

**UNIVERZITET SINGIDUNUM
FAKULTET ZA POSLOVNU INFORMATIKU
Danijelova 32, Beograd**

Seminarski rad

predmet: **Poslovna informatika**
tema: **Malware programi**

student: Marko Domanović III-49/2004
profesor: Dr. Zoran Banjac

Beograd, april 2005.

SADRŽAJ

1. Opšte o malware programima	2
2. Kratka istorija kompjuterskih virusa.....	3
3. Vrste malware programa	5
3.1. Virusi	5
3.2. Crvi (worms)	6
3.3. Webbits.....	7
3.4. Trojanci (Trojan horses).....	7
3.5. Spyware/adware.....	8
3.6. Exploiti.....	8
3.7. Rootkit	8
4. Izvori malware-a.....	9
5. Simptomi infekcije i čišćenje	11
6. Preventiva i zaštita od malware programa	13
6.1. Anti-virusni i anti-spyware programi	13
6.2. Firewall sistemi	15
6.3. Email klijenti i serveri naprednih karakteristika.....	16
7. Zaključak.....	17
8. Literatura	18

1. Opšte o malware programima

Pojam "malware", a to je kovanica od reči "malicious software", je termin koji se koristi za sve vidove programa koji nanose štetu, bilo da se ona odnosi na sigurnost podataka na računaru ili na štetu nanetu korisnikovoj privatnosti. Postoje malware programi koji čak ne nanose nikakvu štetu sistemima i postoje samo zbog toga da bi njihov autor isprobao metode širenja, pa je zato, logično pitanje da li se takvi programi mogu svrstati u malware. Obzirom da bespotrebno zauzimaju memorijski prostor i koriste mrežne veze za širenje, mogu se ubrojati u malware.

Malware programi se klasifikuju prema tome šta čine, kako se izvršavaju, i prema načinu na koji se umnožavaju. Međutim, razlike između tipova malware programa nisu uvek tako jasno definisane, pa se mnoge vrste "preklapaju", pa na neki način postoje i "hibridni" malware programi koji kombinuju osobine više vrsta.

Zajedničko za sve vrste malware programa je to da se šire uglavnom bez obzira na volju korisnika, osim ukoliko sam korisnik ne želi da "zarazi" određeni sistem, i na taj način ga ugrozi. Motivi za ovakvo ponašanje nekih korisnika mogu biti različiti:

- edukativni
- dokazivanje u hakerskom svetu
- finansijska korist istraživanjem ponašanja korisnika kako bi se svrstali u određenu ciljnu grupu, a potom servirale određene reklame
- industrijska špijunaža
- krađa novca elektronskim putem
- prenošenje raznih drugih poruka (političkih, ličnih, pa čak i totalno besmislenih poruka)

2. Kratka istorija kompjuterskih virusa

Kompjuterski virusi su prva forma malware programa koja se pojavila 1981 godine. Prvi kompjuterski virus se zvao *Elk Cloner* i bio je napisan za Apple II računar. Termin "kompjuterski virus" je dao Fred Cohen, 1983 godine dok je eksperimentisao sa DEC VAX računarima u okviru naučno-istraživačkog rada. Tada je on klasifikovao viruse na "istraživačke" i viruse "u divljini".

1986 – kreiran je prvi virus za PC računar po imenu Brain, i to je bio boot-sektor virus napisan u Pakistanu i inficirao je isključivo boot sektor disketa formatiranih na 360 KB. Nanosio je štetu tako što je prepunjavao preostali prostor na disketi i na taj način onemogućavao dalje korišćenje. To je bio i prvi "stealth" virus što znači da je pokušavao da se sakrije od detekcije. Kada bi korisnik kompjutera hteo da vidi inficirani boot sektor, prikazivao bi mu se lažni (neinficirani) boot sektor.

1987 – u novembru je napravljen *Lehigh* virus i to je bio prvi virus koji je inficirao "rezidentni" deo memorije tako da je napadao i menjao svaki izvršni fajl koji je bio pokretnut. U decembru, napravljen je *Jerusalem* virus koji je u sebi imao bug, zbog koga je inficirao već inficirane fajlove.

