HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza NetSky.B i NetSky.D crva

CCERT-PUBDOC-2004-03-64

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

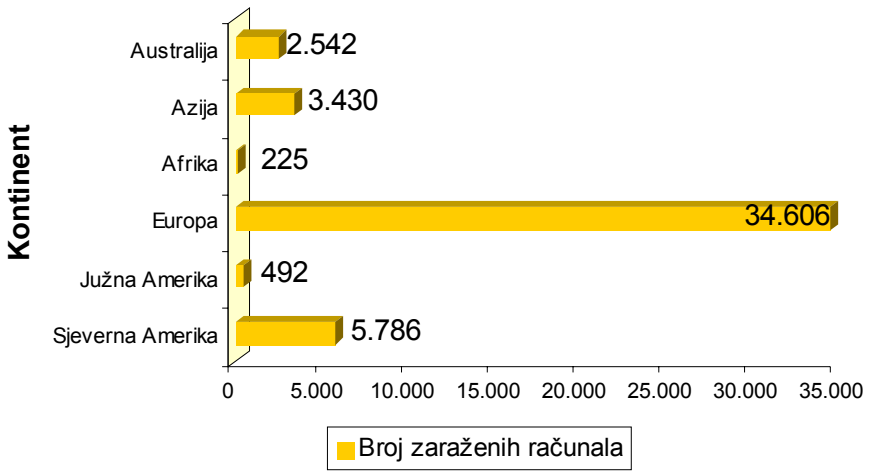
1. Uvod

U dokumentu su analizirane dvije inačice NetSky crva, NetSky.B i NetSky.D. Kao njihovog prehtodnika, potrebno je spomenuti prvu inačicu crva, NetSky.A, koja je otkrivena 16. veljače 2004. godine, a poznata je i pod imenima W32/Netsky.A, I-Worm.Moodown i Moodown. Osnovni način širenja prve inačice crva bio je putem poruka elektroničke pošte i dijeljenih mapa. Ubrzo nakon prve inačice, 18. veljače 2004. godine pojavila se i druga inačica pod imenom NetSky.B (poznata i pod imenima Win32/Netsky.B, W32.Netsky.B@mm, WORM_NETSKY.B, I-Worm.Moodown.b, Worm.SomeFool), čiji je osnovi način širenja bio putem poruka elektroničke pošte koje su imale slučajno generirani predmet poruke (engl. *subject*) te putem dijeljenih mapa. Iduća inačica crva čija je analiza iznesena u ovom dokumentu je NetSky.D (poznata i pod imenima W32.Netsky.D@mm, W32/Netsky.d@MM, W32/Netsky-D, NetSky.D), otkrivena 1. ožujka 2004., a čiji je osnovni način širenja također putem poruka elektroničke pošte.

Osim spomenutih, do danas je poznato još 16 inačica NetSky crva pod imenima Worm_NetSky.G, Worm_NetSky.J, Worm_NetSky.M, Worm_NetSky.O, Worm_NetSky.P, Worm_NetSky.N, Worm_NetSky.L, Worm_NetSky.K, Worm_NetSky.GEN, Worm_NetSky.DAM, Worm_NetSky.C, Worm_NetSky, Worm_NetSky.H, Worm_NetSky.I i Worm_NetSky.E.

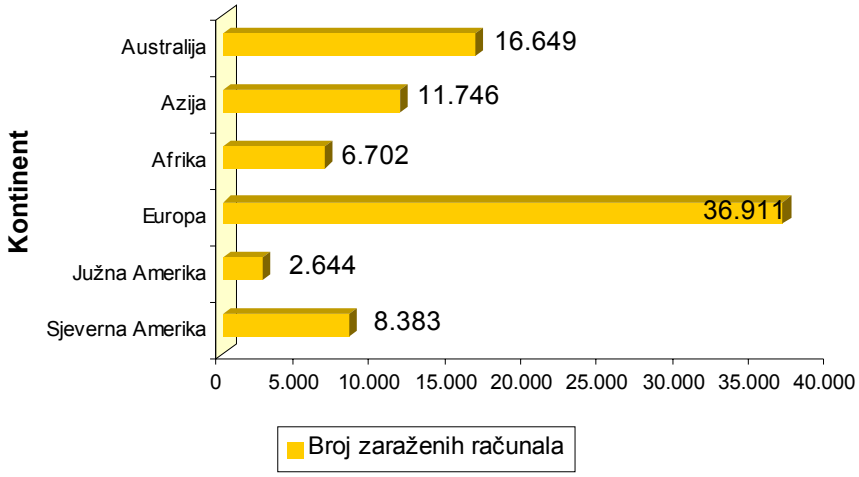
Sve inačice ovog crva napale su računala s Microsoft Windows operacijskim sustavima u vrlo kratkom vremenskom intervalu, ali inačice NetSky.B i NetSky.D i danas zauzimaju visoko mjesto na top listama virusnih prijetnji.

