HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza DeLoder crva

CCERT-PUBDOC-2003-03-11

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.

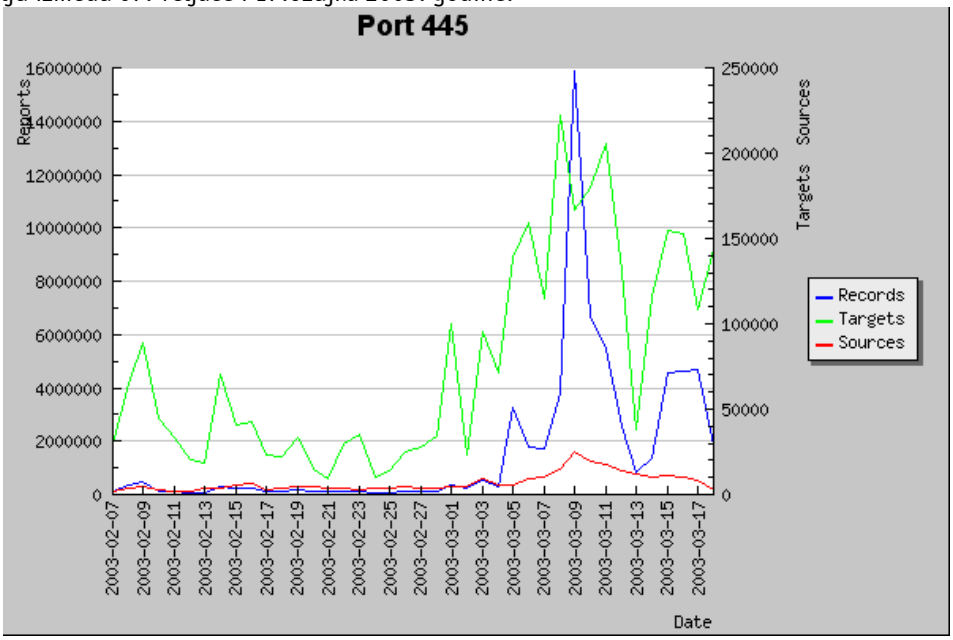
LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument predstavlja vlasništvo CARNet-a (CARNet CERT-a). Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u originalnom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet-a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

Sadržaj

1. Uvod

U posljednje vrijeme primijećen je povećani broj malicioznih programa (crvi, Trojanski konji, virusi i sl), koji se šire putem Windows TCP 445 porta. TCP 445 port uveden je kod Windows 2000 operacijskih sustava u svrhu omogućavanja izravne SMB (engl. ***S**ervice **M**essage **B**lock*) komunikacije preko TCP/IP protokola, bez posredstva *NetBIOS over TCP/IP* transportnog sloja.
Na sljedećoj slici (*Slika 1*) dan je grafički prikaz neovlaštenih aktivnosti usmjerenih na TCP 445 port u razdoblju između 07. veljače i 17.ožujka 2003. godine.



Slika 1: Grafički prikaz malicioznog prometa usmjerenog na TCP port 445

Grafički prikaz dobiven je na temelju analiza provedenih od strane *InternetStormCenter* organizacije (http://isc.incidents.org/) i jasno pokazuje intenzivan rast malicioznog prometa usmjerenog na 445 TCP port.
Provedene analize pokazale su da se većina malicioznih programa usmjerenih prema 445 TCP portu širi putem korisničkih računa sa "slabim" ili nepostojećim zaporkama i da redovito u paketu sadrže i neku vrstu IRC klijent programa, koji se spaja na predefinirane IRC poslužitelje, odnosno kanale.
IRC *bot* programi najčešće se koriste u svrhu neovlaštene distribucije piratskih materijala (engl. *warez*), i upravo iz toga razloga su najčešće mete napada nezaštićena računala s "brzim" pristupu Internetu kao što su sveučilišta i kućni korisnici s stalnim pristupom Internetu (ADSL, *cable* modem, i sl.) .
Iskustvo je pokazalo da se u takvim okruženjima puno manje vodi računa o računalnoj sigurnosti, nego što je to slučaj kod komercijalnih i drugih organizacija gdje je sigurnost vrlo važan element u svakodnevnom rješavanju poslovnih zadataka. Upravo stoga su takve računalne mreže vrlo česte mete neovlaštenih korisnika.
Jedan od primjera malicioznog programa koji posjeduje ranije navedena svojstva je *DeLoder* crv, čija je detaljna analiza dana u nastavku dokumenta.
Ideja dokumenta je da se korisniku pojasne osnovne karakteristike širenja *DeLoder* i njemu sličnih malicioznih programa, zajedno s tehničkim detaljima i metodama zaštite. Smatra se da je poznavanje tehnika koje neovlašteni korisnici koriste za kompromitiranje računalnih sustava osnovni preduvjet za kvalitetnu i učinkovitu zaštitu.

