*PEDAGOŠKI FAKULTET U ZENICI* *Škol. god. 2002/03*

*MATEMATIKA I INFORMATIKA*

***SEMINARSKI RAD IZ INFORMATIKE***

# - Kompjuterski virusi –

**Student:**
**Arnaut Rabija**

**Asistent:**
**Mr. Samir Lemeš**

***SADRŽAJ***

# *- UVOD -*

Stručnjak za viruse, Fred Cohen je kroz svoja istraživanja, doktorsku disartaciju i različite publikacije praktički zasnovao novu znanost o virusima. On je razvio teoretski, matematički model o ponašanju kompjuterskih virusa. Cohenova formalna definicija (model) ne bi se mogla tako jednostavno prevesti iz matematičkog na obični jezik ljudi, ali njegova skraćena definicija otprilike glasi: "Kompjuterski virus je kompjuterski program koji može inficirati druge kompjuterske programe modificirajući ih na taj način da to podrazumjeva stvaranje stvaranje svoje vlastite kopije."

- Problem sa Cohenovom skraćenom definicijom je što ona ne obuhvaća mnogo karakteristika koje daje njegov matematički model. No, na drugu stranu, koristeći Cohenov formalni model, on neke stvari svrstava u viruse koje nitko ne bi smatrao virusom npr. program DISKCOPY.
- Većina od nas bi se složila sa ovakvom definicijom virusa: "Kompjuterski virus je program koji ima mogućnost razmnožavanja, a sadrži kod koji kopira sam sebe i tako može "zaraziti" druge programe modificirajući njih ili njihovu okolinu na taj način da poziv inficiranog programa zapravo upućuje na izvršavanje moguće kopije virusa."
- Većina ljudi koji se bave računarima, koriste termin "virus" za svaku vrstu programa koji pokušava sakriti svoju destruktivnu funkciju i / ili se pokušava razmnožiti na što je više moguće računara, iako bi se neki od tih programa mogli nazvati "crvima" (worms) ili "Trojanskim konjima" (Trojan horses).

Ovi programi su zapravo veoma ozbiljna stvar, razmnožavaju se brže nego ih se pronalazi i zaustavlja. Najbezazleniji virus može biti stvarna životna prijetnja.
Npr. u slučaju neke bolnice i kompjuterskog sistema koji održava i prati životne funkcije pacijenta, virus koji bi "jednostavno" zaustavio računalo i nebi učinio ništa drugo osim pokazao bezazlenu poruku na ekranu i čekao dok netko ne pritisne neku tipku zapravo bi mogao uzrokovati fatalan kraj za pacijenta.
Oni koji razvijaju viruse ni sami ne mogu zaustaviti njihovo širenje pa čak ukoliko bi i sami to željeli.
Kompjuterski virusi su zapravo poseban slučaj nečega poznatog pod nazivom "bolesna logika" (malicious logic) ili malware.

## *1. ŠTA SU KOMPJUTERSKI VIRUSI?*

***Kompjuterski virusi*** su mali programi koji imaju za cilj nanošenje štete tj. zloupotrebu. Nazvani su tako jer imaju sposobnost razmnožavanja (sami sebe iskopiraju na više mjesta na disku ili disketi).
Prvi virusi su bili programi koji 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 promjenile.

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 manifestovati 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 floopy 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 modifikovan 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.

### *1.1. Aktiviranje kompjuterskih virusa*

Svaki postupak u računaru provodi se izvršavanjem nekog programa. Savremeni računari mogu izvršiti širok spektar programa za različite namjene i pri tome je moguće odjednom pokrenuti i koristiti i više od jednog programa. Namjena nekog programa određena je u trenutku njegova pisanja, što omogućava da se osim korisnih programa napišu i štetni, odnosno opasni programi koji će zapravo uništavati podatke ili na neki drugi način oštetiti informacije na računaru.
Korisnik pokreće ove programe nesvjesno i potpuno neprimjetno. Na ekranu se ne pojavljuju nikakve informacije o tome da je program pokrenut niti će podatak o tome na bilo koji način biti vidljiv korisniku. Korisnik će djelovanje ovog programa primjetiti tek po posljedicama, odnosno nakon što je šteta već počinjena.
Virus se ne mora odmah aktivirati, nego može biti tempitan na tačno određeni datum, dan u sedmici, vrijeme ili kad se ispuni neki drugi uvjet. U novije vrijeme jako je porasla upotreba Interneta pa su se razvili i novi postupci širenja virusa. Danas se u tu svrhu uglavnom koriste različite slabosti i pogreške u sigurnosnim sustavima računara pa se virusi šire uz zapis koji se prenosi Internetom kao dodaci uz elektroničku poštu i slično.
Bez obzira na način dopremanja zaraze, sam virus u pravilu će se ponašati na sličan način. Obično će prvo zaraziti računar na koji je dospio i zatim ući u fazu razmnožavanja. U tom periodu koristit će različite postupke prijenosa informacija kako bi sa zaraženog računara dospio na druge. Za vrijeme tog perioda neće korisniku činiti nikakvu štetu kako bi ostao neopažen. Tek nakon nekog vremena širenja program će postići punu funkcionalnost, odnosno učiniti štetu.

