HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza BugBear crva

CCERT-PUBDOC-2002-10-04

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

Bugbear (W32/Bugbear-A, aliasi W32/Bugbear@MM, I-Worm/Keywo, Worm/Tanatos, WORM_NATOSTA.A) je Internet crv koji se širi putem e-mail poruka ili preko lokalnih mreža, odnosno preko dijeljenih mapa. Crv je napisan u MSVC-u (Microsoft Visual C), te zapakiran korištenjem UPX-a (Ultimate Packer for eXecutables), a pogađa isključivo MS Windows operacijske sustave. MacOS i Linux okruženja nisu ugrožena ovim crvom. U pakiranom obliku crv je velik oko 50kB, dok je raspakirana veličina oko 106kB.
Osim masovnog širenja crv sadrži i *backdoor* komponentu, te mogućnost bilježenja korisničkog unosa sa tastature (*engl. keylogging*).
Bugbear se na samom kraju mjeseca rujna i početkom listopada velikom brzinom proširio po klijentskim sustavima širom svijeta i u Hrvatskoj.

2. Način širenja

2.1. Širenje korištenjem e-maila

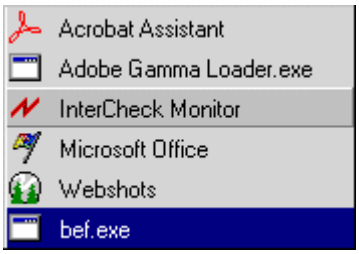
Crv se širi automatskim slanjem na e-mail adrese koje pronađe u korisničkom računalu. Crv se nalazi u privitku poruke (*engl. attachment*) sa slučajno generiranim imenom i sa jednom ili više ekstenzija. Također, naslovi (*engl. subject*) i tijela inficiranih poruka su različiti.
E-mail adrese na koje će se proslijediti crv pronalazi pretraživanjem `.ods`, `.mmf`, `.nch`, `.mbx`, `.eml`, `.tbb`, `.dbx` datoteka, te INBOX-a (Netscape Incoming e-mail baze).
Crv ima mogućnost generiranja lažnih e-mail zaglavlja, tako da ponekad pošiljateljeva e-mail adresa bude zamijenjena proizvoljnom adresom pronađenom na kompromitiranom sustavu.
Tijelo poruka može biti generirano od poruka koje crv pronađe u korisničkoj arhivi na kompromitiranom računalu ili od sadržaja tekstualnih datoteka pronađenih na disku kompromitiranog računala.
Također crv se ne širi na adrese koje sadrže sljedeće stringove: *remove*, *spam*, *undisclosed*, *recipients*, *noreply*, *lyris*, *virus*, *trojan*, *mailer-daemon*, *postmaster@*, *root@*, *nobody@*, *localhost*, *localdomain*, *list*, *talk*, *ticket*, *majordom*. Na taj način crv izbjegava *bouncing*, te druge neželjene pojave.
Tip privitka poruke (*engl. content type*) može biti jedan od sljedećih MIME formata: *image/gif*, *image/jpeg*, *application/octet-stream*, *text/plain*, *text/html*, a sam privitak može imati `.scr`, `.pif` ili `.exe` ekstenziju.
Poruka sa BugBear crvom može sadržati i IFrame napad koji iskorištava sigurnosni nedostatak unutar MS Internet Explorer (Outlook Express) 5.x i 6.0 (opisan u MS Security Bulletin MS01-020). Ukoliko klijentski sustav nema odgovarajuću zakrpu koja eliminira ovaj nedostatak crv se može pokrenuti sam ukoliko korisnik otvori zaraženu e-mail poruku ili ukoliko je samo pregleda kroz *preview pane* unutar Outlook Express-a.

2.2. Širenje preko dijeljenih mapa

Virus pregledava dijeljene mape unutar lokalne mreže, te se pokušava proširiti ukoliko pronađe mogućnost pisanja u korisničke Startup mape na drugim računalima.
To je moguće ukoliko dijeljene mape sadrže sljedeće podmape (obzirom na lokalno računalo s kojeg se mape dijele), te postoji mogućnost pisanja u njih:

```
Win98 : C:\WINDOWS\Start Menu\Programs\Startup\xxx.exe
Win2k : C:\Documents and Settings\%USERNAME%\Start
        Menu\Programs\Startup\xxx.exe
```

Ukoliko se uspije prekopirati na ovaj način, virus se pokreće prilikom sljedećeg podizanja računala.



