



VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA ČAČAK

SEMINARSKI RAD

Predmet: Informatika

Antivirusni programi

Mentor: _____
Profesor: _____

Student: _____
Br.Indeksa: _____

SADRŽAJ

UVOD	1
1.Što su kompjuterski virusi?	2
2.Podjela virusa	2
2.1.Boot sektor virusi	2
2.2. Infektori datoteka	3
2.3. „Trojanski konj“	3
3.Najčešći virusi i njihova djelovanja	4
4. Zaraženo računalo	4
5.Zaštita računala	5
6.Antivirusni programi	5
6.1.Vrste antivirusnog programa	6
6.1.1.Norton antivirus	6
6.1.2.Sophos antivirus	8
6.1.3. Nod32	8
6.1.4. Panda antivirus titanijum	8
7.Antivirusne metode	8
7.1.Skeneri	8
7.2. CRC skeneri	9
7.3. Blockeri događaja-Behaviour blockers	9
7.4. Imunizatori	9
8.Pokretanje antivirusnog programa u Windowsu	9
9.Šest zlatnih koraka u antivirusnoj zaštiti	10
ZAKLJUČAK	11
LITERATURA	12

UVOD

Informatičkim početnicima je gotovo nemoguće objasniti što je to **virus**. Kompjutorski virusi se zovu virusi jer se nekome nekada činilo da je to pojam koji će neiskusnim korisnicima najlakše predočiti kako se oni šire i kakve su njihove posljedice. Oni pravi virusi se ne vide golim okom, a kompjutorski još manje. Ukratko, kompjutorski virus (u daljnjem tekstu: virus) je neka vrsta programa koji se na neki automatizirani način širi po računalima i radi neku štetu na tim računalima.

“Kompjutorski virus je kompjutorski program koji može inficirati druge kompjuterske programe modificirajući ih na taj način da to podrazumijeva stvaranje svoje vlastite kopije.”¹

Dobro je naglasiti kako nije nužno da taj program mora učiniti nekakvu štetu (kao što je brisanje i oštećenje fajlova) kako bi ga se moglo svrstati u skupinu virusa. Postoji očita razlika između onog što Cohen smatra “virusem” i onog za što bi se većina složila da jest virus.

Bespotrebno zauzima prostor na hard disku ili memoriji (pa tako usporava rad vašeg računala, ili usporava vašu vezu kada ste spojeni na internet), bilo da vam samo izbaci poruku u kojoj vam kaže da ste glupi (pa vas to možda psihički pogodi), bilo da vam briše vaše podatke na računalu, ili ih mijenja (npr. financijske podatke iz siječnja pomiješa nasumice sa kolovozom), ili, možda najgore, pošalje vaše ugovore, slike ili neke tekstove privatne prirode na neku slučajnu e-mail adresu (možda ako nemate sreće i nekome koga poznajete).

Iz ovih spoznaja je jasno da je potrebno uložiti određen napor kako bi ljudi koji koriste računala postali svjesni postojanja virusa i kako ne bi nastavljali s nezainteresiranošću za ovaj problem stvarajući ga tako zapravo još većim.

¹ Fred Cohen, stručnjak za viruse

1. ŠTO SU KOMPJUTERSKI VIRUSI?

Kompjuterski virusi su programi napravljeni s namjerom stvaranja smetnji u radu i različitih oštećenja datoteka i organiziranih podataka na PC računalu.²

Nazvani su tako jer imaju sposobnost razmnožavanja (sami sebe iskopiraju na više mjesta na disku ili disketi).

Prvi virusi su bili programi koji su ispisivali zanimljive, propagandne ili duhovite poruke na monitoru. Nisu bili destruktivni, tako da nije bilo potrebe razvijati neku posebnu zaštitu.

No, stvari su se ubrzo promijenile.

Kasnih 80-tih, računarski virusi bili su dijelovi koda prikačeni na program kao što su bile igre ili tekst procesori. Bili su dizajnirani tako da se izvršavaju kada se pokrene neki od tih programa. Upisivali su se u memoriju i tražili pogodno tlo za širenje.

