```
:encoding: UTF8 (ISO-8859-1)
```

```
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
 __     ___                _      _
 \ \   / (_)_ __ ___ _ __ / |_  _/ |
  \ \ / /| | '__/ _ \ '_ \| \ \/ / |
   \ V / | | | |  __/ | | | |>  <| |
    \_/  |_|_|  \___|_| |_|_/_/\_\_|

Das (DOS) VIREN 1x1 (deutsche Version)
++++++++++++++++++++++++++++++++++++++
```

edited 1999-2019 by Ralph Roth
edited 2003 by Florian Eichelberger
Als „ADD ON“ für VSP, F_Mirc, RHBVS und Mr2S

```
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

Inhaltsverzeichnis

1 Vorwort

Achtung: Veraltet, spiegelt unter Umständen nicht den allerneusten Kenntnisstand von 2019 wieder!

Dieses kleine Dokument soll Ihnen als Einstieg in die verzwickte Welt der Computerviren dienen. Eine detaillierte Virenbeschreibung finden Sie in der Datei VIRUSDEF.DOC/VirusDef.pdf, welche z.B. dem Programm VirScan Plus beiliegt.

Viren sind gefährlich, sie sind zahlreich, _*Panik mache*_ ist dabei aber fehl am Platz! Wissen ist Macht, und Nichtwissen schützt vor Schaden nicht!

-=-

2 Verbreitungswege von Computerviren

Computerviren, Würmer, Trojaner und andere schädliche Programme (Malware) können sich über vielfältige Arten verbreiten und vermehren:

Disketten und Wechselmedien (ZIP Laufwerke, CD usw.): Auf Disketten gelangen fast alle Virentypen einfach von einem Opfer zum nächsten. Die auf einer Diskette oder Wechselplatte befindlichen Programme oder Dokumente sowie der entsprechende Bootsektor sind bevorzugtes Ziel eines jeden Virus, da dieser Datenträger sehr häufig mit anderen Benutzern ausgetauscht wird.

Netzwerke: Der Datenaustausch erfolgt immer mehr über lokale (LAN) und globale (WAN) Netzwerke. Vielen der modernen Viren bereitet es keine Probleme, sich beim Daten- und Programmaustausch selber weiter auszubreiten. Hierbei sind die Programme und Dokumente die bevorzugten Träger der Viren.

Email: Im Text einer normalen mail kann sich (noch) kein Virus verstecken, sehr wohl aber im Anhang (Attachment). Dieser Anhang kann - je nach Typ - alle möglichen Arten von Viren enthalten.

Internet Downloads: Hier gilt das gleiche wie bei den Netzwerken. In jeder weitergegebenen oder geladenen Datei unbekannter Herkunft kann sich ein Virus verbergen.

Internet: In jüngster Zeit tauchen vermehrt Schädlinge direkt in den HTML Seiten des World Wide Web auf. VB-Script, Java und vor allem Active-X sind hierbei die Angriffsziele der Virenschreiber. Speziell der MS-Internet Explorer ist durch seine Ausbaufähigkeit mit VB-Script und Active-X anfällig gegen solche Virentypen. Diverse Programmfehler und Sicherheitslücken (Active-X) fördern dies noch weiter.

-=-

3 Worauf kommt es bei Computer-Viren an?

¦ Was wird infiziert?
~~~~~~~~~~~~~~~~~~~~~

- Bootsektor oder MBR
- FAT
- ausführbare Dateien (Programme)
- Batchdateien oder ausführbare Skripts (BAT, VBS)
- Dokumente (Makros)

¦ Wie breitet sich der Virus aus?
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

- Geschwindigkeit
  schnell/langsam
- gebunden an bestimmte Plattformen
  ein Amiga-Virus wird keinen IBM/PC infizieren!
- über Disketten, Bootsektor oder ausführbare Dateien (COM/EXE)
  bzw. Dokumente (Excel, Word, Access)
- über Sicherheitslücken (Exploits)

