

norman

the virus control

Norman Buch der Computerviren



Peace of Mind

Norman is one of the world's leading companies within the field of data security. With products for virus control, personal fire wall, encryption, data recovery, and certified data erasure, the company plays an important role in the data industry.

NORMAN[®]
www.norman.com

Norman ASA haftet nicht für andere Formen von Verlust oder Schäden, die sich aus der Verwendung der Dokumentation oder aus eventuell darin enthaltenen Fehlern oder Mängeln ergeben, einschließlich, aber nicht beschränkt auf finanzielle Einbußen.

Insbesondere und ohne die Einschränkungen durch die Lizenzvereinbarung hinsichtlich irgendeiner speziellen Verwendung oder irgendeines speziellen Zwecks haftet Norman ASA in keinem Fall für entgangene Einnahmen oder andere kommerzielle Schäden, einschließlich, jedoch nicht beschränkt auf Folgeschäden.

Die Informationen in diesem Dokument sowie die Softwarefunktionen können ohne Ankündigung geändert werden. Kein Teil dieser Dokumentation darf in irgendeiner Form (Fotokopie, Aufzeichnungsverfahren oder Systeme zur Informationsspeicherung oder zur Informationsabfrage) ohne die ausdrückliche schriftliche Genehmigung von Norman ASA zu einem anderen Zweck als dem persönlichen Gebrauch durch den Käufer reproduziert oder unter Verwendung elektronischer Systeme übertragen werden.

Mitarbeiter der *Das Norman Buch der Computerviren*:

Snorre Fagerland, Sylvia Moon, Kenneth Walls, Carl Bretteville

Editiert durch Yngve Ness

Das Norman-Logo ist ein eingetragenes Warenzeichen der Norman ASA.

Die in dieser Dokumentation erwähnten Produktnamen sind entweder Warenzeichen oder eingetragene Warenzeichen der jeweiligen Eigentümer. Sie werden ausschließlich zu Identifikationszwecken erwähnt.

Norman Dokumentation ist

Copyright © 1990-2003 Norman ASA.

Alle Rechte vorbehalten.

Zuletzt bearbeitet Februar 2003.

Norman Offices

Norman Data Defense Systems AS

Dronningensgade 23, DK-5000 Odense C, **Denmark**
Tel: +45 6311 0508 Fax: +45 6313 3901
E-mail: normandk@normandk.com Web: <http://www.norman.no/dk>

Norman Ibas OY

Läkkisepäntie 11, 00620 Helsinki, **Finland**.
Tel: +358 9 2727 210 Fax: +358 92727 2121
E-mail: norman@norman-ibas.fi Web: <http://www.norman-ibas.fi>

Norman Data Defense Systems GmbH

Kieler Str. 15, D-42697 Solingen, **Germany**.
Tel: +49 212 267 180 Fax: +49 212 267 1815
E-mail: norman@norman.de Web: <http://www.norman.de>

Norman/SHARK BV

Postbus 159, 2130 AD, Hoofddorp, **The Netherlands**.
Tel: +31 23 789 02 22 Fax: +31 23 561 3165
E-mail: support@shark.nl Web: <http://www.norman.nl>

Norman ASA

Mailing address: P.O. Box 43, N-1324, Lysaker, **Norway**.
Physical address: Strandveien 37, Lysaker, N-1324 Norway.
Tel: +47 67 10 97 00 Fax: +47 67 58 99 40
E-mail: norman@norman.no Web: <http://www.norman.no/no>

Norman Data Defense Systems AB

Vällingplan 26, 162 65 Vällingby, **Sweden**
Tel: +46 46 21 12 000 Fax: +46 8 87 62 62
E-mail: support.se@norman.no Web: <http://www.norman.com>

Norman Data Defense Systems AG

Postfach CH-4015, Basel, **Switzerland**.
Tel: +41 61 487 2500 Fax: +41 61 487 2501
E-mail: norman@norman.ch Web: <http://www.norman.ch>

Norman Data Defense Systems (UK) Ltd

Lawn Farm, Oakhill Road
Woodhill, Milton Keynes, Bucks MK5 6AH, **United Kingdom**.
Tel: +44 1908 520 900 Fax: +44 1908 520 909
E-mail: norman@normanuk.com Web: <http://www.normanuk.com>

Norman Data Defense Systems Inc.

9302 Lee Highway, Suite 950A, Fairfax, VA 22031, **USA**
Tel: +1 703 267 6109, Fax: +1 703 934 6367
E-mail: norman@norman.com Web: <http://www.norman.com>

Training and Technical Support

For training or technical support, please contact your local dealer or Norman ASA.

Inhalt

Einleitung	5
Was ist ein Virus?	7
Was ist ein Programm	7
Was ist eine Residency	8
Schadensklassenüberblick	8
Virus	9
Wurm	9
Trojaner, Backdoors, Sicherheitsrisiken	9
Denial-of-service tools, Nukers, Mailbomben	10
Hacking tools, Viren Herstellungs Kits	11
Bugs, Logische Bomben, Zeitbomben	11
Hoax	12
Viren/Wurmtypen Überblick	12
Bootviren	14
Vielteilige Viren	14
Dateiviren	14
Skript Datei Viren	18
Makrovirus	19
Wie funktioniert er?	19
Worin besteht das hohe Risiko?	20
Einbetten und Verknüpfen	20
MS Word	21
MS Excel	22
Office 97, Office 2000, Office XP	22
Bootviren	23
Der Bootvorgang	23
So infiziert ein Boot Virus	25
Spezieller Fall: Der CIH Virus (W95/CIH.1003.A)	26
Spezieller Fall: Der Melissa Virus (W97M/Melissa.A@mm)	27

Spezieller Fall: Der CodeRed Wurm (NT/CodeRed.A).....	28
Spezieller Fall: Der LoveLetter Virus (VBS/LoveLetter.A@mm)....	29
Spezieller Fall: Nimda (W32/Nimda.A@mm)	29
Spezieller Fall: Sircam (W32/Sircam.A@mm).....	31
Voraussagen für die Zukunft.....	32
Wie viele Viren gibt es... ..	33
...und welche Rolle spielt das?	34
Viren in freier Wildbahn	34
Entwicklung des Virenproblems	36
Viren in verschiedenen Betriebssystemen	37
MS-DOS	38
Windows	38
OS/2	39
Windows 95/98/ME	41
Windows NT/2000/XP	43
Lösungen des Virenproblems	44
Standardabläufe einführen.....	44
Lösungen zur Bekämpfung von Viren	44
Industriefakten	48
Norman Virus Control	49
NVC 5 – eine neue Annäherung zur Virenkontrolle	49
Zertifizierung	51
Auszeichnungen	52
Virus Alarmprogramm	52

Einleitung

Es ist nur schwer zu glauben, daß der erste IBM Personal Computer (PC) erst im August 1981 auf den Markt kam. Am Anfang wurden diese Computer nur von wenigen Personen benutzt. Heute jedoch kann man sich ein Leben ohne sie nicht mehr vorstellen. Sowohl bei der Arbeit als auch zu Hause sind sie unentbehrlich geworden. Falls in Ihrem Büro der Strom ausfallen sollte, werden Ihre Mitarbeiter sich wohl die Zeit mit einem Schwätzchen vertreiben, weil sie ohne Computer keine Arbeit erledigen können.

Mittlerweile sind wir von diesen Maschinen und den in ihnen gespeicherten Informationen abhängig. Je wichtiger ein „Ding“ wird, desto wichtiger ist es auch, dieses Ding zu sichern. (Wie viele von Ihnen sichern ihr Auto durch ein Alarmsystem?)

Ein großer Bereich des modernen Lebens mit Computern beschäftigt sich damit, die erstellten und verarbeiteten Informationen zu sichern. Es gibt viele Aspekte der Informationssicherheit, angefangen von tatsächlichen Zugriffskontrollen bis hin zur Sicherstellung, daß die Informationen nicht in irgendeiner Form geändert werden.

Eine der größten und auffälligsten Gefahren, die die Informationsintegrität bedrohen, stellen Computerviren dar. Erstaunlicherweise leben die IBM PCs schon 2/3 ihrer Lebenszeit mit Computerviren. Sie traten erstmals 1986 auf. Durch die zunehmende Bedeutung der globalen Computerverarbeitung gewann auch das Virenproblem in den letzten zwei Jahren an Transparenz.

"Es gibt nur einen sicheren Computer, dieser ist nicht vernetzt, und befindet sich in einem Safe 20 Meter unter der Erde an einem geheimen Ort... und auch bei diesem habe ich meine Zweifel."

Attributed Dennis Huges, FBI

Dazu hat auch die Unterhaltungsindustrie beigetragen, die in Filmen wie „Independence Day“, „Das Netz“ und „Sneakers“ die Auswirkungen der Viren aufgezeigt hat.

Computerviren finden sich auch auf Macintosh-Computern und anderen Plattformen, jedoch soll in diesem Buch in erster Linie auf PC-Viren eingegangen werden. Folgende Themen werden behandelt:

- Was ist ein Virus
- Die Entwicklung des Virenproblems
- Viren in verschiedenen Betriebssystemen
- Lösungen des Virenproblems
- Wie die Produkte von Norman Virus Control helfen

Was ist ein Virus?

Die Begriffe „Computervirus“ und „Virus“ werden in der Umgangssprache sehr weit gefasst und sind gleichbedeutend mit „Ärger“ und „Schwierigkeiten“..

Ein Virus ist im allgemeinen nichts, dass coole Bildschirmeffekte hervorruft oder es Ihnen erlaubt sich in den Pentagon Rechner einzuschleusen. Der in Hollywood Filmen dargestellte „Launching Virus“ entspricht in keiner Weise real existierenden Viren. In der Realität ist eine Vireinfektion für den Benutzer meist nicht sichtbar. Der Rechner wird möglicherweise etwas langsamer oder einige Programme stürzen in unregelmässigen Abständen ab. Aber wenn wir ehrlich sind, ist dies auch bei saubereren Systemen nicht ungewöhnlich.

Es gibt immer noch einige Viren, die Bildschirmeffekte hervorrufen. Der „Marburg“ Virus beispielsweise füllt das Desktop mit roten Kreisen, die ein weisses „X“ enthalten. Ein paar Viren führen dazu, dass die Desktop Symbole der Maus „entfliehen“. Solche Effekte sind jedoch nicht üblich, da sie das Vorhadensein des Virus preisgeben.

Um solche störenden Programme zu erklären, müssen wir zunächst erläutern was Programme wirklich sind.

Was ist ein Programm

Ein Programm ist nichts anderes als ein Rezept für das Verhalten des Computers. Aber Computer lesen diese nicht so wie wir. Sie können freie Textnachrichten nicht verstehen – sie müssen sich stattdessen auf Zahlen verlassen, da Computer in Wahrheit nichts anderes als glorifizierte Rechenmaschinen sind. Lassen Sie uns z.B. auf die Anweisung für „Nichtstun“ sehen. In gebräuchlichen Intel Prozessoren (tatsächlich gibt s hierfür eine Anweisung) – hat sie die Nummer 144. Übersetzt man die Nummer in Binärcode kann sie als 10010000 dargestellt werden.

Physikalisch umgesetzt bedeutet dies Spannung an, aus, aus, an, aus, aus, aus, aus in den Drähten, die in den Prozessor gehen.

Wenn ein Programm auf Ihrem Rechner läuft, liest das Betriebssystem z.B. Windows das Programm von der Platte, untersucht es und bestimmt dann, um welche Art von Programm es sich handelt. Der Prozessor wird dann von hier mit den entsprechenden Nummern „gefüttert“. Moderne Betriebssysteme können gleichzeitig mit mehreren Programmen arbeiten – dass heisst sie sind multitasking fähig. Aus diesem Grund können Sie gleichzeitig Fenster für verschiedene Programme geöffnet haben.

