NAPADI NA RAČUNARSKE SISTEME

Vuletić V. *Dejan*, Ministarstvo odbrane Republike Srbije,
Institut za strategijska istraživanja, Beograd

OBLAST: IT – informacione tehnologije
VRSTA ČLANKA: stručni članak

Sažetak:

Računarski sistemi su kritični segment ljudskog društva u 21. veku. Ekonomski sektor, odbrana, bezbednost, energetika, telekomunikacije, industrijska proizvodnja, finansije i druge vitalne infrastrukture zavise od računarskih sistema koje rade u lokalnim, nacionalnim ili globalnim razmerama. Poseban problem jeste što se zbog ubrzanog razvoja informaciono-komunikacione tehnologije i nezaustavljivog rasta njene primene u svim sferama ljudskog društva uvećava njegova ranjivost i izloženost vrlo ozbiljnim potencijalnim opasnostima.

U radu su analizirani određeni, karakteristični, napadi na računarske sisteme.

Ključne reč: *računarski sistem, računarski napad.*

Uvod

Društvena zavisnost od računarskih sistema uvećava posledice napada, nezgoda i padova računarskih sistema.

Pod **računarskim sistemom** podrazumeva se „svaki uređaj ili grupa međusobno povezanih uređaja kojima se vrši automatska obrada podataka (ili bilo kojih drugih funkcija)“ [1].

Napad je pretnja koja je izvršena i, ako je uspešan, dovodi do kompromitovanja računarskog sistema odnosno narušavanja bezbednosti. Svaki sistem ima ranjivosti. Kompleksniji sistem podrazumeva i potencijalno veći broj ranjivosti i propusta. Napad u suštini predstavlja eksploatisanje tih ranjivosti, a sastoji se od serije namernih koraka koje preduzima napadač da bi se postigao određeni cilj.

Nezgode predstavljaju širok spektar slučajno iskrslih i potencijalno štetnih događaja, kao što su npr. prirodne nepogode.

Padovi sistema su mogući štetni događaji prouzrokovani manjkavostima u sistemu ili u spoljnim elementima od kojih sistem zavisi. Padovi sistema prouzrokovani su greškama u izradi softvera, zastarevanju hardvera, ljudskim greškama i drugo.

dejan.vuletic@mod.gov.rs

Vuletić, D., Napadi na računarske sisteme, pp. 235–249

Napadi na računarske sisteme mogu se klasifikovati prema više kriterijuma. Prema poreklu napada, razlikuju se [2]:

1. unutrašnji napad – realizovan od strane napadača unutar sistema, insajdera, koji imaju mogućnost da pristupe resursima, ali ih koriste na način za koji nije ovlašćen,

2. spoljašnji napad – realizovan od strane napadača van sistema.

Prema posledicama po sistemske resurse, napad može biti [2]:

1. aktivni napad – pokušaj da se promene sistemski resursi ili utiče na njihove operacije (npr. DoS napad),

2. pasivni napad – pokušaj da se neovlašćeno pristupi informacijama u sistemu, ali bez uticaja na sistemske resurse (prisluškivanje odnosno nadgledanje prenosa podataka, npr. Sniffing).

Karakteristični napadi na računarske sisteme

Imajući u vidu navedene, i druge, kriterijume klasifikacije napada na računarske sisteme, u praksi je čest slučaj da neželjeni događaji sa aspekta bezbednosti u računarskim sistemima predstavljaju kombinaciju različitih vrsta napada. Radi boljeg sagledavanja ugroženosti računarskih sistema, biće predstavljeni samo određeni, karakteristični, napadi (pretnje): *DoS (DDoS), Phishing, Botnet, SPAM, Social Engineering, Sniffing, Spoofing i Malware*.

Napad uskraćivanjem usluga

Napad uskraćivanjem usluga (*Denial-of-Service – DoS*) je tip napada koji pokušava da spreči legitimne korisnike da pristupe mrežnim uslugama. To se ostvaruje preopterećenjem mrežnih servisa ili prekomernom konekcijom, što uzrokuje pad konekcije ili servisa. Infrastruktura međusobno spojenih sistema i mreža sastoji se od ograničenih resursa. *DoS* alati su namenjeni da pošalju veliki broj zahteva ciljanom serveru (obično *web*, *FTP*, *e-mail server*), s ciljem da preplavi resurse servera i učini ga neupotrebljivim. Napad uskraćivanjem usluga je organizovan tako da ometa ili potpuno obustavlja normalno funkcionisanje *web* sajta, servera ili drugih mrežnih resursa. Postoje različiti načini kojima napadači to postižu. Jedan od uobičajenih načina je jednostavno preplavljivanje servera slanjem prevelikog broja zahteva. To će onemogućiti normalno funkcionisanje servera (i *web* strane će se otvarati mnogo sporije), a u nekim slučajevima može dovesti i do potpunog obaranja servera (prouzrokujući tako pad svih *web* sajtova na serveru).

Svaki sistem koji je spojen na internet i koji je opremljen mrežnim uslugama baziranim na *TCP* (*engl. Transmission Control Protocol*) protokolu potencijalna je žrtva napada. U napadima s jednim izvorom postoji jedan napadač koji poplavljuje žrtvu, dok u napadima s više izvora postoji više napada-

ča. U oba slučaja mogu se koristiti dodatni *zombie* računari. Zombie je računar koji je zaražen pomoću iskorišćavanja neke ranjivosti. Takav računar sadrži skriveni program koji omogućava upravljanje računarom iz daljine. Najčešće se koriste za izvođenje napada na neki drugi računar.

