



## Virenbeschreibungen von ITW Computer Viren

# 1 Virenbeschreibung

(C)Copyright 1990-2025 by ROSE SWE, Dipl.-Ing. Ralph Roth

<http://rose.rult.at>

👉 **Alle Rechte vorbehalten!**



Die nachfolgende Beschreibung enthält relevante Informationen zu den am weitesten verbreiteten DOS-Viren. Diese Datei ist Bestandteil der AntiLink-, VirScan- und ViBa-Programme. Die kommerzielle Nutzung ist nur in der registrierten Vollversion gestattet.

Die hier beschriebenen DOS-Viren (Kapitel 4-6) sind alle bei verschiedenen Kunden aufgetreten (ITW = infections in the wild)!

## 1.1 Einführung in Computerviren

Ein Computervirus ist eine Art von bösartiger Software oder Malware, die sich zwischen Computern verbreitet und dabei Daten sowie Software beschädigen kann. Es gibt verschiedene Arten von Computerviren, die jeweils unterschiedliche Methoden zur Infektion und Verbreitung nutzen.

Arten von Computerviren

- Dateinfektoren: Diese Viren hängen sich an ausführbare Dateien an. Sie verbreiten sich, wenn die infizierte Datei ausgeführt wird. Dies ist eine der häufigsten Arten von Viren.
- Boot-Sektor-Viren: Diese Viren infizieren den Boot-Sektor einer Diskette oder Festplatte. Sie werden aktiv, wenn der Computer hochgefahren wird und können das System erheblich stören.
- Makroviren: Diese Viren sind in Makrosprache geschrieben und infizieren häufig Microsoft Office-Dokumente. Sie nutzen die

Funktionalität von Makros, um sich zu verbreiten und Schaden anzurichten.

- Polymorphe Viren: Diese Viren sind besonders gefährlich, da sie ihren Code jedes Mal ändern, wenn sie eine neue Datei oder ein neues System infizieren. Dadurch wird es schwieriger, sie zu erkennen und zu bekämpfen.

## Fazit

Das Verständnis der verschiedenen Arten von Computerviren ist entscheidend, um sich besser vor ihnen zu schützen. Es ist wichtig, regelmäßig Sicherheitssoftware zu verwenden und das System auf mögliche Infektionen zu scannen, um Schäden zu vermeiden.

## 1.2 Details

**Dateiinfektoren** sind Viren, die sich an ausführbare Dateien anhängen und sich verbreiten, indem sie die infizierte Datei ausführen. Diese Viren können den Code der Datei ändern oder zusätzlichen bösartigen Code einfügen, um ihre schädlichen Funktionen auszuführen.

**Boot-Sektor-Viren** infizieren den Boot-Sektor von Disketten oder Festplatten. Der Boot-Sektor ist der Bereich, der das Betriebssystem lädt, wenn ein Computer hochgefahren wird. Ein Boot-Sektor-Virus kann den Boot-Sektor so verändern, dass er zuerst den Virus lädt, bevor das Betriebssystem gestartet wird. Dadurch erhält der Virus die Kontrolle über den Computer und kann andere Disketten oder Festplatten infizieren. Ein bekanntes Beispiel für einen Boot-Sektor-Virus ist der Michelangelo-Virus, der im Jahr 1992 große Schäden anrichtete.

**Makroviren** werden in Makrosprachen geschrieben und infizieren z.B. Microsoft Office-Dokumente. Makros sind kleine Programme, die innerhalb von Dokumenten ausgeführt werden können, um bestimmte Aufgaben zu automatisieren. Ein Makrovirus versteckt sich in einem Dokument und breitet sich aus, wenn das infizierte Dokument geöffnet oder geschlossen wird. Es kann das Verhalten von Makros verändern oder neue Makros erstellen, um schädliche Funktionen auszuführen. Ein Beispiel für einen Makrovirus ist der Melissa-Virus, der im Jahr 1999 Millionen von E-Mails verschickte.

**Polymorphe** Viren ändern ihren Code jedes Mal, wenn sie eine neue Datei oder ein neues System infizieren. Dadurch wird es für Antivirenprogramme schwieriger, sie zu erkennen und zu entfernen. Polymorphe Viren verwenden verschiedene Techniken, um ihren Code zu verschlüsseln oder zu verstecken, wie zum Beispiel Verschlüsselungsalgorithmen oder Junk-Code. Ein Beispiel für einen polymorphen Virus ist der Win32.Zmist-Virus, der seinen Code mit dem Code anderer Programme mischen konnte.

Der Begriff "**In the wild**" wird in Bezug auf Computerviren und -würmer verwendet, um solche Viren und Würmer zu beschreiben, die tatsächlich außerhalb kontrollierter Umgebungen wie Laboren oder geschützten Netzwerken zirkulieren. Diese Viren und Würmer sind in der Lage, sich aktiv auf Systemen zu verbreiten, die mit dem Internet oder anderen Medien verbunden sind, und stellen somit eine unmittelbare Gefahr für Benutzer dar. Im Gegensatz dazu gibt es viele Varianten von Viren und Würmern, die entweder in Laboren von Antivirenprogramm-Herstellern oder in geschlossenen Umgebungen entwickelt und getestet werden. Diese Varianten sind nicht in der "freien Wildbahn" vorhanden und stellen keine direkte Bedrohung für Benutzer dar. Sie dienen häufig als Forschungsobjekte, um neue Abwehrmechanismen zu entwickeln oder um die Funktionsweise von Viren und Würmern zu untersuchen. Die Unterscheidung zwischen "In the wild" und nicht in der Wildbahn befindlichen Varianten von Viren und Würmern ist wichtig, um das tatsächliche Ausmaß der Bedrohung für Benutzer und Systeme zu verstehen. Viren und Würmer, die in freier Wildbahn zirkulieren, erfordern effektive Schutzmaßnahmen wie Antivirensoftware, regelmäßige Updates und sicheres Online-Verhalten, um Infektionen zu verhindern.

## 2 Inhaltsverzeichnis

### Table of Contents

<b>1 Virenbeschreibung.....</b>	<b>1</b>
1.1 Einführung in Computerviren.....	1
1.2 Details.....	2
<b>2 Inhaltsverzeichnis.....</b>	<b>4</b>
<b>3 Beschreibung Würmer und Trojaner.....</b>	<b>8</b>
3.1 Win32.WannaCry.....	8
3.2 Win32.Beagle.....	10
3.3 Win.Sasser.....	11
3.4 Win.Sobig.....	13
3.5 Win.Netsky.....	14
3.6 Win.Mimail.....	18
3.7 Win.MS-Blaster.....	19
3.8 W32/ExploreZip.worm.....	19
3.9 VBS/Loveletter.....	20
<b>4 Beschreibung DOS Dateiviren.....</b>	<b>21</b>
4.1 Maltese Amoeba.2365.....	21
4.2 Burglar.....	22
4.3 Cascade Familie.....	23
4.3.1 1701.....	24
4.3.2 1701-B.....	24
4.3.3 1704.....	25
4.3.4 1704-B.....	25
4.3.5 1704-C.....	25
4.3.6 1704-D.....	25
4.3.7 1704-DESTROY.....	25
4.3.8 1704-FORMAT.....	25
4.3.9 17XX.....	25
4.3.10 17Y4 - Crunning.....	25
4.4 Civil Defense.....	26
4.5 Clonewar.....	27
4.6 Darth Vader.....	28
4.7 Devide Overflow.....	30
4.8 Eddie/Dark Avenger.....	31
4.9 Eicar Testdatei.....	32
4.10 Enmity.808.....	33

4.11 Fish-Virus.....	33
4.12 Frodo.....	34
4.13 Grief.3584.....	35
4.14 Hexametricx.....	37
4.15 Hallöchen.....	38
4.16 Imperial Probe.....	39
4.17 Jerusalem Familie.....	39
4.17.1 Jerusalem A.....	40
4.17.2 Jerusalem B.....	40
4.17.3 Jerusalem C.....	40
4.17.4 Jerusalem D.....	41
4.17.5 Jerusalem DC.....	41
4.17.6 Jerusalem E.....	41
4.17.7 Jerusalem Related.....	41
4.17.8 Jeruslaem.A-204.....	41
4.17.9 Anarkia.....	41
4.17.10 Anarkia-B.....	41
4.17.11 Apokalypse, Phoneme.....	41
4.17.12 Mendoza, Puerto.....	42
4.17.13 Park ESS, Skism-1.....	42
4.17.14 Fu-Manchu.....	42
4.17.15 21.st Century.....	42
4.17.16 Sunday.....	42
4.17.17 PSQR.....	43
4.17.18 Frere Jaques.....	43
4.18 LeHigh.....	43
4.19 Quit.....	44
4.20 Tai-Pan.....	44
4.21 Teraz.....	46
4.22 Tiny.163.....	46
4.23 TPE:Coffeeshop und MtE:Coffeeshop.....	47
4.24 Trojector.....	49
4.25 Vacsina-Virus.....	50
4.26 Vienna.Reboot.....	51
4.26.1 Vienna.A.....	52
4.26.2 Vienna.B.....	52
4.26.3 Vienna.645.....	52
4.26.4 Vienna.Lisbon.....	52
4.26.5 Vienna.AntiVir.....	52
4.26.6 Vienna.FatherChristmas.....	53
4.27 Whale.....	54
4.28 Yankee-Doodle.....	54
<b>5 Beschreibung einiger Hybridviren.....</b>	<b>56</b>
5.1 Anthrax.....	56
5.2 Dir-II.....	57
5.3 Delwin.....	59
5.4 Emperor.....	62

5.5 Flip-Virus.....	64
5.6 Implant Familie.....	66
5.7 Hare.....	67
5.8 Kuarahy.....	68
5.9 Natas.....	69
5.10 Neuroquila.....	70
5.11 Nightfall (N8Fall).....	70
5.11.1 Nightfall.B.....	71
5.11.2 Nightfall.Spawn.....	71
5.12 Junkie.....	71
5.13 Telecom/Kampana.....	73
5.14 Tequila-Virus.....	74
5.15 Thanksgiving.....	76
5.16 Tremor.....	77
<b>6 Beschreibung einiger Bootviren.....</b>	<b>79</b>
6.1 AntiCMOS.....	79
6.2 AntiExe.....	81
6.2.1 Telecom Boot.....	82
6.3 Anti-Tel.....	82
6.4 ASBV.....	83
6.5 Boot-437.....	84
6.6 DrDemon.....	85
6.7 EDV-Virus.....	85
6.8 Form-Virus.....	86
6.8.1 Form.Headcrash.....	87
6.9 Joshi.....	87
6.10 MusicBug.....	88
6.11 Orge/Disk Killer.....	89
6.12 Ping-Pong.....	90
6.13 Parity Check/Parity Boot.....	91
6.14 Quandary.....	92
6.15 Stoned.....	93
6.15.1 Stoned.A.....	94
6.15.2 Stoned.B.....	94
6.15.3 Stoned.C.....	94
6.15.4 Stoned.D.....	94
6.15.5 Stoned.E.....	94
6.15.6 Stoned.F.....	95
6.15.7 Stoned II.....	95
6.15.8 Stoned.Azusa.....	95
6.15.9 Stoned.Hong Kong-2.....	95
6.15.10 Stoned.Michelangelo.....	96
6.15.11 Stoned.Rostov.....	97
6.15.12 Stoned.Sex_Revolution 1.1 bzw. 2.0.....	97

6.16 V-Sign.....	97
6.17 WYX.....	98
<b>7 UEFI Bootkits.....</b>	<b>99</b>
7.1 Windows UEFI Malware.....	99
7.2 Bootkitty: Der erste UEFI-Bootkit für Linux.....	100
7.2.1 Funktionsweise:.....	100
7.2.2 Gefahren und Gegenmaßnahmen:.....	101
<b>8 Ende der Dokumentation.....</b>	<b>101</b>

## 3 Beschreibung Würmer und Trojaner



### 3.1 Win32.WannaCry

ca. 350 Varianten bekannt  
größter Ausbruch 12. Mai 2017

Es handelt sich um einen Kryptotrojaner, der Daten auf den betroffenen Computern verschlüsselt. Der Erpressungstrojaner WannaCry soll innerhalb von drei Tagen schon mehr als 220.000 Computer in 150 Ländern befallen haben und richtet enorme Schäden an. In krassem Missverhältnis dazu steht das Lösegeld von schätzungsweise wenig mehr als 30.000 Euro, das die Autoren der gefährlichen Schadsoftware bisher erpressen konnten. Das geforderte Lösegeld von 300 bis 600 Euro muss in Form von Bitcoins gezahlt werden; bisher sind fünf Bitcoin-Adressen der Erpresser bekannt geworden.



**Ooops, your important files are encrypted.**

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

Es sind vor allem ältere Windows-Versionen betroffen, die nicht mehr mit Sicherheits-Updates versorgt werden. Microsoft hatte die verantwortliche Sicherheitslücke bereits im März durch Sicherheits-Updates geschlossen (Sicherheitsupdate MS17-010). Diese Patches liefert der Hersteller jedoch nur für die aktiv unterstützten Windows-Versionen. Ältere Windows-Versionen blieben also weiter ungeschützt – dazu gehören insbesondere Windows XP und Windows Server 2003. Nach bisherigen Erkenntnissen nutzt WannaCry zwei Angriffsvektoren: Einmal verbreitet er sich – wie bei Kryptotrojanern üblich – per E-Mail. Wenn der Schädling ein System infiziert hat, versucht er auch, wie ein Wurm andere Rechner im gleichen Netz zu kompromittieren. Dafür nutzt WannaCry offenbar eine Lücke in Windows Dateifreigaben (SMB). Diese Lücke war bekannt geworden, nachdem eine Hackergruppe namens „Shadow Brokers“ einige Exploits der NSA-nahen Equation Group veröffentlicht hatte. Der Exploit, der die von WannaCry genutzte Lücke ausnutzt, ist unter dem Namen EternalBlue bekannt.

Am 9. Mai soll der Nutzer den Code für die Entschlüsselung erhalten, ansonsten sei die Löschung veranlasst. Die Zahlungen sollten in Bitcoin abgewickelt werden. Bislang zahlten 126 Opfer insgesamt etwa 30.000 Euro. Weltweit sollen zur Stunde über 220.000 Systeme betroffen sein. Anders als Locky & Co springt der Schädling von einem infizierten

Rechner auf andere, übers Netz erreichbare Windows-Systeme über.

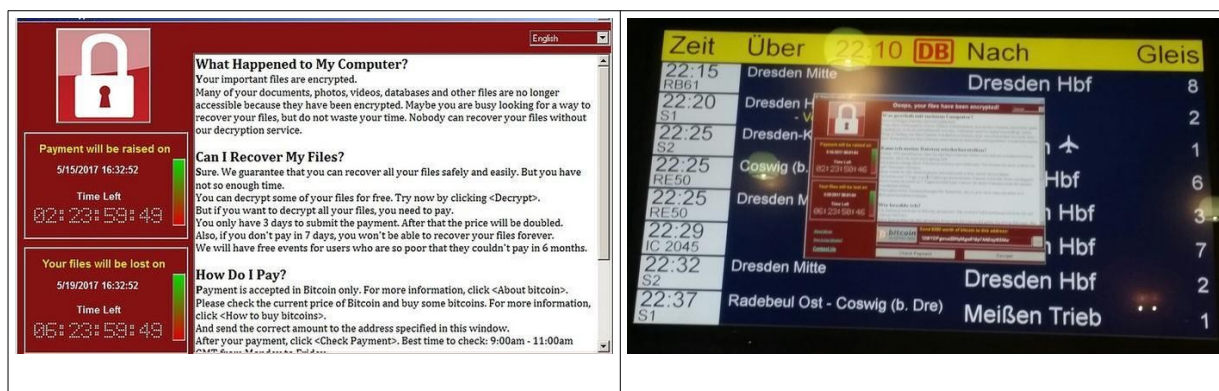


Table 3.1: Infizierte Systeme mit WannaCry

## 3.2 Win32.Beagle

W32.Beagle.M@mm ist ein Massenmailer Wurm, der sich über seine eigene SMTP Maschine versendet. Er verbreitet sich auch über Netzwerkfreigaben, die den Wortteil shar enthalten. Dies trifft beispielsweise für die Tauschbörse KaZaA zu. Wie seine Vorgänger installiert der Wurm eine Backdoor und infiziert zusätzlich .EXE Dateien.

Dem Anwender wird in der gefälschten Absenderadresse eine vertrauenswürdige Stelle in der eigenen (Empfänger-) Domäne vorgespielt. (Beispiel: Supports<Empfänger-Domain>)

Größe des Anhangs: variiert zwischen 21 und 22 kB. Der Wurm sucht Email Adressen in Dateien mit den Endungen:

adb, asp, cfg, cgi, dbx, dhtm, eml, htm, jsp, mbx, mdx, mht, mmf, msg, nch, ods, oft, php, pl, sht, shtml, stm, tbb, txt, uin, wab, wsh, xls, xml

Der Wurm kopiert sich im infizierten System unter %System%\winupd.exe, %System%\winupd.exe open, %System%\winupd.exeopen open und %System%\winupd.exe open open open

Hinweis: %System% ist eine Systemvariable, die den tatsächlichen Dateipfad enthält. Dieser variiert bei den verschiedenen Windows Versionen. Beispiel: %System% enthält C:\Windows\System bei Windows 95/98/Me, C:\Winnt\System32 bei Windows NT/2000, und C:\Windows\System32 bei Windows XP.

Mit dem Registrierungsschlüssel

- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Curre

ntVersion\Run winupd.exe"="%System%\winupd.exe

wird Beagle.M beim Rechnerstart aktiviert. Eine Backdoor wird installiert und öffnet auf dem infizierten Computer den TCP Port 2556.

Worm/Bagle.U hat eine Dateigröße von 8.208 Bytes und kopiert sich als GIGABIT.EXE in das Windows Systemverzeichnis. Die versandten Emails des Wurms haben keinen Text im Subject und Body. Er legt den folgenden Registry-Eintrag an, damit er beim nächsten Systemstart automatisch gestartet wird:

- [HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run] "gigabit.exe"="C:\\WINDOWS\\SYSTEM\\gigabit.exe"

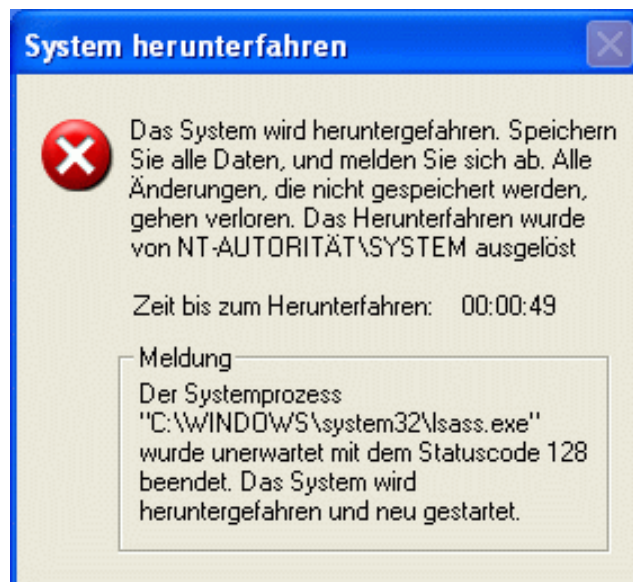
### 3.3 Win.Sasser

Sasser (Bedeutung des Namens: Wortspiel aus dem englischen Verb „to sass“ – „freche Antworten geben“ und der Tatsache, dass er den Dienst LSASS ausnutzt) ist der Name eines Computerwurms, der sich Anfang Mai 2004 in hoher Geschwindigkeit auf Computern mit den Microsoft-Betriebssystemen Windows 2000 sowie Windows XP verbreitete. Sein „offizieller“ Name ist W32.Sasser. Unter den betroffenen Systemen waren Computer bei Banken, Reiseunternehmen und öffentlichen Einrichtungen. Betroffen waren die Computer der deutschen Postbank, der finnischen Sampo Bank, der Delta Air Lines und der Europäischen Kommission sowie weiterer Unternehmen und Behörden weltweit. Der Programmierer von Sasser, ein damals 17-jähriger Schüler aus Waffensen, einem Ortsteil der Stadt Rotenburg (Wümme), wurde am 7. Mai 2004 vorübergehend festgenommen. Der Informatikschüler (Berufsfachschule) ist auch für die Viren der Netsky-Reihe verantwortlich.

Sasser wird nicht als E-Mail-Anhang versandt. Sobald sich ein Benutzer mit dem Internet verbindet, nutzt der Wurm einen Fehler in einem Windows-Systemdienst mit dem Namen Local Security Authority Subsystem Service (LSASS) aus. Findet er einen verwundbaren Rechner, infiziert er ihn mit einem Code, der den eigentlichen Wurm von bereits infizierten Rechnern kopiert. Dazu startet er auf Port 5554 einen FTP-Server.



Der befallene Rechner wird von dem Wurm in unregelmäßigen Abständen ein- und ausgeschaltet. Der materielle Schaden ist dabei schwer zu bemessen, da es sich bei den Schäden im Wesentlichen um allgemeine Produktivitätsverluste in Unternehmen bzw. um Mängel in der Erreichbarkeit und Nutzbarkeit von Internetseiten durch die Kunden handelt.



Innerhalb kurzer Zeit tauchten mehrere Varianten des Wurms auf: Sasser.B, Sasser.C und Sasser.D (das Original wird Sasser.A genannt). Zudem nutzt ein E-Mail-Wurm mit dem Namen Netsky.AC die Angst von Anwendern vor Sasser aus: Als Absender gibt er sich als ein Hersteller von Antivirensoftware aus und tarnt sich unter anderem als Programm zum Entfernen von Sasser.B.

Ein weiterer Wurm mit dem Namen Phatbot schließt normalerweise die Hintertüren, die andere Würmer geöffnet haben, und löscht beispielsweise

bei den Würmern Bagle oder Mydoom den Schädling. Sasser jedoch wird von Phatbot verändert, um alle IP-Adressen des Wurms herauszufinden und folgt Sasser nach, um die neu befallenen Rechner zu infizieren. Man kann diese Infektion an einer Datei mit dem Namen wormride.dll im Windowsverzeichnis erkennen. Ist diese Datei vorhanden, ist der Rechner mit beiden Würmern infiziert.

Sasser hat schätzungsweise zwei Millionen Rechner infiziert. Die bisher schlimmste Attacke durch den Wurm W32.Blaster, der auch Lovsan genannt wird, hatte nach Schätzungen von Microsoft 9,5 Millionen Computer infiziert und weltweit erhebliche finanzielle Schäden verursacht. Um den Programmierer ausfindig zu machen, setzte der Softwarekonzern eine Belohnung von 250.000 Dollar aus, die zur Ergreifung des Täters führte.

Der Entwickler der Computerwürmer wurde am 8. Juli 2005 vom Jugendschöffengericht des Landgerichts Verden zu einer Jugendstrafe von einem Jahr und neun Monaten auf Bewährung und 30 Stunden gemeinnütziger Arbeit verurteilt.

