1008 Virus

Alias: Suomi, Oulu
Art: Residenter .COM-Infektor
Länge: 1008 Bytes
Symptome: COMMAND.COM wird größer, Stack-Fehler im Betriebssystem, Rechner bleibt beim Booten stehen

Der 1008 Virus ist verschlüsselt und stammt möglicherweise aus Finnland. Er installiert sich resident im Speicher und befällt sofort COMMAND.COM. Jedes nun gestartete .COM-Programm wird ebenfalls infiziert. Die Vergrößerung der befallenen Dateien kann nicht erkannt werden, wenn der Virus im Speicher aktiv ist.

12-Ticks (Trojanisches Pferd)

Dieses trojanische Pferd ersetzt den Master-Bootsektor einer Festplatte mit seinem eigenen. Das Programm kommt "huckepack" auf dem Festplattentest der Firma Core und kann Namen wie CORETST, CORETnnn etc. haben. Die Veränderung des Bootsektors kann leicht durch folgenden Text im Master-Bootsektor ausgemacht werden:

SOFTLoK+ V3.0 SOFTGUARD SYSTEMS INC
2840 St. Thomas Expwy,suite 201
Santa Clara,CA 95051 (408)970-9420

12-Tricks, der seinen Namen von der Anzahl der 'Tricks', die er veranstaltet, bekommen hat, versucht auf verschiedenen Wegen an den originalen Einsprungspunkt in das Festplatten-BIOS im ROM zu kommen. Hat er diesen Einsprungspunkt gefunden, kann er den Master-Bootsektor ändern, ohne auf residente Wächterprogramme Rücksicht nehmen zu müssen. Aus diesem geänderten Master-Bootsektor kopiert 12-Tricks bei einem Neustart rund 200 Bytes in einen selten genutzten Bereich der Interrupttabelle. Dies hat den Vorteil, daß er sich nicht via Betriebssystem resident installieren muß oder durch eine Verringerung des 640KB Bereiches auffällt.

12-Tricks installiert eine von zwölf verschiedenen Routinen beim Neustart eines Systems. Neben Verzögerungen sind langsame Veränderungen an der FAT möglich.

1253

Art: Residenter .COM Infektor
Länge: 1253 Bytes

Der Virus installiert sich auf herkömmlichen Weg resident und infiziert jede geladene .COM Datei. Im vierten bis sechsten Byte einer infizierten Datei ist folgende Kennung zu finden:

V-1

Am 24. Dezember jeden Jahres überschreibt der Virus den kompletten Datenträger mit einem sich wiederholenden Muster von neun Sektoren. Unter Umständen kann es zu unkontrollierten Diskettenaktivitäten nicht angesprochener Laufwerke kommen.

1260

Alias: V2P1
Art: COM-Infektor
Länge: 1260 Bytes
Ähnlichkeit: Wiener

Stark verschlüsselter Virus, infiziert extrem schnell

405

Art: Überschreibender, nicht residenter .COM Zerstörer
Länge: 405 Bytes

Der 405 Virus ist leicht zu entdecken, da er die ersten 405 Bytes einer zu infizierenden Datei einfach überschreibt. Hierdurch werden die befallenen Programme in der Regel unbrauchbar und müssen ersetzt werden. Programmdateien kleiner als 405 Bytes haben nach der Infektion eine Länge von 405 Bytes.

4096

Alias: 100 Years, IDF, Stealth, Frodo, Century
Art: Residenter .COM und .EXE Infektor
Länge: 4096 Bytes

Ein durchaus übler Zeitgenosse. Der Virus versucht sich resident unter Umgehung des Betriebsystemes zu installieren und reserviert für seine Zwecke am oberen Ende des Hauptspeicher Platz für sich. Diese Verringerung des Hauptspeichers wird nicht im BIOS vermerkt. Im Single Step Verfahren klinkt sich der Virus auf unterster Ebene in das Betriebssystem ein und umgeht dabei selbst eventuell installierte 'Wachhund-Programme'. Der Virus verfügt über einige Techniken, die das Auffinden erschweren. Hierzu gehört auch die sehr eigenwillige Verlängerung der MCB-Chain. Merkt der Virus, daß auf ihn selbst zugegriffen wird, so verzieht er sich schleunigst, um seine Spuren zu verwischen. Er infiziert alles, was er bekommen kann und am allerschnellsten versucht er COMMAND.COM zu infizieren. Auch der 4096 infiziert Dateien sowohl beim Laden als auch beim Öffnen. Über die in der Hunderterstelle des Directoryeintrages um 100 erhöhte Jahreszahl 'merkt' sich der Virus, welche Datei infiziert ist. Diesen Taschenspielertrick nutzt er, um bei der Ausgabe des Directories die originale Dateilänge zurückgeben zu können. Darüber hinaus legt er auch noch CRC-Programme flach, da infizierte Dateien zwar physikalisch infiziert sind, der Virus aber auf DOS-Ebene beim Öffnen einer Datei immer nur die Originaldatei zurückgibt und Änderungen elegant vor anderen Programmen verbirgt. Zwischen dem 22.9. und dem 31.12. eines Jahres bleibt ein infizierter Rechner einfach stehen. Eigentlich sollte am Bildschirm über einen infizierten Bootsektor folgende Meldung erscheinen:

FRODO LIVES

Der 4096 manipuliert die FAT einer Festplatte, so daß in der Regel das Dateisystem gründlich durcheinander gebracht wird. Dies wird besonders beim CHKDSK Befehl deutlich. Darüber hinaus kann der Virus auch Datendateien befallen.

8 Tunes

Art: Residenter .COM und .EXE Infektor
Länge: 1971 Bytes

Nach etwa 30 Minuten ertönt ein Potpourri acht verschiedener deutscher Volkslieder, bei einigen Versionen vergehen zwischen der Infizierung und er ersten Melodie drei Monate.

903

Länge: 903 Bytes
Art: residenter .COM-Infektor

Der nach seiner Länge benannte 903-Virus installiert sich auf konventionelle Weise im unteren DOS-Speicher und infiziert alle Dateien im aktuellen Verzeichnis. Der Virus enthält Code, um die ersten 6 Sektoren auf der Festplatte zu zerstören. Derzeit wird analysiert, ob und wann dieser Code ausgeführt wird. Sollten mehrere speicherresidente Programme installiert sein, ist ein Systemabsturz zu erwarten, da der Virus für eigene Zwecke einen Bereich ab 384 KByte benutzt. Dieser Bereich könnte von anderen Programmen belegt sein.

Durch eine Interruptroutine prüft der 903, ob ALT-CTRL-DEL gedrückt wurde und bleibt auch nach dem Warmstart im Speicher aktiv.

AIDS Information Introductory Disk 2.0 (Trojanisches Pferd)

Am Montag, den 11. Dezember 1990, wurden in Großbritannien mehrere tausend Disketten per Post an etwa 7.000 Abonnenten der englischen Zeitung PC Business World und an eine unbekannte Anzahl weiterer Teilnehmer einer Aids-Konferenz des Oktobers 1988 versandt. Das Programm sollte Informationen über das persönliche Aids-Risiko ausgeben können, ließ sich jedoch nicht ohne Installationsprogramm anwenden. Das Installationsprogramm enthielt ein trojanisches Pferd.

Dieses Installationsprogramm erzeugt während der Installation einige neue Dateien und versteckte Verzeichnisse auf der Festplatte. Ihre Namen bestehen aus einer Kombination des ASCII-Zeichens 255, welches normalerweise als Leerzeichen dargestellt wird, und dem 'normalen' Leerzeichen, ASCII-Code 32. Beginnend beim Hauptverzeichnis der Festplatte erzeugt das Installationsprogramm fünf weitere Verzeichnisebenen mit Variationen dieser Zeichenkombinationen.

In diesen Unterverzeichnissen legt das Installationsprogramm verschiedene Dateien ab, die für den weiteren Verlauf einer Zählerschleife nötig sind. Die Datei AUTOEXEC.BAT wird im Hauptverzeichnis dahingehend geändert, daß nach Abarbeitens der AUTOEXEC.BAT-Datei die 'normale' AUTOEXEC.BAT unter dem Namen AUTO.BAT aufgerufen wird. Ein unscheinbarer Eintrag in dieser neuen AUTOEXEC.BAT ist eine Zeile mit folgendem (gekürztem) Inhalt:

REM PLEASE USE THE auto.bat FILE INSTEAD OF autoexec.bat

Normalerweise fallen die zwei Leerzeichen nach dem REM nicht auf. Das erste Leerzeichen ist aber wiederum das ASCII-Zeichen 255. Das Betriebssystem interpretiert diese vier Zeichen nun nicht als ein normales REM in Batchdateien, sondern als Programmaufruf. Tatsächlich hat doch das Installationsprogramm in einem dieser Unterverzeichnisse eine Datei namens REM .EXE installiert, welches nun aufgerufen wird und einen in einem anderen Unterverzeichnis stehenden Zähler hochzählt.

Nach etwa 90 Neustarts beginnt die Schadensroutine: die Festplatte wird verschlüsselt. Während dieser Zeit wird der Benutzer am Bildschirm gebeten, den Rechner doch bitte nicht abzustellen. Danach wird man aufgefordert, seine Softwarelizenz zu erneuern. Die Festplatte enthält nur eine 'sichtbare' Datei: CYBORG.DOC.

Die Verschlüsselung findet durch Ändern der Dateinamenserweiterung statt. Die Dateinamenserweiterungen aller Dateien werden mit einer internen Tabelle verglichen. Existiert ein Tabelleneintrag für eine Dateinamenserweiterung, wird die Dateinamenserweiterung durch den

zweiten Tabelleneintrag ersetzt, der für diesen Eintrag in der ersten Tabelle existiert. Die Buchstaben des Dateinamens selbst werden Zeichen für Zeichen verschlüsselt. Anschließend werden alle Verzeichnisse selbst als READ-ONLY und HIDDEN markiert, erscheinen also nicht mehr beim "dir". Die Directorynamen selbst, die beiden Systemdateien im Hauptverzeichnis und der COMMAND.COM werden nicht verschlüsselt.

Akuku

Alias: Hybrid
Art: Residenter .COM-Infektor
Länge: 1306 Byte
Ähnlichkeiten: Vienna

Ab 1992 jeden Freitag den 13. kopiert der Virus nach einem Aufruf eines infizierten Programms ein trojanisches Pferd in den Bootsektor des aktuellen Laufwerks, setzt er die Anzahl der Laufwerke auf 1 und die Speichergröße auf 256 KB. Folgende Nachricht erscheint:

Wirus v. 1.0 (c) Hybrid Soft Specjalne podziekowania dla Andrzeja Kadlofa i Marriuze
Deca za artykuly w Komtuterze 11/88.

Anschließend teilweise Formatierung dieses Laufwerks.

Alabama

Art: Residenter .EXE Infektor
Länge: 1560 Bytes

Der Virus installiert sich unter Umgehung des Betriebsystemes etwa 30KB unter der Oberkante DOS resident, reduziert aber nicht die maximale Größe von DOS, was zu unvorhersehbaren Problemen führen kann. Er hängt sich noch in den Tastaturinterrupt ein und 'überwacht' mit diversen IN und OUT Befehlen die Tastatur, während er auf die Resetkombination <Ctrl-Alt-Del> (<Strg-Alt-Lösch>) wartet. Erfolgt ein Systemreset durch <Ctrl-Alt-Del> (<Strg-Alt-Lösch>), verbleibt der Virus trotzdem im Speicher, indem er selbst den Rechner bootet.

Nachdem der Virus für etwa eine Stunde aktiv im System war, erscheint die folgende Nachricht in einem blinkenden Fenster:

> SOFTWARE COPIES PROHIBITED BY INTERNATIONAL LAW.....
> Box 1055 Tuscambia ALABAMA USA.

Der eigentliche Clou an diesem Virus aber ist seine Infektionsroutine. Er infiziert nicht das gerade aufgerufene Programm, es sei denn, dies ist das letzte nicht infizierte Programm in diesem Directory. Ab und zu tauscht der Virus aber, anstelle eine Datei zu infizieren, einfach deren FAT Einträge mit denen des gerade auszuführenden Programmes aus, ohne es aber umzubenennen. So startet man mit XCOPY vielleicht unbeabsichtigt den HDFORMAT. In der Regel erfolgt dieses Austauschen von FAT-Einträgen aber nur an jedem Freitag.

Amilia

Art: Speicherresidenter File-Virus
Länge: 1164 Byte
Ähnlichkeiten: Murphy

Infizierung von allen COM- und EXE- Files die ausgeführt oder geöffnet werden und größer als 1614 Byte sind.
COM-Files müssen kleiner als 64000 Byte sein. Wenn am Sonntag ein infiziertes EXE-Programm aufgerufen wird, erscheint der Text:

> Amilia I Virii - [Nuke]
> Released Dec91 Montreal
> (C) Nuke Development Software Inc

Anschließend wird das Programm beendet.

Amoeba

Alias: Khetapunk, 1392, Maltese
Art: speicherresidenter .COM- und .EXE-Infektor
Länge: 1392 Byte

Die Files werden nur infiziert, wenn Sie mindestens 512 Byte und maximal 60 KByte lang sind. Der Virus hat keine Schadensfunktionen, sondern simuliert ausschließlich Fehler, die zu Nebeneffekten führen können. Der Virus enthält den verschlüsselten Text:

SMA KHETAPUNK - NOUVEL Band A.M.O.E.B.A by Primesoft Inc"

Angelina (Bootsektorvirus)

Alias: Stoned-Angelina
Ähnlichkeiten: Parity

Der Angelina-Virus ist ein residenter Bootsektor-Infektor (BSI) mit der Fähigkeit, sich auf dem infizierten Medium zu verstecken (also ein Stealth-Virus). Wie jeder reine BSI gelangt er durch verseuchte Medien in das System, wenn von diesen gebootet wird. Während der Infektion kopiert der Virus den sauberen Original-Bootsektor in einen meist unbenutzten Bereich im Hauptverzeichnis des Mediums und lenkt alle Lesezugriffe vom Bootsektor auf diese Kopie um. Er installiert sich oben im konventionellen Speicherbereich und reduziert den für DOS verfügbaren Speicher um 1 KB.

Angelina besitzt eine kleine Installations-Routine, um sich im Speicher zu verankern. Diese Routine dekrementiert zuerst die Speichergröße um das benötigte Kilobyte und berechnet dann anhand dieses Wertes das Segment, in welches er sich nun hineinkopiert. Danach wird der Text "Greetings for ANGELINA !!!/by Garfield/Zielona Gora" im Datenbereich des Virus entschlüsselt, der Interrupt-Vektor 13h gesichert und auf den Int 13h-Handler des Virus umgebogen. Nun ist Angelina (genauer: der virulente Int 13h) installiert, und der Boot Strap Loader (Interrupt 19h) kann noch einmal ausgeführt werden.

Der Int 13h-Handler fängt ausschließlich Lesezugriffe auf den Bootsektor ab, alle anderen Sektoren können normal gelesen oder geschrieben werden. Der Bootsektor wird in den Speicher gelesen, der von der Anwendung bestimmt worden ist, und der Angelina-Virus testet, ob der Sektor bereits infiziert worden ist. Ist das der Fall, liest Angelina die Kopie des sauberen Bootsektors in den Puffer der Anwendung und kehrt zu dieser zurück. Falls der Bootsektor nicht infiziert ist, berechnet Angelina die Position, an die der eben gelesene Sektor geschrieben wird. Diese Position errechnet sich aus den Disk-Parametern und hängt daher von der Speicherkapazität des Mediums ab. Der Virus versucht dann, den saubereren Bootsektor dorthin zu schreiben. Auf schreibgeschützten Disketten wird der dort auftretende Schreibfehler verdeckt. Die Anwendung wird in ihrem Ablauf fortgesetzt, ohne das sie etwas von der Tätigkeit des Virus mitbekommt. Nach der erfolgreichen Sicherung des Bootsektors werden die Bereiche der Disk Parameter Table und des Partition Records in das Segment des Virus kopiert und zusammen mit dem Angelina-Code in den Bootsektor geschrieben. Damit ist der Bootsektor infiziert. Zuletzt werden die eingangs gesicherten Prozessor-Register auf ihre alten Werte zurückgesetzt. Die Anwendung, die den Bootsektor anforderte, bekommt lediglich den gesicherten, sauberen Sektor vom Int 13h zurück. Der Angelina wird als Stoned-Variante bezeichnet, obwohl er dem Parity wesentlich ähnlicher ist.

Anthrax

Länge: 1048 Bytes
Art: Residenter .EXE- und .COM-Infektor

Auf Festplatten kopiert Anthrax seinen Code ans Ende der Startpartition der ersten Festplatte. Falls dort Daten gespeichert waren, sind diese anschließend zerstört. Wird ein infiziertes Programm gestartet, setzt sich der Virus in den Master-Bootsektor und bleibt zu diesem Zeitpunkt nicht resident im Speicher. Erst nachdem von der Festplatte gestartet wurde, setzt sich Anthrax im Speicher fest und infiziert jedes gestartete Programm ohne zu prüfen, ob dies bereits infiziert ist. Das hat zur Folge, daß COMMAND.COM mit jedem Aufruf auf eine Größe wächst, die es dem Betriebssystem schließlich unmöglich macht, diese Datei zu laden und auszuführen. Es kann nicht mehr gebootet werden. Interessanterweise schaut ein anderer Virus (V2100) am oberen Ende der Festplatte nach, ob sich dort Code von Anthrax befindet und kopiert diesen wieder in den Master-Bootsektor. Soll hier eine manuelle Reparatur - beispielsweise mit den Norton Utilities - durchgeführt werden, muß dieser Bereich nach der Restauration des Master-Bootsektors überschrieben werden.

AntiExe (Bootsektorvirus)

Alias: D3, NewBug

Der AntiEXE-Virus, auch NewBug oder D3 genannt, ist ein reiner Bootsektorvirus und verkleinert den zur Verfügung stehenden Hauptspeicher im 640 KB-Bereich. Er sucht nach bestimmten Antiviren-Programmen.

Der Virus ist ein residenter Stealth-Bootsektorvirus. Wird ein Rechnersystem von einer infizierten Diskette gestartet, infiziert der Virus das System. Während der Infektion einer Festplatte kopiert er den sauberen Master-Bootsektor in einen unbenutzten Bereich (Head 0, Cylinder 0, Sector 13) und lenkt alle weiteren Lesezugriffe auf den Master-Bootsektor auf diese Kopie um.

Bei der Infektion einer Diskette wird eine Kopie des nicht infizierten Bootsektors im letzten Sektor des Rootdirectories abgelegt. Hier stehende Einträge gehen verloren, Datenverluste sind hierdurch vorprogrammiert, jedoch eher selten.

Die Installationsroutine des AntiEXE-Virus ermittelt die Einsprungadresse des Interrupts 13h. Anschließend vermindert der Virus den zur Verfügung stehenden unteren Hauptspeicherbereich (0-640 KB) um ein Kilobyte und korrigiert die Angabe des konventionellen Hauptspeichers. In den auf diese Art "belegten" Speicher kopiert sich der Virus hinein. Die ermittelte Adresse des Interruptvektors 13h wird auf den Interruptvektor D3h übertragen. Beide Interruptvektoren "zeigen" zu diesem Zeitpunkt noch auf denselben Programmcode, später verwendet der Virus zum Ausschalten residenter Virenwächter und -Blocker anstelle des Interrupts 13h einfach den Interrupt D3h.

Beim Systemstart von einer infizierten Diskette prüft der Virus nach residenter Installation, ob der Master-Bootsektor der ersten Festplatte bereits infiziert wurde. Ist dieser noch nicht infiziert, wird der originale Master-Bootsektor "zur späteren Verwendung" wegkopiert. Anschließend wird der aktuelle Master-Bootsektor modifiziert und der originale Bootsektor der Diskette für einen weiteren Systemstart nachgeladen.

Bei aktivem Virus wird nicht bei jedem Zugriff auf eine nicht infizierte Diskette der Bootsektor infiziert. Mit den üblichen Stealth-Eigenschaften versehen, gibt der Virus beim Zugriff auf den Bootsektor bei Disketten bzw. den Master-Bootsektor bei Festplatten immer den jeweils originalen Sektor zurück, d.h. der Virus leitet die Zugriffe einfach um.

Bei einem lesenden Zugriff auf einen beliebigen Sektor prüft der Virus bei gesetzten Bits 0 und 1 des Tick counters (Hochzählregister, daß die Anzahl

der "Ticks" seit Mitternacht mitführt), ob der gelesene Sektor den Startsektor eines bestimmten EXE-Programmes entspricht und modifiziert dann diesen Sektor. Das Programm ist danach nicht mehr lauffähig.

April

Alias: Suriv
Art: Residenter .COM- und .EXE-Infektor
Länge: ca. 900 Bytes und mehr

Der April Virus arbeitet auf zwei verschiedene Arten. Am ersten April wird der eher harmlose Teil aktiv und schickt das System in eine Schleife, aus der es nicht mehr zurückkehrt, nebenbei werden auch noch Dateien gelöscht. Der zweite Teil ist schon etwas effektvoller. Nach residenter Installation wird jedes neue Programm infiziert. Es werden sowohl '.COM' als auch '.EXE' Dateien betroffen und nach 53 Minuten hört das befallene Rechnersystem auf zu arbeiten. Es erscheint dann folgende Meldung am Bildschirm:

> 'APRIL 1ST HA HA HA - YOU HAVE A VIRUS'.

