HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza IRAQ crva

CCERT-PUBDOC-2003-01-01

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.

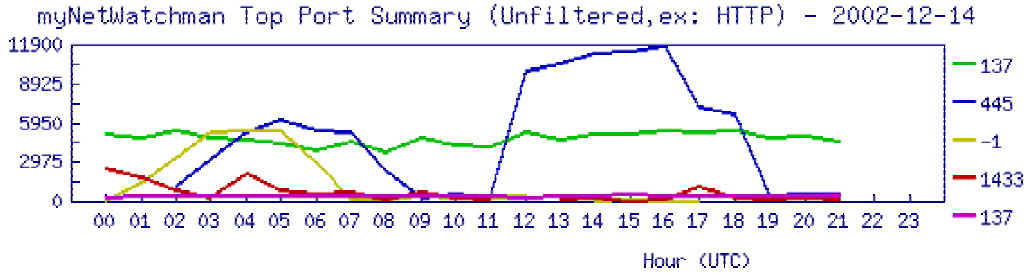
CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

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

14. listopada.2002. godine oko 11:00 sati detektiran je novi crv pod imenom `Iraq Worm`, čije je maliciozno djelovanje usmjereno prema Windows 2000 i Windows XP operacijskim sustavima.
Provedene analize pokazale su da se `Iraq Worm` crv širi isključivo putem TCP/445 porta, koji je kod Windows 2000/XP sustava povezan s SMB protokolom.
SMB (eng. *Service Message Block*) protokol, originalno je razvijen od tvrtke IBM 1985. godine, da bi kasnije bio preuzet je od strane Microsofta koji je SMB protokol iskoristio kao temeljni protokol za komunikaciju između Windows računala.
Kod ranijih implementacija Windows operacijskih sustava (Win95/Win98, WinNT), SMB komunikacija između računala odvijala se putem NBT (eng. *NetBIOS over TCP/IP*) protokola, koji je koristio TCP port 139 te UDP portove 137 i 138.
Kod Windows 2000 i Windows XP operacijskih ustava dodana je nova mogućnost koja omogućuje SMB komunikaciju direktno putem TCP/IP protokola (bez potrebe za NetBIOS-om). Komunikacija se u ovom slučaju odvija se preko TCP/445 porta koji je upravo meta `Iraq Worm` crva.
Grafički prikaz *myNetWatchman* sustava, potvrđuje vidljivi porast mrežnog prometa usmjerenog prema TCP/445 portu, koji je posljedica Iraq Worm crva.



Slika 1.1: *Vidljiv porast mrežnog prometa usmjerenog prema TCP/445 portu*

Analizom nekoliko kompromitiranih sustava utvrđeno je da se crv u većini slučajeva kopira u `C:\WINNT\system32` direktorij pod imenom `iraq_oil.exe`.
Također se pokazalo da u iznimnim situacijama crv koristi i druga slučajno odabrana imena i direktorije kako bi prikrio svoje djelovanje.

2. Analiza crva

Provedene analize pokazale su da `Iraq Worm` crv napada isključivo Windows 2000 i Windows XP operacijske sustave, budući da se crv širi putem TCP/445 porta i iskorištava `IPC$`, `ADMIN$`, `C$` i ostale dijeljene resurse koji ne postoje kod ranijih inačica Windows operacijskih sustava.
Za odabir ciljnih računala crv koristi pseudo-slučajni generator IP adresa, koji se bazira na `rand()` programskoj funkciji.
Sam mehanizam generiranja IP adresa implementiran je prilično loše. Spomenuta funkcija kao rezultat vraća vrijednosti između 0 i 0x7FFF, na temelju čega se pokazalo da generirane IP adrese nisu u potpunosti slučajne.
Budući da je svaka IP adresa velika 32 okteta, ovim načinom samo će 30 okteta biti potpuno slučajno. Na mjestu drugog i četvrtog okteta uvijek će se nalaziti vrijednosti 0x7F što će suziti broj IP adresa koje je moguće generirati.
Na temelju gore iznesene činjenice može se pokazati da IP adrese koje na mjestu drugog ili četvrtog okteta sadrže vrijednosti u području između 128-255 (adrese x.128-255.x.128-255) nikada neće biti napadnute ovim crvom, s obzirom na način na koji se generiraju IP adrese.
Dodatni pokazatelj površne implementacije crva vezan je činjenicu što se generirane IP adrese uopće ne provjeravaju te se pokušavaju napasti adrese koje teoretski nemaju smisla.
Npr. `Iraq Worm` crv će, osim regularnih IP adresa, ravnopravno pokušati inficirati i IP adrese kao što su 127.0.0.1 (lokalno računalo), adrese koje počinju s 0 (0.x.x.x) ili 255 (255.x.x.x), što je besmisleno budući da navedene adrese imaju posebno značenje.

