HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Malware programi

CCERT-PUBDOC-2005-02-107

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Malware programi predstavljaju široku grupu malicioznih programa s kojima se korisnici Interneta, pogotovo u posljednje vrijeme, sve češće susreću. Nakon virusa, crva, trojanskih konja i drugih sličnih programa, korisnici sada moraju voditi računa i o tzv. *spyware*, *adaware*, *dialer* programima koji ozbiljno mogu ugroziti sigurnost osobnog računala.

Prilikom pretraživanja Interneta, dohvaćanja besplatnih programa i njihove instalacije na računalo, postoji ozbiljan rizik od zaraze nekim od navedenih tipova programa. Ovisno o tipu aktivnosti koje provode na korisničkom računalu, *malware* programi mogu se podijeliti u nekoliko različitih skupina. Od neopasnih, ali dosadnih *pop-up* prozora oglašivača, zatim različitih programa koji prate aktivnosti korisnika na računalu te ih šalju na predefinirane maliciozne adrese, pa sve do iznimno opasnih *dialer* programa koji troše telefonske impulse pozivanjem brojeva u inozemstvu.

U ovom dokumentu opisane su općenite karakteristike i tipovi *malware* programa te tipični simptomi koji korisnika mogu uputiti da je njegovo računalo zaraženo nekim od takvih programa. Opisani su najčešći tipovi *malware* programa te su prikazane razne tehnike njihova prepoznavanja i uklanjanja. U dokumentu su također opisane i neke preventivne metode kojima korisnici mogu zaštititi svoje računalo i osobne podatke te *autostart* metoda ovih programa koja je prvenstveno namijenjena naprednim korisnicima i administratorima sustava. Konačno, u dokumentu je dana referentna lista korisnih programskih alata koji se mogu iskoristiti za zaštitu od *malware* programa.

2. Općenito o malware programima

Kako je u uvodu rečeno, pojam *malware* programa opisuje široku grupu programa čija osnovna namjena je maliciozno, odnosno zlonamjerno djelovanje, prikriveno od korisnika. Benigni *malware* programi najčešće su tzv. *spyware* programi kojima je cilj da od korisnika, na čijem računalu su instalirani, prikupe razne podatke te da ih pošalju na ciljana mjesta na Internetu. Za korisnika, ti programi nemaju nikakvu korist, a šteta koju mogu prouzrokovati je različita. Takvi programi uglavnom informiraju oglašivače o području interesa i navikama korisnika, kako bi ih se na taj način privuklo na kupovinu određenog proizvoda ili usluge. Način na koji *spyware* programi dolaze do informacija jest da pregledavaju datoteke o već posjećenim Internet stranicama (engl. *History*), stranice koje je korisnik stavio u popis najdražih stranica (engl. *Favorites*), mape s privremenim Internet datotekama (engl. *Temporary Internet Files*), te kolačiće (engl. *Cookies*). Svi navedeni podaci otkrivaju navike i sklonosti korisnika računala tijekom korištenja Interneta.

Benigni *spyware* programi vrlo često se distribuiraju i instaliraju uz druge, uglavnom besplatne i legitimne programe, a njihova prisutnost obično je vidljiva prikazivanjem različitih oglasa, promjenom početnih stranica unutar Web preglednika, itd. Deinstalacija ove vrste programa obično je jednostavna, no posljedica može biti da programi uz koje su instalirani izgube svoju funkcionalnost.

Prvi *malware* programi uglavnom su se instalirali upravo uz besplatne ili demo aplikacije, no u današnje vrijeme autori *malware* programa za njihovu instalaciju koriste i druge metode kao što su npr. iskorištavanje ranjivosti u operacijskim sustavima i programskim paketima (najčešće Web preglednicima).

Osim opisanih benignih *malware* programa postoje i oni drugi, maligni koji mogu biti vrlo opasni i koji mogu nanijeti velike štete korisnicima. Najopasnijom vrstom *malware* programa smatraju se *dialer* programi. Oni su uglavnom instaliraju na računalo prilikom posjeta korisnika pornografskim Web stranicama, a osnovna namjena im je da, umjesto biranja telefonskog broja legitimnog pružatelja Internet usluge (npr. T-com, Vipnet, Iskon, itd.), biraju međunarodne brojeve s posebnim i vrlo visokim tarifama. Na taj način autori takvih programa ostvaruju profit, a oštećeni korisnici se mogu suočiti s astronomskim iznosima telefonskih računa.

Način instalacije takvih programa može biti različit. Ponekad se ti programi instaliraju čak i uz interakciju neupućenih korisnika prilikom posjeta određenim Web stranicama koje korisniku otvaraju dijaloški okvir u kojem potvrđuje (pritiskom na dugme *Yes*) ili opovrgava (pritiskom na dugme *No*) instalaciju. Maligni *malware* programi mogu se instalirali i bez korisnikova znanja, ovisno o samom programskom kodu. Njih je teško prepoznati, ali i ukloniti upravo zbog njihova načina instaliranja i tehnika prikrivanja koje koriste.

