HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Bizex crva

CCERT-PUBDOC-2004-02-60

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

Crv Bizex (aliasi Worm.Win32.Bizex, W32/Bizex.worm, W32/Bizex-A), koji se pojavio se u drugoj polovici veljače 2004. godine, u određenoj mjeri se razlikuje od velikog broja crva koji su se širili ili se još šire Internetom. Ne toliko zbog same tehnologije, koja se temelji na već dulje poznatim sigurnosnim nedostacima unutar Windows operacijskih sustava, odnosno Internet Explorer Web preglednika, nego zbog svoje namjene, odnosno ciljeva.
Za svoje širenje crv koristi ICQ, popularnu *instant messaging* aplikaciju, u kombinaciji sa spomenutim nedostacima u operacijskim sustavima i Internet Explorer Web pregledniku.
Velika je vjerojatnost da je Bizex crv napravljen namjerno, pa čak i po narudžbi , a sve u cilju stjecanja materijalne koristi. Naime, crv se ponaša tako da, nakon što je inficirao ranjivo računalo i pretvorio ga u *zombie*-a koji služi za daljnje širenje crva, nastoji prikupiti povjerljive informacije koje se tiču bankovnih transakcija koje se izvode s kompromitiranog računala.
U nastavku dokumenta biti će detaljno analiziran način širenja crva, sigurnosni nedostaci koje koristi, zlonamjerne akcije koje crv provodi, te će na kraju biti dane i upute za njegovo uklanjanje.

