# Računalni virusi

# Sadržaj :


**1. Uvod** 2
**2. Hackeri – Cyber terrorizam** 3
**2.1**. Kevin Mitnick – Cyber terrorist ili društveno korisna osoba 4
**2.2.**Hackeri u hrvata 4
**3. Povijest virusa** 5
**4. Kako se šire virusi** 6
**5. Vrste virusa** 7
**5.1**. Osnovna podjela virusa 7
5.1.1. Crv ("Worm") 7
5.1.2. Trojanski konj 8
5.1.3. Backdoor 9
5.1.4. Dialer 9
5.1.5. HOAX (lažna uzbuna) 9
5.1.6. Spyware 10
**5.2**. Podjela virusa obzirom na način funkcioniranja 10
5.2.1. Infektori datoteka 10
5.2.2. BOOT sector i Master BOOT Record infektori 11
5.2.3. Parazitski virusi 12
5.2.4. Svestrani virusi 12
5.2.5. Virusi pratioci 12
5.2.6. Link virusi 13
5.2.7. ANSI bomba 14
5.2.8. Tunelirajući virusi 14
5.2.9. Kernel virusi 14
**6. Neke virusne tehnike** 14
**6.1.** Enkripcija 14
**6.2.** Polimorfni virusi 15
**6.3**. Stealth 15
**7. Zaštita računala** 16
**8. Zaraženo računalo** 17
**9. Neki noviji virusi** 18
**10. Pitanja** 20
**11. Literatura i izvori podataka** 20

# 1. Uvod

Informatičkim početnicima je gotovo nemoguće objasniti što je to **virus**. Onda se još netko sjetio, pa je i nekim podvrstama virusa dao drugačija imena, samo u svrhu zbunjivanja ljudi. Međutim, davanjem drugačijih imena određenim vrstama virusa, za malo naprednije informatičare bitno olakšava snalaženje i borbu protiv virusa. 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.

Stručnjak za viruse, Fred Cohen je kroz svoja istraživanja, doktorsku disertaciju i različite publikacije praktički zasnovao novu znanost o virusima. On je razvio teoretski, matematički model o ponašanju virusa ikoristio ga za testiranje raznih hipoteza o širenju virusa. Cohenova formalna definicija (model) ne bi se mogla tako jednostavno prevesti iz matematike na obični jezik ljudi, ali njegova skraćena definicija odprilike glasi:

**"Kompjuterski virus je kompjuterski program koji može inficirati druge kompjuterske programe modificirajući ih na taj način da to podrazumijeva stvaranje svoje vlastite kopije."**

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. Većina od nas bi se složila s jednom 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 viruse."**

Dobro je znati da velika većina ljudi koji se bave računalima koristi termin "virus" za svaku vrstu programa koji pokušava sakriti svoju destruktivnu funkciju i/ili se pokušava razmnožiti na što je više računala iako bi se neke od tih programa prije moglo nazivati "crvima" (worms) ili "trojanskim konjima" (Trojan horses). Također treba biti svjestan da građa programa koji može inficirati druge programe može uključivati puno više stvari nego što se to isprva zapaža i zato i ne pretpostavljate što sve virus može ili može učiniti! Ovi programčići su zapravo vrlo ozbiljna stvar; razmnožavaju se brže nego što ih se pronalazi i zaustavlja, a čak i naoko najbezazleniji virus može biti stvarna životna prijetnja.

Svaki virus radi neku štetu na računalu, bilo da se radi o tome da vam

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. Kompjuterski virusi su zapravo poseban slučaj nečega poznatog pod nazivom **"bolesna logika" (malicious logic) ili malware.**

# 2. Hackeri – Cyber terorizam

Postavlja se pitanje tko su autori ovakvih štetnih programa, tko je kriv? Netko valjda nije imao dovoljno roditeljske pažnje? Nema svrhe diskutirati o psihičkom profilu nekog od njih. Ljudi su u stanju raditi i gore stvari, pa ovo ne čudi. Tko je kriv? Hm, vjerovali ili ne, jedan od najvećih krivaca za ekspanziju virusa u zadnje vrijeme je Microsoft. Nije jedini i isključivi krivac, ali gospodin Bill Gates uz Windowse isporučuje (besplatan) program za čitanje e-mailova zvan **Outlook Express**. Taj program je toliko ranjiv i podoban širenju virusa da je to strašno.Kasnije su u Microsoft-u napravili "zakrpe" koje štite od automatskog širenja virusa, ali već je bilo kasno. Prema nekim anketama, u Hrvatskoj se 85% ljudi koristi Outlook Express-om za čitanje e-maila, ostatak priče ne moram ni pisati. Pa ako i dalje želite vjerovati Billu Gatesu i Outlook Express-u...No, ipak su (naravno) za viruse odgovorni njihovi autori, za koje se usvojilo popularno ime **hackeri**. Pa saznajmo nešto o hackerima.

Ne postoji točna definicija "hackera". Neki kažu da su to programeri koji su namjerno (u većini slučaja) izazvali raspad nekog informatičkog sistema zbog nekih osobnih frustracija, drugi kažu da su to kolekcionari koji se bave preprodajom povjerljivih informacija, a neki opet kažu da su to ljudi koji iz čiste dosade nastoje svojim virus programima privući pažnju velikih kompanija kako bi ih zaposlili…

Prvi slučaj "hakiranja" zabilježen je davne 1972. godine kada je John T. Draper na sasvim slučajan način otkrio da se uz pomoć obične zviždaljke mogu emitirati tonovi koji su u stanju prevariti signal telefonske centrale, te se na taj način može besplatno telefonirati. Taj slučaj zabilježen je pod imenom BLUE BOX (plava kutija) koju je kasnije John napravio da ne bi trebao sam stalno puhati u zviždaljku. Današnji se hakeri najviše koriste uporabom posebno napisanih računalnih programa (mi ih zovemo virusi) koji se "nastane" u neko računalo s određenim ciljem. Cilj može biti brisanje podataka, kopiranje podataka, ili preimenovanje podataka. Upad u računalne sisteme najviše se raširio po SAD-u, tako da je američki Kongres morao izglasati

zakon o zlouporabi računala. Zakonom je donesena odluka o petogodišnjoj zatvorskoj kazni i/ili visokoj novčanoj kazni. Prva osoba koja je napravila veću štetu bio je Robert Moris. On je 1988. pronašao pogrešku u jednom računalnom sustavu i uz pomoć virusa "srušio" 6000 računala na Internetu. Zbog toga je morao platiti odštetu od 10.000 USD, tri godine privremene zatvorske kazne, i 400 sati dobrovoljno korisnog društvenog rada.

