



Informationen über Computerviren und Spionagemöglichkeiten

1. Trojanische Pferde	4
1.1. Was sind Trojaner?.....	4
1.2. Wozu sind Trojanische Pferde in der Lage?	4
1.3. Was kann ein Trojaner?.....	4
1.3.1. Dateimanager.....	4
1.3.2. FTP-Server.....	5
1.3.3. Keylogging	5
1.3.4. Passwortspionage.....	5
1.3.5. Registryeditor	5
1.3.6. Webcam- und Screencapturing.....	5
1.4. Erkennung Trojanischer Pferde.....	6
1.4.1. Viren- oder Trojanerscanner.....	6
1.4.2. Autorun-Einträge überprüfen.....	6
1.4.3. Als "Explorer.exe" auf Laufwerk C:\	6
1.4.4. Laufende Prozesse überprüfen.....	6
1.5. Schutz vor Trojanischen Pferden	6
2. Spione auf dem PC	7
2.1. Web-Bugs.....	7
2.2. Spyware.....	8
2.3. Phonehome	8
3. Viren	9
3.1. Virenarten.....	9
3.1.1. Bootviren	9
3.1.2. Companion-Viren	9
3.1.3. Dateiviren	10
3.1.4. Filesystem-Viren	10
3.1.5. Makroviren	10
3.1.6. Polymorphe Viren.....	10
3.1.7. Retroviren	10
3.1.8. Stealth-Viren.....	10
3.1.9. Würmer	11
3.2. Virenschutz.....	11
4. Rootkits	12
4.1. Was sind Rootkits?.....	12
4.2. Grundsätzliches zu Windows Rootkits	12
4.3. Definition	13

4.4. Rootkit-Arten	13
4.4.1. Kernel-Mode Rootkits	13
4.4.2. User-Mode Rootkits oder auch Datei-Rootkits genannt.....	14
4.5. Wie werden Rootkits übertragen?	14
4.6. Wofür werden Rootkits benutzt?.....	14
4.6.1. Beispiele für Rootkitverwendungsarten:	14
4.7. Wie gefährlich sind Rootkits?	14
4.7.1. Beispiel-Rootkit.....	14
4.8. Wie sieht ein Schutz vor Rootkit-Infektion aus?	15
4.9. Windows-Rootkits aufspüren.....	15
4.9.1. Signaturbasierte Erkennung.....	15
4.9.2. Heuristische Erkennung.....	15
4.9.3. Kreuzverhör	15
4.9.4. Integritätschecks	15
4.10. Programme zum Aufspüren von Rootkits.....	16
4.11. Was ist zu tun bei Verdacht auf Rootkit-Befall?.....	16
5. Dialer, 0900/0190-Einwahl-Programme.....	17
5.1. Was sind Dialer?	17
5.2. Vortäuschen falscher Tatsachen.....	17
5.2.1. Die Frau aus dem Chat	17
5.2.2. Unerwünschte Downloads	17
5.2.3. Einige 0190-Dialer verhalten sich wie Trojanische Pferde	18
5.2.4. Verbindung getrennt! Wirklich getrennt?.....	18
5.2.5. Angeblich gecrackte Dialer-Software.....	18
5.2.6. Es wird keine 0190-Servicenummer, sondern eine andere Vorwahl verwendet	18
5.2.7. Vortäuschen einer Sicherheitslücke.....	19
5.3. Woran erkenne ich Dialer-Software?	19
5.4. Wie kann ich mich dagegen schützen?	19
5.4.1. Der beste Schutz ist 0190 sperren zu lassen	19
5.4.2. DFÜ-Verbindung neu einstellen.....	20
5.4.3. Schutzsoftware gegen ungewünschte 0190 Einwahl	20
5.4.4. Einwahlkosten bei Mehrwertnummern.....	20
5.5. Häufig gestellte Fragen	21
6. Phishing – Passwort angeln mit Köder	22
6.1. Vorgehensweise beim Phishing	22
6.2. Wie schütz ich mich vor Phishing?	22
7. Pharming und Hijacking	23
7.1. Was ist Pharming/Hijacking?.....	23
7.2. Welche Arten des Pharming/Hijacking gibt es?	23
7.3. Wie werden diese Einstellungen vorgenommen?	23
7.4. Was kann ich dagegen machen?.....	23
7.5. Hilfreiche Programme zum Aufspüren und beseitigen von Pharming/Hijacking.....	24

8. Junk-Mails (SPAM®)	25
8.1. Was ist Junk oder SPAM®?.....	25
8.2. Wie kommen die Spammer an meine E-Mail-Adresse?	25
8.3. Was kann ich gegen Junk/Spam machen?.....	25
9. Botnetze	26
9.1. Was sind Bots und was sind Botnetze?.....	26
9.2. Wie gefährlich sind Botnetze?	26
9.3. Wie verbreiten sich Botnetze?.....	27
9.4. Wie kann man Botnetze entfernen?	27
10. Hoaxes	28
10.1. Hoaxes, was ist das?.....	28
10.2. Was ist so schlimm an einem Hoax?.....	28
10.3. Einige Hoax-Arten und wie man sie erkennen kann.....	28
10.4. Was soll man mit Hoaxes machen?.....	28
11. Cookies	29
11.1. Was sind Cookies und welche Arten gibt es?	29
11.2. Sind Cookies gefährlich?	29
11.3. Welche Cookie-Einstellungen sind sinnvoll?	29
12. Dateiendungen	30
12.1. Alleine ausführbaren Dateien unter Windows	30
12.2. Endungen von weiteren gefährlichen Dateianhängen	30
13. Quellen, weitere Informationen und Programmseiten	31
13.1. Quellen und weitere Informationen.....	31
13.2. Interessante Programmseiten.....	31

1. Trojanische Pferde

1.1. Was sind Trojaner?

Trojanische Pferde sind Programme, die eine schädliche Funktion beinhalten. Oftmals verfügen Trojanische Pferde über eine für den Anwender nützliche Funktion. Die schädliche Funktion läuft dabei unbemerkt im Hintergrund ab.

Einmal aktiviert installieren sich viele Trojaner so auf dem System, das sie bei jedem Systemstart mitgestartet werden. Somit läuft dieses Programm ständig im Hintergrund mit.

Andere Trojanische Pferde starten wiederum erst, wenn ein bestimmter Vorgang auf dem System stattfindet, z.B. der Start eines Programms.

1.2. Wozu sind Trojanische Pferde in der Lage?

Die meisten Trojaner sind darauf aus, private Daten, z.B. Benutzerdaten eines Online-Dienstes, auszuspähen. Oft sogar auf einem bestimmten Provider zugeschnitten. Trojaner, die ständig im Hintergrund im betroffenen System mitlaufen, zeichnen mitunter sämtliche Tastaturfolgen auf. Dieses bedeutet, alle Daten, die der Anwender über die Tastatur eingibt, werden protokolliert. Hier nutzt es leider gar nichts, wenn der Anwender sein Passwort für einen Online-Dienst nicht abspeichert, sondern erst bei der Anmeldung eingibt.

Diese Arbeitsweise von Trojaner ist als sehr gefährlich einzustufen, da diese die Eigenschaften besitzen können, an sämtliche Daten eines Anwenders zu gelangen.

Andere Trojaner sind so programmiert, dass sie sich die Dateien auf einem System suchen, wo ein Programm (z.B. Onlinesoftware, FTP-Mail - Programme) die Passwörter des Nutzers abspeichert. Viele Anwender nutzen auch heute leider noch die Funktion des Abspeichern von Passwörtern, damit diese nicht immer wieder neu eingegeben werden müssen. Man muss sich aber bewusst sein, dass diese Funktionen ein erhöhtes Sicherheitsrisiko darstellt.

Die dritte Art von Trojanischen Pferden nennt man auch Serverprogramme. Sie ermöglichen dem Hacker auf das betroffene System zuzugreifen. Diese Trojaner sind mit Abstand die gefährlichsten, die es zurzeit gibt, da sie sehr oft alle auf dieser Seite genannten Arbeitsweisen vereinen.

Server-Programme sind in der Lage zum Aufzeichnen der Tastaturfolgen, Auslesen von Passwörtern, herunter- und/oder hochladen von Dateien von/auf Ihr System. Der Hacker hat dabei vollen Zugriff auf Ihren Rechner und kann fast alles machen, was er gerade möchte. Diese Trojaner bestehen aus einem Client-Programm, welches auf Ihrem Computer installiert ist und benutzt wird um auf Ihr System zugreifen zu können, dies ist der eigentlichen Trojaner, und dem Server-Programm, welches auf dem Rechner des Angreifers installiert ist.

1.3. Was kann ein Trojaner?

Im Folgendem wird beschrieben, welche Möglichkeiten ein Trojaner hat und wozu diese eingesetzt werden. Dies soll verdeutlichen, welche Gefahr von solchen, scheinbar harmlosen, Programmen ausgehen. Die Palette reicht von trivialen Spielereien bis zu wirklich ernsthaften Funktionen wie Keylogging.

1.3.1. Dateimanager

Ein sehr effizientes Werkzeug ist der Dateimanager, über den praktisch jeder Trojaner verfügt. Im Grunde ist dieser vergleichbar mit einem lokalen Dateimanager wie zum Beispiel dem Explorer. Er bietet praktisch den gleichen Funktionsumfang mit dem kleinen Unterschied, dass sich Daten auch vom Zielrechner herunterladen lassen.

1.3.2. FTP-Server

Einige Trojanerserver haben zudem noch einen bereits integrierten FTP-Server im Funktionsumfang, mit dem es dann nicht nur möglich ist, Dateien vom Zielrechner herunterzuladen, sondern auch auf diesen zu verschieben. So wäre es zum Beispiel ohne Weiteres möglich, damit einen Virus auf Ihren Rechner Hochzuladen und zu aktivieren. Weit verbreitet ist auch der Einsatz als Datei- und E-Mail-Server. Ohne das Sie es wissen, wird Ihr Computer dazu eingesetzt um Werbe-E-Mails zu versenden oder um illegale Programme/Bilder zu verteilen. So einen Rechner bezeichnet man auch als Zombie. Versuchen Sie Mal der Polizei zu erklären, wie Kinderpornobilder auf Ihren Rechner kommen!

1.3.3. Keylogging

Beim Keylogging wird jeder Tastendruck den sie tätigen in einer Logdatei protokolliert und auf Ihrem Rechner abgespeichert. Der Angreifer kann diese Datei beim nächsten Kontakt mit Ihrem Rechner einsehen oder herunterladen. Eine elegantere Möglichkeit bietet zum Beispiel das Programm „Sub Seven“. Bei diesem ist es möglich, den Server so zu konfigurieren, dass er automatisch jedes Mal wenn Sie sich ins Internet einwählen im Hintergrund die Logfiles per E-Mail an den Angreifer übermittelt. So ist es ein Leichtes an Ihre Passwörter und Kreditkartennummern zu gelangen, wenn sie diese über Ihre Tastatur eingegeben haben. Da nützen selbst die besten Verschlüsselungstechniken nichts, denn es werden ja die Tastenanschläge geloggt und die lassen sich nicht ohne Weiteres verschlüsseln.

1.3.4. Passwortspionage

Eine der Hauptaufgaben von Trojanern ist, wie oben beschrieben, dass Ausspionieren von Benutzerdaten aller Art. Diese Passwortspione zeigen zum Beispiel den Inhalt verschiedener Dateien an, in denen oft Passwörter abgelegt werden.