2. Testno okružje

U svrhu analize *DeLoder* crva postavljeno je testno okružje bazirano na Windows 2000 operacijskom sustavu, posebno prilagođeno hvatanju i analizi malicioznih programa koji se šire putem Windows 2000 445 TCP porta (engl. *honeypot*).

Slijedi opis konfiguracije sustava:

- Windows 2000 Professional (Build 5.0.2195) sa instaliranom SP3 sigurnosnom zakrpom;
- Inicijalna Windows instalacija;
- Onemogućen *NetBIOS over TCP* protokol (zatvoreni portovi 137/TCP, 138, 139/UDP);
- Lista otvorenih portova na računalu:

```
epmap           135/tcp    DCE endpoint resolution
epmap           135/udp    DCE endpoint resolution
microsoft-ds    445/tcp    Microsoft-DS
microsoft-ds    445/udp    Microsoft-DS
```

Budući da je sustav bio namijenjen isključivo hvatanju i analizi malicioznih programa, sigurnosni nivo W2K sustava bio je postavljen na minimum. Ostavljene su inicijalne postavke nakon instalacije sustava, s praznom zaporkom *Administrator* korisničkog računa. *Guest* korisnički račun onemogućen je s obzirom na inicijalnu instalaciju sustava.

3. Analiza crva

U ovom poglavlju dana je detaljna analiza *DeLoder* crv programa. Opisane su osnovne tehničke karakteristike crva zajedno s promjenama na sustavu koje upućuju na njegovo postojanje, a priložena je i kratka analiza svih malicioznih datoteka povezanih s *DeLoder* crvom.

Provedene analize pokazale su da računala inficirana *DeLoder* crvom sadrže sljedeće komponente:

- IRC Trojan program;
- VNC alat za udaljeni pristup računalu;
- Datoteke vezane uz IRC Trojan program smještene u `winnt\fonts\` direktoriju;
- `Cygwin1.dll` biblioteka smještena u `winnt\system32\` direktorij;

DeLoder crv širi se pregledavanjem slučajno odabranih područja IP adresa te spajanjem na Windows 2000/XP dijeljenje resurse preko TCP 445 porta. Nakon što je pronađeno računalo sa dijeljenim \\[system]\IPC$ direktorijom, crv koristi ugrađeni rječnik zaporki za pokušaje spajanja na sustav. U sljedećoj tablici (*Tablica 1*) dana je lista zaporki kojima se pokušava ostvariti pristup sustavu pod ovlastima Administrator korisničkog računa:

Korisničko ime	Zaporka
Administrator	0 000000 00000000 007 1 110 111 111111 11111111 12 121212 123 123123 1234 12345 123456 1234567 12345678 123456789 1234qwer 123abc 123asd 123qwe 2002 2003 2600

Korisničko ime	Zaporka
	54321 654321 88888888 a aaa abc abc123 abcd Admin admin admin123 administrator alpha asdf computer database enable foobar god godblessyou home ihavenopass Internet Login login love mypass mypass123 mypc mypc123 oracle owner pass passwd Password password pat patrick pc pw pw123 pwd qwer root secret server sex super sybase temp temp123 test test123 win xp xxx yxcv

Korisničko ime	Zaporka
	zxcv

Tablica 1: Lista zaporki koje DeLoder crv koristi za pristup sustavu

U slučaju uspješnog spajanja s jednom od navedenih zaporki, crv automatski dalje pregledava područja IP adresa kako bi se omogućilo njegovo daljnje širenje.

Budući da crv kompromitira korisnički račun administratora sustava, na računalu će imati potpunu kontrolu. Moguće je proizvoljno pokretanje i zaustavljanje servisa te brojne druge radnje koje omogućuju daljnju infekciju sustava. Pomoću `psexec.exe` programa (http://www.sysinternals.com/) na ranjivi sustav prebacuju se maliciozne datoteke i programi *DeLoder* crva.

