FAQ - virusi, antivirusi - Zaštita od virusa i spywarea - OBAVEZNO ZA POČETNIKE 23.08.2003. u 23:26

OBJAŠNJENJA OSNOVNIH POJMOVA **BY SUNDANCE A.K.A SUNNIS**

-opisi virusa su preuzeti iz maturalnog rada Mladena Jovanovića - **Izrada .COM virusa i antivirusa**

1 KOMPJUTORSKI VIRUSI

1.1 ŠTO JE TO VIRUS?

Za definiciju virusa najbolje je uzeti onu dr. Fredericka Cohena po kojoj virus predstavlja program koji može inficirati druge programe, modificirajući ih tako da uključe kopiju njega samoga, koja također može biti modificirana. Pod infekcijom se ovdje misli na mogućnost virusa da ubaci svoje izvršenje u postupak izvođenja programa.

Ova definicija ključna je za određivanje virusa jer ne smatramo svaki maliciozni program virusom, drugim riječima nije svaki destruktivni program virus, jer bi u tom slučaju i program Format bio virus. Struktura virusa može se najlakše podijeliti na tri komponente, od koje virus mora obavezno imati samo prvu.

Prva komponenta predstavlja mogućnost infekcije. Dakle nije nužno da virus radi bilo kakvu štetu na računalu, sama činjenica da se širi infekcijom dovoljna je da ga se okarakterizira kao virus.

Drugi dio virusa, koji nije obavezan, predstavlja nosivu komponentu. Taj dio definira sve aktivnosti koje će biti izvedene uz njegovo širenje.

Treći dio predstavlja funkcija za okidanje koja definira vrijeme ili događaj prilikom kojeg će biti izvršena nosiva komponenta virusa.

Zlonamjerno napisani kompjutorski program ili dijelovi programskog koda nazivaju se raznim imenima. To su crvi (worm), trojanski konji (trojan horse), logičke bombe (logic bomb), zamke (trap-door) i naravno virusi.

1.1.1 **Crv** je program koji se širi samoumnožavanjem kroz kompjuterske mreže. Crv je samostalan i za razliku od virusa ne treba program domaćin da bi radio. Također, crva u ˝pogon˝ pušta i kontrolira sam autor.

1.1.2 **Logička bomba** je metoda aktivacije procesa temeljem zadovoljavanja logičkog uvjeta-postojanja ili nepostojanja nekog podatka, protoka, određenog vremena ili u određeno vrijeme i sl. Logička bomba u stvari predstavlja princip djelovanja, a ne cjelovit mehanizam. Logičke bombe su često sastavni dio mnogih kompjutorskih virusa.

1.1.3 **Trojanski konj** je program koji naizgled služi za neku drugu operaciju od one za koju je napravljen. Trojanski konj bi recimo bio program koji izgleda kao tekst procesor, a zapravo jednom pokrenut formatira hard disk. Mnogi autori virusa koriste trojanske konje kako bi olakšali razmnožavanje svojim mezimcima.

1.1.4 **Zamka** predstavlja posebnu nedokumentiranu funkciju programa koja se može pokrenuti na unaprijed određen način. Programeri koji pišu različite programe često znaju predvidjeti posebnu lozinku ili sekvencu znakova koja jednom utipkana omogućava dostup do inače nevidljivih funkcija programa.

1.1.5 Njegovo veličanstvo **virus** je dio programskog koda koji je sposoban izvršiti samokopiranje (infekciju) dodavanjem svog sadržaja u druge programe ili dijelove operativnog sistema. Kao što se može primijetiti postoji velika sličnost između kompjutorskih i bioloških virusa.

Virus se obično sastoji od dva dijela. Prvi dio je samokopirajući kod, koji omogućava razmnožavanje virusa, a drugi je dio korisni teret (payload) koji može biti bezopasan (benigan) ili opasan (destruktivan, maligan). Neki se virusi sastoje isključivo od samokopirajućeg koda i nemaju nikakav korisni teret.

Iako virus ˝u promet˝ najčešće pušta sam autor, kontrola nad razmnožavanjem oslobođenog virusa nije u rukama autora.

1.2 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 kompjutorske programe na UNIVAC 1108 kompjuterskom sistemu, a napadnuti programi su čak bili označeni posebnom signaturom u svrhu samoprepoznavanja.

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 upotrebio riječ ˝virus˝ opisujući samokopirajući kod.

Prijelomna je i 1986. godina kada se pojavljuje kompjuterski 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.

1.3 VRSTE VIRUSA

Kompjutorski virusi mogu se podijeliti na šest vrsta:

• boot sektor viruse

• parazitske viruse

• svestrane (multipartite) viruse

• viruse pratioce (companion)

• link viruse

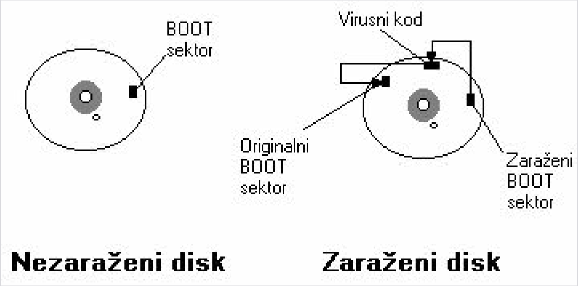
• makro viruse

Ova podjela prvenstveno vodi računa o načinu na koji virus može zaraziti različite dijelove kompjuterskog sistema. Bez obzira kojoj grupi pripada, svaki virusni kod mora biti izvršen da bi proradio i razmnožavao se. Osnovna razlika između različitih virusa je u načinu na koji to pokušavaju osigurati.

Postoji još i podjela na viruse ovisno o tome da li je virus prisutan u memoriji na:

• viruse koji su rezidentni u memoriji
• viruse koji nisu rezidentni u memoriji

1.3.1 Boot sektor virusi



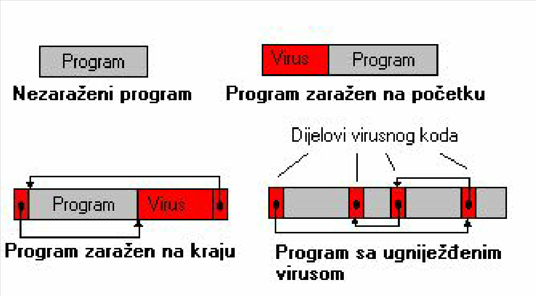
Boot sektor virusi napadaju Master BOOT sektor (partitition table), DOS BOOT sektor (oba na hard diskovima) ili BOOT sektor floppy disketa, odnosno program koji se u njima nalazi. BOOT sektor je idealan objekt za infekciju, budući da sadrži prvi program koji se izvršava na kompjuteru, čiji se sadržaj 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 nakazi 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, nazvanih dropper (bacač) - 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.

1.3.2 Parazitski virusi

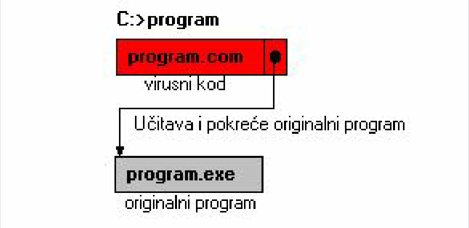


Najčešća vrsta virusa su upravo parazitski virusi. Ovi su virusi sposobni zaraziti izvršne datoteke na kompjutorskom sistemu dodavanjem svog sadržaja u samu strukturu programa, mijenjajući tok inficiranog programa tako da se virusni kod izvrši prvi. Poznati kompjutorski virusi sposobni su zaraziti .COM,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

1.3.3 Svestrani virusi

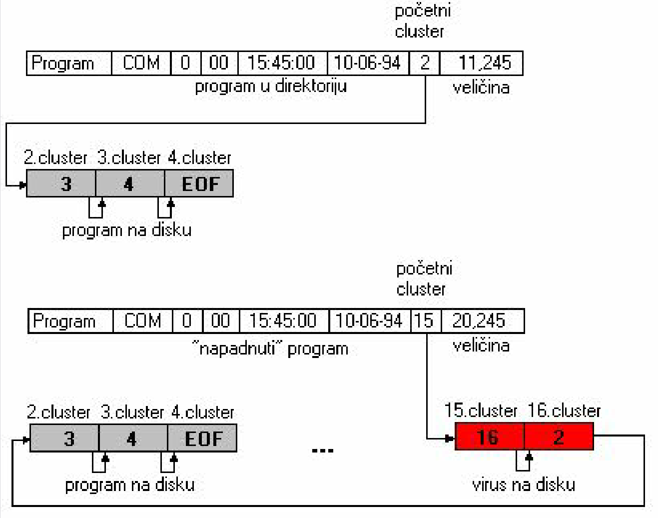
˝Dobre˝ osobine boot sektor i parazitskih virusa ujedinjene su kod svestranih virusa (multipartite) virusa. Ovi virusi sposobni su zaraziti i BOOT sektore i izvršne programe, povećavajući tako mogućnost širenja. Poput boot sektor virusa i ovi su virusi iznimno efikasni u širenju.

1.3.4 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, program 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.

1.3.5 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 kao na disku, ima trenutno samo dva predstavnika i ukupno četiri varijante.

1.3.6 Makro ili skriptni virusi

Najčešći virusi u posljednje vrijeme koriste mogućnost izvršavanja skripti u programima koji su u širokoj upotrebi, npr. Internet Explorer, Outlook i Outlook Express, zatim Word, Excel. Mnogi od tih programa imaju puno sigurnosnih rupa za koje se zakrpe ne izdaju često, a korisnici ih još manje primjenjuju. Ukoliko je sigurnost prioritet pri radu na računalu predlaže se isključivanje skriptnih jezika (Java, VBscript itd.)

1.4 VIRUSI KOJI NISU REZIDENTNI U MEMORIJI

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. Zarazili 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.

1.5 VIRUSI REZIDENTNI 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.

1.6 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 zasštite.

1.6.1 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.

1.6.2 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.

Polimorfizam 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.

1.6.3 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˝.

1.7 PUTEVI ZARAZE

Najčešće postavljano pitanje nakon otkrivanja virusa je ˝kako je do zaraze došlo?˝. Iako su mnoge stvari vezane uz viruse vrlo složene, odgovor na ovo pitanje je više nego jednostavan. Kao što smo rekli svaki virusni kod, da bi se umnožavao, treba prethodno biti izvršen. Neki se programi na kompjuteru izvršavaju voljom korisnika, a neki automatski, bez njegove volje.

1.7.1 Diskete

Floppy diskovi (diskete) su najčešći medij kojima se prenose virusi. Budući da su diskete standardno sredstvo razmjene programa i informacija, njima se odvija i najveći dio komunikacije između korisnika kompjutora. Zapamtite, disketa ne mora biti sistemska da bi prenijela boot sektor virus i zarazila vaš kompjutor.

1.7.2 Izmjenjivi hard-diskovi

Izmjenjivi hard-diskovi, iako se rjeđe koriste također predstavljaju pogodan medij za prijenos svih vrsta virusa.

1.7.3 CD-ROM

CD-ROM-ovi su se pokazali kao odličan medij za prijenos virusa, iako se sa CD-ROM-ova u pravilu ne obavlja startanje sistema pa nisu pogodan medij za prijenos boot sektor virusa. Nezgodna je činjenica da programi i podaci na njima dolaze u komprimiranoj formi, što dodatno otežava pregled antivirusnim programima.

1.7.4 Mreže

Virusi na kompjutorskim mrežama predstavljaju jedan od najvećih sigurnosnih rizika danas, a predstavljat će ga i u budućnosti.

1.8 CRVI

Klasični virusi danas su zapravo rijetki. Današnji korisnici uglavnom se susreću sa crvima. Crvi su maliciozni programi koji se šire računalnim mrežama i računalima, a da pritom ne inficiraju druge programe. Ovdje vidimo osnovnu razliku između virusa i crva, a to je da crvi nemaju prvu i obaveznu komponentu virusa, mogućnost infekcije programa. Crvi obično upotrebljavaju računalnu mrežu ne bi li se širili i danas najčešće na adresu primatelja stižu u vidu privitka poruke elektroničke pošte. Neki drugi crvi za svoje širenje koriste različite sigurnosne probleme, ali svima im je karakteristika da ne inficiraju druge programe.

1.8.1 NAČIN OTKRIVANJA METE

Skeniranje - označava testiranje raspona adresa da se indefiticiraju ranjiva računala. Postoje dvije varijante skeniranja, sekvencijalna ili slučajna. Zbog svoje jednostavnosti to je vrlo čest način širenja crva. Ovo nije jako brz način širenja, ali kod crva sa automatskom aktivacijom širenje može biti vrlo brzo, za što je primjer Blaster ili Code Red I crv. Skeniranjem crv uzrokuje puno abnormalnog mrežnog prometa pa ga se po tome može prepoznati, a neki antivirusni programi i vatrozidi (firewall) automatski reagiraju i ograničavaju taj promet, što može zaustaviti crva.

Prije generirana lista adresa - napadač može napraviti listu adresa prije lansiranja crva na kojima bi bile vjerojatne žrtve. Mala lista bi se mogla iskoristiti za ubrzavanje skenirajućeg crva, a stvaranjem velike liste dobivamo nevjerojatno brzog crva, koji može u nekoliko minuta zaraziti milijune računala. Takav crv osim u laboratorijskim uvjetima još nije napravljen.

Vanjski generirana lista adresa - Vanjski generirana lista je ona koju održava neki neovisni server. Serveri koji imaju popis adresa drugih servera nazivaju se metaserveri. Najbolji primjer za to je servis Gamespy koji održava listu pokrenutih servera nekih od najpopularnijih mrežnih igra današnjice, a kada pogledamo koliko ljudi se igra na internetu dobivamo ogromne liste adresa. Ova tehnika bi se mogla iskoristiti i na tražilicama, jer npr. Google ima listu većine web servera na svijetu. Metaserver crvi još uvijek nisu primjećeni na slobodi, ali rizik je velik zbog velike brzine širenja koju bi crv mogao postići.

Interna lista adresa - Mnoge aplikacije na računalu sadrže informacije o IP ili e-mail adresama drugih računala. Nakon što crv zarazi računalo, pretraži neke najčešće aplikacije u potrazi za adresama i šalje se na na njih. To često viđamo kod novijih crva koji pretražuju adresar u Outlooku i šalju se na sve e-mail adrese koje pronađu. Ove crve je teško otkriti skeniranjem mrežnog prometa jer crv na računalu nalazi adrese računala s kojima se ionako komunicira pa dodatni mrežni promet nije sumljiv.

Pasivni - Pasivni crv ne traži adrese računala žrtve, već čeka da se žrtva javi ili se oslanja na korisnika koji mu otkriva nove mete, naprimjer surfanjem po internetu. Gnuman crv se pretstavlja kao Gnutella čvor, koji se koristi za distribuiranu izmjenu podataka (većinom glazbe i filmova) na internetu. Kada se žrtva javi sa zahtjevom za određenom datotekom crv šalje sebe. Iako potencijalno spori, pasivni crvi ne proizvode abnormalni mrežni promet pa ih je teško otkriti.

1.8.2 NAČIN ŠIRENJA

Samonoseći - Samonoseći crv sam sebe prenosi kao dio procesa infekcije. Ovaj mehanizam je čest kod samoaktivirajućih skenirajućih crva, gdje je čin infekcije ujedno i prenošenje crva, kao naprimjer kod crva CRClean.

Sekundarni kanal - Neki crvi, kao naprimjer Blaster, zahtjevaju sekundarni komunikacijski kanal da izvrše infekciju. Iako Blaster koristi sigurnosnu rupu u RPC, računalo žrtva otvara TFTP kanal preko kojeg se prenosi sam crv, završavajući proces infekcije.

Umotani - Taj tip crva se prenosi kao dio normalnog komunikacijskog kanala, ili dodavajući se normaloj poruci ili zamjenjujući ju. Kao rezultat dobivamo širenje koje izgleda kao normalni mrežni promet, pa je crva teže otkriti.

1.8.3 AKTIVACIJA CRVA

Ljudska aktivacija - Najsporiji način aktivacije zahtjeva da crv uvjeri lokalnog korisnika računala da izvrši lokalnu kopiju crva. Da bi potakli korisnike autori crva se koriste raznim tehnikama socijalnog inžinjeringa. Neki kao Mellisa crv glume hitno pismo od poznanika ("Attached is an important message for you"), neki kao Iloveyou crv ciljaju na taštinu korisnika ("Open this messege to see who loves you"), a neki kao Benjamin koriste pohlepu ("Download this file to get copyrighted material for free"). Dok neki zahtjevaju pokretanje privitka kojeg dobivamo e-mailom, neki (npr. Klez) koriste sigurnosne propuste u Outlooku i samim gledanjem poruke računalo je zaraženo.

Aktivacija ljudskim postupkom - Neki crvi se nemogu pokrenuti automatski prilikom zaraze, ali mogu zapisati svoje podatke na bilo koje mjesto na disku, pa se onda pokreću prilikom resetiranja sustava ili logiranja na sustav.

Zakazani proces aktivacije - Neki prilično brzi crvi koriste zakazane sistemske procese. Mnogi operativni sistemi i programi imaju mogućnost automatskog unaprijeđivanja programa skidanjem novije verzije sa određene adrese. Ako autor crva zamijeni zakrpu programa crvom, ili ga nadoda u zakrpu on će se nakon skidanja automatski izvršiti. Ako program nema provjeru autentičnosti izvora, dovoljno je najobičnijije DNS preusmjeravanje adresa da se računalo zarazi.

Samoaktivacija - Uvjerljivo najbrži način širenja crva. Operativni sustavi i razni programi puni su sigurnosnih propusta koji omogućuju neovlašteno pokretanje programa, npr. Code Red koristi IIS Web server koji dolazi zajedno sa Windows operativnim sustavom. Takvi crvi se dodaju pokrenutim procesima i koriste njihova dopuštenja za pokretanje programa. Najbolja zaštita je redovito stavljati sigurnosne zakrpe na ugrožene programe.

1.8.4 TERET

Teret je drugi naziv za kod koji crv nosi, a ne služi za njegovo širenje. Taj kod je limitiran jedino ciljem i maštom autora crva.

Nepostojeći/Nefunkcionalan - Najčešći slučaj kod većine crva je upravo ovaj, kada ne postoji kod osim koda za širenje, ili u njemu postoji nekakva pogreška pa nije funkcionalan.

Daljnska kontrola - Code Red II je otvarao tzv. backdoor na računalu žrtvi, dajući svakome sa web tražilicom mogućnost pokretanja programa na žrtvinu računalu. Postojali su i anti-Code Red internet stranice koje su taj backdoor koristile da maknu crva i resetiraju računalo, pa ono više nije bilo zaraženo.

Spam relays - Dio crva Sobig kreira "mail relay" koji spammeri mogu koristiti da bi slali neželjenu elektroničku poštu. Većina internet providera ima sigurnosne mehanizme koji blokiraju spam sa poznatih IP adresa, ali kod zaraze ovim crvom spam dolazi sa svih strana i nemoguće je na taj način kontrolirati njegovo širenje.

HTML-proxiji - Još jedna osobina crva Sobig je distribucija HTML-proxija. Preusmjerujući web zahtjeve preko mnogo proxija web stranice sa zabranjenim sadržajem dobivaju na vremenu jer providerima treba puna vremena da otkriju na kojoj se adresi web stranica fizički nalazi. Ovo se koristi za razne nelegalne aktivnosti, uključujući prijevare sa upisivanjem financijskih podataka ili brojeva kartica.

Internet DOS - Još jedan česti teret je internet DOS (Denial Of Service) napad. Code Red, Yaha i još mnogo crva sadrže DOS alate, koji su ili upereni protiv određene stranice ili se mogu uperiti protiv bilo koga ako autor crva to zaželi. Kada crv zarazi 100 000 ili više računala zombija moguće je nedostupnom učiniti bilo koju stranicu, pa čak i cijeli DNS sustav!

Skupljači podataka - Većina ljudi na računalu na kojem rade imaju osjetljive podatke poput poslovnih tajni, nacrta novih uređaja, financijskih izvješća itd. Crv može pretražiti disk računala u potrazi za tim podacima i zatim ih poslati na prije određeno mjesto. SirCam crv je vršio nenamjernu špijunažu, jer je slučajnu datoteku sa diska slao slučajnoj osobi iz adresara na računalu.

Brisači podataka - Postoji mnogo virusa, kao naprimjer Chernobyl koji su sadržavali kod za brisanje podataka nakon određenog vremena. Budući da se crvi mogu širiti mnogo brže, mogli bi početi brisati podatke odmah nakon infekcije. Podaci bi mogli biti i kodirani umjesto prebrisani da bi se izvukli iz sustava.

Daljinska kontrola - Postoje računala koja kontroliraju razne mehanizme i naprave u fizičkom svijetu. Svima nam odmah padaju na pamet vojna računala koja kontroliraju razne mehanizme obrane, ali zapravo je velik dio elektronike koja nas okružuje kompjuterski kontroliran. Crv bi mogao preuzeti kontrolu nad sustavom i predati ju napadaču, to jest autoru crva.

DOS napad u fizičkom svijetu - Crv bi mogao preuzeti veliki broj računala i preko ugrađenih modema pozivati neki broj, naprimjer 92 i time tu liniju onemogućiti jer će biti konstantno zauzeta.

Fizička šteta - Većina današnjih računala podržava nadogradnju pokretačkog softvera, pa tako i računala imaju BIOS čip koji je moguće flashati direktno iz Windowsa. Ukoliko se u flash čip upišu pogrešni podaci računalo se više neće moći pokrenuti.

Održavanje crva - Zadnja klasa tereta je ona koja služi održavanju crva. Crvi kao Sonic i Hybris su pregledavali Usenet grupe i kriptografski provjeravali module koje su tamo nalazili prije svoje nadogradnje.

1.9 PREPOZNAVANJE VIRUSA - ANTIVIRUSNI PROGRAMI

Današnje antivirusne programe možemo podijeliti na dvije skupine - programe za prepoznavanje specifičnih virusa i programe za nespecifično prepoznavanje virusa.

1.9.1 Skeneri

Skeneri su u pravilu programi za specifično prepoznavanje virusa, mada bi neki od njih, koji koriste heurističke metode traženja virusa, mogli biti svrstani u grupu programa za nespecifično prepoznavanje virusa, budući da su, bar teoretski, sposobni prepoznati i nepoznate viruse. Skener tradicionalno prepoznaje virus na temelju (u njega) ugrađenih podataka, koji su prethodno pribavljeni analizom virusa koji se pojavio među korisnicima. Ti podaci mogu se odnositi na niz heksadecimalnih znakova (search string) - koji katkad mogu sadržavati i *wildcard* (džoker) znakove.

Glavna prednost skenera je mogućnost trenutnog otkrivanja poznatih virusa jednostavnim pregledom sumnjivog sadržaja. Ako skener prepozna virus, on će dojaviti točno o kojem se virusu radi, a to je vrlo korisno jer se prema tom podatku mogu procijeniti i moguće posljedice napada virusa. Pravilno korišten skener pomoći će nam da otkrijemo virus na pristiglim disketama PRIJE nego zarazi štićene kompjutore.

Nedostaci skenera odnose se na potrebu za stalnim dograđivanjem radi prepoznavanja novonastalih virusa, no nemogućnost prepoznavanja virusa o kojima nemaju potrebne podatke. Iako postoje heuristički skeneri, sposobni za otkrivanje novonastalih, nepoznatih virusa, koji su bazirani na tehnologiji znanja (knowledge based), kao i svaki takav sustav ima i puno mana.

Skeneri su danas najrasprostranjeniji antivirusni softver.

1.9.2 Provjera checksum-om

Tehnika provjere checksumm-om temelji se na mogućnosti prepoznavanja svake promjene na štićenom sadržaju. Checksumm-om se ˝zaledi˝ stanje sustava za koji prethodno utvrdimo da je neinficiran. Nakon toga se u određenim vremenskim razmacima provjerava da li je na sustavu došlo do nekih promjena.

Checksummiranje je jedina poznata metoda kojom se sigurno otkloniti svi virusi, bez obzira na to jesu li poznati ili ne. Ova činjenica čini checksummere jednim dugoročnim osloncem svake mudre antivirusne strategije.

Nedostatak checksummera leži u činjenici da se njima otkriva infekcija virusom tek nakon što se već dogodila, međutim, njihovom redovitom primjenom sigurno se može otkriti virus prije nego što dođe do značajne štete.

1.9.3 Programi za motrenje

Programi za motrenje najčešće rade kao TSR koji pregledava odvijanje pojedinih funkcija sistema preko odgovarajućih interrupta. Tako npr. kad god sistem dobije nalog za učitavanjem neke izvršne datoteke, može se i izvršiti provjera. Neki monitori ne traže specifične viruse nego pokušavaju otkriti sumnjive aktivnosti kao što su primjerice pisanje po Master BOOT sektoru ili izvršnim programima, pokretanje formatiranja diska, pokušaj programa da se učini rezidentnim u memoriji i sl. Jedina prednost monitora je da mogu otkriti virus u realnom vremenu.

Nedostaci monitora su brojni. Najveći nedostatak je nemogućnost djelotvorne primjene TSR programa koji bi u sebi sadržavao podatke za prepoznavanje svih poznatih virusa. Monitori koji otkrivaju sumnjive aktivnosti često izazivaju brojne lažne uzbune, jer označavaju sumnjivim i redovne aktivnosti kao što su formatiranje disketa ili instaliranje raznih programa u memoriju.

1.10 POSLJEDICE NAPADA VIRUSA

U pravilu, svaki program inficiran virusom već je u određenoj mjeri oštećen i potrebno ga je dovesti u ispravno stanje. Ovo se dešava uvijek, bez obzira na to da li virus ima tkz. korisni teret i bez obzira koja mu je namjera. Danas je sve veći trend izrade virusa koji pri infekciji jednostavno prepišu dio koda napadnutog programa i na taj način nepopravljivo oštete napadnuti objekt. Na primjer link virusi mogu napraviti pravi krš na disku jer dovode do tkz. cross-linked datoteka.

Program zaražen virusom može griješiti u radu, virus koji se instalira u memoriju može izazvati greške u radu drugih programa koji se instaliraju u memoriju ili može programima oduzeti memoriju potrebni za rad. Mnogi pisci kompjutorski virusa uključuju u virus koristan teret, kod koji je sposoban izvršiti neku zadaću kao što je npr. ispisivanje poruka, ometanje rada sistema, brisanje određenih podataka, formatiranje diska ili korupcija podataka.