1.3.5. Registryeditor

Mit einem solchen Registryeditor, über den auch sehr viele Trojaner verfügen und der im Grunde ähnlich arbeitet, wie das Programm „regedit.exe“ ist es möglich, Daten innerhalb der Windowsregistry, dem Herz aller Windows-Betriebssysteme, zu verändern, was unter Umständen verheerende Folgen haben kann da praktisch alle wichtigen Funktionen von Windows über diese Registry koordiniert werden.

1.3.6. Webcam- und Screencapturing

Screencapturing ermöglicht es dem Angreifer, Ihnen direkt auf den Ihren Desktop zu sehen, und Ihre Arbeit zu verfolgen. Dies ist mit einem Screenshot zu vergleichen, der in regelmäßigen Abständen von Ihrem Desktop geschossen und an den Angreifer übermittelt wird. Aber abweichend von einem bloßen Screenshot ist es dem Angreifer über die Trojaner-Software möglich, selbstständig auf dem Ihrem Desktop tätig zu werden. Er kann zum Beispiel wie sie selbst auch per Mausclick Anwendungen öffnen oder schließen.

Webcamcapturing funktioniert in ähnlicher Weise, nur dass der Angreifer hier den Datenstrom einer bei Ihnen installierten und aktiven Webcam anzapfen kann. Er kann somit die von Ihnen mittels Webcam aufgezeichneten Bilder empfangen.

1.4. Erkennung Trojanischer Pferde

1.4.1. Viren- oder Trojanerscanner

Zunächst sollte der Anwender sich einen Virens scanner kaufen oder aus dem Internet herunterladen. Sehr viele Hersteller bieten eine in den Funktionen uneingeschränkte Testversion zum Ausprobieren an.

1.4.2. Autorun-Einträge überprüfen

In der Regel macht ein Trojaner nur dann "Sinn", wenn er sich auf dem System dahingehend installiert, indem dieser bei jedem Systemstart ausgeführt wird. Das bedeutet: Der Trojaner läuft ständig im Hintergrund des Systems mit und "wartet" nur darauf, bis der User eine Onlineverbindung aufbaut. Hier sind einige Möglichkeiten aufgelistet, die dafür zuständig sind ein Programm automatisch zu starten.

- **Autostart-Ordner**
- **Win.ini**
- **System.ini**
- **autoexec.bat**
- **Config.sys**
- **Winstart.bat**
- **Wininit.ini**
- **progman.ini**
- **control.ini (theoretisch möglich, bisher ist jedoch noch kein Fall bekannt)**
- **Windows-Registrierung**
- **Tarnung als Gerätetreiber**

1.4.3. Als "Explorer.exe" auf Laufwerk C:\

Aufgrund eines Bugs in Windows wird immer zunächst die erste „explorer.exe“ ausgeführt (also in Verzeichnis C:\), bevor die eigentliche explorer.exe (in c:\windows\) gestartet wird. Die „explorer.exe“ in c:\ kann bewirken, dass ein Trojaner geladen wird.

1.4.4. Laufende Prozesse überprüfen

Häufig kommt man einem Trojaner schon auf die Schliche, indem man die so genannten laufenden Prozesse überprüft. Bei „laufenden Prozessen“ handelt es sich um ausführbare Dateien, die gerade im System „mitlaufen“.

1.5. Schutz vor Trojanischen Pferden

Einen 100%igen Schutz gibt es nur, wenn Sie überhaupt keine neuen Programme auf Ihrem System zulassen. Wenn man jedoch einiges beachtet, ist die Gefahr erheblich geringer sich einen Trojaner einzufangen.

Sie sollten keine Programme aus unbekanntem Quellen auf Ihrem Computer auszuführen. Dazu gehören z.B. Programme von Internet-Seiten, die einem nicht bekannt sind, oder etwas merkwürdig vorkommen. Es kann auch sein, dass Ihnen unaufgefordert ein Programm per E-Mail zugeschickt wird. Löschen Sie solche Mails bitte vollständig, auch wenn vielleicht doch keine bösen Absichten vom Versender gegeben sind. Sicher ist sicher.

Installieren Sie auf Ihrem Computer einen Virens scanner. Mittlerweile werden auch Trojanische Pferde gut erkannt.

2. Spione auf dem PC

2.1. Web-Bugs

Der Name Web-Bug hat an sich keine besondere Bedeutung und er hat auch nichts mit Fehlern zu tun, wie der darin enthaltene Begriff Bug zunächst vermittelt. Sein Entdecker Richard Smith hat diese Technik in Ermangelung eines besseren Begriffes ursprünglich so benannt und der recht einprägsame Name hat sich dann in der Fachwelt durchgesetzt.

Technisch gesehen ist ein Web-Bug eigentlich eine recht einfache Sache. Statt eine Grafikdatei auf dem gleichen Server abzulegen, auf dem eine Webseite läuft, zeigt die URL des Bildchens auf einen völlig anderen Server, der somit ebenfalls in die Lage versetzt wird, beim Besucher ein Cookie anzulegen. Da auf jedem Webserver zudem ein Protokoll in einer Log-Datei erstellt wird, wird so nebenbei auch die IP-Adresse des Surfers erfasst und gespeichert.

Interessanterweise muss das Bild, das hinter diesem Web-Bug steckt, für den Surfer nicht einmal sichtbar sein. Es genügt ein transparentes Bild im Gif-Format (Blind-Gif), oder Bilder von 1x1 Pixel Größe, die von den Webdesignern übrigens auch gerne dazu benutzt werden, um ihre Seiten korrekt zu formatieren.

Für die Werbefirmen sind Web-Bugs eine praktische Sache, denn im Gegensatz zu herkömmlicher Werbung lässt sich durch den Zugriff auf deren Webserver stets genau ermitteln, wie oft eine Bannerwerbung abgerufen bzw. betrachtet wurde. Verbindet man diese Web-Bugs mit Cookies, sind Werbefirmen dann auch in der Lage zu bestimmen, von wem eine Webseite bzw. die darauf enthaltene Werbung betrachtet wurde und damit die Surfer in Zielgruppen einzuteilen. Durch dieses Monitoring wird eine unmittelbare Erfolgskontrolle über die geschaltete Werbung möglich und ein lang gehegter Wunsch der Werbeindustrie plötzlich wahr: Der gläserne Verbraucher.

Somit kann man kontrollieren, wann ein Empfänger seine Mail liest und ob er anschließend eine bestimmte Webseite besucht, sofern diese ebenfalls wieder den gleichen Web-Bug enthält. Das Ausspähen könnte natürlich auch unbemerkt erfolgen, wenn der Web-Bug ein transparentes Bild enthält und somit vom Leser der Mail unbemerkt bleibt.

Beliebt sind diese Mails vor allem bei den Versendern von Newslettern, oder bei Werbefirmen, die damit eine Kontrolle darüber haben, ob ihre Mails beachtet werden und ob der Leser dem Angebot folgt. Das bedeutet zwar nicht gleich den Weltuntergang, aber sympathisch erscheint eine solche Überwachung sicher nicht, zumal es ohne Wissen des Empfängers geschieht. Ein interessantes E-Mail Programm ist „**The Bat**“. Es kann HTML-Mails darstellen, aber es lädt keine Daten nach. Es wird also nur das gezeigt, was mit der E-Mail gesendet wurde, Web-Bugs sind wirkungslos.

Nicht nur moderne Mailprogramme kommen mit HTML und damit auch mit Web-Bugs zurecht, sondern auch in moderne Dokumentenformate wie z.B. Word-, Access-, Excel- und Powerpoint-Dateien lassen sich Web-Bugs einbetten. Dies ist aber kein Microsoft-spezifisches Problem, sondern kann bei jedem Dokumentformat auftreten, solange es nur in der Lage ist, HTML-Code zu verarbeiten. Verschickt man dann diese präparierten Dokumente per Mail, so lässt sich jederzeit kontrollieren, wann, wie oft und von welcher IP-Adresse das Dokument geöffnet wurde. Vor allem in Firmennetzwerken sind natürlich die IP-Adressen der Rechner meist mit einer Person oder einer Abteilung verknüpft. Wenn nun beispielsweise die Geschäftsleitung ein vertrauliches Dokument an die Buchhaltung versendet, so lässt sich durch eine Überprüfung der IP-Adressen der Empfänger leicht feststellen, ob die Information auch von Unbefugten gelesen wurde.

Verfeinern lässt sich diese Methode noch, wenn man die Dokumente mit individuellen Web-Bugs ausstattet und sie den Empfängern namentlich zuordnet. So lässt sich schnell feststellen, wo die undichte Stelle bei der Verbreitung von vertraulichen Informationen zu finden ist, weil die unerlaubt verbreitete Version beim Öffnen immer exakt die Grafik auf dem Server des Absenders abrufen wird, die dem Empfänger zugeordnet ist, der das Dokument ursprünglich einmal erhalten hat.

Immer mehr Homepages im Internet bieten ihren Besuchern mittlerweile kostenlose und werbefinanzierte Dienste an und naturgemäß steigt damit nicht nur die Anzahl der geschalteten Werbungen, sondern auch die Anzahl der Werbefirmen, die mit Web-Bugs arbeiten. Meist sind auf den populären Webseiten auch gleich Web-Bugs von mehreren Werbefirmen eingebaut.

2.2. Spyware

Ebenso unverschämt wie auch ärgerlich wie die im vorherigen Abschnitt erwähnten Web-Bugs sind bestimmte Shareware-Programme, die unbemerkt Spyware auf dem eigenen PC installieren. Diese Spyware nimmt dann heimlich Kontakt zum Hersteller auf, überträgt dabei statistische Daten über den Benutzer und lädt sogar Werbung auf die eigene Festplatte. Dies geschieht selbst dann, wenn man das Shareware-Programm nicht gestartet oder inzwischen sogar wieder deinstalliert hat, da sich die Spyware unbemerkt in das Betriebssystem einklinkt und schon mit dem Browser geladen wird.

Wozu soll das gut sein? Die Programmierer von Shareware wählen manchmal diesen Weg der Finanzierung, um einen Teil der Unkosten für das Erstellen der Software wieder hereinzuholen. Dabei nehmen sie billigend in Kauf, dass der PC des möglichen Kunden mit Spionagesoftware verseucht wird, die dann unbemerkt Informationen an den Hersteller der Spyware übermittelt.

Wer also schon öfter einmal Shareware auf seinem Rechner installiert hat, sollte sich unbedingt das Programm Ad-Aware herunterladen und damit seinen Rechner prüfen. Eine ständig aktualisierte Liste der verseuchten Software stellt die Firma Radiate freundlicherweise gleich selbst zur Verfügung.

2.3. Phonehome

Während man Spyware beispielsweise mit Ad-Aware recht einfach wieder los wird, weil sie nur Zusatzprogramme darstellen, ist es schon sehr viel unangenehmer, wenn die auf einem PC installierten Programme von sich aus schon den Hersteller kontaktieren. Dieses Verhalten nennt man Phonehome oder aber noch treffender: Heimweh. Dies lässt sich am besten mit einer Firewall, z.B. ZoneAlarm, unterbinden.

3. Viren

Internet und E-Mail beflügeln die Verbreitung von Viren, Trojanischen Pferden und Würmern, hier ist ein schneller Infektionsweg vorhanden.