Was ist eine Residency

“Residency” ist ein Ausdruck, dem Sie in diesem Buch sehr häufig begegnen werden. Es bedeutet „im Speicher aktiv“. Ein residentes Programm ist ein Programm, das für eine verlängerte Zeitperiode im Speicher des Computers bleibt. Der Ausdruck war in der „Blütezeit“ von DOS noch wesentlich relevanter, als die meisten Programme nicht-resident waren – d. h. die Programme führten die Aufgabe aus und „starben“ dann. Im Zeitalter von Windows sollte fairerweise gesagt werden, dass die meisten Programme resident sind. Sie bleiben aktiv, bis sie geschlossen werden

Schadensklassenüberblick

Viren, Würmer, trojanische Pferde, logische Bomben etc. sind alles Beispiele für das, was wir gefährliche Software Programme oder auch kurz Schadenssoftware nennen.

Schadenssoftware sind in erster Linie unerwünschte, potentiell gefährliche, unerwünschte Eindringlinge. Es gibt jedoch wichtige Unterschiede zwischen den verschiedenen Untertypen. Der folgende Überblick soll einen Überblick zu den wichtigsten Kategorien geben:

Virus

Viren erfordern einen Host (Wirt), ihr Ziel ist es, andere Dateien zu infizieren, um dem Virus ein längeres Leben zu ermöglichen. Manche Viren haben einfach zerstörende Funktionen, jedoch nicht alle. Viele Viren versuchen, sich ihrer Entdeckung zu entziehen.

Hinweis: Viren sind nichts anderes als Softwareprogramme.

Vermehrung?

Ja, alle Viren kopieren sich fortlaufend selbst und infizieren bei Gelegenheit Boot-Sektoren, Programme oder Datendateien.

Wurm

Erfordert keinen Host, obwohl in einigen Fällen argumentiert werden kann, dass der Host des Wurms die Maschine ist, die er infiziert hat. Daher definieren einige Forscher Würmer als Untertypen von Viren. Am Anfang wurden Würmer hauptsächlich als Problem von Grossrechnern angesehen. Dies veränderte sich mit der Verbreitung des Internets; Würmer gewöhnten sich schnell an das Windows Betriebssystem und begannen sich selbst via e-Mail, IRC oder andere Netzwerkfunktionen zu versenden. Dazu kam ein Wiederauftauchen der UNIX-basierten Würmer, die Sicherheitslücken in den verschiedenen UNIXvarianten ausnutzten.

Vermehrung?

Ja, ein Wurm kopiert sich selbst bei jeder Gelegenheit.

Trojaner, Backdoors, Sicherheitsrisiken

Benötigt keinen Host. Das Wort Trojaner stammt vom Ausdruck „Trojanisches Pferd“ und obwohl es sich manchmal auf den im Programm enthaltenen zerstörerischen Code bezieht, ist jedoch häufiger damit die gesamte Programmdatei gemeint. Trojaner sind Programme, die ungewollte Aktionen ausführen, während sie vorgeben nützlich zu sein. Die meisten Trojaner werden bei Ihrer Ausführung aktiv und zerstören manchmal die Struktur des betroffenen Laufwerks (FAT, Verzeichnisse etc.). Dabei zerstören sie sich selbst.

Ein spezieller Typ ist der Backdoor Trojaner, der oft nichts offensichtlich Destruktives ausführt, er öffnet jedoch Ihren Computer für Remote Control und unautorisierte Zugriffe. Bei bestimmten Einstellungen können leider sogar einige Remote Administrationswerkzeuge als Trojaner verwendet werden. Werkzeuge, die nicht genügend Vorsichtsmaßnahmen gegen diesen missbräuchlichen Gebrauch getroffen haben, können von Norman Virus Control als „Sicherheitsrisiko“ festgestellt werden.

Vermehrung?

Nein.

Denial-of-service tools, Nukers, Mailbomben

Bei diesen Kategorien handelt es sich um Software Waffen. Sie führen keine direkte Aktion auf dem Computer aus, auf dem sie installiert sind, sie sind vielmehr dazu gedacht die Operationen anderer Netzwerk Computer zu unterbrechen. Manchmal können diese Waffen unbemerkt installiert werden, um von ahnungslosen Benutzern benutzt zu werden. In Bezug darauf entsprechen Sie auch der Beschreibung Trojaner.

Denial-of-service (DOS) tools werden verwendet um andere Computer mit Verbindungsanfragen zu bombardieren. Die Zahl der Versuche ist so hoch, dass der attackierte Computer die Last nicht mehr verarbeiten kann und so legitime Anfragen abgewiesen werden. Ein spezieller Fall des Denial-of-Service ist das sogenannte „Distributed Denial-of-Service“ oder DDOS. Von DDOS spricht man, wenn viele Maschinen einen koordinierten Angriff auf ein Ziel starten.

Nukers senden falsch formatierte Netzwerkanfragen, um die attackierte Maschine so zu verwirren, dass sie abstürzt.

Mail bombers sind selbsterklärend – sie werden verwendet um Leute durch das Füllen ihrer Mailbox zu schikanieren

Vermehrung?

Nein. Keiner der oben genannten Aktionen repliziert sich selbst, sie können aber mit Viren kombiniert werden.

Hacking tools, Viren Herstellungs Kits

Es gibt einige wenige Leute, die zwielichtigen Aktivitäten nachgehen und eine Vielzahl von Werkzeugen die sie hierbei unterstützen.

Hacking, der Versuch unautorisierte Zugriffe auf einen Remote Computer auszuführen, war bereits ein Problem lange bevor der erste Virus auftauchte. Es gibt eine grosse Zahl von Werkzeugen, die verwendet werden können, um Wissen über Computer zu erlangen oder in diese einzubrechen.

Es gibt auch einige wenige Programme, die einfach Computerviren erstellen können. Diese Programme sind als Hilfe für Mächtigen Virenautoren gedacht und einer der Hauptgründe für die heutige Virensituation. Diese Werkzeuge sind so einfach zu verwenden, so dass auch Personen ohne Programmierkenntnisse neue Viren erzeugen können. Die Programme werden Virengeneratoren, Virenherstellungs Kits oder einfach Kits genannt.

Vermehrung?

Nein. Ein Viren Herstellungs Kit erstellt neue Viren repliziert sich aber nicht selbst.

Bugs, Logische Bomben, Zeitbomben

Es handelt sich um Programm Fehlfunktionen. Sie erfordern einen Host — Programmierer können keinen Bug erstellen ohne gleichzeitig anderen Code zu schreiben — fairerweise sei gesagt, daß die meisten Programmierer Bugs nicht absichtlich erstellen. Logische Bomben und Zeitbomben werden absichtlich in Code eingefügt, welcher ansonsten „gesund“ ist.

Vermehrung?

Nein. Dieser Code hat im Allgemeinen besseres zu tun, als sich selbst zu kopieren. Logische Bomben und Zeitbomben versuchen, im Verborgenen zu bleiben und nur ihre Auswirkungen sichtbar werden zu lassen. Auch Bugs richten alles mögliche an, mit Ausnahme der eigenen Vermehrung.

Hoax

Bei einem Hoax handelt es sich um einen Kettenbrief, der üblicherweise via e-mail versendet wird. Sie enthält eine falsche Warnung zu Viren oder Trojanern. Wohlmeinende Benutzer senden die Warnung im Glauben etwas Gutes zu tun weiter. Meist sieht es so aus, als würden die Warnungen von bekannten Firmen oder Organisationen stammen. Dies ist jedoch nicht der Fall. Hoaxes können auch andere Meldungen enthalten, die den Benutzer veranlassen sollen, die Mail weiterzuleiten, wie z.B. den Erhalt von Geld als Antwort auf die Weiterleitung der Mail an Freunde.

Wenn Sie eine Warnung zu einem Virus erhalten, senden Sie diese bitte nicht an andere Benutzer! Diese Warnung gilt auch wenn es den Virus wirklich gibt und vor allem auch dann, wenn die Warnung die Aufforderung enthält sie weiterzusenden. Dies steigert nur die Angst und erhöht die Arbeitslast.

Vermehrung?

Nein, nicht durch sich selbst. Sie überlisten den Benutzer dazu Kopien zu machen.

Viren/Wurmtypen Überblick

Wenn wir über Viren und Würmer sprechen, sprechen wir normalerweise über die folgenden Hauptkategorien:

Binäre Datei Viren und Würmer

Dateiviren infizieren ausführbare Dateien (Programm Dateien). Sie sind in der Lage netzwerkweite Infektionen auszuführen. Normalerweise bestehen diese EXE-Dateien und Viren aus Instruktionen, die eine einfache Maschinen Interpretation ermöglichen, sogenannter Maschinen Code. Für untrainierte Augen sieht dieser Maschinen Code unverständlich aus, da es sich lediglich um Zahlenreihen handelt, die in den Prozessor geleitet werden. Datei Würmer sind ebenfalls in Maschinen Code geschrieben, sie infizieren aber keine anderen Dateien sondern ihr Fokus liegt in der Verbreitung auf andere Maschinen. Details siehe auch Seite 26.

Binäre stream Würmer

Code Red ist ein binärer stream Wurm, der das Netzwerk gebraucht.

Unter „Flut“ Wümmern versteht man eine Gruppe von Wümmern, die sich über ein Netzwerk verteilen, ohne sich je selbst als Datei zu

manifestieren. Stattdessen „reisen“ sie von Computer zu Computer nur als Codeteile, die lediglich im Speicher existieren. Der berühmteste dieser Gruppe ist die *Code Red* Serie von Wümmern, die sich zwischen IIS Systemen ausbreitet. Details siehe auch Seite 28.

Skript Datei Viren und Würmer

Ein Skript Virus ist technisch gesehen ein Datei Virus. Skript Viren sind jedoch als reiner Text geschrieben und daher leicht für jeden zu lesen. Da Computer Textinstruktionen nicht direkt verstehen können, muss der Text zunächst in Maschinen Code übersetzt werden. Diese Prozedur nennt man „Interpretation“ und wird von separaten Programmen auf dem Computer ausgeführt. Visual Basic Script (VBS) wird beispielsweise durch das Programm WSCRIPT.EXE interpretiert und die alte DOS batch Sprache (BAT) wird durch die COMMAND.COM gelesen. Skript Viren infizieren andere Skript Dateien, häufiger sind jedoch die Skript Würmer, die von Maschine zu Maschine weitergehen, bevorzugt via e-Mail. Details siehe auch Seite 29.

Makrovirus

Makroviren infizieren Datendateien oder Dateien, die normalerweise als Datendateien verstanden werden, wie etwa Dokumente oder Spreadsheets. Viele Datendatei Typen haben die Möglichkeit Anweisungen zusammen mit dem normalen Inhalt zu transportieren - z.B. Microsoft Word Dateien können Anweisungen enthalten die Word vorschreiben, wie ein spezielles Dokument angezeigt wird oder Anweisungen, die Windows mitteilen bestimmte Aktionen auszuführen. Alles was sie auch mit normalen Programmen auf einem Computer ausführen können, kann auch durch solche Makro Instruktionen veranlasst werden.

Makroviren sind heute die häufigsten Viren. Sie können sich in Netzwerken verbreiten. Details siehe auch S.27

Bootviren

Bootviren infizieren Bootsektoren von Festplatten und Disketten. Sie sind **nicht** in der Lage über Netzwerke zu infizieren.

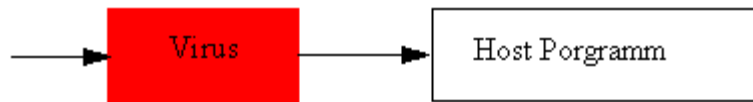
Vielteilige Viren

In den nächsten Abschnitten werden die binären, Skript-, Datei-, Makro- und Bootviren eingehender erläutert.

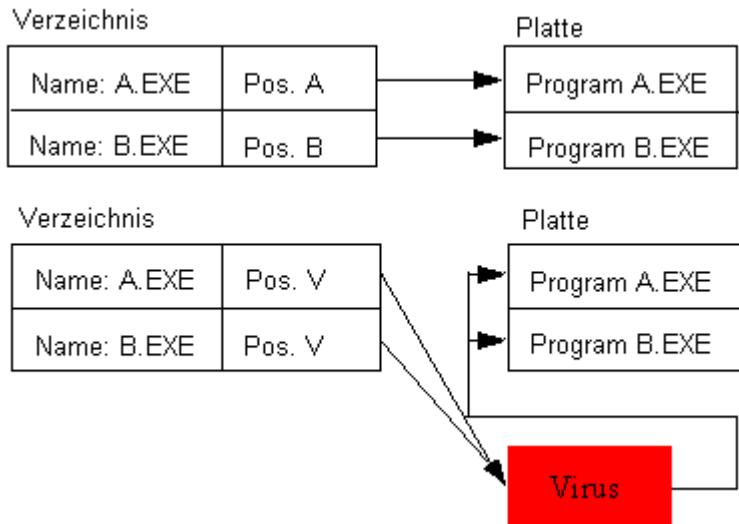
Dateiviren

Ein Dateivirus hängt sich an eine Programmdatei (den Host) an und verwendet verschiedene Verfahren, um andere Programmdateien zu infizieren.