¦ Womit verbirgt der Virus seine Anwesenheit im System?
~~~~~~

- Stealth oder Tarnkappenfähigkeit
  wenn der Virus sich im Speicher befindet, versucht er
  seine Anwesenheit zu verbergen

- Polymorpher Code
  Verschlüsselung des Virencodes, d.h. Virus hat von
  außen betrachtet keinen einheitlichen Code

-=-

4 Bootsektor- und Partitionsviren / FAT-Viren

Jeder bootfähige Datenträger beinhaltet einen sogenannten Bootcode, bei Disketten an Sektor 0 und bei Festplatten an Sektor 1, durch welchen das Betriebssystem geladen wird.

Festplatten besitzen an dieser Stelle (Sektor 0) einen Master Boot Record (MBR) mit den sog. Einteilungsdaten (Partition). Die Partitionstabelle beinhaltet eine logische Laufwerkseinteilung, durch welche das physikalische Laufwerk (HardDrive) unterteilt wird.

Jedes bootfähige logische Laufwerk (jede Partition) beinhaltet im jeweils ersten logischen Sektor ihren eigenen Bootsektor mit dem eigentlichen Urladerprogramm.

Viren können nun:
~~~~~~

- den Bootsektor überschreiben oder
- den Bootsektor verschieben in andere Sektoren des gleichen Mediums/Partition

und eigenen Code beim nächsten Systemstart zu Ausführung bringen.

Dabei können/müssen die Viren im Speicher resident verbleiben.

Problem!! Rekursive Partitionen
PC kann nicht mehr von einer Notfall Diskette gebootet werden!

Problem!! Verschlüsselung des MBR:
Ohne Virus sind die Partitionsdaten verloren!
»> One_Half, Neuroquila Virus

Problem!! Verschlüsselung der FAT:
Ohne residenten Virus haben sie eine zerstörte Dateistruktur!
»> Dir_II, Byway Virus

-=-

5 Datei- oder Linkviren (Datei=File)

Hierbei verwenden Viren ausführbare Programme (meist COM/EXE/OVL) um sich zu vermehren. Dabei besteht ein Unterschied zwischen DOS/exe und WIN/exe Dateien. Ausführbare Windowsdateien z.B. "Explorer.exe" können mit einem DOS/Virus infiziert werden, werden dann aber unter Windows nicht aktiv.

Die Infektion erfolgt:

- appending/overlayend (Virencode hängt sich an das Programm an)
  »> Jerusalem/EXE, Tremor, Natas, Junkie

- prepending/destruktiv (Virencode überschreibt Programmcode am Anfang)
  »> Trivial, HLLO

- prepending/overlayend (Wirtsprogramm wird um "Viruslänge" verschoben)
  »> Jerusalem/COM, HLLP Viren

-=-

6 Companionviren (begleitende Viren)

(am Beispiel "test.exe")

Ist nur für DOS/exe relevant, da hier eine COM-Datei vor einer EXE-Datei gleichen Namens ausgeführt werden kann.

C:\>test
- sucht im root directory des Laufwerkes C
- zuerst nach "test.com" und startet dasselbe, wenn gefunden
- falls "test.com" nicht existiert

- dann erst "test.exe" und startet es

Infektionsschema:

- Virus erstellt eine Datei "test.com", welche den Virencode beinhaltet und bei deren Ausführung der Virus aktiviert wird und startet danach erst das ursprüngliche Programm "test.exe".
- Beide Dateien befinden sich i.d.R. im gleichen Verzeichnis.

-=-

7 Multipartite- oder Hybridviren

Hierbei handelt es sich um eine Kombination von Boot- und Linkvirus mit möglicher Stealth Eigenschaft. Sehr gefährlich!!

»> Neuroquila, Tequila, Natas

-=-

8 Speicherresidente oder TSR-Viren

Der normale RAM (Top Of Memory=TOM) beträgt 640KB. Dieser Wert wird durch den Virus herabgesetzt, Interrupts werden gehookt und der Virencode verbleibt resident im Speicher als Hintergrundprozess (TSR).

Achtung: Warmstart oft nicht ausreichend! Kaltstart erforderlich..

Typischerweise werden Dateien infiziert die entweder/oder

- created/erstellt werden
- opened/geöffnet werden
  read
  write
  sonstiger Zugriff

Die Infektion erfolgt als

Fast Infector : ausführbare Dateien werden sofort infiziert, bzw. beim Einlesen des Verzeichnisses

Slow Infector : Dateien werden nur bei create infiziert, schleichender Befall, sehr gefährlich

-=-

9 Tarnkappen- oder Stealth Viren

Zum Schutz vor Entdeckung muss der Virus resident sein, und dabei werden häufig der INT 13h, INT 25h, INT26h, INT21h auf eine eigene Routine gesetzt.

Sie können sich aus Dateien entfernen und nach einer Überprüfung bzw. Ausführung der Datei wieder einnisten.