Die erste Tatsache, die man sich klar machen sollte: Viren sind Programme. Sie kommen als echtes Programm im exe- oder com-Format, als Bootcode für Disketten und Festplatten oder als Makro in einem Dokument. Solange dieser Programmcode nicht gestartet wird, ist er harmlos und kann sich weder verbreiten noch Schaden anrichten. Das Problem: Bei diversen Gelegenheiten führt ein PC solchen Code automatisch ohne Rückfrage aus, zum Beispiel beim Systemstart.

Viren haben zwei Ziele: Sie verbreiten sich, und sie richten Schäden an.

Das Ziel für einen effektiven Schutz vor Viren ist also klar:

- **möglichst alle Wege, auf denen ein Virus in den PC gelangen kann, sperren oder zumindest überprüfen**
- **den Virencode entdecken, bevor er ausgeführt wird,**
- **keine Programme unbekannter Herkunft starten.**

Dazu sollte man über Virenarten und Infektionswege Bescheid wissen. Zurzeit haben Makroviren die größte Verbreitung, gefolgt von den Boot- und Dateiviren und Trojanern.

3.1. Virenarten

3.1.1. Bootviren

Beim Start eines PC liest das BIOS einen exakt festgelegten Bereich der ersten Festplatte aus: Im Master Boot Record (MBR) steckt ein kleines Programm, das dabei aktiviert wird. Es sucht auf der Festplatte nach der Bootroutine der Partition, die als aktiv markiert ist, und startet sie.

Erst jetzt werden die Startdateien des eigentlichen Betriebssystems wie DOS oder Windows aktiviert. Auch jede Diskette hat einen Bootsektor, den der Virus für seine Zwecke nutzen kann. Liegt eine Diskette beim Einschalten im Laufwerk, versucht das BIOS den Bootsektor zu laden und auszuführen, sofern im BIOS-Setup nicht eine andere Bootreihenfolge eingestellt ist. Bootviren ersetzen nun den Startcode im MBR und/oder im Bootsektor der Partition oder Diskette. So wird der Bootvirus aktiv, bevor ein anderes Programm ihn daran hindern kann. Dann kann ein Bootvirus im Hintergrund arbeiten und beispielsweise jede eingelegte Diskette infizieren.

Der Infektionsweg für einen Bootvirus ist klar: Beim Einschalten des PC liegt eine Diskette im Laufwerk und der PC versucht davon zu booten.

Da ein Bootvirus keine Datei zur Verbreitung benötigt, kann auch eine ganz "leere" Diskette einen Bootvirus enthalten. Weil Bootviren so auf scheinbar harmlosen Disketten lange Zeit unbemerkt bleiben, gehören sie zu den hartnäckigsten Vertretern der Viren. Aber Vorsicht: Ein beliebiges Programm, Dropper oder Trojaner genannt, kann beim Start einen Bootvirus auf die Festplatte kopieren. Es gibt sogar einige Makroviren, die so vorgehen. Darüber hinaus gibt es so genannte Multipartite-Viren, welche Eigenschaften von Boot- und Dateiviren vereinen.

3.1.2. Companion-Viren

Dies sind Viren, die den gleichen Dateinamen wie ein Anwendungsprogramm tragen, und die Optionen des jeweiligen Betriebssystems ausnutzen, um vor dem echten Programm zu starten. So würde zum Beispiel ein Virus der den Dateinamen „Editor.com“ besitzt vor der Originaldatei „Editor.exe“ ausgeführt werden. Das liegt daran, dass DOS Dateien mit der Erweiterung „.COM“ Vorrang vor allen anderen ausführbaren Dateien gibt.

3.1.3. Dateiviren

Mit Dateiviren hat alles angefangen: Wenn ein Virus aktiv ist, manipuliert er eine Programmdatei (com oder exe): Er kopiert seinen eigenen Viruscode in den Programmcode hinein. Wenn man das manipulierte Programm startet, wird zunächst der Virus aktiv. Er kann jetzt weitere Programme infizieren oder seine Schadensfunktion ausüben. Danach aktiviert er das Originalprogramm, sodass man nichts von dem Virus bemerkt. Bei der Infektion kann der Virus vorsichtig oder brutal vorgehen: Entweder er sichert die Originaldaten an einer anderen Stelle der Festplatte, oder er überschreibt einfach irgendwelchen Programmcode. Dann kann es passieren, dass das Programm an manchen Stellen abstürzt. Durch das Überschreiben ist es auch ausgeschlossen, dass ein Virens Scanner den Virus rückstandsfrei wieder entfernen kann. Es hilft nur noch löschen.

3.1.4. Filesystem-Viren

Dieser klassische Virentyp verändert den Code einer Programmdatei und bettet sich in das fremde Programm ein. Jedes Mal, wenn Sie die infizierte Anwendung aufrufen, beginnt der Virus seine Schadensfunktion auszuüben.

3.1.5. Makroviren

Das Office-Paket von Microsoft verfügt über eine ausgefeilte Makrosprache mit mächtigen Befehlen: VBA (Visual Basic für Applikationen). Mit diesen Befehlen kann ein Makro etwa Dateien und andere Office-Dokumente manipulieren oder Windows-Programme fernsteuern. Der Knackpunkt bei MS-Office: Die Makros sind direkt im Dokument gespeichert. Wenn man ein Word-, Excel-, oder PowerPoint-Dokument weitergibt, sind eventuelle Makros mit dabei. Und es gibt eine Autostart-Funktion. Sobald ein Dokument mit einem entsprechend deklarierten Makro geöffnet wird, wird das Makro aktiv. Dann verändern die meisten Makroviren die Standard-Dokumentvorlage - „normal.dot“ - so, dass der Virus bei jedem Start von Word etc. aktiv wird. Bei anderen Office-Programmen ist die Vorgehensweise im Detail etwas anders. Besondere Brisanz haben Makroviren, die sich selbstständig über E-Mail weiterverbreiten. Das bekannteste Beispiel dafür ist Melissa: Der Virus sucht sich aus der Outlook-Datenbank 50 Empfänger und schickt ihnen eine E-Mail mit dem Virus als Anhang. Wenn der Empfänger den Anhang dann per Doppelklick aktiviert, nistet sich Melissa im System ein. Da die E-Mail von einem bekannten Absender stammt, erhöht die Chance auf einen unbedachten Doppelklick. Mittlerweile gibt es etliche Nachahmer. Grundsätzlich ist jedes Programm, das Makros verarbeiten kann, anfällig für einen Makrovirus.

3.1.6. Polymorphe Viren

Viren werden von Virens Scannern häufig an bestimmten Code-Sequenzen erkannt. Polymorphe Viren versuchen der Erkennung zu entgehen, indem sie ständig veränderte Kopien von sich selbst erstellen.

3.1.7. Retroviren

Die Ziele von Retroviren sind weniger Anwendungsdaten, als vielmehr Antiviren-Programme. Sie löschen gezielt die Dateien von Antivirus-Software.

3.1.8. Stealth-Viren

Stealth-Viren tarnen sich, indem sie Systemprogramme manipulieren. Durch diese Veränderungen zeigt das Betriebssystem zum Beispiel nicht an, dass eine verseuchte Datei größer geworden ist oder dass Sie wegen des laufenden Virus weniger Hauptspeicher zur Verfügung haben.

3.1.9. Würmer

Ein Wurm ist ein Trojanisches Pferd, das sich selbst an neue Empfänger verschickt. Damit der Wurm aktiv werden kann, muss der Empfänger das Programm selbst starten.

Das Peer-To-Peer-Netzwerk von Windows 95/98/ME/NT und XP erlaubt den Zugriff auf die Festplatten fremder PCs. Standardmäßig ist diese Freigabe gesperrt, aber viele Anwender haben die Option aktiviert. Der Wurm sucht gezielt nach solchen freigegebenen Laufwerken und installiert sich dann selbstständig auf solchen Windows-Laufwerken.

3.2. Virenschutz

Die Abwehrmaßnahmen lassen sich auf einen Punkt bringen: Verhindern Sie, dass fremder Programmcode ungeprüft auf Ihrem PC ausgeführt wird. Das gilt für Programme genauso wie für Dokumente mit Makros.

- Öffnen Sie keinerlei Word- oder Excel-Dokumente, die Sie per E-Mail von einem unbekanntem Absender erhalten. Benutzen Sie vorher zumindest einen Virens Scanner, am besten löschen Sie die Dateien. Seien Sie auch bei einem bekannten Absender vorsichtig.
- Besondere Viren wie Melissa benutzen den E-Mail-Account infizierter PCs zur Weiterverbreitung. Fragen Sie deshalb im Zweifelsfall lieber noch einmal nach. Besonders eine englische E-Mail von einem deutschen Bekannten sollte Sie stutzig machen.
- Starten Sie keine Programmdateien, die Sie als E-Mail-Anhang erhalten. Dateien eines unbekanntem Absenders sollten Sie gleich löschen. Jedes beliebige Scherz- oder Hilfsprogramm kann Träger eines Virus/Trojaners sein.
- Verändern Sie im BIOS-Setup die Bootreihenfolge so, dass direkt von der Festplatte C gebootet wird. Damit verhindern Sie das Eindringen von Bootviren über Disketten oder bootfähige CD-ROMs.
- Und natürlich sollten Sie ein Antiviren-Programm benutzen. Virens Scanner haben ein deutliches Limit: Sie erkennen nur solche Viren sicher, die bereits bekannt sind. Bei der Suche nach neuen Viren verwenden die Scanner so genannte Heuristiken. Das sind Programmmodule, die nach virentypischen Code-Abschnitten suchen. Üblicherweise greifen Programme zum Beispiel nicht auf den Master Boot Sektor oder andere Programmdateien zu. Natürlich kann es dabei zu Fehlermeldungen kommen, je nach Empfindlichkeit der Heuristik.
- Sorgen Sie dafür, dass von den wichtigen Dateien, also den arbeitsintensiven Dokumenten, Backups vorhanden sind. Dabei sollten Sie mehrere Versionen sichern. Windows und Programme lassen sich nach einem Totalschaden wieder installieren - die Rekonstruktion des Inhalts von Dokumenten kann aber viel Zeit, Mühe und Geld kosten.
- Ein weiteres Manko unter Windows ist, dass standardmäßig die Einstellung „Dateinamenerweiterung bei bekannten Dateitypen ausblenden“ aktiviert ist. Bekannte Endungen sind z.B.: exe, com, txt, vbs, doc. Eine Datei mit dem Namen „Liesmich.txt“ erscheint dann nur noch als „Liesmich“ und eine Datei mit dem Namen „Liesmich.txt.vbs“ erscheint dann als „Liesmich.txt“. Fast jeder Benutzer meint im letzterem Fall eine Textdatei vor sich zu haben und denkt nicht daran, dass ja keine Dateierweiterungen angezeigt werden. Ein Klick auf diese Datei öffnet dann nicht den Editor mit dem Text, sondern startet ein „Visual Basic Script“. Als Empfehlung sollte jeder sich die Dateierweiterungen anzeigen lassen. Dazu im Explorer auf „Ansicht“ gehen, dort auf Ordneroptionen...“. Hier wieder „Ansicht wählen und anschließend das Häkchen von „Dateinamenerweiterung bei bekannten Dateitypen ausblenden“ entfernen.

