

Trojaner



von Stefan Seperant

Übersicht

„Trojanische Pferde“

- Woher kommt der Name?
- Begriffsdefinition
Trojaner, Backdoors & Viren.
- Ablauf einer Trojaner-Infektion.
- Wie sind Trojaner aufgebaut?
- Arbeitsweise eines Trojaners.
- Trojaner-Funktionen (Beispiel)
- Erweiterte Funktionen
- Abhilfe
 - Anti-Trojaner Tools
 - Firewalls
 - Manueller Schutz vor Trojanern

Woher kommt der Name „Trojanisches Pferd?“

- **Name kommt von der Stadt Troja.**
- **Über 10 jährige Belagerung der Stadt durch die Griechen.**
- **Odysseus ersinnt die kriegsentscheidende List:**
 - Belagerung wird scheinbar aufgegeben.
 - Griechen hinterlassen ein großes Holzpferd mit Soldaten im Inneren als „Geschenk“.
 - Trojaner ziehen das Pferd in die Stadt.
 - Soldaten im Pferd öffnen ihrer Armee die Tore zur Stadt.
- **Troja wird niedergebrannt, nur wenige überleben.**

Nach dem gleichen Prinzip funktionieren moderne Trojanische Pferde!

Unterschiede Trojaner, Backdoors, Viren.

Trojaner:

Gibt vor ein harmloses Programm (z.B. ein Spiel etc.) zu sein, führt dann aber in Wirklichkeit eine Schadfunktion auf dem infizierten Rechner aus.

Backdoors:

Backdoors öffnen „Hintertüren“ im Betriebssystem, um Angreifern einen Zugang zum System zu ermöglichen.

- Andere Bezeichnung „RAT“ (Remote Administration Tool).
- Heute die häufigste Form der Trojaner.

Viren / Würmer:

sind keine Trojaner, da Selbstverbreitungsmechanismen vorhanden sind.

Hybride:

Viren-Wurm-Trojaner-Kreuzungen, die alle Eigenschaften vereinigen.

Ablauf einer Trojaner Infektion.

- „Mithilfe“ des Anwenders ist erforderlich:

- Datei muss mindestens einmal vom Anwender gestartet werden.

- Einschleusen ins System durch Hybride:

- Anwender muss keine Datei starten.
- Anwender erfährt in der Regel nichts von der Infektion.
- Wurm- Virus installiert den Trojaner.

Ablauf der Infektion:

1. Angreifer schickt den Trojaner
2. Empfänger startet die erhaltene Datei

1. Angreifer schickt den Trojaner

Verschieden Transportwege möglich:

- Email
- Messenger Programme
(ICQ, AIM, MS-Messenger etc.)
- Filesharing-Dienste
(E-Donkey, Gnutella, Bittorrent usw.)

An: mc@anti-trojan.net
Cc:
Betreff: Guck dir das mal an!
Anlagen:  tolles-spiel.exe (228 KB)

Hallo!

Du mußt dir unbedingt mal dieses
geniale neue Spiel ansehen, welches
ich soeben im Internet gefunden habe!

...

Trojaner ist immer eine ausführbare Datei. (.exe .bat .js usw.)

Bei Filesharing-Diensten neuerdings auch Musikdateien!

**Allein das Empfangen stellt keine Gefahr dar.
Trojaner liegt inaktiv auf der Festplatte!**

2. Empfänger startet die erhaltene Datei



- einmaliges Starten der Datei reicht aus.
- Trojaner setzt Autostarteinträge im System.

Beispiele:

- Autostartsektion in der Registry
 - Früher gerne: autoexec.bat, config.sys, win.ini usw.
 - Als Plugins unterschiedlicher Programme
 - Als Active-X Komponenten in der Registry
 - usw.
-
- Ursprünglich gestartete Dateien werden oft gelöscht.

Wie sind Trojaner aufgebaut?

