www.mudsucker-tuts.de.vu

Trojanische Pferde

(einfach und leicht erklärt)

by

MudSucker

Inhaltsverzeichnis

1.Allgemeines Verhalten

1.1 Was ist ein Trojanisches Pferd?Warum heißt es so?

Nun sicher kennt der eine oder andere das Trojanische Pferd aus der griechischen Mythologie. Dort heißt es, dass Epeios ein großes Pferd aus Holz gebaut hat, in dem sich Soldaten verstecken konnten. Dieses Pferd wurde den Trojanern als Geschenk dargeboten. Diese nahmen das Geschenk an. Als die Nacht einbrach krochen die Soldaten aus dem Pferd und haben die Stadttore geöffnet. Dadurch konnten die Griechen in die Stadt einfallen und sie zerstören.

1.2 Was hat das mit den Elektronischen Trojanern zu tun?

Ganz einfach, das Prinzip eines Trojaners ist es, sich wie das Originale Holzpferd, als etwas nützliches zu tarnen(z.B. als nützliches Programm oder als Hacker Software) , und wenn man dieses Nützliche nun benutzt, öffnet dieser Trojaner die „Tore zu deinem PC“ und derjenige, der den Trojaner „erschaffen“ bzw. „verschenkt“ hat, kann unbemerkt auf deinen PC(also in die Stadt).

1.3 Wie fängt man sich einen ein?

Es gibt mehrere Möglichkeiten, hier sind ein paar aufgezählt:

1. Durch P2P Programme wie Kazaa. Wenn man z.B. nach einem Programm sucht, kommt es oft vor, dass es zwar in der Liste/ in den Suchergebnissen angeboten wird, aber es handelt sich hierbei um einen Trojaner.
2. Von vermeidlichen Freunden oder Chatpartnern aus dem Internet die dir einfach eine Datei schicken und du diese ahnungslos öffnest.
3. Es gibt die Möglichkeit, dass ein User sich per Telnet (bei falsch eingestellter Freigabe etc.) mit deinen Rechner verbinden kann. Hat er nun die nötigen Rechte kann er den Trojaner in den Autostart Ordner laden und beim nächsten Neustart wird der Trojaner aktiv.

TIP:

- Eine guter Trick ist auch folgender:
  Man erstellt sich eine „ Sexy-Diashow“(am besten mit Amateur Bildern aus dem Internet) und verbindet diese mit einem Trojaner. Nun geht man in einen öffentlichen Chat und gibt sich dort als weiblich aus. Man schreib ein bisschen in den öffentlichen Chat.
  Z.B. dass man FKK mag oder ähnliches(Halt etwas, was die Männer aufmerksam auf einen macht.)
  Dann ab in den Privatchat. Ein bisschen rumflirten und wenn es soweit ist und er fragen sollte ob er Nacktfotos haben darf, sagst man das man nur eine Diashow, die für den Ex-Freund sei, hat. Der Chatpartner wird höchst wahrscheinlich nicht locker lassen und irgendwann gibt man nach. Man fragt auch nach Fotos von ihm, damit es realistisch bleibt.
  Und...nun öffnet der Chatpartner vor Erregung die „Diashow“ und ist infiziert.

  ANMERKUNG: Viele Instant Messenger, wie MSN lassen das verschicken von ausführbaren Dateien(.exe, .scr, .bat, .com) nicht zu. Es empfiehlt sich diese mit WinRar zu packen.

1.4 Wenn ich den PC neu starte muss er doch weg sein oder?

Es kommt ganz auf den Trojaner an. Die meisten haben die „Fähigkeit“ sich bei jedem Systemstart starten zu lassen. Das erreichen sie durch:

1. erstellen einer eigenen Kopie in den Autostart Ordner
2. erstellen eines Registry-Schlüssels im run Verzeichnis.
3. durch Injektion in eine andere ausführbare Datei(z.B. IE.exe, dem Internet Explorer)
4. Oder alles zusammen