4. Rootkits

4.1. Was sind Rootkits?

Der Begriff Rootkit stammt aus der Zeit der UNIX-Systeme. Rootkits wurden für UNIX-Betriebssysteme genutzt, um die User-Rechte auf den Root-Level auszudehnen (=Administrator). Ein Rootkit ist eine Sammlung von Softwarewerkzeugen, die (nach dem Einbruch in ein Computersystem) auf dem System installiert werden. Rootkits für Windows arbeiten allerdings vollkommen anders und dienen normalerweise dazu, schädlichen Code zum Beispiel vor einem Virenschanner zu verbergen.

Die starke Zunahme von Rootkits scheint Antiviren- Unternehmen offenbar unerwartet getroffen zu haben, denn kein bekanntes Virenschutzsystem ist zur Zeit in der Lage, Rootkits zu erkennen oder gar beseitigen zu können.

Während Trojaner, Würmer und andere Schädlinge dieser Art auf "User" Ebene des Betriebssystems arbeiten und daher noch leichter zu erkennen sind, arbeiten Rootkits im "Kernel" Modus des Systems und kann hier auf sämtliche Systemaufrufe zugreifen und manipulieren. Mit Systemaufrufe sind in der Tat Basisfunktionen des Betriebssystems gemeint, mit denen das gesamte System kontrolliert und beliebig manipuliert werden kann. So können beispielsweise Ordner versteckt und unbemerkt benutzt oder Ports geöffnet werden, ohne eine Chance für den Anwender, dies zu bemerken.

Entfernen oder stoppen lassen sich Rootkits mit Virenschanner oder Firewallsystem nicht, weil Rootkits auf anderer und sehr viel tieferer Ebene arbeiten. Liegt der Verdacht auf Infizierung mit einem Rootkit nahe, ist eine komplette Formatierung der Festplatte sowie Neuinstallation von System und Anwendungen unabwendbar. Das funktioniert aber nur in den Fällen, wenn die Startbereiche von Datenträgern nicht betroffen sind.

Hilfreiche Software oder Funktionen wie die Windows Systemwiederherstellung greifen in dem Fall nicht, da Rootkits Systemaufrufe abfangen, die Wiederherstellung bemerken und sich entsprechend in gesperrten, unüberschreibbaren Bereichen selbst schützen.

4.2. Grundsätzliches zu Windows Rootkits

Egal, welche Aktivitäten vom System selbst, Administratoren oder Anwendern ausgelöst werden, Rootkits erkennen, analysieren und kontrollieren bzw. manipulieren sie entsprechend der Ziele des Rootkits. Im simpelsten Fall ist es eine einfache Shell für ungehinderte Zugriffe auf das System und/oder Netzwerk, im schlimmsten anzunehmenden Fall eine vollständige Kontroll- und Steuerungssoftware, mit der praktisch jedes Systemereignis reglementiert wird. Die Ziele sind vielfältig und reichen von der einfachen Spionage bis hin zur gezielten Manipulation von Anwenderdaten.

In den meisten Fällen werden Rootkits benutzt, um Rechner oder ganze Netzwerke kontrollieren zu können. Kompromittierte Rechner oder Netzwerke werden in der Folge als kostenlose Lager für weitere Schädlinge, als Angriffswerkzeuge für verteilte Angriffe oder als Marktplatz für illegale Produkte wie Kinofilme und Ware Software (raubkopierte Software) benutzt. Die realen Besitzer der Maschinen wissen in der Regel nichts von ihrem Glück und können dadurch in peinliche Situationen geraten. Beispielsweise dann, wenn ihre Rechner als Angriffsrechner identifiziert werden oder auch als Lagerstätte für illegale Produkte. Hier die ermittelnden Beamten zu überzeugen, ist nicht immer ganz einfach und hängt wesentlich vom Wissenstand der Ermittler ab.

Rootkits sind mit heute zur Verfügung stehenden Erkennungsmethoden noch schwer identifizierbar und ebenso schwierig sind sie aus laufenden Systemen so einfach wie Trojaner oder Würmer wieder zu entfernen. Rootkits sind unsichtbar im wahrsten Sinn des Wortes und in fast allen Fällen lassen sie sich bestenfalls an ihren Aktivitäten erkennen.

4.3. Definition

- Ein Rootkit ist ein Programm, das
 - Prozesse,
 - Registry Schlüssel,
 - Dateien,
 - Hauptspeichernutzung oder auch Netzwerkverbindungen versteckt.

Der Angreifer versucht damit, so lange wie möglich den Zugriff auf ein kompromittiertes System zu behalten.

Ein Rootkit ist also ein Programm oder ein Paket von Programmen, das ein Einbrecher benutzt, um seine Anwesenheit auf einem Computer zu verbergen, und das ihm auch zukünftig Zugriff auf das System gewährt. Dazu ändert das Rootkit interne Abläufe des Betriebssystems oder es manipuliert Datenstrukturen, auf die sich das Betriebssystem beim Verwalten und Überprüfen verlässt.

4.4. Rootkit-Arten

Der Kern muss vor Anwenderprogrammen geschützt sein, aber diese Anwenderprogramme benötigen bestimmte Funktionen des Kernels. Um das zu gewährleisten, implementiert Windows zwei Modi in denen Code ausgeführt werden kann: den User-Mode und den Kernel-Mode.

Applikationen laufen im User-Mode und User-Mode-Prozesse sind unprivilegiert. Der Kernel-Mode bezeichnet einen Ausführungsmodus, in dem der Prozessor Zugriff auf den gesamten Systemspeicher und alle Prozessorbefehle gewährt. Auch Gerätetreiber von Drittherstellern laufen im Kernel-Mode.

Windows legt zwar fest, welche Privilegien erforderlich sind, um auf Speicherseiten zuzugreifen, aber es schützt Kernel-Speicher nicht vor anderen Threads, die im Kernel-Mode laufen.

Bei der Betrachtung von Windows-Rootkits fällt schnell auf, dass sie sich entsprechend den Privileg-Stufen in zwei Kategorien einteilen lassen: User-Mode und Kernel-Mode. User-Mode-Rootkits laufen als separate Applikation oder innerhalb einer existierenden Applikation. Ein Kernel-Mode-Rootkit hat alle Befugnisse des Betriebssystems und korrumpiert damit das gesamte System.

Beim Betriebssystem Windows wird somit zwischen zwei verschiedenen Rootkit Formen unterschieden:

4.4.1. Kernel-Mode Rootkits

Einem Windows Administrator ist es generell möglich, zur Laufzeit verschiedene Manipulationen am Systemkern durchzuführen. So können beispielsweise Treiber für Geräte installiert werden oder für Software, wie sie eben auch in Desktop-Firewallsystemen vorkommen.

Was der Administration eines Windows Systems hilft, lässt sich auf der anderen Seite auch wunderbar ausnutzen. Kontrolliert ein Angreifer den Systemkern, beherrscht er das gesamte System und auch eventuell an einem Netzwerk angeschlossene weitere Rechner.

Das Kernel-Mode Rootkits fängt jegliche Ereignisse ab, kontrolliert und auch zensiert. Auf diese Weise verhindern es zum Beispiel die eigene Identifikation.

Kernel Rootkits ersetzen Teile des Betriebssystem-Kerns durch eigenen Code, um sich selbst zu tarnen und dem Angreifer zusätzliche Funktionen zur Verfügung zu stellen, die nur im Kontext des Kernels ausgeführt werden können. Dies geschieht am häufigsten durch Nachladen von Kernelmodulen. Unter Windows werden Kernel Rootkits häufig als neuer .sys-Treiber realisiert.

4.4.2. User-Mode Rootkits oder auch Datei-Rootkits genannt

User-Mode Rootkits manipulieren einzelne Prozesse und können primär nicht so tief in das System eingreifen wie Kernel-Mode Rootkits. Als Beispiels ist hierbei der Browser, der selbst auf gut mit Virenschanner und Firewall geschützten Systemen Verbindungen über TCP Port 80 (oder einem Proxy Port) aufnehmen darf, da er sonst nicht benutzt werden kann. Über diese Verbindung können umfangreiche, beliebige Daten nach außen transportiert und verwertet werden.

4.5. Wie werden Rootkits übertragen?

Prinzipiell auf dem gleichen Weg wie alle anderen Schädlinge auch. Auch aus dem Grund ist eine regelmäßige Aktualisierung des Systems und die Nutzung von zur Verfügung gestellten Patches zwingend notwendig. Ausgenutzt wird hierbei die unglücklich gewählte Standard Systemkonfiguration, die nicht alle Dateiendungen anzeigt sondern nur die Dateien mit unbekanntem Datei-Extensionen. So wird aus einem unverfänglichen und harmlos scheinenden Foto namens **meinbild.jpg** sehr schnell die gefährliche Datei **meinbild.jpg.exe**.

4.6. Wofür werden Rootkits benutzt?

Grundsätzlich für alle Angriffsformen. Seien es Angriffe auf andere Server, groß angelegte Phishing - Aktionen, oder einfach nur um die persönlichen Daten auszuspionieren.

4.6.1. Beispiele für Rootkitverwendungsarten:

- **Zum Verstecken von Viren, Würmern, Keyloggern oder anderer Spyware**
- **Ausspähen von Passwörtern**
- **Industrie-Spionage**
- **Web- und FTP-Servern**
- **Backdoors (Hintertüren)**
- **DDOS- oder andere Attacken**
- **SPAM/Junk-Versand**
- ...

Rootkits werden besonders dann gern und häufig benutzt, wenn der Zeitraum des Missbrauchs nicht festgelegt ist oder von vornherein für eine lange und/oder unbestimmte Zeit festgelegt wurde.

4.7. Wie gefährlich sind Rootkits?

Ein Rootkit an sich verursacht typischerweise keinen Schaden. Nutzt ein Virus, Wurm oder ein Backdoor - Trojaner ein Rootkit, kann der Schädling lange Zeit unentdeckt im System bleiben, selbst dann, wenn der PC mit einem handelsüblichen Virenschanner oder Firewall ausgestattet ist. Die Grenze zwischen Rootkits und Trojanischen Pferden ist fließend.

4.7.1. Beispiel-Rootkit

Hacker_Defender ist so ein Rootkit, mit dem Angreifer und insbesondere kriminelle Banden Rechner ohne Wissen des Anwenders kapern und für ihre eigenen Zwecke missbrauchen. Er kann ganze Verzeichnisse verstecken, in denen er dann Dateien, Passwortlisten, illegale Software oder Pornografie speichert. Zudem öffnet **Hacker_Defender** unbemerkt und unidentifizierbar Ports, versteckt seine Prozesse vor neugierigen Augen oder verbirgt sich hinter anderen laufenden Prozessen. Ziel solcher Rootkits ist Spionagetätigkeit, um Passwörter oder Kontodaten zu erhalten, die meist ganze Banden weltweit für Kontoplünderungen benutzen.

4.8. Wie sieht ein Schutz vor Rootkit-Infektion aus?

Zunächst gilt die generelle Empfehlung, sich ein gesundes Misstrauen anzutrainieren. Denn Rootkits werden auch wie alle anderen Schädlinge übertragen. Siehe hierzu auch Kapitel „3.2. Virenschutz“ und Kapitel „12. Dateiendungen“. Öffnen Sie **NIE** ungefragt zugesendete Anhänge aus Ihren E-Mails. Selbst vermeidlich harmlose Anhänge wie Bilder können in Wirklichkeit virenverseucht sein. Speichern Sie die Anhänge immer erst ab und prüfen Sie sie dann mit einem aktuellen Virenschanner, ggf. können Sie die Datei auf der Seite <http://virusscan.jotti.org/de/> hochladen und überprüfen lassen.