Backdoor-Trojaner bestehen immer aus zwei Komponenten:

1. Trojaner-Server (Host)

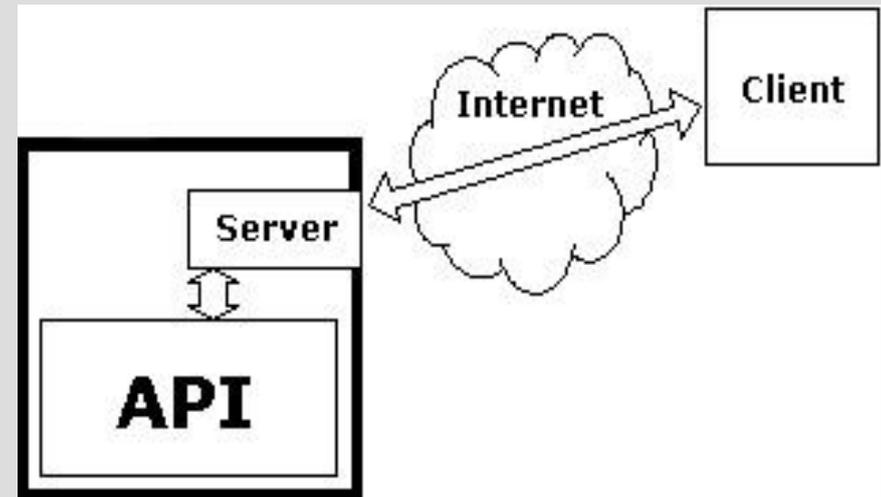
- Server wird auf dem Opfer-PC installiert.
- Server öffnet einen oder mehrere Ports zur Kommunikation.

2. Trojaner-Client

- Client kann sich über die geöffneten Ports mit dem Server verbinden.
- Schädliche Aktionen können durchgeführt werden.

Arbeitsweise eines Trojaners

- Der Trojaner-Server stellt die Schnittstelle zur API (Application Programming Interface) des Opfer-PCs dar.
- Client verbindet sich via Internet oder LAN mit dem Server.
- Angreifer kann je nach Umfang des Servers verschiedene Funktionen auf dem Opfer-System ausführen.