-=-

10 Direkt Action Virus (sofortiger Einsatz)

Nach dem Start der verseuchten Datei werden potentielle Wirte gesucht und infiziert. Lange Laufwerkszugriffzeiten bei der Ausführung bestimmter Programme sollten eine Warnung sein.

Vergleiche in diesem Zusammenhang Dropper.

Prüfsummenprogramme sind hier Gold wert!

-=-

11 Polymorphe Viren

Der Virencode ist verschlüsselt und/oder ändert sich zu gewissen zeitlichen Abständen. Zuverlässige Erkennung wird nur über algorithmische Suche bzw. heuristische Analysen oder Code-Emulation möglich.

- bösartig ist dabei eine slow polymorphic engine (gebremste Mutation)

- selbst verschlüsselnde Baukästen (polymorphic engines) waren eine zeit lang Trend, erlangten aber durch den schnellen Vormarsch von Windows, als Standardbetriebssystem, nicht die große Verbreitung.

  1. MtE - Mutation Engine
  2. DAME
  3. TPE
  4. MutaGEN
  5. NED
  6. SMEG
  7. DSME
  8. DGME
  9. PME
  10. VME

  Bitte lesen sie weiterführend, das unter 1. erwähnte Dokument!

-=-

12 Neue Viren

- Makroviren
  ~~~~~~~~~~

  sind Viren die sich durch Word, Excel, Access, AmiPro Dokumente verbreiten,
  ~~~~~~~~~~

in welchen Visual Basic Makrocode enthalten ist. Im Gegensatz zu anderen Viren infizieren Makroviren keine Programme oder den Bootsektor – obwohl einige von ihnen Programme auf der Festplatte des Benutzers hinterlegen.

Problem: deutsche und englische Versionen der Makrosprache unterscheiden sich
Möglichkeit DOS-Viren auszusetzen via
debug
format in batches "@echo j format c: /U >nul"
deltree in batches
oder Virencode in eine Datei kopieren

Viewer ohne die Möglichkeit Makros auszuführen, sollten bei unbekannten Dokumenten bevorzugt verwendet werden!

- Cross-Infector-Viren

sind Makroviren, die nicht nur an eine Windowsanwendung gebunden sind.
Der Virus kann als Excelmacro z.B. auch Word-Dokumente befallen.
»> O97M.Tristate.A

- HTML Viren

siehe Java Skript Viren

- WSH-Viren

sind in Windows Skript Host (WSH) geschriebene Dateien, WIN98 batches

- Browser-Viren oder Java-Viren

sind (meist bösartige) PlugIns wie JAVA-Applets oder ActiveX-Controls die Dateien manipulieren oder sonstigen Schaden verursachen können.

Eine ActiveX-Steuerung ist ein Komponentenobjekt, das in eine Internetseite eingebettet ist und bei der Anzeige der Seite automatisch ausgeführt wird. Hacker, Virenschreiber und andere Personen, die in irgendeiner Form Schaden anrichten wollen, können böswilligen ActiveX- Code für einen Angriff auf das System verwenden. Schalten sie in ihrem System (falls möglich) die Unterstützung für JAVA und Active-X ab! Verwenden Sie die höchste Sicherheitseinstellung für ihren Internetbrowser und für ihren Mailreader! In vielen Fällen kann der Web- Browser (eigentlich ist nur der Internet Explorer von Microsoft betroffen) so konfiguriert werden, dass diese ActiveX-Steuerung nicht ausgeführt wird. Hierfür werden die Sicherheitseinstellungen des Browsers auf „hoch“ gesetzt. Stellen Sie sicher, dass Emailanhänge (attachments) nicht mit einem einfachen Mausklick zur Ausführung gebracht werden können!

- Research-Viren

sind nur in Virenlabors beheimatet und erlangten bisher keine große öffentliche Verbreitung (NO ITW).