## 2.1 Kevin Mitnick – Cyber terrorist ili društveno korisna osoba

Kevin je najpoznatiji hacker svih vremena. Uspio je uz pomoć računala falsificirati oko 20 tisuća brojeva kreditnih kartica, ukrao je nekoliko tisuća mobilnih telefonskih brojeva koje je besplatno dijelio, te je provodio dane i dane ilegalno po raznim računalnim mrežama u SAD-u, a iako to nije priznao na suđenju, pretpostavlja se da je ušao u sistem NORAD za navođenje projektila vojske sjedinjenih država. To mu je donijelo status da se nađe u FBI-evom popisu najtraženijih računalnih kriminalaca. 15. veljače 1995. godine Kevina je FBI uhapsio. Proveo je nekoliko godina u zatvoru, a nakon izlaska iz zatvora imao je zabranu pristupa Internetu. Danas je Kevin jedan od savjetnika za siguronosna pitanja velikih korporacija u svijetu. Osnovao je tvrtku Defensive Thinking u Los Angelesu. Kevin je na vrlo jednostavne načine ulazio u računalne sustave. Doslovce je "kopao" po kontenjerima za otpad velikih korporacija gdje je nalazio interesantne podatke koje je iskoristio za svoje pothvate.

Uz Kevina, najveći računalni kriminal napravio je Vladimir Levin, koji je od poznate banke Citibank 1994. godine otuđio oko 10 mil. USD u razdoblju od nepuna tri mjeseca. Levina su uhvatili na Londonskom aerodromu 1997.godine. Novac je vraćen banci, ali još uvijek nedostaje oko pola mil. USD. Osuđen je na 36 mjeseci zatvora i 250 tisuća USD kazne**.**

## 2.2. Hackeri u hrvata!

Ima li hakera i računalnog kriminala u nas. Odgovor – ima, ima ali ne u onoj mjeri kao što ga ima u SAD-u, Europi, Aziji. Prvi slučaj bio je 1996. godine kada su učenici iz Zadra na slučajan način ušli u sustav Pentagona. Ni oni sami nisu znali gdje su ušli jer nisu ništa razumjeli, ali su ipak ostali dosta dugo u sustavu da se otkrije od kuda dolaze. Javnost i mediji su tada ipak preuveličali taj slučaj. U Hrvatskoj tada još nije postojao kazneni zakon za računalni kriminal.

Godine 1998. citiram "*U Kazneni Zakon ubačen je članak 223 koji pokriva ovu problematiku, a taj članak tretira sve korisnike, s tim da kod privatnih osoba policija postupa tek po prijavi, a u slučaju štete kod državnih tijela postupa se po službenoj*

*dužnosti*".

Hrvatska je još uvijek zemlja gdje nema upada u računalne sustave. Postoje neki pokušaji, ali oni su tako maleni da nisu ni vrijedni spomena. Ono što kod nas predstavlja računalni kriminal je kopiranje softvera, preprodaja istog, kopiranje audio kazeta, muzičkih kompakt diskova i u zadnje vrijeme kopiranje DVD filmova i njihova preprodaja.

# 3. Povijest virusa

Šezdesetih i sedamdesetih godina, još u vrijeme velikih mainframe računala, postojao je fenomen zvan **zec** (rabbit). Zec je najčešće nastajao slučajem ili greškom kada je "pomahnitali" kompjuterski program počeo sam sebe kopirati po sistemu, izazivajući usporenje ili pad sistema. No nisu svi "zečevi" nastali slučajno. Prvi pravi predak današnjih virusa – Prevading animal (prožimajuća zvijer) bio je program sposoban da se nadodaje na druge kompjuterske programe na UNIVAC 1108 kompjuterskom sistemu. Prvi potvrđen nalaz kompjuterskog virusa daleke 1981. godine bio je Elk Cloner – virus koji je inficirao BOOT sektor disketa za legendarni Apple II kompjuter. U studenom 1983. Len Adleman prvi put u povijesti upotrijebio riječ "virus" opisujući samokopirajući kod. Prijelomna je i 1986. godina kada se pojavljuje kopjuterski virus Brain (mozak). Ovaj virus, sposoban inficirati BOOT sektore 360 KB disketa IBM PC kompjutera brzo je osvojio svijet. Na svu sreću, virus nije bio destruktivan, nego je u sebi samo nosio podatke o autorima. Nakon toga stvari kreću brže. Pojavljuje se kompjuterski virus Jerusalem (1988.) koji je brisao sve pokrenute programe, te prvi pravi destruktivac virus Datacrime (1989.) koji je bio sposoban izvršiti low-level format nulte staze na disku. 1989. aktivirana je tvornica virusa u Bugarskoj. Izvjesna osoba (ili skupina) koja sebe naziva Dark Avenger (Crni osvetnik) do danas je napisala najmanje 50-tak virusa uključujući neke od najpoznatijih kao što su New Zeland i Michelangelo.