U konačnici, takvi programi budu instalirani uglavnom kao dodaci (engl. *plug-in*) Web preglednika ili kao BHO objekti (engl. *Browser Helper Object*) koji su vezani isključivo uz Windows operacijske sustave i Internet Explorer wweb preglednik. Detaljniji opis BHO objekata dan je u dokumentu na referentnoj adresi http://www.cert.hr/filehandler.php?did=110.

3. Prepoznavanje i uklanjanje *malware* programa

Kao što je već ranije spomenuto, kompleksnost detekcije i uklanjanja *malware* programa ovisi o njihovom tipu i složenosti. U nastavku dokumenta opisane su neke od metoda prepoznavanja te uklanjanja ovih programa. Metode prepoznavanja programa korištenjem specijaliziranih programskih alata preporučljiva je za manje iskusne korisnike, dok su ostale metode namijenjene naprednim korisnicima i administratorima sustava.

3.1. Sumnja na prisutnost programa

Uobičajeni simptomi računala za koje se sumnja da je zaraženo *malware* programima jesu slijedeći:

- rad računala vidljivo je usporen,
- prilikom pretraživanja Interneta samostalno se otvaraju prozori pornografskog ili drugih neželjenih sadržaja,
- računalo se automatski spaja na pornografske stranice korištenjem nepoznatih telefonskih brojeva,
- pretraživanje Interneta po određenom pojmu biva izvedeno od nekog drugog pretraživača (npr. *CoolWebSearch*), a ne korisničkog (npr. *Google*),
- u listu najdražih Web stranica (engl. *Favorites*) dodane su Web stranice bez korisnikova znanja,
- početna stranica (engl. *home page*) je promijenjena i svako nastojanje korisnika da vrati svoje postavke završava je neuspješno,
- otvaraju se oglašivački prozori prilikom rada na računalu, čak kada ono i nije spojeno na Internet.

Osim uočavanja navedenih simptoma, sigurna metoda prepoznavanja *malware* programa je korištenje specijaliziranih programskih alata.

3.2. Prepoznavanje korištenjem specijaliziranih programskih alata

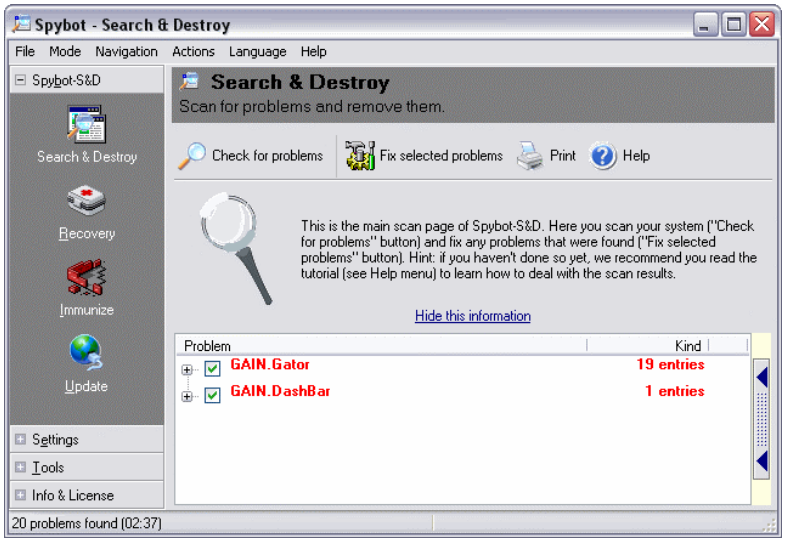
Postoji priličan broj specijaliziranih programskih alata čija je primarna funkcija prepoznavanje i uklanjanje *malware* programa s računala. Za korisnike je pozitivna činjenica da su najbolji takvi programski alati besplatni za osobnu uporabu. Korisnik ih može dohvatiti na Internetu, instalirati i pokrenuti na svom računalu.

Najpoznatiji takvi alati su *Spybot Search & Destroy* (*Spybot S&D*) koji se može dohvatiti s referentne adrese http://www.safer-networking.org i *Ad-aware* koji se može pronaći na adresi http://www.lavasoftusa.com/software/adaware/. Navedene alate također je moguće dohvatiti i sa Web stranica CARNet CERT-a (http://www.cert.hr) u kategoriji "Čistaći neželjenih programa".

3.2.1. Spybot Search & Destroy

Programski alat *Spybot Seacrh & Destroy* već je duže vrijeme na tržištu i smatra se da drži prvo mjesto među aplikacijama te namjene. Stalnim poboljšanjima program omogućava sve bolju zaštitu osobnih računala u smislu prepoznavanja i uklanjanja *spyware*, *adware*, *dialer* i drugih sličnih malicioznih programa. Nakon jednostavnog postupka instalacije te osvježavanja identifikacijske datoteke, program je spreman za rad. Podržana su dva načina rada programa, *Easy mode* i *Advanced mode*, koji se međusobno razlikuju prema funkcionalnostima koje su korisniku stavljene na raspolaganje.