### 3.4 Win.Sobig

**Sobig.F** oder exakt **W32.Sobig.F@mm** ist ein am 18. August 2003 entdeckter Computerwurm. Er wurde vermutlich über eine pornografische Newsgroup freigesetzt und ist der sechste aus einer Serie von immer ausgeklügelter Internet-Würmern, die seit Januar 2003 ins Netz gebracht worden sind. W32.Sobig.F@mm wird als netzwerk aktiver Massen-Mail-Wurm charakterisiert, der sich an alle E-Mail-Adressen sendet, die er in Dateien mit den Erweiterungen .dbx, .eml, .hlp, .htm, .html, .mht, .wab oder .txt findet. Der eingekerkerte Wurm öffnet auf den befallenen Rechnern Ports zum Internet, installiert einen eigenen Mailserver und sendet parallel unablässig infizierte E-Mails an beliebige Empfänger.

Wenn der Virus Sobig.F aktiviert ist, kopiert er sich in das Windows-Verzeichnis mit dem Namen „WINPPR32.EXE“ und legt eine Konfigurationsdatei mit dem Namen „WINSTT32.DAT“ im selben Verzeichnis ab.

Folgende Einträge in der Registry werden durchgeführt:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- "TrayX" = C:\WINNT\WINPPR32.EXE /sinc
- HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- "TrayX" = C:\WINNT\WINPPR32.EXE /sinc

Der Virus ist darauf programmiert, bis zum 10. September 2003 jeden Freitag und Sonntag Kontakt zu bestimmten Rechnern aufzunehmen, um von dort – wie es scheint – weitere Instruktionen zu erhalten. Dabei wird

ein UDP-Paket an Port 8998 eines Remote-Servers gesandt. Diese Rechner wurden aufgrund der ermittelten IP-Adressen inzwischen bereits vom Netz genommen. Aufgrund der seit dem „Verfallsdatum“ praktisch nicht mehr auftretenden Neuinfektionen mit Sobig.F wurde der Virus beispielsweise von Symantec aus der Gefahrenstufe 4 in die Kategorie 2 verschoben.

Von Sobig.F betroffen sind potenziell alle Microsoft-Betriebssystemversionen von Windows 95 bis Windows XP.

### 3.5 Win.Netsky

Größe des Anhangs: 29.568 Bytes

Der Wurm sucht E-Mail Adressen in Dateien mit den Endungen:

.adb, .asp, .cgi, .dbx, .dhtm, .doc, .eml, .htm, .html, .jsp, .msg, .oft, .php, .pl, .rtf, .sht, .shtm, .tbb, .txt, .uin, .vbs, .wab, .wsh, .xml

Infektion des Systems

Der Wurm kopiert sich im infizierten System mehrfach unter:

- %windir%\FVProtect.exe
- %windir%\userconfig9x.dll
- %windir%\base64.tmp
- %windir%\zip1.tmp
- %windir%\zip2.tmp
- %windir%\zip3.tmp
- %windir%\zipped.tmp

Hinweis: %windir% ist eine Systemvariable, die den tatsächlichen Dateipfad enthält. Dieser variiert bei den verschiedenen Windowsversionen. Beispiel: %windir% enthält C:\Windows bei Windows 95/98/Me, C:\Winnt bei Windows NT/2000, und C:\Windows bei Windows XP.

Mit dem Registrierungsschlüssel

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] "Norton Antivirus AV"="%Windir%\FVProtect.exe"
```

wird Netsky.P beim Rechnerstart aktiviert.

Weiterhin werden von dem Wurm mehrere Registrierungsschlüssel gelöscht. Dabei handelt es sich um Schlüssel, die u.a. zum Wurm Mydoom.A und Mydoom.B gehören. Löschen von Einträgen in der



## Registrierungsdatei

Der Computerwurm löscht die folgenden Einträge und Schlüssel in der Registrierungsdatei, die bei Infektion mit bestimmter anderer Malware vorgenommen werden:

### WORM\_MYDOOM.A

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Taskmon
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run Taskmon

### WORM\_MYDOOM.B

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Explorer
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run Explorer

### WORM\_MYDOOM.A und WORM\_MYDOOM.B

- HKEY\_CLASSES\_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32

### WORM\_MIMAIL.T

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run KasperskyAv
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run KasperskyAv

### WORM\_NETSKY.A oder WORM\_NETSKY.B

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Service

### WORM\_DEADHAT.B

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run msgsvr32

### WORM\_BAGLE.A

- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run d3dupdate.exe

### WORM\_BAGLE.A

- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run au.exe

### WORM\_NACHI.B und WORM\_NACHI.C

- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Service

s WksPatch

PE\_PARITE.A

- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer PINF

Darüber hinaus werden die folgenden Einträge aus der Registrierungsdatei entfernt, die möglicherweise von anderer Malware für Autostart Routinen genutzt werden:

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run System.
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Sentry
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Windows Services Host
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run Windows Services Host

Payload bzw. Schadensteil

Bei aktuellem Systemdatum = 2. März 2004 und Systemzeit zwischen 6.00 und 9.00 Uhr sendet die Malware Pieptöne aus.

Größe des Anhangs: 22.016 Bytes

Der Wurm sucht E-Mail Adressen in Dateien mit den Endungen:

.dhtm, .cgi, .shtm, .msg, .oft, .sht, .dbx, .tbb, .adb, .doc, .wab, .asp, .uin, .rtf, .vbs, .html, .htm, .pl, .php, .txt, .eml

Der Wurm kopiert sich im infizierten System mehrfach unter %windir%\Winlogon.exe

Hinweis: %windir% ist eine Systemvariable, die den tatsächlichen Dateipfad enthält. Dieser variiert bei den verschiedenen Windowsversionen. Beispiel: %windir% enthält C:\Windows bei Windows 95/98/Me, C:\Winnt bei Windows NT/2000, und C:\Windows bei Windows XP.

Mit dem Registrierungsschlüssel

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] "ICQ Net" = "%Windir%\winlogon.exe -stealth"

Verbreitung über Tauschbörsen



Netsky.K sucht auf dem infizierten Computer nach Verzeichnisnamen, die folgende Zeichenketten enthalten:

- bear
- donkey
- download
- ftp
- htdocs
- http
- icq
- kazaa
- lime
- morpheus
- mule
- my shared folder
- shar
- shared files
- upload

In diese Verzeichnisse kopiert sich der Wurm mit einem der folgenden Dateinamen:

- |                           |                             |
|---------------------------|-----------------------------|
| • more.rtf.exe            | • Britney Spears            |
| • 3D Studio Max 6         | fuck.jpg.exe                |
| 3dsmax.exe                | • Britney Spears full       |
| • ACDSee 10.exe           | album.mp3.exe               |
| • Adobe Photoshop 10      | • Britney Spears            |
| crack.exe                 | porn.jpg.exe                |
| • Adobe Photoshop 10      | • Britney Spears Sexy       |
| full.exe                  | archive.doc.exe             |
| • Adobe Premiere 10.exe   | • Britney Spears Song text  |
| • Ahead Nero 8.exe        | archive.doc.exe             |
| • Altkins Diet.doc.exe    | • Britney Spears.jpg.exe    |
| • American Idol.doc.exe   | • Britney Spears.mp3.exe    |
| • Arnold                  | • Clone DVD 6.exe           |
| Schwarzenegger.jpg.exe    | • Cloning.doc.exe           |
| • Best Matrix Screensaver | • Cracks & Warez            |
| new.scr                   | Archiv.exe                  |
| • Britney sex xxx.jpg.exe | • Dark Angels new.pif       |
| • Britney Spears and      | • Dictionary English 2004 - |
| Eminem porn.jpg.exe       | France.doc.exe              |
| • Britney Spears          | • DivX 8.0 final.exe        |
| blowjob.jpg.exe           | • Doom 3 release 2.exe      |
| • Britney Spears          | • E-Book Archive2.rtf.exe   |
| cumshot.jpg.exe           | • Eminem blowjob.jpg.exe    |

- Eminem full album.mp3.exe
- Eminem Poster.jpg.exe
- Eminem sex xxx.jpg.exe
- Eminem Sexy archive.doc.exe
- Eminem Song text archive.doc.exe
- Eminem Spears porn.jpg.exe
- Eminem.mp3.exe
- Full album all.mp3.pif
- Gimp 1.8 Full with Key.exe
- Harry Potter 1-6 book.txt.exe
- Harry Potter 5.mpg.exe
- Harry Potter all e.book.doc.exe
- Harry Potter e book.doc.exe
- Harry Potter game.exe
- Harry Potter.doc.exe
- How to hack new.doc.exe
- Internet Explorer 9 setup.exe
- Kazaa Lite 4.0 new.exe
- Kazaa new.exe
- Keygen 4 all new.exe
- Learn Programming 2004.doc.exe
- Lightwave 9 Update.exe
- Magix Video Deluxe 5 beta.exe
- Matrix.mpg.exe
- Microsoft Office 2003 Crack best.exe
- Microsoft WinXP Crack full.exe
- MS Service Pack 6.exe
- netsky source code.scr
- Norton Antivirus 2005 beta.exe
- Opera 11.exe
- Partitionsmagic 10 beta.exe
- Porno Screensaver britney.scr
- RFC compilation.doc.exe
- Ringtones.doc.exe
- Ringtones.mp3.exe
- Saddam Hussein.jpg.exe
- Screensaver2.scr
- Serials edition.txt.exe
- Smashing the stack full.rtf.exe
- Star Office 9.exe
- Teen Porn 15.jpg.pif
- The Sims 4 beta.exe
- Ulead Keygen 2004.exe
- Visual Studio Net Crack all.exe
- Win Longhorn re.exe
- WinAmp 13 full.exe
- Windows 2000 Sourcecode.doc.exe
- Windows 2003 crack.exe
- Windows XP crack.exe
- WinXP eBook newest.doc.exe
- XXX hardcore pics.jpg.exe

### 3.6 Win.Mimail

Der Dateiname der angehängten Datei ist InfoUpdate.exe oder www.paypal.com.pif und hat eine Größe von 13.856 Bytes. Wird diese Datei ausgeführt, erzeugt Mimail.J einen Eintrag in der Registry, mit dem der Wurm beim Rechnerstart aktiviert wird.

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "SvcHost32"="%Windir%\svchost32.exe"

### 3.7 Win.MS-Blaster

W32.Blaster.Worm ist ein Wurm, der sich über das Netzwerk vorzugsweise über das Internet verbreitet. Er nutzt dazu die so genannte DCOM RPC Schwachstelle aus. Diese Schwachstelle befindet sich in nicht gepatchten Windows NT/2000/XP und Windows 2003 Serversystemen. Informationen zu dieser Schwäche finden Sie im deutschen Microsoft Security Bulletin MS03-026 . Hier gelangen Sie zum Download der Sicherheit Patches für die unterschiedlichen Betriebssysteme.

Der W32.Blaster.Worm legt sich im Systemverzeichnis (Standard: C:\Windows\System32 bzw. C:\Winnt\System32) unter dem Namen MSBLAST.EXE ab. Durch Änderungen in der Registrierung wird diese Datei bei jedem Neustart des Rechners aufgerufen und ausgeführt.

Der Wurm verbreitet sich weiter und führt eine sog. DDoS-Attacke (Distributed Denial of Service) gegen einen Microsoft-Server (windowsupdate.com) durch ; dabei wird versucht, diesen Server mit so vielen Anfragen zu überfluten, dass er nicht mehr antworten kann. Diese Attacke wird in den Monaten Januar bis August vom 16. bis zum Ende des Monats, in den Monaten September bis Dezember fortlaufend (täglich) durchgeführt.

### 3.8 W32/ExploreZip.worm

Entdeckung: 10.06.1999  
Aka ExplorerZip

Der Wurm befällt Computer mit den Betriebssystemen Windows 95, Windows 98 und Windows NT. Er verbreitet sich auf Systemen mit MS Outlook bzw. MS Outlook Express und MS Exchange. Dabei wird eine Email Nachricht versendet, an die eine ausführbare Datei angehängt ist. Führt der Empfänger dieses Programm aus, wird es auf seinem Rechner aktiviert. Das Attachment erweckt den Eindruck, dass es ein selbst extrahierendes ZIP-Archiv mit DOC-Dateien ist. Die angehängte Datei (Attachment) heißt zipped\_files.exe. Wird das Attachment ausgeführt, wird eine Fehlermeldung in einem Fenster mit folgendem Text ausgegeben, die der von WINZIP gleicht.

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

Der Wurm versendet Nachrichten an Adressen, von denen der Computerbenutzer selbst eine Mail empfangen hat (Posteingang). Die Nachricht enthält folgenden Text:

*Hi [Name des Empfängers]!  
I received your email and i shall send you a reply ASAP.  
Till then, take a look at the attached zipped docs.  
bye  
Attachment: zipped\_files.exe*

Der Wurm kopiert sich mit dem Dateinamen EXPLORE.EXE in das Verzeichnis C:\WINDOWS\SYSTEM. Anschließend modifiziert er die Datei WIN.INI, wodurch das Programm bei jedem Start von Windows ausgeführt wird.

Der Wurm enthält eine gefährliche Schadensfunktion: Er durchsucht alle verfügbaren Laufwerke nach Dateien von MS Office und Quelltexten (DOC, XLS, PPT, ASM, CPP, ...) und zerstört diese, indem er deren Länge auf 0 Byte setzt.

## Entfernung von Hand

Windows 95/98:

Löschen Sie in der Datei WIN.INI die Zeile "run=c:\windows\system\explore.exe", damit der Wurm beim nächsten Windows Start nicht mehr aktiviert wird. Nach einem Neustart läßt sich auch der Wurm selbst, die Datei EXPLORE.EXE im Verzeichnis C:\WINDOWS\SYSTEM problemlos löschen.

Windows NT:

Unter Windows NT ist der Wurm als "explore" im Task Manager zu finden; dort sollte er zunächst deaktiviert werden. Anschließend muß mit RegEdit der Pfad

- "[HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows]"

bearbeitet werden, wobei der Schlüssel "run=C:\\WinNT\\System32\\Explore.exe" zu entfernen ist. Nach einem Systemneustart kann auch hier die Datei EXPLORE.EXE gelöscht werden.

## 3.9 VBS/Loveletter

Bei Loveletter, oft auch I-love-you-Virus genannt, handelt es sich um einen Computerwurm, der sich am 4. Mai 2000 und den Folgetagen explosionsartig per E-Mail verbreitete. Die Betreffzeile lautete

„ILOVEYOU“. Der Wurm verursachte weltweit Schäden in Höhe von geschätzten 10 Milliarden Dollar.

---

*Abbildung 3.1: E-Mail mit Loveletter Anhang*

Neben dem Neugier erweckenden Betreff versuchte „I love you“ gezielt, die Empfänger in falscher Sicherheit zu wiegen – er verschickte sich an Einträge aus dem persönlichen Adressbuch, so dass die Empfehlung „Öffnen Sie keine Mailanhänge von fremden Personen“ nicht griff. Außerdem hieß der Anhang LOVE-LETTER-FOR-YOU.TXT.vbs, so dass sich viele Empfänger an „.txt-Dateien sind harmlos“ erinnerten, da die richtige Erweiterung .vbs in einer Standard-Windowsinstallation nicht angezeigt wird.

Da der Wurm aus einer Skript-Datei besteht, die mit jedem gewöhnlichen Editor bearbeitet werden kann, gibt es mehr als 100 Varianten. Oft handelt es sich nur um kleine Veränderungen, wie ein alternativer e-Mail oder IRC- Text oder andere Dateinamen.

## 4 Beschreibung DOS Dateiviren

### 4.1 Maltese Amoeba.2365

Maltese Amoeba wurde ursprünglich in Malta geschrieben, aber seltsamerweise wurde er erst Ende 1991 in Irland gefunden - was bedeutet, dass sich der Virus unbemerkt von einer Seite der Welt zur anderen verbreiten konnte.

Maltese Amoeba ist ein residenter Virus, der COM- und EXE-Dateien

infiziert. Infizierte Dateien wachsen um 2504 bis 2564 Bytes an. Die Zeit- und Datumsstempel der Dateien werden nicht verändert. Die Infektion erfolgt beim Laden und Ausführen sowie beim Schließen eines Programms. Der Virus verwendet eine sich selbst modifizierende Verschlüsselung und es ist kein Suchmuster möglich.

Es ist ein destruktiver Virus, der die ersten vier Sektoren der Spuren 0 bis 29 der Festplatte und jede Diskette im Laufwerk überschreibt, wenn das Datum der 1. November oder der 15. März eines beliebigen Jahres ist. Es folgt ein psychedelischer Bildschirmeffekt. Wenn das Gerät eingeschaltet wird, erscheint ein Fragment eines Gedichts (The Auguries of Innocence) von William Blake (1745-1827) auf dem Bildschirm und der Computer bleibt hängen. Dabei lässt es die folgende Meldung auf dem Bildschirm aufblinken:

```
„To see a world in a grain of sand,  
And a heaven in a flower  
Hold infinity in the palm of your hand  
And eternity in an hour.“
```

THE VIRUS 16/3/91

```
"To see a world in a grain of sand,  
And a heaven in a wild flower  
Hold Infinity in the palm of your hand  
And Eternity in an hour."
```

THE VIRUS 16/3/91

Der Virus enthält auch eine weitere Nachricht, die nie angezeigt wird und die man nicht sehen kann, wenn man sich den Virencode ansieht:

```
AMOEBA virus by the Hacker Twins (C) 1991 This is nothing, wait for  
the release of AMOEBA II-The universal infector, hidden to any eye but  
ours! Dedicated to the University of Malta-the worst educational  
system in the universe, and the destroyer of 5X2 years of human life.
```

## 4.2 Burglar

Aka Graveyard

Dieser Virus trat das erste Mal im Sommer 1996 in Deutschland auf. Inzwischen ist der Burglar Virus in Deutschland sehr weit verbreitet

(ITW). Verbreitet wurde der Virus anscheinend auf einer Party (siehe E-Mail Auszug in K\_Burglar.DOC) sowie über viele infizierte Sharewareprogramme oder BBS Intros.

Burglar ist ein speicherresidenter EXE Infektor mit Tarnkappeneigenschaften (Dateilänge) und einer Größe von 1150 Bytes. Burglar infiziert beim Kopieren von Dateien sowie bei der Eingabe des DIR Befehles. Der Virus ist nicht verschlüsselt und enthält die Texte:

AT THE GRAVE OF GRANDMA  
Burglar/H\*.\*

Die Originaldaten des Wirtprogramms (EXE-Header) sind jedoch verschlüsselt im Virus abgespeichert, vermutlich sollte verhindert werden dafür ein Killerprogramm zuschreiben. Trotzdem kann der Virus problemlos mit dem Killerprogramm K-Burglar oder mit VirScan Plus entfernt werden.

Merkmale:

- Größe (Dateischreibzugriff): 1150 Bytes
- Größe (Programmsegment bis Dateiende): 1150 Bytes
- Größe (Programmstart bis Dateiende): 1150 Bytes
- Virus aktualisiert Dateidatum- und Uhrzeit beim Infizieren
- Virus benutzt Datei-Stealthfunktionen (Länge) (1150 Bytes)
- Virus benutzt Dateiuhrzeit als Markierung (Sekunde=62)
- Virus benutzt undokumentierte Interruptfunktion (Selbsterkennung): 21/F078 21/0000
- Virus fängt das Öffnen von Programmen ab (Extended Open)
- Virus gibt Texte aus oder verändert Grafikspeicher
- Virus hängt sich an das Ende des Programmes
- Virus infiziert .EXE Programme
- Virus infiziert beim Setzen des Dateiattributes
- Virus infiziert Programme beim Öffnen („Fast Infector“)
- Virus ist möglicherweise speicherresident
- Virus kann READ-ONLY, HIDDEN oder SYSTEM Attribute nicht umgehen
- Virus manipuliert den Dateianfang
- Virus prüft auf .EXE-Programmheader („MZ“)
- Virus prüft auf .EXE-Programmheader („ZM“)
- Virus überprüft die Systemuhrzeit
- Virus verschiebt seinen Code im Speicher (1333 Bytes)

## 4.3 Cascade Familie

(Alias: Herbstlaub, Black-Jack, 1701, 1704, Fall, Falling Letters, August)

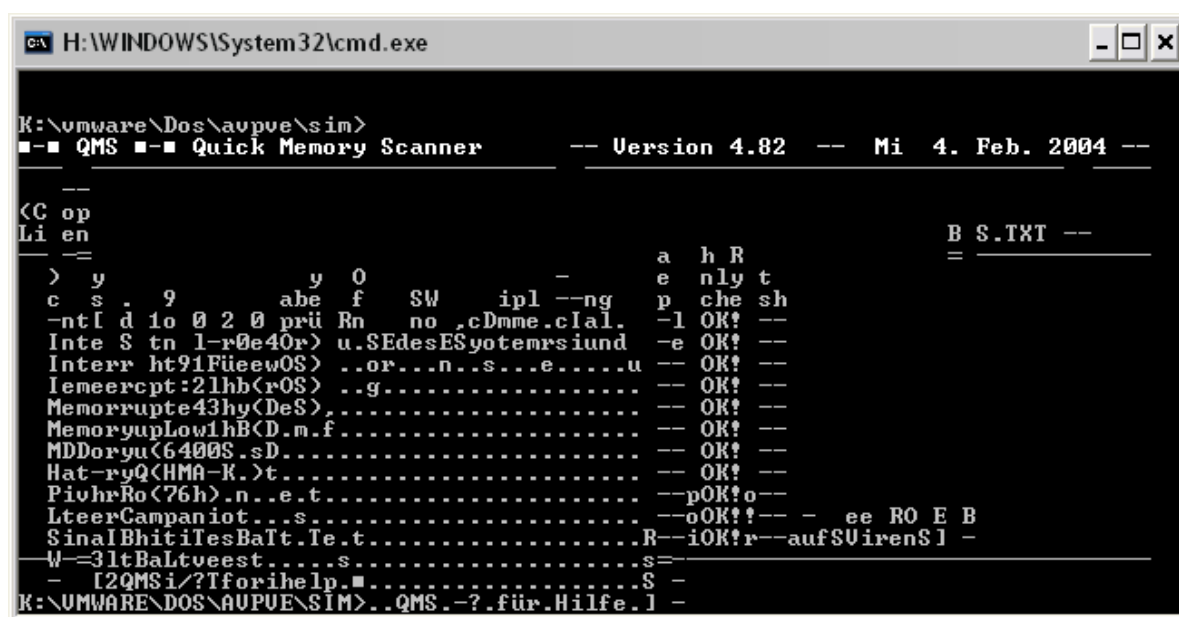
Dieser Virus stammt vermutlich aus Deutschland und befällt aus-

schließlich COM-Dateien, die um 1701 bzw. 1704 Bytes verlängert werden, COMMAND.COM wird nicht befallen.

Der Virus enthält MSDOS Funktionsaufrufe, die zum damaligen Zeitpunkt der breiten Öffentlichkeit nicht zugänglich waren. Da eine Häufung von Infektionen mit dem 1701/1704-Virus im Stuttgarter Raum auftraten, wird angenommen, dass der Virus in einer, in Stuttgart ansässiger, Computerfirma geschrieben wurde.

#### 4.3.1 1701

Beim ersten Aufruf installiert sich der Virus speicherresident und befällt danach jede aufgerufene COM-Datei. Seine Schadensfunktion ist auf die Manipulation des Bildschirms beschränkt. Zwischen Oktober und Dezember jeden Jahres beginnen zeitverzögert die Buchstaben auf dem Bildschirm verschoben zu werden (daher der englische Name "Falling Letters").



Während die Buchstaben fallen, ist der Zugriff auf den PC gesperrt. Dieser Effekt tritt jedoch nur bei Rechnern auf, die eine CGA- oder eine VGA-Karte besitzen.

Während der übrigen Zeit des Jahres werden Dateien nur infiziert und keine Schadensfunktion ausgeführt, sieht man einmal vom Zeitdiebstahl und möglichen Problemen mit anderer speicherresidenter Software ab.

#### 4.3.2 1701-B

Diese Variante ist nicht auf die zeitliche Auslösefunktion beschränkt, sondern kann zu jedem beliebigen Datum die Schadensfunktion auslösen.



#### 4.3.3 1704

Dieser Virus ist mit der 1701-Variante nahezu identisch und befällt nur COM-Dateien, die um 1704 Bytes verlängert werden. Original IBM-PC's werden von diesem Virus nicht befallen. Der Virus verfügt über eine ausgeklügelte Verschlüsselungstechnik. Schadensfunktion und Manipulationsaufgabe sind ebenfalls mit dem 1701 identisch. Die Routine, die die Buchstaben fallen lässt, wird nur in den Jahren 1980-1987 (im Herbst) ausgeführt. COMMAND.COM wird nicht infiziert. Ich besitze eine Variante, die jedoch auch die Datei COMMAND.COM infiziert.

#### 4.3.4 1704-B

Das Herabfallen der Buchstaben auf dem Bildschirm wurde durch eine Reboot-Routine ersetzt. Diese wird, nachdem der Virus speicherresident ist, nach einem Zufallsprinzip ausgeführt.

#### 4.3.5 1704-C

Wie der 1704-B, jedoch Aktivierung nur im Dezember.

#### 4.3.6 1704-D

Diese Variante befällt nun auch alle Original IBM-PC's.

#### 4.3.7 1704-DESTROY

Diese Form verfügt über alle bereits bekannten Funktionen von 1704, mit dem Unterschied, dass es zu Veränderungen und zur Zerstörung der FAT von Festplatten kommen kann.

#### 4.3.8 1704-FORMAT

Diese Variante formatiert unter bestimmten Bedingungen die Festplatte.

#### 4.3.9 17XX

Diese Variante unterscheidet sich vom Original in zwei Byte der Verschlüsselung-Routine.

#### 4.3.10 17Y4 - Crunning

Diese Variante unterscheidet sich vom 1704-Virus in nur einem Byte im Code. Varianten von diesem Virus spielen jedoch Musik (Crunning).

## 4.4 Civil Defense

Alias Civil.6656, CD.6656, CD.6672, CDV 1.1, CDV 3.3  
Ursprung: Ost-Europa? Evtl. Russland. 1992?

Von diesem Virus gibt es mindestens zwei verschiedene Varianten (wahrscheinlich sogar drei), nähere Informationen hierzu scheint es jedoch nicht zu geben. Dies ergab eine weltweite Nachfrage in verschiedenen Virendatenbanken.

Beim Start überprüft der Virus, ob er sich schon im Arbeitsspeicher und in den MBR (Partitionstabelle) der Festplatte eingenistet hat. Falls dies noch nicht geschehen ist, schreibt er sich in den MBR der Festplatte. Hierzu wird ein kleines Ladeprogramm in den MBR geschrieben. Civil Defense bleibt solange inaktiv, bis Sie beim nächsten Bootvorgang den Virus aus dem MBR aktivieren. Dann infiziert er alle EXE Programme, wenn sie gestartet werden. Eine Infizierung von Programmen kann man an einem Zuwachs von ca. 6656 Bytes an der Datei erkennen (z. B. mit AntiLink), wenn der Virus sich NICHT im Arbeitsspeicher befindet! Der Virus überprüft anscheinend nicht, ob die EXE Dateien interne Overlays besitzen und zerstört solche Programme durch die Infektion. Mit einer Codelänge von über 6500 Bytes gehört der Civil-Defense Virus zu den größten TSR-Viren überhaupt!

Der Virus gehört zur so genannten vierten Generation von Viren, weil er alle möglichen Tricks benutzt, um unerkannt zu bleiben (Stealth-Techniken). Im MBR, in infizierten EXE-Dateien sowie im Arbeitsspeicher ist der Virus jedoch teilweise unverschlüsselt. Der Virus ist ein vollständiger Tarnkappenvirus, er versteckt erfolgreich den infizierten MBR. Beim Laden von infizierten Programmen werden diese zuerst komplett gereinigt. Wird der Virens Scanner TBSCAN gestartet, wird der Zugriff auf die Datei mit den Meldungstexten (TBSCAN.LNG) abgeblockt, weshalb TBSCAN seinen Dienst verweigert. Der Virus belegt u. a. die Interrupts 8, 9, 13h, 17h und 21h.

Als Schadensfunktion ist die Darstellung einer Meldung in Russisch und in Englisch implementiert. Zusätzlich spielt er Töne und formatiert die Festplatte. Folgende Meldung wird z. B. von der CD.6656 Variante ausgegeben:

CIVIL DEFENSE VIRUS VER 1.1

Formating disc c: complete.  
Format another ? (y/n)

Hard disk 1 formatted. All your data lost.

How are you feel now ?

Press any key

Folgende Meldung wird von der CD.6672 Variante ausgegeben:

```
|-----  
|<..> Civil Defence Virus ( CDV ver 3.3 ) (c) 1992 <..>  
|<rusischer Text>  
|-----  
|
```

Anmerkung: Der Großteil der Bildschirmmeldungen sind in russischer Schrift, der Virus schiebt dabei den Bildschirm von rechts nach links. Diese Variante lässt die Caps-Lock Taste regelmäßig aufleuchten und spielt in ca. 4 Minuten Abstand unterschiedliche Melodien.

Diese Meldungstexte sind selbst im Arbeitsspeicher verschlüsselt und können nicht im Viruscode gefunden werden!

Der Virus kann aus der Partitionstabelle entfernt werden, nachdem von einer virenfreien Systemdiskette gebootet wurde. Wenn nicht mit BootVir die Partitionstabelle und der MBR gesichert wurde, können Sie mit meinem Programm MBR-KILL (evtl. anfordern) ganz einfach den Virus entfernen. Zur Zeit existiert für diesen Virus noch kein Virenkiller für infizierte EXE-Programme!

Bekannte Varianten:

- Civil\_Defense.6656
- Civil\_Defense.6672.A
- Civil\_Defense.6672.B
- Civil\_Defense.6672.C
- Civil\_Defense.6672.D
- Civil\_Defense.6672.E
- Civil\_Defense.6672.F

Beschreibung (C) 1995 by ROSE Softwareentwicklung, Ralph Roth

## 4.5 Clonewar

Aka: Trekwar, ACME, Annihilator.Spawn  
Virusname: Clonewar.923  
Bekannt seit: Oktober 1992

Ursprung:	USA, Varianten aus Deutschland und Rußland
Virustyp:	Companion (Erzeugt Com-Files zu Exe-Files), Non-resident
Größe:	923 Bytes (Viruscode), je nach Variante unterschiedlich
Infiziert:	Erstellt zu einer EXE-Datei gleichnamige COM-Datei (Companion)
Symptome:	Es existieren zu EXE-Programmen gleichnamige COM-Programme. Programme funktionieren nicht mehr, da ggf. schon vorhandene COM-Dateien überschrieben werden. Je nach Variante wird Musik gespielt oder ein Teil der Festplatte zerstört.
Reinigung:	Löschen aller infizierten COM-Programme

Clonewar.923.A fragt am Anfang des Virus die aktuelle Systemzeit ab. Ist es 16:00 Uhr oder später, springt der Virus in eine endlose Soundschleife, welche Geräusche über den PC Speaker ausgibt.

Falls es jedoch früher ist, sucht der Virus mittels Findfirst (AH=4Eh, Handle) nach EXE-Dateien im aktuellen Verzeichnis. Wird er fündig erstellt er mittels den DOS-Funktionen (AH=3D, Open; AH=3C, Truncate) eine COM-Datei mit gleichem Namen wie die gefundene EXE-Datei und löscht ggf. eine schon vorhandene COM-Datei des selben Namens. Dann schreibt er seinen Viruscode (AH=40h, CX=039Bh) in diese Datei und fügt den EXE-Dateinamen in sie ein, um die EXE-Datei später auszuführen. Nun schließt er die COM-Datei (AH=3Eh) und ändert die File-Attributes auf Hidden und Read-Only. (AX=4301h) Nun führt er das zu ihm gleichnamige EXE-File aus (Int 2E). Danach beendet er sich selbst (AX=4C00h).

Bekannte Varianten:

Clonewar.194, Clonewar.200, Clonewar.207, Clonewar.220, Clonewar.228, Clonewar.229, Clonewar.235, Clonewar.242, Clonewar.246, Clonewar.247, Clonewar.252.A, Clonewar.252.B, Clonewar.255, Clonewar.258, Clonewar.260, Clonewar.261, Clonewar.267, Clonewar.546, Clonewar.547, Clonewar.551, Clonewar.923.A, Clonewar.923.B, Clonewar.923.C, Clonewar.923.D, Clonewar.923.E, Clonewar.923.F, Clonewar.923.G, Clonewar.923.H

Analyse 22.09.96 (c) Thorsten Pipe/PIPE AV-Software, Parts by ROSE SWE

## 4.6 Darth Vader

Darth\_Vader ist ein einzigartiger bulgarischer DOS-Virus, der als Darth Vader bekannt ist. Er wurde Anfang 1991 von Waleri Todorov in Sofia, Bulgarien, geschrieben und zeichnet sich durch seine unkonventionellen Techniken aus, die eine Herausforderung für generische Antivirenprogramme darstellen.

Der Virus ist einzigartig in seiner Art, sich sowohl im Speicher als auch auf der Festplatte zu verstecken. Anders als einige Viren, die Dateien infizieren und im Speicher verbleiben, verwendet Darth Vader eine einzigartige Strategie. Er sucht nach Bereichen in DOS oder einer Datei mit genügend aufeinanderfolgenden Nullen, um sich darin zu verstecken. Indem er nur .COM-Dateien mit mehr als 255 aufeinanderfolgenden Nullen infiziert, geht er davon aus, dass diese Nullen uninitialisierten Variablenplatz darstellen und die Funktionalität des Programms nicht beeinträchtigen.

Bemerkenswert ist, dass Darth Vader in Tasmc geschrieben ist, einem Assembler, der in Bulgarien weit verbreitet für die Virenerstellung verwendet wurde, da er nur minimale Speicheranforderungen hat. Der Virus ist nicht destruktiv und kann Probleme in bestimmten Versionen von DOS verursachen, die infizierte Dateien auf eine eigenartige Weise beeinflussen.

Die Fähigkeit des Virus, sich im Speicher zu verstecken, besteht darin, ein Segment in DOS zu finden und einen Bereich von 255 aufeinanderfolgenden Nullen zu identifizieren, um sich selbst dorthin zu kopieren. Dies ermöglicht es ihm, in Speicherlistings unentdeckt zu bleiben. Für die Dateinfektion verwendet er eine "langsame Infektions"-Technik, die Änderungen an Diskettendateien vermeidet und sich auf DOS verlässt, um eine .COM-Datei zu schreiben und den Virus zum Speicherpuffer hinzuzufügen.

Die Analyse hebt die Funktionalität des Virus hervor, wie z.B. seine Verwendung von NOP-Anweisungen, seine Abhängigkeit von spezifischen Assembler-Funktionen und seine Suche nach geeigneten Bereichen im Speicher. Darth Vader modifiziert den Interrupt 21h, um seine Infektionsroutine zu installieren, indem er die DOS-Funktion 40h (Datei schreiben) auf seinen Code umleitet. Diese nicht standardisierte Methode ermöglicht es dem Virus, immer dann zu laufen, wenn eine Datei kopiert wird, ohne dass er im Speicher erkannt wird.

Diese Analyse hebt die Funktionalität des Virus hervor, wie zum Beispiel seinen Gebrauch von NOP-Anweisungen, seine Abhängigkeit von bestimmten Assembler-Funktionen und seine Suche nach geeigneten Bereichen im Speicher. Darth Vader modifiziert den Interrupt 21h, um seine Infektionsroutine zu installieren, und leitet die DOS-Funktion 40h (Datei schreiben) auf seinen Code um. Diese nicht-standardisierte Methode ermöglicht es dem Virus, immer dann zu laufen, wenn eine Datei kopiert wird, und dabei resident zu bleiben, ohne entdeckt zu werden.

Diese Analyse schließt mit der Hervorhebung der geringen Größe des Virus (255 Bytes) und seiner innovativen Technik ab, die als Warnung

dient, sich nicht allein auf generische Antivirenprodukte zu verlassen. Darth Vader ist mit herkömmlichen Methoden schwer zu erkennen, was die Notwendigkeit verschiedener und fortschrittlicher Ansätze in der sich ständig weiterentwickelnden Computer-Virus-Landschaft zeigt.

Diese Analyse liefert wertvolle Einblicke in die Feinheiten von Darth Vaders Design und beleuchtet die Raffinesse bestimmter Viren und die Grenzen traditioneller Antiviren-Lösungen.

Der Darth Vader-Virus hat eine Reihe von Varianten, die sich durch einzigartige Aliase und mögliche Modifikationen auszeichnen. Die ursprüngliche Variante, die einfach als "Darth" bekannt ist, hat mehrere Namen wie Darth Vader, Darth Vader, Intended.Darth, Univ.PS, Darth\_vader.441 und Darth Vader 3. Nachfolgende Varianten, die durch Erweiterungen wie .1, .2, .3 usw. gekennzeichnet sind, führen den Alias Darth Vader mit zusätzlichen numerischen oder alphabetischen Identifikatoren fort. Bemerkenswert ist, dass einige Varianten wie DarthVader mit anderen Viren wie Assassin.952 und Lobotomy.966 in Verbindung gebracht werden.

Eine Variante kann den Wirt mit folgenden Text überschreiben und dadurch zerstören:

```
The Evil Impire wasn't destroyed,I'm the ghost of DARTH VADER !
```

## 4.7 Devide Overflow

- Größe (Dateischreibzugriff) : 66 Bytes
- Virus infiziert .EXE Programme (?)
- Virus infiziert .COM Programme
- Virus manipuliert den Dateianfang
- Virus hängt sich an das Ende des Programms
- Virus benutzt Datei-Stealthfunktionen (Länge)
- Virus behält Dateidatum- und Uhrzeit beim Infizieren bei
- Virus umgeht READ-ONLY, HIDDEN oder SYSTEM Dateiattribute
- Virus unterdrückt Schreibschutz-Fehlermeldungen bei Disketten
- Virus ist speicherresident
- Virus durchsucht/verändert die MCB-Kette
- Virus markiert MCB als SYSTEM-Bereich
- Virus benutzt INT 22h,24h,21h
- Virus verschiebt seinen Code im Speicher (5663 Bytes)
- Virus löscht Dateien !
- Virus gibt Texte aus oder verändert Grafikspeicher
- Virus überprüft die Systemuhrzeit
- Virus überprüft das Systemdatum (24.5.????)

## 4.8 Eddie/Dark Avenger

Eddie ist ein Virus aus Bulgarien, der von Dark Avenger erstellt wurde. Es war Dark Avengers erster Virus und einer der frühen bulgarischen Viren, die eine Epidemie auslösten. Dark Avenger gab dem Virus selbst den Namen „Eddie“. Er entlehnte den Namen vom Maskottchen "Eddie" der Band "Iron Maiden". Antivirenprodukte benennen ihn in der Regel nach dem Ersteller.

Verhalten: Nach der Ausführung wird Eddie im Arbeitsspeicher resident. Der Virus infiziert .com- und .exe-Dateien nicht nur bei ihrer Ausführung, sondern auch beim Lesen. Dies kann beim Kopieren, Verschieben oder Scannen der Dateien nach ihrem Inhalt geschehen. Es ist auch möglich, dass, wenn der Scanner eines Antivirenprogramms infiziert wird, es jede Datei infiziert, die auf Viren gescannt wird. Der Viruscode wird an die Datei angehängt. Nach jeder 16. Infektion überschreibt der Virus einen zufälligen Sektor.

Varianten: Irgendwann wurde der Quellcode des Eddie-Virus im Internet veröffentlicht, was zu mehreren Varianten führte. Nur wenige davon wurden von Dark Avenger selbst erstellt.

Varianten von Dark Avenger:

- Eddie.V2000: Diese 2000-Byte-Variante enthält den Text "Copy me - I want to travel" und "(c) 1989 by Vesselin Bontchev". Eine Unterart enthält den Tippfehler "Zopy" statt "Copy". Eine andere enthält den Text "Only the Good die young...".
- Eddie.V2100: Diese 2100-Byte-Variante enthält den Text "Eddie lives", "(c) 1990 by Vesselin Bontchev" und "Eddie". Wenn sie eine Kopie des Anthrax-Virus in den letzten Sektoren der Festplatte findet, platziert er diese in der Partitionstabelle und belebt den Virus praktisch wieder.
- Unterarten beider Varianten enthalten leichte Variationen des im Virus enthaltenen Texts. Einige enthalten den Namen "Diana P.", entweder in lateinischen Buchstaben oder kyrillisch. Einige von ihnen könnten nicht von Dark Avenger erstellt worden sein.

Varianten, die von anderen erstellt wurden oder deren Ursprung unklar ist:

- Eddie.651
- Eddie.1028
- Eddie.1530
- Eddie.1797
- Eddie.1799
- Eddie.1800.B



- Eddie.2000.C
- Eddie.2000.D
- Eddie.Alexander
- Eddie.Apa
- Eddie.Father
- Eddie.Jasper
- Eddie.Jericho (zwei Varianten)
- Eddie.Korea
- Eddie.Major
- Eddie.Oliver
- Eddie.Psko
- Eddie.Satan
- Eddie.Shyster
- Eddie.Sign
- Eddie.Uriel
- Eddie.VAN

Auswirkungen: Eddie verbreitete sich weit über Bulgarien hinaus und machte Dark Avenger in einigen Kreisen berühmt. Es war bekannt, dass es lange Zeit das am weitesten verbreitete Virus in Bulgarien war und auch in Westdeutschland, den USA und der UdSSR gefunden wurde. 1992 wurde es versehentlich von Sony auf eine Laser Library Distribution Disk installiert.

## 4.9 Eicar Testdatei

Die **EICAR-Testdatei** (auch „**Eicar test file**“ genannt) ist ein am European Institute for Computer Antivirus Research entwickeltes Testmuster, mit dessen Hilfe die Funktionen von Antivirenprogrammen getestet werden können. Dabei handelt es sich um eine reine Textdatei mit 68 ASCII-Zeichen und einer daraus resultierenden Dateigröße von 68 Byte (bzw. 70 Byte), welche somit in jeden beliebigen Texteditor eingegeben werden kann. Die Datei ist gutartig und richtet keinerlei Schaden an, sollte aber dennoch von allen Virensclannern als Virus erkannt und angezeigt werden. Damit lässt sich beispielsweise auch testen, ob ein Virensclanner ein Archiv korrekt lesen kann.