Ukoliko bi pronašli ono što traže, počeo bi njihov rad koji se može manifestirati na više načina.

Vremenom su tvorci virusa postajali kreativniji, jer su učili nove "trikove". Jedan od boljih bila je mogućnost upisivanja virusa u memoriju, tako da bi ostajao onoliko dugo koliko bi računar bio upaljen. To je virusu omogućavalo masovnije repliciranje. Drugi zanimljiv trik bila je mogućnost inficiranja boot sektora floppy ili hard diska.

To je dio diska koji sistem prvo čita nakon paljenja računara.

Danas je širenje virusa po ovoj osnovi višestruko umanjeno, jer programi za zaštitu od virusa čuvaju boot sektore, a i razmjena programa odvija se putem CD-a ili Interneta.

CD ne može biti modificiran što značajno smanjuje mogućnost širenja virusa. Ipak, ukoliko se podaci prije snimanja na CD ne provjere, postoji šansa da se i virus "snimi" s njim.

2. PODJELA VIRUSA

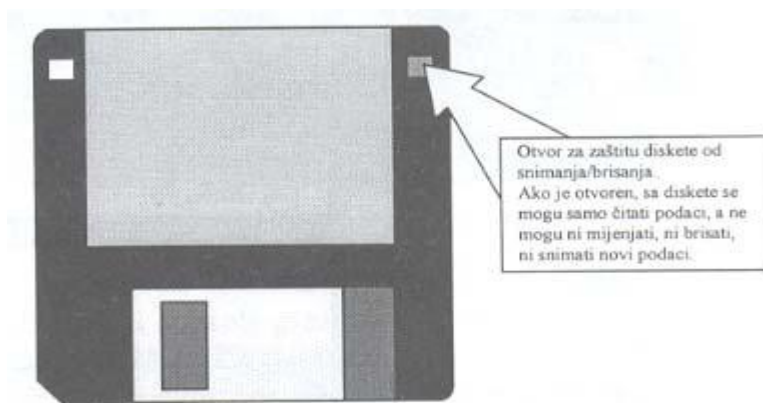
Virusi su podjeljeni u osnovne klase:

- boot sektor virusi,
- infektori datoteka (file infector),
- „trojanski konj“

2.1. BOOT SEKTOR VIRUSI

Boot sektor je dio diska koji sadrži kod za učitavanje operativnog sistema. Virus obriše sadržaj tog sektora i umjesto programa za podizanje sistema snimi sebe. Ako se podigne sistem sa tako zaraženog diska, virus se aktivira i učitava se u RAM memoriju, odakle će zaraziti svaku disketu koja se od tog trenutka bude koristila (osim diskete koja je zaštićena od snimanja).

² Niko Majdandžić, Primjena računala, 1996.g., Slavonski Brod, od 142. do 149.str.



Slika1. Jedina sigurna zaštita diskete od virusa Boot sektor

Boot sektor virusi inficiraju boot sektor floppy ili hard diska.

2.2. INFEKTORI DATOTEKA

Poznati i kao program virusi, generalno se prenose preko fajlova koji su ili izvršni ili sadrže izvršne komponente fajlova i grupirani su prema klasama programa koje inficiraju. Mogu biti izuzetno infektivni i mnogo teže ih je otkriti nego viruse koji napadaju boot sektor zbog širokog obima potencijalnih meta. Mogu se podijeliti na parazitne, pridružene, povezujuće i prepisujuće.

