HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Sasser.B crva

CCERT-PUBDOC-2004-05-72

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

Početkom svibnja, točnije 1. svibnja 2004 godine pojavio se crv pod imenom Sasser. U ovom dokumentu biti će opisana inačica crva pod imenom Sasser.B. Naime, istog dana pojavila se prva inačica pod imenom Sasser.A, međutim prošla je nezapaženo. Sasser.B je vrsta crva koja se ne širi putem poruka elektroničke pošte, što je učestali način širenja crva, nego koristi LSASS MS-RPC sigurnosni nedostatak unutar određenih Windows operacijskih sustava kako bi zarazio računala spojena na Internet. Po načinu širenja Sasser.B crv sličan je prošlogodišnjem Blaster crvu koji je zapamćen kao jedan od većih sigurnosnih incidenata vezanih uz crve. Crv je još poznat pod imenima WORM_SASSER.B, W32/Sasser.worm.b, Worm.Win32.Sasser.b, W32/Sasser-B, Win32.Sasser.B, Sasser.B, W32/Sasser.B.worm, Win32/Sasser.B.worm te W32/Sasser.B. Nastao je kao modifikacija već dobro poznatog i još uvijek aktivnog crva NetSky. Operacijski sustavi koji su pogođeni ovim sigurnosnim nedostatkom su Windows 2000 Professional i Windows XP dok ostale Windows verzije nisu pogođene ili moraju zadovoljiti određene uvjete koji će omogućiti ranjivost sustava.
Dokument opisuje sigurnosni nedostatak koji omogućuje zarazu računala ovim crvom, način širenja crva, preporuke za zaštitu računala te upute za ručno i automatsko uklanjanje crva.

2. Analiza

2.1. Sigurnosni nedostatak

Sasser.B crv koristi LSASS (engl. ***L**ocal **S**ecurity **A**uthority **S**ubsystem **S**ervice*) sigurnosni nedostatak koji omogućuje udaljenom korisniku (napadaču) izvršenje proizvoljnog koda na računalu na kojem je spomenuti nedostatak uočen. Sigurnosni nedostatak obilježen je prepisivanjem spremnika u Microsoft LSASS procesu. Ova vrsta eksploatacije sustava ne zahtjeva autentikaciju korisnika, a može dovesti do potpunog kompromitiranja sustava što napadaču omogućuje instalaciju programa, pregled, promjenu i brisanje datoteka te kreiranje novih korisničkih računa s administratorskim pravima. Prepisivanje spremnika napadač izvodi tako da zadaje dugačak argument poruke koristeći *lsasrv.dll* funkciju *DsRoleUpgradeDownlevelServer()* kako bi se pažljivo kreirala poruka koja se šalje određenom spremniku. Ovaj nedostatak zabilježen je u Windows 2000 Professional i XP verziji operacijskog sustava. Kod Windows Server 2003 i Windows XP 64-bit verziji operacijskog sustava nedostatak je zabilježen, ali se može iskoristiti samo ako je na računalu prijavljen lokalni administrator. Kod operacijskih sustava Windows verzije 98, 98 SE i NT nije uočen ovaj sigurnosni nedostatak, ali računala s tim operacijskim sustavima mogu poslužiti kao posrednici za širenje crva na računalima s ranjivim sustavima u lokalnoj mreži. Za ispravak LSASS sigurnosnog nedostatka potrebno je instalirati zakrpu koju možete pronaći na web stranici http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx. Instalacijom zakrpe modificira se način na koji LSASS procjenjuje dužinu poruke prije nego li ju proslijedi određenom spremniku.