Manche Abarten geben beim Infizieren einer Datei noch einen kleinen Text von sich:

> 'YOU HAVE A VIRUS'

Dieser Virus weicht bei der Infektion von .EXE-Dateien von der standardmäßigen Infektionsmethode ab. Er klemmt sich zwischen den letzten Relokationseintrag der Relokationstabelle und dem Code. Dies erfordert ein Umrechnen aller Relokationseinträge in der Relokationstabelle, da er den Code des Programmes selbst verschoben hat.

Azusa (Bootsektorvirus)

Der Azusa-Virus versucht sich im Master-Bootsektor der Festplatte und im Bootsektor von Diskette einzunisten. Er prüft bei jedem Diskettenzugriff, ob die eingelegte Diskette nicht schon infiziert ist. Es genügt bei aktivem Virus also bereits ein DIR A: um die Diskette zu infizieren.

Barrotes

Art: Residenter .EXE- und .COM-Infektor
Länge: 1310 Bytes
Symptome: Zerstört Master-Bootsektor am 4. Januar!

Der scheinbar aus Spanien stammende Virus infiziert Programme und Programmodule (Overlays in separaten Dateien) bei deren Ausführung. Zusätzlich befällt er sofort COMMAND.COM im Hauptverzeichnis von Laufwerk C:. Nicht infiziert werden Programme, deren Overlays innerhalb der .EXE-Datei des Hauptprogrammes liegen. Der Virus prüft mit INT 21h/AH=EEh ob er schon resident im Speicher sitzt. Dies ist der Fall, wenn AH=FEh zurückgeliefert wird. Am 5. Januar überschreibt der Virus den Master-Bootsektor der ersten Festplatte im System mit Teilen der Interrupttabelle! Danach erscheinen Balken in ständig wechselnden Farben auf dem (Farb)Bildschirm und folgender Text wird ausgegeben:

Virus¯BARROTES¯pos¯OSoften

Der Virus enthält die Texte: "c:\command.com" und am Ende infizierter Dateien "I7SO".

Basic

Art: Nicht residenter .COM und .EXE Infektor
Länge: 5120, 5128, 5135 Bytes

Die erste Form des Basic Virus infiziert nach dem 6. Juli 1989. Der Virus wurde vermutlich in Turbo Basic mit Assemblerteilen geschrieben. In der Regel infiziert der Virus pro Aufruf eine Datei im aktuellen Unterverzeichnis, anschließend versucht er auf Laufwerk C: eine weitere Datei zu infizieren. Die Fehlermeldungen des Betriebsystemes werden vom Virus nicht abgefangen. Es besteht die Gefahr der Zerstörung von Datendateien bzw. der Zerstörung von Daten/Programmen durch 'Cross-Linking' von Dateien.

Ab dem 1. April 1992 werden aufgerufene Programme abgebrochen und folgende Meldung erscheint am Bildschirm:

Access denied

Die gestartete Programmdatei existiert aber trotzdem noch. Der Basic-I Virus kann durch folgende Textstrings im Viruscode identifiziert werden:

"BASRUN"
"BRUN"
"IBMBIO.COM"
"IBMDOS.COM"
"COMMAND.COM"
"Access denied"

Beim Basic-II Virus sind die Zerstörungsroutinen neu. Festplatten werden unbrauchbar gemacht, CMOS-Inhalte zerstört. Der Basic-II Virus kann durch folgende Textstrings identifiziert werden:

"BRUN"
"BASRUN"
"COBRUN"
"NET$OS"
"LOGIN"
"USERLIB"
"AV"
...
"IBMBIO.COM"
"IBMDOS.COM"
"COMMAND.COM"
"Access denied"

Diese Strings stehen nahe dem Dateiende. Bemerkenswert ist hierbei, daß

der Virus nun auch gezielt nach 'AV' sucht (unter diesem Namen wurde das Programm AntiVir früher ausgeliefert). Wie Sie sehen, empfiehlt es sich, das Programm AntiVir umzubenennen. In einer weiteren Abart wurde der String "AV" in "AVS" geändert, einer früheren Utility.

Bei Basic-III finden sich folgenden Sequenzen:

"KEYB*.COM"
"KEYB*.EXE"
"BASRUN"
"BRUN"
"COBRUN"
"NET$OS"
"LOGIN"
"USERLIB"
"AV"
...
"IBMBIO.COM"
"IBMDOS.COM"
"COMMAND.COM"
"Access denied"

Bestwish

Art: Residenter .COM Infektor
Länge: 970 Bytes

Infiziert neben .EXE- auch Windows- und OS/2-Dateien. Verlängert diese aber nur um 970 Bytes, ohne den Virus eigentlich bei einem Programmstart aktivieren zu können. Das Reparaturprogramm AntiVir kann diese Verlängerungen nur im GURU-Modus entdecken.

Black Jack

Alias: Cascade, 1701, 1704, Falling Letters, Falling Leaves, Herbstlaub
Art: Residenter .COM Infektor (eine Version auch .EXE)
Länge: meist 1701 Bytes oder 1704 Bytes

Black Jack (der Name stammt von seiner Länge in Anlehnung an das Kartenspiel '17 und 04') ist eine sogenannte Zeitbombe, da er erst ab einem bestimmten Zeitpunkt aktiv wird (lediglich die Infektion anderer Dateien findet auch vor diesem Auslösedatum statt). Als Auslösedatum von Black Jack kann man bestenfalls den sehr ungenauen Termin 'Herbst eines jeden Jahres' angeben, da es mittlerweile eine große Anzahl von Varianten und Abkömmlingen gibt, die ihrerseits andere Auslösedaten tragen können. Black Jack stört nach seiner Aktivierung die Bildschirmausgabe - Buchstaben fallen 'vom Bildschirm' (daher auch der Name 'Herbstvirus' oder 'Falling Letters/Falling Leaves'). Diese Effekte treten allerdings erst nach längerer Zeit auf, womit seitens des Virus bezweckt wird, daß der Anwender keinen Verdacht schöpft und die Störungen auf einen Systemfehler zurückführt. Eine weitere Besonderheit von Black Jack ist die Tatsache, daß eine Version keine originalen IBM-Systeme befällt (auch Computer, die über ein IBM-ROM-BIOS verfügen, werden verschont). Darüber hinaus befällt eine neue Art auch .EXE Dateien. Befallene Dateien werden um 1704 Bytes (+/- ein paar Bytes für die Varianten) vergrößert. Der Virus selbst ist intern verschlüsselt und decodiert sich zur Laufzeit erst einmal selbst. Wie auch der Israel Virus überwacht er das Laden von Programmen und läßt sich die Dateinamen zu infizierender Dateien 'frei Haus' liefern. Über die Unterfunktion 0FFh des INT 21h prüft der Virus nach, ob er selbst nicht schon aktiv im System vorhanden ist.

Brain Boot (Bootsektorvirus)

Alias: Pakistani
Ähnlichkeiten: Ashar

Diesen Virus gibt es sowohl in einer reinen Diskettenversion als auch in einer Version, die zusätzlich Festplatten infiziert. Je nach Größe belegt der Virus zwischen 3KB und 7KB Speicher. Meist tragen die infizierten Datenträger als Volume Label '(c) Brain'. Infizierte Disketten haben etwa 3KB an schlechten Sektoren, 6 Stück á 512 Bytes. Eine Version soll ab dem 5. Mai 1992 die FATs (FAT - File Allocation Tables) zerstören. Zumeist meldet sich der Virus mit der Meldung:

> Welcome to the Dungeon
> (c) 1986 Brain & Amjads (pvt) Ltd
> VIRUS_SHOE RECORD V9.0
> Dedicated to the dynamic memories
> of millions of virus who are no longer with us
> today - Thanks GOODNES!!

Darüber hinaus verlangsamt der Virus Diskettenzugriffe und verursacht sogenannte Time Outs, was manche Diskettenlaufwerke unbenutzbar macht. Er überwacht den INT 13h, über den alle Diskoperationen laufen, wodurch es auch Antivirus-Programmen sehr schwer gemacht wird, den ursprünglichen Bootsektor zu lesen, denn der Virus gibt den anscheinend originalen zurück. So nebenbei wird beim erstmaligen Lesen einer Diskette bei verseuchter Festplatte die Diskette auch infiziert.

Breasts (Bootsektorvirus)

Breasts ist ein sehr einfacher Bootsektorvirus, ist unverschlüsselt und besitzt keine Tarnkappeneigenschaften. Er belegt im Speicher 16384 Bytes und "verbiegt" den Interruptvektor 13h auf eine eigene Routine.

Breasts speichert den originalen Bootsektor von HD-Disketten auf Spur 79 ab. Sollten sich dort Daten befinden, so werden diese überschrieben (Datenverlust!). 2D-Disketten (z.B. 360K oder 720K) besitzen nur 40 Spuren. Da der Virus das Diskettenformat nicht prüft, geht somit auf diesen Disketten der originale Bootsektor verloren: Von einer infizierten 2D-Diskette kann nicht gebootet werden, da sich der Virus in einer Endlosschleife immer wieder selbst startet.

Der Master-Bootsektor von Festplatten wird in einem (normalerweise) unbenutzten Bereich "hinterlegt" und kann somit von AntiVir restauriert werden. Eine Schadensroutine ist in der uns vorliegenden Variante ebensowenig vorhanden wie eine Textausgabe auf den Bildschirm.

Burger Virus

Alias: 909090, CIA
Art: Überschreibender, nicht residenter '.COM' (einer auch '.EXE') Infektor
Länge: 560, 736, 1280 Bytes

Die Kennung dieses Virus ist zumeist 909090h am Anfang einer Datei. Wird eine infizierte Datei geladen, so versucht der Virus eine andere .COM Datei zu infizieren. Eine Version benennt, wenn es keine .COM Dateien mehr findet, einfach alle '.EXE' in '.COM' um und wiederholt das Spielchen. In der Regel werden dann aber die ersten 560 Bytes überschrieben.

Nachdem in unseren Programmen dieser Virus als Burger Virus klassifiziert wurde, haben wir auch eine Abmahnung von den Rechtsanwälten des im Copyright namentlich Genannten bekommen. Diese haben übrigens teilweise an seinen Büchern mitgewirkt. Die Antwort auf unsere Erwiderung auf die Abmahnung steht aber seit einem halben Jahr aus. Leider verfügen die heutigen Computer noch nicht über soviel Rechtsverständnis, daß dieser Virus gar kein Virus ist, sondern ein abgemahnter. Was ist denn ein abgemahnter Virus, na ja, eben ein Virus der nicht sein darf. Entgegen der Aussage der Rechtsanwälte, daß dies kein Virus sei, verschrottet dieser 'Un-Virus' trotzdem Dateien (und erfüllt damit ganz nebenbei einen Straftatbestand laut StGB). Die logische Schlußfolgerung der Rechtsanwälte kann hier also nur sein, daß sich der Computer strafbar macht, wenn er mit diesem Programm etwas tut, was er laut Aussage der Rechtsanwälte gar nicht machen dürfte.

CMOS-One (Bootsektorvirus)

Alias: Häufig als ExeBug (A) fehlerkannt

Der Virus belegt im Speicher 1024 Bytes und verbiegt den Interrupt 13h auf eine eigene Routine. Er verwendet eine Tarnkappenfunktion, um sich vor Erkennung zu schützen.

Seine Schadensroutine löscht den CMOS-Eintrag des ersten Diskettenlaufwerkes, das Laufwerk A: gilt dann als nicht installiert. Werden Daten auf Diskette oder Platte geschrieben, prüft der Virus, ob der erste Sektor mit dem Buchstaben 'M' beginnt. Trifft dies und noch eine weitere Prüfung zu, kopiert der Virus eine von zwei möglichen Routinen an den Anfang des Sektors und überschreibt dadurch dessen originalen Inhalt. Die so veränderten EXE-Dateien beginnen zumeist mit den Buchstaben 'MZ'!

Wurde bei dieser Manipulation eine EXE-Datei erwischt, so wird diese nun von DOS als COM-Datei behandelt, da die Signatur am Dateianfang nicht mehr 'MZ' lautet. Ist die betroffene Datei größer als 65280 Bytes, kann sie nicht mehr gestartet werden. Ist die Datei jedoch kleiner, wird die vom Virus eingetragene Schadensroutine ausgeführt.

Die eine Routine ist vergleichsweise harmlos, da durch einen Fehler darin das Programm sofort beendet wird. Die zweite mögliche Routine überschreibt große Teile der ersten Festplatte beginnend mit Cylinder 0. Sollte dieser Fall eintreten, muß die Festplatte neu formatiert werden. Nicht gesicherte Daten sind verloren!

CSFR 1000

Länge: 1000 Bytes
Art: residenter .COM-Infektor

Dieser Virus infiziert alle .COM-Dateien, die ausgeführt oder kopiert werden. Er installiert sich im oberen von DOS genutzten Speicherbereich. Dort wird der vom Virus belegte Speicher als nicht benutzt markiert. Dadurch können größere Programme oder Programme, die den gesamten verfügbaren Speicher anfordern, den Virus überschreiben. Eines dieser Programme ist AntiVir - das heißt, AntiVir löst nur dadurch, daß es geladen wird, sofort einen Systemabsturz aus.

Cascade

Alias: Black Jack, 1701, 1704, Falling Letters, Falling Leaves, Herbstlaub
Art: Residenter .COM Infektor (eine Version auch .EXE)
Länge: meist 1701 Bytes oder 1704 Bytes

Cascade oder Black Jack (der Name kommt von seiner Länge in Anlehnung an das Kartenspiel 17 und 4) ist eine sogenannte Zeitbombe, da er erst ab einem bestimmten Zeitpunkt aktiv wird (lediglich die Infektion anderer Dateien findet auch vor diesem Auslösedatum statt). Als Auslösedatum von Black Jack kann man bestenfalls den sehr ungenauen Termin 'Herbst eines jeden Jahres' angeben, da es mittlerweile eine große Anzahl von Varianten und Abkömmlingen gibt, die ihrerseits andere Auslösedaten tragen können. Black Jack stört nach seiner Aktivierung die Bildschirmausgabe - Buchstaben 'fallen vom Bildschirm' (daher auch der Name 'Herbstvirus' oder 'Falling Letters/Falling Leaves'). Diese Effekte treten allerdings erst nach längerer Zeit auf, womit seitens des Virus bezweckt wird, daß der Anwender keinen Verdacht schöpft und die Störungen auf einen Systemfehler zurückführt.

Eine weitere Besonderheit von Black Jack ist die Tatsache, daß eine Version keine originalen IBM-Systeme befällt (auch Computer, die über ein IBM ROM-BIOS verfügen, werden verschont). Darüber hinaus befällt eine neue Art auch .EXE Dateien. Befallene Dateien werden um 1704 Bytes (+/- ein paar Bytes für die Varianten) vergrößert.

Der Virus selbst ist intern verschlüsselt und decodiert sich zur Laufzeit erst einmal selbst. Wie auch der Israel Virus überwacht er das Laden von Programmen und läßt sich die Dateinamen zu infizierender Dateien 'frei Haus' liefern. Über die Unterfunktion 0FFh des INT 21h prüft der Virus nach, ob er selbst nicht schon aktiv im System vorhanden ist.

Casper

Art: nicht speicherresidenter .COM-Infektor
Länge: 1200 Bytes

Der Virus enthält in verschlüsselter Form den Text:

> "Hi! I'm Casper the Virus; And On April The 1'st
> I'm Gonna Fuck Up Your Hard REAL BAD!
> In Fact It Might Just Be Impossible To Recover!
> How's That Grab Ya! <Grin>".

Wird am 1. April ein infiziertes Programm aufgerufen, formatiert der Virus die Spur 0 der Diskette im Laufwerk A:.

Christmas

Alias: Syslock
Art: Nicht residenter .COM und .EXE Infektor.
Länge: 2764 Bytes
Ähnlichkeiten: Cookie, Macho

Der Virus kann, wie seine genannten Verwandten, durch eine Environmentvariable namens 'VIRUS' gesteuert werden. Steht im Environment 'VIRUS=OFF' so wird der Virus nicht aktiv. Zu der Melodie von 'Oh Tannenbaum' werden während der Adventszeit eines jeden Jahres Kerzen und 'Merry Christmas' auf dem Bildschirm dargestellt. Für jeden der Adventssonntage brennt eine Kerze. Es werden nur Dateien im aktuellen Unterverzeichnis befallen. Der Virus ist variabel verschlüsselt.

Cookie

Alias: Syslock
Art: Nicht residenter .COM und .EXE Infektor
Länge: 2232 Bytes
Ähnlichkeiten: Christmas, Macho

Dieser Virus wird seit 1988 am 1. April eines jeden Jahres aktiv. Es erscheint folgende Meldung am Bildschirm:

'I want a COOKIE !'

Diese Nachricht liegt in verschlüsselter Form im Virus vor. Anschließend wird meistens die Festplatte Low Level formatiert. Gibt man daraufhin 'COOKIE' ein, 'rülpst' der Virus:

'BURPS'

Der Virus kann durch eine Environmentvariable namens 'VIRUS' gesteuert werden. Steht im Environment 'VIRUS=OFF' so wird der Virus nicht aktiv. Diese Nachricht liegt in verschlüsselter Form im Virus vor. Anschließend wird meistens die Festplatte Low-Level formatiert. Eine Variante verhält sich vom 1. April an ganz still, d.h. es werden keine Infektionsversuche ausgeführt etc.

Crazy Eddie

Art: Residenter .COM und .EXE-Infektor
Länge: 2727 Bytes

Stürzt auf vielen Rechnersystemen ab, da stark von der Version des Betriebsystemes abhängig. Crazy Eddie infiziert COM- und EXE-Dateien bei deren Ausführung, aber auch beim DIR-Befehl. Er überschreibt an jedem Montag den 28. und am 28. Juni die Festplatte.

Datacrime

Alias: Columbus Day
Art: Nicht residenter .COM (einige Varianten auch .EXE) Infektor
Länge: 1168, 1514, 2280 Bytes

Der Virus hängt sich zumeist hinten an eine Datei an. Er infiziert in der Regel alle .COM Dateien, die in ihrem siebten Buchstaben kein 'D' haben. Wird der Virus aktiviert, erscheint zwischen dem 12. Oktober und dem 31. Dezember jeden Jahres folgende Meldung am Bildschirm:

> DATACRIME VIRUS
> RELEASED: 1 MARCH 1989

Befällt der Datacrime II eine .EXE-Datei, überschreibt er die im EXE-Header gespeicherten Werte für SS und SP. War die infizierte Datei kleiner als 60 KByte, so sollten keine Laufzeitprobleme auftreten größere könnten unkontrolliert abstürzen. AntiVir benennt derart geschädigte Dateien um. Sollten Sie zu den Unerschrockenen gehören und die Dateien wieder in *.EXE umbenennen um deren Verhalten auszuprobieren ... ?!?

Devils Dance

Art: .COM-Infektor
Länge: 941 Bytes

Nach etwa 5000 Tastenanschlägen überschreibt der Virus die erste FAT. Nach einem Warmstart mit der finalen Geierkralle <Ctrl-Alt-Del> (<Strg-Alt-Lösch>) erscheint folgende Meldung auf dem Bildschirm:

DID YOU EVER DANCE WITH THE DEVIL IN THE WEAK MOONLIGHT?
PRAY FOR YOUR DISKS!!
The Joker

Diamond

Alias: V1024
Art: speicherresidenter .COM- und .EXE-Infektor
Länge: 1024 Byte

Der Virus zeigt auf einem Farbbildschirm jeweils zur vollen Stunde einen Diamanten, zusammengesetzt aus vier kleineren Diamanten. Kurz darauf beginnen die vier kleinen Diamanten zu wandern. Treffen diese auf ein Zeichen, so wird dieses gelöscht. Nur Files mit einer Mindestlänge von 1024 Byte werden infiziert. Desweiteren setzt der Virus die Sekunden der Dateierstellungszeit auf den Wert von 60 Sekunden.

Disk Killer (Bootsektorvirus)

Alias: Ogre

Disk Killer infiziert den Bootsektor und lädt sich selbst mit etwa zwischen 3KB bis 8KB unter die Oberkante des Hauptspeichers. Er patcht den Bootsektor wie seine Artgenossen derart, daß seine Routinen zuerst ausgeführt werden. Diese Routine sitzt in drei Clustern auf dem Datenträger. Während einer Infektion versucht der Virus die drei belegten Cluster in der FAT als 'schlecht' zu markieren. Bei manchen Varianten klappt das Markieren dieser Sektoren als 'schlechte Sektoren' in der FAT nicht, so daß zum Überschreiben einiger Daten auch noch falsche schlechte, nämlich falsch markierte Sektoren dazukommen. Je nach Ausführung des Virus werden nach etwa 48 Stunden entweder die Festplatte formatiert oder die Datensektoren einer Festplatte abwechselnd mit den Werten 0AAAAh und 05555h verschlüsselt (für Techies: geXORt). Vorher gibt der Virus allerdings noch eine Meldung aus:

> Disk Killer -- Version 1.00 by COMPUTER OGRE 04/01/89

Der Virus kann im Bootsektor in der Regel durch die Kennung 03CCBh an Offset 03Eh erkannt werden.

