HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Eyeveg.F mrežnog crva

CCERT-PUBDOC-2005-05-123

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 prvoj polovici mjeseca svibnja, između 9. i 11. svibnja 2005. godine pojavio se novi mrežni crv pod imenom *Eyeveg*. U ovom dokumentu opisana je inačica crva pod imenom *Eyeveg.F. Eyeveg.F* je vrsta crva koji se širi putem poruka elektroničke pošte, a neovlaštenom korisniku omogućuje bilježenje aktivnosti na tipkovnici (eng. *keylogger*), praćenje mrežnog prometa usmjerenog prema Web poslužiteljima, prikupljanje korisničkih zaporki i sl.
Crv je još poznat pod imenima *Worm.Win32.Eyeveg.f* (Kaspersky Lab), *W32/Eyeveg.worm.gen* (McAfee), *W32/Eyeveg-F* (Sophos), *Lanieca.A@mm* (Symantec) te *Wurmark.J* (TrendMicro).
Operacijski sustavi koji mogu biti inficirani ovim crvom su Windows operacijski sustavi inačica 9x, Me, NT, 2000, XP i Server 2003. Dokument opisuje osnovne karakteristike crva, način širenja te upute za njegovo ručno uklanjanje.

2. Način širenja

Crv *Eyeveg.F* je memorijski crv koji se širi putem sustava elektroničke pošte. Međutim, moguće ga je dohvatiti i pokretanjem trojanskog konja pod imenom *Troj_Dloader.MI* koji generira slučajne nazive datoteka koje su zapravo *Eyeveg.F* crv. Crv u Windows sistemsku mapu postavlja `DLL` datoteku koja je detektirana i kao *spyware* program pod imenom *Tspy_Agent.C*. Spomenuti *spyware* program biti će registriran i kao *browser helper object* (*BHO*). Više o *spyware* programima i BHO objektima može se pročitati u dokumentima: http://www.cert.hr/filehandler.php?did=194 i http://www.cert.hr/filehandler.php?did=110.
Veličina datoteke crva jest 80,384 okteta. Po izvršenju crv kreira *registry* zapis koji mu osigurava automatsko izvršavanje pri svakom ponovnom pokretanju operacijskog sustava.
Registry zapis izgleda ovako:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Run
"[The volume serial number of the compromised computer]" = "[The volume
serial number of the compromised computer].exe"
```

Osim navedenog zapisa koji mu omogućuje automatsko izvršavanje, crv također kreira i slijedeće *registry* zapise:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{84695FD5-A8A8-11D8-978E-
005022E14DE2}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{84695FD5-A8A8-11D8-978E-
005022E14DE2}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Typelib\{84695FD5-A8A8-11D8-978E-
005022E14DE2}
HKEY_LOCAL_MACHINE\SOFTWARE\IESpy.SpyBHO
HKEY_LOCAL_MACHINE\SOFTWARE\IESpy.SpyBHO.1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
Browser Helper Objects\{84695FD5-A8A8-11D8-978E-005022E14DE2}
```

Nadalje, crv se kopira u Windows sistemsku mapu pod imenom `[Volume serijski broj zaraženog računala].exe`. U istoj mapi crv kreira i datoteku imena `[Volume serijski broj zaraženog računala].dll` u koju će biti pohranjene sve aktivnosti korisnika na tipkovnici, što znači da ovaj crv ujedno ima i komponentu *keylogger* programa.
Crv ima i mogućnosti *backdoor* programa koji omogućuju udaljeni pristup i kontrolu zaraženog računala. Akcije koje su omogućene su slijedeće:

1. slanje datoteka na poslužitelj `www.melaniecarroll.biz`,
2. dohvaćanje datoteka s poslužitelja `www.melaniecarroll.biz`,
3. pronalaženje datoteka na računalu,
4. kopiranje datoteka,
5. pokretanje datoteka,
6. brisanje datoteka,
7. sakupljanje sistemskih informacija.

Nakon što se instalira, crv navedene datoteke `.scr` tipa kopira u `%TEMP%` mapu:

```
details.doc{multiple spaces}.scr
girls.jpg{multiple spaces}.scr
image.jpg{multiple spaces}.scr
love.jpg{multiple spaces}.scr
message.txt{multiple spaces}.scr
music.mp3{multiple spaces}.scr
news.doc{multiple spaces}.scr
photo.jpg{multiple spaces}.scr
pic.jpg{multiple spaces}.scr
readme.txt{multiple spaces}.scr
resume.doc{multiple spaces}.scr
screensaver{multiple spaces}.scr
song.wav{multiple spaces}.scr
video.avi{multiple spaces}.scr
```

Crv se dalje širi tako da se samostalno šalje kao prilog poruci elektroničke pošte na ciljne adrese primatelja, a pri tome koristi vlastiti *SMTP* (*Simple Mail Transfer Protocol*) poslužitelj. U tu svrhu koristi se slijedeći *registry* zapis:

```
HKEY_CURRENT_USER\Software\Microsoft\
Internet Account Manager\Accounts
```

Adrese pošiljatelja crv sakuplja iz mape *Temporary Internet Files* i iz datoteka koji imaju ekstenzije:

```
ADB
ASP
DBX
EML
HTM
HTML
MBX
PHP
SHT
TBB
WAB
```

Među pronađenim adresama crv izbjegava slanje poruka na adrese koje sadrže neku od navedenih riječi:

```
abuse
admin
hostmaster
localdomain
localhost
mcafee
messagelab
microsoft
noreply
postmaster
recipients
reports
root
spam
symantec
webmaster
```