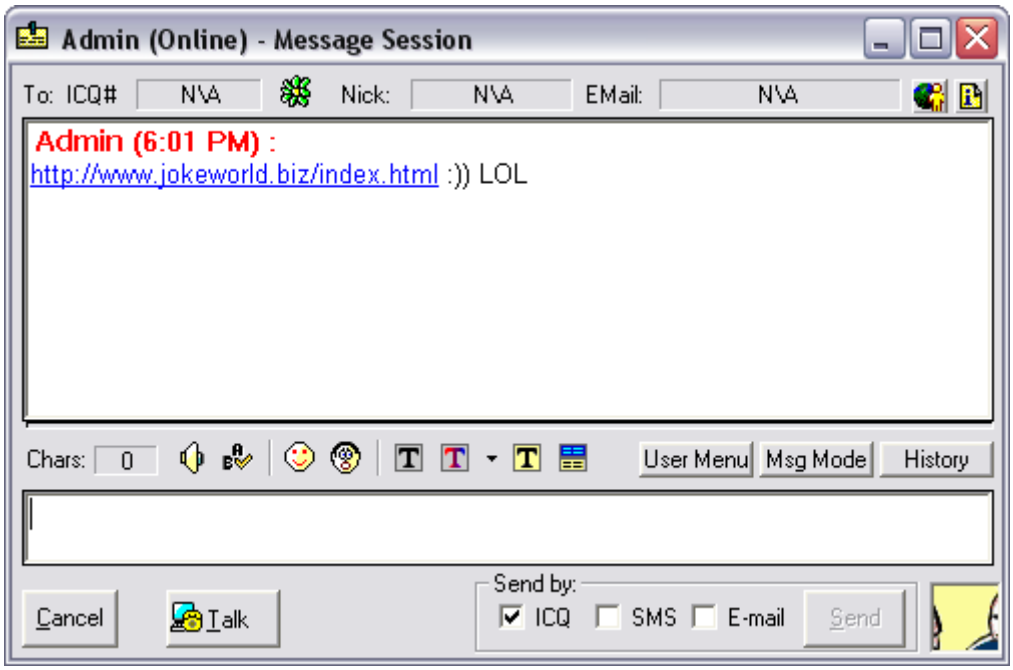
2. Analiza

2.1. Sigurnosni nedostaci

Crv se širi i pogađa isključivo Windows operacijske sustave (Windows 9x, Me, NT, 2000, XP). Za svoje širenje koristi dva već ranije uočena sigurnosna nedostatka na tim sustavima, te sigurnosni nedostatak unutar ICQ *instant messaging* aplikacije.
Prvi nedostatak koji crv koristi jest sigurnosni propust unutar Microsoft VM, virtualnog stroja za izvođenje Java aplikacija. Propust se nalazi u *ByteCode verifier* dijelu VM koda, a zlonamjerni napadač propust može iskoristiti da bi izvršio proizvoljne Java *applete* u sigurnosnom kontekstu korisnika koji je otvorio zlonamjernu web stranicu ili e-mail poruku. Microsoft je još u travnju 2003. objavio odgovarajuću zakrpu. Više informacija o samom nedostatku moguće je pronaći na adresi:
http://support.microsoft.com/default.aspx?scid=kb;en-us;816093.
Drugi nedostatak odnosi se na propust unutar *showhelp()* funkcije unutar Internet Explorer-a, koja napadaču omogućava otvaranje lokalnih `.chm` datoteka. Zakrpe koje ispravljaju ovaj nedostatak također su dostupne. Više informacija o navedenom nedostatku moguće je pronaći na adresama:
http://support.microsoft.com/default.aspx?scid=kb;en-us;811630 i
http://support.microsoft.com/default.aspx?scid=kb;en-us;822925.
Nedostatak unutar ICQ *instant messaging* aplikacije odnosi se na način na koji ICQ zvučne sheme (`.scm` datoteke) pohranjuju `.wav` datoteke u poznate direktorije. Sadržaj tako kreiranih `.wav` datoteka moguće je kontrolirati na zlonamjeran način. Više o tom nedostatku moguće je pronaći na sljedećoj adresi:
http://secunia.com/advisories/10970/.

2.2. Način širenja

Kako je spomenuto, crv za svoje širenje koristi ICQ *instant messaging* aplikaciju. Crv šalje ICQ poruku u kojoj se nalazi URL na Web stranicu (`http://www.jokeworld.xxx/xxx.html`) koja sadrži zlonamjerni sadržaj (Slika 1).



Slika 1: *ICQ poruka koja sadrži URL na zlonamjernu Web stranicu*

Ukoliko ICQ korisnik klikne na taj URL dešava se sljedeće:

1. skida se datoteka imena `meine.scm` duljine 13052 okteta koja predstavlja ICQ zvučnu shemu (engl. *sound scheme*), koja je referencirana u IFRAME tag-u originalne `.html` datoteke.
2. ICQ pohranjuje zvučnu shemu sadržanu u `meine.scm` u datoteku `Startup.wav` na poznatu lokaciju na disku ranjivog računala (`C:\Program Files\ICQ\Sounds`).
3. Originalna .html datoteka iskorištava nedostatak unutar *showhelp()* funkcije kod Internet Explorer-a, čime se izvršava `iefucker.html` datoteka, također sadržana u `meine.scm` datoteci.
4. Izvršavanjem `iefucker.html` datoteke stvara se `WinUpdate.exe` datoteka duljine 4650 okteta u `%Startup%` direktoriju klijentskog računala (`C:\Documents and Settings\All Users\Start Menu\Programs\Startup` na NT/2000/XP sustavima, odnosno `C:\Windows\Start Menu\Programs\Startup` na Windows 9x/Me sustavima).
5. Prilikom ponovnog pokretanja računala `WinUpdate.exe` datoteka se izvršava te skida `aptgetupd.exe` datoteku, koja predstavlja glavnu komponentu Bizex crva u `%Temp%` direktorij (`C:\Windows\TEMP` na 9x/Me sustavima, `C:\WINNT\Temp` na NT/2000, te `C:\Document and Settings\<UserName>\Local Settings\Temp` na XP sustavima).
   Datoteka `aptgetupd.exe` se izvršava, te se kopira u `%System%\sysmon` direktorij (`C:\Windows\System\sysmon` na 9x/Me sustavima, `C:\Winnt\System32\sysmon` na NT/2000 sustavima, te `C:\Windows\System32\sysmon` na XP sustavima) pod imenom `sysmon.exe`. Također se u *registry* datoteci u ključ:
   `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
   dodaje vrijednost `"sysmon"="%System%\sysmon\sysmon.exe"`, čime se osigurava pokretanje komponente prilikom svakog pokretanja operacijskog sustava.