- Javascript Viren

~~~~~~~~~~~~~~~~

sind in Javascript programmierte Viren, die in eine HTML Datei oder HTML Mail eingebettet sein können, und beim Besuchen der Seite aufgerufen werden. Streng genommen sind es keine Viren, sondern eher Malicious Code da sie keine eigene Fortpflanzungsroutinen haben. Der Schaden reicht von Ändern der IE Startseite(wie beim JS_SEEKER.G Virus), bis hin zur Formatierung von Festplatten beim (JS_SECBREACH.A Virus). Einige Viren verwenden den Microsoft Windows Skript Encoder um ihre Entdeckung zu erschweren.

- VB Skript Viren (VBS)

~~~~~~~~~~~~~~~~~~~~~

sind in Visual Basic Skript geschrieben, einer Skriptsprache die in (fast) allen Microsoft Produkten vorhanden ist, speziell aber in Microsoft Outlook. Diese neue Klasse von Viren hat sich in der letzten Zeit rasant verbreitet und sich innerhalb kürzester Zeit an die Spitze der Viren Hitliste gesetzt. Einige der VBS Viren verwenden VB Script, um sich via Outlook an alle Einträge im Adressbuch zu verbreiten. Diese Viren sind extrem einfach zu programmieren und verbreiten sich oft innerhalb weniger Stunden per email um den ganzen Erdball. Dadurch einfaches Ändern einiger Textzeilen ein "neuer" Virus erzeugt werden kann, tauchen auch immer wieder leicht veränderte Varianten auf, die vielen Antivirenprogrammen Probleme bereiten. Obwohl die Verbreitung bei den meisten VBS Viren das Hauptziel ist, gibt es auch destruktive Varianten wie z.B. VBS_JADRA.B, der wichtige Dateien im Windowsverzeichnis löscht, oder LOVELETTER, der unter anderem mp3, mp2 und JPEG Dateien mit seinem eigenen Code überschreibt.

- Internet Worms (Würmer)

~~~~~~~~~~~~~~~~~~~~~~~

sind selbständige Programme in irgendeiner Hochsprache oder Assembler, die sich selbständig verbreiten und ihre Schadensroutinen ausführen. Oft wird ein Bug in einer Software genutzt, um sich verbreiten zu können, was zu Engpässen auf den Internet Backbones führen kann. Der SQL-Slammer Wurm, der nur wenige hundert Bytes groß war, aber durch einen BUG im MS-SQL Server sich unkontrolliert verbreiten konnte und so einen Großteil der Internet Leitungen überlastete, ist so ein Beispiel. Ein weiteres Beispiel ist IWorm oder W32.Opaserv, der sich selbst auf Netzwerkfreigaben kopieren konnte, da er einen BUG im Freigabesystem von Win9X ausnutzte.

Der bekannteste Wurm dürfe im Jahr 2017 der Erpressung Trojaner/Wurm „WannaCry“ sein der eine ungepatchte Sicherheitslücke in Windows SMB Dienst ausnutzte.

-=-

13 Sonstige Malware

- Tunnelnde Viren

~~~~~~~~~~~~~~~

suchen den Interrupthandler (DOS) bis zu dessen Ursprung durch via Trapflag und INT 01h und umgehen so residente Virenschutzschilde

- Worms (Computerwürmer)

  - Im klassischen Sinne (Großrechner) dringen in Computernetze ein und führen sinnlose Aufgaben durch, wie die fortlaufende Berechnung der Zahl PI, was das Netz letztendlich durch Überlastung zum Absturz bringt.

  - Neue Art (PC basierend): Ein Computerwurm besteht aus einem in sich geschlossenen Programm (oder aus einer Reihe von Programmen), das funktionsfähige Kopien von sich selbst oder seinen Segmenten in anderen Computersystemen verbreitet. Die Vermehrung findet normalerweise über Netzwerkverbindungen oder email-Attachments statt.

- Dropper
  ~~~~~~~

  ist eine ausführbare Datei mit einem Partitions- oder Bootvirus die ein System infiziert. Dies sind einzigartige Programme die mit einem Viewer betrachtet völlig normal aussehen.

- Trojanische Pferde (Trojaner)
  ~~~~~~~~~~~~~~~~~~

  ist eine Installationsroutine, die dem Computernutzer Schaden zufügt dergestalt, dass z.B. Informationen via Daten Fern Übertragung (DFÜ) vom eigenen System abgerufen werden können. Ein Trojaner infiziert keine anderen Wirtsdateien, daher ist ein Säubern nicht notwendig.

  Installationsroutinen und Updates zweifelhafter Herkunft nur starten, wenn ein aktueller Antivirenwächter im System aktiv ist!!

  »> Back Orifice, Netbus   Vorsicht !!!