Blesave poruke, nemušte ljubavne izjave ili usamljeničke rođendanske čestitke - najmanji su dodatni problem. Nedestruktivno ometanje rada sistema, blokiranje kompjutora, usporenje rada stroja - predstavljaju drugu stepenicu. Očigledno brisanje programa i podataka ili formatiranje diska, koliko je god nezgodno i štetno nije najveći stupanj oštećenja, kako to mnogi misle. Ako se redovito provodi temeljito arhiviranje podataka, već nakon kraćeg vremena kompjutor može biti ponovno osposobljen i spreman za rad. Najgori mogući oblik štete je korupcija podataka, neprekidno i progresivno propadanje integriteta ili točnosti podataka. Korupcija podataka može biti izazvana namjerno ili se javiti slučajno. Oštećene mogu biti baze podataka, arhivi s programima i podacima, tekstualne datoteke i sl. Slučajan oblik korupcije je kada virus greškom inficira tekstualnu datoteku. Datoteka će biti oštećena, a virus u toj datoteci neće se moći razmnožavati.

Namjeran oblik korupcije je kada virus pregleda disk u potrazi za bazama podataka, te u nađenoj nasumice izmjeni neki podatak. Ako korupcija traje dulje vrijeme doći će do nepopravljivih posljedica. Arhiviranje podataka nije dovoljna zaštita od korupcije podataka, jer ako ona ne bude otkrivena tijek jednom jednog punog ciklusa arhiviranja, podaci će biti nepopravljivo oštećeni, budući da će sve arhivske kopije sadržavati oštećene podatke. Jedina zaštita od korupcije podataka je provjera njihovog integriteta, pri čemu nije dovoljno provjeravati samo vanjski, već i unutrašnji integritet.

1.11 ČIŠĆENJE VIRUSA

U antivirusne programe možemo još ubrojiti i programe za čišćenje virusa koji mogu biti izrađeni za čišćenje specifičnih ili nespecifičnih virusa.

U prvu grupu dolaze programi koji na temelju poznavanja određenog virusa i metoda kojom inficira program, pokušavaju odstraniti virus i program dovesti u ispravno stanje.

Druga grupa su programi za nespecifično čišćenje virusa. Neki su autori pokušali razviti programe koji bi izolirali i spremili na sigurno kritične dijelove rizičnih sadržaja (BOOT sektore, headere i duljinu izvršnih datoteka i sl.), te nakon otkrivene infekcije pokušavali stvari dovesti na svoje mjesto. Budući da se ova metoda zasniva na predviđanju moguće štete, njena sigurnost je vrlo upitna.

1.12 POPULARNIJI VIRUSI

FormB
BOOT sektor virus
Podrijetlom iz Švicarske, 18. dana svakog mjeseca virus proizvodi zvukove prilikom tipki na tastaturi. Prema nekim podacima na njega otpada 40% svih infekcija.

New Zealand (Stoned, Marijuana)
BOOT sektor virus
Virus ispisuje ˝LEGALISE MARIJUANA˝. Uzročnik oko 20% infekcija.

Tequila
Svestrani virus
Pdrijetlom iz Švicarske. Enkriptirani, polimorfni virus. Iscrtava na ekranu grubi mandelbrot. Oko 10% infekcija izazvano je ovim virusom

Spanish Telecom (Anti-Tel, Anti-CTNE)

Svestrani virus Enkriptirani, stealth virus.
Poruka u virusu navodi da je izrađen u Španjolskoj. Nakon 400 startanja sistema virus prepiše podatke na dva tvrda diska. Zaslužan za 10% infekcija.

Cascade (Fall, Russian, Halstorm, 170h)
Parazitski virus
Enkriptirani virus koji napada .COM datoteke. Originalna verzija uzrokuje ˝padanje˝ znakova s ekrana između 1.studenog i 31. prosinca 1988. Formatirajuća verzija formatira disk između istih datuma svake godine. Izaziva oko 7% infekcija.

Joshi
BOOT sektor virus
Virus iz Indije koji 5. siječnja ispisuje poruku ˝Type `Happy Birthday Joshi`˝. Ako korisnik poruku ne otipka doslovno, kompjuter će se ˝objesiti˝. Virus koristi stealth i preživljava worm boot (CTRL-ALT-DEL). Joshiu rođendan čestita oko 5% zaraženih.

Michelangelo
BOOT sektor virus
To je mutacija virusa New Zealand, koja 6. ožujka prepiše hard-disk. Nalazi se u oko 2% infekcija.

Q: Želim naučiti pisati viruse. Odakle da počnem?
A: Pisanje virusa, crva i slicnih malicioznih programa zahtjeva neke osnovne programerske vjestine. Najbolje je poceti sa C-om i polako uciti win32asm. Za win32asm su najbolji Iczelionovi tutoriali koji su u novije vrijeme lokalizirani (vidi link na asm forumu) i to barem prvih desetak poglavlja u kojima su objasnjeni osnovni principi. Nakon toga procitajte sljedece tutoriale:

http://www.29a.host.sk/29a-4/29a-4.202
http://vx.netlux.org/lib/static/vdat/tutorial.htm#LJ

Maticni siteovi za pocetnike u asmu na win i linuxu:
www.win32asm.cjb.net
http://linuxassembly.org/

Najpopularniji win32 asembleri su tasm32 i masm32. Kojekakve spasm, fasm i HLA p.m. su cista egzotika. Ako planirate pisati linux viruse, nemojte koristiti gas jer koristi ruznu AT&T sintaxu koja je zbunjujuca i posve neprikladna za pisanje programa sa vise od 100-ak instrukcija (neki se GNU fanatici i dalje kunu u njega, ali oni si oni...). yasm je takodjer ok jer moze generirati flat binary output. za linux viruse su korisni ovi linkovi:

http://www.29a.host.sk/29a-4/29a-4.205
http://www.inet.hr/~sunnis/theory/ljinuks.txt
http://www.big.net.au/~silvio/
http://www.lwfug.org/~abartoli/virus-writing-HOWTO/_html/

Jako je korisno poznavanje formata izvrsnih datoteka, PE na win32 i ELF na unix sistemima:

http://frizemall.narod.ru/pefmt120.zip
http://www.29a.host.sk/29a-4/29a-4.210
http://spiff.tripnet.se/~iczelion/files/pe1.zip
http://spiff.tripnet.se/~iczelion/files/pe-tuts.zip
http://www.msdn.microsoft.com/…g/issues/02/02/PE/default.aspx
http://www.msdn.microsoft.com/…/issues/02/03/PE2/default.aspx

Osim pisanja binarnih virusa, u novije je vrijeme (zadnjih 5-6 godina) iznimno postalo popularno pisanje crva i raznih samopropagirajucih skripti. Skriptni virusi nisu odvec kvalitetni i pisu ih obicno osobe kojima nedostaje znanja u pisanju non-script virusa, tj. koje zele da napisu nesto brzo (makar bilo nekvalitetno), ali barem da radi. Shell skriptanje je s druge strane prilicno evoluiralo i pojavilo se nekolikom kvalitetnih clanaka o perl i bash skriptama:

http://www.29a.host.sk/29a-6/29a-6.212
http://www.29a.host.sk/29a-6/29a-6.220

Q: Gdje mogu skinuti izvorne kodove virusa i odgovarajuce binarne fileove da ih mogu secirati?
A: Sirenje virusa je u svim manje-vise civiliziranim zemljama *ilegalno*, a s obzirom na cinjenicu da se vecina danasnjih virusa/crva samostalno siri na bezbroj nacina, ukoliko se samostalno zarazite i postanete makar nenamjerno baza za sirenje novih generacija, imajte na umu da mozete biti zakonski procesuirani.

Izvorni kodovi i prateci binarni oblici virusa dolaze obicno u zineovima u kojima se oni predstavljaju javnosti, dok cete teze naci binarne fileove na osobnim stranicama virusopisaca ukoliko su hostani na nekom free servisu. Dobra baza za pocetak jest kolekcija od strane bcvg:
http://www.ebcvg.com/category.php?cat=1&p=1

Q: Nisam neki talent za programiranje, sto je sa ovim trojan generation kitovima i sl. alatima?
A: NGVCK i sl. alati obicno proizvode fileove koji su skoro 100% detektabilni od strane AV (antivirusa). S obzirom da vecina AV koriste byte signature za detekciju trojana napisanih u HLL, koristenje kojekakvih packera moze pomoci, iako danas i AV imaju ugradjene dekompresore za upx i sl. Druga su stvar razni morphing alatichi tipa CodePervertor/Revert.

Q: Koji je najbolji antivirus?
A: Dva su (donekle) relevantna testa, one koje provode oni sami koji prave antiviruse:

http://www.virusbtn.com/vb100/

i oni koji prave viruse:

http://www.virus.gr/english/fullxml/default.asp?id=16&mnu=16

-primjetite da nijedan nema 100% :)

Uglavnom tih nekoliko najboljih su stalno pri vrhu.

Neka misljenja od strane vx-era: [29a #6]:

Citat:

> Results for the "bests of 20th century" poll were published. Results:
>
> Who was the best VX group?
> 29A with 28 votes. (53,84% / 54,90%)
> 1 vote in blank.
>
> Who was the best virus coder?
> Vecna with 24 votes. (46,15% / 47,05%)
> 1 vote in blank.
>
> Who was the best virus collector?
> VirusBuster with 30 votes. (57,69% / 71,42%)
> 10 votes in blank.
>
> What was the best virus web site?
> No winner in this category: coderz.net and Asterix site both had 8 votes. (15,38% / 18,60%)
> 9 votes in blank.
>
> What was the best virus?
> Hybris with 16 votes. (30,76% / 36,36%)
> 8 votes in blank.
>
> What was the best virus zine?
> 29A with 27 votes. (51,02% / 54,00%)
> 2 votes in blank.
>
> Who was the best antivirus coder? (person, not company)
> Eugene Kaspersky with 13 votes. (25,00% / 61,90%)
> 31 votes in blank.
>
> Who was the best virus analyzer from antivirus companies? (person, not company)
> Eugene Kaspersky with 11 votes. (21,15% / 52,38%)
> 31 votes in blank.
>
> What was the best antivirus product?
> Antiviral Toolkit Pro with 35 votes. (67,30% / 81,39%)
> 9 votes in blank.
>
> What was the best antivirus company?
> Kaspersky Labs Pro with 27 votes. (51,92% / 69,23%)
> 13 votes in blank.
>
> What was the best antivirus web site?
> **www.avp.ru** (Kaspersky Labs) with 27 votes. (51,92% / 65,85%)
> 11 votes in blank.

I za kraj neki korisni linkovi:

VX-eri koji nisu hostani na nekoj od zajednica

http://z0mbie.host.sk/
http://anaktos.host.sk/
http://www2.coderz.net/belial/
http://www.geocities.com/SiliconValley/Code/3403/
http://www.geocities.com/Area51/Dimension/8145/
http://www.angelfire.com/ak5/bumblenet/index.html
http://www.delly.fr.st/
http://www.geocities.com/ratty_dvl/BATch/main.htm
http://eos.host.sk/
http://members.fortunecity.com/svl/
http://utenti.lycos.it/g1ld0/index.html
http://gl-st0rm.wz.cz/index2.html
http://griyo.hellsparty.com/
http://himan.by.ru/
http://kenerman.ar.gs/
http://litesys.host.sk/
http://members.fortunecity.com/m0n30/
http://vx.netlux.org/~melhacker/
http://www.nbk.hpg.ig.com.br/index.htm
http://raenius.cjb.net/
http://ppacket.20m.com/
http://psyx.gq.nu/
http://pbat.cjb.net/
http://pxr.wz.cz/
http://www.volny.cz/radix16/
http://www.fortunecity.com/skyscraper/cyburbia/28/
http://stress.8m.net/under/index1.html
http://net.supereva.it/sad1cpage/index.html?p

http://www.spth.de.vu/
http://sennaspy.cjb.net/
http://www.ikarus-software.at/portal/index.php
http://www.tokugawa.es.vg/
http://vampir0.by.ru/
http://vovan-smf.wz.cz/
http://pagina.de/wintermute/
http://mitglied.lycos.de/yoda2k/index.htm
http://membres.lycos.fr/zemckiller98/index.html

TRADING

http://www.virustrading.com/traders.php
http://mions.wz.cz/
http://vx_satanikchild_vx.tripod.com/main.htm
http://usuarios.lycos.es/bigblok/
http://www.gold.pl/basketcase/
http://members.tripod.com/thermopyle/
http://www.virusbuster.tk/
http://akap.com.ne.kr/trade.htm
http://welcome.to/BuddyMusic
http://home.megapass.co.kr/~acy78/
http://www.geocities.com/nexus_crusader/
http://www.geocities.com/Muncher_98/
http://it.geocities.com/loscriba/index.html
http://www.geocities.com/jahmmm70/
http://www.virus.gr/english/fullxml/default.asp
http://vx.netlux.org/~nfission/
http://www.mr-virus.cc/vlog/
http://www.perikles.tk/
http://frizer.tsx.org/
http://www.virustrading.com/roadkil/
http://neptune.spaceports.com/~stram/
http://ggnome.cjb.net/
http://virax.cjb.net/
http://www.geocities.com/algol_p/
http://www.geocities.com/cyphonix/
http://www.geocities.com/stagglevx/
http://aappoocc.virtualave.net/
http://strony.wp.pl/wp/polish_basketcase/
http://cyberviper.chat.ru/
http://www.websamba.com/panoix/
http://nathan.wirefire.com/
http://vx.netlux.org/~toxic/highres.htm
http://www.geocities.com/vanbluefish/
http://www5c.biglobe.ne.jp/~TRNEY/
http://www.nemesizz.host.sk/
http://www.funkymonkey.org/tiker/
http://whitemaster.pisem.net/
http://www.virustrading.com/asad/
http://stadt.heim.at/hongkong/150414/
http://www.numentec.com/aver/seak/
http://www.virustrading.com/buddy/
http://stress.8m.net/under/index.html
http://lovingod.host.sk/eindex.htm

VX grupe

http://29a.host.sk/
http://www.geocities.com/SiliconValley/Bay/3056/
http://www.ebcvg.com/
http://brigada8.cjb.net/
http://cip.host.sk/
http://vx.netlux.org/~fat/
http://skyscraper.fortunecity.com/dos/819/
http://www.linezer0-tribe.tk/
http://vx.netlux.org/~nitz/
http://www.rrlf.de/
http://hackers.b3.nu/
http://teamnecrosis.20m.com/
http://vdxgroup.host.sk/
http://www.virus.go.ro/
http://sbvc.cjb.net/
http://www.virusbrasil.8m.com/

ZAJEDNICE

http://vxers.host.sk/
http://vx.netlux.org/
http://coderz.net/
http://www.virustrading.com/

RAZNI RESURSI

http://coderz.net/zines/
http://madchat.org/vx/

BESPLATNI anti-malware programi 04.12.2004. u 03:55

BESPLATNI ANTIVIRUSI

AVG Free Edition

avast! 4 Home Edition

AntiVir Personal Edition

F-Secure Anti-Virus for DOS

BitDefender Free Edition

ClamWin - upozorenje, ovaj open source piece of crap je **vrlo** supalj

MicroWorld Anti Virus Toolkit - on-demand skener

BESPLATNI FIREWALLOVI

Windows Firewall

ZoneAlarm Free

Agnitum Outpost Personal Firewall Free

Sygate Personal Firewall Standard

Kerio Personal Firewall Free

Tiny Personal Firewall

Look 'n' Stop Lite - postaje *Lite* nakon sto istekne *trial*

Jetico Personal Firewall Beta

SoftPerfect Personal Firewall

Filseclab Personal Firewall

Omniquad Personal Firewall

CHX-I Packet Filter i/ili NAT - nije za pocetnike

Securepoint Personal Firewall & VPN Client

Firewall 2004

Primedius Firewall Lite

Sphinx A-Wall Personal Firewall

SafeZone Free

Enigma Firewall

Xeon Personal Firewall

BartWare Personal Firewall

GoldTach Free

Firewall Builder - nije za pocetnike

ON-LINE VIRUSNI SKENOVI

BitDefender

Kaspersky

Dr. Web

Panda ActiveScan

PC-cilin

PC Pitstop

RAV

Trend Micro Housecall(ActiveX)

Trend Micro Housecall(Java)

Mcafee Virusscan Online

Symantec Security Check (Norton AV)

eTrust

Freedom - bazirano na f-prot Pro engine-u

f-prot

commandondemand

ON-LINE SPYWARE SKENOVI

spy audit

provjera za parazitima

još jedna i **još jedna** provjera za parazitima

PestPatrol - razni spyware, samo detektira

Winguard - klasičan spyware

XCheck

SpywareInfo

CounterSpy

Xblock

ON-LINE SIGURNOSNI SKENOVI

BLACKCODE - trojanci

GFI TrojanScan - trojanci

PC Flank - trojanci, sigurnost browsera, privatnost

Pop-up test - provjerite koliko ste šuplji za *pop-ups*

SPECIJALIZIRANI PROGRAMI ZA MICANJE VIRUSA

McAfee AVERT Stinger

Microsoft Malicious Software Removal Tool

avast! Virus Cleaner

AVG vcleaner

Panda PQRemove

Sophos SAV32CLI

NOD32 - odaberite virus sa padajuće liste na glavnoj stranici

Symantec - odaberite odgovarajući virus na stranici

http://www.kaspersky.com/removaltools - odaberite odgovarajući virus na stranici

Trend Micro Sysclean

F-Secure - odaberite virus sa padajuće liste na glavnoj stranici

BitDefender - odaberite odgovarajući virus na stranici

(...)
Microsoft AntiSpyware - MS-ov anti-shitware alat, štiti i od dialera, nekih trojana, otimača browsera, realtime zaštita motri više od 50 različitih postavki!

SpywareBlaster - alat protiv *spyware-a*

SpywareGuard - alat koji u stvarnom vremenu (real-time) sprečava da neki program otme vaš *browser*

Spybot-Search&Destroy - još jedan alat za zaštitu i micanje *spyware-a*

Ad-Aware Personal - odličan alat za micanje *spyware-a*, što Spybot S&D ne nađe, ovaj hoće!

Ewido - alat sa velikom bazom signatura protiv trojana, *dialer-a*, crva i ostale gamadi..

HijackThis - protiv gamadi koja se nakači na vaš browser, **popis BHO i *toolbar-a***, **LSP-ova**, za listu gamadi koja se pokreće automatski sa windozima vidi komentar za Autoruns.

Script Defender - spriječite izvršavanje potencijalno malicioznih skripti!

System Safety Monitor - spriječite neke kompleksnije napade poput *DLL injection*, *rootkit-ove*, također prati promjenu *registry-a*, win32 servisa, postavka IE-a...

FileChecker - program koji prati promjenu važnih sistemskih fajlova od strane malicioznih programa

WinPatrol - alat za zaštitu koji ima veliku bazu *malware-a*

a^2 Free (a-squared) - odličan komplement za AV, ima veliku bazu *malware-a*.

Prevx Home - jedan od najnaprednijih besplatnih alata koji pruza širok spektar zaštite od *malware-a*.

IE-SPYAD - spriječite kompromitiranje IE-a. Za detaljne upute vidi post dolje.

[**Ovu poruku je menjao Sundance dana 21.01.2005. u 23:44 GMT+1**]

[**Ovu poruku je menjao Sundance dana 23.01.2005. u 01:55 GMT+1**]

[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

BESPLATNI alati za poboljsanje sigurnosti sustava **04.12.2004. u 03:57**

ProcessGuard - napredan alat za povecanje sigurnosti OS-a

RegistryProt - zastitite registry od modifikacije od strane zlocudnih programa, idealno protiv trojana koji se podizu automatski sa windozima

WMP Scripting Fix - sprijecite skriptne napade na Windows Media Player

CCleaner i **RegSeeker** - optimizacija sistema (registry, privremeni fajlovi) - ubrzajte svoju masinu!

Filemon - alat koji u stvarnom vremenu prati operacije nad fajlovima, odlicno za dijagnozu problema

Regmon - alat koji u stvarnom vremenu prati operacije nad registryem, takodjer idealno za dijagnozu problema

TCPView i **TDIMon** - napredni alati za dijagnozu problema mrezom, za dijagnozu problema povezanih sa trojanima..

Autoruns - jedan od najboljih alata koji moze iskljuciti programe koji se pokrecu sa windozima, popis najpopularnijih i dobrih i losih mozete naci **ovdje** i **ovdje**.

Process Explorer - najnapredniji i najbolji preglednik i analizator aktivnih procesa na svijetu! Idealno za upoznavanje sa sistemom i trazenje aktivnog malware-a. Popis procesa koji su poznati ili dio windoza mozete naci **ovdje**

[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

GENERIČKE UPUTE ZA MICANJE VIRUSA I TROJANACA **10.12.2004. u 06:02**

GENERIČKE UPUTE ZA MICANJE VIRUSA I TROJANACA

ovaj tekst je (uglavnom) napisao kolega NOD32 evangelist Blackspear@wilderssecurity.com, ja sam samo prevoditelj (uz dopuštenje ofkors :)

Disklejmer: **SVE KORAKE OVDJE OPISANE ČINITE SAMO I ISKLJUČIVO NA VLASTITI RIZIK.**

I NEMA NIKAKVIH GARANCIJA DA ĆE USPJETI.

BAŠ NIKAKVIH.

ČAK NI TIH.

Molim ISPRINTAJTE ove upute i pročitajte ih u POTPUNOSTI prije nego što krenete dalje..

Slijedite korake onako kako su napisani, JEDAN PO JEDAN.

NEMOJTE ići jedan korak naprijed sve dok niste završili onaj na kojem ste sad.

Također provjerite da li imate NAJSVJEŽIJE verzije svih programa ovdje navedenih i/ili da su u potpunosti *update-ovani*.

Ako nemate AV (Antivirus), skinite jednog **OVDJE** i napravite *update* virusne baze.

KORAK 1. Skinite **WinSock XP Fix**. **NEMOJTE ga još pokrenuti.**

KORAK 2. Ako nemate FW (Firewall), skinite i instalirajte neki besplatni kao što je **ZoneAlarm** - FW sa VIZUALNIM UPOZORENJIMA tako da možete vidjeti koji programi žele pristupiti Internetu. Lista besplatnih se nalazi **ovdje**

KORAK 3. Skinite besplatni alat **Stinger**. **NEMOJTE ga još pokrenuti.**

KORAK 4. Skinite **jedan** od ovih Anti-Trojan programa: **TDS-3 (Trojan Defence Suite) - evaluacijska verzija**, **TrojanHunter - evaluacijska verzija** ili **ewido - besplatan, *plus* verzija je evaluacijska**. Instaliraj i nadogradi bazu trojana. **NEMOJTE ga još pokrenuti.**

KORAK 5. Instaliraj **Spybot Search and Destroy** - besplatan alat za micanje i zaštitu od *spyware-a*, sa *registry* monitorom. Instaliraj i nadogradi bazu. **NEMOJTE ga još pokrenuti.**

KORAK 6. Skinite **Ad-Aware**. Ovaj će besplatni program detektirati svu gamad koju ne detektira Spybot Search and Destroy, vrijedi i obrnuto :) Instaliraj i nadogradi bazu. **NEMOJTE ga još pokrenuti.**

KORAK 7. Skinite CWShredder **odavde** ili **odavde** - besplatan alat protiv jedne kategorije *malware-a*. Instaliraj i nadogradi bazu. **NEMOJTE ga još pokrenuti.**

KORAK 8. Skinite **VX2 Cleaner** - besplatan alat za micanje specifičnog *spyware-a*. **NEMOJTE ga još pokrenuti.**

KORAK 9. OBAVEZNO NADOGRADITE BAZU SVOG ANTIVIRUSA PRIJE NEGO NASTAVITE.

KORAK 10. Ugasite *System Restore* prije nego što nastavite, ovo se odnosi samo na Windows ME i Windows XP.

UPOZORENJE: Gašenje *System Restore* znači da više NEĆETE moći vratiti OS u prijašnje stanje.

Upute za **Windows XP** (**upute sa slikama na engleskom**)

1. Desni klik na **My Computer** ikonicu na Windows desktopu.

2. Kliknite na **Properties**.

3. Kliknite na **System Restore** tab.

4. Označite kvačicom opciju **Turn off System Restore on all Drives**.

5. Kliknite **OK**.

6. Zatvorite aktivne programe i restartajte komp.

ILI

Upute za **Windows ME** (**upute sa slikama na engleskom**)

1. Desni klik na **My Computer** ikonicu na Windows desktopu.

2. Kliknite na **Properties**.

3. Kliknite na **Performance** tab.

4. Kliknite na **File system**.

5. Kliknite na **Troubleshooting**.

6. Označite kvačicom opciju **Disable system restore**.

7. Kliknite **OK**.

8. Zatvorite aktivne programe i restartajte komp.

KORAK 11. Restarajte vaš komp u ***SAFE MODE-u*** tako što ćete za vrijeme podizanja Windowsa pritiskati taster **F8**. Probajte ovo nekoliko puta ako ne uspije iz prve.

Ako i dalje ne radi *boot-anje* u *Safe mode*, pogledajte upute na **ovoj** stranici (na engleskom).

KORAK 12. Izbrišite privremene (engl. *temporary*) datoteke sljedećim koracima:

Otvorite *Internet Explorer*.

Kliknite na **Tools**

Kliknite na **Internet Options**

Kliknite na **General** tab.

Kliknite na **Temporary Internet Files**.

Klikinte na **Delete Files**.

Klikinte na **Delete All Offline Content**.

Dok ste u *Safe mode* uradite **SVE** od sljedećih koraka i OSTANITE U SAFE MODE-U sve do koraka 19:

KORAK 13. Pokrenite sken sa programom *Stinger* kojeg ste skinuli u 3. koraku.

KORAK 14. Pokrenite sken sa anti-trojan programom kojeg ste skinuli u 4. koraku.

KORAK 15. Pokrenite sken sa *Spybot Search and Destroy* programom kojeg ste skinuli u 5. koraku.

KORAK 16. Pokrenite sken sa *Ad-Aware* programom kojeg ste skinuli u 6. koraku.

KORAK 17. Pokrenite sken sa *CWShredder* programom kojeg ste skinuli u 7. koraku.

KORAK 18. Pokrenite sken sa *VX2 Cleaner* programom kojeg ste skinuli u 8. koraku.

KORAK 19. Restartajte vaš komp u **NORMAL MODE**

KORAK 20. Pokrenite *online* virusni sken koji se nalazi **ovdje** ili jedan sa **ove** liste.

KORAK 21. **OBAVENO I BEZ IZLIKA** napravite **KOMPLETAN** *update* svoje Windows mašine sljedećim koracima:

1. Za vrijeme dok ste spojeni na Internet kliknite na ikonicu od *Internet Explorer-a* (plavo "e");

2. Kliknite na **Tools**.

3. Kliknite na **Windows Update** opciju u meniju.

Ovo će vas odvesti na stranicu od *Windows Update* gdje trebate slijediti upute čarobnjaka za instaliranje, počevši od *EXPRESS INSTALL*. Instalirajte **SVE** *Critical Updates* i *Service Pack-ove*.