2.2. Način širenja

Kao što je već spomenuto, Sasser.B crv se ne širi putem poruka elektroničke pošte, već putem Internet mreže koristeći prethodno opisani sigurnosni nedostatak te na taj način inficira računala. Za širenje među računalima koja koriste Windows 2000 Professional i XP operacijski sustav crv kreira 128 izvršnih niti, odnosno serija poruka, koje generiraju slučajne IP (engl. ***I**nternet **P**rotocol*) adrese. Nakon toga crv šalje specijalno oblikovane pakete slučajno odabranih IP adresa na TCP (engl. ***T**ransmission **C**ontrol **P**rotocol)* port 445 no pri tome zaobilazi rezervirane IP adrese:

```
10.0.0.0
127.0.0.0
169.254.0.0
172.16.0.0 – 172.31.0.0
192.168.0.0
213.191.74.19
```

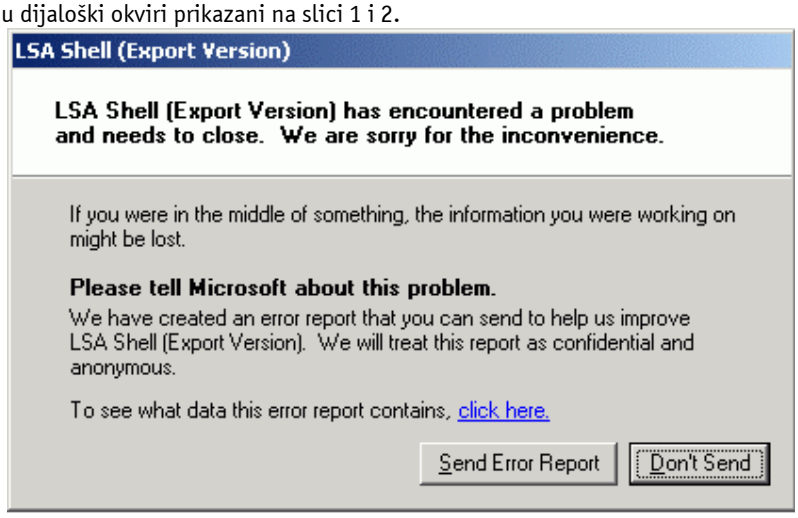
Paketi izazivaju prepisivanje spremnika ranjivih sustava u datoteci *lsass.exe* što rezultira izvršenjem udaljene komandne linije koja otvara port 9996 za daljnje udaljene naredbe. Sa udaljene lokacije crv šalje naredbe za generiranje FTP skripte pod imenom *cmd.ftp* kao i za njeno pokretanje. Cilj skripte je dohvaćanje kopije crva s izvornog inficiranog računala na računalo na kojem je skripta pokrenuta korištenjem TCP porta 5554. Dohvaćena kopija crva sprema se na lokalnom računalu pod imenom *<slučajan broj>_up.exe* (npr. *34567_up.exe*), a veličine je 15,872 okteta. Po završetku postupka dohvaćanja kopije crva, datoteka *cmd.ftp* se briše s novo inficiranog računala, a kreira se bezopasna tekstualna datoteka *win2.log* u root direktoriju (C:\). Novokreirana datoteka sadrži broj sustava koji su inficirani te IP adrese tih računala. Nakon pokretanja izvršne datoteke *<slučajan broj>_up.exe*, crv se samostalno kopira u Windows mapu kao datoteka *avserve2.exe*. Kako bi se osiguralo automatsko pokretanje izvršne datoteke prilikom svakog slijedećeg pokretanja Windows operacijskog sustava, crv kreira sljedeći zapis u *registry* datoteci:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
avserve2.exe = %Windows%\avserve2.exe
```

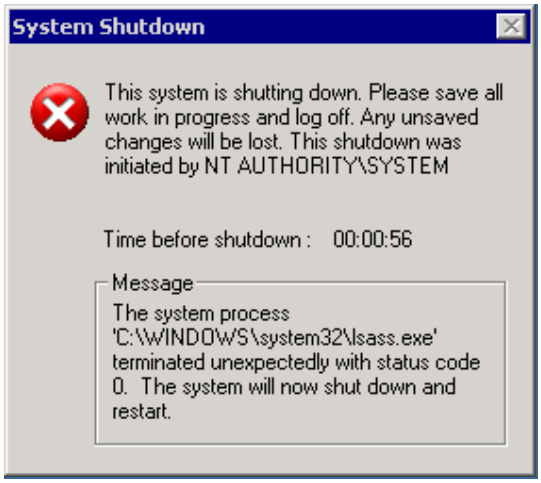
pri čemu `%Windows%` predstavlja standardnu Windows mapu (uobičajena putanja je `C:\Winnt` za Windows 2000 i XP operacijske sustave).
Također, crv kreira *mutex* (engl. ***mut**ual **ex**clusion object*), program koji omogućuje izvršnim nitima dijeljenje istog resursa, pod imenima:

```
Jobaka3
JumpallsNlsTillt
```

Ukoliko je instanca *JumpallsNlsTillt mutex-a* pronađena na računalu, crv prekida svoje izvršenje jer prepoznaje svoje postojanje na računalu.
Po izvršenju izvodi se prepisivanje spremnika sustava u datoteci *lsass.exe* što izaziva grešku u spomenutoj datoteci, rušenje operacijskog sustava te prisilno ponovno pokretanje sustava, a pri tome se pojavljuju dijaloški okviri prikazani na slici 1 i 2.



Slika 1: *Dijaloški okvir koji ukazuje na grešku u datoteci lsass.exe*



Slika 2: *Dijaloški okvir koji ukazuje na prisilno ponovno pokretanje operacijskog sustava*

3. Detekcija i uklanjanje

Prije postupka detekcije crva strogo je preporučljivo instalirati zakrpu koju možete pronaći na web stranici http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx kako ne bi došlo do ponovne zaraze računala te blokirati TCP portove 445, 9996 i 5554 kako bi se spriječilo daljnje širenje crva na računala na kojima još nije instalirana zakrpa. Ukoliko se tijekom postupka nadgradnje sigurnosne zakrpe operacijski sustav prisilno ponovno pokreće i onemogućuje postupak nadgradnje, potrebno je učiniti slijedeće:

1. Prekinuti konekciju računala s Internet ili lokalnom mrežom.
2. Ponovno pokrenuti operacijski sustav.
3. Kliknuti dugme *Start > Run*.
4. Upisati naredbu `cmd` i kliknuti dugme OK.
5. Upisati komandnu liniju `shutdown -i` i pritisnuti tipku `Enter`.
6. Otvorit će se *Remote Shutdown Dialog* u kojem je potrebno izvršiti promjenu broja sekundi kojim se određuje dužina prikaza obavijesti korisniku o gašenju računala. Broj `20` promijeniti u `9999` i kliknuti dugme OK.
7. Uspostaviti konekciju računala s Internet ili lokalnom mrežom.
8. Provesti postupak nadgradnje sigurnosne zakrpe.
9. Ponoviti korake od 3 do 6 ukoliko se postavke vremenskog intervala žele vratiti na prethodne.

Također se, prije samog postupka detekcije te ručnog uklanjanja crva, korisnicima Windows XP operacijskog sustava preporučuje privremeno onemogućavanje System Restore opcije. Za uspješnu detekciju crva potrebno je koristiti antivirusni program koji ima ažuriranu bazu virusa. Pokretanjem antivirusnog programa izvodi se postupak traženja malicioznih datoteka na računalu. Kada je takva detektirana, potrebno ju je zaustaviti na slijedeći način:

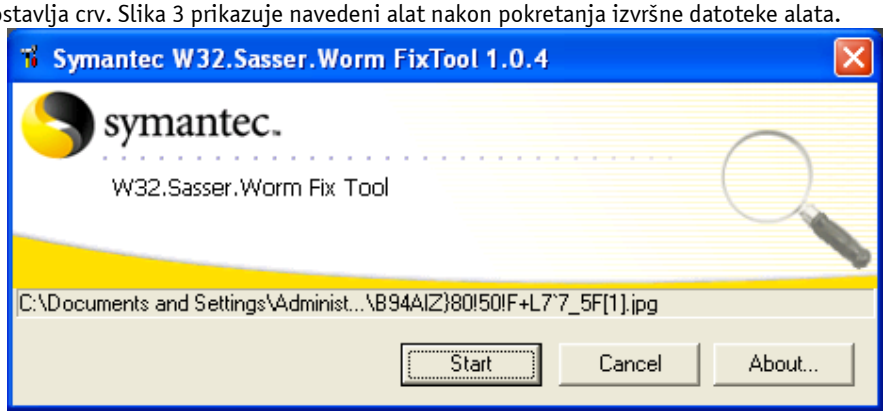
10. Otvoriti `Windows Task Manager` dijaloški okvir. Na računalima s Windows 2000 i XP operacijskim sustavom treba pritisnuti kombinaciju tipki `CRTL+SHIFT+ESC`.
11. U dijaloškom okviru otvoriti karticu `Processes`.
12. U popisu aktivnih programa pronaći detektiranu datoteku (ili datoteke) te kliknuti na svaku od njih, a zatim kliknuti dugme `End Process`.