Eddie

Alias: Dark Avenger
Art: Residenter .COM und .EXE Infektor
Länge: 1800 (+16) Bytes

Dark Avenger alias Eddie ist ein sehr ansteckender Virus. Der Virus infiziert auch beim reinen Lesen einer Datei, es reicht schon ein XCOPY oder COPY sowohl bei der Original- als auch bei der Zieldatei. Im Bootsektor führt der Virus einen Zähler, mit 16 initialisiert, im Countdown-Verfahren mit. Nach jedem 16. Bootvorgang überschreibt der Virus einen zufällig gewählten Sektor mit dem Bootsektor des jeweiligen Datenträgers.

Überschriebene Programme sollten unbedingt gelöscht und erneuert werden, da der ursprüngliche Inhalt des überschriebenen Sektors meist nicht wiederherstellbar ist. In der Regel infiziert der Virus auch beim Schließen einer Datei. Dies bedeutet, daß auf einem verseuchten Rechner auch frisch erstellte/kompilierte Programme den Virus enthalten. Frühere Versionen dieses Virus infizierten .COM Dateien mehrfach, während neuere Varianten den Countdown-Zähler bei 64 beginnen lassen. Der Virus überschreibt bei jeder Infektion den transienten Teil des COMMAND.COM. Um mehr Platz für Anwendungsprogramme zu schaffen, teilten die Entwickler von DOS den COMMAND.COM in zwei Teile auf - einen residenten Teil und einen transienten Teil. Der residente Teil ist immer vorhanden. Er enthält die Fehlerroutinen und den Nachladeteil für den transienten Teil. Der Bereich des transienten Teiles darf von Anwendungsprogrammen für eigene Zwecke in Anspruch genommen werden. Dark Avenger verrät sich auch dadurch, daß COMMAND.COM häufiger als sonst nachgeladen werden muß. Am Beginn des Virus kann man folgende Meldung entdecken: 'Eddie lives ... somewhere in time' Am Ende einer infizierten Datei läßt meist sich folgendes entdecken: 'This Program was written in the City of Sofia (C)1988-1989 Dark Avenger'

FSP Killer

Art: Residenter .COM und .EXE Infektor
Länge: 789 Bytes

Dieser Virus scheint gezielt im Codesegment des letzten geladenen INT 21h Vektors herumzuarbeiten. Dieser Virus wird zur Zeit analysiert. Erste Ergebnisse sind, daß der Virus 66.288 Bytes im residenten Zustand belegt. Über INT 21h, Unterfunktion 0A1D5h, prüft der Virus, ob er nicht schon resident im System ist. Er erwartet im AX Register den Hexwert 900Dh zurück. Ist der Virus resident, so modifiziert er einmal die Attribute zweier Dateien, indem das Hidden-Attribut dieser Dateien eingestellt wird.

Faust

Alias: Spyer
Art: Residenter .COM und .EXE-Infektor
Länge: 1181 Bytes

Belegt im Hauptspeicher etwa 1,7 KB. Faust alias Spyder infiziert jedes neu geladene Programm und läßt anschließend das Rechnersystem abstürzen.

Fiche

Alias: FEXE
Art: speicherresidenter .EXE-Infektor
Länge: 897 Bytes

Dateien werden beim Öffnen und Schließen infiziert. Eine Version des Virus überschreibt die ersten sechs Sektoren der ersten Festplatte mit dem Text:

"FEXE 1.0 vous a eu".

Fish

Art: Residenter .COM und .EXE-Infektor
Länge: 3584 Bytes
Ähnlichkeiten: Whale

Belegt zwischen 4 KB und 8 KB im Hauptspeicher und infiziert alle Dateien beim reinen Öffnen. CHKDSK /F bei aktivem Virus führt zu Lost Clusters.

Flash

Art: Residenter COM- und EXE-Infektor
Länge: 688 Bytes

Flash installiert sich resident im obersten Speicherbereich und markiert diesen Bereich als nicht vorhanden, damit er selbst nicht überschrieben wird. Wird ein Programm ausgeführt, hängt sich der Virus an diese Datei hintendran. Auf einem infizierten System wird der Virus ab dem Jahr 1990 aktiv. Es tritt alle paar Minuten ein Flackern des Bildschirms auf, das durch Manipulation der Register der Videokarte ausgelöst wird.

Flip

Alias: Omicron
Ähnlichkeiten: Tequila

Überschreibt die Laderoutine des Masterbootsektors (Partitionssektor) mit seiner eigenen Laderoutine. Der richtige Masterbootsektor wird an anderer Stelle auf der Festplatte gesichert.

Durch weitere Manipulationen verringert sich die Kapazität der 1. logischen Festplatte um 6 Sektoren (3 KByte). Im Speicher nistet sich Flip an der Oberkante DOS ein. Infiziert werden Programme und Overlaydateien. Die Erstellungszeit einer infizierten Datei weist im Sekundenfeld die Zahl 62 auf. Ist die erste zu ladende Datei nach dem Bootvorgang COMMAND.COM, wird diese derart verändert, daß bei dem Befehl DIR die scheinbar korrekte Dateigröße angezeigt wird. Abgesehen von der Infektion wird Flip zwischen 16.00 und 17.00 Uhr aktiv. Bei EGA- und VGA-Videoadaptern wird der Bildschirm zeitweilig horizontal gespiegelt (daher Flip).

Form (Bootsektorvirus)

Dieser Virus ist ein speicherresidenter Bootsektorinfektor und belegt im Hauptspeicher zwei Kilobyte. Er infiziert die Bootsektoren sowohl von Festplatte als auch von Disketten und belegt zwei Sektoren. Auf Disketten wird der originale Bootsektor verschoben und in einem als "bad" markierten Bereich abgelegt. Verändert werden die Interruptvektoren 13h auf Offset 0346h und 09h auf Offset 035dh.

Folgender Text ist im Bootsektor zu lesen, wird aber nicht am Bildschirm angezeigt:

The FORM-Virus sends greetings to everyone who's
reading this text. FORM doesn't destroy data!
Don't panic! Fuckings go to Corinne.

In der Regel sind am 18. eines Monats durch einen nur an diesem Tag installierten Tastatur-Handler "Klicks" durch den Lautsprecher zu hören. Hierdurch kann auch die Annahme von Tastenbetätigungen verzögert werden. Der Virus hat bis auf die Programmierfehler keine offensichtliche Schadensfunktion - lediglich auf der Festplatte werden die letzten beiden Sektoren überschrieben, was bei Unformat-Operationen zu "Verwirrungen" des Unformat-Programmes führen kann.

Gegenüber "normalen" Bootsektorviren infiziert der Form-Virus auf Festplatten nicht wie üblich den Master-Bootsektor, sondern den Bootsektor. Auch dieser Virus kann nur durch den Start von einem infizierten Datenträger in das System gelangen - auch der Start von einer infizierten Datendiskette gehört dazu.

Nach dem Systemstart von einer infizierten Diskette vermindert der Virus den zur Verfügung stehenden unteren Hauptspeicherbereich (0-640 KB) um zwei Kilobyte und korrigiert die Angabe des konventionellen Hauptspeichers. In den auf diese Art "belegten" Speicher kopiert sich der Virus hinein. Dies war allerdings nur die halbe Miete, denn der momentan geladene Sektor besteht nur aus 512 Bytes, der Virus selbst ist aber größer. Also wird der Rest "nachgeladen", die Einsprungsadressen (Segmentadresse und Offsetadresse) in diesen "belegten" Speicherbereich hinein auf den Stack gelegt und das Ganze mit einem Ret Far angesprungen. Der Virus wird nun in diesem oben "belegten" Speicherbereich ausgeführt und ist durch die Korrektur der konventionellen Hauptspeichergröße vor Überschreiben sicher.

Anschließend wird vom verseuchten Datenträger der saubere, wegkopierte Bootsektor an seine ursprüngliche Position im Hauptspeicher während eines Startvorganges eingelesen. Danach ermittelt der Virus die Partitionsparameter einer Festplatte: Der Master-Bootsektor des Laufwerkes

80h wird gelesen und die Partitionstabelle nach der ersten, als aktiv markierten Partition durchsucht. Der Virus speichert sich die physikalische Position des Bootsektors der als aktiv markierten Partition und liest diesen Bootsektor ein. Falls er nicht infiziert ist, wird er in den letzten Sektor der Festplatte geschrieben - dort stehende Daten werden überschrieben. Der zweite Sektor des Viruscodes wird im vorletzten Sektor gespeichert - auch hier werden bereits vorhandene Daten überschrieben.

Im ersten Sektor des residenten Virus werden die für den BPB (BIOS-Paramater Block) relevanten Bereiche innerhalb des Virus auf die Werte des zu infizierenden Bootsektors angepaßt. Dieser Sektor wird dann als neuer Bootsektor an die zuvor abgespeicherte physikalische Stelle des originalen Bootsektors geschrieben. Nach der Infektion einer Festplatte und Umbiegen des Interruptvektors 13h wird das aktuelle Tagesdatum auf "18" getestet. Stimmt das Datum überein, wird auch der Tastaturinterrupt verbogen. Der originale Bootsektor der Diskette oder Festplatte steht schon an der richtigen Stelle im Hauptspeicher und übergibt dem Virus diesen Programmcode zur Ausführung des weiteren Systemstarts die Kontrolle.

Der viruseigene Interrupt 13h-Handler beschäftigt sich fortan nur noch mit dem Infizieren von Disketten. Er wird nur bei Lesezugriffen auf Track 0 aktiv, wenn er beim Einlesen eines Bootsektors einen nicht infizierten Bootsektor feststellt. Ist die Diskette nicht infiziert, berechnet der Virus den Start des Datenbereiches einer zu infizierenden Diskette. In diesem Bereich sucht er den ersten unbenutzten Cluster und markiert zwei Sektoren in der FAT als defekt. In den ersten Sektor schreibt er den sauberen, originalen Bootsektor, in den zweiten Sektor den zweiten Teil seines eigenen Codes. Nach einer Anpassung der diskettenrelevanten Teile im Virus selbst wird der Bootsektor der Diskette infiziert.

Friday

Alias: South African, Miami, Munich
Art: Nicht residenter .COM Infektor
Länge: 416, 540 Bytes

In der Regel infiziert dieser Virus alle noch nicht infizierten Dateien im angemeldeten Verzeichnis, obwohl Abarten hiervon auch solche '.COM' Dateien infizieren, die sich im Pfad des Systems befinden. Mache Abarten infizieren aber auch nur zwei zusätzliche Dateien. Am Freitag den 13. löscht eine Abart ein aufgerufenes Programm, während eine andere Abart folgende Nachricht auf den Bildschirm bringt:

> We hope, we haven't inconvenienced you

Fu Manchu

Art: Residenter .COM und .EXE Infektor
Länge: 2080 Bytes
Ähnlichkeiten: Israel

Über die Unterfunktion 0E1h des INT 21h sieht der Virus nach, ob er schon resident im System vorhanden ist. Wenn nicht, fügt er sich bei .COM Dateien an den Anfang, bei .EXE Dateien an das Ende an. Die Checksumme im '.EXE-Header' einer infizierten Datei enthält den Hex-Wert 1988H (ähnlich dem Israel Virus, von dem Fu Manchu abstammt). Gegen Ende des eigentlichen Virusteiles wird meistens der folgende Text ausfindig gemacht:

sAXrEMHOr
COMMAND.COM

Der Virus infiziert alle ausführbaren Programme und installiert sich unter Umgehung des Betriebsystemes resident, indem die MCBs direkt manipuliert werden. Je nach Version erscheint nach einem Warmstart oder der 16. erfolgreichen Infektion folgende Meldung:

The world will hear from me again!!

Außerdem überwacht der Virus alle Tastatureingaben und reagiert auf die Namen bestimmter Politiker (Waldheim, Thatcher) mit eher rauhen Kommentaren.

Ghost

Alias: Ghost Ball, Ghostballs
Art: Nicht residenter .COM Infektor
Länge: 2351 Bytes

Infizierte Dateien haben eine '62' im Sekundenfeld des Directoryeintrages und jede 8. infizierte Datei wird zumeist überschrieben. Der Virus versucht, einen Ping Pong ähnlichen Bootsektorvirus zu installieren, der aber nicht reproduzieren kann. Nachdem ein Bootsektor infiziert wurde, erscheint ein 'hüpfender' Ball auf dem Bildschirm. Folgender Klartext kann im Virus gefunden werden:

GhostBalls, Product of Iceland
CopyRight 1989, 4418 and 5F19

HONNECKER Trojan (Trojanisches Pferd)

Der Honnecker-Trojan, auch DOSINFO Trojan genannt, ist im eigentlichen Sinne gar kein echter Virus, eher ein Trojanisches Pferd. Honnecker-Trojan verbreitet sich, in dem er Batchfiles dahingehend modifiziert, das er möglichst oft aufgerufen wird. An bestimmten Tagen, spielt HONECKER dann die Nationalhymne der DDR und bringt eine nette Grafik auf den Schirm. Ansonsten ist HONECKER nicht weiter schädlich.

1.5. - Tag der Arbeit
17.6 - Aufstand vom 17. Juni
13.8. - Tag des Mauerbaues
3.10. - Tag der dt. Einheit
7.10. - Tag der Republik (Nationalfeiertag der DDR)
9.11. - Grenzöffnung
25.12 - eigentlich kein soz. Feiertag

Das Wirtsprogramm DOSINFO.EXE kopiert sich bei jedem Aufruf in einige Verzeichnisse, in denen auch Batchdateien liegen. Diese Batchdateien erhalten außerdem als ersten Aufruf den Call von DOSINFO, um zu gewährleisten, daß das Programm auch gestartet wird.

Werden alle DOSINFO.EXE-Dateien gelöscht und alle Aufrufe auf diese Dateien aus den Batchdateien entfernt, ist der "Virus" ebenfalls entfernt.

Hafenstraße

Art: nicht speicherresidenter EXE-Infektor
Länge: 809 Bytes

Bei jedem Aufruf eines infizierten Programms erstellt der Virus im aktuellen Verzeichnis eine unsichtbare Datei. Diese Datei enthält den Text:

Hafenstraße

Hallöchen

Alias: Halloechen, Hello
Art: Residenter .COM und .EXE Infektor
Länge: 2011 Bytes

Der Virus installiert sich durch direkte Manipulation der MCB-Chains im Rechnersystem resident, ohne das Betriebssystem mit seinem INT 21h in Anspruch zu nehmen. Mit den MCBs (Memory Control Blocks) verwaltet das Betriebssystem einzelne Speicherbereiche aus dem normalerweise 640KB großen Pool. Ein Rechnersystem wird verlangsamt, wenn eine infizierte Datei aufgerufen wird. Es werden nur solche Dateien befallen, deren Monats- und Jahresangabe im Dateidatum sich vom aktuellen Systemdatum unterscheidet. Zwei Zeichenketten erlauben die Identifizierung des Virus innerhalb einer Datei:

> Hallöchen, here I'm
> Acrivate Level I

Icelandic

Alias: Disk Eating, One In Ten, Disk Crunching, Saratoga 2
Art: Residenter .EXE Infektor
Länge: 542, 656 Bytes
Ähnlichkeiten: MIX

In den letzten vier Bytes einer infizierten Datei steht die Hexkombination

44 18 5F 19

Hieran kann der Virus erkannt werden. Der Virus installiert sich unterhalb der Oberkante DOS und reduziert den gemeldeten freien Speicher um 2KB. Jedes zehnte gestartete Programm wird infiziert, sofern der INT 13h noch nicht von einem anderen Programm benutzt wird. In der Regel markiert der Virus einen noch freien Sektor als schlecht, wenn er eine Datei infiziert hat. Das führt zu einer ständigen Abnahme der freien Festplatten- bzw. Diskettenkapazität.

Inhalt

{ewc FF_BTN.DLL,FFHelpButton,"1-9"[Macro=JumpId (`'/: `1_9_glossary')][Font="Arial"/S8/B4]/W567/H300/B12TBLR/D36}
{ewc FF_BTN.DLL,FFHelpButton,"A"[Macro=JI(`'/:`a_glossary')][Font="Arial"/S8/B4]/W300/H300/B12TBLR/D36}{ewc FF_BTN.DLL,FFHelpButton,"B"[Macro=JI(`'/:`b_glossary')][Font="Arial"/S8/B4]/W300/H300/B12TBLR/D36}{ewc FF_BTN.DLL,FFHelpButton,"C"[Macro=JI(`'/:`c_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc FF_BTN.DLL,FFHelpButton,"D"[Macro=JI(`'/:`d_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc FF_BTN.DLL,FFHelpButton,"E"[Macro=JI(`'/:`e_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc FF_BTN.DLL,FFHelpButton,"F"[Macro=JI(`'/:`f_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc FF_BTN.DLL,FFHelpButton,"G"[Macro=JI(`'/:`g_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc FF_BTN.DLL,FFHelpButton,"H"[Macro=JI(`'/:`h_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc

FF_BTN.DLL,FFHelpButton,"I"[Macro=JI(`'/:`i_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"J"[Macro=JI(`'/:`j_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"K"[Macro=JI(`'/:`k_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"L"[Macro=JI(`'/:`l_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"M"[Macro=JI(`'/:`m_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"N"[Macro=JI(`'/:`n_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"O"[Macro=JI(`'/:`o_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"P"[Macro=JI(`'/:`p_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"Q"[Macro=JI(`'/:`q_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"R"[Macro=JI(`'/:`r_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc

FF_BTN.DLL,FFHelpButton,"S"[Macro=JI(`'/:`s_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"T"[Macro=JI(`'/:`t_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"U"[Macro=JI(`'/:`u_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"V"[Macro=JI(`'/:`v_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"W"[Macro=JI(`'/:`w_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"X"[Macro=JI(`'/:`x_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"Y"[Macro=JI(`'/:`y_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}{ewc
FF_BTN.DLL,FFHelpButton,"Z"[Macro=JI(`'/:`z_glossary')][Font="Arial"/S8/B4]/W300/H300/B15TBLR/D30}

Lesen Sie die folgenden Informationen bitte mit dem Wörtchen 'können' über allen Beschreibungen, denn jeder 08/15-Programmierer hat die Möglichkeit, Schadensroutinen oder Bildschirmausgaben zu verändern. Alle Viren werden ständig geändert und als 'neue' Viren von zweifelhaften Zeitgenossen wieder auf die Menschheit losgelassen.

1-9
1008
1253
1260

12-Ticks (Trojanisches Pferd)
405
4096
8 Tunes
903

A
AIDS Information Introductory Disk 2.0 (Trojanisches Pferd)
Akuku
Alabama
Amilia
Amoeba
Angelina (Bootsektorvirus)
Anthrax
AntiExe (Bootsektorvirus)
April
Azusa (Bootsektorvirus)

B
Barrotes
Basic
Bestwish
Black Jack
Brain Boot (Bootsektorvirus)
Breasts (Bootsektorvirus)
Burger

C
Cascade
Casper
Christmas
CMOS One (Bootsektorvirus)
Cookie
Crazy Eddie
CSFR 1000

D
Datacrime
dBase
Devils Dance
Diamond
Disk Killer (Bootsektorvirus)

E
Eddie

F
Faust
Fiche
Fish
Flash
Flip
Form (Bootsektorvirus)
Friday
FSP Killer
Fu Manchu

G
Ghost

H
Hafenstraße
Hallöchen
HONNECKER Trojan (Trojanisches Pferd)

I
Icelandic
Israel
Itavir

J
Jack Ripper (Bootsektorvirus)
Jerusalem
Joshi (Bootsektorvirus)
Junkie

K
Kennedy
Keypress
Kiev (Bootsektorvirus)

L
Lehigh
Liberty
Lisbon

M
Macho
Michelangelo (Bootsektorvirus)
MIX
Mummy
Murphy

Music Bug (Bootsektorvirus)
MVF

N
Natas
Neuroquila
Neuroquila.N8FALL.A
Neuroquila.N8FALL.B
Neuroquila.N8FALL.Companion
No Bock

O
Ohio (Bootsektorvirus)
Omega
One Half
Oropax

P
Parity (Bootsektorvirus)
Perfume
Ping Pong (Bootsektorvirus)
Plastique

Q

R
RedX

S
Sampo (Bootsektorvirus)
SillyWilly
Stimulation
Solano
Stoned (Bootsektorvirus)
Sunday Virus
Sylvia

T
Tai Pan
Taiwan
Tenbytes
Tequila
Traceback
Tremor
Tumen
Typo COM

U

V
V163
Vacsina
VGen
Victor
Vienna
Vriest

W
Whale
Wiener
WinWord.Concept
WitCode

X

Y
Yankee Doodle

Z
Zero Bug

Israel

Alias: Jerusalem, PLO, Freitag der 13.
Art: Residenter .COM und .EXE Infektor
Länge: 1803, 1808, 1813 Bytes

Dies ist zur Zeit einer der verbreitetsten Viren. Er vergrößert befallene Dateien um 1803 bzw. 1813 Bytes, bei Abarten dieses Virus sind auch andere Werte möglich. Verhält sich bis zu jedem Freitag den 13. relativ still. Je nach Abart des Virus werden an einem solchen "Glückstag" entweder Dateien gelöscht oder die Festplatte formatiert. In der Regel wird COMMAND.COM nicht infiziert aber etwa 30 Minuten nach der Erstinfizierung eines Systems verlangsamt der Virus das Rechnersystem.

