HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Microsoft Windows Malicious Software Removal Tool

CCERT-PUBDOC-2005-05-122

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

Virusi, crvi, trojanski konji i drugi maliciozni programi danas su česta prijetnja za sve korisnike računala, od krajnjih korisnika do velikih kompanija. Također, i rezultirajući sigurnosni rizik, odnosno potencijalna šteta može varirati od malih ili nikakvih posljedica sve do nasilnog prekidanja rada sustava ili trajnog gubitka podataka. Većina malicioznih programa ne može se širiti ukoliko ih korisnik sam ne pokrene, osim crva koji se, nakon infekcije, mogu širiti i bez djelovanja korisnika. Najčešće se distribuiraju kao privitci u porukama elektroničke pošte, iako ih je moguće pokupiti neopreznim pregledavanjem Internet stranica ili neopreznim dohvaćanjem raznih datoteka, posebno preko P2P mreža. Simptomi infekcije su usporavanje rada računala, smanjenje mrežne propusnosti, automatsko pokretanje nepoznatih aplikacija i sl. Zbog toga je potrebno redovito nadograđivati antivirusne programe kako bi mogli prepoznati i najnovije maliciozne programe, te je potrebno usvojiti i pridržavati se sigurnosnih pravila i procedura kojima se rizik od infekcije malicioznim programima može umanjiti.

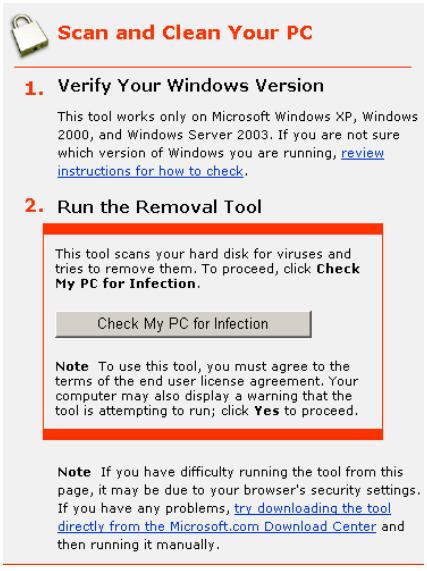
Postoje mnogi alati, uglavnom antivirusni, koji korisnika štite od aktiviranja poznatih malicioznih programa, te omogućuju odstranjivanje već pokrenutih. Microsoft je u prvom mjesecu 2005 godine izdao novi alat naziva *Microsoft Windows Malicious Software Removal Tool* (u daljnjem tekstu MSRT) koji služi za identifikaciju i uklanjanje najzastupljenijih malicioznih programa na MS Windows 2000/XP/2003 platformama. U dokumentu su opisana svojstva tog alata, te su dane upute o dohvaćanju i pokretanju u različitim okruženjima i na različiti MS sustavima.

2. Instalacija

MSRT alat ne instalira se na uobičajeni način: ne nadograđuje datoteke na računalu, ne stvara posebne mape u i izborniku niti je vidljiv kroz *Add/Remova Programs*. Datoteka je dostupna u obliku samo-otvarajuće izvršne CAB arhive pod imenom `Windows-KB890830-Vx.x.ENU.exe`, veličine 474 KB. Arhiva sadrži datoteke `Mrt.exe` i `mrtstub.exe`, a moguće ju je dohvatiti na više načina:

- Putem *Windows Update* (ili *Automatic Updates*) servisa omogućeno je dohvaćanje MSRT-a sa adrese http://www.windowsupdate.com. Alat je ponuđen kao jedna od sigurnosnih zakrpa.
- Putem *Microsoft Download Center*-a moguće je dohvatiti MSRT sa stranice http://go.microsoft.com/fwlink/?linkid=40587 .

Također, na stranici http://www.microsoft.com/malwareremove moguće je pokrenuti *online* inačicu MSRT-a (Slika 1).