1988 – u martu je kreiran prvi anti-virusni program. Detektovao je i popravljao štetu koju je činio *Brain* virus. *Cascade* virus je takođe tada napravljen, a značajan je po tome što je bio kodiran.

1990 – Pojavljuju se virusi koji imaju napredne karakteristike, kao što su polimorfizam (enkriptovani virusi, gde je kod za dekodiranje promenljiv), oklopljavanje (armoring tj. onemogućavanje disasembliranja virusa) i „multipartite“ (virusi koji inficiraju i boot sektor i programe).

1991 – Virus *Tequila* kombinuje sve tri napredne osobine. On je polimorfan, oklopljen i multipartitan. Pojavljuje se i Norton Antivirus anti-virusni program.

1993 – Pojavljuje se *Cruncher* virus koji je prvi koji je na neki način bio shvaćen kao "dobar". Isti je inficirane izvršne fajlove kompresovao i na taj način štedeo korisnicima prostor na disku.

1995 – pri kraju godine su se pojavili Microsoft Word makro virusi.

1996 – *Concept* postaje najrašireniji Word macro virus. *Boza* je prvi virus koji se pojavio za Windows 95.

1999 – Pojavio se *Melissa* virus koji se širio preko Microsoft Outlook i Outlook Express email klijenata.

2000 – *I Love You* virus se širi nekontrolisano putem emaila i automatski se šalje svima iz adress book-a.

U novijoj istoriji, pojavljuje se sve više i više novih virusa koji se uglavnom zasnivaju na iskorišćenju grešaka u operativnim sistema i raznim programima koji komuniciraju sa Internetom, a posebno P2P filesharing mrežama. Naročito je ugrožen Windows, a u mnogoj manjoj meri ostali operativni sistemi koji se danas koriste. Treba reći da je napravljeno dosta virusa i za C64, AmigaOS, MacOS i MS-DOS. Malware programe je jednostavno nemoguće iskoreniti, jer će uvek biti novih varijanti koje iskorišćavaju nove propuste. Činjenica je i da sa napretkom programa nestaju stari bagovi, a postojeći operativni sistemi i programi jednostavno postaju tehnološki zastareli, pa se povlače iz upotrebe i zbog toga malware programi vremenom postaju nefunkcionalni.

3. Vrste malware programa

Postoji nekoliko osnovnih vrsta malware programa, među kojima su:

- virusi
- crvi (worms)
- wabbiti
- trojanci
- backdoor programi
- spyware/adware
- exploiti
- rootkit-ovi

Osobine različitih vrsta malware programa se u velikom broju slučajeva kod virusa zapravo kombinuju, tako da je ponekad veoma teško odrediti kojoj vrsti malware-a neki virus pripada.

3.1. Virusi

Virusi su samo-kopirajući programi koji ubacuju svoj izvršni kod u izvršne fajlove na zaraženom kompjuteru ili preko mreže. Mogu da inficiraju čak i dokumente i to su macro virusi, a infekcije boot sektora hard diskova ili disketa su nešto ređe u poslednje vreme. Zbog načina raznožavanja koji je sličan biološkim virusima, oni su tako i nazvani, a analogno tome, kompjuter sa virusom se često naziva i inficirani ili zaraženi kompjuter. Virusni mogu isključivo da nanesu štetu softveru, a ne i hardveru, ali je zanimljivo spomenuti da postoje virusi (npr. CIH) koji napadaju određene vrste BIOSa, brišući sve podatke iz njega, i ostavljajući kompjuter neupotrebljivim sve dok se u BIOS chip ponovo ne upiše njegov program, tj. izvrši "flešovanje". Međutim, mogućnost da virusi oštete hardver ne treba u potpunosti odbaciti jer postoje ideje na koji bi se način to moglo postići. Recimo, virus koji bi mogao da promeni rezoluciju slike na monitoru više puta u sekundi bi najverovnije posle nekog relativno kratkog vremena izazvao kvar na istom. Mogućnost oštećenja hardvera uz pomoć malicioznog softvera u mnogome zavisi od same konstrukcije hardvera i od toga da li sam hardver ima grešaka u konstrukciji.