Registry

- Die Registry werden Benutzer spezifische Informationen gespeichert, die es Programmen ermöglicht z.B. Passwörter oder Layout Einstellungen zu speichern. Unter anderem auch welche Programme beim Systemstart gestartet werden.
- Die Registry erreicht man wie folgt: Start/Ausführen und dort „regedit“ oder „“ eingeben.
- Der am häufigsten genutzte Schlüssel ist: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

1.5 Kann man sich dagegen schützen?

Ja kann man, sogar sehr gut!Dabei gibt es folgendes zu beachten:

1. Aktuelle Anti Virus Programme benutzen: AntiVir
2. Eine gute Firewall benutzen: Zone Alarm
3. Firewall und Anti Viren Programm immer Updaten.
4. Darauf achten, wenn man sich in P2P Netzwerke begibt, dass man keine Ausführbaren Daten runter lädt und wenn man weiß, dass das Programm etwas größer ist und die Suchergebnisse um die 100 – 800 Kb ausfallen(also deutlich kleiner), kann man davon ausgehen das es ein Trojanischen Pferd oder ein Virus ist. Aber daran denken, dass ein Programm, was ca. 2 MB groß ist, mit WinRar gepackt auch so klein sein kann. Man muss differenzieren.
5. Wenn man Besitzer eines Routers ist diesen mit WAP verschlüsseln.
6. Keinen Email Anhang runter laden, von Adressen die man nicht kennt, aber das sollte eh allgemein bekannt sein.
7. Wenn man jemanden im Internet kennen lernt, auf keinen Fall Programme oder ausführbare Dateien annehmen bzw. öffnen!!!
8. Wenn man ein Programm öffnet, und die Firewall meldet Alarm, obwohl das Programm nichts mit dem Internet zu tun hat, kann das ein Trojaner sein -> Zugang verweigern und Viren suche machen.

1.6 Wie lösche ich den Trojaner?

Am besten man geht in den Abgesicherten Modus von Windows. Dazu hält man die F8 Taste, beim Starten des PCs, solange gedrückt, bis ein Menü kommt in dem man verschiedene Bootmodi auswählen kann. Dort wählt man den abgesicherten Modus.
Im abgesicherten Modus lädt Windows nur die nötigsten System Dateien, also keinen Trojaner oder

dergleichen.

Achtung:

- Trojaner könnte man rein Theoretisch so Programmieren, dass sie teil einer System notwendigen Datei werden!!! Bisher habe ich noch keinen Trojaner gesehen der das tut.

Dort führt man dann sein Anti Viren Programm aus und macht einen kompletten Systemscan. Sollte der Trojaner trotzdem noch irgendwie vorhanden sein, dann hilft vielleicht das manuelle entfernen des Trojaners. Es gibt Seiten im Internet die die Installation eines Trojaners Protokollieren, anhand dieser Informationen kann man den Trojaner löschen.
www.megasecurity.org hat z.B. eine große Auswahl, einfach auf Archiv klicken.

1.7 Warum gibt es so etwas überhaupt?

Trojaner stammen von den RAT's (Remote Administration Tool. zu deutsch: Fern Administrations Werkzeug) ab bzw. sind gleichgestellt.
RAT's werden genutzt um seinen eigenen PC fern zuwarten. Sprich man hat dadurch die Möglichkeit seinen PC z.B von einem Internet Café aus zu steuern.
Diese Idee wurde nun ein wenig geändert und es gibt Trojaner.
Im Gegensatz ist das Ziel eines Trojaners so unbemerkt wie möglich zu laufen.

1.8 Was kann man mit einem Trojaner alles machen?

Je nach Trojaner ist dies unterschiedlich. Ich zähle hier die Möglichkeiten auf, die in einem „guten“ Trojaner enthalten sind:

- Funny Stuff, sprich CD-Rom Laufwerk öffnen, Maus einfrieren, Desktop auf den Kopfstellen etc.
- File Manager, sprich man hat die Möglichkeit die Daten durch zu gucken, diese auf seinen eigenen Rechner oder eigene Daten auf den Infizierten Rechner zu laden.
- FTP - Auf dem Zielrechner eine FTP Funktionalität einzurichten.
- Telnet nutzen.
- Password Grabber – Man hat die Möglichkeit sich sämtliche gespeicherte Passwörter an zugucken, die auf dem Infizierten Rechner gespeichert sind.
- Serial/CD-Key Grabber – Das selber wie der Password Grabber, aber auf Serials und CD-Key spezialisiert
- Keylogger – Der Keylogger speichert alle Tastaturanschläge, diese kann man sich dann angucken.
- Zwangschat – Chat den der User des infizierten Rechners nicht beenden kann.
- Schadens-Funktionen – Etwas PC Formatieren oder ähnliches.
- Notify Funktion – Der Server schickt notwendige Daten zur Verbindung zum „bösen“ Benutzer der den Trojaner verbreitet hat(IP-Adresse, Port)

und sicherlich noch etliche mehr...

2.Technisches Verhalten

2.1 Wie ist ein Trojanisches Pferd aufgebaut?

Ein Trojanisches Pferd besteht im wesentlichen aus zwei Programmstücken:

- Client
- Server

Der Client ist das Programm was der „böse“ Benutzer benutzt um den anderen PC zu steuern. Der Server ist das „böse“ Programm, was die Türen auf dem PC öffnet, damit der Client arbeiten kann.

2.2 Wie funktionieren Server und Client?

Der Client verbindet sich zum Server. Dies geschieht durch die Eingabe der IP-Adresse und des Ports. Jeder PC der sich ins Internet einwählt, erhält eine IP-Adresse. Diese kann man mit einer normalen Hausanschrift vergleichen. Der Port ist wie eine Tür zu betrachten. Der Client verbindet sich durch den Port mit den Server. Ein PC Kann über 5000 Ports haben.
Sind beide Teile miteinander verbunden, hat der Client die Möglichkeit befehlen an den Server zu senden

Beispiel:
Man drückt auf den Knopf „Laufwerk-Öffnen“, der Client sendet nun den Befehl(z.B. „openCD“). Der Server erhält den Befehl „openCD“ und weiß was zu tun ist und tut dies.

Hat der Client nun noch die Möglichkeit den Status des Laufwerks des Infizierten PCs anzuzeigen, dann wird wie folgt vorgegangen:

Der Server sendet nun eine Information an den Client (z.B. „CD-OPENED“). Der Client weiß damit etwas anzufangen und zeigt an das das Laufwerk erfolgreich geöffnet wurden konnte.

So läuft das mit allen Funktionen des Trojanischen Pferdes ab.

2.3 Wie kommt es, das man es nicht bemerkt, wenn man infiziert ist?

Das liegt daran, dass der Server über kein Fenster verfügt, wie es z.B Word, Excel usw. haben. Dadurch ist das Programm nicht sichtbar. Der einzige Weg ihn ausfindig zu machen ist im Task Manager zu gucken. Zumindest bei Windows XP sieht man die Prozesse.
(Aufruf mit Strg+Alt+Entf)
Doch da oft als Prozessname ein Name, der so ähnlich ist wie ein Systemprozessname aussieht, genommen wird, ist es schon schwer ihn zu finden, wenn man die Standard-Prozessnamen nicht kennt.

Es gibt dennoch Möglichkeiten, den Server nicht im Task Manager anzeigen zu lassen.
Das einzige was jetzt noch hilft sind Firewall und Anti Viren Programme.
Aber auch Auffälligkeiten wie langsamer PC, öffnendes CD-Rom Laufwerk oder ähnliche ungewöhnliche Dinge sind Anzeichen einer Infektion.

2.4 Was ist Reverse Connection?

Unter Reverse Connection versteht man, das nicht der Client sich zum Server verbindet, sondern der Server zum Clienten. Damit das funktioniert, muss der Server die IP des Clienten wissen. Diese muss auch statisch sein, das heißt sie muss immer gleich sein.

Info:

- Die meisten Nutzer des Internets, surfen mit einer Dynamischen IP-Adresse, das heißt sie ändert sich mit jeder neuen Einwahl ins Internet! Eine statische IP-Adresse hingegen nicht. Die meisten Provider bieten die Möglichkeit an, eine Statische IP zu bekommen, aber das kostet extra.

Statt einer Statischen IP reicht auch eine DynDNS aus.