Slika 1: Pokretanje online inačice MSRT-a

Trenutna inačica alata je 1.4, a nove inačice alata biti će dostupne svakog drugog utorka u mjesecu, osim ako se ne pokaže potreba za prijevremenim objavljivanjem u slučaju novih opasnosti.
Važno je napomenuti da korisnici Windows 2000 platforme ne mogu koristiti *Windows Update* i *Automatic Updates* za dohvaćanje alata, što će biti omogućeno tek u novijim inačicama alata.

2.1. Korporativno okruženje

MSRT je primarno namijenjen klijentskim računalima, ali ga je moguće koristiti i u korporativnom okruženju kao nadopunu za postojeće antivirusne programe. Za korištenje MSRT-a u korporativnom okruženju na raspolaganju su sljedeće metode:

- *Windows Server Update* servis (omogućeno od sljedeće inačice),
- *SMS Software Package,*
- *Group Policy* bazirana *computer startup* skripta,
- *Group Policy* bazirana *user logon* skripta.

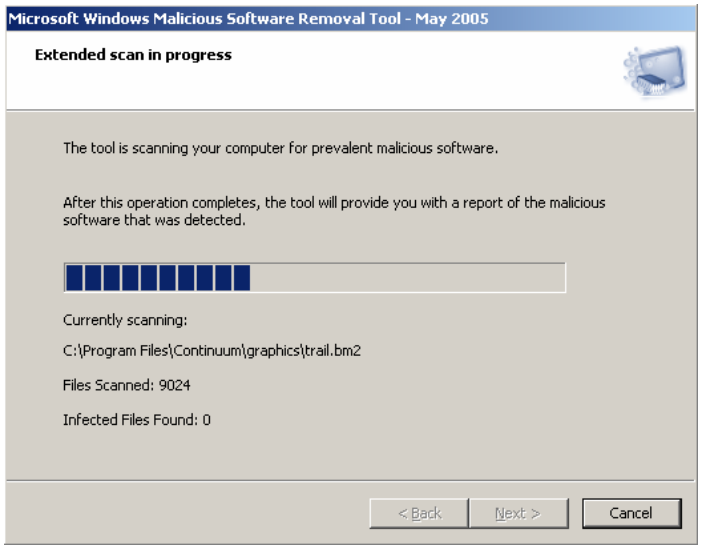
U ovom trenutku nije moguće dohvaćanje MSRT-a korištenjem *Windows Update Cataloga*, *Software Update Services (SUS)* servisa, niti pokretanje MSRT-a na udaljenom računalu

3. Pokretanje

Pri prvom dohvaćanju i pokretanju MSRT-a potrebno je prihvatiti uvjete licenčnog ugovora (engl. *End User Licence Agreement*, *EULA*). Pokretanje MSRT-a na računalu je moguće jedino ako je korisnik član administratorske grupe. Ako ti uvjeti nisu ispunjeni pokretanje alata neće biti moguće.
Dohvaćanjem MSRT-a preko *Windows Update* ili *Automatic Updates* alat se automatski pokreće u pozadini (engl.*quiet mode*), korisniku se naknadno samo dojavljuju poruke o mogućoj zarazi računala.
Ako se MSRT želi pokretati iz komandne linije ili s grafičkim sučeljem potrebno ga je dohvati preko *Microsoft Download Center*-a ili pokrenuti *online* verziju MSRT-a.
Prije pokretanja MSRT-a preporučuje se napraviti sigurnosnu kopiju podataka (engl. *backup*) na računalu.
MSRT je moguće pokrenuti iz komandne linije koristeći slijedeće parametre komandne linije (engl. *command-line switch)*:

- /Q ili /quiet – alat se pokreće u pozadini, bez korisničkog sučelja,
- /? – prikazuje dijaloški okvir sa listom parametara komandne linije,
- /N – alat se pokreće u *detect* načinu rada, maliciozni programi biti će prijavljeni, ali neće biti obrisani,
- /F – pokreće *extended* tip skeniranja računala.

