvršen porukama elektroničke pošte sa zloćudnim privitkom posebno dizajniranim za krađu podataka sa zaraženog računala.



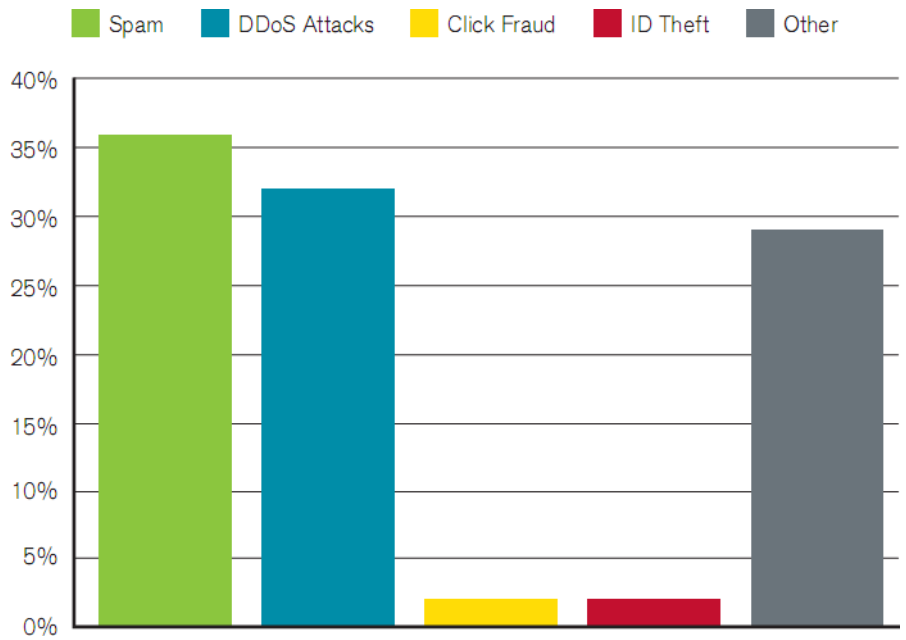
Slika 7.1. "Defacement" web stranice gruzijskog Ministarstva vanjskih poslova

Iako su rijetki slučajevi međudržavne računalne špijunaže službeno potvrđeni, i novinari u ovakvim slučajevima često barataju više indicijama nego provjerenim informacijama, nema sumnje da se oni događaju. Sophos-ovi stručnjaci predviđaju da će u 2009. godini biti još i više ovakvih slučajeva, iako će javnost saznati samo za mali dio njih.

8. Botnet mreže

Botnet mreže su odgovorne za najveći broj današnjih sigurnosnih prijetnji i računalnih kriminalnih aktivnosti. Kriminalci koriste botnet mreže za širenje svojih zloćudnih programa, krađu identiteta, kao i za izvođenje spam i DDoS (eng. Distributed Denial of Service) napada. Botnet mreža se sastoji od tisuća računala zaraženih zlonamjernim programima, a da njihov vlasnik toga nije ni svjestan. Računalima najčešće upravlja napadač s neke udaljene adrese. Procjenjuje se da je u 2008. godini čak 10% svih računala koja se spajaju na Internet, što zapravo znači na desetke milijuna računala, bilo dio botnet mreže. Još 2007. godine provedeno je istraživanje koje je pokazalo da se upravo tijekom 2008. godine očekuje daljnji razvoj i progresivni rast botnet mreža. Nažalost, crne slutnje su se i ostvarile.

Pojava botneta kao sigurnosne prijetnje nije ništa novo, ali njihovo je djelovanje u 2008. godini bilo usmjereno prvenstveno na krađu osjetljivih podataka, zatim za slanje spam poruka te izvođenje DDoS napada. Značajan porast doživjela je njihova primjena za krađu informacija, bilo kao oblik financijske prijevare ili gospodarske špijunaže. Zlonamjerni napadači za širenje svoje mreže zombija (računala u botnet mreži) najčešće koriste P2P (eng Peer To Peer) mreže, kako bi se izbjeglo njihovo prepoznavanje putem sustava za detekciju i sprečavanje neovlaštenih radnji (eng. Intrusion Detection and Prevention System). U trenutku kad je botnet otkrven i kad mu se zna središnje mjesto upravljanja (poslužitelj), IDS/IPS uređaji lako mogu blokirati vezu sa poslužiteljem.