IRC Trojan komponenta *DeLoder* crva sastoji se od dva dijela. To su IRC klijent program za pristup različitim IRC poslužiteljima i VNC program za udaljeni pristup kompromitiranom sustavu. Maliciozni IRC *bot* program koristi ranije spomenutu `Cygwin1.dll` biblioteku, što je ukazuje na činjenicu da je program izvorno razvijen za Linux/Unix operacijske sustave.

Cygwin je programski paket koji omogućuje emulaciju Unix/Linux okruženja pod Windows operacijskim sustavima i sastoji se od dva dijela:

- `Cygwin1.dll` – biblioteka kojom se emulira Unix/Linux okružje na Windows platformama,
- alati – skup programa izvorno razvijenih za Unix/Linux operacijske sustave, koji se pomoću *Cygwin* funkcionalnosti pokreću na Windows sustavima.

`Cygwin1.dll` datoteka na sustav je prebačena u fazi njegove infekcije (direktorij `winnt\system32\`), budući da je neophodna za rad IRC *bot* programa..

Sve ostale maliciozne datoteke smještene su u `/winnt/fonts` direktorij. Programeri malicioznih programa kao što je *DeLoder*, vrlo često koriste `fonts` direktorij kao lokaciju za prikrivanje datoteka. Razlog tomu je taj što Windows Explorer programom nije moguće vidjeti kompletni sadržaj tog direktorija. Windows Explorer prikazati će samo fontove trenutno instalirane na sustavu, dok ostale datoteke unutar `fonts` direktorija neće biti prikazane.

Kompletni sadržaj direktorija moguće je vidjeti ili pomoću *Find/Search* programa za pretraživanje datotečnog sustava, ili izvršavanjem `dir` naredbe u naredbenom retku Windows 2000/XP sustava.

VNC komponenta *DeLoder* crva (inačica 3.3.3.9) je u svrhu prikrivanja preimenovana u `explorer.exe`, a također su dodane i *registry* vrijednosti koje su vezane uz ovaj program (*HKEY_LOCAL_MACHINE\SOFTWARE\ORL\WinVNC3*).

Jedan od identificiranih *registry* ključeva VNC programa sadrži vrijednost "`F3 40 BB C8 07 36 DE 47`" za koju se pokazalo da predstavlja kriptirani oblik zaporke koja se koristi za udaljeni pristup sustavu. Primjenom *VNCrack* (http://www.phenoelit.de/vncrack) alata ustanovljeno je da zaporka glasi **"strict"**.