Prvi virusi su ozbiljno zarazili računala u našoj zemlji krajem 1988. godine. Pojavili su se, doduše, već nešto ranije na računalima Atari i Mac, ali je fenomen uglavnom ostao u granicama kompjuterskih igara omladine. Prvi ozbiljni udarac je profesionalna upotreba računala doživjela kroz napad virusa na računala IBM PC, PS/2 i kompatibilne. To se dogodilo u listopadu 1988. na zagrebačkom Interbirou. Zanimljivo je da smo u Hrvatskoj najprije dobili virus koji je nastao među posljednjima. No, veoma brzo su uslijedili i drugi, stariji, i nakon godinu dana može se reći da je Hrvatska razmjerno intezivno bila zaražena sa više vrsta virusa, prije svega za računala tipa IBM PC.

Statistika navodi za 1988. godinu čak i za SAD, gdje postoji relativno visoka informatička kultura, porazne brojke: u prva dva mjeseca te godine bilo je prijavljeno 3 000 zaraza, a u posljednja dva mjeseca preko 30 000. Virus Internet je za svega

nekoliko sati zarazio 6 200 računala (listopad '88.). Cijele 1988. godine bilo je prijavljeno preko 90 000 zaraza samo na osobnim računalima. Istina je još gora, budući da mnogi zaraženi zarazu ne prijavljuju. Zaraza prijavljenih donosi slabu reputaciju u svakom pogledu. Mnogi korisnici pokušavaju da u što većoj tišini eliminiraju viruse, pa makar i robusnim postupcima (formatiranjem diskova), samo da ne dođu na loš glas. Iz istog razloga oni ne iniciraju istrage odakle su virus dobili, što virusu samo olakšava nesmetano dalje širenje.

# 4. Kako se šire virusi ?

U početku su se virusi širili preko disketa. Ljudi su se koristili disketama da bi izmjenjivali datoteke (programe, tekstove, tablice, slike...). Ubacite nečiju disketu sa njegovim programima u svoje računalo, pokrenete igricu (npr. TETRIS) koji je zaražen virusom i taj virus uđe u vaše računalo , te nakon toga taj virus presnimi sebe na sve diskete koje vi iza toga ubacite u svoje računalo. Diskete iz vašeg računala bi kasnije nekako dospjele u tuđe kompjutore i to je to.... Eto zaraze! Kasnije su CD-i preuzeli uloge disketa kao prijenosnika. Nekako paralelno sa CD-ima je postao popularan jedan drugi medij za izmjenu informacija (datoteka) – Internet. Internet je dosta pomogao brzini razmnožavanja virusa, jer se sa jednog kraja zemlje može poslati virus na drugi kraj zemlje za samo pet sekundi. Uz to, popularnost interneta je rapidno rasla, tako da je na kraju internet postao glavni medij za širenje virusa.

Npr. kada bi netko tko ima virus poslao nekome e-mail poruku, nerijetko bi se virus (bez korisnikova znanja) “naselio” u tu poruku i zajedno sa njom otišao primaocu. Primatelj bi morao samo otvoriti poruku da je pročita da bi se virus sam aktivirao i prešao u njegovo računalo. Naravno, sa primateljevog računala se virus širio i na druga računala. Virusi su toliko “napredovali” i toliko postali “pametniji” da sada sami mogu sastaviti neku poruku i sami sebe poslati nekome iz korisnikovog imenika (ili je koristio e-mail adrese od raznih pošiljatelja i primatelja sa kojima se korisnik prije dopisivao, te njima slao privatne dokumente). Budući da se većina današnjih virusa širi na prethodno opisan način, često je od velike važnosti znati nešto više detalja o pristigloj poruci.

Sadrži li poruka .exe datoteku ili datoteku s dvije ekstenzije (npr. .scr.exe), velike su šanse da se radi o nekoj vrsti virusa. Ukoliko je poruka stigla od nepoznate osobe te se u tijelu poruke ne nalazi nikakav tekst, poruka je također potencijalno opasna. Čak i ako poruka stiže s poznate adrese, ne mora značiti da je bezazlena; današnji virusi u stanju su krivotvoriti zaglavlje poruke ili se automatski poslati bez znanja vlasnika računala (kao što smo već opisali).

# 5. Vrste virusa

## 5.1. Osnovna podjela virusa

### 5.1. 1. Crv ("Worm")

Kompjuterski crv je program (ili skupina programa) koji je sposoban raširiti svoje funkcionalne kopije ili samo neke segmente na druga računala. Obično to radi preko mreže. Crv na domaćinskom računalu (HOST WORM) cjelokupan se nalazi i izvršava na tom domaćinskom računalu, a vezu s mrežom koristi samo za svoje razmnožavanje na druga računala. Ovaj tip crva nakon što pokrene svoju kopiju na novom inficiranom računalu samostalno uništava svoju prvobitnu kopiju. Na taj način u određenom trenutku negdje na mreži uvijek se nalazi samo jedna kopija tog crva. Na taj način crv neprestano kulja mrežom zamećući trag za sobom. Ovaj tip crva naziva se još i "zec" (RABBIT) upravo zato što stalno bježi uokolo mrežom.

Crvi relativno rijetko posjeduju destruktivan kod namijenjen uništavanju podataka, no zbog svoje sposobnosti neograničenog kreiranja vlastitih kopija, u stanju su zagušiti promet na pojedinim segmentima mreže.

**Crv Swen.A**

Otkriven: 18.09.2003.

Aliasi: Swen [F-Secure], W32/Swen@mm [McAfee], W32/Gibe-F [Sophos], Worm Swen.A

Širi zarazu na: Windows operacijskim sustavima

Swen je crv koji se širi putem maila, ali i preko dijeljenih resursa (KaZaA-e i IRC-a).

Na zaraženom računalu pokušava onemogućiti rad antivirusnih programa i vatrozida (firewalla).

Postoji više varijanti mailova putem kojih se crv Swen širi, ali najčešća je ona u kojoj mail izgleda kao obavijest od strane Microsofta da se hitno pokrene datoteka koju šalju u sklopu maila. Npr. kao na slici:


Pokretanjem datoteke koja dolazi u sklopu maila kao attachment računalo će se zaraziti ovim crvom.