Der Virus fängt den INT 21h, Unterfunktion 04Bh, ab, über den das Betriebssystem neue Programme startet, und bekommt so die zu infizierenden Dateinamen 'frei Haus' geliefert. '.COM' Dateien werden nur einmal infiziert, '.EXE' Dateien mehrfach. Durch diesen Programmfehler verrät sich der Virus eigentlich am schnellsten, da ganz normale Programme oft plötzlich nicht mehr geladen werden können. Dieser Fehler wurde in neueren Versionen behoben.

Über den Timer Interrupt hängt sich der Virus in die systeminterne Uhr ein. Viele Varianten des Israel erzeugen etwa eine halbe Stunde nach Infektion des Rechnersystems ein 'schwarzes Loch' auf der linken Seite des Bildschirmes. Unter anderem zum Zweck der Selbsterkennung definieren die Israelviren eine neue Funktion zum INT 21h (meist Funktion 0E0H). Über diese Funktion 0E0H schaut der Virus nach, ob er selbst schon resident installiert ist. Trotzdem muß AntiVir bei einigen Israelinfektionen "die Waffen strecken", da eine Reparatur eines infizierten Programmes mitunter wegen eines Programmfehlers im Virus nicht mehr möglich ist. Der Virus wechselt bei bestimmten Originalprogrammgrößen durch besagten Fehler von einer 'anhängenden' Arbeitsweise in eine 'überschreibende'. Dabei zerstört sich der Virus oft teilweise auch selbst. Dies bedeutet, daß AntiVir in diesem Fall zwar den Virus vielleicht noch entfernen, überschriebene Bereiche aber aus offensichtlichen Gründen nicht mehr restaurieren kann. Das infizierte Programm ist also bereits vor einer eventuellen Reparatur nicht mehr lauffähig. AntiVir gibt eine entsprechende Meldung aus und bietet an, die befallene Datei gleich zu löschen, um eine weitere Verbreitung des Virus (oder einen unkontrollierten Programmabsturz der infizierten Datei!) zu verhindern.
Falls man sich nicht dazu entschließen kann, diese Datei zu löschen oder anderweitig zu eliminieren, dann läßt man eventuell einen Virus auf seinem Rechnersystem. Viel schlimmer aber ist, daß dieser Virus durch seinen eigenen Fehler eventuell nicht mehr vollständig sein kann, und somit auch unkontrolliert in andere Bereiche hineinschreiben kann, wenn das Programm

aufgerufen wird. Also ist es besser, das Programm doch zu löschen und das Programm von den Originaldisketten neu zu installieren.

Der Israel Virus läßt sich unter anderem leicht daran erkennen, daß er in vielen Versionen den String 'MsDos' enthält und darüber hinaus die Prüfsumme in EXE-Dateien auf den Wert 1984h setzt.

Itavir

Art: Residenter .EXE Infektor
Länge: 3880 Bytes

Infiziert neben .EXE- auch Windows- und OS/2-Dateien. Itavir überschreibt nach 24 Stunden Systemaktivität den Bootsektor.
Dieser Virus verlängert manchmal aber nur Dateien, ohne den Virus bei einem Programmstart aktivieren zu können. Die Reparaturfunktion von AntiVir kann diese Verlängerungen nur im /GURU-Modus entdecken.

Jack Ripper (Bootsektorvirus)

Alias: Jack The Ripper

Jack Ripper ist ein einfacher Bootsektorvirus, vergleichbar dem Parity-Bootsektorvirus. Je nach Verschlüsselung wird der Virus im Speicher manchmal auch als Parity-Virus erkannt. Der direkte Zugriff auf Boot- bzw. Master-Bootsektoren unter laufendem Virus bringen die originalen, unverseuchten Sektoren zu Tage.

Der Virus belegt im Speicher 2048 Bytes und "verbiegt" den Interruptvektor 13h auf eine eigene Routine. Der zur Verfügung stehende Hauptspeicher wird um diese 2048 Bytes verkleinert angezeigt. Bei einem mit 640KB unterem Hauptspeicher ausgerüsteten Rechnersystem zeigt CHKDSK daher anstelle der 655360 Bytes nur 653312 Bytes Speicher an. Darüber hinaus kann Windows oft nicht im 32Bit-Modus gestartet werden.

Jack Ripper speichert den originalen Bootsektor von Disketten im letzten Sektor des Rootdirectories ab. Sind hier Verzeichniseinträge vorhanden, werden diese überschrieben und dadurch können Datenverluste auftreten. Der Masterbootsektor von Festplatten wird in einem (normalerweise) unbenutzten Bereich "hinterlegt" und läßt sich daher von AntiVir restaurieren.

Jack Ripper infiziert den Master-Bootsektor einer Festplatte, wenn von einer infizierten Diskette (auch Datendiskette) gebootet wurde. Nach dem Start von einer infizierten Festplatte werden nicht schreibgeschützte Diskette durch einen Lesezugriff infiziert, ein einfaches "DIR" reicht hierfür aus!

Der Name des Virus kommt aus verschlüsselten Textteilen im Viruskörper, die Meldung FUCK EM UP! läßt auf die Schadensroutinen des Virus schließen: Der Virus verändert beim Schreiben die zu schreibenden Daten langsam und unmerklich. Mit einer Möglichkeit von 1 zu 1024 Schreibzugriffen auf einen Datenträger wechselt der Virus in dem zu schreibenden Sektor einfach zwei aufeinanderfolgende Doppelbytes aus. Dies führt zu einer schleichenden und nur allmählichen Datenveränderung auf dem jeweiligen Datenträger. Daher sollte bei Auftreten dieses Virus immer der gesamte Datenbestand auf Konsistenz geprüft werden.

Jerusalem

Alias: Israel, PLO, Freitag der 13.
Art: Residenter .COM und .EXE Infektor
Länge: 1803, 1808, 1813 Bytes
Ähnlichkeiten: Anarkia, Mendoza, Frere Jacques

Sehr bekannter Virus. Vergrößert befallene Dateien um 1803 bzw. 1813 Bytes, bei Abarten dieses Virus sind auch andere Werte möglich. Verhält sich bis zum Freitag den 13. relativ still. Je nach Abart des Virus werden an einem solchen "Glückstag" entweder Dateien gelöscht oder die Festplatte formatiert. In der Regel wird COMMAND.COM nicht infiziert, aber etwa 30 Minuten nach der Erstinfektion eines Systems verlangsamt der Virus das Rechnersystem.

Der Virus fängt den INT 21h, Unterfunktion 04Bh, ab, über den das Betriebssystem neue Programme startet, und bekommt so die zu infizierenden Dateinamen 'frei Haus' geliefert. .COM Dateien werden nur einmal infiziert, .EXE Dateien mehrfach. Durch diesen Programmfehler verrät sich der Virus eigentlich am schnellsten, da ganz normale Programme oft plötzlich nicht mehr geladen werden können. Dieser Fehler wurde in neueren Versionen behoben.

Über den Timer Interrupt hängt sich der Virus in die systeminterne Uhr ein. Viele Varianten des Jerusalem erzeugen etwa eine halbe Stunde nach Infektion des Rechnersystemes ein 'schwarzes Loch' auf der linken Seite des Bildschirmes. Unter anderem zum Zweck der Selbsterkennung definieren die Jerusalem-Viren eine neue Funktion zum INT 21h (meist Funktion 0E0h). Über diese Funktion 0E0h guckt der Virus nach, ob er selbst schon resident installiert ist.

Den Jerusalem-Virus kann man selbst unter anderem leicht daran erkennen, daß er in vielen Versionen den String 'MsDos' enthält und darüber hinaus die Prüfsumme in EXE-Dateien auf den Wert 1984h setzt.

Joshi (Bootsektorvirus)

Dieser Virus installiert sich resident beim Start des Systems und benötigt neben dem Bootsektor auf Disketten und dem Master-Bootsektor auf der Festplatte etwa acht Sektoren. Joshi ist ein 'Stealth'-Bootsektorvirus und zerstört Daten auf 720 KB-Disketten. Am 5. Januar eines jeden Jahres aktiviert sich der Virus und bringt folgende Meldung auf den Bildschirm:

Type "Happy Birthday Joshi!"

Nach Eingabe des Geburtstagsglückwunsches startet der Rechner weiter durch. Wie auch andere Bootsektorviren kann der Joshi-Virus nur dann eine Festplatte infizieren, wenn von einer verseuchten Diskette gebootet wird. Von einer infizierten Festplatte aus formatiert sich der Virus, wenn er eine Diskette infizieren will, einfach einen neuen Track am Ende der Diskette, um dort den originalen Bootsektor und seinen eigenen Programmcode abzulegen. Der vom Virus erstellte neue Bootsektor an der Stelle des alten enthält alle Meldungen, so daß eine oberflächliche Analyse keinen Virusverdacht aufkommen läßt. Auf einer 360 KB-Diskette liegt der Virus auf Track 40 (wenn von 0 bis 39 gezählt wird) in den ersten fünf Sektoren, auf 1,2 MB-Disketten auf Track 80 (wenn von 0 bis 79 gezählt wird), wiederum in den ersten fünf Sektoren. Bei 720 KB-Disketten werden Daten auf Track 41 zerstört und die Diskette wird unbrauchbar gemacht.

Wird ein infiziertes Rechnersystem gestartet, prüft der Virus nach, ob er schon resident im System verankert ist, da er einen Warmstart überleben kann. Falls nicht, reduziert er den verfügbaren Hauptspeicher um 6 KB, wohin er sich selbst lädt. Nach einer Überprüfung, ob die von ihm verwendeten Interruptvektoren auch auf sich in diesen Bereich zeigen, lädt der Virus den originalen Bootsektor an die Speicherstelle, die dieser originale Bootsektor bei einem normalen Start eingenommen hätte. Diesem Sektor wird dann die Kontrolle übergeben.

Junkie

Art: Residenter .COM Infektor
Länge: 3880 Bytes

Der JUNKIE-Virus wurde Ende Mai 1994 durch verschiedene europäische Mailboxen verbreitet. In den meisten Fällen durch das File HV-PSPTC.ZIP. Laut der Beschreibung sollte das Programm ermöglichen, illegale Kopien eines Spieles auf Festplatte zu installieren, doch das Paket enthielt nur das Programm PSPATCH.COM, welches der JUNKIE-Virus war.

JUNKIE stammt aus Schweden und ist ein Multipartite-Virus, er infiziert also Master-Bootsektoren und COM-Dateien. Wird auf einem unverseuchten Rechner zum ersten mal ein infiziertes Programm gestartet, überschreibt der Virus den Master-Bootsektor der Festplatte (sonst macht er nichts). Beim nächsten Virusaufruf wird JUNKIE speicherresident und infiziert alle von da ab gestarteten COM-Programme.

Infizierte COM-Dateien werden um 1035 Bytes vergrößert. Da der Virus nur COM Dateien infizieren kann, zerstört er alle Programme, die zwar eine COM-Extension haben, aber keine echten COM-Dateien sind (mache EXE Programme). Der Virus ist zweifach verschlüsselt und enthält folgenden (ebenfalls verschlüsselten) Text:

> Dr White - Sweden 1994
> Junkie Virus - Written in Malmo...M01D

Den JUNKIE kann man auch daran erkennen, daß der zu Verfügung stehende Hauptspeicher verringert ist. Manche Programme bringen daher auch eine Fehlermeldung wie beispielsweise "Program too big to fit in memory".

Kennedy

Art: nicht speicherresidenter COM- Infektor
Länge: 333 Byte

Durch den Virus werden die FATs verändert. Dies resultiert in Lost Clusters und Cross Linked-Dateien. Im Virus ist folgender Text zu lesen:

\command.com
The Dead Kennedys

Keypress

Art: Residenter .COM und .EXE-Infektor
Länge: 1232, 1472 Bytes

Etwa eine halbe Stunde nach einer Infektion eines Rechnersystemes "verlängert" der Virus Tastatureingaben meist um das Vierfache. .COM-Dateien werden nur dann infiziert, wenn sie größer als 1232 Bytes sind.

Kiev (Bootsektorvirus)

Der Virus belegt im Speicher 1024 Bytes und verbiegt den Interrupt 13h auf eine eigene Routine. Eine Tarnkappenfunktion ist nicht vorhanden. Wird von einer infizierten Diskette gebootet, prüft der Virus, ob eine eventuell installierte Festplatte bereits infiziert ist und holt dies nach, falls noch nicht geschehen.

Die Interrupt 13h Routine wird bei jedem ersten Zugriff auf ein Diskettenlaufwerk aktiv, läuft der Diskettenmotor bereits, dann unterbleiben weitere Aktionen. Die eingelegte Diskette wird geprüft und infiziert, indem der Virus den originalen Bootsektor auf einen anderen Sektor speichert und seinen Code in den Bootsektor schreibt.

Wird von einer infizierten Festplatte gebootet, dekrementiert der Virus einen Zähler im Master-Bootsektor. Erreicht dieser Zähler den Wert 0, verschlüsselt er einen Teil der Festplatte (die ersten 17 Sektoren der Zylinder 0 bis 4 und von allen Schreib-Leseköpfen). Der Zähler wird vom Virus nicht initialisiert und hat in der Regel den Wert 0, so daß diese Schadensroutine nach dem 256. Bootvorgang ausgelöst wird. Der Virus benötigt einen 80286-Prozessor oder höher.

Lehigh

Art: Überschreibender, residenter COMMAND.COM Infektor
Länge: 1280 Bytes

Der Lehigh infiziert nur den COMMAND.COM, indem er dort nach dem Stackbereich sucht und sich dort einnistet. Hierdurch vermeidet er eine Verlängerung. Eine Abart dieses Virus hängt sich allerdings an einen infizierten COMMAND.COM an. Am Ende einer Datei befindet sich bei beiden Versionen die Kennung:

A9 65

Nach vier bzw. zehn Infektion zerstört der Virus in der Regel den Bootsektor und die FAT. Am Ende des Virus kann der Name von COMMAND.COM gefunden werden:

command.com

Liberty

Art: speicherresidenter COM- und EXE- Infektor
Länge: 2858 Byte

Der Virus Liberty weist keinerlei Schadensfunktionen auf. Er enthält den Text:

-MYSTIK -COPYRIGHT (c) 1989 - 2000, by SsAsMsUsEsL

Dateien, die kleiner als 1280 Byte sind, werden nicht infiziert.

Lisbon

Art: nicht speicherresidenter COM- Infektor
Länge: 648 Byte
Ähnlichkeiten: Vienna

Der Virus enthält den Text "@AIDS". Dieser Text steht in den letzten fünf Bytes einer infizierten Datei. Dateien, die kleiner als 10 Byte oder größer als 64 000 Byte sind, werden nicht infiziert. Der Virus überschreibt in einigen Dateien die ersten fünf Bytes mit "@AIDS" und zerstört diese auf diese Weise.

MIX

Art: Residenter .EXE Infektor
Länge: 632, 1618, 1636 Bytes
Ähnlichkeiten: Icelandic

Infizierte Dateien können durch folgenden String am Ende erkannt werden:

MIX1

Ist im Systemspeicher an der Stelle 0:33Ch der Wert 77h zu finden, ist der Virus vermutlicherweise resident. Die Ausgabe auf ein an einem seriellen oder parallelen Port angeschlossenen Gerät wird verstümmelt. Darüber hinaus geht die NUM Leuchte bei den neueren Tastaturen konstant an. Nach der 6. Infektion führt ein Systemstart zum Absturz des Rechnersystems. Es erscheint ein 'Ball' auf dem Bildschirm.

MVF

Alias: Mad Virus Factory
Art: Residenter .COM-Infektor
Länge: 1903 Bytes

Der verschlüsselte Virus infiziert beim Ausführen eines Programmes. Er befällt auch den COMMAND.COM - danach bleibt das Rechnersystem allerdings oft hängen. Spätere Versionen des MVF infizieren auch beim Öffnen von Dateien.

Macho

Alias: Syslock
Art: Nicht residenter .COM und .EXE Infektor
Länge: 3551 Bytes
Ähnlichkeiten: Cookie, Christmas

Dieser Virus wird über das Environment eines Rechnersystemes gesteuert, ist verschlüsselt und versucht, alle ausführbaren Programme zu infizieren. Infektionen unterbleiben jedoch, wenn im Environment des Rechners 'SYSLOCK=@' angegeben ist. Andernfalls infiziert er Programmdateien. Witzigerweise ersetzt er manchmal in infizierten Dateien alle Vorkommen von 'Microsoft' durch 'Machosoft'. Eine Abart erzeugt eine Datei IBMIONET.SYS.

Michelangelo (Bootsektorvirus)

Der Michelangelo-Virus nistet sich im Bootsektor einer Diskette oder dem Master-Bootsektor einer Festplatte ein. Er ersetzt den an diesen Stellen liegenden originalen (Start-)Programmcode mit seinem eigenen Code. Hierdurch erhält der Virus beim nächsten Systemstart vor dem Betriebssystem selbst die Kontrolle und wird in den Hauptspeicher geladen.

Beim Start eines Rechnersystems von einer Diskette wird zuerst der Bootsektor der Diskette eingelesen, damit das auf der Diskette liegende Betriebssystem nachgeladen werden kann. Anstelle des üblicherweise vorhandenen Startprogrammes wird nun aber bei einer infizierten Diskette der Michelangelo-Virus geladen, der sich im Hauptspeicher verankert.

Anschließend erlaubt der Virus dem Rechnersystem das Fortsetzen der Startsequenz, überwacht allerdings alle Zugriffe auf Diskette und Festplatte. Ist das Rechnersystem infiziert, prüft Michelangelo bei jeder neu eingelegten Diskette, ob diese schon infiziert ist und holt dies, falls nötig, nach.

Solange nicht von einer infizierten Diskette gebootet wird, können die Dateien von dieser Diskette problemlos mit dem Befehl COPY oder XCOPY auf einen nicht infizierten Datenträger übertragen werden. Die infizierte Diskette sollte anschließend sicherheitshalber formatiert werden (ab DOS 5.0 mit dem Parameter /U, da sonst die UNFORMAT-Infomationen den infizierten Bootsektor enthalten). Der Master-Bootsektor einer infizierten Festplatte kann nach einem Start von einer 'bekanntermaßen guten DOS-Diskette' ab DOS 5.0 mit FDISK /MBR (undokumentierter Parameter) wieder mit einer guten Kopie überschrieben werden, ohne die variablen Partitionsdaten selbst zu verändern. Anwendern früherer DOS-Versionen bleibt, sofern ein Low-Level Format vermieden werden soll, nur der Weg mit Hilfe der Norton-Utilities den originalen Master-Bootsektor von Cylinder 0, Head 0, Sector 7 auf Cylinder 0, Head 0, Sector 1 zurückzukopieren.

Infiziert der Michelangelo-Virus eine Diskette, dann kopiert er den originalen Bootsektor vom ersten Sektor der Diskette in den letzten Sektor des Rootdirectories. Hierdurch können Dateien verlorengehen oder, wenn neue Dateien hinzugefügt werden, die Diskette vollkommen unbrauchbar werden. Auf Festplatten können unter DOS-Versionen kleiner als 3.0 Datenverluste durch die Abspeicherung des Master-Bootsektors entstehen. Zumeist ist auch das Einrichten einer RAM-Disk nicht mehr möglich.

Am 6. März eines jeden Jahres führt der Michelangelo-Virus seine Schadensroutine aus. Er kopiert den Speicherinhalt ab der Adresse 5000:0000h über die Köpfe 0 bis 4, Cylinder Ø bis 255 und die Sektoren 1 bis acht einer Festplatte. In der Regel werden hierdurch die ersten 9 MB einer Festplatte unbrauchbar und die wichtigsten Teile, FAT und Rootdirectory,

ebenfalls irreparabel geschädigt. Die Festplatte ist nicht mehr startfähig und muß inklusive Partitionierung wieder frisch aufgebaut werden.

Der Michelangelo-Virus reduziert den verfügbaren Hauptspeicher um 2048 Bytes. Dies bedeutet, daß CHKDSK auf einem mit 640KB ausgestattetem Rechnersystem anstelle von 655.360 Bytes nur noch 653.312 Bytes frei meldet. Diese Speicherverminderung kann aber auch durch Varianten des Stoned-Virus, BIOS-Shadowing oder PS/2-Busmaus hervorgerufen werden.

Infizierte Disketten haben möglicherweise einen unvollständigen Bootsektor, dann sind nicht alle Meldungen vollständig lesbar. Auf Festplatten haben die Master-Bootsektoren verkleinerte freie Bereiche und ebenfalls unvollständige Meldungen.

Mummy

Alias: Platinum
Art: speicherresidenter .EXE-Infektor
Länge: 1399-1414 Byte
Ähnlichkeiten: Jerusalem

Dieser Virus installiert sich als TSR-Programm und markiert den benutzen Speicher als zu DOS gehörig. EXE-Dateien werden bei deren Ausführung und beim Öffnen infiziert: Es genügt also, eine Datei zu kopieren, um sie zu infizieren. Eine Version des Virus besitzt einen Infektionszähler, der nach jeder erfolgreichen Infektion erniedrigt wird. Erreicht der Zähler Null, dann überschreibt der Virus die ersten 100 Sektoren auf der Festplatte.