U nastavku je dana lista svih *registry* vrijednosti vezanih uz VNC komponentu *DeLoder* crva. To su:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ORL\WinVNC3]
"SocketConnect"=dword:00000001
"AutoPortSelect"=dword:00000001
"InputsEnabled"=dword:00000001
"LocalInputsDisabled"=dword:00000000
"IdleTimeout"=dword:00000000
"QuerySetting"=dword:00000002
"QueryTimeout"=dword:0000000a
"Password"=hex:f3,40,bb,c8,07,36,de,47
"PollUnderCursor"=dword:00000001
"PollForeground"=dword:00000001
"PollFullScreen"=dword:00000001
"OnlyPollConsole"=dword:00000001
"OnlyPollOnEvent"=dword:00000001
```

Explorer.exe program veže se na TCP portove 5800 i 5900 na kojima osluškuje zahtjeve VNC klijenata. Pomoću ranije spomenute zaporke moguće je s odgovarajućim klijentskim programom preuzeti potpunu kontrolu nad sustavom te pratiti sve događaje na njemu.
Osim ranije navedenih *registry* vrijednosti vezanih uz VNC program, dodane su i druge vrijednosti koje omogućuju pokretanje programa pri podizanju sustava. Unutar Registry key = HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Run kategorije dodani su sljedeći zapisi prikazani u *Tablica 2*:

1	Value:	Explorer
	Data:	C:\Winnt\fonts\explorer.exe
2	Value	taskman (u nekim analizama primijećena je vrijednost messnger).
	Data:	C:\Winnt\fonts\rundll32.exe

Tablica 2: Registry zapisi koji omogućuju pokretanje crva pri pokretanju sustava

U slučaju da ne uspije pokretanje crva pri podizanju sustava, instalacijski program inst.exe kopira se na još nekoliko mjesta koja će omogućiti redundantne metode pokretanja. Postavljenjem inst.exe programa u navedene direktorije sustava omogućiti će se pokretanje crva prilikom korisnikova prijavljivanja u sustav (engl. *logon)*. Radi se o sljedećim lokacijama:

- C$\WINNT\All Users\Start Menu\Programs\Startup\inst.exe
- C$\WINDOWS\Start Menu\Programs\Startup\inst.exe
- C$\Documents and Settings\All Users\Start Menu\Programs \Startup\inst.exe

Ukoliko je crv pokrenut putem jednog od navedenih *Startup* direktorija, dvdr32.exe i inst.exe instalacijski programi brišu se iz prilikom postupka instalacije i pokretanja crva. Izvorna inačica inst.exe programa koja se nalazi u *c:\winnt\system32* direktoriju ostaje netaknuta, čime se željela se minimizirati mogućnost otkrivanja potencijalno sumnjivih datoteka, koje bi korisnika navele na postojanje crva.
Nakon pokretanja, crv uklanja sljedeće dijeljenje mape sa sustava,

- ADMIN$
- IPC$
- C$
- D$
- E$
- F$

kako bi se na taj način onemogućila ponovna infekcija sustava istim crvom.
Sljedeći korak koji slijedi, je automatizirano spajanje IRC *bot* klijenta na jedan od konfiguracijom predefiniranih IRC poslužitelja. IRC *bot* programi su automatizirani programi koji prihvaćaju naredbe putem IRC kanala, što neovlaštenom korisniku omogućuje udaljeno upravljanje kompromitiranim sustavom. Ovisno o tipu i namjeni crva, ovakvi programi mogu se ponašati na različite načine.
Poznati su slučajevi gdje su isti iskorišteni kao DDoS agenti za provođenje distribuiranih napada uskraćivanjem računalnih resursa, jednako kao i slučajevi gdje su ovakvi programi iskorišteni u svrhu neovlaštenog distribuiranja *warez* materijala.
U nastavku je dana lista IRC poslužitelja s kojima *DeLoder* crv pokušava uspostaviti komunikaciju:

- h13-2-4-00-0396.beready.communitech.net (6667)
- 64.23.55.21 (6667)
- dedicated1.airwire.net (6667)
- sowqube.ten6.com (6667)
- j1.mediag3.com (6667)
- boom.sh3ll.la (6667)
- 198.65.147.245 (6667)

Provedene analize identificirale su oko 3000 pokušaja spajanja na poslužitelj h13-2-4-00-0396.beready.communitech.net (maskiranim pod imenom AOL.ICQ.COM) i približno oko 15000 pokušaja spajanja prema ranije navedenim IRC poslužiteljima. Ovakav podatak upućuje na

prilično intenzivno širenje crva, a jednako tako može se pretpostaviti i da se kompromitirana računala koriste kao DDoS agenti.
Slijedi analiza datoteka identificiranih na sustavu zaraženim DeLoder crvom. Datoteke su redom navedene u sljedećoj tablici s kratkim opisom svake od njih.

Ime datoteke	Veličina	Opis
\WINNT\fonts\ direktorij		
dvldr32.exe	745,984	Maliciozni program koji omogućuje širenje crva.
inst.exe	684,562	Maliciozni proigram zadužen za instalaciju crva.
explorer.exe	212,992	VNC poslužitelj prikriven pod imenom explorer.exe.