Općenito, s attachmentima mailova treba biti iznimno oprezan.

Za uklanjanje crva s računala potrebna je najnovija definicija virusa za antivirusni program koji koristite. Više o ovom crvu možete pročitati na: Symantec, Sophos…

### 5.1.2. Trojanski konj

Trojanski konj zapravo nije virus, iako se pod tim pojmom često podrazumijeva. On je upravo ono što mu govori ime, program koji je u stanju učiniti stvari koje nisu definirane njegovim specifikacijama ili dokumentacijom. Trojanski konj sam po sebi nije destruktivan, no vrlo često sadrži kod koji se aktivira nakon što korisnik pokrene naizgled neki bezazleni program. Npr. s interneta skinete neki "shareware" za rad npr. s fontovima. Program je po vama genijalan, s fontovima činite čuda, jedino nakon što iz izbornika tog programa deset puta izaberete opciju About...on vam obriše cijeli disk. 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.

### 5.1.3. Backdoor

Backdoor će se uvući u vaše računalo i npr. omogućiti nekome da se "služi" vašim računalom kada se spojite na internet, kao daljinski upravljač. Vi se spojite na internet, radite što inače radite (e-mail, vijesti, portali, ICQ, vremenska prognoza...), a za to vrijeme netko kopira podatke iz vašeg računala na svoje, ili briše neke podatke. Može raditi sa vašim računalom šta hoće; pomicati strelicu na ekranu (iako vaš miš stoji na mjestu), tipkati poruke umjesto vas i slično.

Nerijetko se backdoor i trojanski konj koriste u duetu. Npr. pokrenete neki program za koji mislite da je igrica, a dok se vi igrate on vam ubaci nekakav "backdoor" u vaše računalo. Nakon igranja se vi spojite na internet, a onda počinje "ludnica". Jedan od najpopularnijih backdoora je (bio) ICQ – program koji je prebrzo stekao popularnost, a razvojni tim to valjda nije mogao pratiti , tako da je bio prepun "rupa".

Zaštita?

Instalirajte VATROZID. To je jedan od popularnijih prijevoda engleskog izraza "Firewall". Nakon što instalirate vatrozid i ponovo pokrenete računalo (restart), kada god neki program želi pristupiti internetu vi ćete biti upitani za dozvolu. Ja osobno sam tako primjetio da imam instalirane neke "krtice" u svom računalu. Problem kod Firewall-a je u tome što svojim upitima zna zbuniti početnika. Prvo vrijeme bude dosta upita, dok ne odredite koji programi smiju (npr. Internet Explorer, ICQ i sl.)pristupati internetu, a koji ne smiju (bit će zanimljivo kad otkrijete da neki program koji niste nikada instalirali stoji u vašoj memoriji i želi pristupiti internetu).

### 5.1.4. Dialer

Dialeri možda ne bi trebali imati poseban pasus, ali su tako cool da ih moram spomenuti. To su programi koji se najčešće instaliraju preko interneta, sa stranica na kojima se nalazi nekakva pornografija. Kliknete na sliku nekog golog komada ispod koje piše "*Kliknite ovdje ako želite vidjeti cijeli film*". Vi (razmišljajući krivom glavom) kliknete, ali se na ekranu pojavi upozorenje "*Da biste vidjeli ovaj ultrasuperzanimljiv film morate instalirati program za gledanje filmova*" uz pitanje "*Da li ste sigurni?*". Naravno, vi kliknete na "*Yes*" i pustite instalaciju tog programa, odgledate 10 sekundi filma (za ostatak treba platiti) i to je to. Pored programa za gledanje filma ste instalirali i Dialer. Naime, kada slijedeći put pokušate uspostaviti vezu na internet , bez vašeg znanja kompjutor neće zvati broj vašeg internet provider-a (Iskon-a,VIPonline-a...), nego neki broj u inozemstvu, čiji čitav prihod ide na račun nekog šaljivdžije. Vama će i dalje internet vjerojatno raditi normalno, ali će vas iznenaditi račun za telefonske usluge na kraju mjeseca.

### 5.1.5. Hoax (lažna uzbuna)

Kao što se može zaključiti iz naziva, riječ je o obavijestima,vrlo često pristiglim

od strane prijatelja ili poznanika. Hoax-i su klasične e-mail poruke u kojima vi sami preuzimate ulogu virusa. Za ovu vrstu virusa idealno paše Einstein-ova uzrečica:"*Beskonačni su svemir i ljudska glupost!*".

Npr. netko vam pošalje poruku u kojoj kaže:"*UZBUNA! Pojavio se novi virus. Niti jedan antivirusni program ga ne može otkriti, a aktivirat će se za nekoliko dana i izbrisati sve datoteke na zaraženom kompjutoru. Provjeri da li imaš datoteku ABC.EXE u svom WINDOWS direktoriju. Ukoliko imaš tu datoteku to znači da je tvoje računalo već zaraženo. Odmah je izbriši kako se virus ne bi dalje širio i obavijesti sve svoje poznanike o tome.*" Netko povjeruje u tu priču, izbriše navedenu datoteku i nakon toga mu ne radi pola programa.

Najpoznatiji primjer Hoax-a u Hrvatskoj je priča o "uzgoju mačaka u boci", koja je dospjela i u najtiražniji dnevni tisak. Dakle, Hoax-i su, u stvari, lažne priče/obavijesti. Morate priznati da je cool, uglavnom ne nasjedajte.

Zaštita?
Vaš mozak.

### 5.1.6. Spyware

Spyware-i su programi koji prate vaš rad na računalu i o tome obavještavaju nekog drugog (u pravilu, nepoznatu osobu). Postoje programi koji se namjerno instaliraju po (većim) firmama kako bi direktor(i) imali uvida u to što se radi na njihovim računalima. Oni spyware-i o kojima ovdje pišem su programi koji prate gdje vi surfate po internetu i o tome izvještavaju razne marketinške agencije. Ako primjete da surfate npr. po stranicama proizvođača štampača, svako malo će vam na ekranu iskočiti stranica sa "najpovoljnijom" ponudom štampača. Nekada može biti korisno, ali je vaša privatnost debelo narušena. Inače, čim instalirate Microsoft-ove Windows-e na vaše računalo, sa njima na poklon dobijete "Alexu" – Microsoft-ov spyware. Tako da gotovo sigurno u ovom trenutku imate barem jedan spyware na svom računalu.