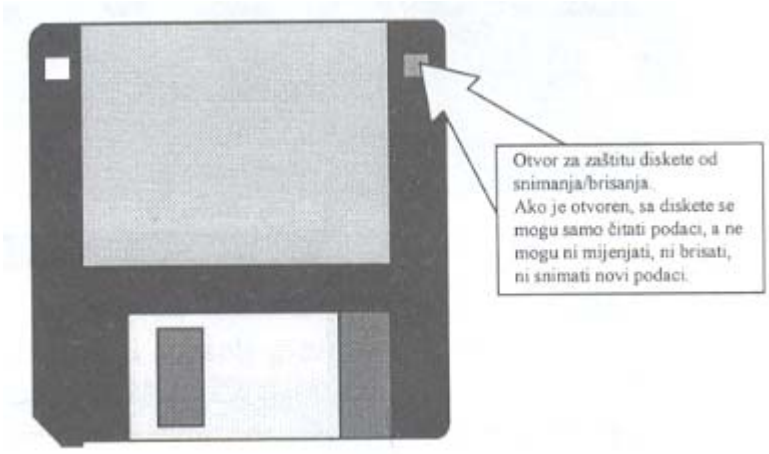
# 2. KLASE VIRUSA

Nakon godina evolucije i razvijanja alata za zaštitu od virusa, te sve više stečenog znanja o njima od strane kompanija koje ih proizvode, virusi su podjeljeni u osnovne klase:

- boot sektor virusi,
- infektori datoteka (file infector),
- makro virusi i
- Internet virusi.

## 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 učita se u RAM memoriju, odakle će zaraziti svaku disketu koja se od tog trenutka bude koristila (osim diskete koja je zaštićena od snimanja).




Slika1. Jedina sigurna zaštita diskete od virusa

Boot sektor virusi inficiraju boot sektor floopy ili hard diska, a u mogućnosti su inficirati i Master Boot Record (MBR) korisničkog hard diska. Najčešće mjenjaju orginalni sadržaj MBR-a sadržajem virusnog koda da bi se virus učitao u memoriju prilikom paljenja računara. Eliminisanje boot sektor virusa vrši se isključivo bootanjem računara preko "čiste" sistemske diskete ili CD-a koji sadrži alat za uklanjanje virusa.

### *2.2. Infektori datoteka*

Poznati i kao program virusi, generalno se prenose preko fajlova koji su ili izvršni ili sadrže izvršne komponente fajlova i grupisani 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 podjeliti na *parazitne, pridružene, povezujuće i prepisujuće.*
Svaki fajl virus može sadržati različite tehnike za poboljšanje brzine širenja ili za izbjegavanja otkrivanja.

***Parazitni virusi***
Čine većinu od svih fajl virusa i šire se tako što modifikuju kod izvršnog programa. Oni se kače na izvršni fajl i mijenjaju njegov sadržaj tako da se aktiviraju čim operativni sistem pokuša da izvrši inficirani program.

***Pridruženi virusi***
Koriste sistemske osobine DOS-a vezane za sekvencu učitavanja i izvršavanja programa. Oni ne modifikuju inficirani program i obično prolaze kontrolu orginalnog EXE – fajla ali kada se jednom detektuju laki su za čišćenje.

***Povezujući virusi***
Inficiraju program tako što mijenjaju informaciju u strukturi direktorijuma i modifikuju poentere fajlova, tako da se svaki inficirani program startuje sa iste lokacije koja sadrži kod virusa.

***Prepisujući virusi***
Prepišu dio inficiranog fajla tako da on više nije operativan. To ih čini prilično primjetnim, tako da se rijetko dešava da se daleko prošire.

### *2.3. Macro virusi*

Macro virusi su "mini – programi" napisani u nekom internom programskom jeziku (skript – language ili macro – language) nekog aplikativnog programa kao što je to WORD, EXCEL, itd. Ovi virusi tipično pisani da se razmnožavaju unutar dokumenata kreiranih tom aplikacijom. Mogu se proširiti i na druga računala ukoliko se na oba računara koristi dotična aplikacija i vrši se razmjena inficiranih dokumenata. Macro – virusi mogu se izvršavati na svakoj platformi na kojoj postoji ovakav program ( i pripadajući interni jezik). Oni nisu ograničeni na pojedinačna računala ili samo određeni operativni sistem.

### *2.4. Internet virusi*

***E-mail virus*** se kreće u sklopu e-mail poruka i najčešće se replicira automatski putem adresa koje se nalaze u adresaru (Address Book). Najpoznatiji virus ovog tipa bio je virus *Mellisa* iz marta 1999 godine. Širio se pomoću MS Word dokumenata poslanih putem e-maila. Nastao je tako što je neko na Internet news grupu presnimio Word dokument. Tko je god kopirao i otvorio dokument, povukao je i virus. Virus je inficirao

*Noral.dat* datoteku i prilikom slanja uzimao je 50 prvih adresa i slao im inficirani dokument. Nakon virusa Melissa, virus *I love you* se pojavio u maju 2000. sadržao je mali dio koda i zakačku za e-mail. Virus se izvršavao dvostrukim klikom na zakačku. Cijela koncepcija bila je bazirana na ljudskoj znatiželji, neopreznosti i želji da se pregleda "ljubavna poruka".