2.3. „TROJANSKI KONJ“

Kompjuterski "trojanski konj" pod maskom stiže putem e-maila, news grupe ili popularnih chat programa do lakovjernih i nedovoljno informiranih korisnika mreže, navodeći ih da ga pokrenu i instaliraju na računar. Za razliku od virusa, trojanci su kompleksne klijent – server aplikacije za pristup udaljenom računar u mreži. Zadatak trojanca je da pronalazi datoteke koje sadrže šifre potrebne za instaliranje na računar, server ili konektiranje na Internet i distribuirati ih udaljenom hakeru. Ovaj program nema u sebi ugrađen kod koji mu omogućuje samostalno razmnožavanje, ali se ipak može razmnožavati ukoliko netko posudi nekome kopiju na kojoj se nalazi ovaj program. Današnji trojanski konji najviše se šire putem peer to peer mreža “pretvarajući” se da su trenutno popularni programi ili crackovi za najnovije uslužne programe.

3. NAJČEŠĆI VIRUSI I NJIHOVA DJELOVANJA

Tablica 1. najčešći virusi i njihova djelovanja

FROM	Boot sektor virus	Porijeklom iz Švicarske, 18. dana svakog mjeseca virus proizvodi zvukove prilikom pritiskanja tipki na tastaturi. Na njega otpada 40% svih infekcija.
NEW ZEALAND (STONED, MARIJUANA) 	Boot sektor virus	Virus ispisuje poruku „LEGALISE MARIJUANA“. Na njega otpada oko 20 % svih infekcija.
TEQUILA 	Svestrani virus	Porijeklom iz Švicarske. Virus na ekranu iscrtava grubi Mandclbort. Oko 10 % infekcija.
SPANISH TELECOM	Svestrani virus	Izrađen u Španjolskoj, Nakon 400 startanja sistema virus prepíše podatke na prva dva tvrda diska. Oko 10% infekcija.
JOSHI	Boot sektor virus	Iz Indije, koji 5. siječnja ispisuje poruku „Happy Birthday Josh“.

4. ZARAŽENO RAČUNALO

Što kad računalo oboli? I uz najveće mjere sigurnosti korisniku se može dogoditi da mu na računalo dospije virus. To se obično događa korisnicima koji nisu primijenili sve mjere sigurnosti, odnosno koji su zanemarili upozorenja. Otkrijete li na vašem računalu virus, posjetite stranice vašeg antivirusnog programa jer se tamo nalaze i detaljne biblioteke s informacijama što virus radi i kako se širi. Isto tako, tamo ćete pronaći i detaljnije upute o tome kako virus ukloniti s računala. U većini slučajeva ovaj ćemo postupak provest

programom za zaštitu od virusa jer on u sebi objedinjava i mogućnosti uklanjanja virusa. No ponekad će trebati detaljno slijediti upute dane na Web stranici i kopije virusa ukloniti ručno. Pri uklanjanju zaraženih i oštećenih zapisa ponekad ćete morati obrisati i neki koristan skup podataka ili dijelove nekog programa. Zbog toga je mudro imati arhive, odnosno sigurnosne kopije kako ne biste izgubili podatke. U slučaju da brišete dijelove programa, njih valja iznova instalirati kako bi se omogućio nesmetan rad programa.

Informatika

Seminarski rad



Slika 2., www.virusi.com

5. ZAŠTITA RAČUNALA

Osnovni oblik obrane od virusa je zaštita računala. Riječ je o dosta složenom postupku koji osim primjene odgovarajućih programa od korisnika zahtijeva i oprezno ponašanje. Osnovna zaštita od virusa na samom računalu provodi se upotrebom programa za borbu protiv virusa. Zajedničkim imenom ovakvi programi se nazivaju **antivirusni programi**. Zamisao je da se na računalo postavi računalni program koji će stalno provjeravati sve zapise koji dopijevaju na računalo. Program u sebi ima podatke koji mu omogućavaju prepoznavanje različitih virusa. Zbog toga će u trenutku kad naiđe na zapis zaražen virusom spriječiti aktiviranje tog zapisa i podići uzbunu. Jednostavno rečeno, na ekranu će se pojaviti prozor s upozorenjem da je određeni zapis zaražen virusom. Pri instalaciji program će od korisnika zatražiti da odredi stupanj zaštite. Najniži stupanj zaštite ne sadrži nikakvu automatiku već korisnik može samostalno pokrenuti provjeru u slučaju kad na računalo donosi neke podatke. Ovakav način rada je izuzetno nesiguran jer korisnik može jednostavno zaboraviti provjeru. Najviši stupanj zaštite zapravo uključuje stalnu provjeru podataka koji se koriste, nadzor nad svim prispjelim elektroničkim porukama i periodičnu provjeru svih podataka na računalu. Ovakav oblik zaštite bez sumnje troši nešto više računalnih resursa. Zbog toga neki autori odbacuju ovakvo rješenje unatoč njegovim očiglednim prednostima. Vrlo je važno naglasiti slijedeće! Bilo koji program za zaštitu od virusa u stanju je prepoznati samo viruse koji su postojali u trenutku njegovog pisanja. Pojavi li se novi virus samo dan nakon što je program izašao, taj je virus programu nepoznat, pa prema tome ne može prepoznati virus, odnosno ne može spriječiti njegovo širenje.