Slika 1 prikazuje rezultat pretraživanja zaraženog računala korištenjem *Spybot Search & Destroy* programskog alata.

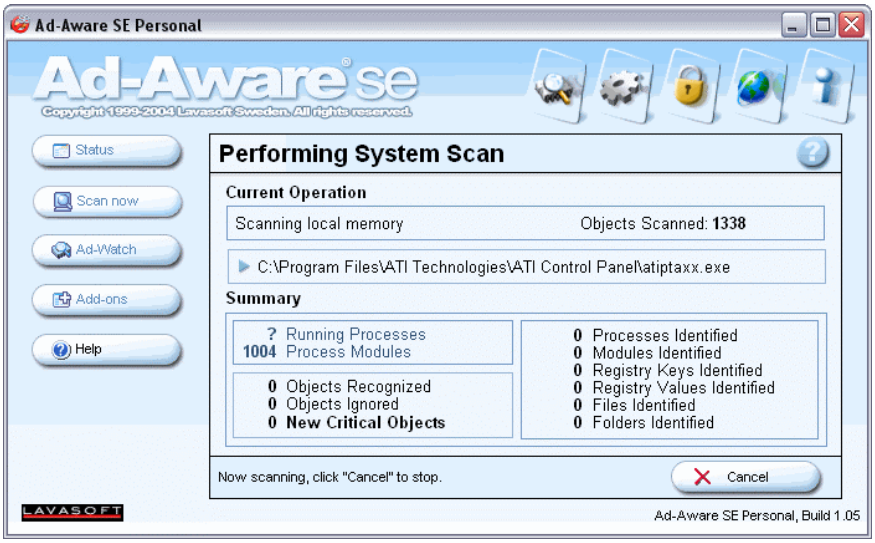


Slika 1: Rezultat pretraživanja alata Spybot Search & Destroy

3.2.2. Ad-aware

Programski alat *Ad-aware* omogućuje pregledavanje radne memorije sustava, *registry* zapisa i datoteka na tvrdom disku u potrazi za neželjenim malicioznim programima. Pregledavanje sustava ovim alatom izuzetno je jednostavno i intuitivno, a nakon obavljenog pregledavanja računala od korisnika se zahtijeva da analizira dobivene rezultate te da pristupi uklanjanju malicioznih komponenti. Mogućnost lažnih upozorenja kod ovog programa vrlo je mala pa je u većini slučajeva moguće ukloniti sve komponente koje program prepozna.

Slika 2 prikazuje sučelje *Ad-aware* programskog alata tijekom trajanja procesa pregledavanja računala.



Slika 2: Pretraživanje računala alatom Ad-aware

3.3. Prepoznavanje *malware* procesa

Administratori u mrežnim okruženjima često imaju tešku zadaću prepoznavanja *malware* procesa na računalima za koje postoji sumnja da su zaraženi nekim *malware* programom.

Za prepoznavanje *malware* procesa važno je korištenje alata za nadgledanje procesa jer se time povećava mogućnost pravilnog prepoznavanja i poduzimanja odgovarajućih akcija. Obzirom da starije inačice Windows (Windows 9x) operacijskih sustava nemaju mogućnost nadgledanja procesa,

preporučljivo je koristiti alate treće strane koji na Windows operacijskim sustavima dobro obavljaju svoju funkciju.

3.3.1. Biblioteka procesa

Jedan od alata za nadgledanje procesa je komercijalni *Wintasks Pro*. Na referentnoj Web adresi http://www.liutilities.com/products/wintaskspro/processlibrary/ prikazana je *WinTasks* biblioteka procesa koju čini popis procesa, podijeljenih na kategorije, te njihova namjena. U ovoj biblioteci može se provjeriti da li je proces koji je prepoznat kao aktivan na računalu *spyware*, trojanski konj ili legitiman proces.

Kategorije u koje su podijeljeni procesi su:

- procesi koji predstavljaju potencijalni sigurnosni rizik (engl. *security risks*),
- sistemski procesi (engl. *system processes*), te
- aplikacije (engl. *applications*).

Slika 3 prikazuje dio liste procesa sigurnosnog rizika.