Virusi su čak u velikom broju slučajeva benigni ili samo smetaju pri radu, a mogu biti i "tempirani", kada se nazivaju "bombe", a šteta koju prouzrokuju može biti "okinuta" na vremenskoj ili logičkoj bazi. Recimo, virus se aktivira na određeni datum ili period posle, ili je potrebno da korisnik učini nešto nevezano za sam

virus da bi isti to „osetio“ i aktivirao se. Termini koji se koriste za ovakve viruse su time-bombs ili logic-bombs.

Sa inficiranog kompjutera, virusi se prenose na druge kompjutere ili korisnikovim kopiranjem, ili putem mreže i u tom smislu su različiti od crva koji uglavnom koriste Internet za svoje širenje.

U pogledu načina širenja, postoje rezidentni i nerezidentni virusi. Rezidentni virusi su oni koji ostaju u RAM memoriji posle izvršenja inficiranog programa, a nerezidentni virusi odmah po pokretanju zaraženog programa zaražavaju ostale programe, ali ne ostaju u memoriji.

Host za viruse mogu biti različiti entiteti računarskog sistema, a najčešće, to su:

- Binarni izvršni fajlovi
- Boot sektori disketa i hard diskova
- Master Boot Record (MBR) hard diskova
- Batch fajlovi (batch fajlovi u DOS-u i Windowsu) i shell skript fajlovi na Unix sistemima
- Skriptovi specifični za određenu aplikaciju
- Dokumenti koji imaju makroe (MS Word, Excel, Access, itd...)

3.2. Crvi (worms)

Za razliku od virusa, crvi nisu deo drugih programa, već su to zasebni programi koji se prenose i izvršavaju koristeći slabosti operativnog sistema, a posebno programa za transmisiju podataka na Internetu.

Prvi crv se pojavio 1978 godine, a stvorila su ga dva istraživača u Xerox PARC istraživačkom centru, a prvi koji je pridobio veću pažnju je Morris crv, koji se pojavio 1988 godine i koji je vrlo brzo zarazio puno kompjutera a koristio je greške u Unix operativnom sistemu.

Pored umnožavanja, crvi mogu biti dizajnirani i da rade druge radnje, kao što je brisanje podataka, instaliranje backdoor programa, slanje emailova, itd... a takva funkcija kod crva se naziva "payload". Samo po sebi, širenje crva može predstavljati priličan problem kod performansi mrežnih veza, a primer za to je globalno usporenje Interneta pri maksimalnom širenju jednog od najpoznatijih i najraširenijih virusa današnjice – MyDoom crva.

Najuobičajeniji payload crva je backdoor program koji može ima različite funkcije ali je najčešća ona kada se instalira SMTP server i kompjuter tada služi kao tačka

sa koje se šalju neželjene email poruke (SPAM), najčešće komercijalne prirode. Ima slučajeve da su kompjuteri na koji su instalirani backdoor programi uz pomoć crva služili kao potencijalne tačke sa kojih se izvode DDOS napadi (Distributed Denial of Service), pa je bilo pokušaja ucena velikih kompanija uz pomoć pretnji napadom. Čak postoje crvi koji koriste backdoorove instalirane od drugih crva, kao što je Doomjuice, koji koristi backdoor MyDoom crva. Ukratko, DDOS napad predstavlja pokušaj obaranja bilo koje vrste serverskog sistema na Internetu, uz pomoć neprekidnog slanja velikog broja klijentskih zahteva, u nadi da će sistem pasti kada dosegne potpuno iskorišćenje svojih resursa, a ovo se obično odnosi na iskorišćenost memorije i broj procesa.

3.3. Webbits

Specijalna i veoma retka varijanta malware programa. Za razliku od virusa, ne inficiraju programe ili dokumente na hostu, već su to zasebni programi koji se najčešće automatski pokreću. Za razliku od crva, ne koriste mrežu da bi se širili već se samo repliciraju u okviru zaraženog kompjutera. Obično su maliciozni, koriste se najčešće kao baza za DOS napade.

3.4. Trojanci (Trojan horses)

“Trojanac” je maliciozni program koji je “prerušen” u potpuno naizgled legitimni program. Naziv je naravno preuzet iz grčke mitologije, i tu praktično postoji potpuna analogija između mitskog i stvarnog, pa je i ovo bio prikladan naziv za ovu vrstu malware programa. Obično, trojanci instaliraju backdoor programe koji omogućavaju potpunu remote kontrolu nad zaraženom mašinom, a često se instaliraju i keyloggeri ili packet snifferi (programi koji pamte svu ili određenu vrstu mrežne komunikacije). U poslednje vreme, trojanci poprimaju osobine virusa i crva, tako da se razlika između njih sve teže uočava.