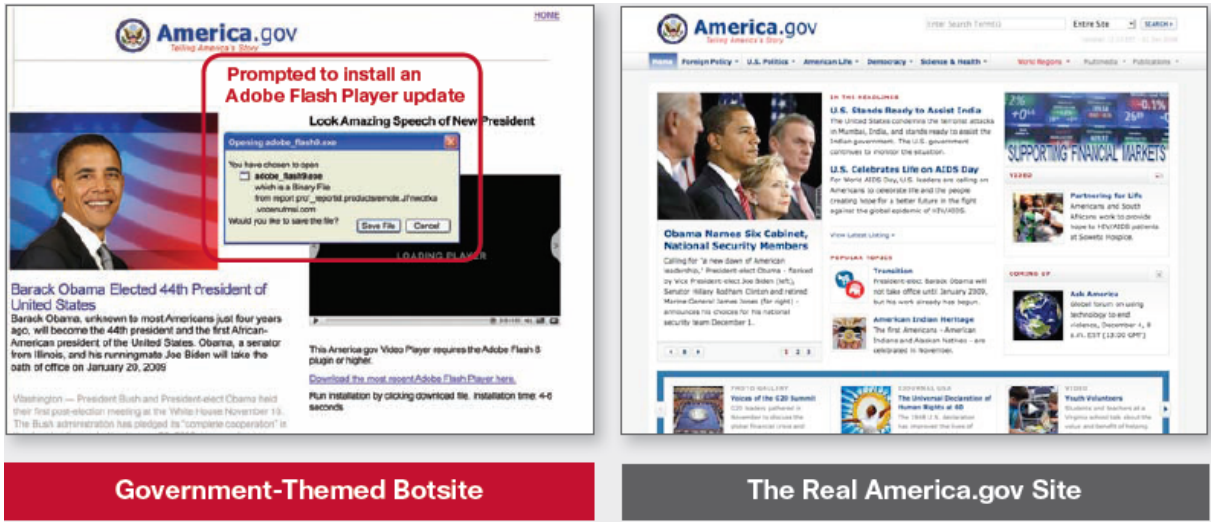


Slika 8.1. Zastupnjenost pojedinih radnji botnet mreže (prema Cisco 2008 Annual report)

Kao što se vidi na slici 8.1., usprkos povećanju broja slučajeva u kojima se botnet mreže koriste za prijevare i krađe identiteta, njihova glavna zadaća i dalje se slanje neželjenih poruka elektroničke pošte (spam) te izvođenje distribuiranih DoS napada.

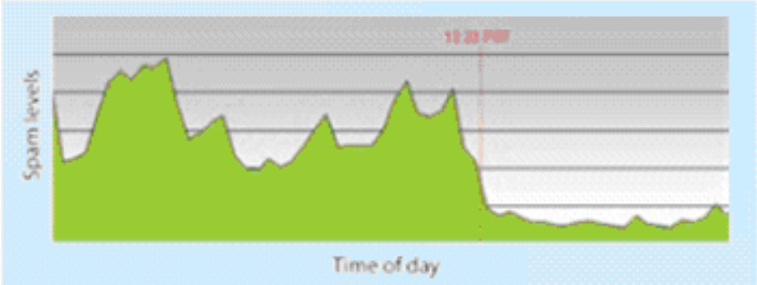
Jedan od najučinkovitijih botnet-a u 2008. godini pojavio se svibnju. Bio je to *Asprox*, već odavno poznati trojanski konj, promijenjen i pretvoren u izrazito sofisticiran botnet koji je korišten u tisućama napada umetanjem SQL koda na legitimne stranice. Zloćudni alat ne izgleda opasno korisnicima zaraženih računala jer se pokreće kao Microsoft Security Center ekstenzija (msscntr32.exe). U međuvremenu, u pozadini, koristi Google kako bi pretraživao Internet u potrazi za ASP (eng. Active Server Pages) stranicama, koje bi mogle biti osjetljive na napad umetanje SQL koda. Kada je ranjiva stranica pronađena i kompromitirana, program umeće u sadržaj stranice zloćudnu iFrame oznaku. iFrame oznaka (eng. tag) je dio jezika XHTML, koji se koristi za izradu web sadržaja. iFrame tiho i neprimjetno preusmjerava korisnika na zloćudnu stranicu koja koristi

različite metode napada na korisnikovo računalo te ga istodobno dodaje u Asprox botnet. Kako bi ga bilo što teže otkriti, Asprox komunicira putem proxy poslužitelja na TCP portovima 80 i 82. Prema procjenama stručnjaka dnevno je zaraženo čak 31 000 web stranica kada je Asprox bio na svojem vrhuncu.



Slika 8.2. Web stranica američke vlade zaražena Asproxom i izvorna web stranica

Još jedan važan događaj obilježio je 2008. godinu. Riječ je o padu poznate ruske botnet mreže McColo. Radi se o mreži za koji se vjeruje da upravlja i nadzire centre za pet najvećih svjetskih botnet-ova : Srizbi (Zlob), Mega-D, Rustock, Dedler i Storm. 11.11.2008. godine u 13 sati i 23 minute naglo je prekinuta veza između McColo mreže i Interneta. U tom je trenutku zabilježen drastičan pad količine spama, za čak 75%. Takav pad još nije zabilježen u povijesti borbe protiv računalnog kriminala. Mnogi zlonamjerni korisnici, od tog događaja, pokušavaju vratiti nadzor nad srušenim botnetovima, ali ne sa stopostotnim uspjehom.



