HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza MS Blast i Welchia crva

CCERT-PUBDOC-2003-08-33

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

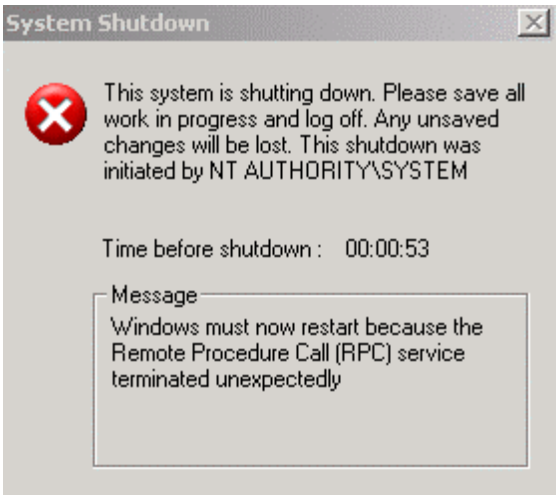
Sukladno očekivanjima, vrlo brzo nakon otkrivanja sigurnosnog propusta u implementaciji RPC sučelja na Microsoftovim operacijskim sustavima (ranjivost MS03-026), pojavile su se i prve inačice crva koje iskorištavaju navedeni propust. Njihovo vrlo brzo širenje opravdalo je bojazni od velikog sigurnosnog rizika koji su predstavljali pronađeni sigurnosni propusti. Širenje MsBlast i Welchia crva otkrilo je vrlo lošu ili nikakvu politiku nadogradnje sigurnosnim zakrpama u mnogim ustanovama i upozorilo na ozbiljnost ovakvih sigurnosnih propusta.

2. MSBlast crv

MSBlast, poznat i pod imenima Blaster, Lovesan ili jednostavno RPC DCOM crv, prvi je u nizu crva koji koriste sigurnosni propust u RPC DCOM sučelju. Budući da njegovo širenje nije uvjetovano interakcijom korisnika, niti ga je moguće zaustaviti antivirusnim alatima, MSBlast je zarazio vrlo velik broj računala u kratkom vremenskom razdoblju, uzrokujući svojim širenjem napad uskraćivanjem računalnih resursa na ranjivim računalima.
Iako je najveći broj zaraženih računala pripadao kućnim korisnicima, koji redovito ne nadograđuju svoja računala sigurnosnim zakrpama, ovaj crv je zarazio i pozamašan broj računala u mnogim velikim kompanijama, što je rezultiralo znatnom materijalnom štetom.

2.1. Analiza

MS Blast napada Windows 2000 i Windows XP računala, pri čemu svaka nova kopija napada isključivo jedan od navedenih operacijskih sustava. Statistički gledano, jedna od pet inačica crva napasti će Windows XP računalo, dok će se preostale četiri inačice pokušati proširiti na Windows 2000 sustave. Razlog ovome su različite povratne adrese prilikom prepisivanja podataka u spremniku koje, kao što je kasnije objašnjeno, dovode do rušenja RPC servisa, što znači da crv ima samo jedan pokušaj na raspolaganju za inficiranje udaljenog sustava. Kada se uspješno pokrene na zaraženom računalu, u 60% slučajeva crv će redom, od svoje IP adrese nadalje, započeti pregledavanje mreže u potrazi za ranjivim računalom. U preostalih 40% slučajeva, pregledavanje će se započeti od nasumce odabrane IP adrese.
Budući da u velikom broju slučajeva, pokušaj iskorištavanja RPC ranjivosti završi nasilnim prekidanjem rada RPC servisa, što uzrokuje resetiranje računala, širenje MSBlast crva lako se može uočiti po učestalom pojavljivanju poruka koje prikazuje *Slika 1*. Ovakve poruke pojavljuju se na Windows XP računalima, dok se prekid rada RPC servisa na Windows 2000 računalima može osjetiti kao drastično usporavanje rada sustava i gubitak pojedinih funkcija.