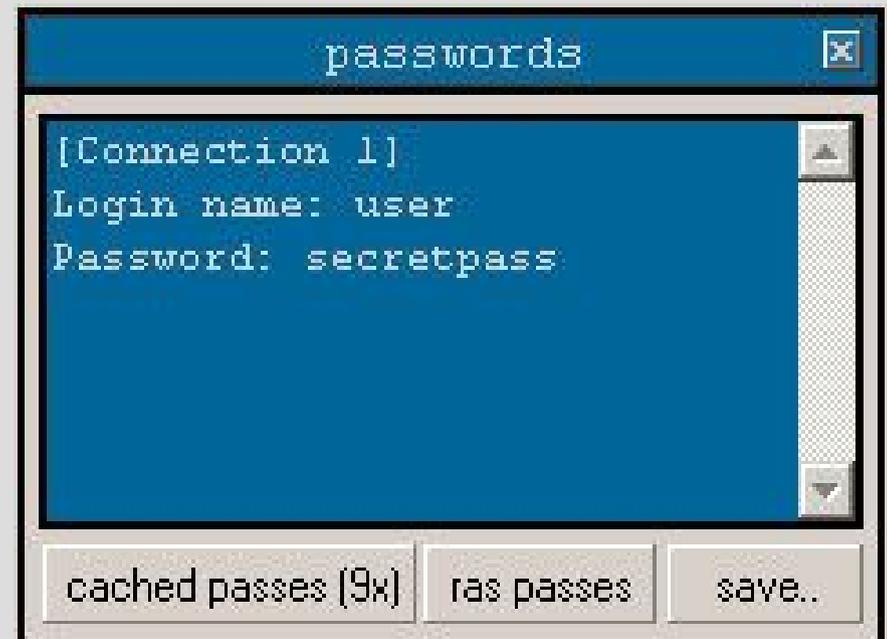
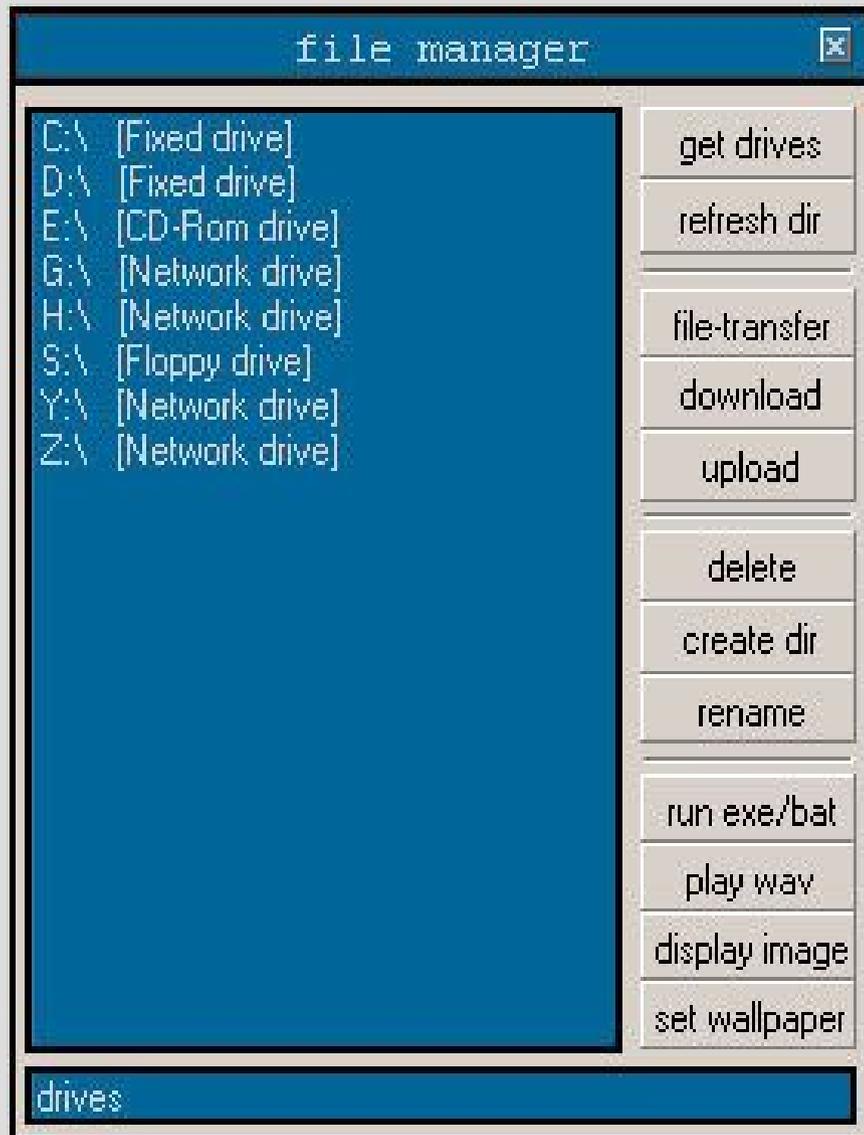
Trojaner Funktionen

am Beispiel „NET DEVIL“ Ver. 1.5

Funktionen:

- Filemanager (Ordner und Dateien erstellen und editieren)
- Passwörter ausspähen
- Prozesse anzeigen und beenden
- Fenster abfragen
- Chat mit Opfer
- Webcam fernsteuern
- Screenshots erstellen
- Keylogger (Tastaturanschläge aufzeichnen)
- Systemregistrierung editieren

Komplette Verzeichnisstruktur des Opfer-Systems kann abgebildet werden:



Passwörter können ausspioniert und verändert werden!



Prozesse können, wie beim Taskmanager unter Windows, angezeigt und terminiert werden.

