TEHNIKA I INFORMATIKA U OBRAZOVANJU
3. Internacionalna Konferencija, Tehnički fakultet Čačak, 7–9. maj 2010.
TECHNICS AND INFORMATICS IN EDUCATION
3rd International Conference, Technical Faculty Čačak, 7–9th May 2010.

UDK: 004.492 Stručni rad

ZAŠTITA RAČUNARSKIH SISTEMA OD VIRUSA

Marko Ćirović [1]

***Rezime**: Primena računarskih sistema u svim oblastima rada zahteva primenu mera zaštite kako bi se sprečili i izbegli rizici koje donose računarski virusi. Pravilnom primenom određenih mera moguće je uspešno zaštititi računarske sisteme od virusa. Namera mi je da ovim radom svim korisnicima računara približim značaj poznavanja zaštite računarskih sistema od virusa, kako oni funkcionišu i šta im je cilj.*

***Ključne reči:** Zaštita računara,računarski virusi, mere zaštite.*

PROTECTION OF COMPUTER SYSTEMS FROM VIRUSES

***Summary**: The application of computer systems in all areas of work requires the application of safeguards to prevent and avoid risks brought by computer viruses. Proper implementation of specific measures it is possible to successfully protect computer systems from viruses. The intent is to present the work of all computer users closer to knowing the importance of protecting computer systems from viruses, how they work and what they target.*

***Key words:** Computer protection, computer viruses, protection measures.*

1. UVOD

Računarski virusi su oduvek izazivali strah kod ljudi. Sama reč "virus", priznaćete, asocira na nešto što pravi štetu, uništava i zadaje velike muke. Isto kao i prirodni virusi, računarski virusi su sposobni da se razmnožavaju, uništavaju i skrivaju, samo što se svi ti procesi odvijaju na računaru. U ovom radu ćemo detaljno objasniti šta su to računarski virusi, kako funkcionišu i šta im je cilj i kako se uspešno zaštititi od njih.

2. ŠTA JE TO VIRUS I KAKO SE KOMPJUTER INFICIRA VIRUSOM?

Kompjuterski virus je kompjuterski program koji može da se rasprostre po računarima i mrežama tako što kopira samoga sebe, obično bez znanja korisnika. Virusi mogu da imaju štetne sporedne efekte, počev od prikazivanja iritirajućih poruka pa do brisanja svih datoteka sa kompjutera.

[1] Marko Ćirović, kapetan, Načelnik telekomunikacija i informatike u 72.idb, Vespučijeva 23/10, Beograd, E-mail: marko.cirovic@hotmail.com

Virus program mora da se startuje da bi inficirao računar. Virusi koriste različite metode da obezbede da se to dogodi. Mogu da se prikače za druge programe ili da se sakriju u kodu koji se startuje automatski kada otvorite određeni tip fajlova. Inficirani fajl može se primiti na disketi, u e-mail-u (*attachment)* ili u datoteci „skinutoj" sa Interneta. Čim pokrenete datoteku, kod virusa se startuje. Nakon toga virus može da kopira samoga sebe u druge datoteke, ili diskove i da menja sadržaj računara.

2.1. Trojanski konj

Trojanski konji su programi koji rade stvari koje nisu opisane u njihovim specifikacijama. Korisnik startuje ono što za šta misli da je legitiman program, čime dozvoljava da se izvrše skrivene i često štetne funkcije. Trojanci se ponekad koriste kao sredstvo da se neki korisnik inficira računarskim virusom.

Backdoor („ na zadnja vrata") Trojanci su programi koji omogućavaju drugim korisnicima da preuzmu kontolu nad računarom preko Interneta.

2.2. Crvi (worms)

Crvi su slični virusima, ali njima nije potreban prenosilac (kao makro ili boot sektor). Crv prosto pravi kopiju samoga sebe i koristi komunikaciju između računara da se širi. Mnogi virusi kao što su *Kakworm (VBS/Kakworm)* ili *Love Bug (VBS/LoveLet-A)* ponašaju se kao crvi i koriste e-mail da bi se forward-ovali, raširili na druge korisnike.

2.3. Boot sektor virusi

Ovo je prvi tip virusa koji su se prvi pojavili. Oni se šire tako što modifikuju boot sektor, koji sadrži program koji izvodi startovanje računara. Kada se uključi, hardver traži boot sektor program – koji je obično na hard disku, ali može da bude i na disketi ili disku i startuje ga. Onda ovaj program učitava ostatak operativnog sistema u memoriju. Boot sektor virus zamenjuje originalni boot sektor svojom, modifikovanom verzijom (a orginal obično sakrije negde na hard disku). Kada se sledeći put startuje, koristi se zaraženi boot sektor i virus postaje aktivan. Inficira se samo ako se računar startuje sa inficiranog diska. Mnogi od njih su sada zastareli jer su pisani za DOS mašine i obično se ne šire na Windows programima mada ih mogu sprečiti da se regularno startuju.