PONAVLJAJTE GORE NAVEDENE KORAKE 3 PUTA, jer neki virusi, trojani i spyware se znaju jako duboko zakopati u sustav..

Ako nakon ili za vrijeme gore navedenih koraka vaša Internet veza **jednostavno prestane raditi**, pokrenite *WinSock XP Fix* program kojeg ste skinuli u 1. koraku.

ILI

Uradite sljedeće korake da biste izbrisali koruptirane *registry* ključeve i reinstalirali TCP/IP protokol.

KORAK 1. Izbrišite koruptirane *registry* ključeve:

1. Kliknite **Start** dugme, kliknite na **Run**.

2. Upišite **regedit** i kliknite **OK**.

3. U *Registry Editor-u* dođite do sljedećih ključeva i za svakog od njih kliknite **Delete**:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock2

4. Kad vam iskoči dijalog za potvrdu da li želite izbrisati, kliknite na **Yes**.

5. Restartajte komp.

KORAK 2. Instalirajte TCP/IP:

1. Desni klik na vašu konekciju na net (LAN/modem ikonica, stogod, ako ne znate gdje su u *Windows Explorer-u* upišite **Network Connections** i klikinte *enter*) te kliknite na **Properties**..

2. Kliknite na **Install**.

3. Kliknite na **Protocol** i kliknite na **Add**.

4. Kliknite **Have Disk**.

5. Upišite **C:\Windows\inf** i kliknite **OK**.

6. Na listi dostupnih protokola odaberite **Internet Protocol (TCP/IP)** i kliknite **OK**.

7. Restartajte komp.

Nakon što ste prešli sve navedene korake podijelite sa nama Vaše iskustvo kako bismo svi nešto novo naučili...

[**Ovu poruku je menjao Sundance dana 18.01.2005. u 16:00 GMT+1**]

[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

Re: FAQ - virusi, antivirusi **19.12.2004. u 00:18**

Pošto ima dosta problema oko uklanjanja virusa/crva/trojanaca odlučio sam napisati jedan «osnovni» tutor za uklanjanje malocijozni programa.

Mnogi misle da je uklanjanje malocijozni programa neka posebna vještina ali nije, za to samo trebaš malo znati o OS (Operativni Sistem) i neke fore koje virusi koriste. Kod nekih malocijozni program nepa spasa nego komanda

Code:
```
Format C
```

. Lai se većina malocijozni programa da ukloniti.

Uklanjanje:

Za početak instalirajte AntiVirus i obnovite mu definicije, zatim vidite je li on što našao, ako je i može ukloniti onda nema problema ali ako nemože onda morate pokušati sami ukloniti. A to radite ovako:
1.Potražite sumljive procese u task menegeru, ako je on disejblan obrišite ovaj ključ u registri bazi:

Code:
```
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr
```

. Zatim uklonite «sumnjivi proces»
2. Pritisnite Start>Run i unesite

Code:
```
msconfig
```

odatlem također uklonite sumljive startup fajlove.
3. Pritisnite Start>Run i unesite

Code:
```
regedit
```

. U registriju ima dosta fora koje malocijozni programi koriste, većina tih fora rade na principu da sakriju/uklne neke alate koji se nalaze u Windowsu npr. (sakrivanje sata, skrivanje runa, zaključavanje registrija i task menegera itd. Većina tih fora nalaze se tu:

Code:
```
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
```

&

Code:
```
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\
```

odatle izbrišite sumljive ključeve, ali pazite prije ikakog brisanja napravite backup baze. Pogledajte imate li i što ovdje:

Code:
```
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun\
```

kao te također izbrišite jer to zabranjuje pokretanje nekih programa. I još sami malo prozujajte registrijem...
4. Restartajte PC. Ako i dalje imate probleme ponovite ovo toče od 1 do 3. Ao i dalje imate probleme provajte ih ukloniti sa System Restorom

Code:
```
%SystemRoot%\System32\restore\rstrui.exe
```

pokrenite ga i vratite sistem u neku prijašnju točku.

Sa gore navedene toče trebali bi riješt vaš problem sa malocijoznim programima. Za više informacija kontaktirajte me na PP ili vrkljan@gmail.com Sva pitanja možete ovdje postaviti, ubrzo e još ovdje doći neki linkovi. Puno sreće

---
-=VrKy=-

[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

Upute protiv spyware-a **18.01.2005. u 00:15**

Pošto smo primetili da dosta ljudi postavlja teme u kojima traže rešenja za različite probleme sa Windowsom i Internetom, a za koje se kasnije ispostavi da su posledica virusa ili spyware-a, Sundance i ja smo pripremili ovo malo uputstvo u kome možete pročitati kako da na pravi način zaštitite svoj sistem od zlonamernih programa, i napada sa Interneta...

1. INSTALIRAJTE SERVICE PACK 2 ZA WINDOWS XP, I PODESITE SIGURNOSNE PARAMETRE U

WINDOWSU I INTERNET EXPLORERU

Najčešći uzrok inficiranja *malware-om* su preniski sigurnosni parametri vašeg OS-a i browsera. Postoji mnogo načina za poboljšanje sigurnosti, a neki od najpraktičnijih su sledeći:

a) Pazite šta skidate sa Interneta! Klijenti za P2P (peer to peer) mreže poput Kazaa, eMule... su često uzrok problema jer se na njima nalazi masa programa koji dolaze sa integrisanim *spyware-om*. Osim toga, većina današnjih crva obavezno imaju metodu širenja preko P2P mreža tako što se iskopiraju u *shared* direktorijume i to pod imenima tipa *teen_porn.avi*, *winamp_6_preview.exe*, tj. uglavnom pod imenima za koje misle da bi mogli ciljati na širu publiku i da bi ih ljudi mogli masovno skidati. Pazite na veličinu takvih programa, instalacija Photoshopa od 300KB je gotovo sigurno virus! Obavezno sve skinute datoteke naknadno skenirajte sa AV.

b) Ako imate Windows XP obavezno razmislite o instalaciji SP2. Najbolje na *clean* instalaciju Windowsa jer će to eliminisati veliki broj problema sa kompatibilnošću sa već instaliranim programima. Nakon instaliranja SP2 proverite i uradite sledeće:

1. Desni klik na **My Computer**

2. Kliknite na **Properties**

3. Kliknite na **Automatic Updates**

4. Odaberite vreme koje vam odgovara.

Nadalje:

1. Desni klik na **My Computer**

2. Kliknite na **Properties**

3. Kliknite na **System Restore**

4. Kvačica na **Turn off System Restore on all drives** mora biti ISKLJUČENA.

Iako *System Restore* može pomoći prilikom nekih problema sa Windowsom, mnogi virusi mogu ostati u *System Restore* direktorijumu zato što AV programi često skeniraju taj direktrorijum, ali ga ne mogu dezinficirati, ili ga uopće ne skeniraju!

1. Pokrenite IE tj. **Internet Explorer**

2. Kliknite na **Tools**

3. Kliknite na **Windows Update**

4. Instalirajte SVE *update-ove* vezane za sigurnost (security)!

Najbolje da odaberete opciju za *Express Install* i prepustite se čarobnjaku za instalaciju.. Obavezno proverite da li je vaša instalacija Java VM (*Virtual Machine*) *up-to-date* jer velik broj *malware-a* koristi propuste u njemu.

Dok ste još u IE:

5. Kliknite na **Tools**

4. Kliknite na **Internet Options**

5. Kliknite na **Security**

6. Označite ikonicu **Internet**

7. Kliknite na **Default Level**.

Nakon toga kliknite na **Custom Level** i dođite do dela za *ActiveX* i uverite se su postavljene sledeće opcije:

1. Promenite **Download signed ActiveX controls** na **Prompt**
2. Promenite **Download unsigned ActiveX controls** na **Disable**
3. Promenite **Initialize and script ActiveX controls not marked as safe** na **Disable**
4. Promenite **Installation of desktop items** na **Prompt**
5. Promenite **Launching programs and files in an IFRAME** na **Prompt**
6. Promenite **Navigate sub-frames across different domains** na **Prompt**

Kliknite **OK**. Iskočit će vam poruka koja će vas pitat da li želite spremiti postavke, kliknite na **Yes**. Nakon toga kliknite na **Apply** dugme da se promene apliciraju pa kliknite na **OK** dugme za izlaz.

Ubuduće će vam se za sve *ActiveX* kontrole koje žele biti pokrenute i instalirane pokazati prozor sa pitanjem da li želite dozvoliti njihovo izvršavanje. Za sajtove za koje ste 100% sigurni da su OK (recimo od *Windows Update* i sl.) možete dodati pod **IE->Tools->Internet Options->Security->Trusted sites**.

ActiveX objekti su jako opasni, i kad dopustite vašem browseru da ih izvršava to je isto kao da ste sami kliknuli na neki .exe na disku. Zato **NIKAD** ne instalirajte *ActiveX* kontrole sa xxx, warez, cracks sajtova, **MA KOLIKO PUTA ISKAKALI POP-UP PROZORI ZA NJIHOVU INSTALACIJU**.

Detaljnije upute o podešavanju sigurnosti IE-a imate **ovdje**, a najbolje je da koristite besplatan program

Enough is Enough! koji većinu opisanih stvari radi automatski.

2. UKLJUČITE FIREWALL

U *Security Center-u* Windowsa XP SP2 se nalazi Microsoftov firewall koji pruža osnovnu zaštitu i sa SP2 je dobio i kontrolu aplikacija koje izlaze na mrežu. Može da bude dovoljan kao osnovno rešenje, ali ako želite bolju zaštitu možete instalirati neki drugi firewall. Postoji veliki izbor besplatnih i komercijalnih firewalla, pogledajte listu besplatnih **ovde**. Prvih nekoliko je sortirano po popularnosti/kvalitetu, oni na dnu liste se ne preporučuju početnicima.

Pogledajte **ovaj** test ukoliko se ne možete odlučiti za neki na listi, a nakon što ste se odlučili, možete proveriti koliko je vas FW siguran preko nekog od URL-ova s ove liste:

ON-LINE SKENOVI ZA PROVERU SIGURNOSTI SISTEMA

SG Security Scan Information.

Broadband

Shields UP!

AuditmyPC

GFI Email Security Testing Zone

Mail relay testing

YALTA firewall leaktest

Tooleaky firewall leaktest

BlackCode Security Scan

Takođe ukoliko mislite analizirati statistike blokiranih upada vašeg FW-a, dobro će vam doći sledeće alatke:

DODACI ZA FIREWALLE

ZoneLog Analyzer - za analizu ZoneAlarm logova

VisualZone - vrlo lep i doteran analizirator ZoneAlarm logova, ima mogućnost slanja na **DShield**

VisualICE - analizator upada za BlackIce Defender

myNetWatchman - centralizirana analiza logova za ZoneAlarm, BlackICE Defender, Windows XP ICF/ Windows Firewall...

3. INSTALIRAJTE ANTIVIRUS

Za zaštitu od virusa, crva, trojanaca morate imati instaliran antivirusni program. Za razliku od firewall-a u windowsu zasad ne postoji integrisano rešenje, pa morate nabaviti odgovarajući antivirus. Osim komercijalnih rešenja Kasperskog, Nortona, Pande... postoje i **besplatni** antivirusi. Za diskusiju oko kvaliteta pojedinih AV pogledajte **ovu** i **ovu** temu na Virii forumu.

Ukoliko još niste instalirali antivirusni software, ili možda niste sigurni da vaš antivirus pruža odgovarajuću zaštitu možete uraditi **online virus scan**, bez instalacije antivirusa. Sama nabavka antivirusa nije garant sigurnosti. Da bi ste bili sigurni morate redovno sa neta skidati nove definicije, inače će antivirus samo zauzimati memoriju, a zaštita će biti slaba.

4. REŠITE SE REKLAMNIH I ŠPIJUNSKIH PROGRAMA, I ISKLJUČITE SUMNJIVE PROCESE U SVOM KOMPJUTERU

Pre nekoliko godina se pojavila interesantna ideja da uz besplatne programe dobijete i "dodatak" koji prikazuje reklame i skuplja informacije o vama. Kad su kompanije uvidele da ovo prolazi kod korisnika postali su sve nametljiviji, i ovo je postao ozbiljan problem. Otišlo se dotle da se prilikom posete određenim sajtovima instalira aplikacija koja menja početnu stranu, izbacuje prozore s reklamama i kada niste na netu...

Pojavili su se brojni programi za zaštitu od Spyware-a, najpopularniji su **AD-Aware SE**, i **SpyBot Search & Destroy**. I njih je potrebno redovno ažurirati, da bi bili dobro zaštićeni, pošto se novi spyware stalno pojavljuje.

Program sličan *Spybotu* jest i **SpywareBlaster** koji štiti od spyware-a u svojoj bazi tako što blokira njihove *ActiveX* objekte. Skinite i instalirajte ga i videćete listu spyware-a koju program može detektovati. Označite **select all** i **kill all checked** i gotovi ste. Na ovaj način ste postavili *kill bit* za sav spyware u bazi i ova je mogućnost SpywareBlaster-a slična *Immunize* mogućnosti *Spybot-a*. Nije naodmet imati ih oba instalirana.

SpywareGuard je takođe odličan besplatan program koji služi kao komplmenent *SpywareBlaster-u* i omogućuje *real-time* zaštitu (zaštitu u realnom vremenu). Zaštita u realnom vremenu je slična, kao kad rezidentni modul antivirusa blokira pokretanje izvršnih datoteka koje su zaražene nekim virusom, samo sto *SpywareGuard* to radi za spyware! Takođe ima opcije za *Download Protection* i *Browser Hijacking Protection* koje će onemogućiti maliciozne programe da otmu *homepage* vašeg omiljenog Internet *browser-a*. (Napomena: *SpywareGuard*-ova zaštita u realnom vremenu ne znači da u isto vreme ne možete imati i antivirus uključen, čak je preporučljivo imati oba!)

IE-SPYAD je program koji će staviti više od 5000 sajtova u *Restricted Zone* i tako vas zaštiti kad odete na neki sajt koji se čini da je potpuno nevin, a u stvari sadrži *malware*. Takođe će vas zaštiti od skripti, *ActiveX* i *Java* programa te *cookies* koje možete pokupiti sa tih sajtova. IE-SPYAD2 verzija ovog programa služi za instaliranje za **sve** korisnike na mašini. Ako ste vi jedini korisnik tada će vam biti dosta i IE-SPYAD.

Ovaj *IE HOSTS fajl* će vas zaštiti od reklama, *cookies*, te većine otimača *browser-a* tako što će *HOSTS* fajl blokirati server koji bi navedene poslastice ponudio vašem *browser-u*. Takođe vam na taj način ubrzava surf, te štiti privatnost tako što blokira servere koji "pamte" vaše navike pri surfovanjnju koristeći *click-thru tracking* metodu.

HOSTS fajl se instalira tako što prvo skinete **hosts.zip** i *HOSTS* fajl u njoj dearhivirate u odgovarajući direktorijum:

Windows XP => **C:\WINDOWS\SYSTEM32\DRIVERS\ETC**
Windows 2K => **C:\WINNT\SYSTEM32\DRIVERS\ETC**
Win 98\ME => **C:\WINDOWS**

Nedavno je Microsoft izdao beta verziju svoj *anti-spyware* alata zvanog (zamisli samo) **Microsoft AntiSpyware**. Stvar je fenomenalna, ali je trenutno još u beta verziji tako da bismo je preporučili samo za one koji vole živeti "na rubu". Posebno treba istaknuti opcije za vraćanje postavki otetog browsera, brisanje tragova korištenja dokumenata, auto-update i *realtime* monitor koji prati više od 50 različitih klasa postavki!

Pošto još uvek ne postoji software koji 100% sigurno uklanja spyware preporučujem da instalirate sve spomenute programe, koji su se najbolje pokazali kad rade zajedno (ali koristite samo jedan *realtime* monitor!).

Na kraju bi bilo najbolje posetiti **Jason's Toolbox** gde ćete možda malo više naučiti gde je vaš omiljeni *browser* najviše ranjiv.

IE ima notornu povijest sigurnosnih problema, iako je *update-ovana* verzija manje-više sigurna od šireg *adware-a*, bilo bi korisno kao sigurnosnu mjeru razmisliti o alternativnim browserima tipa **Firefox** ili **Opera** ili **Mozilla**

Ukoliko ne vjerujete softveru koji radi i na linuxu, onda koristite napredne i uberkewl ljuske za IE poput **Maxthon** koji IE proširuju sa super-korisnim dodacima poput tabova, *mouse gestures*, automatsko blokiranje reklama na stranicama i pop-upova, skinovi, zaštita privatnosti...

5. URADILI STE SVE NAVEDENO, ALI SE KOMPJUTER I DALJE ČUDNO PONAŠA....

Možda je u memoriji aktivan neki proces koji ovi programi nisu prepoznali. Aktivne procese možete videti ako startujete *C:\windows\System32\taskmgr.exe* koji se još pokreće i kombinacijom <CTRL>+<ALT>+<DEL>. Besplatan, puno napredniji program koji daje jako detaljne informacije o aktivnim procesima i win32 servisima jest i **Process Explorer**. Spisak procesa sa objašnjenjima pogledajte **ovde**.

Još jedan program koji izbacuje listu aktivnih procesa, *ActiveX dodatke*, *start-up* programe.... koji mogu biti potencijalno opasni je **HijackThis**. Pošto ovaj program izlista sve aktivne stvari, i korisne i štetne brišite samo stvari za koje ste 100% sigurni da predstavljaju opasnost. Za to možete konsultovati **google**, ili postaviti pitanje na forumu. Ovaj program sam naveo zato što sam jedino uz pomoć njega uspeo da očistim neke aplikacije, i trebalo bi ga koristiti samo kad je neophodno.

Na **ovom** domaćem sajtu možete videti spisak windows start-up programa i servisa, sa objašnjenjima, kao i uputstva za zaštitu i ubrzanje vašeg kompjutera.

[**Ovu poruku je menjao Sundance dana 18.01.2005. u 16:45 GMT+1**]

[**Ovu poruku je menjao Sundance dana 20.01.2005. u 01:37 GMT+1**]

[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

IE-SPYAD - Instalacija i podešavanje 18.01.2005. u 12:49

IE-SPYAD - Instalacija i podešavanje

IE-SPYAD je *Registry* datoteka (IE-ADS.REG) koja dodaje dugu listu sajtova i domena koje su poznate kao izvorišta reklama, oglašivača i *malware-a* u *Restricted* zonu IE-a. Jednom kad je ova lista sajtova ubačena u vaš *Registry*, većina takvih sajtova koji su izvorišta reklama, oglašivača i *malware-a* na Internetu neće moći koristiti *cookie-e*, *ActiveX* kontrole, Java *applet-e* ili skriptanje da bi kompromitirali vašu privatnost ili PC dok surfate Internetom. Niti će moći koristiti vaš *browser* da vam ubace nepoželjne *pop-up-e*, *cookie-e* ili auto-instalirajuće programe.

Imajte na umu činjenicu da IE-SPYAD nije blokator reklama. On neće blokirati standardne *banner* reklame u IE-u (za takve stvari koristitie ljuske za IE poput **Maxthon** koji imaju ugrađen napredni mehanizam blokiranja svih vrsta reklama i čime štedite ne samo na brzini surfanja, već su i stranice preglednije i manje šarene) - ono što *Restricted* lista sajtova poznatih oglašivača i širitelja malware hoće uraditi jest sljedeće:

- spriječiti neželjeni *malware* od instalacije Vama "iza leđa" dok surfate i skidate programe

- spriječiti otimanje Vašeg *homepage-a* i ostalih postavki IE-a

• ugasiti *ActiveX*, *Java-u* i skriptanje, tj. mehanizme koji omogućuju širenje reklama i kompromitiranje privatnosti i sigurnosti

• blokirati *cookie-e* koji mogu biti korišteni za praćenje vašeg surfanja Internetom.

• boriti se protiv dosadnih skriptnih *pop-up-a* koji nagrđuju surfanje i prisiljavaju vas na gledanje neželjenih reklama

Da biste skinili i instalirali IE-SPYAD molimo posjetite link na dnu ove stranice. IE-SPYAD se regularno nadograđuje i instrukcije za instaliranje najnovijih *update-a* su također na stranici.

IE-SPYAD će raditi samo sa IE (*Internet Explorerom*), ne i sa drugim *browser-ima*.

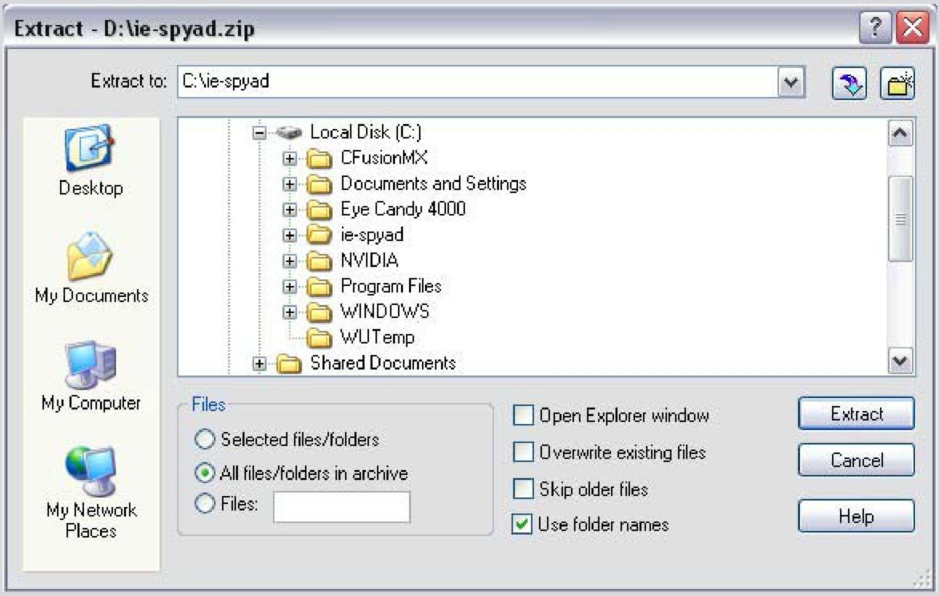
1. Kako instalirati i podesiti IE-SPYAD dodatak za *Internet Explorer*

Za početak posjetite sljedeću web stranicu:

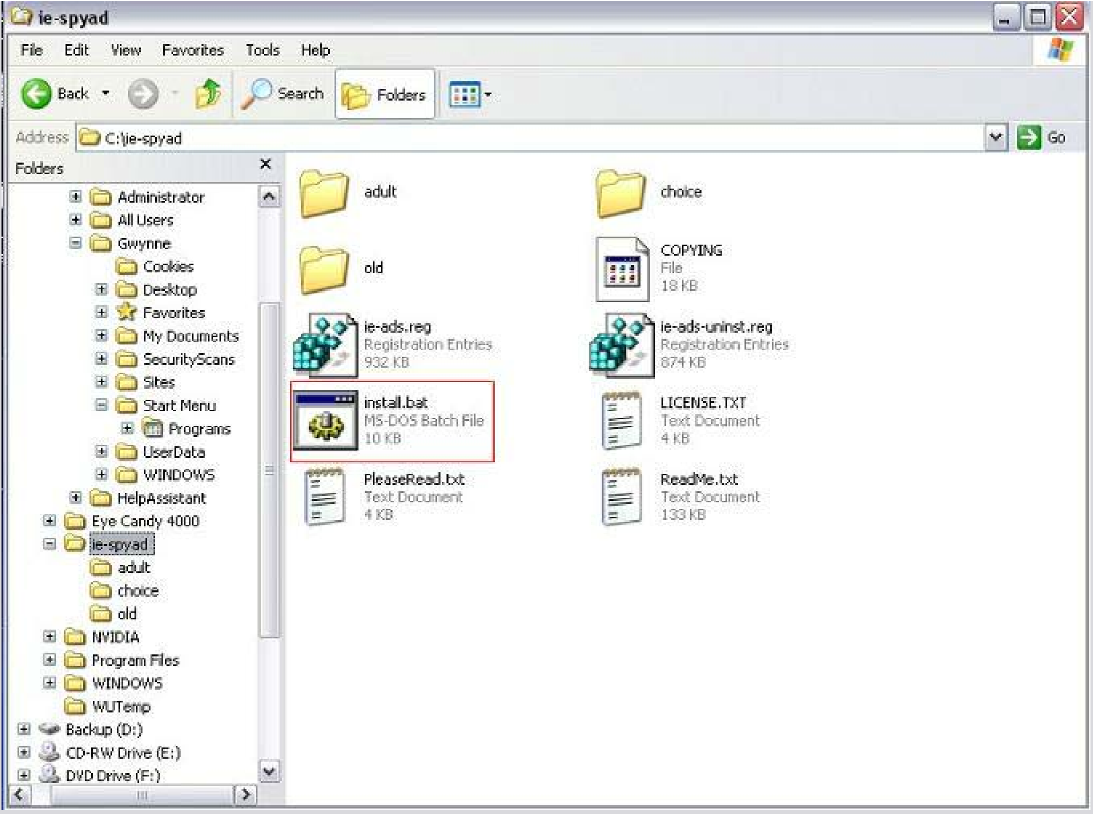
https://netfiles.uiuc.edu/ehowes/www/resource.htm

Bilo bi dobro da (ako znate engleski) pročitate sve informacije tamo tako da se upoznate sa načinom na koji IE-SPYAD radi te pročitate informacije o licenci.