Slika 1 prikazuje je broj zaraženih računala inačicom crva NetSky.B u periodu od 16. ožujka do 23. ožujka po kontitentima.



Slika 1: *Grafički prikaz broja zaraženih računala inačicom crva NetSky.B u periodu od 7 dana*

Slika 2 prikazuje broj zaraženih računala inačicom crva NetSky.D u periodu od 16. ožujka do 23. ožujka po kontitentima.



Slika 2: *Grafički prikaz broja zaraženih računala inačicom crva NetSky.D u periodu od 7 dana*

Prema grafičkim prikazima vidljivo je da je broj računala koja su zaražena inačicom crva NetSky.D veća u odnosu na broj računala zaraženih varijantom NetSky.B crva na svim kontitentima. Također je lako uočiti da je istaknuto najizloženiji kontinent bila Europa.

Ovaj dokument detaljno će analizirati način širenja navedenih inačica crva NetSky, kao i osnovne metode za njegovu detekciju te ručno i automatsko uklanjanje.

2. Analiza

2.1. NetSky.B

Kao što je spomenuto u uvodnom dijelu, crv NetSky.B širi se putem poruka elektroničke pošte koje imaju slučajno generirani predmet poruke (engl. *subject*) te putem dijeljenih mapa.

Poruke elektroničke pošte koje sadrže zaraženu datoteku prepoznatljive su prema predmetu poruke (engl. *Subject*) koji može biti bilo koja od slijedećih riječi:

```
fake
hello
hi
information
read it immediately
something for you
stolen
unknown
warning
```

Tijelo poruke čini bilo koja od navedenih riječi:

```
about me
anything ok?
do you?
from the chatter
greetings
here
here is the document.
here it is
here, the cheats
here, the introduction
here, the serials
i found this document about you
```

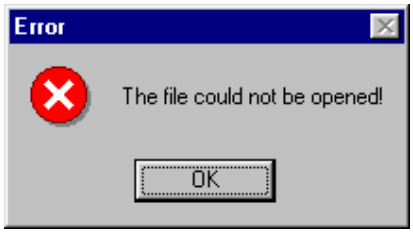
```
I have your password!
i hope it is not true!
i wait for a reply!
i'm waiting
information about you
is that from you?
is that true?
is that your account?
is that your name?
kill the writer of this document!
misc
my hero
ok
read it immediately!
read the details.
reply
see you
something about you!
something is fool
something is going wrong
something is going wrong!
stuff about you?
take it easy
that is bad
that's funny
thats wrong
what does it mean?
why?
yes, really?
you are a bad writer
you are bad
you earn money
you feel the same
you try to steal
your name is wrong
```

Slijedeća karakteristika koja zaraženu poruku elektroničke pošte čini prepoznatljivom jest privitak poruke (engl. *attachment*) čije ime može biti bilo koja od slijedećih riječi:

```
aboutyou
attachment
bill
concert
creditcard
details
dinner
disco
doc
document
final
found
friend
information
jokes
location
mail2
mails
me
```

```
message
misc
msg
nomoney
note
object
part2
party
posting
product
ps
ranking
release
shower
story
stuff
swimmingpool
talk
textfile
topseller
website
```