Nakon prihvaćanja licenčnog ugovora alat se pokreće, te skenira memoriju računala za aktivnim malicioznim programima.
Ako je identificiran neki od malicioznih programa zaustavlja se njegov proces, te se brišu datoteke i *Registry* ključevi povezani s detektiranim programom. U slučaju da je maliciozni program promijenio korisnikovu početnu stranicu (engl. *homepage*) MSRT upozorava korisnika na tu promjenu, te ga upućuje na stranicu gdje je objašnjeno kako vratiti prijašnje postavke. Ako je prilikom *quick scan* skeniranja pronađen neki od malicioznih programa MSRT će predložiti korisniku da pokrene *extended* tip skeniranja. Ovim testiranjem pregledavaju se sve datoteke na svim diskovima što može potrajati i nekoliko sati.



Slika 2: MSRT sučelje u extended scan načinu rada

Ako je MSRT-a utvrdio da je došlo do inficiranja ili promjene datoteka zbog djelovanja malicioznog programa otvorit će se novi prozor u kojem će korisniku biti omogućen izbor da očisti neke ili sve zaražene datoteke.

Napomena: može se dogoditi da MSRT-a nije u mogućnosti vratiti datoteke u njihovo prvobitno stanje.

Nakon skeniranja rezultati će biti prikazani korisniku (ako nije pokrenut u *quiet* načinu rada), te spremljeni u datoteku `Mrt.log` u mapi `%windir%\debug`. Moguća su 4 različita rezultata:

- na računalu nisu pronađeni maliciozni programi,
- pronađen je i odstranjen najmanje jedan maliciozni program,
- pronađeni su maliciozni programi, ali nisu odstranjeni (za odstranjivanje potrebno je koristiti druge metode ili antivirusne programe),
- pronađeni su maliciozni programi, ali nisu mogli biti potpuno odstranjeni (za odstranjivanje potrebno je koristiti druge metode ili antivirusne programe).

Također, MSRT može zatražiti ponovno pokretanje računala ili od korisnika zatražiti da ručno odstrani sumnjive datoteke.

Nakon pokretanja MSRT moguće je da dođe do pogrešaka prilikom testiranja. Postupak utvrđivanja razloga pogreške je slijedeći:

1. Otvoriti log datoteku `Mrt.log` koja se nalazi u `%windir%\debug` mapi.
2. Nakon otvaranja datoteke pronaći posljednji upis koji se nalazi na kraju datoteke.
3. Usporediti pogrešku u log datoteci s pogreškama navedenim u tablici na stranici http://support.microsoft.com/?kbid=891717 i slijediti dane upute. Neke pogreške mogu sadržavati i Windows kod pogreške o čemu je moguće više saznati na stranici http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/system_-error_codes.asp .

Slijedeći primjer je dio `Mrt.log` datoteke nakon skeniranja računala koje je zaraženo crvom Sasser.A:

```
Microsoft Windows Malicious Software Removal Tool v1.2, March 2005
Started On Wed May 01 21:21:42 2002
Scanning Results:
----------------
Found virus: Win32/Sasser.A.worm in process 1856
Found virus: Win32/Sasser.A.worm in process 1856
Found virus: Win32/Sasser.A.worm in file C:\WINDOWS\avserve.exe
Found virus: Win32/Sasser.A.worm in process 1856
Found virus: Win32/Sasser.A.worm in file C:\WINDOWS\avserve.exe
Removal Results:
----------------
```

```
Terminating process with pid 1856
Operation succeeded !
Terminating process with pid 1856
Operation had previously completed.
Terminating process with pid 1856
Operation had previously completed.
Deleting registry value
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, entry:
avserve.exe
Operation succeeded !
Deleting file C:\WINDOWS\avserve.exe
Operation succeeded !
Deleting file C:\WINDOWS\avserve.exe
Operation had previously completed.
Results Summary:
----------------
Found Win32/Sasser.A.worm and Removed!
Return code: 6
Microsoft Windows Malicious Software Removal Tool Finished On Wed
May 01 21:21:45 2002
```