Najraniji oblik *DoS* napada bio je *SYN flood*, koji se pojavio 1996. godine i eksploatiše slabosti u *TCP*. Ostali napadi eksploatišu slabosti u operativnim sistemima i aplikacijama što dovodi do nedostupnosti mrežnih usluga ili čak do pada servera. Mnogi su alati razvijeni i postali su slobodno dostupni na internetu za izvršavanje takvih napada (*Bonk, LAND, Smurf, Snork, WinNuke, Teardrop*). *TCP* napadi su još uvek najpopularniji oblik *DoS* napada. Razlog je što ostali tipovi napada, kao što je upotreba (potrošnja) celokupnog prostora na disku, modifikovanje tabele rutiranja na ruteru i slično, prvo zahtevaju upad u mrežu, što može predstavljati problem za potencijalnog napadača ako je sistem dobro zaštićen [3].

Postoje tri osnovna načina izvršavanja *DoS* napada [4]:

1. potrošnja svih resursa, kao što je propusni opseg što onemogućava legitimni saobraćaj (*SYN flooding attacks* – veliki broj zahteva da se otvori *TCP* konekcija, tj. veliki broj otvorenih konekcija, *smurf* napadi[1] – veliki broj paketa usmerenih ka mreži);
2. uništenje ili oštećenje konfiguracionih informacija (npr. rutera);
3. fizičko oštećenje komponenti mreže da bi se sprečio pristup uslugama (računara, rutera, stanica za napajanje električnom energijom).

Distributed Denial of Service (DDoS) je tip *DoS* napada koji se služi snagom (moći) višestrukih posrednih korisnika. Klasični *DoS* napadi su jedan-na-jedan napadi u kojima moćan host generiše saobraćaj koji „zatrpava“ konekciju ciljanog hosta, što ometa ovlašćene klijente da pristupaju mrežnim uslugama. *DDoS* napadi su otišli korak dalje što se višestruko pojačava, što ima za posledicu da serveri ili delovi mreže mogu biti potpuno neupotrebljivi za klijente. Prvi put su se pojavili 1999. godine, a masovniji *DDoS* napadi počeli su 2000. godine kada su oboreni popularni sajtovi kao što su *Amazon*, *CNN*, *eBay*, *Yahoo* i drugi. Najbolji način odbrane od takvih napada je promena konfiguracije rutera kod provajdera internet usluga [3].

DDoS napadi koriste veliki broj računara zaraženih crvima ili trojancima da realizuju jednovremeni napad na ciljani sistem, za veoma kratko vreme. Daljinski kontrolisani zaražen računar naziva se zombi (zombi). Računari zombiji mogu, na primer, poslati na hiljade mejlova izazivajući prekid usluga na *e-mail* serveru [4].

U Estoniji DDoS, 2007. godine, bio je najveći napad ikada viđen. U tom napadu bilo je uključeno više različitih bot mreža, svaka sa desetinama hiljada zaraženih mašina [5]. Često se u informatičkim krugovima događaji u Estoniji nazivaju prvi rat na mreži (*Web War One – WWI*).

[1] Štrumf (smurf) napadi se realizuju tako što napadač šalje ogroman broj ICMP echo-request (ping) svim adresama u mreži, pri čemu se adresa ciljanog računara navodi kao izvorna adresa. Pingovane mašine šalju njihove odgovore ka računaru žrtvi, tj. ciljanom sistemu, što može preplaviti ciljani sistem.

Ako napadač izvodi *smurf*[2] napad sa jednog izvora, takav napad biće prepoznat kao *DoS* napad. Ako napadač koristi hiljade *zombie* sistema da istovremeno izvedu *smurf* napad, napad će biti prepoznat kao *DDoS* napad.

DoS i *DDoS* je veoma teško identifikovati i sprečiti. Simptomi *DoS* napada mogu biti: usporavanje mrežnih performansi, nemogućnost pristupanja određenim *web* sajtovima, veliko povećanje primljenih spemova itd.

Zaštita od *DoS* napada se postiže:

1. isključivanjem (disejblovanjem) nepotrebnih mrežnih usluga;
2. ograničavanjem tj. normiranjem korišćenja diska za sve korisnike kao i za mrežne usluge;
3. obezbeđivanjem filtriranja na ruterima i zakrpama (*patch*) operativnih sistema da bi se smanjila izloženost *SYN* napadima;
4. definisanjem tj. određivanjem šta je normalna upotreba (opterećenost) mreže da bi se lakše identifikovalo i suprotstavilo napadu;
5. redovnim bekapovanjem informacija o konfiguraciji sistema i obezbeđivanjem stroge politike zaštite po pitanju lozinki.

Fišing

Fišing (*phishing*) je vrsta napada na internetu kada se napadači koriste postojećim internet servisima da namame i prevare korisnike da otkriju osetljive informacije (korisnička imena, lozinke, podatke sa kreditnih kartica…) koje mogu biti iskorišćene u kriminalne svrhe.