# *3. WORM (CRV) I TROJANSKI KONJ*

## *3.1. Worm*

Worm je mali računarski program koji koristi računarsku mrežu i sigurnosne propuste da se replicira sa računara na računar. Najčešći način širenja crva je putem e-maila ili IRC kanala. Kao uslov replikacije neophodna je računarska mreža (obično Internet). Koristeći se njom, program pretražuje mrežu i pronalazi računare sa specifičnim sigurnosnim propustima. Dalje se sam kopira na drugu mašinu, sve dok ne bude otkriven i uklonjen.
Postoje dvije vrste crva: crv na domaćinskom računaru (HOST WORM) i mrežni crv (NETWORK WORM).
*HOST WORM* se cjelokupan nalazi i izvršava na domaćinskom računaru, a vezu s mrežom koristi samo za svoje razmnožavanje na druge računare. Ovaj tip crva nakon što pokrene svoju kopiju na novom inficiranom računaru samostalno uništava svoju prvobitnu kopiju. Na taj način u određenom trenutku negdje na mreži uvijek se nalazi samo jedna kopija tog crva. Ovaj tip crva naziva se još i "zec" (RABBIT) upravo zato što stalno bježi uokolo mrežom.
*Mrežni crv (NETWORK WORM)* sastoji se od više dijelova, segmenata, od kojih se svaki pokreće na različitom računaru u mreži i najčešće svaki segment obavlja različitu funkciju koristeći mrežu samo za određene komunikacijske svrhe. Mrežni crv koji ima jedan glavni segment koji koordinira radom ostalih segmenata na mreži naziva se još i "hobotnicom" (OCTOPUS).
19. jula 2001 godine pojavio se worm *Code Red* koji se za nepunih devet sati replicirao 250.000 puta. Napao je Windows platformu, i to NT i 2000 servere na kojima su se "vrtili" Internet Information Server-i. Karakteristika crva je da pored standardne replikacije, nanose dodatno zlo. *Code Red* se replicirao prvih 20 dana u mjesecu, mjenjao sadržaj web sajtova na inficiranim serverima stranicom pod nazivom Hacked by Chinese. *Code Red* je usporavao Internet saobraćaj kada bi se replicirao. Svaka kopija provjerava da li WINDOWS NT ili WINDOWS 2000 server ima instalisanu sigurnosnu zakrpu i ukoliko ustanovi da nema – kopira se na njega. Ta nova kopija radi isto što i orginal, sve dok ne bude otkrivena i uklonjena.

### *3.2. Trojanski konj*

Trojanci su svoje ime dobili prema čuvenom epu o opsadi Troje, koju su grci bezuspješno napadali 10 godina i na kraju se povukli ostavljajući pred njenim ulazom ogromnog konja kao znak priznavanja poraza.Trojanski ratnici su oduševljeno konja uvukli unutar grada i posvetili su se proslavljanju svoje velike pobjede. Međutim, kada su svi zaspali pijani, na konju su se otvorila dobro skrivena vrata i iz njega je izašao odred grčkih ratnika koji su otvorili vrata tvrđave, puštajući unutra ostale grke, koji su povlačenje iscenirali i čekali na taj trenutak... Nakon toga Troju su veoma lako zauzeli.
Potpuno je pogrešno trojance zvati virusima, zato što su oni kompletne aplikacije i ne šire se kao virusi. Trojanski konji se mogu ukloniti brisanjem njihovog fajla iz određenog direktorijuma, za razliku od virusa koji su obično zakačeni za druge datoteke i ubacuju se u memoriju. Većina njih nije sama po sebi destruktivna ali zato omogućuje bilo kome na Internetu da upravlja vašim kompjuterom ili mu šalje vaše lozinke itd., tako da to kolika će nam šteta biti nanjeta zavisi samo od onoga ko se domogao podataka.
Kompjuterski "trojanski konj" pod maskom stiže putem e-maila, news grupe ili popularnih chat programa do lakovjernih i nedovoljno informisanih korisnika mreže, navodeći ih da ga pokrenu i instaliraju na računar. Za razliku od virusa, trojanci su kompleksne klijent – server aplikacije za pristup udaljenom računaru u mreži. Server se nalazi na računaru žrtve i to je sam trojanac, dok je klijent program pomoću koga se njime upravlja. Klijent se nalazi na računaru osobe koja namjerava da dođe do bitnih informacija sa računara žrtve. Zadatak trojanca je da pronalazi datoteke koje sadrže šifre potrebne za instaliranje na računar, server ili konektovanje na Internet i distribuira ih udaljenom hakeru. Osoba koja kontroliše trojanca na računaru žrtve u mogućnosti je potpuno preuzeti kontrolu nad njim. U tom trenutku jedino rješenje je fizičko gašenje računara ili nasilni prekid Internet konekcije. Trojanci su u mogućnosti dobro sakriti kod i iskoristiti mnoštvo sigurnosnih propusta u e-mail klijentima. Većina trojanaca instalira se u *Start Up* grupu Windows-a.Pregledanje tog foldera može pospješiti zaštitu računara.
Najefikasniji način zaštite od trojanaca je instaliranje *firewall* sistema ili jednostavno ne otvaranje poruka od nepoznatih osoba.
Najpoznatiji trojanac je svakako *Back Orifice*, koga je samo za mjesec dana preuzelo i koristilo skoro 100.000 ljudi na Internetu. On izgleda kao obična klijent – server aplikacija za rad na udaljenom računaru sa izuzetkom što se server, tj. sam trojanac, instalira bez pitanja, kao virus, kada startujete zaraženu aplikaciju i omogućava svakome ko dođe do vašeg IP broja da preuzme kontrolu nad računarom. Pored BO-a poznati su još *NetBus*, *Millenium* itd.