Es gibt verschiedene grundlegenden Verfahren zur Infizierung von ausführbaren Dateien diese sind: begleiten, verknüpfen, überschreiben, einfügen, voranstellen, anhängen und andere.

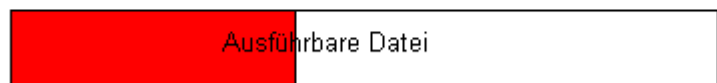


Ein begleitender Virus verändert nicht direkt den Host. Stattdessen überlistet er das Betriebssystem dazu ihn statt der Host Datei auszuführen. Manchmal wird dies dadurch erreicht, dass die Host Datei umbenannt wird und der Virus dann den Namen des Originalprogramms annimmt. Oder der Virus infiziert eine .EXE Datei durch das Erzeugen einer .COM Datei mit dem gleichen Namen im gleichen Verzeichnis. DOS führt immer zuerst die .COM Datei aus, wenn nur der Programmname eingegeben wird. Wenn Sie am DOS Prompt z.B. „EDIT“ eingeben und im selben Verzeichnis eine EDIT.COM und eine EDIT.EXE existieren, wird die Datei EDIT.COM ausgeführt.



Ein verknüpfender Virus nimmt Veränderungen in den niederen Bereichen des Dateisystems vor, so dass der Programmname nicht länger auf das Originalprogramm hinweist, sondern auf eine Kopie des Virus. Es ist daher möglich, dass es nur ein Beispiel des Virus vorliegt auf das alle Programmnamen zeigen.

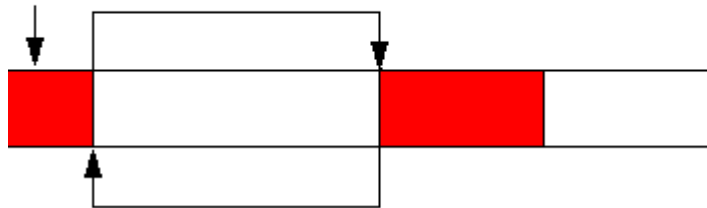
Der Virencode überschreibt die ausführbare Datei und macht sie nutzlos.



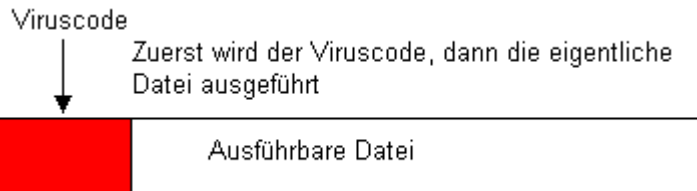
Ein überschreibender Virus setzt sich an den Anfang eines Programms direkt über den ursprünglichen Programmcode und beschädigt so das Programm. Das Programm kann nicht mehr ausgeführt werden. Wenn Sie es versuchen, wird lediglich eine weitere Datei befallen.

Diese Viren sind leicht zu erfassen und können von Benutzern und Unterstützungspersonal einfach zerstört werden, so daß sie sich kaum ausbreiten können. Die Wahrscheinlichkeit, daß sich ein solcher Virus auf Ihrem Rechner befindet, ist sehr gering.

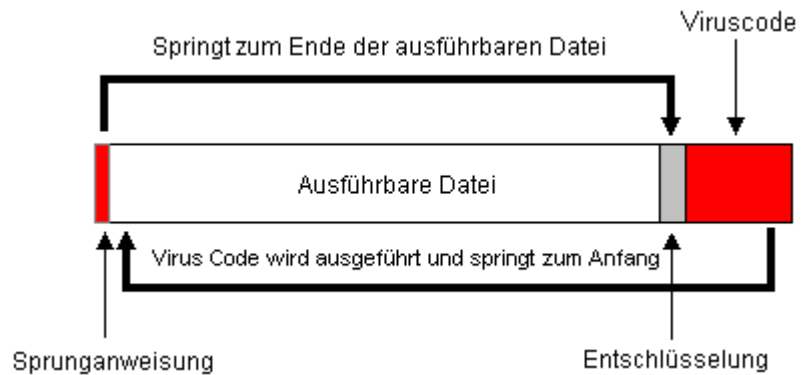
Der Virus verwendet den unbenutzten Platz und wird zuerst ausgeführt. Dann springt er zurück zum Host Programm



Ein einfügender Virus kopiert sich selbst in das Host Programm. Programme enthalten manchmal Bereiche, die nicht verwendet werden. Viren können diese finden und sich selbst hier einfügen. Ein Virus kann auch so designed sein, dass er ein grosses Stück der Host Datei irgendwohin verschiebt und dann den freien Platz einnimmt.



Die reine Form des voranstellenden Virus setzt einfach den gesamten Virencode vor das infizierte Originalprogramm. Wenn Sie ein Programm ausführen, das von einem solchen Dateivirus befallen wurde, wird vor dem Programm zunächst der Viruscode ausgeführt.



Ein anhängender Virus setzt eine Sprunganweisung an den Anfang der Programmdatei, verschiebt den ursprünglichen Anfang der Datei an das Dateiende und setzt sich selbst zwischen das ursprüngliche Dateiende und den ursprünglichen Dateianfang. Wenn Sie dieses Programm ausführen möchten, ruft die „Sprunganweisung“ den Virus auf, und der Virus wird ausgeführt. Der Virus verschiebt dann den ursprünglichen Dateianfang an die richtige Position und das Programm wird ausgeführt.

Dies war ein kurzer Überblick darüber, wie sich ein Virus an eine Programmdatei anhängt. Zur Infizierung werden verschiedene Verfahren verwendet. Die meisten Dateiviren nisten sich im Arbeitsspeicher ein, so daß sie alle Aktionen überwachen und auch andere Programmdateien befallen können. Andere Dateiviren wiederum infizieren durch „Direktangriffe“, d.h. sie infizieren eine Programmdatei, wenn auf diese Datei zugegriffen wird. Unter Windows verwischt dieser Unterschied, da viele Viren resident sind und auch „Direktangriffe“ ausführen können. Es gibt noch viele andere Verfahren.

Skript Datei Viren

Skript Datei Viren sind eigentlich keine neue Klasse von Viren, sie haben sich aber ganz aktuell zu einer grossen Bedrohung entwickelt. Wie bereits erwähnt, sind Skripte reine Textanweisungen, die von einigen Programmen interpretiert werden können. Es gibt nur wenige Skript Sprachen:

Visual Basic Script: Diese Skripte findet man normalerweise als separate *.VBS Dateien oder eingebunden in Web Seiten. VB Skripte haben eine Funktionalität, die ein Unterabteilung der Microsoft Visual Basic Sprache ist und kann durch den Import der Funktionen anderer Programme erweitert werden. Es können z.B. viele der Microsoft Word Funktionen über VB Skripte genutzt werden.

JavaScript: Diese Skript Sprache wurde von Sun Microsystems neben der Entwicklung des HTML Standards eingeführt. Standardisiertes Java Script ist normalerweise sehr sicher, da es keine Auswirkungen auf das Dateisystem hat. Java Script finden Sie normalerweise auf Web Seiten.

JScript: Die Microsoft Version des Java Skriptes. Es ist genauso flexibel und erweiterbar (und unsicher) wie Visual Basic Script. JScript finden Sie in *.JS Dateien oder auf Web Seiten.

DOS BAT Sprache: Wenn Sie das alt ehrwürdige DOS zu einer Aktion auffordern wollten, war es üblich die Kommandos in die Kommandozeile einzugeben. Z.B. die Anzeige der Dateien eines Verzeichnisses wurde ausgeführt durch Eingabe des Befehls DIR<Enter>.

Sie können DOS aber auch instruierten einige Aufträge auszuführen, wenn Sie nicht anwesend sind, um die Kommandos einzugeben. Für diesen Zweck wurde die BAT (batch) Sprache entwickelt: geben Sie die Kommandos in eine Textdatei ein und geben Sie dann deren Namen in die Kommandozeile ein, um DOS einen Satz von auszuführenden Aufgaben vorzugeben. Diese Dateien werden immer batch Dateien genannt und haben die Erweiterung *.BAT.

UNIX shell script: Dieses Skript ist ähnlich wie die DOS batch Sprache wurde jedoch speziell für die verschiedenen Anforderungen von UNIX entwickelt. In UNIX haben Sie die Möglichkeit sehr viele Kommandos von der Kommandozeile einzugeben. Diese Shell Skripte sind daher sehr machtvoll und können sehr viele Aufträge ausführen.

IRC scripts: Der Internet Relay Chat ist ein Chat System für das Internet. Chat Systeme können über Skripte verschiedenen Aufgaben automatisch ausführen, z.B. Grüße an Leute aussenden, die den Chat room ausgewählt haben. Diese Skripte unterstützen aber auch die Versendung von Dateien und so kommt es dazu dass viele Würmer und Viren über IRC verbreitet wurden. Bekannte IRC Programme, die so ausgenutzt wurden, sind mIRC, pIRCH und VIRC Klienten.

Andere Skript Sprachen: Es gibt noch viele andere Skript Sprachen. Corel Draw, Visual Foxpro, SuperLogo, InstallShield etc. können mittels Skripten verwendet werden und wurden auch für schädigende Zwecke verwendet.

Makrovirus

Seit dem Aufkommen des ersten Makrovirus im August 1995 und auch heute hat sich diese Kategorie der Virustypen, als die am schnellsten wachsende erwiesen. Zum Zeitpunkt der ersten Erwähnung des Phänomens in dieser Veröffentlichung, im Januar 1997, belief sich die Zahl bekannter Makroviren auf 100. Bis zum Juni 2001 hat Norman mehr als 8.000 Makroviren identifiziert, und ihre Zahl wächst weiter.

Wie funktioniert er?

Traditionelle Dateiviren sind nicht auf die Infektion von Datendateien aus, da sich diese zur Verbreitung nicht eignen. Datendateien werden nämlich nicht „ausgeführt“, sondern „gelesen“ und „bearbeitet“. In den letzten Jahren wurden in den Unternehmen jedoch offene Systeme eingeführt, die den Austausch von Daten vereinfachen. Darunter leidet wiederum die Datensicherheit. Makroviren nutzen es für sich aus, daß viele Anwendungen **Makro-Programmiersprachen** enthalten.

Diese Sprachen gewähren Benutzern (und Virenautoren) eine größere Flexibilität und mehr Einflußmöglichkeiten auf die Anwendung als jemals zuvor. Oft werden Makroviren nicht früh genug erkannt, da viele Benutzer mit den Feinheiten der Makros nicht vertraut sind. Als Folge ist die Infektionsrate durch Makroviren viel größer als die durch traditionelle Datei- und Bootviren.

Am Anfang war das das Hauptangriffsziel von Makroviren die Makrosprache WordBasic, die Sprache innerhalb von Microsoft Word. Später wurde die Makro Programmiersprache wurde Visual Basic for Applications oder VBA, die in Viren vorherrschende Sprache. Diese Programmiersprache wird in vielen Anwendungen verwendet - Word, Excel, Access, PowerPoint, Project, Visio und viele andere.

Worin besteht das hohe Risiko?

Da Datendateien häufiger als ausführbare Programmdateien gemeinsam benutzt und ausgetauscht werden, stellen Makroviren ein sehr hohes Sicherheitsrisiko dar. Auch VBA ist eine sehr einflussreiche Programmiersprache, die dazu verwendet werden kann, nahezu alles im Computer zu kontrollieren.