Nakon što je generiran odgovarajući broj "slučajnih" IP adresa, crv se pokušava spojiti na TCP/445 SMB port, kako bi se utvrdilo da li je servis omogućen. U nastavku su priloženi log zapisi koji na to upućuju:

```
Raw tcp/445 probe to see if service available
1 0.000000    IraqiWorm  2648    NxtVictm   445      62     TCP      2648 >
445 [SYN] Seq=2178295388 Ack=0 Win=16384 Len=0
2 0.410328    NxtVictm   445    IraqiWorm   2648     62     TCP      445 >
2648 [SYN, ACK] Seq=1037301398 Ack=2178295389 Win=17520 Len=0
3 0.410402    IraqiWorm  2648    NxtVictm   445      54     TCP      2648 >
445 [ACK] Seq=2178295389 Ack=1037301399 Win=17520 Len=0
4 0.410650    IraqiWorm  2648    NxtVictm   445      54     TCP      2648 >
445 [FIN, ACK] Seq=2178295389 Ack=1037301399 Win=17520 Len=0
5 0.415573    IraqiWorm  2656    NxtVictm   445      62     TCP      2656 >
445 [SYN] Seq=2178795847 Ack=0 Win=16384 Len=0
6 0.570727    NxtVictm   445    IraqiWorm   2648     60     TCP      445 >
2648 [FIN, ACK] Seq=1037301399 Ack=2178295390 Win=17520 Len=0
7 0.570877    IraqiWorm  2648    NxtVictm   445      54     TCP      2648 >
445 [ACK] Seq=2178295390 Ack=1037301400 Win=17520 Len=0
8 0.596340    NxtVictm   445    IraqiWorm   2656     62     TCP      445 >
2656 [SYN, ACK] Seq=1037396301 Ack=2178795848 Win=17520 Len=0
9 0.596449    IraqiWorm  2656    NxtVictm   445      54     TCP      2656 >
445 [ACK] Seq=2178795848 Ack=1037396302 Win=17520 Len=0
Create Server Message Block - SMB Connection
```

Spajanje na sam port 445 implementirano je korištenjem `connect()` programske funkcije, koja čeka točno pet sekundi kako bi se utvrdilo da li je moguće spajanje na spomenuti port.
U slučaju uspješnog spajanja na 445 port, uslijediti će detaljnija ispitivanja identificiranog sustava pomoću *Win32* `net` programskih funkcija te pokušaj spajanja na `IPC$` dijeljenu mapu putem NULL sesije.
NULL sesija korisniku omogućuje anonimni pristup udaljenom računalu, kojim je moguće doći do korisnih informacija o udaljenom sustavu (dijeljeni resursi, korisnički računi i grupe, podaci o domeni i sl.). Slijede log zapisi koji to potvrđuju:

```
Create Null Session to IPC$
     16 1.037551    IraqiWorm  2656    NxtVictm   445      152    SMB
Tree Connect AndX Request, Path: \\166.82.152.112\IPC$
     17 1.192369    NxtVictm   445    IraqiWorm   2656     114    SMB
Tree Connect AndX Response
```

Ukoliko je NULL sesija uspostavljena s udaljenim računalom, crv će ovu mogućnost iskoristiti za dolazak do liste korisničkih računa na sustavu. Log zapisi koji upućuju na dolazak do liste korisnika sustava dan je u nastavku:

```
List usernames in domain..
     30 1.994557     IraqiWorm   2656     NxtVictm    445        198     SAMR
EnumDomainUsers request
     31 2.139707     NxtVictm    445     IraqiWorm    2656       302     SAMR
EnumDomainUsers reply
```

Sve korisničke račune otkrivene ovim putem crv će pokušati kompromitirati prilično jednostavnom *brute-force* metodom. Metoda se sastoji u uzastopnim pokušajima spajanja, sa sljedećim korisničkim zaporkama:

- bez zaporke
- admin
- root
- 111
- 123
- 1234

- 123456
- 654321
- 1
- !@#$
- asdf
- asdfgh
- !@#$%
- !@#$%^
- !@#$%^&
- !@#$%^&*
- server

Ukoliko se ostvari pristup sustavu s nekom od navedenih zaporki, crv se pokušava kopirati na udaljeni sustav. Ime pod kojim će crv biti pohranjen na udaljenom sustavu generira se korištenjem `GetModuleHandle()` programskom funkcijom.
Samo kopiranje provodi se zadavanjem sljedeće naredbe:

```
COPY myFileName \\remoteIP\\Admin$\system32\iraq_oil.exe
COPY myFileName \\remoteIP\\c$\winnt\system32\iraq_oil.exe
```