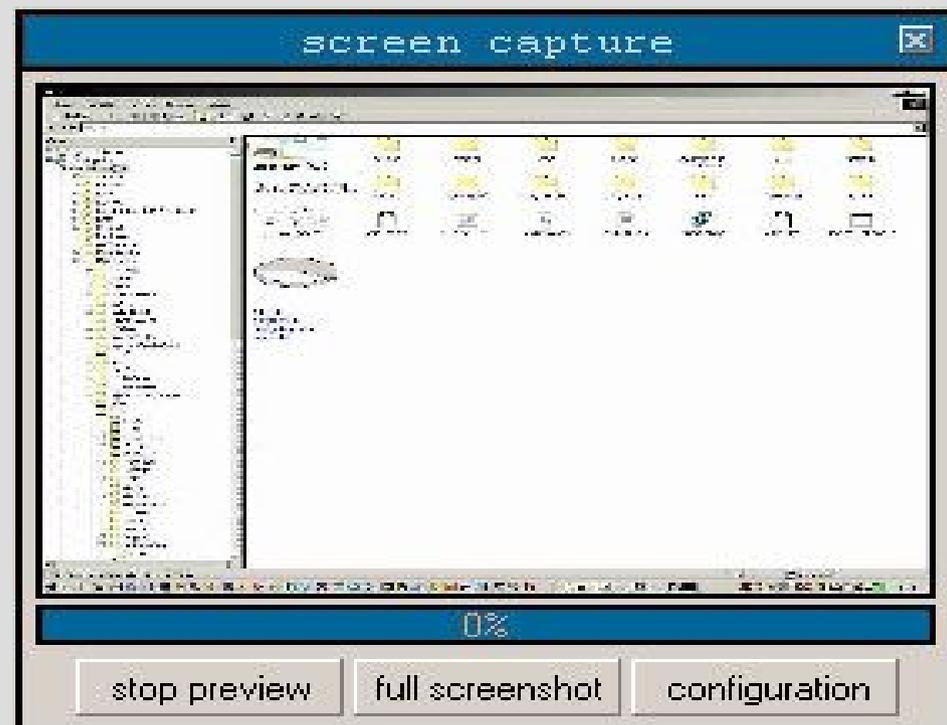
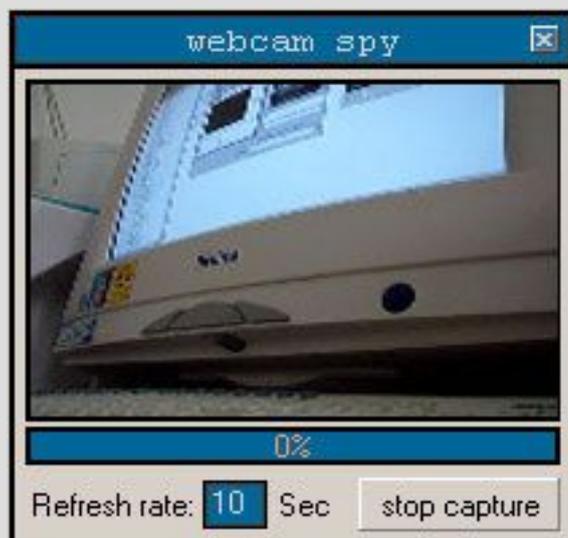


Verschafft dem Angreifer einen Überblick über die auf dem Opfer-System geöffneten Fenster.



Das Opfer kann in eine Unterhaltung verwickelt werden!

Fernsteuern einer Webcam.

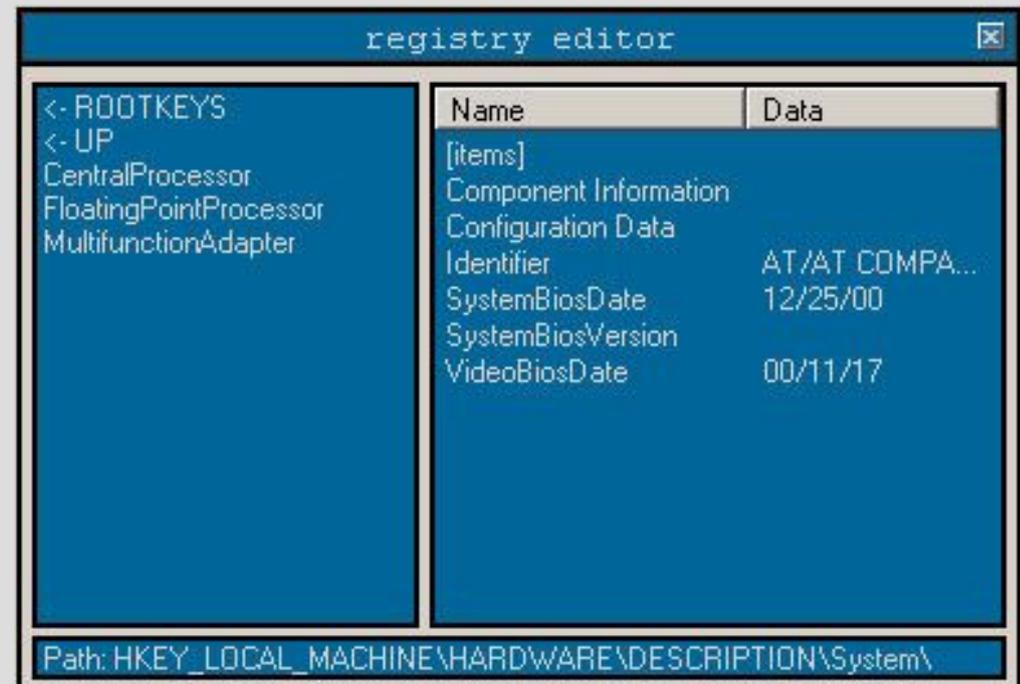


Es können Screenshots des Opfer-Systems erstellt werden.



