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.

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.

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.

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 effektiver. 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.

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.

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!

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.

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.

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 ... ?!?

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.

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'

ExploreZip

W32/ExploreZip (in unseren Produkten gelistet unter Tr.ExploreZip.Worm)

Alias: Worm.Explore.Zip
Zipped Files
Troj.Explore.Zip
Merkmale: Trojanisches Pferd, Wurm
Textstring: zipped_files
Länge: 210432 Bytes
Plattform: Windows 9x/Windows NT

W32/ExploreZip verbreitet sich über E-Mail auf Windows 9x- und Windows NT-Rechnersystemen. Als E-Mailprogramm kommt jeder MAPI-fähige E-Mail-Client in Betracht. Hierzu gehören unter anderem:

MS Outlook
NetScape Mail
MS Exchange
Outlook Express

Im aktiven Zustand verteilt er sich über MAPI-Kommandos weiter, indem er sich selbst als Attachment mit dem Namen 'zipped_files.exe' versendet. Im Gegensatz zu Melissa versendet sich W32/ExploreZip selbständig an die Adressen unbeantworteter E-Mail im Posteingang. Melissa hingegen verschickte Kopien von sich selbst an bis zu 50 Empfänger aus dem Adreßbuch.
Durch diesen Trick sieht die E-Mail beim Empfänger ganz unverfänglich aus. Ist sie doch eine Antwort auf die - an einen bekannten Empfänger - versandte Nachricht.

Eine infizierende E-Mail sieht folgendermaßen aus:

From:
[Name des Email-Absenders]

Subject:
re:*[Subject der unbeantworteten Nachricht]*

To:
[Name des Email-Empfängers]

Body:
Hi *[Name des Email-Empfängers]* !
I received your email and I shall send you a reply ASAP.
Till then, take a look at the attached zipped docs.
Bye oder sincerely
[Name des Email-Absenders]

Attachment:
zipped_files.exe

Zu diesem Zeitpunkt ist der Virus aber schon aktiv und "arbeitet". Er kopiert sich selbst entweder unter dem Namen 'Explore.exe' oder '_setup.exe' in das jeweilige System-Verzeichnis. Dies ist %windir%\System (üblicherweise c:\windows\system) unter Windows 9x, bzw. %windir%\System32 (üblicherweise c:\winnt\system32) unter Windows NT.

Anschließend modifiziert er die WIN.INI unter Windows 9x, bzw. die Registry unter Windows NT. Durch die Modifikation der INI-Datei, bzw. der Registry erreicht der Virus, daß er bei jedem Hochfahren des Systemes erneut gestartet wird. Hierdurch hat er die Möglichkeit, auch neue Posteingänge entsprechend zu beantworten.

In seiner Schadensroutine ist der Virus multi-threading-fähig: Er erzeugt zwei "Killer-Threads". Einer der Threads sorgt für die 'E-Mail-Behandlung', ein anderer Thread ist für das "Leeren" der Dateien zuständig. Der erste Thread überwacht via MAPI neue Posteingänge. Durch das Überwachen neuer Posteingänge "beantwortet" der Virus eingegange E-Mails sofort wieder mit sich selbst. Bestehende, bisher ungelesene Nachrichten werden ebenfalls sofort beantwortet.

Ein zweiter Thread "leert" Dateien mit folgenden Extensions '.doc, .c, .cpp, .h, .asm, .xls und .ppt'. Das "Leeren" ist ein Kürzen der Dateien über die Windows-Funktion 'CreateFile' auf 0 Byte! Durch diesen Vorgang werden Dateien nicht gelöscht und stehen auch nicht für eine Wiederherstellung über den Papierkorb zur Verfügung. Die gekürzten Dateien können nicht wiederhergestellt werden, da der Inhalt verlorengegangen ist.

Das Leeren von Dateien läßt sich auch an einer verstärkten Festplattenaktivität feststellen. Doch der Virus leert auch solche Dateien, die über "gemappte" Laufwerke bis hin zum Laufwerksbuchstaben 'Z:' als Netzwerklaufwerke zur Verfügung stehen (WnetEnumResource).
Die Schadensroutine des Virus ist solange aktiv, wie auch der Virus selbst im Speicher ist.
Der Virus kann jedoch recht einfach durch Löschen der infektiösen Dateien und Modifizieren der WIN.INI bzw. Registry entfernt werden.

Entfernen der Autostart-Einträge unter Windows 9x:
Entfernen aus der WIN.INI (mittels SysEdit) durch Löschen folgender Zeile:
```
run=C:\WINDOWS\SYSTEM\Explore.exe
(run=%windir%\SYSTEM\Explore.exe)
```
oder
```
run=C:\WINDOWS\SYSTEM\_setup.exe
(run=%windir\SYSTEM\_setup.exe)
```

Entfernen der Autostart-Einträge unter Windows NT:
Entfernen eines Keys aus folgendem Registry-Pfad (mittels RegEdit):
```
HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows
```
Hier muß unter \Run folgender Eintrag gelöscht werden:
```
run=C:\\WINNT\\SYSTEM32\\Explore.exe
(run=%windir%\\SYSTEM32\\Explore.exe)
```
bzw.
```
run=C:\\WINNT\\SYSTEM32\\_setup.exe
(run=%windir%\\SYSTEM32\\_setup.exe
```

Entfernen der infizierten Datei unter Windows 9x:
Nach einem Neustart oder einem "Abschießen" des Virus über den Taskmanager sollte der Virus selbst gelöscht werden. Die Datei befindet sich unter dem Namen 'Explore.exe' oder '_setup.exe' unter:
c:\windows\system\Explore.exe
bzw.
c:\windows\system_setup.exe

Entfernen der infizierten Datei unter Windows NT:
Die Pfade für Windows NT sind (nach Neustart oder 'Abschießen'):
c:\winnt\system32\Explore.exe
bzw.
c:\winnt\system32_setup.exe

Es kann daher nicht oft genug vor E-Mails mit unbekannten Dateianhängen gewarnt werden. Es ist auch eher unüblich, daß Dokumente als selbstextrahierende .EXE-Dateien versandt werden. Anwender sollten mit geeigneten Antivirenprogrammen - auch zur Vorsorge - einmal alle Dateien eines Rechnersystemes untersuchen. Es werden dann auch die temporären Dateien der diversen E-Mailprogramme untersucht und die darin gespeicherten Viren ggf. entdeckt.
Darüber hinaus zeigt dieser Virus mit seinem agressiven Schadensteil wieder einmal deutlich, wie durch sinnvolle Rechtevergabe in Netzwerken die Schäden hätten begrenzt werden können.

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

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.

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

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

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.

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

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 Schädlinge werden ständig geändert und als 'neue' Schädlinge von zweifelhaften Zeitgenossen wieder auf die Menschheit losgelassen.

Ghost
Hafenstraße
Hallöchen
HONNECKER Trojan (Trojanisches Pferd)
Icelandic
Israel
Itavir
IWorm.BleBla
Jack Ripper (Bootsektorvirus)
Jerusalem
Joshi (Bootsektorvirus)
Junkie
Kennedy
Keypress
Kiev (Bootsektorvirus)
Kit/VBSWormGen.150
Lehigh
Liberty
Lisbon
Macho
Michelangelo (Bootsektorvirus)
MIX
Mummy
Murphy
Music Bug (Bootsektorvirus)
MVF
Natas
Navidad
Neuroquila
Neuroquila.N8FALL.A
Neuroquila.N8FALL.B
Neuroquila.N8FALL.Companion
No Bock
O97M/Cybernet.A
Ohio (Bootsektorvirus)
Omega
One Half
Oropax
Parity (Bootsektorvirus)
PDF/Peach
Perfume
Ping Pong (Bootsektorvirus)
Plastique
RedX
Sampo (Bootsektorvirus)
Silly Willy
Solano
SONIC
Stimulation
Stoned (Bootsektorvirus)
SubSeven Version 2.13
Sunday Virus
Sylvia
Tai Pan
Taiwan
Tenbytes

Tequila
TR.Sub7
Traceback
Tremor
Tumen 0.5
Typo COM
V163
Vacsina
VBS.Elva
VBS.Fireburn
VBS.Guorm
VBS.HappyTime
VBS.LiveStages.A
VBS.LoveLetter
VBS.LoveLetter.BD
VBS.LoveLetter.CM
VBS.NEWLOVE
VBS/Caroline.B
VBS/HomePage.1
VBS/Lee-ATX
VBS/NeueTarife
VBS/SST.A
VBS/Staple.A
VBS/Vierika
VGen
Victor
Vienna
Vireninformationen - Inhalt
Vriest
W32.Kriz
W32.TR.Worm/QAZ
W32.Vote
W32/Apost.A
W32/ExploreZip
W32/FBound.C
W32/Klez
W32/Naked
W32/Nimda
W32/Perrum
W32/ProLin@mm
W32/Yaha.E
W32/YAWsetup
W95.Hybris
W95/Begemont.B
W95/CIH
W95/MTX
W97M/Resume.A
Whale
Wiener
WinWord.Concept
WitCode
Worm.Pikachu
Worm/Anset.B
Worm/Aphex
Worm/Badtrans
Worm/Badtrans.B

Worm/Brit.B
Worm/Brit.F
Worm/Calil
Worm/Cervivec
Worm/CodeRed
Worm/Cuervo
Worm/Frethem
Worm/Frethem.J
Worm/Frethem.I
Worm/Gnutella.MG
Worm/Goner
Worm/Kazaa
Worm/Klez.E
Worm/Lee.SP
Worm/Maldal.C
Worm/Maldal.I
Worm/Matcher
Worm/Myba.A
Worm/MyLife.A
Worm/MyLife.B
Worm/MyLife.C
Worm/MyLife.D
Worm/MyLife.E
Worm/MyLife.F
Worm/MyLife.G
Worm/MyLife.H
Worm/MyLife.I
Worm/MyLife.J
Worm/Paukor
Worm/Tettona
Worm/W32.Sircam
WScr.Kak.Worm
Yankee Doodle
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.

IWorm.BleBla

Der Virus 'BleBla' (auch Romeo & Julia genannt) ist ein Wurm, der sich über das Internet verbreitet. Er verschickt sich per Email mit zwei Attachments (Dateianhängen). Dieser Wurm erweist sich als besonders gefährlich, da er bereits beim Öffnen bzw. durch die Vorschau der Email aktiviert wird und das System infiziert. Für seine Verbreitung setzt der Wurm voraus, dass Windows im Verzeichnis C:\WINDOWS\ installiert ist.

Der Email sind folgende beiden Dateien als Attachments beigefügt: MYJULIET.CHM und MYROMEO.EXE. Beim Öffnen einer infizierten Email wird von Windows automatisch die Datei MYJULIET.CHM ausgeführt, die aus einer komprimierten HTML-Seite besteht. Das Script in dieser HTML-Seite führt dann die Datei MYROMEO.EXE aus.

Die Datei ROMEO.EXE ist der Programmiersprache Delphi programmiert und ist etwa 30Kbyte groß. Dieses Programm öffnet das Adressbuch von Windows, liest dort Email-Adressen aus und versendet sich an diese weiter. Für den Versand nutzt der Wurm sechs polnische SMTP-Server.

Der Betreff solcher Emails lautet folgender Maßen:

```
Romeo&Juliet
where is my Juliet ?
where is my Romeo ?
Re:
hello world
Matrix has you....
I LOVE YOU :)
from shake-beer
my picture
ble bla, bee
merry christmas
surprise !
Caution: NEW VIRUS !
newborn
hi
last wish ???
lol :)
scandal !
^_^
!!!
,,....´
!!??!?!?
```

Eine Variante des Wurmes verändert die Registry-Einträge. Die ROMEO.EXE kopiert sich nach \ WINDOWS\SYSRNJ.EXE und verändert die Einträge in der Registry-Datei.

Es werden folgender Eintrag erstellt:

```
HKEY_CLASSES_ROOT\rnjfile
\DefaultIcon =%1
\shell\open\command =sysrnj.exe "%1" %*
```

und folgende Einträge geändert:

```
\.exe =rnjfile
```

```
\.jpg = rnjfile
\.jpeg = rnjfile
\.jpe = rnjfile
\.reg = rnjfile
\.arj = rnjfile
\.bmp = rnjfile
\.lha = rnjfile
\.rar = rnjfile
\.gif = rnjfile
\.avi = rnjfile
\.zip = rnjfile
\.mpg = rnjfile
\.mpeg = rnjfile
\.xls = rnjfile
\.doc = rnjfile
\.vqf = rnjfile
\.mp2 = rnjfile
\.mp3 = rnjfile
\.wmf = rnjfile
\.wma = rnjfile
\.wmv = rnjfile
```

Durch diese Einträge wird der Wurm jedesmal gestartet, wenn eine Datei mit einer entsprechenden Endung aufgerufen wird.

'IWorm.BleBla' nutzt eine Sicherheitslücke des Windows Scripting Host: eine Email mit entsprechendem Inhalt wird automatisch ausgeführt. Um diese Sicherheitslücke zu schließen bietet Microsoft ab sofort ein Patch auf folgender Internetseite an:

http://www.microsoft.com/technet/security/bulletin/ms00-037.asp

Und so entfernen Sie den Virus:

Löschen Sie zuallererst die infizierten Emails aus ihren Postfächern.

Laden Sie bitte anschließend den von uns bereitgestellten Registry-Key bb_key.reg zum Wiederherstellen ihres Systems herunter. Wechseln Sie nun in den MS-DOS-Modus und geben Sie folgenden Befehl ein:

```
regedit %Pathname%\bb_key.reg
```

Wobei %Pathname% für den Pfad steht, wo Sie die Datei bb_key.reg abgespeichert haben (es empfiehlt sich diese Datei z.B. in "C:\" oder "C:\temp" abzuspeichern).

Starten Sie nun Windows erneut und löschen Sie den Eintrag in der Registry mit dem Programm "regedit":
`HKEY_CLASSES_ROOT\RNJFILE`

Um den Internet-Wurm 'IWorm.BleBla' nun endgültig von ihrem Computersystem zu entfernen, löschen Sie die beiden Dateien MYJULIET.CHM und MYROMEO.EXE sowie die Datei SYSRNJ.EXE aus dem Windows-Verzeichnis.

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 bei 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 schaut 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.

Kit/VBSWormGen.150

Mit dem VBS Wurm-Generator 1.5 können sehr einfach Internetwürmer erzeugt werden. Dieses Programm wurde bekannt durch den Virus VBS/SST.A (alias VBS.AnnaKournikova.jpg oder VBS/OnTheFly), der sich innerhalb weniger Stunden auf viele Rechnersysteme verbreitet hat.

Mit Hilfe weniger Mausklicks können über den Wurm-Generator Optionen ausgewählt werden, durch die verschiedene Schadensroutinen ausgeführt werden können. Zum Ausführen des Programmes selbst müssen auf dem Rechnersystem Visual Basic 5 Laufzeitbibliotheken installiert sein. Auf den Zielsystemen muß, wie bisher auch, der Windows Scripting Host (WSH), der standardmäßig beim Internet Explorer 5 dabei ist, installiert sein.

Abarten:

VBS/SST	alias VBS.AnnaKournikova.jpg.vbs
VBS/NeueTarife	alias VBS.VBSWG.K@MM
VBS/PicaWorm	

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.

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.

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.

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 Bytes 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.

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.

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

Navidad

Der Internetwurm TR.Worm.Navidad wird als Attachment (Dateianhang) über Emails von einem verseuchten Computer versendet. Das Attachment hat den Namen NAVIDAD.EXE. Aufgrund eines Programmierfehlers können nach seiner Aktivierung keine Anwendungen mit der Endung .EXE mehr ausgeführt werden.

Seit Januar 2001 gibt eine neue Variante von Navidad, die von AntiVir als W32.Navidad.B erkannt wird. Er hat die gleiche Schadensroutine wie sein Vorgänger, ist aber in seinem Aussehen unterschiedlich. Anstatt des Augensymbols in der Taskleiste bspw. zeigt diese Variante ein Blumensymbol.

Wenn sie die NAVIDAD.EXE ausgeführt haben, bekommen Sie folgende falsche Fehlermeldung zu sehen:

Während die vermeintliche Fehlermeldung erscheint, erstellt der Internetwurm im Verzeichnis %WINDOWS%\SYSTEM\ die Datei WINSVRC.VXD und verändert in der Registry die Standardeinträge für .EXE - Dateien um:

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
C:\WINDOWS\SYSTEM\winsvrc.exe "%1" %*"
```

Damit sollte der Wurm jedes Mal ausgeführt werden, wenn eine .EXE Datei geöffnet wird. Hier ist dem Programmierer aber ein Fehler unterlaufen, da die WINSVRC als .VXD und nicht als .EXE angelegt wurde. Aus diesem Grund lassen sich anschließend keine Anwendungen mit der Endung .EXE mehr ausführen.

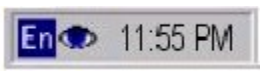
Desweiteren fügt er einen Eintrag in der Registry ein, um bei jedem Windows-Start ausgeführt zu werden (aber auch hier wieder der gleiche Fehler wie oben):

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Win32BaseServiceMOD = C:\%ROOT%\System\winsvrc.exe
```

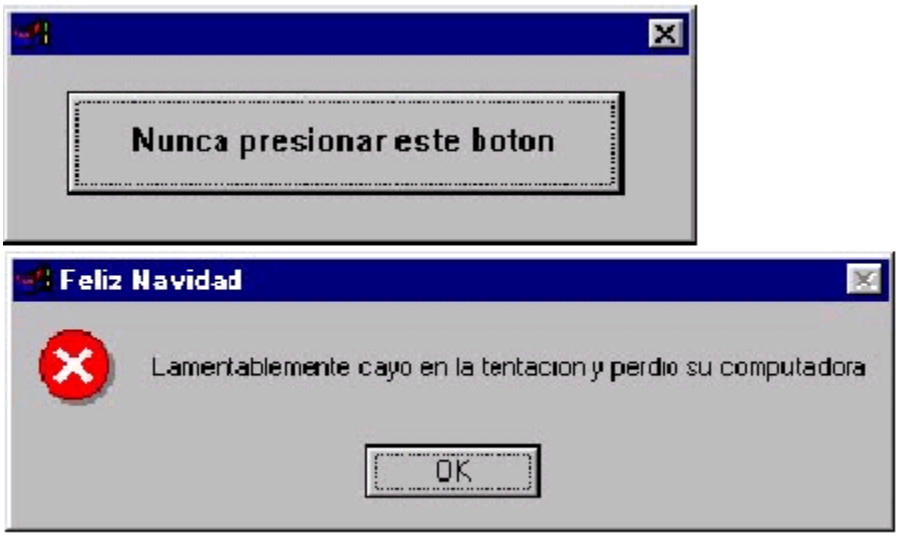
Als letztes trägt sich der Internetwurm noch in dem folgenden Registry-Key ein:

```
[HKEY_CURRENT_USER\Software\Navidad]
```

Nachdem Sie nun den "OK" Button gedrückt haben erscheint ein "Auge" in Windows Taskbar, das dann folgendermaßen aussieht:



Jetzt sehen Sie, dass der Internetwurm ihr System infiziert hat. Wenn Sie das Auge in der Windows Taskbar angeklickt haben kommen die zwei folgenden Meldungen, die Sie dann mit "OK" bestätigen können.



Wenn Sie nun einen MAPI-fähigen Email-Client (benötigt die MAPI32.DLL) im Einsatz haben, infiziert der Internetwurm die ungelesenen Emails, indem er die Datei NAVIDAD.EXE anhängt und die Email wird an den jeweiligen Absender zurückgeschickt.

Entfernung

Als erstes korrigieren Sie bitte den Eintrag, der für das Ausführen von .EXE Dateien zuständig ist. Dazu führen sie bitte die von uns bergeitgestellte Datei shell_op.reg aus. Anschließend öffnen Sie den Taskmanager und löschen dort die aktiven Tasks des Wurmes (NAVIDAD oder WINSVRC). Danach löschen Sie bitte die Dateien NAVIDAD.EXE sowie WINSVRC.VXD. Als letztes sollten noch die vom Wurm angelegten Registryeinträge entfernt werden.

Entfernung (Variante W32.Navidad.B)

Zur Entfernung dieser Variante müssen Sie ebenfalls die shell_op.reg (s. oben) von unserer Seite downloaden. Nun starten Sie bitte von einer Systemdiskette und löschen die Datei WINTASK.EXE im WINDOWS\SYSTEM\ Verzeichnis. Danach rufen Sie das Programm REGEDIT unter DOS auf und geben als Parameter den Dateinamen mit Pfadangabe an (z.B. REGEDIT A:\SHELL_OP.REG). Nun können Sie Windows wieder starten und zusätzlich noch den RUN Eintrag der WINTASK.EXE in der REGISTRY löschen (`HKLM\Software\Microsoft\Windows\CurrentVersion\Run`).

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.

O97M/Cybernet.A

Dieser Makrovirus infiziert Word- und Excel Dokumente gleichermaßen. Er infiziert die Datei "Normal.dot", die bei jedem Start eines Word-Dokuments von Word selbst mitgeladen wird. Außerdem setzt er die Sicherheitseinstellungen von MS Word und MS Excel auf niedrig. Danach erstellt er im Excel Startverzeichnis "C:\Programme\Microsoft Office\Office\XLStart" die Datei "CyberNet.xls". Er versendet sich über MS Outlook an die ersten 50 Einträge im Adressbuch. Die Email sieht so aus:

Von:
<"Name des infizierten Nutzers">

An:
<"Name aus dem Adressbuch">

Betreff:
You´ve GOT Mail

Body: Please, saved the document after you read and don´t show to anyone else. The document is also VIRUS FREE... so DISREGARD the Virus protection warning!!!

Wird der Virus am 17.August oder 25.Dezember ausgeführt, richtet er erheblichen Schaden auf dem Rechnersystem an. In aktiven Word-Dokumenten werden zufällig gewählte Figuren eingefügt. In aktiven Excel-Dokumenten wird eine zufällige Anzahl von Kommentaren eingefügt. Diese beinhalten alle "c 2000 - CyberNet From Indonesia". Der Virus ändert die "Autoexec.bat" so ab, dass beim Aufruf die Festplatte "C" formatiert wird. Außerdem wird folgender Kommentar eingefügt:

```
#########################################################
# Vine...Vide...Vice...Moslem Power Never End...                              #
# I´m Really Sorry, This System Have Been Recycled BY-=CyberNET=-Virus!!!   #
# Brought To You From Indonesia...                                              #
#########################################################
```

Danach erscheint eine Warnmeldung auf dem Bildschirm:

Assalamualaikum Li Kulli Muslim...Moslem Power Never End...
Nothing Can Stop << CyberNET >> Virus. Your System Has Already Infected !!!
Now...I Am Outta Here...
Wenn hier auf "OK" geklickt wird startet Windows neu.

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.

PDF/Peach

Mit dem PDF/Peach ist das der erste Virus, der eine PDF-Datei als Verbreitung nutzt. Er versendet sich als Email über Outlook mit Hilfe des Outlook Adressbuchs an die ersten 100 Mailempfänger.

Der Betreff und Text der empfangenen Email hat ein unterschiedliches aussehen:

Betreff:
"FW: You have one Minute to find the peach"

oder

"FW: Find the peach"

oder

"FW: Find"

oder

"FW: Peach"

oder

"FW: Joke"

Text:
">Try finding the peach"

oder

">Try this"

oder

">Interesting search"

oder

">I don´t usually send this things, but.."

und als Abschluss: "!" oder ":-)" oder ":)" oder "=)" oder ":-]"

Attachment:
find.pdf , peach.pdf , find the peach.pdf , find_the_peach.pdf , joke.pdf oder search.pdf

Damit der Virus sich verbreiten kann, müssen Sie allerdings Adobe Acrobat installiert haben. Sollten Sie die Freeware Version, den Acrobat Reader, installiert haben, kann PDF/Peach seinen virulenten Code nicht installieren.
Wird nun die PDF-Datei des Attachments geöffnet, wird ein Bild gezeigt mit "You have one minute to find the peach!" als Überschrift. Darunter ist eine Grafik mit kleinen Bildern, die nackte Hintern zeigen.

Neben dem Bild steht eine Aufforderung, nach der man mit einem Doppelklick auf das Bild machen soll. Tut man dies, aktiviert sich der Wurm PDF/Peach, indem er seine virulente Dateien startet, welcher er folgend in den TEMP-Ordner des Windowsverzeichnisses installiert hat:

```
Peach.vbs
Peach.vbe
Peach.wsf
Peach.jpg
```

Danach versendet sich der Wurm über Outlook mit Hilfe des Adressbuches.
Wenn er sich versandt hat, erstellt er folgenden Eintrag in der Registry, der zufolge hat, dass er sich nicht noch einmal versenden kann:

```
HKLM\Software\OUTLOOK.PDFWorm "Version 1.0 By Zulu"
```

Zuletzt löscht er seine Dateien, welche er im TEMP Verzeichnis abgelegt hat.

PDF/Peach ist ein reiner Massenmailer und hat weiter keine Schadensroutinen.

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.

SONIC

Der neue Email-Wurm "Sonic" ist ein sogenannter "Mehrkomponenten-Infektor": Dieser Virus kann, sobald er erfolgreich infizieren konnte, beliebig weitere Komponenten aus dem Internet "nachladen" und somit fast uneingeschränkte Funktionen "updaten". Es ist möglich, daß die Erstinfektion nur mit einer Komponente des Virus, dem "Loader", stattfindet. Dieser lädt dann die restlichen Komponenten des Virus aus dem Internet auf den infizierten Rechner herunter.

Der Sonic-Wurm ist bei seiner Infektion vielseitig: Er infiziert sowohl Systeme unter Windows 95/98/ME als auch unter Windows NT/2000.

