
VIREN1X1

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

(c) 1999-2004 by Michael Hering & ROSE SWE
edited 1999-2004 by Ralph Roth
edited 2003 by Florian Eichelberger
ADD ON für VSP, RHBVS und Mr2S
(Build: \$Id: viren1x1.txt,v 1.12 2003/12/23 21:35:05 ralproth Exp \$)

0. Vorwort

~~~~~

Diese kleine Textdatei 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. VirScan Plus beiliegt.

Viren sind gefährlich.. sie sind zahlreich.. "Panikmache" ist dabei aber fehl am Platz!

Wissen ist Macht, und Nichtwissen schützt vor Schaden nicht!

## 1. 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 Email 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.

2. Worauf kommt es bei 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)

| 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

### 3. 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

### 4. 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

5. 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.

-----

#### 6. Multipartite- oder Hybridviren

~~~~~

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

»> Neuroquila, Tequila, Natas

7. 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

-----

#### 7a. 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.

8. Direkt Action Virus (sofortiger Einsatz)

~~~~~

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

Vergleiche in diesem Zusammenhang Dropper.

Prüfsummenprogramme sind hier Gold wert!

-----

#### 9. 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.

- bössartig ist dabei eine slow polymorphic engine (gebremste Mutation)
- selbstverschlüsselnde Baukästen (polymorphic engines) waren eine zeitlang Trend, erlangten aber durch den schnellen Vormarsch von Windows, als Standardbetriebssystem, nicht die große Verbreitung.

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

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

10. Neue Viren

~~~~~

### - Makro-Viren

~~~~~

sind Viren die sich durch Word, Excel, Access, AmiPro Dokumente verbreiten, in welchen VisualBasic 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.

>> 097M.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 bösertige) 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).

- Java-Script Viren

~~~~~

sind in Javaskript 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 Hitlisten 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

~~~~~

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.

11. Sonstiger zerstörerischer Code

~~~~~

#### - Tunnelnde Viren

~~~~~

suchen den Interrupthandler bis zu dessen Ursprung durch
via Trapflag und INT 01h und umgehen so residente Virenschutzschilder

- 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 Computervorm 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 systemschädigende Maßnahmen durchführen.

»> Michelangelo Vorsicht !!!!

- Retroviren

~~~~~

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

-----

### 12. Malicious Code

~~~~~

- 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

Die Geschichte des Jungen der Krebs hatte und in das Guinnessbuch 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.

- 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!

-----

### 13. 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

---