HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Sobig.F crva

CCERT-PUBDOC-2003-08-36

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

18.08.2003. uočeno je širenje nove, šeste po redu, inačice Sobig crva nazvane Sobig.F. Kao i njegovi prethodnici, Sobig.F za svoje širenje koristi poruke elektroničke pošte i mrežne dijeljene direktorije.
Sobig koristi tehniku nazvanu *e-mail spoofing*, kojom krivotvori izvornu adresu pošiljatelja poruke. Iz gomile adresa elektroničke pošte pronađenih na zaraženom računalu, nasumce se odabire nekolicina njih i na te adrese se šalju nove zaražene poruke.
Na taj način izaziva se pomutnja među korisnicima, koja otežava pronalaženje zaraženog računala. Ova tehnika također ubrzava širenje crva jer je napadnuti korisnik uvjeren u to da je poruka elektroničke pošte koju dobije od poznate osobe sigurna. Dodatan izvor pomutnje stvaraju i antivirusni programi integrirani u poslužitelje elektroničke pošte, koji prilikom otkrivanja virusa u poruci elektroničke pošte automatski šalju upozorenje na adresu pošiljatelja, koja je u ovom slučaju krivotvorena.
Osim *e-mail spoofing* tehnike, crv prikuplja podatke i o mrežnim dijeljenim direktorijima, na koje zaraženo računalo ima ovlasti pisanja podataka. Iako ovaj podatak upućuje na to da se Sobig-F može širiti i preko mrežnih direktorija, detaljnije analize pokazale su da se zbog propusta u programskom kodu crv ipak ne širi na taj način.
Programski kod crva napisan je tako da se automatski prestaje širiti 10.09.2003.

2. Analiza

Zaražena poruka elektroničke pošte može se prepoznati po naslovu koji je nasumce izabran između sljedećih vrijednosti:

```
Re: Details
Re: Approved
Re: Re: My details
Re: Thank you!
Re: That movie
Re: Wicked screensaver
Re: Your application
Thank you!
Your details
```

Unutar tijela poruke nalazi se rečenica `See the attached file for details` ili `Please see the attached file for details`, koja upućuje korisnika da otvori datoteku koja se nalazi u privitku poruke. Ime datoteke u privitku također se bira nasumce između sljedećih vrijednosti:

```
your_document.pif
document_all.pif
thank_you.pif
your_details.pif
details.pif
document_9446.pif
application.pif
wicked_scr.scr
movie0045.pif
```

Kada korisnik pokrene datoteku u privitku zaražene poruke, Sobig.F se kopira u korijenski direktorij sustava (`C:\Windows` ili `C:\Winnt`), kao datoteka pod imenom `winppr32.exe`. Osim toga, u istom direktoriju kreira se datoteka `winstt32.dat`, a u *Registry* se upisuju ključevi koji osiguravaju pokretanje crva pri svakom ponovnom pokretanju sustava.
Za svoje daljnje širenje crv koristi vlastiti ugrađeni SMTP klijent, a za izvorne i odredišne adrese zaraženih poruka nasumce bira adrese elektroničke pošte pronađene u `.dbx`, `.eml`, `.hlp`, `.htm`, `.html`, `.mht`, `.wab`, `.txt` datotekama na sustavu.
Osim što šalje zaražene poruke elektroničke pošte, Sobig.F u sebi sadrži i listu poslužitelja sa kojih pokušava dohvatiti nove datoteke. Lista sadrži sljedeće poslužitelje:

```
12.232.104.221
12.158.102.205
24.33.66.38
24.197.143.132
24.206.75.137
24.202.91.43
24.210.182.156
61.38.187.59
63.250.82.87
65.92.80.218
65.92.186.145
65.95.193.138
65.93.81.59
65.177.240.194
66.131.207.81
67.9.241.67
67.73.21.6
68.38.159.161
68.50.208.96
218.147.164.29
```

Ovakvo ponašanje ostavlja mogućnost ubacivanja trojanskih konja na sustav, ili u najmanjem slučaju dohvat nadogradnje koja bi ponovno aktivirala prikriveni virus. U trenutku pojavljivanja Sobig.F-a niti jedan od navedenih poslužitelja nije bio aktivan.