Top Security Risks		
180ax.exe	a.exe	actalert.exe
adaware.exe	Alchem.exe	alevir.exe
aqadcup.exe	arr.exe	ARUpdate.exe
asm.exe	av.exe	avserve.exe
avserve2.exe	backWeb.exe	bargains.exe
basfipm.exe	belt.exe	Biprep.exe
blss.exe	bokja.exe	bootconf.exe
bpc.exe	brasil.exe	BRIDGE.DLL
Buddy.exe	BUGSFIX.EXE	bundle.exe
bvt.exe	cashback.exe	cdaEngine
cmd32.exe	cmesys.exe	conime.exe
conscorr.exe	crss.exe	cxtpls.exe
datemanager.exe	dcomx.exe	directs.exe
divx.exe	dllreg.exe	dmserver.exe
dpi.exe	dssagent.exe	dvdkeyauth.exe

Slika 3: Popis procesa sigurnosnog rizika

Pritiskom na određeni proces o kojem se želi saznati više informacija otvara se stranica s relevantnim informacijama (Slika 4).

bargains - bargains.exe - Process Information

Process File: bargains or bargains.exe
Process Name: Bargains Spyware

Description:
bargains.exe is a spyware which generates pop-up advertisements and analyses your computer usage for analysis by Exact Advertising. This program is a registered security risk and should be removed immediately. Please see additional details regarding this process

Slika 4: Opis odabranog procesa

Prikazani podaci korisnika upućuju na točan naziv procesa te opis njegovog "ponašanja". Dodatne informacije čine podaci:

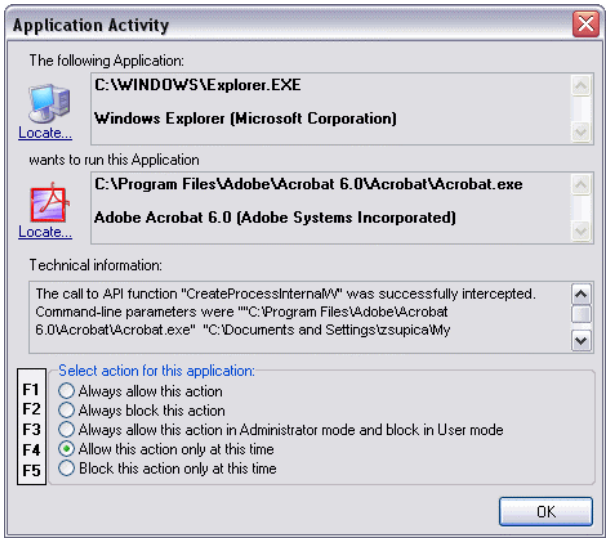
- o autoru procesa (*author*),
- o aplikaciji kojoj proces pripada (*part of*),
- da li je sistemski proces (*system process*),
- da li je pozadinski proces (*background process*),
- da li koristi računalu mrežu (*uses network*),
- da li ima povezanosti s hardverom (*hardware related*),
- koje su uobičajene pogreške (*common errors*),
- koliki je sigurnosni rizik procesa (*security risk*),
- da li je virus,
- da li je *spyware*, te
- da li je trojanski konj (*trojan*).

Prema ovom opisu procesa korisnik, odnosno administrator može izvesti odgovarajuću akciju, a da pri tome ne ugrozi rad računala. Problem nastaje ukoliko se računalo zarazi malicioznim programom koji se ubacuje u neki od legitimnih aktivnih procesa. Detekcija i uklanjanje takvih programa je vrla teška, ali ne i nemoguća,. Više o samom načinu ubacivanja malicioznog koda u aktivan proces može se pronaći na referentnoj adresi http://www.cert.hr/filehandler.php?did=180.

3.3.2. System Safety Monitor

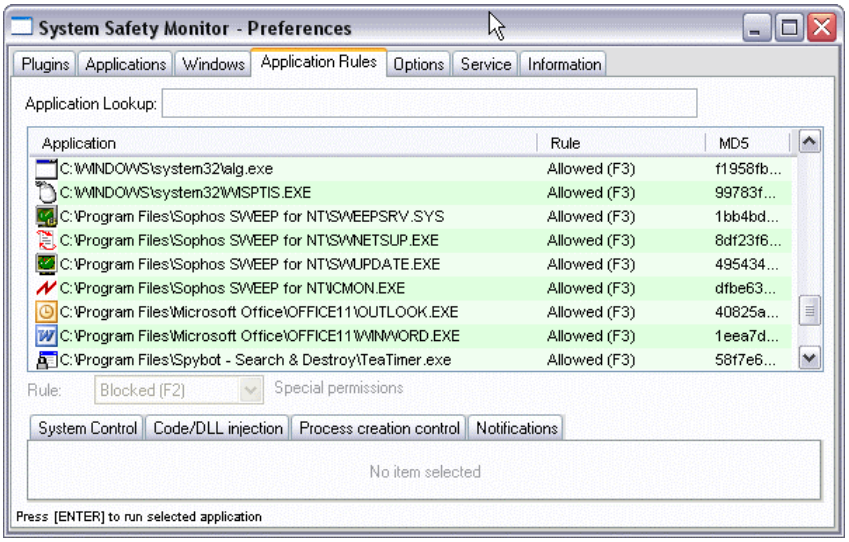
Kako bi se spriječio prethodno spomenuti način instalacije malicioznih programa ubacivanjem u legitiman aktivan proces, može se koristiti *System Safety Monitor* programski alat koji je besplatan, a funkcija mu je kontrolirati programe i procese koji su aktivni na računalu. Program se može dohvatiti s adrese http://maxcomputing.narod.ru/ssme.html?lang=en.