Lijek?
Na www.lavasoft.de stranici skinite zadnju verziju programa **AdAware** (nije velik i jednostavno se instalira, bez puno pitanja). Za takve programe vrijedi isto pravilo kao i za antivirusne programe – morate redovito obnavljati bazu spyware-a. Naravno, Adaware nije jedini program za tu namjenu.

## 5.2. Podjela virusa obzirom na njihov način funkcioniranja

### 5.2.1. Infektori datoteka

Ova skupina virusa se može još podijeliti na dvije podskupine, a to su:

- oni koji direktno izvršavaju neku akciju nakon što se pokrenu (DIRECT – ACTION)
- oni koji čuče u memoriji i čekaju na žrtvu (RESIDENT). Općenito, većina virusa je rezidentna u memoriji računala

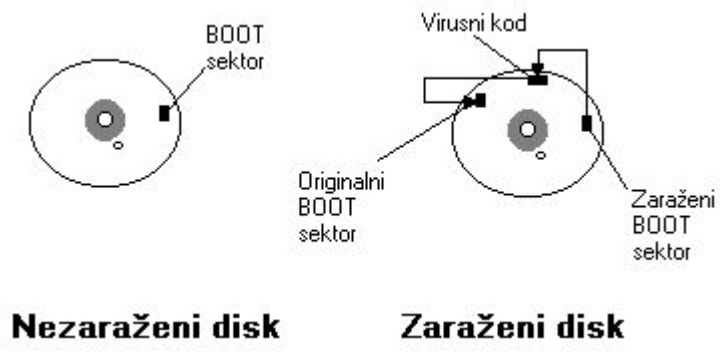
Osnovna vrsta su virusi koji, kada njihov kod bude izvršen i pošto vrate kontrolu originalnom programu, ne ostaju aktivni u memoriji. Ova vrsta operira tako da tijekom svog izvršenja pronađe objekt pogodan za infekciju i zarazi ga. Teoretski su ovi virusi manje infektivni od virusa rezidentnih u memoriji, ali nažalost u praksi to nije uvijek slučaj. Zarazi li virus program koji se često izvršava, bit će izuzetno učinkovit. Kako ovi virusi ne mijenjaju količinu slobodne radne memorije, moguće ih je primijetiti samo po promjeni duljine programa na disku. Danas ova vrsta virusa sve više ″izlazi iz mode″ budući da se ne mogu koristiti tehnike samosakrivanja koje zahtijevaju da virus bude aktivan u memoriji.

Kao što samo ime kaže, ova se vrsta virusa instalira u radnoj memoriji kompjutera i ostaje aktivna dugo nakon što zaraženi program bude izvršen. Virus aktivan u memoriji može biti sposoban zaraziti svaki izvršeni program, svaku disketu koja bude pokrenuta (pod uvjetom da nije zaštićena od pisanja), on može motriti aktivnost sistema ili u svakom trenutku izvršiti svoj korisni teret. Ovi virusi su iznimno infektivni. Osim toga, oni su sposobni koristiti sve moguće virusne tehnike, te predstavljaju trend u razvoju virusa. Neki virusi koriste kombinacije ovih dviju tehnika. Tako na primjer, virus može inficirati programe na način koji je tipičan za viruse koji nisu rezidentni u memoriji, ali nakon izvršenja virusnog koda ostavlja u memoriji mali rezidentni program sa korisnim teretom koji sam po sebi nije sposoban inficirati druge programe.

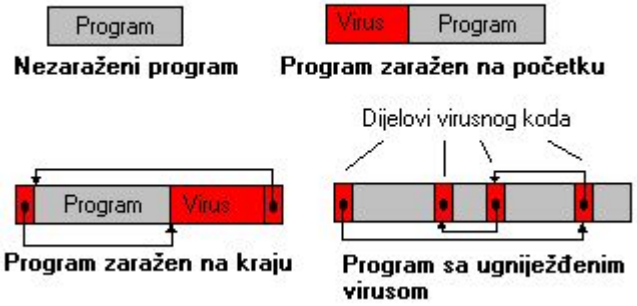
### 5.2.2. Boot sektor i Master Boot Record Infektori

Druga velika skupina virusa su tzv. sistemski (SYSTEM) ili boot-sektor (BOOT-RECORD ili BOOT-SECTOR) virusi. Ovi virusi napadaju Master BOOT sektor, DOS BOOT sektor ili BOOT sektor floppy disketa, odnosno program koji se u njima nalazi. BOOT sektor je idealan objekt za infekciju, budući da sadrži prvi program koji se izvršava na kompjuteru, čiji se sadržaj može mijenjati. Kada jednom kompjuter bude uključen, program u ROM-u (BIOS) će bez pitanja učitati sadržaj Master BOOT sektor u memoriju i izvršiti ga. Ako se u njemu nalazi virus, on će postati aktivan. No kako je virus dospio u master BOOT sektor? Najčešće pokušajem startanja sistema sa inficirane floppy diskete, ali boot sektor virusi se mogu širiti i pomoću posebnih programa, trojanskih konja, kojima je glavna namjena da neprimjetno “ubace” virus u BOOT sektor. Boot sektor virusi su iznimno učinkoviti u razmnožavanju. Od sedam najčešćih kompjutorskih virusa, čak šest ih je sposobno zaraziti BOOT sektor. Samo neki predstavnici iz ove skupine su Brain, Empire, Michelangelo. Obije ove podskupine virusa, čisti boot-sektor virusi i MBR virusi,

rezidentni su u memoriji.