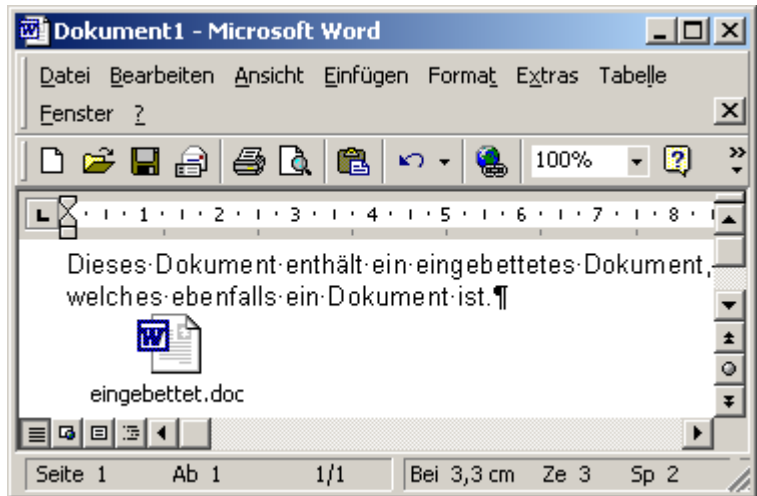
Einige Makroviren enthalten destruktiven Code und andere sind sogar in der Lage traditionelle Datei- und Bootviren zu erzeugen und auszuführen. Während traditionelle Datei- und Bootviren Einfluss auf die Funktionen im Computer nehmen, wirken sich Makroviren auf die Qualität und Zuverlässigkeit der Informationen in Datendateien aus.

Einbetten und Verknüpfen

Die offenen Systeme vieler Anwendungen von Microsoft verwenden OLE, um verschiedene Datentypen zu kombinieren.

Sie können beispielsweise ein Objekt wie eine Bitmap in ein Word-Dokument **einbetten**. Das bedeutet, daß die Bearbeitungen, die Sie an dem Objekt vornehmen, sich nicht auf andere Kopien des Objekts auswirken. Sie können Objekte auch **verknüpfen**, so z.B. eine Tabellenkalkulation von Excel mit einem Dokument von Word.

Verknüpfen bedeutet, daß Sie das Objekt entweder in der Quellanwendung oder in der Anwendung, mit der es verknüpft ist, bearbeiten können und alle Kopien des Objekts gleichzeitig aktualisiert werden.



Microsoft Office Produkte verfügen über die Fähigkeit des Einbettens und Verknüpfens von Objekten. Darüber hinaus können sie in andere Anwendungen eingebettet und mit anderen Anwendungen verknüpft werden. Das Risiko besteht also darin, daß ein Word-Makrovirus in einer anderen Anwendung ausgeführt werden kann oder eine infizierte ausführbare Datei in Microsoft Office.

MS Word

Bis jetzt wurden die meisten Makroviren für Microsoft Word geschrieben. Dies liegt zum Teil daran, dass Word die erste Anwendung war, die mit Makroviren durchlöchert wurde aber auch weil Word Dokumente wesentlich häufiger als andere Datentypen ausgetauscht werden. Der erste Makro virus, WM/Concept.A wurde Mitte 1995 erstellt und wurde schnell zu einem der am weitesten verbreitetn Viren weltweit - ungeachtet der Tatsache, dass er keien Mail Verbreitungsfunktion enthält, die mit dem Jahrtausendwechsel immer häufiger wurde.

MS Excel

Nicht lange nach dem ersten Word-Makrovirus tauchte der erste Excel-Virus auf: *XM/Laroux.A*. Dies war zu erwarten, da die zur Erstellung solch eines Virus erforderlichen Techniken dieselben, wie für Word-Makroviren sind.

Der Unterschied zwischen Viren für Word und Excel ist, daß Viren für Word in WordBasic geschrieben werden, während Viren für Excel in VBA3 (Visual Basic für Anwendungen, Version 3) erstellt werden. Das Format ist unterschiedlich, zudem werden die Makros nicht in der Arbeitsmappe abgelegt (bei Word 6/7 werden die Viren im Word-Dokument gespeichert), sondern in gesonderten Streams. Diese Technik erschwert das Aufspüren, Identifizieren und Entfernen von Viren.

Wegen der Auswirkungen in der Praxis stellen Makroviren für Excel eine größere Bedrohung dar als Word-Viren. Stellen Sie sich vor, ein Makrovirus für Excel multipliziert eine bestimmte Zelle mit 10 und speziell diese Zelle ergibt Ihr Gehalt. Das wäre sicherlich nicht das Ende der Welt, aber wie verhielte es sich bei einer *Teilung* durch 10?

Dies sind geringfügige Unannehmlichkeiten, verglichen mit ähnlichen Veränderungen der Berechnungsformeln für die Abschätzung der Betonstärke eines Wolkenkratzers. Arbeitsmappen sind häufig umfangreich und Abweichungen nicht einfach zu erkennen.

Office 97, Office 2000, Office XP

Die Einführung von Office 97 beinhaltet auch veränderte Formate für fast alle Programme des Paketes, zumindest jedoch waren diese Änderungen konsistent. Excel wie auch Word verwenden beide VBA5 (Visual Basic für Anwendungen, Version 5), basierend auf VBA3, mit vielen Erweiterungen.

Weil VBA5 nicht kompatibel zu WordBasic ist, wäre zu erwarten, daß Makroviren, welche für frühere Versionen von Word geschrieben wurden, Word 8.0 in Office 97 nicht befallen können.

Microsoft hat jedoch Umstellungen jeweils von WordBasic und von VBA3 auf VBA5 angeregt, um bestehende Makros an die neuen Formate anpassen zu können. Folgerichtig können Makroviren für frühere Versionen von Word und Excel ebenfalls "angepasst" werden. Nicht jeder Virus wird nach der Umstellung funktionieren, wir wissen jedoch, daß recht viele es dennoch tun.

Dasselbe passierte mit der Dokument Umstellung von VBA5 zu VBA6. Dies ist die VBA Version, die von den neueren Office Formaten Office 2000 und Office XP verwendet wird.

Folgerichtig können Makroviren für frühere Versionen von Word und Excel ebenfalls "angepasst" werden. Nicht jeder Virus wird nach der Umstellung funktionieren, wir wissen jedoch, daß recht viele es dennoch tun.

Bootviren

Bootviren infizieren System-Boot-Sektoren (SBS) und Master-Boot-Sektoren (MBS).

Der MBS befindet sich auf allen physischen Festplattenlaufwerken. Unter anderem enthält er Informationen zur Partitionstabelle (Informationen über die Aufteilung des physischen Datenträgers in logische Datenträger) und ein kurzes Programm, das die Partitionsinformationen interpretiert und so erfährt, wo sich der SBS befindet. Der MBS ist unabhängig vom Betriebssystem. Der SBS enthält unter anderem ein Programm, das ein Betriebssystem sucht und ausführt.

Da Disketten häufiger als Programmdateien ausgetauscht werden, verbreiten sich Bootviren wesentlich effektiver als Dateiviren

Weitere Informationen siehe "Viren in verschiedenen Betriebssystemen" auf Seite 37.

Der Bootvorgang

Um die Wirkungsweise von Bootviren zu verstehen, muß zunächst einmal der Boot-Vorgang untersucht werden.

Das BIOS (Basic Input/Output System), das den Boot-Vorgang steuert, wird mit Einschalten des Stroms eingeleitet.

Als nächstes wird nach dem Einschalten der Selbsttest POST (Power On Self Test) ausgeführt. Er stellt sicher, daß der Computer richtig funktioniert. Eine Funktion von POST, die bestimmt alle Benutzer kennen, ist die Zählanzeige zur Größenbestimmung des RAM (Random Access Memory) Ihres Rechners.

Als letzte Aktion leitet POST den Boot-Vorgang ein. Zunächst wird festgestellt, ob sich eine Diskette im Diskettenlaufwerk befindet. Wenn ja, wird der System-Boot-Sektor auf der Diskette gelesen und der Rechner versucht, von Diskette zu booten.

Wenn die Diskette nicht bootfähig ist (weitere Einzelheiten siehe unten), wird die folgende Meldung auf dem Bildschirm angezeigt:

Wenn die Diskette nicht bootfähig ist (weitere Einzelheiten siehe unten), wird die folgende Meldung auf dem Bildschirm angezeigt:

```
Non system-disk or disk error.
```

```
Replace and strike any key when ready.
```

Dieser Text wird durch ein kleines Programm erzeugt, das sich im SBS der Diskette befindet, wenn diese nicht bootfähig ist.

In der Regel ist keine Diskette eingelegt und es wird der Master-Boot-Sektor auf dem Festplattenlaufwerk gelesen. Danach wird der System-Boot-Sektor gelesen und das Betriebssystem gestartet.

Der gleiche Vorgang wird auf Rechnern mit DOS, Windows, Windows 9x/ME, Windows NT/2000, Linux und OS/2 ausgeführt. Unterschiede treten erst auf, wenn die Betriebssysteme selbst geladen werden.

Bootfähige Diskette

Bei der Formatierung einer Diskette wird ein System-Boot-Sektor erstellt. Die Diskette kann zwei Aufgaben haben: Speichern von Programm- und Datendateien oder Verwendung als bootfähige Diskette.

Bootfähig ist eine Diskette dann, wenn mit ihr der Boot-Vorgang von der Festplatte umgangen werden kann. Stattdessen wird der Boot-Vorgang von Diskette ausgeführt.

Zur Erstellung einer bootfähigen Diskette müssen Sie die Diskette entweder mit der Option „System“ (/S) formatieren oder den DOS-Befehl SYS auf die Diskette anwenden.

Eine formatierte Diskette verfügt immer über einen System-Boot-Sektor, unabhängig davon, ob die Diskette bootfähig ist oder nicht. Ein Boot-Virus ist im SBS beheimatet, d.h. alle formatierten Disketten können mit einem Boot-Virus infiziert sein.

So infiziert ein Boot Virus

Wird eine Diskette im Laufwerk A: eines Rechners belassen und der Rechner so eingerichtet ist, daß er zunächst von Laufwerk A: bootet, wird der SBS der Diskette gelesen. Enthält der SBS einen Boot-Virus, wird dieser aktiviert, speicherresident, infiziert die Systembereiche des Festplattenlaufwerks und versucht, andere Disketten mit Schreibzugriff, auf die zugegriffen wird, zu infizieren.

Viele Benutzer lassen Disketten in den Laufwerken, wenn sie den Rechner ausschalten und erinnern sich nicht daran, wenn sie den Rechner am nächsten Tag wieder einschalten. Daher booten viele Benutzer ohne es zu bemerken Ihren Rechner von der Diskette. Als Folge davon waren die Bootviren für lange Zeit die häufigsten Viren.

Spezieller Fall: Der CIH Virus (W95/CIH.1003.A)

Typ: Binärer Dateivirus
Infiziert: ausführbare Windows 32-bit
Programme

Bis zum 26. April 1998 war es wahr, dass Viren ernsthafte Schäden an der Software aber nicht an der Hardware ausführen konnten. An diesem speziellen Tag schlug zum ersten Mal der Virus *W95/CIH.1003.A* zu. Opfer mussten den Flash BIOS Chip austauschen und sogar (speziell bei Laptops) das Motherboard des PC's. In den darauf folgenden Monaten wurde der CIH Virus aus allen Teilen der Welt In the Wild gemeldet. Er existiert zur Zeit in einer grossen Zahl von Varianten. Einige werden am 26. des Monats aktiv.

Der CIH Virus infiziert sehr versteckt die ausführbaren Dateien in Windows 95/98. Die infizierten Dateien verändern zum Beispiel nicht ihre Länge. Oft ist die Längenveränderung bei binären Dateien ein Anzeichen für eine Virenaktivität.

Eine genaue technische Beschreibung der Aktivitäten, die der Virus ausführt, würde den Rahmen dieses Buches sprengen. Einfach ausgedrückt, wenn der CIH Virus das Flash BIOS reprogrammiert wird der PC verlangsamt und vergisst seine interne Sprache. Wenn dies passiert gibt es kein anderes „Heilmittel“ als den Austausch dieses Hardware Teils. Der Virus kann auch Teile der Festplatte überschreiben und diese nutzlos zurücklassen.