Napadači (fišeri) obično izvršavaju fišing napade koristeći falsifikovane e-mejlove tako da izgleda da ih šalje određena institucija sa kojom žrtva ima kontakt (npr. banka, osiguravajuća kuća i slično). Fišeri obično izvode fišing napad tako što pošalju mejl korisniku banke (ili druge institucije) u kome se navodi da će mu račun biti ukinut ukoliko ne ažurira lične informacije. U mejlu je dat i link ka lažnom sajtu, odnosno vernoj kopiji stvarnog sajta određene institucije. Na taj način potencijalna žrtva je namamljena na lažni *web* sajt gde će biti navedena da ukuca broj svog računa i lozinku koji se kasnije mogu zloupotrebljavati, pre svega iz finansijskih motiva [4].

Pored elektronske pošte, fišeri koriste i druge servise na internetu kao što su *Windows Messenger*, *ICQ*, *Skype*, *Google Talk*, društvene mreže (*Facebook, Twitter, MySpace*) i dr.

[2] *DoS* napad koji eksploatiše *Internet Control Message Protocol – ICMP*. Bazira se na spufingu *ICMP echo request* paketa (koristi za tzv. pingovanje prilikom rešavanja problema). Napadač falsifikuje *ICMP echo request* pakete sa izvornom *IP* adresom koja je identična *IP* adresi žrtve. Ti paketi se emituju na mreži gde se nalazi žrtva. Kada drugi korisnici prime takav zahtev, emituju *ICMP echo replay* pakete.

Fišing napadi oslanjaju se na socijalni inženjering i tehničke postupke. *Spem* je glavni alat da postignu veliki broj potencijalnih fišing žrtava. Fišeri koriste baze podataka (*spamer's database*) koje sadrže veliki broj e-mail adresa radi slanja mejlova koji će izgledati što je moguće više kao legitiman zahtev. Fišeri koriste i botnetove radi jednovremenog pokušaja velikog broja fišing napada [4].

Fišing pretnje predstavljaju jednu od ozbiljnijih pretnji na internetu. Cilj napada je [4]:

1. da se dođe do osetljivih, ličnih, informacija koje se mogu zloupotrebiti pre svega iz finansijskih motiva;
2. da se instalira maliciozni program (*malware)* i proširi mreža zombija uzrokujući finansijske gubitke i ličnu štetu.

Fišing napadi se mogu podeliti na nekoliko kategorija [4]:

1. *Deceptive attacks* – oslanja sa na obmanjujuće poruke. To je najčešći fišing napad. Koristeći propuste u *SMTP*, pošiljalac vrši *spoofing* izvorne *e-mail* adrese. Od primaoca će se uvek zahtevati da klikne na link i reši problem brzo i sigurno. Napadač koristi razne tehnike da bi poruka izgledala kao da je od originalnog pošiljaoca.
2. *Malware attacks*. Bazira na socijalnom inženjeringu. Korisnik se ubeđuje da otvori atačment u mejlu ili da preuzme interesantan softver koji sadrži maliciozni program. Ovaj napad oslanja se i na tehničke ranjivosti koje omogućavaju malicioznom programu da se širi u mreži.
3. *DNS-based attacks* – preusmeravanje na lažni server koji sadrži maliciozni sadržaj. *Malware* obično sadrži trojanca, *keyloggers*, *screenloggers* i dr. Maliciozni program se koristi da instalira *Browser Helper Object* koji kontroliše *Internet Explorer web* pretraživač i usmerava *HTTP* saobraćaj ka nelegitimnim sajtovima. Napredniji *DNS-based attack* naziva se *pharming***.** Predstavlja *DNS spoofing* metod koji kompromituje proces pretraživanja imena domena.
4. *Content-injection attacks* predstavlja ubacivanje koda u legitimni sajt. Napadač može koristiti maliciozni sadržaj ili da preusmeri žrtvu na drugi *web* sajt ili da instalira maliciozni program na računar žrtve. Napadači obično ubacuju maliciozni sadržaj na legitimni sajt kroz *cross-site scripting* ranjivosti.[3] Maliciozni sadržaj postaje deo podataka na sajtu.

Zaštita of fišinga:

1. ne odgovarati na mejlove u kojima finansijske institucije traže lične podatke;
2. ne klikati na linkove koji su sadržani u mejlovima dobijenim od nepoznatih osoba;
3. često menjati i koristiti dobro zaštićene lozinke;
4. koristiti antivirusni softver, *firewall*, filter za filtriranje spemova, *antispyware* softver;

[3] *Cross-site scripting (XSS)* je ranjivost u web aplikacijama koja omogućava malicioznim napadačima da ubace kratak fragment (script) u bazu podataka koji koji im kasnije omogućava da zaobiđu mehanizme zaštite i pristupaju osetljivim sadržajima stranice.

5. lično kontaktirati, na drugi način, institucije koje od nas traže lične podatk,

6. proveriti da li stranica preko koje unosimo podatke koristi *HTTPS* protokol (finansijske institucije trebalo bi da koriste,

7. redovno praćenje računa za obavljanje novčanih transakcija;

8. edukacija korisnika o zloupotrebama na internetu.

Kao nove varijante fišing napada pojavljuju se [4]:

1. *Spear phishing* **–** ciljaniji napadi pri čemu napadač mora ukrasti ili prikupiti mnogo više informacija o žrtvi radi većeg osećanja legitimnosti;

2. *Vishing* – fišing napad koji obuhvata *Voice over IP (VoIP)*. Fišeri šalju *e-mail* koji sadrži telefonski broj dostupan preko *VoIP* tehnologije.[4] Od žrtve se traži da pozove *VoIP* broj. Kontrakt se umesto linka ostvaruje preko *VoIP*. Žrtva pozove broj, a napadač je pita za lične informacije direktno putem telefonom.