## 5.2.3. Parazitski virusi




Najčešća vrsta virusa su upravo parazitski virusi. Ovi su virusi sposobni zaraziti izvršne datoteke na kompjutorskom sistemu dodavanjem svog sadržaja u samu strukturu programa, mijenjajući tok inficiranog programa tako da se virusni kod izvrši prvi. Poznati kompjutorski virusi sposobni su zaraziti .COM, .EXE, .SYS, .OVL i druge datoteke.

## 5.2.4. Svestrani virusi

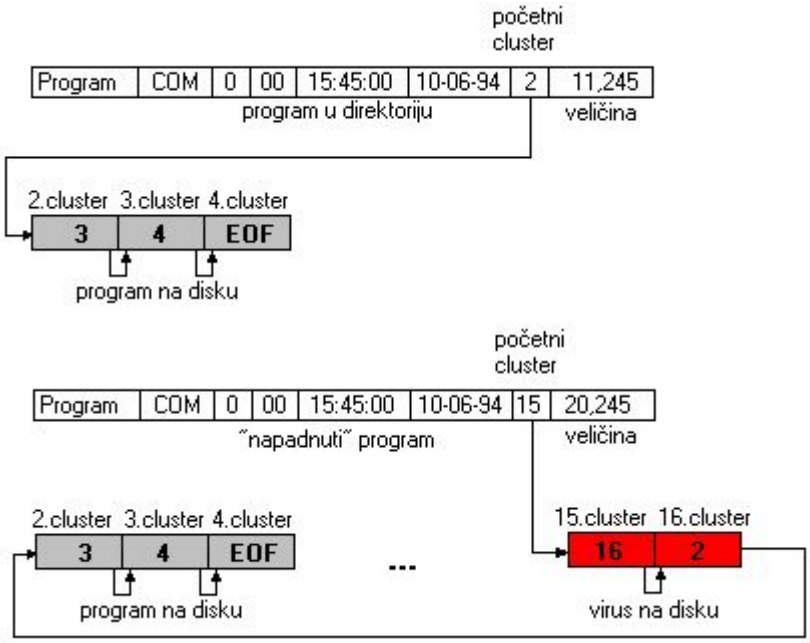
″Dobre″ osobine boot sektor i parazitskih virusa ujedinjene su kod svestranih (multipartite) virusa. Ovi virusi sposobni su zaraziti i BOOT sektore i izvršne programe, povećavajući tako mogućnost širenja. Poput boot sektor virusa i ovi su virusi iznimno efikasni u širenju.

## 5.2.5. Virusi pratioci

Najjednostavniji oblik kompjutorskih virusa su upravo virusi pratioci. Oni koriste prioritet kojim se izvršavaju programi s istim imenom pod DOS-om. .COM datoteke se uvijek izvršavaju prije .EXE datoteka, programi iz direktorija koji su na početku PATH niza izvršavaju se prije onih sa kraja. Virus pratilac obično stvori .COM datoteku koristeći ime već postojećeg .EXE programa i ugradi u nju svoj kod.

Princip je jednostavan - kada program bude pozvan, umjeste originala s .EXE ekstenzijom, prvo će se izvršiti podmetnuti .COM program s virusnim kodom. Kada izvršavanje virusnog koda bude završeno, virus će kontrolu vratiti kontrolu programu s .EXE ekstenzijom. Da bi prikrio prisustvo, virus pratilac će postaviti skriveni atribut za .COM program u koji je stavio svoj sadržaj. Ova vrsta ne mijenja ″napadnuti″ program, a zbog nespretnog načina širenja ne predstavlja veću opasnost.


## 5.2.6. Link virusi




Najinfektivnija vrsta virusa su link virusi koji jednom pokrenuti, u trenu inficiraju napadnuti kompjutorski sistem. Poput virusa pratioca ovi virusi ne mijenjaju ″napadnute″ programe već mijenjaju pokazivače u strukturi direktorija na takav način da ih preusmjere na cluster na disku gdje je prethodno sakriven virusni kod. Na svu sreću, ova izrazito infektivna i neugodna vrsta virusa, koja zbog samog načina razmnožavanja može izazvati pravi kaos na disku, ima trenutno samo dva predstavnika i ukupno četiri varijante.

### 5.2.7. ANSI bomba

ANSI bomba je sekvenca karaktera, obično umetnuta u tekst fajl koji reprogramira različite funkcije tipaka na računalima s ANSI terminalskim driverima. Teoretski, specijalna sekvenca karaktera može biti uključena u neku poruku kako bi reprogramirali tipku ENTER da izvrši komandu "format c:" (s return karakterom na kraju).

### 5.2.8. Tunelirajući virusi

Ovo su virusi koji pronalaze originalni prekidni potprogram (interrupt handler) u DOS-u i BIOS-u i pozivaju ih direktno tako zaobilazeći bilo koju aktivnost programa za nadgledanje. Takav program za nadzor od infekcije može biti učitan i presretnut u svom pokušaju da detektira aktivnost virusa. I obratno, neki antivirusni programi koriste tehniku tuneliranja u pokušaju da zaobiđu neki nepoznati ili nedektirani virus koji može biti aktivan dok se ovaj program izvodi.

### 5.2.9. Kernel virusi

Kernel virusi su oni virusi koji ciljaju na specifične osobine i funkcije programa koji koriste ljusku (kernel ili core) operativnog sistema. Npr. 3APA3A je DOS-kernel virus, ali istovremeno spada i u skupinu multipartitnih virusa.

# 6. Neke virusne tehnike

″Uspješnost″ virusa mjeri se duljinom vremena u kojem virus neprimjetno ostaje aktivan, inficirajući druge programe. Što je ″vrijeme inkubacije″ dulje, to su mogućnosti za opstanak virusa i eventualno izvršenje korisnog tereta veće. Osim toga, jednom otkriven virus može se pokušati braniti od postupka analize koji se redovito provodi radi utvrđivanja načina za njegovo sigurno pronalaženje. Važno je napomenuti da su sve ultraopasne tehnike o kojima će biti riječ u nastavku potpuno bezopasne ako se pri korištenju antivirusnih programa poštuju osnovne mjere antivirusne zaštite.