# *4. ANTIVIRUSNI PROGRAMI*

Predstavljaju prvi nivo zaštite od virusa i trojanaca. To su softverski paketi sposobni da detektuju, izdvoje i (ili) eliminišu viruse. Svi antivirusni programi sastoje se iz više cjelina. Jedan njegov dio "Monitor" je rezidentan u memoriji i obezbjeđuje 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 računaru. 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, stim da se opasnim smatra nekoliko stotina. Kvalitetna zaštita svodi se na opreznost, upotrebu dobrih antivirusnih programa, redovno osvježavanje virusnih definicija.

## *4.1. Vrste antivirusnih programa*

Najpoznatiji i najčešće korišteni antivirusni programi su:

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

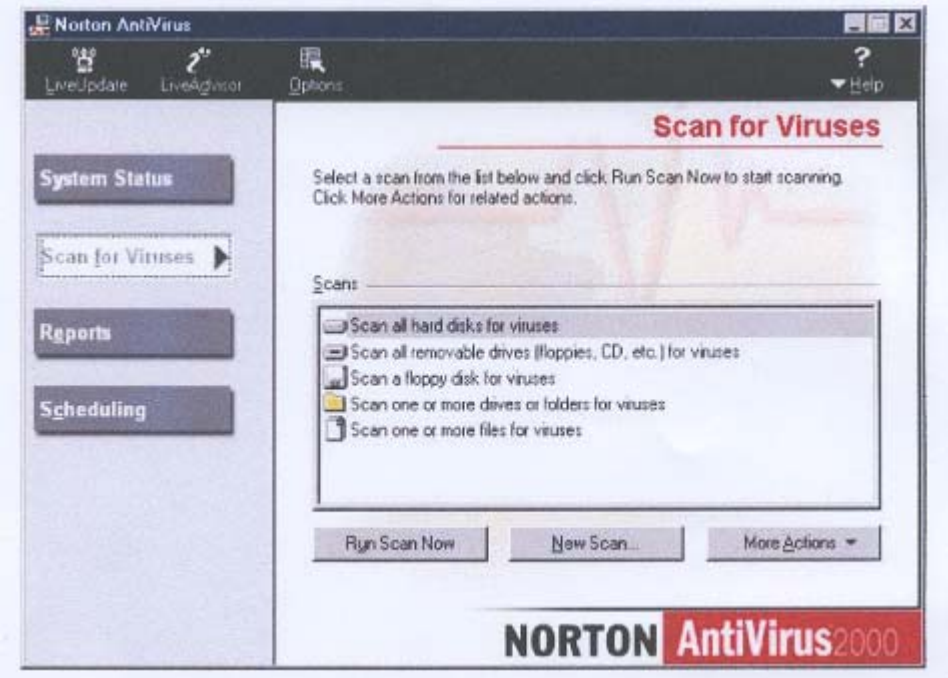
### *4.1.1. NORTON ANTI – VIRUS*

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*. Ovaj proizvod, namjenjen desktop računarima, kućnim korisnicima sada se izbacuje na godišnjoj osnovi. Svake godine predstavlja se nova verzija sa više ili manje napretka u odnosu na prethodne.
Verzija 2000 najviše se razlikovala od prethodnika dok su verzije 2001 i 2002 tek njeni nešto napredniji nasljednici. Verzija 2002 odlikuje se jednostavnom i automatizovanom upotrebom i lakim obnavljanjem virusnih definicija. Verzija 2002 je prvi antivirus alat koji je dobio logo *"Designed for Windows XP"*, a ujedno i jedina verzija Norton Anti-Virusa koja radi na XP-u.
Norton AntiVirus 2002 je pun korisnih opcija. Posebna pažnja posvećena je skeniranju e-mail poruka kako dolaznih tako i odlaznih (da se zaraza ne bi širila) jer se u posljednje vrijeme 90 % virusa širi upravo e-mailom. 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. Ovaj antivirusni program posjeduje ogromnu bazu virusa koje može prepoznati i uz mogućnost prepoznavanja novih virusa pomoću *Bloodbound* tehnologije. Viruse koje ne može otkloniti otpremit će u karantin, gdje će čekati nove antivirus definicije ili nadogradnju programa, kako bi se ponovo pokušalo sa popravkom.