Botnet

Botovi (*engl. bots,* skraćenica od robots) su programi (obično izvršni fajlovi) koji su instalirani na računar s ciljem da automatski pokrenu set funkcija i dopuste neovlašćenim korisnicima da dobiju daljinsku kontrolu pomoću komunikacionog kanala. Ti zaraženi računari se nazivaju zombiji (*zombies*) ili botovi (*bots*), a mogu se nalaziti svuda širom sveta. Predstavljaju skrivenu armiju računara s ciljem slanja spemova, *DoS* napada, fišing napada, distribucije oglašavačkih programa (*adware*) i slično.

Botovi nikada ne deluju pojedinačno. Oni su deo velike mreže zaraženih računara koja se naziva botnet (skraćenica od *engl. bot network*). U svakom botu instalirana su „zadnja vrata *(backdoor)*"[5] da bi mogao da izvršava komande.

Botnetovi su koordinirane grupe od nekoliko (desetina, stotina ili hiljada) personalnih računara ili čak novih generacija mobilnih telefona (*smartphones*) pri čemu su svi zaraženi istim malicioznim programom. Njihova moć, daljinski kontrolisana, može se rangirati od spemova i krađe identiteta do špijunaže i napada na kritične informacione infrastrukture [6].

---

[4] Glas preko internet protokola (*Voice over Internet Protocol – VoIP*) je tehnologija koja omogućava prenos glasa i multimedijalnih sadržaja preko računarskim mreža (interneta). Često se kao sinonimi pojavljuju odrednice IP telefonija, internet telefonija i slično.

[5] Skriveni mehanizam za pristup aplikacijama, sistemu ili mreži. Obično ga ostavljaju napadači da bi mogli ponovo, skriveno, upasti u sistem i napraviti veću štetu. Ako se to desi, neophodno je izbrisati sistem i instalirati novi za koji smo sigurni da je bezbedan. Popularan alat za instaliranja backdoor u koji smo prodrli je Netcat koji može inicirati ili primiti *TCP* ili *UDP (User Datagram Protocol)* konekcija nekog porta. *Netcat* je alat za skeniranje portova i prenos informacija pomoću mrežnih konekcija. Može čitati i pisati podatke koristeći *TCP* i *UDP* s ciljem: izvršavanja prenosa fajlova, prikriveno slanje/prijem podataka od l ka kompromitovanim sistemima, testiranje mrežnih servisa i sl. To je izuzetno fleksibilan alat koji može koristiti neku lokalnu adresu i port da inicira konekciju.

Botnetovi se koriste za napade na određene zemlje i kritične informacione infrastrukture kao što je bio slučaj u maju 2007. godine u Estoniji, kada je *DDoS* napad izveden je pomoću 560 računarskih mreža iz više od 50 zemalja [6].

Najvidljivija upotreba botneta jeste emisija spemova i malicioznih programa, koji zaokupljuju veliku pažnju donosilaca odluka i provajdera internet usluga širom sveta, u pokušaju da spreče navedene štetne sadržaje, najčešće restrikcijama saobraćaja oko porta 25 (*SMTP*). To je samo vrh ledenog brega, odnosno „pokušaj lečenja kancera pluća sirupom protiv kašlja“ [6].

Internet Relay Chat (IRC)[6] ili *peer-to-peer* mreža,[7] *VoIP* omogućavaju cyber kriminalcima da centralizovano kontrolišu zombije i realizuje koordinisane i jednovremene napade. Napadači obično napadaju računare koji imaju širokopojasni pristup internetu i nizak nivo bezbednosti. Širenje infekcije obično se obavlja trojancima, mejlovima, malicioznim *web* sajtovima. Napadači koriste kontrolere bazirane na *Web*-u, kao što je protokol *HTTP*, da kontrolišu botove i *instant message controllers*. *VoIP* može postati novi komunikacioni kanal za napadače i možda najbolji način za napadače da kontrolišu zombije, obrišu tragove i prikriju napad [4].

Noviji roboti mogu automatski skenirati okruženje u kojem se nalaze i širiti se koristeći pronađene ranjivosti i slabe tačke. Najpopularnije korišćenje botneta za izvođenje *DoS* napada jeste korišćenje istih za slanje spem poruka. Slanjem enormne količine beskorisnih poruka korisnicima, korisne poruke i resursi mogu biti izgubljeni. Maliciozni programi takođe mogu biti poslati putem spema da bi stvorili početni skup zaraženih računara, koji šalju navedene maliciozne programe ostalim računarima.

Spem

Spem (*spam*) je neželjena elektronska pošta, odnosno pošta koju korisnik nije tražio niti je dao saglasnost pošiljaocu da šalje takve poruke na njegovu adresu. Najčešće su to reklamne poruke ili ponude, ali mogu biti i poruke s ciljem ubacivanja malicioznog softvera u željeni računar.

To je oblik elektronske pošte koji pokušava da sakrije *e-mail* adresu pošiljaoca s ciljem onemogućavanja njegovog praćenja ili koji se koristi obmanjivanjem prilikom ispisa u polje „predmet (*subject*)“, s namenom da natera primaoca da otvori primljenu poštu [3].

Pošiljaoci (spameri) često svoju infrastrukturu smeštaju u zemlje koje nemaju zakonski definisane kazne za slanje spem poruka. *E-mail*

[6] Mreža servera koja omogućava diskusije uživo, između ljudi u celom svetu. Najčešći način kontrolisanja botova zato što je to popularan protocol prilagođen da se pokreće na različitim mašinama i zato što omogućava kriminalcima da prikriju svoje aktivnosti u okviru legitimnog *IRC* saobraćaja.