Mit dieser Funktion kann der Angreifer die Tastaturanschläge, die auf dem verseuchten System ausgeführt werden, aufzeichnen.

Es wird dem Angreifer ermöglicht die Systemregistrierung zu verändern. Das bedeutet, dass weitere Schadprozesse gestartet werden können usw. Dem Angreifer stehen alle Möglichkeiten offen, das System zu manipulieren.



Erweiterte Funktionen

- Plugins

Es können durch den Angreifer erstellte Programmteile dem Server hinzugefügt werden. (Viren-Baukästen!)

- Manipulation der Windows API

System kann so manipuliert werden, dass Trojaner-Server-Datei nicht mehr sichtbar ist. (Trojaner Optix)

- Deaktivieren von Firewalls und Virenschannern

Moderne Trojaner schaffen es die Schutzmechanismen des Opfer-Systems auszuschalten.

- Umgehen von Personalfirewalls

Kommunikationsmodul wird in bekannte Anwendung injiziert, z.B Internet-Explorer. Browserhijacking! (Trojaner Assassin 2)

Abhilfe

- Anti-Trojaner Tools
- Firewalls
- Manueller Schutz vor Trojanern

Anti-Trojaner Tools

- Grundsätzlich alle handelsüblichen Virens Scanner (AntiVir, ...)
- Trojancheck
- Adaware
- Spybot
- etc.

Firewalls

1. Filterung der übertragenen Daten

- es kann ein Übertragen von bekannten schädlichen Dateien verhindert werden.
- keine Hilfe bei bereits im Netzwerk aktiven Trojanern (andere Infektionswege z.B Datenträger wie USB Sticks usw.)

2. Portblockerfirewalls

- es kann die Kommunikation auf bestimmten Ports gesperrt werden.
- für die Kommunikation mit dem Internet müssen einige Ports geöffnet sein. (Port 80, Port 21, Port 25, Port 110) -> nur „relativ“ sicher.

3. Proxyserver oder NAT

- Bieten nahezu keinen Schutz, da der Datenverkehr vom Trojaner-Server von innerhalb des Netzwerks initiiert werden kann und somit die Kommunikationsports geöffnet werden.

Manueller Schutz vor Trojanern

1. Vorsicht mit Dateien

- alle ausführbaren Dateiendungen (.exe, .vbs, .doc, .com, .scr, .js, .hta, .wsf, ...)
- nur E-Mailanhänge aus vertrauenswürdiger Quelle (?!)
- Vorsicht bei Downloads

2. Updates

- System und Anwendungen immer auf dem aktuellen Stand

3. Programme und Ports im Griff

- Auf dem System laufende Prozesse sollten alle bekannt sein!
- Überprüfung der hergestellten Verbindungen mit NETSTAT!

NETSTAT /?: gibt Informationen über die Syntax.

NETSTAT -a: zeigt alle Verbindungen an.

NETSTAT -o: zeigt die zugehörige ProzessID.

- Überprüfen der geöffneten Ports mit Online Portscanner!

4. Autostarteinträge im Griff

Autostarteinträge überprüfen

Startmenü – Autostart: Wird von Trojanern kaum genutzt, da sehr leicht zu finden.

autoexec.bat: Kaum von Windows-Trojanern genutzt, hauptsächlich für DOS-Programme verwendet.

config.sys: Ebenfalls hauptsächlich für DOS-Programme.

system.ini: Beim Eintrag „shell=“ können Programme geladen werden.

win.ini: Über die Sektionen „run=“ und „load=“ werden manchmal Trojaner geladen.