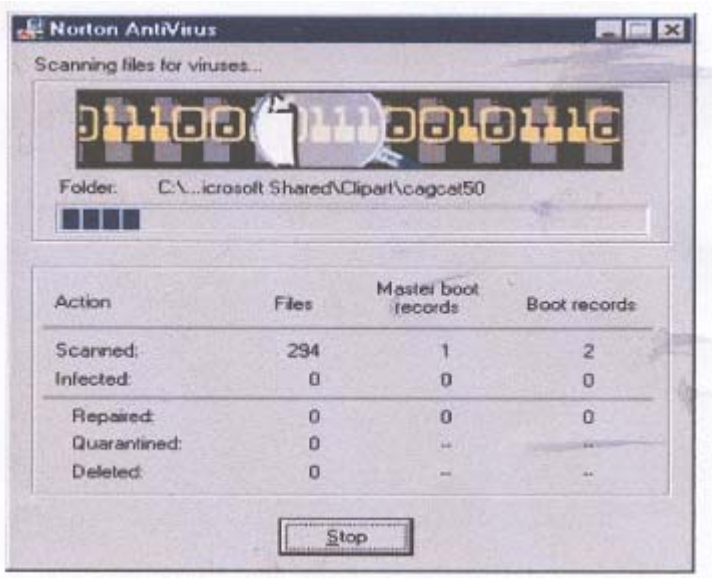
### *Korištenje Norton Anti – Virus programa*

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. Pokretajem programa dobije se maska kao na slici 2.



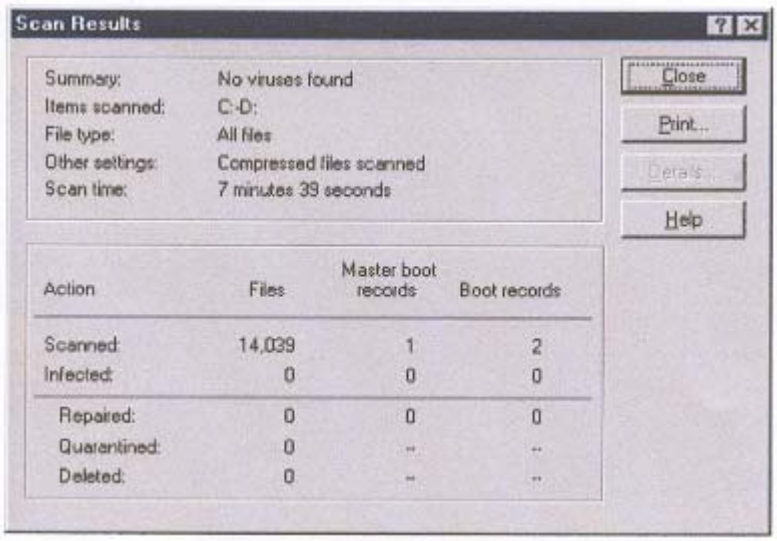

Slika 2. Maska koja se dobije pokretanjem Norton AntiVirus programa

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 3. Prvo se skeniraju fajlovi na odabranom memorijskom medijumu, a zatim *Boot* i *Master Boot* zapis.




Slika 3. Prikaz progresa tokom skeniranja

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




Slika 4. Rezultati pretrage

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

### *4.1.2. SOPHOS ANTI – VIRUS*

*Sophos Anti – Virus* već duže vrijeme čini favorita iz sjenke na sceni "pencilin" alata. Naravno, sjenka je vodećih Norton i Mcaffee 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.
Potraga za virusima može se podjeliti na dvije vrste. Jedna od njih je ona koju sam korisnik zahtjeva u slučaju da posumnja na infekciju – skeniranje. Druga je automatska, koju program obavlja u pozadini. Ova druga vrsta se zasniva na pregledu datoteka kojima operativni sistem trenutno pristupa tj. svih datoteka koje u bilo kom momentu mogu biti potencijalna opasnost.
Pregled je zasnovan na *Sophos InterCheck* tehnologiji, koji ima i klijent – server podršku preko lokalne mreže. Tada se na jednom serveru datoteke sa Sophos server instalacijom čuvaju informacije o aktivnostima klijentskih Sophos aplikacija i eventualnim pronađenim virusima, čime se povećava mrežna sigurnost. Naravno tu su i one standardne mogućnosti poput pregleda velikog broja različitih datoteka, planiranje redovnih pregleda itd.
Što se tiče instaliranja novih definicija virusa, ne postoji mehanizam automatske nadgradnje, nego to korisnik mora uraditi ručno, preko web sajt proizvođača. Sophos kao kvalitetan antivirusni alat ima mnogo opcija ali je ipak neodređen.