3.5. Spyware/adware

Spyware i adware programi su varijante malicioznog softvera koji prikuplja i šalje podatke o ponašanju korisnika kompjutera bez njegovog znanja. Ovi programi mogu vršiti puno različitih funkcija uključujući prikazovanje neželjenih reklama, prikupljanje privatnih podataka kao što su brojevi kreditnih kartica, re-rutiranje zahteva za web stranicama kako bi se ostvarili prihodi od referisanja novih korisnika, instaliranje teško uočljivih "dialera", itd... Adware se u mnogome poklapa sa definicijom spyware-a, sa tom razlikom da adware-a isključivo služi u komercijalne svrhe (ad je skraćenica od advertisement). Adware programi prikupljaju informacije o ponašanju korisnika, web sajtovima koje korisnik posećuje i uz pomoć različitih mehanizama (najčešće cookie,activex, javascript), istim korisnicima se serviraju odgovarajuće reklame, nude odgovarajući proizvodi putem emaila i sl.

Zanimljiv podatak je da je čak 90% kompjutera u svetu zaraženom nekom vrstom spyware programa.

3.6. Exploiti

Exploiti su programi koji iskorišćavaju određenu slabost nekog programa, oni najčešće sami po sebi ne nanose štetu i postoje samo da bi se demonstrirala slabost nekog programa, ali njihove "usluge" često vrlo rado koriste wormovi, virusi, spyware i sl.

3.7. Rootkit

Rootkit je softver koji se ubacuje na kompjuter pošto je napadač dobio kontrolu sistema a namena mu je da olakša remote kontrolu i da sakrije tragove upada brisanjem log fajlova ili sakrivanjem procesa koji su pod kontrolom napadača. Često rootkitovi sadrže i backdoorove, omogućavajući olakšani naknadni upad ili exploit programe za napade na druge sisteme. Važno je primetiti da se ciljani napadi obično izvode sa sistema koji su takođe prethodno bili ugroženi, da bi se sa njih lako mogli ukloniti dokazi o identitetu napadača, jer sam napadač dobija mogućnost da ukloni dokaze. Rootkitovi se vrlo često vezuju za kernel nivo, pa ih je teško otkriti, a kada se jednom otkriju vrlo je bitno da se kompletno reinstalira sistem, kako bi se sigurno uklonili svi tragovi rootkita.

4. Izvori malware-a.

Malware programi mogu dospeti u operativni sistem na nekoliko načina:

- Prostim kopiranjem zaraženog programa sa mobilnog medija, preko LAN mreže ili preuzimanjem sa Interneta putem FTP, HTTP, nekog od P2P protokola, i slično.
- Putem email attachmenta
- Putem malicioznih ActiveX, Java i Javascript programa
- Iskorišćavanjem sigurnosnog propusta u sistemu (koristeći exploite), a to je put kojim se šire crvi (worms). Serverski program na napadnutom sistemu predstavlja prolaz.
- Preko multimedijalnih fajlova koji u sebi sadrže takav niz podataka, da iskorišćavaju propuste u klijentskim aplikacijama sistema. Takav slučaj je i jedna verzija biblioteke gdiplus.dll, dela operativnog sistema Windows XP u nekoj od ranijih verzija.

Crvi, i maliciozni ActiveX, Java i Javascript programi se uglavnom automatski izvršavaju posle uspešnog ulaženja na sistem, što nije slučaj sa virusima i trojancima koje korisnik treba sam da pokrene, posle čega oni koriste jedan od načina za automatsko pokretanje pri dizanju sistema.

Pri korišćenju weba treba biti posebno obazriv sa određenim tipovima sajtova, a najopasniji su sajtovi koji sadrže "crack" programe, jer se pokazalo da u relativno velikom broju slučajeva programi za krekovanje drugih programa u sebi sadrže i maliciozni kod, ako ne i isključivo maliciozni kod. U slučaju da se koriste sajtovi koji izvršavaju kod na klijentu, veoma je poželjno imati uključen rezidentni anti-virusni skener, ali ni u njega se ne treba pouzdati previše. Treba dozvoliti izvršavanje ActiveX i Java programa samo sa onog sajta za koji smo sigurni da je ozbiljan, tačnije da iza njega stoji ozbiljna firma.