DynDNS:

- Eine DynDNS (Dynamischer Domain Name System) teilt einer IP-Adresse einen Domain-Namen zu.
  Z.B. name.no-ip.info
  Dazu wird noch ein Programm benötigt, was ständig diese DynDNS mit der Aktuellen IP-Adresse „versorgt“
  Ein Anbieter ist www.no-ip.com

Anhand der DynDNS versucht der Server sich ständig zu dieser Adresse durch einen bestimmten Port zu verbinden, bis es geklappt hat. Der Client muss nun auf seiner Seite die Verbindung entgegen nehmen. Der Rest ist der selbe wie bei einer „normalen“ Verbindung.

2.5 Was bringt Reverse Connection?

Die Reverse Connection ist immer dann sinnvoll, wenn:

1. man keine Notify per ICQ, Email etc., mit der IP bekommen möchte.
2. wenn der User der infiziert werden soll einen Router benutzt.

Punkt 2 ist wichtig, denn ein Router lässt die Verbindung von außen nicht zu, der Server muss sich mit den Client verbinden. Durch die Reverse Connection ist diese Möglichkeit gegeben. Aber nicht jeder Trojaner hat diese Funktion.

3.Diverses

3.1 Was ist ein Edit Server?

Darunter versteht man eine zusätzliche Möglichkeit, den Server zu konfigurieren, welchen man später verbreiten will. Folgende Möglichkeiten sind meist gegeben:

- IP und Port Angabe
- Notify Auswahl
- Verbinden mit anderer Datei
- Icon Auswahl

- Kill Parameter(Welche Programme beendet werden sollen, wenn der Server ausgeführt wird)
- etc...

3.2 Was sind die bekanntesten Trojaner?

- CIA Trojan 1.3
- Optix Pro 1.3
- ProRat 1.9 / SE / FIX-2
- SubSeven
- BackOrifice
- B2k3
- BiFrost
- Turkojan
- beast

Die meisten diese Trojaner sind zwar frei erhältlich, aber der/die Programmierer solcher Trojaner sehen dies meist als Möglichkeit Geld zu verdienen, man kann diese Trojaner kaufen. Aber warum sollte man?Man hat ihn doch schon.
Man sollte es tun, wenn man will, dass der Trojaner nicht von Anti Viren Programmen erkannt werden soll.
Andere Möglichkeit wäre den Trojaner zu „stealthen“, aber das ist ein kompliziertes unterfangen, was sich so nicht leicht erklären lässt und deshalb den Rahmen dieses Tutorials sprengt.

Stealthen;

- Wer sich damit näher beschäftigen will, sollte sich einen Disassembler besorgen und Assembler lernen. Das stealthen von Servern hängt vom Anti Viren Programm ab, wie es die Dateien „enttarnt“.
  Bei einigen Anti Viren Programmen reicht vielleicht auch ein Hex Editor. Aber vor allen Anti Viren Programmen kann man ein Trojaner nicht stealthen, da die meisten heutigen Viren Programme sich Programmteile als „Erkennungsmerkmal“ aussuchen, die nicht verändert werden können, ohne die Datei zu beschädigen. Da ist die Zeit besser investiert, wenn man sich eine Programmiersprache aneignet. Visual Basic, C++, Delphi um nur ein paar zu nennen, wobei Visual Basic die einfachste wäre.

Das der Trojaner nicht mehr erkannt wird, wenn man ihn kauft, liegt daran weil der Programmierer teile des Programmcodes ändert und somit nicht mehr in das „Profil“ der Anti Viren Programme passt.

4.Schlusswort

Ok, ich denke mal das reicht jetzt. Wenn noch allgemeine fragen offen sind, oder du etwas gefunden hast was nicht ganz stimmt, dann mail mir:

fin_mudsucker_fin@hotmail.com

!!!KEINE FRAGEN ZU SPEZIELLEN TROJANERN!!!

5.Greetings

My Girl- I Love You
FerHat
Sucuk
I.M.S.
KAYA
Black Lotus
Schweio
BIG(LoW ;))
und sonst jedem den ich hier jetzt vergessen habe.

CYa