6. ANTIVIRUSNI PROGRAMI

Predstavljaju prvi nivo zaštite od virusa i trojanaca. To su softverski paketi sposobni da detektiraju, izdvoje i (ili) eliminiraju viruse. Svi antivirusni programi sastoje se iz više cjelina. Jedan njegov dio "Monitor" je rezidentan u memoriji i osigurava neprestanu zaštitu od virusa, dok drugi dio "Scan" omogućava skeniranje cijelog sistema. Antivirusi su danas neophodan dio softvera koji svako treba imati instaliran na svom računalu. Ovi programi uključuju različite načine nadgledanja i zaštite računara od malicioznog koda. Najčešće se radi o zaštiti u realnom vremenu i skeniranju na zahtjev korisnika, dok moderne verzije ovih programa nude razne druge vidove zaštite od virusa koji se šire putem Interneta.

Postoji dosta kompanija koje razvijaju i nude ove programe, a najpoznatiji među njima su: Symantec, Sophos, Panda, Kaspersky ... One nude dopunu antivirusnih definicija svakodnevno. Dosadašnja praksa bazirala se na petnaestodnevnom osvježavanju. Broj danas poznatih virusa je oko 65.000, s tim da se opasnim smatra nekoliko stotina. Kvalitetna zaštita svodi se na opreznost, upotrebu dobrih antivirusnih programa, redovno osvježavanje virusnih definicija.

6.1. VRSTE ANTIVIRUSNIH PROGRAMA

Najpoznatiji i najčešće korišteni antivirusni programi su:

- NORTON ANTIVIRUS,
- SOPHOS ANTI-VIRUS,
- MCAFFEE,
- PCCLLIN.

6.1.1. NORTON ANTIVIRUS

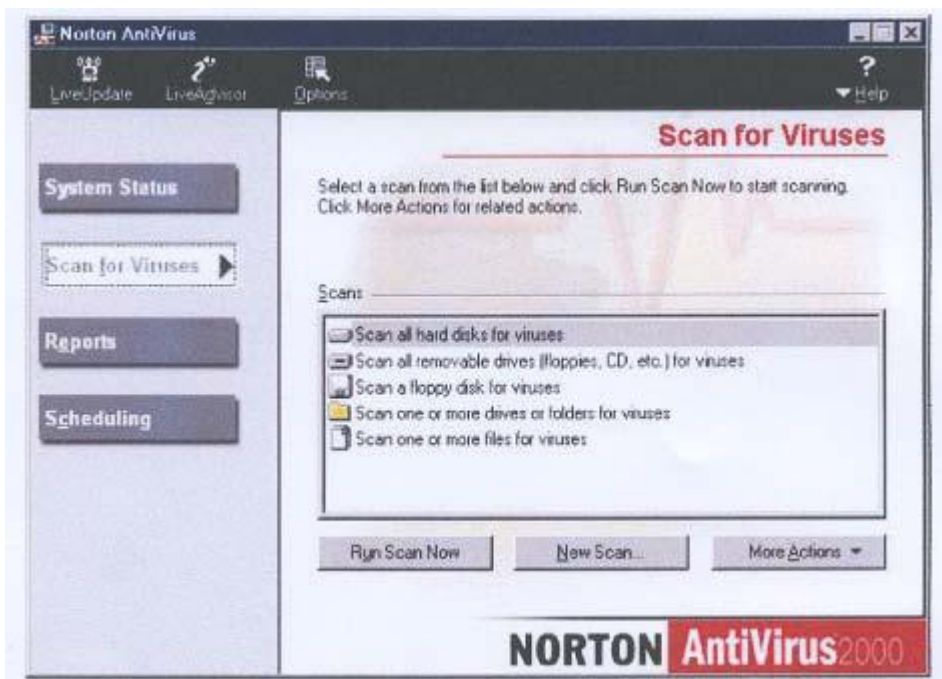
Najpoznatija antivirusna kuća na svijetu Symantec, stekla je svjetsku slavu upravo po proizvodu koji se jednostavno zove Norton AntiVirus, koji je ime dobio po osnivaču firme Peteru Nortonu.

