HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza CodeRed.F crva

CCERT-PUBDOC-2003-03-10

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

11.4.2003. otkrivena je nova varijanta CodeRed II crva pod nazivom CodeRed.F. Kao i njegovi prethodnici, crv napada Microsoft IIS poslužitelje, koristeći identičan sigurnosni propust koji uzrokuje prepisivanje spremnika. Izmjene u programskom kodu u odnosu na prethodnu inačicu su minimalne i ponašanje crva je praktički isto. Nakon infekcije CodeRed.F crvom, na zaraženom računalu ostaje otvoren *Backdoor* koji neovlaštenim korisnicima omogućuje kontrolu nad poslužiteljem. Budući da je na većini poslužitelja uklonjen spomenuti sigurnosni propust, ne očekuje se širenje u većim razmjerima, kao što je to bio slučaj sa originalnim CodeRed II crvom.

2. Analiza rada

2.1. Širenje crva

Crv se širi instalirajući se na nasumično odabrana računala, koristeći propust u datoteci `idq.dll` Microsoftovog IIS poslužitelja.

Kada crv dospije na zaraženo računalo, pokreće inicijalizacijsku funkciju koja pregledava nasumce odabrane IP adrese u potrazi za ostalim IIS poslužiteljima. Algoritam za nasumično odabiranje IP adresa dizajniran je tako da je širenje crva vjerojatnije na računala koja se nalaze u blizini zaraženog poslužitelja. Nakon tri stotine pokušaja spajanja na udaljena računala ili vremenskog perioda od 24 sata, računalo će se resetirati i crv će se prestati širiti. Za vrijeme pokušaja širenja na ostala računala, crv će na računalu na kojemu je pokrenut, otvoriti *Backdoor* koji neovlaštenom korisniku omogućuje udaljeno izvršavanje naredbi.

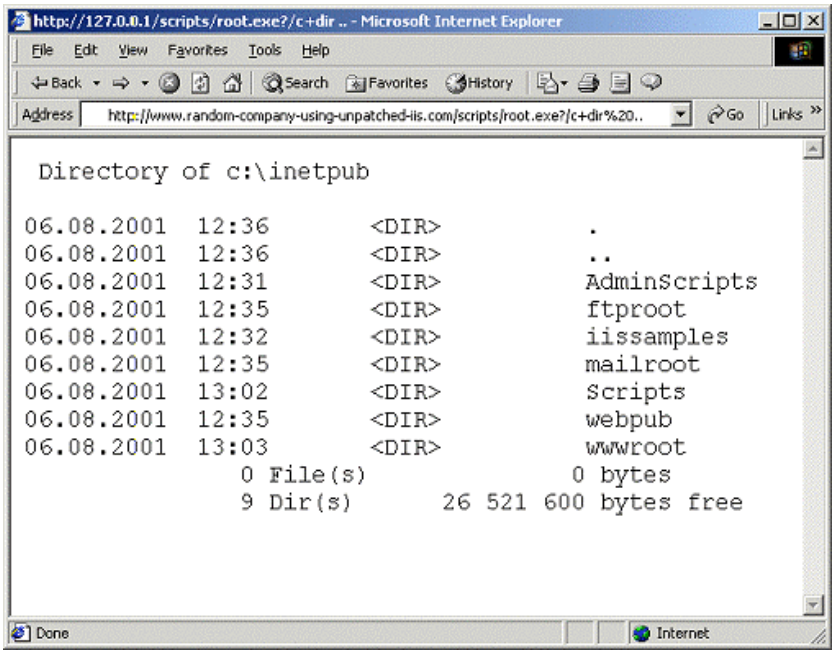
Zanimljivo je da je programski kod crva dizajniran je tako da se agresivnije širi na kineskim računalima tj. svim računalima koja za glavni jezik na sustavu imaju podešen kineski. U slučaju da crv naiđe na računalo sa podešenim kineskim jezikom izvršiti će šest stotina pokušaja daljnjeg širenja, a vremenski period za širenje biti će povećan na 48 sati. Bez obzira na prestanak širenja virusa, trojanski dio koda ostaje aktivan tj. *backdoor* će i dalje postojati.

2.2. Trojanski dio kôda

Gore opisani dio koda ne razlikuje se mnogo od originalnog CodeRed crva. Ono što je specifično za CodeRed II i CodeRed.F modifikacije je da otvaraju *Backdoor* koji bilo kojem neovlaštenom korisniku omogućuje pokretanje proizvoljnog koda sa ovlastima administratora na zaraženom računalu.