Pri čitanju email poruka, postoji relativno mala mogućnost da samim pozicioniranjem pointera na poruku ili downloadom email poruke email klijent automatski pokrene maliciozni program, ali takvu mogućnost ne treba potpuno odbaciti, jer sigurnosni propusti u email klijentima omogućavaju i to. Email attachmente nikako ne treba pokretati ukoliko nismo sigurni da je to sigurno ono što je trebalo da primimo. Vrlo često se dešava da vam prijatelj pošalje neki attachment, a ustvari to nije uradio on već neki maliciozni program sa bilo kog kompjutera koji je imao njegovu email adresu koju je iskoristio je za stavljanje u From: polje. Valja napomenuti da je From: polje apsolutno proizvoljno sa stanovišta protokola za prenos email poruka. Za utvrđivanje izvora poruke, merodavno je jedino zaglavlje email poruke koje sadrži informacije o putanji email poruke, odnosno IP adresama SMTP servera preko kojih je putovala. "IP spoofing" tehnike, tj. tehnike sakrivanja stvarne IP adrese mogu omesti i ovo, a

takođe i korišćenje nezaštićenih ("relaying") SMTP servera, odnosno email servera čiji administrator je ostavio mogućnost da preko njega email šalje svako, bez obzira koju IP adresu imao. Email poruke sa virusima često su "oplemenjene" primamljivim porukama koje povećavaju šansu da attachment bude pokrenut. O efikasnom načinu zaštite od neželjenih i zaraženih email poruka, biće još reći nešto kasnije u posebnoj tački.

Većina BIOS programa sadrži opciju za detektovanje promene boot sektora hard diska, pa je korisno uključiti ovu opciju, jer je promena boot sektora veoma retka operacija i dešava se uglavnom samo pri instalacijama operativnog sistema. Njegova promena u toku regularnog rada najverovatnije znači da je sistem već zaražen. Treba znati da se zaraženi boot sektor može prebrisati dobrom verzijom uz pomoć softvera, ali uz napomenu da to nikako ne garantuje da se boot sektor opet neće inficirati izvršavanjem zaraženog izvršnog fajla.

5. Simptomi infekcije i čišćenje

Postoji širok spektar simptoma postojanja malware programa u sistemu, manje ili više uočljivih. Najteži simptomi uključuju nemogućnost podizanja operativnog sistema zbog obrisanih ili promjenjenih sistemskih fajlova ili potpuno brisanje podataka sa hard-diska. U ovakvim slučajevima uglavnom je vrlo neizvesno da li je moguće popraviti nastalu štetu i dovesti operativni sistem i podatke u prethodno stanje. Preporučuje se podizanje sistema sa diskete na kojoj postoji antivirusni softver i skeniranje sistema kako bi se utvrdila vrsta infekcije i pokušalo "čišćenje", prvo sa samim antivirusnim programom (ako nudi tu mogućnost), a potom i "ručno", prateći uputstvo za čišćenje virusa, ukoliko ono postoji. Uglavnom je kod težih infekcija potrebno podići operativni sistem sa Windows instalacionog diska i odabrati opciju "Repair", kako bi se sistemski fajlovi vratili u originalno stanje.

Među simptomima može biti i usporenje LAN i Internet komunikacije, a izazvano je najčešće širenjem crva. Simptomi ovakve infekcije se efikasno suzbijaju sa firewallom, a pored toga, firewall može i da onemogući širenje crva.

Promena podataka u izvršnim fajlovima i dokumentima još jedan je od simptoma zaraze, mada to može biti i rezultat disfunkcije hardvera.

Dalje, funkcionalnost sistema može biti promjenjena i usporena. Moguće je pojavljivanje neočekivanih poruka na ekranu, zvučnih signala, remećenje normalnog rada ulaznog hardvera – najčešće tastature i miša, a sve su ovo simptomi sasvim sigurne infekcije. Ukoliko simptomi i nisu veoma izraženi, na infekciju treba posumnjati i poželjno je skeniranje svih particija hard diska sa najnovijim verzijama nekih od anti-virus i anti-spyware programa.