Kupovinom licence stječe se pravo na godinu dana besplatnih osvježavanja antivirus definicija, ali i svih programskih obnova koje se u tom periodu pojave. Za to se brine Live Update koji diskretno svaki put kad se spojimo na Internet, provjeri postoji li nadogradnja za program ili nove definicije.

Korištenje Norton AntiVirus programa

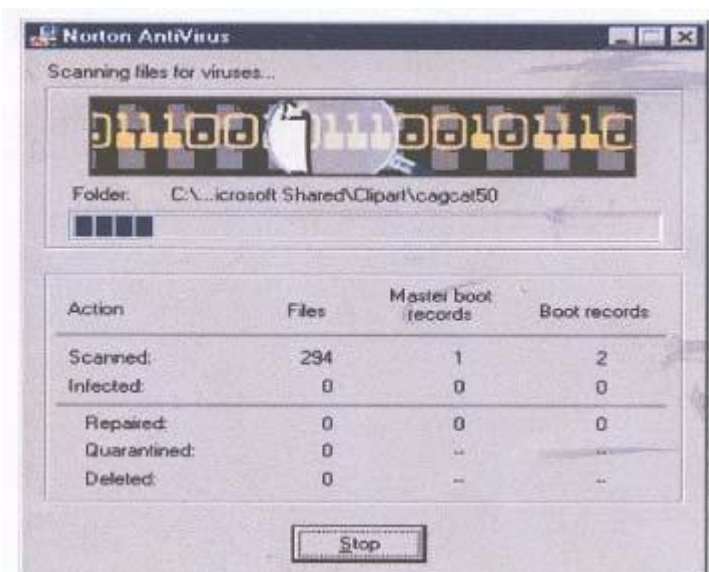
Po završenoj instalaciji i određenom update-u program je spreman za korištenje.

Dopunjavanje baze podataka antivirusnog programa potrebno je iz razloga što se praktično svakog dana pojavi desetak novih virusa. Pokretanjem programa dobije se maska kao na slici 3.



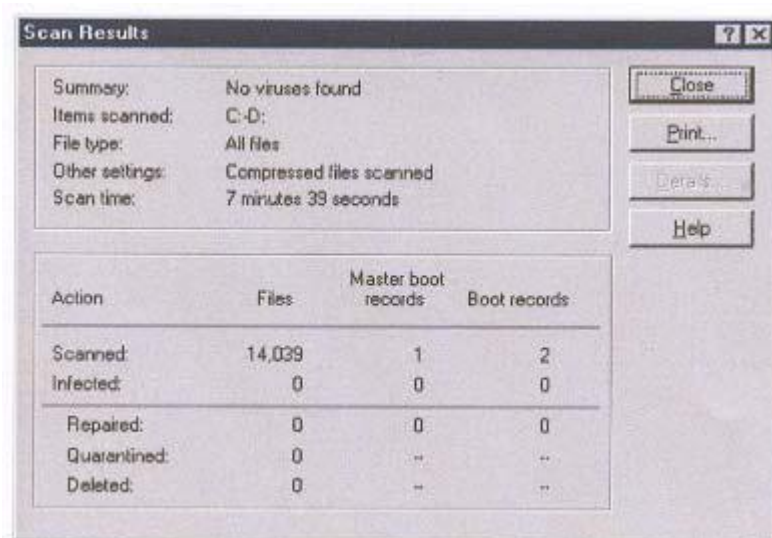
Slika 3. Maska koja se dobije pokretanjem Norton AntiVirus programa