Murphy

Art: speicherresidenter COM- und EXE-Infektor
Länge: 1614 Bytes

Es werden die oben genannten Dateien, sofern Sie größer als 1614 Bytes sind, beim Öffnen infiziert. COM Files, die größer als 64 000 Byte sind, weisen eine Resistenz auf. Alle infizierten Dateien enthalten die Nachricht:

Amilia I Virii (NuKE),99i; By Rock Steady/NuKE

Wird sonntags ein EXE-File aufgerufen, erscheint der Text:

Amilia I Virii-(NuKE) Released dec.91 Montreal (c) NuKE Development Softwarw Inc.

Anschließend wird das Programm abgebrochen. Besonderheit: Der Virus überprüft ständig INT 13H, um nicht von Virenwächtern erkannt zu werden.

Music Bug (Bootsektorvirus)

Der Music Bug infiziert auf Disketten wie auf Festplatten die Bootsektoren. Wenn von einer infizierten Diskette gebootet wird, so spielt der Virus auf dem Lautsprecher eine zufällige Folge von Tönen. Werden auf einem infizierten AT HD-Disketten formatiert, verändert der Virus das Diskettenformat auf 360 KB und alle 1.2 MB Disketten werden nicht mehr erkannt.

Natas

Alias: Satan
Art: Resident, Stealth, Polymorph, Multipartite
Länge: 4744 Bytes, Speicher 6144 Bytes, 9 Sektoren HD/FD

Natas ist ein komplexer Virus, der neben .COM und .EXE-Programmen auch den Partitionssektor der Festplatte und Bootsektoren von Disketten infiziert. Er ist in allen Bereichen vollständig stealth und kann außer im Speicher nicht gefunden werden, solange der Virus aktiv ist. Der Virus ist polymorph und zudem noch destruktiv. Natas entpuppt sich als ein kleines Teufelchen (Tip: lesen Sie den Namen mal rückwärts...).

Wird ein infiziertes Programm gestartet, entschlüsselt sich der Virus und prüft, ob er bereits resident ist. Dazu benutzt Natas die selbstdefinierte Interruptfunktion INT 21h/30h, BX=F99Ah wobei als Resultat AX/BX = 0 erwartet wird. Ist der Virus noch nicht aktiv, wird der letzte MCB um 5664 Bytes gekürzt und die DOS-Speicherobergrenze um 6K verringert. Natas kopiert sich dann in diesen Bereich und ermittelt durch Tracen die ursprünglichen Interruptvektoren 13h, 15h, 21h und 40h.

Der Tracer weist einen besonderen Trick auf: soll festgestellt werden, ob das Trace-Flag der CPU gesetzt ist, täuscht der Virus ein nicht gesetztes Trace-Flag vor, um residente Virenblocker zu unterlaufen. Natas belegt dann die Interruptvektoren und infiziert den Partitionssektor der Festplatte.

Während der Installation wird an mehreren Stellen geprüft, ob TBCLEAN oder Debugger aktiv sind. Ist das der Fall, wird TBCLEAN bzw. der Debugger ausgeschaltet und Natas formatiert alle vorhandenen Festplatten. Die Methode zur Erkennung von TBCLEAN funktioniert allerdings nur mit älteren Versionen, die noch den Einzelschrittmodus der CPU benutzten.

Der Virus ist jetzt aktiv, und da der transiente Teil von COMMAND.COM überschrieben wurde, wird der Kommandointerpreter beim Nachladen direkt von Natas infiziert.

Der infizierte Partitions- und Bootsektor enthält nur einen kleinen Lader, der den Speicher um 6K reduziert und den restlichen Teil des Virus nachlädt. Diese 9 Sektoren befinden sich auf der Festplatte am Ende des Cylinders 0, Head 0 und auf Disketten innerhalb des letzten Tracks des Datenträgers. Es werden nur Bootsektoren infiziert, die als ersten Befehl einen SHORT oder NEAR JMP aufweisen. Der Virus kopiert sich dann an die Stelle, auf die dieser Sprungbefehl zeigt.

Im Sektor- wie im Dateibereich ist Natas vollständig stealth. Lesezugriffe auf den Partitions- oder Bootsektor werden auf die gespeicherten Originale

umgeleitet. Beim Lesen von infizierten Programmen wird im RAM die originale Dateilänge, das alte Dateidatum und der ursprüngliche Dateiinhalt vorgetäuscht. Virenscanner oder Prüfsummenprogramme, die den Virus nicht bereits im Speicher erkennen, können Natas nicht finden, wenn der Virus aktiv ist. Wird versucht, eine infizierte Datei zu verändern, wird diese vorher komplett gereinigt. CHKDSK gibt keine Fehlermeldungen aus wie es sonst bei Datei-Stealthviren üblich ist.

Der Virus deaktiviert seine Datei-Stealtheigenschaften, sobald er feststellt daß das aktive Programm ARJ, LHA oder PKZIP heißt. Ebenfalls wird kontrolliert, ob der Namen des aktiven Programmes BACK oder MODEM enthält. Diese Eigenschaft wird jedoch zufällig beim Aktivieren des Virus ausgewählt und ist nicht immer festzustellen.

Der Virus infiziert Programme beim Starten und Schließen, wobei während der Infektion INT 13h und INT 40h auf die ursprünglichen Werte gesetzt werden, um residente Virenprogramme zu umgehen. Diese Methode führt zu Datenverlust, wenn ein Cache mit Schreibverzögerung, wie beispielsweise SmartDrv, aktiv ist. Befindet sich das zu infizierende Programm auf einer Diskette, prüft der Virus mittels direkten Sektorzugriffes nach, ob die Diskette schreibgeschützt ist. Gleichzeitig wird INT 24h deaktiviert, um Fehlermeldungen zu unterdrücken. Natas prüft auf die EXE-Signaturen "MZ"/"ZM" und infiziert auch Programme die kein ".EXE" als Dateierweiterung haben. Weiterhin werden keine EXE-Programme infiziert, die interne Overlays aufweisen. Der Virus addiert 100 Jahre auf das Dateidatum einer infizierten Datei, was jedoch normalerweise nicht sichtbar ist. Der Virus benutzt während der Infektion die System File Table, um unter anderem den Zugriffsmodus von Dateien zu verändern.

Natas benutzt eine Polymorph-Engine, die eine große Anzahl möglicher Entschlüsselungsroutinen erzeugen kann. Eine Suche mit Scanstrings ist nicht möglich, der Virus erkennt sich selber anhand des Dateidatums. Neben dem Text "Natas" sind die Texte "BACK" und "MODEM" verschlüsselt im Code ablegt.

Der Autor dieses Virus (Pseudonym "Priest") ist ebenfalls verantwortlich für den Virus "SatanBug".

Natas-4988

Der Sourcecode von Natas wurde in dem Virenmagazin 40Hex veröffentlicht, was dazu geführt hat, daß einige Varianten dieses Virus erschienen. Die aus Belgien stammende Variante ist fast identisch mit dem Original. An einigen Stellen wurde der Code geringfügig verändert. Die Viruslänge beträgt jetzt 4988 Bytes und der Text im Virus wurde geändert auf:

Time has come to pay (c)1994 NEVER-1

Neuroquila

Alias: <HAVOC>, Neuro.Havoc, Wedding
Länge: EXE-Programme: 4644-4675 Bytes, Festplatte & Disketten: 9 Sektoren
Art: Residenter Retrovirus, Stealth, Polymorph, Multipartite

Neuroquila infiziert die Partition der Festplatte, Bootsektoren von 1.2 und 1.44MB Disketten und .EXE Programme. Er kann durch alle drei Infektionsarten aktiv werden. Wird von einer verseuchten Partition oder Diskette gebootet, kopiert sich der Virus in den freien Speicher ab 7C00:0. Interrupt 13h und 21h werden auf normale Art belegt und der Virus damit aktiv. Im Speicher ab 0:4E0 und 0:4F0 werden Sprungbefehle eingefügt, auf die die Interruptvektoren 21h bzw. 13h von Neuroquila umgeleitet werden. Der Virus versucht an dieser Stelle die Partition der Festplatte zu infizieren und lädt dann den ursprünglichen Partitions- oder Bootsektor nach, der erst entschlüsselt und dann gestartet wird.

Der Virus wartet, bis Interrupt 21h von DOS belegt wird und aktiviert dann eine weitere INT 21h-Routine, die das Starten von MSDOS.SYS abfängt. Ist zu diesem Zeitpunkt DOS- oder XMS-UMB vorhanden, belegt der Virus dort Speicher, andernfalls verlängert er den STACKS-Bereich. Der Virus belegt in beiden Fällen 5344 Bytes an Speicher. Nachdem der Viruscode in den neuen Speicherbereich kopiert wurde, und die beiden "Hooks" bei 0:4e0h und 0:4f0h korrigiert wurden, versucht der Virus den Einsprung ins DOS-Kernel in der HMA zu berechnen. Dort wird in den INT 21h-Einsprung ein Sprung auf den Viruscode eingefügt (Splicing). Interruptlister und Systeminfoprogramme zeigen keinerlei Veränderung von Int 21h an. Die endgültige INT 21h-Routine überprüft folgende DOS-Funktionen: 4Bh, 4Ch, 11h, 12h, 4Eh, 4Fh, 3Fh, 3Eh, 3Dh, 32h, 44h, 25h, 40h. Während des Bootvorganges wird die CONFIG.SYS kontrolliert und folgende Programme übersprungen: "VIRSTOP.EXE" (F-PROT) und DOSDATA.SYS (QEMM). Ebenfalls wird ein Programm namens "QC*" deaktiviert, wobei es sich um das Antiviren-Programm "QCDRV" von H+BEDV handelt.

Wird ein infiziertes Programm gestartet, installiert sich der Virus, falls nicht schon aktiv (Selbsttest: INT 13h, Funktion F2h: Carryflag), in den freien Speicher ab 7C00:0 und überschreibt dabei möglicherweise speicherresidente Programme, die dort bereits aktiv sind. Interrupt 13h und 21h werden im Einzelschrittmodus durchlaufen (Tracer) und die ursprünglichen Einsprungsadressen im DOS Kernel bzw. BIOS ermittelt. Wie beim Bootvorgang wird das DOS-Kernel gepatcht, die INT 13h und INT 21h-Routinen des Virus aktiviert, die Partition infiziert und schließlich das eigentlich aufgerufene Programm gestartet. Beim Tracen werden bereits aktive Antivirenprogramme so gepatcht, daß sie den Virus nicht mehr aufhalten können. Dieselbe Methode benutzt Neuroquila bei der Überprüfung

der Funktion 25h des Int 21h. Residente Antivirenprogramme die sich installieren wollen werden noch im gleichen Augenblick vom Virus im Speicher deaktiviert. Neuroquila modifiziert "TBDRIVER", "TBDISK" (TBAV), "VSAFE/TSAFE" (CPAV, MSAV und TNT) und "-D". (KAMI) Ist das Antivirenprogramm "NEMESIS" (1.10) aktiv, bleibt der Rechner stehen, oder eine Exception wird ausgelöst.

Da der Virus im freien Speicher aktiv ist, führt das Starten von größeren Programmen zum Absturz des Rechners. Da allerdings sofort die Partition infiziert wird, kann sich der Virus beim nächsten Neustart des Systems normal aktivieren und es treten keine Systemabstürze mehr auf.

Die Partition und der Bootsektor der Festplatte werden verschlüsselt und die Partition nach Cylinder 0, Head 0 und Sector 7 kopiert. Der infizierte Partitionssektor enthält nur einen kleinen Lader, der den restlichen Virus von Cylinder 0, Head 0 und Sector 8 nachlädt. Die Partitionsdaten werden gelöscht und der eigentliche Viruscode in die Sektoren 8 bis 16 geschrieben. Versucht man von einer saubere Startdiskette aus auf die Festplatte zuzugreifen, erhält man lediglich die Fehlermeldung "Ungültiges Laufwerk C:" bzw. "INVALID DRIVE C:".

Der Versuch, den Virus mit "FDISK /MBR" zu entfernen, führt von einer Bootdiskette aus zu Datenverlust, bei aktiven Virus hat er keine Auswirkungen. Neuroquila infiziert nur Partitionen vom Typ DOS-12BIT, DOS-16BIT und BIGDOS. Ist die Partition mit "TBUTIL" (TBAV) immunisiert, wird jedesmal vor dem Start dieser Partition diese so modifiziert, das der Virus nicht bemerkt wird. Windows im 32-Bit Zugriffsmodus erzeugt keine Fehlermeldung, wie es normalerweise bei Partitions- oder Bootsektorviren der Fall ist.

Disketten, die nicht schreibgeschützt sind, werden beim Zugriff auf den Bootsektor infiziert, beispielsweise schon bei "DIR A:". Der Virus formatiert 10 Sektoren ab Track 81 und kopiert dorthin den originalen Bootsektor und seinen Programmcode. Der verseuchte Bootsektor enthält wieder nur den kleinen Viruslader.

Ist der Virus einmal aktiv, kontrolliert er das komplette Betriebssystem. Lese- und Schreibzugriffe auf die verseuchte Partition, den verschlüsselten Bootsektor der Festplatte und auf Bootsektoren von Disketten werden erkannt und auf die gespeicherten Originale umgeleitet, die vom Virus im Speicher wieder entschlüsselt werden. Lese- und Schreibzugriff auf infizierte Programme werden ebenfalls erkannt und gefiltert. Verseuchte Programme haben die gleiche Dateilänge und den gleichen Datei-Inhalt wie vor der Infektion. "CHKDSK" meldet keine Dateibelegungsfehler wie bei anderen Datei-Stealthviren. Der Virus unterläuft mit seinen Stealthfunktionen alle Scanner und Prüfsummenprogramme und kann außerhalb des Speichers nur

gefunden werden, wenn der Virus im Speicher deaktiviert ist. Der Virus benutzt nicht das Dateidatum (+100 Jahre) oder die Dateiuhrzeit (Sekunden über 59) als Infektionsmarkierung. Obwohl der Virus Programme um einen variablen Wert verlängert, wird bei DIR die korrekte, ursprüngliche Dateilänge angezeigt. Enthält ein Verzeichnis viele infizierte Programme, wird die Anzeige von DIR spürbar verlangsamt, falls kein Disk-Cache aktiv ist.

Neuroquila umgeht den Selbsttest von "TBSCAN" und deaktiviert dessen Antistealth-Modus beim Dateizugriff. Der Virus manipuliert den Zugriff auf die Prüfsummendateien "SMARTCHK" oder "CHKLIST" von CPAV bzw. MSAV.

Der Virus infiziert EXE-Programme beim Starten. Programme werden um 4644 bis 4675 Bytes verlängert, obwohl die Veränderung bei aktiven Virus nicht mehr sichtbar ist. Das Dateidatum und die Uhrzeit bleiben erhalten, Schreibschutzattribute werden umgangen. Der Virus erzeugt keine Schreibschutzfehlermeldungen, falls versucht wird, Programme auf schreibgeschützten Disketten zu infizieren. Programme werden nur befallen, wenn sie größer als 10000 Bytes sind, keine internen Overlays haben (z.B. Windows-Programme) und ein Dateidatum ungleich dem aktuellen Monat und Jahr haben. Während des Infizierens belegt der Virus Speicher ab BE00:0 (Textspeicher). Der Virus überprüft ob sich die Anzeige im Textmodus befindet und infiziert keine Programme, wenn Grafik angezeigt wird (z.B. unter Windows). Wird versucht, verseuchte Programme zu debuggen oder zu verändern, werden diese vorher komplett von Neuroquila gereinigt.

In infizierten Programmen ist der Virus polymorph verschlüsselt. Die Neuroquila-Engine nimmt etwa 1300 Bytes der Viruslänge ein und erzeugt eine gewaltige Anzahl von Verschlüsselungen, wobei die Auswahl der Verschlüsselungsmethoden und Füllbytes extrem datums- und zeitabhängig ist. Die erzeugten Entschlüsselungsroutinen (Decryptors) sind ca. 64 Bytes lang und benutzen unter anderem XOR, ADD, ADC, SUB, SBB, NEG, NOT, ROL und ROR als Verschlüsselungstechnik. Bei der Neuroquila-Engine handelt es sich offenbar um keine der bekannten Engines wie etwa MtE, TPE oder SMEG. Der Viruscode in der Partition und in den Bootsektoren liegt unverschlüsselt vor und kann mit Scanstrings gefunden werden, falls der Virus nicht bereits aktiv im Speicher ist.

Beim Infizieren der Partition wird im Virus das aktuelle Systemdatum gespeichert. Nach drei Monaten werden Verzögerungsschleifen aktiviert, die das System bei jedem Zugriff immer mehr verlangsamen und beim Erreichen eines bestimmten Wertes eine Textausgabe aktivieren:

<HAVOC> by Neurobasher'93/Germany

-GRIPPED-BY-FEAR-UNTIL-DEATH-US-DO-PART-

Das gerade unterbrochene Programm wird nach Drücken einer Tasten fortgesetzt. Der aktive Virus verlangsamt das Starten von Programmen, die Anzeige von DIR und den Zugriff auf Disketten.

Neuroquila enthält 80286 Opcodes, hat anti-heuristische Strukturen und besitzt Ähnlichkeiten zu den Viren "Tremor" und "AlphaStrike", die laut internem Text ebenfalls vom gleichen Autor stammen.

Neuroquila.N8FALL.A

Alias: Neuroquila, Art & Strategy, Nightfall
Länge: EXE-Programme: 4554-4585 Bytes, Speicher: 4688 Bytes
Art: Residenter Retrovirus, Stealth, Polymorph

N8FALL basiert offensichtlich auf Neuroquila, obwohl die Fähigkeit, Festplatten und Disketten zu infizieren, fehlt. Die Polymorphic-Engine stimmt bis auf ein paar kleinere Änderungen mit der von Neuroquila überein. Statt dessen infiziert N8FALL jetzt auch beim Schließen von Programmen (Fast Infektor) und neben EXE-Programmen befällt N8FALL jetzt auch COM-Programme.

Wird ein infiziertes Programm gestartet, entschlüsselt sich der Virus zuerst im Speicher und überprüft anhand der Speicherstelle 0:4e0h, ob er bereits aktiv ist. Ist das nicht der Fall, belegt der Virus DOS- bzw. XMS-UMB, oder, falls dies nicht möglich ist, Speicher unterhalb der 640K-Grenze. Es werden 4688 Bytes belegt und als SYSTEM-Bereich markiert. Der Virus benutzt wie Neuroquila kein Einzelschritt-Modus (Tracer) zum Ermitteln des ursprünglichen INT 21h-Einsprungs, sondern sucht direkt innerhalb der HMA nach den typischen Einsprung und patcht ihn so, daß der Virus aufgerufen wird. Die Adresse von INT 2Fh wird auf die gleiche Methode ermittelt, der Interrupt selber aber nicht belegt. War die Suche nach dem DOS-Kernel erfolgreich, infiziert der Virus über die "COMSPEC="-Angabe den Kommandointerpreter, üblicherweise COMMAND.COM.

Bei COM-Programmen stellt der Virus die ersten drei Bytes des Programmes, bei EXE-Programmen die ursprüngliche MCB-Länge (ohne Virus) wieder her, bevor er zum eigentlichen Programm springt. (MCB-Stealth)

Wie <Neuroquila> überprüft der Virus eine Reihe von INT 21h-Funktionen: 4Bh, 4Ch, 11h, 12h, 4Eh, 4Fh, 42h, 3Fh, 3Eh, 3Dh, 32h, 44h, 25h, 40h, 48h, 4Ah, 45h und 46h. Anhand dieser Funktionen kann der Virus den Dateizugriff total kontrollieren. Programme werden beim Starten oder Schließen infiziert, wobei intensiver Gebrauch der SYSTEM FILE TABLE gemacht wird, um u.a. den Schreibzugriffmodus des geöffneten Programmes zu ändern. Der Virus infiziert nur Programme, die entweder "COM" als Dateierweiterung oder "MZ" bzw. "ZM" als Programmerkennung haben. Wird ein infiziertes COM-Programm mit aktivem Virus umbenannt, ist die Kopie sauber. Desweiteren werden nur Programme mit mindestens 4000 Bytes und bei COM mit maximal 60000 Bytes infiziert. Zusätzlich werden keine Programme befallen, die das aktuelle Systemdatum (Monat und Jahr) als Dateidatum haben oder "NE*.*" / "IB*.*" heißen. Programme mit internen Overlays wie etwa Windows-Programme werden ebenfalls nicht infiziert. Der Virus benutzt den Textspeicher während des Infizierens als Buffer. Ist der Rechner im Graphikmodus (z.B. unter Windows) werden keine Programme befallen.

N8FALL verlängert Programme um 4554-4585 Bytes, wobei sich der Virus auf die übliche Art ans Dateiende hängt.

Ist der Virus aktiv, kann keine Dateiverlängerung oder Veränderung festgestellt werden. Der Virus ist vollständig stealth, benutzt aber nicht wie viele andere Stealthviren das Dateidatum als Erkennung, sondern die Dateilänge. CHKDSK meldet keine Fehler, DIR ohne Festplattencache wird verlangsamt. N8FALL kann außer im Speicher nur in Programmen gefunden werden, wenn der Virus nicht aktiv im Speicher ist.

Wird ein Programm mit DEBUG aufgerufen, reinigt N8FALL die Datei vorher komplett. Ist die Schadensroutine aktiviert zeigt der Virus nach Verlassen des Programmes folgenden Text an:

Invisible and silent - circling overland :

\\\ N 8 F A L L ///

Rearranged by Neurobasher - Germany

-MY-WILL-TO-DESTROY-IS-YOUR-CHANCE-FOR-IMPROVEMENTS-!