- ANSI-Bomben (bestimmte ESC-Sequenzen)
  ~~~~~~~~~~~

  funktioniert nur mit einem ANSI-Treiber, der Tastaturumbelegung via ESC-Sequenzen ermöglicht. Eine bestimmte harmlose Taste ist dann mit einem zerstörerischen Befehl belegt.

- logische Bomben
  ~~~~~~~~~~~~~~~

  sind versteckte Viren, die zu einem bestimmten Datum System schädigende Maßnahmen durchführen.

  »> Michelangelo   Vorsicht !!!!

- Retroviren
  ~~~~~~~~~~
  ~~~~~~~~~~

richten sich gezielt gegen Antivirenprogramme. Suchen nach deren Namen und löschen bestimmte Dateien oder deaktivieren residente Scanner.

-=-

14 Malicious Code/Malware

Als Malware (ein Kofferwort von engl. *malicious* »boshaft« und Software) bezeichnet man Computerprogramme, welche vom Benutzer unerwünschte (schädliche) Funktionen ausführen. Da ein Benutzer im Allgemeinen keine schädlichen Programme duldet, sind die Schadfunktionen gewöhnlich getarnt oder die Software läuft gänzlich unbemerkt im Hintergrund (Typisierung siehe unten).

Schadfunktionen können zum Beispiel die Manipulation oder das Löschen von Dateien oder die technische Kompromittierung der Sicherheitssoftware oder anderen Sicherheitseinrichtungen (wie z. B. Firewalls und Antivirenprogramme) eines Computers sein. Es ist bei Malware auch nicht unüblich, dass eine ordnungsgemäße Deinstallation mit den generell gebräuchlichen Mitteln fehlschlägt, so dass zumindest Software-Fragmente im System verbleiben. Diese können möglicherweise auch nach der Deinstallation weiterhin Schaden anrichten.

Malware bezeichnet keine fehlerhafte Software, auch wenn diese Schaden anrichten kann. Malware wird unterschieden in folgende Typen:

* Computerviren sind die älteste Art der Malware, sie verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreiben. Einen teilweise defekten Virus nennt man „Intended Virus“. Dieser bewirkt meist nur eine „Erstinfektion“ einer Datei, ist jedoch nicht fähig sich weiter zu reproduzieren.

* Ein Computerwurm ähnelt einem Computervirus, verbreitet sich aber direkt über Netzwerke wie das Internet und versucht, in andere Computer einzudringen.

* Ein Trojanisches Pferd ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogrammes mit einem versteckt arbeitenden, bösartigen Teil, oft Spyware oder eine Backdoor. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

* Eine Backdoor ist eine verbreitete Schadfunktion welche üblicherweise durch Viren, Würmer oder Trojanische Pferde eingebracht und installiert wird. Es ermöglicht Dritten einen unbefugten Zugang („Hintertür“) zum Computer, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft genutzt um den kompromittierten Computer als Spamverteiler oder für Denial-of-Service- Angriffe zu missbrauchen.

* Als Spyware bezeichnet man Programme, die Informationen über die Tätigkeiten des Benutzers sammeln und an Dritte weiterleiten. Ihre Verbreitung erfolgt meist durch Trojanische Pferde.

Oft werden auch Dialer (Einwahlprogramme auf Telefon-Mehrwertrufnummern) zur Malware gezählt, obwohl sie grundsätzlich nicht dazu zählen. Illegale Dialer-

Programme allerdings führen die Einwahl heimlich – unbemerkt vom Benutzer – durch und fügen dem Opfer (oft erheblichen) finanziellen Schaden zu (Telefonrechnung).

- Spam-Mail

Werbung via Internet durch email, die Firmennetze und Mailboxen verstopft. Merken sie sich die Adresse, und warnen sie andere durch Benachrichtigung mittels einer bekannten Mailinglist. Seien Sie aber vorsichtig, dass ihre Warnung nicht zu einem Hoaxes wird.

- Hoaxes, Junk-Mails

gezielte Falschmeldungen, Kettenbriefe im Schneeballsystem
»> Good_Times, It_Takes_Guts, Win_A_Holiday

Falschmeldungen und Kettenbriefe sind E-Mail-Nachrichten, die den Empfänger dazu bringen sollen, sie an so viele Personen wie möglich zu verbreiten. Obwohl sie sich auf eine reale Situation beziehen können, basieren sie fast immer auf falschen Angaben. Die meisten Falschmeldungen rühren an das Bestreben der Menschen, anderen helfen zu wollen. Falschmeldungen - Ratschlag: Wenn Sie eine Benachrichtigung über einen Virus erhalten, prüfen Sie dessen Existenz. Wenn Sie eine Meldung als falsch erkannt haben, müssen Sie niemanden benachrichtigen. Löschen Sie einfach die Nachricht.