3.1. Korporativno okruženje

MSRT-a mora biti pokrenut s administratorskim ili *local system* ovlastima. Pokretanje se obavlja preko slijedeće skripte (kojoj je dodijeljeno proizvoljno ime `Mrt.cmd`):

```
@echo off
call \\ServerName\ShareName\Sleep.exe 5
Start /wait \\ServerName\ShareName\Windows-KB890830-V1.4-ENU.exe /q
copy %windir%\debug\mrt.log
\\ServerName\ShareName\Logs\%computername%_%username%_mrt.log
```

Skripta ima slijedeću funkciju:

- pokreće MSRT u *silent* načinu rada,
- kopira log datoteku u označenu dijeljenu mapu,
- postavlja prefiks na ime log datoteke u obliku: `%computername%_%username%_mrt.log`

Za ispravan rad skripte prije pokretanja potrebno je postaviti potrebne dozvole kako je opisano na stranici http://support.microsoft.com/kb/891716#4.

3.1.1. Pokretanje pomoću *SMS Software Package*

Slijedeći koraci objašnjavaju korištenje SMS 2003 za korištenje MSRT u korporativnom okruženju:

1. Otpakirati datoteku `Mrt.exe` iz paketa `Windows-KB890830-V1.4-ENU.exe /x`.
2. Stvoriti `.bat` datoteku koja će uhvatiti odgovor koji vraća `ISMIF32.exe`. U `.bat` datoteci potrebno je uključiti sljedeće naredbe:

```
@echo off
Mrt.exe /q
If errorlevel 13 goto error13
If errorlevel 12 goto error12
Goto end
:error13
Ismif32.exe –f MIFFILE –p MIFNAME –d ”text about error 13”
Goto end
:error 12
Ismif32.exe –f MIFFILE –p MIFNAME –d “text about error 12” Goto end
:end
```

3. Za izradu paketa u SMS 2003 konzoli slijediti korake:
   a) Otvoriti **SMS Administrator** konzolu.
   b) Desnim gumbom miša kliknuti na polje **Packages**, kliknuti na **New**, te na **Package**. Otvorit će se dijaloški okvir **Package Properties**.
   c) Na kartici **General** imenovati paket.
   d) Na kartici **Data Source** označiti **This package contains source files** *check box*.

e) Kliknuti **Set** i izabrati mapu u kojoj se nalazi MSRT.
f) Na kartici **Distribution Settings** postaviti **Sending priority** na **High**.
g) Na kartici **Reporting** kliknuti na **Use these fields for status MIF matching**, te upisati ime u polje **MIF file name** i polje **Name**. Defniranje **Version** and **Publisher** su opcionalne.
h) Kliknuti na **OK** za stvaranje paketa.

4. Za definiranje distribucijske točke (engl. *Distribution Point*) paketa slijediti korake:
a) U **SMS 2003** konzoli pronaći novi paket u polju **Packages**.
b) Raspakirati paket. Desnim gumbom miša kliknuti na **Distribution Points**, pozicionirati pokazivač miša na **New**, te kliknuti na **Distribution Points**.
c) Pokrenuti **New Distribution Points Wizard**. Odabrati postojeću distibucijsku točku.
d) Kliknuti na **Finish**.