Kada se utvrdi da je sistem inficiran, ne treba upadati u ishitrene i nepromišljene akcije. Prvo je dobro načiniti backup važnih podataka, a potom uz pomoć antivirusnog programa utvrditi o kakvom se tipu virusa radi i da li sa istim programom može i da se ukloni. Ako ne, na Internetu je najverovatnije moguće pronaći specijalni program za uklanjanje tog tipa virusa. Korisni programi za najrasprostranjenije viruse se mogu naći na adresi: <http://securityresponse.symantec.com/avcenter/tools.list.html>.

Ako nema uspeha u pronalaženju odgovarajućeg programa za čišćenje, treba potražiti uputstva za ručno uklanjanje virusa. Ukoliko i taj pokušaj propadne, ostaje opcija da korisnik sam utvrdi o kom procesu se radi i na koji način se isti pokreće. Treba znati da pored velikog iskustva koje je potrebno za tako nešto,

uspeh u tome nikako nije zagarantovan, pa lako možemo doći i do nekih polurešenja za koja možemo samo misliti da su rešenja.

Poslednja solucija je formatiranje hard diska i reinstalacija sistema, uz prethodni backup podataka, što je vremenski i najzahtevnija opcija, ali u nekim slučajevima i neizbežna, uzimajući u obzir da je za neke vrste infekcije potreban izuzetno visok nivo znanja i iskustva da bi se računar dezinfikovao.

Pri izboru anti-virus programa, a posebno anti-spyware programa, potrebno je posebno obratiti pažnju na reputaciju firme koja ga proizvodi, kao i na mišljenje korisnika koje se lako može pronaći po forumima i u raznim kako štampanim, tako i on-line publikacijama. Količina malware program koju program može da otkrije je možda i manje bitna od sposobnosti brzog ažuriranja programa sa najnovijim "otiscima" malware-a, dakle osobine da je što pre po pojavi novog malware programa, anti-malware program sposoban da isti i pronađe. U praksi, poznatiji programi se ažuriraju skoro svakodnevno sa novim definicijama malware-a.

Anti-virusni programi sa najboljom reputacijom su:

- NOD32 (<http://www.eset.com>, \$39)
- Norton Antivirus (<http://www.symantec.org>, \$50)
- Kaspersky Antivirus (<http://www.kaspersky.com>, \$41.5),
- Avast! (<http://www.avast.com>, besplatan za home upotrebu),
- AVG (<http://www.grisoft.com>, \$33.3 za dve godine)

Test najpoznatijih anti-spyware i firewall programa se može naći na <http://www.adwarereports.com>, a zanimljivo je i da je i sam Microsoft zajedno sa Windows XP Service Pack 2 paketom izdao i svoj anti-spyware program, pa se po tome se može zaključiti koliki se značaj pridaje zaštiti od malware programa.

6. Preventiva i zaštita od malware programa

Zaštita od malware programa je jedna velika grana kompjuterske industrije, a svakako jedna od najznačajnijih. U poslednje vreme zaista nije lako zaštititi sistem, a naročito Windows operativni sistem od napada koji "vrebaju na svakom koraku". Da bi se korisnik uspešno zaštitio od virusa i crva potreban je određen nivo znanja i discipline u korišćenju kompjutera, koga u slučaju spyware i trojanaca često nikad nije dovoljno.

Borba protiv malware programa se vodi na nekoliko frontova. Najvažnije je da korisnik bude svestan bar većine načina na koje malware programi mogu zaraziti računar i da postigne nivo discipline kako bi uspešno primenio to znanje.

Osnovni tipovi zaštite su:

1. Anti-virusni programi
2. Anti-spyware programi
3. Firewall sistemi
4. Email klijenti i serveri naprednih karakteristika sa prepoznavanjem virusa i SPAM-a

6.1. Anti-virusni i anti-spyware programi

Granica između ove dve vrste programa sve više se briše, pa se i sve više pojavljuju programi koji kombinuju ove dve vrste zaštite. Tehnički gledano, ne postoji velika razlika između načina otkrivanja virusa, crva i spyware programa. Ovakvi programi obično imaju nekoliko komponenti, pa ću na primeru NOD32 antivirusnog programa (<http://www.eset.com>) koji je jedan od kompletnijih i boljih opisati njihove funkcije.