Prilikom pokretanja svakog programa na računalu ovaj alat prijavit će ukoliko je program modificiran. Naravno, ovisno o podešavanju alata, obavljat će se i ostale aktivnosti kao što je prijava baš svakog pokretanja programa. Na slici 5 prikazan je dijaloški okvir koji prijavljuje otvaranje jednog od programa na korisničkom osobnom računalu.



Slika 5: Dijaloški okvir koji prijavljuje otvaranje programa

Unutar okvira korisnik bira akciju koju želi poduzeti.
Slika 6 prikazuje popis zadnje odabranih pravila za pristup aplikacijama.



Slika 6: Aplikacijska pravila

4. Prepoznavanje *malware auto-start* metoda

Prilikom uklanjanja *malware* programa s računala, jedan od glavnih koraka jest prepoznavanje i uklanjanje *auto-start* metode *malware* programa. Ovaj korak onemogućuje ponovno izvršavanje malicioznog programa nakon ponovnog pokretanja operacijskog sustava.
Auto-start metode koje najčešće koriste *spyware* programi su:

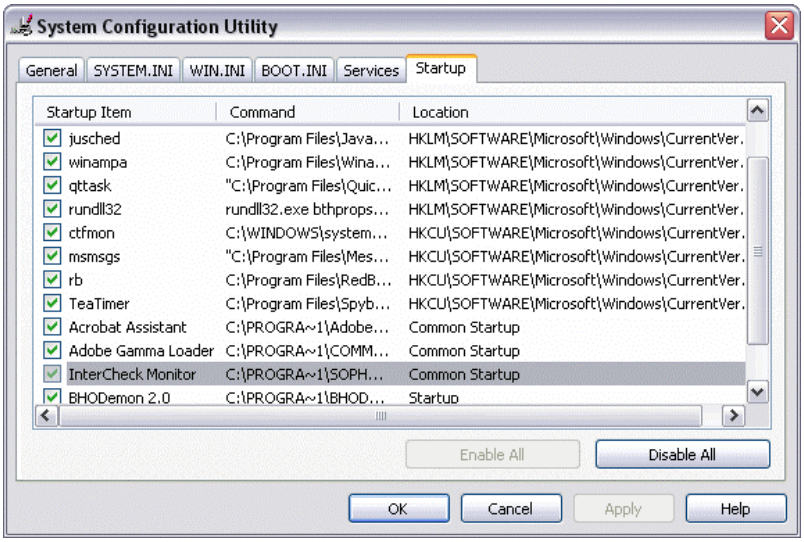
- mapa `Autostart`,
- datoteka `Win.ini`,
- datoteka `System.ini`,
- *registry*.

4.1. Mapa `Autostart`

Mapa `Autostart` sadrži popis svih programa tj. dijelova programa koji se automatski pokreću prilikom svakog ponovnog pokretanja operacijskog sustava. Problem kod automatskog pokretanja programa jest što su neki od njih vidljivi na traci sa zadacima (*system tray*), no neki su potpuno skriveni pa ih je vrlo teško uočiti.
Windows operacijski sustavi inačice XP sadrže alat *System Configuration Tool* (*Msconfig.exe*) koji, između ostalog, služi za upravljanje *autostart* procesima.
Za pokretanje tog alata potrebno je učiniti slijedeće:

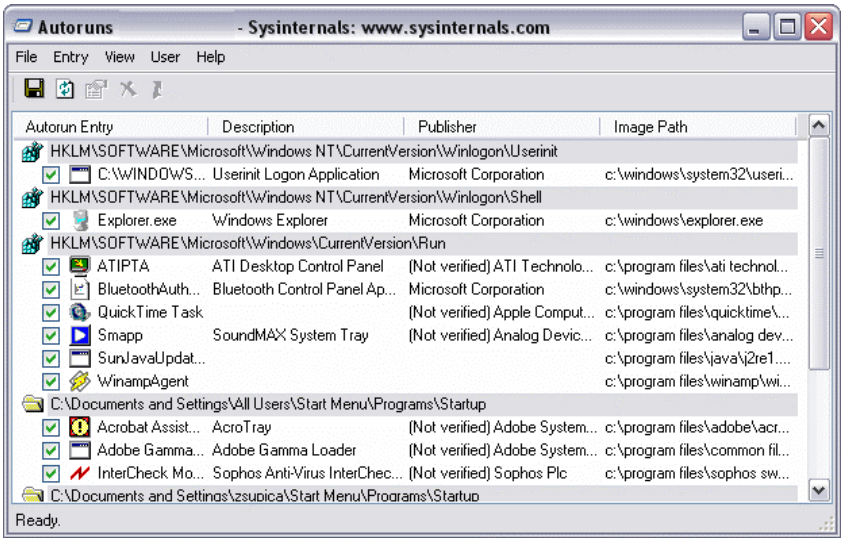
1. kliknuti `Start`, `Run`
2. upisati `msconfig`,
3. kliknuti `OK`.