## 6.1. Enkripcija

Enkripcija ili šifriranje je postupak kojim se originalna informacija mijenja (premeće) u cilju prikrivanja njenog pravog sadržaja. U osnovi šifriranja postoji obrnuti postupak dekripcije (dešifriranja) kojim se ponovno dobivaju originalne informacije. Prvi razlog upotrebe šifriranja je pokušaj otežavanja pronalaženja virusa. Teoretski, ako virus mijenja svoj sadržaj i u svakom inficiranom sadržaju izgleda drugačije, teže je na temelju proučavanja njegovog tijela izvući search string ili

napraviti algoritam za pronalaženje. U praksi stvari stoje drugačije. Naime, nije moguće izvesti šifriranje cijelog virusnog koda, budući da onaj dio koda koji vrši dekripciju mora ostati neenkriptiran. Osim toga svaki enkriptirani virus mora prije izvršenja svoj dekriptirati u memoriji. Upotreba enkripcije možda može otežati analizu virusa, ali ne mora nužno i otežati njegovo pronalaženje.

## 6.2. Polimorfni virusi

Korak dalje u igri skrivača je polimorfizam (višeobličje). Polimorfizam predstavlja preoblikovanje izvršnog koda, na takav način da se očuva funkcija, ali istovremeno bitno promjeni njegov izgled. Pogledajte slijedeći primjer:

```
Code:

Instrukcije                                  Asembliraju se kao

1.    mov   ah,4ch                              B4 4C
      mov   al,00h                              B0 00

2.    mov   al,00h                              B0 00
      mov   ah,4ch                              B4 4C

3.    mov   ax,4c00h                            B8 00 4C

4.    mov   dx,4c00h                            BA 00 4C
      mov   ax,dx                               89 D0
```

Rezultat izvršenja dijela koda iz prethodna četiri primjera bit će isti, ali svaki od njih u memoriji izgleda drugačije. Polomorfizam je najčešće nadopuna tehnike enkripcije. Nakon što je glavnina tijela virusa već šifrirana nastoji se premetanjem redoslijeda instrukcija ili korištenjem drugih instrukcija prilikom svake naredne infekcije izmijeniti i dio virusa koji obavlja dekripciju. Ovim se nastoji doskočiti nemogućnosti šifriranja i tog dijela koda. Enkripcija kombinirana sa polimorfizmom predstavlja jedan od najopasnijih trendova u razvoju virusa.

## 6.3. Stealth

Stealth (nevidljivost, samosakrivanje) je još jedna kompleksna tehnika koju koriste vješti pisci kompjutorskih virusa. Temelj tehnike samosakrivanja je pokušaj prijevare korisnika, sistema ili antivirusnog programa na takav način da ga se uvjeri da je sa sistemom ne događa ništa neobično. Na primjer, najjednostavnija tehnika samosakrivanja je presretanje DIR komande na takav način da se umjesto stvarne,

pokaže duljina zaraženih programa prije infekcije. Tehnike samosakrivanja koriste način komunikacije između softvera i hardvera na PC kompjutoru. U osnovi, ova se komunikacija odvija preko interrupta. Kada procesor dobije zahtjev za čitanjem s diska on će izvršiti dio koda na koji je usmjeren odgovarajući interrupt. Ako virus izmjeni interrupt vektor i izvođenje pojedinih funkcija preusmjeri prvo na sebe, može lako pratiti sva događanja na sistemu i njima bez problema ″vladati″.

# 7. 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 dospijevaju na računalo. Program u sebi ma 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. Postoji više komercijalnih programa za ovu namjenu. Na žalost, korisnici u Hrvatskoj (prema nekim anketama) rijetko kada izdvajaju novac za zaštitu od virusa. Zbog toga se kod nas većina korisnika odlučuje na različite probne inačice antivirusnog programa koje obično imaju ograničeno vremensko trajanje. To je dovelo do toga da su kod nas najčešće korišteni programi kompanije McAffee i Symantec. No bez obzira na to koji program izaberete, u suvremeno programu za ovu namjenu pronaći ćete iste mogućnosti.

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. Osim toga ovakav je oblik zaštite posebno nepovoljan pri radu s Internetom jer se neki virusi koji se šire elektroničkom poštom mogu aktivirati i prije nego što korisnik dobije priliku da podatke provjeri. Stupanj zaštite može se postupno povećavati sve do najvišeg stupnja. 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. Činjenica je da će rad antivirusnog programa ponešto usporiti rad računala. No ovo je usporenje kod suvremenih računala jedva zamjetno, a pruža najviši stupanj sigurnosti. Uzmete li u obzir vrijeme potrebno da računalo očistite od virusa nakon zaraze, kao i ukupne štete koju je virus proizveo uništavajući podatke

vrlo brzo ćete vidjeti da je ovakvo usporenje sasvim prihvatljivo. Zbog toga se ovakav oblik zaštite može slobodno preporučiti svim korisnicima.

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. Zbog toga kompanije koje izrađuju antivirusne programe sve informacije izdvajaju u poseban zapis koji se naziva **biblioteka virusa**. Ovaj zapis sadrži sve podatke potrebne za prepoznavanje virusa i na stranicama kompanije učestalo se pojavljuju nove inačice tog zapisa. Zbog postojanja biblioteke virusa nije potrebno ponovo instalirati antivirusni program, nego treba samo obnoviti vašu biblioteku virusa. Taj proces obično ne traje dugo, a većina današnjih antivirusnih programa čak taj proces obavlja automatski. Znači, kad antivirusni program otkrije da ste se spojili na Internet, on automatski obnovi svoju biblioteku virusa. Međutim, ako antivirusni program to ne obavlja automatski, vi sami morate napraviti. Kako? Pročitajte upute od vašeg antivirusnog programa. Obavezno redovito obnavljajte (update-irajte) antivirusni program, jer u suprotnom bitno ugrožavate sigurnost računala.