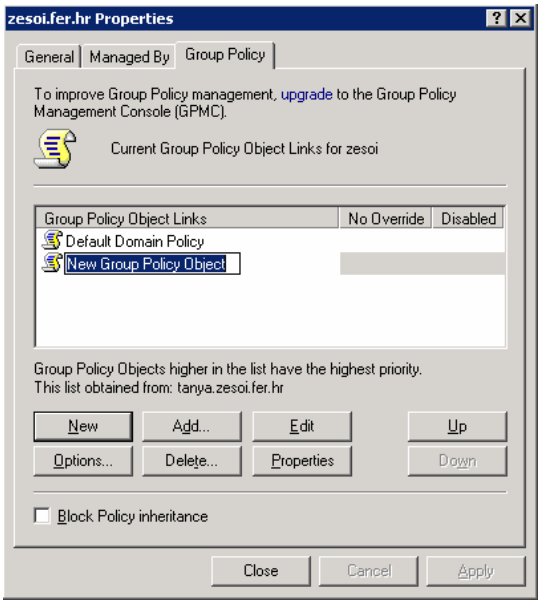
5. Za dodavanje prehodno kreirane `.bat` datoteke u paket potrebni su sljedeći koraci:
a) Unutar polja **New Package** kliknuti na polje **Programs**.
b) Desnim gumbom miša kliknuti na **Programs**, pozicionirati pokazivač miša na **New**, te kliknuti na **Program**.
c) Kliknuti na karticu **General** i unijeti ispravno ime.
d) U komandnoj liniji (engl. *Command line*)kliknuti na **Browse** za selektiranje .bat datoteke koja pokreće Mrt.exe.
e) Promjeniti **Run** u **Hidden**. Promjeniti **After** u **No action required**.
f) Kliknuti na karticu **Requirements**, te nakon toga kliknuti na **This program can run only on specified client operating systems**.
g) Kliknuti na **All x86 Windows 2000**, **All x86 Windows Server 2003** i **All x86 Windows XP**.
h) Kliknuti na karticu **Environment**, te nakon toga klknuti na **Whether a user is logged** u listi **Program can run**. Postaviti **Run** način rada na **Run with administrative rights**.
i) Kliknuti na **OK**.

6. Za oblikovanje obavijesti koja će bit poslana klijentima potreno je sljedeće:
a) Desnim gumbom miša kliknuti na polje **Advertisement**, kliknuti na **New**, te na **Advertisement**.
b) Na kartici **General** unijeti ime obavijesti. U polju **Package** odabrati koji smo prethodno stvorili. U polju **Program** odabrati program koji smo prethodno stvorili. Kliknuti na **Browse**, te na **All System** kolekciju ili kolekciju računala koju sadrže Microsoft Windows 2000 ili kasniju inačicu.
c) Na kartici **Schedule** ostaviti *default* opciju ako će se program pokretati samo jedanput, inače dodijeliti definirani raspored (engl. *schedule*).
d) Postaviti **Priority** na **High**.
e) Kliknuti na **OK**.

3.1.2. Pokretanje korištenjem *Group Policy*-bazirane *computer startup* skripte

Ova metoda nakon postavljanja skripte i primjenjivanja grupne politike (engl. *group policy*) zahtjeva ponovno pokretanje klijentskog računala. Postupak je slijedeći:

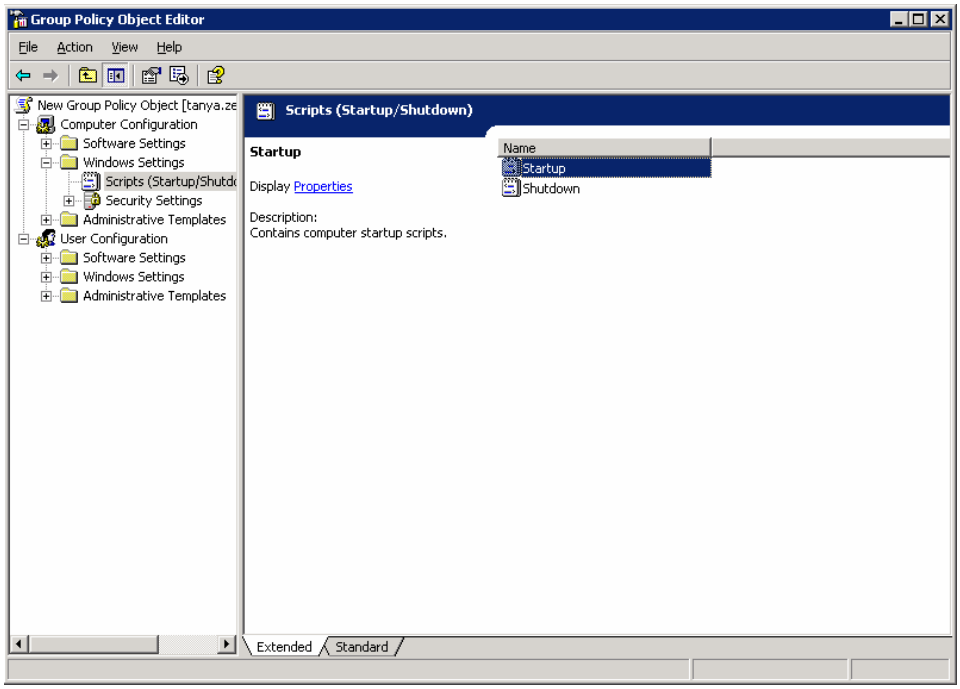
1. Postaviti dijeljene mape na način opisan na stranici http://support.microsoft.com/kb/891716#4.
2. Postaviti *startup* skriptu na slijedeći način:
a) U **Active Directory Users and Computers** MMC konzoli desnim gumbom miša kliknuti na **domain name** (ili na odgovarajući OU), te na **Properties**.
b) Kliknuti na karticu **Group Policy**.
c) Odabrati **New** za izradu novog GPO (engl. *group policy object*) objekta (moguće je i uređivanje postojećeg ili postojećih *group policy* objekata) i unijeti **MRT Deployment** kao ime novo-definirane politike (Slika 3).



Slika 3: Dodavanje novog group policy objekta

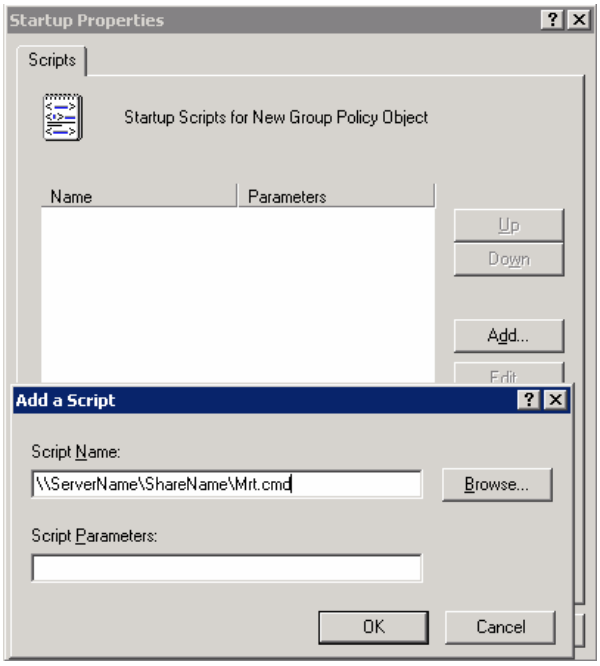
d) Kliknuti na **new policy**, te na **Edit.**

Otvoriti **Windows Settings for Computer Configuration**, te kliknuti na **Scripts (**Slika 4**).**



Slika 4: Podešavanje computer startup skripte

e) Dvostruko kliknuti na **Startup**, te na **Add.** Otvoritće se dijaloški okvir **Add a Script** (Slika 5).



Slika 5: Dodavanje nove computer startup skripte

f) U polju **Script Name** unijeti: `\\ServerName\ShareName\Mrt.cmd`.
g) Kliknuti na **OK**, te na **Apply**.