Slika 1: Poruka uzrokovana prestankom rada RPC servisa

Ukoliko uspješno iskoristi ranjivost, MSBLast će na napadnutom stroju pokrenuti udaljenu naredbenu ljusku na portu 4444, pomoću koje će kontrolirati instalaciju izvršnih datoteka na udaljenom računalu.

Izvršna datoteka crva dohvaća se pomoću TFTP poslužitelja, kojeg MSBlast pokreće na računalu s kojeg se vrši napad i kopira u sistemski direktorij, nakon čega se u Windows *Registry* ubacuje ključ:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
windows auto update=msblast.exe
```

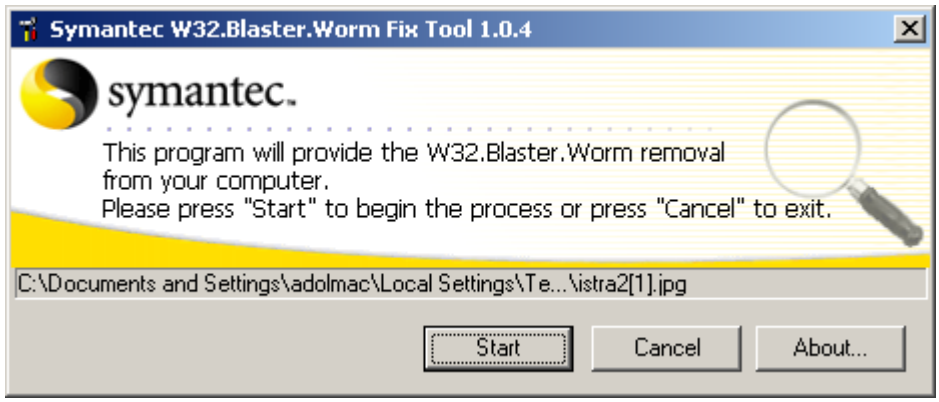
čiji je zadatak osigurati pokretanje crva pri svakom ponovnom pokretanju računala. Odmah po tome, crv resetira napadnuto računalo, kako bi se i na njemu pokrenuo.
MSBlast je napisan tako da se automatski deaktivira 31.12.2003.

2.2. Detekcija i uklanjanje

MSBlast se može prepoznati po pojačanom prometu na mrežnim portovima 135 i 4444, kao i povremenim prekidima rada operacijskog sustava, uzrokovanima problemima u radu RPC servisa.
Korisnici koji na mreži posjeduju IDS sustav, za lakšu detekciju širenja ovog crva, mogu iskoristiti sljedeći potpis za Snort IDS sustav:

```
Alert tcp $EXTERAL_NET any -> $HOME_NET 135 \
(msg:"DCE RPC Interface Buffer Overflow Exploit"; \
content:"|00 5C 00 5C|"; \
content:!"|5C|"; within:32; \
flow:to_server,established; \
reference:bugtraq,8205; rev: 1; )
```

Ubacivanjem ovog potpisa u Snort sustav omogućuje se detekcija svakog pokušaja iskorištavanja RPC ranjivosti u Microsoft-ovim operacijskim sustavima, što znači da je ovom metodom moguće prepoznati i sve buduće crve koji koriste identičan mehanizam širenja.
U slučaju sumnje u zaraženost računala, potrebno je među pokrenutim procesima potražiti `msblast.exe`, kao i provjeriti postoje li specifični *Registry* ključevi opisani u prethodnom poglavlju.
Tvrtka Symantec izdala je besplatan alat za uklanjanje MSBlast crva sa zaraženih računala (*Slika 2*), koji se nalazi na:
http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html.



Slika 2: Prozor alata za uklanjanje MSBlast crva

Ukoliko prilikom svog pokretanja alat pronađe proces pod imenom `msblast.exe`, zaustaviti će ga, ukloniti iz *Registry-a* linije koje su zadužene za pokretanje crva, te pretražiti disk u potrazi za izvršnom datotekom koja sadržava crva. U direktoriju u kojemu se nalazi alat za uklanjanje crva kreirati će se log datoteka u koju će biti zapisan tijek uklanjanja MSBlast-a. Osim u grafičkom sučelju, ovaj alat se može pokrenuti i iz naredbene ljuske, unošenjem naredbe `FixBlast.exe`.
Ukoliko korisnik trenutno nije u mogućnosti probaviti alat, dezinfekcija računala može se obaviti i ručno. Unutar prozora s pokrenutim procesima Windows *Task Manager-a*, potrebno je pronaći proces pod imenom `msblast.exe` i zaustaviti ga pritiskom na *End Process*. Nakon što je proces zaustavljen, može se obrisati izvršna datoteka crva pod nazivom `msblast.exe`. Datoteka se obično nalazi u sistemskom direktoriju Windows operacijskog sustava, ali poželjno je pretražiti cijeli tvrdi disk u potrazi za datotekama sa zadanim imenom. Poslije uspješnog uklanjanja crva, iz *Registry-a* je potrebno obrisati sljedeći ključ:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CrrentVersion\Run\ windows auto update=msblast.exe`

Prije uklanjanja crva preporučuje se instalirati sigurnosne zakrpe, kako bi se računalo zaštitilo od ponovne zaraze.

3. Welchia crv

Nedugo nakon pojavljivanja MSBlast crva počeo se širiti i drugi crv sličnog djelovanja pod imenom Welchia (poznat i pod imenima Nachi i Lovsan.D). Iako je dizajniran tako da sa zaraženog računala izbriše MSBlast crva i nadogradi operacijski sustav sigurnosnim zakrpama za ranjivost u RPC DCOM sučelju, ovaj crv je svojim širenjem izazvao napad uskraćivanjem računalnih resursa na velikom broju računalnih mreža. Mehanizam pomoću kojega se Welchia širi uzrokovao je drastično povećanje ICMP prometa na računalnoj mreži, što je dalje rezultiralo preplavljivanjem mreže ICMP prometom i samim time uskraćivanjem mrežnih resursa.
Za razliku od MSBlast crva, Welchia za svoje širenje iskorištava čak dvije ranjivosti unutar Microsoftovog sustava. Uz već spomenuti propust u implementaciji RPC DCOM sučelja, Welchia se širi i pomoću WebDav ranjivosti unutar Microsoft IIS poslužitelja.

3.1. Analiza

Čim se pokrene na zaraženom računalu, Welchia se smješta u datoteku `%System%\Wins\Dllhost.exe` (gdje `%System%` predstavlja stazu do sistemskog direktorija). Crv će također kopirati izvršnu datoteku TFTP poslužitelja `%System%\Dllcache\Tftpd.exe` u `%System%\Wins\svchost.exe`. Kopija TFTP poslužitelja koristiti će se za slanje Welchie na napadnuta računala. Izvršna datoteka Welchie i kopija TFTP poslužitelja pokreću se kao servisi pod imenom `RpcTftpd` i `RpcPatch`. Kako bi se oba servisa uspješno pokrenula svaki puta kada se računalo resetira, u Windows *Registry*, unutar ključa:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services ubacuju se podključevi RpcPatch i RpcTftpd`

Nakon uspješne instalacije Welchia će, ukoliko postoji, zaustaviti proces `msblast.exe`, obrisati izvršnu datoteku MSBlast crva i započeti proces svojeg širenja na udaljena računala. Odabir IP adrese ciljanog računala provodi se na dva načina. Crv ili preuzme početak IP adrese zaraženog računala (npr. 192.168.3.54 rezultira ciljanom adresom 192.168.0.0) ili generira slučajnu IP adresu. Odabirom polazne adrese Welchia se pokušava proširiti na sva računala u B klasi adresa. Pri tome se aktivna računala traže jednostavnim slanjem ICMP Ping paketa.
Na računala koja su identificirana kao aktivna, crv će se pokušati proširiti slanjem malicioznih paketa na port 135, ne bi li iskoristio ranjivost u RPC servisu. Osim toga, kao što je već rečeno, crv će probati i poslati pakete na port 80 te iskorištavanjem ranjivosti unutar WebDav modula na IIS poslužitelju inficirati udaljeno računalo. U trenutnu kada na napadnutom računalu preuzme kontrolu, crv se spaja na računalo s kojeg je izvršen napad i TFTP protokolom dohvaća svoju izvršnu datoteku (`Dllhost.exe`) i po potrebi i datoteku TFTP poslužitelja (`svchost.exe`). Kako bi podaci mogli biti dohvaćeni sa računala napadača, na njemu je pokrenut TFTP poslužitelj na nekom od port-ova između 666 i 765. U velikoj većini slučajeva otvara se port 707. Nakon što zarazi računalo, Welchia će se pokušati spojiti na Web stranice Microsoft Windows Update-a i instalirati zakrpu za RPC ranjivost.
Crv će automatski obustaviti svoje djelovanje 01.01.2004. godine.

3.2. Detekcija i uklanjanje

Zaraženo računalo vrlo je lako prepoznati, budući da crv u većini slučajeva ostavlja otvoren mrežni port 707. Jednostavnom provjerom pomoću nmap alata lako je pregledati cijelu mrežu i uočiti zaražena računala. Primjer naredbe nmap koji bi pregledao cijelu mrežu od 255 računala izgleda ovako