Sollte sich auf Ihrem System bereits ein aktiver Trojaner befinden, so könnte ein Angreifer mit Hilfe dieses Trojaners das Rootkit auf Ihren Rechner übertragen und ausführen.

Schädlinge lassen sich weniger leicht installieren, wenn man mit eingeschränkten Rechten arbeitet, also nicht als Administrator. Ein einmal aktiviertes Rootkit hat immer Administratorrechte, selbst wenn der Benutzer nur noch mit eingeschränkten Rechten arbeitet.

Halten Sie Ihr System aktuell und schließen, durch regelmäßige Updates, die Sicherheitslücken des Betriebssystems und der verwendeten Software. Damit verringern Sie das Risiko, dass Ihr System durch Fremde mit Rootkits verseucht wird. Teilweise schließen die Eindringlinge die Sicherheitslücken, um zu verhindern, dass sie von anderen Eindringlingen aus den von ihnen gekaperten System wieder herausgeschmissen werden.

4.9. Windows-Rootkits aufspüren

4.9.1. Signaturbasierte Erkennung

Antivirenprodukte setzen bereits seit Jahren signaturbasierte Erkennungsmethoden ein. Das Konzept ist einfach: Man durchsucht Dateien auf bestimmte, eindeutige Byte-Folgen, die eine Art Fingerabdruck eines Rootkits darstellen. Wird er gefunden, signalisiert das eine Infektion. Da diese Technik traditionell auf Dateien angewendet wird, ist sie bei der Entdeckung von Rootkits wenig nützlich, zumindest sofern sie nicht mit fortgeschritteneren Methoden kombiniert wird. Denn Rootkits neigen dazu, Dateien zu verstecken.

4.9.2. Heuristische Erkennung

Wo Signatur-Scans scheitern, springt die heuristische Erkennung ein. Ihr primärer Vorteil liegt darin, dass sie auch neue, bislang unbekannte Rootkits aufspüren kann. Sie erkennt Abweichungen von "normalen" Verhaltensmustern. Es sind bereits mehrere Heuristiken bekannt, um Rootkits aufzuspüren, die sich in den Ausführungspfad einklinken.

4.9.3. Kreuzverhör

Kreuzverhörtechniken sind bei der Rootkit-Erkennung noch recht neu und viel versprechend. Sie beruhen auf der Tatsache, dass es meist mehr als einen Weg gibt, die gleiche Frage zu stellen. Bei der Kreuzverhörmethode ruft der Scanner die gängigen API-Funktionen auf, um zentrale Systeminformationen abzufragen: Listen der Dateien, der Prozesse oder Registry Keys. Dieselben Informationen ermittelt er mit einem zweiten Algorithmus, der von den API-Funktionen unabhängig ist. Jeder Unterschied in den Ergebnissen zeigt etwas Verstecktes, das aus den Ergebnissen der API-Aufrufe ausgeblendet wurde.

4.9.4. Integritätschecks

Integritätschecks sind eine Alternative zu Signaturen und Heuristiken. Sie beruhen auf dem Vergleich einer Momentaufnahme des Dateisystems oder des Speichers mit einem bekannten, vertrauenswürdigen Grundzustand - der Baseline. Unterschiede zwischen den beiden Schnappschüssen werden als Hinweise auf verdächtige Aktivitäten interpretiert. Allerdings kann ein Integritätscheck normalerweise die Ursache dieser Aktivitäten nicht lokalisieren.

4.10. Programme zum Aufspüren von Rootkits

Wie schon beschrieben, ist es schwer Rootkits aufzuspüren und nahezu unmöglich diese zu beseitigen. Erschwerend kommt hinzu, dass viele Programme noch im BETA-Stadium sind. Dies bedeutet, dass sie noch nicht ausgereift und zuverlässig sind.

RootkitRevealer	http://www.sysinternals.com/Utilities/RootkitRevealer.html
F-Secure BlackLight	http://www.f-secure.com/blacklight/
Rootkit Detector	http://www.3wdesign.es/security/principal.html?u=82pxv20n
RootKit Hook Analyzer	http://www.resplendence.com/hookanalyzer
BitDefender RootkitUncover	http://www.freewarefiles.com/program_9_90_21306.html
WinPatrol	http://www.winpatrol.com/

Aufgrund des BETA-Stadiums können sich die o.g. Adressen noch ändern.

4.11. Was ist zu tun bei Verdacht auf Rootkit-Befall?

Für die Suche nach auffälligen Dateien, Schädlingen, Spyware, Rootkits und anderen Schadensprogrammen reichen die Systemwerkzeuge sowie Virens Scanner und Firewallsystem nicht mehr aus und auch zahlreiche Hilfsprogramme von Dritt-Herstellern sind teils nur bedingt einsetzbar. Selbst Systemkenner können sich in heutiger Zeit nicht mehr ganz sicher sein und aus dem Grund empfehlen wir dringend, unerfahrene Anwender sollten sich lieber direkt nach der ersten Systeminstallation und Anwendungsprogramme ein Image anlegen und dieses dann im Bedarfsfall wieder neu aufspielen.

5. Dialer, 0900/0190-Einwahl-Programme

5.1. Was sind Dialer?

Dialer sind eine Software, die beabsichtigt, oder unbeabsichtigt teure Servicenummer anwählt. Oft werden diese Programme auch "Highspeed-Zugängen" genannt.

Früher mussten die Leistungen einer Webseite per Kreditkarte, Überweisung, Abbuchung o.ä. bezahlt werden und heute kann der Kunde per Telefonrechnung bezahlen, indem die Verbindung über eine 0190-Servicenummer aufgebaut wird. Um die Sache zu erleichtern, werden so genannte Dialer oder auch „Highspeed-Zugänge“ zum Download angeboten. Man lädt sich das Programm herunter, installiert es und wählt sich ein. Der Preis für eine Minute sind in der Regel 2,-- €

Die Idee auf dieser Art und Weise etwas zu verkaufen ist eigentlich gar nicht so schlecht, da der Nutzer auch mehr oder weniger anonym bleiben kann. Vorausgesetzt, der Kunde wird genauestens über die anfallenden Kosten informiert. Leider gibt es jedoch auch sehr dubiose Anbieter, die den Anwender mit voller Absicht täuschen und abzocken.

5.2. Vortäuschen falscher Tatsachen

5.2.1. Die Frau aus dem Chat

Ein ahnungsloser Mann lernt im Chat eine nette Frau kennen. Die Frau verweist auf eine Webseite, wo man sie über eine WebCam betrachten kann. Der Mann muss nur noch das kleine WebCam - Programm von der Webseite laden und es installieren. Danach steht nichts mehr im Wege die Frau mit den eigenen Augen zu sehen. Was dem ahnungslosen Nutzer hier jedoch verschwiegen wird, ist die Tatsache, dass dieses kleine WebCam Programm in Wirklichkeit ein 0190/0900-Dialer ist. Der Blick auf die hübsche Frau kostet 2,-- €/min.

Derartige Praktiken sind keine Seltenheit und werden in verschiedenen Varianten ausgeübt. Ahnungslose Anwender in eine Gebührenfalle tappen zu lassen, könnte ebenso auch per E-Mail oder über andere Wege geschehen.

In ähnlicher Art und Weise werden im übrigen auch immer wieder den Nutzern Trojanische Pferde untergejubelt. Das liebe Mädchen aus dem Chat kommt mit einer Datei auf ihrem Computer nicht klar. Welcher hilfsbereite Mann kann da noch widerstehen, sich die Datei mal anzuschauen? Schon wurde ein Trojanisches Pferd oder eben auch eine 0190-Software installiert.

5.2.2. Unerwünschte Downloads

Beim Betreten einer Webseite wird dem Besucher dieses Webangebotes die Software aufgespielt und installiert, z.B. als ActiveX Plug-in mit dem Hinweis, dass dieses Programm zertifiziert wurden ist, oder dass es notwendig ist, um die Seite korrekt darstellen zu können. Dadurch wird einem suggeriert, dass alles in Ordnung ist. Bei jedem Download geht aber erst ein Fenster auf mit dem Hinweis, dass etwas heruntergeladen oder installiert wird. Dort sollte man dann auf „Nein“ oder „Abbrechen“ klicken. Auf gar keinem Fall auf „**Vom aktuellen Ort aus ausführen**“, denn dies startet das Programm gleich.

5.2.3. Einige 0190-Dialer verhalten sich wie Trojanische Pferde

Diese Dialer legen entsprechende Eintragungen im System an, damit sie bei jedem Start von Windows automatisch mitgestartet werden. Somit ist die Dialer-Software ständig im Hintergrund geladen. Doch noch schlimmer ist, wenn sich die Software selbstständig macht, indem ohne Nachfrage bzw. Hinweise an den Anwender, 0190-Verbindungen aufgebaut werden.

Eine Variante besteht darin, dass die neu angelegte DFÜ-Verbindung als Standardverbindung definiert wird. Viele PC-Anwender haben ihre DFÜ-Einstellungen gleich mit dem Browser oder dem Mailprogramm gekoppelt. Gibt der Nutzer eine Internetadresse in seinen Browser ein, so verbindet die Standardverbindung gleich automatisch mit dem Internet. Wenn der Anwender nun auch sein Zugangspasswort abgespeichert hatte, fällt es gar nicht auf, dass während der gesamten Internetsitzungen eine 0190-Verbindung besteht. Vor der Einwahl wird zwar die Rufnummer angezeigt, aber welcher Anwender achtet schon darauf? Sollte doch das gewohnte Passwort eingegeben werden, so ist das auch egal, da die Verbindung dahingehend durch die Software eingestellt wurde, indem ein beliebiges Passwort eingegeben werden kann. Es braucht wohl nicht erwähnt zu werden, welche enormen Kosten entstehen, wenn sich der Benutzer 50 Std. oder mehr jeden Monat im Web aufhält. Wer über ISDN verfügt, kann sogar noch das große Pech haben, indem der Dialer gleich zwei Verbindungen (also auf beiden Leitungen) aufbaut. So entstehen doppelte Kosten, die kaum ein normaler Mensch noch bezahlen kann.

5.2.4. Verbindung getrennt! Wirklich getrennt?

Der Kunde nutzt ein derartiges Angebot und wählt sich nach einiger Zeit ab. Das Programm bestätigt dieses auch. Aber im Hintergrund bleibt die Verbindung entweder noch für einige Zeit bestehen oder sogar so lange, bis das System komplett heruntergefahren wird.

5.2.5. Angeblich gecrackte Dialer-Software

Auf einigen Webseiten wird eine Dialer-Software angeboten, die den Zugang zu mehreren 1000 Erotik-Angeboten verspricht. Die entstehenden Kosten werden jedoch bewusst verschwiegen. Teilweise verspricht der Webseitenbetreiber auch, dass die gecrackte Software dafür "sorgt", dass gar keine Telefongebühren entstehen.