-> Die Geschichte des Jungen der Krebs hatte und in das Guinessbuch der Rekorde wollte. Der Junge warb um Postkarten aus aller Welt. Heute (Jahre später) ist er vollständig geheilt, soll aber immer noch wöchentlich sackweise Post bekommen.

- Betrügereien

Beschreibung: Wie Falschmeldungen sind auch Betrügereien auf die Ausbeutung des Empfängers ausgerichtet. So werden Sie zum Beispiel zur Preisgabe Ihrer Kontoinformationen aufgefordert, um Ihnen Geld ab zunötigen.

- Ransomware

Ransomware sind Computerprogramme, mit deren Hilfe ein Eindringling private Daten auf einem fremden Computer verschlüsseln kann, um für die Entschlüsselung ein „Lösegeld“ zu fordern. Dabei kann entweder das gesamte System chiffriert werden oder nur einzelne Dateien. Ihre Bezeichnung setzt sich aus der Zugehörigkeit zu der Klasse der Malware sowie der englischen Bezeichnung für Lösegeld (ransom) zusammen.

Die Idee geht auf das Jahr 1989 zurück, als der Schädling AIDS TROJAN DISK mit Hilfe einer infizierten Diskette Daten verschlüsselte. Der Autor dieses Schädlings konnte jedoch überführt werden und wurde zu einer Haftstrafe verurteilt. Einer der ersten Angreifer, der Ransomware zur Verbreitung über das Internet einsetzte, ist der Trojaner TROJ_PGPCODER.A, für dessen Entschlüsselung 2004 mehrere hundert US-$ gefordert wurden. Ein aus Sicht des Angreifers entscheidender Nachteil von Ransomware ist der Kontakt zum Opfer zur

Lösegeldforderung und -bezahlung, wobei selbst diese digital erfolgen kann, bspw. über Online-Bezahldienste wie PayPal. Daher gingen in der Vergangenheit die Expertenmeinungen auseinander, ob sich Ransomware zu einem Massenphänomen ausbreiten könnte. Ein gutes Beispiel für hochwertige Ransomware ist CryptoLocker, eine Malware die 2014 von globalen Rechtshütern ins Visier genommen wurde. Es gibt auch Ransomware as a Service wie z.B. Ransom32. Dieses Programm bietet eine Tauschplattform für Ransomware an, die man gegen eine monatliche Gebühr oder ähnliches nutzen kann. Manchmal werden Betroffene sogar durch eigene Kundenservices angewiesen, wie sie die Erpressungszahlungen leisten zu haben.

- Fun-Proggies (Scherzprogramme)
  ~~~~~~~~~~~~

  täuschen vor ein Computervirus zu sein, beinhalten aber eigentlich keine Schadensroutine. Die angebliche Meldung über die Durchführung einer Festplattenformatierung ist aber trotzdem schockierend!

  Vorsicht: Übereilte Handlungen, meist das Ausschalten des Computers, kann dann aber zum Datenverlust führen!

-=-

15 Root-Kits

Ein Rootkit (engl., etwa "Administratorenausrüstung") ist eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Computersystem auf dem kompromittierten System installiert werden, um zukünftige Logins des Eindringlings zu verbergen, Prozesse zu verstecken, Daten zu kopieren und Eingaben mit zuschneiden.

Der Begriff ist heute nicht mehr allein auf unixbasierte Betriebssysteme beschränkt, da es inzwischen Werkzeugkästen gibt, die ähnliche Funktionalität auch für Nicht-Unix-Systeme bieten, auch wenn diese keinen root Login des Administrators haben. Die Tarnfunktion des Rootkits erfolgt hier vor allem hinsichtlich parallel laufender Antivirensoftware, vor denen die Dateien und Prozesse des Angreifers versteckt werden.

Entwicklung

Die ersten Sammlungen von Unix-Tools zu oben genannten Zwecken bestanden aus modifizierten Versionen der Programme ps, passwd usw., die dann jede Spur des Angreifers, die sie normalerweise zeigen würden, verbergen und es dem Angreifer so ermöglichten, mit den Rechten des Systemadministrators root zu agieren, ohne dass der wirkliche Administrator dies bemerken konnte. Der Name Rootkit entstand also aus der Tatsache, dass der Angreifer sich die Root-Rechte (Admin-Rechte) aneignet und dazu ein Kit (engl., „Baukasten“) aus verschiedenen Programmen auf dem angegriffenen Rechner installiert und ausführt.

Ein Rootkit versteckt normalerweise Logins, Prozesse und Logs und enthält oft Software, um Daten von Terminals, Netzwerkverbindungen und der Tastatur abzugreifen. Dazu können Backdoors (Hintertüren) kommen, die es dem Angreifer
  ~~~~~~~~~~~~