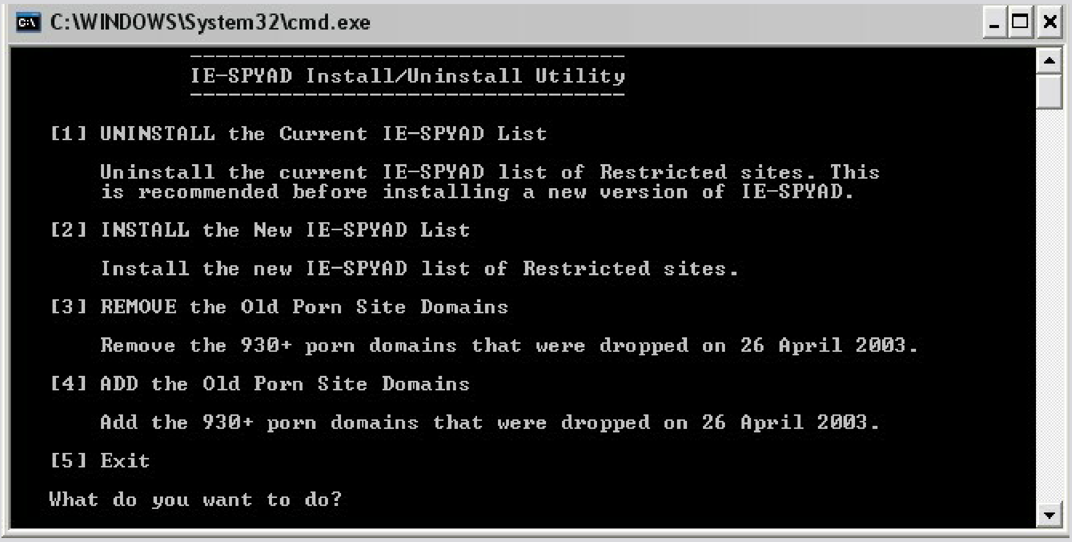
Skinite IE-SPYAD **zip datoteku** ili verziju preko **samoraspakirajuće arhive** te je spremite na pogodnu lokaciju na vašem disku. Kreirajte folder za IE-SPYAD i ekstrahirajte zip datoteku u taj folder.



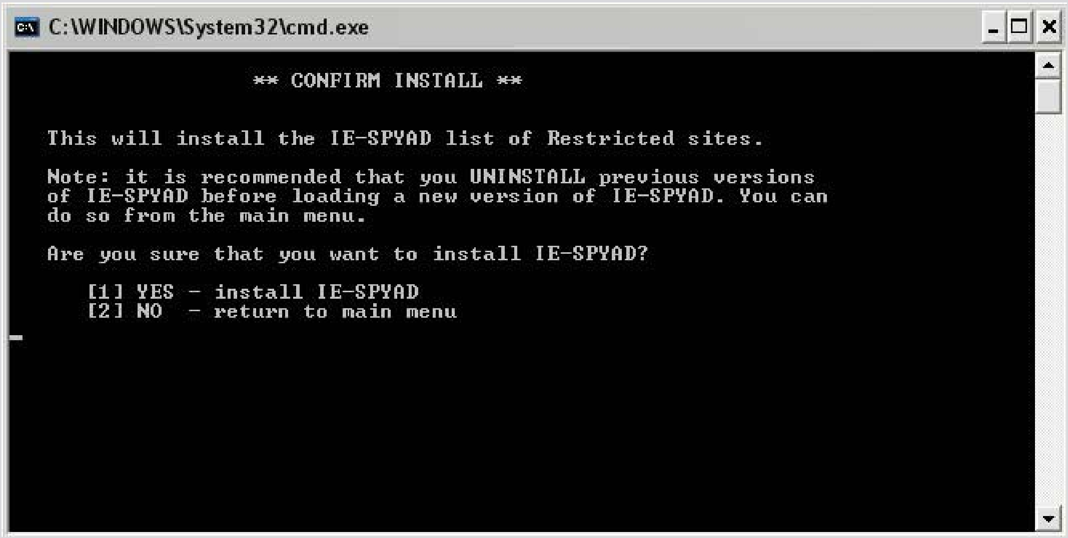
Jednom kad se ekstrahirali sve datoteke, pozicionirajte se u folder te napravite dvoklik na **install.bat** datoteku.



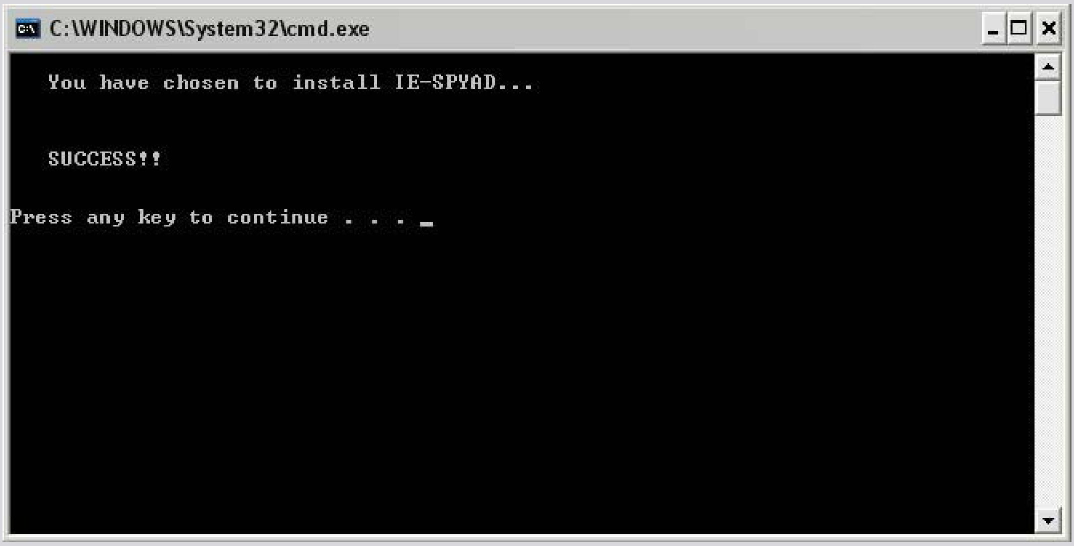
Iskočit će DOS-ovski prozor koji će vam ponuditi razne opcije.



Ako instalirate IE-SPYAD **prvi put**, pritisnite **2** na Vašoj tastaturi, pri čemu će vam se prikazati sljedeća poruka:



Pritisnite **1** na Vašoj tastaturi i IE-SPYAD će se instalirati.



Sada možete pritisnuti bilo koji taster za nastavak ili **2** za izlaz.

2. Konfigurirajte *Restricted* zonu za sajtove

Ako već niste konfigurirali *Restricted* zonu za sajtove na postavke maksimalne sigurnosti, tada biste to trebali napraviti, jer inače IE-SPYAD neće pravilno funkcionirati. Uradite sljedeće:

1. Pokrenite **Internet Explorer**.

2. Kliknite u meniju na **Tools**.

3. Kliknite na **Internet Options**.

4. Kliknite na **Security** tab.

5. Kliknite na **Restriced sites** ikonicu.

6. Kliknite na **Custom Level** dugme.

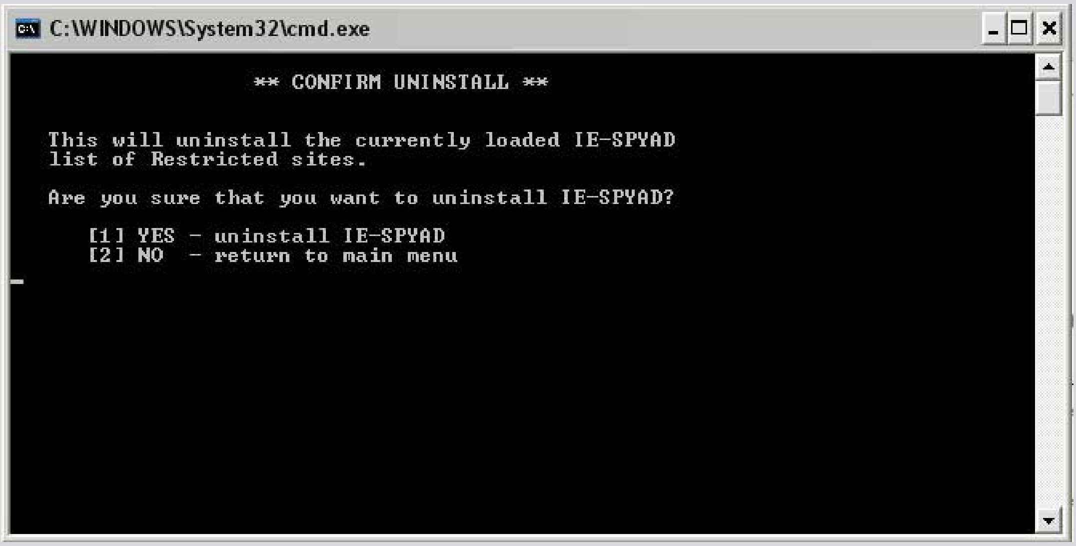
7. Označite **svaku** stavku unutar postavki na ili **Disable** ili **Prompt** ili **High safety**, ovisno o tome što je ponuđeno. Posebnu pažnju obratite na stavku **Use Pop-up Blocker** koji ostavite na **Enable**.

8. Kliknite **OK** 2 puta.

Sad ste spremni ste za sigurno surfanje!

3. Kako nadograditi IE-SPYAD

Kada izađe nova verzija IE-SPYAD, skinite sa službene stranice novu zip datoteku na prikladno mjesto na hard disku. Nakon toga trebate deinstalirati Vašu trenutnu verziju. Da biste to napravili, dođite do vašeg IE-SPYAD foldera i napravite dvoklik na **install.bat** datoteku koja će otviriti DOS-ovski prozor. Ovog puta želite deinstalirati pa pritisnite **1** na tastaturi kao što je prikazano na slici:



Opet pritisnite **1** na tastaturi.

Možete pritisnuti bilo koji taster za nastavak i **2** za izlaz iz programa. Sada se možete vratiti na početak ovog teksta i pratiti upute za instalaciju nove verzije IE-SPYAD.

NE ZABORAVITE REDOVNO NADOGRAĐIVATI IE-SPYAD

[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

HOSTS datoteka i šta sa njom **20.01.2005. u 05:52**

Uvod

Kada se većina Internet korisnika spaja na web sajtove, ftp serveri ili drugi Internet serveri se spajaju na ime domene, kao što je npr. **www.elitesecurity.org**. Internet aplikacije ne komuniciraju sa imenama domena, već sa IP adresama, kao što je npr. 192.168.1.1. Stoga kad unesete ime domene u program koji se želite na nju spojiti (recimo Vaš *browser*), program je prvo treba pretvoriti u IP adresu na koju će se spojiti.

Način na koji se to ime domene pretvara u IP adresu se zove *Domain Name Resolution*. Na većini OS-eva, bilo da se to Mac, Linux, Unix, Netware ili Windows, većina tih pretvorbi iz imena domene u IP adresu se događa kroz proceduru zvanu kao DNS.

Šta je to DNS

DNS je kratica za *Domain Name System* i standardan je servis za rezoluciju imena domena na Internetu. Kadgod se neki uređaj spoji na neki drugi uređaj ne Internetu, mora se spojiti preko IP adrese na ta udaljeni uređaj. Da bi se dobile te IP adrese, DNS se koristi kako bi se ime domene mapiralo u odgovarajuću IP adresu. Ovo uređaj radi tako što "pita" svoj konfigurirani DNS Server koja je IP adresa odgovarajuće domene. DNS server će tad pitati druge servere na Internetu koji znaju točnu informaciju o imenu te domene, i vratiti uređaju natrag točnu IP adresu. Uređaj će tad otvoriti konekciju direktno na IP adresu i obaviti traženu operaciju.

Unos HOSTS datoteke

Postoji još jedan način kako se ime domene može pretvoriti u IP adresu bez korištenja DNS-a, a to je upravo HOSTS datoteka. Gotovo svaki OS koji komunicira preko TCP/IP-a, standardne metode komunikacije preko Interneta, ima datoteku koja se zove HOSTS. Ova datoteka Vam dozvoljava da stvorite vaša vlastita mapiranja između imena domena i IP adresa.

HOSTS datoteka je u biti tekstualna datoteka koja sadrži IP adrese koje su odvojene bar jednom razmaknicom (*space*) i nakon koje slijedi ime domene, s tim da svaki zapis počinje u novoj liniji. Npr. recimo da želimo da ako unesemo **www.google.com** da ne odemo na Google tražilicu već da odemo na recimo **www.yahoo.com**. Da bismo ovo postigli moramo naći adresu Yahoo-a i mapirati **www.google.com** na tu IP adresu.

Jedna od IP adresa Yahoo-a jest 216.109.118.69. Ako želimo mapirati Google na tu IP adresu, u HOSTS datoteku ćemo dodati sljedeći unos:

216.109.118.69 **www.google.com**

Upozorenje: kada dodajete unose u HOSTS datoteku mora biti barem jedan razmak (space) između IP adrese i imena domene. Nemojte koristiti web notacije kao što su \, /, ili http://. Možete onemogućiti pojedini unos tako da ga komentirate stavljanjem znaka "#" na početku linije.

Možda ćete se zapitati kako ovo može raditi kad smo maloprije rekli da kad uređaj želi mapirati ime domene u IP adresu koristi konfigurirani DNS server. U uobičajenim slučajevima ovo je istina, ali na većini OS-eva *default-na* konfiguracija jest da sva mapiranja sadržana unutar HOSTS datoteke premošćuju sve informacije koje bi se dobile sa DNS servera i koje vrijede za tu domenu, i umjesto toga da se čita IP adresa iz HOSTS datoteke. Također je važno uočiti da kad dodamo više unosa u HOSTS datoteku oni automatski počnu raditi. Nema potrebe da restartamo mašinu ili da pokrećemo neku drugu komandu kako bi unosi u HOSTS datoteci počeli raditi.

HOSTS datoteka se nalazi na različitim lokacijama ovisno koji OS koristite:

Linux/Unix => /etc/hosts

Windows 3.1/95/98/ME => C:\WINDOWS\hosts

Windows NT/2000/XP Pro => C:\WINNT\SYSTEM32\drivers\etc\hosts ili C:\WINDOWS\SYSTEM32\drivers\etc\hosts

Windows XP Home => C:\WINDOWS\SYSTEM32\drivers\etc\hosts

Netware => SYS:ETC/HOSTS

Apple => System Folder:Preferences i u samom System Folder

Na Windows mašinama moguće je da po *default-u* HOSTS datoteka još ne postoji. U tom slučaju će najvjerojatnije biti testna datoteka **hosts.sam** koju možete preimenovati u HOSTS i koristiti. Ovu datoteku možete editirati direktno iz komandne linije preko **edit** komande ili Notepada na win mašinama ili recimo VI na *nix. U biti bilo koji tekstualni editor može otvoriti i modificirati HOSTS datoteku. Također se preporuča da je redovno bekapirajte kopirajući je pod drugim imenom. Neki ljudi preporučuju da ovu datoteku postavite na *read-only* tako da je teža za modificiranje malicioznim programima, među kojima se posebno ističu otimači browsera (*Browser Hijackers*), ali postoje i otimači browsera poput CoolWebSearch koji dodaju unose bez obzira na to da li je datoteka *read-only* ili ne. Stoga ne biste trebali misliti da tim što je postavljate na *read-only* da je zauvijek osiguravate od modifikacije.

Zašto mi treba HOSTS datoteka?

Postoji mnoštvo razloga zašto biste trebali koristiti HOSTS datoteku između kojih možemo istaknuti sljedeće:

Potencijalno poboljšanje brzine surfanja - dodavanjem mapiranja IP adresa na sajtove u Vašu HOSTS datoteku možete potencijalno poboljšati brzinu Vašeg surfanja. Ovo se događa zato jer kompjuter više ne mora pitati DNS server za IP adresu i čekati na njegov odgovor, već umjesto toga može puno brže pogledati unos u lokalnoj datoteci. Imajte na umu da ova metoda nije puno preporučena jer ne postoji garancija da će ista domena uvijek imati istu IP adresu. Stoga ako vlasnik sajta odluči promijeniti IP adresu, više se nećete moći spojiti.

Blokiranje *Spyware-a*/reklama - ovo postoje jako popularan razlog za korištenje HOSTS datoteke. Dodavanjem ogromne liste poznatih mreža koja su izvorišta reklama i *Spyware* sajtova u vašu HOSTS datoteku i mapiranjem imena domena na 127.0.0.1, što je tzv. *loopback* IP adresa koja uvijek pokazuje na vašu vlastitu mašinu, blokirat ćete ove sajtove od učitavanja. Ovo ima najmanje dvije beneficije: jedna je da će značajno ubrzati vaše surfanje jer više nećete trebati čekati na skidanje reklama iz tih reklamnih mreža (sajtova koji su specijalizirani kao skladišta reklama) i kao drugo: Vaše će surfanje biti puno sigurnije jer više nećete biti u mogućnosti doći do malicioznih sajtova.

Upozorenje: Važno je napomenuti da postoji dosta pritužbi o usporavanju sustava kada se koristi velika HOSTS datoteka. Ovo se obično rješava gašenjem *DNS Client* servisa pod *Services applet-om Control Panel-a* pod *Administrative Tools*. DNS klijent kešira DNS zahtijeve u memoriji i kao trebao bi ubrzati cijeli proces, ali također i čita HOSTS datoteku u keš što može usporiti sustav. Ovaj servis je nepotreban i može biti izgašen.

Postoje HOSTS datoteke koje su već napravljene tako da ih možete besplatno skinuti i koje sadrže ogromnu listu reklamnih servera, sajtova sa *banner-ima*, sajtova koji prate navike korisnika preko špijunskih *cookie-a*, sadrže exploite ili vas inficiraju sa otimačima. Ispod je tipična lista najpopularnijih HOSTS datoteka:

MVPS HOSTS datoteka (moja preporuka): **http://www.mvps.org/winhelp2002/hosts.htm**

hpguru-ova HOSTS datoteka: **http://webpages.charter.net/hpguru/hosts/hosts.html**

HOSTS datoteka projekt: **http://remember.mine.nu/**

Preporuča se da prije skidanja bekapirate izvornu HOSTS datoteku tako što ćete je preimenovati u HOSTS.ORIG

Korisni programi za održavanje HOSTS datoteke

Ako ne planirate modificirati vašu HOSTS datoteku previše i planirate je korititi s vremena na vrijeme za testne namjene, tada će osnovni tekstualni editori poput VI, Notepad ili DOS Edit biti sasvim dovoljni za održavanje Vaše HOSTS datoteke. S druge strane, ako HOSTS datoteku mislite koristiti u velikoj mjeri za blokiranje reklama/*spyware-a* ili zbog nekog trećeg razloga, tada postoje dva alata koja Vam mogu pomoći:

eDexter - Kada blokirate reklame na sajtovima koristeći HOSTS datoteku, na ekranu se nacrtaju prazne rupe (četverokuti) na mjestima gdje bi se inače pojavile reklame. Ako vam omo smeta, možete koristiti eDexter da poputnite tu sliku sa nekom proizvoljnom poput prazne slike ili neke koja vam je po volji. Ovo zamjenjuje prazne četverokute i brzo je jer se slika učitava sa Vašeg diska.

Hostess - Hostess je aplikacija koja služi za održavanje i organiziranje Vaše HOSTS datoteke. Ovaj program čita Vašu HOSTS datoteku i organizira unose sadržane u bazi podataka. Možete zatim koristiti tu bazu pri skeniranju za duplikate i održavanjem unosa. Ovaj program definitivno morate isprobati ako mislite ozbiljno prčkati po HOSTS datoteci.

Nevidljive ekstenzije - što ne vidiš, ne može ti nauditi. Po *default-u* Windows nemaju pregled ekstenzija datoteka uključen. Ovo omogućava piscima virusa da distribuiraju izvršne datoteke prerušene kao neizvršne. Npr. .EXE datoteka može izgledati poput nedužnog tekstualnog dokumenta.

Omogućavanje pregleda ekstenzija na Windows 95/98/NT

1. Pokrenite **Windows Explorer** (Klikom na *My Computer*).

2. Kliknite u meniju na **View**.

3. Kliknite na **Options**.

4. **Maknite** kvačicu sa sa **Hide file extensions for known file types**.

Omogućavanje pregleda ekstenzija na Windows 2000 i XP

1. Pokrenite **Windows Explorer** (Klikom na *My Computer*).

2. Kliknite u meniju na **Tools**.

3. Kliknite na **Folder Options**.

4. Kliknite na **View**.

5. **Maknite** kvačicu sa sa **Hide file extensions for known file types**.

Omogućavanje pregleda ekstenzija za .SHS datoteke

Za .SHS datoteke treba još jedan dodatni korak. Nakon prošlih instrukcija za Vašu verziju Windowsa, uradite sljedeće:

1. Kliknite na **Start** dugme.

2. Kliknite na **Run**.

3. Upišite **regedit** i kliknite <enter>.

4. Dođite do ključa **HKEY_CLASSES_ROOT\ShellScrap**.

5. Unutar tog ključa izbrišite vrijednost **NeverShowExt** tako što ste ga označili i pritisnuli <delete>.

Imena ekstenzija izvršnih datoteka

Slijedi parcijalna lista tipova datoteka koji bi se trebali smatrati sumnjivim kada ih primite preko e-maila i ne biste ih smjeli otvarati osim ako ih ne očekujete kao *attachment*:

Code:

```
ADE - Microsoft Access Project Extension
ADP - Microsoft Access Project
BAS - Visual Basic Class Module
BAT - Batch File
CHM - Compiled HTML Help File
CMD - Windows NT Command Script
COM - MS-DOS Application
CPL - Control Panel Extension
CRT - Security Certificate
DLL - Dynamic Link Library
DO* - Word Documents and Templates
EXE - Application
HLP - Windows Help File
HTA - HTML Applications
INF - Setup Information File
INS - Internet Communication Settings
ISP - Internet Communication Settings
JS - JScript File
JSE - JScript Encoded Script File
LNK - Shortcut
MDB - Microsoft Access Application
MDE - Microsoft Access MDE Database
MSC - Microsoft Common Console Document
MSI - Windows Installer Package
MSP - Windows Installer Patch
MST - Visual Test Source File
OCX - ActiveX Objects
PCD - Photo CD Image
PIF - Shortcut to MS-DOS Program
POT - PowerPoint Templates
PPT - PowerPoint Files
REG - Registration Entries
SCR - Screen Saver
SCT - Windows Script Component
```

```
SHB - Document Shortcut File
SHS - Shell Scrap Object
SYS - System Config/Driver
URL - Internet Shortcut (Uniform Resource Locator)
VB - VBScript File
VBE - VBScript Encoded Script File
VBS - VBScript Script File
WSC - Windows Script Component
WSF - Windows Script File
WSH - Windows Scripting Host Settings File
XL* - Excel Files and Templates
```

[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

Kako onemogućiti WSH 20.01.2005. u 14:42

Kako onemogućiti WSH

Ove upute će vam objasniti kako da provjerite je li WSH (*Windows Scripting Host*) instaliran na Vašoj mašini i kako da onemogućite izvršavanje VBS (*Visual Basic Script*) skripti. Ovo može spriječiti neke crve od inficiranja Vašeg kompa.

Kada su Windowsi, Internet Explorer ili neki drugi proizvodi instalirani ili nadograđeni, WSH može također biti reinstaliran. U tom ćete slučaju trebati ponoviti dolje navedene korake.

Važna uputa: Neke aplikacije zahtijevaju WSH za svoje izvršavanje i **neće raditi** ako ga onemogućite ili maknete.

Windows 98

WSH je instaliran ako odaberete standardnu instalaciju OS-a, ili ako instalirate Internet Explorer 5 ili ako skinete WSH sa MS-ovih stranica.

Da biste onemogućili WSH i izvođenje skripti uradite sljedeće:

1. Kliknite na **Start** dugme.

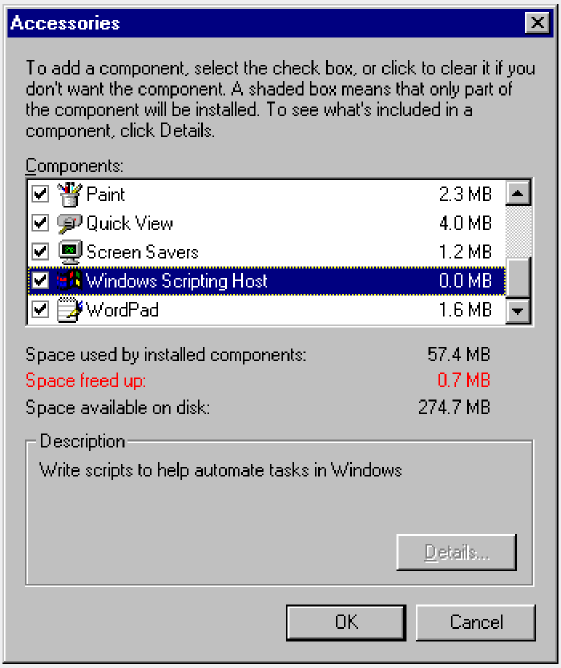
2. Kliknite na **Settings**.

3. Kliknite na **Control Panel**.

5. Dvoklik na **Add/Remove programs** ikonicu.

6. Kliknite na **Windows Setup** tab.

7. Dvoklik na **Accessories**.



8. Nađite u listi naziv **Windows Scripting Host** i maknite kvačicu sa njega.

9. Kliknite **OK**. Još jednom kliknite **OK**.

Windows 95

WSH je instaliran ako instalirate Internet Explorer 5, ili ako skinete WSH sa MS-ovih stranica.

Da biste onemogućili WSH i izvođenje skripti uradite sljedeće:

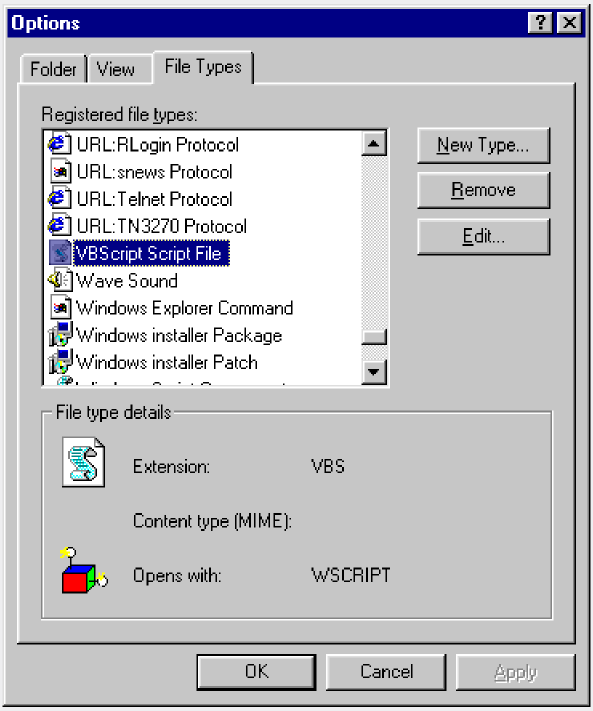
1. Desni klik na **My Computer**.

2. Kliknite u meniju na **Open**.

3. Kliknite u meniju na **View**.

4. Kliknite na **Options**.

5. Kliknite na **File Types** tab.



6. Potražite **VBScript Script File** u listi tipova datoteka - ako ne postoji ne morate ništa uraditi! Ako postoji kliknite na **Remove** dugme.

7. Ukoliko vam iskoči dijalog za potvrdu kliknite na **Yes**.

Windows NT 4.0

WSH je instaliran ako instalirate Internet Explorer 5 ili ako skinete WSH sa MS-ovih stranica.