Systemregistrierung (Registry)

So gut wie alle neuen Trojaner nutzen die Registry um automatisch geladen zu werden.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

sowie

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices

Beispiel: TR/Dldr.Harnig.BD.1 - Trojan

Verbreitungsmethode:

- Keine eigene Verbreitungsroutine

Aliases:

- Kaspersky: Trojan-Downloader.Win32.Harnig.bd
- TrendMicro: TROJ_DLOADER.COH
- Bitdefender: Trojan.Downloader.Small.YU

Betriebssysteme:

- Windows 98
- Windows 98 SE
- Windows NT
- Windows ME
- Windows 2000
- Windows XP
- Windows 2003

Auswirkungen:

- Lädt Dateien herunter
- Lädt schädliche Dateien herunter
- Setzt Sicherheitseinstellungen herunter

Vorher

Windows Task-Manager

Datei Optionen Ansicht ?

Anwendungen Prozesse Systemleistung Netzwerk

Name	PID	Benutzername	CPU-Au...	Speicher...
wdfmgr.exe	1932	LOKALER DIENST	00	1.596 K
avguard.exe	1832	SYSTEM	00	19.804 K
avgnt.exe	1828	steseq	00	3.600 K
mdm.exe	1812	SYSTEM	00	2.756 K
ctfmon.exe	1648	steseq	00	2.660 K
VMwareUser.exe	1632	steseq	00	2.616 K
VMwareTray.exe	1612	steseq	00	2.404 K
spoolsv.exe	1504	SYSTEM	00	4.280 K
explorer.exe	1448	steseq	00	23.320 K
mspaint.exe	1428	steseq	00	17.180 K
cmd.exe	1396	steseq	00	84 K
taskmgr.exe	1392	steseq	08	4.056 K
svchost.exe	1208	LOKALER DIENST	00	4.300 K
svchost.exe	1140	NETZWERKDIENT	00	3.120 K
svchost.exe	1072	SYSTEM	00	20.060 K
svchost.exe	972	NETZWERKDIENT	00	3.936 K
svchost.exe	880	SYSTEM	00	4.760 K
rwptqeqj.exe	800	steseq	00	6.484 K
lsass.exe	724	SYSTEM	00	936 K
services.exe	712	SYSTEM	00	3.980 K
winlogon.exe	668	SYSTEM	00	788 K
csrss.exe	644	SYSTEM	00	1.180 K
smss.exe	572	SYSTEM	00	372 K
sched.exe	300	SYSTEM	00	3.692 K
svchost.exe	204	SYSTEM	00	4.012 K
VMwareService.exe	180	SYSTEM	00	1.684 K
System	4	SYSTEM	00	212 K
Leerlaufprozess	0	SYSTEM	92	16 K

Prozesse aller Benutzer anzeigen

Prozess beenden

Prozesse: 28 CPU-Auslastung: 8% Zugesicherter Speicher: 130444K

Nachher

Windows Task-Manager

Datei Optionen Ansicht ?

Anwendungen Prozesse Systemleistung Netzwerk

Name	PID	Benutzername	CPU-Au...	Speicher...
wdfmgr.exe	1932	LOKALER DIENST	00	1.596 K
avguard.exe	1832	SYSTEM	00	19.824 K
avgnt.exe	1828	steseq	00	3.600 K
mdm.exe	1812	SYSTEM	00	2.748 K
mspaint.exe	1788	steseq	00	12.964 K
guardgui.exe	1776	steseq	00	3.880 K
ctfmon.exe	1648	steseq	00	2.660 K
VMwareUser.exe	1632	steseq	00	2.616 K
VMwareTray.exe	1612	steseq	00	2.404 K
spoolsv.exe	1504	SYSTEM	00	4.280 K
explorer.exe	1448	steseq	00	24.556 K
cmd.exe	1396	steseq	00	84 K
taskmgr.exe	1392	steseq	06	4.184 K
svchost.exe	1208	LOKALER DIENST	00	4.292 K
svchost.exe	1140	NETZWERKDIENT	00	3.120 K
svchost.exe	1072	SYSTEM	00	20.036 K
svchost.exe	972	NETZWERKDIENT	00	3.936 K
svchost.exe	880	SYSTEM	00	4.740 K
guardgui.exe	832	steseq	00	3.824 K
rwptqeqj.exe	800	steseq	00	6.484 K
lsass.exe	724	SYSTEM	00	1.204 K
services.exe	712	SYSTEM	00	3.980 K
winlogon.exe	668	SYSTEM	00	912 K
csrss.exe	644	SYSTEM	02	1.280 K
smss.exe	572	SYSTEM	00	372 K
sched.exe	300	SYSTEM	00	3.692 K
ytjdqmv.exe	236	steseq	00	748 K
svchost.exe	204	SYSTEM	00	4.044 K
VMwareService.exe	180	SYSTEM	00	1.684 K
System	4	SYSTEM	00	212 K
Leerlaufprozess	0	SYSTEM	92	16 K