5.2.6. Es wird keine 0190-Servicenummer, sondern eine andere Vorwahl verwendet

Scheinbar haben mitbekommen, dass viele Internetanwender haben die Anwahl von Rufnummer mit der Vorwahl 0190 durch die Telekom sperren lassen. Denn es ist bereits bekannt, welche hohen Telefonrechnungen eine Dialer-Software über die Einwahl einer teuren 0190-Rufnummer verursachen kann. Einige dubiose Anbieter verwenden aus diesem Grund Vorwahlen, die für Onlineprovider bestimmt sind (z.B. 0193/0192/0191 etc.). Diese Provider können die Minutenpreise selber bestimmen. Auch hier sind somit Minutenpreise von weit über 2,- € möglich. Trotz "0190-Sperre" ist nun wieder die Einwahl zu teuren Diensten möglich. Auch so genannte Schutzprogramme erkennen weder die Einwahlnummer, noch geht eine Warnung von diesen Programmen bei der Anwahl durch den Dialer aus. Hilfreich ist es hier, immer wieder die DFÜ-Einstellungen von Hand zu überprüfen. Es ist jedoch nicht auszuschließen, dass derartige Dialer-Programme in Zukunft mehr anzutreffen sind. Gerade da viele Anwender gewarnt sind und ihren Telefonanschluss für die Anwahl der Servicevorwahl 0190 gesperrt haben.

5.2.7. Vortäuschen einer Sicherheitslücke

Beim Betreten einer Webseite wird einem der Inhalt der eigenen Festplatte präsentiert. Dazu der Vermerk, dass man ein Sicherheitsproblem hat und jeder den Inhalt der Festplatte auslesen und verändern kann. Zur Abhilfe wird einem eine Software angeboten, die das Problem beheben soll, bzw. mit der man sich Zugang zu einem Archiv mit Sicherheitssoftware verschaffen kann. Tatsache ist aber, dass kein anderer als man selbst den Inhalt der eigenen Festplatte sehen kann und die angebotene Software ist ein Dialer. Ggf. bekommt man den versprochenen Zugang zu einem Archiv mit Sicherheitssoftware, die es sonst überall gratis im Internet bekommt.

5.3. Woran erkenne ich Dialer-Software?

Die meisten Dialer legen eine neue DFÜ-Verbindung an. Diese kann der Anwender über folgenden Weg per Mausklick erreichen:

Arbeitsplatz -> DFÜ-Netzwerk oder Start -> Verbinden mit... (Win XP)

Hier befinden sich alle festgelegten Verbindungen.

Da einige Dialer Verhaltensmuster eines Trojanischen Pferdes an den Tag legen, können die üblichen Methoden zur Erkennung von Trojanern angewendet werden.

Siehe Kapitel **“1.4. Erkennung Trojanischer Pferde“**.

Auch sollte der PC-Anwender stutzig werden, sollte sich ein bisher unbekanntes Icon unten rechts in der Desktop-Leiste befinden (links neben der Uhrzeit).

Wenn der Anwender einen Internetzugang per DFÜ-Netzwerk nutzt, sollte auch die eingestellte Einwahlnummer kontrolliert werden. Kein normaler Provider wird eine Einwahlnummer nutzen, die mit 0190xxx beginnt.

5.4. Wie kann ich mich dagegen schützen?

In jedem Fall sollten keine automatisch angebotenen Downloads bei Eintritt einer Webseite angenommen werden.

Keine Programme unbekannter Herkunft aus dem Web herunterladen und ausführen. Das Gleiche gilt natürlich auch für ausführbare Dateien, die einem unverwünscht per E-Mail übermittelt worden sind. Dabei spielt es keine Rolle, ob der Absender bekannt ist oder nicht. Häufig werden derartige (Spam-) Mails mit gefälschten Absendern verschickt.

5.4.1. Der beste Schutz ist 0190 sperren zu lassen

Gegen eine einmalige Gebühr bietet die Deutsche Telekom seinen Kunden an, die Einwahl zu 0190-Diensten von einem Anschluss aus komplett sperren zu lassen. Dieser Betrag kann sich jedoch sehr schnell bezahlt machen. Verwendet man andere Telefongesellschaften, so sollte man dort nachfragen. Aber wahrscheinlich werden sie so etwas ebenfalls anbieten.

Bei dieser Methode hat kein Dialer mehr die Chance eine dieser Servicenummern durch den Anwender gewollt oder ungewollt anzuwählen.

Laut Auskunft der Deutschen Telekom kann die Sperrung der 0190-Vorwahl durch vorangestellte Call-by-Call Rufnummern nicht umgangen werden. Der Kunde kann zwar vor jeder Servicenummer (z.B. 0190, 0180, 0900, 0137 usw.) die Vorwahl einer anderen Telefongesellschaft wählen, doch wird diese durch die Technik der Telekom ignoriert.

Im übrigen bietet die Telekom verschiedene so genannte Sperrklassen an. Hier steht einem der T-Punkt oder die Hotline mit Rat und Tat zur Seite.

5.4.2. DFÜ-Verbindung neu einstellen

Sollte das Zugangspasswort für den Onlinezugang abgespeichert worden sein, so ist dieses zu entfernen. Man gewöhnt sich sehr schnell daran, das Zugangspasswort vor dem Aufbau einer Verbindung einzugeben. Diese Prozedur hat den Vorteil, indem auf diese Art und Weise hin und wieder auf die Einwahlnummer geschaut wird.

5.4.3. Schutzsoftware gegen ungewünschte 0190 Einwahl

Zwischenzeitlich gibt es auch immer mehr Programme zum Schutz vor der ungewünschten Einwahl über eine 0190-Rufnummer.

YAW-Yet Another Warner	http://www.yaw.at/
0190 Warner	http://www.wt-rate.com
Oleco (Einwahlprogramm)	http://www.oleco.de/
0190 Alarm	http://www.OnlineTimer.de
a-squared	http://www.ants-online.de

Schutz bietet unter anderem auch eine Firewall wie z.B. ZoneAlarm. Dieser meldet jedes Programm, welches Kontakt vom Computer nach außerhalb, bzw. von Außen in den Computer aufnehmen will. Dies kann dann erlaubt oder verboten werden, auch dauerhaft.

Achtung!

Leider gibt es auch zunehmend Dialer im Netz, die 0190 - Schutzsoftware ausschalten oder umgehen können. Diese Programme können somit keinen 100%igen Schutz gewährleisten!

5.4.4. Einwahlkosten bei Mehrwertnummern

Alle Angaben sind natürlich ohne Gewähr und werden auch nicht regelmäßig aktualisiert.

Vorwahl	Abrechnung / Taktung	Kosten
0900-9	flexibel	max. 2 Euro / Minute 30 Euro / Einwahl
0192	flexibel	nach oben offen
0193	flexibel	nach oben offen
0190-0	flexibel	nach oben offen, bekannt bis 300 Euro / Einwahl
0190-8	2-Sekunden-Takt oder sekundengenau	1,855 Euro / Minute
0137-1,2,3,4...	flexibel	pauschal
118x	flexibel	variabel
0088	flexibel	ca. 3 Euro / Minute
0800	kostenlos	kostenlos

5.5. Häufig gestellte Fragen

Kann eine normale, bestehende Internetverbindung während der Onlinesitzung auf eine 0190-Nummer umgelenkt werden?

Soweit mir bekannt ist, ist dies nicht möglich. Es muss erst die bestehende Verbindung getrennt werden und dann die neue Verbindung aufgebaut werden. Ein einfaches JavaScript genügt schon, um ein Hinweisfenster zu erzeugen mit der Meldung: "Sie surfen für 1,855€/Min.", doch handelt es sich hier um einen Scherz des Webseitenbetreibers. Eventuell wurde vorher automatisch ein Programm installiert und der Webseitenbetreiber will mit diesem Trick versuchen, dass der Nutzer seine Verbindung trennt und sich neu einwählt. Diesmal dann natürlich unbemerkt über eine 0190-Nummer.

Kann eine DFÜ-Verbindung die bisher gewohnte Einwahlnummer anzeigen, doch im Hintergrund wird eine teure 0190-Verbindung aufgebaut?

Theoretisch schon. Jedoch nur in dem Fall, wenn auch die Dialer-Software beim Verbindungsaufbau über DFÜ ausgeführt wird. Einige Dialer koppeln diese "Eigenart" miteinander.

Muss ich die Einwahlgebühren bezahlen, obwohl ich mich nie über diese Servicenummern bewusst eingewählt habe?

Laut der Deutschen Telekom ist jeder Kunde für seinen Telefonanschluss selber verantwortlich. Auch, was die Nutzung durch Dritte angeht. Wird ein Betrug seitens einer Anbieterfirma (die Dienste mittels Dialer-Software über 0190 anbietet) vermutet und nachgewiesen, so muss versucht werden, die angefallenen Kosten über diese Firma zu erhalten. Hierbei sollte unbedingt ein Rechtsanwalt zurate gezogen werden.

6. Phishing – Passwort angeln mit Köder

6.1. Vorgehensweise beim Phishing

Beim Phishing (Kunstwort aus Passwort und fischen) wird versucht durch Vortäuschen falscher Tatsachen an Ihre persönlichen Daten zu kommen. Wie beim richtigen Angeln wird auch hier ein Köder benutzt. Dieser Köder kann entweder eine gefälschte E-Mail sein oder eine gefälschte Internetseite. Hat der Benutzer nun so eine E-Mail bekommen oder befindet er sich auf so einer Webseite, so muss man ihn nur noch dazu bringen seine Daten einzugeben. Bei E-Mails muss man dazu sagen, dass sie oftmals versuchen einen ahnungslosen Nutzer auf die gefälschte Seite zu locken.

Webseiten, die gerne nachgebildet werden, sind z.B. Homebanking-Seiten, Postbank, eBay, PayPal.

Eine Gemeinsamkeit bei diesen Webseiten ist, dass man über einen angeklickten Link auf sie gerät. Dieser Link ist dann so gestaltet das man nur schwer erkennen kann, dass er nicht auf die richtige Seite führt. Hat man dort einmal seine PIN/TAN- oder Kreditkartennummer hinterlassen, so steht der Ausnutzung nichts mehr im Wege und das auf legaler Weise.

6.2. Wie schütz ich mich vor Phishing?

- Gehen Sie nie über E-Mails auf Seiten, auf denen Sie Ihre Benutzerdaten eingeben sollen.
- Geben Sie sensible Daten nur auf gesicherten Seiten ein. Zu erkennen am Schloss in der Statusleiste und/oder am <https://> in der Adressleiste.
- Fragen Sie notfalls per Telefon nach, bevor Sie Ihre Daten eingeben.
- Geben Sie die Adressen zu sicherheitsrelevanten Seiten per Hand ein und fügen Sie diese Seite danach Ihren Bookmarks/Favoriten zu.
- Deaktivieren Sie HTML in Ihren E-Mails um Phishing-E-Mails leichter zu erkennen. HTML hat in E-Mails sowieso nichts zu suchen, siehe „[Informationen zur E-Mail-Sicherheit](#)“.