3. Ponovno pokrenuti računala na domeni.

3.1.3. Pokretanje pomoću *Group Policy*-bazirane *user logon* skripte

Ova metoda slična je kao i prethodna, osim što se *logon* skripta pokreće prilikom prijave korisnika za rad, a ne prilikom podizanja računala kao u prethodnom slučaju. Za ovu metodu nužno je korištenje domenskog korisničkog računa s administratorskim ovlastima na lokalnom računalu. Postupak dodavanja skripte je slijedeći:

1. Postaviti dijeljene mape na način opisan na stranici http://support.microsoft.com/kb/891716#4.
2. Postaviti *startup* skriptu na slijedeći način:
   a) U **Active Directory Users and Computers** MMC konzoli desnim gumbom miša kliknuti na **domain name**, te na **Properties**.
   b) Kliknuti na karticu **Group Policy**.
   c) Kliknuti na **New** za izradu novog *Group Policy* objekta (GPO) i unijeti **MRT Deployment** kao ime novo-definirane politike.
   d) Kliknuti na **new policy**, te na **Edit**.
   e) Otvoriti **Windows Settings for User Configuration**, te kliknuti na **Scripts**.
   f) Dvostruko kliknuti na **Logon**, te na **Add**. Otvoriti će se dijaloški okvir **Add a Script**.
   g) U polju **Script Name** unijeti: `\\ServerName\ShareName\Mrt.cmd`.
   h) Kliknuti na **OK**, te na **Apply**.
3. Odlogirati se i logirati se na klijentsko računalo.

3.1.4. Pregled povratnih kodova

MSRT će nakon završetka testiranja u log datoteku `Mrt.log` unijeti rezultate testiranja. Također, u datoteku će bit zapisan i jedan od povratnih kodova zapisanih u slijedećoj tablici (Tablica 1).

Kod	Opis pogreške
0	Infekcija nije pronađena.
1	Pogreška OS okruženja.

Kod	Opis pogreške
2	Račun nije član administratorske grupe.
3	OS nije podržan.
4	Pogreška pri inicijalizaciji (dohvatiti novi kopiju MSRT-a).
5	Nekorišten.
6	Pronađena bar jedna infekcija. Nema pogrešaka.
7	Pronađena bar jedna infekcija, postoje pogreške.
8	Pronađena bar jedna infekcija koja je odstranjena, ali su potrebni dodatni koraci za potpuno odstranjivanje.
9	Pronađena bar jedna infekcija koja je odstranjena, ali su potrebni dodatni koraci za potpuno odstranjivanje. Postoje pogreške.
10	Pronađena bar jedna infekcija koja je odstranjena, ali je potrebno ponovno pokretanje računala za potpuno odstranjivanje.
11	Pronađena bar jedna infekcija koja je odstranjena, ali je potrebno ponovno pokretanje računala za potpuno odstranjivanje. Postoje pogreške
12	Pronađena bar jedna infekcija koja je odstranjena, ali su potrebni dodatni koraci i ponovno pokretanje računala za potpuno odstranivanje. Postoje pogreške.
13	Pronađena bar jedna infekcija koja je odstranjena, ali je potrebno ponovno pokretanje računala. Ne postoje pogreške.

Tablica 1: Povratni kodovi koje vraća MSRT

4. Funkcionalnost

U slijedećoj tablici (***Tablica 2***) su dani maliciozni programi koje ovaj alat može identificirati i ukloniti sa računala. Također alat identificira i uklanja sve poznate inačice tih programa do datuma izlaska alata. U tablici se nalaze i inačice alata u kojima se po prvi put identificira odgovarajući maliciozni program, te stupanj opasnosti prema Microsoftovoj ljestvici.