[7] Neki botovi mogu koristiti vlastite *peer-to-peer* mreže da uspostave kriptovane komunikacije koristeći proizvoljne mrežne portove.

adrese se sakupljaju preko raznih četova, *web* stranica, *news* grupa ili malicioznim programom zaraženih računara. Najčešći način sakupljanja *e-mail* adresa je pomoću robotskih sakupljača (eng. *harvester*) – bota koji na internetu traži *e-mail* adrese. Spameri, takođe međusobno razmenjuju baze prikupljenih *e-mail* adresa. Izvor poruke može se pratiti korišćenjem određenih alata kao što su *Traceroute*, *Whois* i drugi.

Spem je delom problem slobode govora i prirode interneta kao distribuiranog sistema koji niko realno ne kontroliše i koji je razvijen brojnim odlukama do kojih se došlo konsenzusom.

Spem postaje sve ozbiljniji problem na internetu. Problem nastaje kada to postane svakodnevno i u takvim količinama da je teško razlikovati „legalnu" poštu od te neželjene, što takođe dovodi do ubrzanog popunjavanja ograničenog slobodnog prostora za legitimne poruke, tj. nemogućnosti pristizanja novih poruka. Osim za obične korisnike, velike količine spem poruka su i problem za provajdere internet usluga (*Internet Service Provider – ISP*) koji zbog njih moraju povećati svoje kapacitete.

Zaštita od spema ostvaruje se primenom softvera za filtriranje, skrivanjem svoje e-mail adrese da ne bude javno dostupna, npr. na mejling listama, edukacijom, antispem regulativom i drugim merama.

Socijalni inženjering

Socijalni inženjering (*social engineering*) je tehnika manipulacije ljudima (ubeđivanjem, obmanjivanjem, domišljatošću, lažnim predstavljanjem…) radi dobijanja poverljivih informacija ili pristupanja poverljivim sistemima.

Koristeći ljudske slabosti, na taj način zaobilaze se mehanizmi zaštite s ciljem izvršenja krađe, prevare, industrijske špijunaže, krađe identiteta, izazivanja prekida u radu sistema i drugih ciljeva.

Napadači se ne služe primarno tehnologijom (mada i ona može delimično biti uključena), već se koriste lakovernošću zaposlenih. Najčešći napadi socijalnog inženjeringa izvršavani su telefonom. Posebno su ranjiva lica (slabo edukovana) koja su zadužena da pružaju pomoć (*help desk*). Kopanje po smeću (*dumpster diving*) može pružiti značajne informacije. Do podataka se često dolazi domišljatošću a mozaik se sklapa postepeno, deo po deo.

Napadači se obično fokusiraju na veće entitete kao što su: sistem odbrane, finansijske institucije, velike kompanije, telefonske kompanije, bolnice, vladine agencije. Na svaki način pokušavaju dobiti na legitimnosti i uverljivosti, stvarajući povoljno psihološko okruženje za delovanje. Na primer, lažnim predstavljanjem kao *IT* podrška ili administrator od korisnika se može zatražiti lozinka direktnim pozivom ili slanjem elektronske pošte.

Osnovna zaštita od socijalnog inženjeringa, kao pretnje na internetu, leži u edukaciji zaposlenih i dobroj politici zaštite informacija i sistema.

Snifing

Njuškala (*sniffers*) su uređaji, hardver ili softver, koji mogu nadgledati pakete u računarskoj mreži odnosno nadgledati mrežni saobraćaj, i zakonito ili nezakonito prikupljati podatke koji se prenose. Njuškala mogu čitati sve aktivnosti koje se pojavljuju između protokola mrežnog sloja. Njuškala se generalno koriste da izoluju probleme na mreži. Mada su nevidljivi za krajnjeg korisnika, degradiraju mrežne performanse.

Alati se često nazivaju „analizatori protokola“. Njuškanje (*sniffing)* se lako realizuje na tzv. segmentiranoj, podeljenoj, mreži (*shared network)* gde su segmenti mreže povezani habovima. Ako neko ima fizički pristup mreži, može prikačiti *protocol analyzer* na mrežu i „uhvatiti“ sve što se dešava na određenom segmentu mreže [3].

Ruter u mreži čita svaki paket podataka koji prolazi preko njega, određujući da li je namenjen destinaciji u okviru ruterove vlastite mreže ili treba da bude prosleđen nekom drugom ruteru na internetu. Međutim, ruter sa sniferom može da čita podatke u okviru paketa kao i izvorišnu i destinacionu adresu.

Njuškala se dosta razlikuju po funkcionalnosti i dizajnu. Neki analiziraju samo jedan protokol dok drugi mogu više njih. Poznatiji sniferi su *Ethereal*, *tcpdump* i drugi.

Njuškala mogu uhvatiti veliki broj korisničkih imena i lozinki, poverljivih i privatnih informacija. Pošto se u mreži obavlja saobraćaj, tj. protiče ogromna količina paketa, sniferi će njuškati samo prvih 200–300 bajtova svakog paketa u kojima je i sadržano korisničko ime i lozinka. Informacije koje su poslate portu 23 (*Telnet*), 80 (*HTTP*) i 21 (*FTP*) naročito su korisne za napadača [7].