Bitno je naglasiti da crv koristi proizvoljne adrese elektroničke pošte kao one od pošiljatelja, tako da se identifikacija inficiranog računala ne može provesti samo provjerom adrese pošiljatelja.
Ovaj crv pokušava onesposobiti *Windows Firewall* politiku na inficiranom računalu kreirajući pri tome slijedeći *registry* zapis:

```
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfileEnableFirewall
dword:00000000
```

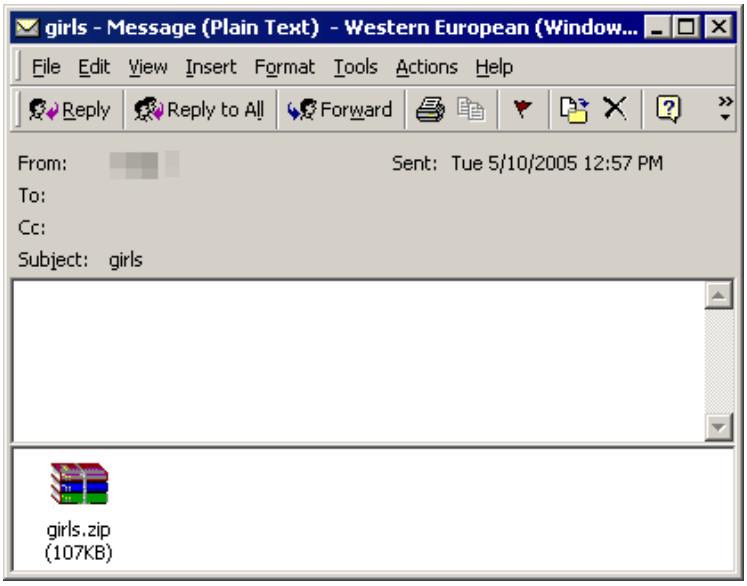
Poruke elektroničke pošte koje sadrže ovaj crv imaju slijedeći predmet poruke:

```
details
girls
image
love
message
music
news
photo
pic
readme
resume
screensaver
song
video
```

Unutar inficirane poruke nalaze se i slijedeće priložene datoteke:

```
details.zip
girls.zip
image.zip
love.zip
message.zip
music.zip
news.zip
photo.zip
pic.zip
readme.zip
resume.zip
screensaver.zip
song.zip
video.zip
```

Inficirana poruka ne sadrži nikakav popratni tekst, već poruka otvorena u klijentu *Outlook Express* izgleda kao na slici (Slika 1).



Slika 1: Poruka koja je zaražena crvom

3. Detekcija i uklanjanje

Prije samog postupka detekcije te ručnog uklanjanja crva, korisnicima Windows ME i XP operacijskog sustava preporučuje se privremeno onemogućavanje *System Restore* opcije. Za uspješnu detekciju crva potrebno je koristiti antivirusni program koji ima ažuriranu bazu virusa. Pokretanjem antivirusnog programa izvodi se postupak traženja malicioznih datoteka na računalu. Kada je maliciozna datoteka detektirana, potrebno ju je zaustaviti pokrenuti proces pod istim imenom na slijedeći način:

1. Otvoriti `Windows Task Manager` dijaloški okvir. Na računalima s Windows 2000 i XP operacijskim sustavom treba pritisnuti kombinaciju tipki `CRTL+SHIFT+ESC`.
2. U dijaloškom okviru otvoriti karticu `Processes`.
3. U popisu aktivnih programa pronaći detektirani proces (ili procese) te kliknuti na svaki od njih, a zatim kliknuti dugme `End Process`.
4. Zatvoriti dijaloški okvir.

Nakon zaustavljanja pokrenutog procesa crva omogućeno je ručno uklanjanje crva sa zaraženog računala. Postupak uklanjanja crva sastoji se 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 vrijednost: "`[The volume serial number of the compromised computer]`" = "`[The volume serial number of the compromised computer].exe`".
4. Dalje detektirati i brisati slijedeće *Registry* zapise:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{84695FD5-A8A8-11D8-978E-
005022E14DE2}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{84695FD5-A8A8-11D8-
978E-005022E14DE2}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Typelib\{84695FD5-A8A8-11D8-
978E-005022E14DE2}
HKEY_LOCAL_MACHINE\SOFTWARE\IESpy.SpyBHO
HKEY_LOCAL_MACHINE\SOFTWARE\IESpy.SpyBHO.1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explore
r\
Browser Helper Objects\{84695FD5-A8A8-11D8-978E-005022E14DE2}
```

5. Zatvoriti *Registry editor*.

Osim ručnog uklanjanja crva, u vrijeme pisanja dokumenta niti jedan proizvođač antivirusnih alata nije kreirao programski alat za automatsko uklanjanje crva sa zaraženog računala.

4. Zaključak

Crv *Eyeveg.F* definiran je kao crv s visokim potencijalom distribucije, što je vidljivo iz velikog broja zaraženih računala u kratkom vremenskom intervalu, te visokim potencijalom mogućeg uskraćivanja računalnih resursa, no unatoč tome, nije destruktivan. Računalo zaraženo ovim crvom postaje sustav daljnjeg širenja zaraze pri čemu smanjuje propusnost mreže. Također, moguća je krađa korisničkih zaporki jer crv ima svojstva *keylogger* programa te preuzimanje kontrole nad računalom što omogućuju svojstva *backdoor* programa.

Korisnicima se preporučuje korištenje antivirusnog programa koji svakako mora imati ažuriranu bazu virusa.

5. Reference

[1] Trendmicro: Wurmark.J
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FWURMARK%2EJ&VSect=P

[2] Sophos: Eyeveg-J
http://www.sophos.com/virusinfo/analyses/w32eyevegf.html

[3] Symantec: Lanieca.A@mm
http://securityresponse.symantec.com/avcenter/venc/data/w32.lanieca.a@mm.html

[4] F-secure: Eyeveg.f
http://www.f-secure.com/v-descs/eyeveg.shtml