Samo korištenje programa je vrlo intuitivno. Treba označiti što želimo da provjerimo (FD, HD particije ili CD) i pritisnemo New Scan. Program skenira izabrano i to pokazuje na prozoru koji je prikazan na slici 4. Prvo se skeniraju fajlovi na odabranom memorijskom medijumu, a zatim Boot i Master Boot zapis.



Slika 4. Prikaz progressa tokom skeniranja

Nakon završene pretrage, program saopćuje rezultate. Ukoliko se na računaru ne nalazi virus ili trojanac dobije se odgovarajuća poruka. Izgled prozora dat je na sljedećoj slici.



Slika 5. Rezultati pretrage

Ukoliko je pronađen virus ili trojanac dobije se odgovarajuća poruka i korisnik poziva da poduzme odgovarajuću akciju.

6.1.2. SOPHOS ANTIVIRUS

Sophos Antivirus već duže vrijeme čini favorita iz sjenke na sceni "penicilin" alata. Naravno, sjenka je vodećih Norton i McAfee alata koji su ipak za klasu iznad Sophosa.

Za jednostavan program kakav je ovaj mora se proći instalacija koja običnom korisniku

i nije tako jednostavna. Nakon toga će se program smjestiti u memoriju i očekivati neželjene napade virusa.

6.1.3. NOD32

Jedini antivirusni program koji se jasno razlikuje od ostalih je NOD32. NOD32 se pokazao najboljim programom sa jedva uočljivim narušavanjem performansi. Jedan od

dokaza kvaliteta ovog programa su i česte nagrade koje dobiva. NOD32 već je 17 puta

dobio nagradu 100 % Virus Buletina. NOD32, kažu stručnjaci Virus Buletina, "nikad nije propustio niti jedan virus, dok se drugim alatima dogodilo da ih propuste".

Za instalaciju ovog antivirusnog programa potreban je mali prostor, tako da ostaje dovoljno prostora za ostale programe. Antivirusni alat NOD32 odlikuje se preglednim grafičkim sučeljem. Za detekciju virusa potrebno je tek odrediti područje skeniranja, definirati akciju koju će program izvršiti kada pronađe virus i u Setup opcijama odrediti način rada.

6.1.4. PANDA ANTIVIRUS TITANIJUM

Panda Titanijum je automatizirani i ne previše zahtjevnii eliminator virusa, sa naglaskom na praktičnost i jednostavnost upotrebe. Sadrži sve opcije neophodne za kvalitetnu protekciju računara i elegantno podešavanje mogućnosti. Namijenjen je kućnim korisnicima i svima sa slabijim konfiguracijama.

7.ANTIVIRUSNE METODE

7.1. SKENERI

Princip rada antivirus skenera bazira se na provjeravanju datoteka, sektora i systemske memorije u potrazi za poznatim i nepoznatim malicioznim kodom. Potraga za poznatim virusima naziva se maskiranje (masking). Virus "maska" je specifični dio koda sadržan u virusu. Ako neka datoteka ne sadrži masku (taj dio koda) ili je veličina maske nedovoljna, koriste se druge metode za pronalaženje virusa. Heurističko skeniranje je analiza dijela instrukcija u kodu datoteka koje se provjeravaju, za koje postoji mogućnost da je maliciozni kod. Na ovaj način pronalaze se još uvijek neotkriveni virusi.