Sniferi su pasivni programi koji se teško otkrivaju, naročito na velikoj mreži (postoje specijalizovani alati). Postoje dve glavne odbrane protiv njuškala [7]:

1. sigurna topologija (podeliti mrežu tj. napraviti čvršće mrežne segmente korišćenjem svičeva, rutera i bridževa; periodično proveravati svaki segment kao i *MD5* provere periodično po segmentima);
2. jaka enkripcija (kriptovati podatke a enkripcija mora biti dovoljno jaka; problem je što sve aplikacije nemaju integrisanu podršku za enkripciju; problem je i što se korisnici odupiru korišćenju enkripcije, tj. inicijalno se slažu ali ih se retko pridržavaju; postoje aplikacije koje podržavaju jaku, dvostruku enkripciju kao što je *Secure Shell*).

Spufing

Spufing (*spoofing*) je obmana, tj. prevara kojom se stvara utisak da prenos vrši ovlašćeni korisnik. To je prefinjena tehnika provere autentičnosti jedne mašine prema drugoj, falsifikovanjem paketa iz adrese izvora kojoj se veruje. Autentičnost koja se javlja u trenutku konekcije potpuno se bazira na *IP* adresi izvora. *IP* adrese (i mnoga polja *IP* zaglavlja) mogu se falsifikovati. Ovo je najlakši mehanizam zloupotrebe *IP* rutiranja izvora [7].

IP spufing je jedan od oblika spufinga i tada se falsifikuje izvorna adresa *IP* paketa. Postoje i druge tehnike (*ARP, DNS i TCP spoofing*) [7]. *Address Resolution Protocol (ARP) spoofing* – falsifikovanje *Media Access Control (MAC)* adrese *Ethernet* frejmova. *Domain Name System (DNS) spoofing* – falsifikovanjem podataka u DNS paketima.

TCP spoofing napad bazira se na činjenici da *TCP* protokoli uspostavljaju logičku konekciju između dva krajnja korisnika radi podrške razmene podataka. Logički identifikatori (brojevi portova) koriste se da se uspostavi *TCP* konekcija. Neki brojevi portova su fiksirani i dobro poznati, tj. rezervisani za određene programe. Drugi se dodeljuju dinamički, tokom konekcije, po određenom algoritmu. *TCP port number attack* obuhvata pretpostavku ili predviđanje sledećih brojeva portova koji će biti dodeljeni za razmenu podataka radi upotrebe tih brojeva umesto legitimnih korisnika. To im omogućava da prođu kroz *firewalls* i uspostave sigurnu konekciju između dva entiteta, napadača i cilja. Za to vreme, legitimni korisnik je blokiran, ali je to dovoljno vremena za napadača da pošalje žrtvi poruku da je zahtevani sistem neaktivan. Da bi se ova vrsta napada sprečila, *firewall* mora biti pravilno konfigurisan tako da onemogućava prolazak *IP* paketa koji sadrže dolazeću *IP* adresu na spoljni komunikacioni port. Procedure autentifikacije *firewall*-a ne treba da se baziraju samo na *IP* adresi, već i na dodatnim funkcijama enkripcije [4].

Ruteri su jedno od rešenja za spufing problem, tj. mogu zaštititi dolazeće pakete koji imaju potvrdu da su nastali unutar mreže. Pažljivo nadgledanje mreže takođe je preventivna mera. Rešenje je, dakle, u filtriranju na ruteru (kroz kontrolne liste pristupa – *Access Control List ACL*), enkripciji i autentifikaciji (obe funkcije biće zadovoljene u *IPv6*).

Maliciozni (zlоćudni) programi

Sa razvojem interneta i različitih servisa javljaju se brojni maliciozni programi (*malware* – *malicious software*) koji se brzo i lako šire mrežom (internetom) zbog ranjivosti sistema, sistemskih grešaka, neopreznosti korisnika i drugih razloga. Maliciozni programi predstavljaju softvere koji nanose štetu ciljanom, zaraženom, računarskom sistemu. Razlikuju se po malicioznoj aktivnosti koju čine, kako se umnožavaju, kako se izvršavaju.

O ozbiljnosti problema dovoljno govori i činjenica je 2009. godine prosečno na svake 2,2 sekunde dolazilo do pojave (ulaska) malicioznog programa u cyber prostor. Tri ili četiri kompanije koje se bave antivirusnim softverima imale su sofisticirane mreže da nadgledaju nove maliciozne programe, ali su one našle i rešile jedan od deset malicioznih programa. Rešenje podrazumeva deo softvera napravljen da blokira maliciozni program. Nekada su potrebni dani pa i nedelje da bi se problem rešio. Do pronalaska rešenja, kompanije, vladini organi i obični korisnici potpuno su ranjivi na nove maliciozne programe [5].

Krajem 2010. godine, specijalno napravljen maliciozni program *Stuxnet* zarazio je „Simensove“ SCADA uređaje koji kontrolišu naftovode, električna, nuklearna i druga industrijska postrojenja u Iranu, inficirajući najmanje 30.000 računara širom zemlje. Prema procenama stručnjaka, Stuxnet je najsofisticiraniji maliciozni program ikad napravljen, tj. predstavlja kombinaciju koja eksploatiše četiri različite ranjivosti u Windows operativnim sistemima [8].