Nach Aufruf der EXE-Datei (die etwa die Größe von 25kb besitzt) schreibt sich der Virus in den Arbeitsspeicher und bleibt im Hintergrund aktiv. Damit ihm dies auch nach einem Neustart des Systems möglich ist, kopiert er sich nach C:\%WinSystem% und trägt sich in die Registry unter folgendem Key ein:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
GDI =% WinSystem%\GDI32.EXE
```

Bei % WinSystem% handelt es sich um das Windows-Systemverzeichnis.

Um seine Aktivität zu vertuschen, zeigt der Virus nach dem Aufruf eine von ihm generierte Fehlermeldung an.

Der Pfad vor dem Dateinamen hängt davon ab, von welchem Verzeichnis der Virus aufgerufen wird.

Danach versucht der Virus mehrere Dateien von einer Geocities-Seite herunterzuladen. Nach einem erfolgreichen Download setzt der Virus seine "Arbeit" auf dem Computer fort: "Sonic" versucht dann, infizierte Emails via Email-Adressbuch zu versenden. Gelingt ihm das, sehen diese Emails wie folgt aus:

Subjekt:
`Choose your poison`

Attachment:
`GIRLS.EXE`

Eine andere Variante des Virus verbreitet sich unter diesen Angaben:

Subjekt:
`I’m your poison`

Attachment:
`LOVERS.EXE`

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.

SubSeven Version 2.13

Alias: Zeckentod.exe

Ein neuerer Fall geisterte als "Zeckentod" durch die Presse. Eine Server-Datei des Spionageprogrammes SubSeven wird unter dem Namen "Zeckentod.exe" verbreitet. Mit Hilfe dieser Datei können Daten unverlangterweise ins Internet verschickt werden.

Einer Email mit dem Betreff "Zeckentod - das Programm zum Abschießen "linker" Homepages" ist ein Attachment beigefügt. Das Attachment selbst ist diese Serverdatei. Die Email wurde von dem Absender SaargauKameraden@hotmail.com verschickt.

Dieses Backdoorprogramm kann von AntiVir aufgespürt und entfernt werden. Es existiert auch eine defekte Version dieser Serverdatei. Sie ist nur 220409 Bytes groß, diese 220409 Bytes sind allerdings mit dem Original identisch. Bei der "zu kurzen" Datei kommt eine Meldungsbox (wohl vom UPX-Entpacker) mit der Titelleiste "Error starting program" und dem Inhalt "filename.exe file appears to be corrupt. Reinstall the file and then try again". Nach Betätigen der OK-Taste kommt eine Windows-Meldung "Windows cannot run this program because it is in an invalid format" bzw. dessen deutsches Äquivalent. Diese zu kurze Datei wird also nicht richtig ausgeführt.

Bei einer Infektion mit dieser SubSeven-Variante wird eine Datei mit einem zufällig gewähltem Dateinamen im Windows-Verzeichnis erzeugt. Hinter diesem Namen verbirgt sich der Server des Spionageprogrammes. Dieses Serverprogramm lässt sich nicht mehr einfach löschen, da sonst keine Anwendungen (*.exe) mehr ausgeführt werden können. Nach Löschen des Servers lässt sich ggf. auch Windows nicht mehr vollständig starten. Deshalb gestaltet sich die Entfernung des SubSeven etwas schwieriger, sofern AntiVir diesen nicht schon beim Systemcheck eliminiert und in der Registry aufgeräumt hat.

Entfernung:

Notieren Sie bitte zuerst die entsprechenden Einträge (mit dem Key WinLoader) in der Registry unter:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
```

In beide Äste trägt sich der Server unter dem Key "WinLoader" ein. Bitte notieren Sie sich den auf den Key "WinLoader" folgenden Dateinamen und entfernen Sie diese Einträge. Ebenso die Einträge in der Win.ini unter "load=" oder "run=" sowie in der System.ini hinter shell=Explorer.exe. Auch hier ist der gesuchte Dateiname der auf den Key "WinLoader" in der Registry folgende Dateiname. Entfernen Sie dann diese Einträge.

Jetzt muss noch folgender Eintrag in der Registry kontrolliert werden:

```
HKEY_CLASSES_ROOT\exefile\shell\open\command
```

Der Wert sollte "%1" %* (Standardwert) sein. Ist davor noch ein Eintrag mit dem auf den Key "WinLoader" in der Registry folgenden Dateinamen, dann notieren Sie den Dateinamen und setzen den Eintrag auf den Standardwert "%1" %* zurück.

Starten Sie danach Windows neu und löschen im Windows-Verzeichnis die notierte Datei (der auf den Key "WinLoader" in der Registry folgende Dateiname). Zum Schluss muss noch der Server (die Datei mit dem notierten Dateinamen) aus dem Windows-Verzeichnis gelöscht werden.

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!"

WARNUNG!!

Jede Änderung in der Registry-Datei kann dazu führen, dass sich Anwendungen oder Teile des Betriebssystemes nicht mehr starten lassen. Überlassen Sie Änderungen in dieser Datei ausschließlich Fachleuten. Um wieder auf die Daten der alten Registry-Datei zurückgreifen zu können, sollten Sie diese Datei vor einer Änderung unter einem anderen Namen (z. B. REGISTRY.ALT) abspeichern.

Bei SubSeven handelt es sich um ein Backdoor-Programm (wie z.B. NetBus, Back Orifice etc.), welches einem Hacker ermöglicht, auf ein fremdes System zuzugreifen. Das Programm besteht aus einem Server- und einem Client-Programm welches zur Fernbedienung von Rechnern in einem Netzwerk eingesetzt werden kann. Mit Hilfe des Client kann ein Hacker in ein mit dem Server (dies ist der eigentliche Trojaner) infiziertes System eindringen. Bei den neueren Versionen von SubSeven wird auch immer noch ein Editserver mitgeliefert, mit dessen Hilfe sich viele unterschiedliche Einstellungen am Server vornehmen lassen.

Ein System, das mit SubSeven befallen ist, kann mit Hilfe des Client also vollständig kontrolliert werden. Zur Zeit sind folgende Versionen von SubSeven bekannt:

1. SubSeven Version 1.0 - 1.4

Nach dem Aufruf des Servers auf einem System kopiert sich dieser in den Windows-Ordner. Damit er bei jedem Systemstart in den Speicher geladen wird, trägt er sich in die win.ini und in die Registry ein.

Der Eintrag in der Registry wird unter folgendem Pfad erstellt:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\`

In der WIN.INI ist der Eintrag unter "load=" oder "run=" zu finden.

Leider ist der Name, mit der sich der Server in den Windows-Ordner kopiert, nicht einheitlich, bei Version 1.0-1.4 lautet er aber meist "Systrayicon.exe", "window.exe" oder "nodll.exe"

Entfernung

Löschen Sie bitte zuerst den Eintrag in der Registry
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\`
und soweit vorhanden den Eintrag in der Win.ini unter "load=" oder "run=". Starten Sie danach Windows neu und löschen anschließend die Datei "Systrayicon.exe", "window.exe" oder "nodll.exe" aus dem Windows-Verzeichnis.

2. SubSeven Version 1.5

Subseven Version 1.5 nutzt für die Autostartfunktion nur die Datei Win.ini aus. Der Eintrag ist unter "run=" zu finden.

Entfernung

Löschen Sie bitte zuerst den Eintrag "run=kerne132.dl nodll" aus der Win.ini und starten danach Windows neu. Löschen Sie anschließend die Trojaner-Dateien "window.exe", "nodll.exe" und "winduh.dat" aus dem Windows-Verzeichnis.

3. SubSeven Version 1.6

SubSeven Version 1.6 nutzt für die Autostartfunktion nur die Registry aus. Der Eintrag ist unter `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices` zu finden und lautet "Kernel16".

Entfernung

Löschen Sie bitte zuerst den oben genannten Eintrag in der Registry und starten danach Windows neu. Löschen Sie anschließend die Dateien "SysTray.exe", "imdrki_33.dll", "pddt.dat" und rundll16.com" im Windows-Systemverzeichnis (meist c:\windows\system).

4. SubSeven Version 1.7

Bei SubSeven Version 1.7 wird zum ersten mal ein "Editserver" mitgeliefert, welcher die Entfernung etwas erschwert, da der Hacker den Server leicht verändern kann.

Entfernung

Löschen Sie bitte zuerst den Eintrag "Kernel16" unter `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices` aus der Registry und starten Sie danach Windows neu. Anschließend müssen noch die Dateien "kernel16.dl" im Windows-Verzeichnis und "watching.dll" im Windows-Systemverzeichnis (meist c:\ windows\system) gelöscht werden.

5. SubSeven Version 1.8

Die Version 1.8 enthält einen weiterentwickelten "Editserver ", der dem Hacker noch weitere Einstellungsmöglichkeiten bietet. So kann zum Beispiel der Name oder auch die Infizierungsart frei gewählt werden. Bei der Infizierung gibt es 4 verschiedene Möglichkeiten:

1. System.ini

2. Win.ini

3. Registry-Run

4. Registry-RunServices

Entfernung

Da immer nur eine der vier oben genannten Infizierungsmöglichkeiten zutrifft, muss zuerst der verwendete Eintrag gesucht werden, d.h. nur einer der vier möglichen Einträge wird tatsächlich genutzt.

Sie müssen also entweder

1. den Eintrag "shell=Explorer.exe kerne132.dl" in der System.ini ändern in "shell=Explorer.exe",

2. den Eintrag "run=kerne132.dl" aus der Win.ini löschen,

3. Den Registry-Key "Kernel32" (evtl. ist hier ein abweichender Name angegeben, den Sie sich notieren sollten) unter dem Pfad
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
   entfernen oder

4. den Registry-Key "Kernel32" (evtl. weicht auch hier der Name ab) unter dem Pfad
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices`
   entfernen.

Starten Sie danach den Computer neu und löschen die Dateien "kerne132.dl" im Windows-Verzeichnis und "MVOKH_32.dll" im Windows-Systemverzeichnis. Haben Sie bei der Variante c) oder d) festgestellt, dass die Datei "kerne132.dl" einen anderen Namen besitzt (da im Editserver jeder Name eingestellt werden kann) muss die Datei mit dem geänderten Namen gelöscht werden.

6. SubSeven Version 1.9 und SubSeven Apocalypse

Diese Versionen ähneln der Version 1.8, nur der Dateiname, mit dem sich der Server im Originalzustand kopiert, hat sich verändert. Daher gibt es ebenfalls 4 verschiedene Infizierungsmöglichkeiten:

1. System.ini

2. Win.ini

3. Registry-Run

4. Registry-RunServices

Entfernung

Da wiederum nur eine der vier oben genannten Infizierungsmöglichkeiten zutrifft, muss zuerst der verwendete Eintrag gesucht werden, d.h. nur einer der vier Einträge wird tatsächlich genutzt.

Sie müssen also entweder

1. den Eintrag "shell=Explorer.exe mtmtask.dl" in der System.ini ändern in "shell=Explorer.exe"

2. den Eintrag "run= mtmtask.dl" aus der Win.ini löschen

3. den Registry-Key "Kernel32" (evtl. ist hier ein abweichender Name angegeben, den Sie sich notieren sollten) unter dem Pfad
`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
entfernen.

4. den Registry-Key "Kernel32" (evtl. weicht auch hier der Name ab) unter dem Pfad
`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices`
entfernen.

Starten Sie danach den Computer neu und löschen die Dateien "mtmtask.dl" im Windows-Verzeichnis. Haben Sie bei der Variante c) oder d) festgestellt, dass die Datei "mtmtask.dl" einen anderen Namen besitzt (da im Editserver jeder Name eingestellt werden kann) muss die Datei mit dem geänderten Namen gelöscht werden.

7. SubSeven Version 2.0 - 2.2

Bei einer Infizierung mit dieser Variante ist meistens eine Datei namens MSREXE.exe im Windows-Verzeichnis vorhanden. Hinter diesem Namen verbirgt sich der Server des Virus. Jedoch ist auch jeder andere Name möglich. Neu ab der Version 2.0 ist, dass sich der Server nicht mehr einfach löschen lässt, da sonst keine Anwendungen (*.exe) mehr ausgeführt werden können. Nach Löschen des Servers lässt sich ggf. auch Windows nicht mehr vollständig starten. Deshalb gestaltet sich die Entfernung des SubSeven etwas schwieriger.

Entfernung

Entfernen Sie bitte zuerst die entsprechenden Einträge in der Registry unter:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
```

Bitte notieren Sie sich die Einträge in der Win.ini unter "load=" oder "run=" sowie in der System.ini hinter shell=Explorer.exe (in der Regel MSREXE.exe) und entfernen dann diese Einträge.

Jetzt muss noch folgender Eintrag in der Registry kontrolliert werden:

```
HKEY_CLASSES_ROOT\exefile\shell\open\command
```

Der Wert muss "%1" %* (Standardwert) sein. Ist davor noch ein Eintrag "Windos.exe", "run.exe" oder eine andere ausführbare Datei angegeben, notieren Sie den Namen und setzen den Eintrag auf den Standardwert "%1" %* zurück.

Starten Sie danach Windows neu und löschen im Windows-Verzeichnis die Datei "Windos.exe", "run.exe" bzw. die Datei mit dem Namen, auf welchen der Registry-Eintrag verwiesen hat.

Zum Schluss muss noch der Server (in der Regel MSREXE.exe) aus dem Windows-Verzeichnis gelöscht werden.

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.

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.

Vacsina 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.

VBS.Elva

Dieser Email-Wurm versendet sich genau wie sein berühmter Vorgänger "Loveletter" via MS Outlook. Alle im Adressbuch eingetragenen Kontakte erhalten eine Email.

Subject:
`BIRTHDAY CARD !!!`

Body:
```
Hello Jo,
Happy birthday ELVA forever.
This I made birthday card for you.
Please open it and I hope you like.
```

Attachment:
`CARD.HTA`

Wird die als Attachment beigefügte Datei CARD.HTA ausgeführt, geschieht folgendes:

1. Der Virus erzeugt im Verzeichnis C:\WINDOWS\ die Datei FS.VBE und kopiert diese dann nach C:\WINDOWS\SYSTEM\FS.VBS.

2. Folgende Registry-Einträge werden erzeugt:

   * `HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\FS "C:\WINDOWS\SYSTEM\FS.VBS"`
     Der Virus wird bei jedem Systemstart mitgeladen.
   * `HKCU\Software\Microsoft\Office\9.0\Word\Security\Level "1"`
     Die Sicherheitseinstellung von Word 9 wird auf "niedrig" gesetzt.
   * `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1201 "0"`
     Auf dem lokalen Rechner darf der im Moment angemeldete Benutzer ActiveX Steuerelemente ausführen, die nicht sicher sind.
   * `HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1201 "0"`
     Auf dem lokalen Rechner dürfen ActiveX Steuerelemente ausgeführt werden, die nicht sicher sind.
   * `HKLM\Software\Microsoft\FSD; HKLM\Software\Microsoft\FSW`
     Hier wird der aktuelle Tag gespeichert.
   * `HKLM\Software\Microsoft\FSH; HKLM\Software\Microsoft\FSV`
     Der gesamte Code des Virus wird hier gespeichert.

3. Es wird die Datei CARD.HTA angelegt und diese dann an alle Einträge im MS Outlook Adressbuch verschickt.

4. Die Internetadresse "http://www.jasonnet.cc/elva" wird unter dem Namen "Elva's Page" zu den Favoriten hinzugefügt.

5. Der Wurm sucht nach allen VBS-Dateien und ersetzt deren Code mit seinem eigenen.

6. Außerdem werden folgende Dateitypen mit dem Windows Skripting Host verknüpft:
   *.JS; *.JSE; *.GIF; *.JPG; *.MP3; *.WSH; *.WSF; *.WSC; *.SHS; *.SCT. Diese Dateien werden jetzt genauso wie eine *.vbs Datei ausgeführt.

7. Die globale Vorlage von Word wird von dem Virus infiziert. Ein kleiner Fehler im Virus verhindert,

daß weitere Word Dokumente infiziert werden. Es ist jedoch zu erwarten, daß neue Varianten auftauchen, in denen der Fehler behoben ist.

8. Es erscheint ein Fenster mit dem Inahlt "Happy Birthday".

9. Drei Tage nachdem der Virus zum erstem mal gestartet wurde, scannt er die gesamte Festplatte. Findet er Dateien mit folgenden Endungen: *.JS; *.JSE; *.GIF; *.JPG; *.MP3; *.WSH; *.WSF; *.WSC; *.SHS; *.SCT, wird deren Inhalt mit dem Viruscode überschrieben.

10. Am 24.8 eines jeden Jahres wird folgende Meldung am Bildschirm ausgegeben: "-=Happy Birthday=- I love ELVA 4 ever".

VBS.Fireburn

Der neue Email-Wurm Fireburn versendet sich wie seine beiden Vorgänger "ILOVEYOU" und "NewLove" via Outlook. Seine Schadensfunktion startet am 20. Juni eines jeden Jahres.

Der Wurm versendet sich an alle Einträge im Adressbuch von OutLook. Dabei erstellt er nicht für jede Person eine eigene Email, sondern er trägt alle Kontakte in eine einzige Email als "Blind Carbon Copy" (BCC) ein. Außerdem kopiert er sich selbst nach c:\windows\rundll32.vbs.

Wird das infektiöse Attachment auf einem deutschen Rechnersystem ausgeführt, so wird auch eine Email mit deutschem Text versendet. Diese könnte so aussehen:

Subject:
```
Moin, alles klar?
```

Body:
```
Hi, wie geht's dir?
Guck dir mal das Photo im Anhang an, ist echt geil ;)
bye bis dann..
```

Attachment:
```
Ultra-Hardcore-Bondage.JPG.vbs
```

Wird der Virus auf einem englischem Rechnersystem ausgeführt, sieht die Email so aus:

Subject:
```
Hi, how are you?
```

Body:
```
Hi, look at that nice Pic attached !
Watching it is a must ;)
cu later ...
```

Attachment:
```
Christina__NUDE!!!.JPG.vbs
```

Der Anhang der Email kann folgende 8 Dateinamen haben:

```
"Ultra-Hardcore-Bondage.JPG.vbs"
"Christina__NUDE!!!.JPG.vbs"
"CuteJany__BigTits!.GIF.vbs"
"MyGirlfriend__NUDE!.JPG.vbs"
"Aguiliera__NUDE!!.JPG.vbs"
"!Jany__Gets-fucked!.GIF.vbs"
"cute__EmmaPeel!!!.JPG.vbs"
"Julie17__xxx.GIF.vbs"
```

Windows wird auf den Namen FireburN registriert. Dies kann man nachprüfen, indem man auf "START" -> "Einstellungen" -> "Systemsteuerung" -> "System" geht.

Ist das Chatprogramm mIRC in einem der folgenden zwei Pfade installiert, so wird eine eventuell

vorhandene "script.ini" überschrieben:

Pfad 1: C:\Programme\mirc
Pfad 2: C:\mirc

Die neue "script.ini" versendet die im c:\windows erstellte rundll32.vbs an alle anderen Personen im IRC Chat.

Der Wurm trägt sich auch unter folgendem Schlüssel in die Registry ein:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
MSrundll32=rundll32.vbs
```

Am 20. Juni aktiviert er seine Schadensfunktion. Folgende Meldung wird auf dem Bildschirm ausgegeben: "I'm proud to say that you are infected by FireburN!"

Danach werden Maus und Tastatur deaktiviert. Dies kann auch nicht durch ein zurückstellen des Datums wieder rückgängig gemacht werden. Die Registryschlüssel für die Deaktivierung von Tastatur und Maus lauten:

1. `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Shut_Up rundll32 mouse,disable`

2. `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Shut_Up2 rundll32 keyboard,disable`

VBS.Guorm

Dieser Virus nützt wieder einmal die Möglichkeiten der Visual Basic Scriptsprache (VBS). Doch Vorsicht! Obwohl der Virus in VB-Skript realisiert wurde, ist er als Dropper als Makrovirus in Microsoft Word Dokumenten zu finden. Beim Öffnen eines infizierten Dokuments wird er aktiviert und erstellt sich selbst unter dem Dateinamen GuormEx.vbs im Windows-Systemverzeichnis. Anschließend wird diese Datei sofort ausgeführt.

Anmerkung:
Allerdings kann es unter bestimmten Umständen zu einem Absturz von Microsoft Word führen. Für Windows 95- oder Windows 98 Anwender kann dies der Absturz des ganzen Betriebsystems bedeuten. Dafür ist jedoch nicht der Virus verantwortlich.

Dieses VB-Skript vervielfältigt sich selbst nochmals als winuser.dll und user32.dll.vbs in das Windows-Systemverzeichnis. Außerdem sorgt er noch dafür, daß das Skript auch bei jedem Systemstart automatisch aufgerufen wird. Dafür fügt es den Schlüssel user32=wscript.exe <Windows-System-Verzeichnis>\user32.dll.vbs % in den Ast `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` der Registry ein.

Als nächstes überprüft er, ob er sich bereits die Anwender im Outlook-Adressbuch per Email versandt hat. Dies merkt sich der Virus in der Registry in dem Ast `HKCU\software\Guorm`, Platzhalter mailed. Falls nicht, generiert er einen zufälligen Dateinamen aus den Worten links, cool, funny, anti-loveletter, guorm, pot, win2k, icq2k, money, funnypic.jpg, quake, Year2K, Mirc2K, Word2001, FunStuff oder WindowsMe. Auch die Dateinamenserweiterung kann zwischen den Worte .vbs, .vbe, .txt.vbs, .jpg.vbs, .avi.vbs oder .scr.vbs variieren.

Unter diesem Namen verschickt er sich nun an alle Kontakte, die im Adressbuch von Microsoft Outlook eingetragen sind. Allerdings muss hierfür bereits die Version OutLook 2000 installiert sein, damit dem Virus diese Funktionsmerkmale zur Verfügung stehen.

Subject:
```
You know what it is ;-P
```

Body:
```
Check it out!
```

Attachment:
```
funnypic.jpg.jpg.vbs
```

Desweiteren durchsucht der Virus alle Festplatten nach dem Programm mIRC. In jedem Verzeichnis, in dem die Dateien mirc.ini, mirc32.exe oder mlink32.exe , gefunden werden, ersetzt bzw. erstellt er eine Datei script.ini. Dies erfolgt jedoch nur dann, wenn er noch nie danach gesucht hat (der Platzhalter Mirqued im Schlüssel `HKCU\software\Guorm` der Registry existiert nicht). Durch diese Ini-Datei verschickt sich der Virus innerhalb des IRC.

Eine Schadensroutine besitzt der Virus nicht, doch kann er für Administratoren von Email-Servern evtl. Überstunden bedeuten. Fraglich bleibt nur noch, wieso er sich bei jedem Windows-Start ausführen läßt, obwohl er nur einmal aktiv wird.

VBS.HappyTime

HappyTime ist ein VBS Wurm, welcher zwei unterschiedliche Schadensroutinen beinhaltet: er löscht alle .DLL und.EXE Dateien im Windowsverzeichnis und versendet seinen Wurmcode via Outlook oder Outlook Express.

Wird eine infizierte Datei ausgeführt, kopiert sich der Wurm nach

C:\WINDOWS\UNTITLED.HTM

und erstellt im Windowsverzeichnis folgende Dateien, die wiederum den Wurmcode beinhalten:

Help.vbs
Help.hta
Help.htm

Danach erstellt der Wurm im folgenden Registry - Ornder:

```
HKEY_CURRENT_USER\Identities\{96E63FC0-4AAC-11D5-8541-000476177D8E}\Software\
Microsoft\Outlook Express\5.0\Mail\
```

den Eintrag : `Stationery Name = C:\\WINDOWS\\Untitled.htm`

Als nächstes überprüft der Wurm, ob die Summe des Tages und des Monats die Zahl 13 ergibt. Sollte dies der Fall sein, löscht HappyTime alle .EXE und .DLL Dateien im Windowsverzeichnis (einschließlich aller Unterverzeichnisse).

Der Wurm HappyTime beinhaltet weiter einen internen Zähler. Wird der Zählerstand 366 erreicht, versendet sich dieser an alle Emailadressen, welche im Inbox - Ordner von Outlook oder Outlook Express stehen mit folgender Email:

Subject:
`Help`

Attachment:
`Untitled.htm`

oder

Subject:
`Fw: <email des Absenders>`

Attachment:
`Untitled.htm`

Das Attachment UNTITLED.HTM beinhaltet wiederum den Wurmcode.

VBS.LiveStages.A

Dieser Visual Basic-Scriptvirus ist sehr geschickt bei seiner Tarnung. Er liegt im Windows-Format .SHS (Scrap Object) vor. Dieses Dateierweiterung wird nicht von Windows angezeigt - auch wenn explizit alle Dateierweiterungen angezeigt werden sollen. Somit bleibt nur noch der Dateiname LIFE_STAGES.TXT zu sehen. Um seine Funktion nach dem Start nicht aufliegen zu lassen, erzeugt der Virus eine gleichnamige Textdatei im Temp-Verzeichnis und zeigt diese zur Täuschung an. Um das ganze noch zu perfektionieren, wird sogar das standartmäßige Icon der .SHS-Dateien durch das .TXT-Icon ersetzt.

Das eigentliche Einnisten auf dem betroffenen Rechner erfolgt nach einem Neustart des Systemes, da er sich bei seinem ersten Aufruf in den Autostart-Ordner kopiert hat. Weiterhin legt er Kopien von sich selbst an:

* Windows-Verzeichnis
* Als "MSINFO16.TLB" im Windows\System-Verzeichnis
* (Nicht sichtbar) als "MSRCYCLD.DAT" im Papierkorb
* Einem Zufallsnamen aus den Wörtern "IMPORTANT", "INFO", "REPORT", "SECRET" oder "UNKNOWN". Dahinter kann evtl. noch das Zeichen "-" oder "_" angehängt sein inkl. einer Zahl zwischen 1 und 999.
  Die Kopie unter diesem Namen wird in alle Root-Verzeichnisse aller verfügbaren Laufwerken (inkl. Netzwerk), sowie in den Ordner "Eigene Dateien" und in das Verzeichnis "Programme" kopiert.

Nun wird noch eine Datei "SCANREG.VBS" im Windows-Systemverzeichnis erstellt. Diese Datei ist hauptsächlich dafür verantwortlich, fehlende Dateien aus den angelegten Backups wieder zu rekonstruieren. Sie wird bei jedem Systemstart über folgenden Eintrag in der Registry aufgerufen:

* `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\ScanReg=SCANREG.VBS`

Auch von dieser wird eine Kopie unter dem Namen "RCYCLDBN.DAT" nicht sichtbar im Papierkorb gesichert. Eine zweite Datei namens "DBINDEX.VBS" wird noch in den Papierkorb erstellt inkl. eine Kopie davon im Windows-System-Verzeichnis als VBASET.OLB.

Ist das Programm ICQ installiert, modifiziert das Programm folgende Registry-Einträge:

* `HKEY_USERS\.DEFAULT\Software\Mirabilis\ICQ\Agent\Apps\ICQ\Enable=Yes`
* `HKEY_USERS\.DEFAULT\Software\Mirabilis\ICQ\Agent\Apps\ICQ\Parameters=<C:\RECYCLED>\DBINDEX.VBS>`
* `HKEY_USERS\.DEFAULT\Software\Mirabilis\ICQ\Agent\Apps\ICQ\Path=<C:\WINDOWS\WSCRIPT.EXE>`
* `HKEY_USERS\.DEFAULT\Software\Mirabilis\ICQ\Agent\Apps\ICQ\Startup=<C:\WINDOWS>`

Darüber hinaus wird auch die "`SCRIPT.INI`" ausgetauscht, so dass er sich auch über dieses Programm weiterverschickt.

Der Virus verschiebt das Programm ebenfalls "`REGEDIT.EXE`" nicht sichtbar in den Papierkorb unter dem Namen "`RECYCLED.VXD`".

Ist Microsoft Outlook 9 (2000) installiert, dann versucht er sich an 100 Adressen im Adressbuch weiterzuverschicken. Bei mehr als 100 Adressen im Adressbuch werden zufällig 100 Adressen ausgewählt.

Der Text des Email-Kopfes kann jedoch in den verschiedensten Variationen auftreten. Der Haupttext ist jedoch immer "Life stages", "Funny" oder "Jokes".

Davor kann evtl. noch ein "Re:" und am Ende noch das Wort "text" stehen.