Slijede log zapisi koji to potvrđuju:

```
Push worm.
69 4.445819    IraqiWorm  2660    NxtVictm   445      188    SMB      NT
Create AndX Request, Path: \system32\iraq_oil.exe
70 4.587690    NxtVictm   445    IraqiWorm   2660     193    SMB      NT
Create AndX Response, FID: 0x4001
71 4.606496    IraqiWorm  2660    NxtVictm   445      142    SMB
Transaction2 Request SET_FILE_INFORMATION, FID: 0x4001
72 4.757555    NxtVictm   445    IraqiWorm   2660     118    SMB
Transaction2 Response SET_FILE_INFORMATION
73 4.772114    IraqiWorm  2660    NxtVictm   445      1514   SMB      Write
AndX Request, FID: 0x4001
```

Nakon što je crv kopiran na udaljeni sustav, slijedi postupak kojim se dolazi do točnog vremena na udaljenom sustavu kako bi se omogućilo njegovo pokretanje putem at naredbe.
Log zapisi:

```
Get current Time-of-Day (TOD) from remote
63 4.062821    IraqiWorm  2660    NxtVictm   445      216    SRVSVC
NetrRemoteTOD request
64 4.193736    NxtVictm   445    IraqiWorm   2660     194    SRVSVC
NetrRemoteTOD reply
65 4.194035    IraqiWorm  2660    NxtVictm   445      99     SMB      Close
Request, FID: 0x4000
66 4.315161    NxtVictm   445    IraqiWorm   2660     93     SMB      Close
Response
```

Nakon što je poznato točno vrijeme na udaljenom sustavu, crv definira novi zadatak (eng. *job*), koji će ga pokrenuti nekoliko minuta nakon infekcije sustava.
Program `iraq_oil.exe` statički je vezan za `KERNEL32.dll`, `MPR.DLL` i `WSOCK32.dll` datoteke, a nakon pokretanja dinamički učitava `NETAPI32.dll` biblioteku putem `LoadLibrary` funkcije.
Detaljne analize `Iraq Worm` crva pokazale su da kompletni postupak identifikacije ranjivog sustava zajedno s njegovom infekcijom traje svega oko petnaestak sekundi.

3. Metode zaštite

Najpouzdanija metoda zaštite od `Iraq Worm` crva, i njemu sličnih, je blokiranje TCP/445 porta i to ili na vatrozidu (ukoliko isti postoji) ili na samoj mrežnoj opremi. Osim TCP/445 porta svakako se preporučuje i blokiranje TCP/139, UDP/137 i UDP/138 portova, budući da imaju identičan značaj.
Ovim putem onemogućit će se neautorizirani pristup Windows dijeljenim resursima s javnog Interneta čime se otklanja velik broj problema slične prirode.
S korisničke strane preporučuje se korištenje što "jačih" zaporki kako bi iste bile imune na različite tipove *brute-force* napada. Zaporke koje se sastoje od kombinacije malih i velikih slova, brojeva i specijalnih znakova trebale bi biti dovoljno kompleksne da sustave učine imunima na spomenuti tip napada.
Windows operacijski sustavi dodatno se mogu zaštititi onemogućavanjem NULL sesija, što je moguće postići ili uređivanjem lokalne sigurnosne politike sustava ili uređivanjem Windows *registry*-a.
Kod Win2000 i WinXP sustava, NULL sesije moguće je onemogućiti uređivanjem lokalne sigurnosne politike (*Administrative Tools -> Local Security Settings)*.
U sljedećoj tablici prikazani su parametri koje je potrebno modificirati zajedno s pripadajućim vrijednostima.

Naziv parametra	Vrijednost
Windows XP	
Do not allow anonymous enumeration of SAM accounts	Enable
Do not allow anonymous enumeration of SAM accounts and shares	Enable
Windows 2000	
Additional restrictions of anonymous connections	No access without explicit anonymous permissions

Tablica 3.1: *Onemogućavanje NULL sesija kod Win2000 i WinXP sustava*

Kod Windows NT sustava jedini način da se onemoguće NULL sesije je uređivanje *registry*-a.

4. Zaključak

Iako način na koji `Iraq Worm` crv inficira udaljena računala izgleda prilično trivijalno s obzirom na korištene zaporke, dosadašnja iskustva pokazala su da se crv širi vrlo velikom brzinom. U svrhu zaštite korisnicima i administratorima preporučuje se provođenje preventivnih mjera opisanih u prethodnom poglavlju (3).