2.3. Funkcionalnost

Nakon što je glavna komponenta (`sysmon.exe`) osigurala vlastito pokretanje izvršavaju se koraci koji osiguravaju osnovnu funkcionalnost crva:

1. U `%System%` direktoriju stvaraju se sljedeće dinamičke biblioteke:

```
ICQ2003Decrypt.dll
icq_socket.dll
```

```
java32.dll
javaext.dll
```

Dinamičke biblioteke `ICQ2003Decrypt.dll` i `icq_socket.dll` služe za daljnje širenje, odnosno propagiranje, crva preko ICQ-a slanjem poruka s malicioznim URL-om svim osobama s kontakt liste korisnika zaraženog računala. Biblioteke `java32.dll` i `javaext.dll` služe pak za praćenje rada korisnika i bilježenje njegovih akcija u odgovarajuće datoteke.

2. Također se u `%System%\sysmon\` direktoriju stvaraju sljedeće log datoteke:

```
%System%\sysmon\~post.log
%System%\sysmon\~key.log
%System%\sysmon\~pass.log
```

U datoteke bilježe se određene korisničke akcije.

Glavna funkcionalnost Bizex crva jest bilježenje povjerljivih informacija o financijskim transakcijama korisnika. Crv koristi mogućnost presretanja informacija koje se prenose šifrirane, korištenjem HTTPS protokola.

Crv prati sljedeće financijske servise:

- Acceso a Banca por Internet,
- Accueil Bred.fr,
- Espace Bred.fr,
- American Express UK - Personal Finance,
- Banamex.com,
- baNK,
- Banque,
- Banque en ligne,
- Barclaycard Merchant Services,
- Collegamento a Scrigno,
- Commercial Electronic Office Sign On,
- Credit Lyonnais interacti,
- CyberMUT,
- E*TRADE Log On,
- e-gold Account Access,
- Home Page Banca Intesa,
- LloydsTSB online – Welcome,
- Merchant Administration,
- Page d'accueil ,
- Secure User Area,
- SUNCORP METWAY,
- Tous les produits et services,
- VeriSign Partner Manager,
- VeriSign Personal Trust Service i
- Wells Fargo - Small Business Home Page.

Osim toga crv prati HTTPS sjednice vezane uz:

- login.yahoo.com i
- .passport.

Svi podaci se bilježe u `.log` datoteke koje se zatim šalju unaprijed definiranom Web poslužitelju korištenjem FTP protokola.

3. Uklanjanje

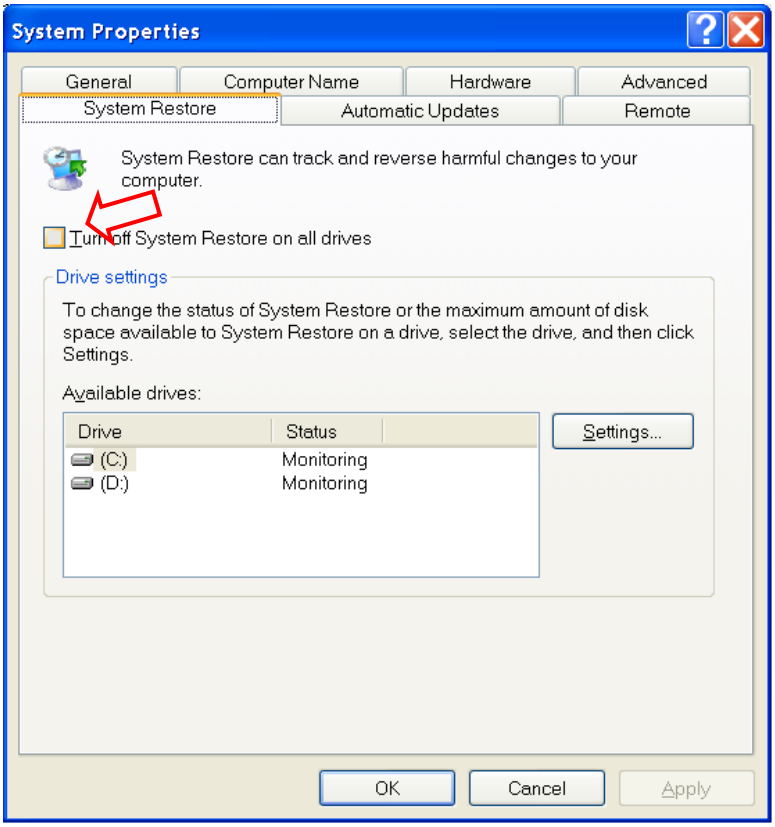
Crv se može ukloniti korištenjem antivirusnih alata, za što postoje preporuke na stranicama proizvođača (http://www.sophos.com, http://www.symantec.com, http://www.kaspersky.com, http://www.mcafee.com i drugi). Također, crv se može ukloniti i ručno na sljedeći način:

1. Instalirati sve sigurnosne zakrpe koje je objavio Microsoft na svojim stranicama. Zakrpe se mogu instalirati korištenjem sljedećeg URL-a http://windowsupdate.microsoft.com.

2. Potrebno je terminirati zlonamjernu `sysmon.exe` aplikaciju. Na NT/2000/XP sustavima to je moguće korištenjem *Task Manager* aplikacije, dok je na 9x/Me sustavima operacijski sustav potrebno pokrenuti u tzv. *Safe mode* načinu rada.
3. Iz *registry* ključa:
   `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
   potrebno je obrisati vrijednost `"sysmon"="%System%\sysmon\sysmon.exe"`.
4. Obrisati sve datoteke koje je koristio crv:

```
%System%\ICQ2003Decrypt.dll
%System%\icq_socket.dll
%System%\java32.dll
%System%\javaext.dll
%System%\sysmon\sysmon.exe
%System%\sysmon\~post.log
%System%\sysmon\~key.log
%System%\sysmon\~pass.log
```

Korisnicima Microsoft Windows Me i XP operacijskih sustava se također preporučuje privremeno isključivanje *System Restore* funkcije (Slika 2), koja je na tim operacijskim sustavima inicijalno uključena.
Zadatak ove funkcije je restauracija oštećenih datoteka na računalu i njenim korištenjem nehotice se može napraviti sigurnosna kopija zaraženih datoteka, čijom restauracijom bi se moglo izazvati ponovno aktiviranje crva. Dodatan problem predstavlja i činjenica da antivirusne aplikacije nisu u mogućnosti ukloniti maliciozne programe iz datoteka pohranjenih u *System Restore* arhivi.
Po uklanjanju crva *System Restore* funkciju je moguće ponovno aktivirati.



Slika 2: *Isključivanje System Restore opcije*

4. Zaključak

Bizex crv se prilično brzo počeo širiti koristeći ranjivosti u Internet Explorer-u i ICQ *instant messaging* programu. Širenje crva, međutim, također je brzo obuzdano zatvaranjem zlonamjerne Web stranice. Može se zaključiti da crv nije nanio neku veću materijalnu štetu, no ponovno valja istaknuti da je instalacija objavljenih sigurnosnih zakrpi i dalje jedan od najvažnijih aspekata sigurnosti.

Vrlo često se događa da crvi za svoje propagiranje koriste sigurnosne nedostatke koji su trebali i mogli biti davno ispravljeni, kao što je slučaj i kod Bizex crva.

Obzirom na ponašanje Bizex crva, odnosno na njegovu funkcionalnost, može se uočiti da taj crv nije proizvod nekog studenta željnog dokazivanja, već da je nastao ciljano, pa možda i prema narudžbi, u cilju otkrivanja osjetljivih financijskih informacija, odnosno direktne materijalne koristi. Za očekivati je da će se u budućnosti ovakvi crvi pojavljivati još češće, pogotovo zato što sve više ljudi svoja računala koristi i za obavljanje financijskih transakcija. Zbog toga je izuzetno važno da se korisnici pridržavaju osnovnih sigurnosnih pravila.

5. Reference

1. Symantec, http://securityresponse.symantec.com/avcenter/venc/data/w32.bizex.worm.html.
2. Sophos, http://www.sophos.com/virusinfo/analyses/w32bizexa.html.
3. F-Secure, http://www.f-secure.com/v-descs/bizex.shtml.