Der CIH Virus erinnert uns daran, das Virenautoren manchmal detaillierte Informationen zu undokumentierten internen Prozessen tief im Betriebssystem besitzen. Wenn sie diese Kenntnisse nutzen, um weitgehend fehlerfreie und so gefährliche Viren wie den CIH Virus zu schreiben, ist das Vorhandensein eines adäquaten Virenschutzes ein Muss.

Es ist allgemein bekannt, das Opfer des CIH Virus durch das Herunterladen von Dateien von einer Internet Spiele Seite infiziert wurden. Wir denken daher, dass es wichtig ist alle Surfer im Web an die täglichen Gefahren zu erinnern.

Daher empfehlen wir unbedingt die Verwendung einer Antiviren Software, die über einen qualifizierten Update Mechanismus verfügt. Die Tage, in denen es ausreichte die Antiviren Software einmal im Vierteljahr zu aktualisieren sind definitiv vorbei.

Spezieller Fall: Der Melissa Virus (W97M/Melissa.A@mm)

Typ: Makrovirus
Infiziert: Word 97 und Word 2000
Dokumente

Ende März 99 erreichten uns Meldungen, dass sich eine Datei namens `password.doc` selbständig per e-mail versendet. Die Anzahl der Mails war so gross, dass viele e-mail Server diese nicht mehr verarbeiten konnten und abstürzten. Hier zeigte sich uns der erste e-mail Virus, der mit Massensendungen arbeitet. Das Dokument enthielt einen Virus namens *W97M/Melissa.A*, der sich nicht nur selber in den Dokumenten des Benutzers ausbreitete, sondern auch Kopien von sich selbst an die ersten 50 Adresseeinträge aus dem Adressbuch des Benutzers versendete. Ein besonders schwieriger Nebeneffekt war die unbeabsichtigte Versendung von Dokumenten an andere. Word Dokumente enthalten oft vertrauliche Informationen, so dass der Schaden, der durch die Verbreitung entsteht, erheblich war.

Spezieller Fall: Der CodeRed Wurm (NT/CodeRed.A)

Typ: Binärer stream Wurm
Infiziert: Windows 2000 Rechner auf denen IIS läuft

Bis zum August 2001 existierte Schadenssoftware generell in *Dateien*. Programme sind, während sie ausgeführt werden existent im Speicher, aber da sie normalerweise durch eine Datei gestartet werden, haben sich Antivirensoftware Hersteller traditionell auf die Entdeckung von Schadenssoftware in Dateien fokussiert.

Diese Erkenntnis änderte sich mit *CodeRed*. *CodeRed* ist ein Programm ähnlich jedem anderen Programm. Dennoch gibt es einen entscheidenden Unterschied: es manifestiert sich nie selber auf der Festplatte. Dies erschwert es für die meisten Antivirenprogramme den Wurm überhaupt zu entdecken. Er gelangt als eine Art von Datenstrom aus dem Netzwerk in den Computer. Die empfangende Maschine erkennt das Ereignis als ein Programm und führt es von seinem Platz im Speicher aus. Natürlich sollte dies keine erlaubte Aktion sein, aber CodeRed nutzt, um dies zu erreichen, einen bekannten Fehler oder Fehlfunktion im Internet Information Server aus.

Einmal auf einer lokalen Maschine ausgeführt, wird er erneut versuchen Kontakt zu anderen Rechnern aufzunehmen, um sich zu verbreiten. Der Wurm kann einfach gestoppt werden, indem man ein Patch für den IIS Server einspielt, um den Bug, den der Wurm ausnutzt, zu eliminieren. Es ist jedoch möglich, dass in Zukunft andere Würmer andere Sicherheitslücken ausnutzen.

Spezieller Fall: Der LoveLetter Virus (VBS/LoveLetter.A@mm)

Typ: Script Dateivirus
Infiziert: VBScript Dateien

Anfang Mai 2000 klingelten die Telefone bei allen Antiviren Vertreibern auf der Welt „Unterstützen Sie die Erkennung des Virus I love you?“ Der Frage folgte zunächst eine atmelose Stille, gefolgt von der Antwort „Welcher I love you Virus?“

Diese Viren Epidemie demonstrierte eine sehr unangenehme Eigenschaft moderner e-mail Viren und Würmer: sie sind sehr schnell. Bevor überhaupt die Antivirenindustrie den Virus gesehen hatte, hatten Benutzer überall auf der Welt Kopien in ihrer Mail Box empfangen. *LoveLetter* ist ein sehr gutes Beispiel für die Wichtigkeit von häufigen Antiviren Updates und die Wichtigkeit eine gute Heuristik zu verwenden („Erkennung unbekannter Viren“).

Randnotiz: *VBS/LoveLetter.A* ist ein reeller Virus, da er VB Skript Dateien durch sich selbst überschreibt. Dennoch zeigt er nur seine Wurm Funktionalität. Das entscheidende Merkmal der schnellen Verbreitung ist der Grund warum LoveLetter manchmal nicht überraschend als Wurm bezeichnet wird.

Spezieller Fall: Nimda (W32/Nimda.A@mm)

Typ: Binärer ausführbarer Virus
Infiziert: Windows 9x/Me/NT/2000 Rechner

Dies ist ein sehr interessanter Fall. Dieser Virus verwendet eine Ansammlung von Techniken zur Verbreitung. Dennoch ist der verblüffendste Teil die Internet Verbreitungs Technik.

Vor dem Erscheinen von *Nimda* hatten bereits einige Virenautoren mit der Infektion von Benutzern vom Web Server aus experimentiert. Das Problem aus Sicht der Virenschreiber war, dass eine Infektion auf diesem Weg einen Angriffspunkt darstellte. Sobald die angreifende Webseite indentifiziert war, wurde diese geschlossen. Dies führte automatisch zur Beseitigung des Virus. Andere Würmer, wie etwa *CodeRed* versuchen in Web Server einzudringen oder diese zu infizieren. *Nimda* war der erste, der diese Effekte kombinierte.

Wenn *Nimda* auf einer Maschine ausgeführt wird (bitte bedenken Sie es handelt sich um eine ausführbare Datei), beginnt er nach Web Servern zu suchen. Hierfür erzeugt er zufällige Internet Adressen und versucht einen Kontakt zu diesen aufzubauen. Kann eine Verbindung aufgebaut werden, hackt *Nimda* den Web Server effektiv und kopiert sich selbst dorthin. Läuft er auf dem Web Server modifiziert er Webseiten in der Art, dass Surfer die diese Seite besuchen infiziert werden. Diese zwei Wege Infektion birgt auch ein zweiseitiges Problem: Benutzer sind es nicht gewöhnt Webseiten als mögliche Infektionsquelle zu betrachten und es gibt nicht länger nur einen Web Server, der zum Stoppen des Virus abgeschaltet werden kann. Der Verbeitungsmechnismus im Web ist mehr als schädlich, wenn man bedenkt, dass der Benutzer keinen Anhang öffnen muss, um sich zu infizieren - *Nimda* nutzt einen Programmierungsfehler in einigen Versionen des Internet Explorers aus, um automatisch ausgeführt zu werden, wenn eine Web Seite (oder Mail Text) angesehen wird.

Nimda besitzt auch andere üblichere Verbreitungsmechanismen, er infiziert binäre ausführbare Dateien, verbreitet sich über freigegebene Verzeichnisse in lokalen Netzwerken und versendet sich selbst via e-mail.

Spezieller Fall: Sircam (W32/Sircam.A@mm)

Typ: Binärer ausführbarer Wurm
Infiziert: Windows 9x/Me/NT/2000 Rechner

Von diesem mittelmässigen Wurm wurde bei seinem Erscheinen kein grosser Schaden erwartet. Er verbreitet sich durch gewöhnliche e-mails und hat einen teilweise festgelegten Body Text, so dass er einfach bemerkt werden kann. Dennoch hat sich dieser Wurm als sehr hartnäckig und schwer aufzuspüren erwiesen. Während dieser Text geschrieben wird ist er wahrscheinlich der am weitesten verbreitete Wurm weltweit. Aus welchem Grund?

Das bemerkenswerteste Merkmal von *Sircam*, ist der Trick, den er anwendet, wenn er sich selbst via e-mail versendet. Er findet ein zufälliges Dokument, eine Tabellenkalkulation oder eine Zip Datei auf der Festplatte und hängt dieses einfach an sich selbst an. Die daraus entstehende Datei hat den Namen des Originaldokuments, fügt jedoch eine Dateiendung hinzu. Zum Beispiel `mydocument.doc` wird zu `mydocument.doc.exe`. Wenn Sie beim Lesen der e-mail nicht genau aufpassen, kann die Datei fälschlicherweise für das unifizierte Originaldokument gehalten werden.

Die schreckliche Konsequenz dieses Tricks ist, dass persönliche und/oder geheime Informationen unbeabsichtigt versendet werden können. Der Wurm achtet nicht darauf ob er ein einfaches Memo oder firmen-interne Finanzinformationen versendet. Dies demonstriert die Gefahr der modernen Computernutzung - sogar ihre eigene Festplatte kann für jedermann sichtbar gemacht werden. Vertrauliche Informationen sollten immer verschlüsselt werden und bevorzugt auf einem herausnehmbaren Datenträger, wie z.B. Floppies oder CD's gespeichert werden.

Voraussagen für die Zukunft

Norman erwartet, daß Makroviren nach wie vor eine ernste Bedrohung der Datensicherheit darstellen, wenn es auch Grund zu der Annahme gibt, daß die Wachstumsrate sich verringern wird.

Einige Skriptsprachen haben es völlig deutlich gemacht, dass von Ihnen ein grosses Sicherheitsrisiko ausgeht und oft zeigen sich neue Skriptsprachen. Skriptviren bleiben auch in Zukunft ein vorhersehbares Problem.

In den letzten paar Jahren tauchten binäre Dateiviren und Würmer wieder verstärkt auf. Die Verbreitung dieser Gruppe von Viren hatte in den frühen und mittleren 90'er Jahren stark abgenommen, da mit der Einführung von Windows der Austausch von ausführbaren Dateien immer weniger wurde, während zur gleichen Zeit die e-mail Systeme noch nicht so hoch entwickelt waren, dass e-mail Würmer unterstützt wurden. Das Internet und die moderne Windows Software haben die Situation völlig geändert. Heutzutage werden sehr häufig Dateien und mit ihnen Viren via e-mails und andere Netzwerkfunktionen ausgetauscht. So lange, wie Programme frei ausgetauscht werden können, werden auch binäre Dateiviren vorhanden sein.

Andere Bereiche der Computernutzung ändern sich. Das Internet als „Umgebung“ wird immer komplexer und immer enger verbunden. Dies birgt neue Möglichkeiten für Schadenssoftware. Genau wie die Terroristen des Internet zeigen ist die neue Realität hart, wenn nicht unmöglich vorherzusehen. Es ist nicht unmöglich, dass die nächste ernstzunehmende Virenepidemie auf einem dieser nicht vorhersehbaren neuen Wege auftauchen wird. Bereits durch das *CodeRed* Vorkommen wurde klar, dass Teile der Internet Infrastruktur angreifbar sind und eine Rolle bei zukünftigen Ausbrüchen spielt.

Norman wird weiterhin versuchen mit dem Problem der Viren Schritt zu halten. Einige der weltweit bekanntesten Experten arbeiten bei uns daran, die Entwicklung der Computersicherheit zu überwachen und wir werden darauf vorbereitet sein, Vorfälle zu unterbrechen, bevor ein Schaden entsteht.

Wie viele Viren gibt es...

Anbietern von Anti-Virus-Programmen wird diese Frage ständig gestellt. Die Frage ist aus mehreren Gründen schwer zu beantworten:

1. Es gibt keine zentrale Stelle, die die Zahl der Viren zählt.
2. Jeden Tag kommen neue Viren hinzu. Einige Experten meinen, daß die Zahl der neuen Viren exponential ansteige, andere sehen einen quadratischen Anstieg. Wenn wir in der Lage wären, alle zu zählen, wäre das Ergebnis nur für kurze Zeit, vielleicht einen Tag lang, gültig.
3. Basierend auf einem Virus entdecken wir häufig viele Varianten und oft besteht innerhalb der Gemeinschaft der Virenforscher Uneinigkeit darüber, wie „Variante“ zu definieren ist.
4. Es gibt keine standardisierte Benennungskonvention für Viren. Als Folge tauchen für denselben Virus mehrere verschiedene Bezeichnungen auf.