Nazivu privitka dodaju se jedna ili dvije ekstenzije. Prva ekstenzija može biti `.doc`, `.htm`, `.rtf` ili `.txt`, dok drugu ekstenziju čine `.com`, `.exe`, `.pif` i `.scr`.
Privitak također može biti i komprimiran u `.zip` formatu pri čemu zaražena poruka elektroničke pošte nema neku od navedenih ekstenzija, već u tom slučaju ima `.zip` ekstenziju. Međutim, potrebno je napomenuti da datoteka koju sadrži `komprimirana` arhiva ima prvi ili oba navedena nastavka.
Pošiljatelj (engl. *From*) i primatelj (engl. *To*) zaražene poruke elektroničke pošte je slučajno odabrana adresa iz baze sakupljenih adresa elektroničke pošte.
Nakon primitka zaražene poruke elektroničke pošte i otvaranjem privitka poruke dolazi do aktiviranja crva pri čemu se prikazuje lažna poruka o pogrešci nastaloj prilikom otvaranja datoteke prikazana na slici **(**Slika 3**).**



Slika 3: *Poruka na računalu nakon aktivacije crva NetSky.B*

Crv se samostalno kopira u Windows mapu kao datoteka *services.exe*. Kako bi se osiguralo automatsko pokretanje izvršne datoteke prilikom svakog slijedećeg pokretanja Windows operacijskog sustava, crv kreira sljedeći zapis u *registry* datoteci:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run\"service" = %Windows%\services.exe serv
```

pri čemu `%Windows%` predstavlja standardnu Windows mapu (uobičajena putanja `C:\Windows` za Windows 9x i ME operacijske sustave ili `C:\Winnt` za Windows NT, 2000 i XP operacijske sustave).
Istovremeno, crv briše *registry* zapise postavljene od strane crva WORM_MYDOOM i WORM_MIMAIL.T kako bi spriječio automatsko pokretanje izvršnih datoteka prilikom svakog pokretanja operacijskog sustava. Za crv Worm_MyDoom.A brišu se sljedeći *registry* zapisi:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
"Taskmon"
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
"Taskmon"
```

Za crv Worm_MyDoom.B brišu se sljedeći *registry* zapisi:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
"Explorer"
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
"Explorer"
```

Za oba navedena crva briše se ključ:

```
HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\
InProcServer32
```

Za crv Worm_Mimail.T briše se *registry* zapis:

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

Za sva tri crva brišu se *registry* zapisi:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
"system"
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
"system"
```

Nakon aktivacije crv pokreće *mass-mailing* rutinu pri čemu koristi vlastiti SMTP (engl. ***S**imple **M**ail **T**ransfer **P**rotocol*) poslužitelj kako bi se širio putem poruka elektroničke pošte. SMTP poslužitelj šalje upit za MX (mail exchanger) zapisom u ciljnoj domeni, spaja se direktno na MTA (engl. *message transfer agent*) i šalje zaraženu e-mail poruku. Kao podrazumijevani DNS poslužitelj crv koristi IP adresu 217.5.100.1. Adrese primatelja zaraženih poruka elektroničke pošte crv pronalazi pretraživanjem datoteka na lokalnim diskovima od C: do Z. Pretražuju se datoteke sljedećih ekstenzija: `.adb`, `.asp`, `.dbx`, `.doc`, `.eml`, `.htm`, `.html`, `.msg`, `.oft`, `.php`, `.pl`, `.rtf`, `.sht`, `.tbb`, `.txt`, `.uin`, `.vbs` i `.wab`.
Uočeno je da inačice NetSky crva, prilikom sakupljanja adresa elektroničke pošte sva velika štampana slova automatski mijenjaju u mala pisana slova što znači da u slučaju pronalaska adrese elektroničke pošte u obliku Ime.Prezime@domena.hr, adresu mijenjaju u adresu oblika ime.prezime@domena.hr**.**
Drugi način širenja crva jest putem dijeljenih mapa. U ovom slučaju crv ostavlja svoje mnogobrojne kopije u mapama koje unutar svog imena sadrže skup znakova `sharing` i `share`.
Primjer mape koja zadovoljava navedeni uvjet jest `C:\Program Files\My Shared Folder\Kazaa`.
Imena pod kojima crv ostavlja svoje kopije unutar dijeljenih mapa su:

```
angels.pif
cool screensaver.scr
dictionary.doc.exe
dolly_buster.jpg.pif
doom2.doc.pif
e.book.doc.exe
e-book.archive.doc.exe
eminem - lick my pussy.mp3.pif
hardcore porn.jpg.exe
how to hack.doc.exe
matrix.scr
max payne 2.crack.exe
nero.7.exe
office_crack.exe
photoshop 9 crack.exe
```

```
porno.scr
programming basics.doc.exe
rfc compilation.doc.exe
serial.txt.exe
sex sex sex sex.doc.exe
strippoker.exe
virii.scr
win longhorn.doc.exe
winxp_crack.exe
```