Danach piepst der Rechner solange bis eine Taste gedrückt wird. Der Virus aktiviert sich 3 Monate nachdem COMMAND.COM infiziert wurde. In zufälligen Abständen führt der Virus dann ein Print Screen durch und verändert INT 33h (Maus-Unterstützung).

Während der Installation und des normalen Betriebes kontrolliert der Virus, ob Antiviren-TSRs installiert sind. Ist NEMESIS (1.10) resident wird der Virus nicht aktiv, TBDRIVER und VSAFE/TSAFE werden im Speicher gepatcht und unwirksam gemacht. Wird TBSCAN gestartet schaltet der Virus den Scanner in den Kompabilitäts-Modus und kann somit unbemerkt bleiben.

Werden Programme mit dem Namen "ME*.*", "MI*.*", "MF*.*", "CH*.*", "CO*.*", "SI*.*" oder "SY*.*" (z.B. MEM, SYSINFO, CHKDSK) gestartet, gibt der Virus den von ihm belegten Speicher scheinbar frei; diese Programme zeigen dann die ursprüngliche freie Speichermenge an.

Der Virus ist polymorph verschlüsselt, es können keine Scanstrings angegeben werden. Die Engine entspricht der von Neuroquila, sie ist nur geringfügig modifiziert. N8FALL ist zweistufig verschlüsselt, wobei nur die äußere Ebene polymorph ist. Die Engine erzeugt eine Vielzahl von möglichen Verschlüsselungsmethoden; wobei der Zufallsgenerator stark die Zeit- und Datumsfunktionen des System benutzt. Der Virus stammt offenbar vom selben Autor wie Tremor und Neuroquila.

Neuroquila.N8FALL.B

Alias: Neuroquila, Art & Strategy, Nightfall
Länge: EXE-Programme: 5801-5832 Bytes, Speicher: 6048 Bytes
Art: Residenter Retrovirus, Stealth, Polymorph

Dieser Virus ist wesentlich größer als die ursprüngliche Variante, enthält aber keine wesentlichen Veränderungen am eigentlichen Viruscode. Die Viruslänge liegt jetzt bei 5801 bis 5832 Bytes bei infizierten Programmen und 6048 Bytes Speicherbelegung. Wie N8FALL.A belegt der Virus den Speicher durch direkte MCB-Manipulation oder allokiert DOS- bzw. UMB-Speicher.

Der Sprungbefehl zu dem eigentlichen Viruscode wurde von 0:4E0h nach 0:5E0h verschoben, die Methode wie der Virus sich im DOS-Kernel aktiviert ist gleichgeblieben.

Die Verschlüsselung in der zweiten Stufe enthält jetzt Anti-Debugger Tricks, wurde aber sonst nicht weiter modifiziert. Auch die eigentliche polymorphe Verschlüsselung ist identisch mit der von N8FALL.A.

Neu ist, daß der Virus jetzt nur Programme mit mindestens 5000 Bytes infiziert, den Text "C:\NCDTREE\NAVINOC.DAT" und einen weiteren, völlig selbständigen Virus "N8FALL.Companion" enthält. Die Pfadangabe der Prüfsummendatei von Norton Antivirus liegt in verschlüsselter Form vor, wird allerdings seltsamerweise nicht weiter genutzt. Ebenfalls wurde die Wartezeit der Auslösefunktion von drei auf sechs Monate erhöht und der im Virus enthaltene, verschlüsselte Text geändert:

'Any means necessary for survival'

* N8FALL/2XS *

'By the perception of illusion we experience reality'

Art & Strategy by Neurobasher 1994 - Germany

'I don't think that the real violence has even started yet'

Aus dieser Angabe läßt sich schließen, daß diese Variante nach dem Virus Neuroquila programmiert wurde, von dem auch große Teile an Programmcode übernommen wurden.

N8FALL.B erzeugt keine Print Screens mehr und manipuliert auch nicht mehr Interrupt 33h (Maus), dafür wird nach sechs Monaten Aktivität der zweite, im Code enthaltene Virus "N8FALL.Companion" aktiviert. Wird ein verseuchtes Programm mit einem Debugger geladen, reinigt der Virus das Programm vor

dem Zugriff und zeigt nach Beenden des Debuggers den oben genannten Text an.

Neuroquila.N8FALL.Companion

Alias: Neuroquila-Companion
Länge: COM-Programme: 527 Bytes, Speicher: 672 Bytes
Art: Residenter Companion-Virus, Semi-Stealth, Fast Infector

Dieser Virus wird von Neuroquila.N8FALL.B, sechs Monate nachdem COMMAND.COM infiziert wurde, aktiviert.

N8FALL.Companion ist speicherresident und belegt 672 Bytes an konventionellem DOS-Speicher, indem der letzte MCB verkürzt und als Systembereich markiert wird. Als Selbsterkennung benutzt der Virus die Speicheradresse 0:5D2h, an der bei aktivem Virus die Zahl 5832h zu finden ist.

INT 21h wird auf die übliche Methode mittels direkter Manipulation der Interrupttabelle belegt. Normalerweise würden Antivirus-Wächterprogramme diesen Virus beim Installieren blockieren, aber da N8FALL.B bereits aktiv ist und seinerseits viele der bekannten Schutzprogramme deaktiviert hat, kann sich N8FALL.Companion meist ungestört aktivieren.

Der Virus infiziert Programme beim Aufruf der DOS-Funktionen 'Programme Starten' und 'Datei Erstellen', wobei sich der Virus allerdings auf Disketten nur beim Erstellen von Programmen verbreitet. N8FALL.Companion prüft, ob das gestartete oder erzeugte Programm EXE-Strukturen hat und erzeugt dann gleichnamige COM-Programme, die das READ-ONLY, HIDDEN und SYSTEM Dateiattribut sowie das Dateidatum auf den 1-1-94, 11:55:00 gesetzt haben. Diese erzeugten Dateien enthalten den Virus in unverschlüsselter Form und sind stets 527 Bytes lang. Zu Programmen mit den Dateinamen "F-" erzeugt der Virus keine Datei, damit wird verhindert das F-PROT den Virus bemerkt. Ist der Virus aktiv, versteckt er mittels Stealthroutinen bei der Anzeige von Verzeichnissen die erzeugten doppelten Dateien, verursacht allerdings keine Fehlermeldungen bei CHKDSK. Außer der Unart, Programme zu infizieren, hat dieser Virus keine weiteren Schadensfunktionen. Folgender Text kann in den 527 Bytes langen Dateien gefunden werden:

-A-VICTORY-THAT-WON`T-LAST-

No Bock

Art: Nicht residenter .COM Infektor
Länge: 440 Bytes

Der Virus enthält diese verschlüsselte Nachricht:

No Bock today Error, System halted!

Diesen Virus hat die Menschheit übrigens einer Göttinger Firma zu verdanken (der Name des Programmierers und dieses Unternehmens ist uns bekannt). Die Firma gibt vor, sie habe damit eines ihrer Programme gegen 'Änderungen des Copyrights' schützen wollen. Das Programm wird mittlerweile ohne das kleine 'Geschenk' ausgeliefert.

Ohio (Bootsektorvirus)

Alias: Den Zuk, Venzuelan
Ähnlichkeiten: Brain Boot

So wie der Code aussieht, hat der Autor einige Teile vom Brain Virus entnommen und als Baukasten für einen eigenen Virus verwendet, was offenbar die klassische Art ist, einen neuen Virus zu schreiben. Wie der Brain Virus ist dieser Virus etwa zwischen 3KB und 7KB lang und ist 'Brain aware'. Dies bedeutet, daß der Virus, wenn er auf einen Brain Virus im Bootsektor stößt, den bereits vom Brain Virus abgespeicherten Bootsektor holt und diesen für sich abspeichert. Eine vom Ohio oder Denzuk infizierte Diskette kann nicht mehr vom Brain Virus befallen werden.

Der Virus läßt sich durch folgenden Textstring im Viruscode identifizieren:

Y.C.1.E.R.P

Die Punkte bei der ersten Meldung sind die Zeichen mit dem Hexcode 0F9h. Der Virus schreibt sich selbst in den Bootsektor, nachdem er den Originalbootsektor auf Spur 40 und Kopf 0 einer Diskette abgespeichert hat. Die Diskette wird nötigenfalls in einem nicht standardgemäßen Format an dieser Stelle formatiert. Bei manchen Varianten dieses Virus erscheint bei jedem Start eines Rechners der Schriftzug DEN ZUK am Bildschirm. Manchmal wird, ausgelöst durch einen internen Zähler, einfach die Diskette in Laufwerk 'A:' formatiert.

Omega

Art: .COM-Infektor
Länge: 440 Bytes

Am Freitag den 13. wird das griechische Omega ausgegeben und die Festplatte zerstört.

One Half

Alias: FreeLove, Slovak Bomber
Art: Resident, Stealth, Polymorph, Multipartite
Länge: 3544, 3577 Bytes, Speicher 4096 Bytes, 8 Sektoren HD/FD

One Half infiziert die Partition der Festplatte und Programme vom Typ .COM und .EXE. Beim Start eines infizierten Programmes entschlüsselt sich der Virus im Speicher und überprüft mit der selbstdefinierten INT 21h-Funktion AX=4B53h (Resultat: AX=454Bh), ob er bereits im Speicher aktiviert wurde. Ist das nicht der Fall, durchläuft der Virus INT 13h im Einzelschrittmodus, um mit der ursprünglichen Adresse aktive Antivirenprogramme unterlaufen zu können. Während des Tracens wird der Partitionssektor der Festplatte gelesen und geprüft, ob er bereits infiziert ist. (Offset 25h=00d3h, Offset 180h=072eh). Ist die Partition noch nicht infiziert, ermittelt der Virus die maximale Anzahl der Sektoren und Zylinder der Festplatte und sucht die aktive Partition der Festplatte, wobei nur Partitionen vom Typ DOS 12 Bit, DOS 16 BIT und DOS 32 BIT infiziert werden. Ein Schlüssel wird ermittelt und zusammen mit den Daten über die Festplatte verschlüsselt in den Partitionsektor geschrieben. Der Rest des Virus (7 Sektoren) befindet sich innerhalb der ersten Zylinders der Festplatte. Der Virus restauriert jetzt die Stellen der gestarteten Datei, die mit seiner Entschlüsselungsroutine und dem Sprung zum Viruscode überschrieben worden sind. Ist das infizierte Programm vom Typ EXE und wurden bei der Infektion Relokationseinträge überschrieben, lädt der Virus die ursprünglichen Einträge nach und korrigiert das Programm im Speicher. Der Virus wird erst resident, wenn von einer verseuchten Partition gestartet wird.

Wird von einer infizierten Festplatte gestartet, verringert der Virus die Speicherobergrenze um 4K, belegt Interrupt 13h und 1Ch und lädt die restlichen 7 Sektoren nach. One Half verschlüsselt bei jedem Start des Rechners einen weiteren Sektor und arbeitet sich vom Ende der Festplatte bis zur Hälfte der vorhandenen Zylinder vor. Erreicht er diesen Sektor, gibt One Half bei jedem Neustart eine Meldung aus:

Dis is one half. Press any key to continue

Der Schüssel ist variabel und ist innerhalb des infizierten Partitionssektors gespeichert (Offset 29h). Ist der Virus aktiv, werden verschlüsselte Sektoren vor einem Zugriff anderer Programme entschlüsselt. Wird der Virus allerdings entfernt, tritt höchstwahrscheinlich Datenverlust auf! Man kann nicht mehr feststellen, welchen Wert der Virus zur Verschlüsselung benutzt hat und wie weit die Verschlüsselung bereits fortgeschritten war.

Wie bei Multipartite-Viren üblich, wartet One Half solange, bis die INT 1Ch-Routine bemerkt, daß DOS geladen wird und wird dann erst vollständig aktiv,

in dem noch zusätzlich Interrupt 21h belegt wird.

Ist der Virus aktiv, kann er nicht mehr in der Partition und innerhalb des ersten Zylinders der Festplatte gefunden werden. Beim Lesen der Partition wird der Zugriff auf den gespeicherten originalen Sektor umgeleitet, beim Lesen des Festplattenbereiches, den der Virus nutzt, wird der Lesepuffer mit Nullen aufgefüllt.

Der Virus infiziert .COM und .EXE Programme beim Programmstart, Öffnen, Umbenennen, Schließen und Erstellen, allerdings nur, wenn sich das betreffende Programm auf einer Diskette oder sonstigen entfernbaren Medien befindet - in der Regel werden also keine Programme auf einer Festplatte infiziert. Der Virus prüft auf die Signatur "MZ"/"ZM", infiziert also auch Programme, die nicht die Dateierweiterung "EXE" haben. One Half umgeht alle Schreibschutzattribute von DOS und erzeugt keinerlei Fehlermeldung, falls die Diskette, auf der sich das zu infizierende Programm befindet, schreibgeschützt ist.

One Half verlängert Programme um 3544 bzw. 3577 Bytes (je nach Variante), wobei die Dateiverlängerung bei DIR nicht sichtbar ist und die infizierten Programme anhand des Dateidatums erkannt werden. CHKDSK gibt keine Fehlermeldungen aus. Der Virus umgeht Warnungen von Antivirenprogrammen, indem er SCAN, CLEAN, FINDVIRU, GUARD, NOD, VSAFE und MSAV nicht infiziert.

Der Virus hängt sich ans Programmende an, modifiziert allerdings noch ca. 1K vor dem Viruscode das ursprüngliche Programm. Hier befinden sich die Codefragmente der Entschlüsselungsroutine in zufälliger Anordnung und Abstand, was die Erkennung des Virus ohne speziellen Algorithmus unmöglich macht. Das Einstreuen der Codefragmente erinnert an den Virus COMMANDER BOMBER, erreicht allerdings nicht dessen Komplexität.

Die Verschlüsselungsroutine wird polymorph generiert, besteht im Grunde aber nur aus XOR [Offset],Faktor1 / ADD Faktor1,Faktor2 wobei Faktor1 und Faktor2 zufällig gewählt werden.

Der Virus enthält auch den Text "Did you leave the room ?", wobei dieser Text in Programmen wegen der Verschlüsselung nicht sichtbar ist.

Der Virus sollte nicht einfach mit "FDISK /MBR" oder sonstigen Hilfsmitteln aus der Partition entfernt werden, weil dann die vom Virus verschlüsselten Bereiche unwiderruflich verloren gehen! Viele Antivirenprogramme entfernen den Virus nur aus Programmen und aus der Partition, lassen aber den verschlüsselten Bereich der Festplatte unangetastet! Die sicherste Methode ist, ein Backup aller Daten auf der Festplatte zu machen, wenn der Virus noch aktiv ist, die Platte dann mit FDISK /MBR und FORMAT zu behandeln

und schließlich alle Daten zurückzulesen.

Oropax

Alias: Music, Musician
Art: Direkter, residenter .COM Infektor
Länge: 2756 bis 2806 Bytes

Etwa fünf Minuten nach Infektion einer Datei spielt dieser Virus bis zu sechs verschiedene Musikstücke im Sieben-Minuten-Takt. Eine andere Abart spielt bis zu drei verschiedene Musikstücke. Das Lied 'An der schönen blauen Donau' klingt nicht schlecht. Infizierte Dateien haben eine durch 51 teilbare Länge. Eine genaue Analyse wird durch selbstmodifizierenden Code erschwert. Dieser Virus infiziert Dateien nicht nur bei Schreibzugriffen, sondern auch beim Löschen.

Parity (Bootsektorvirus)

Alias: Parity Check

Der Parity-Virus ist ein reiner Bootsektorvirus und verkleinert den zur Verfügung stehenden Hauptspeicher im 640 KB-Bereich um 1 KB. Ohne geladenen Tastaturtreiber läßt der Virus das Rechnersystem zur vollen Stunden abstürzen. Am Bildschirm wird im 40*25-Modus die Meldung "PARITY CHECK", jedoch ohne weitere Adressangaben über die Stelle, an der dieser Paritätsfehler aufgetreten sein soll, ausgegeben. Beim Laufenlassen eines Debuggers können Systemabstürze erfolgen, die Warmbootsequenz (Strg)+(Alt)+(Entf) führt nur scheinbar einen Warmstart aus.

Der Virus ist ein residenter Stealth-Bootsektorvirus. Wird ein Rechnersystem von einer infizierten Diskette gestartet, infiziert der Virus das System. Während der Infektion einer Festplatte kopiert er den sauberen Master-Bootsektor in einen unbenutzten Bereich (Head 0, Cylinder 0, Sector 14) und lenkt alle weiteren Lesezugriffe auf den Master-Bootsektor auf diese Kopie um.

Bei der Infektion einer Diskette wird eine Kopie des nicht infizierten Bootsektors im letzten Sektor des Rootdirectories abgelegt. Hier stehende Einträge gehen verloren, Datenverluste sind vorprogrammiert, jedoch eher selten. Die erstellten Kopien des Bootsektors befinden sich bei 360 KB und 720 KB-Disketten auf Head 1, Track 0, Sector 3, bei 1.2 MB-Disketten auf Head 1, Track 0, Sector 5 und bei 1.44 MB-Disketten auf Head 1, Track 0, Sector 14.

Die Installationsroutine des Parity-Virus ermittelt die Einsprungadresse der Interrupts 09h und 13h und diese werden wie auch der Stundenwert der aktuellen Systemzeit gespeichert. Anschließend vermindert der Virus den zur Verfügung stehenden unteren Hauptspeicherbereich (0-640 KB) und korrigiert die Angabe des konventionellen Hauptspeichers. In den auf diese Art "belegten" Speicher kopiert sich der Virus hinein. Die Interruptvektoren 09h und 13h in der Interruptvektortabelle werden mit den neuen Adressen der beiden Handler versehen, die sich jetzt unterhalb der Oberkante DOS befinden. Nun wird als Abschluß der Installationsroutine der Interrupt 19h aufgerufen und damit ein neuerlicher Systemstart ausgeführt. Im Verlaufe dieses Neustarts soll wiederum (vom BIOS ausgelöst) über den Interrupt 13h entweder von Disketten der Bootsektor von Head 1, Track 0, Sector 0 oder von Festplatten der Master-Bootsektor von Head 0, Cylinder 0, Sector 1 gelesen werden. In diesem Interrupt "hängt" aber der Virus drin und leitet diesen Lesezugriff auf den jeweils uninfizierten Sektor um. Nachdem dem Programmcode des originalen Bootsektors bzw. Master-Bootsektors die Programmkontrolle übergeben wurde, startet das Rechnersystem mit etwas weniger Speicher als normal durch. Da das Betriebssystem nun von der

Existenz eines zusätzlichen Speichers der Größe von einem Kilobyte keine Ahnung hat, ist der Virus vor einem Überschreiben relativ sicher.

Die Behandlungsroutine des Virus für den Interrupt 13h des Virus kehrt bei Aufruf mit dem Funktionscode AH=AAh sofort zum Aufrufer zurück. Ein Lesezugriff auf einen Bootsektor und Master-Bootsektor wird erst einmal ausgeführt. Im gelesenen Sektor prüft der Virus, ob dieser bereits infiziert ist. Ist er nicht infiziert, wird der gelesene, originale Sektor in einen bestimmten Sektor zur späteren Verwendung geschrieben. Hierzu wird vor einem Schreibvorgang der BPB (BIOS Parameter Block) innerhalb des Virus auf die Werte der zu infizierenden Diskette angepaßt. Soll auf eine schreibgeschützte Diskette oder Festplatte geschrieben werden, wird die vom jeweiligen Controller kommende Fehlermeldung weggeworfen und die Diskette bzw. Festplatte nicht infiziert. Bei jeder neuen Infektion wird der gespeicherte Stundenwert um eins erhöht. Vor einer Rückkehr zum Aufrufer werden stets alle Register wieder so in Ordnung gebracht, als sei der saubere Sektor von seiner normalen Stelle gelesen worden.

Durch Abfangen des Tastatur-Interrupts bekommt der Virus neben den normalen Tastenbetätigungen auch die Tastenkombination für einen Warmstart mit. Bei jeder normalen Tastenbetätigung vergleicht der Virus den Stundenwert der aktuellen Systemzeit mit dem Wert, der sich aus dem Stundenwert des Systemstarts erhöht um die Anzahl der infizierten Bootsektoren zusammensetzt. Sind beide gleich, wird der Bildschirm in den 40*25-Modus geschaltet, gelöscht, die Meldung "PARITY CHECK" ausgegeben und der Prozessor angehalten.

War die letzte Tastenkombination ein (Strg)+(Alt)+(Entf) für einen Warmstart, wird anstelle eines richtigen Warmstarts einfach das System ohne Löschen bzw. Zurücksetzen von Interruptvektoren neu gestartet. Dies bewirkt zwar auch ein Neuladen der Systemdateien, beläßt jedoch den Virus im aktivierten, residenten Zustand. Ein solcher "simulierter" Warmstart läßt sich leicht daran erkennen, daß die normalerweise üblichen Copyrightausgaben des BIOS-Herstellers unterbleiben und das System sofort mit dem Bootvorgang beginnt.