Dies führt uns zu der Frage, wie Viren zu ihren Bezeichnungen kommen. Manchmal fügen Virenautoren Text in den Virus ein, der den Namen für den Virus oder den eigenen Namen wiedergibt (z.B. Der Virus XXX ist da; Grüße von yyy). Meistens jedoch werden die Namen von den Leuten vergeben, die die Viren entdecken. Dabei werden verschiedene Vorgehensweisen angewendet:

Angenommener Herkunftsort oder Entdeckungsort (z.B. der Lehigh Virus), Anzahl der vom Virus an die Dateien angehängten Byte, Auswirkungen des Virus usw.

Vor diesem Hintergrund erkennen die Produkte von Norman Virus Control zum Zeitpunkt der Erstellung dieses Handbuchs (Juli 2001) über 51.000 Virenvarianten.

...und welche Rolle spielt das?

Für den normalen Benutzer spielt es keine Rolle wie viele Viren es gibt, solange seine Anti Viren Software die Maschine virenfrei hält. Die Anzahl der bekannten Viren spiegelt nicht wirklich die Änderungen und Vorgänge in der weltweiten Virenentwickler Szene wieder.

Statistiken können jedoch zum Beispiel hilfreich sein, als visuelle Manifestation der Entwicklung der Computer Viren.

Das Problem der Computer Viren kann am besten erforscht werden, indem man die Natur der Viren und was sie hervorrufen analysiert und nicht dadurch, daß man festhält wie viele Viren es gibt. Dies kann eine mögliche Aussage der Virenentwickler gewesen sein, die 14.000 brandneue Viren an Anti Viren Hersteller/Vetrreiber in aller Welt schickten (Herbst 1998). Alle diese Viren waren automatisch erzeugt und waren daher technisch nicht sehr ausgefeilt. Es konnten daher die meisten dieser Viren mittels heuristischer Methoden erkannt werden. Nichts desto trotz hat sich die *Anzahl* der Virensignaturen in unseren Definitionsdateien fast über Nacht verdoppelt, obwohl sich die Bedrohung durch Viren nicht verändert hat.

Viren in freier Wildbahn

Virenforscher kennen zwar Tausende von Viren, nicht alle müssen Sie jedoch beunruhigen. Die meisten dieser Viren kommen nur in Forschungslaboren vor und nur die verbleibende Handvoll befällt tatsächlich Heim- und Unternehmenscomputer auf der ganzen Welt.

Virenforscher sprechen von zwei Virenkategorien: Viren, die „in freier Wildbahn“ auftreten und Viren „im Zoo“. Diese werden oft auch mit der Abkürzung der englischen Bezeichnung „ITW“ und „ITZ“ bezeichnet.

Viren „in freier Wildbahn“ wurden außerhalb der Forschungslabore entdeckt. Diese „wildernden“ Viren machen ca. 10% der bekannten Viren aus und sind diejenigen, mit denen Sie und Ihr Unternehmen sich auseinandersetzen sollten.

Weitere Einzelheiten hierzu erhalten Sie vom Händler in Ihrer Nähe oder direkt von Norman.

Sowohl Firmen als auch Einzelplatzbenutzer müssen sich selbst durch häufige Aktualisierung ihres Antivirenwerkzeugs schützen. Im Umkehrschluss heisst das, dass die Antivirenindustrie kontinuierlich ihre Definitionsdateien aktualisieren und verteilen müssen.

Die Definitionsdateien enthalten die Virensignaturen (Fingerabdrücke der Viren) und wird von der Suchmaschine verwendet, um Viren zu entdecken und zu beseitigen.

Jeder Virusscanner kann nur so effektiv sein, wie sein aktuelles Update, daher ist es wichtig so oft wie möglich mit Aktualisierungen versorgt zu werden, da nur so eine sichere Umgebung geschaffen werden kann.

Norman Virus Control Version 5 oder neuer macht diesen Prozess durch automatisches Downloads und Installation von Norman sehr einfach für sie.

Entwicklung des Virenproblems

Am Anfang waren die Computer untereinander noch nicht sehr gut verbunden und Computerviren konnten sich nur langsam ausbreiten. Dateien wurden über Bulletin-Board-Systeme (BBSs) oder über Disketten übertragen. Die Übertragung von infizierten Dateien und Boot-Sektoren war demzufolge geografisch beschränkt.

Mit der zunehmenden Verbindung von Computern, hauptsächlich der Computer am Arbeitsplatz, in Netzen erweiterten sich auch die Grenzen für die Computerviren. Zuerst kam das lokale Netzwerk (LAN), dann das Weitbereichsnetz (WAN) und nun das Internet. Die verbreitete Verwendung von E-Mail hat ebenfalls dazu beigetragen, daß die Zahl der Infizierungen durch Makroviren rasant angestiegen ist.

Wir leben heute in einer Gesellschaft, in der globale Technologien an erster Stelle stehen und globaler Handel über Kommunikationswege getätigt wird. Computer sind ein integraler Teil dieser Technologie und auch die Informationen, die sie speichern (ebenso wie der böartige Code, den sie unwissentlich enthalten), werden global. Es ist also heute viel wahrscheinlicher sich einen Virus einzufangen als noch vor zwei Jahren. Heute sind jedoch andere **Arten** von Viren gängig als vor zwei Jahren.

Steve White, Jeff Kephart und David Chess vom IBM Thomas J. Watson Research Center verfolgen die Entwicklung der Viren und haben (unter anderem) herausgefunden, daß die Vorherrschaft von bestimmten Virenarten teilweise durch die Änderungen bei Betriebssystemen bedingt ist.¹

1. Steve R White, Jeffrey O Kephart and David M Chess, 'The Changing Ecology of Computer Viruses' *Proceedings of the Fifth International Virus Bulletin Conference*, Brighton, UK, 1996.

Viren in verschiedenen Betriebssystemen

Computerviren wurden zuerst Anfang 1981 erstellt als ein Programm mit dem Namen „Elk Cloner“ für den Apple IIe Computer entwickelt wurde. Es tauchte auf einigen Bulletin Board Systemen auf, verbreitete sich jedoch nicht sehr stark und wurde nie als Virus bezeichnet. Dr. Fred Cohen prägte diesen Begriff 1983 als er Konzepte und Experimente mit Replizierungsprogrammen untersuchte (<http://all.net/books/virus/index.html>). Diese Experimente wurde in kontrollierten Mainframe Umgebungen ausgeführt.

Obwohl die zuerst auftretenden Viren für Betriebssysteme wie Apple II und VAX entwickelt wurden, wurden sie nicht zu einem ernststen Problem, bis die ersten für MS-DOS erstellt wurden. MS DOS war das erste bedeutende Betriebssystem und als dieses hatten die Viren für dieses Betriebssystem ein wesentlich höheres Potential zur Verbreitung als Viren für andere Betriebssysteme. Es dauerte einige Jahre um Windows zu stabilisieren und populär zu machen, dass heisst Viren breiteten sich vor allem in MS DOS aus. In der Tat waren auch Jahre nach der Einführung von Windows fast alle Dateiviren DOS basiert und die erste Windows Generation (bis hoch zu Windows 3.11 für Workgroups) wurden nicht sehr stark von Viren bedroht. Dennoch erhielten wir mit dem Auftauchen von Microsoft Word auf dieser Plattform und die mit diesem Programm einhergehenden Makroviren einen Ausblick darauf was später auf uns zukam.

Obwohl OS/2 kurz nach Erscheinung der Viren eingeführt wurde, ist OS/2 als Betriebssystem nicht so gängig wie DOS. Deshalb war und ist es unwahrscheinlicher, daß Virenautoren selbst mit OS/2 arbeiten und auch wenn OS/2-Viren häufig geschrieben würden, wären sie nicht so weitverbreitet wie MS-DOS-Viren. Gegenwärtig sind nur eine handvoll OS/2-Viren bekannt.

Heutzutage ist DOS aus der Mode gekommen obwohl DOS ähnliche Funktionalitäten immer noch auf Windows Rechnern existieren. Wie dem auch sei auf einem Virus Schauplatz ist DOS für alle Intentionen und Zwecke genauso tot wie Disko.

Die heutzutage aktuellen Betriebssysteme sind 32-bit Windows Varianten (Win 95/98/ME, Win NT/2000/XP) und die verschiedenen UNIX Varianten. Schauen wir uns die Viren in MS-DOS, Windows, OS/2, Windows 95/98 und Windows NT/2000 und UNIX einmal an.

MS-DOS

Da die Makroviren, die bis heute aufgetreten sind, Datendateien infizieren, die von Windows-Anwendungen erzeugt und gelesen werden, stellen Makroviren auf Rechnern, die nur über MS-DOS verfügen, kein Problem dar.

Traditionelle Dateiviren und Boot-Viren gedeihen auf MS-DOS-Rechnern, da MS-DOS nicht über eigene Sicherheitsfunktionen verfügt. Viren haben deshalb freien Lauf bei der Infizierung von Speicher und Programmdateien, wie unter "Dateiviren" auf Seite 14 beschrieben.

Windows

Als Windows eingeführt wurde, mußten Benutzer bei der Interaktion mit dem Computer umlernen. Die Bilder auf dem Bildschirm waren farbiger, das Navigieren innerhalb eines Programms wurde einfacher und direkter und die Aussicht, zwischen Aufgaben umschalten zu können, ohne die jeweiligen Programme beenden zu müssen, war sehr aufregend.

Da DOS „unterhalb“ von Windows 3.x ausgeführt wird, können Dateiviren Rechner infizieren, die Windows ausführen, jedoch ist ihre Lebensspanne sehr kurz. Im allgemeinen können Dateiviren die ausführbaren Dateien von Windows infizieren, aber dann arbeiten diese Dateien in der Regel nicht richtig. Ungeduldige Benutzer werden entweder die ausführbaren Dateien ersetzen oder, wenn sie frustriert genug sind, Windows neu installieren. Das reicht schon aus, um den traditionellen Dateivirus umzubringen. Darüberhinaus ist die Struktur der ausführbaren Dateien unter Windows 3.x komplizierter als die der EXE Dateien in Windows 9x/NT und der Speicher ist besser geschützt. Daher können diese Viren unter Windows 3.x nie zu dem gleichen großen Ärgeris, wie unter neueren Windows Versionen werden.

Makroviren und Bootviren erleiden jedoch nicht dasselbe Schicksal. Makroviren werden bis heute so geschrieben, daß sie Windows-Anwendungen angreifen. Deshalb ist das Vorhandensein von Windows erforderlich. Die breite Akzeptanz von Windows zusammen mit der Tatsache, daß Makroviren statt Programmdateien eher Datendateien infizieren (siehe siehe “Makrovirus” auf Seite 19), hat dazu geführt, daß sechs Makroviren , heute zu den zehn verbreitetsten Viren gehören.

Der eigentliche Boot-Vorgang auf einem Windows-Rechner unterscheidet sich nicht von dem eines reinen DOS-Rechners. Deshalb werden Boot-Viren durch Windows nicht behindert und verbreiten sich weiter, indem sie Festplattenlaufwerke infizieren, speicherresident werden und dann Diskettenlaufwerke infizieren.

OS/2

Wie bereits oben erwähnt, ist OS/2 nicht so weit verbreitet wie Windows und andere Betriebssysteme von Microsoft. Aufgrund seiner Konzeption ist OS/2 jedoch trotzdem anfällig auch für Viren, die nicht OS/2-spezifisch sind.

Im Gegensatz zu Windows, wird OS/2 nicht über MS-DOS ausgeführt. OS/2 ist ein leistungsstarkes 32-Bit-Betriebssystem, das DOS-Anwendungen, Windows-Anwendungen und eigene OS/2-Anwendungen unterstützt. Um DOS-Anwendungen ausführen zu können, ist OS/2 mit VDMs (virtuellen DOS-Maschinen) ausgestattet.

Wie der Name besagt, sehen die VDMs für DOS-Programme wie DOS aus. Deshalb kann ein infiziertes DOS-Programm andere DOS-Programmdateien innerhalb dieses VDM infizieren, nicht jedoch DOS-Programme in anderen VDMs. Die neu infizierten DOS-Programmdateien können dann weitere Programmdateien infizieren, die in VDMs zukünftig noch gestartet werden. Auf diese Weise setzt sich der Infektionsweg fort.