zukünftig vereinfachen, auf das kompromittierte System zuzugreifen, indem beispielsweise eine Shell gestartet wird, wenn an einen bestimmten Netzwerkport eine Verbindunganfrage gestellt wurde. Die Grenze zwischen Rootkits und Trojanischen Pferden ist fließend.

Es gibt zwei große Gruppen von Rootkits. Bei Application-Rootkits werden einfach legitime Programmdateien durch modifizierte Versionen ersetzt. Diese Rootkits sind jedoch relativ einfach durch den Vergleich der Prüfsummen der Programmdateien aufzuspüren. Hierbei ist zu beachten, dass Prüfprogramme wie md5sum ebenfalls oft kompromittiert werden. 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. Man nennt diese Klasse von Rootkits daher auch LKM-Rootkits (LKM steht für engl. „loadable kernel module“). Einige Kernel-Rootkits kommen durch die direkte Manipulation von Kernelspeicher auch ohne LKM aus.

Weiteres
++++++++

Die Firma Sony BMG kam in die Schlagzeilen und musste diverse Musik-CDs zurückrufen, nachdem im Weblog von Sysinternals am 31. Oktober 2005 bekannt wurde, dass der Sony-Kopierschutz für Musik-CDs sich mit Methoden eines Rootkits in Windows-Systemen einnistet.

Siehe auch: Skriptkiddie, Dropper, Malware

16 Weblinks

- c't-Artikel „Kostenloser Spürhund, RootkitRevealer spürt Hintertüren auf“ zu Rootkits unter Windows XP (siehe auch [1])
- BlackLight von F-Secure erkennt und entfernt Rootkits unter Windows
- http://research.microsoft.com/rootkit/
- RootkitRevealer von Sysinternals.com Hilft verdächtige Hinweise auf Rootkits unter Windows XP zu finden (en)
- RootKit Hook Analyzer Analysiert die Adressen der Systemdienste des Windows-Kernels
- chkrootkit - Erkennt Rootkits unter Linux und anderen UNIX-Derivaten (en)
- Rootkit Hunter (rkhunter) - Erkennt Rootkits unter Linux und BSD (en)
- Spiegel-Online: Gefahr durch Rootkits – Virenfiltern droht der Knockout
- Rootkit.com - Umfangreiches Rootkit-Archiv und Programmierbeispiele (en)
- SonyBMG's digitaler Hausfriedensbruch – Ein Review der Ereignisse

-=-

17 Weiterführende Literatur

- Felix Martin: "VirusReport`98" Franzis Verlag (c) 1997
- Andreas Marx, Martin Michl: Chip Computerzeitschrift Ausgabe 02/99
- Ralf Burger: "Das große Computervirenbuch" Data Becker (c) 1989

oder entsprechende Dokumentationen in Antivirenprogrammen

- Eric Amberg: KnowWare 183. Sicherheit im Internet. IPV, Hamburg 2004, ISBN 87-91364-38-8
- Klaus Brunnstein: Computer-Viren-Report. WRS Verl. Wirtschaft Recht und Steuern, München 1989, ISBN 3-8092-0530-3
- Ralf Burger: Das große Computer-Viren-Buch. Data Becker, Düsseldorf 1989, ISBN 3-89011-200-5
- Andreas Janssen: KnowWare 170. Viren, Hacker, Firewalls. KnowWare, Osnabrück 2005, ISBN 87-90785-83-5
- Mark A. Ludwig: The Giant Book of Computer Viruses. American Eagle Publications, Show Low, Ariz. 1998, ISBN 0-929408-23-3
- Rune Skardhamar: Virus. Detection and Elimination. AP Professional, Boston 1995, ISBN 0-12-647690-X
- Peter Szor: The Art Of Computer Virus Research And Defense. Addison-Wesley, Upper Saddle River NJ 2005, ISBN 0321304543