NOD32 antivirus se sastoji od sledećih komponenti:

5. Rezydentnog antivirusnog monitora
6. MS Office macro virus detektora
7. Internet monitora (zajedno sa skenerom dolazećeg i odlazećeg email-a)
8. On-demand skenera
9. On-line update

Rezidentni antivirusni monitor je neprekidno aktivan proces i konstantno proverava ostale procese koji su trenutno pokrenuti, tražeći otiske poznatih virusa ili proveravajući procese heurističkim metodama, a to znači otkrivanje virusa iako za njega u programu ne postoji definisan otisak.

Monitor MS Office macro virusa je takodje rezidentni monitor i otkriva macro viruse u Word, Excel i Access dokumentima.

Internet monitor konstantno "posmatra" Internet konekciju i otkriva maliciozne ActiveX, Javascript i Java aplete koji dolaze putem HTTP protokola, a vrši i "presretanje" email poruka, tj. preuzima njihov download na sebe, skenira ih, pa tek onda isporučuje klijentu.

NOD32 on-demand skener se koristi ako želimo da skeniramo hard disk, određene direktorijume ili određene fajlove, a najčešće se koristi pri stavljanju novih drajvova (najčešće disketa) u sistem.

On-line update komponenta služi za ažuriranje samog programa i definicija virusa i worm-ova i ukoliko je Internet veza na računaru neprestano aktivna, obično se definicije novih virusa downloaduju automatski, a može se i korisnički definisati ritam ažuriranja.

Po otkrivanju malicioznog programa NOD32 će obavestiti korisnika, ali da bi se virus očistio, najčešće će biti potrebno skinuti specijalni program za tu vrstu virusa ili manuelno, po nekom uputstvu, a najčešće se tu radi o ručnoj promeni registry-ja i brisanju određenih fajlova i ponovnom nabavljanju ispravnih verzija.

Spybot Search & Destroy (<http://www.safer-networking.org>) je najpoznatiji i program za zaštitu od spyware i adware programa. Posедуje rezidentnu zaštitu za Internet Explorer, onemogućavajući instalaciju malicioznih toolbarova i blokirajući cookie. Za razliku od mnoštva ovakvih programa, on je besplatan i ne sadrži u sebi bilo kakav spyware, a i otkriva najviše spyware-a. Takođe ima komponentu za update, mada to kod njega nije automatizovano.

Važan korak u zaštiti kompjutera je i korišćenje tehnološki naprednijeg Mozilla Firefox web čitača, koji u odnosu na MS Internet Explorer ima mnogo manje sigurnosnih propusta, a i u njemu je nemoguće izvršiti ActiveX skriptove koji su i najčešći uzrok narušavanja sigurnosti preko HTTP protokola.

6.2. Firewall sistemi

Firewall može predstavljati hardver ili softver koji onemogućava određeni tip TCP/IP komunikacije između 2 tačke u mreži. Na taj način kontroliše se saobraćaj i neomogućava se konekcija koja se uspostavlja da bi se kompjuter zarazio, a u slučaju već zaraženog kompjutera firewall može da onemogući rad backdoor-a.

Filtracija TCP/IP paketa se može vršiti po nekoliko kriterijuma. Može se ispitivati njihov sadržaj, i njihov izvor i destinacija u smislu IP adrese, kao i porta. Pritom se za kućne korisnike najčešće koriste personalni softverski firewall sistemi koji filtriraju pakete po izvoru, destinaciji i portu.

Firewall je značajan faktor zaštite u firmama, gde su kompjuteri u internoj mreži (intranetu) jednostavno nedostupni za dolazeći saobraćaj sa Interneta i obično se tu radi o gateway sistemima koji su zapravo kombinacija rutera i firewall-a. Za kuće korisnike, a pogotovo one koji koriste Internet sa realnom IP adresom, značajni su softverska firewall rešenja, a jedno od njih je Kerio Personal Firewall (<http://www.kerio.com>).