Die Installation eines Tastaturtreibers (KEYB, MFKEY) deaktiviert die Tastaturroutine des Virus. Der Virus kann zwar das System nicht mehr anhalten, aber das Infizieren nicht infizierter Datenträger funktioniert weiterhin.

Perfume

Alias: 4711, G
Art: Residenter .COM Infektor
Länge: 765 Bytes

Der Perfume Virus ist ein weitläufiger Verwandter des Black Jack und funktioniert ähnlich, der Virus wird ebenfalls resident installiert. Perfume ist jedoch eher ein 'Spaßvirus', da sich jede infizierte Datei nach dem 80. Infektionsversuch nur noch durch Eingabe eines Paßwortes (derzeit '4711') starten läßt. Zerstörungen werden nicht angerichtet.

Ping Pong (Bootsektorvirus)

Alias: Bouncing Ball, Italian, Big Italian

Gibt es sowohl als reine Diskettenversion wie auch in einer Harddiskversion. Gegenüber dem Stoned Virus macht der Ping Pong schon eine Reihe von Fehlerchecks. So prüft er beispielsweise nach, ob eine Infektion überhaupt möglich und sinnvoll ist. Beim Booten einer infizierten Diskette wird, wenn die Festplatte nicht schon verseucht ist (Kennung 01357h an Offset 02FCh), der originale Bootsektor der Festplatte in den Speicher geladen. Anschließend sucht sich der Virus einen freien Cluster (Cluster - in der Regel ein Bereich von vier Sektoren á 512 Bytes) auf der Festplatte aus und überschreibt den Bootsektor mit dem ersten Teil von sich selbst. Der zweite Teil landet im ersten freien Sektor des Clusters und der originale Bootsektor wird in dem zweiten Sektor des Clusters abgespeichert. Der Cluster wird dann vom Virus in nur einer FAT als schlecht markiert. Frühere Versionen des Virus belegten etwa 2KB unter der Oberkante des maximal verfügbaren Speichers und liefen nicht auf 80286er und 80386er Rechnern.

Manchmal, so etwa jede halbe Stunde, läßt der Virus einen herumhüpfenden Ball oder Punkt erscheinen. Dies läßt sich nur durch einen Neustart des Rechners beenden. Eine Infektion einer Diskette von der Festplatte aus ist schon mittels 'dir a:' zu bewerkstelligen.

Plastique

Art: Residenter .COM und .EXE Infektor
Länge: 3004, 4096 Bytes
Ähnlichkeit: Plastique Virus A, Plastique Virus B

Plastique Virus A:
Nach etwa 20 Minuten ertönt Musik, es werden einzelne Spuren formatiert, Festplatten sind nicht mehr bootfähig. Plastique befällt sowohl .EXE Dateien als auch .COM Dateien, aber nicht COMMAND.COM. Er verträgt sich aber nicht mit Speichermanagern wie QEMM oder 386MAX. Infizierte Dateien werden durchschnittlich um 3012 Bytes verlängert, maximal um 3020 (Plastique Virus B). Und auch gleich zu dieser Abart:

Plastique Virus B:
Gegenüber der A-Version ändert er neben dem INT 21h auch die Interrupts 13h, 9h und 8h. Wozu er Interrupt EDh braucht, ist noch nicht bekannt. Infizierte Dateien vergrößern sich um 4096 Bytes - aber bitte nicht mit dem 4096 Virus verwechseln.

RedX

Alias: Ambulance, Ambulance Car, Emergency
Art: Nicht residenter .COM Infektor
Länge: 796 Bytes

Man erkennt diesen Virus daran, daß von Zeit zu Zeit ein Krankenwagen über den Bildschirm fährt. Dieser Krankenwagen mit Blinklicht auf dem Dach ist aus ASCII-Zeichen als Blockgrafik aufgebaut, also ein einfaches Modell. Bei einer Infektion einer Datei versucht der Virus noch bis zu zwei andere Dateien zu infizieren, jedoch nicht die erste '.COM' Datei in einem Directory.

Sampo (Bootsektorvirus)

Alias: Wllop, Turbo

Dieser Bootsektorvirus infiziert den Master-Bootsektor einer Festplatte, wenn von einer infizierten Diskette gestartet wird. Wurde von einem infizierten Datenträger gestartet, infiziert der Virus nicht schreibgeschützte Disketten bei jedem Lese- oder Schreibzugriff, beispielsweise DIR A:

Ist der Virus resident, wird beim Zugriff auf einen infizierten Master-Bootsektor der nicht infizierte zurückgegeben. Sampo überlebt einen Warmstart mit dem Affengriff (Strg)+(Alt)+(Entf).

Wird auf eine schreibgeschützte Diskette zugegriffen, gibt der Virus einen angeblich mit dem Telefonica-Virus infizierten Bootsektor zurück. Am 30. November gibt der Virus folgende Textmeldung aus:

S A M P O
"Project X"
Copyright (c)1991 by the
SAMPO X-Team. All rights
reserved.
University Of The East
Manila

Silly Willy

Art: Nicht speicherresidenter File-Virus
Erstvorkommen: 1991 in München
Länge: .COM-Files: ca. 2261 bis 2314 Byte; .EXE-Files: 803 Byte werden überschrieben

Infizierte EXE-Programme geben mit ASCII-Zeichen ein Gesicht auf dem Bildschirm aus. Augenbrauen und Mund verändern sich laufend (traurig und fröhlich). Folgende Texte erscheinen:

> The User of This Computer ist Stupid!
> Please wait while I'm formatting your Harddisk.

Trotz der Meldung und aufleuchtender Laufwerkslampe wird NICHT formatiert. EXE-Files werden nur infiziert (zerstört), wenn das Jahr des Systemdatums größer als 1989 ist. Nur .COM-Dateien sind infektiös.

Solano

Art: speicherresidenter COM- und EXE-Infektor
Länge: 2000 Byte

12 Minuten, nachdem sich der Virus im Speicher festgesetzt hat, vertauscht er die Zeichen auf dem Bildschirm. Dieser Vorgang wiederholt sich alle paar Minuten erneut.

Stimulation

Art: Verlängernder File-Virus.

Dieser Virus durchsucht das aktuelle Directory nach .COM-Dateien. Jede Kopie des Virus ist unterschiedlich verschlüsselt. Wenn die Systemuhr auf Null steht, erscheint:

HA HA HA YOU HAVE A VIRUS FRODO LIVES!
Have you ever danced with the Devil in the pale moonlight?
DATA CRIME VIRUS RELEASED: 1 MARCH 1989 ALIVE:
Your system is infect by the STIMULATION virus. Have a nice day!

Danach wird der PC blockiert.

Stoned (Bootsektorvirus)

Alias: New Zealand, Donald Duck
Ähnlichkeiten: Stoned II, Angelina

Häufiger anzutreffender, residenter Bootsektorvirus. Wie auch beim Brain konnten erste Versionen dieses Virus nur 360 KB-Disketten infizieren. Nach einer "Verbesserung" kann er nun auch Festplatten und HD Disketten "richtig" infizieren. Frühere Versionen taten sich hier schwer und löschten schlicht und einfach vermeintlich unbenutzte Sektoren im Directory-Bereich.

Im Virus sind zwei Textkennungen enthalten. Eine von beiden, "LEGALISE MARIJUANA!", wird nicht angezeigt.

Der Virus gibt zumeist nach jedem achten Booten folgende Meldung aus:

Your computer is now stoned

oder

Donald Duck is a lie

Im unteren Hauptspeicher belegt der Virus zwei Kilobyte (ist selbst aber nur 400 Byte lang), auf der Festplatte einen Sektor. Dies ist meist der Sector 7 oder der Sector 11. Auf einer Festplatte (mit FDISK unter DOS 3.0 oder höher) macht dies fast nichts aus, denn dieser Bereich des ersten Zylinders wird vom Betriebssystem nicht genutzt. Dies ist aber nur für Festplatten gültig, die mit DOS 3.0 oder größer partitioniert wurden. Bei Betriebsystemversionen kleiner 3.0 ist dieser Bereich zumeist nicht frei, sondern mit der FAT belegt. Das Überschreiben dieser Bereiche führt zu unvorhersehbaren Schäden. Bei der Infektion einer Diskette wird eine Kopie des uninfizierten Bootsektors im letzten Sektor des Rootdirectories abgelegt. Hier stehende Einträge gehen verloren, Datenverluste sind hierdurch vorprogrammiert, jedoch eher selten. Bei einigen Versionen wird bei Tagesdatum 1-1-80 (häufig anzutreffen bei Batterieausfall) die Festplatte formatiert.

Der Stoned-Virus ist einer der ältesten Bootsektorviren mit vielen Varianten und recht einfach gehalten. Wird ein Rechnersystem von einer infizierten Diskette gestartet, infiziert der Virus das System. Während der Infektion einer Festplatte kopiert er den sauberen Master-Bootsektor in einen unbenutzten Bereich (Head 0, Cylinder 0, Sector 7) und lenkt alle weiteren Lesezugriffe auf den Master-Bootsektor auf diese Kopie um.

Nach dem Systemstart von einem infizierten Datenträger speichert der Virus den Interrupt 13h-Vektor, vermindert den zur Verfügung stehenden unteren

Hauptspeicherbereich (0-640 KB) um zwei Kilobyte und korrigiert die Angabe des konventionellen Hauptspeichers. In den auf diese Art "belegten" Speicher kopiert sich der Virus hinein, der Interrupt 13h-Vektor wird auf die vireneigene Routine umgebogen und die Programmausführung in dem oberen Speicherbereich fortgesetzt. Hierdurch ist die residente Installation abgeschlossen.

Anschließend wird nach einem Reset der originale Sektor an seine normale Stelle im Hauptspeicher nachgeladen. Der Virus entscheidet nun, ob er von einer Festplatte oder Diskette gestartet wurde.

Wurde von Festplatte gestartet, ist die Festplatte bereits infiziert und der Virus kann dem Programmcode des bereits an die richtige Hauptspeicherstelle geladenen originalen Sektors zur Ausführung des weiteren Systemstarts die Kontrolle übergeben.

Stellt der Virus allerdings fest, daß ein Systemstart von einer Diskette ausgeführt wurde, entscheidet zufällig der System Timer, ob nun der Text "Your PC is now Stoned!" ausgegeben wird oder nicht. Danach wird der Master-Bootsektor der ersten physikalischen Festplatte eingelesen und geprüft, ob dieser bereits infiziert ist. Ist dieser schon infiziert, wird das System angehalten, sofern ein Text ausgegeben wurde.

Ist der Master-Bootsektor nicht infiziert, wird er auf Sector 7 zur "besonderen weiteren Verwendung" gespeichert. Nach Modifikation des noch im Speicher stehenden Master-Bootsektors schreibt der Virus den infizierten Bootsektor zurück auf die Festplatte. Nach dieser Infektion setzt der Virus den normalen Startvorgang fort und übergibt dem originalen Bootsektor der Diskette die Programmkontrolle.

Der Virus ist aber bereits resident und überprüft während eines jeden Interrupt 13h-Zugriffes, ob sich der Diskettenmotor des Laufwerkes A: bereits dreht. Solange sich der Motor des Diskettenlaufwerkes dreht, wird keine Prüfung auf Infektion vorgenommen. Dreht sich der Motor allerdings nicht und muß erst hochlaufen, überprüft der Virus, ob eine eingelegte Diskette bereits infiziert wurde. War sie nicht infiziert, wird sie infiziert. Bei diesem Vorgang wird die FAT neuerer Diskettenformate überschrieben.

Sunday Virus

Art: Residenter .COM und .EXE Infektor
Länge: 1631 Bytes

Dieser Virus hat etwas gegen Sonntagsarbeit. Er gibt folgende Meldung aus:

Today is Sunday! Why do you work so hard?
All work and no play make you a dull boy!
Come on! Let's go out and have some fun!

Ein Teil des Virus stammt vom Israel Virus. Teilweise zerstört der Virus unter bestimmten Umständen die FATs. Eine Abart des Sunday aktiviert sich nie, d. h. die Meldung wird nicht angezeigt.

Sylvia

Alias: Holland Girl
Art: nicht speicherresidenter COM- Infektor
Länge: 1332 Byte

Der Virus infiziert .COM-Dateien im aktuellen Verzeichnis und im Hauptverzeichnis von Laufwerk C:. Der Viruscode enthält den Text:

This program is infected by a HARMLESS Text Virus V2.1
Send a FUNNY postcard to : Sylvia
You might get an ANTIVIRUS program.....

Mit der letzten Bemerkung hat Sylvia nicht ganz unrecht...

Tai Pan

Alias: Whisper
Art: Residenter .EXE Infektor
Länge: 438 Bytes
Ähnlichkeiten: Tai Pan-666, Tai Pan 434

Tai-Pan ist ein einfacher, residenter Dateivirus. Beim Starten eines infizierten Programmes überprüft der Virus mit einer selbstdefinierten INT 21h-Funktion AX=7BCEh (Resultat: AX=7BCEh), ob er bereits im Speicher aktiv ist. Ist das nicht der Fall verkürzt der Virus die MCB-Kette um 528 bzw. 752 Bytes und kopiert sich in diesen Speicherbereich hinein. Um nicht überschrieben zu werden, markiert der Virus diesen Speicherbereich als SYSTEM-MCB. Der Virus belegt Interrupt 21h ohne besondere Tricks und springt nach der Aktivierung zurück zum eigentlichen Programmstart.

Der Virus überwacht die EXEC-Funktion von DOS und infiziert alle Programme, die kleiner als 64833 Bytes sind und die EXE-Signatur "MZ" aufweisen. Der Wert von IP im EXE-Header wird als Infektionsmarkierung benutzt, um erneute Infektionen auszuschließen. Tai Pan verlängert die Datei um 438 Bytes und befindet sich am Dateiende. Der Virus behält bei der Infektion das ursprüngliche Dateidatum bei, er kann allerdings nicht das DOS-Dateiattribut READ-ONLY, SYSTEM oder HIDDEN umgehen.

Der vom Virus berechnete neue EXE-Header hat einen ungültigen Stack und kann unter Umständen zum Absturz des Programmes führen. Sonst hat der Virus keine weiteren Schadensroutinen.

Folgender Text kann in jeder infizierten Datei gefunden werden:

> [Whisper presenterar Tai-Pan]

Tai-Pan ist in Deutschland recht stark verbreitet. Er wurde mit Terminate 1.50, einer CD der Zeitschrift Power-Play und anderen Sharewarearchiven in Umlauf gebracht.

Tai Pan-434

Die Variante Tai Pan-434 ist gegenüber den ursprünglichen Virus leicht modifiziert. Der Virus verlängert jetzt Programme um 434 Bytes und enthält den Text:

> CoSmO

Zusätzlich wird das Schreiben von Daten (über Datei-Handles) kontrolliert. Bildschirmausgaben sind mit aktiven Tai Pan-434 nicht mehr lesbar.

Tai Pan-666

Diese Variante ist fast identisch mit dem ursprünglichen Tai-Pan. Die Interrupt-Selbsterkennung wurde auf AX=7BCFh geändert und die neue Viruslänge beträgt jetzt 666 Bytes. Geändert wurde auch der Text innerhalb des Virus:

DOOM2. EXE
Illegal DOOM II signature
Your version of DOOM2.EXE matches the illegal RAZOR release of DOOM2
Say bye-bye HD
The programmer of DOOM II DEATH is in no
way affiliated with ID software.
ID software is in no way affiliated with DOOM II DEATH.

Dieser Text ist zum Glück ein Scherz, der Virus enthält keinerlei destruktive Routinen. Er kontrolliert nicht einmal, ob ein Programm "DOOM2. EXE" heißt.

Diese Variante wurde mit einem Tool für das Spiel DOOM II - DMNCHEAT.ZIP - in Umlauf gebracht.

Taiwan

Art: Nicht residenter .COM Infektor
Länge: 708, 743 Bytes

Am 8. eines jeden Monats überschreibt der Virus 160 Sektoren ab dem Sektor 1 der Festplatten 'C' und 'D'. Hierdurch werden unter anderem die FAT und das Hauptverzeichnis zerstört. Ist eine .COM-Datei kleiner als die Virusgröße, so wird die infizierte Datei in der Größe verdoppelt. Bei jeder Infektion startet der Virus noch drei zusätzliche Infektionsversuche. Der Virencode wird am Beginn einer infizierten Datei eingefügt.

Tenbytes

Alias: V-Alert
Art: Residenter .COM und .EXE-Infektor
Länge: 1554 Bytes

Nach seiner Aktivierung zwischen September und Dezember überschreibt der Virus bei jeder zum Schreiben geöffneten Datei die ersten zehn Bytes.

Tequila

Länge: 2468
Art: Residenter EXE-Infektor
Ähnlichkeiten: Flip

Überschreibt die Laderoutine des Masterbootsektors (Partitionssektor) mit seiner eigenen Laderoutine, nicht jedoch, ohne den richtigen an anderer Stelle auf der Festplatte zu sichern. Durch weitere Manipulationen verringert sich die Kapazität der 1. logischen Festplatte um 6 Sektoren (3 KByte), wohin sich der Virus selbst kopiert. Im Speicher nistet er sich an der Oberkante DOS ein, jedoch nicht, wenn ein infiziertes Programm gestartet wird, sondern erst nachdem Sie Ihren Rechner von der Festplatte booten. Programme und Overlaydateien werden bei der Ausführung infiziert. Die Erstellungszeit einer infizierten Datei weist im Sekundenfeld die Zahl 62 auf. Versucht ein Programm die Dateigröße einer infizierten Datei zu ermitteln, zieht Tequila hiervon erst einmal seine eigene Größe ab. Das geschieht auf einer niedrigeren Ebene als bei Flip, Tequila kann damit auch andere Programme als COMMAND.COM foppen.

WARNUNG:
Ist Tequila resident, also aktiv, erkennt CHKDSK Dateizuordnungsfehler - die in Wirklichkeit aber gar keine sind, da der Virus durch Stealth-Techniken dem Betriebssystem eine andere Dateilänge vorgaukelt. Wenn Sie hier CHKDSK /F eingeben, zerwürfeln Sie Ihre Daten.

Folgender Text ist verschlüsselt im Virus enthalten:

> Welcome to T.TEQUILA's latest production.
> Contact T.TEQUILA/P.o.Box 543/6312 St'hausen
> Switzerland.
> Loving thought to L.I.N.D.A.
> BEER and TEQUILA forever !"
> "$Execute: mov ax, FE03 / int 21. Key to go on!"

Traceback

Art: Residenter .COM und .EXE Infektor
Länge: 2930, 3066 Bytes

Der Virus kann durch die folgende 16 Byte lange Zeichenkette erkannt werden, die am Ende des Viruscodes zu finden ist:

58 2B C6 03 C7 06 50 F3 A4 CB 90 E8 E2 03 8B

Etwa eine Stunde nach einer Infektion eines Systems beginnen, ähnlich wie bei Black Jack, die Buchstaben vom Bildschirm zu fallen. Nach einer Minute kehren die Buchstaben automatisch wieder an Ihren Platz zurück. Je nach Abart und Version des Virus kann diese Zeitspanne durch einen Tastendruck abgekürzt werden. Andernfalls schickt diese Tastenbetätigung den Rechner in eine Endlosschleife.

Tremor

Länge: 4000 Bytes
Art: Residenter Virus, Stealth, Fast Infector

Vergrößert die infizierten Dateien um 4000 Byte und setzt das Dateidatum um 100 Jahre hinauf. Tremor verwendet INT 21h, INT 15h, INT 9 und INT 24h.

Selbsterkennung:

```
MOV  AH,2Ah
int  21h
MOV  AH,30h
INT  21H
MOV  AX,0F1E9H
INT  21H
CMP  AX,0CADEh
JE   already_resident
```

Der Virus ist polymorph und versucht sich bei der Installation in den Upper Memory Bereich zu installieren. Dabei verwendet er zunächst die DOS-Funktion, dann die XMS-Funktion. Tremor benutzt eine Tracing-Funktion, um den Einsprungspunkt für den INT 21h zu finden. Das Master-PSP wird so geändert, daß nach jedem Programmende der aktuelle Kommandointerpreter die Kontrolle an Tremor übergibt. Er infiziert immer als erstes den COMMAND.COM, der Rechner wirkt sehr "lahm".

CHKDSK zeigt die alten Werte für den Hauptspeicher an. Werden CLEAN, SCAN, MEM, CHKDSK, F-PROT, SYS, MIRROR, SI oder ARJ gestartet, dann werden diese Files auf der Festplatte (!) gereinigt, ebenso wird nach residenten Wächterprogramm gefahndet. VSAFE und TSAFE werden einfach abgeschaltet.

Bedingt durch die Stealth-Funktionen des Virus scheitert jeder Versuch, eine infizierte Datei zu erkennen. Das Dateisystem selbst wird nicht angegriffen. Bei einem Warmstart wird gelegentlich folgender Text ausgegeben, der verschlüsselt im Virus abgespeichert ist:

T.R.E.M.O.R was done by NEUROBASHER / May-June'92, Germany
.MOMENT.OF.TERROR.IS.THE.BEGINNING.OF.LIFE.

Anschließend wird das Rechnersystem neu gestartet.