Prozesse aller Benutzer anzeigen

Prozess beenden

Prozesse: 31 CPU-Auslastung: 8% Zugesicherter Speicher: 134500K

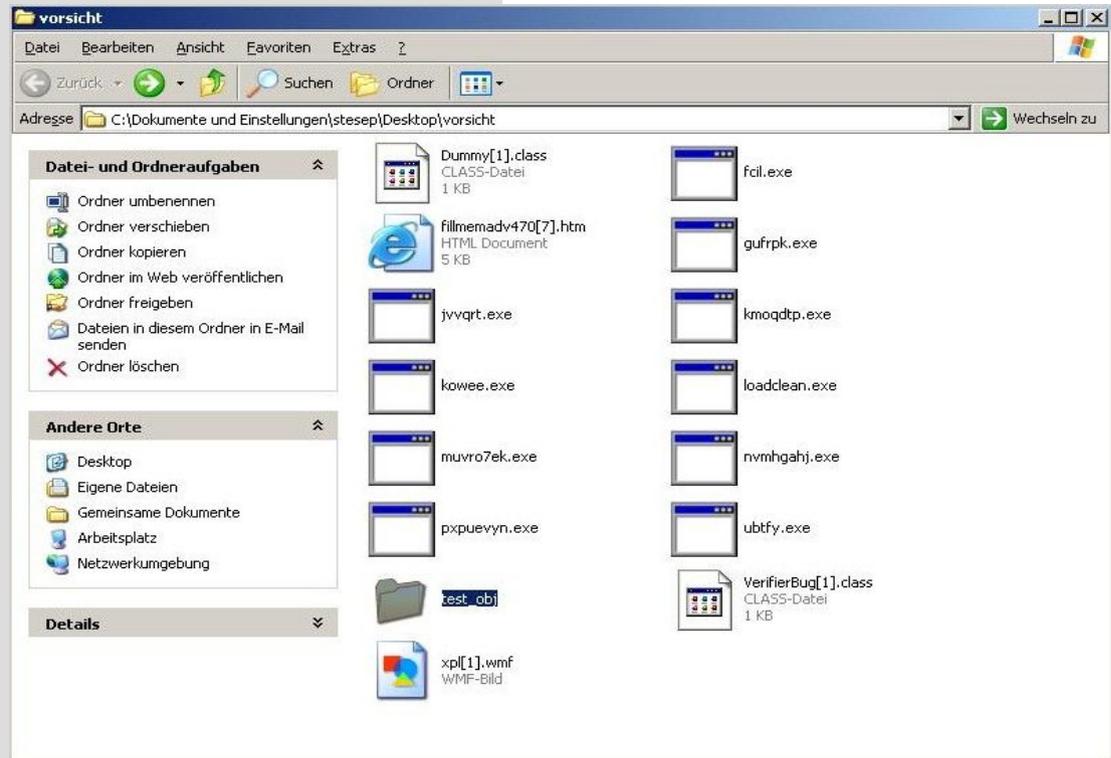
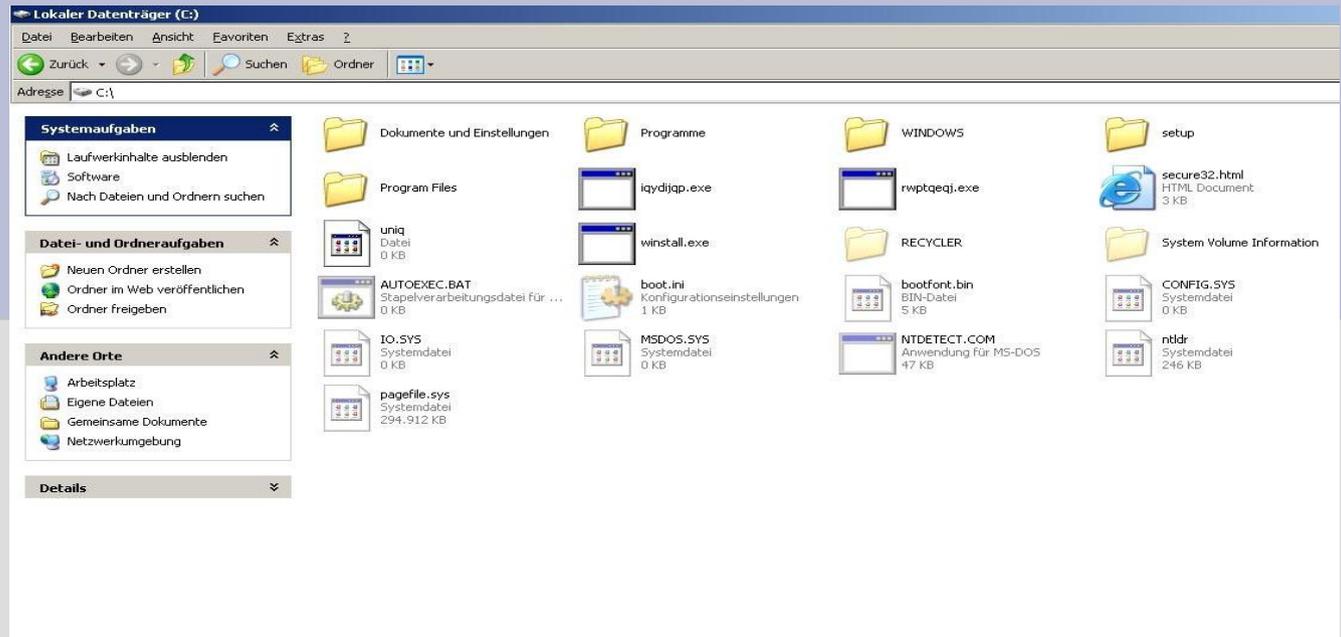
Starteinträge in der Registry