7. Pharming und Hijacking

7.1. Was ist Pharming/Hijacking?

Ähnlich wie beim Phishing soll versucht werden den Internetnutzer auf eine falsche, bzw. gefälschte Internetseite zu locken. Im Unterschied zum Phishing geschieht dies hier allerdings auch, wenn korrekte Links angeklickt werden, die Bockmarks/Favoriten benutzt werden und sogar wenn die gewünschte Adresse korrekt in die Adressleiste eingegeben wird. Der Browser wird dabei unbemerkt auf die falsche Adresse umgeleitet, sozusagen entführt (hijack). Hierbei ist die Gefahr natürlich sehr groß, da selbst korrekt eingegebene Adressen auf falsche Seiten führen und dem Nutzer Schaden zugeführt werden kann.

7.2. Welche Arten des Pharming/Hijacking gibt es?

Einmal können die Favoriten des Browsers ergänzt oder verändert werden und zum Anderen werden auch oftmals eine ganze Reihe von Schlüsseln und Werten in der Windows-Registry verändert. Teilweise werden die unerwünschten Seiten noch bei den „Vertauenswürdigen Seiten“ des Internetexplorers eingetragen.

Eine weitere Möglichkeit ist die gefälschten Seiten in die Host-Datei einzutragen. In dieser Datei werden den Namen die IP-Adressen zugeordnet und normalerweise steht fort nicht viel mehr an Zuweisungen drin wie: **127.0.0.1 localhost**

Dies bedeutet, wenn der Name localhost eingegeben wird, so wird die IP-Adresse 127.0.0.1 aufgerufen, was dem eigenen Rechner entspricht. Jetzt können hier natürlich noch andere Eintragungen vorgenommen werden und damit bestimmte Seiten auf andere IP-Adressen umleiten.

7.3. Wie werden diese Einstellungen vorgenommen?

Eine Möglichkeit ist über den Browser. Prinzipiell ist dafür jeder Browser anfällig, nur der IE ist aufgrund von ActiveX anfälliger als andere Browser. Bei mozillabasierten Browsern ist ein aktives Zutun des Benutzers möglich und da die Einbindung nur als Plug-in passiert, ist sie auch ebenso einfach wieder zu deinstallieren. Eine zweite Möglichkeit ist durch Ausführen eines Trojaners, der diese Einstellungen vornimmt.

7.4. Was kann ich dagegen machen?

Als Erstes müssen die Ursachen beseitigt werden, da sonst die Korrektur nicht von Dauer ist. Das heißt, prüfen Sie Ihr System mit einem aktuellen Virenschanner auf Trojaner und/oder mit [Ad-Aware](#). Außerdem können Sie auch noch mit [HijackThis](#) die laufenden Prozesse überprüfen und auswerten lassen. Ebenfalls sollten Sie Ihre Host-Datei mit einem Texteditor prüfen. Sie befindet sich in einem Windows-Unterverzeichnis und hat nur den Namen host, ohne Endung.

Bringen Sie mit dem Windows-Update Ihr System auf den aktuellen Stand. Dies sollten Sie etwa einmal pro Monat wiederholen.

Verwenden Sie einen aktuellen Virenschanner, den Sie mindestens einmal pro Woche Aktualisieren. Eine Firewall hilft hier nicht!

Überlegen Sie sich, ob Sie Ihren Browser wechseln. Der Internet Explorer ist anfälliger und wegen seiner großen Verbreitung auch ein beliebtes Angriffsziel. Außerdem sind ActiveX-Komponenten schwerer zu entfernen. Dabei ist darauf zu achten, dass Outlook und Outlook Express auch den Internet Explorer zum Anzeigen von HTML-E-Mails verwenden. Darum E-Mail-Programm auch wechseln oder auf „nur Text“ Anzeige umstellen.

7.5. Hilfreiche Programme zum Aufspüren und beseitigen von Pharming/Hijacking

Programmname	Kurzbeschreibung
Ad-Aware	Ein Programm, welches Werbung, Spionageprogramme (Spyware) und Ähnliches vom Computer löschen kann.
BHODemon	Das Programm startet automatisch mit dem Internet Explorer und kann vor böartigen BHOs (Browser Helper Objects) schützen.
HijackThis	Überprüft Windows-Prozesse und Registry-Einträge. Diese können dann bei Bedarf gelöscht werden.
Browser Hijack Blaster	Dieses Programm läuft im Hintergrund und meldet, wenn versucht wird bestimmte Einstellungen zu verändern.

8. Junk-Mails (SPAM[®])

8.1. Was ist Junk oder SPAM[®]?

Hierunter versteht man unverlangt zugestellte E-Mails. Der Name SPAM kommt vom Dosenfleisch SPAM[®] (Spiced Porc and Ham) der Firma Hormel Foods (<http://www.spam.com/>).

Im Gegensatz zur Werbung auf dem normalen Postweg kann Werbung per E-Mail einfach, schnell und kostengünstig an viele Empfänger versendet werden.

Junk-Mails lassen sich grob in drei Arten einteilen:

- **Kommerzielle Werbung**
- **Kettenbriefe und Viruswarnungen (siehe Kapitel 10. Hoaxes)**
- **Durch Viren und Würmer versendete E-Mails**

8.2. Wie kommen die Spammer an meine E-Mail-Adresse?

Kommerzielle Spammer führen eine Datenbank mit E-Mail-Adressen, die sie z.B. mithilfe von Programmen (Robots) aus Newsgroups, Foren, Homepages und E-Mailverzeichnissen auslesen. Wieder andere werden durch Ausprobieren erraten (info@..., webmaster@...) oder einfach durch globales versenden möglicher Buchstabenkombinationen bei Freemail-Anbietern (z.B. bei GMX oder WEB.DE). Außerdem werden E-Mail-Adressdatenbanken weiterverkauft. Um nicht von den vielen Fehlermeldungen bei nicht zugesendeten E-Mails erschlagen zu werden, setzen die Versender falsche Absenderadressen ein.

8.3. Was kann ich gegen Junk/Spam machen?

Einfach gesagt, verringern Sie den Bekanntheitsgrad Ihrer E-Mail-Adresse. Antworten Sie nie auf Werbung oder Erotik/Sex-E-Mails und bestellen Sie auch keine unverlangt zugesendeten Newsletter ab. Damit erreichen Sie wahrscheinlich genau das Gegenteil von dem, was Sie wollten.

Wenn Sie jetzt schon viel Junk/Spam bekommen, dann können Sie sich auch einen Spam-Filter installieren. Der beseitigt zwar nicht die Ursachen für Ihr Spam-Aufkommen, aber er lindert etwas die Symptome.

Mehr Informationen hierzu finden Sie in unserem Thema „E-Mail-Sicherheit“ und in unserer Linksammlung „[Informationen und Programme zum Spamschutz](#)“.

9. Botnetze

9.1. Was sind Bots und was sind Botnetze?

Unter einem **Bot** wird zumeist ein Programm verstanden, welches ohne menschlichen Eingriff Aktionen ausführt. Einer der bekanntesten klassischen Bots ist z.B. der IRC-Bot (IRC = Internet Relay Chat). Mittlerweile wird der Begriff "Bot" im Umfeld der IT-Sicherheit für Fernsteuerprogramme, über die kompromittierte Systeme von einem Angreifer zentral befehligt werden können, verwendet. Die nachfolgende Beschreibung behandelt nur Bots und Botnetze, die nach erfolgreicher Infizierung von einem Angreifer zentral ferngesteuert werden können.

Als **Botnetz** versteht man einen virtuellen Verbund infizierter Client-Systeme, also eine Zusammenschaltung von Bots. In einem Botnetz befinden sich meist mehrere Tausend Bots, die zu bestimmten Aktionen missbraucht werden. Ein Botnetz ist also ein fernsteuerbares Netzwerk (im Internet) von PCs, welches aus untereinander kommunizierenden Bots besteht. Darüber hinaus werden Botnetze oft gegen Geld an Dritte weitervermietet. Zur zentralen Fernsteuerung wird bei den derzeitigen Bot-Varianten zumeist das IRC eingesetzt.

Die Bots verbinden sich hierbei zu einem IRC-Server und treten einem sogenannten *Channel* bei. Ein Channel ist ein gemeinsamer Kanal auf dem sich die Teilnehmer unterhalten können. Der IRC-Server dient dabei als Relaisstation. Dieser Channel ist zumeist mit einem Passwort versehen, wodurch nicht autorisierten Personen ein Einblick und die Kontrolle über die Bots verwehrt werden soll. Durch einen IRC-Server-Administrator können die Bots "fremd-administriert" werden. Hierzu zählen z.B. folgende Funktionen:

- **Scanne nach weiteren Systemen die ebenfalls infiziert werden können**
- **Führe einen DDoS - Angriff aus**
- **Führe einen download durch und anschließend das Programm aus (z.B. Initialverbreitung von neuer Malware)**
- **Versende Spam/Junk**

Und das alles ohne das die betroffenen PC-Nutzer etwas davon mitbekommen.

Dabei existieren immer ein so genannter „Hub-Bot“ sowie „Leaf-Bots“. Der Hub-Bot kontrolliert alle anderen Bots, wobei sich durchaus alternative Hub-Bots festlegen lassen, welche bei einem eventuellen Ausfall des Real-Hubs als Alternative genutzt werden können.

In den Medien taucht für Bots übrigens öfter der Begriff "Zombie-Rechner" auf, weil der Rechner wie ein Zombie, ein willenloses Werkzeug, zum Leben erweckt wird.

9.2. Wie gefährlich sind Botnetze?

Durch Botnetze ist Ihr Rechner nicht mehr nur Opfer, sondern er wird gleichzeitig auch zum Täter. Er erhält die entsprechenden Befehle und führt diese willenlos aus. Einige Computerwürmer konnten sich beispielsweise nur durch Botnetze so schnell und wirkungsvoll verbreiten.

Die Gefahr, die von Botnetze ausgeht, ist extrem hoch, da die von ihnen ausgeführten DDoS - Attacken und Spam-Nachrichten eine enorme Bedrohung für Anbieter von Internetdiensten jeglicher Art darstellen. Das Hauptpotenzial von Botnetzen besteht darin, dass die Netzwerke Größen von tausenden Rechnern erreichen können, deren Bandbreitensumme die der meisten herkömmlichen Internetzugänge sprengt. Somit ist es einem Botnetz von ausreichender Größe durch Senden von immensen Datenmengen möglich, die Anbindungen der attackierten Serviceanbieter zu verstopfen. Da die Netze meistens aus übernommenen Heim-PCs aus verschiedensten Regionen (und somit breitem IP-Adressenspektrum) bestehen, können die betroffenen Anbieter nur bedingt mit Schutzmaßnahmen wie Paketfiltern vorgehen.

9.3. Wie verbreiten sich Botnetze?

Die Verbreitung geschieht auf mehreren Wegen. Einmal wird der Standardweg zum Verbreiten von Malware benutzt als da wären E-Mail und Tauschbörsen. Und zum Anderen beinhalten die meisten Bots Scanroutinen zur Verbreitung der Malware. Dies geschieht dann unter Ausnutzung von Sicherheitslücken. Wieder andere werden von entsprechenden Personen unter Ausnutzung von fehlerhaften Programmen auf Webservern unbemerkt installiert.

Die Kontrolle wird durch Würmer bzw. Trojanische Pferde erreicht, die den Computer infizieren und dann auf Anweisungen warten, ohne auf dem infizierten Rechner Schaden anzurichten.