2.4. Parazitski virusi (virusi datoteka)

Parazitski virusi, takodje poznati kao virusi datoteka, atačuju se na programe (tzv.„ executables"). Kada se startuje program zaražen virusom, prvo se pokreće virus. Da bi se prikrio, virus zatim startuje i originalni program. Operativni sistem računara vidi virus kao deo programa koji je pokušan da se startujete i daje mu ista prava. To znači da kopira samoga sebe, da se instalira u memoriji, ili da sačuva svoje rezultate. Iako su se pojavili u ranoj istoriji virusa još uvek predstavljaju pravu pretnju jer je Internet olakšao distribuciju programa i pružio virusima nove mogućnosti za širenje.

2.5. Makro virusi

Makro virusi koriste makroe, komande koje su ugradjene u datoteke i startuju se automatski. Mnoge aplikacije, naročito one koje se bave obradom teksta ili tabelarnih prikaza, koriste makroe. Makro virus je makro program koji može da kopira sebe i da se širi

sa jedne datoteke na drugu. Ako otvorite datoteku koja sadrži makro virus, virus se kopira u datoteke za startovanje aplikacije i računar je zaražen. Takodje mogu da se šire na svakoj platformi na kojoj se izvodi aplikacija koja ih „hostuje“. Iznad svega, lako se šire jer se dokumenti često razmenjuju preko elektronske pošte i Internet sajtova.

2.6. Šta virusi mogu da učine?

Sporedni efekti virusa, često nazvani „*payload*“ (ceh), su za korisnike najzanimljiviji aspekt virusa. Evo šta neki virusi mogu da urade:

- **Poruke** *WM97/Jerk* prikazuje poruku „I think (user’s name) is a big stupid jerk!“ (Mislim da je taj i taj veliki mamlaz!)
- **Obesne šale** *Jenki* svira „Yankee Doodle Dandy“ u 5 ujutru.
- **Odbijanje prestupa** *WM97*/*NightShade* lozinkom zaštićuje tekući dokument u petak, 13. u mesecu.
- **Kradja podataka** *Troj*/*LoveLet-A* prosledjuje preko mail-a informacije o korisniku i mašini na jednu adresu na Filipinima.
- **Kvarenje podataka** *XM/Compatable* pravi izmene na podacima u Excellovim tabelama.
- **Brisanje podataka** *Michelangelo* prepisuje delove hard diska 6.marta
- **Onesposobljavanje hardvera** *CIH* ili *Černobil (W95/CIH-10xx)* pokušava da prepiše BIOS 26.aprila, što čini računar neupotrebljivim

3. MERE ZAŠTITE ZA SIGURNIJE KORIŠĆENJE RAČUNARA

3.1 Anti Virusi

Za borbu protiv virusa se koriste **Antivirusi** - programi koji sprečavaju da se vaš računar inficira i koji uništavaju viruse, ako do infekcije ipak dodje!

Antivirus programi sprečavaju zarazu tako sto skeniraju datoteke koje pokrenete u potrazi za kodom (programom unutar programa) i ako nađu kod koji odaje prisustvo virusa, oni zabrane pokretanje zaraženog programa. Datoteke koje su vec zaražene čiste tako sto jednostavno unutar zaražene datoteke brišu kod za koji su sigurni da je virus. Antivirusi imaju bazu kodova virusa koje su proizvođači Antivirusa uspeli da nabave. Ako vam je Antivirus stalno uključen, za ručnim skeniranjem nema potrebe, jer će aktivni Antivirus skenirati svaku datoteku koju pokrenete! Osim sto treba da na svom računaru stalno imate uključen program Antivirus, treba da tom Antivirusu svakog meseca obezbedite najnovije baze podataka o novim virusima, kako bi on otkrivao i nove viruse!

Osim upotrebe anti virus softvera, postoje brojne jednostavne mere koje se mogu preduzeti da bi se zaštitili od virusa i to:

3.2. Ne koristiti dokumente u formatu .doc i .xls

Sačuvajte svoja Word dokumenta u RTF (Rich Text Format) a Excel spredšitove u CSV (Comma Separated Valeus) formatu. Ti formati ne podržavaju makroe pa ne mogu da prenesu makro viruse koji su ubedljivo najčešća pretnja virusima. Tražiti i od drugih da

Vam šalju RTF ili CSV datoteke. Paziti, ipak! Neki makro virusi presreću FileSaveAs RTF i sačuvaju datoteku sa RTF ekstenzijom ali u DOC formatu. Da bi bili potpuno sigurni treba koristiti samo text-only datoteke.