Računarski virus

Računarski virusi su samoreplicirajući maliciozni programi koji se šire tako što ubacuju kopije samih sebe u drugi izvršni kod ili dokument odnosno inficiraju datoteke i programe na ciljanom računaru. Štetu na zaraženom računaru realizuju tako što brišu ili menjaju fajlove na disku. Svojim malicioznim aktivnostima mogu oštetiti softver ciljanog sistema. Pokreću se tako što korisnik pokretanjem odgovarajućeg zaraženog programa u stvari prvo pokreće virus, a zatim program.

Lako se prenose prenosnim diskom, preuzimanjem zaraženih fajlova sa interneta ili drugog računara u mreži, prijemom zaraženih fajlova putem elektronske pošte odnosno dospevanjem zaraženih fajlova na drugi računar. Računarski virusi su sve manje aktuelni, pošto nisu programirani da se šire preko računarskih mreža. Potreban je host program za njihovo širenje, i to je osnovna razlika u odnosu na crve.

Postoje različite vrste računarski virusa, kao što su: *polimorfni (polymorphic) virusi* – menjaju oblik s ciljem izbegavanja detekcije; *nevidljivi (stealth*) – prikrivaju svoje prisustvo od aplikacija s ciljem izbegavanja detekcije, *retro* – napadaju ili zaobilaze AV programe (anti AV programi) i drugi.

Računarski crv

Računarski crv (*worm*) je tip malicioznog softvera koji se višestruko umnožava putem računarskih mreža. To su samostalni programi koji se, za razliku od virusa, ne prilepljuju uz glavne izvršne programe.

Računarski crv koristi mrežu da bi se preneo na druge sisteme, samostalno, bez intervencije ljudi. Kopira se sa jednog računara na drugi, automatski, preuzimanjem kontrole nad funkcijama računara. Mnogo brže se šire od virusa. Crv škodi mreži i zauzima protok, dok virus škodi ciljanom računaru (ne utiče na mrežne performanse).

Maliciozne aktivnosti realizuju se tako što zauzimaju resurse računara, brišu fajlove, šalju podatke bez znanja korisnika (npr. elektronskom poštom) i slično.

Trojanski konj – trojanac

Trojanski konj (*trojan horse*) je zlonamerni program prerušen u legitimni program, tj. predstavlja se kao drugi računarski program koji radi obično zabavne stvari (npr. igrica), a u stvari je namenjen za krađu informacija i zauzimanje resursa računara (prostor na disku, memoriji…). Maliciozne aktivnosti čine tako što brišu datoteke, šalju podatke iz računara bez znanja korisnika (npr. slanjem e-mail svakom iz adresara) i dr.

Za razliku od virusa, ne može se sam umnožavati, već se prenosi tako što ga korisnik prekopira na drugi računar. Ne umnožavaju se i ne šire sami.

Postoje različite vrste trojanaca: trojanci za daljinski pristup, trojanci za otkrivanje i davanje lozinki, Keyloggers, FTP trojanci i drugi.

Logička bomba

Logička bomba (*logic bomb*) je maliciozni program koji se pokreće kada se ispune određeni uslovi, tj. kada korisnik nekom svojom aktivnošću pokrene aktiviranje logičke bombe.

Vremenska bomba

Vremenska bomba (*time bomb*) je maliciozni program koji se aktivira u određenom, unapred isprogramiranom, trenutku, a ne delovanjem korisnika.

Kao i logička bomba, dovodi do toga da se nekontrolisanom samoreprodukcijom zauzimaju resursi računara.

Špijunski programi

Špijunski programi (*spyware*) su maliciozni programi koji prikupljaju podatke o korišćenju računara, poseti određenih sajtova (frekvencija, interesovanja…), lične informacije (npr. brojevi kreditnih kartica).

Oglašavački programi

Oglašavački programi (*adware*) su maliciozni programi koji se instaliraju na određeni računar bez znanja korisnika i prikazuju oglase (*advertisements*) kada se koristi pretraživač na internetu.

Pokazatelji prisustva malicioznog programa na računaru mogu biti sledeći:

1. usporavanje rada na računaru, sporije učitavanje programa,
2. česti iskakajući (pop-up) prozori,
3. neobične promene u radu računara – neočekivane poruke o greškama, gubljenje datoteka, pojavljivanje novih datoteka, nepravilan rad aplikacija (web pretraživački, programi za obradu teksta…).

Zaštita od malicioznih programa može se ostvariti primenom sledećih mera:

1. korišćenjem legalnih, ažurnih softvera za zaštitu (*antivirus, antispy, antitrojan, online* skeneri),
2. čestom promenom lozinki i nesnimanjem,
3. selektivnih pristupanjem sajtovima,
4. korišćenjem različitih verzija pretraživača na internetu,
5. korišćenjem i pravilnim konfigurisanjem *firewall*-a i drugih mrežnih uređaja,
6. zatvaranjem mrežnih servisa koji se ne koriste,
7. redovnim zakrpama (*patch*) sistema.

Zaključak

Računarski sistemi su podložni greškama (u korisničkim aplikacijama, operativnim sistemima itd.) što dovodi do ranjivosti sistema i izloženosti ozbiljnim potencijalnim opasnostima. Sama priroda interneta (otvorenost i mogućnost jednostavnog povezivanja) dovodi do sve većeg broja korisnika i sve veće dostupnosti alata za napad čak i za one korisnike sa skromnim informatičkim znanjem.