Crv također ostavlja i svoje komprimirane kopije unutar Windows mape koristeći neko od navedenih imena:

```
aboutyou
attachment
bill
concert
creditcard
details
dinner
disco
doc
final
found
friend
information
jokes
location
mail2
mails
me
message
misc
msg
nomoney
note
object
part2
party
posting
product
ps
ranking
release
shower
story
stuff
swimmingpool
talk
textfile
topseller
website
```

Komprimirane kopije imaju `.zip` ekstenziju, a datoteka unutar komprimirane datoteke ima neki, jednu ili obje ranije navedene ekstenzije.

2.2. NetSky.D

NetSky.d, kao i prethodno opisani NetSky.B, također koristi vlastiti SMTP (engl. ***S**imple **M**ail **T**ransfer **P**rotocol*) poslužitelj kako si se širio putem poruka elektroničke pošte. Poruke elektroničke pošte koje

sadrže zaraženu datoteku prepoznatljive su prema predmetu poruke (engl. *Subject*) koji može biti bilo koja od slijedećih riječi:

```
Re: Approved
Re: Details
Re: Document
Re: Excel file
Re: Hello
Re: Here
Re: Here is the document
Re: Hi
Re: My details
Re: Re: Document
Re: Re: Message
Re: Re: Re: Your document
Re: Re: Thanks!
Re: Thanks!
Re: Word file
Re: Your archive
Re: Your bill
Re: Your details
Re: Your document
Re: Your letter
Re: Your music
Re: Your picture
Re: Your product
Re: Your software
Re: Your text
Re: Your website
```

Tijelo poruke čini bilo koja od navedenih riječi:

```
Your file is attached.
Please read the attached file.
Please have a look at the attached file.
See the attached file for details.
Here is the file.
Your document is attached.
```

Privitak poruke zaražene ovim crvom nosi ime jednako nekoj od slijedećih riječi:

```
all_document.pif
application.pif
document.pif
document_4351.pif
document_excel.pif
document_full.pif
document_word.pif
message_details.pif
message_part2.pif
mp3music.pif
my_details.pif
your_archive.pif
your_bill.pif
your_details.pif
your_document.pif
your_file.pif
your_letter.pif
your_picture.pif
your_product.pif
```

```
your_text.pif
your_website.pif
yours.pif
```

NetSky.D datoteka komprimirana je s Petite arhiverom koja ima veličinu od 17424 okteta. Nekomprimirana datoteka ima veličinu 28 KB. Razlika između ove i ranije opisane inačice crva jest u tome što NetSky.D crv, prilikom prve aktivacije, ne prikazuje lažnu poruku o pogrešci nastaloj prilikom otvaranja datoteke. Bitno je napomenuti da ovaj crv za svoju aktivaciju mora zadovoljavati specifični uvjet. Na dan kada je sistemski datum jednak datumu 2. ožujka 2004., generira sistemski zvuk u vremenskom intervalu od 6.00 do 8.59 sati.
Nakon aktivacije, crv se samostalno kopira kao datoteka *winlogon.exe* u Windows mapu. Važno je napomenuti da Windows operacijski sustavi NT, 2000 i XP imaju legalnu datoteku *winlogon.exe* u Windows mapi te ih je potrebno razlikovati. Radi osiguranja pokretanja izvršen datoteke prilikom svakog pokretanja Windows operacijskog sustava u *registry* datoteku se dodaje zapis:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
ICQ Net = "%Windows%\winlogon.exe -stealth"
```

Za širenje putem poruka elektroničke pošte, crv pokreće *mass-mailing* rutinu koristeći vlastiti SMTP poslužitelj. Adrese primatelja zaraženih poruka elektroničke pošte crv pronalazi pretraživanjem datoteka na lokalnim diskovima od C: do Z: koje imaju nastavak: `.adb`, `.asp`, `.dbx`, `.doc`, `.eml`, `.htm`, `.html`, `.msg`, `.oft`, `.php`, `.pl`, `.rtf`, `.sht`, `.tbb`, `.txt`, `.uin`, `.vbs` i `.wab`, kao što to čini i NetSky.B. Međutim, NetSky.D crv, prilikom slanja zaraženih poruka, preskače adrese elektroničke pošte koje u sebi sadrže navedeni skup znakova:

```
abuse
antivi
aspersky
avp
cafee
fbi
f-pro
f-secur
Icrosoft
itdefender
messagelabs
orman
orton
skynet
spam
ymantec
```

kako bi se izbjeglo slanje zaraženih poruka proizvođačima antivirusnog softvera.
SMTP poslužitelj crva u potrazi za *mail exchanger* (MX) zapisima koristi lokalni DNS poslužitelj. Ukoliko takav DNS upit ne uspije, SMTP poslužitelj šalje upit prema navedenim vanjskim DNS poslužiteljima:

```
212.44.160.8
195.185.185.195
151.189.13.35
213.191.74.19
193.189.244.205
145.253.2.171
193.141.40.42
194.25.2.134
194.25.2.133
194.25.2.132
194.25.2.131
193.193.158.10
```

```
212.7.128.165
212.7.128.162
193.193.144.12
217.5.97.137
195.20.224.234
194.25.2.130
194.25.2.129
212.185.252.136
212.185.253.70
212.185.252.73
62.155.255.16
```

Ukoliko na računalu zaraženim ovim crvom, postoje *registry* zapisi postavljeni od strane crva Worm_MyDoom.A, Worm_MyDoom.B, Worm_Mimail.T, Worm_NetSKy.A, Worm_NetSky.B, Worm_Deadhat.B, Worm_Bagle.A, Worm_Bagle.B, Worm_Nachi.B, Worm_Nachi.C i Pe_Parite.A, crv će obrisati slijedeće zapise iz *registry* datoteke:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
au.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
d3dupdate.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
KasperskyAv
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
OLE
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
Taskmon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
DELETE ME
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
KasperskyAv
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
msgsvr32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
Sentry
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
service
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
system
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
Taskmon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
RunServices\system
HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\
InProcServer32
```

3. Detekcija i uklanjanje

U ovom poglavlju opisan je postupak detekcije crva, te postupci ručnog i automatskog brisanja crva nekim od dostupnih alata.

Za uspješnu detekciju bilo kojeg od ova dva crva, potrebno je koristiti antivirusni program koji ima ažuriranu bazu virusa. Pokretanjem antivirusnog programa izvodi se postupak traženja zaražene datoteke na računalu. Kada je zaražena datoteka detektirana, potrebno ju je zaustaviti na slijedeći način:

1. Otvoriti `Windows Task Manager` dijaloški okvir. Na računalima s Windows 9x i ME operacijskim sustavom, potrebno je pritisnuti kombinaciju tipki `CTRL+ALT+DELETE`, a za Windows NT, 2000 i XP kombinaciju tipki `CRTL+SHIFT+ESC`.
2. U dijaloškom okviru otvoriti karticu `Processes`.
3. U popisu aktivnih programa pronaći zaraženu datoteku (ili datoteke) te kliknuti na svaku od njih, a zatim kliknuti dugme `End Task` (ili `End Process`), ovisno o inačici Windows operacijskog sustava.
4. Zatvoriti dijaloški okvir.

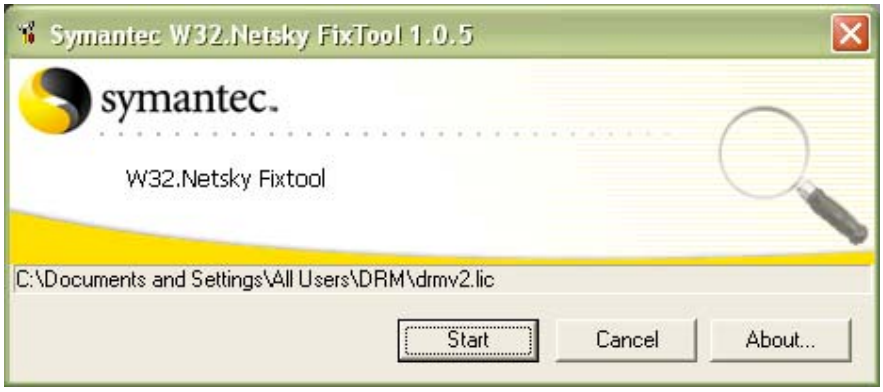
Nakon zaustavljanja pokrenute datoteke crva omogućeno je ručno uklanjanje crva sa zaraženog računala. Prije samog postupka detekcije te ručnog uklanjanja crva sa zaraženog računala, potrebno je napomenuti da se korisnicima Windows ME i XP operacijskih sustava preporučuje privremeno onemogućavanje System Restore opcije. Za NetSky.B crva postupak uklanjanja se sastoji od slijedećih koraka:

1. Otvoriti *Registry editor* (*Start – Run* – upisati naredbu *regedit*).
2. U lijevom okviru otvorenog prozora otvoriti `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`.
3. U desnom okviru detektirati i obrisati slijedeću vrijednost: `service = %Windows%\services.exe -serv`.
4. U lijevom okviru otvoriti `HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}`.
5. Desnom tipkom miša kliknuti na odabrani ključ i kreirati novi podključ imena `InProcServer32`.
6. U desnom okviru izmijeniti vrijednost *Default* u `%System%\WEBCHECK.DLL`.
7. Zatvoriti *Registry editor*.

Za NetSky.D crva postupak uklanjanja se sastoji od slijedećih koraka:

1. Otvoriti *Registry editor* (*Start – Run* – upisati naredbu *regedit*).
2. U lijevom okviru otvorenog prozora otvoriti `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`.
3. U desnom okviru detektirati i obrisati slijedeću vrijednost: `ICQ Net = "%Windows%\winlogon.exe -stealth"`.
4. U lijevom okviru otvoriti `HKEY_CLASSES_ROOT>CLSID>{E6FB5E20-DE35-11CF-9C87-00AA005127ED}`.
5. Desnom tipkom miša kliknuti na odabrani ključ i kreirati novi podključ imena `InProcServer32`.
6. U desnom okviru izmijeniti vrijednost *Default* u `%System%\webcheck.dll`.
7. Zatvoriti *Registry editor*.

Za manje iskusne korisnike preporučljivo je korištenje gotovih alata koji će obaviti detekciju crva te ga ukloniti sa zaraženog računala. Jedan od takvih programa je i Symantec W32.Netsky FixTool 1.0.5 koji se može pronaći na adresi http://securityresponse.symantec.com/avcenter/FxNetsky.exe, a koji ima mogućnost detekcije i uklanjanja sljedećih varijanti NetSky crva: W32.Netsky.B, W32.Netsky.C, W32.Netsky.D, W32.Netsky.E, W32.Netsky.K i W32.Netsky.P. Ovaj alat ima funkciju detekcije zaraženih datoteka, njihovog uklanjanja te brisanja Registry ključeva koje postavlja crv. Slika 4 prikazuje navedni alat nakon pokretanja izvršne datoteke alata.



Slika 4: Prozor alata Symantec W32.Netsky FixTool 1.0.5

Pritiskom na dugme Start pokreće se alat koji pretražuje datoteke računala kako bi, u slučaju detekcije zaraženih datoteka, izvršio uklanjanje istih. Rezultat postupka pretraživanja računala upisuje se u log datoteku koja se kreira u mapi u kojoj se nalazi i izvršna datoteka alata.

4. Zaključak

Uzevši u obzir vremenski interval od pojave prve inačice crva NetSky (NetSky.A) pa do sada poznatih 19 preostalih inačica, dolazi se do zaključka da se mutacije pojavljuju vrlo brzo i u velikom broju. Oba crva opisana u dokumentu definirana su kao crvi s visokim potencijalom oštećenja te visokim potencijalom distribucije. Preporuka koja se može dati korisnicima je korištenje antivirusnog programa koji svakako mora imati ažuriranu bazu virusa. Na taj način detektirat će se zaražena poruka elektroničke pošte prije nego korisnik otvori privitak i uspije aktivirati zlonamjerni sadržaj.

5. Reference

Trendmicro
NetSky.B, http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_NETSKY.B
NetSky.D, http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_NETSKY.D

Sophos
NetSky.B, http://www.sophos.com/virusinfo/analyses/w32netskyb.html
NetSky.D, http://www.sophos.com/virusinfo/analyses/w32netskyd.html

F-secure
NetSky.B, http://www.f-secure.com/v-descs/netsky_b.shtml
NetSky.D, http://www.f-secure.com/v-descs/netsky_d.shtml

Symantec
NetSky.B, http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.b@mm.html
NetSky.D, http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.d@mm.html