Da der Virus bei jedem Systemstart durch die Registry aufgerufen wird, löscht er sich anschließend selbst aus dem Autostart-Ordner.

Die infizierten Dateien werden seit der Virendefinitionsdatei 6.01.00.11 erkannt, dort allerdings noch unter dem Namen TR.Scrap.Worm - seit der VDF 6.01.00.14 werden die Dateien als VBS.LifeStages erkannt.

VBS.LoveLetter

VBS.LoveLetter ist ein Scriptvirus, der sich über Windows-Emailprogramme ausbreitet. Es sind nur solche Emailsysteme betroffen, die aktive Inhalte ausführen können oder dürfen. Der Wurm benutzt selbst die Automatisierungsfähigkeiten von Outlook und ähnelt in seiner Verbreitungsmethode dem Melissa-Virus. Nur werden im Gegensatz zum Melissa-Virus alle Kontaktadressen aus Outlook als Empfänger herangezogen.

Infizierte Emails haben den Betreff (Subject) "ILOVEYOU" und im eigentlichen Text (Body) der Email "kindly check the attached LOVELETTER coming from me." Der Dateianhang (Attachment) unter dem Namen "LOVE-LETTER-FOR-YOU.TXT.vbs" ist der eigentliche Wurm.

Je nach Einstellung von Windows bzw. des Emailsystems kann die Dateinamenserweiterung (Extension) ".vbs" angezeigt werden - oder eben auch nicht. Ohne zumindest verräterische Erweiterung ".vbs" wirkt der Dateianhang natürlich unverdächtiger. Wird der Dateianhang ausgeführt, wird der Standardbrowser gestartet, dies ist üblicherweise der Internet Explorer. Es erscheint ein Bildschirm mit dem Hinweis auf ein ActiveX Control.

Je nach Einstellung der Internet-Sicherheitsstufe erscheint folgende Sicherheitsabfrage:

```
Ein ActiveX-Objekt dieser Seite ist möglicherweise nicht
sicher. Soll die Initialisierung und der Zugriff durch
Scripte zugelassen werden?
```

Erste Merkmale für einen Befall auf Windows-Rechnern sind auf einmal zusätzliche Dateien im Windows- und im Windows-Systemverzeichnis. Im Windows-Verzeichnis ist die Datei Win32DLL.vbs und im System-Verzeichnis sind die Dateien MSKernel32.vbs und LOVE-LETTER-FOR-YOU.TXT.vbs zu finden. In allen diesen Dateien steckt der Wurm selbst drin. Darüber hinaus kopiert bzw. setzt sich der Wurm in alle erreichbaren Dateien mit "unscheinbaren" Erweiterungen wie etwa VBS, VBE, JS, JSE, CSS, WSH, SCT, HTA, MP3, MP2, JPG und JPEG. Nachdem Windows u.U. die Dateinamenserweiterung nicht anzeigt (Ansicht -> Dateinamenerweiterung bei bekannten Dateitypen ausblenden), können solche Veränderungen erst einmal verborgen bleiben.

In die Registry setzt sich der Wurm im Run- und im RunService-Eintrag fest. Durch diese Einträge in der Registry wird der Wurm bei jedem Neustart des Systems aktiv. Die Einträge lauten:

`HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32\`
Hier zeigt der Eintrag auf das Windows-Systemverzeichnis mit dem Dateinamen MSKernel32.vbs, üblicherweise ist dies C:\WINDOWS\SYSTEM\MSKernel32.vbs.

`HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL\`
Hier zeigt der Eintrag auf das Windows-Verzeichnis mit dem Dateinamen Win32DLL.vbs, üblicherweise ist dies C:\WINDOWS\Win32DLL.vbs.

Sofern keine (!) Datei namens WINFAT32.EXE im Windows-Systemverzeichnis existiert, versucht der Wurm einen Passwort-Trojaner zu installieren. Hierzu verwendet er den Internet Explorer, indem er einen Eintrag in `HKCU\Software\Microsoft\Internet Explorer\Main\Start` Page hineinsetzt. Von einer der vier möglichen URLs versucht er den Passwort-Trojaner aus dem Internet herunterzuladen. Nach erfolgreichem Download dieses Trojaners lässt der Wurm diesen Key auf eine leere Seite zeigen (about:blank).

Der Passwort-Trojaner ist in der Registry wie folgt zu finden: `HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX\`
Der Eintrag zeigt auf das Windows-Downloadverzeichnis mit dem Dateinamen WIN-BUGSFIX.exe, beispielsweise ist dies C:\WINDOWS\TEMP\WIN-BUGSFIX.exe oder C:\WINDOWS\DOWNLOADED PROGRAM FILES\WIN-BUGSFIX.exe.

Doch es geht in der Registry noch weiter: Nach erfolgreicher Verbreitung via Email legt der Wurm für jede verschickte Email einen Eintrag unter `HKCU\Software\Microsoft\WAB\` an. Dort sind alle betroffenen Kontaktadressen zu finden, die eine infizierte Email erhalten haben. Diese Liste stammt ursprünglich aus Outlook, wohl um einen Mehrfachversand zu vermeiden.

Seine Schadensroutine ist ein mehr oder weniger umfangreiches Dateilöschen auf allen verfügbaren Laufwerken. Hierzu gehören auch gemappte Netzwerklaufwerke.

Der Wurm sucht nach Dateien mit der Endung *.mp3 und *.mp2. Diese Dateien werden im Verzeichnis als versteckt gekennzeichnet und gleichnamige Dateien, jedoch mit zusätzlicher Dateinamenserweiterung *.vbs, angelegt. In diesen Dateien, beispielsweise *.mp3.vbs, ist der Code des Wurmes enthalten.

Weiterhin sucht der Wurm nach Dateien mit der Endung *.jpg und *.jpeg. Diese werden gelöscht und der gesamte Dateiname um *.vbs erweitert. In diese neue Datei hinein kopiert sich der Wurm, die alte Datei ist komplett verlorengegangen und auch nicht mehr durch den Papierkorb wiederherstellbar.

Dateien mit der Endung *.js, *.jse, *.css, *.wsh, *.sct, *.hta werden gelöscht und mit der Dateinamenserweiterung *.vbs neu erzeugt. Der Inhalt der neu erzeugten Datei ist der Code des Wurmes selbst, die alte Datei ist komplett verlorengegangen und auch nicht mehr durch den Papierkorb wiederherstellbar.

Dateien mit der Dateinamenserweiterung *.vbs oder *.vbe werden vom Wurm mit sich selbst überschrieben. Der alte Inhalt der Dateien ist verlorengegangen.

Doch auch Anwender des Chatprogrammes mIRC bleiben nicht verschont. Findet der Wurm eine der Dateien Mirc32.exe, Mlink32.exe, Mirc.ini, Script.ini oder Mirc.hlp, dann wird in demjenigen Verzeichnis, in dem eine dieser Dateien gefunden wurde, eine Scriptdatei des mIRC-Programmes erzeugt. Eine evtl. bestehende Script.ini wird überschrieben. In der Scriptdatei sind folgende Texte zu finden: ";mIRC Script", "; Please dont edit this script... mIRC will corrupt, if mIRC will", " corrupt... WINDOWS will affect and will not run correctly. thanks", ";", ";Khaled Mardam-Bey", ";http://www.mirc.com". Durch das Script würde die vom Wurm erzeugte "LOVE-LETTER-FOR-YOU.HTM" an alle Chat-Teilnehmer verschickt werden, die neu in den IRC-Channel eintreten

Dem Wurm selbst sind noch folgende Klartexte zu entnehmen: "barok -loveletter(vbe) <i hate go to school>" und "by: spyder / ispyder@mail.com / @GRAMMERSoft Group / Manila,Philippines". Dies läßt den Schluss nahe, dass der Wurm ursprünglich von den Philippinen stammt.

Der Wurm funktioniert nur unter Outlook 98 oder Outlook 2000. Er funktioniert nicht unter Outlook Express. Varianten dieses Wurmes sind VBS.LoveLetter.B (Susitikim) und VBS.LoveLetter.C (Joker, VeryFunny). Es ist mit weiteren Varianten dieses Wurmes zu rechnen.

Es wird daher dringend empfohlen, keine ausführbaren Anhänge (aktive Inhalte) aus Emails heraus auszuführen. Besonders dann nicht, wenn diese Anhänge nicht vorher definitiv verabredet wurden. Es ist doch zumindest ungewöhnlich, wenn "Mann" ebenfalls von "Mann" eine Email mit dem Betreff "ILOVEYOU" bekommt?

Doch auch neben diesen .vbs-Dateien gibt es noch andere, die ebenfalls (automatisch) ausgeführt werden könnten. Neben den bekannten reinrassigen Programmen (.com, .exe), Batchdateien (.bat), gibt es weitere Dateitypen, der Inhalte latent gefährlich sein können: Dokumente, Spreadsheets, Office-Dateien (.xls, .doc, .ppt etc.) aber auch andere Dateien: Fontdateien (.ttf), Scratchdateien (.shs), Screensaver (.scr). Nachdem in Windows und/oder Emailsystemen die Anzeige der Dateinamenserweiterungen standardmäßig ausgeschaltet sein kann, müssen diese Erweiterungen als solche gar nicht als gefährlich in Erscheinung treten! Die Sicherheitsstufe beim Internet Explorer sollte nicht ohne zwingenden Grund verringert werden.

AntiVir erkennt über 100 Varianten.

VBS.LoveLetter.BD

Zur Zeit macht wieder ein neuer Email-Wurm namens "VBS/Loveletter.BD" die Runde. Dieser Scriptvirus basiert auf den VBS.LoveLetter und breitet sich über die Windows-Emailprogramme aus. Es sind nur solche Emailsysteme betroffen, die aktive Inhalte ausführen können oder dürfen. Der Wurm benutzt selbst die Automatisierungsfähigkeiten von Outlook und ähnelt in seiner Verbreitungsmethode dem Melissa-Virus. Nur werden im Gegensatz zum Melissa-Virus alle Kontaktadressen aus Outlook als Empfänger herangezogen.

Beim ersten Aufruf versucht der Virus sich an alle Personen im Adressbuch von Microsoft Outlook zu verschicken. Dafür legt der Virus den Schlüssel `HKEY_CURRENT_USER\Software\ACH0""=1` in der Registry an, um beim jedem weiteren Aufruf diesen Schritt zu überspringen.

Als nächstes prüft der Virus, ob folgender Schlüssel vorhanden ist: `HKEY_CURRENT_USER\Software\UBS\UBSPIN\Options\Datapath`

Wird der Schlüssel gefunden, versucht der Virus ein weiteres Programm - sofern noch nicht vorhanden - von einem der drei folgenden FTP-Server zu downloaden und es auszuführen.

1. 165.121.181.24/hcheck.exe
2. alw.nih.gov/incoming/hcheck.exe
3. archive.egr.msu.edu/incoming/hcheck.exe

Diese Datei, das Programm ist ein Passwort-Stealer, ist nicht mehr auf den Servern verfügbar.

Anschließend verschickt er die ausgelesene Datei, welche im o.g. Eintrag in der Registry hinterlegt ist, an folgende Email-Adressen:

1. ct102356@excite.com
2. acch01@netscape.net
3. deroha@mailcity.com

Außerdem speichert er noch eine Kopie der Daten in der Datei CP_21863.NLS im Windows-System-Verzeichnis ab.

VBS.LoveLetter.CM

AntiVir erkennt diesen Wurm als: VBS.LoveLetter.C

Der Wurm verbreitet sich über das Email Programm Outlook von Microsoft. Er versendet sich an alle im Adressbuch eingetragenen Kontakte.

Wird die Datei JENNIFERLOPEZ_NAKED.JPG.vbs ausgeführt, so kopiert sich der Wurm nach c:\ windows. Danach registriert sich der Wurm 2 mal in der Registry:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
WORM"="wscript.exe C:\\WINDOWS\\JENNIFERLOPEZ_NAKED.JPG.vbs %

HKEY_CURRENT_USER\Software\JENNIFFERLOPEZ_NAKED
@="Worm made in algeria"
mailed"="1
```

Der Wurm sucht außerdem auf allen Festplatten und gemappten Netzwerklaufwerken nach Dateien mit folgenden Endungen: *.vbs, *.vbe, *.js, *.jse, *.css, *.wsh, *.sct, *.hta, *.jpg, *.jpeg, *.mp3, *.mp2
Alle Diese Dateien werden mit dem Code des Wurmes überschrieben.

Als letztes wird der Virus "W95/CIH.A" in das Verzeichnis "c:\windows\" gedroppt. Der Dateiname des Virus ist: "Cih_14.exe".

VBS.NEWLOVE

Zur Zeit macht wieder ein neuer Email-Wurm namens "NewLove" die Runde. Durch eine destruktivere Schadensroutine verursacht dieser Email-Wurm einen weitaus größeren Schaden als seine Vorgänger aus der ILOVEYOU-Familie.

Der Wurm hat 3 Funktionen:
Funktion 1: Der Wurm versendet sich an alle Kontakte in Outlook
Funktion 2: Alle Dateien werden mit 0 Bytes überschrieben
Funktion 3: Windows kann nicht mehr gestartet werden

Details:
Wird der Wurm durch Doppelklick auf das infektöse Attachment des empfangenen Emails gestartet, kopiert er sich in das Windows- und Windows\System-Verzeichnis. Hierbei wird der Code des Wurmes mit unterschiedlich vielen Kommentarzeilen aufgefüllt, vermutlich um einer schnellen Entdeckung zu entgehen. Dadurch wird er von mal zu mal größer. Der eigentliche Code selbst ist nur rd. 5 KB groß. Außerdem werden folgende Registryeinträge gemacht.

1. `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\`
2. `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\`

Hierbei trägt sich der Wurm unter einen von ihm zufällig gewählten Namen um. Dies kann auch der Namen einer Datei sein, die es bereits auf dem Rechnersystem gibt. Der Wurm schaut hierzu in C:\ WINDOWS\APPLOG nach. Falls hier keine Datei gefunden werden kann, wählt er einen zufälligen Namen zwischen einem und 31 Zeichen und hängt eine der folgenden 11 Erweiterungen an:

```
DOC, XLS, MDB, BMP, MP3, TXT, JPG, GIF, MOV, URL, HTM
```

Ist auf dem Rechnersystem MS Outlook installiert, verschickt sich der Wurm zeitabhängig an alle im Adressbuch eingetragenen Empfänger. Ist kein Outlook installiert ist, beginnt er sofort mit seiner Schadensroutine.

Die Email wird so oder ähnlich aussehen:

Subject:
`FW: PKUPLRXOOHBOZGNEMFHUO.Txt`

Attachment:
`PKUPLRXOOHBOZGNEMFHUO.Txt.Vbs`

Nachden sich der Wurm nun selbst verschickt hat, beginnt er auf allen lokalen und allen Netzlaufwerken alle Dateien mit 0 Byte zu überschreiben. Er verschont nur diejenigen (mangels Öffnungserfolg), die bereits geöffnet oder vom System gelockt sind. Alle Dateien werden außerdem mit der Endung .vbs versehen. Explorer.Exe wird beispielsweise zu Explorer.Exe.Vbs. Hierbei kann es dazu kommen, dass der Wurm mehrmals die Datei umbenennt. z.B. Explorer.Exe.Vbs.Vbs.Vbs

Fazit:
Aus dem Email-Sturm, ausgelöst durch ILOVEYOU in den letzten Wochen, ist bereits gelernt geworden. Es sind bisher keine Schäden gemeldet worden. Ebenso steht eine echtes ITW-Auftreten in Deutschland bisher noch aus - es ist bisher kein einzige Meldung bei uns eingegangen. Aus diesem gegebenen Anlaß möchten wir nochmals darauf hinweisen, nicht abgesprochene Attachments (Dateianhänge) mit größter Vorsicht zu behandeln. Ebenso keinen unbedachten Doppelklick auf Attachments zu machen.

Sinnvollerweise sollte auch der WSH (Windows Scripting Host) deinstalliert und die Verknüpfung mit Visual Basic Script (VBS) aufgehoben werden. Evtl. ist auch über den Einsatz eines nicht so sorglos mit aktiven Inhalten umgehenden Emailprogrammes, besonders im Firmenumfeld, nachzudenken.

Das aktuelle AntiVir-Update 6.01.00.08 erkennt nicht nur diesen Email-Wurm, sondern die Spezialisten von H+BEDV haben auch bereits weitere Verbreitungsmöglichkeiten mit berücksichtigt. Damit erhalten Ihre Daten auch einen Schutz gegen weitere "NewLove"-Mutationen.

VBS/Caroline.B

Alias: VBS/Australia.jpeg.vbs

Dieser Wurm kopiert sich nach dem Ausführen in das C:\WINDOWS\SYSTEM\ -Verzeichnis und erstellt einen RUN - Eintrag in die Registry unter

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run\Wurmname.vbs
```

trägt er den Namen (z.B. RX4YYX.VBS) ein. In

```
HKEY_LOCAL_MACHINE\Wurmname.vbs
```

stellt er den Wert "1" ein.

Danach versucht sich das Wurmprogramm über Outlook zu versenden.
Die Email sieht wie folgt aus:

Subject:
```
much greets from Australia
```

Body:
```
vacation 2001 in Australia !
```

Attachment:
```
Australia.jpeg.vbs
```

VBS/HomePage.1

Dieser Wurm verbreitet sich über Microsoft Outlook und Outlook Express, indem er das Outlook Adressbuch öffnet und sich an alle Email - Adressen versendet, die angelegt worden sind.

Wird das Attachment ausgeführt, versendet der Wurm sich und löscht alle Emails mit dem Betreff ’Homepage ’, die sich im ’Posteingang’ und ’gelöschte Objekte’ befinden. Der Wurm kopiert sich in das temporäre Windowsverzeichnis (C:\Windows\Temp\) und fügt folgenden Eintrag in die Registry mit dem Wert 1 ein:

```
HKCU\software\An\mailed
```

Nach dem versenden der Emails öffnet der Wurm die folgenden Internetseiten mit dem Internet Explorer:

http://hardcore.pornbillboard.net/shannon/1.htm
http://members.nbci.com/_XMCM/prinzje/1.htm
http://www2.sexcropolis.com/amateur/sheila/1.htm
http://shiela.issexy.tv/1.htm

VBS/Lee-ATX

Alias: VBS/Anthrax

Der Wurm VBS/Lee-ATX verbreitet sich via Email über Outlook mit Hilfe des Outlook -Adressbuches oder über die Chatprogramme mIRC bzw. PIRCH. Desweiteren überschreibt er alle Dateien mit den Extensions VBS und VBE mit seinem eigenen Viruscode.

VBS/Lee-ATX versendet sich an alle Emailadressen, die im Outlook Adressbuch stehen. Die Email sieht folgendermaßen aus:

Subject:
```
Antrax Info
```

Body:
Der Inhalt der Email ist je nach Variante unterschiedlich. Die Texte des Email Body können wie folgt lauten:

```
si no sabes que es el antrax o cuales son suss efectos aqui te mando una
foto para que veas los efectos que tiene
Nota: la foto esta un pco fuerte
Aqui te mando este documento para que sepas que es y cuales son los efectos
des "Antrax"
```

oder

```
como ahorita esta de moda hablar sobre el antrax aqui les mando una foto de un
enfermo terminal
```

Attachment:
Der Name der angehängten Datei ist kann wie folgt lauten:

```
antraxinfo.vbs, antrax.jpg.vbs oder antrax.doc.vbs
```

Wird das Attachment ausgeführt, kopiert sich der Wurm als erstes in das Windows Systemverzeichnis mit dem Namen ANTRAXINFO.VBS. Danach modifiziert VBS/Lee-ATX die Registry, damit er bei jedem Windowsstart ausgeführt wird:

```
HKML\Software\Microsoft\Windows\CurrentVersion\Run\antraxinfo =
"wscript.exe C:\Windows\System\antraxinfo.vbs %"
```

Er versucht sich über Email mit Hilfe des Outlook Adressbuches an alle darin stehenden Einträge zu versenden. Hat der Wurm das getan, erstellt er in der Registry

folgenden Eintrag:

```
HKCU\Software\Antrax\Mailed = "1"
```

Sollte der Wurm das Chat-Programm mIRC auf C:\MIRC oder C:\MIRC32 finden, überprüft er diese Verzeichnisse auf die Datei MIRC.INI. Sollte diese Datei vorhanden sein, erstellt er die Datei SCRIPT.INI und in der Registry folgenden Eintrag:

```
HKCU\Software\Antrax\Mirqued = "1"
```

Wird im Pfad C:\PIRCH oder C:\PIRCH32 das Chat-Programm Pirch gefunden, erstellt der Wurm die Datei EVENTS.INI. Mit Hilfe dieser Datei wird beim nächsten Aufruf von Pirch sichergestellt, dass die Datei ANTRAXINFO.VBS in Windows Systemverzeichnis via Pirch versandt wird. Danach wird der folgende Registry Eintrag angelegt:

```
HKCU\Software\Antrax\Pirched = "1"
```

Wird der Wurm VBS/Lee-ATX am 26.Januar ausgeführt, zeigt sich ein Fenster mit dem Text: "Antrax Worm By wAsEk". Es werden alle Dateien, die die Extensions .VBS oder .VBE besitzen, mit dem Virencode überschrieben.

VBS/NeueTarife

Alias: VBS/VBSWG.K@MM

Die Variante "Neue Tarif.txt.vbs" erstellt im C:\MIRC Verzeichnis eine Datei mit dem Namen SCRIPT.INI und kopiert sich dann nach C:\WINDOWS\Neue Tarife.txt.vbs. Danach trägt er sich in den RUN - Eintrag der REGISTRY

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run\neue
Tarife.txt.vbs
```

und in

```
HEKY_CURRENT_USER\Software\
```

mit dem Eintrag "Mirqued"="1" ein.
Danach versucht sich das Wurmprogramm über das Outlook zu versenden.

Die Email zeigt folgenden Inhalt:

Subject:
Neues von Ihrem Internetdienstleister - Robert T. Online informiert

Body:
Sehr geehrter Internetsurfer,

es hat sich einiges bei uns getan. Die Telekom kann auch Ihre Internetkosten reduzieren. Wir haben auch für Sie den richtigen Tarif... Damit auch Sie sich entscheiden können, haben wir eine Übersicht aller für Sie relevanter Termine an diese eMail gehängt.

Wir sind Sicher, auch Sie werden Ihren Wunschtarif finden.

Bei fragen stehen wir Ihnen natürlich jederzeit zur Verfügung...

Ihr T-Online Service Team

Attachment:
Neue Tarife.txt.vbs

VBS/SST.A

Der Wurm VBS/SST.A wurde in Visual Basic Script (VBS) geschrieben und arbeitet mit dem Windows Scripting Host (WSH). WSH wird üblicherweise mit IE5 bzw. diversen Service Paks installiert.

Der Wurm versendet sich per Email und hat das Attachment AnnaKournikova.jpg.vbs angehängt. Dieser Dateianhang sieht auf den ersten Blick wie ein Bilddatei und wird von vielen Usern unbedacht geöffnet werden. Die Dateinmanserweiterung ".vbs" wird üblicherweise NICHT angezeigt, da im Explorer in den Einstellungen die Option "Dateinamenerweiterung bei bekannten Dateitypen ausblenden" standardmäßig angewählt ist.

Wenn der Wurm ausgeführt wird, erzeugt er folgende Registryeinträge:

`HKCU\Software\OnTheFly mit dem Inhalt "Worm made with Vbswg1.05b"`. Dies stellt wohl die Signatur des es Wurmes dar.

Als erstes kopiert sich der Wurm in das Windowsverzeichnis (üblicherweise C:\WINDOWS) unter dem Dateinamen "AnnaKournikova.jpg.vbs".

Nach dem Versenden über Outlook erstellt er zusätzlich einen zweiten Registryeintrag:

`HKCU\Software\OnTheFly\mailed mit dem Wert "1".`

Er verschickt sich an alle Email-Adressen, die im Outlook-Adressbuch stehen. Die Email sieht wie folgt aus:

Subject:
`Here you have ;o)`

Message Body:
`Hi:`

`Check This!`

Attachment:
`AnnaKournikova.jpg.vbs`

Die Nachrichten werden nach dem Versenden sofort gelöscht - und verbleiben so nicht in dem Ordner "Gesendete Objekte".

Der Code dieses Wurmes enthält noch eine Anweisung, dass zu jeden 26. Januar die Internetseite http://www.dynabyte.nl aufgerufen werden soll, eine Internetseite einer wohl unbeteiligten niederländischen Computerzeitschrift.

VBS/Staple.A

VBS/Staple.A ist ein VBS (Visual Basic Script) Wurm und versendet sich mit Hilfe von Microsoft Outlook an die ersten 50 Emailadressen, die im Outlook Adressbuch stehen. Die Email sieht folgendermaßen aus:

Subject:
RE:Injustice

Body:
Dear <Emailadresse>

Did you send the attachment message,
I was not expecting this from you !

Attachment:
INJUSTICE.TXT.VBS

VBS/Staple.A versendet auch jeweils eine Kopie der Email an folgende Adressen:

amuta@ehudbarak.co.il
arie@kba.org
doar@mof.gov.il
doar@shaam.gov.il
foundation@habonimdror.org
hachnasot@mof.gov.il
holyland@inisrael.org
info@azm.org
mafkal@police.gov.il
menahel@saam.gov.il
naamatusa@naamat.org
ncli@laborisrael.org
office@JAFI.org.il
pniotmas@mof.gov.il
rmarkus@parliament.gov.il
Sar@mod.gov.il
sar@mof.gov.il
Sar@moin.gov.il
Sar@mops.gov.il
webmaster@israel.com
wlzm@jazo.org.il
yor@knesset.gov.il

Nach dem Emailversand wird der Registry Key

HKEY_CURRENT_USER\Software\Microsoft\WAB\"&mailed,1,"REG_DWORLD"

angelegt und es werden die folgenden Internetseiten automatisch mit dem Internet Explorer geöffnet:

http://freesaj.org.uk
http://hanthala.virualave.net
http://www.palestine-info.org
http://www.petitiononline.com/palpet/petition.html
http://www.sabra-shatilia.org

http://www.ummah.net/unity/palestine/index.htm

Zuletzt wird folgendes Fenster geöffnet mit dem Fenstertitel

"HELP US STOP THE BLOOD SHED!!".

VBS/Vierika

Der Wurm VBS/Vierika ist ein Internet-Wurm und wurde in mit Visual Basic Script programmiert. Dieser Wurmcode wurde direkt in das HTML Dokument Vindex2.html implementiert und auf einer Webseite von GeoCities bereitgestellt. VBS/Vierika führt sich automatisch mit dem Aufruf dieser HTML Seite aus.

Der Wurm erstellt eine Datei auf C:\ mit dem Namen Vierika.jpg.vbs, die aber keinen Wurmcode oder ein VB Script enthält, lediglich das Word free.

Danach startet VBS/Vierika Microsoft Outlook und versendet sich an alle Email-Adressen, die im Adressbuch von Outlook stehen. An die Email hängt er ein Attachment an.

Die Email sieht folgendermaßen aus:

Subject:
`Vierika is here`

Body:
`Virieka.jpg`

`Attachment:  Vierika.jpg.vbs`

Zuletzt ändert der VBS/Vierika noch die Startseite des Internet Explorers. Auf einem infizierten System zeigt die Startseite nun auf http://www.geocities.com/msxxl/Vierika.html.

Wurde das versandte Attachment gestartet, wird bei diesem Rechner die Startseite des Internet Explorers automatisch auf oben genannte Internetadresse gesetzt. Wird nun der Internet Explorer aufgerufen, wird diese Seite als erstes angezeigt und der Wurm wird automatisch aufgeführt.

VGen

AntiVir 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 AntiVir mit einem VGen-Virus erkannt wurden, ins Haus zu schicken. Da bei VGen-Viren nur eine Virensignatur gefunden wird, können diese Dateien von AntiVir leider auch nicht repariert werden.

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 effektiver 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.

W32.Kriz

Der Virus W32.Kriz wird als .EXE-Datei versendet, verbreitet sich unter Windows 32-bit Systemen und infiziert .EXE-Dateien. Um als residenter Virus im Arbeitsspeicher verbleiben zu können, infiziert 'W32.Kriz' auch die KERNEL32.DLL.

Bei der Infektion einer .EXE-Datei erstellt der Virus einen neuen Abschnitt am Ende dieser Datei, in dem er seinen Code ablegt. Zum Auffinden solcher infizierter Dateien sucht man einfach nach dem String "666", welcher in die Kopfzeile des Codes geschrieben wird. Der Virus infiziert nicht alle .EXE-Dateien bzw. Programme. Folgende Dateien werden nicht verändert:

```
ALERTSVC.EXE, AVPM.EXE, AMON.EXE, AVP32.EXE, N32SCANW.EXE, NAVAPSVC.EXE,
NOD32.EXE, NAVAPW32.EXE, NAVWNT.EXE, NAVLU32.EXE, NAVRUNR.EXE, NPSSVC.EXE,
NSCHEDNT.EXE, SCAN.EXE, SMSS.EXE, _AVP32.EXE, _AVPM.EXE, NSPLUGIN.EXE,
```

Zum Infizieren der KERNEL32.DLL speichert der Virus diese Datei unter dem Namen KRIZED.TT6 ab und verändert diese anschließend. Beim nächsten Systemstart wird die KERNEL32.DLL mit Hilfe eines entsprechenden Eintrages in der WININIT.INI durch die Datei KRIZED.TT6 ersetzt. Der Virus verändert die Adressbereiche der externen Windows-Befehle, so dass diese in den Programmcode des Virus eingeschlossen werden. Der Virus ändert auf diese Weise sechzehn KERNEL32 Funktionen: Datei öffnen, kopieren, löschen, Ändern der Dateiattribute und viele mehr...

Der Virus hat zusätzlich noch eine gefährliche Schadensroutine in seinem Code: Am 25. Dezember zerstört der W32.Kriz den CMOS-Speicher, überschreibt alle Dateien auf allen vom BIOS verwalteten Festplatten und zerstört den Flash BIOS mit der selben Routine wie der CIH-Virus.

W32.TR.Worm/QAZ

Der Wurm 'QAZ' ist eine ausführbare .EXE-Datei und breitet sich auf allen Windows 32-bit Systemen aus. Er wurde in der Programmiersprache C unter Visual C++ programmiert. Seine Länge beträgt 120320 Bytes. Er wurde das erste mal im Juli/August 2000 gemeldet.
Wird der Wurm aktiviert, trägt er sich so in die Registry ein, damit er bei jedem Systemstart erneut ausgeführt wird:

```
[HKLM\SOFTWARE\Microsoft\Windows\Current Version\Run]
startIE = "notepad.exe qazwsx.hsq"
```

Wurde der Wurm auf diese Weise gestartet, werden zwei Funktionen dieses Wurmes ausgeführt: eine Backdoor-Funktion sowie ein Programm zur sicheren Verbreitung seines Codes.
'QAZ' breitet sich auf allen erreichbaren Netzlaufwerken aus, indem er auf allen Laufwerken die Datei NOTEPAD.EXE sucht und diese dann, entsprechende Schreibrechte vorausgesetzt, in NOTE.COM umbenennt. Anschließend schreibt er seinen eigene Programmcode in eine Datei unter dem Namen NOTEPAD.EXE.

Wird nun das vom Virus erzeugte Programm NOTEPAD.EXE vom Benutzer gestartet, verbreitet sich der Wurm auf diesem System. Damit der Benutzer von der Infektion nichts merkt, wird danach das eigentliche NOTEPAD, nämlich die Datei NOTE.COM, gestartet.

Die Backdoor-Routine ist mit wenigen Kommandos ganz einfach gehalten: RUN (Starten eines Programmes), UPLOAD (zum Erstellen einer Datei auf dem infizierten System) und QUIT (zum Beenden der Wurm-Routine). Diese drei Kommandos reichen allerdings aus, um ein anderes, gefährlicheres Backdoor-Programm, einen Wurm oder einen Virus auf einem System zu installieren.

'QAZ' versucht sich nach der Infektion des Rechners in das Internet einzuwählen. Er versucht, eine Verbindung zu einer Website in China (http://202.106.185.107) aufbauen, um wahrscheinlich dorthin die IP-Adresse des infizierten Rechners zu übermitteln. Dies kann nicht mehr nachvollzogen werden, da diese IP-Adresse gesperrt wurde. Da diese Seite nicht mehr erreichbar ist, startet der Trojaner alle 4 bis 6 Minuten erneut einen neuen Versuch, diese Seite zu kontaktieren. Hierdurch hält der Wurm bestehende Internetverbindungen offen bzw. öffnet diese erneut.

Um den 'QAZ' von einem infizierten System zu entfernen, sollten als erstes die infizierten Rechnersystem von Netzwerkverbindungen getrennt und Modemverbindungen beendet werden. Danach sollte der oben genannten Registryeintrag in der Autostart-Routine entfernt und die Datei NOTEPAD.EXE gelöscht werden. Zuletzt bracuht nur nich Datei NOTE.COM wieder in NOTEPAD.EXE umbenannt werden.

W32.Vote

W32.Vote.a

Bei W32.Vote handelt es sich um einen Massenmailer, der in Visual Basic geschrieben wurde. Er verbreitet sich mit Hilfe von Microsoft Outlook, indem er sich an alle Emailadressen versendet, die im Adressbuch aufgeführt sind.

Die Email wird wie folgt versandt:

Subject:
```
Fwd:Peace Be Tween AmeriCa And IsLam!
```

Body:
```
Hi!
iS iT A waR Against AmeriCa Or IsLam!
Let`s Vote To Live in Peace!
```

Attachement:
```
WTC.EXE
```

Wird das Attachement WTC.EXE ausgeführt, installiert W32.Vote.a folgende Dateien:

C:\WINDOWS\WTC.EXE

C:\WINDOWS\SYSTEM\ZACKER.VBS
C:\WINDOWS\SYSTEM\MIXDALAL.VBS

Danach legt er folgenden Registry-Key an, damit er nach dem Systemstart erneut ausgeführt wird:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run\]
"Norton.Thar"="C:\\WINDOWS\\SYSTEM\\ZaCker.vbs"
```

W32.Vote.a ändert die AUTOEXEC.BAT und fügt die Befehlszeile "format c:" hinzu. Wird das System neu gestartet, wird die Partition C: formatiert. Sollte Windows vollständig geladen werden, führt er die Datei ZACKER.VBS aus und löscht alle Dateien, die im Windows-Verzeichnis vorhanden sind. Danach wird folgende Textmeldung ausgeben:

> I promiss We WiLL Rule The World Again...
> By The Way, You Are Captured By ZaCker !!!

Hat W32.Vote.a nun die Modifikationen in der Registry sowie in der AUTOEXEC.BAT vorgenommen, ändert er die Startseite des Internet Explorers. Anschließend startet er den Internet Explorer und lädt automatisch ein Programm namens TimeUpdate.exe aus dem Internet herunter. Dieses Programm ist ein Backdoor-Server, der von AntiVir bereits als TR/Barrio50.PSW.6 erkannt wird.

Die Startseite des Internet Explorers wird auf folgende URL geändert:

http://us.f1.<locked>.com/users/da26d538/bx/TimeUpdate.exe?bcaVq97AtaW0yAxk

W32.Vote.a ruft das VBS Script MIXDALAL.VBS auf. Dieses Visual Basic Script sucht auf allen lokalen bzw. gemappten Laufwerken nach .HTM und .HTML Dateien, dessen Inhalt durch folgenden ersetzt wird:

AmeRiCa ...Few Days WiLL Show You What We Can Do !!! It's Our Turn >>> ZaCkEr is So Sorry For You.

W32.Vote.b

In der Variante B des W32.Vote werden folgende Dateien auf dem Rechner installiert:

C:\WINDOWS\ANTI_TERRORISM.EXE
C:\WINDOWS\MIXDALAL.EXE
C:\WINDOWS\SYSTEM\DALAL.EXE
C:\WINDOWS\SYSTEM\WAIL.EXE

Im Gegensatz zur Variante A des W32.Vote wird folgender Registry-Eintrag erstellt

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"ZACker"="C:\\WINDOWS\\SYSTEM\\DaLaL.vbs"
```

und die Startseite des Internet Explorers wird auf folgende URL geändert:

"about:I SwEar , We WiLL Rule This World SooN !!!"

Alle weiteren Schadensroutinen sind dieselben wie auch schon bei der Variante A des W32.Vote.

W32.Vote.c

In der C-Variante werden die folgenden Dateien auf dem Rechner installiert

C:\WINDOWS\WTC.EXE
C:\WINDOWS\MIXDALAL.EXE
C:\WINDOWS\SYSTEM\DALAL.EXE
C:\WINDOWS\SYSTEM\WAIL.EXE

und die Startseite des Internet Explorers wird auf folgende URL geändert:

http://us.f1.<locked>.com/users/da36d538/bc/TimeUpdate.exe?bc6sNA8A_jiPyAxk

Alle weiteren Schadensroutinen sind dieselben wie auch schon bei der Variante A des W32.Vote.

W32/Apost.A

Alias: Worm/Readme

W32/Apost ist einen Internetwurm, der in Visual Basic 6 programmiert wurde. Er besitzt eine Größe von 24576 Bytes und versendet sich per Email mit Hilfe von Microsoft Outlook.

Wird der Wurm 32.Apost.A ausgeführt, zeigt dieser eine gefaiktes Fenster mit einer WinZip Fehlermeldung an: "CRC error: 234#21".

Wenn der Anwender die falsche Meldung mit einem Klick auf den 'Aceptar'-Button bestätigt, versendet sich der Wurm per Email. Hierzu verwendet er das Microsoft Outlook Adressbuch, um eine Email mit folgenden Inhalt an die darin enthaltenen Emailadressen zu versenden:

Subject:
```
As per your request!
```

Body:
```
Please find attached file for your review
I lokk forward to hear form your again very soon. Thank you.
```

Attachment: README.EXE

Hat sich der Wurm erfolgreich versandt, wird ein weiteres Windowsfenster geöffnet und anzeigt. Es enthält nur einen Open-Button.

Der Wurm selbst kopiert sich in das System Verzeichnis von Windows, sowie in die Root-Verzeichnisse der lokalen Laufwerke (C:\; D:\; usw.) als README.EXE, welche das Standart Icon von Visual Basic 6 Anwendungen trägt.

Der Wurm legt folgenden Registry Eintrag an:

```
HKCU\Software\Microsoft\Windows\Current Version\Run\macrosoft = %Windows%\
Readme.exe
```

W32/ExploreZip

Alias: Worm.Explore.Zip, Zipped Files, Troj.Explore.Zip
Merkmale: Trojanisches Pferd, Wurm
Textstring: "zipped_files"
Länge: 210432 Bytes
Plattform: Windows 9x/Windows NT

Bekommen Sie eine Email mit dem Inhalt "Hi [Name des Email-Empfängers]! I received your Email and I shall send you a reply ASAP. Till then, take a look at the attached zipped docs. Bye", dann ist dies der Virus.

Wie auch Melissa nutzt dieser Virus die Emailfähigkeiten der Windows-Systeme aus. Er verbreitet sich über beispielsweise mittels Outlook, Exchange oder NetScape Mail. Darüber hinaus kürzt er - auch über die Netzwerkumgebung - Dateien auf 0 Byte!

W32/ExploreZip verbreitet sich über Email auf Windows 9x- und Windows NT-Rechnersystemen. Als Emailprogramm kommt jeder MAPI-fähige Email-Client in Betracht. Hierzu gehören unter anderem:

* MS Outlook
* NetScape Mail
* MS Exchange
* Outlook Express

Im aktiven Zustand verteilt er sich über MAPI-Kommandos weiter, indem er sich selbst als Attachment mit dem Namen "zipped_files.exe" versendet. Im Gegensatz zu Melissa versendet sich W32/ExploreZip selbständig an die Adressen unbeantworteter Emails im Posteingang. Melissa hingegen verschickte Kopien von sich selbst an bis zu 50 Empfänger aus dem Adreßbuch.

Durch diesen Trick sieht die Email beim Empfänger ganz unverfänglich aus. Ist sie doch eine Antwort auf die - an einen bekannten Empfänger - versandte Nachricht.

Eine "infizierende" Email sieht folgendermaßen aus:

```
From:
[Name des Email-Absenders]

Subject:
re:[Subject der unbeantworteten Nachricht]

To:
[Name des Email-Empfängers]

Hi [Name des Email-Empfängers] !

I received your Email and I shall send you a reply ASAP.
Till then, take a look at the attached zipped docs.

Bye oder sincerely
[Name des Email-Absenders]

Attachment:
zipped_files.exe
```

Wird das infizierte Attachment ausgeführt, erscheint folgende Warnmeldung auf dem Bildschirm:

```
Cannot open file: it dis not appear to be a vakud archive. It this is
part of a ZIP format
backup set, insert the last disk of the backup set and try again. Please
press F1 for help.
```

Zu diesem Zeitpunkt ist der Virus aber schon aktiv und "arbeitet". Er kopiert sich selbst entweder unter dem Namen "Explore.exe" oder "_setup.exe" in das jeweilige System-Verzeichnis. Dies ist %windir%\System (üblicherweise c:\windows\system) unter Windows 9x, bzw. %windir%\System32 (üblicherweise c:\winnt\system32) unter Windows NT.

Anschließend modifiziert er die WIN.INI unter Windows 9x, bzw. die Registry unter Windows NT. Durch die Modifikation der INI-Datei, bzw. der Registry erreicht der Virus, daß er bei jedem Hochfahren des Systemes erneut gestartet wird. Hierdurch hat er die Möglichkeit, auch neue Posteingänge entsprechend zu beantworten.

In seiner Schadensroutine ist der Virus multi-threading-fähig: Er erzeugt zwei "Killer-Threads". Einer der Threads sorgt für die "Email-Behandlung", ein anderer Thread ist für das "Leeren" der Dateien zuständig. Der erste Thread überwacht via MAPI neue Posteingänge. Durch das Überwachen neuer Posteingänge "beantwortet" der Virus eingegange Emails sofort wieder mit sich selbst. Bestehende, bisher ungelesene Nachrichten werden ebenfalls sofort beantwortet.

Ein zweiter Thread "leert" Dateien mit folgenden Extensions ".doc, .c, .cpp, .h, .asm, .xls und .ppt ". Das "Leeren" ist ein Kürzen der Dateien über die Windows-Funktion "CreateFile" auf 0 Byte! Durch dieses "Leeren" werden Dateien nicht gelöscht und stehen über den Papierkorb auch nicht für eine Wiederherstellung zur Verfügung. Die gekürzten Dateien können nicht wiederhergestellt werden, da der Inhalt "verlorengegangen" ist.

Das Leeren von Dateien läßt sich auch an einer verstärkten Festplattenaktivität feststellen. Doch der Virus "leert" auch solche Dateien, die über "gemappte" Laufwerke bis hin zum Laufwerksbuchstaben "Z:" als Netzwerklaufwerke zur Verfügung stehen ("WnetEnumResource"). Die Schadensroutine des Virus ist solange aktiv, wie auch der Virus selbst im Speicher ist.

Der Virus kann jedoch recht einfach durch Löschen der infektiösen Dateien und Modifizieren der WIN.INI bzw. Registry entfernt werden:

1. Entfernen der Autostart-Einträge unter Windows 9x durch das Löschen der folgenden Zeile aus der WIN.INI (mittels SysEdit):

```
run=C:\WINDOWS\SYSTEM\Explore.exe oder
run=C:\WINDOWS\SYSTEM\_setup.exe
```

Entfernen der Autostart-Einträge unter Windows NT durch das Löschen des Keys aus folgendem Registry-Pfad (mittels RegEdit):

```
HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows

run=C:\WINNT\SYSTEM32\Explore.exe oder
run=C:\WINNT\SYSTEM32\_setup.exe
```

2. Entfernen des Virus

Nach einem Neustart oder einem "Abschießen" des Virus über den Taskmanager sollte der Virus

selbst gelöscht werden. Die Datei befindet sich unter dem Namen "Explorer.exe" oder "_setup.exe" im jeweiligen Verzeichnis von Windows:

Unter Windows 9x c:\windows\system\
unter Windows NT c:\winnt\system32\

Es kann daher nicht oft genug vor Emails mit unbekannten Dateianhängen gewarnt werden. Es ist auch eher unüblich, daß Dokumente als selbstextrahierende .EXE-Dateien versandt werden. Anwender sollten mit geeigneten Antivirenprogrammen - auch zur Vorsorge - einmal alle Dateien eines Rechnersystemes untersuchen. Es werden dann auch die temporären Dateien der diversen Emailprogramme untersucht und die darin gespeicherten Viren ggf. entdeckt.

Darüber hinaus zeigt dieser Virus mit seinem agressiven Schadensteil wieder einmal deutlich, wie durch sinnvolle Rechtevergabe in Netzwerken die Schäden hätten begrenzt werden können.

W32/FBound.C

Beim W32/Fbound.C handelt es sich um einen Wurm, der sich mit Hilfe des Windows Adressbuches mit seiner eigenen SMTP-Engine als Email versendet. Eine vom W32/Fbound.C versendete Email sind folgendermaßen aus:

Subject:
Important

Body:

Attachment:
patch.exe

Der Wurm hat eine Größe von 12.228 Bytes und keinerlei weitere Schadensroutinen. Es werden keine Dateien oder Registry Einträge angelegt und somit ist der Wurm nach einem Neustart des infizierten Rechners inaktiv. Es wird lediglich eine infizierte Datei im \<WINDIR>\TEMP\ Ordner abgelegt, die W32/Fbound.C benötigt, um sich zu versenden.

W32/Klez

Der Virus W32/Klez wird als .EXE-Datei versendet, verbreitet sich unter Windows 32-bit Systemen und infiziert .EXE-Dateien. Um als residenter Virus im Arbeitsspeicher verbleiben zu können, infiziert 'W32/Klez' auch die KERNEL32.DLL.

Bei der Infektion einer .EXE-Datei erstellt der Virus einen neuen Abschnitt am Ende dieser Datei, in dem er seinen Code ablegt. Zum Auffinden solcher infizierter Dateien sucht man einfach nach dem String "666", welcher in die Kopfzeile des Codes geschrieben wird. Der Virus infiziert nicht alle .EXE-Dateien bzw. Programme. Folgende Dateien werden nicht verändert:

ALERTSVC.EXE, AVPM.EXE, AMON.EXE, AVP32.EXE, N32SCANW.EXE, NAVAPSVC.EXE, NOD32.EXE, NAVAPW32.EXE, NAVWNT.EXE, NAVLU32.EXE, NAVRUNR.EXE, NPSSVC.EXE, NSCHEDNT.EXE, SCAN.EXE, SMSS.EXE, _AVP32.EXE, _AVPM.EXE, NSPLUGIN.EXE,

Zum Infizieren der KERNEL32.DLL speichert der Virus diese Datei unter dem Namen KLEZED.TT6 ab und verändert diese anschließend. Beim nächsten Systemstart wird die KERNEL32.DLL mit Hilfe eines entsprechenden Eintrages in der WININIT.INI durch die Datei KLEZED.TT6 ersetzt. Der Virus verändert die Adreßbereiche der externen Windows-Befehle, so daß diese in den Programmcode des Virus eingeschlossen werden. Der Virus ändert auf diese Weise sechzehn KERNEL32 Funktionen: Datei öffnen, kopieren, löschen, Ändern der Dateiattribute und viele mehr...

Der Virus hat zusätzlich noch eine gefährliche Schadensroutine in seinem Code: Am 25. Dezember zerstört der W32/Klez den CMOS-Speicher, überschreibt alle Dateien auf allen vom BIOS verwalteten Festplatten und zerstört den Flash BIOS mit der selben Routine wie der CIH-Virus.

W32/Naked

Der Internetwurm W32/Naked ist eine Win32-Anwendung, hat eine Länge von 73.728 Bytes (72KB) und wurde in Visual Basic geschrieben. Der Wurm versendet sich über Outlook

Die Email sieht wie folgt aus:

Subject:
```
Fw: Naked Wife
```

Body:
```
My wife never look like that ;-)

Best Regards,
<Name des Anwenders>
```

Attachment:
```
NakedWife.exe
```

Wird die NAKEDWIFE.EXE vom Anwender ausgeführt, öffnet dieser ein vorgetäuschtes Macromedia Flash Player-Programm. Währenddessen versendet sich der Virus per Email über das MS Outlook an alle Adressen, die im Outlook Adressbuch eingetragen sind.

Danach startet er seine Schadenroutine, indem er alle .INI, .LOG, .DLL, .EXE, .COM, .BMP im Windows-Verzeichnis und alle .INI, .LOG, .DLL, .EXE, .BMP Dateien im Windows System-Verzeichnis löscht.

Der Internetwurm installiert sich nicht auf dem System und erstellt bzw. ändert auch keine Registry-Einträge. Er führt seine Schadenroutinen nur einmal beim Öffnen der NAKEDWIFE.EXE durch und ist danach wieder inaktiv.

Das vorgetäuschte Programm zeigt ein Bild und eine "Loading..."-Nachricht, die in einer Endlosschleife programmiert wurde.

Wird im Menü Help die Option "About Macromedia Flash Player 5..." ausgewält, wird ein weiteres Fenster geöffnet mit der Meldung "You're are now FUCKED! (C) 2001 by BGK (Bill Gates Killer), die mit OK bestätigt werden kann.

W32/Nimda

Alias: W32/Nimda.eml

Bei dem Wurm W32/Nimda handelt es sich um einen Internet-Wurm, der sich als Massen-Mailer per Email versenden kann. Er kann auf allen Microsoft Windows 9x/Me und NT/2000 Plattformen ausgeführt werden.

Nimda verschickt sich selbst in einer Email als Attachment. Dieses Attachement trägt den Namen README.EXE, wobei die Dateinamenserweiterung .EXE standardmäßig nicht sichtbar ist.

Das Aussehen der Email ist unterschiedlich: Die Betreffszeile enthält einen zufälligen Text und der Body der Email ist zu meist leer. Werden Outlook oder Outlook Express eingesetzt, wird das Attachment selbst nicht in der Vorschau angezeigt.

In seltenen Fällen können die Attachments auch die Dateinamenserweiterungen .COM oder .WAV tragen.

Wird die README.EXE beispielsweise automatisch oder durch einen Doppelklick ausgeführt, kopiert sich der Wurm in des Temp-Verzeichnis von Windows. Er erstellt eine Datei unter einem veränderlichen Namen der FormMExxxx.TMP.EXE, wobei xxxx variabel ist. Diese Datei wird ausgeführtund unter Windows 9x/Me beim nächsten Systemstart wieder gelöscht.

Danach kopiert sich der Wurm als folgende Dateien im Windows- bzw. System-Verzeichnis:

WINDOWS\LOAD.EXE
WINDOWS\RICHED20.DLL
WINDOWS\SYSTEM\RICHED20.DLL
WINDOWS\SHELLNEW\RICHED20.DLL

Bereits bestehende Dateien gleichen Namens werden hierbei überschrieben.

Die Datei LOAD.EXE wird in die SYSTEM.INI eingetragen. Hierdurch wird der Wurm beim nächsten Start von Windows automatisch ausgeführt:

SHELL=exploerer.exe load.exe -dontrunold

Nach einigen Minuten erstellt der Wurm in allen Unterverzeichnissen des Windows-Laufwerkes verschiedene .EML (Email-Dateien) -oder .NWS-Dateien (Newsgroup Postings). Diese Dateien enthalten wiederum den Wurm. Existieren Freigaben mit Schreibrechten, so kopiert sich der Wurm auch in diese Netzwerklaufwerke. Auch hier als zufällige .EML- oder .NWS-Dateien in den Unterverzeichnissen.

Anschliessend setzt der Wurm alle Anzeige-Einstellungen des Windows-Explorers auf seine Standardwerte zurück. Es werden nach der Umstellung keine als 'versteckt' bzw. 'system' deklarierte Dateien mehr angezeit. Auch die Anzeige der Dateinamenserweiterungen bei bekannten Programmen wird unterdrückt.

Besteht eine Verbindung zum Internet, versucht sich Nimda per FTP eine Datei namens ADMIN.DLL herunterzuladen. Unter NT versucht der Wurm einen Guest-Account dem System hinzuzufügen und versucht ebenfalls, diese, Account Administratorrechte zu verschaffen. Darüber hinaus gibt er das komplette Laufwerk C:\ mit Schrei- und Leserechten frei. Anschließend löscht der Wurm alle Keys im folgenden Registry-Eintrag:

```
\System\CurrentControlSet\Services\Ianmanserver\Shares\Security
```

Wird der Wurm auf einem IIS Web-Server ausgeführt, erstellt er eine Datei namens README.EML. Zur automatischen Ausführung dieser Datei (beim Aufruf einer Webseite) baut er ein Java-Script ggf. in

folgende Dateien ein:

```
Index.html
Index.htm
Index.asp
Readme.html
Readme.htm
Readme.asp
Main.html
Main.htm
Main.asp
Default.html
Default.htm
Default.asp
```

Wird nun eine der oben genannten veränderten Seiten aufgerufen, wird das Java-Script ausgeführt. Der Browser lädt die Datei README.EML auf den lokalen Rechner herunter. Einige Browser öffnen diese Datei je nach Sicherheitseinstellung sofort und führen das Attachement README.EXE gleich aus.

Um sich vor dieser Art der Infektion zu schützen, sollte die Sicherheitsstufe des Internet Explorers auf HOCH gestellt werden und die IIS Web-Server mit den aktuellen Patches von Microsoft versehen werden:

Microsoft IIS 4.0

http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

Microsoft IIS 5.0
http://www.microsoft.com/windows2000/downloads/critical/q269862/daufault.asp

W32/Perrum

Der W32/Perrum ist ein Windowsvirus, der .JPG Dateien infiziert. Er ist in Visual Basic programmiert und mit dem Laufzeitpacker UPX gepackt. Die virulente Datei PROOF.EXE droppt die zwei Dateien EXTRK.EXE und REG.MP3 in das selbe Verzeichnis und legt folgenden Registry Key an:

```
HKEY_CLASSES_ROOT\jpegfile\shell\open\command
"(Default)"="EXTRK.EXE %1"
```

Danach überprüft der Virus W32/Perrum, ob sich im selben Verzeichnis .JPG Dateien befinden und infiziert diese mit seinem virulenten Code. Dieser Code wird jeweils am Ende der jeweiligen .JPG Datei angefügt. Eine .JPG Datei kann jeweils nur einmal infiziert werden und es wird pro Infektionszyklus nur eine .JPG Datei infiziert.

Führt man die .JPG Datei auf einem anderen infizierten Rechnersystem aus, sucht W32/Perrum nach einer nichtinfizierten .JPG Datei im aktuellen Verzeichnis und infiziert diese wiederum mit seinem virulenten Code.

Öffnet man eine infizierte Datei auf einem nicht infizierten System, kann der virulente Code nicht ausgeführt werden. Hierzu benötigt W32/Perrum immer die Datei EXTRK.EXE.

PROOF.EXE = 11.780 Bytes (12Kbytes) (UPX gepackt)
EXTRK.EXE = 5.636 Bytes (6 Kbytes) (Extraktor Komponente)
REG.MP3 = Enthält den Registry Key, den W32/Perrum anlegt.

W32/ProLin@mm

Der Internetwurm W32/ProLin@mm wurde in Visual Basic 6 geschrieben und versendet sich mit dem Attachment (Dateianhang) 'CREATIVE.EXE'. Als Icon enthält er das 'Shockwave Media Player' Symbol.

Wird dieser Internet-Wurm ausgeführt, erstellt er von sich folgende Kopien in folgenden Verzeichnissen: C:\CREATIVE.EXE , C:\%WINDOWS%\TEMP\CREATIVE.EXE und C:\%WINDOWS%\STARTMENÜ\PROGRAMME\AUTOSTART\CREATIVE.EXE

Im Hauptverzeichnis des Laufwerkes C:\ erstellt der Internet-Wurm eine Datei 'MESSAGEFORU.TXT', die folgende Mitteilung des Autors erhält. folgendes schreibt:

"Hi, guess you have got the message. I have kept a list of files that I have infected under this. If you are smart enough just reverse back the process. i could have done far better damage, i could have even completely wiped your harddisk. Remember this is a warning & get it sound and clear... - The Penguin"

Darunter wird eine Liste mit den erstellten Dateien und dem dazugehörigen Pfad angezeigt. Allerdings werden diese Dateien im Hauptverzeichnis des Laufwerkes C:\ angelegt (und nicht, wie es in der Liste angegeben ist, beispielsweise unter C:\WINDOWS\JAVA\....) und mit dem Anhang CHANGE AT LEAST NOW TO LINUX also "%DATEI% .ZIPchange at least now to LINUX" oder "%DATEI% .JPGchange atleast now to LINUX" angelegt.

"C:\WINDOWS\JAVA\Packages\NBDRZ1F5.ZIP
C:\WINDOWS\JAVA\Packages\FPR9ZNXF.ZIP
C:\WINDOWS\JAVA\Packages\CAIYR7FT.ZIP
C:\WINDOWS\JAVA\Packages\6BVDF1NF.ZIP
C:\WINDOWS\JAVA\Packages\FP7HFDR9.ZIP
C:\WINDOWS\JAVA\Packages\LVVBBDJP.ZIP
C:\WINDOWS\JAVA\Packages\E86LVJNP.ZIP
C:\WINDOWS\JAVA\Packages\PNRDJDFD.ZIP
C:\WINDOWS\JAVA\Packages\Q27FD3BL.ZIP
C:\Program Files\Common Files\Microsoft Shared\Stationery\Balloon Party Invitation Bkgrd.jpg
C:\Program Files\Common Files\Microsoft Shared\Grphflt\MS.JPG
C:\Program Files\WinZip\EXAMPLE.ZIP
C:\Program Files\Microsoft Office\Templates\Access\100.JPG
C:\Program Files\Microsoft Office\Templates\Access\GRAY.JPG
C:\Program Files\Microsoft Office\Templates\Access\GRAYST.JPG
C:\Program Files\Microsoft Office\Templates\Access\MC.JPG
C:\Program Files\Microsoft Office\Templates\Access\MCST.JPG
C:\Program Files\Microsoft Office\Templates\Access\MSACCESS.JPG
C:\Program Files\Microsoft Office\Templates\Access\SKY.JPG
C:\Program Files\Microsoft Office\Templates\Access\STONES.JPG
C:\Program Files\Microsoft Office\Templates\Access\TILES.JPG
C:\Program Files\Microsoft Office\Templates\Access\ZIGZAG.JPG"

Diese Dateien sind Java-Scripts, die aber nicht beschädigt oder vom Virus infiziert worden sind. Diese können einfach gelöscht werden.

Danach versucht sich der Internet Wurm via Outlook an alle im Adreßbuch stehenden Email-Adressen zu versenden.

Diese Email sieht folgendermaßen aus:

Subject:
A great Shockwave flash movie

Body:
Check out this new flash movie that I downloaded just now ... It's Great
Bye

Attachment:
CREATIVE.EXE

Um den W32/ProLin@mm entfernen zu können, müssen Sie auf die DOS-Ebene wechseln und die CREATIVE.EXE in allen oben genannten Verzeichnissen löschen. Starten Sie nun Windows neu und löschen in der Task-Leiste im Start-Menü unter Programme / Autostart den dortigen Eintrag 'CREATIVE.EXE'. Als letzteres können sie noch die .ZIP und .JPG-Dateien im Hauptverzeichnis löschen, die dort vom Wurm erstellt worden sind (siehe auch die Datei MESSAGEFORU.TXT).

W32/Yaha.E

Alias: I-Worm.Lentin.f

W32/Yaha.E ist ein Massenmailer, der sich an alle Email-Adressen versendet, die im Microsoft Windows Adressbuch, in der MSN Messenger-, Yahoo Messenger- und der ICQ-Liste stehen. Ebenfalls durchsucht er alle Dateien mit der Dateinamenserweiterung .*HT*
nach Email-Adressen ab. Das Attachment einer Email des W32/Yaha.E besitzt die Dateinamenserweiterung .BAT, .PIF oder .SCR.

Der Betreff, der Body und das Attachment einer vom W32/Yaha.E generierten Email kann unterschiedliche Inhalte besitzen. So setzt sich z.B. der Name des Attachments aus den folgenden Namensteilen zusammen:

Erster Namensbestandteil:

* loveletter
* resume
* love
* weeklyreport
* goldfish
* report
* mountan
* biodata
* dailyreport
* lovegreetings
* shakingfriendship

und folgt mit der ersten Dateinamenserweiterung:

* .wav
* .doc
* .mp3
* .bmp
* .jpg
* .gif
* .txt
* .xls
* .htm
* .mpg
* .zip
* .dat

und endet mit einer zweiten Dateinamenserweitung:

* .pif

* .bat
* .scr

Wird ein Attachment ausgeführt, kopiert sich W32/Yaha.E in das überlicherweise nicht sichtbare Recycled-Verzeichnis (C:\Recycled\) unter einem von ihm selbst gewählten Dateinamen. Im Windows-Verzeichnis wird eine Textdatei mit dem selben Dateinamen angelegt, jedoch mit der

Dateinamenserweiterung .TXT. Die Textdatei hat folgenden Inhalt:

<<<>>> <<<>>> <<<>>> <<<>>> <<<>>> <<<>>> <<<>>> <<<>>> <<<>>> <<<>>>

iNDian sNakes pResents yAha.E

iNDian hACkers,Vxers c0me & w0Rk wITh uS & f*Ck tHE GFORCE-pAK shites

bY

sNAkeeYes,c0Bra
<<>>> <<<>>> <<<>>> <<<>>> <<<>>> <<<>>> <<<>>> <<<>>> <<<>>> <<<>>>

Damit sich der Wurm W32/Yaha.E auch nach einem Systemstart erneut ausführen und Emails versenden kann, erstellt er folgenden Registry-Eintrag:

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
@="\"c:\\recycled\\<RANDOM NAME>\" %1 %*"
```

Mit diesem Eintrag wird der W32/Yaha.E bei jedem Aufruf einer .EXE Datei erneut gestartet.

Sollte eine der folgenden Anwendungen aktiv sein, versucht W32/Yaha.E diese zu beenden:

* SCAM32
* SIRC32
* WINK
* ZONEALARM
* AVP32
* LOCKDOWN2000
* AVP.EXE
* CFINET32
* CFINET
* ICMON
* SAFEWEB
* WEBSCANX
* ANTIVIR
* MCAFEE
* NORTON
* NVC95
* FP-WIN
* IOMON98
* PCCWIN98
* F-PROT95
* F-STOPW
* PVIEW95
* NAVWNT
* NAVRUNR
* NAVLU32
* NAVAPSVC
* NISUM
* SYMPROXYSVC
* RESCUE32
* NISSERV
* ATRACK

* IAMAPP
* LUCOMSERVER
* LUALL
* NMAIN
* NAVW32
* NAVAPW32
* VSSTAT
* VSHWIN32
* AVSYNMGR
* AVCONSOL
* WEBTRAP
* POP3TRAP
* PCCMAIN
* PCCIOMON

Nach erfolgreicher Infektion startet W32/Yaha.E in den meisten Fällen seinen ’Bildschirmschoner’.

W32/YAWsetup

Dieser Wurm erreicht als eine gefälschte Newsletterausgabe von www.trojaner-info.de und hat folgendes Aussehen:

Absender: webmaser@trojaner-info.de
Betreff: Trojaner-Info Newsletter 19.02.2002
Inhalt:

Hallo !

Willkomen zur neuesten Newsletter-Ausgabe der Webseite Trojaner-Info.de.

Hier die Themen im Ueberblick:

1. YAW 2.0 - Unser Dialerwarner in neuer Version

****

1. YAW 2.0 - Unser Dialerwarner in neuer Version
Viele haben ihn und viele moegen ihn - unseren Dialerwarner YAW. YAW ist nun in einer brandneuen und stark erweiterten Version verfuegbar. Alle unsere Newsletterleser bekommen ihn kostenlos zusammen mit diesem Newsletter. Also einfach die angehaengte Datei starten und YAW 2.0 installieren. Bei Fragen steht Ihnen der Programmierer des bislang einzigartigen Programmes Andreas Haak unter andreas@ants-online.de zur Verfügung. Viel Spaß mit YAW!

<http://www.trojaner-info.de/dialer/yaw.shtml>

****

Das war die heutige Ausgabe mit den aktuellsten Trojaner-Info News. Wir bedanken uns fuer eure Aufmerksamkeit und wuenschen allen Lesern noch eine angenehme Woche.

Mit freundlichem Gruss

Thomas Tietz & Andreas Ebert

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

****

Anzahl der Subscriber: 5.966
Durchschnittliche Besuchzahl/Tag: 4.488
Diese Mail ist kein Spam ! Diesen Newsletter hast du erhalten, da du in unserer Verteilerliste aufgenommen wurdest. Solltest du unseren Newsletter nicht selber abonniert haben, sondern eine andere Person ohne dein Wissen, kannst du diesen auf unseren Seiten wieder abbestellen. Oder sende uns einfach eine entsprechende E-Mail.

****

Dateianhang: yawsetup.exe

Nachdem der Dateianhang ausgeführt wurde kopiert sich der Wurm unter einem zufällig gewählten Dateinamen nach in das Windows Verzeichnis. Damit der Wurm bei jedem Systemstart geladen wird erstellt er auch folgenden Eintrag in der Registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce]
"<Zufallsname>"="\"C:\\WINDOWS\\<Zufallsname>\""
```

Außerdem benennt der Wurm die Datei Notepad.exe welche im Windows Verzeichnis zu finden ist in Notedpad.exe um. Anschließend ersetzt es die Notepad.exe durch eine Kopie seiner selbst.

Der Wurm fängt nun an, die Festplatte nach Dateien mit folgenden Erweiterungen abzusuchen: *.htm; *.php; *.cgi; *.pl; *.shtm. Aus diesen Dateien entnimmt er Emailadressen.

Danach verschickt sich der Wurm an alle gefundenen Adressen und zusätzlich an alle Einträge im Microsoft Outlook Adressbuch.

Weiter Infos finden Sie direkt auf der Webseite von www.trojaner-info.de

W95.Hybris

Der Internet-Wurm verbreitet sich über den Attachment (Dateianhang) von Emails. Hybris ist ausschließlich auf WIN32 - Systemen (Windows95/98/ME/NT/2000) funktionsfähig und benutzt hierbei die WSOCK32.DLL Library. Der Wurm verschlüsselt seinen Wurmcode semipolymorph.
HYBRIS enthält folgende Zeichenkette:

HYBRIS
© Vecna

Während der Infektion führt er folgende Schritte aus:
- Er schreibt seinen Code an das Ende der letzten File Section
- manipuliert die Funktionen conect, recv und send
- manipuliert die Adresse der DLL Entry Routine

Wenn Windows die WSOCK32.DLL benutzt und der Wurm diese nicht verändern kann, erstellt dieser eine Kopie dieser Datei, verändert diese und läßt die veränderte Datei durch die Orginaldatei beim nächsten Systemstart mit Hilfe der WININIT.INI austauschen. (Siehe hierzu auch W95/MTX)

Als weiteres erstellt der Wurm eine zufällige Datei, der seinen Code enthält im Windowsverzeichnis und erzeugt hierzu zugleich einen Registry-Eintrag, damit er beim Start auch ausgeführt wird:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
{Default} = %Windows%\WurmName
```

oder

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
{Default} = %Windows%\WurmName
```

HYBRIS nimmt z.B. folgende zufällige Namen an:

```
CCMBOIFM.EXE
LPHBNGAE.EXE
LFPCMOIF.EXE
```

Ist nun die WSOCK32.DLL durch den Wurm infiziert, überwacht dieser das Netzwerk einschließlich dem Internet. Er fängt den gesamten Datenverkehr auf dem Netzwerk bzw. Internet ab und durchsucht diesen nach Email - Adressen. Werden welche gefunden, werden an diese Adresse nach einer Weile infizierte Mails verschickt.

Die Funktionsfähigkeit des Wurmes hängt von seinen Plugins ab, die er mit einem 128 Bit langen Key (RSA) verschlüsselt und gespeichert hat. Die Plugins liegen auf der Website von VietMedia.com verschlüsselt und der Wurm kann sich aktualisieren, indem er diese Plugins von dieser Website holt. Es wurden Exemplare dieses Wurmes gefunden, die bis zu 32 Plugins enthielten.

Es ist auch bekannt, daß der HYBRIS - Wurm für seine Aktualisierungen auch die Newsgroup alt.comp.virus benutzt. Er konvertiert seine Plugins in Newsgroups-Messages und sendet Sie an den Server. Gleichzeitig schaut er auch nach neuere Versionen seiner Plugins. Diese Mails sehen dann meisten folgendermaßen aus:

```
text LNLM LmnajmnKdyfebuLuPaPmzaLyXGXKPSLSXWjKvWnyDWbGH
encr HVGT GTeLKzurGbGvqnuDqbivKfCHWbizyXiPOvKD
```

Die ersten 4 Buchstaben ist der Pluginname und die zweiten vier Buchstaben die verschlüsselte Versionsnummer.

HYBRIS kann auch Plugins in Form einer Datei erzeugen, die dann im Windows System Verzeichnis zu finden ist. Diese Dateien können dann wie folgt aussehen:

```
GAFIBPFM.AFI
DACMAPKO.ACM
MALADOLI.MAL
....
```

Diese Plugins haben verschiedene Aufgaben:
1. Senden und Empfangen von Plugins alt.comp.virus
2. Verschlüsseln der Plugins vor dem Versenden
3. Infizieren aller ZIP & RAR - Archive (fügt in alle EXE - Dateien seinen Wurm - Code ein, sichert aber alle EXE - Dateien indem er sie in EX$ umbenennt)
4. Erstellen von Betreff, Namen und Message Text in der Email
5. Verbreitung eines Virus auf Remote - Systemen mit Hilfe von dem Backdoor SubSeven

Ein Beispiel eines Plugins, das seit Anfang Dezember 2000 im Umlauf ist, sieht folgendermaßen aus: Eine große rotierende Scheibe bewegt sich auf Ihrem Bildschirm. Dieses Plugin läuft immer im Vordergrund und lässt sich nicht mehr beenden, selbst nicht über den Taskmanager.

In diesem Fall trägt sich das Plugin in die WIN.INI unter dem Eintrag: run= ein und startet automatisch mit Windows.

Beispiele für das Erstellen von Betreff, Namen und Message Texte:

Absender:
```
Hahaha <hahaha@sexyfun.net>
```

Subject:
```
Snowhite and the Seven Dwarfs - The REAL story
Branca de Neve prono!
Enanito si, pero con Sque pedazo
Les 7 coquir nains
```

Body:
```
Today, Snowhite was turning 18. The 7 Drawfs always where very educated and
polite with Snowwhite. When thy go out work at mornign, they promissed a .....

C" etait un jour avant son dix huitiem anniversaire. Les 7 nains, qui avaient
aidé "blanche neige" toutes ves années aprés qu'elle se soit enfuit.....
```

Name der Attachments:
```
sexy virgins.scr
joke.exe
atchim.exe
dunga.scr
midgets.exe
blancheneige.exe
enano.exe
enano porno.exe
blanca de nieve.scr
enanito fisgon.exe
sexynain.scr
blanche.scr
nains.exe
```

branca de neve.scr
anáo pronó.scr

Name des Attachments:

famous.exe
celebrity rape.exe
leather.exe
sex.exe
hottest.exe
cum.exe
cumshot.exe
Anna.exe
Raquel Darian.exe
Xena.exe
Xuxa.exe
Suzete.exe horny.exe
anal.exe
gay.exe
oral.exe
pleasure.exe
sexy.exe
hot.exe
asian.exe
lesbians.exe
teens.exe
virgins.exe
boys.exe
girls.exe
messy.exe
kinky.exe
fist-fucking.exe
amateurs.exe
cheerleader.exe
SM.exe
sado.exe
suck.exe
orgy.exe
black.exe
blonde.exe
sodomized.exe
hardcore.exe
slut.exe
doggy.exe

Also prüfen sie kritisch ihre Emails und öffnen sie keine unbekannten Dateianhänge...

W95/Begemont.B

Alias: Magistr

Der W95/Begemont.B ist ein Win32 Wurm, der eine Länge von 30 KB hat. Er wurde vermutlich teilweise in Assembler geschrieben. Wird dieser Virus ausgeführt, verbleibt er resident im Arbeitsspeicher. Er infiziert andere Windows .EXE Dateien sowohl lokal als auch über ein Netzwerk. W95/Begemont.B verbreitet sich über das Internet, indem er sich mit Hilfe von Outlook Express, Nescape Messenger oder Internet Mail and News er infizierte Dateien per Email verschickt.

Wird eine infizierte Datei ausgeführt, installiert sich Begemont.B resident im Arbeitspeicher und gibt folgende Meldung aus: "Kommandolinjen har forkert format".

Danach verbleibt er einige Minuten im Arbeitsspeicher ohne sichtbare Veränderungen am System durchzuführen.

Als erstes ändert er seinen eigenen Prozessnamen in den des Explorers. Mit Hilfer einer etwa 100 Bytes großen Routine "verschiebt" er sich in den Arbeitspeicherbereich des Explorers und gibt sich als eine Komponente des Explorers aus. Die nächste Schadensroutine wird etwa erst 4 Minuten später von W95/Begemont.B ausgeführt.

W95/Begemont.B infiziert dann im Windows-Systemverzeichnis eine beliebige EXE-Datei. Diese wird als Autorun-Eintrag in die Registry unter `HKLM\Software\Microsoft\Windows\Current Version\Run und in die WIN.INI unter "run="` eingetragen. Somit wird W95/Begemont.B bei jedem Systemstart ausgeführt.

Als nächstes werden alle im Windows-Systemverzeichnis stehenden EXE-Dateien mit dem W95/Begemont.B infiziert. Danach sucht er alle Netzlaufwerke auf Windows-, WINNT-, Win95- oder Win98-Verzeichnisse ab. Hier infiziert er wiederum im Systemverzeichnis die .EXE Dateien und ändert den "run=" - Eintrag der WIN.INI ab. Auch hierdurch kann er auf derart veränderten Systemen bei einem Neustart die lokale Systemumgebung infizieren.

Während der Begemont.B seine Schadensroutine ausführt, legt dieser eine DAT-Datei auf C:\ an. Der Name der Datei ist immer der Computername, der gerade unter Windows verwendet wird.

Computername	Dateiname
`WIN95`	`WIN95.DAT`
`PC750M`	`PC750M.DAT`

Einen Monat, nachdem das System infiziert wurde, führt der W95/Begemont.B eine Schadensroutine aus, indem er den Inhalt aller Dateien, die auf Disketten gespeichert werden, mit dem Text "YOURESHIT" überschreibt.

Versand per Email

Zum Versenden von Emails liest W95/Begemont.B die Einstellungen von folgenden Email-Clients direkt aus der Registry aus.

* Microsoft Outlook Express
* Netscape Messanger

* Internet Mail and News

Er entnimmt allen Email-Adressbüchern diejenigen Adressen, an die er seine infizierten Dateien verschickt. Der Dateiname für das Attachment selbst kann unterschiedlich sein. W95/Begemont.B sucht nach EXE-Dateien mit einer Größe von bis zu 132 KByte. Diese Datei wird infiziert und als Attachment versschickt.

Der Betreff der Email wird aus Wörtern und Sätzen gebildet, die der Wurm in verschiedenen DOC- und TXT-Dateien findet. Der Body der Email bleibt dabei leer.

Bekannte Varianten seit September 2001: W95/Magister.b

W95/CIH

Alias:	PE_CIH, CIH, Tschernobyl, Spacefiller	
Merkmale:	Resident, PE-Infector (Windows-EXE)	
Textstring:	Version 1.2	CIH v1.2 TTIT
	Version 1.3	CIH v1.3 TTIT
	Version 1.4	CIH v1.4 TATUNG
Länge:	Version 1.2	1003 Bytes
	Version 1.3	1010 Bytes
	Version 1.4	1019 Bytes
Plattform:	Windows 95/Windows 98	

W95/CIH ist ein residenter Virus, der Windows-Programme (PE-Dateien) befällt. Er infiziert PE-Dateien derart, daß die Länge infizierter Dateien nicht verändert wird. Anhand der Kenntnisse über unbenutzte Bereiche innerhalb dieser PE-Dateien kann er sich in mehrere Teile aufteilen. W95/CIH enthält destruktive Schadensroutinen: Überschreiben des BIOS im Flash-ROM und Überschreiben aller Festplatten.

Dieser Virus ist in den letzten zwei Wochen verstärkt auch in Deutschland aufgetreten. H+BEDV stellte bereits mit der Version 5.13.1 eine wirksame und leistungsfähige Sucherkennung zu Verfügung. Mit der jetzt freigegebenen Version 5.13.2 ist nun auch die Reparatur dieses Virus möglich. AntiVir geht hier den nicht sonst üblichen Weg, nur den Ladeteil des Virus zu deaktivieren ("Metzgermessermethode"), sondern es erfolgt eine Reparatur nach der "Skalpellmethode". Da W95/CIH sich bei der Infektion einer Datei selbst in verschiedene Teile aufteilt und über verschiedene Sektionen in der zu infizierenden Datei verstreut, müssen bei einer Reparatur alle vom Virus veränderten Sektionen gesondert behandelt werden. Dadurch läuft AntiVir nicht Gefahr, Teile des Virus intakt zu lassen.

Viele andere Antivirenprogramme überschreiben nur die Installationsroutine des Virus oder "reparieren" allein durch Berichtigen des Programmeinsprunges. So verbleiben andere Teile des Virus in der eigentlich immer noch infizierten Datei in ausführbarer Form. Dies bedeutet, daß auch die Schadensroutinen noch in der Datei vorhanden sind und ggf. auch unkontrolliert (z.B. durch Programmabsturz, Fehler im Wirtsprogramm, Doppelinfektion etc.) ausgeführt werden können.

Da AntiVir genaue Kenntnisse sowohl über den Aufbau des Virus als auch den Aufbau der PE-Dateien besitzt, ist es AntiVir möglich, eine Qualitätsreparatur durchzuführen. AntiVir entfernt die einzelnen Teile des Virus in den unterschiedlichen Sektionen und stellt die internen Verwaltungsinformationen der Sektionen wieder her. Hierdurch sind diese Programme nach Reparatur durch AntiVir wieder gefahrlos einsetzbar.

Die Schadensroutinen des Virus variieren je nach Version. Die Version 1.2 versucht am 26. April und die Version 1.3 am 26. Juni eines jeden Jahres das BIOS im Flash-ROM zu überschreiben. Die Version 1.4, sie ist momentan die am häufigsten festgestellte Version, scheint eine Weiterentwicklung zu sein: Sie versucht das Überschreiben des BIOS im Flash-ROM am 26. eines jeden Monats durchzuführen. Allen Versionen gemeinsam ist, daß auch noch alle Festplatten am jeweiligen Auslösedatum durch direkte Zugriffe überschrieben werden. Damit dürften die meisten sog. Notfalldisketten wertlos sein, wenn nicht zusätzlich ein komplettes Backup vorliegt!

Da von dieser Art der Schadensroutinen alsbald Nachahmer zu erwarten sind, stellt die H+BEDV PC-Anwendern das Leseprogramm IROMREAD für Flash-ROM zur Verfügung. Dieses Programm liest den Inhalt eines Flash-ROMs über den jeweiligen Chipsatz aus und speichert die Daten als Datei auf einem Datenträger ab.

Technische Informationen:

Persönliche Vorbemerkung: W95/CIH ist nicht unbedingt ein "Killervirus", CIH ist halt ein Virus, der einmal etwas anders, evtl. auch etwas Neues macht. Deswegen geht die Welt nicht unter und es ist auch kein "hardwarezerstörender" Virus (wobei sich aber trefflich über das Bewegen von Atomen in Festplatte/Flash-ROM streiten ließe). Nicht jeder Virus ist gleich so gefährlich, weil aus jeder Pressemitteilung das Blut nur noch so herausläuft. So haben beispielsweise viele englischsprachige Makroviren die angenehme Eigenschaft, auf deutschsprachigen Office-Installationen gar nicht lauffähig zu sein.

W95/CIH ist ein reinrassiger Windows 95/98-Virus und nur unter diesen beiden Plattformen lauffähig. Aufgrund der von ihm überwachten Schnittstelle zum Dateisystem (IFSMGR-Hook) läuft er nicht unter Windows NT bzw. Windows 3.1x. Er infiziert nur die 32bit-Programmdateien (Windows-EXEs, die PE-Dateien). Wird eine infizierte Datei auf einem nicht infizierten Rechnersystem zum ersten Mal gestartet, fordert er über PageAllocate Speicher an und kopiert zuerst einmal seinen (gerade laufenden) "Infektionsteil" dorthin. Anschließend kopiert er seine übrigen Programmbestandteile ebenfalls in diesen Speicher. Vermutlich aufgrund eines Programmierfehlers fordert W95/CIH insgesamt 8KB an Speicher an, 4KB wären ausreichend gewesen. Zuletzt "klinkt" er sich noch in die Schnittstelle zum Dateisystem (IFSMGR-Hook) ein und übergibt die weitere Kontrolle dem eigentlichen Wirtsprogramm. Durch Überwachen der IFSMGR-Hooks bekommt er jedes Öffnen einer Datei mit und kann entsprechend reagieren. Um nun nicht allzutief in jede neue Datei "hineinzusuchen", ob sie noch infiziert werden muß, bedient sich der Virus eines kleines Tricks: Ist das letzte Byte des DOS-Stubs ("Dieses Programm benötigt Microsoft-Windows") ungleich 00h, dann wird nicht mehr infiziert.

Der Virus "springt" direkt vom Ring 3 (Ebene der Applikationsprogramme) zum Ring 0 (Ebene der Systemprogramme). Auf diesem Ring 0 stehen dem Virus alle Systemfunktionen zur Verfügung, hier laufen seine wichtigen Programmteile ab. Der Virus prüft alle EXE-Dateien und infiziert ab der Version 1.4 solche EXE-Dateien nicht, die als Sektionsnamen "nZIP" enthalten (der WinZip-SelfExtractor prüft, ob sein Header und/oder seine komplette Sektion unverändert ist).

Muß infiziert werden, hat der Virus bereits alle wichtigen Informationen parat: Er sucht nach unbenutzten Bereichen ("Löchern") in den einzelnen Sektionen einer PE-Datei. Hierbei ist bis auf die Startsektion, sie muß mindestens 184 Bytes unbelegten Platz frei haben, die Länge des unbelegten Bereiches eigentlich egal. Jede Seite ("Page") belegt unter Windows 95/98 exakt 512 Bytes. Wird vom Wirtsprogramm innerhalb einer Sektion die letzte Page nicht komplett benötigt, bleiben unbenutzte Bereiche übrig. Daß der Virus auch die Verwaltungsinformationen zu diesen einzelnen Sektionen verändert, sei nur am Rande erwähnt.

Nach einer Infektion überprüft der Virus das Datum, ob seine Auslösebedingung erfüllt ist. Danach versucht W95/CIH sowohl das Flash-ROM als auch die Festplatten zu überschreiben. Festplatten werden über direkte Schreibzugriffe (IOS_SendCommand) angesprochen bzw. überschrieben.

Am meisten diskutiert wird momentan die Möglichkeit des Löschens oder Überschreibens des Flash-ROMs. Diese Flash-ROMs sind ab Rechnern der Pentium-Klasse im Einsatz. In der Tat sind im Virus Programmsequenzen enthalten, die das Überschreiben des Flash-ROMs in ganz bestimmten Fällen erlauben, jedoch nicht in allen Fällen. Der Virus wurde vermutlich auf einem Rechnersystem mit einem TX-Chipsatz "getestet". Insgesamt ist das Lesen aus einem bzw. das Schreiben in ein Flash-ROM ein mehrstufiger Prozeß und hardwarespezifisch.

Physikalisch kennt das Rechnersystem bzw. ein Anwendungsprogramm nur Speicheradressen, an die etwas geschrieben bzw. von denen etwas ausgelesen wird. Seit langer Zeit belegt das ROM-BIOS das gesamte F000-Segment im ersten Megabyte Adressraum. In Zeiten von Shadow-ROM müssen aber Daten aus dem "logischen" F000-Segment nicht mehr aus dem "physikalsichen" F000-Segment stammen: Über die Kombination Chipsatz und MMU (Memory Management Unit) kann der komplette ROM-Inhalt schon ins (schnellere) RAM kopiert worden sein. Ein Zugriff auf das F000-Segment wird nun von einer anderen Speicherstelle aus bedient, die irgendwo im Adressraum des Prozessors liegen kann. Darüber hinaus sind die moderneren BIOSse zumeist größer als 64KB, nämlich 128KB, und belegen

zusätzlich noch das E000-Segment. Nach dem Booten ist dieser Bereich verschwunden und nicht mehr sichtbar, da der verwendete Programmcode (Setup etc.) nicht mehr benötigt wird. Beim Schreiben auf das Flash-ROM müssen also zuerst wieder "geordnete Verhältnisse" hergestellt werden. Hierzu wird der Chipsatz benötigt, dem über bestimmte Kommandos mitgeteilt werden kann, vom Shadow-ROM bzw. Mapping von Speicherbereichen Abstand zu nehmen. Hat der Chipsatz dies vorgenommen, erst dann kann dem Flash-Writer über geeignete Kommandos mitgeteilt werden, bestimmte Adreßbereiche bzw. Speicherzellen zum Schreiben zu öffnen bzw. vorzubereiten.

Die Chipsatz-spezifischen Kommandos zum Einblenden der "richtigen" Adreßbereiche können unterschiedlich sein, die Befehle zum Programmieren der Flash-ROMs waren sich bei den getesteten LX/HX/TX-Chipsätzen doch sehr ähnlich.

Bisher konnten wir folgende Flash-ROM-Typen (nicht Chipsätze) als gefährdet herausfinden:
Flash-ROM

Vpp
AMD 29F010 5V
ATMEL 29C010A 3V
ATMEL 29C010A 5V
INTEL 28F001BX-T 12V
INTEL 28F010 12V
MXIC 28F1000A 12V
MXIC 28F1000AP 12V
SST 28EE010 5V
SST 28EE011 5V
WINBOND 29ee011 5V

Die Angabe der Programmierspannung ist deshalb von Interesse, da sich anhand der Programmierspannung ablesen läßt, ob evtl. noch ein Schreibschutzjumper vorhanden ist oder sein müßte. Generell kann gesagt werden, daß alle Flash-ROMs durch solche Attacken "verwundbar" sind, es sei denn, sie haben einen funktionierenden Schreibschutzjumper bzw. eine funktionierende Boot-Block-Protection. Ist der verwendete Typ aus dem 12V-Lager und der Jumper steht in Stellung schreibgeschützt, dann besteht keine Gefahr und das Flash-ROM kann nicht überschrieben werden. Ist das Flash-ROM ein Mehrbereichstyp (dual voltage flashable), dann ist selbst ein vorhandener Schreibschutzjumper mehr oder weniger wertlos. Lediglich in den Fällen, in denen der Boot-Block des Flash-ROMs als extra geschützt markiert ist, wäre nach dem Flashen noch eine Wiederherstellung mit einfachen Mitteln möglich. Bei einigen Flash-ROMs werden (PCI-)Setup-Informationen dynamisch gespeichert, Flash-ROMs werden hier als willkommener Zwischenspeicher "mißbraucht".

Hat das verwendete Rechnersystem eine zu diesem Virus "kompatible" Chipsatz/Flash-ROM-Kombination, dann versucht der Virus an seinem Auslösedatum Teile des Flash-ROMs mit den Werten 55 und FF zu überschreiben. Stürzt dabei das Rechnersystem mit einem Page Fault ab, wurde vermutlich versucht, in das "nicht umgemappte" E000-Segment zu schreiben bzw. auf den ursprünglichen ("gemappten") Inhalt zuzugreifen.

W95/CIH ist auf den TX-Chipsatz abgestimmt. Es ist jedoch zu erwarten, daß zukünftige Viren sich nicht nur mit einem Chipsatz "begnügen". Besonders problematisch wird dies, wenn man an eingelötete und/oder dauerhaft beschreibbare Flash-ROMs denkt. Diese werden häufig in Notebooks oder Laptops eingesetzt. Hier ist das Einsenden des kompletten Rechners an den Hersteller schon fast unvermeidlich. Aber auch dem normalen Anwender wird vermutlich ein neues Systemboard verkauft werden, wenn sich das alte als kaputt, sprich nicht mehr bootfähig erweist.

Intel-Chipsatz-kompatibles Leseprogramm für Flash-ROM

Um für den "Fall des Falles" aber noch eine Kopie seines kompletten BIOS zu haben, wurde das

Programm IROMREAD geschaffen. Dieses Programm legt bei handelsüblichen Chipsätzen eine Kopie des BIOS als Datei auf Diskette ab. Die H+BEDV stellt dieses Programme als selbstextrahierendes Diskettenimage zur Verfügung. Der Anwender braucht nur noch eine formatierte 1,44MB-Diskette einzulegen und das Imageprogramm aufzurufen.

W95/MTX

Alias: Iworm_MTX, I-Worm.MTX, Matrix

Der MTX - Wurm besteht aus drei Komponenten : Virus, Email-Wurm, und Backdoor. Der Virus läuft auf allen Win32 - Systemen (Windows 9x, Windows NT, Windows 2000). Er infiziert .EXE und .DLL Dateien, sendent Emails mit einem infizierten Attachment (Dateianhang) und installiert Backdoor-Module, um Plugins von einem Server zu hohlen und zu aktivieren, auf ihren PC.

Die Virus Komponente
Der Virus entschlüsselt zuerst seinen Code und führt sich dann aus. Der Virus sucht nach aktiven Komponenten folgendender Anti - Viren - Programme:

```
AntiViral Toolkit Pro
AVP Monitor
Vsstat
Webscanx
Avconsol
McAfee VirusScan
Vshwin32
Central do McAffee VirusScan
```

Wird eines der Komponenten gefunden, wird der Virus nicht aktiv!

Anschließend dekomprimiert der Virus seine Komponenten und installiert diese im Windows Verzeichnis. Dann befinden sich folgende Komponente auf Ihrem PC:

`IE_PACK.EXE` - "sauberer" Wurm - Code
`WIN32.DLL` - Wurm - Code mit Virus infiziert
`MTX_.EXE` - Backdoor -Code

Diese drei Dateien sind mit dem Attribut "versteckt" versehen und stehen im Windows - Verzeichnis, wie auch im Windows\System - Verzeichnis. Der Virus infiziert alle .EXE und .DLL Dateien die sich im Windows, Temp und in dem Verzeichnis stehen, in dem der Virus ausgeführt wird. Es ist nicht auszuschließen, daß lebenswichtige Windows-Dateien beschädigt oder zerstört werden, so daß Sie Windows beim nächsten Neustart nicht mehr starten können.

Die Wurm Komponente
Die Wurm - Komponente manipuliert die Datei WSOCK32.DLL im Windows - Verzeichnis, indem er Teile seines Codes an das Ende dieser Datei anhängt und einen Send - Befehl an WSOCK32.DLL gibt. Dadurch manipuliert der Wurm alle Emails, die vom infizierten System versendet werden.

WSOCK32.DLL wird möglicherweise von Windows schon genutzt und somit kann der Wurm keine Änderungen an dieser Datei vornehmen. Um dies zu ändern, kopiert er WSOCK32.DLL mit dem Namen WSOCK32.MTX, infiziert diese Kopie und schreibt eine Anweisung in die WININIT.INI, daß die orginale WSOCK32.DLL beim nächsten Start gegen die infizierte WSOCK32.MTX ausgetauscht wird.
In die WININIT.INI schreibt er folgende Anweisung:

```
NUL=C:\WINDOWS\SYSTEM\WSOCK32.DLL
C:\WINDOWS\SYSTEM\WSOCK32.DLL=C:\WINDOWS\SYSTEM\WSOCK32.MTX
```

Dadurch wird der Wurm aktiviert und überwacht sämtliche Internet-Zugriffe (Web und FTP) des betreffenden Systems ebenso wie alle Emails, die von diesem System versandt werden. An manche Internet-Sites werden die Zugriffe verhindert und es können keine Email an diese Domains verschickt werden. Für die Erkennung benutzt der Virus die folgenden Kombinationen von vier Zeichen:

```
afee
avp.
nai.
nii.
f-se
lywa
mapl
ndmi
pand
soph
tbav
yenn
```

Weiterhin verhindert der Wurm das versenden von Email an folgende Domains:

```
bca.com.nz*
beyond.com*
bmcd.com*
cellco.com*
earthlink.*
f-secure.*
il.esafe.c*
mcafee.com*
netsales.n*
perfectsup*
symantec.c*
wildlist.o*
```

Der Wurm spioniert beim erstellten von anderen Email hinterher und versucht eine zweite Email zu verschicken mit einem Attachment (Dateianhang) , die aber keinen Betreff und keine Email- Text enthält. Die angehängte Datei hat meist einer der folgenden Namen:

```
ALANIS_Screen_Saver.SCR
ANTI_CIH.EXE
AVP_updates.EXE
BILL_GATES_PIECE.JPG.pif
BLINK_182.MP3.pif
FEITICEIRA_NUA.JPG.pif
FREE_xxx_sites.TXT.pif
FUCKING_WITH_DOGS.SCR
Geocities_Free_Sites.TXT.pif
HANSON.SCR
INTERNET_SECURITY_FORUM.DOC.pif
IS_LINUS_GOOD_ENOUGH!.TXT.pif
I_am_sorry.DOC.pif
I_wanna_see_You.TXT.pif
```

Der Wurm sendet die Datei WIN32.DLL, die bei der ersten Installation von MTX von der Virus - Komponente auf dem infizierten System generiert wurde.

Die Backdoor Komponente
Wird die Backdoor Komponente ausgeführt, fügt sie einen neuen Registry-Key ein:

```
HKLM\Software\[MATRIX]
```

Ist der Key bereits eingetragen, wird die Installation übersprungen. Ist dies nicht der Fall, trägt sich das Backdoor in der Registry in die Auto Run Section ein:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
SystemBackup=%WinDir%\MTX_.EXE
```

Dabei ist %WinDir% das Windows Verzeichnis.

Das Backdoor bleibt als eine verborgene Anwendung im Hintergrund aktiv und ruft eine Routine auf, die irgendwann Verbindung mit dem Internet aufnimmt. Hier holt er sich Dateien, die er in das infizierte System einfügt. Dadurch kann der MTX andere Viren, Trojaner oder Backdoors holen.

In der bekannte Version hat diese Routine allerdings einen Programmierfehler, der einen Windows Fehler verursacht.

Um den MTX Virus zu entfernen rufen Sie über START - AUSFÜHREN das Programm REGEDIT auf und entfernen Sie die Auto - Run - Funktion und den MATRIX - Key aus der Registry!

Um ein von MTX infiziertes System weithin wieder zu säubern, müssen Sie Windows beenden und ins DOS gehen und von hier die folgenden drei Dateien löschen:

```
IE_PACK.EXE
WIN32.DLL
MTX_.EXE
```

Das Orginal der sauberen WSOCK32.DLL sollte von einem Backup geholt werden.

W97M/Resume.A

Nach Liebesgruß jetzt neue Gefahr in Form eines Bewerbungsschreibens.

Der Wurm selbst versteckt sich in einem MS Word Dokument. Beim öffnen des Attachments verschickt sich der Wurm an alle Adressen im Outlook Adressbuch. Die Email sieht wie folgt aus:

Subject:
Resume - Janet Simons

Body:
To: Director of Sales/Marketing,

Attached is my resume with a list of references contained within. Please feel free to call or email me if you have any further questions regarding my experience. I am looking forward to hearing from you.

Sincerely,

Janet Simons

Attachment:
Resume.doc

Nachdem das Dokument geschlossen wurde kopiert sich der Wurm in das Autostart-Verzeichnis. Somit wird er bei jedem Systemstart mitgeladen.
Der Wurm fängt jetzt an, alle Dateien auf der Festplatte zu löschen. Auch Dateien auf einer eingelegten Diskette oder gemappten Netzwerklaufwerken sind hiervon betroffen. Bisher ist der Virus noch nicht in Deutschland aufgetreten.

Dieser Makrovirus wird seit der Version 6.01.00.09 der 'ANTIVIR.VDF' erkannt.

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 effektiver 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.

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.

Worm.Pikachu

Der neue Internet-Wurm Pikachu (alias Pokey) versendet sich nach dem Ausführen - wie auch schon der VBS-Virus "I love you" - via MS Outlook an alle Kontakte im Adressbuch. Jedoch ist er kein VBS-Wurm sondern eine normale Anwendung (.exe).

Im Virenlabor von AntiVir ließ sich der Virus zwar verschicken, jedoch fehlte der Dateianhang, denn ursprünglich sollte sich der Virus an jede Email anhängen. Dies könnte am leicht fehlerhaften Programmcode des Virus liegen.

Ein harmloses Pokemon-Icon verleitet den Anwender zum Öffnen der Datei.

Nach dem Ausführen des Virus erscheint dieses Bild auf dem Monitor:

Während der Anwender sich noch über das Bild freut, überschreibt der Virus die Autoexec.bat:

```
@ECHO OFF
del C:\WINDOWS\*.*
del C:\WINDOWS\SYSTEM\*.*
```

Durch diesen Eintrag werden bei einem Neustart das gesamte Windows- und Windows-System Verzeichnis gelöscht, was für den Anwender einen totalen Datenverlust bedeuten kann, da eine komplette Neuinstallation des Betriebssystems fällig ist.

Der Email-Wurm wird seit der Version 6.03.00.14 von AntiVir erkannt.

Worm/Anset.B

Der Wurm Worm/Anset.b hat eine Größe von 179.712 Bytes und ist UPX gepackt. Er versendet sich mit Hilfe einer eigenen SMTP-Komponente. Die Email sind folgendermaßen aus:

Subject:
ANTS Version 3.0

Body:
Hi,

Anhängend die neue Version 3.0 von ANTS, dem bislang einzigartigen

kostenlosen Trojanerscanner. Zum installieren einfach die angefügte Datei ausführen.

Attached you will find the brand new Version 3.0 of ANTS, the unique

freeware trojan scanner. To install ANTS simply run the attached setup file.

Adieu, Andreas

webmaster@avnetwork.de

http://www.ants-online.de

Attachment:
ANTS3SET.EXE

Wird das Attachment ANTS3SET.EXE ausgeführt, kopiert der Wurm eine .EXE Datei in das Windowsverzeichnis mit einem zufällig gewählten Dateinamen. Danach erstellt er folgenden Registry-Eintrag:

```
[HKCU\Software\Microsoft\Windows\Current Version\RunOnce]
<%Zufallsname%> = "C:\WINDOWS\<%Zufallsname.EXE%>
```

Der Wurm sucht nach Emailadressen. Er durchsucht das Outlook Adressbuch, danach alle auf dem Laufwerk C: befindlichen .PHP, .HTM, .SHTM, .CGI und .PL Dateien. Er versendet sich an die gefundenen Emailadressen.

Er erstellt eine Liste verfügbarer SMTP Server. Zusätzlich nutzt der Wurm folgende 8 anonyme Server, über die er sich versenden kann:

```
200.52.69.xxx
200.52.69.xxx
193.92.94.xxx
12.34.208.xxx
195.229.189.xxx
196.40.0.xxx
```

196.40.0.xxx
txxxd.com

Sollte es sich um einen anonymen Server handeln, versendet sich der Wurm mit dem Absendernamen "Andreas Haak" und der Emailadresse "webmaster@avnetwork.de". Handelt es sich um keinen anonymen Server, wird die Emailadresse entsprechend abgeändert, damit die Email nicht zurückgewiesen wird.

Worm/Aphex

Alias: W32/Aplore.A

Worm/Aphex ist ein Massenmailer, der sich über Email, IRC oder den AOL Instant Messenger (AIM) verbreiten kann. Er versendet sich als Email über Microsoft Outlook mit Hilfe des Outlook Adressbuchs. Eine vom Worm/Aphex versandte Email sieht folgendermaßen aus:

Subject:

Body:

Attachment:
`psecure20x-cgi-install.version6.01.bin.hx.com`

Führt man das Attachment aus, kopiert sich der Wurm als Explorer.exe und psecure20x-cgi-install.vers.... in das Windows Systemverzeichnis und fügt folgenden Key der Registry hinzu:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
Explorer=C:\Windows\System\Explorer.exe
```

Zusätzlich wird die Datei Email.vbs in das Windows Systemverzeichnis gedroppt. Die benötigt Worm/Aphex um sich über Outlook zu versenden.

IRC-Client

Worm/Aphex besitzt eine eigene IRC-Engine. Mit deren Hilfe kann er sich auf öffentliche IRC-Server einloggen. Aphex wechselt zwischen mehrere Channels und sendet eine private Nachricht an alle eingeloggten User.

Die private Nachricht hat folgenden Inhalt:

<deloria14> FREE PORN: http://free:porn@192.xxx.xxx.xxx:8180

Klickt der Anwender auf den Link, wird eine Internetseite angezeigt.

Klickt der Anwender auf den Link HERE, öffnet sich ein Download-Fenster. Wählt der Anwender die Option "Öffnen vom aktuellen Ort", infiziert Wurm/Aphex das System.

AOL Instant Messanger (AIM)

Hat Worm/Aphex Ihr System infiziert, wartet dieser, bis der AOL Instant Messanger gestartet wird. Dann sendet er eine von diesen folgenden Nachrichten an alle Anwender, die auf der Kontaktliste stehen:

* I wanted to show you this,
* please check out,
* hey go to,
* try this,
* this is cool,
* I like this,
* what about,
* have you seen,

* lol,
* wow,
* btw, download this,

Dahinter wird ein Hyperlink angezeigt (siehe "IRC-Client'). Klickt der Anwender auf diesen Link, wird ihm eine Webseite angezeigt, von der sich Worm/Aphex auf das System installieren kann.

Worm/Badtrans

Bei dem Internetwurm Badtrans handelt es sich um eine Win32 Anwendung, welche sich mit Hilfe von Emails über Microsoft Outlook oder Outlook Express verbreitet. Der Wurm versendet ein infiziertes Attachment (PE EXE Datei), welches eine Wurm- und eine Trojanerkomponente beinhaltet.

Wenn die infizierte Datei ausgeführt wird, installiert Worm.Badtrans seine Komponenten auf dem System. Der Wurm kopiert sich selbst als INETD.EXE in das Windows Verzeichnis. Die Trojaner Komponente wird mit dem Namen HKK32.EXE in das Windows Verzeichnis kopiert und wird ausgeführt. Der Trojaner verschiebt sich in das Windows System Verzeichnis mit dem Dateinamen KERN32.EXE und installiert im selbigen Verzeichnis die Datei HKSDLL.DLL.

Der Wurm registriert sich in die WIN.INI unter Windows 9x mit dem Eintrag :

run=C:\WINDOWS\INETD.EXE

während unter Windows NT / 2000 der Wurm folgender Registry Eintrag vornimmt:

```
HKCU\Software\Microsoft\Windows NT\Current Version\Windows
RUN = C:\WINDOWS\INETD.EXE
```

Der Trojaner registriert sich mit einem Registry Eintrag in RunOnce:

```
HKLM\Software\Microsot\Windows\Current Version\RunOnce\
kernel32 = kern32.exe
```

Mit diesem Eintrag wird der Trojaner bei jedem Start von Windows automatisch geladen.

Um seine Aktivitäten während der Infektion des Systems zu verbergen, zeigt der Wurm ein gefälschtes Fenster mit dem Inhalt:

Install error

File Data corrupt

Probably due to bad data transmission or bad disk access.

Der Wurm versendet sich nicht gleich nach dem Infizieren des Systems, sondern wartet den nächsten Start von Windows ab. Er registriert sich selbst als versteckten Service Prozess und warten 5 Minuten, bevor seine Routine gestartet wird. Der Wurm öffnet alle gelesenen oder ungelesenen Emails, die im Microsoft Outlook oder Outlook Express stehen und versendet diese mit dem Originaltext und einem infizierten Attachment zurück an den Absender.

Die **Attachments** können folgende Namen haben:

```
images.pif
hamster.ZIP.scr
YOU_are_FAT!.TXT.pif
Pics.ZIP.scr
README.TXT.pif
new_Napster_Site.DOC.scr
S3msong.MP3.pif
searchURL.scr
SETUP.pif
Card.pif
```

Me_nude.AVI.pif
Humor.TXT.pif
fun.pif
Sorry_about_yesterday.DOC.pif
docs.scr

Worm/Badtrans.B

Badtrans.B ist ein Wurm, der sich über Email mit Hilfe von MAPI (Messaging Application Program Interface) versendet. Der Name des Attachments setzt sich aus den folgenden drei Teilen zusammen, die in zufälliger Reihenfolge einer Liste entnommen werden:

erster Teil:

```
FUN
HUMOR
DOCS
S3MSONG
RESUME
IMAGES
PICS
CARD
SETUP
Sorry_about_yersterday
ME_NUDE
YOU_ARE_FAT!
HAMSTER NEWS_DOC
README
SEARCHURL
```

zweiter Teil:

```
.DOC.
.MP3.

.ZIP.
```

dritter Teil:

```
pif
scr
```

Einen Text im Body oder Betreff der Email gibt es nicht.

Wird das Attachment ausgeführt, kopiert der Wurm sich in das Windows Systemverzeichnis unter dem Namen KERNEL32.EXE und fügt den folgenden Key der Registry hinzu:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce]
"Kernel32"="\%WINDIR%\SYSTEM\KERNEL32.EXE
```

Weiterhin droppt der Wurm die Datei KDLL.DLL in das Windows System Verzeichnis, die einen Trojaner zum Protokollieren von Tastatureingaben darstellt.

Worm/Brit.B

Bei dem Wurm BritneyPic.2 handelt es sich um einen Massenmailer, der sich über Microsoft Outlook mit Hilfe des Outlook Adressbuches versendet. Eine von Brit.B versendete Email sieht folgendermaßen aus:

Subject
```
RE:Nuevo video de Caifanes
```

Body
```
Caifanes regresa y te muestra su nuevo video musical ...

Regards,

Harry Hirsch
```

Attachment
```
caifanes.chm
```

Führt man das Attachment "CAIFANES.CHM" aus, öffnet sich ein Fenster mit dem Text "Permite Active X para ver el nuevo video de Caifanes", während Brit.B in das Verzeichnis \Windows\Application Data\ Microsoft\HTML Help\ eine Datei namens hh.dat erstellt und sich über Outlook versendet.

In der Datei hh.dat werden für den Wurm nützliche Informationen gespeichert, z.B. von welchem Pfad das Attachment gestartet wurde.

Worm/Brit.F

Alias: Chick.F, I-Worm.Brit.g

Bei Brit.F handelt es sich um einen Internet Wurm, der sich über das Emailprogramm Microsoft Outlook und über das mIRC-Programm mit Hilfe der 'Script.ini'.

Eine vom Wurm versandte Email hat den folgenden Inhalt:

Subject:
```
RE: Korea Japan Results
```

Body:
```
Take a look at these results ...
Regards,
<User Name>
```

Attachment:
```
Koreajapan.chm
```

Wird das Attachment geöffnet, wird der Benutzer gefragt:"Enable Active X To See Korea Japan results?"

Wird diese Frage mit YES beantwortet, führt der Wurm seine Schadensroutine aus. Worm/Brit.F kopiert sich in das Windows Verzeichnis als koreajapan.chm. Er sucht auf den lokalen Laufwerken C:, D: und E: nach der Datei Script.ini des Programmes mIRC und verändert diese. Danach versendet sich Brit.F über Outlook an den ersten Adressat im Outlook Adressbuch.