Wenn Windows-Anwendungen, die Makrosprachen enthalten, auf einem OS/2-Rechner ausgeführt werden, ist der OS/2-Rechner genauso anfällig für Makroviren wie ein Windows-Rechner.

Noch einmal - da der Boot-Vorgang vor dem Laden des Betriebssystems auf allen IBM-kompatiblen Rechnern gleich ist, können Boot-Viren auch OS/2-Rechner infizieren. OS/2 behandelt Disketten anders als DOS und Windows, daher ist die Wahrscheinlichkeit, daß der Boot-Virus sich nach der Infektion der Festplatte ausbreitet, ist auf einem OS/2-Rechner niedriger als auf einem Rechner mit Windows oder DOS. Das Risiko besteht eher in den Aktionen, die der Boot-Virus auf der Festplatte ausführt. Wenn der Boot-Virus über eine Ladung verfügt, kann man davon ausgehen, daß diese auch abgegeben wird, unabhängig davon, ob Disketten infiziert werden konnten.

OS/2 unterstützt zwei Dateisysteme: FAT (File Allocation Table - Dateizuordnungstabelle) und HPFS (High Performance File System - Leistungsfähiges Dateisystem). Sie können nur eines oder beide verwenden. HPFS ist ausgefeilter und speichert Informationen an verschiedenen Orten. Ein Boot-Virus, der nur auf FAT eingerichtet war, kann schwerwiegende Folgen für ein HPFS-System haben.

Windows 95/98/ME

Windows 95 wurde zu einer Zeit veröffentlicht als das Internet allgemein zugänglich wurde. Heute ist das World Wide Web für alle nutzbar nicht nur für registrierte Benutzer. Obwohl die meisten PC Benutzer das Internet, die Möglichkeiten, die e-mail und Chatting Programme bieten begrüßen, ist die andere Seite der Medaille, dass sich das Internet auch als eine Art großer "Spielplatz" für Viren Entwickler darstellt, die manchmal auch als Internet Terroristen bezeichnet werden. Die weit verbreitete Nutzung dieser Möglichkeiten, hat dazu geführt, dass die Verbreitung von Viren unter Windows 9x/ME immer mehr zunimmt.

Im Gegensatz zu Windows und DOS sind in Windows 95/98 Sicherheitsfunktionen integriert. Diese Funktionen sind jedoch nicht ausreichend, um Windows 95/98 gegen Viren zu schützen. Tatsächlich wurde der erste Virus, der speziell für Windows 95 geschrieben wurde (der Boza-Virus) Ende 1995 veröffentlicht. Darüber hinaus verfügt die Netzwerkumgebung der Workgroup von Windows 95/98 über keinen Schutz auf Dateiebene, was die Virenverbreitung unterstützen kann.

Nach der Veröffentlichung des relativ primitiven Boza Viruses, hat die Zahl der Windows 95/98 und Windows NT/2000 Viren an Zahl und Komplexität stark zugenommen. Wie die ersten Viren in der DOS Umgebung waren auch hier die ersten Viren recht amateurhaft. Nachdem die Virenschreiber jedoch immer mehr Erfahrung sammeln konnten, wurden auch die Viren technisch immer komplexer. Einige der Viren in Windows 95/98 und Windows NT/2000 verbreiten sich durch die aktive Nutzung der Netzwerk Protokolle. Ein temporärer Höhepunkt dieser Entwicklung immer komplexerer und zerstörerischer Viren war mit dem Erscheinen des CIH Viruses im Jahr 1998 erreicht (siehe auch Seite 26). Spätere Viren wurden zunehmend verschlagener.

Windows 95/98 hat, was die Systemarchitektur und die Vireninteraktion betrifft, viele Merkmale mit OS/2 gemeinsam:

Wie OS/2 ist Windows 95/98 ein 32-Bit Betriebssystem, das DOS-Anwendungen, Windows-Anwendungen und eigene Windows 95/98-Anwendungen unterstützt.

Ähnlich wie die VDMs von OS/2, hat Windows 95/98 VMs (virtuelle Maschinen) eine virtuelle System-Maschine mit unterschiedlichen Adreßbereichen für Win32-Anwendungen und einem gemeinsamen Adressbereich für alle Win16-Anwendungen sowie eigene virtuelle Maschinen für einzelne DOS-Anwendungen.

Dateiviren können sich auf einem Windows 95/98-Rechner mühelos ausbreiten, da DOS-Programmdateien unter Windows 95/98 nur der Beschränkung unterliegen, daß sie nicht direkt auf die Festplatte schreiben können.

Die einzelnen DOS-VMs nehmen die Charakteristiken des Systems von dem Punkt ab an, an dem die Maschine gestartet wurde. Da Windows 95/98 zunächst dieselben Programme ausführt wie ein reiner DOS-Rechner, ist es möglich, daß ein infiziertes Programm während des Startvorgangs andere Programmdateien innerhalb dieser VM infizieren kann. Darüber hinaus würde ein beim Startvorgang infiziertes Programm in allen VMs aktiviert, die zukünftig gestartet würden. Auch wenn Programmdateien einer VM keine Programmdateien einer anderen VM infizieren können, ist es doch möglich, daß eine infizierte Programmdatei irgendwann einmal auf eine eigene VM geladen wird und dabei den Infektionsweg fortsetzt.

Die bis zum jetzigen Zeitpunkt geschriebenen Makroviren greifen Datendateien an, die von häufig auf Windows 95/98 ausgeführten Win16- und Win32-Anwendungen erstellt und gelesen werden. Die Folge davon ist, daß auf Windows 95/98 Infektionen durch Makroviren verbreitet sind.

Da der Boot-Vorgang für Windows 95/98 (bis zu einem gewissen Punkt) dem für DOS- oder Windows-Rechner entspricht, können Boot-Viren die Festplattenlaufwerke von Windows 95/98-Rechnern infizieren. Beim Laden von Windows 95/98 werden Boot-Viren jedoch häufig deaktiviert und können sich nicht verbreiten. Allerdings können Boot-Viren, die eine Ladung führen, diese Ladung abgeben, auch wenn sie sich vorher nicht reproduziert haben.

Windows NT/2000/XP

Wie in den Abschnitten zu OS/2 und Windows 95/98 erläutert, unterstützt Windows NT DOS-Anwendungen, Windows-Anwendungen und eigene Windows NT-Anwendungen. Wie Windows 95/98 ist auch Windows NT rückwärts kompatibel und bis zu einem gewissen Grad auch mit DOS und Windows. Auch wenn NT über robustere Sicherheitsfunktionen verfügt als Windows 95/98, kann es trotzdem von Dateiviren befallen werden, die sich dort verbreiten. DOS-Anwendungen werden in eigenen VDMs (virtuellen DOS-Maschinen) ausgeführt und Dateiviren können innerhalb der VDM funktionieren. Einige DOS-Dateiviren arbeiten vielleicht unter NT nicht in der beabsichtigten Weise, aber die NT-Sicherheitsfunktionen halten Dateiviren bestimmt nicht davon ab, weitere Dateien zu infizieren. NT besitzt eine Funktion, die sich System File Checker (SFC) nennt, doch dieses kann umgangen werden.

Auch Windows NT (wie Windows 95/98) unterstützt Anwendungen, die Makrosprachen enthalten. NT ist deshalb genauso anfällig für Makroviren wie reine Windows-Rechner.

Da Rechner mit Windows NT auf die gleiche Weise booten wie DOS-Rechner (bis zu dem Punkt, an dem NT aufgerufen wird), können Boot-Viren die Festplattenlaufwerke von NT infizieren. Wenn diese Boot-Viren jedoch versuchen, sich im Speicher einzunisten, werden Sie von NT gestoppt und können keine Disketten infizieren. Auf diese Weise wird auch der Infektionsweg gestoppt, der Benutzer muß jedoch trotzdem mit möglichen Nebeneffekten, die die Boot-Viren auf das System haben fertig werden — destruktive Ladungen oder Falschbehandlung des Boot-Bereichs von NT, die das Laden von NT verhindert.

Einige Viren greifen Windows NT auch direkt an. Der W32/Funlove und der W32/Bolzano Virus unterminieren das NT Sicherheitshandling und die gerade entdeckte NT/CodeRed Serie von Viren nutzt Sicherheitslöcher aus, die in Software gefunden wurden, die exklusiv auf NT läuft.

Lösungen des Virenproblems

Standardabläufe einführen

Bevor Organisationen und Einzelnutzer interne Standardabläufe zur Datenverarbeitung eingeführt haben, ist der virenfreie Betrieb einer Datenverarbeitungsumgebung unwahrscheinlich. Unserer Erfahrung nach ist eine Organisation, innerhalb derer Strategien und Abläufe zur Datenverarbeitung auf Managementebene angeregt werden, weniger anfällig für Virenbefall. Falls er dennoch auftritt, vereinfachen Abläufe die Ausrottung der befallenen Dateien vor ihrer Ausbreitung.

Lösungen zur Bekämpfung von Viren

Die meisten denken bei Lösungen zur Bekämpfung von Viren sicherlich an Virensuchprogramme. Suchprogramme sind die am leichtesten erhältliche, jedoch nicht die einzige Art der Virenbekämpfung.

Man sollte die Lösungsmöglichkeiten vielleicht unter folgenden Gesichtspunkten erörtern:

- Was ist nötig, um den Virus zu erkennen?
 - allgemeine Methoden
 - spezielle Methoden

und

- Wann wird der Virus entdeckt?
 - vor der versuchten Infizierung
 - nach der Infizierung

Ein Virus kann anhand allgemeiner oder spezieller Methoden erkannt werden. Allgemeine Methoden suchen nach virenkonformen Verhaltensweisen und nicht nach bestimmten Viren. Auf diese Weise können sogar neue Viren entdeckt werden und es besteht keine Notwendigkeit, das verwendete Werkzeug häufig zu aktualisieren.

Da allgemeine Methoden nach Verhaltensweisen und nicht nach bestimmten Viren suchen, wird normalerweise der Name der Viren nicht angegeben. Statt dessen wird lediglich eine Warnung an den Benutzer ausgegeben, daß wahrscheinlich ein Virus vorhanden ist. Einige schrecken vor dieser Methode zurück, da sie falschen Alarm verursachen kann.

Beispiele für angewendete allgemeine Methoden:

- Prüfsumme und Integritätsüberprüfung
- Heuristik
- Köder
- Behavior Blocking

Spezifische Methoden vertrauen auf zuvor gewonnene Kenntnisse über den Virus. In diesem Fall kann das Tool sowohl einen vorhandenen Virus erkennen als auch diesen Virus identifizieren. Das Tool muß häufig aktualisiert werden. Die meisten Benutzer möchten gerne wissen, mit was sie es zu tun haben, und um das herauszufinden ist es am besten, das Wesen der Bestie genau zu bestimmen. Aus diesem Grund bevorzugen viele Benutzer dieses Verfahren, aber letzten Endes finden Sie keinen Gefallen daran, daß das Tool sehr häufig aktualisiert werden muß.

Beispiele für eingesetzte spezifische Erkennungsmethoden:

- Bedarfsgesteuerte und zeitgesteuerte Suche
- Suche in Echtzeit

Bitte beachten Sie das die oben genannten Methoden nicht immer nur spezifisch sind - heuristische Methoden sind normalerweise Teil von bedarfsgesteuerten Suchen und Echtzeitscannern.

Ein weiterer, nicht minder wichtiger Gesichtspunkt betrifft den Zeitpunkt der Virenerkennung. Alle Benutzer stimmen wahrscheinlich darin überein, daß die Viren idealerweise davon abgehalten werden sollen, Dateien zu infizieren. Die nächste Stufe wäre die, alle Bereiche zu erkennen, die bereits infiziert wurden.