Skeneri se dijele u dvije kategorije: opći (general) i specijalni (special). Generalni skeneri su dizajnirani da pronađu i onemoguće sve vrste virusa za određeni tip operativnog sistema dok specijalni pronalaze ograničen broj virusa ili određene tipove virusa, recimo makro viruse.

Skeneri se još dijele na rezidentne i nerezidentne (provjeravaju sistem samo ako se to

traži od njih). Rezidentni pružaju sistemu bolju zaštitu, jer reagiraju odmah po pojavi

virusa, dok nerezidentni detektiraju virus tek kad bude pokrenut.

7.2. CRC SKENERI

CRC skeneri djeluju tako što kalkuliraju sa CRC sumama za tekući disk, datoteku ili sistem sektora. CRC sume sadrže bazu podataka sa podacima kao što su veličina

datoteka, datum i sl. Oni uspoređuju informaciju sa bazom i kontroliraju vrijednosti.

Ako

su podaci u bazi različiti od onih koje je skener pronašao, ukazuje na mogućnost postojanja virusa na računaru.

CRC skeneri koriste moćne anti – stealth algoritme u borbi protiv virusa i često se zna desiti da virusi mogu biti detektirani samo ovom metodom. Problem kod ove vrste skenera je što ne mogu registrirati postojanje virusa u trenutku inficiranja sistema, jer još uvijek nisu napravljene potrebne izmjene u *sis* datotekama. CRC skeneri ne mogu detektirati postojanje virusa u pristiglim datotekama, kao što su e-mail, diskete, vraćene backup datoteke, raspakovane arhive i sl., jer njihova baza nema podatke o njima.

7.3. BLOKERI DOGAĐAJA – BEHAVIOUR BLOCKERS

Anti – virus blokeri događaja su memorijski rezidentni programi koji "osluškuju" reakciju virusa i obavještavaju o tome korisnika. Takve informacije mogu se dogoditi za

vrijeme pokretanja izvršnih datoteka, zapisivanje u Boot sektor diskova ... Dobra osobina blokera je što zaustavljaju izvršavanje virusa u trenutku infekcije, a loša je što

vrlo često griješe.

7.4. IMUNIZATORI

Dijele se u dva tipa: one koji upozoravaju na infekciju i one što blokiraju pokušaj virusa

da uđe u sistem.

Prvi tip se i sam ponaša kao virus, tako što se dodaje na kraj datoteke i pri svakom njenom pokretanju provjerava izmjene. To uradi samo jedanput.

Drugi tip ove metode štiti sistem na način da mijenja datoteke i praktično uvjerava virus

da su te datoteke zaražene. Za zaštitu od rezidentnih virusa koristi se mali TRS (rezidentni) program koji je ubačen u memoriju računara. On također nastoji uvjeriti virus (ako pokuša pristupiti memoriji), da je memorija već zaražena. Ova metoda nije

potpuno pouzdana, jer je nemoguće zaštititi sve datoteke od svih mogućih virusa.

8. POKRETANJE ANTIVIRUSNOG PROGRAMA U WINDOWSU

Iz Microsoft Tools skupine potrebno je dvaput kliknuti na Anti-virus ikonu ili iz tools izbornika File Managera izabrati Anti-Virus naredbu. Na zaslonu se prikazuje Microsoft Anti-Virus for windows. Mogućnosti i naredbe izbornika imaju istu funkciju kao i isto imene mogućnosti u DOS verziji programa.

Ako nakon izbornika Detect mogućnosti anti-virus otkrije virus, na zaslonu se prikazuje poruka o pronađenom virusu. Izaberemo jednu od opcija.

Clean za uklanjanje virusa

Continue za nastavak pregledavanja

Informatika

Seminarski rad

Stop Za prestanak pregledavanja

Delete Za brisanje inficirane datoteke

Nakon završetka pregledavanja memorije računala i izabranog diska na zaslonu se pokazuje statusne informacije.