Worm/Calil

Alias: W32/Lilac

Worm/Calil ist ein Internet Wurm und wurde in der Programmiersprache Visual Basic geschrieben. Er hat eine Größe von 12.208 Bytes (ungepackt 30.720 Bytes). Wird Worm/Calil ausgeführt, versendet er sich über Microsoft Outlook an alle Emailadressen im WAB (Windows Adressbuch).

Eine vom Worm/Calil versandte Email hat den folgenden Inhalt:

Subject:
```
FW:FW: LILAC project video attach
```

Body:
```
Things that the govt. dont want you
```

Attachment:
```
Lilac_What_a_wonderfulname.avi.exe
```

Es kann vereinzelt vorkommen, dass das Attachment mit einer Größe von 0 Bytes versendet wird oder dass es komplett vergessen wird. Hierbei handelt es sich um eine fehlerhafte Programmroutine des Wurmes.

Wird das Attachment der Email ausgeführt, zeigt Worm/Calil ein Fenster mit der Meldung: "Error54: Media Player not installed correctly", das mit OK bestätigt werden kann.

Und kopiert sich als 'Lilac_What_a_wonderfulname.avi.exe' in eines der Verzeichnisse:

C:\Win98\Temp\
C:\Win95\Temp\
C:\Winnt\Temp\
C:\Winme\Temp\
C:\Winxp\Temp\
C:\Windows\Temp\

Danach ändert der Wurm folgende Keys in der Registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion]
RegisteredOwner=xEnOcrAtEs
LegalNoticeCaption=Owned by:
LegalNoticeText=Owned by: xEnOcrAtEs
```

und fügt den folgenden Registry Key hinzu:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"Lilac"="c:\\windows\\temp\\LILAC_WHAT_A_WONDERFULNAME.avi.exe"
```

Er versendet sich an alle Emailadressen im WAB (Windows Adressbuch) mit Hilfe von Outlook.

Sollte sich Worm/Calil nicht korrekt ausführen können, wird in der Autoexec.bat folgende Zeilen hinzugefügt, welche aber keinerlei Schadensroutinen enthalten:

echo MERRY CHRISTMASS AND A HAPPY NEW YEAR !!!
echo HAPPY HALLOWEEN !!!
echo HAPPY VALENTINES DAY !!!

```
echo   HAPPY LABOR DAY !!!
echo   BONIFACIO DAY !!!
echo   RIZAL DAY   !!!
echo   HAPPY INDEPENDENCE DAY !!!
echo   HOLY WEEK   !!!
@echo   off
echo from:   OPEY A .
pause
```

Worm/Cervivec

Bei dem Worm/Cervivec handelt es sich um einen Massenmailer. Die .EXE Datei hat eine Größe von 228.872 Bytes. Er versendet sich als Email mit Hilfe der Kontakliste des ICQ. Er formuliert eine von Ihm gesendeten Emails in verschiedenen Sprachen:

Email1:
```
"Cau posilam ti cerviky tak se na to podivej (virus to neni)"
```

Email2:
```
"Cau posielam ti cerviky tak sa na to pozri (virus to neni)"
```

Email3:
```
"Hallo, Ich habe ein guter Witz-Wurm so sieh! (kein virus)"
```

Email4:
```
"Hi, I have some cool joke - worms so have a look at it (no virus)"
```

Email5:
```
"J'ai une bonne blague ca s'appelle verre de terre alors jette un coup d'oeil
(il n'y a pas de virusi)"
```

Email6:
```
"Czesc, mam swietnz dowci te mando los gusanilloes. Pues mirarlos (no es un
virus)"
```

Email7:
```
"Hola te mando los gusanilloes. Puesmirarlos (no es un virus)"
```

Attachment:
```
Ntknrl.exe
```

Wird das Attachment einer vom Worm/Cervivec versandten Email ausgeführt, installiert er sich in das Windows Systemverzeichnis als "ntkrnl.exe" und legt folgenden Autorun Key in der Registry an:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Kernel Loader=C:\WINDOWS\system32\ntkrnl.exe -LOADDRIVERS=TRUE
```

Somit wird Cervivec bei jedem Systemstart automatisch ausgeführt. Danach wird ein Fenster angezeigt, das man mit OK bestätigen kann: "Press restart button to close this application".

Zuletzt wird noch eine lästige Schadenroutine ausgeführt. Es werden viele bunte Würmer auf dem Bildschirm dargestellt.

Worm/CodeRed

Der Worm/CodeRed nutzt eine Sicherheitslücke des Microsoft Internet Information Sever (IIS) aus, um sich zu verbreiten. Sollte der Wurm ein Server infiziert haben, sucht er nach anderen angreifbaren Servern, um diese zu infizieren.

Damit der "Code Red"-Wurm das System infizieren kann, müssen folgende Vorraussetzungen erfüllt sein:

- Microsoft Windows NT 4.0 oder Windows 2000 mit IIS 4.0 oder IIS 5.0

- Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager

Sollte ein Rechner von dem Wurm infiziert sein, ist die Datei C:\notworm. auf der Festplatte vorhanden.

Der "Code Red" besitzt folgende Schadensroutinen:

1. Der Wurm baut eine Verbindung über den TCP Port 80 zu 100 zufällig gewählten IP Adressen auf und versucht sich dorthin zu versenden.
2. Sollte das Systemdatum des Rechners zwischen den 20. und 28. Tag eines Monats betragen, startet "Code Red" eine DoS (Denial-of-Service) Attacke einer Website der US-Regierung (www1.whitehouse.gov)
3. Wenn die Infektion erfolgreich war, werden die infizierten Server vom Wurm auf die Standardsprache Englisch zurückgestellt. Weiterhin werden auf angeforderten Seiten folgende Nachrichten ausgegeben:

    HELLO! Welcome to http://www.worm.com! Hacked By Chinese!

Microsoft hat bereits einen Patch zum Schließen der Sicherheitslücke auf folgender Website bereitgestellt:

http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

Worm/Cuervo

Alias: VBS/Cuerpo.A

Worm/Cuervo ist ein Wurm, der als Visual Basic Script geschrieben wurde und sich mit Hilfe von Microsoft Outlook versendet. Er erstellt eine Reihe von .HTML und .VBS Dateien, ändert Einträge in der Registry und ersetzt die Internet Explorer Startseite durch seine eigene HTML Datei.

Der Wurm durchsucht alle Dateien, die die Extensions txt, na2, wab, mbx, dbx, und dat besitzen nach Email Adressen. Cuervo schaut weiterhin in den Posteingang von Outlook nach Emails mit Attachments. Sollte er eine Email finden, kopiert der Wurm seinen Code mehrmals in das Windows Systemverzeichnis in eine Datei, welche den Orginalnamen eines Attachments trägt mit der Extension .VBS. Sollte der Wurm keine Email mit Attachments finden, generiert er selbst einen Namen und kopiert sich dann in das Systemverzeichnis.

Danach versendet Worm/Cuervo sich mit folgender Email:

Subject:
`der Betreff ist der Attachmentnamen ohne Dateiextension`

Attachment:
`Der Dateinamen ist unterschiedlich, hat aber den gleichen Namen, wie die Datei, die in das Systemverzeichnis erstellt wurde.`

Priority:
`Hoch`

Nach dem Ausführen erstellt der Worm/Cuervo im Windows Verzeichnis eine Datei mit dem Namen WINSTART.BAT, die beim nächsten Windows Start automatisch ausgeführt wird.

Beim Ausführen der WINSTART.BAT versucht sich der Wurm in folgende Verzeichnisse zu kopieren:

c:\windows\startm~1\programs\startup\<dateiname>
c:\windows\menud'~1\programmes\d'marrage\<dateiname>
c:\windows\menuin~1\programas\inicio\<dateiname>
c:\windows\alluse~1\menuin~1\programas\iniciar\<dateiname>
c:\windows\startmenü\programme\autostart\<dateiname>

Worm/Cuervo erstellt auch eine Datei in das C:\RECYCLED Verzeichnis und das Windows Systemverzeichnis, die er in die Registry einträgt:

`HKLM\Software\Microsoft\Windows\CurrentVersion\Run\<eintrag> = <dateiname>.vbs`

Danach ersetzt der Wurm die Internet Explorer Startseite durch eine eigens generierten Dateien mit dem Namen BLANK.HTM. Diese Datei steht im Systemverzeichnis und nach der Infektion die folgende Internetseite aufgerufen: http://www.freedonation.com. Hierzu wird folgender Registry Eintrag verändert:

`HKLM\Software\Microsoft\Internet Explorer\Main\Start Page = C:\WINDOWS\SYSTEM\BLANK.HTML`

Worm/Frethem

Alias: W32/Frethem

Worm/Frethem ist ein Internet Wurm, der sich per Email versendet. Die Emailadressen werden aus dem Windows Adressbuch und allen .dbx Dateien gesammelt. Da Worm/Frethem seine eigene SMTP Engine besitzt, braucht er kein Emailprogramm wie Outlook um sich zu versenden. Eine vom Wurm versandte Email hat folgenden Inhalt:

Subject:
```
Re: Your password!
```

Body:
```
ATTENTION!

You can access
very important
information by
this password

DO NOT SAVE
password to disk
use your mind

now press
cancel
```

Attachment:
```
decrpyt-password.exe, password.txt
```

Bei der Datei "Decrypt-password.exe' handelt es sich um die eigentliche Wurm-Datei. Das zweite Attachment "password.txt' ist eine reine Textdatei und hat keinerlei Schadensroutine. Die Textdatei hat folgenden Inhalt:
'Your password is W8dqwq8q918213'

Worm/Frethem kopiert sich selbst in den Autostart-Ordner des Windows Startmenüs. Er wird bei jedem Systemstart erneut ausgeführt.

Worm/Frethem.J

Der Wurm Worm/Frethem.J hat eine Größe von 47.616 Bytes und wurde mit den Laufzeitpackern PE-Pack und UPX gepackt. Er versendet sich über seine eigene SMTP Egine an alle Emailadressen, die er im Windows Adressbuch oder in Dateien mit der Dateierweiterung .dbx, .wab, .mbx, .mdb oder .eml finden kann. Eine vom Worm/Frethem.J versandte Email hat den folgenden Inhalt:

Subject:
```
Re:Your password!
```

Body:
```
ATTENTION!

You cann access
very important
information by
this password

DO NOT SAVE
password to disk
use your mind

now press
cancel
```

Attachment:
```
Decrypt-password.exe
Passwort.txt
```

Führt man die Datei Decrypt-password.exe aus, kopiert sich der Wurm in das Windowsverzeichnis als Taskbar.exe und legt folgenden Registry Key an:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVerion\Run\
Task Bar=C:\Windows\Taskbar.exe
```

Da Worm/Frethem.I die SMTP Daten des lokalen Benutzer benützt um sich zu versenden, sucht er in folgenden Registry Einträgen nach diese Daten:

```
HKEY_CURRENT_USER\Software\Microsoft\
Internet Account Manager\Accounts\00000001\SMTP Server

HKEY_CURRENT_USER\Software\Microsoft\
Internet Account Manager\Accounts\00000001\SMTP Display Name

HKEY_CURRENT_USER\Software\Microsoft\
Internet Account Manager\Accounts\00000001\SMTP Email Adress
```

Worm/Frethem.I

Der Wurm Worm/Frethem.I hat eine Größe von 48.640 Bytes und wurde mit den Laufzeitpackern PE-Pack und UPX gepackt. Er versendet sich über seine eigene SMTP Egine an alle Emailadressen, die er im Windows Adressbuch oder in Dateien mit der Dateierweiterung .dbx, .wab, .mbx, .mdb oder .eml finden kann. Eine vom Worm/Frethem.I versandte Email hat den folgenden Inhalt:

Subject:
Re:Your password!

Body:
ATTENTION!

You cann access
very important
information by
this password

DO NOT SAVE
password to disk
use your mind

now press
cancel

Attachment:
Decrypt-password.exe
Passwort.txt

Führt man die Datei Decrypt-password.exe aus, kopiert sich der Wurm in das Windowsverzeichnis als Taskbar.exe und legt folgenden Registry Key an:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVerion\Run\
Task Bar=C:\Windows\Taskbar.exe
```

Da Worm/Frethem.I die SMTP Daten des lokalen Benutzer benützt um sich zu versenden, sucht er in folgenden Registry Einträgen nach diese Daten:

```
HKEY_CURRENT_USER\Software\Microsoft\
Internet Account Manager\Accounts\00000001\SMTP Server

HKEY_CURRENT_USER\Software\Microsoft\
Internet Account Manager\Accounts\00000001\SMTP Display Name

HKEY_CURRENT_USER\Software\Microsoft\
Internet Account Manager\Accounts\00000001\SMTP Email Adress
```

Worm/Gnutella.MG

Alias: P2P/Mandragore

Mandragore ist ein Wurm, der sich über das Gnutella-Netzwerk verbreitet. Gnutella ist vergleichbar mit Napster, einem auf Peer-to-Peer (P2P) basierenden File Sharing-Netzwerk. Um auf das Gnutella-Netzwerk zuzugreifen, werden Programme wie etwa ToadNode oder BearShare eingesetzt.

Bei diesem Wurm handelt es wohl eher um einen "Proof-of-Concept", einem Machbarkeitsversuch. Es handelt sich nicht um einen schädlichen "Virus". Anwender sind nur dann betroffen, wenn mit Gnutella-kompatiblen Programmen gearbeitet wird, d.h. dieser Wurm wird nur in Verbindung mit dem Gnutella-Netzwerk gefährlich.

Der Wurm selbst hat eine Länge von 8192 Bytes und ist eine Win32-Applikation. Wird der Wurm ausgeführt, kopiert dieser sich in den Autostart-Ordner des jeweiligen Users unter dem Dateinamen GSPOT.EXE. Die Datei selbst ist mit den Dateiattributen "System" und "Versteckt" versehen. Nach dem nächsten Windowsstart wird diese Datei automatisch ausgeführt und verbleibt als Hintergrundprozess resident im Arbeitsspeicher. Unter Windows 9x registriert sich der Wurm zusätzlich als versteckter Prozess, der nicht in der Taskleiste zu sehen ist.

Der Wurm kontaktiert das Gnutella-Netzwerk. Ein infizierter Rechner beantwort als "Server" Anfragen zu Dateien und kann durch die Vielzahl von Anfragen sehr leicht überlastet werden. Er stellt diejenige Datei, die den Wurmcode selbst enthält, zum Download zur Verfügung. Die Datei kann einen beliebigen Dateinamen haben.

Zum Beispiel kann die Datei "rare pictures of butterflies.exe" heißen. Diese Datei ist nach der Infektion im Gnutella-Netzwerk zu finden und kann von anderen Usern heruntergeladen werden. Bei dem Programm BearShare ist die Anzeige der Dateinamenserweiterungen standardmäßig abgeschaltet und sollte sicherheitshalber angeschaltet werden.

Worm/Goner

Bei dem Worm/Goner handelt es sich um einen Massen Mailer mit einer Größe von 38.912 Bytes, der in Visual Basic programmiert wurde. Er versendet sich als Email über Outlook und infiziert andere Computer mit Hilfe des ICQ Instant Messanger. Eine vom Worm/Goner versendete Email hat folgenden Inhalt:

Subject:
Hi

Body:
How are you?

When I saw this screen saver, I immediately thougt about you
I am in a harry, I promise you will love it!

Attachment:
Gone.scr

Wir das Attachment ausgeführt, erscheint auf dem Bildschirm eine Dialogbox mit Grüßen und einer kleinen Animation. Darauf erscheint eine Messagebox mit folgender falschen Meldung:

Error While Analyze DirectX!

Worm/Kazaa

Worm/Kazaa ist ein Wurm, der sich über das über das Peer-to-Peer Netzwerk Kazaa verbreitet. Mit Hilfe dieses Netzwerkes können die verschiedenste Programme, Spiele, Filme usw. ausgetauscht werden.

Wird eine infizierte Datei ausgeführt, zeigt der Wurm folgendes Dialogfenster an:

Error

Access error #03A:94574: Invalid pointer operation
File possibly corrupted

[OK]

Der Wurm kopiert sich in das Windows Systemverzeichnis als Explorer.scr und legt folgenden RegistryKey an:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"System-Service"="C:\Windows\System\Explorer.scr"
```

Mit diesem Eintrag wird der Worm/Kazaa bei jedem Windowsstart ausgeführt.
Ein zweiter Registry Eintrag mit einer zwanzigstelligen Hexadezimalzahl wird ebenfalls angelegt:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Syscod]
"syscod"="007A5000000758A6BEA1"
```

Danach kopiert sich der Wurm etwa 1000 Mal mit verschiedenen Dateinamen in das Verzeichnis C:\Windows\Temp\Sys32\. Dieses Verzeichnis wird als Shared-Ordner bei der P2P Software Kazaa registriert, auf welchem die Kazaa-Anwender sich dann unbeabsichtigt den Wurm herunterladen. Die Dateien im Verzeichnis \Sys32\ tragen alle den Namen von bekannten Filmen und Programmen. So sind die Chancen für den Wurm gedownloaded zu werden, sehr hoch.

Die vom Wurm benutzte Dateinamen können wie folgt lauten:

...
A.I-Artificial Intelligence- divx -full-downloader
A.I-Artificial Intelligence- Filme -full-downloader
ABeautifulMind
AbsoluteZero-installer
Adobe InDesign 2.0 Build 416 -full-downloader
Adobe Pagemaker -full-downloader
Adobe Photoshop 6.0 -full-downloader
Adobe Photoshop update (6.1) -full-downloader
After Dark Deluxe-Bildschirmschoner-full-downloader
Age of Empires 2- Games -full-downloader
Age of Empires 2 Gold +Strat.Comm.-Games-full-downloader
Age of Empires 2 Gold +Strat.Comm.-Spiel-full-downloader
Age of Empires Screensaver
Age of Mythology - Games -full-downloader

Age of Mythology (Beta) -full-downloader
Age of Wonders II The Wizard#39s-installer
Airxonix -full-downloader
Alarm Stufe Rot 2 -full-downloader
Alarm Stufe Rot 2 Yuris Rache -full-downloader
Alfred Hitchcock - The Final Cut - Games -full-downloader
Alien vs. Predoator 2-Games-full-downloader
Alien vs. Predoator 2-Spiel-full-downloader
All Serials
Allout-Games-full-downloader
Almost Famous-Komödie-Filme-full-downloader
American McGee#39s Alice-Games-full-downloader
American McGee#39s Alice-spiel-full-downloader
American Pie 2 -divx-full-downloader
American Pie 2- Filme -full-downloader
American Pie 2-divx-full-downloader
American Pie -divx-full-downloader
Anam
Anno 1503 (Beta) -full-downloader
Anno 1503- Games -full-downloader
Anno 1602 Königs Edition Classic- Games -full-downloader
Anno 1602 Königs Edition Classic-Spiel-full-downloader
Anstoss 3 -full-downloader
Appz
Aquanox -full-downloader
aquanox-full-downloader
AsterixundOberlix
...

Die Dateiname endet nach einer unterschiedlicher Zahl von Leerzeichen mit der Extension .EXE oder .SCR.

Der Wurm/Kazaa wird mit der aktuellen VDF erkannt.

Worm/Klez.E

Alias: W32/Klez.G, W32/Klez.H@mm

Die neue Variante des Worm/Klez kopiert sich als WINKxxx.EXE ('xxx' = zufällig gewählte Buchstabenkombination) in das Windows Systemverzeichnis und legt folgenden Key in der Registry an:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Winkxxx=C:\Windows\System\Winkxxx.exe
```

Worm/Klez.E kopiert sich wahllos in verschiedene Verzeichnisse sowie Unterverzeichnisse auf allen lokalen Laufwerken, sowie alle gesharte Netzlaufwerken mit Schreib-/Lesezugriff. Diese Dateien haben als Dateiextensions .EXE, .PIF, .COM, .SCR, .RAR, .SCR. In einigen Fällen erzeugt der Wurm auch Doppelextension z.B. "Dateiname.txt.exe"

Der Worm/Klez.E droppt einen neuen Virus in das Programme Verzeichnis (meist C:\Programme\) und führt diesen aus. Der Dateiname wird mit einer zufällig gewählten Buchstabenkombination erstellt. Bei dem Virus handelt es sich um einen Fileinfektor und wird mit der aktuellen VDF als W32/Elkern.C erkannt.

Klez.E versendet sich als Email mit Hilfe seiner eigenen SMTP Engine. Die Empfängeradressen erhält der Wurm aus Windows Adressbuch oder aus Dateien mit der Extension .HTM, .HTML, .DOC, .XLS, .BAT, .TXT, .SCR, .CPP, .C, .BAK. Die **Betreffzeile** einer solchen Email kann folgendermaßen aussehen:

```
powful
WinXP
IE 6.0
new
funny
nice
humour
excite
Symantec
Mcafee
F-Secure
Kaspersky
Sophos
Trendmicro
W32.Elkern
W32.Klez.E
```

Die Betreffzeile kann auch Variieren. So kann der **Betreff** der Email auch wie folgt aussehen:

a new new game

oder

```
nice path
```

oder

```
a powerful new website
```

oder

a IE 6.0

Worm/Klez.G erstellt eine HTML-Mail, die eine base64 enkodierte Kopie von sich selbst enhält. Beim Email-Empfang führt sich Klez.E aus, auch wenn dieser nicht aktiv geöffnet wird, sondern nur in der Vorschau angezeigt wird. Dies Betrifft I.E.-basierten E-Mail-Clients (z.B. Microsoft Outlook).

Worm/Lee.SP

Worm/Lee.SP ist ein Wurm, der sich mit Hilfe der Emailadressen des Outlook Adressbuches versendet. Eine vom Wurm versandte Email sieht folgendermaßen aus:

Subject:
```
Shakira's Pictures
```

Body:
```
Hi:
i have sent the photos via attachment
have funn..
```

Attachment:
```
ShakiraPics.jpg.vbs
```

Wird das Attachment ausgeführt, kopiert sich Worm/Lee.SP als ShakiraPics.jpg.vbs in das Windowsverzeichnis und überschreibt alle .vbs Dateien mit seinem Code. Der Wurm kopiert sich in den \ Recycled\-Ordner auf einer der lokalen Festplatten und versendet sich über Microsoft Outlook. Er kann sich ebenfalls über IRC mit Hilfe der Datei Script.ini versenden. Damit er bei jedem Systemstart ausgeführt wird, legt er folgenden Registry Key an:

```
[HKEY_LOKAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Registry=wscript.exe C:\Windows\ShakriaPics.jpg.vbs %
```

Worm/Lee.SP zeigt nach der Infektion folgende Message angezeigt: "You have been infected by the ShakiraPics Worm".

Worm/Maldal.C

Alias: Keyluc, Zacker, Zaker, Christmas.exe

Der Wurm Maldal.C verbreitet sich mit Hilfe des Email Attachment CHRISTMAS.EXE. Wird dieses Attachment ausgeführt, versendet der Wurm sich über Outlook an alle Emailadressen, die er im Windows Adressbuch findet. Die Email hat folgenden Inhalt:

Subject:
```
Happy New Year
```

Body:
```
Hii, I can't describe my fellings But all I can say
is Happy new year :-) bye
```

Attachment:
```
Christmas.exe
```

Danach kopiert sich der Wurm in das Windows Verzeichnis als Christmas.exe und legt folgenden Registry Key an:

```
[HKLM\Software\Microsoft\Windows\CurrentVerison\Run]
"Zacker"="C:\\WINDOWS\CHRISMTAS.EXE"
```

Maldal.C ändert die Startseite des Internet Explorers auf eine URL einer Internetseite des Providers Geocities.com.

Worm/Maldal.I

Der neue E-Mail Wurm Maldal.I verschickt sich über Microsoft Outlook. Die E-Mail sieht wie folgt aus:

Absender:
<E-Mail Adresse der Absenders>

Betreff: <Der Wurm wählt eine der folgenden Zeilen als Betreff>

* Zakia Zakaria & Najati :P
* Take a picture for your self (Don't be mad its only a joke)
* Re:Fwd:Romantic Day
* Fwd: Let's Dance & forget pains
* Fwd: WoOoOoOow
* Fwd: Are you looking for FUN !!!?
* Fwd: The rights of women !!!
* Fwd: [sex-is] HoT MoVies
* Fwd: [SpanishGirlsGroup] Hola ...
* Fwd: [LsbianLovers-group] Lick my asshole
* Fwd: [Muzicana-Group] Download what you want
* Fwd: [PussyLand-egroup] How sweet...
* Fwd: [DrFun-egroup] Let's Laugh
* Fwd: [FuNnY-egroup]Hehehehehe damn
* Fwd: [SexyGurls-egroup] Raping a little girl
* Fwd: [Scr-News-egroup] Have u ever seen BLOOD
* Fwd: [Yabdoo-egroup]For HaCkers Lovers
* Fwd: [Jews-egroup] Sharoon Owns The World
* Fwd: [FunMaiL-group]Bush under bin laden's cock !!!
* Fwd: [Teen-egroup] Three Ways For Love
* Fwd: [RomanticLife-group] Learn How To Love ...
* Fwd: [Gays-egroup]Oh Shitttttt
* Fwd: [JewsFood-egroup] Dogs Meat !!!
* Fwd: [PianoMoZart-egroup] Wow Romantic
* Fwd: [PussyPiss-egroup] Piss On my face :O
* Fwd: [Finance-group] Do you wanna be a rich man?
* Fwd: [lovedreams-egroup] love speaks from the heart ...
* Fwd: [TeroNews-Group] Too Late ... Bin Laden has been killed
* Fwd: [Pc.CLup-Group] Learn how to deal with DOS
* Fwd:[Anal-sex-team] OOOH Faster
* Fwd:[RapingTeen-eGroup] Oh My God !!!
* Fwd:The demand of sex ... where does it lead us to ?
* Fwd:Wow , We are the same !
* Fwd:Is there any true love ?
* Fwd:Have u ever seen your face?! (Funny)
* Fwd:Against the power of women
* Fwd:Fwd:If you care about your wife
* Fwd:Say 'I Love You' in 300 languages
* Fwd:Send it to every body you love ;)
* Fwd:Loneliness ...
* Fwd:Remember our survivors
* Fwd:Tonight is... The Night Of Sex
* Fwd:Change your life with Dr.Jobreee

Inhalt:
<Der Inhalt dieser E-Mail ist leer>

Dateianhang:
<Der Dateianhang hat einen zufälligen Dateinamen>

Nachdem der Wurm gestartet wurde, erscheint folgendes Fenster:

Sorry! You are not registered.
Please contact us:
444-452-
474-452-

Email:
Zak <Zak@ >
Mochelle <msl@ >
join@

Gleichzeitig kopiert er sich in das Windows und Windows-Systemverzeichnis unter dem Dateinamen ZaCker.pif. Eine dritte Kopie wird im Windows-Verzeichnis unter dem Namen Hide.pif erstellt.