Otvara se dijaloški okvir prikazan na slici 7.



Slika 7: MSconfig dijaloški okvir

`Startup` kartica sadrži popis svih programa i procesa koji se automatski pokreću prilikom svakog novog pokretanja Windows operacijskog sustava. Uključivanje, odnosno isključivanje programa i procesa obavlja se kliktanjem na oznaku kvačice. Kvačica označava programe i procese koji se pokreću, a prazan okvir znači da se odabrani program odnosno proces neće automatski pokretati.
Nakon promjena, potrebno je kliknuti na dugme `OK` i ponovno pokrenuti operacijski sustav kako bi se promjene primijenile.
Drugi način da se pregleda ova mapa je uporaba besplatnog alata *Autoruns* tvrtke *Sysinternals*. Alat se može dohvatiti na adresi http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml i funkcionira na svim inačicama Windows operacijskih sustava. Na slici 8 prikazano je sučelje alata.



Slika 8: Sučelje alata Autoruns

Ovaj alat prikazuje sve programe koji se automatski pokreću svakim novim pokretanjem operacijskog sustava, a pomoću njega moguće je jednostavno brisati i mijenjati postavke programa. Velika prednost alata jest ta što omogućuje da se, prije brisanja programa, pogledaju postavke kako bi se dobile opširnije informacije o tome što odabrani program znači i čemu služi.

4.2. `Win.ini` datoteka

`Win.ini` datoteka je sistemska datoteka koja sadrži popis programa koji su se u još u inačici 3.x Windows operacijskih sustava automatski pokretali pri ponovnom pokretanju operacijskog sustava.
`Load` kategorija unutar `win.ini` datoteke sadrži popis programa koji se automatski pokreću prije nego li se korisnik prijavi za rad u sustavu. Kategorija `Run` sadrži popis programa koji se automatski pokreću nakon što se korisnik prijavi za rad u sustav. Inačice 9x/ME/NT/2000/XP/2003 sadrže ovu datoteku, no ona nije jednake važnosti za sve inačice.
Korisnici inačica 9x/ME/NT unutar `win.ini` datoteke imat će slijedeći zapis (u slučaju postojanja *Adware.Replace* malicioznog programa):

```
[windows]
run=%system%\Services\Services.exe
load=%system%\Services\Services.exe
```

i u njima je potrebno prepoznati i ukloniti *spyware* programe. Postupak uklanja izvodi se tako da se izbriše sve, osim `"run="` i `"load="` te se pohrane promjene u datoteci. Datoteka se može pregledati i izmijeniti pomoću tekst editora, ali i pomoću već spomenutog alata *Msconfig*.
Windows NT i noviji NT bazirani sustavi (2000, XP, 2003) koriste *Registry* ključ za automatsko pokretanje programa:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Prepoznavanje i uklanjanje *malware* programa iz *Registry* datoteke biti će opisano u nastavku.

4.3. `System.ini` datoteka

`System.ini` datoteka je konfiguracijska datoteka koja opisuje trenutno stanje računalnog sustava. Sadrži popis objekata koji su spremni za rad prilikom ponovnog pokretanja operacijskog sustava. Informacije u ovoj datoteci mijenjaju se prilikom svake promjene postavke računala.
Ovo je (kao i `win.ini`) datoteka koja je kreirana i korištena još u prvim inačicama Windows operacijskog sustava (3.x), a koristi još i kod Windows 9x i NT inačica.
Primjer zapisa u `system.ini` datoteci:

```
[boot]
Shell=Explorer.exe malware.exe
```

Postupak uklanjanja izvodi se, kao i u prethodnom slučaju, tako da se izbriše sve, osim `"Shell=Explorer.exe"` zapisa. Datoteka se također može pregledati i izmijeniti pomoću tekst editora, ali i pomoću ranije opisanog alata *Msconfig*.

4.4. Registry

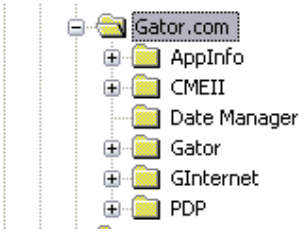
Prepoznavanje i uklanjanje *malware* programa iz *Registry* datoteke nije sasvim jednostavno, jer se oni ugnijezde i u skrivene ili neupadljive mape i ključeve unutar *Registry* datoteke.
Ključevi koje *malware* programi, mogu koristiti za *autostart* su sljedeći:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServ
ices
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServ
icesOnce
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunService
s
```

Primjer prepoznavanja *autostart* metode ove vrste programa prikazat će se na primjeru računala koje je zaraženo *Adware.Gator* programom.
Po instalaciji programa koja mora biti ručna tj. instalacijom nekog drugog besplatnog programa, u *Registry* se smješta ključ:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Gator.com
```

koji sadrži još nekoliko podključeva, a prikazani su na slici 9.