9.4. Wie kann man Botnetze entfernen?

Da von einem Bot vorgenommene Systemänderungen nicht zuverlässig erkannt und rückgängig gemacht werden können, ist eine Neuinstallation des Systems dringend angeraten. Üblicherweise besitzen Bots einen Keylogger und eine Netzwerksniffer - Funktion. Deshalb muss davon ausgegangen werden, dass Authentifizierungsdaten ausgespäht wurden. Dies hat zur Folge, dass ALLE Passwörter (ggf. auch auf anderen Systemen) geändert werden sollten.

Primäres Einfallstor von Bots sind zumeist fehlende Microsoft-Sicherheitsupdates. Sollte nur der Bot entfernt werden, ohne die potenziellen Einfallstore zu schließen, ist eine Reinfizierung binnen kurzer Zeit zu erwarten.

Sollte das Botnetz nicht mithilfe eines Rootkit getarnt worden sein, kann eine Firewall helfen den Kontakt zu verhindern. Eine Firewall sollte Sie aber auf keinen Fall davon abhalten die Malware von Ihren Rechner zu entfernen.

Es kann versucht werden ein Botnetz durch einen aktuellen Virenschanner oder extra dafür geschriebenen Programmen zu entfernen. Ist der Name der Malware bekannt, so kann man nach speziell dafür gedachten Removal - Tools bei den Antiviren-Programmherstellern suchen.

Es ist aber denkbar, dass zum Beispiel die ISPs (Internet Service Provider) mit Hilfe von IDS (Intrusion Detection System) Botnetz - Aktivitäten beobachten könnten, um eine Verbreitung der Botnetze zu verhindern. Botnetze sind schwer zu bekämpfen, da jeder Rechner für sich allein und ungesehen Verbindungen zu anderen herstellt (jeder stirbt für sich allein). Würde man die Verbindungen (Ziel und Herkunft) sammeln, könnte man diese Netze beenden. Leider geht man dabei die Gefahr ein, dem Internet zu schaden, da dabei der gewollte Gedanke der flexiblen Wegesuche zum Ziel untergraben werden würde bzw. werden könnte.

10. Hoaxes

10.1. Hoaxes, was ist das?

Fast jeder hat wohl schon einmal einen Hoax bekommen. Ein Hoax ist kommt per E-Mail und ist eine unwahre Meldung zu irgendeinem Anlass, z.B. die Warnung vor einem Virus. Hat man so eine Virenwarnung bekommen, so verschicken viele diese E-Mail an Freunde und Bekannte mit der Absicht Ihnen etwas Gutes zu tun.

10.2. Was ist so schlimm an einem Hoax?

Zu erst einmal verbreitet er natürlich Angst und Verunsicherung, gerade bei unerfahrenen Personen. Da es sehr viele unterschiedliche Hoaxes gibt, belasten sie natürlich auch den E-Mailverkehr im Internet und binden unter Umständen Arbeitskraft um diese Meldungen zu prüfen.

Eine große Gefahr besteht aber darin, dass in einigen Hoaxes eine Anweisung gegeben wird, um einen Virus auf dem eigenen System aufzuspüren und zu beseitigen. Dabei handelt es sich aber fast immer um eine wichtige Systemdatei die gelöscht werden soll. Dies hat zur Folge, dass danach das System nicht mehr funktioniert (Stichwort: JDBGMGR.EXE).

10.3. Einige Hoax-Arten und wie man sie erkennen kann

- **Kettenbriefe**
- **Gewinnspiele**
- **Mitleidsbriefe**
- **GEZ-Gebührenerstattung**
- **Viren-Warnungen**
- **Nigeria-Connection**
- ...

Viren-Warnungen sind oft sehr dramatisch geschrieben und es wird eine Anti-Viren-Firma erwähnt, die den Virus schon sehr hoch eingestuft hat. Es werden E-Mails beschrieben, die den angeblichen Virus enthalten sollen und es wird empfohlen diese sofort zu löschen.

Bei den Mitleidsbriefen wird gehörig auf die Tränendüse gedrückt und um Unterstützung gebeten. Außerdem soll man diese E-Mail nicht löschen, eventuell sogar noch weiterleiten.

Gewinnspiele und Nigeria-Connection versprechen nahezu 100%igen Geldzuwachs für kleinen Einsatz.

10.4. Was soll man mit Hoaxes machen?

Auf keinen Fall weiterleiten oder die darin enthaltenen Anweisungen befolgen. Auch wenn man als Spielverderber hingestellt wird (Kettenbriefe), oder wenn man der Meinung ist es könnte doch was dran sein. Diese E-Mails am besten sofort löschen! Kein seriöses Unternehmen verschickt per E-Mail irgendwelche Warnungen und auch keine Organisation versendet Bittbriefe.

Kommt der Hoax von einer Ihnen bekannten Person, so können Sie ihn ggf. darauf Hinweisen.

11. Cookies

11.1. Was sind Cookies und welche Arten gibt es?

Cookies sind kleine Textdateien, die eine Webseite bei dem Besucher ablegen kann. Darin kann diese Webseite dann beliebige Informationen ablegen. Dieses Ablegen auf der eigenen Festplatte macht die Webseite oder der Web-Server natürlich nicht direkt, dazu fehlen die Berechtigungen, sondern es wird dazu der Browser benutzt. Die Informationen die in einem Cookie gespeichert werden stehen eigentlich immer im Zusammenhang mit der Besuchten Webseite.

Es gibt drei verschiedene Arten von Cookies. Dies sind einmal die Sitzungs-Cookies, die nur solange vorhanden sind wie der Browser geöffnet ist. Wird der Browser geschlossen, so werden diese automatisch gelöscht. Eine zweite Variante sind die Cookies mit vorgegebener Lebensdauer. Dies können Tage, Wochen, Monate oder Jahre sein. Diese Cookies werden oft für Login-Zwecke oder zum Personalisieren einer Webseite benutzt. So muss man sich nicht jedes Mal neu einloggen, bzw. alle gemachten Angaben wiederholen, wenn man die Seite neu betritt oder wechselt.

Die dritte Art Cookies sind Cookie von Drittanbietern. Hierbei handelt es sich fast ausschließlich um Werbe-/Tracing-Cookies. Jede Webseite kann nur Cookies ablegen, wenn sie angezeigt wird. Um trotzdem Cookies ablegen zu können, werden dazu nicht direkt die Werbebilder geladen und angezeigt, sondern kleine eingebettete Webseiten, die dann das Bild anzeigen.

11.2. Sind Cookies gefährlich?

Cookies können keine Programme starten oder herunterladen, sie können auch nicht das System ausspionieren. Sie können nur das Speichern, was die Webseite an Informationen hat und auch nur dieses wieder abrufen.

Für den einen oder anderen Surfer sind die Cookies von Drittanbietern unangenehm, sogenannte Tracing-Cookies. Eine eingebettete Webseite wird natürlich die Information ablegen, auf welcher Seite sie eingebettet wurde und kann natürlich alle von ihr erzeugten Cookies lesen. Durch das Auswerten dieser Cookies weiß die Webseite genau, welche Webseiten der Surfer besucht und für welche Themen er sich interessiert. Dadurch kann dann genau auf den Surfer zugeschnittene Werbung angezeigt werden. Diese Cookie-Informationen können dann natürlich auch serverseitig in einer Datenbank gespeichert werden, um Benutzerprofile anzulegen. Im Extremfall kann dadurch ein Surfer wiedererkannt werden.

11.3. Welche Cookie-Einstellungen sind sinnvoll?

So pauschal lässt sich das nicht sagen, es hängt von jedem selbst ab. Der eine mag gar keine Cookies und der nächste sagt: „Natürlich erlaube ich Cookies von Drittanbietern. Wenn schon Werbung, dann welche die mich interessiert!“

Sehr viele Webseiten legen Cookies ab und funktionieren teilweise nicht korrekt, wenn sie dies nicht können. Darum würde ich Sitzungs-Cookies immer annehmen. Cookies von Drittanbietern blockiere ich dagegen immer. Das Nachfragen, ob ein Cookie abgelegt werden darf, halte ich dagegen für nervig. Moderne Browser (Firefox, Opera) haben mittlerweile eine sehr gute Cookie-Verwaltung, so dass eigentlich alle Cookie, bis auf Cookies von Drittanbietern, angenommen werden können. Hier können dann im nachhinein einzelne Cookies gelöscht werden oder gar von bestimmten Webseite blockiert werden.

Ist Ihnen das aber alles zu unsicher, so schauen Sie mal auf die Seite:
<http://www.cookiecooker.de/>

12. Dateiendungen

12.1. Alleine ausführbaren Dateien unter Windows

Unter Windows gibt es einige Dateien, die können ohne Hilfe von anderen Programmen ausgeführt werden. Häufig bekommt man diese Art von Programmen per E-Mail geschickt. Folgende Dateien sollten nur angeklickt werden, wenn man sich sicher ist worum es sich handelt.

Endung	Dateiart
.bat	ausführbare Batch-Datei für DOS-Umgebung
.com	ausführbare Datei für DOS-Umgebung
.exe	ausführbare Datei für DOS/Windows-Umgebung
.lnk	ausführbare Datei für Windows-Umgebung zum Starten von anderen Programmen (Verknüpfung)
.pif	ausführbare Datei für Windows-Umgebung zum Starten von anderen Programmen
.scr	ausführbare Datei für Windows-Umgebung. Endung wird für Bildschirmschoner benutzt
.vbe	ausführbare Datei für Windows-Umgebung. Kodiertes Visual-Basic-Script zum Automatisieren von Vorgängen
.vbs	ausführbare Datei für Windows-Umgebung. Visual-Basic-Script zum Automatisieren von Vorgängen
.wsh	ausführbare Datei für Windows-Umgebung. Windows-Scripting-Host-Script zum Automatisieren von Vorgängen

12.2. Endungen von weiteren gefährlichen Dateianhängen

Außer diesen ausführbaren Dateien gibt es noch andere Dateien, die Schaden anrichten können. Hier eine weitere Liste, bei denen Vorsicht geboten ist.

Endung	Dateiart	Gefährdung
.chm	kompilierte HTML-Datei	kann andere Anwendungen starten
.cmd	Kommandodatei für Windows	kann andere Anwendungen starten
.doc	MS-Word-Dokument	kann Macro-Viren enthalten
.hta	HTML-Applikation	hat vollen Benutzerzugriff (oft Adminrechte)
.mdb	Access-Datenbank	kann Macro-Viren enthalten
.pps	PowerPoint-Dia-Show	kann Macro-Viren enthalten
.ppt	PowerPoint-Datei	kann Macro-Viren enthalten
.reg	Registry-Datei	kann die Windows-Registry verändern
.xls	Excel-Datei	kann Macro-Viren enthalten

13. Quellen, weitere Informationen und Programmseiten

13.1. Quellen und weitere Informationen

<http://www.it-secure-x.de/>

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

<http://www.computerbetrug.de/>

<http://www.firewallinfo.de/>

<http://www.hoax-info.de/>

<http://www.bsi-fuer-buerger.de/>

<http://virusscan.jotti.org/de/>

<http://de.wikipedia.org/>

<http://www.heise.de/security/>

<http://www.netzwelt-kali.de/rechts/links/index.php?seite=080000>

13.2. Interessante Programmseiten

<http://www.hijackthis.de/>

http://www.pcworld.com/downloads/file_description/0,fid,23611,00.asp

<http://www.majorgeeks.com/download.php?det=3786>

<http://www.cookiecooker.de/>

<http://www.sysinternals.com/>