Kerio Personal Firewall je namenjen za kućnu upotrebu, mada se mora reći da je namenjen nešto naprednijim korisnicima zbog svojih veoma detaljnih mogućnosti podešavanja. Za početnike će sasvim dovoljan biti i "fabrički" firewall koji se ugrađuje u sam Windows XP operativni sistem. Princip rada personalnog firewalla je da za svaki program koji hoće da uspostavi Internet komunikaciju biva presretnut od strane firewalla, kada korisnik može da odobri ili zabrani konekciju. Recimo, ako smo instalirali neki Internet server na operativni sistem, kao što je recimo FTP server, firewall će pri prvom pokušaju komunikacije spoljnog klijenta sa serverom upitati korisnika da li taj tip komunikacije dozvoljava ili ne, samo jednom ili permanentno. Na taj način, mogu se onemogućiti mnogi backdoor programi koji otvaraju "listening" port za dolazeći saobraćaj. Pri svakom pokušaju programa instaliranog na sistemu da uspostavi komunikaciju sa nekim Internet serverom, firewall će takođe upitati korisnika za dozvolu. Postoji još dve bitne funkcije Kerio Personal Firewall-a, jedna je da svaka aplikacija koja želi da pokrene neku drugu aplikaciju mora dobiti odobrenje korisnika, a druga je da Kerio detektuje kada je neki program promenjen i upoznaje korisnika sa tim, nudeći mu da ne omogući njegovo izvršavanje. Takođe, firewall može sprečiti "skeniranje" kompjutera, na taj način što blokira ICMP pakete putem kojih napadači uglavnom saznaju za postojanje kompjutera na mreži. Kerio ima dobar sistem logovanja paketa, kao i zaštitu od reklama i pop-up prozora preko kojih najčešće i ulaze maliciozni skriptovi u sistem. Takođe podržava i automatski self-update.

Personalni firewall spada u osnovne načine zaštite od malicioznih programa, i ništa manje nije važan od anti-virus i anti-spyware programa.

6.3. Email klijenti i serveri naprednih karakteristika

Treći u nizu vrsta programa koje treba koristiti pri zaštiti su email klijenti sa mogućnošću prepoznavanja i brisanja virusa na samom email serveru, pre nego što je email zapravo i prenet na računar. Jedan od standardnih programa ove namene je Mailwasher (<http://www.mailwasher.com>), koji pored toga što uglavnom može da prepozna virus u poruci, prepoznaje i SPAM poruke uz pomoć javnih servisa kao što su Spamcop (<http://www.spamcop.net>) ili ORDB (<http://www.ordb.org>). Pored te vrste zaštite na klijentskim sistemima, na administratorima je i da ugrade odgovarajuće anti-virus programe na serverskoj strani, a među kojima je najpoznatiji za Spamasassin za Linux operativni sistem (<http://spamassassin.apache.org>).

7. Zaključak

Malware programi su objektivni problem računara uopšte, a priroda tog problema je takva da on sasvim sigurno nikada neće biti iskorenjen, već da će se korisnici manje ili više uspešno i ubuduće štititi od njih. Veliki problem sa raznim tipovima malware programa imaju korisnici koji nisu spremni da steknu bar minimalno znanje o načinima zaštite. Međutim, problematika malware programa je takva da svako može relativno sigurno da koristi računar, ako sprovede samo nekoliko mera u cilju zaštite i ako stekne osnovno znanje o malware-u.

Ukoliko je sigurnost na prvo mestu pri radu sa nekim računarom, svakako da je bolje instalirati Linux operativni sistem za koji postoji neuporedivo manje malware programa, mada to ne znači da Linuxu nedostaju programi za zaštitu. To je situacija danas, ali jedno je sigurno: kako se povećava udeo Linux instalacija na desktop konfiguracijama, pojavljivaće se sve više i više malware-a i za ovaj operativni sistem.

8. Literatura

Introduction to computer viruses

<http://www.grassrootsdesign.com/intro/virus.php>

Wikipedia.org

<http://www.wikipedia.org>

The history of computer viruses

<http://www.exn.ca/nerds/20000504-55.cfm>

History of viruses

http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_1_1.html

Next generation viruses

<http://www.sorgonet.com/virus/nextgenviruses/>

Malware: what is it and how to prevent it?

<http://arstechnica.com/articles/paedia/malware.ars>