Prilikom pokretanja, trojanski dio koda isključuje System File Checker funkcionalnost u Windows operacijskom sustavu, čime je onemogućena provjera integriteta sistemskih datoteka.

Standardni Windows naredbeni interpreter `cmd.exe` kopira se u `scripts` direktorij na Web poslužitelju pod imenom `root.exe`. Na taj način, neovlašteni korisnik putem Web preglednika može pokrenuti bilo koju naredbu na računalu. *Slika 1* prikazuje prozor Internet Explorer-a pomoću kojega je na udaljenom računalu pokrenuta dir naredba.



Slika 1 Udaljeno pokretanje naredbi na zaraženom računalu

U korijenski direktorij IIS poslužitelja dodaju se dva nova direktorija /c i /d koji pokazuju na c:\ i d:\ korijenske direktorije na sustavu. Na taj način korisnicima je dostupna i originalna `cmd.exe` naredba.

Trojanski dio koda radi sljedeće izmjene u Windows Registry-u:

U ključu `HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\WinLogon`, vrijednost `SFCDisable` postavlja se na `0xffffff9d`, što isključuje provjeru integriteta datoteka.

Ključevima `'SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\Scripts'` i `'SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\VirtualRoots\MSADC'` pridijeljene su vrijednosti 217, a u ključ `'SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\VirtualRoots\'` upisuju se vrijednosti c i d, što omogućuje pristup sistemskim diskovima c i d putem Web poslužitelja.

3. Uklanjanje crva

Većina tvrtki koje se bave razvojem antivirusnih programa (Sophos, Symantec...) napravile su odgovarajuće alate za uklanjanje CodeRed II crva. Zbog identičnog načina rada, isti alati mogu se primijeniti i za uklanjanje CodeRed.F crva. Crv se može ukloniti i ručno u nekoliko jednostavnih koraka.

3.1. Uklanjanje propusta u IIS poslužitelju

Prije uklanjanja crva potrebno je instalirati Microsoft-ovu zakrpu (MS01-033) za IIS poslužitelj, kako bi se spriječila mogućnost ponovne zaraze. Zakrpa se može pronaći na adresi http://www.misrosoft.com/technet/security/bulletin/MS01-033.asp. Ovaj problem rješava i kumulativna zakrpa za IIS poslužitelj pod oznakom MS01-044 (http://www.microsoft.com/technet/security/bulletin/MS01-044.asp).

3.2. Brisanje kreiranih datoteka

Nakon instalacije zakrpi potrebno je u Task Manager-u zaustaviti sve procese koje je prilikom inicijalizacije pokrenuo crv. CodeRed se prikriva pod procesom `Explorer.exe`. Budući da je na operacijskom sustavu već pokrenut legitiman proces sa istim imenom, potrebno je utvrditi koji od ta dva procesa je stvarno CodeRed crv. To se lako može utvrditi po broju niti (engl. *Threads*) koje proces

ima. Proces koji ima samo jednu nit predstavlja CodeRed, dok legitiman `Explorer.exe` redovito ima više niti.
Nakon uspješnog zaustavljanja procesa, potrebno je izbrisati `Explorer.exe` datoteke koje je CodeRed kreirao na sustavu. Datoteke se nalaze u korijenskom direktoriju C: diska i D: diska ukoliko isti postoji, te posjeduju `hidden`, `system` i `read-only` atribute. U naredbenom retku portebno je upisati sljedeće naredbe kako bi se datoteke obrisale:

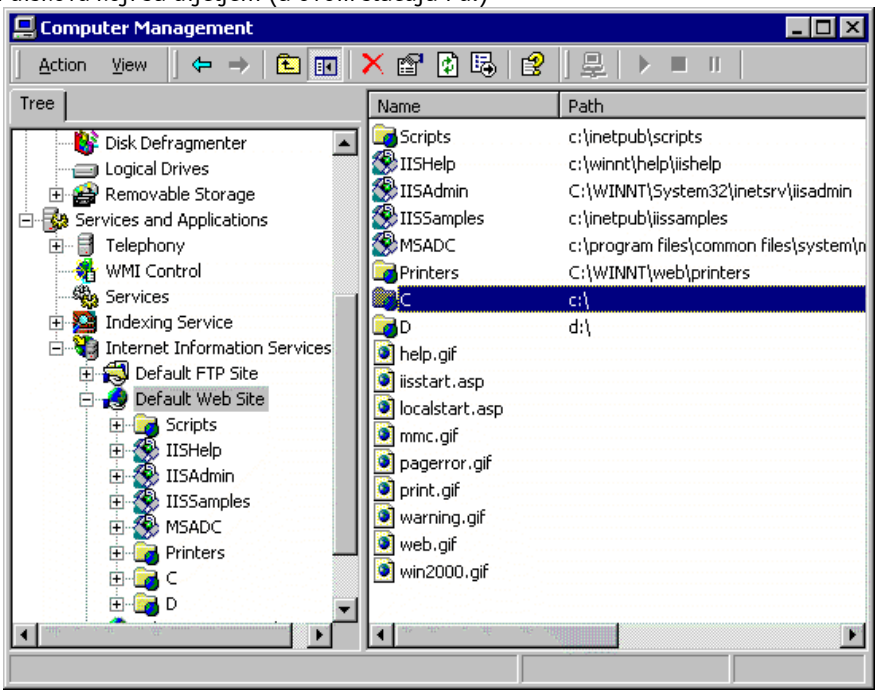
```
Cd c:\
Attrib -h -s -r explorer.exe
Del explorer.exe
```

Iste naredbe potrebno je ponoviti i za datoteku koja se nalazi na d: disku.
Osim izvršnih datoteka koje predstavljaju CodeRed crv, brišu se i kopije `root.exe` datoteke koje je crv smjestio na sljedeća mjesta (nije nužno postojanje svih datoteka):

```
C:\Inetpub\Scripts\Root.exe
D:\ Inetpub\Scripts\Root.exe
C:\Progra~1\Common~1\System\MSADC\Root.exe
D:\Progra~1\Common~1\System\MSADC\Root.exe
```

3.3. Brisanje dijeljenih direktorija na Web poslužitelju

Pomoću Computer Manager-a uklanjaju se svi dijeljeni direktoriji, koje je CodeRed kreirao na Web poslužitelju. U lijevom dijelu prozora potrebno je odabrati `\Computer Management (local)\Services and Applications\Default Web Site`. Sa liste na lijevoj strani Computer Management prozora (*Slika 2*) potrebno je obrisati dijeljenje C: diska i eventualno ostalih sistemskih diskova koji su dijeljeni (u ovom slučaju i d:)



Slika 2 Computer Management prozor

3.4. Izmjena Windows Registry-a

Posljednji korak u uklanjanju crva je brisanje Registry zapisa koje je kreirao. Budući da neispravne izmjene u Registry-u mogu rezultirati gubitkom podataka i problema sa sustavom, preporučuje se napraviti sigurnosnu kopiju prije bilo kakvih izmjena, kao što je i mijenjanje samo onih ključeva koji će biti spomenuti u tekstu koji slijedi.

Registry se mijenja pomoću `regedit` programa (slika), koji sa lijeve strane ima navigaciju do pojedinih ključeva, dok su sa desne strane izlistane vrijednosti ključeva. U navigacijskom prozoru potrebno je doći do `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots` ključa, koji ima nekoliko vrijednosti. Dvije vrijednosti je kreirao CodeRed crv i njih je potrebno o brisati , dok je ostale vrijednosti potrebno samo izmijeniti. Brišu se vrijednosti /C i /D, dok je kod vrijednosti /MSADC i /Scripts broj 217 potrebno zamijeniti sa brojem 201.

Na svim sustavima osim Windows 2000 potrebno je još izmijeniti ključ `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\WinLogn`, u čiji parametar `SFCDisable` se umjesto postojećeg zapisa upisuje broj nula. Postupak uklanjanja potrebno je završiti ponovnim pokretanjem računala.

4. Zaključak

U gornjem tekstu je opisan rad CodeRed.F crva i postupak koji ga u potpunosti uklanja sa zaraženog sustava. Budući da je za cijelo vrijeme postojanja crva na sustavu bio otvoren *backdoor*, vrlo je teško utvrditi da li je sustav bio izložen napadu tj. da li su se na njemu odvijale neke neovlaštene aktivnosti. Ukoliko postoji bilo kakva sumnja u takve aktivnosti, preporučuje se reinstalacija sustava.