omnithread_rt.dll	57,344	DLL biblioteka VNC poslužitelja.
VNCHooks.dll	32,768	DLL biblioteka VNC poslužitelja.
rundll32.exe	29,336	Maliciozni IRC-Pitchfork *bot* program.
\WINNT\SYSTEM32\ direktorij		
psexec.exe	36,352	Legitimni program koji omogućuje izvršavanje programa na udaljenom računalu.
inst.exe	684,562	Maliciozni proigram zadužen za instalaciju crva.
Cygwin1.dll	944,968	DLL biblioteka IRC-Pitchfork *bot* programa.

Tablica 3: Lista datoteka DeLoder crva

4. Preporuke za uklanjanje

Prije samog postupka uklanjanja malicioznog programa sa sustava vrlo važno je pouzdano identificirati njegovo postojanje.
U svrhu prepoznavanja *DeLoder* crva može se iskoristiti *TCPViewer* (http://www.sysinternals.com/ntw2k/source/tcpview.shtml) aplikacija, koja omogućuje analizu otvorenih portova na sustavu te njihovo povezivanje s pripadajućim programima. Program se može opisati kao naprednija inačica `netstat` programa, s dodanim grafičkim sučeljem koje korisniku olakšava njegovo korištenje.
U nastavku će biti dani osnovni pokazatelji koji upućuju na postojanje *DeLoder* crva te preporuke za njegovo otklanjanje.
Ukoliko je na sustavu pokrenut `explorer.exe` program, čija se izvršna verzija nalazi unutar `c:\winnt\fonts\`, umjesto `c:\winnt\system32` direktorija, sa velikom vjerojatnošću može se pretpostaviti da se radi o VNC komponenti *DeLoder* crva. U tom slučaju moguće je zaustaviti maliciozni `explorer.exe` program ili putem Windows *Task Managera* (*Ctrl+Alt+Delete -> Task Manager*), ili unutar same *TCPViewer* aplikacije.
Na sličan način potrebno je postupiti ukoliko je na sustavu pokrenut `rundll32.exe` program iz `c:\winnt\fonts\` direktorija, budući da se legitimna inačica istog programa nalazi unutar `c:\winnt\system32` direktorija.
DeLoder crva moguće je također detektirati i pomoću nekog od antivirusnih programa, pod uvjetom da je baza potpisa svježe nadopunjena najnovijim informacijama o poznatim virusima i malicioznim programima.
Na sličan način moguće je upotrijebiti i neki od alata specijaliziranih za uklanjanje Trojanskih konja i crva. Programi ovog tipa sadrže bazu s podacima o najnovijim Trojanskim programima i crvima te omogućuju njihovu detekciju i uklanjanje sa sustava. Kao primjer može se navesti `swat` (http://lockdowncorp.com/bots/downloadswatit.html), besplatni program *LockDown* tvrtke koji omogućuje detekciju i uklanjanje preko 3000 različitih malicioznih Trojan i crv programa.
Potrebno je provjeriti i ranije spomenute *Startup* direktorije, koji omogućuju pokretanje programa prilikom prijavljivanja korisnika u sustav. Ukoliko se unutar bilo kojeg od *Startup* direktorija primijete programi sumnjivog podrijetla (u ovom slučaju `inst.exe`) potrebno ih je smjesta ukloniti.

Za uspješno uklanjanje *DeLoder* crva također je potrebno ukloniti sve maliciozne datoteke prikazane u *Tablica 3*. Nakon što je sustav osiguran i nakon što su sa sustava uklonjene sve komponente crva, preporučuje se promjena svih zaporki, budući da neovlašteni korisnik u tom trenutku vrlo vjerojatno posjeduje dovoljno informacija koje će mu omogućiti ponovni pristup.

5. Mogućnosti zaštite

Na nivou zaštite pojedinih računala svakako se preporučuje korištenje "snažnijih" zaporki, koje će se sastojati od kombinacije velikih i malih slova, brojeva te specijalnih znakova kao što su #, $, $, % i sl. Budući da postoji intenzivan porast virusa koji se šire putem slabijih ili nepostojećih zaporki, ovo je svakako jedan od temeljnih koraka zaštite. Dodatno se može preporučiti obavezna instalacija antivirusnih programa koji će omogućiti pravovremenu detekciju malicioznih programa.
Na nivou zaštite računalne mreže može se preporučiti postavljanje vatrozida koji bi blokirao neautorizirani promet prema 137, 445/TCP, 138/, 139/UDP portovima. Na taj način bi se u velikoj mjeri otklonile neovlaštene aktivnosti vezane za Windows SMB portove koje dolaze s javnog Interneta.
U slučaju potrebe za udaljenim pristupom Windows resursima, u razmatranje treba svakako uzeti VPN tehnologiju, koja u određenoj mjeri rješava ovaj problem. VPN tehnologija udaljenim korisnicima omogućuje pristup internim resursima preko javne računalne infrastrukture kao što je Internet, pri čemu se kompletni promet kriptira i autenticira.