Die Chronologie des Channel-Videodat-Unfalls (Tremor), Mai 1994:

Zunächst einige Bemerkungen zur Übertragung von Daten per Satellit. Für

die Ausstrahlung von TV-Bildern werden nicht alle Zeilen benötigt. Pro Bildschirmseite sind jeweils drei Zeilen frei, die für andere Aufgaben genutzt werden können. Die zusätzliche Kapazität eines Videokanals, kann beispielsweise für die Übertragung von Texten oder von Programmen genutzt werden. Jeder Teilnehmer benötigt für deren Empfang zwischen seinem Fernsehgerät und seinem PC einen Konverter (Hersteller: unter anderen Wiegand Video Datensysteme GmbH in Wesseling).

Die Firma Videodat Medien GmbH in Wesseling hatte damals einen Teil der Kapazität des Kanals gemietet, der für die Ausstrahlung des TV-Programmes Pro 7 genutzt wird. Dieser Kanal kann in Europa über Satellit und über Kabel empfangen werden. Für die unter dem Namen "Channel Videodat" ausgestrahlten Informationen und Programme trägt die Firma Videodat Medien GmbH, Wesseling, die redaktionelle Verantwortung.

Ein von dem Virus betroffenes Unternehmen gab an, daß der Virus durch ein Download eines Programmes aus Channel Videodat eingeschleppt worden wäre. Ein eindeutiger Nachweis, wer die Tremor-infizierten Dateien verteilt hat, konnte aber bisher nicht geführt werden. Die Videodat Medien GmbH wurde sofort über diesen Verdacht informiert. Sie entgegnete einerseits, daß keine infizierten Programme ausgestrahlt worden wären, schilderte aber andererseits die Techniken, die von ihr für die Prüfung auf Virenfreiheit verwendet werden - es lag bereits eine schriftliche Anfrage eines Teilnehmers vor.

Am 17. Mai strahlte Channel Videodat um 14.04 Uhr die Version 104 von McAfee's SCAN und das Programm PKUNZIP.EXE aus, mit dem die Datei SCANV104.ZIP vor ihrem Einsatz dekomprimiert werden muß. Die Datei PKUNZIP.EXE war mit dem Tremor-Virus infiziert. Die ausgestrahlte Version von SCAN kann den Tremor nicht erkennen. Mit dem von MicroBIT zur Verfügung gestellten speziellen Programm zur Erkennung des Tremor-Virus wäre es aber möglich gewesen, die Infektion auf einem (durch Kaltstart von einer sauberen Diskette) sauberen PC (besser: sauberen Hauptspeicher) vor der Ausstrahlung zu erkennen und den Unfall zu vermeiden. Die Infektion der Datei PKUNZIP.EXE wurde vermutlich von aufmerksamen Teilnehmern sofort gemeldet. Auf jeden Fall wurde bereits am gleichen Tag gegen 16.00 Uhr über Channel Videodat eine saubere Version ausgestrahlt. Nur die Teilnehmer, die zu dieser Zeit noch online waren, erhielten die saubere Version, mit der die infizierte überschrieben wurde. Zusätzlich hat Channel Videodat anschließend mehrfach Anti-Viren-Programme und Warnungen ausgestrahlt.

Einige Viren-Opfer behaupten, daß - wie oben bereits erwähnt - schon früher infizierte Dateien über Channel Videodat ausgestrahlt worden seien. Das läßt sich heute jedoch nicht mehr nachweisen. Tatsache ist, daß sich der Tremor-Virus, der zum ersten Mal im Januar 1993 auftauchte, zumindest in

Deutschland sehr schnell und stark ausgebreitet hat.

Tumen 0.5

Art: Speicherresidenter File-Virus
Länge: 1663 Byte

Durch Drücken von STRG+ALT und einer beliebigen Taste ertönt ein akustisches Signal. Anschließend wird auf EGA- oder VGA-Bildschirmen die Farbpalette ausgegeben. Das geschieht übrigens auch nach jeder erfolgreichen Infektion.

Typo COM

Alias: Fumble
Art: Residenter .COM Infektor
Länge: 712, 867 Bytes

Wird eine Datei infiziert, untersucht der Virus alle Dateien im angemeldeten Directory und infiziert diese, sofern das noch nicht geschehen ist. Je nach Version stört der Virus entweder die Druckausgabe zum Parallelport oder verfälscht Tastatureingaben. Dies ist besonders störend für Schnellschreiber. Eine Abart des Virus infiziert Dateien nur an geraden Tagen.

V163

Art: speicherresidenter COM- und EXE- Infektor
Länge: 163 Byte

Der Virus infiziert sämtliche Dateien, die nicht mit einem "M" (4Dh) beginnen. Den Wert "M" (4Dh) setzt V 163 selbst im ersten Byte einer Datei ein. Der Virus scheitert an Readonly-Dateien.

VGen

AVWin findet bei einem VGen-Virus nur eine Virensignatur. Dies bedeutet, daß hier aller Wahrscheinlichkeit nach virulenter Code gefunden wurde. Um hier auf Nummer sicher zu gehen, bitten wir Sie, uns die Dateien, die von AVWin mit einem VGen-Virus erkannt wurden, ins Haus zu schicken.
Da bei VGen-Viren nur eine Virensignatur gefunden wird, können diese Dateien von AVWin leider auch nicht repariert werden.

Vacsina

Art: Residenter .COM, .EXE, .SYS und .BIN Infektor
Länge: 1339, 2764 (+ 132) Bytes
Ähnlichkeiten: Yankee Doodle

Vacsina ist ein Virus mit einer automatischen Updatefunktion. Trifft eine neuere Version auf eine ältere Version, wird die ältere Version vom Virus selbst entfernt und durch die neue ersetzt. In der Regel piepst der Vacsina Virus, wenn er eine Datei infiziert.

Das Infizieren von .EXE Dateien erfolgt in zwei Schritten, da der Virus anscheinend nur .COM Dateien 'richtig' infizieren kann. Bei dem ersten Aufruf einer .EXE Datei wird bei residentem Virus die zu infizierende Datei mit einem Relocator versehen. Mit diesem Relocator verhält sich die Datei nach außen für den Vacsina als .COM Datei und kann dann bei einem zweiten Aufruf von ihm infiziert werden.

Vascina stellt in den vorliegenden Versionen bei infizierten Dateien Originaldatum und -zeit nicht wieder her. Hierdurch erhalten infizierte Dateien das zum Infektionszeitpunkt gültige Systemdatum und -zeit.

Interessant ist auch die Kennzeichnung der internen Versionen. Zumeist stellen die beiden letzten Bytes einer infizierten Datei die 'Versionsnummer' des Virus dar. Im Speicher ist die Versionsnummer im Segment 0 an Offset 0C7h wiederzufinden.

Victor

Art: speicherresidenter COM- und EXE- Infektor
Länge: 2442 bis 2458 Byte

Der Virus zerstört in den Zeiten von 9.00-10.00, von 11.00-12.00, von 13.00-14.00 sowie von 15.00-16.00 Uhr Dateien im jeweils aktuellen Verzeichnis. Der Viruscode enthält den Text:

Victor V1.0 The incredible high Performance Virus Enhanced versions available soon. This program was imported from USSR. Thanks to Ivan.

Vienna

Alias: DOS-62, Blue Danube, Wiener, P, Unesco, Austrian
Art: Nicht residenter .COM Infektor
Länge: 648 Bytes

Der Vienna-Virus ist ein sehr primitiver, aber dennoch effektvoller Virus. Er zerstört unter bestimmten Bedingungen Dateien, und zwar immer dann, wenn beim Infektionsversuch die letzten 3 Bits der Systemzeit gerade auf 0 gesetzt sind. Bei manchen Versionen macht Vienna bei einem von acht Infektionsversuchen die zu infizierende Datei unbrauchbar, die neu infizierte Datei ist vollständig 'geschrottet'.

Eine Eigenart des Vienna-Virus ist, daß er nur Dateien im aktuellen Pfad und im aktuellen Unterverzeichnis infiziert bzw. löscht. Setzt man also 'PATH = C:\TEST' und arbeitet in diesem leeren Directory TEST, kann der Virus zwar keine Dateien mehr infizieren, man selbst kann aber meist auch nicht mehr sehr effizient arbeiten.

Da der Vienna-Virus ab und zu Dateien zerstört, ist bei der Entfernung dieser zerstörten Dateien mit dem Reparaturprogramm AntiVir im GURU-Modus darauf zu achten, daß nicht versehentlich Datendateien gelöscht werden. AntiVir kann nicht entscheiden, ob die ersten fünf Bytes einer Restart-Sequenz (JMP FFFF:00F0) ein gültiges - und gewolltes - Neustart-Programm darstellen, oder eine durch eine vom Virus hergestellte Zerstörung vorliegt. Dies müssen Sie selbst entscheiden. Ganz schwierig wird die Sache, wenn der Virus 'manchmal' anstelle der Sprunginstruktion von oben fünf NOPs in die Datei hineinschreibt.

Vriest

Art: Residenter .COM Infektor
Länge: 1280 Bytes

Verlängert Dateien um 1280 Bytes. Am 3.5.1991 wird folgender Text auf dem Bildschirm angezeigt:

> Something's coming up ...

Dann folgt ein Sirenenton, anschließend scrollt der Bildschirm hoch und es wird angezeigt:

> Vriest of g greats Vic ear Moeli~

Der Virus bedient sich des Betriebsystemes, um sich resident zu installieren. Er belegt im Speicher 1584 Bytes und infiziert Dateien nicht, wie sonst üblich, etwa beim Laden einer .COM Datei - nein, er infiziert sie beispielsweise beim COPY-Vorgang.

Whale

Alias: Motherfish, Z the wahle
Länge: 9216 Bytes
Art: Residenter .COM und .EXE Infektor
Ähnlichkeiten: Fish

Einer der größten wie auch ungefährlichsten Viren überhaupt. Eine Infektion wird sofort erkannt, da sich die Rechnerleistung auf einen Wert vermindert, der ein sinnvolles Arbeiten verhindert und sich Bildschirmausgaben endlos in die Länge ziehen. In aller Regel stürzen infizierte Programme sofort ab. Durch die sofortige Entdeckung mit nachfolgender Beseitigung tritt meist kein ernsthafter Schaden auf.

Bei resident aktivem Virus darf kein "CHKDSK /F" ausgeführt werden, da der Virus durch Stealth-Techniken seine Anwesenheit zu verschleiern versucht. In diesem Fall würden Dateien geschädigt. Gut vier Fünftel des Codes des Virus sind Debuggerfallen, um ein Disassembly des Codes zu erschweren. Vermutlicherweise wurde der Virus von zwei Programmierern geschrieben: einer war für die Assembler-Sachen (die Selbstverschlüsselung und Verschlüsselungs-/Entschlüsselungsteile), ein anderer für die sonstigen Routinen zuständig, die hauptsächlich in Hochsprache geschrieben wurden. Dieser Virus bekam das Attribut 'armoured', was soviel wie 'bewaffnet' bedeutet. Die merkliche Zeitverzögerung bei aktivem Virus ist eine direkte Folge dieser 'Bewaffnung': sie kostet Prozessorzeit. Ist der Virus aktiv, liegen immer nur Teile des Programmcodes in lauffähiger Form vor, da diese Teile vor einem Ausführen erst ent- und nach Ausführung wieder verschlüsselt werden, bevor ein neuer Teil wieder ent- und verschlüsselt wird.

Wiener

Alias: DOS-62, Blue Danube, Vienna, P, Unesco, Austrian
Art: Nicht residenter .COM Infektor
Länge: 648 Bytes

Der Wiener Virus ist ein sehr primitiver, aber dennoch effektvoller Virus. Er zerstört unter bestimmten Bedingungen Dateien und zwar immer dann, wenn beim Infektionsversuch die letzten 3 Bits der Systemzeit gerade auf 0 gesetzt sind. Bei manchen Versionen macht der Virus bei einem von acht Infektionsversuchen die zu infizierende Datei unbrauchbar, die neu infizierte Datei ist vollständig 'geschrottet'.

Eine Eigenart des Wiener Virus ist, daß er nur Dateien im aktuellen Pfad und im aktuellen Unterverzeichnis infiziert bzw. löscht. Setzt man also 'PATH = C:\TEST' und arbeitet in diesem leeren Directory TEST, so kann der Virus zwar keine Dateien mehr infizieren, man selbst kann aber meist auch nicht mehr sehr effizient arbeiten.

Da der Wiener-Virus ab und zu Dateien zerstört, ist bei der Entfernung dieser zerstörten Dateien mit dem Reparaturprogramm AntiVir im GURU-Modus darauf zu achten, daß nicht versehentlich Datendateien gelöscht werden. AntiVir kann nicht entscheiden, ob die ersten fünf Bytes einer Restart-Sequenz (JMP FFFF:00F0) ein gültiges - und gewolltes - Neustart-Programm darstellen, oder eine durch eine vom Virus hergestellte Zerstörung vorliegt. Dies müssen Sie selbst entscheiden. Ganz schwierig wird die Sache, wenn der Virus 'manchmal' anstelle der Sprunginstruktion von oben fünf NOPs in die Datei hineinschreibt.

WinWord.Concept

Alias: WW6Macro
Art: Makro-Virus

Dieser "Virus" ist ein reiner Makro-Virus, der Dokumentendateien (DOC) verändert. WinWord.Concept nutzt die ausführlich dokumentierte Makrosprache WinBasic des Applikationsprogrammes Word für Windows. Der "Virus" selbst enthält keine direkten Prozessorbefehle, sondern besteht nur aus reinen Makros.

Sofort beim Öffnen einer mit diesen Makros versehene Dokumentendatei wird das Makro AutoOpen ausgeführt. Der "Virus" hat somit erst einmal die Kontrolle erhalten, da ein Makro aus der dem aktiven Dokument zugewiesenen Dokumentenvorlage die größte Priorität hat - und das Dokument ist die Vorlage selbst! Er verändert die globale Vorlagendatei, üblicherweise ist dies die Datei NORMAL.DOT. Eine Meldung (Message-Box) erscheint und gibt die Zahl "1" aus:

Streng genommen ist die geöffnete Dokumentendatei keine Dokumentendatei (DOC), sondern ein Vorlagendatei (DOT). Der "Virus" verändert das standardmäßige Makro "DateiSpeichernUnter". Dokumente werden jetzt im Format 1, das heißt als Dokumentenvorlage gespeichert. Daher auch die Schwierigkeiten beim Abspeichern in angewählten Verzeichnissen. Jede mit "Datei / Speichern unter..." abgelegte Datei enthält ihrerseits wieder die Makros aus WinWord.Concept.

Wird ein derart gespeichertes Dokument, oder genauer gesagt: diese Vorlage, auf einem unveränderten Word für Windows System geöffnet, wird auch der AutoOpen-Makro wieder ausgeführt und die globale Vorlagendatei mit den neuen Makros versehen. Nachdem WinWord.Concept auf der Makrosprache WordBasic "aufsetzt", ist er auch unter den verschiedenen Betriebssystemen (Windows 3.1, Windows für Workgroups, Windows 95, Windows NT, Mac OS) lauffähig, bei denen Word mit dieser Makrosprache ausgerüstet ist (Word für Windows 6.0, Word für Windows 7.0, etc.).

WinWord.Concept läßt sich recht einfach durch die Existenz folgender drei Makros feststellen:

AAAZAO
AAAZFS

Payload

Eventuell ist noch das Makro AutoOpen dazugekommen. Falls das Makro AutoOpen bereits vorher existiert hat, wurde dessen Inhalt geändert. Darüber hinaus sind neben den Makronamen in den Dokumenten noch folgende Textstrings erkennbar:

see if we´re already installed
iWW6IInstance
That´s enough to prove my point

In der Datei WINWORD6.INI ist noch folgender Eintrag hinzugekommen:

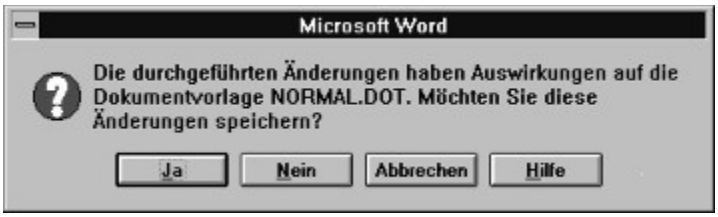
WW6= 1

WinWord.Concept kann durch manuelles Löschen der fraglichen Makros aus allen Dokumenten entfernt werden. Falls man sich nicht sicher ist, ob ein Dokument oder die bestehende globale Formatvorlage bereits von diesem "Virus" verändert wurden, sollte das Programm mit "disableten" Makros aufgerufen werden. Dies kann zum einen über die Kommandozeilen geschehen oder wenn WinWord selbst durch Shift+Klick auf das Icon gestartet wurde, es werden dann keine Makros ausgeführt. Bei Word für Windows 6.0 darf beim Anwählen eines Dokumentes nicht auf den Dokumentennamen doppelgeklickt oder einfach OK gedrückt werden, sondern das Dokument muß mit Shift+OK geöffnet werden, dann öffnet WinWord 6.0 das Dokument ohne Makros.

Generell läßt sich auch die bestehende NORMAL.DOT auf READONLY stellen, allerdings muß dann manuell vor jedem Ändern das Attribut READONLY erst wieder entfernt werden. Eine andere Möglichkeit wäre das Unterdrücken aller automatischen Makrofunktionen, beispielsweise durch folgendes Makro als AutoExec:

```
Sub MAIN
AutoMakroUnterdrücken 1
MsgBox "Automatische ablaufende Makros werden unterdrückt", "AutoMakro-
Unterdrückung", -1
"AutoMakro-Unterdrückung", -1
End Sub
```

Solch ein Makro kann auch der globalen Vorlage unter einem anderen Namen hinzugefügt und später beim Start von Word für Windows (winword /M<name> dann gezielt aufgerufen werden. Über den Parameter /A kann WinWord auch angewiesen werden, ohne Dokumentenvorlage und Add-Ins zu starten.


Microsoft Word
Die durchgeführten Änderungen haben Auswirkungen auf die Dokumentvorlage NORMAL.DOT. Möchten Sie diese Änderungen speichern?
Ja
Nein
Abbrechen
Hilfe

WitCode

Art: .EXE-Infektor
Länge: 974 Bytes

Der Virus holt sich vom Betriebssystem ca. 1,5 KB Speicher und kopiert sich in diesen freien Speicher. Der MCB dieses PSP wird derart verändert, daß er wie ein Teil des aktiven Kommandointerpreters aussieht. Beim Beenden eines Programmes werden anhand verschiedener Werte der Systemuhr diverse Meldungen ausgegeben. Am 24. Dezember gibt es Weihnachtsglückwünsche und jeden Sonntag erscheint die Meldung:

You really shouldn't work on Sundays...

Ausgehend von der Art des installierten Prozessors beschwert sich der Virus über einen zu langsamen Rechner:

Gee, I wanna sleep now!

Besitzer schneller Rechner beglückwünscht er:

You got a fine machine!

Abhängig von der Systemuhr ändert WitCode an Montagen und an jedem Freitag den 13. den Bootsektor in der Weise, daß folgende Neustarts in einer Endlosschleife im Bootsektor hängenbleiben.

Yankee Doodle

Alias: TPxx
Art: Residenter .COM und .EXE Infektor
Länge: 1881+16 Bytes
Ähnlichkeiten: Vacsina

Je nach Abart spielt der Virus über den eingebauten Lautsprecher den Yankee Doodle. Dies kann sowohl um 17:00, aber auch nach der erfolgreichen Infektion einer Datei sein. Bei der Installation umgeht der Virus das Betriebsystem durch direkte Modifikation der MCBs und infiziert anschließend jedes neu gestartete Programm. Da dieser Virus vom Vacsina Virus abstammt, hat er auch die Fähigkeit geerbt, sich selbst durch neuere Versionen zu ersetzen. Eine Version des Virus 'killt' einen eventuell vorhandenen Ping Pong auf der Festplatte.

Zero Bug

Alias: Palette, ZBug
Art: Residenter .COM Infektor
Länge: 1536 Bytes

Die Vergrößerung einer Datei wird nicht im Directory angezeigt. Der Virus schreibt zur Kennzeichnung einer bereits infizierten Datei eine '62' in das Sekundenfeld. Nachdem auch der COMMAND.COM auf der Festplatte infiziert wurde, werden in der Regel nach einer gewissen Zeitspanne Buchstaben auf dem Bildschirm durch den 'Smiley', (ASCII Code 01) 'aufgegessen'.
Große .COM-Dateien werden vom Virus 'geschrottet'. Der Virus kann durch folgenden Zeichenketten in einer befallenen Datei erkannt werden:

ZE
COMPSEC=C:
C:\COMMAND.COM

dBase

Art: Residenter .COM und Overlay Infektor
Länge: 1864 Bytes

Ist dieser Virus resident installiert, verändert er die Daten von dBase-kompatiblen Datenbanken. In der nicht sichtbaren Datei BUGS.DAT legt der Virus die Namen derjenigen Datenbanken ab, deren Inhalte er modifiziert hat. Beim Schreiben von Daten in eine .DBF-Datei werden benachbarte Bytes ausgetauscht, beim Lesen der Daten wird diese 'Verschlüsselung' wieder rückgängig gemacht. Dieses Spielchen geht für zwei Monate gut, danach überschreibt der Virus die FATs und das Rootdirectory. Im Virus selbst ist der Name der Datei in Klarschrift abgelegt: 'c:\bugs.dat'. Über INT 21h, Unterfunktion 0FB0Ah sieht der Virus nach, ob er nicht schon resident installiert ist.