Iz navedenih razloga nužno je permanentno praćenje trendova i poznavanje karakterističnih napada na računarske sisteme. Aktuelni sistemi za detekciju napada nisu u mogućnosti da otkriju sve vrste napada na računarske sisteme imajući u vidu činjenicu da se neprestano menjaju tehnike, metodi, sredstva i motivi napadača. Da bi se prikupili podaci i proučavala priroda napada na računarske sisteme, primenjuju se različite tehnike kao što je npr. *honeypot* gde se računarski resursi (hardverski, aplikativni i mrežni) koriste kao mamac i bivaju napadnuti ili kompromitovani od strane neovlašćenih korisnika. [9,10]

Treba imati u vidu činjenicu da je nemoguće ostvariti apsolutnu zaštitu. Pored nužnosti poznavanja pretnji na internetu nužno je stalno razvijati nove mehanizme zaštite u skladu sa bezbednosnim problemima koji nastaju. Najslabija karika svakog računarskog sistema je čovek i njemu se mora posvetiti naročita pažnja.

Literatura

[1] *Convention on Cyber-crime*, http://conventions.coe.int/treaty/en/treaties/html/185.htm (koristio 10. 1. 2011. godine)

[2] Stallings, W., Brown, L., *Computer Security – Principles and Practice*, Pearson Education, Inc, New Jersey, 2008.

[3] Tulloch, M., *Microsoft Encyclopedia of Security*, Microsoft Press, Redmond – Washington, 2003.

[4] Solange, Ghernaouti-Helie., *Cybersecurity Guide for Developing Countries*, International Telecommunication Union, Geneva, 2009.

[5] Clarke, R., Knake R., *Cyber War – The next treat to National Security and What to do about it*, HarperCollins e-books, 2010.

[6] *ITU Botnet Mitigation Toolkit*, International Telecommunication Union, Geneva, 2008.

[7] Anonymous, *Hakerski vodič za zaštitu*, Kompjuter biblioteka, Čačak, 2004.

[8] *EU Agency analysis of Stuxnet malware: a paradigm shift in threats and Critical Information Infrastructure Protection*, European Network and Information Security Agency, http://www.enisa.europa.eu (koristio 10. 1. 2011. godine)

[9] Bobar, Z., *Zaštita računarskih mreža Ministarstva odbrane i Vojske Srbije primenom virtuelnog honeyneta*, Vojnotehničkih glasnik/Military Technical Courier, Vol. 57, No. 3, pp. 80–87, Ministarstvo odbrane Republike Srbije, Beograd, 2009.

[10] Terzić, M., *Predlog ad hoc računarske mreže Katedre vojnih elektronskih sistema VA*, Vojnotehničkih glasnik/Military Technical Courier, Vol. 59, No. 1, pp. 111–120, Ministarstvo odbrane Republike Srbije, Beograd, 2011.

ATTACKS ON COMPUTER SYSTEMS

FIELD: IT – Information Technologies
ARTICLE TYPE: Professional Paper

Summary:

Computer systems are a critical component of the human society in the 21st century. Economic sector, defense, security, energy, telecommunications, industrial production, finance and other vital infrastructure depend on computer systems that operate at local, national or global scales. A particular problem is that, due to the rapid development of ICT and the unstoppable growth of its application in all spheres of the human society, their vulnerability and exposure to very serious potential dangers increase.

This paper analyzes some typical attacks on computer systems.

Introduction

A computer system represents any device or a group of interconnected or related devices which, pursuant to a program, performs automatic processing of data.

The attack is a threat which, if successful, results in compromising a computer system or compromising security. Each system has its vulnerabilities. A complex system implies a potentially large number of vulnerabilities and failures. The attack is essentially an exploitation of these vulnerabilities and consists of a series of deliberate steps taken by attackers in order to achieve a specific goal.

Typical attacks on computer systems

Bearing in mind different criteria of classification of attacks on computer systems, in practice it is often a case that unwanted events from the aspect of security in computer systems are a combination of different types of attacks. For a better perception of vulnerability of computer systems, this paper presents only specific typical attacks (threats):

1. Denial-of-service (DoS, DDoS) attack is a type of the attack that attempts to prevent legitimate users to access online services

2. Phishing is a type of attack on the Internet when the attackers use the existing Internet services to lure and deceive users to disclose sensitive information (usernames, passwords, credit card data, etc.) which can be used for criminal purposes.

3. Botnet is a large network of infected computers.

4. Spam is unsolicited email, or mail that the user neither asked for nor gave his consent to the sender of such messages to send them to his address

5. Social Engineering is a technique to manipulate people (persuasion, deception, cleverness, false representation, etc.) in order to obtain sensitive information or access to computer systems.

6. Sniffing - Sniffers are devices, hardware or software that can monitor the packets in a network and monitor network traffic, and legally or illegally collect data to be transferred.

7. Spoofing is a delusion ie. fraud which creates the impression that the transfer occurs by an authorized user.

8. Malware is software that harm the target and infect a computer system.

Conclusion

Computer systems are subject to errors (in user applications, operating systems, etc.) which lead to vulnerability and exposure to serious potential dangers. Protection from various types of attacks (threats) on the Internet is a very complex problem that requires significant financial resources to minimize risk. One should be aware of fact that it is impossible to achieve absolute protection. The weakest chain of any computer system is a man and he must be given a special attention.

Key words: *computer system, computer attack*

Datum prijema članka: 20. 01. 2011.

Datum dostavljanja ispravki rukopisa: 11. 02. 2011.

Datum konačnog prihvatanja članka za objavljivanje: 12. 02. 2011.