```
# nmap –sS –p 707 192.168.10.0/24
```

Sva računala na kojima je otvoren zadani mrežni port potrebno je potom detaljno pregledati kako bi se utvrdilo da li su stvarno zaražena. Tvrtka Symantec izdala je besplatan alat za uklanjanje Welchia crva,

koji se može dobaviti sa adrese http://www.symantec.com/avcenter/FixWelch.exe. Izgled i način korištenja alata identični su onome kod alata za uklanjanje MSBlast crva.
Prije uklanjanja crva također je potrebno provjeriti da li je računalo nadograđeno zakrpama koje uklanjanju oba sigurnosna propusta, kako ne bi došlo do ponovne zaraze. Naime, iako Welchia pokušava dohvatiti zakrpu i instalirati je, proces instalacije na Windows 2000 računalima neće uspjeti ukoliko sustav nije nadograđen minimalno *Service Pack-om* 2. U tom slučaju, potrebno je instalirati najnoviji *Service Pack* za Windows 2000 i nakon njega pokrenuti instalaciju zakrpi.
Crv Welchia također se sa zaraženog računala može ukloniti ručno. Unutar prozora *Services* koji se nalazi u *Administrative Tools*, potrebno je pronaći i zaustaviti servise pod imenom `Network Connections Sharing` i `WINS Client`. Unutar *Windows Registry-a* potrebno je pronaći ključ:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`
I izbrisati njegove podključeve `RpcPatch` i `RpcTftpd`. Unutar direktorija `C:\WINNT\system32\wins` nalazi se izvršna datoteka Welchia crva pod nazivom `Dllhost.exe` i preimenovani TFTP poslužitelj po nazivom `Svchost.exe`. Obje datoteke treba obrisati. Nakon ručnog uklanjanja crva, preporučuje se nekim od antivirusnih alata pregledati tvrdi disk i obrisati sve datoteke u kojima je pronađen Welchia crv.

4. Zaključak

Iako je djelovanje ovih crva vremenski ograničeno (01.01.2004.), realno je očekivati da će se njihove mutacije pojaviti vrlo brzo nakon prestanka aktivnosti originalnih crva. Imajući na umu velik broj računala koja i nakon navedenog datuma neće biti nadograđena sigurnosnim zakrpama, očekuje se vrlo brzo širenje novih inačica crva.
Kao osnovnu mjeru zaštite od novih incidenata korisnicima se preporučuje redovita nadogradnja operacijskog sustava najnovijim sigurnosnim zakrpama i filtriranje odgovarajućih portova na mrežnoj opremi.