About all Trojan

Innanzitutto vorrei chiarire il concetto di trojan o backdoor (se gia' sapete tuto vi consiglio di passare avanti).Un trojan o Cavallo di troia ,che deriva dalla legendaria storia e dopo scoprirete xchè questo nome,una volta eseguito ill file patch risiede sul computer e ne fa un server accessibile facilmente tramite un clint o collegamento e quindi prenderne il controllo senza che l'utente se ne possa accorgere (da cui il nome di "cavalli di troia").Molti di loro dopo eseguiti non danno alcun messaggio ,alcuni invece simulano un errore delle librerie.per accederci da remoto al computer infeto basta prelevare il suo IP.Non essendo i trojan ed i backdoors dei veri e propri virus (anche se sono altrettanto pericolosi) non tutti gli antivirus sono in grado di rilevarli; vi consiglio di procurarvi uno o piu' antivirus in grado di aggiornarsi tramite internet, anche perche' nascono nuovi backdoors ogni giorno...

I trojan piu' recenti sono quelli piu' in basso.

Rimuoverli

Esiste un sistema per tenere sotto controllo tutte le porte aperte ed è questo, scrivete sotto dos : netstat -a .

se oltre alla porta 0 ne è aperta un'altra allora iniziate anche a preoccuparvi.Io vi consiglio con un antivirus aggiornato di scansionare la cartella windows se rileva virus NOn cancellateli ancora come riporta l'antivirus(non preoccupatevi se non siete in rete il trojan non potra' farvi niente).Oppure adesso esistemo mille programmi per la rimozione dei trojan come "The cleaner" anche per specifici,ad esempio programmi che scovano il server back orifice e lo cancellano definitivamente ,lo stesso col Netbus.Quindi avete piu' possibilita'...

Un'altra osservazione da fare è questa,tutti questi virus si eseguono in background(significa dietro le quinte ,termine usato nei sistemi linux) quindi per vedere ad ogni avvio cosa la macchina esegue andate nel regedit e fatene una copia con il comando "export" poi andate in HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun

da qui potrete vedere tutto quello che partira' in avvio.

Cmq adesso vi riporto come ripulire alcuni di questi trojan,quando scivo poi è meglio che riavviate il sistema,ad esempio cancellate una riga nel registro poi cancellate il file...:

BACK ORIFICE

Descrizione:il file patch è un'applicazione ".exe" senza icona ed è circa 180kb.

Il file si piazza in c/windows/del.exe ma come la versione 1.20 puo' darsi si trovi in c:WindowsSystem.Trovatelo e cancellatelo da Dos.

Poi andate nel regedit e cancellate la voce ,mi sembra si trovi in HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRunServices

.

NETBUS

Descrizione:il oatch si chiama appunto "patch.exe" ma si trova sempre rinominato ovviamente ha come icona una "piccola parabola" , è grande circa 483kb.

Andate in HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun e cancellate la riga.Poi andate in c:Windows e cancelate il file che vi hanno mandato e avete precedentemente eseguito.Atenzione puo' avere anche l'estensione .ini cancellatelo cmq.

TELECOMMANDO

Descizione :il server è Odbc.exe ed è circa 206kb.

Si piazza in c:WindowsSystem ma voi andate nel regedit in HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun e cancellate la riga SystemApp "ODBC.EXE" poi cancellate il file file odbc.exe da WindowsSystem

GIRLFRIEND

Descizione:il patch è Windll.exe circa 336kb o 302kb, ha per icona il simbolo di Windows oppure un piccolo fax.Il file si piazza in C:WINDOWSWindll.exe

Quindi andate in dal regedit HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun

e poi cancellate il file in c:windows.

MASTER'S PARADISE 98

Descizione:il patch è SysEdit.exe sono circa 462kb.

Andate in HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun

cancellate la riga e poi andate in c:windows e cancellate sysedit.exe e KeyHook.dll .

DEEP THROAT

Descizione:il patch è Systray.exe ,circa 304kb.

Qundi andate in HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun
cancellate la riga e poi cancellate il file systray.exe da c:Windows.
NETBUS PRO2
Come il Netbus ,infatti si piazza sempre in c:windows pero' nel regedit ci sono delle varianti che sono :
HKEY_CURRENT_USERNetBus
HKEY_CURRENT_USERNetBus ServerGeneral
HKEY_CURRENT_USERNetBus ServerProtection
HKEY_CURRENT_USERNetRex
HKEY_CURRENT_USERNetRex ServerGeneral
HKEY_CURRENT_USERNetRex ServerProtection

POLY (sconosciuto)
Descizione:il file patch è un .exe circa 389kb,ha l'icona di un filmato multimediale quando lo si esegue appare una finestra che ci comunica che mancano le librerie del quicktime.
Si piazza in c:windows è "rhwtcnxb.exe" ma puo' darsi anche ci siano delle varianti,per sicurezza fate uno scan con un antivirus aggoirnato ,il norton2000 preferibilmente e controllate.
Quindi andate in HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun e cancellate la riga ,che mi sembra simuli una .dll .
Poi cancellate il file in c:windows.

TIPS per sfruttare i trojan

Innanzitutto per vedere se un utente è infettato da un trojan e conoscete la porta di aperture (ad esmpio per il Netbus è la 12345) andate con telnet all'host che sara' l'ip della vittima e la porta del trojan esempio pratico :
123.242.24.23:12345 vi dira' anche che versione (nometrojan)! .
Se avete individuate un ip infetto da Netbus e volete illuderlo da password(solo voi potete accedere al computer) fate i seguenti comandi col telnet:
una volta scritto l'ip e la porta del netbus
Password;1;any

poi
ServerPwd;lapasswordchevolete
Attenzione:funziona dalla versione precedente alla 1.70 ,per controllarlo verificatelo con telnet.
Potete cambiare anche l'icona ad un trojan,prendete un programma che crea icone come il microangelo e prendiamo un icona che ci garba.Poi la apriamo con l'editor di icone e facciamo un copia di tutto e incolla sull'icona del trojan sempre editandolo.
Si avra' una Patch meno sospettabile.
Potete anche creare un bel "pacchetto" per nascondere meglio.Mettete in un file zippato la patch rinominata Setup.exe con una bella icona di istallazione! Poi ci mettete dei file .doc magari chiamandoli leggimi.doc o leggimi.txt ,fate dei file di help,dei file .bin o altro per simulare un bel programma ,se volete anche un'immagine fatta da voi(per simulare l'immagine che parte appena si esegue l'istallazione)!!Così sara' un programma "in regola".
un'altro metodo sarebbe quello di mettere come icona al patch quella del self-extractor del winzip,catturandola con il microangelo che ha l'apposita opzione, che in realta' è un .exe quindi insospettabile!