Im folgenden wird untersucht, wo die obengenannten Methoden fehlschlagen:

Methode	Diskussion der Virenerkennung
Prüfsumme und Integritätsüberprüfung	Beide Methoden speichern Informationen zu (hoffentlich) nicht infizierten Dateien an einen bestimmten Ort. Überprüfungen des aktuellen Status der Dateien gegen die gespeicherten Informationen werden in regelmäßigen Abständen durchgeführt. Bei festgestellten Änderungen wird eine Warnmeldung ausgegeben. Diese Methode entdeckt die Viren nach der Infizierung.
Heuristik	Bei dieser Methode werden die Dateien und Boot-Bereiche in einem allgemeinen Sinn untersucht, um zu bestimmen, ob der Code virenkonform aussieht. Heuristische Untersuchungen erkennen Viren nach der Identifizierung.
Köder	Bei dieser Methode werden bestimmte Dateien als Köder ausgelegt, die bei vorhandenem Virus infiziert werden. Köder erkennen Viren bei der Infizierung und geben eine Warnung aus.
Behavior blocking	Diese Methode analysiert das Verhalten aller Verarbeitungsaktionen und stellt dadurch fest, ob sich die Summe der Teile zu einer viruskonformen Aktion verbindet. Wenn ja, wird die Aktion gestoppt, bevor es zu einer Infizierung kommen kann. Behavior blocking erkennt Viren vor der Infizierung.
Bedarfsge- steuerte und zeitgesteu- erte Suche	Diese Methode sucht zu bestimmten Zeiten nach bestimmten Viren. Auf diese Weise können Viren immer erst nach der Infizierung erkannt werden.
Suche in Echtzeit	Bei dieser Methode wird ein Suchprogramm verwendet, der Erkennungsprozeß findet jedoch gleichzeitig mit anderen Computerprozessen, wie z.B. dem Kopieren einer Datei, statt. Als Folge erfahren Benutzer von vorhandenen Viren, bevor diese ausgelöst werden können..

Das Thema der Virenentfernung ist ähnlich komplex. Viele Betroffene haben eine enggesteckte Vorstellung von Virenentfernung -wenn die Datei gelöscht oder die Festplatte formatiert wird, ist der Virus weg. Beachten Sie jedoch, daß diese drastischen Maßnahmen häufig nicht nötig sind und daß die sinnvolle Virenentfernung lediglich den Virencode entfernt und ein benutzbares, sauberes System übrig bleibt.

Einige der oben aufgeführten Erkennungsmethoden können auch Virenentfernung ausführen (nach der sinnvollen und „gesunden“ Methode):

Methode	Diskussion der Virenentfernung
Prüfsumme und Integritätsprüfung	Kann Viren entfernen.
Heuristik	Kann manchmal Boot- und Makroviren entfernen.
Köder	Kann keine Viren entfernen.
Behavior blocking	Kann Viren aus dem Speicher und Bootviren von Disketten entfernen.
Bedarfsgesteuerte und zeitgesteuerte Suche	Kann Viren entfernen.
Suche in Echtzeit	Kann Viren entfernen.

Industriefakten

Virenstatistiken

„99,67% aller überprüften Firmen fanden mindestens einen Virenvorfall während der Überprüfungszeitraumes. 51% nahmen an, das sie mindestens ein „Virendesaster“ hatten, während der 12 monatigen Periode bevor sie überprüft wurden.“

- *Quelle: 2000 Computer Virus Prevalence Survey, IICSA.net, October 23, 2000*

Allgemeine Statistiken

„Heutzutage werden 45% aller Firmeninformationen oder Ideen im e-mail System der Firma gespeichert.“

- *Quelle: SC Magazine, August 2001*

Finanzielle Statistiken

„Eingeschlossen aller Kosten, liegen die wahren Kosten des Virendesasters zwischen \$100.000 und \$1 Million pro Firma.“

- *Quelle: Computer Crime & Security Survey, Computer Security Institute, March 12, 2001*

Die Sicherheitsbedrohung

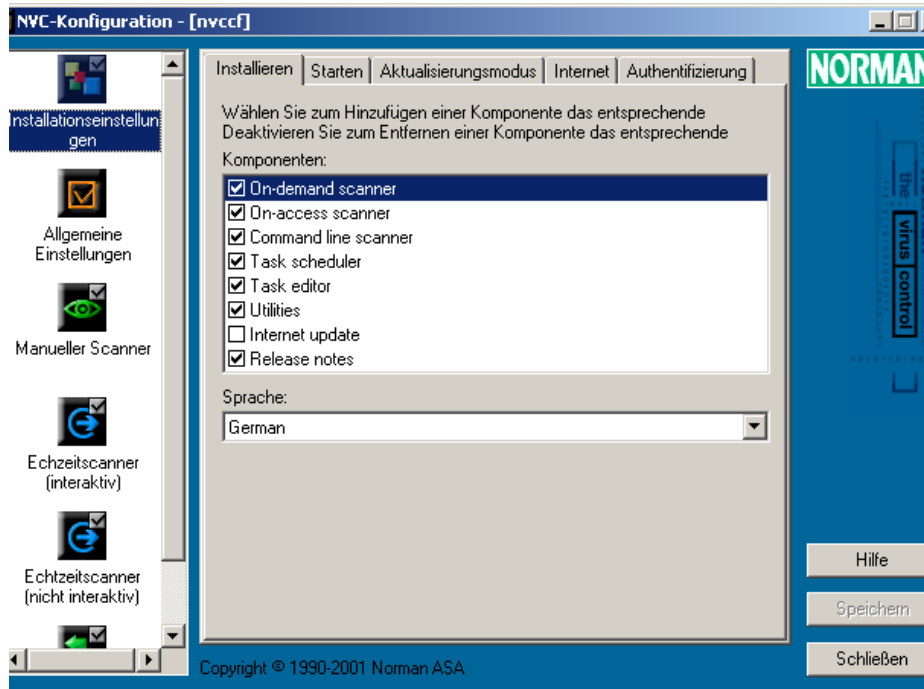
- Reuters berichtete , das ein Schaden von \$12 Mrd. allein in den ersten 6 Monaten des Jahres 2000 durch Computerviren verursacht wurde.
- Laut „Tippets Law of Malicious Code“ verdoppelt sich das Virenproblem alle 14 Monate.

Norman Virus Control

NVC 5 – eine neue Annäherung zur Virenkontrolle

Seit 1989 hat Norman eines der weltweit führenden Viren Control Software Pakete. Die aktuelle Version NVC5 ist das Ergebnis eines Entwicklungszyklus der im Jahr 1999 begann und ein Jahr später beendet wurde.

Virenkontrolle bezieht normalerweise die Benutzerinteraktion wie das Durchsuchen von Dateien mit ein. In den letzten 3 oder 4 Jahren haben wir eine Änderung bezüglich Zugriffsscannern, internet basierten Aktualisierungen und zentralisiertem Management in der Virenkontrolle gesehen. NVC5 nutzt die Möglichkeiten des Betriebssystems vor allem für die volle Integration. Zum Beispiel, ein Dateifilter System Treiber, der unter WindowsNT/2000/XP und OS/2 läuft während ein VxD die gleiche Funktionalität unter Win95/98/Me bietet.



NVC Version 5

Das Produkt wurde entwickelt um vor allem den Anforderungen wie Transparenz, Zuverlässigkeit und einfache Handhabung zu genügen. Es wurden einige Schlüsselziele definiert inklusive:

- **Unsichtbarkeit**
- **Skalierbarkeit**
- **Überprüfbarkeit**
- **Automatischer Support und Wartung**

Das endgültige Design ist das Resultat einer Philosophie, die sich in vielen Dingen von den vorherrschenden Anti Virus Control Produkten unterscheidet.

Zertifizierung

Norman Virus Control wurde von den West Coast Labs mit der Check Marke Level 1 zertifiziert. Von den ICSA labs wurde es für das Zugriffsscannen und Scannen auf Bedarf zertifiziert.



Auszeichnungen



NVC ist eines der Produkte, das in der Vergangenheit des Virus Bulletin Magazins mit 14 von 21 möglichen 100% awards seit der Erstausgabe des Magazins im Januar 1998, die meisten Auszeichnungen gewonnen hat. Der 100% Award zeichnet die Produkte aus, 100% der Viren findet, die zum Testzeitpunkt „in the Wild“ gemeldet wurden.

Virus Alarmprogramm

Im Sog des [Melissa](#) Virus Vorfalls (Ostern 1999) hat Norman ein Viren Alarm Programm eingeführt. Dieses Programm soll Kunden zukünftig in solchen Fällen unterstützen.

Das Norman Virus Control alarm Programm bietet Kunden einen speziellen Service im Falle eines Virenalarms. Nähere Informationen zum Produkt und wie sie es erhalten können finden Sie unter www.norman.de

Index

Symbole

/S 25

Nummern

32-Bit 39

A

anhängen 14

B

Basic Input/Output System 23

BBS 36

Bedarfsgesteuerte Suche 46

begleiten 14

Behavior blocking 46

BIOS 23

Bombe

 Zeit 11

Bomben 11

boot, wie er infiziert 25

Bootfähige Diskette 24

Bootvorgang 23

Boza 41

Bug 11

Bulletin board system 36

C

Chatting Programme 41

Chess, David 36

CIH 26

CodeRed 28, 32

Concept.A 21

D

Diskette, bootfähig 24

DOS 24

DOS BAT Sprache 18

E

Einbetten 20

Einfügender Virus 16

Entwicklung 36

Excel Virus 22

F

FAT 40

File Allocation Table (Dateizuordnungstabelle) 40

H

Heuristik 46

High performance file system (Leistungsfähiges Dateisystem) 40

Hoax 12

HPFS 40

I

Informationssicherheit 5

Integritätsüberprüfung 46

Internet 36

IRC scripts 19

ITW 34

ITZ 34

J

JavaScript 18
JScript 18

K

Kephart, Jeff 36
Köder 46

L

LAN 36
Lehigh virus 33
Linux 24
Logische Bombe 11
Lokales Netzwerk 36
LoveLetter 29

M

Makro-Programmiersprachen 19
 WordBasic 20
Master Boot Sektor 24
MBS 23
Melissa 27
MS-DOS 38

N

Nimda 30
Non system-disk or disk error 24

O

Office 2000 23
Office XP 23
OLE 20
OS/2 24, 39

P

PC 5

POST 24

Power On Self Test 24
Prüfsumme 46

R

RAM 24
Random Access Memory 24

S

SBS 23, 25
Sicherheit, Information 5
Sircam 31
Skriptsprache
 Corel Draw 19
 DOS BAT Sprache 18
 InstallShield 19
 IRC script 19
 JavaScript 18
 JScript 18
 SuperLogo 19
 UNIX shell script 19
 Visual Basic 18
 Visual Foxpro 19
Sprunganweisung 17
Suche in Echtzeit 46
SYS-Befehl 25
System Boot Sektor 23, 24
System-Boot-Sektor 25
Systemoption 25

T

Trojaner 12
Trojanische Pferde 9

U

UNIX shell script 19

V

Variant 33
VBA3 22
VBA5 22
VBA6 23
VDM 39
Verknüpfen 20
verknüpfen 14
verknüpfender Virus 15
Viren
 im Zoo 34
 wie viele 33
Viren im Zoo 34
Viren in freier Wildbahn 34
Virtuelle DOS-Maschine 39
Virus
 anhängend 17
 Boza 41
 CIH 26
 Concept.A 21
 in the wild 34
 Laroux.A 22
 Lehigh 33
 LoveLetter 29
 makro 19
 Melissa 27
 Nimda 29
 überschreibend 15
 voranstellen 14, 16
Virus, was ist das 7
Visual Basic Script 18
Voranstellender Virus 16

W

WAN 36
Weitbereichsnetz 36
White, Steve 36
Wie viele Viren gibt es 33
Windows 24, 38

Windows 95 41
Windows 9x/ME 24
Windows NT/2000 24
WordBasic 20, 22
Worm
 CodeRed 28
 Sircam 31
Wurm 9

Z

Zeitbomben 11

norman

the

virus control

1 0 0 1 0 1 1 0 1 0 0 1 0 0 1 0 1 1

0 1 0 0 1 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 1 0 0

1 0 0 1 0 1 1 0 1

0 1 0 1 1 0 1 0 0

Peace of Mind

Norman is one of the world's leading companies within the field of data security. With products for virus control, personal fire wall, encryption, data recovery, and certified data erasure, the company plays an important role in the data industry.

NORMAN[®]

www.norman.com