Da biste onemogućili WSH i izvođenje skripti uradite sljedeće:

1. Ulogirajte se na mašinu kao **administrator**.

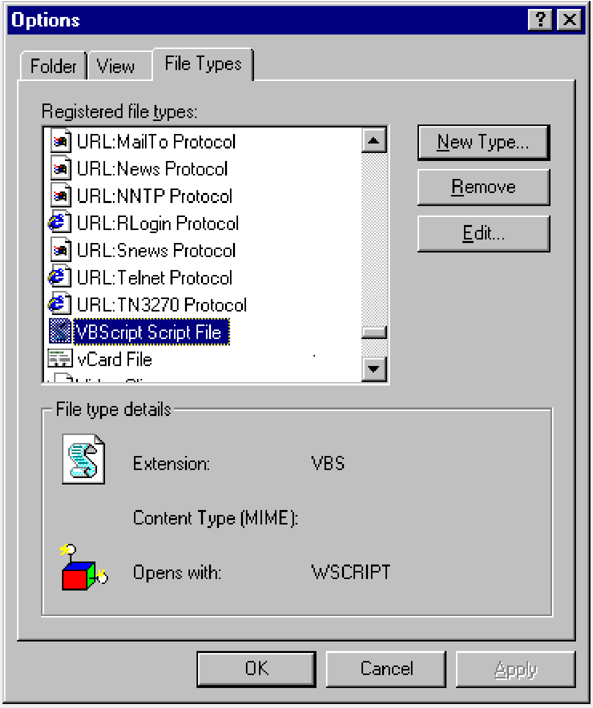
2. Desni klik na **My Computer**.

3. Kliknite u meniju na **Open**.

4. Kliknite u meniju na **View**.

5. Kliknite na **Options**.

6. Kliknite na **File Types** tab.



7. Potražite **VBScript Script File** u listi tipova datoteka - ako ne postoji ne morate ništa uraditi! Ako postoji kliknite na **Remove** dugme.

8. Ukoliko vam iskoči dijalog za potvrdu kliknite na **Yes**.

Windows 2000/Me/XP/2003

WSH je instaliran po *default-u*.

Da biste onemogućili WSH i izvođenje skripti uradite sljedeće:

1. Ulogirajte se na mašinu kao **Administrator**.

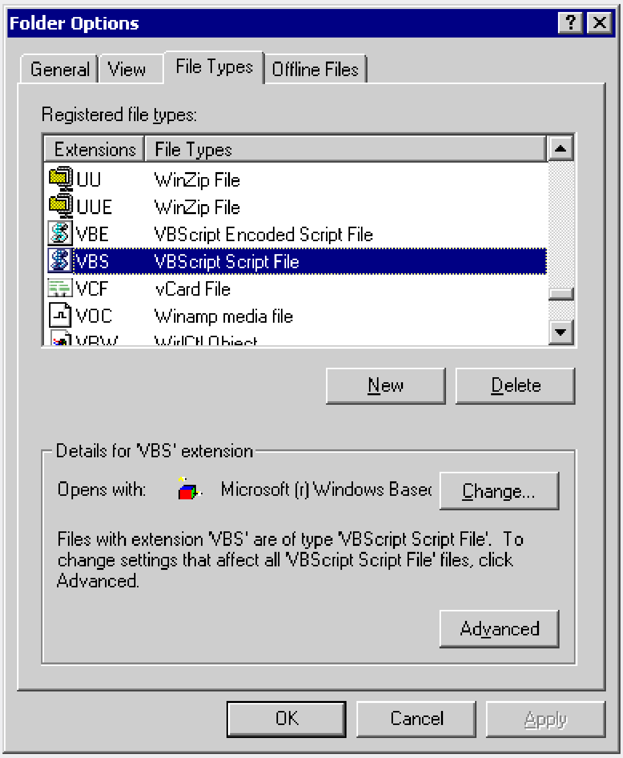
2. Desni klik na **My Computer**.

3. Kliknite u meniju na **Open**.

4. Kliknite u meniju na **Tools**

5. Kliknite na **Folder Options**

6. Kliknite na **File Types** tab.



7. Potražite **VBScript Script File** u listi tipova datoteka - ako ne postoji ne morate ništa uraditi! Ako postoji kliknite na **Delete** dugme.

8. Ukoliko vam iskoči dijalog za potvrdu kliknite na **Yes**.

[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

Kako ugasiti System Restore **20.01.2005. u 18:16**

Windows Me

Jedna od ključnih mogućnosti Windows Me jest *System Restore*. Ova mogućnost, koja je po *default-u* omogućena, služi Windowsima da povrate datoteke na kompu u slučaju da one budu oštećene. Windows Me čuva informaciju o povratu datoteka u _RESTORE direktoriju koji je kreiran na svakom hard disku kompa; ovi direktoriji se *update-aju* kad se komp restarta.

Premda je ova mogućnost Windowsa vrlo poželjna i korisna, u nekim slučajevima bi je bilo poželjno privremeno izgasiti. Ako je komp inficiran sa virusom, tada je moguće da je i sam virus bekapiran u _ RESTORE direktorij. Po *default-u*, Windows sprečava da *System Restore* modificiraju vanjski programi. Kao rezultat, postoji mogućnost da slučajno možete vratiti datoteku inficiranu virusom, ili da *on-line* skeneri otkriju virus na toj lokaciji.

Onemogućavanje *System Restore* ne briše i ne miče neke od vaših osobnih podataka sa kompa. Samo se miču datoteke koji je *System Restore* stvorio u _RESTORE direktoriju, tzv. točke povratka (*restore points*) . Korištenje *System Restore* za vraćanje prethodno spremljenih točka povratka ne djeluje na Vaše osobne podatke ili dokumente koje imate u *My Documents* direktoriju.

Za onemogućavanje Windows Me *System Restore*:

1. Klinite na **Start** dugme.

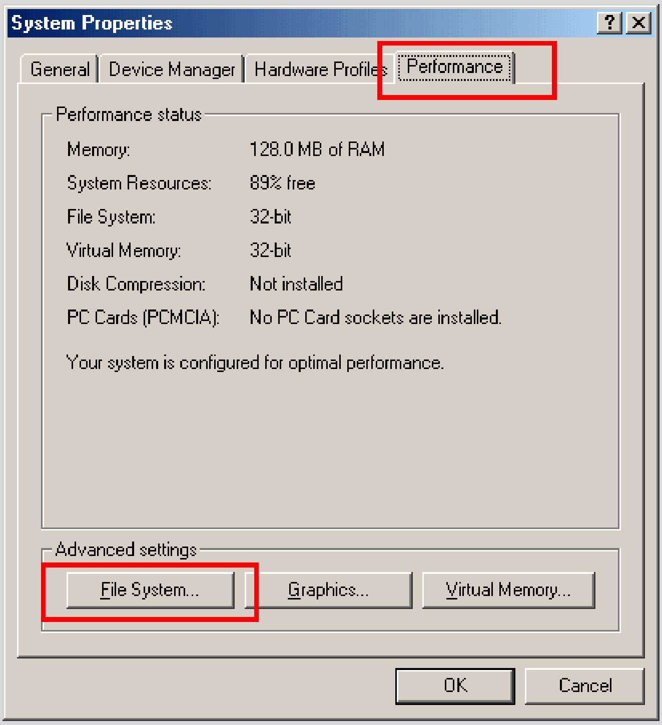
2. Kliknite na **Settings**.

3. Klinite na **Control Panel**.

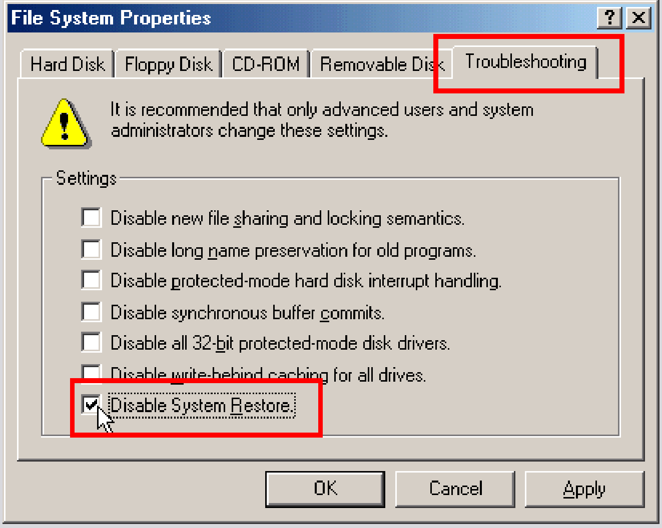
4. Dvoklik na **System** ikonicu.

Upozorenje: ako **System** ikonica nije vidljiva, kliknite na **View all Control Panel options** da postane vidljiva

5. Kliknite na **Performance** tab i na njemu kliknite na **File System** kao što je na slici prikazano:



6. Kliknite na **Troubleshooting** tab i na njemu kliknite na **Disable System Restore** kao što je prikazano na slici:



7. Kliknite **OK**. Kliknite na **Yes** kada vas pita da li želite restartati Windowse.

Slijedite upute u dokumentu koji Vas je savjetovao da ugasite *System Restore*, kao što su recimo upute za micanje virusa. Kada su svi koraci micanja virusa završeni, možete omogućiti *System Restore* na sljedeći način:

Za omogućavanje Windows Me *System Restore*:

1. Klinite na **Start** dugme.

2. Kliknite na **Settings**.

3. Klinite na **Control Panel**.

4. Dvoklik na **System** ikonicu.

5. Kliknite na **Performance** tab i na njemu kliknite na **File System**.

6. Kliknite na **Troubleshooting** tab i na njemu maknite kvačicu sa **Disable System Restore**.

7. Kliknite **OK**. Kliknite na **Yes** kada vas pita da li želite restartati Windowse.

Windows XP

System Restore mogućnost Windowsa XP je slična *Last Known Good Configuration* mogućnosti Windowsa NT i Windowsa 2000. Možete koristiti *System Restore* za vraćanje kompa na prijašnje stanje koristeći bekape koje on pravi od odabranih sistemskih datoteka i programa. Za razliku od *Last Known Good Configuration* mogućnosti, *System Restore* može čivati višestruke točke povratka (*restore points*). Ovo vam daje mogućnost da komp vratite na bilo koje od sačuvanih stanja.

Premda je ova mogućnost Windowsa vrlo poželjna i korisna, u nekim slučajevima bi je bilo poželjno privremeno izgasiti. Ako je komp inficiran sa virusom, tada je moguće da je i sam virus bekapiran u _ RESTORE direktorij. Po *default-u*, Windows sprečava da *System Restore* modificiraju vanjski programi. Kao rezultat, postoji mogućnost da slučajno možete vratiti datoteku inficiranu virusom, ili da *on-line* skeneri otkriju virus na toj lokaciji.

Onemogućavanje *System Restore* ne briše i ne miče neke od vaših osobnih podataka sa kompa. Samo se miču datoteke koji je *System Restore* stvorio u _RESTORE direktoriju, tzv. točke povratka (*restore points*) . Korištenje *System Restore* za vraćanje prethodno spremljenih točka povratka ne djeluje na Vaše osobne podatke ili dokumente koje imate u *My Documents* direktoriju.

Upozorenje:

• **Morate** biti ulogirani kao **Administrator** da biste mogli izgasiti *System Restore*. Ako niste ulogirani kao Administrator, tab za *System Restore* neće biti prikazan. Ako ne znate kako se ulogirati kao Administrator, kontaktirajte svog sistemskog administratora (ako ste na mreži) , prodavača kompa, ili osobu koja vam je instalirala Windowse.

• Gašenje *System Restore* će izbrisati sve vaše prethodne točke povratka. Morate stvoriti novu točku povratka jednom kada ponovo uključite *System Restore*.

Za onemogućavanje Windows XP *System Restore*:

1. Kliknite na **Start** dugme.

2. Kliknite na **Programs**.

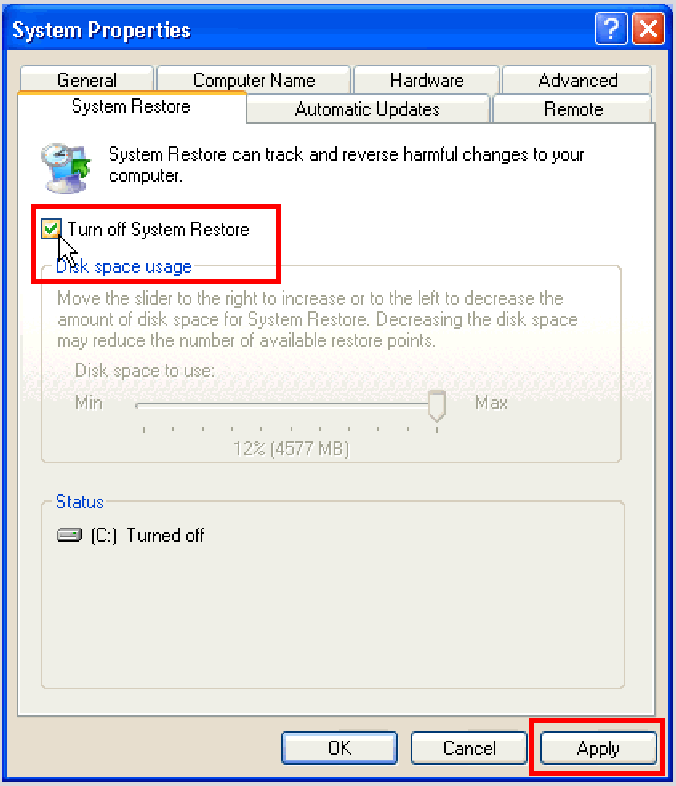
3. Kliknite na **Accessories**.

4. Kliknite na **Windows Explorer**.

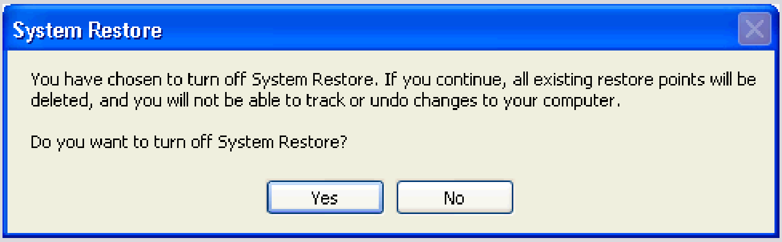
5. Desni klik na **My Computer** i kliknite na **Properties** stavku u meniju.

6. Kliknite na **System Restore** tab.

7. Kliknite na **Turn off System Restore** ili **Turn off System Restore on all drives** kao što je prikazano na slici:



8. Kliknite na **Apply**. Iskočit će sljedeća poruka:



9. Kao što piše u poruci, ovo će izbrisati sve prošle točke povratka. Kliknite na **Yes** da biste to napravili.

10. Kliknite **OK**.

Slijedite upute u dokumentu koji Vas je savjetovao da ugasite *System Restore*, kao što su recimo upute za micanje virusa. Kada su svi koraci micanja virusa završeni, možete omogućiti *System Restore* na sljedeći način:

Za omogućavanje Windows XP *System Restore*:

1. Kliknite na **Start** dugme.

2. Desni klik na **My Computer** stavku u meniju te kliknite na **Properties**.

3. Kliknite na **System Restore** tab.

4. Maknite kvačicu sa **Turn off System Restore** ili **Turn off System Restore on all drives**.

5. Kliknite **Apply**.

6. Kliknite **OK**.

[brisanje! | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

Kako koristiti Microsoft AntiSpyware Beta za micanje Spyware-a **21.01.2005. u 00:13**

Uvod

Nedavno je Microsoft izdao beta verziju svog AntiSpyware programa. Ovaj tekst će u detalje objasniti kako instalirati, konfigurirati i skenirati vaš komp koristeći ovaj program na najučinkovitiji i najbolji mogući način. Budući da je ovaj program još uvijek u beta verziji, postoje neki dijelovi programa koji još ne rade pravilno. Kako nove mogućnosti budu dodavane i promijenjene, ovaj će tekst biti odgovarajuće promijenjen. Molim imajte na umu da, pošto je ovaj program još uvijek u beta verziji, koristite ga na vlastiti rizik.

Instaliranje i pokretanje Microsoft AntiSpyware Beta prvi put

KORAK 1: Skini i instaliraj Microsoft AntiSpyware Beta

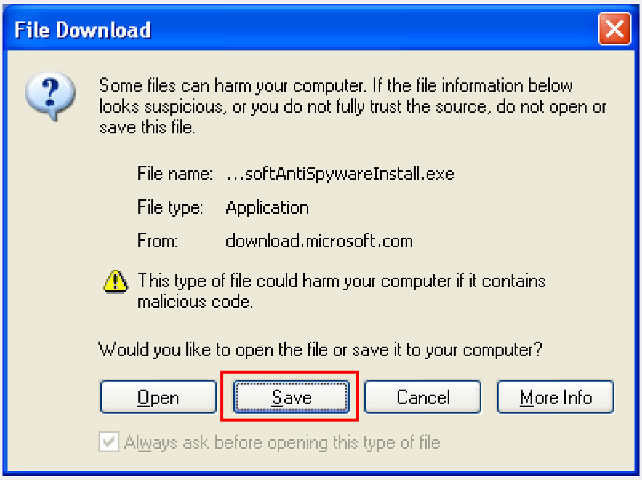
Da biste skinuli besplatan program Microsoft AntiSpyware Beta morate posjetiti njegovu stranicu za *download*. Ovaj se program može skinuti direktno sa sljedećeg linka:

Microsoft AntiSpyware Beta

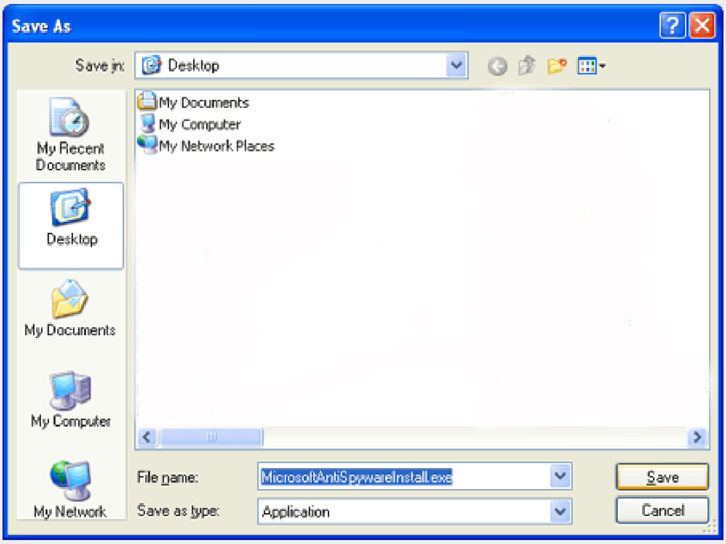
Dok više informacija o samom programu možete vidjeti na njegovoj službenoj stranici:

http://www.microsoft.com/athom.../spyware/software/default.mspx

Ukoliko kliknete na ovaj sajt i slijedite upute za skidanje ili, još bolje, direktno skinete program sa linka iznad, vidjet ćete **Download** dugme na koje ćete kliknuti. Nakon toga ćete vidjeti nešto poput:



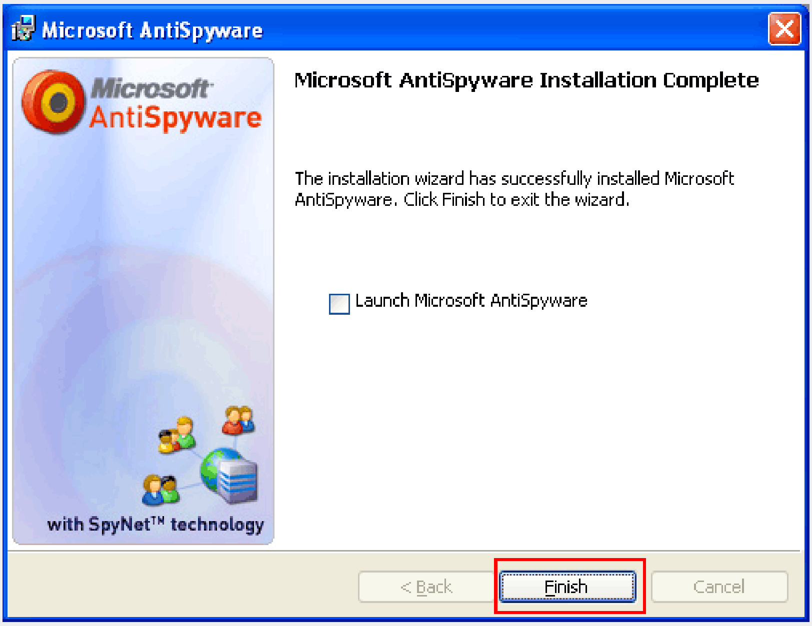
Kliknite na **Save** dugme koje će otvoriti nešto slično ovome:



Promijenite u **Save in:** listi lokacija za spremanje programa na **Desktop** i kliknite na **Save** dugme. Program će nakon toga biti skinut i spremljen na vaš dekstop. Kada je download završen, na desktopu ćete pronaći ikonicu poput ove:

Dvokliknite na ovu ikonicu da biste pokrenuli instalaciju Microsoft AntiSpyware programa. Ovaj program za instalaciju će započeti slikom sličnoj ovoj:

Sada pritisnite **Next** dugme i prihvatite ličenčni ugovor. Nastavite pritiskati **Next** dugme prihvaćajući *default-ne* postavke sve dok ne dođete do ovog dijela instalacije:



Napravite kvačicu na **Launch Microsoft AntiSpyware** stavku i kliknite na **Finish** dugme kao što je na slici prikazano.

KORAK 2: Konfiguriraj Microsoft AntiSpyware koristeći čarobnjaka za prvo pokretanje

Microsoft AntiSpyware će se sad prvi put pokrenuti i pokrenut će se ujedno i čarobnjak za naštimavanje postavki. Izgledat će nešto poput na slici:

Kliknite na **Next** dugme kako biste došli do sljedećeg koraka instalacije. U ovom koraku ćete se morati odlučiti da li da koristite automatski *update* (*autoupdater*). Moj je savjet da ovo ostavite na *default-nim* postavkama tako da se definicije najnovijeg *malware-a* automatski skidaju u program i da uvijek imate najsvježiju moguću zaštitu.

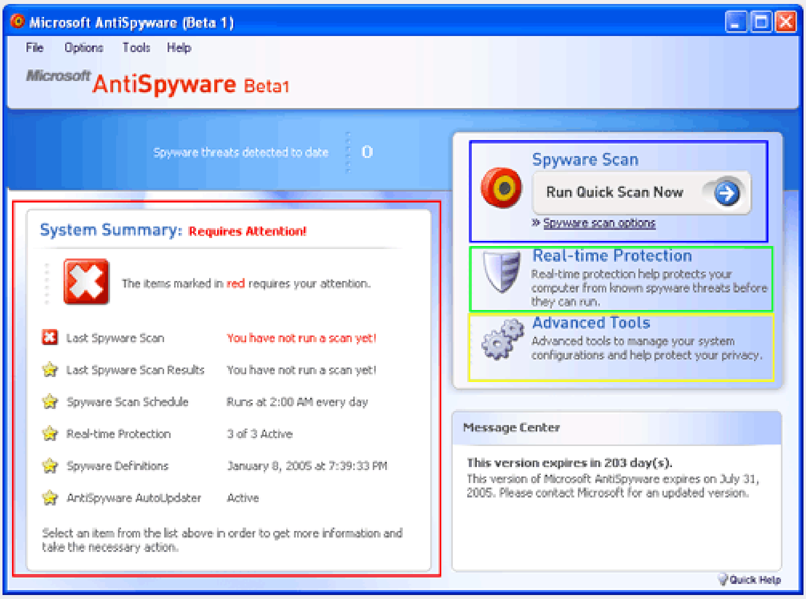
Sada biste opet trebali kliknuti na **Next** dugme. Sljedeći korak će vas pitati za postavke o zaštiti u realnom vremenu (*Real-time Security Agent*). *Realtime* sigurnosni agenti će pratiti Vaš komp za aktivnošću poznatih *spyware-a* i otimača browsera i odmah Vas obavijestiti, slično kao što Vas rezidentni modul antivirusa obavještava kad se spremate pokrenuti virus. Moj je savjet da ovo ostavite na *default-nim* postavkama, **Yes, help keep me secure (recommended)**.

Pritisnite **Next** dugme i doći ćete do koraka u kojem će Vas se pitati da li biste se željeli pridružiti Spynet mreži. Spynet je servis koji vam omogućava da proslijedite uzorke i informacije o *spyware-u* koji Microsoft AntiSpyware trenutno ne zna popraviti. U ovom postupku se neće dijeliti nikakvi vaši privatni podaci i nikakve osobne informacije neće biti poslane bez Vašeg znanja, tako da ako želite sudjelovati u zajednici osoba koje žele povećati znanje o trenutnom *spyware-u* na svijetu, ostavite sve na *default-nim* postavkama **Yes, I want to help fight spyware (recommended)**.

Kliknite na **Finish** dugme da biste došli do do posljednjeg koraka konfiguracijskog čarobnjaka. U ovom ćete se koraku odlučiti da li želite da se AntiSpyware program automatski pokreće svakog jutra u 2 AM. Ako želite da se pokreće, tada postavite kvačicu na na **Run a spyware scan every night at 2 a.m.**, inače je maknite. Nakon toga biste trebali kliknuti na **Run scan later link**.

KORAK 3: Nadogradi *spyware* definicije i pokreni prvi sken

Program će se pokrenuti i prikazati će Vam se glavni prozor programa Microsoft AntiSpyware. Ovaj prozor izgleda otprilike ovako:



Sekcija označena crvenom linijom predstavlja Sistemski Sažetak (*System Summary*). Ova sekcija vam govori o važnim informacijama kao što su posljednje vrijeme skena, što je sve posljednji sken našao, u koje vrijeme starta automatizirani sken, da li je uključena zaštita u realnom vremenu, da li ja uključena automatska instalacija *spyware* definicija sa Interneta i koji je datum posljednjih *spyware* definicija.