Slika 8.3. Nagli pad razine spama nakon isključenja McColo mreže

Ovaj slučaj pokazao je da, ako radi zajedno, sigurnosna zajednica može negativno utjecati na računalni kriminal na globalnoj razini. Uistinu, pad McColo mreže imao je veći negativan učinak na količinu spama na globalnoj razini nego uhićenje bilo kojeg autora spam poruka do sada.

Jedini način na koji korisnik može smanjiti rizik da i njegovo računalo ne postane dio botnet mreže jest korištenje kvalitetnog antivirusnog programa (s uključenim posljednjim definicijama virusa) i vatrozida, zatim redovita nadogradnja sigurnosnih zakrpi za operacijski sustav, ali i za sve instalirane programe koji se koriste na računalu. Upravo izostanak ovih sigurnosnih mjera razlog je zašto stručnjaci predviđaju da će botnet mreže i u budućnosti biti jedna od najvećih prijetnji sigurnosni računalnih sustava i mreža.

9. Zaključak

Predviđanje budućnosti u industrijskoj grani kao što je računalna tehnologija gotovo je nemoguć zadatak. Samo kratki pogled u prošlost otkriva koliko je situacija postala ozbiljna. Računalni kriminal toliko je uznapredovao da je važnost implementacije najosnovnijih sigurnosnih mjera veća nego ikada. 2008. godinu obilježilo je značajno povećanje sigurnosnih prijetnji na webu, te iskorištavanje ranjivosti novih tehnologija (web 2.0, mobilni telefoni nove generacije…). Iako je poprilično nezahvalno detaljnije predviđati razvoj događaja na sceni računalnog kriminala stručnjaci se slažu oko slijedećih par crtica:

- Raznolikost napada i njihova učestalost nastaviti će svoj rast eksponencijalnom brzinom, vođeni željom napadača za provaljivanje u tuđe računalne sustave zbog krađe identiteta, resursa ili osjetljivih informacija.
- Curenje podataka postati će sve veći problem, prvenstveno zbog sve većeg korištenja mobilnih tehnologija u poslovnim okruženjima. Mnoge države rade na zakonima koji bi spriječili tvrtke u sakrivanju sigurnosnih incidenata.
- Kompromitirana osobna računala i dalje će, kao dio botnet mreža, biti glavni izvor spam poruka elektroničke pošte. Botnet mreže novim načinom komuniciranja, putem P2P mreža, vješto izbjegavaju otkrivanje.
- Zlonamjerne poruke će u budućnosti sadržavati sve više raširenih vrsta dokumenata poput PDF i DOC datoteka za koje napadači svakodnevno pronalaze nove ranjivosti.

Trendovi pokazuju kako današnji računalni kriminalci više ne mare za slavom, već isključivo žele financijsku dobit. Kako Internet postaje svakodnevnica i u životu običnih ljudi, a ne samo računalnih stručnjaka, očekuje se da će i napadači i dalje svoje aktivnosti usmjeriti najviše na "mrežu svih mreža" - Internet. Kako bi se sigurnosni incidenti smanjili na najmanju moguću razinu važno je konstantno educirati korisnike računala kako bi koristili što više sigurnosnih mjera i time učinili svoje računalo, ali i računala drugih korisnika, sigurnijima. Upravno ljudski faktor je uzrok mnogim sigurnosnim incidentima, no naša sposobnost da učimo i mijenjamo svoje ponašanje predstavlja područje s najvećim mogućnostima za razvoj i napredak globalne računalne sigurnosti.

10. Reference

[1] Sophos : Security Threat Report 2009 : Preapare for this year's new threats

[2] Georgia Tech Information Security Center : Emerging Cyber Threats Report for 2008 : Leading technology experts share thoughts on top emerging Internet threats for 2008

[3] Cisco : Annual Security Report for 2008

[4] Arbor Networks : Worldwide Infrastructure Security Report, October 2008, Volume IV

[5] Sophos : Security Threat Report 2008

[6] Sophos discovers serious threat for vloggers on Adobe website, http://www.sophos.com/pressoffice/news/articles/2008/10/adobe-infection.html

[7] Anti-virus company Trend Micro: Our website has been hacked, risk of Trojan horse infection, http://www.sophos.com/security/blog/2008/03/1186.html

[8] Euro 2008 football ticket website hacked by cybercriminals to infect unwary fans, http://www.sophos.com/pressoffice/news/articles/2008/03/euro2008.html

[9] Visitors to Sony PlayStation website at risk of malware infection, http://www.sophos.com/pressoffice/news/articles/2008/07/playstation.html

[10] Hackers infect BusinessWeek website via SQL Injection attack, http://www.sophos.com/blogs/gc/g/2008/09/15/hackers-infect-businessweek-website-via-sql-injection-attack/