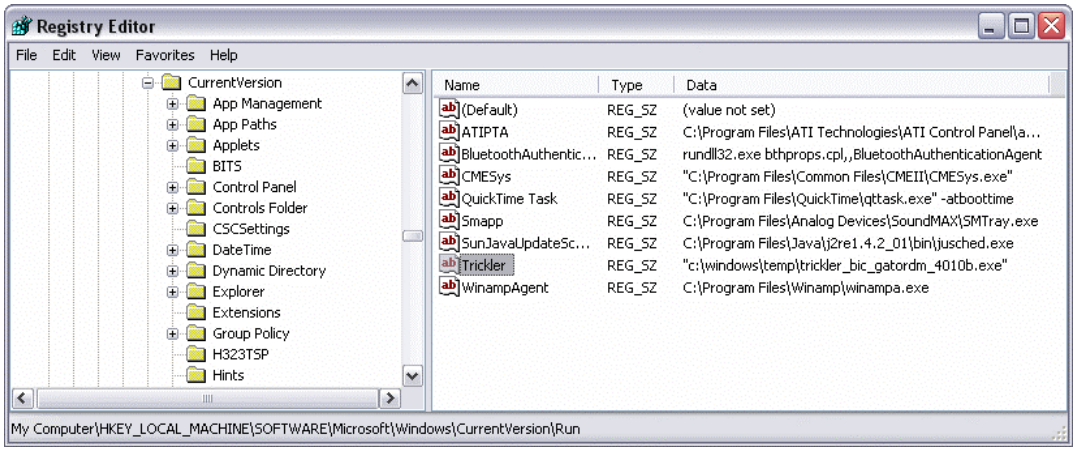


Slika 9: Registry ključevi programa Gator

Nadalje, smještena je vrijednost `Trickler` u ključ:

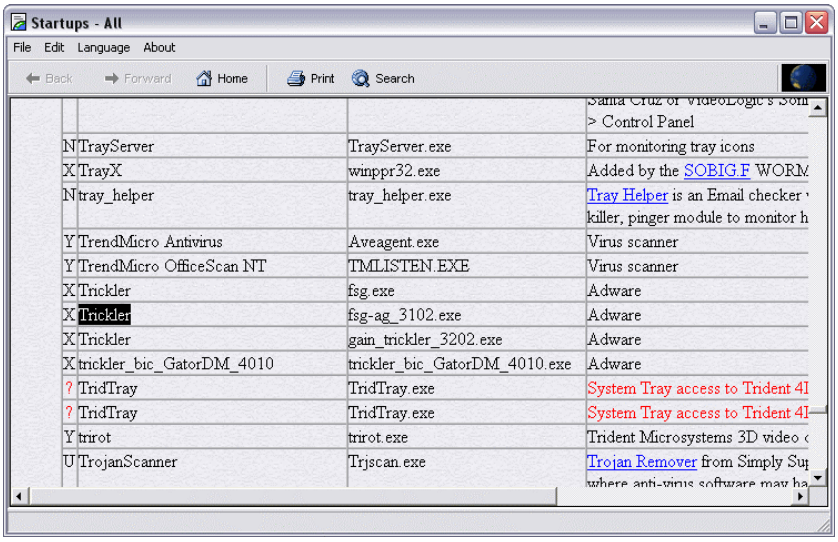
```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

koji je prikazan na slici 10.



Slika 10: Trickler vrijednost ključa

Ukoliko korisnik nije siguran što pojedina vrijednost ključa znači te ne može razlikovati legitimnu od nelegitimne vrijednosti, preporučljivo je korištenje alata *Start_ups* koji se može pronaći na adresi http://www.pacs-portal.co.uk/startup_pages/start_ups.exe, a koji sadrži popis sumnjivih *spyware* vrijednosti ključeva. Slika 11 prikazuje sučelje alata.



Slika 11: Start_ups alat

Također, prije opisana biblioteka procesa također pomaže detaljnim opisom sumnjivih programa. Na korisniku je da odabere koja je od dviju spomenutih mogućnosti njemu jednostavnija za uporabu.

5. Prevencija

5.1. Web preglednici

Prevencija je ipak najbolja moguća mjera zaštite od *malware* programa. Jedna od čestih preporuka jest korištenje alternativnih Web preglednika umjesto *Microsoft Internet Explorera*. Jedan od besplatnih i vrlo jednostavnih, a funkcionalnih je *Mozilla Firefox* koji se može dohvatiti s referentne adrese http://www.mozilla.org/products/firefox/. Na taj način smanjit će se mogućnost zaraze računala putem sigurnosnih propusta u IE aplikaciji.

Također je preporučljivo i blokiranje izvođenja *ActiveX* kontrola i *Java* skripti s nesigurnih izvora, čime se dodatno može podići razina sigurnosti računala. Također, redovita instalacija sigurnosnih zakrpi jedan je od bitnih elemenata prevencije.

Osim navedenoga, korisnicima se savjetuje da izbjegavaju besplatne Web stranice pornografskog sadržaja kako bi izbjegli inficiranje, ranije spomenutim *dialer* programima. Nepoželjne stranicu su i one na kojim se mogu dohvatiti *warez* programi i *crack* ključevi za različite aplikacije.Manje opasne, ali ipak koriste benigni *spyware* su i *mp3* stranice te *P2P* programi koji omogućuju razmjenu datoteka.

5.2. CARNet CERT

CARNet CERT izdao je u siječnju 2005. godine priručnik i CD za računalnu sigurnost korisnika Interneta popularno nazvan "Borbeni komplet". Priručnik na jednostavan i razumljiv način opisuje opasnosti koje nosi Internet. Osim *spyware* programa obuhvaćeni su i ostali maliciozni programi.

Priručnik je besplatan i može se pročitati na web stranici http://www.cert.hr/htmltext.php?id=100&lang=hr, dohvatiti u .pdf formatu s referentne adrese http://www.cert.hr/filehandler.php?id=pri ili se može naručiti tiskana inačica priručnika popunjavanjem forme na adresi http://www.cert.hr/naruci_brosuru.php.

5.3. Uporaba `hosts` datoteke

Za napredne korisnike i administratore postoji još jedan način prevencije od *malware* programa, a to je korištenje `hosts` datoteke. `Hosts` datoteka inače služi mapiranju imena računala u IP adrese, a jednostavnim trikom moguće ju je iskoristiti za blokiranje pristupa poznatim *malware* poslužiteljima.

Uporabom bilo kojeg tekst editora `hosts` datoteku moguće je urediti tako da se imena *malware* poslužitelja mapiraju u nepostojeće IP adrese:

```
127.0.0.1       Localhost
127.0.0.2       iads.adroar.com
127.0.0.3       lists.adroar.com
127.0.0.4       advertisingvision.com
127.0.0.5       ……
```

`Hosts` datoteka se na različitim inačicama Windows operacijskih sustava nalazi u različitim mapama:

```
Windows XP
     C:\Windows\system32\drivers\etc
Windows 2000
     C:\Winnt\system32\drivers\etc
Windows 98/ME
     C:\Windows
```

Izgled i sadržaj predefinirane `hosts` datoteke prikazan je na slici 12.

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```

Slika 12: Predefinirana datoteka `hosts`

Ova datoteka se proširuje popisom nepoželjnih poslužitelja, no `localhost` zapis u datoteci se ne smije brisati ili mijenjati. Također, prilikom uređivanja `hosts` datoteke potrebno je paziti da se datoteka ne pohrani s ekstenzijom `.txt` ili bilo kojom drugom. Na adresi http://www.mvps.org/winhelp2002/hosts.txt moguće je vidjeti opširan popis malicioznih poslužitelja koji se mogu uključiti u korisnički popis.
Pristup poznatim *malware* poslužiteljima u korporativnom okruženju moguće je ograničiti i pravilima na vatrozidu ili korištenjem nekog od *content-filtering* paketa.

6. Zaključak

Obzirom da je tema *malware* programa vrlo aktualna, u ovom dokumentu dane su informacije koje će svakom korisniku pomoći u borbi s takvom vrstom zlonamjernih programa. Ovisno o stupnju svoga znanja, korisnici mogu kombinirati sva predložena rješenja i preporuke za prepoznavanje i uklanjanje malicioznih programa sa svojih računala.

7. Reference

[1] Read, J.: Sypware Explained, http://www.anti-trojan.com/
[2] Spybot Search & Destroy, http://www.safer-networking.org
[3] Ad-aware, http://www.lavasoftusa.com/software/adaware/
[4] Wintasks Process Library, http://www.liutilities.com/products/wintaskspro/processlibrary/
[5] CARNet CERT, http://www.cert.hr
[6] System Safety Monitor, http://maxcomputing.narod.ru/ssme.html?lang=en
[7] Symantec Security Responce,
[8] Start_ups, http://www.pacs-portal.co.uk/startup_pages/start_ups.exe
[9] Mozilla Firefox, http://www.mozilla.org/products/firefox/
http://securityresponse.symantec.com/avcenter/venc/data/adware.gator.html

[10] MVPS Hosts, http://www.mvps.org/winhelp2002/hosts.txt