The screenshot shows the Windows Registry Editor window titled "Registrierungs-Editor". The left pane displays a tree view of the registry, with the path `Arbeitsplatz\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` selected. The right pane shows a list of registry values:

Name	Typ	Wert
(Standard)	REG_SZ	(Wert nicht gesetzt)
avgnt	REG_SZ	"C:\Programme\AntiVir PersonalEdition Classic\avgnt.exe" /min
SysTray	REG_SZ	C:\Dokumente und Einstellungen\stesepe\Desktop\vorsicht\Neuer Ordner\ytjdmv.exe
VMware Tools	REG_SZ	C:\Programme\VMware\VMware Tools\VMwareTray.exe
VMware User Pro...	REG_SZ	C:\Programme\VMware\VMware Tools\VMwareUser.exe

The status bar at the bottom of the window displays the path: `Arbeitsplatz\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`.

Verdächtige Dateien Im Wurzelverzeichnis nach der Infektion mit dem Trojaner.



Sonstige Viren, Würmer
und Trojaner die durch die
Infektion auf das System
gelangt sind.

Zusammenfassung:

Grundsätzlich gilt:

- Vorsicht vor „Geschenken“ jeglicher Art. Man muss nicht alle Geschenke annehmen und schon gar nicht auspacken!
- Man sollte immer einen Überblick haben was auf dem eigenen Rechner läuft!
- Alle ein- und ausgehenden Verbindungen sollten kontrolliert werden.

Vielen Dank für Ihre Aufmerksamkeit.



Quellen:

Bilder:

<http://www.smial.de/virus/>

<http://www.schulphysik.de/troja1.jpg>

<http://www.trojaner.info/>

<http://www.anti-trojan.net/>

Inhalte:

<http://www.trojaner.info/>

http://de.wikipedia.org/wiki/Trojanischer_Krieg#Das_Troianische_Pferd

[http://de.wikipedia.org/wiki/Trojanisches_Pferd_\(Computerprogramm\)](http://de.wikipedia.org/wiki/Trojanisches_Pferd_(Computerprogramm))

<http://www.anti-trojan.net/>

<http://www.antivira.com>