Maliciozni program	Inačica alata	Stupanj opasnosti
Win32/Berbew	01.2005 (V 1.0)	Niski
Win32/Doomjuice	01.2005 (V 1.0)	Niski
Win32/Gaobot	01.2005 (V 1.0)	Srednji
Win32/MSBlast	01.2005 (V 1.0)	Srednji
Win32/Mydoom	01.2005 (V 1.0)	Srednji
Win32/Nachi	01.2005 (V 1.0)	Niski
Win32/Sasser	01.2005 (V 1.0)	Srednji
Win32/Zindos	01.2005 (V 1.0)	Niski
Win32/Korgo	02.2005 (V 1.1)	Srednji
Win32/Netsky	02.2005 (V 1.1)	Srednji
Win32/Randex	02.2005 (V 1.1)	Niski
Win32/Zafi	02.2005 (V 1.1)	Srednji
Win32/Bagle	03.2005 (V 1.2)	Srednji
Win32/Bropia	03.2005 (V 1.2)	Niski
Win32/Goweh	03.2005 (V 1.2)	Srednji
Win32/Sober	03.2005 (V 1.2)	Srednji
Win32/Sobig	03.2005 (V 1.2)	Niski
Win32/Hackdef	04.2005 (V 1.3)	Niski
Win32/Mimail	04.2005 (V 1.3)	Niski
Win32/Rbot	04.2005 (V 1.3)	Srednji
Win32/Sdbot	05.2005 (V 1.4)	Srednji

Tablica 2: Popis malicioznih programa koje MSRT može identificirati i ukloniti

Postoje 3 stupnja opasnosti, a to su niski (engl. *low*), srednji (engl. *moderate*) i visoki/kritični (engl. *critical*). Svojstva svih stupnjeva opasnosti prikazana su u slijedećoj tablici (Tablica 3).

Karakteristike visokog stupnja	Svojstva
Ranjivost Microsoftovog proizvoda	Da/Zakrpa ne postoji
Vektori infekcije	Broj vektora >= 2
Novi vektor infekcije	Da/Ne
Mogućnost distribucije	Velika
Uništenje podataka	Da/Ne
Ometanje rada važnih servisa	Da
Karakteristike srednjeg stupnja	**Svojstva**
Ranjivost Microsoftovog proizvoda	Da/Ne
Vektori infekcije	Broj vektora <= 2
Novi vektor infekcije	Da/Ne
Mogućnost distribucije	Srednja/Velika
Uništenje podataka	Ne
Ometanje rada važnih servisa	Ne
Karakteristike niskog stupnja	**Svojstva**
Ranjivost Microsoftovog proizvoda	Ne
Vektori infekcije	Broj vektora = 1
Novi vektor infekcije	Ne
Mogućnost distribucije	Mala
Uništenje podataka	Ne
Ometanje rada važnih servisa	Ne

Tablica 3: Svojstva pojedinih stupnjeva opasnosti

Za više informacija o metrici klasifikacije opasnosti malicioznih programa pogledati stranicu http://www.microsoft.com/technet/security/alerts/matrix.mspx.
Razlike između Microsoft MSRT alata i standardnih antivirusnih programa dane su u slijedećoj tablici (***Tablica 4***).

Malicious Software Removal Tool	Standardni antivirusni programi
Omogućuje odstranjivanje malicioznog programa tek nakon što je računalo zaraženo.	Omogućuju odstranjivanje malicioznog programa i prije i nakon što je računalo zaraženo.
Odstranjuje samo specifičnih (trenutno najzastupljenijih) malicioznih programa.	Odstranjuju većinu postojećih malicioznih programa.
Fokusira se na detekciju i odstranjivanje samo aktivnih malicioznih programa.	Odstranjuju i aktivne i neaktivne maliciozne programe.

Tablica 4: Usporedba MSRT alata i standardnih antivirusnih programa

5. Zaključak

Alat je namijenjen prvenstveno korisnicima koji žele imati brzu provjeru moguće infekcije sustava. Preporučuje se samo kao nadopuna postojeće antivirusne zaštite i nikako se ne bi smio koristiti kao jedini antivirusni alat. Zbog nedostataka MSRT-a u odnosu na standardne antivirusne alate, sigurno je da MSRT u ovom obliku neće biti prihvaćen od strane velikog broja korisnika. Iako se svakog mjeseca nadopunjuje baza MSRT-a koja sadrži listu malicioznih programa to još uvijek niti blizu nije dovoljno za adekvatnu zaštitu od malicioznih programa, bilo za pojedinačne korisnike, bilo u korporativnom okruženju.