

# Sicher Surfen VII: Das Trojanische Pferd im Computer-Zeitalter

Georg Wagner

10. Februar 2000

## Zusammenfassung

Das Jahr 1999 wird im Bereich der Computersicherheit als das Jahr der *Trojanischen Pferde* in die Geschichte eingehen. Noch nie wurden so viele und so ausgeklügelte *Trojanischen Pferde* programmiert, wie in diesem Jahr. Die Anzahl mit *Trojanischen Pferden*, die via Email auf den Rechnern der ahnungslosen Opfer installiert wurden, dürfte in die tausende gehen.

## 1 Das Trojanische Pferd – ein antiker Mythos?

Unter einem *Trojanischen Pferd* oder einem *Trojaner* versteht man in der Computerwelt ein Programm, das neben seinen offensichtlichen und manchmal wirklich nützlichen Aktionen, noch andere, verdeckte und unerwünschte Aktionen ausführt. *Trojaner* werden beispielsweise benutzt, um

- Passwörter zu ergattern und zu übermitteln
- Hintertüren, die eine Benutzung Ihres Computers von der Aussenwelt ermöglichen, zu installieren
- Schaden anzurichten (Löschen von Dateien)
- den Rechner zum Absturz zu bringen (nuking<sup>1</sup>)
- Ihren Computer als Ausgangsbasis zum Attackieren anderer Computer zu benutzen

Das *Trojanische Pferd* in der Computerwelt hat also mit dem antiken Vorbild gemeinsam, dass in seinem Innern unangenehme Ueberschungen auf den ahnungslosen Bürger Trojas warteten. Die Bewohner Trojas zogen selbst das von den Griechen hinterlassene Holzpferd in Ihre Stadt – auch das eine Parallele zum Computerbenutzer der fast immer selbst das *Trojanische Pferd* auf seinem Computer installiert.

---

<sup>1</sup>Programme diesen Typs heissen z.B. WinNuke.

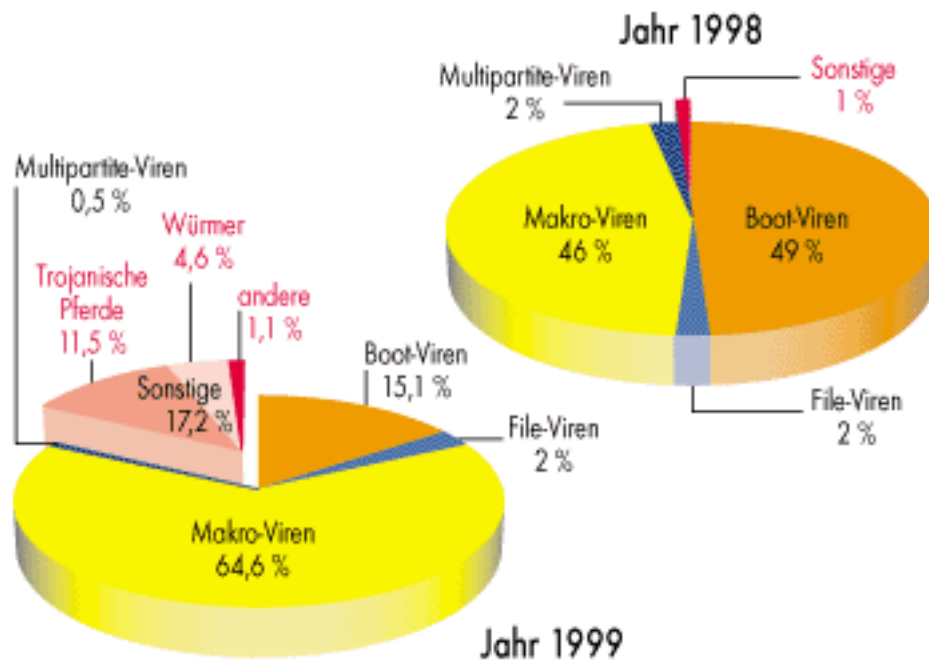


Abbildung 1: Statistik des BSI: 1999 kam es zu einer explosionsartigen Vermehrung von *Trojanern*.

## 2 Armes Troja – armer PC-Benutzer

Das Jahr 1999 wird in der Welt der Computersicherheit auch als das Jahr der *Trojaner* bezeichnet. Unmengen von neuen, immer raffinierteren und einfacheren<sup>2</sup> *Trojanern* wurden entwickelt.

Möchtegern-Hacker brauchen kaum noch Know How, um diese Programme zu bedienen. Sie brauchen nur jemand "Dummen", der ihren *Trojaner* für sie auf seinem Rechner installiert. Meistens sind Sie selbst der "Dumme"; doch dazu kommen wir weiter unten.