# 8. Zaraženo računalo

Što kad računalo oboli? I uz najveće mjere sigurnosti korisniku se može dogoditi da mu na računalo dospije virus. Istini za volju to se obično događa korisnisima koji nisu primijenili sve mjere sigurnosti, odnosno koji su zanemarili upozorenja. Bez obzira na to kako je virus dospio na vaše računalo, morate biti svjesni mogućih posljedica i primjeniti kvalitetne postupke za njegovo uklanjanje. Točno djelovanje virusa zavisi od zamisli autora. No zajedničko je da će odmah nakon zaraze pokušati iskoristiti sve dostupne puteve za daljnje širenje. 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 tom trenutku pred vama je dosta složen i vremenski zahtjevan posao. Potrebno je prvo ukloniti sve zaražene zapise sa 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. Nakon što ste uklonili kopije virusa s računala, provjerite i sve ostale medije (CDR, CDRW, diskete, drugi magnetni mediji...). Naime ako ste na neki od tih medija snimali informacije sa zaraženog računala, moguće je da se i na njima nalazi

kopija virusa. To može učiniti postupak uklanjanja potpuno beskorisnim jer će vraćanje medija u računalo obnoviti infekciju. Ako ni poslije svih ovih koraka ne uspijete skinuti virus s vašeg računala, pozovite profesionalnu osobu ili što je manje popularno, napravite backup podataka, formatirajte hard disk i krenite sa instalacijom računala, iako ni tako niste nažalost 100% sigurni da ste skinuli virus. Nema druge.

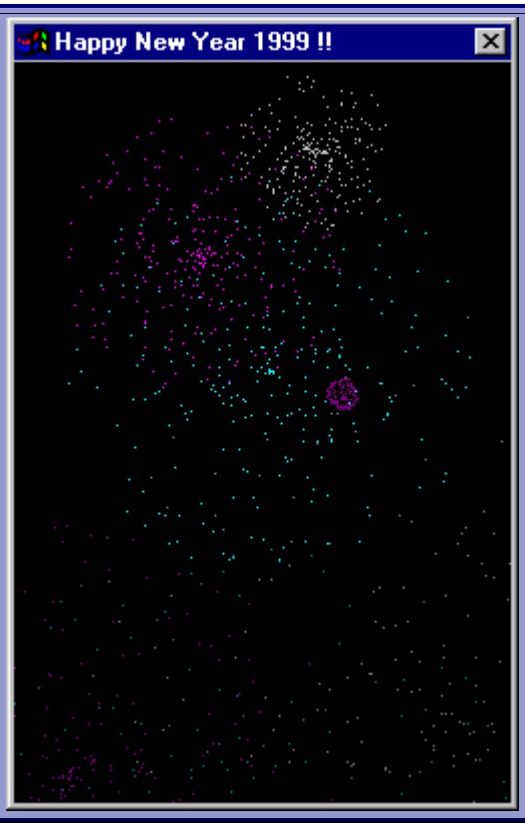
I na kraju, provjerite postupak širenja virusa i razmislite je li se virus s vašeg računala mogao proširiti na neko drugo računalo. Na primjer, jeste li podatke prenosili nekom suradniku , prijatelju ili poznaniku, odnosno je li riječ o virusu koji se širi elektroničkom poštom ili na neki drugi način preko Interneta. Ako je odgovor na bilo koje od ovih pitanja potvrdan, svakako obavijestite korisnike kod kojih se virus od vas mogao proširiti. Potrebno je da i oni poduzmu odgovarajuće mjere čišćenja i zaštitite jer se jedino tako može obuzdati širenje virusa. U protivnom postoji opasnost da se virus ponovno vrati na vaše računalo.

# 9. Neki noviji virusi

**HAPPY 99**

**Ovaj virus se naziva iWin32/Ska.A To je vrsta virusa koji se zove "crv", a napravljen je za E-mail i Novinske grupe. Prikazuje vatromet kada se prvi put izvrši kao Happy99.exe.**

**Uobičajeno on dolazi na određeno računalo kao attachment u E-mail poruci ili se učita sa neke Novinske grupe.**



## TEQUILA

**Ovaj su virus napisala dva brata iz Švicarske.**
**Vrlo ga je teško otkriti jer koristi varijabilni kriptografirani algoritam. Kada se pokrene zaraženi program, virus inficira Master Boot Record hard diska, tako da poslije virus ostane aktivan u memoriji, spreman da dalje inficira .EXE datoteke kad se pokrenu. Zanimljivo je da ovaj virus prikazuje ovakvu sliku na ekranu.**

## ŽIRAFA

**Žirafa ili TPE je virus porijeklom iz Nizozemske. Napisao ga je Masud Khafir 1992., član Triden T virusne grupe; a napisao je uz njega još nekoliko naprednijih virusa. TPE je baziran na kriptografski kodiranim uputama za kompjuter, poznatim kao Masud Kafirov Coffeeshop 3 virus ili TPE.1_0.Girafe.A**

# 10. Pitanja

1) Što je kompjuterski crv?

2) Što je trojanski konj?

3) Što je HOAX?

4) Koja je razlika između rezidentnih i nerezidentnih virusa?

5) Kako se šire virusi?

6) Što je biblioteka virusa?

7) Kako radi antivirusni program i zašto ga koristimo?

8) Što nam je činiti ukoliko nam je zaraženo računalo?

9) Što je stealth?

10) Što je enkripcija?

# 11. Literatura i izvori podataka


- Tom Erjavec: Programski virusi
- http://josip.purger.com/software/stetocine/
- www.cert.hr
- www.sophos.com
- http://www.pefri.hr/~mmilcic/projekt5/vrsteV.htm
- www.elitesecurity.org/tema/28137