### *4.1.3. 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 Bulettina*. NOD32, kažu stručnjaci *Virus Bulettina*, "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.
Nakon što su određene osnovne postavke skenira se stroj akcijom *Scan*, odnosno očisti naredbom *Clean*. Pri skeniranju će memorije NOD32 detektirati viruse, crve i trojance; osim toga neće zaobići niti arhive (zip, rar, arj, ...). Osim osnovnih postavki, NOD32 ima i integrirani Kontrolni centar koji se brine za ažuriranje kompletnog NOD32 sistema. Kontrolni centar provjerava da li se pojavio novi update, i to u vremenskim intervalima koje odredi sam korisnik, nakon čega automatski ažurira bazu podataka. Osim Kontrolnog centra NOD32 sadrži i maleni program Amon koji je "pristupni skener za Windows 95, 98, ME, NT, 2000, i XP platforme", a koji spriječava otvaranje i

pokretanje zaraženih datoteka, skenira disketnu jedinicu prilikom otvaranja i gašenja, šalje obavijest o zarazi putem e-maila i automatski se aktivira kod pokretanja sistema.
Sam NOD32, osim dobrom detekcijom virusa, odlikuje se i brzim radom. To je jedan od najbržih antivirusnih alata koji se trenutno nalaze na tržištu. Prosjek ostalih antivirusnih alata je 825 sekundi, dok NOD32 to obavlja za 135 sekundi (*Scan Rate*).

### *4.1.4. PANDA ANTIVIRUS TITANIJUM*

*Panda Titanijum* je automatizirani i ne previše zahtjevni eliminator virusa, sa naglaskom na praktičnost i jednostavnost upotrebe. Sadrži sve opcije neophodne za kvalitetnu protekciju računara i elegantno podešavanje mogućnosti. Namjenjen je kućnim korisnicima i svima sa slabijim konfiguracijama. Kompanija *Panda Software* osnovana je 1990 god. i do sada je postigla dobre rezultate na polju mrežnih rrješenja.
Panda se nakon instalacije smješta u memoriju, odakle djeluje nevidljivo, a pritom minimalno zauzima memorijske resurse. Svoju djelatnost koncentriše na datoteke koje se na određeni način mijenjaju (kopiranje, otvaranje, snimanje iz pojedinih programa i sl.). Korisnik po želji može pokrenuti skeniranje sistema, što se radi preko tzv. Pretraživača (*Search Engine*). Na njemu se bazira skeniranje nazvano *UltraFast*, koje predstavlja srce softvera. Osvježavanje antivirusnih definicija je automatizirano – sa svakim konektovanjem na Internet softver ih automatski ažurira. Tehnologija *SmartClean* namjenjena je opravljanju grešaka na sistemu uzrokovanih trojancima ili crvima. Kada trojanski kon ili crv "upadnu" na računar, ne inficira samo datoteke, već pokušava da se sakrije u memoriji i poremeti funkcioniranje sistema. *Modul Internet Scan* pazi na podatke koji struje Internetom, e-mail porukama ili news grupama. Posebno dobro je usklađen sa *Microsoft e-mail* klijentima, koji su poznati kao "problematični". *Titanium* je moćan antivirusni alat posebno dizajniran za Windows platformu.

## *4.2. Antivirusne metode*

### *4.2.1. SKENERI*

Princip rada antivirus skenera bazira se na provjeravanju datoteka, sektora i sistemske 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: opšti (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 reaguju odmah po pojavi virusa, dok nerezidentni detektuju virus tek kad bude pokrenut.

### *4.2.2. CRC SKENERI*

CRC skeneri djeluju tako što kalkulišu 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 upoređuju informaciju sa bazom i kontrolišu 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 detektovani samo ovom metodom. Problem kod ove vrste skenera je što ne mogu registrovati postojanje virusa u trenutku inficiranja sistema, jer još uvijek nisu napravljene potrebne izmjene u *sis* datotekama. CRC skeneri ne mogu detektovati 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.

### *4.2.3. 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.

### *4.2.4. IMUNIZATORI*

Djele se u dva tipa: one koji upozoravaju na infekciju i one što blokiraju pokušaj virusa da se inflitrira 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 mjenja datoteke i ipraktično 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.