Folgender Registry Eintrag wird erstellt:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
NAV DefAlert=C:\WINDOWS\SYSTEM\ZaCker.pif
```

Nach ein paar Minuten fängt der Virus an, sich in jedes von ihm gefundene Verzeichnis zu kopieren. Hiervon sind auch Verzeichnisse auf gemappten Netzlaufwerken betroffen.

Diese neuen Kopien haben den gleichen Namen wie das Verzeichnis. Bsp.: c:\windows\temp\temp.pif oder c:\windows\system\system.pif

Zu jeder dieser Dateien wird ein weiterer Eintrag in der Registry erstellt. Bsp.:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
TEMP=c:\windows\temp\temp.pif
```

oder

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
SYSTEM=c:\windows\system\system.pif
```

Der Wurm verschickt sich jetzt mittels Microsoft Outlook an Einträge aus dem Adressbuch. Außerdem zeigt der Wurm die Meldung: ZaCker Is N YoUr MaChiNe.

Nach einem Neustart von Windows werden die Kopien des Wurmes über die Registry aktiviert. Es können viele Hundert Kopien nacheinander geladen werden. Jede Kopie löscht alle nicht gesperrte Dateien im ihrem Verzeichnis.

Worm/Matcher

Der Emailwurm Matcher ist ein .EXE Datei, die in Visual Basic 6.0 geschrieben wurde. Er hat eine Länge von 29 Kbytes und ist nicht encrypted oder gepackt. Um den Wurm auszuführen muss auf dem Rechnersystem die Datei MSVBV60.DLL installiert sein. Er versendet sich mit Hilfe des Adressbuches über Microsoft Outlook und Outlook Express.

Wird die Datei ausgeführt, installiert sich der Wurm in das Windows System Verzeichnis mit dem Namen MATCHER.EXE. Danach ändert er in der Registry folgenden Eintrag ab:

```
HKLM\Software\Microsoft\Windows\Current Version\Run@="C:\Windows\System\
Matcher.exe
```

So wird der Wurm bei jedem Start von Windows neu geladen. Er öffnet Outlook und versendet sich mit Hilfe des Adressbuches an alle Email-Adressen, die er dort zu findet sind. In manchen Fällen versendet sich der Wurm alle zwei bis fünf Minuten.

Die infizierte Email sieht folgendermaßen aus:

Subject:
Matcher

Body:
Want to find your love mates !!! Try this its cool... Looks and A
Maching to opposite sex.

Attachment:
Matcher.exe

Nachdem der Wurm sich versendet hat, ändert dieser die AUTOEXEC.BAT ab. Beim nächsten Start von Windows erscheint die Nachricht ’from: Bugger’ beim Hochfahren des Rechners und muss mit einem Tastdruck bestätigt werden.

Worm/Myba.A

Worm/Myba.A ist eine Win32-Anwendung und wurde in Visual Basic geschrieben. Myba versendet sich als Email über Microsoft Outlook und benutzt dazu die Adressen, die im Outlook Adressbuch eingetragen sind. Eine solche Email sieht folgendermaßen aus:

Subject:
`My Baby pic !!!`

Body:
`Its my animated baby picture !!`

Attachment:
`MYBABYPIC.EXE`

Wird das Attachment MYBABYPIC.EXE ausgeführt, zeigt dies ein nicht jugendfreies Bild an, während der Wurm sich in das Windows-Systemverzeichnis unter folgenden Dateinamen hineinkopiert: WINKERNEL32.EXE, WIN32DLL.EXE, COMMAND.EXE, CMD.EXE und MYBABYPIC.EXE.

Danach ändert der Wurm folgende Registryeinträge:

```
HKLM\Software\Microsoft\Windows\Current Version\Run\mybabypic = WindowsSystem
%\mybabypic.exe

HKLM\Software\Microsoft\Windows\Current Version\Run\WINKernel32 =
WindowsSystem%\WINKernel32.exe
```

und

```
HKLM\Software\Microsoft\Windows\Current Version\RunServices  = %WindowsSystem
%\Win32DLL.exe
```

Dadurch wird der Wurm automatisch mit jedem Windowsstart ausgeführt.

Weiterhin erstellt Myba einen neuen Registry Key in `HKCU\Software\Bugger` mit den Einträgen `Default = HACK[2k]` und `mailed = %number%`

Der Wurm Myba hat verschiedene Schadensroutinen, die abhängig von Datum und Uhrzeit aktiv werden.

* Es werden die NumLock, CapLock and ScrollLock Tasten an/ausgeschaltet

* Sendet zum Keyboardbuffer die Nachricht: .IM_BESIDES_YOU_

* Baut eine Verbindung zu der Internetseite http://www.youvebeenhack.com auf und sendet den folgenden Text:

  FROM BUGGER
  HAPPY VALENTINES DAY FROM BUGGER
  HAPPY HALLOWEEN FROM BUGGER

Der Wurm durchsucht die Unterverzeichnissen auf allen erreichbaren Laufwerken und ändert oder löscht folgende Dateien:

* Dateien mit der Dateiendung .VBS oder .VBE werden sofort gelöscht.

* Dateien mit folgenden Endungen werden mit dem Wurmcode überschrieben: .C, .CPP, .CSS, .H, .HTA, .JS, .JSE, .PAS, .SCT und .WSH. Diese werden dann mit dem urspünglichen Dateinamenamen und der Dateiendung .EXE gespeichert. So wird aus BEISPIEL.CPP die Datei BEISPIEL.EXE, die nun den Wurmcode enthält.

* Bilddateien mit der Dateiendung .JPG und .JPEG werden mit dem Wurmcode überschrieben und es wird die Endung .EXE hinzugefügt. So wird aus BEISPIEL.JPG die infizierte BEISPIEL.JPG.EXE.

* Es wird für jede erreichbare Datei mit der Endung .MP2, .MP3 oder M3U eine neue Datei erstellt, die den Wurmcode enthält. Diese neue Datei erhält den originalen Dateinamen erweitert um die Endung.EXE. Zusätzlich wird das Attribut "Versteckt" aktiviert. So wird aus einer BEISPIEL.MP3 eine BEISPIEL.MP3.EXE.

Worm/MyLife.A

Dateigröße: 30.720 Bytes
Dateiname: My Life.scr

Eine von MyLife.A versandte Email sieht folgendermaßen aus:

Subject:
```
my life ohhhhhhhhhhh
```

Body:
```
Hiiiii
How are youuuuuuuu?
look to the digital picture it's my love
vvery verrrry ffffunny :-)
my life = my car
my car = my house
```

Attachment:
```
My Life.scr
```

Führt man das Attachment aus, kopiert sich MyLife in das Windows Systemverzeichnis (z.B.: C:\Windows\System\) als "My Life.scr" und legt folgenden Registry-Key an:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
stmgr=C:\Windows\System\My Life.scr
```

Wird Worm/MyLife zum ersten mal ausgeführt, zeigt dieser ein Bild auf dem Desktop.

Zum Schluss versendet sich MyLife.A über Microsoft Outlook an alle Emailadressen im Outlook Adressbuch.

Wird MyLife.A ein zweites Mal ausgeführt, löscht er alle .SYS, .COM, .INI und .EXE Dateien im Windows Verzeichnis und alle .EXE, .DLL, .SYS und .VXD Dateien im Windows Systemverzeichnis, sowie alle .SYS und .COM Dateien im Root C:\.

Worm/MyLife.B

Dateigröße: 11.524 Bytes
Dateiname: Cari.scr

Eine von MyLife.B versandte Email sieht folgendermaßen aus:

Subject:
bill caricature

Body:
```
Hiiiii
How are youuuuuuuu?
look to bill caricature it's vvvery verrrry ffffunny :-) :-)
i promise you will love it? ok

buy



========No Viruse Found========

                MCAFEE.COM

-------------------------------------------------------
```

Attachemnt:
cari.scr

Führt man das Attachment aus, kopiert sich MyLife in das Windows Systemverzeichnis als "Cari.scr" und legt folgenden Registry-Key an:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
win=C:\Windows\System\cari.scr
```

Wird Worm/MyLife zum ersten Mal ausgeführt, zeigt er ein Bild auf dem Desktop.

MyLife.B versendet sich über Microsoft Outlook an alle Emailadressen im Outlook Adressbuch.

Wird MyLife.B ein zweites Mal ausgeführt, löscht er alle .SYS Dateien im Windows Verzeichnis und alle .SYS, .OCX, .NLS und .VXD Dateien im Windows Systemverzeichnis, sowie alle Dateien im Root von C:, D:, E: und F:.

Worm/MyLife.C

Dateigröße: 7.680 Bytes
Dateiname: List.TXT.scr

Eine von MyLife.C versandte Email sieht folgendermaßen aus:

Subject:
```
The List
```

Body:
```
Hiiiii
How are youuuuuuuu?
Here is that Notepad you asked for ... don't show anyone else ;-)
Notepad = list
list = 137

buyyyy



========No Viruse Found========

                  MCAFEE.COM
```

Attachemnt:
```
List.TXT.scr
```

Führt man das Attachment aus, kopiert sich MyLife in das Windows Systemverzeichnis als "List.TXT.scr" und legt folgenden Registry-Key an:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
sys=C:\Windows\System\List.TXT.scr
```

MyLife versendet sich über Microsoft Outlook an alle Emailadressen im Outlook Adressbuch.

Wird Worm/MyLife.C zum ersten Mal ausgeführt, zeigt er eine Message Box mit dem Inhalt: Error Notepad.dll ## , die man mit "OK" bestätigen kann.

MyLife.C überprüft die aktuelle Zeit. Beträgt der Wert der Minute über 50, führt er das Format Kommando auf den Laufwerken D:, E:, F:, G:, H: und I: aus und löscht alle Dateien und Verzeichnisse der Partition C:.

Worm/MyLife.D

Dateigröße: 9.088 Bytes
Dateiname: Screen.scr

Eine von MyLife.D versandte Email sieht folgendermaßen aus:

Subject:
```
New Screen Saver
```

Body:
```
Hiii
How are youu!!?
look to the New Screen Saver it's vvvery verrrry ffffunny :-) :-)
i promise you will love it? ok

buy



========No Viruse Found========

                 MCAFEE.COM
```

Attachemnt:
```
Screen.scr
```

Führt man das Attachment aus, kopiert sich MyLife in das Windows Systemverzeichnis als "Screen.scr" und legt folgenden Registry-Key an:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
screen=C:\Windows\System\Screen.scr
```

MyLife versendet sich über Microsoft Outlook an alle Emailadressen im Outlook Adressbuch.

Wird Worm/MyLife.D zum ersten mal ausgeführt, zeigt dieser eine Message Box mit dem Inhalt : Error 1452544 File Not Found , die man mit OK bestätigen kann.

Worm/MyLife.E

Dateigröße: 11.776 Bytes
Dateiname: Screen.scr

Eine von MyLife.E versandte Email sieht folgendermaßen aus:

Subject:
sexxxyyy Screen Saver

Body:
Hiii
How are youu!!?
look to the New Screen Saver it's vvvery verrrry ffffunny :-) :-)
i promise you will love it? ok

buyyyy

========No Viruse Found========

MCAFEE.COM

Attachemnt:
Screen.scr

Führt man das Attachment aus, kopiert sich MyLife in das Windows Systemverzeichnis als "Screen.scr" und legt folgenden Registry-Key an:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
screen=C:\Windows\System\Screen.scr

MyLife versendet sich über Microsoft Outlook an alle Emailadressen im Outlook Adressbuch.

Wird Worm/MyLife.E zum ersten mal ausgeführt, zeigt dieser eine Message Box mit dem Inhalt : Error 1452544 File Not Found , die man mit OK bestätigen kann.

Wurde der Wurm erfolgreich aus dem System installiert, versendet er zusätzlich eine Email an:

anzarx200@email.com mit dem

Subject:

New Screen Saver

Body:

New Never Hood buy

Worm/MyLife.F

Dateigröße: 7.680 Bytes
Dateiname: List480.TXT.scr

Eine von MyLife.F versandte Email sieht folgendermaßen aus:

Subject:
```
sexxxyyy Screen Saver
```

Body:
```
Hiii
How are youu!!?
look to the New Screen Saver it's vvvery verrrry ffffunny :-) :-)
i promise you will love it? ok
Notepad = list
list = 37

buyyyy



=======No Viruse Found========

             MCAFEE.COM
```

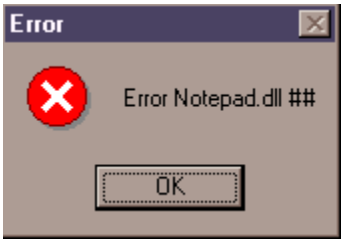
Attachemnt:
```
List480.TXT.scr
```

Führt man das Attachment aus, kopiert sich MyLife in das Windows Systemverzeichnis als "List480.TXT.scr" und legt folgenden Registry-Key an:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
sys=C:\Windows\System\List480.TXT.scr
```

MyLife versendet sich über Microsoft Outlook an alle Emailadressen im Outlook Adressbuch.

Wird Worm/MyLife.F zum ersten mal ausgeführt, wird folgende Message Box angezeigt:



MyLife.F überprüft die aktuelle Zeit. Beträgt der Wert der Minute über 50, führt er das Format-Kommando auf den Laufwerken D:, E:, F:, G:, H: und I: aus und löscht alle Dateien und Verzeichnisse der Partition C:.

Worm/MyLife.G

Dateigröße: 13.824 Bytes
Dateiname: Wife.scr

Eine von MyLife.G versandte Email sieht folgendermaßen aus:

Subject:
```
Ox <--> sharon
```

Body:
```
Hi All,
Look to the ox caricature it's very sad
ox <=== > Sharon
it' funny :-)
Attachments are automatically scanned for viruses using MCAFEE.COM

========No Virus Found========
```

Attachemnt:
```
Wife.scr
```

Führt man das Attachment aus, kopiert sich MyLife in das Windows Systemverzeichnis als "Ox&Wife.scr" und legt folgenden Registry-Key an:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
C:\Windows\System\Ox&Wife.scr
```

Wird Worm/MyLife zum ersten mal ausgeführt, zeigt dieser folgendes Bild auf dem Desktop an, während er sich über Microsoft Outlook an alle Emailadressen im Outlook Adressbuch versendet :

Danach wird folgende Message Box angezeigt:

Title:

KiLlLlLl sHaRoN

Message:

bY: mY llfE
1-oVeR wRiTe 30 <==> eXtEnSiOn
2-dElEte aLl fOlDeRs (C to I)
3-LoOOoOOoL
KiLlLlLl aNd KiLlLlLl

MyLife.G löscht alle Verzeichnisse auf den Laufwerken D:, E:, F:, G:, H: und I:

Worm/MyLife.H

Dateigröße: 16.384 Bytes
Dateiname: peeeeeep.mpeg.scr

Eine von MyLife.H versandte Email sieht folgendermaßen aus:

Subject:
peeeeeep

Body:
```
Hiiiii All
How are youuuuuuuu?
look to the movi peeeeeep it's vvvery verrrry ffffunny :-) ;-)
byyye
========No Viruse Found========

MCAFEE.COM

 ----------------------------------------------------------
```

Attachemnt:
peeeeeep.mpeg.scr

MyLife.H versendet sich über Outlook mit Hilfe des Outlook Adressbuches und der Kontaktliste des MSN Messenger.

Worm/MyLife.I

Dateigröße: 12.288 Bytes
Dateiname: Ox&Wife.scr

Eine von MyLife.H versandte Email sieht folgendermaßen aus:

Subject:
```
Digital Picture --> OX
```

Body:
```
hi
look to the 3d Picture it's very sad
it's OX
bye
```

Attachemnt:
```
ox&Wife.scr
```

MyLife.I versendet sich über Outlook mit Hilfe des Outlook Adressbuches und der Kontaktliste des MSN Messenger.

Führt man das Attachment aus, kopiert sich MyLife in das Windows Systemverzeichnis als "Ox&Wife.scr" und "peeeep~~~.scr" legt folgenden Registry-Key an:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Run\Ox=C:\Windows\System\Ox&Wife.scr
```

Wird Worm/MyLife zum ersten mal ausgeführt, zeigt dieser das gleiche Bild wie Worm/MyLife.G.

MyLife.J

Dateigröße: 22.258 Bytes
Dateiname: USA.scr

Eine von MyLife.J versandte Email sieht folgendermaßen aus:

Subject:
```
sexyy Screen Saver
```

Body:
```
hi
look to the screen saver it's very funny
bye
```

Attachemnt:

```
 "Sh.scr"  oder  "USA.scr"
```

MyLife.J versendet sich über Outlook mit Hilfe des Outlook Adressbuches und der Kontaktliste des MSN Messenger.

Führt man das Attachment aus, kopiert sich MyLife in das Windows Systemverzeichnis als "USA.scr" und "Sh.scr" legt folgenden Registry-Key an:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
scr=C:\Windows\System\sh.scr
```

Wird Worm/MyLife zum ersten mal ausgeführt, zeigt dieser das gleiche Bild wie Worm/MyLife.G.

Worm/Paukor

W32.Paukor ist ein Wurm, der sich über Microsoft Outlook versendet. Die Email sieht folgendermaßen aus:

Subject:
```
Pictures with your loved one
```

Body:
```
Hi!
I'm sorry I have to send you these compromising pictures with the one
you love, or you loved. :((
The quality is not so good because of the cheap camera, but you should
be able to quess where thy were taken.
I compresseed it as a self extracting archive because I didn't knew if
you have WinZip. When you run it, it should display the extract dialog.
I´m really sorrry I have to be the one who told you about this. :((
```

Attachment:
```
Images_zipped.exe
```

Wird das Attachment ausgeführt, erstellt W32.Paukor folgende zwei Dateien im Windows-Verzeichnis:

Systray.exe
Msp.dll

und folgender Key wird der Registry hinzugefügt:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run
Msp=%WinDir%\SYSTRAY.EXE
```

Danach werden folgende zwei Dateien im Windows-Verzeichnis erstellt:

Images_zipped.exe
Msd.vbs

Die Datei Images_zipped.exe ist das Attachment, das über Microsoft Outlook versendet wird. Die Msd.vbs führt die Routine zum Versenden über Outlook, mit Hilfe des Adressbuches, aus.

Zuletzt wird folgende Nachricht als Fehlermeldung auf den Bildschirm ausgegeben, die mit einem OK - Button bestätigt werden muss: "This WinZip archive seems to be incomplete. Please download again the file, or contact the vendor for an other copy".

Worm/Tettona

Der Wurm Tettona verbreitet sich per Email mit seiner eigenen SMTP Routine. Zusätzlich besitzt Worm/Tettona eine Backdoor Server Routine. Wird ein infiziertes Attachment ausgeführt, kopiert sich Tettona in das Windows Verzeichnis mit dem Dateinamen DLLMGR32.EXE und legt folgenden Autorun Key in die Registry Key an:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"DllManager"="C:\WINDOWS\dllmgr32.exe"
```

Worm/Tettona zeigt dann folgende Fake-Message an: "VBRUN49.DLL not found! Unable to execute."

Um sich per Email zu versenden, benützt der Worm/Tettona seine eigene SMTP Routine. Er durchsucht das WAB (Microsoft Windows Adressbuch) und versendet sich an alle darin stehenden Emailadressen. Eine vom Wurm versandte Email hat folgenden Inhalt:

Der **Betreff** kann wie folgt lauten:

```
Incredible...
```

oder

```
Urgente! (vedi allegato)
```

oder

```
Qualsiasi cosa fai, falla al meglio
```

Der **Body** beginnt mit @hello", oder "ciao" und dann der folgende Text:

```
see this interesting file.
okkio all'allegato ;-)
devi assolutamente vedere il file che ti ho allegato.
apri subito l'allegato, e'MOLTO interessante
```

Das **Attachment** kann wie folgt lauten:

```
tettona.exe
euro.exe
tattoo.exe
```

Worm/W32.Sircam

SirCam ist ein Wurm und Win32 Virus mit einer Größe von ca. 150 Kbytes. Wird dieser ausgeführt, so erstellt er folgende Dateien:

"C:\Recyled\SirC32.exe'
"C:\Recyled\LoveJoy_.com'
"C:\Windows\System\Scam32.exe'
"C:\Windows\Temp\LoveJoy_.com'

Die Datei SirC32.exe wird in die Registry Shell - Kommando für EXE Dateien eingetragen, wobei bei jedem Start einer EXE Datei sich der Wurm erneut ausführt. Hierzu nutzt er folgenden Eintrag in der Registry:

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
@="\"C:\\recycled\\SirC32.exe\" \"%1\" %*"
```

Die Scam32.exe wird in die Registry als "Treiber" eingetragen, die bei jedem Systemstart aufgerufen wird:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
"Driver32"="C:\\WINDOWS\\SYSTEM\\SCam32.exe"
```

SirCam kann sich auch in die Autoexec.bat mit folgenden Befehl eintragen:

@win \recycled\SirC32.exe

Der Wurm legt noch einen dritten Eintrag in der Registry an:

```
[HKEY_LOCAL_MACHINE\Software\SirCam]
```

Sollte die Datei Scam32.exe oder SirC32.exe mit der Dateiendung .DOC.COM versehen werden, löscht der Wurm beim Ausführen sämtliche Dateien, die auf dem Laufwerk C: gespeichert worden sind.

SirCam im Netzwerk

Ist eine NT Workstation mit dem SirCam infiziert, kann der Wurm mit Hilfe von gemappten Laufwerken andere Workstations (Windows9x/NT) befallen. Erfolgt ein Schreibzugriff auf eines dieser Laufwerke, schaut der Wurm nach folgenden Dateien bzw. Verzeichnissen:

\Recycled
\Windows
\Windows\Run32.exe
\Windows\Rundll32.exe

Wird eines davon gefunden, kopiert sich der Wurm nach C:\Recycled\SirC32.exe und erstellt einen Eintrag in die Autoexec.bat, mit dem er beim Systemstart geladen wird. Weiterhin wird die Datei RUNDLL32.EXE zur RUN32.EXE umbenannt und eine neue RUNDLL32.EXE erstellt, die den Viruscode enthält.

Zum Versenden benutzt der Wurm seine eigene SMTP-Engine und verschickt sich selbst als ein ausführbares Programm. Die dazugehörigen Emailadressen findet er im Windows-Adressbuch und in Dateien, die mit folgenden Dateinamen beginnen bzw. enden: SHO*, GET*, HOT*, *.HTM, *WAB und einige mehr. Diese Emailadressen werden als DLL Datei getarnt gespeichert, die sich im System-Verzeichnis von Windows befindet. Der Name der Datei ist meistens SCD1.DLL, wobei sich der zweite und dritte Buchstabe beliebig ändern kann.

Das Attachment der infizierten Email hat eine doppelte Dateierweiterung, d.h.

Dateiname.ext1.ext2

Die erste Dateierweiterung (ext1) kann folgende Varianten besitzen: DOC, XLS, ZIP, EXE. Die zweite Erweiterung (ext2) besitzt eine der folgenden Extensions: PIF, LNK, BAT, COM.

Der Name des Attachment (Dateiname.ext1) kommt von einer beliebigen Datei, die im Ordner 'Eigene Dateien' gespeichert wurde. Der Wurm erstellt eine Liste aller dort stehenden .DOC .EXE .GIF .JPG .JPEG .MPEG .MOV .MPG .PDF .XLS .ZIP - Dateien und speichert diese als SCD.DLL im System-Verzeichnis ab. Verschickt sich der Wurm, entnimmt er der Liste einen beliebigen Dateinamen und benennt das entsprechende Attachment um.

Wird der Wurm als Email empfangen, kann sie folgendermaßen aussehen:

Subject:
Der Betreff der Email kann unterschiedlich sein. Der Wurm benützt den Namen des Attachment und trägt ihn in den Betreff ein.

Message:
Der Nachrichten - Body hat verschiedene Inhalte, wobei die erste und letzte Zeile (in der Spanischen und Englischen Version) immer gleich sind.

Englische Version

Erste Zeile: `Hi! How are you?`
Letzte Zeile: `See you later, Thanks`

Spanische Version

Erste Zeile: `Hola como estas ?`
Letzte Zeile: `Nos vemos pronto. Gracias`

Wird das Attachment des Wurmes ausgeführt, wird ein Word Dokument aufgerufen, während im Hintergrund das System infiziert wird.

WScr.Kak.Worm

Der Wurm KAK befällt nur englische und französische Windows 95/98-Systeme. Der Wurm benötigt für seine Infektion den Microsoft Internet Explorer 5 und als Email-Client (für die Fortpflanzung) Microsoft Outlook Express 5.

Sofern die Voraussetzungen erfüllt sind, kann der Virus in jeder Email vom Typ HTML als Java-Script enthalten sein. Da dieses "Programm" keinerlei Ausgaben produziert, bemerkt man dessen Ausführung nicht! Somit kann er unbemerkt eine Datei "KAK.HTA" in das Autostart-Verzeichnis von Windows erstellen.

Erst beim nächsten Systemstart wird diese Datei ausgeführt. Dabei erscheint kurz ein Fenster mit dem Titel "Driver Memory Error" und dem Inhalt "S3 driver memory alloc failed".

In dieser Zeit kopiert sich der Virus unter einem neuen Dateinamen in das Windows-Systemverzeichnis. Dieser Dateiname wird generiert aus den ersten 8 Buchstaben des letzten Verzeichnisses in dem Ordner <Windows>\Application Data\Identities.

Außerdem wird der Wurm in das Windows-Verzeichnis als "KAK.HTM" kopiert und so modifiziert, dass er wieder als neue Systeme infizieren kann.

Als nächstes verändert er die Einstellungen von Microsoft Outlook Express 5 in der Registry so, dass zu jeder neu verfassten eMail die Datei "<Windows>\KAK.HTM" als Signatur angehängt wird. Haben Sie bereits eine Signatur eingerichtet, wird diese ab sofort nicht mehr verwendet! Dafür werden folgende Registry-Einträge verändert:

```
[HKEY_CURRENT_USER\Identities\<UID>\Software\Microsoft\
Outlook Express\5.0\signatures]
"Default Signature"="00000000"

[HKEY_CURRENT_USER\Identities\{DA71B880-3169-11D4-85A2-0020AFB6B97D}
\Software\Microsoft\Outlook Express\5.0\signatures\00000000]
"name"="Signature #1"
"type"=dword:00000002
"text"=""
"file"="C:\\WINDOWS\\kak.htm"
```

Nach vollendeter Arbeit wird die Datei AUTOEXEC.BAT noch so erweitert, dass bei nächsten Systemstart die erstellte Datei im Autostart-Verzeichnis gelöscht wird.

```
@echo off>C:\Windows\STARTM~1\Programs\StartUp\kak.hta
del C:\Windows\STARTM~1\Programs\StartUp\kak.hta
```

Das Original wird unter dem Namen AE.KAK gesichert. Um sein Aufruf trotzdem zu gewährleisten, wird die neu angelegte Datei im Windows-System-Verzeichnis in den Autostart der Registry aufgenommen.

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"cAg0u"="C:\\WINDOWS\\SYSTEM\\DA71B880.hta"
```

Wird Windows ab 17.00 Uhr jeden 1. Tages im Monat gestartet, gibt der Virus folgende Meldung aus: "Kagou-Anti-Kro$oft says not today!"

Anschließend wird Windows wieder heruntergefahren.

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