Slika 1: *Izgled Startup izbornika na kompromitiranom računalu*

3. Promjene na kompromitiranim sustavima

Prilikom pokretanja na računalu crv se kopira u `%WinDir%\%SysDir%` mapu kao `xxxx.EXE`. Efektivno to znači sljedeću putanju na klijentskim sustavima:

```
Win98 : C:\WINDOWS\SYSTEM\xxxx.exe
Win2k : C:\WINNT\SYSTEM32\xxxx.exe
```

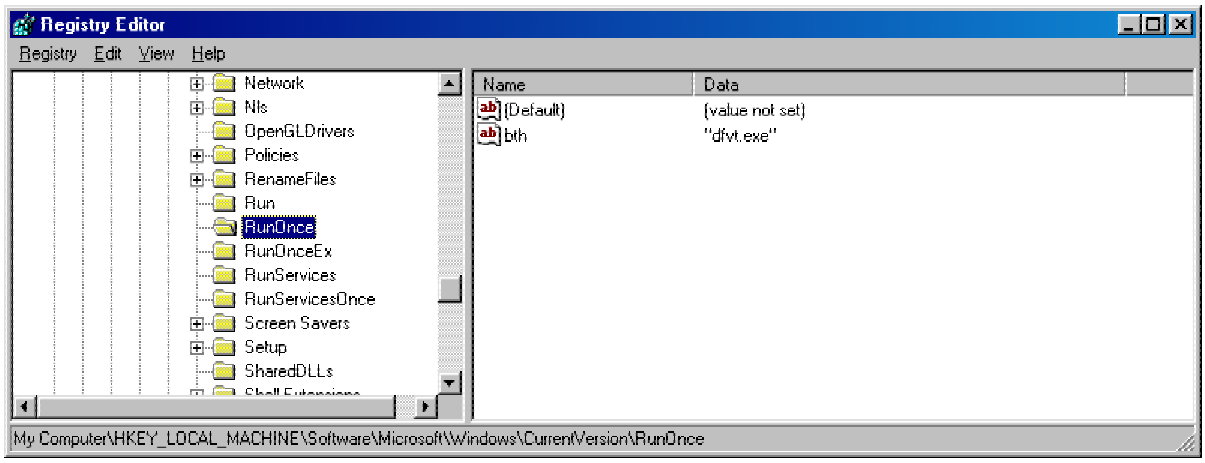
Samo ime izvršne datoteke (`xxxx.exe`) se generira na slučajni način.
Također crv u *registry* datoteku dodaje sljedeću vrijednost:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
"yyyy" = xxxx.exe
```

Na taj način crv osigurava svoje pokretanje prilikom sljedećeg podizanja sustava. Također, iz istog razloga crv se kopira u korisničke *Startup* mape:

```
Win98 : C:\WINDOWS\Start Menu\Programs\Startup\xxx.exe
Win2k : C:\Documents and Settings\%USERNAME%\Start
        Menu\Programs\Startup\xxx.exe
```

Također crv u Windows System mapu umeće `.dll` *backdoor* komponentu slučajno odabranog imena. Osim toga u istoj mapi crv otvara još 2 `.dll` biblioteke slučajno generiranih imena u koje pohranjuje šifrirane podatke. Isto tako u glavnoj Windows mapi kreira dvije `.dat` datoteke, ponovno sa slučajno odabranim imenima.



Slika 2: *RunOnce registry ključ na kompromitiranom računalu*

4. Djelovanje u sustavu

4.1. Daljnja propagacija

Prilikom aktiviranja osnovni proces se grana u nekoliko programskih niti. Neke od njih rukuju širenjem preko lokalne mreže, druge pak služe za slanje zaraženih e-mail poruka, prikupljanje e-mail adresa itd.

4.2. Uklanjanje antivirusnih procesa

Kada je aktivan, crv pokušava ukloniti razne antivirusne procese koji mogu biti pokrenuti na računalu. Popis procesa koje pokušava terminirati je dugačak i uključuje većinu komercijalnih antivirusnih alata. Pri tome se, ovisno o sustavu na kojem je pokrenut (Win9x/Me ili NT/2K/XP), služi različitim rutinama.

4.3. Krađa zaporki

Isto tako, crv ima mogućnost krađe zaporki kroz komponentu za bilježenje unosa s tastature koja bilježi unose i zapisuje ih u datoteku. Nakon toga ta datoteka se šalje na nekoliko e-mail adresa zapisanih u šifriranom tijelu crva. U šifriranom tijelu također su zapisane adrese SMTP poslužitelja kojima se crv služi za slanje e-mail poruka.

4.4. Backdoor komponenta

BugBear crv posjeduje i *backdoor* komponentu koja osluškuje na portu 36794. Ova komponenta napadaču omogućava pristup korisničkom računalu sa udaljenih lokacija uporabom jednostavnog web sučelja. HTML stranice koje omogućavaju prikaz podataka sa korisničkog računala generiraju se dinamički, prilikom postavljanja zahtjeva.
Kroz ovo sučelje napadač ima mogućnost pristupa i svim mrežnim diskovima koji su dostupni sa kompromitiranog računala.
Napadač je u mogućnosti prikupiti važne informacije o diskovnim resursima, mrežnim resursima, ali i o tipu procesora i operativnom sustavu na udaljenom računalu.

4.5. Ispis na mrežnim pisačima

Posljedica izvršavanja virusa jest i slanje ispisa na pisače. Virus pokušava ispisati vlastiti sadržaj na sve mrežne printere kojima može pristupiti. Posljedica toga jest velik broj ispisanih stranica sa svega nekoliko redaka (besmislenog) teksta po stranici.
Na taj način virus može značajno usporiti, pa čak i onemogućiti odvijanje procesa ispisa na mrežnim pisačima unutar lokalne mreže. Korisnički dokumenti mogu zapeti u redu čekanja, pa je u većini slučajeva potrebna administrativna intervencija koja podrazumijeva čišćenje reda dokumenata koji čekaju ispis ili čak resetiranje samog pisača i/ili računala na koje je mrežni pisač povezan.

5. Uklanjanje

Za uklanjanje virusa dovoljno je brisanje njegovih datoteka sa sustava. U mrežnom okruženju potrebno je zaražena računala prije toga izolirati od ostatka mreže, jer u protivnom crv će ponovno pokušati zaraziti računalo.
Postupak ručnog uklanjanja može se izvršiti u sljedećim koracima:

1. Ukloniti sve dijeljene resurse koje omogućavaju pristup korisničkim *Startup* mapama.
2. Napraviti *restart* računala i podignuti ga u *Safe mode* načinu rada. Ukoliko je računalo spojeno na mrežu potrebno ga je prethodno odspojiti.
3. Obrisati sljedeću *registry* vrijednost:
   ```
   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
   "yyyy" = xxxx.exe
   ```
4. Za Win9x/Me obrisati:
   ```
   C:\WINDOWS\Start Menu\Programs\Startup\xxxx.exe
   ```
   za WinNT/2k/XP :

```
C:\Documents and Settings\%USERNAME%\Start
Menu\Programs\Startup\xxxx.exe
```

5. Obrisati sve ostale datoteke koje je postavio virus.
6. Napraviti *restart* računala te instalirati najnoviji skup zakrpi za Internet Explorer (http://www.microsoft.com/windows/ie).
7. Instalirati najnoviju inačicu antivirusnog programa i još jednom pregledati računalo korištenjem antivirusnog alata.

Nakon uklanjanja preporuča se promjena korisničkih imena i/ili zaporki zbog mogućnosti njihove kompromitacije, a također se preporuča postupak detekcije drugih neovlaštenih aktivnosti koje je napadač mogao izvršiti kroz *backdoor* komponentu.