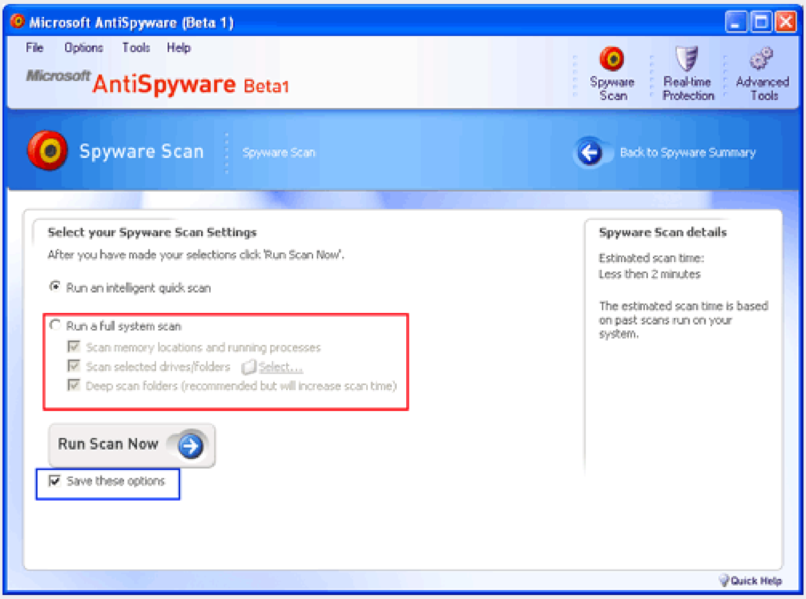
Plavom crtom je označena sekcija koja bi pokrenula sken Vašeg kompa, na što ćemo se uskoro osvrnuti.

Zelenom crtom je označena sekcija koja dozvoljava promjenu postavki zaštite u realnom vremenu Vašeg kompa. Ove postavke biste trebali ostaviti na njihovim *default-nim* vrijednostima budući da baš one osiguravaju maksimalnu zaštitu.

Žutom crtom je označena sekcija u kojoj se nalaze napredni alati kao što su vraćanje sistemskih postavki, browser sistemskih postavki i analizator datoteka. U većini slučajeva prosječni korisnici ne bi trebali prčkati po ovim postavka i trebali bi izbjegavati njihovo mijenjanje.

Prije nego što opalimo prvi sken moramo se uvjeriti da je program nadograđen na najnovije *spyware* definicije. Da biste ih nadogradili, kliknite na **File** stavku u meniju i kliknite na **Check for updates...** dugme. Program će se spojiti na Microsoftove servere i provjeriti da li su izašle nove definicije. Ako ih nađe, sam će ih skinuti i instalirati.

Sada kliknite na **Spyware scan options** link unutar sekcije označene plavom crtom. Ovo će vas doveti na dio u kojem se nalaze postavke skena kao što je prikazano na slici:



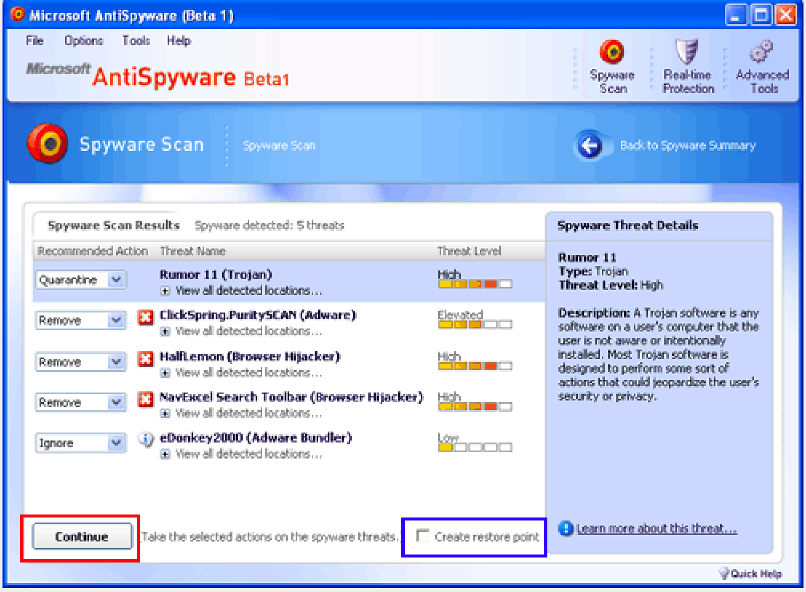
Odaberite naznačenu opciju **Run a full system scan** i postavite kvačicu na sljedeće opcije:

- **Scan memory locations and running processes**
- **Scan selected drives/folders**
- **Deep Scan folders (recommended but will increase scan time)**

Nakon toga kliknite na **Select** link koji se nalazi sa desne strane **Scan selected drives/folders** stavke i pojavit će se izbornik u kojem ćete označiti sve vaše lokalne hard diskove. Nemojte označavati CD-ROM-ove, DVD, flash diskove, *memory stick-ove*, kamere i ostale uređaje. Odaberite **samo** lokalne hard diskove. Nakon toga kliknite na **OK** dugme i vratit će vas natrag na korak sa postavkama skena. Postavite kvačicu na **Save these options** da spremite iste ove postavke za sve buduće skenove i kliknite na **Run Scan Now** dugme.

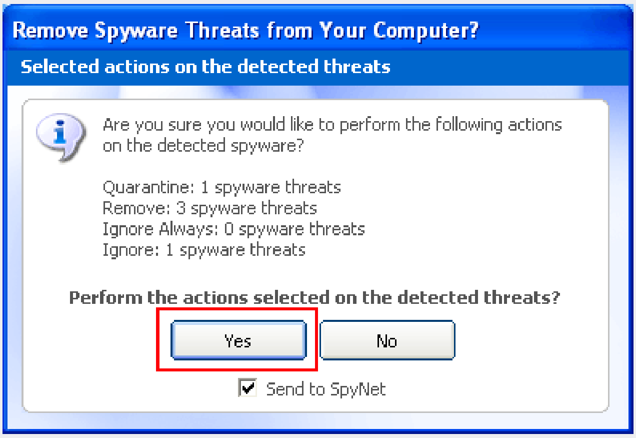
KORAK 4: Skenirajte svoj komp za *spyware-om* i ostalim *malware-om*

Nakon što kliknete na **Run Scan Now** dugme, program će početi skenirati Vaš komp za *spyware-om* i ostalim *malware-om*. Ovo može dosta dugo potrajati budući da radi dubinski sken stoga molim budite strpljivi. Kada sken završi, prezentirat će Vam sažetak onoga što je našao, nešto slično ovoj slici:



Kada je sken završen, bit će Vam prezentirana lista *spyware-a* i ostalog *malware-a* koje je program našao. Ukoliko želite nešto više saznati o nađenim programima možete jednom kliknuti na odabrani element i kratke informacije će se pojaviti u *box-u* sa strane. Nakon proučavanja informacija o detektiranom potencijalno malicioznom programu, trebat ćete odlučiti da li da ga pošaljete u karantenu - **Quarantine**, da li da ga izbrišete - **Remove** ili ignorirajte - **Ignore**. *Default-ne* postavke koje AntiSpyware sam postavi su obično OK, ali ih možete promijeniti po volji.

Nakon što ste odlučili što ćete sa pojedinim detektiranim programom, stavite kvačicu na **Create restore point**, u slučaju da nešto ode kvragu za vrijeme micanja odabranih programa. Kliknite na **Continue** dugme za početak procesa micanja odabranih programa pri čemu će se pojaviti dijalog za potvrdu sličan ovome:



Ukoliko želite poslati informacije o nađenom *spyware-u* na Vašem kompu Microsoftovoj SpyNet mreži, tada možete postaviti kvačicu na **Send to SpyNet** polje. Nakon toga kliknite na **Yes** dugme ako biste željeli nastaviti sa micanjem *spyware-a*. Kada program završi micanje *spyware-a*, vratit će Vas natrag na Sistemski Sažetak pri čemu možete zatvoriti program.

Ako ste pažljivo pratili upute pri instalaciji, sljedeći put kad budete radili sken Vašeg kompa možete jednostavno pokrenuti program, napraviti nadogradnju te kliknuti na **Tools** meni i potom na **Spyware Scan** i kliknuti na **Run a Scan Now**. Sada možete pokrenuti sken klikom na **Run Scan Now** dugme.

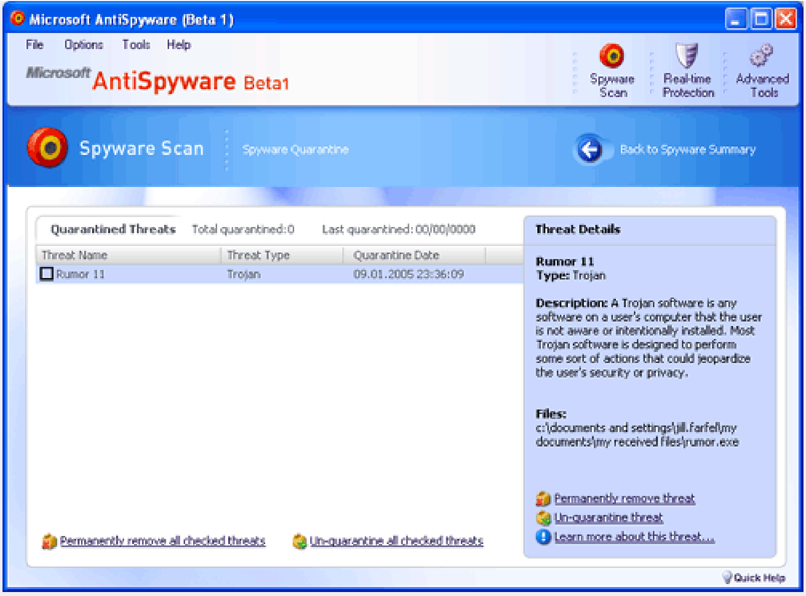
Kako nadograditi *spyware* definicije

Kako biste ostvarili najbolju moguću funkcionalnost programa trebali biste ga nadograđivati odmah prije nego što napravite lokalni sken. Da biste nadogradili *spyware* definicije jednostavno pokrenite Microsoft AntiSpyware, kliknite u meniju na **File** stavku i kliknite na **Check for Updates**. Program će se spojiti na Microsoftove servere te skinuti i instalirati najnovije *spyware* definicije koje postoje. Jednom kad je to završeno, svi sljedeći skenovi će koristiti najnovije definicije.

Kako koristiti karantenu

Kada opalite sken i program nađe sumnjivu datoteku za koju smatra da je potencijalni *malware*, dat će Vam opciju da ga izbrišete - **Remove** ili stavite u karantenu - **Quarantine**. Ako ga stavite u karantenu program će biti kopiran u posebno mjesto za pohranu na Vašem disku tako da ga možete kasnije vratiti po potrebi. U gotovo 99% slučajeva nećete željeti vratiti pohranjeni program i željet ćete izbrisati te pohranjene da Vam više ne zauzimaju prostor na disku.

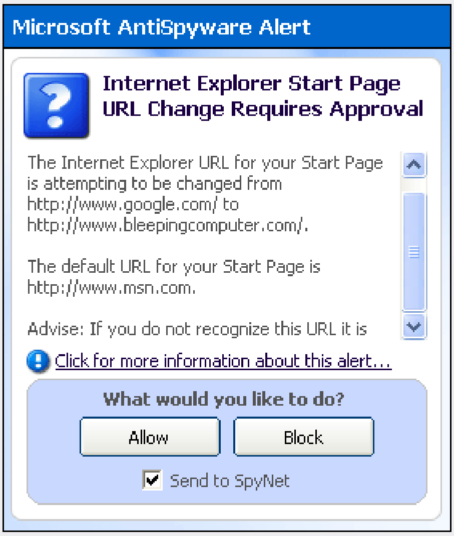
Da biste ušli u karantenu pokrenite AntiSpyware, kliknite na **Tools** stavku u meniju, kliknite na na **Spyware Scan** te na **Manage Spyware Quarantine**. Dobit ćete dijalog sličan sljedećem:



Da vratite neki element postavite kvačicu u polje pored imena tog elementa i odaberite **Un-quarantine all checked threats**. Budite svjesni da ako ovo uradite da ste u mogućnosti da sami sebe ponovno inficirate. Da biste element izbrisali iz svoga kompa, stavite kvačicu pored imena elemeneta i odaberite **Permanently remove all checked threats**.

Kako koristiti zaštitu u realnom vremenu

MS AntiSpyware program sadrži zaštitu u realnom vremenu za vaš komp (*real-time protection*) slično na način na koji radi antivirusni softver. Kada detektira postavke koje će biti promijenjene ili da ste upravo namjeravali pokrenuti poznati *spyware* program, izbacit će vam uzbunu kao što je prikazano na slici:



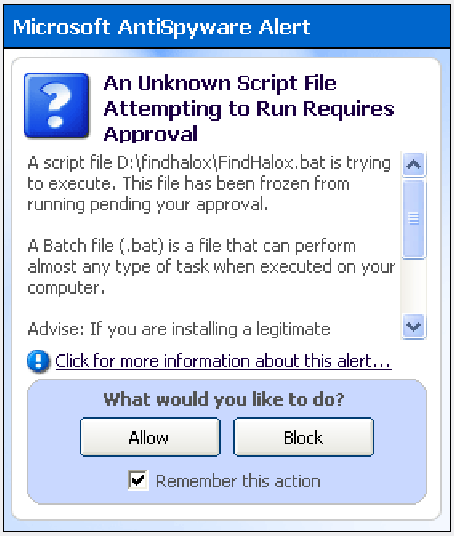
Ako znate da se radi o dobrom programu ili želite da navedena promjena bude dozvoljena tada kliknete na **Allow** dugme. Ako ne prepoznajete o kojem se programu radi ili ne želite da se navedena radnja obavi, kliknete na **Block** dugme.

Kada primite uzbunu zbog pokrenutog programa ili skripte, dobit ćete dodatno polje zvano **Remember this action**. Ako postavite kvačicu na ovo polje tada će AntiSpyware zapamtiti Vašu preferenciju za ovu radnju za ubuduće. Dakle, ako imate **Remember this action** polje označeno kvačicom i odlučili ste blokirati program od pokretanja, ubuduće ako budete željeli pokrenuti taj program, AntiSpyware će ga i dalje blokirati.

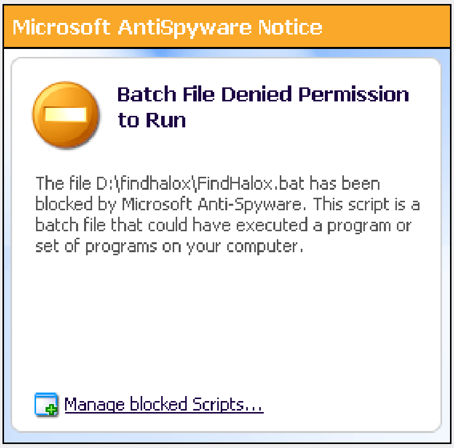
Kontroliranje prijavljivanja uzbuna i modifikacija već postojećih postavki se može napraviti klikanjem na **Real-time Protection** dugme kao što je prikazano na slici:

Jednom kad kliknete na to dugme, imat ćete pristup kontroli raznih agenata koje koristi zaštita u realnom vremenu. Možete kliknuti na agenta koji odgovara pojedinoj radnji koju želite deblokirati i potom kliknuti na odgovarajući *checkpoint* da je selektirate. Sa desne strane biste trebali vidjeti opciju **Manage allowed/blocked** za promjenu postavki dozvoljenim i blokiranim akcija za taj *checkpoint*. Ako kliknite na njega, imat ćete u padajućoj listi opcije za pregled dozvoljenih - **Allowed** i blokiranih - **Blocked** akcija koje možete mijenjati po potrebi.

Obasnimo na konkretnom primjeru kako ovo radi. Recimo da vam je prijatelj poslao datoteku koja je .bat skripta. Kad napravite dvoklik na nju da je pokrenete, Microsoft AntiSpyware će iskočiti sa uzbunom sličnom onoj koji ste već vidjeli:



Naravno da vas je briga i zato nećete dozvoliti njezino izvršavanje. Pitate vašeg prijatelja koji vam je to qrac poslao i onda kad Vam on lijepo objasni da se radi o benignoj skripti i, budući da vjerujete Vašem prijatelju i pošto ćete mu slomiti sve koščice ako Vas zajebaje sa nekim trojanom, pokrećete je ponovno. Ali ovaj put, budući da ste je već blokirali, Microsoft AntiSpyware ne dozvoljava izvršavanje skripte pa dobijate poruku o grešci slično poput ove:



Da biste ovo popravili jednostavno kliknite na **Manage blocked scripts...** opciju u uzbuni i provjerite unos za ovaj program i maknite ga. Ili otvorite glavni program i kliknite na dugme **Real-time Protection** i kliknite na opciju **Application Agents**. Budući da skripta koju ste pokušali pokrenuti jest .bat datoteka, morate odabrati *checkpoint* zvan **Script Blocking**. Nakon toga napravite desni klik na **Manage allowed/ blocked ...** i u padajućoj listi izmjenite iz **Allowed Scripts** u **Blocked Scripts**. Trebali biste vidjeti unos za svaku skriptu koju ste pokušali pokrenuti. Postavite kvačicu pored unosa i kliknite **Remove** dugme za njegovo micanje. Sada možete normalno pokrenuti skriptu.

Kako onemogućiti zaštitu u realnom vremenu

Ponekad želite onemogućiti zaštitu u realnom vremenu. Jedan od razloga za takvo što jest da biste dobili pomoć koristeći analizu HijackThis loga kojeg može omesti korištenje zaštite u realnom vremenu. Ako se od Vas traži da onemogućite zaštitu u realnom vremenu jednostavno napravite desni klik u *tray-u* na ikonicu koja izgleda ovako i kliknite na **Security Agents Status (Enabled)** te kliknite na **Disable Real-time Protection**. Da biste je opet omogućili ponovite ove korake samo u zadnjem kliknite na **Enable Real-time Protection**.

[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

Kako vidjeti skrivene datoteke pod Windowsima

07.02.2005. u 04:55

Uvod

Po *default-u* Windowsi skrivaju određene datoteke od vaših očiju tako što postaju nevidljive u programima poput *Windows Explorer-a*. Ovo je zamišljeno kao isključivo preventivna mjera, da bi se te datoteke zaštitile od modificiranja ili brisanja od strane krajnjeg korisnika. Nažalost, raznorazan malware se skriva na taj način, što otežavanja njegovo lociranje i micanje.

U ovom tekstu ćemo objasniti kako promijeniti postavke vaše verzije Windowsa kako biste bili u mogućnosti vidjeti skrivene (*hidden*) i zaštićene(*protected*) datoteke OS-a. Na ovaj ćete način moći tako otkrivene datoteke mijenjati i brisati, ukoliko se na taj način skriva neki malware.

Windows 95

Da biste omogućili gledanje skrivenih datoteka slijedite sljedeće korake:

1. Zatvorite sve programe tako da imate pregled nad svojim Desktopom.

2. Dvokliknite na **My Computer** ikonicu.

3. Kliknite na **View** stavku u meniju te kliknite na **Options** opciju.

4. Nakon što se pojavi novi prozor, kliknite na **View** tab.

5. Skrolajte do kraja sve dok ne vidite **Show all files** radio dugme te ga odaberite.

6. Kliknite na **OK** dugme te zatvorite prozor od **My Computer**.

Windows 98

Da biste omogućili gledanje skrivenih datoteka slijedite sljedeće korake:

1. Zatvorite sve programe tako da imate pregled nad svojim Desktopom.

2. Dvokliknite na **My Computer** ikonicu.

3. Kliknite na **View** stavku u meniju te kliknite na **Folder Options** opciju.

4. Nakon što se pojavi novi prozor, kliknite na **View** tab.

5. Skrolajte do kraja sve dok ne vidite **Show all files** radio dugme te ga odaberite.

6. Kliknite na **Apply** dugme, pa na **OK** dugme te zatvorite prozor od **My Computer**.

Windows ME

Da biste omogućili gledanje skrivenih i zaštićenih datoteka slijedite sljedeće korake:

1. Zatvorite sve programe tako da imate pregled nad svojim Desktopom.

2. Dvokliknite na **My Computer** ikonicu.

3. Kliknite na **Tools** stavku u meniju te kliknite na **Folder Options** opciju.

4. Nakon što se pojavi novi prozor, kliknite na **View** tab.

5. Pod **Hidden files and folders** skecijom odaberite radio dugme sa nazivom **Show hidden files and folders**.

6. Maknite kvačicu sa stavke **Hide file extensions for known file types**.

7. Maknite kvačicu sa stavke **Hide protected operating system files**.

8. Kliknite na **Apply** dugme, pa na **OK** dugme te zatvorite prozor od **My Computer**.

Windows NT

Da biste omogućili gledanje skrivenih datoteka slijedite sljedeće korake:

1. Zatvorite sve programe tako da imate pregled nad svojim Desktopom.

2. Dvokliknite na **My Computer** ikonicu.

3. Kliknite na **View** stavku u meniju te kliknite na **Options** opciju.

4. Nakon što se pojavi novi prozor, kliknite na **View** tab.

5. Skrolajte do kraja sve dok ne vidite **Show all files** radio dugme te ga odaberite.

6. Kliknite na **OK** dugme te zatvorite prozor od **My Computer**.

Windows 2000

Da biste omogućili gledanje skrivenih i zaštićenih datoteka slijedite sljedeće korake:

1. Zatvorite sve programe tako da imate pregled nad svojim Desktopom.

2. Dvokliknite na **My Computer** ikonicu.

3. Kliknite na **Tools** stavku u meniju te kliknite na **Folder Options** opciju.

4. Nakon što se pojavi novi prozor, kliknite na **View** tab.

5. Pod **Hidden files and folders** skecijom odaberite radio dugme sa nazivom **Show hidden files and folders**.

6. Maknite kvačicu sa stavke **Hide file extensions for known file types**.

7. Maknite kvačicu sa stavke **Hide protected operating system files**.

8. Kliknite na **Apply** dugme, pa na **OK** dugme te zatvorite prozor od **My Computer**.

Windows XP

Da biste omogućili gledanje skrivenih i zaštićenih datoteka slijedite sljedeće korake:

1. Zatvorite sve programe tako da imate pregled nad svojim Desktopom.

2. Dvokliknite na **My Computer** ikonicu.

3. Kliknite na **Tools** stavku u meniju te kliknite na **Folder Options** opciju.

4. Nakon što se pojavi novi prozor, kliknite na **View** tab.

5. Postavite kvačicu na stavku **Display the contents of system folders**.

6. Pod **Hidden files and folders** skecijom odaberite radio dugme sa nazivom **Show hidden files and folders**.

7. Maknite kvačicu sa stavke **Hide file extensions for known file types**.

8. Maknite kvačicu sa stavke **Hide protected operating system files**.

9. Kliknite na **Apply** dugme, pa na **OK** dugme te zatvorite prozor od **My Computer**.

[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

Korištenje LSP-Fix za micanje Spyware-a i Otimača Browsera **07.02.2005. u 06:23**

Uvod

LSP-Fix je vrlo koristan programčić koji se koristi za popravljanje problema koju su vezani za LSP, tj. *Layered Service Provider*. LSP-ovi su dizajnirani da se integriraju direktno u TCP/IP sloj, protokol koji vaš komp koristi za komunikaciju na Internetu, da bi manipulirao podacima koji se šalju "preko žice". LSP-ovi su instalirani na način da su međusobno ulančani. Ukoliko je jedan ovih LSP-ova maknut na neodgovarajući način, taj lanac može lako "puknuti", što će uzrokovati nemogućnost spajanja na Internet ili lokalnu mrežu.

LSP-Fix je program dizajniran da riješi takve probleme. Sa LSP-Fix možete maknuti LSP-ove malicioznih programa na način da se lanac međusobne ovisnosti ne razbije, tako da vaše mrežne aktivnosti i dalje pravilno rade. Ovaj će program također popraviti razbijene lance u slučaju da ih je razbilo brisanje neke specifične datoteke ili bugovita instalacija.

Korištenju ovog programa također treba pribjegnuti sa određenom dozom opreza. Ne biste smjeli koristiti ovaj program ukoliko Vam netko tko jako dobro poznaje virusnu materiju to nije rekao. Micanje pogrešnih LSP-ova sa vašeg kompa može uzrokovati nestabilnost vašeg kompa te potencijalno voditi do rušenja svih mrežnih aktivnosti, uključujući Interneta!

Vrste softvera koje koriste LSP

Mnogi različite vrste softvera koriste LSP-ove i praktično su to sve aplikacije koje koriste mrežne servise ili Internet. Nažalost, neke od ovih aplikacija imaju maliciozne namjere te kroiste LSP za preusmjeravanje prometa prema svojoj želji ili za prikupljanje informacija o tome kako koristite Internet. LSP-ovi koje koriste ove vrste softvera, koje se zovu Spyware ili Otimači Browsera, mogu biti izbrisani koristeći LSP-Fix.

Evo npr. potpuno korisnih i benignih programa koji koriste LSP-ove:

Sygate Firewall
Mcafee Personal Firewall
E-Safe

A sad npr. maliciozni programi koji koriste LSP-ove:

Webhancer
New.net
NewDotNet

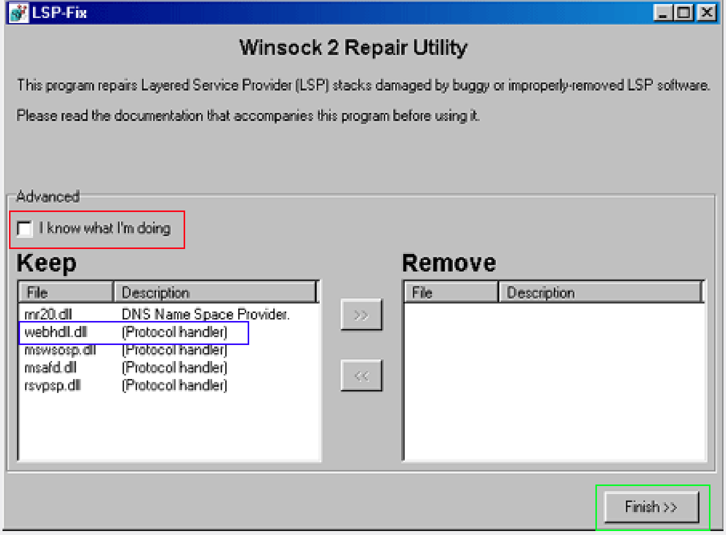
Nažalost, mnogi od ovih malicioznih programa su instalirani bez vašeg znanja ili želje, ali korištenjem LSP-Fix i pravilnim rukovanjem možete maknuti ove programe.

Kako koristiti LSP-Fix

Korak 1: Skini i pokreni LSP-Fix

Skinite LSP-Fix **odavde** i spremite ga u njegov vlastiti direktorij.

Nakon što ste ga skinuli, pozicionirajte se u odredišni direktorij te napravite dvoklik na ime programa. Dobit ćete prikaz kao na slici:



Sad kad je program pokrenut vidjet ćete prikaz sa dvije sekcije označene **Keep** i **Remove**. Sekcija **Keep** je za LSP-ove koje ne želimo maknuti, dok je sekcija **Remove** za LSP-ove koje želimo maknuti.