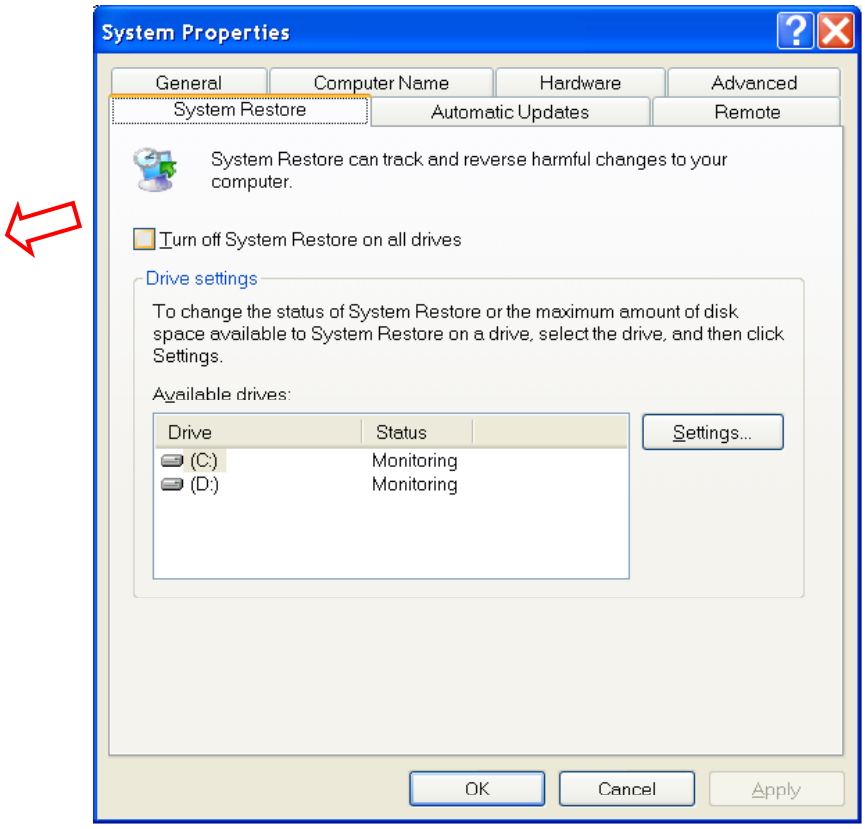
Iako nakon datuma deaktivacije crv prestaje slati zaražene poruke elektroničke pošte, on će prilikom svakog pokretanja operacijskog sustava pokušati dohvatiti programski kod sa nekog od poslužitelja navedenih na listi.

Administratorima se zbog toga preporučuje blokiranje odlaznog mrežnog prometa na UDP portu 8998, te praćenje prometa na portu 123 (NTP protokol), čija bi pojačana aktivnost mogla ukazivati na zaražena računala na mreži. Period između dva NTP upita zaraženog računala iznosi otprilike jedan sat.

3. Uklanjanje

Za automatsko uklanjanje crva potrebno je primijeniti gotove alate, napisane za tu namjenu, koji se mogu dohvatiti sa Web stranica svih većih kompanija koje se bave izradom antivirusnog softvera. Za primjer se može uzeti alat tvrtke Symantec, koji se može dohvatiti sa adrese http://securityresponse.symantec.com/avcenter/venc/data/w32.sobig.f@mm.removal.tool.html. Kao alternativa ovakvim rješenjima, Sobig-F se sljedećim postupkom može ukloniti i ručno.

Prije uklanjanja crva, računalo je potrebno isključiti sa računalne mreže i uključiti ga tek u trenutku u kojem su sva ostala računala na lokalnoj mreži očišćena od Sobig-F crv-a. Korisnicima Microsoft Windows Me i XP operacijskih sustava preporučuje se privremeno isključivanje *System Restore* funkcije (Slika 1), koja je na ovim operacijskim sustavima inicijalno uključena.



Slika 1 Isključivanje System Restore opcije

Zadatak ove funkcije je restauracija oštećenih datoteka na računalu i njenim korištenjem nehotice se može napraviti sigurnosna kopija zaraženih datoteka, čijom restauracijom bi se izazvalo ponovno aktiviranje crva. Dodatan problem predstavlja i činjenica da antivirusne aplikacije nisu u mogućnosti ukloniti viruse iz datoteka pohranjenih u *System Restore* arhivi.

Sljedeći korak je zaustavljanje procesa kojega je crv pokrenuo. Korisnici Windows 95, 98 i ME operacijskih sustava u tu svrhu morati će ponovno pokrenuti operacijski sustav u *Safe Mode* načinu rada. Korisnici Windows NT, 2000 i XP operacijskih sustava proces mogu isključiti u prozoru *Task Manager* aplikacije, do koje se dolazi istovremenim pritiskom na tipke `Ctrl`, `Alt` i `Del`. U listi aktivnih procesa potrebno je pronaći i zaustaviti proces pod imenom `Winppr32.exe`.

Nakon zaustavljanja procesa pod kojim se krije Sobig-F, nekim od antivirusnih alata potrebno je provjeriti sve datoteke na tvrdom disku i obrisati one koje su zaražene. Također je potrebno ukloniti *Registry* ključeve koje je crv kreirao. Unutar ključa

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

potrebno je obrisati vrijednost `"TrayX"="%Windir%\winppr32.exe /sinc"`, dok je unutar ključa

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

potrebno obrisati vrijednost `"TrayX"="%Windir%\winppr32.exe /sinc"`.

Nakon uspješnog uklanjana Sobig-F crva, korisnici Windows XP i Me sustava mogu ponovo uključiti *System Restore* funkciju.

4. Zaključak

Iako na vrlo jednostavan način pokušava zavarati i navesti korisnika na pokretanje zaražene datoteke, Sobig.F se proširio vrlo brzo i u dosad nezabilježenim razmjerima. Imajući na umu da je ovo već šesta po redu inačica Sobig crva, realno je očekivati vrlo skoro pojavljivanje novih inačica, koje biti izvedene tako da rade mnogo veću štetu na zaraženim računalima.