# 5. VIRUSI U MREŽI

Ova vrsta virusa se širi putem globalne mreže – Internet. Način njihovog širenja je raznovrstan. U najčešći način širenja virusa spada i najčešće korišteni Internet servis, elektronska pošta. Pored e-maila, mrežni virus je moguće "zaraditi" i na druge načine – u news grupi, preko IRC-a, ICQ-a ili putem downloada neprovjerenog fajla. Mnogi od ovih virusa preuzimaju potpunu kontrolu nad računarom, tako da zlonamjerniku omogućavaju pristup fajlovima na disku, ekranu ili podacima koje korisnik zaraženog računara ukucava na tastaturu. Dakle, po infekciji računar je najčešće pod kontrolom napadača, a ne žrtve tj. zaraženog korisnika.
Virus kao program, putem e-maila ili news grupe može doći kao attachment. Prilikom preuzimanja sa neke Web ili FTP adrese, program je upravo taj fajl što se preuzima često su virusu "upakovani" kao katalog proizvoda, čestitka za praznik i slično. Međutim, svi imaju jednu zajedničku osobinu – svi su izvršni fajlovi tj. programi. Pod Windows operativnim sistemom, izvršni programi su svi fajlovi koji se završavaju sa *.exe.* Ovo je veoma bitno, pošto ima slučajeva da fajlovi koji nose viruse imaju ime *slika.jpg.exe* ili *katalog.txt.exe.* Iako piše *slika.jpg* to nije slika, već program. Po izvršavanju, ovaj program će možda zaista i prikazati neku sliku, ali gotovo sigurno će zaraziti računar virusom.

### *Zli Attachmenti*

Ukoliko se desi da se dobije poruka koja ima attachment (fajl prikačen uz poruku) ne treba se odmah otvoriti. Time se stvara opasnost da se startovanjem attachmenta zarazi računar. Nažalost, većina modernih programa za e-mail, a među njima i daleko najpopularniji *Microsoft Outlook Express* često ne prikazuju kojeg je tipa prikačeni fajl. Prikazuju samo njegovo ime. Svi e-mail programi omogućavaju da se fajl snimi na disk. Najbolje bi bilo svaki attachment koji stigne, snimiti na disk, a onda ga provjeriti. Provjera snimljenog fajla počinje sa provjerom kojeg je tipa. Ako je zaista u pitanju slika (*.gif, .jpg, .bmp*) ili tekst (*.txt, .asc*) onda ga se slobodno može otvoriti. Ukoliko je u pitanju dokument popularnog tekst procesora, *Word* (*.doc*), izvršni fajl (*.exe, .com, .bot, .cmd*) ili nešto nepoznato, potrebno je da taj direktorijum pretražite (skenirate) antivirusnim programom. Sve što je rečeno za e-mail attachmente, važi i za attachmente iz news grupe.
Fajlovi koji se preuzimaju sa Web ili FTP adresa nisu ništa različiti od attachmenta. Sa njima je potrebno biti isto toliko oprezan, ako ne i više.

- ***Mrežna zaštita računara –***

Zaštita od virusa u mreži računara je kompleksniji zadatak od zaštite pojedinačnih računara. Instalirati dekstop verzije antivirusnog softvera na svaki računar u mreži nije naročito pametno riješenje, iako je manje-više funkcionalno, bar u prvo vrijeme. Ipak,

brzo se pokaže kao nepraktično, čim antivirusne definicije zastare, posebno ako imamo više računara u mreži koji nemaju pristup internetu. Tada se obnova antivirusnih definicija mora raditi ručno na svakom računaru. Mrežni antivirus alati omogućavaju administratoru da sa servera ima pregled svih računara, da vidi da li je na svakom uredno pokrenut klijentski antivirusni program, od kojeg su datuma definicije, kada je bila posljednja zaraza, da li je uklonjena i na kojoj je datoteci bila, te naravno koji je virus bio u pitanju. Obično se sa servera može pokrenuti ručno skeniranje na svakom klijentu (ako je uključen) ili pokrenuti pokretanje punog (full) skeniranja u određeno vrijeme. Ovo je preporučljivo, jer je poznato da je puni sken pouzdaniji i detaljniji od zaštite u realnom vremenu.
Još jedna bitna stvar je mogućnost distribucije novih antivirusnih definicija klijentima sa jednog mjesta. To se obavlja na taj način da server u pravilnim vremenskim intervalima skida sa Interneta nove definicije i zatim ih kroz LAN distribuira svakom klijentu na koji se one nevidljivo instaliraju. Drugi metod je da klijenti sami provjeravaju da li su na serveru u Lan-u (ili na Internetu, ako imaju pristup) pojavile nove definicije i da ih pokupe ako postoje.
Osnovna karakteristika mrežnog antivirusnog softvera mora biti automatizacija na što većem nivou.