9. ŠEST ZLATNIH KORAKA U ANTIVIRUSNOJ ZAŠTITI

Korak 1:

Obavezno instalirati neki od antivirusnih alata!

Iako ne postoji apsolutna zaštita od virusa, instaliranjem i pravilnim podešavanjem nekih od ovih programa znatno se reducira mogućnost zaraze.

Korak 2:

Redovno ažurirati antivirusne definicije.

Podesiti alate da redovno automatski "skidaju" najnovije virusne definicije. Ako antivirusni program ne podržava automatsko osvježavanje (što je malo vjerovatno), onda se to učini ručno sa site-a proizvođača.

Ovaj korak je jako bitan jer se dnevno pojavi oko trinaest novih virusa.

Osvježavanjem

baze dajemo mogućnost antivirusnom alatu da štiti računar od većeg broja virusa.

Korak 3:

Podesiti antivirusni softver da automatski skenira sve datoteke.

Provjeravanjem svih datoteka, ne sami izvršnih, zaštita je potpuna i time se onemogućava širenje virusa. Potrebno je obratiti pažnju da se uključi skeniranje kompresnih datoteka (opcija Scan Compressed Files).

Korak 4:

Skenirati sve datoteke koje dolaze sa Interneta.

Prije svega, obavezno se uključi skeniranje svih odlaznih i dolaznih e-mail poruka. E-mail

je trenutno najčešći način širenja virusa. Također mnogobrojne web stranice sadrže softvere koji mogu biti zaraženi. Zato će i skeniranje svih datoteka kopiranih sa interneta pomoći u zaštiti.

Korak 5:

Povremeno skenirati cijeli disk.

Redovno vršiti skeniranje cijelog diska. Proces skeniranja može potrajati i zavisi od veličine hard diska i broja datoteka kojima raspolaže. Zato nije lože ostaviti računar da skenira tokom noći.

Korak 6:

Skenirati hard disk nakon instalacije softvera.

Nakon instalacije raznih alata (posebno onih koji se kopiraju sa interneta) skenirati hard

disk ili lokacije na koje se softver instalirao. Može se desiti da kompresovane arhive budu zaražene virusima.

ZAKLJUČAK

U današnje vrijeme je gotovo nezamisliv rad na računalu bez zaštite od virusa koje možemo dobiti otvaranjem bilo koje stranice na internetu. Potrebno je imati dobre antivirusne programe kako se ne bi doveli u situaciju da pokupimo raznorazne viruse koji bi obrisali važne datoteke ili nam srušili sistem.

Danas se sva poslovanja vode preko računala i nedopustiv je rizik da se dovedemo u situaciju prekida poslovanja na određeno vrijeme. To nam ne dopušta današnji način života.

Potrebno je redovito obnavljati antivirusne programe jer svakog dana nastaju milijuni novih virusa.

LITERATURA:

- Majdandžić, N., Primjena računala, Slavonski Brod, 1996.g., 142.-149.str.
- Ladislav Krasny, Članak u časopisu "INFO" Br-522/00, str.43-55.str.
- <http://www.cg.yu/zaštita/trojanci.html>
- <http://www.mcafee.com>
- <http://www.sophos.com>

Gotovi seminarski, maturski, maturalni i diplomski radovi iz raznih oblasti, lektire , puškice, tutorijali, referati - specijalizovan tim za usluge visokokvalitetnog pisanja, istraživanja i obradu teksta za kompletan region Balkana.

Posetite nas na sajtovima ispod:

WWW.MATURSKIRADOVI.NET

WWW.SEMINARSKIRAD.ORG

WWW.MATURSKI.NET

WWW.MATURSKI.ORG

WWW.SEMINARSKIRAD.INFO

Dostupni smo Vam 24h 365 dana u godini.

Za gotove verzije rada obratiti se na mail:

maturskiradovi.net@gmail.com

061/ 11-00-105

Seminarski, diplomski, maturski radovi, prevodi na engleski i eseji...