Speziell die Betriebssysteme von *Microsoft* machen es den Programmierern solcher Programme sehr leicht. Da gibt es Mechanismen wie *ActiveX*, Macro-Fähigkeiten – sogar in Emailprogrammen – und einige andere "Fähigkeiten" respektive Sicherheitslöcher. In der Computer-Security-Fachwelt werden diese Mechanismen in *Microsofts* Betriebssystemen denn auch als *Accidental Trojans* bezeichnet. Aber auch in Produkten anderer Hersteller sind solche Möglichkeiten vorhanden. Man könnte mit gleichem Recht *Netscape's* JavaScript auch als *Accidental Trojan* bezeichnen.

Prinzipiell sind *Trojaner* aber nicht auf *Microsofts* Betriebssysteme beschränkt, man kann und es werden auch *Trojaner* für andere Betriebssysteme geschrie-

<sup>2</sup>einfach im Sinne von einfach zu bedienen für den Hacker oder Möchtegern-Hacker.

ben. Die Häufung von *Trojanern* auf *Microsoft*-Plattformen liegt, neben den obengenannten Gründen, in der weiten Verbreitung dieses Betriebssystems in der Bürowelt. Eine weitere Erleichterung für den Hacker ist die heute – besonders in Firmen – übliche *Microsoft*-Monokultur. Der Hacker weiss vom Betriebssystem, über den Browser, dem Mailprogramm bis hin zur Textverarbeitung, was er auf einem fremdem Rechner zu erwarten hat. Eine Abstimmung eines Trojaners auf die Zielplattform stellt somit kein Problem dar.

## 2.1 Wie gelangt ein Trojaner auf Ihren Computer?

In den allermeisten Fällen werden Sie einen *Trojaner* per Email erhalten. Wer kennt Sie nicht, die Emails mit Anhängseln wie `greetings.exe`. Klicken Sie darauf, wird eine nette – meist animierte – Grafik angezeigt, die Ihnen zum Beispiel Fröhliche Weihnachten wünscht, und im Hintergrund den *Trojaner* installiert<sup>3</sup>. Kommt die Email angeblich<sup>4</sup> noch von jemand, den Sie kennen, dann sind Sie umso eher bereit, neugierig auf das angehängte Programm zu klicken.

Andere *Trojaner* erhalten Sie, indem Sie ein Programm aus dem Internet per FTP oder Internet-Browser herunterladen, weil Sie glauben, dass dieses Programm für Sie nützlich ist. Meistens stimmt dies auch, aber nebenbei wird ein *Trojaner* installiert. Oder es existiert eine modifizierte Version eines bekannten, harmlosen Programms, dem ein *Trojaner* angehängt wurde.

## 2.2 SubSeven als Beispiel für einen modernen Trojaner

Das SubSeven-Paket besteht im wesentlichen aus drei Programmen:

- Dem Server (das ist der Teil, der über einen *Trojaner*, der auf dem Computer des Opfers – also auf Ihrem Computer – installiert wird).
- Dem Client, ein Programm mit dem der Hacker den Server und somit Ihren Computer über das Internet hinweg steuern kann; und
- einem Konfigurationsprogramm, mit dem der Server bevor er zu seinem Opfer geschickt wird, konfiguriert wird.

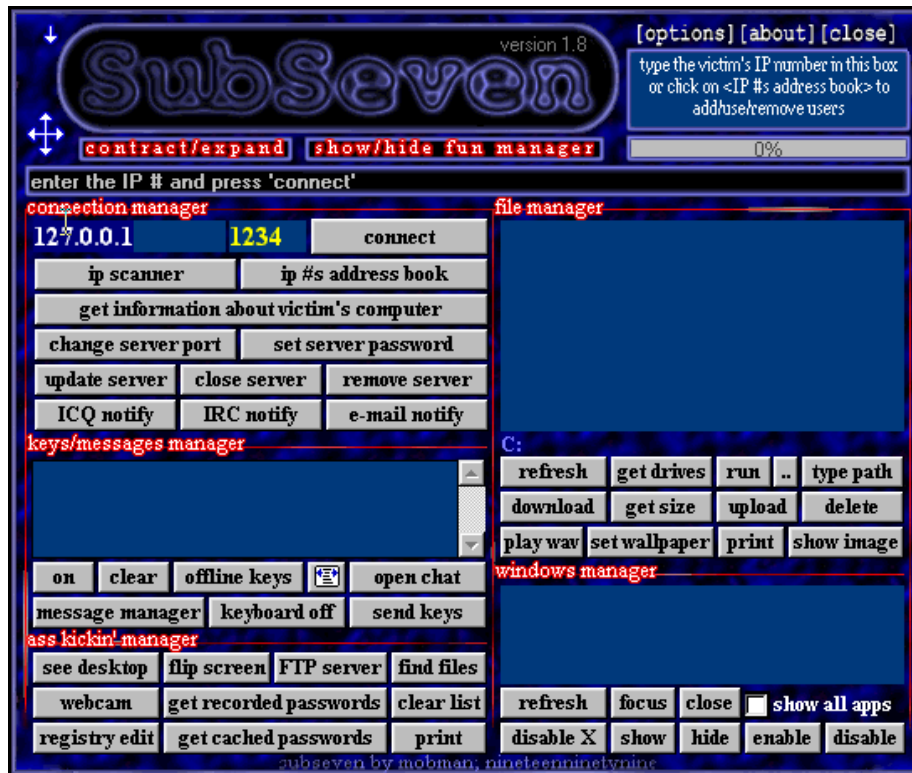
Hat sich der Server erst einmal über ein *Trojanisches Pferd* auf Ihrem Computer eingeknistet, meldet er sich jedesmal selbständig bei dem Hacker, wenn Sie mit dem Internet verbunden sind.