### *Mrežni antivirus alati: Symantec Antivirus filtering for Microsoft Exchange 2000*

Pokretanjem attachmenta, virus se instalira na računar i od tada će vjerovatno biti poslan uz svaku e-mail poruku koja se sa njega pošalje, naravno bez znanja korisnika. Glavni "krivci" za širenje ove vrste virusa, osim zlobnika koji ih stvaraji, su sami korisnici koji nepromišljeno pokreću sumnjive e-mail zakačke (attachmente). Zbog toga je najbolje ne dozvoliti da takva poruka uopšte dođe do korisnikovog mailbox-a, pa mu tako i ne dati priliku za eventualno pokretanje virusa i širenje zaraze. Zato se koriste antivirusi namjenjeni mail serverima. Značajan je posebno *Symantec Antivirus / Filtering for Excange 2000*.
Osnovni zadatak ovog softvera je skeniranje e-mail poruka u realnom vremenu prije nego dospiju do korisnikovog mailbox-a, te povremeno skeniranje svih mailbox-ova i javnih (public) foldera, ako postoje.Da bi ovo ispravno funkcionisalo potrebno je da poruke svakog korisnika dolaze i stoje u njegovom mailbox-u na serveru, a ne lokalno na računaru. Postoje tri vrste skeniranja mailbox-ova. *Auto-Protect* je stalno aktivan i skenira novopridošle stavke u svakom mailbox-u i javnom folderu. Svaki put kada dobije nove antivirusne definicije, vrši skeniranje kompletnog *Information Store-a*. Zatim je tu *Manual Scan*, koji se može pokrenuti po potrebi i po zadanim parametrima na svim zadanim mailbox-ovim. Kao treći imamo *Schedoled Scan* koji se pokreće automatski u zadano vrijeme i skenira sve mailbox-ove i javne foldere. Pored skeniranja mailova u potrazi za virusima, AVF se može koristiti i za selekciju poruka prema sadržaju.

# *6. ZAŠTITA OD VIRUSA*

Osnovna zaštita od virusa na samom računaru provodi se upotrebom programa za borbu protiv virusa. Ovi programi označavaju se zajedničkim imenom *antivirusni programi*. Program u sebi ima podatke koji mu omogućavaju prepoznavanje različitih virusa. Zbog toga će u trenutku kada naiđe na zapis zaražen virusom spriječiti aktiviranje tog zapisa i podići uzbunu, odnosno na ekranu će se pojaviti prozor sa upozorenjem da je određeni zapis zaražen virusom. Antivirusni programi koriste dva pristupa za otkrivanje virusa: skeniranje i heuristiku. Skeniranjem se otkrivaju potpisi tj. redovi koda na osnovu kojih se prepoznaje virus ili neka njegova varijanta. Heuristika je metod traženja neuobičajne aktivnosti na primjer program koji pokušava da upisuje u Windows bazu *Registry*.
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 računar donosi nekakve podatke. Ovakav način rada je nesiguran jer korisnik može jednostavno zaboraviti provjeru. Osim toga ovakav oblik zaštite je posebno nepovoljan pri radu sa internetom jer se neki virusi koji se šire elektroničkom poštom mogu aktivirati i prije nego što korisnik dobije priliku da provjeri podatke. Stupanj zaštite može se postupno povećavati sve do najvišeg stupnja. Najviši stupanji zaštite uključuju stalnu provjeru podataka koji se koriste, nadzor nad svim prispjelim elektroničkim porukama i periodičnu provjeru svih podataka na računaru. Ovakav oblik zaštite bez sumnje troši nešto više računarskih resursa. Činjenica je da će rad antivirusnog programa usporiti rad računara. No ovo je usporenje kod savremenih računara jedva primjetno a pruža najviši stepen sigurnosti.
Proizvođači antivirusnih programa redovno ažuriraju definicije virusa, tj. datoteke koje se koriste za njihovo otkrivanje. Radi maksimalne bezbjednosti treba ih često ažurirati. Neki programi mogu automatski da dodaju definicije čime one postaju dostupne. Osvježavanje definicijama je potrebno kako bi se prepoznali novi virusi. Ukoliko AVP nisu ažurirani novim definicijama oni neće moći prepoznati nove viruse i time oni postaju nesposobni i beskorisni za zaštitu.
Treba posebno biti obazriv sa makroima. Računar se od njih može zaštititi tako što se uključe opcije za makrobezbjednosti u antivirusnom paketu. U aplikacijama paketa *Office 2000* kao što su npr. *Word* i *Outlook* izaberu se *Tools – Macro – Security* i podesi se nivo bezbjednosti (*Security Level*) na visok (*high*) ili srednji (*medium*). Potrebno je ažurirati softver na Internet. Ne treba odmah otvarati e-mail poruke koje stižu od nepoznatih osoba. Naročiti treba paziti kada stigne datoteka sa nastavkom *vbs*. Čak i kada mislimo da je ona pouzdana ne smijemo je otvarati u klijentu e-mail pošte. Snimamo je na disk i prvo propustimo kroz antivirusni program. Pravljenje rezervnih kopija je veoma korisno, to je jedan vid zaštite računara.

## *6.1. 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 redukuje mogućnost zaraze.

**Korak 2:**
Redovno ažuriratiantivirusne 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 sajta 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 kompresovanih 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. Takođe, 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 (ili particija, ako je disk particioniran). Proces skeniranja može potrajati i zavisi od veličine hard diska i broja datoteka kojima rasplaže. 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.

LITERATURA

1. Samir Lemeš, dipl. ing. maš., Muhamed Mujčić, "PC nije bauk", Zenica, Mart 1998. godine,

2. Ladislav Krasny, Članak u časopisu "INFO" Br-522/00, str.43-55,

3. http:\\www.cg.yu\zaštita\trojanci.html,

4. http://www.avp.com,

5. http://www.mcaffee.com,

6. http://symantec.com.