3.3. Ne startovati neproverene i programe ili dokumenta

Ako niste sigurni da je nešto „čisto“ od virusa, pretpostavite da nije. Recite ljudima u svom okruženju da ne bi trebali da download-uju neovlašćene programe ili dokumente, uključujući screensaver-e ili šaljive programe sa Interneta. Uvedita politiku da svi programi moraju biti odobreni od šefa IS i provereni na viruse pre upotrebe.

3.4. Prosleđujte upozorenja samo ovlašćenom licu

Lažna upozorenja su podjednako veliki problem kao i virusi. Tražite od korisnika da ne forward-uju upozorenja na viruse svojim prijateljima, kolegama ili svima iz svog adresara. Uvedite politiku kompanije da sva upozorenja idu samo jednoj imenovanoj osobi ili službi.

3.5. Ako WSH nije potreban, isključiti ga

Windows Scripting Host (WSH) automatizuje neke operacije na Windows računarima ali istovremeno čini računar ranjivim za mail viruse kao što su Love Bug i Kakworm. Ako nije neophodan isključite ga.

3.6. Pratite biltene o sigurnosti softverskih kompanija

Bitan korak u održavanju sigurnosti računara jeste redovno ažuriranje i primena sigurnosnih zakrpa (patches) koje softverske kompanije objavljuju na svojim sajtovima, jer se svakodnevno na Internetu pojavljuju nove i naprednije vrste virusa koje stare baze antivirusa ne prepoznaju.

3.7. Blokirajte nepoželjne tipove fajlova na mail gateway-u

Mnogi virusi danas koriste datoteke tipa VBS (Visual Basic Script) i SHS (Windows scrap object) da bi se širili. Malo je verovatno da treba primati takve datoteke spolja, zato ih najbolje blokirati na gateway-u.

3.8. Promeniti boot sekvencu na računaru

Većina računara prvo pokušava da se podigne sa diskete (A:drive). Informatički personal bi trebao da promeni CMOS setovanje tako da se računari inicijativno podižu sa hard-diska. U tom slučaju, čak i ako se u računaru ostavi zaražena disketa, on ne može da se zarazi boot sektorom virusom. Ako u nekom trenutku zatreba da se podigne računar sa diskete, može se u CMOS podešavanjima vratiti kao što je ranije bilo.

3.9. Zaštiti disketu od upisivanja pre nego što ih damo drugim korisnicima

Disketa koja je zaštićena od upisivanja ne može biti zaražena, jer se na nju ne može ništa upisati.

3.10. Postanite pretplatnik službe za obaveštavanje preko mail-a

Službe za obaveštavanje mogu upozoriti na nove viruse i ponuditi virus identiti datoteke koji će omogućiti da ih anti virus softver detektuje. Nekoliko firmi ima svoje besplatne službe za obaveštenja.

3.11. Redovno praviti *back up* svih svojih programa i podataka

Redovno backup-ovanje bitnih podataka je nešto što bi svaki korisnik trebalo da radi. Najbolji i najjeftiniji način za čuvanje podataka jeste redovno prebacivanje na optičke medije. S obzirom na to da je organizacija datoteka koje treba prebaciti obično prepuštena korisniku, često se događa da on digne ruke od celokupne akcije i prepusti sve „poverenju" u svoje tvrde diskove. To je, nažalost, loša ideja i možda je najbolje jednostavno backup-ovati celu particiju hard diska, čime se znatno olakšava njeno prenošenje na optičke medije. Tako da ako ste inficirani virusom, moći ćete ponovo naći izgubljene programe i podatke pomoću back up softvera.

4. ZAKLJUČAK

Svedoci smo brzog razvoja računara i tehnike, pa samim tim i zaštita od računarskih virusa se mora razvijati u korak sa tehnikom. Kako je danas računar primenjen u svim sferama potrebno je što pre naučiti kako se boriti protiv svih štetnih programa koje virusi donose. U svakom slučaju, viruse, kao i zaštitu od njih, treba shvatiti vrlo ozbiljno, pošto, čak i ako vam nije stalo do vaših podataka, ako niste zaštićeni dovodite u opasnost osobe sa kojima komunicirate e-mail-om ili razmjenjujete programe itd. Iz svega ovoga proizilazi da je najbolja zaštita kupovina anti virus programa, ali i pravilno pridržavanje gore navedenih mera može sprečiti inficiranje računara i širenja virusa.

5. LITERATURA

[1] www.computer viruses /wikipedia
[2] „Zaštita u računarima i računarskim mrežama" Mladen Veinović
[3] *www.sophos.com*
[4] *www.zastita.rs*
[5] *www.apisgroup.org/sec.html?id=7*
[6] *www.sk.rs/2007/09/skin06.html*
[7] *www.sk.rs/2009/03/skpd11.html*