Damit Sie eine Ahnung bekommen, was der Hacker mit SubSeven auf Ihrem Computer alles anstellen kann, möchte ich Ihnen ein Bild des Client-Programms zeigen.

---

<sup>3</sup>Es existieren mehrere Programme, die es dem Hacker erlauben, seine Programme an normale Programme anzuhängen und von diesen installieren zu lassen.

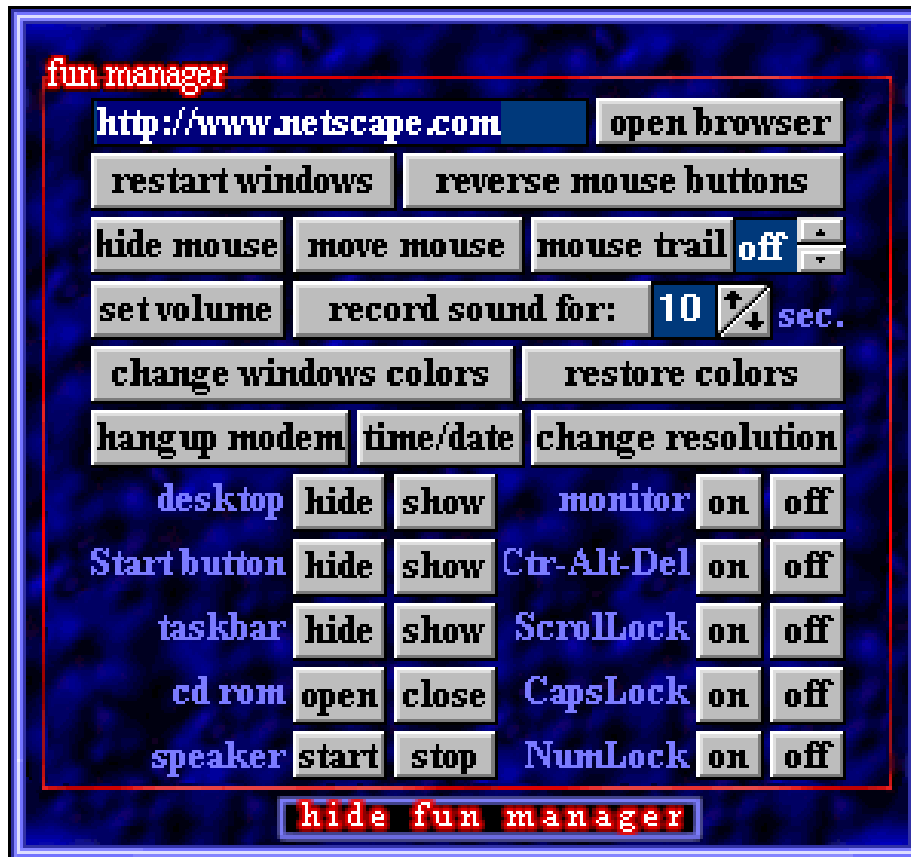
<sup>4</sup>Es kann auch sein, dass ein Kollege ahnungslos dieses Programm angehängt hat, weil er es nett fand und selbst nicht weiss, dass dieses Programm ein Trojaner ist.



Wie Sie sehen können, ist die Oberfläche von SubSeven in 5 Fenster unterteilt; nämlich in den:

- *connection manager*, der die Verbindungsaufnahme von und zu den Computer der Opfer steuert. Der Hacker kann sich ueber 3 verschiedene Kanäle informieren lassen, wenn sein Opfer über das Internet erreichbar ist.
- *key/messages manager*, erlaubt unter anderem die Fernsteuerung der Tastatur der Opfer
- *ass kickin' manager* (Verarschungsmanager), mit dem einige Bosheiten auf dem Computer des Opfers angestellt werden können. Es können auch Passwörter gesammelt werden.
- *file manager*, mit dem Dateien gelesen und geschrieben werden können.
- *windows manager*, mit dem der Hacker sehen kann, was sein Opfer gerade auf seinem Bildschirm hat.