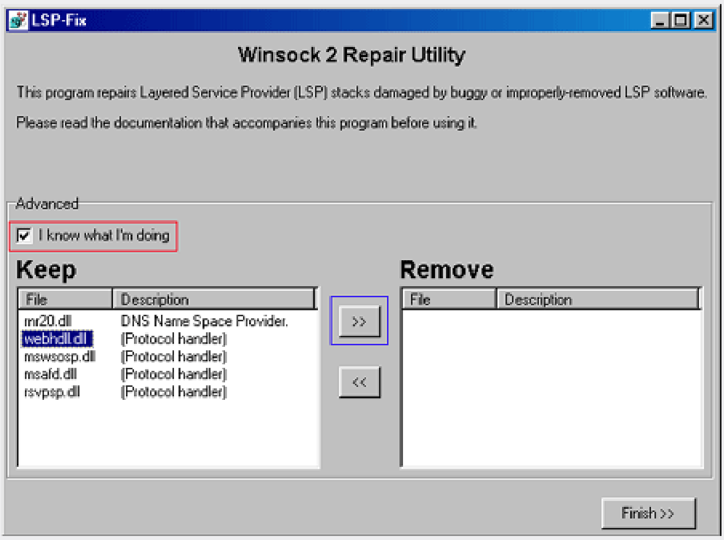
Između ove dvije sekcije postoje dva dugmeta sa nazivima **>>** i **<<**. Dugme **>>** će označeni LSP pomaknuti iz sekcije **Keep** u sekciju **Remove**. S druge strane, ukoliko želite LSP pomaknuti iz sekcije **Remove** u sekciju **Keep** koristit ćete **<<** dugme. Važno je uočiti da ovi dugmići neće raditi sve dok ne postavite kvačicu na stavku **I know what I'm doing** koja je označena crvenom linijom na slici gore.

Ukoliko samo želite popraviti puknuti LSP lanac, a problematični DLL je već maknut iz nekih drugih razloga, možete samo kliknuti na **Finish** dugme, označeno zelenom linijom na slici gore. LSP-Fix će automatski popraviti LSP lanac i (sa malo sreće) vratiti vaše mrežne mogućnosti u puni pogon. Ukoliko pokušavate maknuti specifični DLL iz lanca, pređite na korak broj 2.

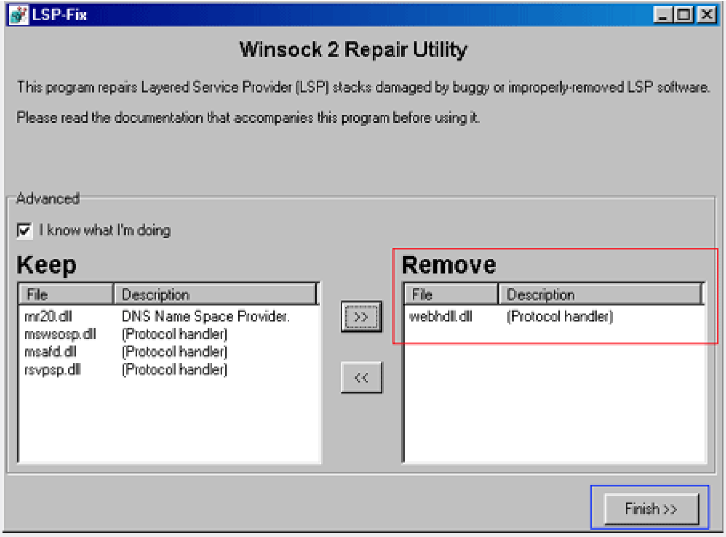
Korak 2: Makni LSP

Sad ćemo na konkrentom primjeru pokazati kako maknuti webhdll.dll kojeg instalira poznati Spyware program zvan Webhancer. Vi ćete, naravno, na vašem konkretnom problemu micati neku potpuno drugu datoteku.

Da bismo maknuli webhdll.dll stavimo prvo kvačicu na stavku **I know what I'm doing** da bismo aktivirali **>>** i **<<** dugmiće, te potom kliknemo na naziv webhdll.dll datoteke da bismo je označili kao što je prikazano na slici:

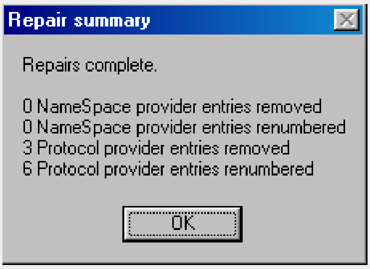


Nakon što ste i postavili kvačicu i označili LSP kojeg želite maknuti, pritisnite **>>** dugme da biste označeni LSP prenijeli u **Remove** sekciju. Nakon što ste ovo napravili, trebali biste vidjeti prikaz kao na slici:



Sad kad je LSP pomaknut u **Remove** sekciju, možete završiti proces klikajući na **Finish** dugme označeno plavom linijom kao na slici gore. Nakon što kliknete na **Finish** dugme, LSP će biti maknut za vašeg kompa na pravilan način, tako da LSP lanac ne pukne.

Kad LSP-Fix bude završio sa micanjem LSP-a, vidjet ćete sažetak u obliku poruke kao na slici:



[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

Korištenje Ad-Aware SE za micanje Spyware-a i Otimača Browsera **08.02.2005. u 06:00**

Uvod

Ukoliko sumnjate da imate spyware instaliran na Vašem kompu, tada je Ad-Aware SE odličan alat za njihovo micanje. Slijedite ovdje opisane korake i naučit ćete kako koristiti Ad-Aware SE za micanje spyware-a sa Vašeg kompa.

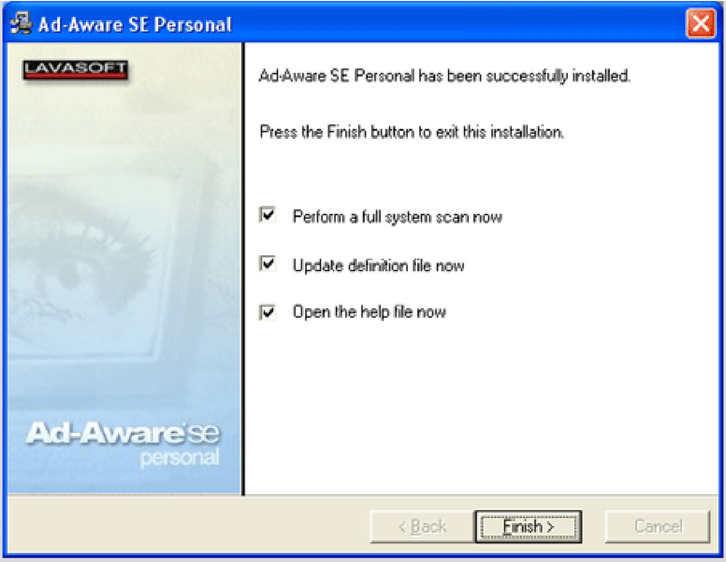
Malo upozorenje: ponekad je spyware usko vezan za neki specifičan program, pa micanje samog spyware-a može uzrokovati nepravilno funkcioniranje odredišnog programa! Stoga pažljivo gledajte što točno želite maknuti.

Kako koristiti Ad-Aware SE

Korak 1: Skinite i instalirajte Ad-Aware SE

Prvi korak jest skidanje i instalacija Ad-Aware SE sa **ovog** linka. Nakon što je program instaliran, nastavite sa sljedećim korakom.

Skinite program na poznatu lokaciju na tvrdom disku (recimo Desktop) te se pozicionirajte u odredišni direktorij. Napravite dvoklik na skinutu instalaciju programa, čiji je naziv obično u obliku aawse<verzija>.exe. Npr. za trenutnu verziju Ad-Aware SE Personal ime datoteke jest **aawsepersonal.exe** Odaberite *default-ne* postavke koje su vam ponuđene pri instalaciji, a kad se instalacija završi, bit će Vam ponuđen prikaz kao na slici:



Maknite kvačice sa svih opcija pošto ćemo ručno obaviti te korake u sljedećoj sekciji teksta. Nakon toga pritisnite **Finish** dugme.

Korak 2: Pokrenite Ad-aware SE

Na dekstopu dvokliknite na ikonicu od Ad-Aware SE. Program će se pokrenuti i bit će Vam prezentiran prikaz kao na slici:

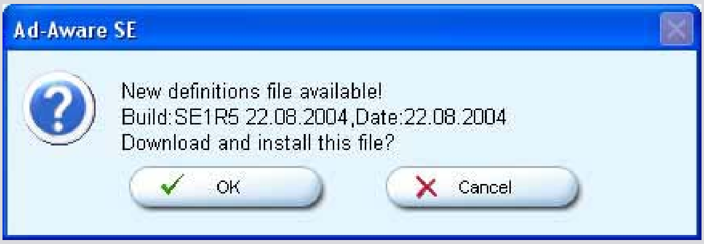
Ovo je glavni statusni prozor za Ad-Aware SE. Svaka sekcija koja je Vama kao korisniku važna jest uokvirena različitom linijom. Crvena linija okružuje **Scan Now** dugme koje se rabi kad želite Vaš komp skenirati za Spywareom i Otimačima Browsera. Plava linija okružuje dugme koje će vas odvesti na prikaz odabira opcija za Ad-Aware SE. Roza linija predstavlja dugme na koje biste kliknuli da želite vidjeti Spyware/Otimače Browsera koji su pohranjeni u karantenu. Žuta linija uokviruje dugme koje koristite za redovan *update* definicija *malware-a* u bazi programa.

Korak 3: Nadogradnja *malware* definicija

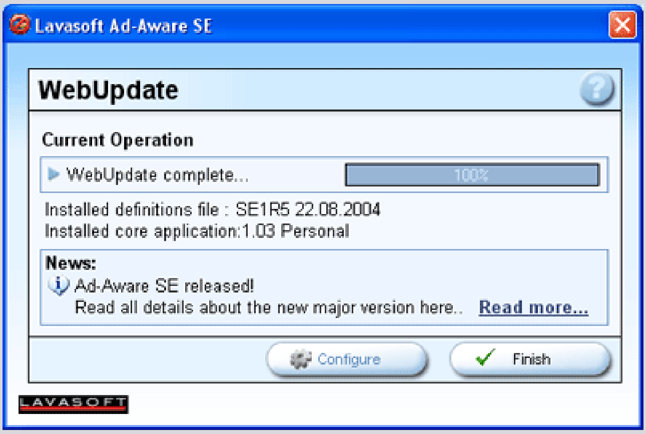
Prvi korak koji biste trebali napraviti jest nadograditi bazu *malware* definicija programa kako biste imali definicije za najnoviji Spyware i Otimače Browsera. Ova akcija omogućava programu da prepozna što je moguće više ovakvih malicioznih programa. Trebali biste kliknuti na **WebUpdate** dugme, uokvireno žutom lijom na prošloj slici, za početak procesa *update-ovanja*. Kada pokrenete proces trebali biste vidjeti nešto slično ovome:

Sada pritisnite **Connect** dugme, ono što je uokvireno crvenom linijom, te tako provjerite da li postoje novije definicije. Ukoliko ne postoje, prikazat će vam se nešto poput ovoga na slici dole. Pritisnite **OK** i pređite na korak 4.

Ukoliko su nadogradnje definicija dostupne, vidjet ćete nešto poput ovoga:



Jednom kliknite na **OK** dugme i pustite da se nove definicije skinu. Nakon toga će vam biti dan prikaz poput ovoga:



Sad možete kliknuti na **Finish** dugme. Kad to uradite, prikazat će vam se ponovno već spomenuti statusni prozor.

Korak 4: Postavljanje opcija skena

Sad kad je Ad-Aware SE nadograđen sa najsvježijim definicijama, spremni ste za njegovo konfiguriranje kako biste optimizirali postavke skena. Za početak kliknite na **Configuration** dugme pri vrhu prozora, na početnoj slici uokvireno plavom linijom, izgleda poput kotača. E sad će vam iskočiti prozor sa hrpom postavki koje možete podesiti. Slijedite ove instrukcije za konfiguraciju:

1. Kliknite na **General** dugme na lijevoj strani. Provjerite i stavite zelene kvačice na sljedeće postavke u kategoriji **Safety**:

1. **Automatically save logfile**

2. **Automatically quarantine objects prior to removal**
3. **Safe Mode (always request confirmation)**

2. Sljedeće kliknite na **Advanced** dugme na lijevoj strani. Proovjerite i stavite zelene kvačice na sljedeće postavke u kategoriji **Logfile Detail Level**:

1. **Include additional object information**
2. **Include negligible objects information**
3. **Include environment information**
4. **Include Alternate data stream details in log file**

3. Sljedeće kliknite na **Tweak** dugme na lijevoj strani. Nakon toga kliknite na + (plus) znak pored **Log Files** sekcije. Ovo će proširiti tu sekciju. Provjerite i stavite zelene kvačice na sljedeće postavke u kategoriji **Logfile Detail Level**:

1. **Include basic Ad-Aware settings in logfile**
2. **Include additional Ad-Aware settings in logfile**

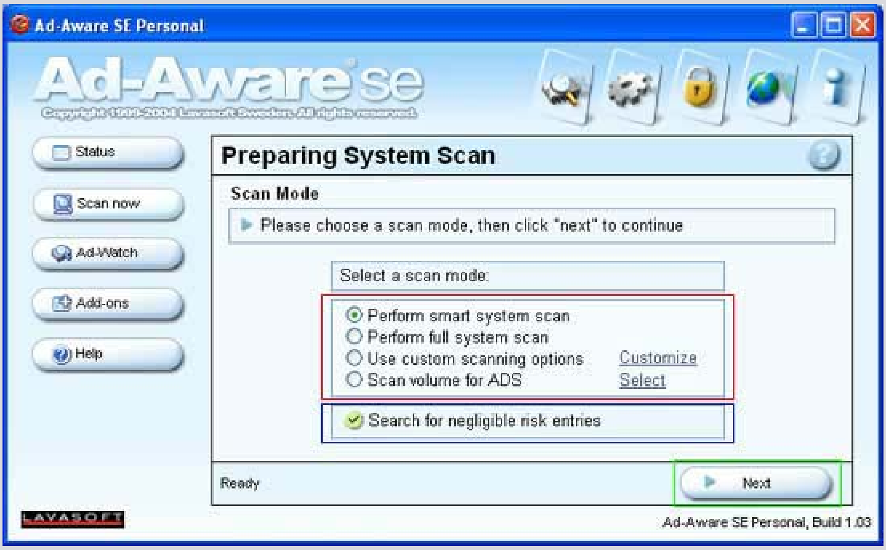
Nakon toga kliknite na + (plus) znak pored **Scanning Engine** sekcije. Ovo će proširiti tu sekciju. Provjerite i stavite zelene kvačice na sljedeće postavke u kategoriji **Logfile Detail Level**.

1. **Unload recognized processes & modules during scan**
2. **Scan registry for all users instead of current user only**

Nakon toga kliknite na + (plus) znak pored **Cleaning Engine** sekcije. Ovo će proširiti tu sekciju. Provjerite i stavite zelene kvačice na sljedeće postavke u kategoriji **Logfile Detail Level**.

1. **Always try to unload modules before deletion**
2. **During removal, unload Explorer and IE if necessary**
3. **Let Windows remove files in use at next reboot**
4. **Delete quarantined objects after restoring**

Nakon što ste završili ova podešavanja, kliknite na **Proceed** dugme. Pojavit će vam se prikaz kao na slici:



Provjerite da je mod skeniranja, gore uokviren crvenom linijom, postavljen na stavku **Perform full system scan**. Nakon toga maknite kvačicu sa stavke **Search for negligible risk entries**.

Korak 5: Skeniranje

Sada kliknite na **Next** dugme da bi Ad-Aware SE počeo skenirati Vaš sistem za Spyware-om i Otimačima Browsera. S obzirom da bi ovo moglo prilično potrajati, napravite nešto korisno u međuvremenu...pošaljite SMS curi, odite na kavu...nešto. Za vrijeme skena prikaz će izgledati kao na slici:

Ad-Aware SE će skenirati razne dijelove Vašeg kompa, uključujući razorazne konfiguracijske postavke, datotečni sustav, memoriju te registar za tragovima poznatih malicioznih programa. Kako bude nalazio infekcije, status skena će se osvježavati sa prikazom trenutno pronađenih infekcija. Nakon što je skeniranje završeno, bit će vam prezentiran prikaz kao na slici:

Komp skeniran na slici ima relativno malo infekcija, kao što vidite, jer je Ad-Aware SE našao samo 4 infekcije. Ukoliko želite kopirati sadržaj rezultata skena, možete kliknuti na **Show Logfile** dugme, koje je uokvireno plavom linijom gore na slici, otvoriti log datoteku te uraditi *copy/paste* u neki drugi program, obično tekst procesor. Da biste završili sa čišćenjem, kliknite na **Next** dugme koje je na slici uokvireno crvenom linijom. Bit će vam prikazana lista objekata za koje Ad-Aware SE smatra da su ili Spyware ili Otimači Browsera, kao što je prikazano na slici:

Sada možete ili napraviti desni klik na prikaz i odabrati **Select All Objects** opciju, ili individualno postaviti kvačice na svaku od njih, kao što je uokvireno plavom linijom na slici, za koje želite da ih pošaljete u karantenu. Nakon što su svi objekti koje želite poslati u karantenu odabrani, kliknite na **Next** dugme. Ad-Aware SE će vam prikazati dijalog za potvrdu u kojem će vas pitati da li želite maknuti objekte koje ste odabrali. Ukoliko želite, kliknite na **OK** dugme, inače kliknite na **Cancel** dugme da biste se vratili na prethodan prikaz za odabir. Ukoliko pritisnete **OK**, Ad-Aware SE će odabrane objekte pomaknuti u karantenu.

Nakon što je završeno micanje označenih objekata u karantenu, prikazat će vam se ponovno statusni prozor kao na sljedećoj slici.

Korak 6: Čišćenje karantene

Nakon što je micanje objekata u karantenu završeno, dobit ćete prikaz kao na slici dole. Kao što je prije rečeno, kad "popravljate" infekciju Ad-Aware SE ih ne briše automatski, već ih dodaje u karantenu koja zauzima prostora na disku. Stoga ih se nije loše potpuno riješiti čišćenjem karantene. Prije nego što to uradite, bilo bi dobro da neko vrijeme intenzivno koristite svoj komp za svakodnevne radnje, da se uvjerite da stavljanje nekog objekta u karantenu nije uzrokovalo "pucanje" neke od instaliranih aplikacija. Ako se uvjerite da nije, tada možete nastaviti.

Kao što vidite, svi objekti koje ste označili kvačicom se sad nalaze u karanteni. Da biste pristupili karanteni, kliknite na link koji kaže **Open Quarantine List**, što će Vas dovesti do sljedećeg prikaza:

Sada možete odabrati datoteku u karanteni koju želite izbrisati i pritisnuti <delete> taster, što će željenu datoteku fizički izbrisati sa Vašeg diska. Nakon što ste završili sa brisanjem datoteka u karanteni, možete izaći iz programa.

[**brisanje!** | Upload uz poruku |Izmena/Brisanje | Odgovor na temu]

Kako rade antivirusi **09.02.2005. u 23:50**

Kako rade antivirusi

by **Ivan Toman**

1. Uvod

Već više od 2 desetljeća, računalni virusi su prisutni na sceni, gdje predstavljaju stalnu i realnu prijetnju svim vrstama računalnih sustava diljem svijeta. Vrlo često, virusi su povezani s velikim financijskim gubicima, poglavito kad je riječ o infekcijama računalnih mreža velikih poduzeća, iako dotični virusi možda i nisu bili napisani u cilju izazivanja štete, a mnogi koji i jesu, ne rade kako treba. Međutim, kako su virusi dizajnirani da utječu ili potpuno onemoguće rad korisničkih programa, te se šire računalnim mrežama, na skoro svim platformama, a u posljednje vrijeme masovno internetom, oni često osim izravne štete uzrokuju i onu neizravnu, koja se opisuje pojmom izgubljene dobiti, točnije, izgubljenog vremena na čišćenju zaraženih sustava, te njihovom ponovnom vraćanju u normalan rad. Kako se popularno s razlogom kaže da je vrijeme novac, zaista je lako zaključiti zbog čega će jedno veliko poduzeće sa tisućama zaraženih kompjutera, koje je potrebno dovesti u normalan rad, izgubiti velike količine profita. Mnogo češće su neizravne štete puno veće od onih izravnih. Dodatno, izvršavanje virusnog, često nepoznatog koda, na osjetljivim računalnim sustavima (banke, bolnice, znanstveni centri, vojska itd.) dovodi do pitanja ispravnosti rada namjenskih aplikacija i podataka vezanih uz njih, što često vodi do potpunog reinstaliranja platforme i aplikacija na svim računalima takvog jednog sustava, te do vraćanja podataka iz nezaraženih backup izvora, ukoliko takvi postoje.

Iako je ova prijetnja svakim danom sve veća, što zbog većeg broja računala, što zbog njihovog boljeg i raznovrsnijeg povezivanja, tehnologija koja joj se odlučila suprostaviti, te ima za cilj obranu računalnih sustava od virusa, nažalost nije dovoljno prihvaćena kod korisnika. S jedne strane, mnogi ne znaju, niti žele znati kako antivirusni programi rade, jer se time "ne trebaju opterećivati", a s druge strane, antivirusni sustavi se često shvaćaju kao skupi programi koji ne donose nikakav profit. Kao rezultat, antivirusni programi, ako i jesu instalirani, vrlo su često nepravilno iskonfigurirani ili se o njima ne vodi računa.

Kratica AV, u užem smislu znači "antivirus", dok u širem opisuje industriju, proizvode, te usluge koji se bave zaštitom računala od virusa.

2. Povijest

Mnogi rani virusi su rijetko napravili više od nekoliko infekcija, te su na taj način sami od sebe odumrli. Razlog takvom "neuspjehu" je vrlo slaba povezanost računala međusobno, te nisu imali kvalitetan medij kojim bi se širili međusobno. Tada je otkrivanje i uklanjanje sa zaraženih strojeva bilo mnogo jednostavnije nego danas. Vrlo kratko nakon pojave prvih virusa, pojavile su se i prve inačice jednostavnih antivirusnih alata. Prvi AV skeneri nisu bili u stanju dezinficirati zaražene sustave, već su jednostavno služili za provjeru datoteka. U to vrijeme, većina virusa bila je distribuirana preko floppy diskova, jer velikih računalnih mreža (internet) nije niti bilo.

Međutim, promjene koje su nastale pojavom velikih računalnih mreža, a poglavito interneta, dovele su do pojave novih vrsta virusa i brzine njihovog širenja. Na primjer, do 1992. godine, broj boot sector virusa i file-infecting virusa bio je podjednak. 1992., broj file-infecting virusa počeo se smanjivati, a boot sector virusa povećavati. Taj trend je nastavljen do 1995. godine, kada većina računala prelazi na Windows platformu, a pogotovo nakon prelaska na Windows 95, sustav koji je mogao obavijestiti korisnika o promjenama u boot-sektoru, što je poslužilo vrlo jednostavnoj detekciji boot sector virusa. Također, s pojavom Microsoftovog paketa Office, autorima virusa postalo je jasno da postoji puno bolja podloga za širenje njihovih uradaka. Mogućnost ove platforme da pomoću više programa koristi iste informacije, dovela je do nastanka velikog broja nove vrste - macro virusa. Ovi virusi vrlo su jednostavni za pisanje u Visual Basicu, te se iznimno lako šire među korisnicima Microsoftovih uredskih aplikacija Word, Excel, PowerPoint i Access. Dodatno, macro virusi su prvi koji su bili u stanju raditi na više platformi (npr. virus napisan za Windowse ne može raditi na Macintosh platformi).

Rani virusi su zahtijevali ljudski faktor da bi se mogli širiti. Korisnici su bili ti koji su im omogućavali širenje, najčešće iz neznanja, tj. nesvjesnosti njihovog prisustva, dijeljenjem datoteka, floppyja i sl. među sobom. Nakon početka automatiziranja mnogih procesa (macro naredbe u Office paketima), ljudska "pomoć" širenju virusa više nije bila toliko neophodna. Danas, samim otvaranjem zaraženog e-maila, moguće je pokrenuti virus, bez ikakvog znanja o njegovom prisustvu, čak štoviše, danas iznimno popularni crvi dolaze putem interneta na računalo bez ikakve ljudske prisutnosti.

Paralelno s razvojem i usavršavanjem virusa, razvijali su se i usavršavali alati za borbu protiv njih. AV programi su nešto poput patrolnog policajca na cesti, koji promatra ponašanje prolaznika i pokušava pretpostaviti nečije loše namjere. I policijski službenik i AV skener traže određene "uzorke" ponašanja, te kreću u akciju ukoliko to ponašanje prijeđe prag prihvatljivosti. No, kao i policijski službenici, i AV skeneri ponekad donose krive zaključke. Jednostavno, nije moguće znati namjeru svakog bita koda koji uđe u računalo, i nije zgodno testirati svaki bit koda prije njegovog izvršavanja, jer bi to ozrokovalo ogroman pad performansi sustava i onemogućilo izvršavanje legitimnih programa. Najviše što AV skener može učiniti je tražiti uzorke ponašanja, bazirane na svojoj bazi podataka, a koji su se u prošlosti pokazali kao "lošima".

Prvi antivirusni alati radili su na principu da je određeni "alat" napisan za određeni virus, te su dakle korisnici najprije trebali otkriti o kojem se virusu radi (što nije bilo teško jer ih je bio vrlo mali broj), te tada nabaviti odgovarajući alat i popraviti što se popraviti može.

Virusi iz toga vremena su ubacivali svoj kod na određena predvidljiva mjesta u programu. AV skeneri su tražili taj kod (tj. specifični string znakova), te ukoliko bi kod bio pronađen, on bi se brisao, te bi se program pokušao dovesti u prijašnje stanje. Ukoliko to nije bilo moguće, AV bi korisniku savjetovao brisanje programa i njegovu reinstalaciju.

Kako je broj virusa počeo naglo rasti, antivirusne kuće su shvatile da izdavanje specifičnih alata za specifične viruse neće objektivno biti moguće u dogledno vrijeme, te je bilo potrebno pronaći nov način za traženje virusa, koji će se sastojati u univerzalnom programu koji će tražiti sve viruse prema određenim predefiniranim uzorcima. Nova generacija AV programa tako se sastojala od dvije komponente: antivirusnog skenera i baze podataka sa uzorcima stringova. Te dvije komponente u potpunosti ovise jedna o drugoj. Mnogi tadašnji antivirusni alati nisu polučivali dobre rezultate, jer nisu bili u stanju pronaći sve poznate viruse, a osim toga, postojao je tada nerješiv problem otkrivanja novih, nepoznatih virusa, kojih nije bilo u bazi s uzorcima.