13. Zatvoriti dijaloški okvir.

Nakon zaustavljanja pokrenute datoteke crva omogućeno je ručno uklanjanje crva sa zaraženog računala. Postupak uklanjanja crva sastoji se od slijedećih koraka:

1. Otvoriti *Registry editor* (*Start – Run* – upisati naredbu *regedit*).
2. U lijevom okviru otvorenog prozora otvoriti `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`.
3. U desnom okviru detektirati i obrisati slijedeću vrijednost: `avserve2.exe = %Windows%\avserve2.exe`.

4. Zatvoriti *Registry editor*.

Za manje iskusne korisnike preporučljivo je korištenje gotovih alata koji će obaviti detekciju crva te ga ukloniti sa zaraženog računala. Jedan od takvih programa je i Symantec W32.Sasser.Worm FixTool 1.0.4 koji se može pronaći na adresi http://securityresponse.symantec.com/avcenter/FxSasser.exe. Ovaj alat ima funkciju detekcije zaraženih datoteka, njihovog uklanjanja te brisanja Registry ključeva koje postavlja crv. Slika 3 prikazuje navedeni alat nakon pokretanja izvršne datoteke alata.



Slika 3: Prozor alata Symantec W32.Sasser.Worm FixTool 1.0.4

Pritiskom na dugme Start pokreće se alat koji pretražuje datoteke računala kako bi, u slučaju detekcije zaraženih datoteka, izvršio uklanjanje istih. Rezultat postupka pretraživanja računala upisuje se u log datoteku koja se kreira u mapi u kojoj se nalazi i izvršna datoteka alata.
Nakon što je crv uklonjen s računala

4. Zaključak

Crv Sasser.B definiran je kao crv s visokim potencijalom distribucije, što je vidljivo iz velikog broja zaraženih računala diljem svijeta, te visokim potencijalom oštećenja, no unatoč tome, nije destruktivan. Širenje je omogućio sigurnosni nedostatak u Windows 2000 Professional i XP operacijskim sustavima. Iako je Microsoft izdao sigurnosnu zakrpu nekoliko dana prije pojave crva, zaraza računala spojenih na Internet dosegla je veliki broj u vrlo kratkom vremenskom periodu. Obzirom da je pojava iskorištavanja sigurnosnih nedostataka za širenje crva vrlo česta, korisnicima se preporučuje redovita instalacija sigurnosnih zakrpa. Također je preporučljivo korištenje antivirusnog programa koji svakako mora imati ažuriranu bazu virusa.

5. Reference

1. Microsoft,
Microsoft Security Bulletin MS04-011, http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

2. Trendmicro,
Sasser.B, http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SASSER.B

3. Sophos,
Sasser.B, http://www.sophos.com/virusinfo/analyses/w32sasserb.html

4. F-secure,
Sasser.B, http://www.f-secure.com/v-descs/sasser_b.shtml

5. Symantec,
Sasser.B, http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.b.worm.html

6. W32.Sasser Removal Tool,
http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.removal.tool.html