Sie sehen, der Hacker kann Ihnen sogar die Tastatur sperren, wenn ihm danach ist. Neben diesen 5 Managern gibt es noch einen weiteren, der eine eigene Benutzeroberfläche hat. Dieser nennt sich *fun manager*.



Mithilfe des *fun manager* kann der Hacker Katz und Maus mit seinem Opfer spielen. Der *fun manager* erlaubt:

- einen Neustart von *Microsoft Windows* auszulösen
- verschiedene Manipulation der Maus (Mauszeiger verstecken, Funktion der Maustasten vertauschen, bewegen der Maus ...)
- Farben zu verändern
- Diverse Komponenten von *Microsoft Windows* unbrauchbar zu machen (verstecken von Startmenü, Desktop, Taskbar, CDROM usw.)
- Ausschalten von Bildschirm, Ctrl-Alt-Del, Scrolllock, Capslock, Numlock, ...
- Die Soundkarte auf Aufnahme schalten, sodass er Sie hören kann, wenn ein Mikrophon angeschlossen ist.

### 3 Kassandra ruft — bitte hinhören

Die Bewohner Trojas zogen das *Trojanische Pferd*, obwohl sie von Kassandra gewarnt wurden, in Ihre Stadt. Vielleicht hätten Sie auch dann noch die Katastrophe verhindern können, wenn sie wachsamer gewesen wären.

Auf dem Computer ist es ähnlich: Ist der *Trojaner* erst einmal auf Ihrem Rechner, brauchen Sie entweder selbst sehr viel Know How oder einen Experten, um ihn wieder zu entfernen. Besser ist es, dass *Trojanische Pferd* aussen vor zu lassen; womit wir bei der Prophylaxe wären.

#### 3.1 Verhaltensmassregeln

- Surfen Sie nie von einem PC aus, der vertrauliche Daten enthält.
- Öffnen Sie keine ausführbaren Email-Attachments!
- Lassen Sie sich Winword-Dokumente nur im RTF-Format zusenden. Dokumente mit der Endung DOC können Makros und somit Viren/*Trojaner* enthalten.
- Schalten Sie die Makro-Unterstützung in allen Programmen aus und deaktivieren Sie ActiveX.
- Laden Sie keine Dateien aus dem Internet herunter, es sei denn die Quelle ist absolut vertrauenswürdig.

#### 3.2 Technische Massnahmen

- Verwenden Sie Viren-Scan-Programme; Sie können *Trojaner* zum Teil erkennen.
- Zum Entfernen von *Trojanern* eignet sich:  
The Cleaner [www.moosoft.com/cleaner.html](http://www.moosoft.com/cleaner.html)
- Installieren Sie einen Firewall.
  - Kommerzielle sind:
    - \* BlackICE [www.networkice.com](http://www.networkice.com) ist ein IDS<sup>5</sup>
    - \* AtGuard [www.atguard.com](http://www.atguard.com), [wrqdownload.wrq.com/techprev/atgd322u.exe](http://wrqdownload.wrq.com/techprev/atgd322u.exe)
    - \* ConSeal Private Desktop: (A certified personal firewall for the non-technical user.)
    - \* Conseal PC Firewall, [beidewww.signal9.com/products/index.html](http://beidewww.signal9.com/products/index.html)

---

<sup>5</sup>Intrusion Detection System, also eine Ergänzung zu einem Firewall

- Gratis: ZoneAlarm [www.zonelabs.com](http://www.zonelabs.com). Aber Achtung, dieser Firewall schickt Ihre Emailadresse an den Hersteller zurück, auch wenn Sie bei der Installation angeben, dass Sie dies nicht wünschen. Daher: Erst installieren, konfigurieren und testen ohne Verbindung zum Internet.
- Für Spezialisten:  
Installieren Sie NukeNabber [www.dynamicsol.com/puppet/nukenabber.html](http://www.dynamicsol.com/puppet/nukenabber.html) oder Inzider [ntsecurity.nu/toolbox/](http://ntsecurity.nu/toolbox/). Beide zeigen an, welche Prozesse auf welchen Ports lauschen.

## Referenzen

- Bundesamt für Informationssicherheit [www.bsi.de](http://www.bsi.de)
- The SubSeven Trojan [www.sans.org/y2k/subseven.htm](http://www.sans.org/y2k/subseven.htm)
- Documents and Links about firewalls [www.oddsites.com/firewall/](http://www.oddsites.com/firewall/)
- Das Trojanische Pferd im Computer-Zeitalter [www.free-x.ch/pub/trojans.pdf](http://www.free-x.ch/pub/trojans.pdf)