Dvije su stvari dovele do revolucije antivirusne tehnologije. 1993. godine, Joe Wells počinje kolekcionirati viruse i stvara "biblioteku" virusa koju naziva "WildList", te ju daje na uvid i korištenje antivirusnim kućama, koje do tog trenutka nisu imale standardiziranu bazu virusa, već se je svaka oslanjala na svoje vlastite podatke. Njegova lista je podijelila viruse u dvije skupine; prva, u koju pripadaju aktivni virusi, tj. oni za koje se zna da trenutno postoje kao aktivni na računalima diljem svijeta, nazvana je in the wild, a druga skupina bi bila ona koji više nisu aktvini, tj. "izumrli" su jer su "istrijebljeni" sa svih aktivnih računala u svijetu (in the zoo). Također, lista je omogućila da se standardiziraju imena virusa.

Druga važna stvar koja se dogodila bila je početak komercijalnog testiranja i davanja certifikata AV produktima od strane NCSA (National Computer Security Association), kasnije znane kao ICSA.net, pa TruSecure Corporation. Antivirusne kuće su slale svoje produkte na testiranje, i time su bile prisiljene da na objektivan način dokažu kvalitetu svojih proizvoda.

3. Ustrojstvo AV programa

Nemoguće je sa sigurnošću znati za svaki program koji se pokreće na računalu da li je legitiman ili pak virus. Kad bi AV skeneri mogli znati sa 100%-tnom sigurnošću da li neki program pripada jednoj ili drugoj skupini, njegov kod bi bilo moguće ugraditi u sam operativni sustav, te ne bi bilo potrebe za dodatnim AV programima. Također, nemoguće je da AV skener provjerava svaku datoteku koja se izvršava u cijelosti, jer bi za tako nešto bilo potrebno jako mnogo sistemskih resursa računala, te bi takvo okruženje bilo gotovo neupotrebljivo. Stoga, AV programi djeluju unutar nekih ograničenja koje im nameće sam operativni sustav. U cilju efektivnog rada, bez velikog utjecaja na ostale programe koji se izvršavaju na računalu, AV programi se koriste raznim trikovima kako bi spriječili virusnu infekciju, pronašli i dezinficirali zaražene datoteke, a pritom zadržali koliko-toliko nedirnutu brzinu izvođenja ostatka sustava.

4 su osnovne metode kojima se AV programi koriste u svojem radu:

• Detekcija - traženje već poznatih virusa

• Prevencija - praćenje promjena, i pokušaja mijenjanja datoteka, boot sektora itd

• Heuristika - traženje dosad nepoznatih virusa, koristeći određena "pravila ponašanja"

• Praćenje stanja svih sistema koji su povezani na središnji sustav izvještavanja (ovo će biti objašnjeno kasnije)

Antivirusni program (engine) i njegova baza podataka sa poznatim uzorcima virusa rade zajedno u cilju detekcije virusa koji ulaze u sistem. Engine je uobičajeno predstavljen kao korisničko sučelje, te pruža osnovni set funkcija i kontrola za podešavanje rada antivirusnog sustava. Sastoji se od mnogo složenih algoritma za traženje uzoraka, CPU emulatora, te raznih formi programske logike. Engine određuje koje će datoteke skenirati, koje funkcije pokretati, te kako djelovati u slučaju kada posumnja da je u određenoj datoteci pronađen virusni kod. Ipak, sam engine ne zna apsolutno ništa o virusima, i gotovo je bespomoćan bez baze podataka sa uzorcima virusa (signature database).

Baza podataka s uzorcima sadrži "otiske prstiju" desetaka tisuća virusa. Kako se novi virusi pojavljuju sve brže, od iznimnog značaja je da se baza podataka stalno nadopunjuje novim podacima. Tako je 1995. godine kao generalna preporuka važila da se baze nadopunjuju barem jednom mjesečno, dok je danas taj rok oko jednom tjedno, a za kritične sustave i svakodnevno. Danas se svi antivirusni programi mogu lagano i brzo obnoviti putem interneta, a mnogi taj posao maksimalno pojednostavnjuju automatizacijom.

Baza s uzorcima, osim egzaktnih stringova, sadrži i neka pravila koja antivirusni programi koriste za heurističko skeniranje. Naime, ukoliko se pojavi novi virus, koji ne postoji još u bazi uzoraka, antivirus ga ne može pronaći, osim prema već spomenutim "pravilima ponašanja", tj. ako utvrdi da bi se određena datoteka prilikom izvršavanja ponašala prema nedopuštenim pravilima, bit će klasificirana kao "sumnjiva". Ovakvo skeniranje je mnogo sporije nego ono koje samo traži poznate stringove, te mu učinkovitost znatno varira od proizvoda do proizvoda. Mnogo proizvoda nam daje na izbor koliko želimo "duboku" heurističku analizu - što je ona "dublja", to je više pravila obuhvaćeno njome, a samim time i proces sporiji, ali mogućnost detekcije nepoznatog virusa veća.

Skeniranje datoteka moguće je u tri načina rada - nakon pokretanja sustava, stalno, ili na zahtjev. Najučinkovitije skeniranje je konstantno, tj. u pozadini se stalno izvršava antivirusni program koji skenira sve procese koji se izvode na računalu. Međutim, ovo može dosta usporiti sistem, ovisno o njegovoj brzini, te postavkama i karakteristikama samog AV programa, ali i o vrsti posla na računalu. Pritom, AV programi koriste i dosta sistemske memorije, kako bi testirali određene sekcije koda datoteka koje se provjeravaju. Dakle, potrebno je pronaći "zlatnu sredinu", tj. AV program mora omogućiti zaštitu računala, a pritom korisnik mora moći nesmetano koristiti sve sistemske resurse, ili barem veliku većinu.

Rani virusi su prilikom inficiranja programa, svoj kod ubacivali na određeno mjesto u prorgamu, tako da je pri skeniranju bilo dovoljno potražiti to mjesto i vidjeti da li na njemu postoji virusni kod, izbjegavajući skeniranje datoteke od vrha do dna i tako drastično štedeći vrijeme. Danas, to više nije u potpunosti slučaj, pa je ponekad potrebno pregledati cijelu datoteku. Tako mnogi AV programi imaju implementiranu mogućnost da koriste pregled kompletnih datoteka, što znatno usporava izvođnje operacija.

Postoji mogućnost da prilikom skeniranja legalnog programa, AV naiđe na kod koji se sasvim slučajno poklapa sa nekim iz baze uzoraka, ili pak sa "pravilom o ponašanju", pa prijavi "čistu" datoteku kao zaraženu. Nažalost, lažnih alarma ima uvijek, no u posljednje vrijeme su ipak sve rijeđi, jer programeri koriste sve bolje rutine za njihovo izbjegavanje.

Nastankom novih, kompleksnijih virusa, skeniranje koristeći isključivo baze sa uzorcima postaje sve nepouzdanije. Neki virusi čak niti nemaju karakterističan kod po kojem bi se mogli bespogrešno prepoznati. Ima virusa koji nastoje ubaciti svoj kod u područja programa koja su već prije bila skenirana, ili pak smještaju svoje fileove u direktorije ili dateoteke koje se uobičajeno ne skeniraju (npr. .cab datoteke). Zatim, virusi koriste promjenjive enkripcije koda, mijenjaju formu, te mutiraju, sve u pokušaju da se što bolje sakriju od AV programa.

U mnoge antivirusne programe danas je ugrađena metoda provjere checksum-e, kao dodatna sigurnosna opcija za traženje nepoznatih virusa. Ovim putem se provjeravaju datoteke, te se traži da li su se mijenjale od vremena posljednje provjere. Prilikom provjere, checksum-e provjerenih datoteka se zapisuju u posebnu bazu podataka. Ukoliko promjene veličine datoteke nema, znači da nije došlo do njezine infekcije u tom periodu. Ako se promjena dogodila, ona može biti legitimna, ali može biti i virus. Da bi AV otkrio o čemu je riječ, poduzimaju se dodatne radnje nad takvim datotekama (skeniranje, obavještavanje korisnika itd, ovisno o postavkama).

Zatim, AV se koriste u svojem radu brute-force dekripcijom enkriptiranih virusa, jer mnogo je virusa danas enkriptirano, koji se prilikom infekcije automatski enkodiraju na drugačiji način, što dovodi do drugačijeg "otiska prstiju", i tako enkriptirani virus se ne poklapa sa svojim uzorkom u AV bazi uzoraka. Ukoliko se pronađe algoritam za dekripciju, on se pohranjuje u bazi uzoraka zajedno sa uzorkom.

Emulacijom programa AV se koriste najčešće za otkrivanje polimorfnih virusa. Program kojeg se provjerava, emulira se u simuliranom orkuženju operativnog sustava, tj. antivirus nastoji simulacijom izvođenja dotičnog programa procijeniti što bi se dogodilo ako se program zaista i pokrene. Tada na snagu stupaju već spomenuta "pravila ponašanja", te ukoliko se prijeđe prag tolerancije, datoteka se smatra sumnjivom ili zaraženom.

Heuristička analiza datoteka, iako vrlo korisna za otkrivanje novih, nepoznatih virusa, ima lošu stranu što nikada ne može biti 100% pouzdana. Neki produkti se hvale sa 80%-tnom pouzdanošću otkrivanja virusa bez poznavanja njihovih uzoraka. Drugi problem je taj što ovakvo skeniranje traži i dosta procesorskog vremena, a u slučaju većih i kompliciranijih datoteka i mnogo sistemske memorije, pogotovo kod emuliranja izvršavanja programa.

Prilikom heurističkog skena, skeniranoj datoteci se dodijeljuju "bodovi", koji označavaju da li je datoteka bila "pozitivna" na određenom testu "pravila ponašanja". Što više bodova skupi, to je na više testova bila "pozitivna", te se ukoliko prijeđe pretpostavljenu granicu, smatra sumnjivom (niža granica) ili zaraženom (viša granica). Pritom se provjeravaju datoteke samo na uobičajenim mjestima na kojima se virusi u njima najčešće nalaze, jer datoteke mogu biti ogromne veličine, te njihovo komplteno provjeravanje bi trajalo iznimno dugo. Npr. video datoteka od par gigabajta se skenira za tren, jer se pretraži samo njezin malen dio (obično je riječ o početku datoteke, prvih nekoliko linija koda), dok bi njezino kompletno skeniranje trajalo minutama (sa današnjim uobičajenim brzinama računala). Navedena metoda se naziva statičkim skeniranjem.

Za razliku od statičkog skeniranja, kod dinamičkog se program još dodatno emulira, a ono se obično poduzima samo ukoliko je "broj bodova" u statičkom skenu bio relativno velik. U virtualnom okruženju pokreće se kod sumnjive datoteke i prati ponašanje simuliranog sustava. Jasno je da će ovakvo izvođenje operacija zahtijevati prilične sistemske resurse računala, no to je cijena koja se mora platiti ukoliko se želi relativno moćno traženje nepoznatih virusa. Valja primjetiti da se dinamički sken ne poduzima ukoliko je u statičkom datoteka prošla dobro, tj. sa malim "brojem bodova", što je u biti dvosjekli mač - štedi se iznimno puno sistemskih resursa, međutim, neki virusi mogu ostati neotkriveni bez dinamičke heurističke analize. Napomenimo samo, kako ni dinamička analiza nije svemoguća, te poneki maliciozni program može i pored nje proći neotkriven, ovisno o njegovim "namjerama".

4.. "Imuni sustavi"

Više od jednog desetljeća, pisci antivirusnih programa pokušavaju smisliti sustav koji će biti otporan na viruse i u slučaju inficiranja sam sebe "izliječiti", bez intervencije korisnika. Pri tome su se istraživači dosjetili da bi mogli pokušati "kopirati" ljudski imunološki sustav, tj. njegovu osnovnu funkcijsku strukturu. Sustav koji su zamislili sastoji se od praćenja stanja, te u slučaju infekcije bilo kojeg njegovog dijela, pokušaja automatskog "izliječenja", te samo u slučaju neuspjeha, pozvalo bi se korsnika na intervenciju. Trenutno u svijetu antivirusa postoje određena rješenja koja manje ili više uspješno prate i pretvaraju u djelo ovu zamisao. Pa, objasnimo pobliže o čemu je riječ.

Izolirano računalo, tj. ono koje nije spojeno na računalnu mrežu, nakon zaraze virusom, nema velike šanse za "samoizliječenje", jer mu nedostaje osnovno sredstvo za borbu protiv virusa - poznavanje njega samog, dakle, ukoliko je virus prošao neopaženo jer nije prepoznat, niti u vremenu koje predstoji, samo od sebe dotično računalo neće "naučiti" ništa novo o virusu. S druge pak strane, računalo koje je povezano u mrežu, već ima dosta veće šanse, jer u slučaju infekcije može lako "pozvati pomoć" od strane računala koja nisu zaražena.

Kada smo spomenuli 4 osnovna načina na koji AV programi pokušavaju spriječiti zarazu računala, naveli smo i "praćenje stanja svih sistema koji su povezani na središnji sustav izvještavanja", ali nismo ništa pobliže rekli o tome. Sustav o kojem je riječ, tj. "sustav izvještavanja", zapravo prati stanje svih svojih dijelova, na način da ima jedan ili više centralnih servera koji služe kao "mozak" sustava, a svaka radna stanica (nazovimo tako ostala računala sustava, mada oni mogu biti bilo što), "vrti" na sebi klijentski dio antivirusne aplikacije, koji prati "zdravstveno" stanje na toj stanici. Centralni server može biti lociran unutar LAN mreže, ali može biti i server u laboratoriju proizvođača antivirusnog sustava.

Ukoliko sustav praćenja "zdravstvenog" stanja određene radne stanice posumnja u prisutnost virusa, kojeg ne pronalazi u svojoj bazi uzoraka, on tada pravi kopiju sumnjivog programa, te ju šalje centralnom serveru na analizu. Nakon primitka sumnjive datoteke, server ju proslijeđuje testnom računalu. Na tom računalu, u kontroliranim uvjetima, nepoznati i sumnjiv kod se može bez opasnosti pokrenuti, jer je to računalo namijenjeno isključivo za potrebe takvog testiranja, te je ono izdvojeno od ostalih, i komunicirati može jedino sa centralnim serverom, i to pod određenim i vrlo strogim uvjetima.

Testno računalo tada pokreće cijeli niz specijaliziranih koraka, da bi što je moguće bolje poručilo ponašanje sumnjivog programa u praksi, tj. u stvarnim uvjetima izvođenja. Cilj cijele ove priče na testnom računalu je da ono pokuša (ukoliko je zaista riječ o virusu) izdvojiti njegov uzorak, te pronaći način za njegovo uklanjanje sa sustava. Kao rezultat analize, testno računalo šalje natrag centralnom serveru, uzorak virusa i metodu za njegovo uklanjanje sa zaraženih računala. Centralni server dalje distribuira svim klijentskim računalima nadopunu baze sa uzorcima, te "lijek", tj. program ili što je već potrebno za čišćenje zaraženih računala, koji se automatski izvršava bez potrebe za korisničkom intervencijom.

Međutim, ukoliko testni sustav nije u mogućnosti pronaći način za čišćenje zaraženih računala, tada centralni server šalje virus programerima koji su i inače zaduženi za analizu virusa na daljnju "ručnu" obradu, i to je jedini slučaj kada bi ovakav sustav trebao zatražiti intervenciju korisnika.

Ovde je gotovo sve receno, svaka cast za detalje a evo i jednog mog tekstica pa mozda i on bude nekom od pomoci.

http://space.tin.it/computer/zristic/paraziti.htm

i ovo:

ZAŠTITA SISTEMA

Spyware, Adware, dialers, hijackers ...

Obicnim surfovanjem, bez vaseg znanja, mozete zakaciti razne spyware, adware dialers programe i time uciniti da vas PC postane domacin ovim napastima.

Spyware je sve rasirenija vrsta softvera koji potajice prenosi podatke o korisnikovim online aktivnostima, a strucnjaci predvidaju kako bi ove vrste programa mogle zaraziti i do 90 posto svih racunala povezanih s Internetom. Ako ga se na vrejeme ne otkrijete, spyware moze dovesti do krade identiteta i osobnih podataka, kvara racunara ili najezde dosadnih pop-up reklama.

Dialers nisu spy programi ali vam mogu napraviti velike tel. racune tako sto vrse dial up konekciju sa udaljenim racunarima u svetu. Obicno se zakace prilikom posete porno sajtovima, kreiraju ikonu u startapu tako da se podizu sa vindowsom.

Adware su programi koji prikazuju reklame dok su programi startovani. Obicno reklame izlaze kao pop-up prozori ili kao prozori u okviru samog programa.

Hijackers su kradljivci vase Home Page strane koja je postavljena kao osnovna. Oni ce promeniti podesavanje Internet Explorera i postavice svoju stranu kao Home Page, prebacivace saobracaj na nezeljene web strane ... Ubacice se u registry bazu tako da se uvek vraca bez obzira na vasu promenu u opcijama Internet Explorera.

Kako se zastititi?

- Najbolje bi bilo iskljuciti ActiveX, Skripting i Cookies
ali time mnoge strane na webu nece biti dostupne.
- Kada posetom nekoj web strani dobijete dijalog sa pitanjem
da li zelite da instalirate nesto, uvek odgovarajte NO !
- Koristite Opera browser koji ima manje sigurnosnih rupa nego IE
- Koristite neki od programa za real time zastitu od ovih
programa:

1. **SpywareGuard 2.2**

2. Ad-watch, koji je deo programa [url=http://www.lavasoft.de/software/adawareprofessional/
]Ad-Aware Professional v6.0.181 Retail[/url]

Ovi programi prate svaki pokusaj upisivanja podataka u registry bazu, blokiraju upis, instalaciju Active X kontrola kao i upis neke strane kao Home Page-a (Hijackers)...

Uklanjanje:

Ukoliko ste ipak zakacili neki spyware program njega lako mozete ukloniti nekim od sledecih alata:

1. **Ad-Aware Professional v6.0.181 Retail**

Povremeno izvrsite update baze : **http://www.lavasoft.de/update/refs/reflist.zip**
Potpuno automatizovano ce pronaci spyware programe i predloziti njihovo uklanjanje, pa je dobar za manje iskusne korisnike.

2. **CWShredder 1.54**
Ovim programom uklanjate razne programe koji vrse kradju Home Page-a i time dosadjuju stalnim otvaranjem u odredjenim vrem. intervalima.

3. **Spybot - Search & Destroy v.1.2**
Uklanjanje raznih vrsta spyware programa koji nisu pokriveni AntiVirusima
Ako dodje do pojave novog toolbara u IE, browser pocinje da se blokira, otvara strane koje niste uneli ... vreme je da startujete ovaj program jer je velika verovatnoca da ste zakacili neki spywere program koji radi u pozadini

4. **Spy Sweeper 2.61**
Slicno kao Ad-aware i Spybot, uklanja spyware, trojance, dialere ...
Radi i skeniranje i zastitu u realnom vremenu - monitor

5. **PestPatrol Corporate v4.4.0.0**
Detektuje i uklanja adware, spyware, key loggere, trojance, napade hakera
Osim toga, radi skaniranje sistema u realnom vremenu i stiti sistem

6. **SpywareBlaster 3.1**

Takodje jedan od alata koji vrse prevenciju instaliranja ActiveX kontrola, spyware programa, raznih dialera ... Program nije aktivan u memoriji i radi i sa Mozilla browserom

7. **HijackThis v1.97**
Program koji uklanja strane koje su se postavile kao Home Page bez vaseg znanja, dodatne toolbar programe ...

8. **Gip@MoveOnBoot 1.95**
Uklanja fajlove koji se ne mogu obrisati na uobicajen nacin jer su zakljucani od strane vindowsa

9. **CopyLock - Version 1.07**
Istu funkciju kao Gip@MoveOnBoot - brise fajlove koji se ne mogu obrisati komandom "delete" (razni trojanci, dialers ...)

10. **Proces Explorer 8.35**
Moze posluziti da pogledate koji su sve procesi startovani i eventualno prepoznate neki sumnjivi proces, ubijete ga (kill) a zatim obrisete program (virus, trojanac ...) koji ga je startovao.

NAPOMENA: cak i kada ne primecujete cudno ponasanje vaseg browsera potrebno je s vremena na vreme pustiti ove programe, kako bi bili sigurni da se nije zakacio neki od zlonamernih programa.

Virusi, worm, trojanci ...

Virusi su programi ili programski kodovi koji se ucitavaju bez vaseg znanja a pisani sa namerom da nanesu neku stetu racunaru. Lako se umnozavaju samostalnim kopiranje a kako su aktivni u memoriji zarazice svaki pokrenuti program. Brsianjem programa, blokiranje racunara ili kompletno formatiranje diska su neki od nacina delovanja virusa.

Wormovi su slicni virusima. Razlika je sto se ne dodaju programima kao virusi vec se repliciraju i postoje kao samostalni programi. Sire se automatski preko mreze sa racunara na racunar i imaju mogucnost da se salju samostalno putem mailova.

Trojanci su programi koji sluze kao back door za ulazak hakera na vas sistem bez vaseg znanja, kradju podataka ili unistenje sistema. Napadac se moze zakaciti na vas racunar, premnositi, brisati, dodavati programe i imati potpunu kontrolu nad vasim racunarom.

Ukoliko se vas sistem ponasa cudno u poslednje vreme (gasi se nasumice, blokira, otvara neke web strane bez vaseg znanja, usporeno radi...), moguce je da ste se zarazili nekim virusom.

I bez startovanja avnti virusa kucanjem komande "msconfig" (Start/run/msconfig) u startup tabu videcete koji se programi podizu sa podizanjem Windowsa. Ukoliko primetite nove stavke sa cudnim nazivima a u medjuvremenu niste instalirali nista od softvera velika je verovatnoca da ste se zarazili nekim od virusa.

Zastita

Zastita od virusa i wormova ukljucuje anti virus program sa najnovijim updateom av baze. Izaberite AV koji vama odgovara (Kasperski, Norton, PC Cillin, NOD32, F-Prot, Panda, McAfee, Sophos ...), redovno skenirajte sistem i vrsite update av baze.

PREVENTIVA I UKLANJANJE

1. **Anti-Virus Personal Pro v4.5.0.94**
Zastitice vas od vecine novih virusa, wormova ...

2. Nikako ne otvarajte tj. ne startujte fajlove koje ste skinuli sa interneta dobili od prijatelja ... a da predhodno niste proverili anti virusom.

3. Ne otvarajte mailove sa attachmentom koji sadrzi: .exe, .bat, .scr, .pif ili slicnu extenziju cak i ako stizu od vasih prijatelja. Novi wormovi generisu nasumice imena i salju mailove sa mailing liste vaseg prijatelja bez njegovog znanja.

4. Pozeljno bi bilo koriscenje mail klijenta koji ima mogucnost pregleda naslova poruka na serveru bez downloada na racunar i njihovim brisanjem direktno na serveru.
- **TheBat!**
ima ovu mogucnost.
- **Email Remover 3.0**
Takodje vrsi pregled mailova na serveru a vi odlucujete sta ce se preneti na vas racunar. Sve sumnivo pregledate kao tekst poruku i brisete direktno na serveru.
- U Outlook Expressu koristite opciju "Do not allow atachment ..." u Tools/Options/Security kako se zlonamerni skriptovi ne bi automatski startovali i iskljucite "Show Privew pane" u View/Layout opciji.

5. Ne ostavljajte prave podatke kod registracije i vas email kod provajdera
vec koristite web nail adrese kao sto je hotmail ili yahoo mail.
http://www.hotmail.com
http://www,mail.yahoo.com
jer time smanjujete mogucnost da primate razne spam poruke koje sadrze
i trojance, wormove ...

6. Antivirus monitor treba da uvek bude aktivan kako bi sistem bio zasticen.
AV nece dozvoliti startovanje programa zarazenog virusom ako je monitor
aktivan.

7. Update AV baze vrsite bar jednom nedeljno jer se novi virusi pojavljuju
svakodnevno i samo AV sa novim bazama moze uspesno zastititi vas sistem

8. Dok ste na internetu koristite neki firewall program (Zone Alarm, McAfee
Personal Firewall, Norton Internet Security ...) koji ce stititi vas sistem
od napada hakera i ostalih upada u sistem.

- **ZoneAlarm Pro with Web Filtering v4.5.538.001**
On vas takodje stiti i od wormova, trojanaca, i zlonamernih mailova

9. Ukoliko ste ipak zakacili neki virus (monitor nije bio aktivan) a AV ga je
kasnije detektovao, desava se da ga AV ne moze ukloniti ukoliko je novijeg
datuma. Preporuka je da potrazite "remover" bas za taj virus, worm ili
trojanac. Svi veci proizvodjaci AV softvera izbacuju samostalne programcice
za uklanjanje najnovijih vrsta virusa, wormova i trojanaca.
- **McAfee AVERT Stinger**
je besplatni, samostalni anti virus alat koji uklanja grupe od 30-ak
najnovijih vrsta virusa, trojanaca ...
Panda takodje ima **Panda Remover**

10. Neki virusi pronalaze sigurnosne rupe u windowsu i ubacuju se i nakon
ciscenja ukoliko nemate instalirane sigurnosne zakrpe za Windows (Hotfix).
Zato redovno posecujte sajt Microsofta posle pojave novih virusa i skinite
najnovije zakrpe: **http://www.microsoft.com/security/**
koje ispravljaju uocene nedostatke i sigurnosne rupe.
Instalirajte SP - service pack za Windows jer on ukljucuje sve sigurnosne
zakrpe koje su izasle u medjuvremenu.
http://support.microsoft.com/default.aspx?scid=kb;en-us;322389

11. Ukoliko je sistem vec zarazen desava se da anti virus nece moci da
ukloni virus iz Windowsa jer je virus vec zarazio anti virus program
ili je virus aktivan u memoriji pa ne dozvoljava start anti virusa ...
U ovom slucaju potrebno je:
- podici sistem sa boot cd-a koji sadrzi anti virus
Hirens boot CD, ERD Commander, Norton System Works ... su neki od
boot CD-ova koji mogu pomoci u uklanjanju virusa
- ukoliko nemate boot cd potrebno je vas hard disk skinuti, zakaciti na
drugi racunar koji nije zarazen i tamo ga ocistiti nekim anti virusom
i vratiti na racunar

12. Na kraju, moze se desiti da je virus tolkio ostetio sistem, zamenio
boot sektor tako da je jedina varijanta formatiranje diska i reinstalacija
sistema. Pre formatiranja koristite komandu
FDISK /MBR
kako bi uklonili virus iz boot sektora racunara.