```
c:\>eicar
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
c:\>
```

Meldung der Eicar-Testdatei nach der Ausführung

Die *Eicar-Testdatei* wurde so entwickelt, dass es unter [MS-DOS](#) eine ausführbare [.COM](#)-Datei bildet. Wenn dieses Programm ausgeführt wird, gibt es die Meldung *EICAR-STANDARD-ANTIVIRUS-TEST-FILE!* auf dem Bildschirm aus und beendet sich daraufhin. Ob diese Datei 70 oder 68



Byte groß ist, hängt davon ab, ob der speichernde Texteditor einen Zeilenvorschub am Ende der Datei erzwingt oder nicht.

So sieht die Datei aus:

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

## 4.10 Enmity.808

Enmity.808 ist ein Computervirus, der erstmals am 26. Oktober 1998 auftrat. Mit einer Größe von 808 Bytes infiziert der Virus .COM-Programme. Er hängt sich an das Ende des infizierten Programms an und ist verschlüsselt, um seine Entdeckung zu erschweren. Eine besondere Eigenschaft des Virus besteht darin, dass er READ-ONLY, HIDDEN oder SYSTEM Dateiattribute umgehen kann, um sich in Dateien einzunisten.

Der Enmity.808-Virus ist äußerst bösartig und kann Dateien löschen. Er greift gezielt Antivirenprogramme an und versucht, ihre Funktionalität zu beeinträchtigen. Zudem überprüft der Virus die Systemuhrzeit, um seine Aktivitäten zu synchronisieren oder bestimmte Aktionen auszuführen.

Der Virus enthält die folgenden Texte innerhalb seines Codes:

```
"WINDOWS\COMMAND. . . . ANTI-VIR.DAT.CHKLIST.MS.CHKLIST.CPS.IVB.NTZ.Ú. "  
"COMMAND. . . . ANTI-VIR.DAT.CHKLIST.MS.CHKLIST.CPS.IVB.NTZ.Ú. .ÉVÚ. .66"
```

Diese Texte dienen vermutlich dazu, dass der Virus sich selbst oder andere Informationen innerhalb des Systems markiert.

Um den Enmity.808-Virus zu entfernen, wird empfohlen, entweder ein entsprechendes Entfernungstool wie RVK zu verwenden oder die befallenen Dateien zu löschen. Es ist wichtig, bei der Entfernung des Virus vorsichtig zu sein und sicherzustellen, dass keine wichtigen Systemdateien versehentlich gelöscht werden.

## 4.11 Fish-Virus

Alias: Fish #6, 3584-Stealth

Der Fish-Virus, auch bekannt als Fish #6 oder 3584-Stealth, ist ein schädlicher Computervirus, der verschiedene Dateitypen wie COM-, EXE-, Overlay- und Daten-Dateien sowie COMMAND.COM befällt. Es wird vermutet, dass er eine Variante des "100-Jahre"-Virus ist. Der Virus verfügt über einen äußerst intelligenten Verschlüsselungsalgorithmus, sowohl im Speicher als auch auf der Festplatte. Er wird zu den sogenannten Stealth-Viren gezählt, da er sich geschickt vor Entdeckung und Entfernung schützt.

Beim Laden des Virus in den Speicher erscheint folgender Text:

"Fish virus #6... ..2/90"

Dieser dient als Identifikation des Virus und ermöglicht es, ihn von anderen Schadprogrammen zu unterscheiden.

Im Fish-Virus sind die Namen mehrerer Fischarten enthalten, darunter SHARK, MACKAREL, COD, CARP und andere. Diese Bezeichnungen werden vermutlich verwendet, um dem Virus eine gewisse thematische Identität zu geben

## 4.12 Frodo

Alias: Stealth, 4096

Wird ein infiziertes Programm ausgeführt, wird der Virus im Hauptspeicher resident und infiziert Dateien, die zu einem späteren Zeitpunkt ausgeführt werden, sowie ausführbare Dateien, die zu einem späteren Zeitpunkt geöffnet und geschlossen werden. Infizierte Dateien wachsen hierbei um ca. 4096 Bytes an. Solange der Virus aktiv ist, ist dies durch seine Tarnkappeneigenschaften jedoch nicht ersichtlich! Erfolgt die Programmausführung zwischen dem 22. September und dem 31. Dezember eines beliebigen Jahres, führt der Virus normalerweise zu einer Blockierung des Systems (aufgrund von Programmfehlern im Code, die offensichtlich den MBR durch ein Programm überschreiben, das die Nachricht "Frodo Lives" beim Booten des Systems anzeigt).



## 4.13 Grief.3584

Aka Lucky.3584, Nostarda.3584 oder Nostradamus  
Ursprung: Kiev, Russland

Genauer Namen steht noch nicht fest. Gefunden wird dieser Virus von VSP z.Z. als Grief von anderen Antivirenprogrammen als Nostradamus.

Dieser Virus wurde im Dezember 1996 in Deutschland entdeckt und stellt einen technisch brillanten Virus dar. Es handelt sich hierbei um einen vollständigen Tarnkappenvirus, der zudem polymorph verschlüsselt ist. Erkannt wird dieser Virus im Dez. 96 nur von VirScan Plus sowie durch AVP, der in ein paar wenigen Dateien einen Nostardamus.3584 findet (dieser Virus wurde in Frühjahr dann von AVP korrekt gefunden).

Infiziert werden COM, OV? und EXE Dateien. Der Längenzuwachs beträgt immer 3584 (0x0E00) Bytes. Der Virus versucht sich im Speicher per MCB zu installieren, ist jedoch UMB Speicher frei, so wird dieser belegt.

Bemerkenswert ist zudem, dass die polymorphe Verschlüsselung Anti-Emulation Code enthält, der einige Virens Scanner irritiert. Nach der polymorphen Verschlüsselung können noch bis zu 3 weitere jedoch konstante Verschlüsselungsebenen nachfolgen. Eine Verschlüsselungsebene hiervon benützt einen Stacktrick, der recht wirksam gegen jeden Realmode Debugger ist. Aus diesen Grund kann der Virus nicht mit DECOM/RVK gereinigt werden. Deshalb ist es auch schwierig einen Virenkiller für diesen Virus zu schreiben, weil ja bis zu 4 Verschlüsselungsebenen dekodiert werden müssen.

Der Virus benützt ein Teil des Videospeichers um seine polymorphe Verschlüsselungen dort zu erzeugen. Wird dieser Teil etwa von EMM386/QEMM als Speicher verwaltet, stürzt der Virus natürlich ab. Das Erzeugen der linearen Verschlüsselung erfolgt auf Zufallsbasis. Hierbei wird der Virus im Puffer jedes Mal neu reloziert. Als Mutation-Engine wird die EMME-3 benutzt, die recht guten "Trashcode" erzeugt. Die damit erzeugten Decryptoren haben jedoch nicht die Qualität einer TPE-Engine. Benutzt werden alle Register, bis auf SP. Wie üblich wird je ein Register für Zeiger, Zähler und Schlüssel verwendet. Der Schlüssel wird hierbei modifiziert. Deshalb kann der Virus nicht mit X-Raying Verfahren gefunden werden!

COM-Dateien, die normalerweise einen Sprung zum Virus aufweisen haben diesen Sprung ebenfalls polymorph "versteckt", was wiederum einige Virens Scanner irritiert. Auch VirScan Plus musste an diese Gegebenheit angepasst werden, findet diesen Virus jedoch ab der Version 11.38c als Grief.

Der Virus hat eine Schadensfunktion: Das Überschreiben der Festplatte. Diese Schadensfunktion tritt in Kraft, wenn folgendes Datum vorliegt:

$(\text{Wochentag}+1)*2 == \text{Tag}$

So habe ich den Virus am Samstag den 14. Dez. 96 gestartet, somit wurde die Schadensfunktion gleich aktiviert, weil der Wochentag Sa=6 und Tag=14 war.

Tarnkappeneigenschaften: Der Virus ist 100% Stealth, selbst VirScan's Live Bait Test wird umgangen! Die Tarnkappenfunktion wird jedoch deaktiviert, wenn ChkDsk, ein Packprogramm (ARJ, ZIP, LHA etc.), Windows, einige Antivirenprogramme oder Ad-Inf gestartet wird. Somit wird einer Verbreitung über Archive Vorschub geleistet bzw. o.g. Software umgangen.

Weiterhin enthält der Virus Anti-Debugger Tricks, kann somit auch nicht mit TBClean gereinigt werden. Ad-Inf Checksummen-Tabellen werden beim ersten Start des Virus gelöscht. Der Virus ermittelt den Int 21h durch einen speziellen Trick, er kann damit auf das so genannte Tracen verzichten und umgeht dadurch etliche Wächterprogramme!

Virusmerkmale:

- Virus infiziert .COM, .OV? und .EXE Programme
- Virus infiziert Programme beim Öffnen ("Fast Infector")
- Virus infiziert Programme beim Ausführen
- Virus fängt das Erstellen von Programmen ab
- Virus infiziert beim Umbenennen von Dateien
- Virus manipuliert den Dateianfang
- Virus hängt sich an das Ende des Programms
- Virus ist polymorph verschlüsselt
- Virus benutzt Datei-Stealthfunktionen (Länge)
- Virus benutzt Datei-Stealthfunktionen (Inhalt)
- Virus benutzt Dateiuhrzeit als Markierung (Sekunde=60+)
- Virus prüft auf .EXE-Programmheader ("MZ")
- Virus prüft auf .EXE-Programmheader ("ZM")
- Virus behält Dateidatum- und Uhrzeit beim Infizieren bei
- Virus umgeht READ-ONLY, HIDDEN oder SYSTEM Dateiattribute
- Virus unterdrückt Schreibschutz-Fehlermeldungen bei Disketten
- Virus ist speicherresident
- Virus durchsucht/verändert die MCB-Kette (3184 Bytes)
- Virus benutzt INT 21h, 24h, 13h
- Virus ermittelt BIOS Disk-Interruptvektor für die Schadensfunktion.
- Virus verschiebt seinen Code im Speicher (3036 Bytes)
- Virus überprüft das Systemdatum
- Virus überschreibt Sektoren der Festplatte oder Diskette (Schadensfunktion)

Der Virus enthält folgende Texte:

```
*****
$-= LUCKY B.R.D 1996 PRESENTS A NEW MONSTER -=
$*****
$DON'T WORRY BE HAPPY. TJA WAS SOLL ICH GROß AN
$DIE GLOCKE HÄNGEN. NUR VIELLEICHT Dass EURE
$ADINF-TABLE JETZT ZERSTÖRT IST..TUT MIR JA SO
$LEID..ABER DAS MUSSTE JETZT MAL SEIN..
$SO UND NUN NOCH VIELE GRÜßE AN MEINEN BESTEN FREUND
$[ UWE POLIAK ] .....CU.....
$
COMEXEOVL0VRPROSCAEXTWEBF-PTBAICEARJRARLHAZIPTARWINVLMCHK
-=LUCKY'B.R.D 1996=-
```

Beschreibung (C) 19.12.1996 by ROSE Softwareentwicklung, Ralph Roth

## 4.14 Hexametricx



Alias Hello, Eumel, Annihilator

Dieser Virus wurde am 06.09.93 von einer mir bekannten Person in Deutschland geschrieben. Dieser Virus wäre nicht weiter bemerkenswert, wenn nicht der Quellcode an verschiedene Personen weitergegeben worden wäre. Aus diesem Quellcode sind bis heute mehr als 50 verschiedene Viren hervorgegangen, die eine Länge von 150 bis ca. 1200 Bytes besitzen. Fast allen Varianten ist gemeinsam, dass sie COM-Dateien nur im C: Laufwerk infizieren und dass sie verschlüsselt sind.

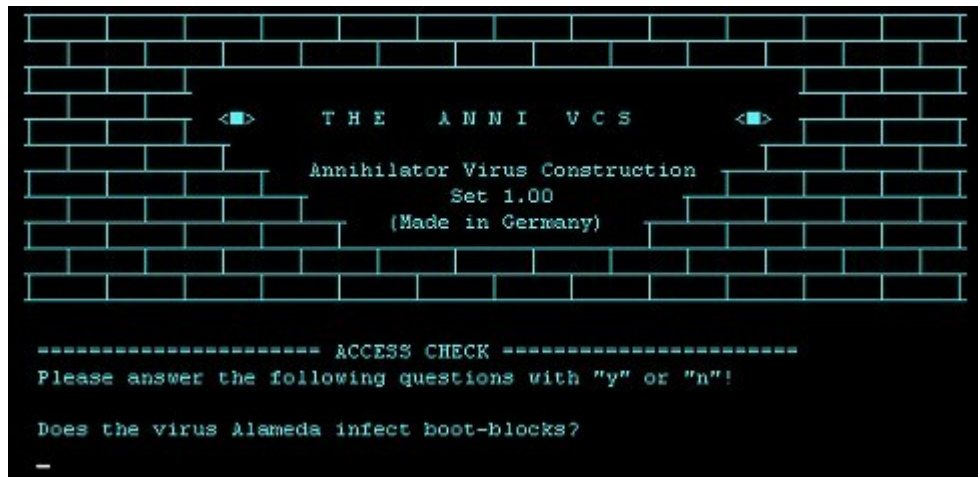
Dieser Virus ist ein nicht speicherresidenter, verschlüsselter COM-Infektor, der auch die COMMAND.COM befällt. Beim ersten Starten eines mit dem Hexametricx Virus infizierten Programms, versucht der Virus, das erste COM-File im aktuellen Verzeichnis des Laufwerk C: zu infizieren. Nachdem die erste Infektion erfolgte, sucht der Virus bei jedem Programmstart eines infizierten Programms nach weiteren COM Files. Dabei werden nur COM-Dateien infiziert, deren ursprüngliche Länge ungefähr größer als 500 Bytes und kleiner als 64100 Bytes sind und deren Sekundeneintrag ungleich 12 Sekunden ist.

Falls das Tagesdatum gleich dem Monat ist (1.1, 2.2, usw.), besteht die Chance (1:8), dass der Virus eine Meldung ausgibt. Alle Hexametricx Varianten können mit dem Programm RVK gekillt werden!

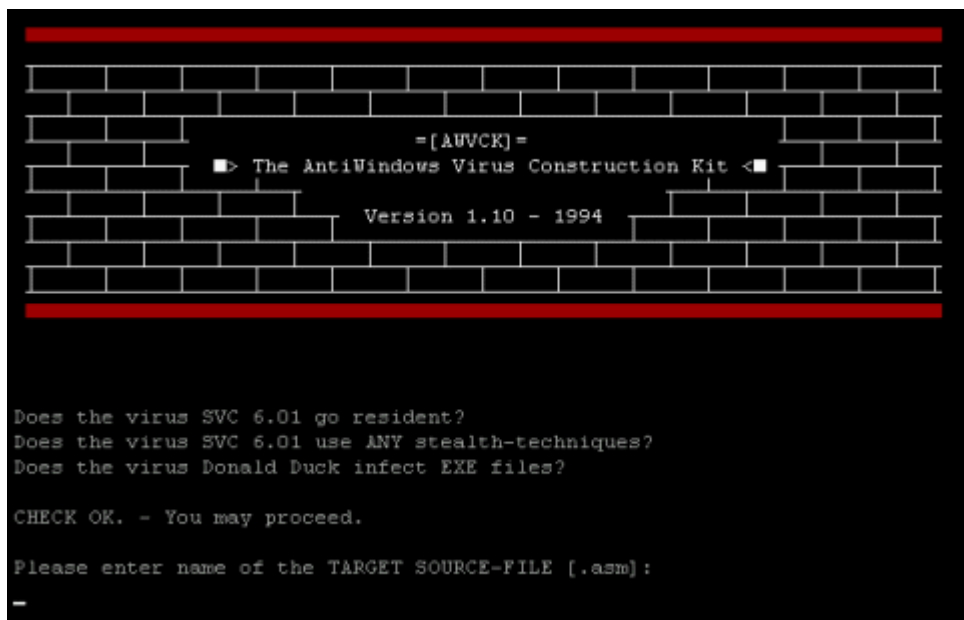
Schadensfunktion: Bildschirmmeldung, siehe oben. Eine Unterscheidung

von COM und EXE Dateien wird nicht vorgenommen, was zu defekten EXE- Programmen führt, die versehentlich in COM umbenannt wurden!

Varianten wurden mit dem Virus Construction Kit AVCS erstellt:



Und dem Kit AUVCK erstellt:



## 4.15 Hallöchen

Alias: Halloecken, Hello

Art: Residenter COM und EXE Infektor, 2011 Bytes

Hallöchen installiert sich durch direkte Manipulation der MCB Kette im Rechnersystem resident, ohne das Betriebssystem mit seinem INT 21h in

Anspruch zu nehmen. Mit den MCB (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. Der Virus enthält folgenden Text

Hallöchen, here I'm

Acrivate Level I

## 4.16 Imperial Probe

Virusname: Imperial Probe V1.07S

Ursprung: Wahrscheinlich Sommer 1995 in Österreich

- Größe (Dateischreibzugriff) : 2141 Bytes
- Größe (Programmstart bis Dateiende) : 2095 Bytes
- infiziert Programme beim Ausführen
- manipuliert den Dateianfang
- hängt sich an das Ende des Programmes
- fügt ein JMP NEAR am Programmstart ein
- prüft auf .EXE-Programmheader ("MZ")
- infiziert COM und EXE Dateien
- aktualisiert Dateidatum- und Uhrzeit beim Infizieren
- umgeht READ-ONLY, HIDDEN oder SYSTEM Dateiattribute
- ist speicherresident
- durchsucht/verändert die MCB-Kette (2752 Bytes)
- markiert MCB als SYSTEM-Bereich
- benutzt INT 21h
- verschiebt seinen Code im Speicher (2141 Bytes)
- überprüft die Systemuhrzeit
- überprüft das Systemdatum

## 4.17 Jerusalem Familie

(Alias: Friday the 13.th, 1813, 1803, Israeli, SUMSDOS, University of Hebrew, Timebomb, PLO)

Dieser Virus wurde in Israel entwickelt und trat erstmals an der University of Hebrew auf. Der Jerusalem-Virus ist ein bekannter Computervirus, der erstmals im Jahr 1987 entdeckt wurde. Es handelt sich um einen DOS-Virus, der auf IBM-kompatiblen Computern verbreitet wurde. Der Virus wurde nach der Stadt Jerusalem benannt, da er von dort aus verbreitet wurde. Er gehört zu den damals weltweit am weitesten verbreiteten Viren unter DOS überhaupt. Es existieren schätzungsweise 200 verschiedene



Varianten und Abkömmlinge des Virus. Er befällt EXE- und COM-Dateien, wobei COM-Dateien um 1813 Bytes länger werden, EXE-Dateien werden im Allgemeinen um 1808 Bytes länger. Nach Aufruf einer infizierten Datei installiert sich der Virus speicherresident über den Interrupt 21h - TBSR.

Schadensfunktionen: Der Jerusalem-Virus zeigt nach 30 Minuten ein schwarzes Rechteck auf dem Bildschirm an (links oben). Danach wird beim Original Jerusalem die Rechengeschwindigkeit um ca. 30 Prozent gebremst, bei anderen Varianten ist der Prozentsatz zum Teil noch größer. An jedem Freitag, dem 13., wird beim Aufruf einer infizierten Datei diese sofort gelöscht. Die "Originalversionen" der Jerusalem-Viren besitzen den folgenden Text "sUMsDos", der zweimal im Viruscode auftritt. Bei Varianten ist dieser Text durch andere Zeichen ersetzt worden.

Der Jerusalem-Virus hatte aufgrund seiner weitreichenden Verbreitung und verschiedenen Varianten erheblichen Schaden angerichtet. Durch die Löschung von Dateien und die Verlangsamung der Rechengeschwindigkeit konnte er sowohl Datenverlust als auch Beeinträchtigungen der Systemleistung verursachen.

#### 4.17.1 Jerusalem A

Die erste Version (Jerusalem A) dieses Virus enthielt einen Fehler: Der Befall von EXE-Dateien wird vom Virus nicht erkannt. Dadurch können sie beliebig oft infiziert werden und wachsen beständig an. Diese Variante ist inzwischen sehr rar, jedoch ist die JERUSALEM-B Variante und deren Abkömmlinge der am meisten verbreiteste Virus.

#### 4.17.2 Jerusalem B

Ein paar Wochen später - nachdem die ersten Antivirenprogramme gegen den JERUSALEM-A geschrieben wurden - tauchte diese Varianten an der Universität in Jerusalem auf. Fast identisch zum JERUSALEM-A, nur leicht verbessert.

Im Unterschied zu JERUSALEM-A befällt diese Variante auch Overlay-Dateien. Es kann vorkommen, dass EXE-Dateien nach erfolgter Infektion nicht mehr funktionieren. Das beruht auf einem kleinen Fehler im Virus-Code, der manchmal zu einer inkorrekten Übertragung auf EXE-Dateien führt. Die Schadensfunktionen sind ähnlich wie bei JERUSALEM-A. Der Fehler der mehrfachen Infizierung von EXE Programmen besteht immer noch.

#### 4.17.3 Jerusalem C

Wie der JERUSALEM-B, jedoch wird die Rechenleistung nicht verzögert.



#### 4.17.4 Jerusalem D

Wie der JERUSALEM-C, zerstört jedoch an jedem Freitag den 13.ten nach dem Jahr 1990 die beiden FAT-Tabellen.

#### 4.17.5 Jerusalem DC

Wie der JERUSALEM-B, der sUMsDos Text wurde durch Nullen ersetzt. Schwarzes Fenster und Rechenleistung wird um ca. 30% vermindert.

#### 4.17.6 Jerusalem E

Jerusalem-D, wird jedoch nur im Jahr 1992 aktiv.

#### 4.17.7 Jerusalem Related

Dieser Virus ist aus JERUSALEM-B hervorgegangen. Er befällt COM- und EXE-Dateien gleichermaßen. Er hat ähnliche Schadensfunktionen wie JERUSALEM-B, mit dem Unterschied, dass kein schwarzes Rechteck gezeichnet wird, sondern eine allgemeine Bildschirmstörung erfolgt, was auf einen Fehler im Virus-Code zurückzuführen ist.

#### 4.17.8 Jeruslaem.A-204

Der sUMsDos-Text wurde durch den Text \*A-204\* ersetzt. Ein paar Maschinenbefehle wurden verändert, um eine Entdeckung zu erschweren. Ursprung: Niederlande.

#### 4.17.9 Anarkia

Wie JERUSALEM-B. Der sUMsDos-Text wurde durch den Text ANARKIA ersetzt. Größere Rechenzeitverzögerung als beim JERUSALEM-B, das Fenster wird nicht angezeigt. Der Virus aktiviert sich jetzt nicht mehr am Freitag den 13.ten, sondern am Dienstag den 13.ten. Ursprung: Spanien.

#### 4.17.10Anarkia-B

Wie der Anarkia-Virus, jedoch wird der Virus an jedem 12.ten Oktober aktiv.

#### 4.17.11Apokalypse, Phoneme

Wie der JERUSALEM-B, der sUMsDos-Text wurde durch \*\*C.J\*\* ersetzt. Ursprung: Italien. C.J stehen für Cracker Jack, einem Viren-Programmierer, dem wir über zehn verschiedene Viren zu verdanken haben. Phoneme ist ähnlich aufgebaut wie der Apokalypse-Virus.

#### 4.17.12Mendoza, Puerto

Wie der JERUSALEM-B, infiziert EXE-Dateien aber nur einmal. Wurden nach ihrem ersten Auftreten benannt.

#### 4.17.13Park ESS, Skism-1

Wie der JERUSALEM-B, der sUMsDos-Text wurde durch PARK ESS bzw. Skism-1 ersetzt.

#### 4.17.14Fu-Manchu

Es handelt sich bei dem Virus um eine Variante von JERUSALEM-B. Er befällt COM- und EXE-Dateien. Beim ersten Aufruf installiert er sich resident im Speicher. Die Schadensfunktionen sind ähnlich wie bei JERUSALEM-B, mit dem Unterschied, dass an jedem Freitag Löschvorgänge von Dateien erfolgen, ausgenommen an Freitagen, die auf einen 13.ten fallen. Der Virus bleibt nach einem Warmstart im Speicher aktiv, und kann daher nur durch einen Kaltstart aus dem Speicher entfernt werden.

Die Schadensfunktionen vom JERUSALEM-B Virus wurden entfernt und durch neue ersetzt. Befallene COM-Dateien werden um 2086 Bytes, EXE-Dateien um 2080 Bytes verlängert. Außerdem installiert sich der Virus speicherresident. Der Virus überwacht Tastatureingaben, löscht bekannte englische Schimpfworte, sobald sie über die Tastatur eingegeben werden und gibt zusätzliche Kommentare aus, sobald folgende Namen über die Tastatur eingegeben werden:

"THATCHER", "REAGAN", "BOTH", und "WALDHEIM".

#### 4.17.1521.st Century

Dieser Virus ist eine Variante von JERUSALEM-A. Er befällt EXE-, COM- und bestimmte OVL-Dateien. Die Manipulationsaufgabe wird am 1. Januar 2000 aktiviert, wobei folgende Meldung auf dem Bildschirm ausgegeben wird:

"WELCOME TO THE 21ST CENTURY!"

Dem Programmierer ist hier jedoch ein "Denk-Fehler" unterlaufen, weil das 21.ste Jahrhundert nicht am 01.01.2000 anfängt. Ferner versucht dieser Virus alle aufgefundenen Programme ausnahmslos zu zerstören, so dass sie nicht mehr restauriert werden können. Von diesem Virus existieren bereits mehrere Varianten.

#### 4.17.16Sunday

Dieser Virus ist vermutlich aus JERUSALEM-A hervorgegangen und hat seinen Ursprung im Staat Washington in den USA. Er befällt COM-, EXE-

und diverse OVERLAY- Dateien. Bei Aufruf installiert er sich speicherresident und verlängert befallene Dateien um ca. 1630 Bytes. Der Virus entfaltet seine Schadensfunktion ausschließlich an Sonntagen, ausgenommen 1989. Nach Aufruf einer infizierten Datei erscheint nach einiger Zeit auf dem Bildschirm folgende Meldung:

"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!"

Von dieser Varianten existieren ebenfalls mehrere Abwandlungen. Verschiedentlich wurde berichtet, dass der Virus die FAT zerstört.

#### 4.17.17PSQR

Dieser Virus hat seinen Ursprung in Spanien und wurde im März 1990 erstmals in Barcelona isoliert und ist mit JERUSALEM-B direkt verwandt. Nach Aufruf einer infizierten Datei installiert er sich sofort resident im Hauptspeicher. Er infiziert COM- und EXE-Dateien (ausgenommen die Datei COMMAND.COM). Auch Overlay-Dateien werden von ihm befallen. An jedem Freitag, den 13.ten, wird jede aufgerufene Datei sofort gelöscht. Ferner prüft der Virus an diesem Tag, ob eine Festplatte vorhanden ist. Falls eine Festplatte gefunden wird, wird die Partition Tabelle überschrieben und somit ist kein Zugriff mehr auf die Platte möglich. In diesem Fall sind alle Daten restlos verloren.

#### 4.17.18Frere Jaques

Der Virus stammt aus Kalifornien und wurde im Mai 1990 erstmals isoliert, er ist mit dem JERUSALEM-B Virus verwandt und befällt COM- und EXE-Dateien, die Datei COMMAND.COM wird jedoch nicht befallen. Beim ersten Aufruf installiert er sich speicherresident und verringert den noch freien Arbeitsspeicher um 2,064 Bytes. Befallene COM-Dateien wachsen um 1813 Bytes, EXE-Dateien zwischen 1808 und 1819 Bytes. An jedem Freitag wird vom Virus die Melodie

"FRERE JAQUES"

abgespielt. Ansonsten kann es bei residentem Virus zu Systemabstürzen kommen, wenn es dem Virus nicht gelingt, Dateien zu infizieren. Der Systemabsturz ist meist mit dem Verlust der Systemdateien verbunden.

#### 4.18LeHigh

Lehigh ist ein DOS-Virus, das ausschließlich COMMAND.COM, die Hauptausführungsdatei des Betriebssystems, angreift. Es verhält sich wie ein Bootsektor-Virus und infiziert die erste geladene Datei beim

Systemstart. Es ähnelt einem früheren Virus namens Rushhour, das eine bestimmte Treiberdatei für die Tastatur infizierte.

Das Virus funktioniert, indem es sich selbst an einen ungenutzten Teil der COMMAND.COM-Datei kopiert, ohne deren Größe zu verändern. Anschließend verbleibt es im Speicher und sucht nach anderen Laufwerken mit COMMAND.COM-Dateien, um sie zu infizieren. Das Virus verfügt über einen Zähler, der die Anzahl der durchgeführten Infektionen erfasst. Nach der vierten Infektion kann es den Bootsektor und die Dateizuordnungstabelle der Festplatte zerstören, was sie unbrauchbar macht.

Es gibt mehrere Varianten von Lehigh, die sich jedoch nur in der Anzahl der Infektionen unterscheiden, bevor sie ihre zerstörerische Funktion auslösen.

Das Virus wurde erstmals an der Lehigh University entdeckt und erhielt daher seinen Namen. Trotz einiger Medienaufmerksamkeit von Ken Van Wyk, der später die VIRUS-L Usenet-Gruppe gründete, verbreitete sich Lehigh nicht weit.

Eine Möglichkeit, das System vor einer Infektion durch das Virus zu schützen, besteht darin, die COMMAND.COM-Datei als schreibgeschützt zu markieren, damit das Virus sie nicht verändern kann.

## 4.19Quit

Alias 555, Quit 1992

Wird eine infizierte Datei ausgeführt, wird der Virus in den Hauptspeicher geladen und infiziert EXE- und COM-Dateien, die zu einem späteren Zeitpunkt ausgeführt werden. Die Dateien wachsen hierbei um ca. 555 Bytes an. Wurde eine infizierte Datei 1992 oder wird sie danach ausgeführt (heute), installiert sich der Virus selbst und kehrt sofort zu DOS zurück, ohne das ursprüngliche Opferprogramm auszuführen.

## 4.20Tai-Pan

Alias Whisper, Doom2

Der Tai-Pan Virus ist ein einfacher und primitiver Virus, der EXE-Dateien befällt, die kleiner als 64.833 Byte sind. Obwohl dieser Virus keine fortgeschrittenen Techniken unterstützt (z. B. Verschlüsselung), ist er weitverbreitet. Tai-Pan verbreitete sich im Herbst 1994 relativ schnell, weil ein mit Tai-Pan verseuchtes Programm verbreitet wurde.

Wenn ein vom Tai-Pan Virus befallenes Programm ausgeführt wird, führt Tai-Pan einen INT 21h Aufruf durch, um zu prüfen ob der Virus bereits im Speicher installiert ist. Wenn es der Fall ist, wird das befallene Programm wie gewohnt ausgeführt. Sollte der Virus noch nicht aktiv sein, so versucht er sich resident am Ende des konventionellen Speichers zu installieren. Wenn Tai-Pan keinen freien Speicherbereich findet, wo er sich installieren könnte, manipuliert er den aktuellen Speicherbereich, indem er ihn um 512 Byte verkleinert und belegt dann den so freigewordenen Speicher. Tai-Pan kopiert seinen Code in diesen neuen Speicherbereich und verändert so seine Kennung, dass dieser Speicherbereich als ein Bestandteil von DOS behandelt wird, obwohl er den Virus enthält. Bei Aufruf von MEM /D ist ein Speicherbereich mit dem manipulierten Namen "IO Systemdaten" von der Größe 512 Byte sichtbar. Von nun an infiziert der aktive Virus EXE Dateien bei deren Ausführung. Der Tai-Pan Virus kopiert sich an das Ende von Dateien und verlängert diese um 438 Byte. Die Datums- und Zeiteinträge werden nicht geändert, weil der Virus sie nach der Infektion restauriert. Wenn versucht wird ein sauberes EXE-Programm von einer schreibgeschützten Diskette zu starten, erscheint die bekannte DOS-Schreib-Fehlermeldung, weil der aktive Virus diese Datei zu infizieren versucht.

Tai-Pan enthält den folgenden Text in seinem Code:

[Whisper presenterar Tai-Pan]

Von Tai-Pan gibt es inzwischen mehrere Varianten, erwähnenswert hiervon ist noch die 666 Bytes lange Doom2-Variante. Sie unterscheidet sich noch durch einen einzigen Befehl und einen zusätzlichen Text.

#### Merkmale für Taipan.438

- Größe (Dateischreibzugriff): 438 Bytes
- Größe (Programmsegment): 926 Bytes
- Größe (Programmstart bis Dateiende): 438 Bytes
- Virus behält Dateidatum- und Uhrzeit beim Infizieren bei
- Virus benutzt INT 21h
- Virus benutzt undokumentierte Interruptfunktion (Selbsterkennung): 21h/AX:7BCE=AX:7BCE
- Virus durchsucht/verändert die MCB-Kette (496 Bytes)
- Virus hängt sich an das Ende des Programmes
- Virus infiziert .EXE Programme
- Virus infiziert Programme beim Ausführen
- Virus ist speicherresident
- Virus kann READ-ONLY, HIDDEN oder SYSTEM Attribute nicht umgehen
- Virus manipuliert den Dateianfang
- Virus markiert MCB als SYSTEM-Bereich
- Virus prüft auf .EXE-Programmheader ("MZ")
- Virus setzt den Programmstack im .EXE-Header auf FFFFh

- Virus verschiebt seinen Code im Speicher (438 Bytes)

## 4.21Teraz

Aka 2717  
 Ursprung: Polen  
 Erste Entdeckung:

1994?

Merkmale:

- Größe (Dateischreibzugriff) : 2717 Bytes
- Größe (Programmsegment bis Dateiende) : 2710 Bytes
- Größe (Programmstart bis Dateiende) : 2710 Bytes
- Virus behält Dateidatum- und Uhrzeit beim Infizieren bei
- Virus benutzt Datei-Stealthfunktionen (Uhrzeit/Datum)
- Virus ermittelt ursprünglichen Interruptvektor ("Tracer")
- Virus hängt sich an das Ende des Programmes
- Virus infiziert .COM Programme
- Virus infiziert .EXE Programme
- Virus infiziert Programme beim Ausführen
- Virus ist speicherresident
- Virus manipuliert den Dateianfang
- Virus prüft auf .EXE-Programmheader ("MZ")
- Virus setzt den Programmstack im .EXE-Header auf 0100h
- Virus spricht den Lautsprecher an (Musik, Geräusche)
- Virus umgeht READ-ONLY, HIDDEN oder SYSTEM Dateiattribute
- Virus verringert DOS-Speicherbergrenze

Weiterhin existiert eine 4004 Bytes lange Variante.

## 4.22Tiny.163

Alias Danish Tiny, 163

Der 163-COM-Virus oder Tiny-Virus wurde von Fridrik Skulason in Island im Juni 1990 isoliert. Dieser Virus ist ein nicht speicherresidenter COM-Infektor, der auch die COMMAND.COM befällt. Beim ersten Starten eines mit dem Tiny-Virus infizierten Programmes, versucht der Virus, das erste COM-File im aktuellen Verzeichnis zu infizieren. Auf bootfähigen Disketten wäre diese, Datei im Normalfall die COMMAND.COM. Nachdem die erste Infektion erfolgte, sucht der Virus bei jedem Programmstart eines infizierten Programmes nach weiteren COM Files. Dabei werden nur COM-Dateien infiziert, deren ursprüngliche Länge größer als etwa 1 KB ist.

Infizierte Dateien werden um 163 Bytes vergrößert. Der Datums-/Zeiteintrag dieser Dateien wird zur Infektionszeit geändert. Größere

Schäden entstehen zunächst nicht; der Virus kopiert lediglich sich selbst immer wieder. Es war lange Zeit der kleinste bekannte MS-DOS-Virus.

## 4.23 TPE: Coffeeshop und MtE: Coffeeshop

Alias: Giraffe, Variante: Bosnia

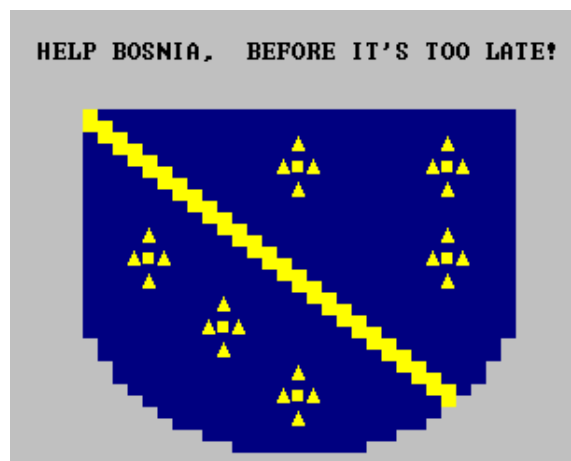
Der Coffeeshop-Virus der aus Holland stammt, infiziert COM- und EXE-Dateien und wird speicherresident. Vom Coffeeshop-Virus gibt es mindestens drei verschiedene Varianten. Die erste Variante benutzt die MtE zur Verschlüsselung, während die anderen Varianten einen Vorgänger der TPE 1.3 benutzen und deshalb polymorphe Viren sind (TPE 1.0). TPE ist die Kurzbezeichnung von "Trident Polymorphic Engine", die von einer Gruppe von Virenautoren (Trident) entwickelt wurde. Die TPE ist von ihrer Funktion her ähnlich der MtE, aber benutzt ausgefeiltere Techniken für eine variable Verschlüsselung und Entschlüsselung. Aus dem Coffeeshop ist (in verbesserter Version) die eigentliche TPE entstanden.

Der Virus wird ab MS-DOS Version 3.30 speicherresident. Der Virus ist bereits im Speicher resident, wenn INT 21h/AX=33DAh den Wert AH=0A5h liefert. Der Virus belegt im Speicher ca. 9000 Bytes im aktuellen MCB (memory control block), wenn es der letzte Block in der MCB-Kette ist. Der zusätzlich reservierte Speicher wird für Daten, Stack und Puffer benötigt. Die Länge des residenten Virus ist 3000 Byte. Die TPE belegt etwa 1400 Byte des Viruscodes (je nach Version). Zusätzlich wird ein Pufferbereich von ca. 4000 Bytes von der TPE für die Ver- und Entschlüsselung verwendet. Der Virus enthält einen Zufallszahlengenerator, der aktiviert wird, wenn der Virus resident wird. Der Zufallsgenerator ist der gleiche, die die MtE verwendet! Der Anfangswert wird aus der Systemzeit und dem Clock-Port bestimmt. Der INT-21h-Handler wird initialisiert und der Zufallsgenerator wird eingestellt. Während der Installation überprüft der Virus das Datum. Je nach Variante wird Donnerstags oder Freitags mit einer Wahrscheinlichkeit von 1/60 eine Anzeigeroutine aufgerufen, bevor das Wirtsprogramm ausgeführt wird. Die Anzeigeroutine kopiert 731 Bytes vom residenten Teil des Virus in einen Puffer, der vom Virus eingerichtet wurde. Anschließend packt der Virus die Routine aus, die ab 100h gespeichert wurde. Diese Routine, die verschlüsselt und komprimiert (mit DIET 1.00 gepackt) ist, ist 4064 Byte lang. Sie gibt eine Grafik auf den Bildschirm aus, die ein Hanfblatt (Coffeeshop) darstellt und den Text





enthält (siehe Scherzprogramm CANNABIS.COM aus den Freeware-Tools) oder ein Wappen (Bosnia) mit dem Text



Schließlich piept der PC und wartet auf die Eingabe einer beliebigen Taste erst dann wird das eigentliche Wirtsprogramm ausgeführt.

Ist der Virus installiert, wartet er, bis ein Programm ausgeführt oder geöffnet wird. Ist der Dateiname länger 127 Byte, wird die Datei ignoriert. Der Dateiname wird in Großbuchstaben umgewandelt. Es wird nur infiziert, wenn der Dateiname auf COM oder EXE endet. Außerdem erfolgt keine Infizierung wenn der Dateiname mit den Anfangsbuchstaben bekannter Antivirenprogramme beginnt. Während der Infektion wird Control-Break blockiert. Eine spezieller Critical-Error-Handler wird installiert und die Dateiattribute und Datum werden gesichert. Für die Selbsterkennung werden 2 Byte ab Offset 12h überprüft. Ergibt die Summe dieser Byte den Wert "@" nimmt der Virus an, dass diese Datei bereits infiziert wurde. Der Wert dieser Bytes wird zufallsgesteuert bestimmt. Findet der Virus die Kennung "MZ" oder "ZM" am Anfang der



Datei, nimmt der Virus an, dass es sich um eine EXE-Datei handelt. COM-Dateien werden nur infiziert wenn sie mindestens 256 Byte und höchstens 52 KB lang sind. COM-Dateien, in deren ersten Byte das Bit 7 = 0 ist, werden nicht infiziert (DEBUG und teilweise Virenfallen). Einige EXE-Dateien werden ebenfalls nicht infiziert. Es handelt sich um Windows- und OS/2-Dateien oder Programme, die Overlays oder einen ungültigen Kopf besitzen. Die Infizierungsroutine generiert die neue Kopie des Virus in dem Speicherbereich in dem auch das "legalize cannabis" Programm entpackt wird. Der Viruscode von Coffeshop wird dann an das Wirtsprogramm angehängt. Zwischen Wirtsprogramm und Viruscode fügt der Virus unsinnigen Code von variabler Länge und den Entschlüsselungscode ein. Der Entschlüsselungscode wird sowohl durch unterschiedliche Verschlüsselungen als auch durch Einschieben zusätzlicher Befehle, die keine Funktion besitzen, schwer identifizierbar. Der eigentliche Viruscode wird nicht verändert ist jedoch verschlüsselt.

## 4.24Trojector

Alias Athens

Der Trojector Virus wurde in Athen, Griechenland entdeckt. Zur Zeit existieren zwei Varianten von diesem Virus. Beide Varianten sind einfach verschlüsselte speicherresidente Dateiviren, die ca. 3776 Bytes Arbeitsspeicher belegen.

Trojector infiziert COM- und EXE-Programme beim Öffnen oder bei Programmstart (Fast-Infecter) und verlängert diese um:

- Variante II: 1463 Bytes. Entdeckung Mai 1992
- Variante III: 1561 Bytes. Entdeckung Januar 1994

Der Kommandointerpreter (COMMAND.COM) wird beim ersten Starten des Virus sofort von diesem infiziert! Beiden Varianten ist gemeinsam, dass sie leichte Tarnkappeneigenschaften besitzen (DIR-Stealth). Der Virus setzt zu diesem Zweck das Dateidatum infizierter Dateien auf den ungültigen Wert von 62 Sekunden.

Folgende Texte sind im verschlüsselten Virus enthalten:

TROJECTOR II,(c) Armagedon Utilities, Athens 1992

bzw.

TROJECTOR ]I[(c) Armagedon Utilities, Athens 1992, Greetings  
to Vesselin

Trojector vermehrt sich praktisch nicht auf Disketten und verursacht bei

der Infizierung von Dateien auf Diskette Systemabstürze.

## 4.25 Vacsina-Virus

Dieser Virus stammt aus Bulgarien, siehe auch Yankee Doodle. Entdeckt wurde er das erste Mal in Köln im August 1989 an der Universität. Zur Zeit existieren ca. 50 verschiedene Varianten, die unter dem Namen TPxxVIR ("xx" steht für die Version) bekannt sind. Die Bezeichnung VACSINA-xx ist ebenfalls geläufig. Er befällt COM-, EXE-, SYS- und BIN-Dateien, wobei EXE-Dateien zunächst in COM-Dateien umgewandelt werden. Beim ersten infizierten Programmaufruf installiert sich der Virus im Arbeitsspeicher. Anschließend werden alle geeignete (s. u.) Programme beim Starten infiziert.

Dabei bedient sich der Virus einer ausgeklügelten (aber inzwischen veralteten) Taktik: Die Kennung "MZ" einer EXE Datei wird zunächst in eine Sprunganweisung umgewandelt. Im Anschluß daran wird eine Relokationsroutine von wenigen Bytes eingebaut, so dass die infizierte Datei wie eine COM-Datei ausgeführt werden kann. Weil COM-Dateien jedoch nur 64 KB groß werden dürfen, befällt der Vacsina-Virus auch nur EXE-Dateien, die kleiner als 64 KB sind (65535 - Virusgröße).

Der Virus selbst hat eine Code-Länge von ca. 1200 Bytes, befallene Dateien wachsen um 1206 Bytes an und erzeugen bei Aufruf einen markanten Beep-Ton (Bei neueren Varianten ist dieses Beepen entfernt worden!). Die Infektion kann daran erkannt werden, dass Datum- und Zeiteintrag der befallenen Datei auf den aktuellen Wert (den Zeitpunkt des Befalls) gesetzt werden. Ferner steht am Ende einer Datei der Text "VACSINA". EXE-Dateien, welche den Relokator eingebaut haben, wachsen zusätzlich noch um 132 Bytes an. Befallene EXE-Dateien haben daher durchschnittlich einen Längenzuwachs von 1338-1353 Bytes. Direkte Erkennung: Die letzten 4 Byte eines infizierten Programmes enthalten:

F4 7A 05 00

Die Bytes F4 7A enthalten den Selbsterkennungscode, 05 00 stellt die Funktionsnummer dar (s. u.).

Es kann vorkommen, dass nach dem Eliminieren des VACSINA-Virus die befallenen Dateien zerstört sind. Dies geschieht aber nicht in jedem Falle. Der VACSINA Virus zerstört in der Regel selbst die letzten 32 Bytes der befallenen Datei. Das bedeutet, dass diese Datei in jedem Falle zerstört ist, sowohl nach dem Befall als auch vor dem Befall, weil der VACSINA Virus unsauber programmiert ist (Fehler im Viruscode). Aus diesem Grunde zerstört er nicht immer die letzten 32 Bytes, sondern nur manches Mal.

Folgende Varianten existieren:

- TP04VIR: geringfügige Unterschiede zu VACSINA.
- TP05VIR: wie TP04VIR, ein Byte Unterschied.
- TP06VIR: wie TP05VIR, zwei Bytes Unterschied.
- TP16VIR: wie TP06VIR, zwei Bytes Unterschied.
- TP23VIR: ähnlich wie TP16VIR.
- TP24VIR: wie TP23VIR.
- TP25VIR: ähnlich wie TP24VIR.
- TP33VIR: ähnlich wie TP25VIR.
- TP34VIR: ähnlich wie TP33VIR.
- TP38VIR: ähnlich wie TP34VIR.
- TP39VIR: ähnlich wie TP38VIR.
- TP41VIR: ähnlich wie TP39VIR.
- TP42VIR: ähnlich wie TP41VIR.
- TP44VIR: ähnlich wie TP42VIR.
- TP45VIR: ähnlich wie TP44VIR.
- TP46VIR: ähnlich wie TP45VIR.
- TP47VIR: eine neue Variante.
- TP48VIR: ähnlich wie TP47VIR.
- Penza: Länge von 700 Bytes, gibt die Meldung "Welcome to Penza" aus

Von machen Varianten existieren wiederum etliche Untervarianten.

Bis zur Variante TP16VIR enthalten alle Formen im Code den Textstring "VACSINA". Einige Varianten sind sehr ähnlich zum YANKEE DOODLE aufgebaut (s. u.).

VACSINA (und der Yankee Doodle) verfügen über eine Spezialität, die einzigartig zu sein scheint: Wird eine neuere Version des Virus aktiviert, so sucht sie nach infizierbaren Dateien. Stößt sie dabei auf Dateien, die bereits von einer älteren Version von VACSINA befallen sind, so wird die ältere Virus-Version durch die neue aktualisiert.

## 4.26 Vienna.Reboot

(Alias: UNESCO, 648, 62-Seconds, Wiener)

Dieser Virus stammt aus Wien und trat das erste Mal in einem Sommerlager der UNESCO für Kinder in Moskau im Jahre 1988 in Erscheinung. Vienna ist einer der ältesten Viren überhaupt. Er befällt ausschließlich COM-Dateien und verlängert diese um 648 Bytes. Die Datei COMMAND.COM wird von einigen Vienna-Varianten nicht befallen. Die Infektion wird im Sekundenbereich des Zeiteintrages der Datei vermerkt. Dieser wird auf 62 Sekunden gesetzt und bleibt für den Benutzer verborgen, da bei einem DIR-Befehl der Sekundenbereich nicht angezeigt wird. Nach jedem 8. Aufruf überschreibt der Virus die ersten 5 Bytes eines

nicht infizierten Programmes mit einem REBOOT-Code. In diesem Fall unterbleibt die Infektion. Wird ein derart geändertes Programm aufgerufen, erfolgt ein WARMSTART!

Aus dem VIENNA-Virus sind zahlreiche andere Viren hervorgegangen. Unter anderem basieren der CHAMÄLEON-Virus (=V-1260, erzeugt von MARK WASHBURN), Byte Warrior, Adolf, Ah, Violator und die VHP-Viren aus Bulgarien auf seinem Programm-Code. Die Rebootroutine ist nur in den wenigsten Vienna-Varianten enthalten (zu auffällig)!

#### 4.26.1 Vienna.A

Es erfolgt kein REBOOT, obwohl die effektive Länge des Virus weiterhin 648 Bytes beträgt.

#### 4.26.2 Vienna.B

Ist ähnlich wie VIENNA aufgebaut. Anstelle des REBOOTS wird das ausgeführte File gelöscht.

#### 4.26.3 Vienna.645

Die Routinen für REBOOT oder das Löschen von Dateien fehlen. Der Virus infiziert COMMAND.COM und hat seinen Ursprung in den USA.

#### 4.26.4 Vienna.Lisbon

Dieser Virus wird des öfteren auch DOS-62-Virus genannt und ist nahezu mit dem VIENNA-Virus identisch. Der Virus wurde im November 1989 erstmals von JEAN LUC in Portugal isoliert. LISBON befällt ausschließlich COM-Dateien, einschließlich der Datei COMMAND.COM. Der Virus verfügt über einen internen Zählmechanismus. Bei jedem achten Aufruf einer infizierten Datei erfolgt keine Infektion, sondern die ersten fünf Bytes einer nicht infizierten Datei werden mit dem Textstring

"@AIDS"

überschrieben. Von dem Virus existieren bereits zwei Varianten.

#### 4.26.5 Vienna.AntiVir

Diese Vienna-Varianten (zur Zeit 14 Varianten; effektive Codelängen 695 - 982 Bytes) sind sehr stark infektiös. Bei Start eines infizierten Programms werden bis zu 6 COM-Dateien im aktuellen Verzeichnis oder in den Verzeichnissen, die über PATH=... erreichbar sind, infiziert. Den Namen AntiVir hat der Virus, weil er z. B. die Virenwächter von MS-DOS 6.xx (VSafe), VDefend oder TSafe umgeht (abschaltet). Ferner werden alle Checksummendateien von diesen (und anderen) Virenwächtern gelöscht

(= eine Infektion wird nicht bemerkt). Als Schadensroutine wird nach einer bestimmten Anzahl von Infektionen die Festplatte formatiert. Dieser Virus kann mit VirScan - wie fast alle Viennaviren - mit der Option /KILL aus Dateien entfernt werden (ab VirScan Version 10.10d).

#### 4.26.6 Vienna.FatherChristmas

Aka Choinka.1881 (Choinka, polnisch für Tannenbaum)

Variante mit 1881 Bytes Länge, entdeckt in Polen. Der größte Teil der zusätzlichen Länge ist einem Weihnachtsgruß gewidmet, siehe nachfolgender Screen-Shoot.



## 4.27Whale

Der Whale-Virus ist ein Computervirus, der am 1. Juli 1990 entdeckt wurde. Der Whale-Virus wurde auch unter dem Alias "Mother Fish" bekannt. Er handelt sich um einen Computervirus, der in Hamburg, Deutschland, seinen Ursprung hat. Seine Dateigröße beträgt 9.216 Bytes. Mit einer Dateigröße von 9.216 Bytes galt er zur damaligen Zeit als der größte je entdeckte Virus. Er ist bekannt für den Einsatz mehrerer fortschrittlicher "Stealth"-Methoden.

Nachdem die Datei unterhalb der 640k DOS-Grenze im Systemspeicher resident geworden ist, erlebt der Benutzer eine erhebliche Verlangsamung des gesamten Systems aufgrund des polymorphen Codes des Virus. Symptome umfassen Bildschirmflackern und sehr langsames Schreiben von Texten. Dateien scheinen "hängen" zu bleiben, obwohl sie letztendlich korrekt ausgeführt werden. Dies ist das Ergebnis der erheblichen Verlangsamung des gesamten Systems innerhalb des Arbeitsspeichers.

Es wurde berichtet, dass ein infiziertes Programm beim Ausführen folgende Nachricht anzeigte:

```
go
Copy code
THE WHALE IN SEARCH OF THE 8 FISH
I AM '~knzyvo}' IN HAMBURG addr error D9EB,02
```

Wenn man die Buchstaben von "~knzyvo}" um 10 Positionen nach links im ASCII-Code verschiebt, ergibt sich der Begriff "tadpoles" (Kaulquappen)

## 4.28Yankee-Doodle

Dieser Virus stammt, so wurde vermutet, vermutlich aus Deutschland oder aus Österreich. Richtig ist vielmehr, dass er von einem Bulgarischen Programmierer namens T. P. geschrieben wurde. Erstmals aufgefunden wurde er von ALEXANDER HOLY in Wien, der bei einem Forschungsprojekt des "North Atlantic Projects" beschäftigt war. Kurze Zeit später wurde er in Bulgarien aufgefunden, wo man ihm den Namen TP44VIR gab. Er befällt COM- und EXE-Dateien bei Programmausführung, nachdem er sich resident im Speicher installiert hat.

Im Anschluss daran wird jedes aufgerufene Programm infiziert. Infizierte Dateien wachsen durchschnittlich zwischen 2885 und 2899 Bytes. Als Manipulationsaufgabe wird der Lautsprecher des PC aktiviert und gelegentlich die Melodie

## "YANKEE DOODLE DANDY"

abgespielt (aber nie vor 5 Uhr abends). Ferner sind CMOS-RAM Änderungen möglich.

Eine weitere unangenehme Eigenschaft dieses Virus ist seine Befähigung Wächterprogramme zu umgehen. Yankee Doodle war der erste Virus, der das sog. Interrupt Tracing beherrscht (siehe VIRSCAN.DOC) und einer der ersten speicherresidenten Viren, die auch EXE-Programme infizieren können, weshalb der Yankee Doodle oft als Prototyp für andere Viren genommen wurde. Die von mir untersuchten Varianten (TP 44) besitzen zusätzlich die (bis jetzt einzigartige) Fähigkeit, sich selbst zu reparieren. Dies ist möglich, weil der Virus intern eine Prüfroutine eingebaut hat, die Manipulationen entdeckt und repariert (Hamming-Code Distanz 2).

Von diesem Virus existieren zahlreiche Varianten, unter anderem sind einige Spielarten der TP-Familie aus ihm hervorgegangen (TP33VIR, TP34VIR, TP38VIR, TP41VIR, TP42VIR, TP44VIR, TP45VIR und TP46VIR). Keiner dieser Viren enthält destruktiven Code.

Folgende Varianten existieren u.a.:

- TP33VIR: unterbindet die Funktion von INT 01h und INT 03h, wodurch es nicht mehr möglich ist, den Virus im Single Step Mode zu debuggen. Er wird nicht speicherresident (auch als OLD YANKEE bekannt).
- TP34VIR: ähnlich wie TP33VIR, jedoch speicherresident.
- TP38VIR: ist ähnlich wie TP34VIR aufgebaut. COM- und EXE-Dateien werden bei der Infektion völlig unterschiedlich behandelt. Der Virus stammt aus Bulgarien und gilt als einer der ältesten Viren in Bulgarien.
- TP41VIR: ??
- TP42VIR: ist ähnlich zu TP41VIR aufgebaut und überprüft, ob der PING PONG-Virus aktiv ist. Wird der PING PONG gefunden, so wird er von TP42VIR entfernt.
- TP44VIR: ähnlich wie TP42VIR, sehr weit verbreitet.
- TP45VIR: ähnlich wie TP44VIR.
- TP46VIR: ist ähnlich zu TP45VIR, findet aber im Gegensatz zu diesem den CASCADE 1701-Virus und entfernt ihn.
- YD 1905: (Länge 1905-1924) basiert auf dem TP44VIR, benötigt 30464 Bytes Speicherplatz. Der Text "Zak!" kann am Ende infizierter Programme gefunden werden.
- YY B: Länge 2772 Bytes
- YD Logon-D: (Länge 3045-3060), Texte: "LOGON.EXE" und "bbuG"
- YD Logon E: wie YD Logon D, Texte: "LOGIN.EXE" und "bb"
- YD Logon X: (Länge 2968-2987)



Diese Aufzählung ist nicht vollständig, soll jedoch einen Überblick über die Yankee Doodle Familie geben.

## 5 Beschreibung einiger Hybridviren

Hybridviren sind eine Art von Computerviren, die Eigenschaften sowohl von Dateiviren als auch von Bootsekturviren kombinieren. Sie nutzen sowohl Dateien als auch den Bootsektor von Speichermedien, um sich zu verbreiten und Schaden anzurichten.

Im Allgemeinen infizieren Hybridviren sowohl ausführbare Dateien als auch den Bootsektor von Festplatten oder Disketten. Durch die Kombination dieser beiden Infektionsmethoden können sie sich beim Ausführen von infizierten Dateien aktivieren und gleichzeitig den Bootsektor des Speichermediums infizieren. Auf diese Weise kann sich der Virus beim Start des Computers von der infizierten Bootsektorregion aus weiter verbreiten.

Die Kombination von Datei- und Bootsektorinfektion ermöglicht es Hybridviren, sich auf verschiedene Weise zu verbreiten und in das System einzudringen. Sie können sich beispielsweise über infizierte Dateien von Computer zu Computer ausbreiten oder beim Booten von infizierten Speichermedien aktiv werden.

Hybridviren können verschiedene Schadensfunktionen haben, wie zum Beispiel das Löschen oder Beschädigen von Dateien, die Störung des Betriebssystems oder das Auslösen anderer schädlicher Aktivitäten. Durch die Nutzung sowohl von Datei- als auch von Bootsektorinfektionen können Hybridviren schwieriger zu erkennen und zu entfernen sein als Viren, die nur eine dieser Methoden verwenden.

### 5.1 Anthrax

Anthrax ist ein multipler unverschlüsselter Virus, der ca. im Juli 1990 von Dark Avenger entwickelt wurde. Es wurde in Bulgarien (Sofia) entwickelt, aber zuerst in den Niederlanden isoliert und nach der gleichnamigen Trash-Metal-Band benannt.

Wenn eine mit Anthrax infizierte Datei zum ersten Mal ausgeführt wird, schreibt sich der Virus in die Partitionstabelle der Festplatte sowie in die letzten Sektoren der Festplatte. Bei dieser ersten Infektion infiziert er keine Dateien und wird auch nicht speicherresident.

Wenn die Festplatte gebootet wird, wird der Virus speicherresident. Wenn eine Datei ausgeführt wird, infiziert der Virus eine Datei, die dem Stammverzeichnis der Festplatte am nächsten liegt. Wenn die neu



infizierte Datei ausgeführt wird, infiziert er eine andere .com- oder .exe-Datei, wiederum ausgehend vom Stammverzeichnis der Festplatte und auf der Suche nach nicht infizierten Dateien. Wenn sich die infizierte Datei auf einem Diskettenlaufwerk befindet, kann es sein, dass er eine Datei infiziert, muss aber nicht.

Der V2100-Virus wird eine Infektion mit Anthrax wiederherstellen, wenn Anthrax entfernt wurde. Wenn V2100 die Kopie von Anthrax auf den letzten Sektoren findet, legt er sie in der Partitionstabelle wieder ab.

In der Datei befinden sich drei Textstrings: "(c)Damage, Inc.", "ANTHRAX" und "София 1990". Der letzte ist "Sofia", die Hauptstadt Bulgariens und Heimat von Dark Avenger.

## 5.2 Dir-II

Alias Dir, Dir-2, Cluster, CD, Creeping Death, Dir.1024

Geschrieben wurde der DIR-II Virus in Bulgarien, Varna von zwei Mathematikstudenten im Herbst 1990. Der DIR-II Virus ist extrem virulent, weshalb er zu den meistverbreiteten Viren gehört, obwohl er im Original nur mit DOS 3.0 bis DOS 5.0 Beta funktioniert.

Wirkungsweise: Wird der Virus das erste Mal gestartet, nistet er sich als Bestandteil des Betriebssystems (im CONFIG-Bereich) speicherresident ein. Der Virus bindet sich als weiterer Devicetreiber ein, deklariert sich aber als Bestandteil von COMMAND.COM. Durch die Deklaration als Betriebssystembestandteil kann man ihn schwerer lokalisieren. Wird jedoch ein schon infiziertes System gebootet, vergrößert er den Bereich des Kommandointerpreters um ca. 1.5 KB! Als nächsten Schritt schreibt sich der Virus selbst in die letzten 1024 Bytes des Datenträgers, d. h. bei Festplatten, 360 KB & 720 KB Disketten in den letzten Cluster, bei 1.2 MB & 1.44 MB Disketten in die zwei letzten Cluster. Diese Cluster werden vom Virus als belegt markiert (als EOF). Daten, die dort standen, sind verloren! Anschließend versucht er auf dem C: Laufwerk die Datei c:" " (Alt-255) auszuführen, was dazu führt, dass DOS das aktuelle Verzeichnis und den ganzen Pfad (PATH=...) durchsucht. Weil der Virus schon aktiv ist, werden beim Durchsuchen alle Programme im Pfad infiziert!

Der Virus selbst verwendet selbst keine Interrupts, sondern fängt DOS Device Treiber Aufrufe ab, die er entsprechend modifiziert. Infiziert werden vom Virus Einträge aller ausführbaren Dateien (.COM & .EXE) in der ersten FAT. Der Virus kopiert und verschlüsselt deren Zeiger auf die ungenutzten Einträge in der ersten FAT, während er den Originaleintrag auf sich selbst umsetzt. Ruft der Benutzer nun ein Programm auf, wird aufgrund des umgesetzten Eintrags zuerst der Virus aufgerufen. Dieser

sieht nun in seiner "eigenen FAT" nach, welches Programm der Benutzer eigentlich starten wollte, und lädt nun dieses von der Festplatte in den Speicher, wo es gestartet wird.

Stealthtechniken: Die Disketten- und Festplattengröße wird vom Virus als um einen Cluster kleiner deklariert, weshalb nicht auf den eigentlichen Virus zugegriffen werden kann. Wenn von DOS aus auf einen infizierten Directorysektor zugegriffen wird, verändert der Virus den Sektor im Arbeitsspeicher derart, dass er uniniziert erscheint (100% Stealth-eigenschaften). Der Benutzer merkt also vom Virus nichts, weil der eigentliche Wirt überhaupt nicht verändert wurde, sondern nur dessen Directory Eintrag! Solange der Virus im Speicher ist, sehen nämlich alle Verzeichnisse und Einträge völlig normal aus. Bootet man jedoch von sauberen Diskette und schaut sich ein Verzeichnis auf der Festplatte an, so haben alle ausführbaren Dateien die Länge 1024 Bytes (Anmerkung: Länge des Virus) und zeigen auf die gleiche Datei, nämlich den Virus, der sich an Ende des Datenträgers befindet (s. o.). Durch die "Cluster"-Technik kann diese Virenart nicht von Checksummenprogrammen und Monitorprogrammen erfasst werden!

Dieser Virus ist so vermehrungsfreudig, dass er sich, einmal resident, bei bloßen Lesezugriffen auf nicht schreibgeschützte Disketten kopiert und dort in gleicher Weise den Datenträger infiziert. Der Name "CD = Creeping Death" (schleichender Tod) ist in diesem Fall sehr treffend! DIR-2 hat sich nach seiner "Freisetzung" durch seine Autoren wie ein Flächenbrand von Bulgarien aus, durch Osteuropa über die ganze Welt verbreitet.

## 5.3 Delwin

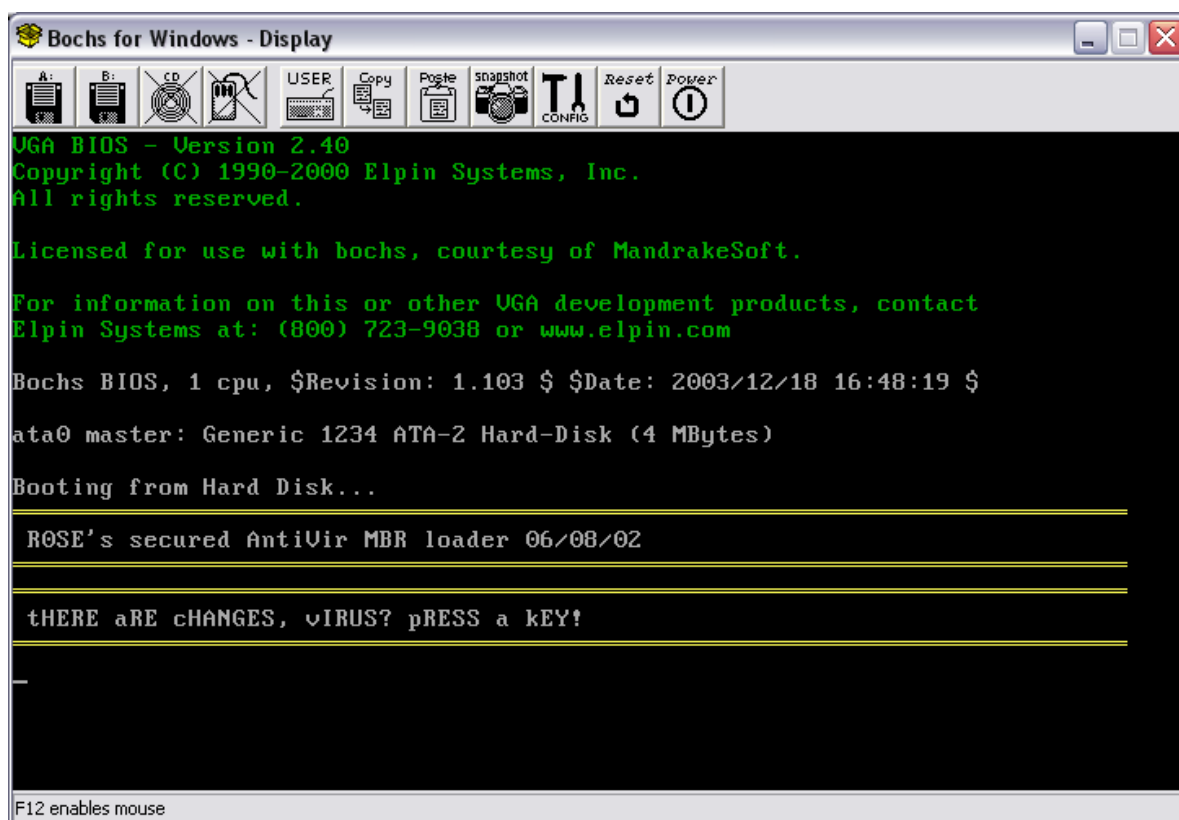
Name:	Delwin.1759, Goblin.1759
Virentyp:	Residenter EXE/MBR-Infektor, Verschlüsselt, Stealth
Größe:	EXE-Programme 1759 Bytes
Sektoren:	1+4+1 Sektoren (MBR/Code/Kopie)
Infiziert:	EXE-Programme ("EXE"-Endung und "MZ"-Test) sowie den MBR
Symptome:	Bildschirmflackern, falsche DOS-Version wird gemeldet
Status:	In Deutschland ist die 1759 Variante stark verbreitet.

Varianten: Von DelWin existieren zur Zeit zwei Varianten, einmal Delwin.1199 der auch als Goblin.1199 bekannt ist und Delwin.1759. Nur die 1759-Byte Variante ist in Deutschland sehr stark verbreitet, sie unterscheidet sich von der 1199-Byte Variante durch die Datei-Stealthfunktionen, die in der kürzeren Variante fehlen. Delwin.1759 enthält den Text "DELWIN", Delwin.1199 den Text "GOBLIN".

Infektionsmechanismus: Wird ein mit DelWin infiziertes Programm gestartet, entschlüsselt sich der Virus zunächst einmal im Speicher. Der Code ist nur mit einer statischen Verschlüsselungsroutine kodiert (XOR [1199] bzw. SUB [1759]), der Virus kann also leicht anhand einer Signatur gefunden werden. Mit der selbst definierten Interrupt 21h-Funktion AX=FD1Ch erkennt der Virus, ob er bereits im Speicher aktiv ist (Rückgabewert: AX=02E3h). Die 1199-Variante verwendet die Werte: AX=E67E -> AX=1981? Ist DelWin bereits aktiv, überspringt er seine Installationsroutine und springt sofort zum ursprünglichen Programmstart des infizierten Wirtprogramms. Ist der Virus noch nicht aktiv im RAM, ermittelt DelWin per INT 21h, AH=52h das DOS-Segment, installiert eine eigene INT 1-Routine (CPU-Einzelschrittmodus) und versucht durch Tracing den ursprünglichen INT 13h (Festplatte/ Diskette) zu ermitteln. Als Dummy-Funktion für den Tracer benutzt DelWin ein Lesezugriff auf den Partitionssektor. Anhand des eingelesenen Sektors erkennt DelWin ob die Partition bereits infiziert wurde, ist das nicht der Fall verseucht der Virus nun den Partitionssektor. Der ursprüngliche Sektor wird nach Spur 0, Kopf 0, Sektor 2 kopiert (0/0/2), der Viruscode (4 Sektoren) nach 0/0/3. Eventuell. dort vorhandene Daten, wie etwa ein Partitionsmanager werden hierbei überschrieben. Der MBR-Code wird infiziert, indem die ersten 46 Bytes durch Viruscode ersetzt werden (Loader). Bevor der Viruscode in die Spur 0 geschrieben wird, ermittelt der Virus das aktuelle Systemdatum, ermittelt ein Datum ungefähr 5 Monate in der Zukunft und speichert diesen Wert im zu sichernden Code ab. Zum Ermitteln des Wertes liest der Virus die Werte der internen Uhr direkt aus dem CMOS aus.

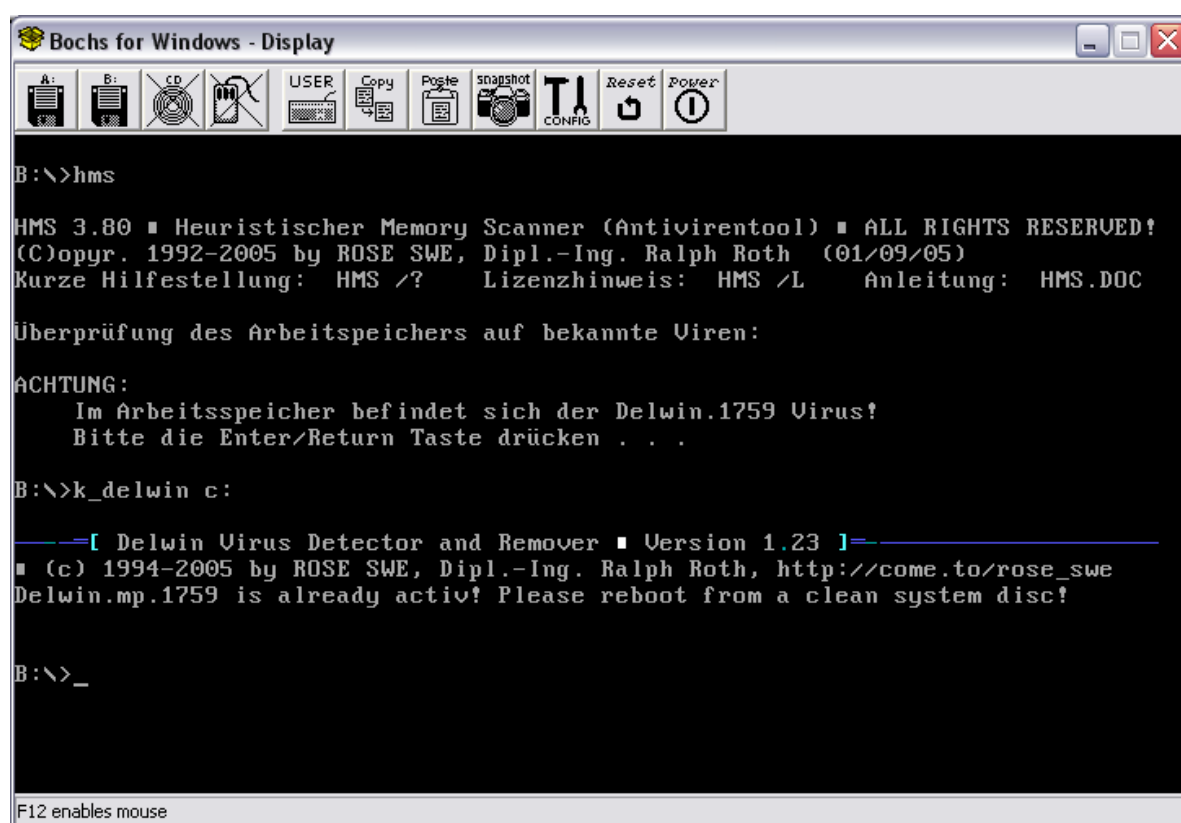
Nachdem das Infizieren abgeschlossen wurde, wird das Wirtprogramm

gestartet. DelWin wird durch das Starten von infizierten EXE-Programmen nicht resident. Wird der Rechner neu gestartet, bleibt der Viruscode aus dem Partitionssektor resident im Speicher. Der DOS-Speicher wird dadurch um 2048 Bytes reduziert und der Interrupt 13h (Sektorzugriffe) belegt. Der Virus wartet dann solange bis DOS geladen wird (INT 21h-Segment unterhalb von 800h) und klinkt sich dann in den INT 21h (Dateistealth, Infektion), INT 13h (Sektorstealth-Routinen) und INT 1Ch (Schadensfunktion) ein. INT 1Ch wird nur dann belegt, wenn das beim Infizieren der Partition festgelegte Systemdatum erreicht ist. Die zweite INT13h-Routine beinhaltet die Stealthfunktion für den Partitionssektor, sämtliche Zugriffe auf den infizierten MBR werden auf die bei Spur 0, Kopf 0, Sektor 2 gespeicherte saubere Kopie umgeleitet. Wichtig: Ist der Virus aktiv kann also der verseuchte Partitionssektor weder erkannt noch gereinigt werden! Mit MBR-Kill behandelte Festplatten erkennen jedoch DelWin, wie folgende Abbildung zeigt:



Infektionsstrategie: DelWin infiziert Programme beim Öffnen (AH=3Dh, 6Ch), beim Umbenennen (AH=56H), Starten (AX=4B00h) sowie unter bestimmten Umständen beim Setzen des Dateidatums (AX=5701). INT 24h wird ausgeschaltet um Fehlermeldungen auf schreibgeschützten Disketten zu vermeiden. Der Virus infiziert EXE-Programme, wobei Programme die mit "SC" (SCAN) und "VI" anfangen nicht infiziert werden. Der Virus infiziert nur EXE-Dateien, die ".EXE" als Dateiendung haben, prüft aber auch noch ob die EXE-Signatur "MZ" vorhanden ist. Zusätzlich

muss das Programm länger als 2048 Bytes sein und darf keine internen Overlays enthalten (Windows-EXE werden somit nicht infiziert). Der Virus setzt das Sekundenfeld von infizierten auf 62 und benutzt diesen Wert als Selbsterkennung beim Infizieren und für die Stealthfunktionen. Der Virus umgeht die Dateiattribute von DOS und behält bis auf die Änderung des Sekundenfeldes auf 62 die alte Dateiuhrzeit bei. Ist der Virus aktiv im Speicher filtert er alle Zugriff auf infizierte Programme so, das die Dateien sauber erscheinen und den alten Inhalt und die alte Dateilänge haben. Die Funktion zum Korrigieren der Dateilänge prüft ob das aktuell laufende Programm im MCB-Namen den Eintrag "DS" enthält. Damit wird vermieden das CHKSDK durch die Stealthfunktionen des Virus irrtümlich Fehler im Dateisystem findet ('Ungültige Programmgröße').

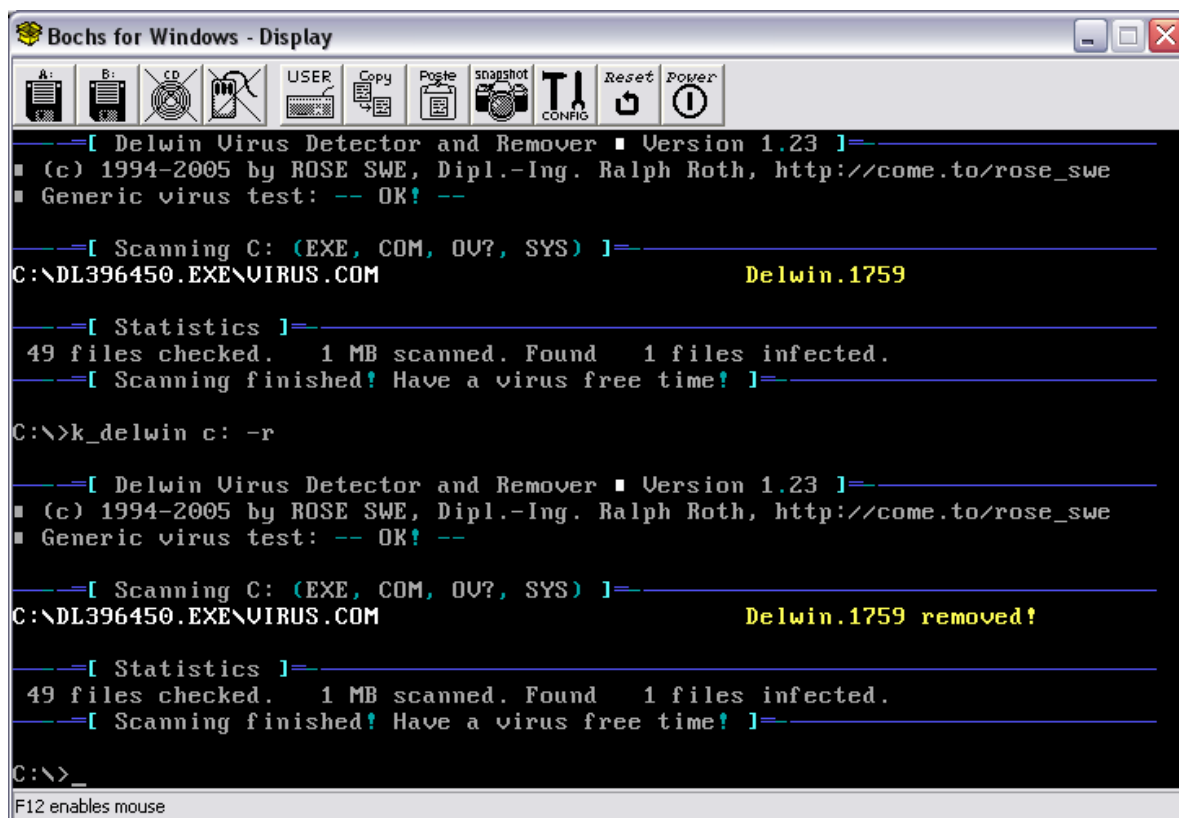


Schadensfunktion: Wird ein Programm mit dem Namen "WIN?????" gestartet (Windows, WIN.COM) gibt der Virus bei der DOS-Funktion AH=30h (DOS-Versionsnummer ermitteln) die DOS-Version 2.10, Hersteller IBM an. Dieser Wert wird normalerweise von OS/2 zurückgeliefert, Windows bricht deshalb den Startvorgang ab. Die Zeitgeber Routine von DelWin verändert in Abhängigkeit des Systemzeitgebers (Daily Counter bei 40:6Ch) das Register 0Fh des CRT Controllers. Das Resultat ist ein schnelles vertikales Flackern der Bildschirmanzeige.

Entfernung: Der Virus muss zuerst aus dem Partitionssektor entfernt werden. Dies erfolgt durch das Programm MBR-Kill. Anschließend von

einer virenfreien Diskette booten und den DelWin-Killer "K-DELWIN" mit folgenden Parametern starten:

```
k-delwin c: -r
```



```
Bochs for Windows - Display
A: B: CD USER Copy Paste snapshot CONFIG Reset Power
--=[ Delwin Virus Detector and Remover ■ Version 1.23 ]=--
■ (c) 1994-2005 by ROSE SWE, Dipl.-Ing. Ralph Roth, http://come.to/rose_swe
■ Generic virus test: -- OK! --

--=[ Scanning C: (EXE, COM, OV?, SYS) ]=--
C:\DL396450.EXE\VIRUS.COM                               Delwin.1759

--=[ Statistics ]=--
49 files checked. 1 MB scanned. Found 1 files infected.
--=[ Scanning finished! Have a virus free time! ]=--

C:\>k_delwin c: -r

--=[ Delwin Virus Detector and Remover ■ Version 1.23 ]=--
■ (c) 1994-2005 by ROSE SWE, Dipl.-Ing. Ralph Roth, http://come.to/rose_swe
■ Generic virus test: -- OK! --

--=[ Scanning C: (EXE, COM, OV?, SYS) ]=--
C:\DL396450.EXE\VIRUS.COM                               Delwin.1759 removed!

--=[ Statistics ]=--
49 files checked. 1 MB scanned. Found 1 files infected.
--=[ Scanning finished! Have a virus free time! ]=--

C:\>_
F12 enables mouse
```

## 5.4 Emperor

Emperor ist ein memory-residenter polymorpher, mehrteiliger Virus. Er infiziert DOS-COM- und EXE-Dateien, indem er seinen Code an das Ende der Datei schreibt, und überschreibt den MBR der Festplatte und des Bootsektors auf Disketten mit seiner eigenen Laderoutine, die den Virus beim Neustart in den Systemspeicher installiert. Der Virus verfügt über viele Anti-Debugging-Tricks, verwendet Stealth-Funktionen und recht komplexe Routinen, um Adressen des DOS-Kernels zu erhalten und so den Virenschutz zu umgehen. Der Virus hat Fehler und in einigen Fällen beschädigt bzw. zerstört er diese Dateien, während er sie infiziert.

Während er den MBR infiziert, verwendet der Virus mehrere Tricks, um den Virenschutz zu umgehen: Er schreibt Daten durch direkte Aufrufe an die Ports des Festplatten-Controllers oder er setzt ein "Y" in den Tastaturpuffer, falls das Megatrends- oder AWARD-BIOS installiert ist, deaktiviert der Virus den VirusWarning-BIOS-Schutz, indem er das notwendige Datenfeld im CMOS löscht.

Der Virus speichert den ursprünglichen MBR und Bootsektoren in den reservierten Sektoren auf dem Laufwerk, verschlüsselt und beschädigt diesen Code jedoch so, dass diese Daten nur dann korrekt funktionieren, wenn die TSR-Kopie des Virus aktiv ist (d.h. nur im Falle einer Infektion der Festplatte hat der Virus seinen Code bereits in den Speicher installiert und die Kontrolle an die ursprüngliche Bootstrap-Routine abgegeben). Der Virus patcht auch die MBR-DiskPartitionTable - er loopt seine Tabellen. Infolgedessen ist es nicht möglich, das System von einer sauberen MS-DOS-Diskette zu laden, und es ist notwendig, andere DOS-Versionen oder spezielle Tools für den Zugriff auf die Festplatte zu verwenden.

Während der Infizierung des MBR- oder Diskettenbootsektors überprüft der Virus diesen auf einen bestimmten Code und löscht den CMOS-Speicher, wenn dieser Code gefunden wird, dann wird die Meldung "Error in CMOS" angezeigt und der Computer wird angehalten. Der Virus hat auch eine gefährlichere Zerstörungsroutine. Er löscht die Daten auf der Festplatte und beschädigt das Flash-BIOS auf die gleiche Weise wie der Virus "Win95.CIH". Der Virus zeigt gleichzeitig die Meldung an:

**EMPEROR**

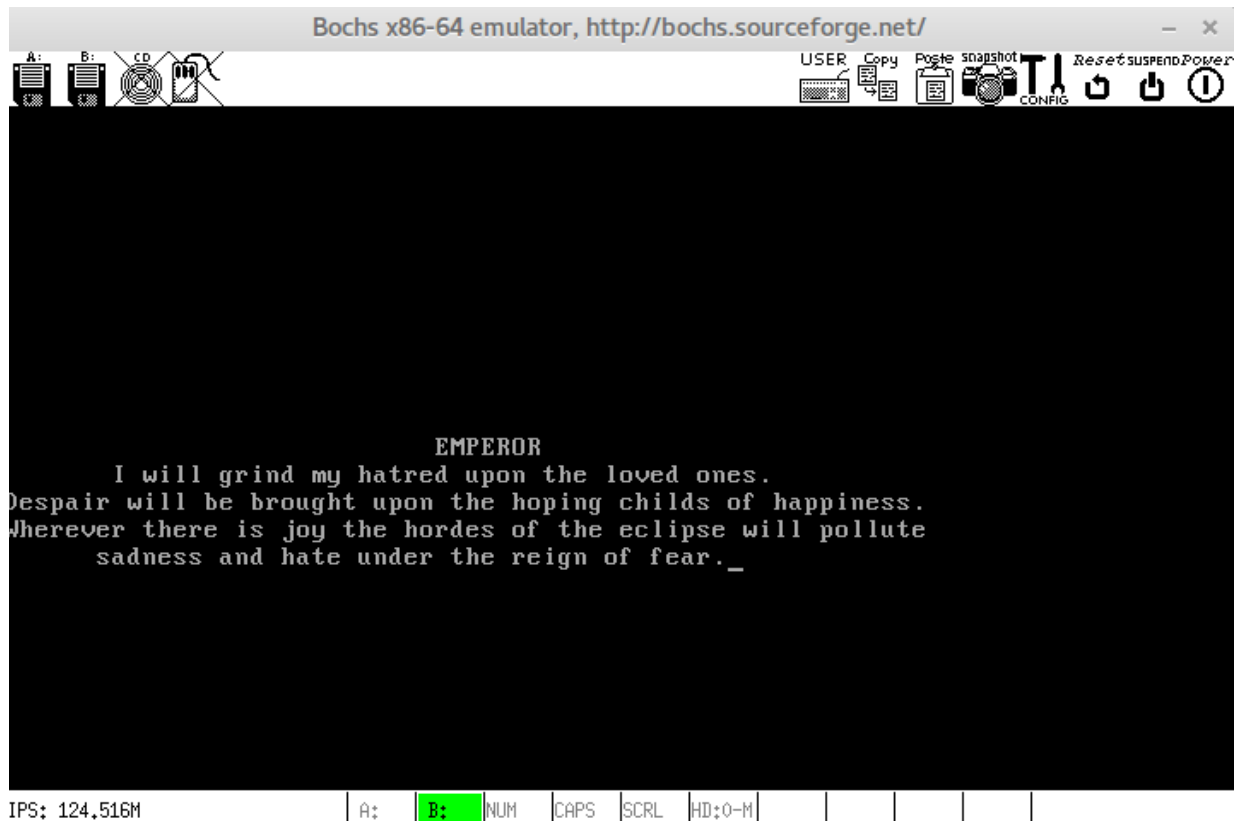
```
I will grind my hatred upon the loved ones.  
Despair will be brought upon the hoping child of happiness.  
Wherever there is joy the hordes of the eclipse will pollute  
sadness and hate under the reign of fear.
```

Der Virus enthält auch die Textzeichenfolgen:

```
In the name of the almighty Emperor....
```

```
the EMPEROR virus  
written by Lucrezia Borgia  
In Colombia, 1999
```





## 5.5 Flip-Virus

Alias Omicrone, Prism

Dieser Virus wurde in Deutschland im Juli 1990 erstmals entdeckt. Er befällt COM- und EXE Dateien, die Datei COMMAND.COM wird ebenfalls von Flip befallen. Weiterhin werden Bootsektoren von Disketten und Festplatten von ihm infiziert.

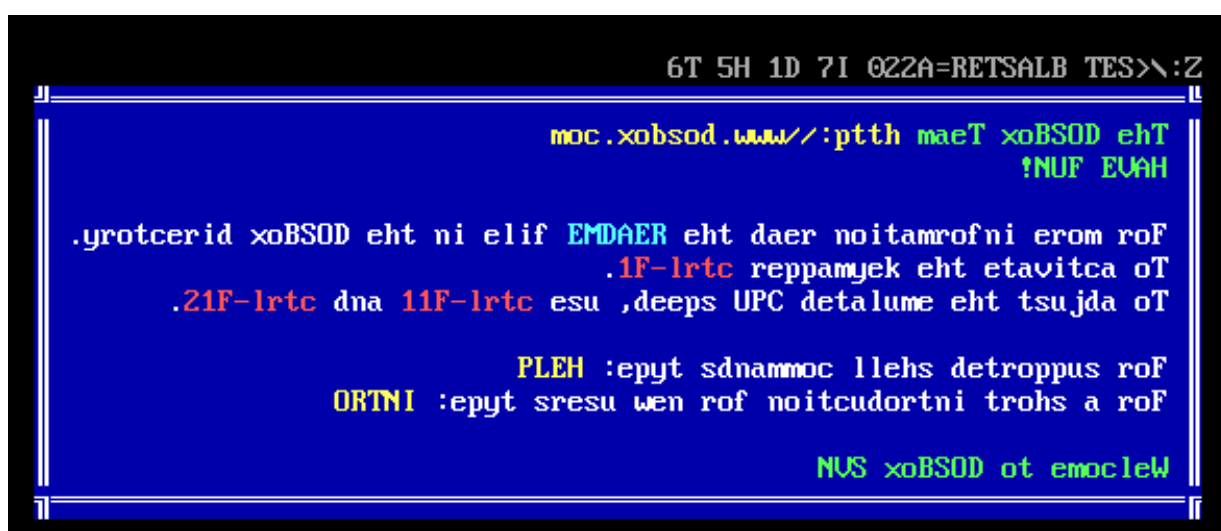
Zum Verständnis dieses sehr komplexen Virus ist es notwendig zu wissen, dass er von befallenen COM-Dateien und befallenen Bootsektoren nicht aktiv werden kann. Er entfaltet seine Aktivität einzig und alleine von EXE-Dateien.

Beim ersten Aufruf von Flip wird der Virus resident im High Memory-Bereich des Speichers geladen. Gesamtspeicher und freier Arbeitsspeicher weisen eine Verringerung um jeweils 3K auf. Zur selben Zeit wird die Datei COMMAND.COM befallen. Im Anschluss daran werden die Partitions Tabelle und der Bootsektor der Hard Disk geringfügig modifiziert. Die Dateilänge des infizierten COMMAND.COM wird bei aktiv im Speicher befindlichen Virus nicht als infiziert ausgegeben, sondern unterdrückt (Tarnkappeneigenschaft). Wird Flip von einer Diskette aus aktiviert, so wird ebenfalls versucht, die Datei COMMAND.COM auf der Floppydisk zu



befallen, wobei anzumerken ist, dass die Längenänderung befallener Dateien nun sehr wohl angezeigt wird. Nachdem Flip speicherresident geworden ist, wird fortan jede aufgerufene COM- und EXE Datei von ihm befallen. Die befallenen Dateien werden um 2,343 Bytes verlängert. Werden OVL-Dateien beim Ladevorgang aktiviert, so werden auch sie von Flip befallen. Die Länge befallener Programme wird nunmehr nicht länger unterdrückt.

Der Virus hat als Schadensfunktion eine Drehung des Bildschirms eingebaut ("FLIP"en), die nur bei EGA- und VGA-Schirmen an jedem 2. Tag in jedem Monat, zwischen vier und fünf Uhr nachmittags durchgeführt wird.



Gelegentlich wurde auch ein Bildschirmflackern beobachtet. Weiterhin können Dateizuordnungsfehler auftreten, die mit CHKDSK angezeigt werden. Durch CROSSLINKS von Dateien kann es bisweilen zur Zerstörung von Datendateien kommen.

Folgende Varianten von Flip sind bekannt:

- Flip 2543 B: Diese Variante wird auch von COM-Dateien aus aktiv.
- Flip 2513 A: Diese Variante ist ähnlich wie das Original aufgebaut, hat aber im Gegensatz zu diesem eine effektive Länge von 2153 Bytes und belegt ca. 2,5 KB freien Speicher, sobald sie resident geworden ist. Der Hauptunterschied besteht darin, dass nun Infektionen auch durch den auf der Partitions Tabelle befindliche Viruscode ausgelöst wird.
- Flip 2153 B: Diese Variante wird auch von COM-Dateien aus aktiv.
- Flip 2513 C: Diese noch relativ unbekannte Variante ist in der Lage, bei der bloßen Anwendung des DIR-Befehls, Infektionen durchzuführen und kann den Bootbereich von Festplatten völlig zerstören.
- Prism: Eine Variante des 2153 B Virus, jedoch wurde die Verschlüsselung so verändert, dass die meisten Virens Scanner den Virus nicht

mehr erkennen.

Das Programm CHKPC.COM kann den Flip 2153 sicher im Arbeitsspeicher und auf der Festplatte erkennen. Mit MBRKill kann der Virus aus der Partition der Festplatte entfernt werden.

## 5.6 Implant Familie

Dieser multipartite Virus, der sowohl ausführbare Dateien als auch kritische Bootsektoren infizieren konnte, zeichnete sich durch seine fortschrittlichen Tarntechniken und einzigartigen Methoden zur Erschwerung der Desinfektion aus, was eine bedeutende Herausforderung für die damalige Antiviren-Technologie darstellte.

Eines der prägenden Merkmale des Implant-Virus war seine polymorphe Natur in Dateien. Beim Infizieren von COM-, EXE- und SYS-Dateien veränderte der Virus seinen Code bei jeder Infektion, was die Erkennung basierend auf statischen Signaturen unglaublich schwierig machte. Dieser Polymorphismus wurde durch ein doppelschichtiges Verschlüsselungsschema noch verstärkt, was eine weitere bedeutende Hürde für Antiviren-Software darstellte, die versuchte, infizierte Dateien zu identifizieren und zu desinfizieren. In Bootsektor-Infektionen war dieser komplexe Polymorphismus jedoch nicht vorhanden; dort behielt der Virus eine unverschlüsselte Struktur bei.

Die Auswirkungen von Implant auf ein kompromittiertes System zeigten sich sofort während des Bootvorgangs. Der Virus nutzte eine clevere Taktik, die eine "zirkuläre erweiterte Partitionstechnik" umfasste, welche Versuche, von einer Standard-Bootdiskette zu starten, effektiv sabotierte. Dies führte häufig zu Systemabstürzen bei der Verwendung gängiger Bootdisketten von MS-DOS 5.x, 6.x oder Windows 95 (MS-DOS 7.x). Benutzer konnten in der Regel nur von älteren, saubereren Systemdisketten wie denen von MS-DOS 3.x, 4.x oder PC DOS 7.x erfolgreich booten.

Unter QEMU sieht das dann wie folgt aus:

```
$ guestmount -a image_cDrive.img -i cDrive
libguestfs: error: inspect_os: parted exited with status 1: Error: Can't
have overlapping partitions.
```

Zur Potenz des Virus trug auch die volle Stealth-Fähigkeit von Implant bei. Wenn der Virus im Speicher resident war, versteckte er seine Anwesenheit aktiv, wodurch das System für den Benutzer und viele damalige Diagnosewerkzeuge sauber erschien. Seine Dateinfektionsroutine war ebenfalls selektiv, wobei der Virus Berichten zufolge die Infektion von Dateien basierend auf ihren Namen vermied. Darüber hinaus integrierte Implant, um die Analyse und Reproduktion durch Sicherheitsforscher zu umgehen, einen Verzögerungsmechanismus und wartete nach der Ausführung bis zu einer Stunde, bevor er mit seinen Verbreitungsaktivitäten begann.

Die Payload des Virus war an ein bestimmtes Datum gebunden: den 4. Juni. Beim Erreichen dieses Aktivierungsdatums versuchte Implant, den Master Boot Record (MBR) der Festplatte zu überschreiben. Diese destruktive Aktion wurde von der Anzeige einer provokanten Nachricht auf dem Bildschirm begleitet:

SuckSexee Automated Intruder  
Viral Implant Bio-Coded by Griyo/29A

Diese Visitenkarte schrieb den Virus "Griyo/29A" zu, wahrscheinlich ein Pseudonym, das mit der damals aktiven Virus-Schreiber-Gruppe 29A in Verbindung gebracht wurde, die dafür bekannt war, die Grenzen der Virentechnologie zu verschieben.

Obwohl die Kernfamilie von Implant diese Eigenschaften teilte, existierten Varianten. Virus.Multi.Implant.6147 ist eine solche Variante, die ebenfalls auf DOS-Systeme abzielte und die gefährliche MBR-Infektionsfähigkeit nutzte, zusammen mit den Stealth- und polymorphen Merkmalen (in Dateien), die die Implant-Linie definierten.

#### Varianten

Implant.5976.com   Implant.6128.A.exe   Implant.6144.com   Implant.6200.com   Virus.Implant.mp.5976.com  
Virus.Implant.mp.6128.a.exe   Virus.Implant.mp.6259.com   Implant.5991.exe   Implant.6128.B.exe  
Implant.6147.com   Implant.exact.boot   Virus.Implant.mp.5991.com   Virus.Implant.mp.6147.pex

## 5.7 Hare

Hare (HD-Euthanasia, Krsna, Krishna, RD Euthanasia) ist ein residenter, multipartite Virus mit polymorpher Verschlüsselungstechnik.

Der Virus infiziert COM- und EXE-Dateien, den Partitionssektor (MBR) von Festplatten und den Bootsektor von Disketten. Infizierte Objekte werden verschlüsselt. Bei Dateien wird die Infektion markiert, in dem der unter DOS nicht angezeigte Sekundeneintrag auf 34 gesetzt wird. Hare infiziert keine Dateien, die mit "TB" oder "F-" beginnen oder den Buchstaben "V" im Dateinamen haben. Dadurch werden die meisten Antivirenprogramme nicht infiziert, was ansonsten durch deren Selbstüberprüfung zu einer frühen Entdeckung des Virus führen würde.

Bei einigen Computern wird bei der Infektion der Inhalt der Partitionstabelle zerstört. Der Virus kopiert sich hinter das Ende des von DOS erreichbaren Festplatten- bzw. Diskettenbereiches. Aufgrund der zerstörten Partitionstabelle darf der Befehl " FDISK /MBR " keinesfalls eingesetzt werden!

Hare verwendet mehr als 9 KByte Hauptspeicher, wenn er resident ist. Infizierte Dateien werden um 7 KByte größer, je nach verwendeter Verschlüsselung.

Der Hare Virus löscht bei Windows 95 die Datei:

Damit versucht der Virus zu verhindern, dass das Betriebssystem sich bei der Infektion von Disketten aufhängt. Nach erfolgreicher Entfernung des Virus bei Windows 95 muss diese Datei wieder re-installiert werden.

Wird ein infizierter Rechner am 22. August oder 22. September gestartet, so erscheint die Virusmeldung:

"HDEuthanasia" by Demon Emperor: Hare Krsna, hare, hare...

Danach versucht Hare den Festplatteninhalt zu überschreiben.

Der Virus wurde über Newsgroups des Internet verteilt und sorgte im Frühjahr 1996 für eine gewisse Hysterie in den Medien, obwohl - im Gegensatz zum Michelangelo kaum Schadensfälle gemeldet wurden. Dies ist auch auf einige Programmierfehler des Virusautors zurückzuführen, die zu einer frühen Entdeckung der Infektion führten und damit glücklicherweise eine größere Verbreitung verhinderten. Die Infektion erfolgt entweder über Booten (bzw. Boot-Versuch) von einer infizierten Diskette, oder durch Ausführen eines infizierten Programms. Der Virus wird speicherresident, wenn der infizierte Rechner gestartet wird, oder ein infiziertes Programm ausgeführt wird. Nach dem Start eines infizierten Rechners versucht der Virus jede Diskette zu infizieren, auf die zugegriffen wird. Ist der Diskettenschreibschutz aktiviert, so bricht der Virus den Versuch ab. Ist der Virus speicherresident, werden COM- und EXE-Dateien bei ihrer Ausführung infiziert. Aufgrund der zerstörten Partitionstabelle muss der Virus mit einem entsprechenden Antivirusprogramm entfernt werden.

## 5.8 Kuarahy

Kuarahy.4606, Kuarahy.4608, Kuarahy.4771

Es handelt sich um einen gefährlichen, residenten, verschlüsselten Multipartite-Virus. Er infiziert den MBR-Sektor der Festplatte und die Bootsektoren von 1,44-MB-Festplatten, infiziert COM-, EXE- und SYS-Dateien und erstellt zugehörige COM-Dateien für BAT-Dateien. Darüber hinaus fügt der Virus Teile seines eigenen Codes zu ARJ-Archiven hinzu. Der Virus versucht auch, OBJ-Dateien zu infizieren, zerstört sie jedoch aufgrund eines Fehlers im Code. Als Folge von Programmier-Fehlern kann der Virus Ihren Computer außer Betrieb setzen.

Der Virus infiziert weder die Datei COMMAND.COM noch Komponenten von Antiviren-Programmen wie COMMAND, SCAN, NAV, F-PROT, GUARD, FINDVIRU, TOOLKIT, AVP.

Der Schädling entfernt diese Dateien: ANTI-VIR.DAT, CHKLIST.MS, CHKLIST.CPS, AVP.CRC.

Am 31. eines jeden Monats zeigt der Virus Text an:

[KUARAHY by Int13h] - Written in the Republic of Paraguay - Please register!

Der folgende Text wird im Virencode gespeichert:

```
[KUARAHY] Koa ha'e Int13h/iKx rembiapokué hina! :)
          HOMO ¿SAPIENS? HAHAHA!
          DOS Infection Device
Learn some guaraní words!:Kuarahy=Sun  Añá=Devil  Kuñá=Woman
          execomsysobjbatovlarj
          E-mail me: Int13h@antisocial.com
          PARAGUAY WORLD CUP '98
          Rohaihú Paraguay!
```

## 5.9 Natas

Alias: SatanBug.Natas,

Varianten: Natas.4646, **Natas.4774**, Natas.4988

Natas = rückwärts SATAN - er wurde von dem Autor des SatanBug geschrieben. Natas wurde erstmals "in the wild" im Januar 1994 in Mexiko entdeckt.

Natas.4744 ist ein gefährlicher, speicherresistenter, multipartiter, polymorpher Virus, welcher den Interrupt 13h und 21h manipuliert und sich in den MBR, in Bootsektoren und ans Ende von .COM und .EXE Files schreibt, auf die zugegriffen wird. Dateien von Archivprogrammen werden nicht infiziert. Abhängig von seinen internen Zählern löscht er Sektoren auf der Festplatte. Der Virus enthält folgende interne Texte:

- BACK MODEM
- Natas

### Varianten

Natas.1744	Natas.4742	Natas.4750.A	Natas.4788	Natas.4872.boot
Natas.1744	Natas.4744.A.exact	Natas.4750.A	Natas.4798.A.exact	Natas.4872
Natas.1894	Natas.4744.A.exact	Natas.4766	Natas.4798.A.exact	Natas.4872
Natas.1894	Natas.4744.C.exact	Natas.4766	Natas.4798.B.exact	Natas.4926
Natas.1910	Natas.4744.C.exact	Natas.4774	Natas.4798.B.exact	Natas.4926
Natas.1910	Natas.4744.D.exact	Natas.4774	Natas.4798	Natas.4988
Natas.4736.A	Natas.4744.D.exact	Natas.4776	Natas.4798	Natas.4988
Natas.4736.A	Natas.4744.E.exact	Natas.4776	Natas.4814	
Natas.4738	Natas.4744	Natas.4786	Natas.4826.boot	
Natas.4740	Natas.4746	Natas.4788	Natas.4826	
Natas.4740	Natas.4746	Natas.4788.exact.boot	Natas.4866.boot	Natas.5006
Natas.4738	Natas.4744.F.exact	Natas.4786	Natas.4814	Natas.exact.boot

Natas.4738	Natas.4744	Natas.4786	Natas.4826.boot
Natas.4740	Natas.4746	Natas.4788	Natas.4826
Natas.4740	Natas.4746	Natas.4788.exact.boot	Natas.4866.boot

## 5.10 Neuroquila

Alias: HAVOC, Wedding

Länge: EXE Programme: 4644-4675 Bytes, Festplatte & Disketten: 9 Sektoren

Siehe auch: Nightfall

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. Der Virus versucht dann die Partition der Festplatte zu infizieren und lädt anschließend 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 und nistet sich dort ein. 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 Interrupt 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), DOSDATA.SYS (QEMM) und "QC\*" ("QCDRV" von H+BEDV).

## 5.11 Nightfall (N8Fall)

Alias: Neuroquila, Art & Strategy, Nightfall

Länge: EXE Programme: 4554-4585 Bytes, Speicher: 4688 Bytes

Nightfall basiert offensichtlich auf Neuroquila, obwohl die Fähigkeit, Festplatten und Disketten zu infizieren, fehlt. Die Mutationengine stimmt bis auf ein paar kleinere Änderungen mit der von Neuroquila überein.

Statt dessen infiziert Nightfall jetzt auch beim Schließen von Programmen („fast infector“) und neben EXE Programmen befällt Nightfall 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 Single Step Tracer zum Ermitteln des ursprünglichen INT-21h Einsprungs, sondern sucht direkt innerhalb der HMA nach den typischen Einsprung und verändert diesen 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=" Umgebungsvariable den Kommandointerpreter (COMMAND.COM).

#### 5.11.1 Nightfall.B

Die Viruslänge liegt jetzt bei 5801 bis 5832 Bytes bei infizierten Programmen und 6048 Bytes Speicherbelegung.

#### 5.11.2 Nightfall.Spawn

Dieser Virus (Dateilänge 527 Bytes) wird von Nightfall.B, sechs Monate nach dem COMMAND.COM infiziert wurde, installiert und aktiviert. Nightfall.Spawn 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.

Nightfall kann mit MBR-Kill, VirScan Plus und K\_N8Fall entfernt werden.

### 5.12 Junkie

Der JUNKIE Virus wurde Ende Mai 1994 durch verschiedene europäische Mailboxen verbreitet. In den meisten Fällen durch das Archiv HV-PSPTC.ZIP. Laut der Beschreibung sollte das Archiv es ermöglichen, illegale Kopien eines Spiels 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 (Hybridvirus). Er infiziert Bootsektoren, den MBR der Festplatte und COM-Dateien. Wenn auf einem unverseuchten Rechner zum ersten Mal ein infiziertes Programm gestartet wird, überschreibt der Virus den MBR der Festplatte (sonst macht er nichts). Beim nächsten Rechnerstart wird JUNKIE vom



MBR aus speicherresident und infiziert alle von da ab gestarteten oder geöffnete COM-Programme („fast infector“) und alle Disketten, die keinen Schreibschutz besitzen.

Vom Junkie Virus existieren zur Zeit zwei Varianten, die sich durch ihre effektive Länge unterscheiden. Die am weitesten verbreitetste Variante ist 1027 Bytes, die zweite 1035 Bytes lang. Infizierte COM-Dateien werden um 1027 oder 1035 Bytes größer. Da der Virus nur COM Dateien infizieren kann, zerstört er alle Programme, die zwar eine COM Endung haben, aber keine echten COM-Dateien sind (z. B. einige COM Programme von MS-DOS). Manche Programme bringen daher auch die Fehlermeldung "Program too big to fit in memory" oder "Programm passt nicht in den Arbeitsspeicher". 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 u. a. daran erkennen, dass der zu Verfügung stehende Hauptspeicher um 3 KB verringert ist. Infizierte Bootsektoren/MBRs sehen ganz normal aus, weil der Virus nur einen ca. 60 Bytes langen Lader einfügt. Dieses Ladeprogramm lädt den eigentlichen Virus von der Spur 4 und 5 der Festplatte bzw. von den letzten Sektoren der Diskette nach und startet ihn.

#### Merkmale

- Größe (Dateischreibzugriff): 1027 Bytes
- Größe (Programmstart bis Dateiende): 1027 Bytes
- Virus infiziert COM Programme
- Virus infiziert Bootsektoren und Partitionen
- Virus infiziert Programme beim Öffnen ("Fast Infector")
- Virus infiziert Programme beim Ausführen
- Virus fängt das Öffnen von Programmen ab (Extended Open)
- Virus manipuliert den Dateianfang
- Virus hängt sich an das Ende des Programms
- Virus fügt ein JMP NEAR am Programmstart ein
- Virus ist verschlüsselt (simples XOR)
- Virus behält Dateidatum- und Uhrzeit beim Infizieren bei
- Virus umgeht READ-ONLY, HIDDEN oder SYSTEM Dateiattribute
- Virus unterdrückt Schreibschutz-Fehlermeldungen bei Disketten
- Virus ist speicherresident
- Virus verringert TOM-Speicherobergrenze (3K)
- Virus benutzt INT 21h, 24h, 13h
- Virus ruft gespeicherten INT 21h direkt auf (CALL FAR)
- Virus ermittelt ursprünglichen Interruptvektor ("Tracer")
- Virus verschiebt seinen Code im Speicher (1024 Bytes)
- Virus umgeht VSAFE/TSAFE
- Virus überprüft die Systemuhrzeit



- Virus enthält den Text: "Junkie Virus - Written in Malmo...M01D"

Entfernung: Entfernt werden kann der Junkie Virus aus Dateien und MBR mit dem Killer K-Junkie. Überschriebene Diskettenbootsektoren müssen mit dem Programm BootKill gereinigt werden.

## 5.13 Telecom/Kampana

**Alias:** 3445, Telefonica, Spanish Telecom, Kampana.3700, Anti-Tel, Campana, Drug, Holo, Holocaust, Holokausto, Kampana Boot, Spanish Telecom, Spanish Trojan, Telecom, Telecom PT1, Telefonica, Telephonica

Der Telecom-Virus wurde erstmals im Dezember 1990 in Spanien entdeckt. Telecom ist ein speicherresidenter, verschlüsselter (zwei verschiedene Verschlüsselungsroutinen) Tarnkappenvirus der COM-Dateien und zusätzlich die Partitionstabelle infiziert. Telecom besteht aus zwei Viren, dem eigentlichen Telecom-Virus und dem Anti-Tel Bootvirus. Der Telecom war einer der am weitesten verbreiteten Viren überhaupt!

Wird ein, mit Telecom infiziertes Programm gestartet, so installiert sich der Virus unterhalb der 640 KB Grenze und verringert den Arbeitsspeicher um 3984 Bytes (-> CHKDSK). Im gleichen Zuge wird die Partitionstabelle der Festplatte mit einer Variante des Anti-Tel Virus infiziert. Der Telecom hat zusätzlich einen zweiten Virus integriert (**Anti-Tel**) der unabhängig ist! Kampana wird oft als multipartite klassifiziert, was bedeutet, dass es Programmdateien und Bootsektoren infiziert. Dies ist jedoch nicht ganz korrekt. Kampana.Anti-Tel ist ein Stealth-Virus und infiziert keine Dateien, sondern wird von einem Dateivirus fallen gelassen. Beispielsweise gibt es einen Dateivirusstamm, Kampana.3700, der .COM-Dateien infiziert und den Kampana-Bootsektorvirus fallen lässt. Der Kampana-Bootsektorvirus wiederum infiziert jedoch keine .COM-Dateien, wie dies bei echten Multipartite-Viren der Fall ist. Darüber hinaus ist der Kampana-Dateivirus überhaupt nicht verbreitet, während der Kampana-Bootsektorvirus sehr verbreitet ist.

Anschließend werden sämtliche COM-Dateien, die größer als 1000 Bytes und kleiner 61000 Bytes sind beim Starten infiziert. Ein Dateizuwachs ist nicht ersichtlich (Tarnkappenvirus)! Die Unterscheidung, ob eine Datei infiziert wurde erkennt der Virus daran, dass das Dateidatum um 100 Jahre erhöht wurde (1993 -> 2093).

Schadensfunktion: Der Anti-Tel Virus überschreibt die Partitionstabelle und kann deshalb nicht ohne weiteres entfernt werden, weil ansonsten die Festplatte nicht mehr ansprechbar ist. Nach 400 Bootvorgängen überschreibt der Anti-Tel Virus die Festplatte!

**Querverweis: Anti-Tel**

Folgende Varianten sind zur Zeit bekannt:

- Kampana.3445 | Telecom (3445) | 4096 [4096]
- Kampana.3700 | Telecom (3700) | Telecom [Tele]
- Kampana.3784 | Telecom (3784) | Holo [Hl]
- Kampana.3445 - Setzt den Kampana-Bootvirus ab.
- Kampana.3770 - Verwendet polymorphe Technologie und löscht den Kampana-Bootvirus.
- Kampana.3784 - Legt den Kampana-Bootvirus ab.

Der ursprüngliche Kampana-Dateivirus enthält einen verschlüsselten Text, der einer Grupo Holokausto in Barcelona, Spanien, die Programmierung des Virus zuschreibt und das Datum 23.8.90 zusammen mit einem Urheberrechtsvermerk angibt. Eine Nachricht in dem Virus verlangt auch niedrigere Telefongebühren und mehr Service.

## 5.14 Tequila-Virus

Tequila bezeichnet eine Gruppe von Computerviren, die sich seit Anfang 1991 weit verbreitet haben. Tequila ist ein sogenannter "Multi-Partite"-Virus und wurde am 4. Januar 1991 entdeckt. Der Programmcode wurde von zwei Brüdern aus der Schweiz im Alter von 18 und 21 Jahren geschrieben. Einige IT-Systeme deutscher Unternehmen wurden mit diesem Virus infiziert. Unter den Betroffenen waren mehrere Gymnasien und eine Frankfurter Großbank.

Tequila infiziert alle EXE Programme, wenn sie gestartet werden. Beim Start überprüft der Virus, ob er sich schon im Arbeitsspeicher und in der Partitionstabelle der Festplatte eingenistet hat. Falls dies noch nicht geschehen ist, schreibt er sich in die Partitionstabelle der Festplatte. Er bleibt solange inaktiv, bis Sie beim Bootvorgang den Virus aus der Partitionstabelle aktivieren. Eine Infizierung von Programmen kann man am 62 Sekundeneintrag des Datums und an einem Zuwachs von 2468 Bytes an der Datei erkennen (z. B. mit AntiLink), wenn der Virus sich NICHT im Arbeitsspeicher befindet! Der Virus befällt jedoch nicht Programme die den Buchstaben "V", "A" oder "S" enthalten. Die Programmierer wollten wahrscheinlich verhindern, dass der Virus Antivirenprogramme infiziert (z. B. SCAN, ANTI., VIR.). Der Virus verschlüsselt sich fortlaufend. Ich habe festgestellt, dass er mindestens zwei verschiedene Verschlüsselungsroutinen verwendet und diese aber mit sinnlosen Maschinenbefehlen auffüllt, d. h. bei allen verseuchten Dateien hat der Virus kein festes Erkennungsmerkmal (polymorpher Virus!). Als Schadensfunktion ist die Darstellung einer umrandeten Meldung (s. u.) und eines Fraktales implementiert, die nach vier Monaten nach der ersten Infizieren auf dem Bild-

schirm dargestellt wird.



Die zwei Programmierer des Virus wurden zwischenzeitlich festgenommen (Ihre Adresse siehe unten!).

Der Virus gehört zur so genannten vierten Generation von Viren, weil er alle möglichen Tricks benützt, um unerkannt zu bleiben (Stealth-Techniken). Im Partitionssektor und im Arbeitsspeicher ist der Tequila Virus aber unverschlüsselt.

Nach Abarbeiten der Verschlüsselungsroutine des Virus habe ich folgenden Text im Virus gefunden. Dieser Text wird in die letzten Sektoren der Festplatte geschrieben und ist auch in verschlüsselter Form in den infizierten Programmdateien zu finden:

```
"Welcome to T. Tequila'6 latest production
Contact: T. Tequila P. o. Box 543
        6132 St'haus / Switzerland "
"Tequila and Beer forever"
"Loving thoughts goes to L.I.N.D.A!"
```

Wenn Sie VirScan Plus starten und der Virus aktiv ist, erhalten Sie pro infizierter Datei folgende Meldung:

```
Warnung Datei xx: Unübliche Zeit xx:xx:62
Warnung Datei xx: Einsprungspunkt außerhalb der Datei
```

Der Virus kann aus der Partitionstabelle entfernt werden, nachdem von einer virenfreien Systemdiskette gebootet wurde. Wenn nicht mit BootVir die Partitionstabelle gesichert wurde können Sie mit meinem Programm MBR-KILL (evtl. anfordern) u. U. den Virus entfernen.

## 5.15Thanksgiving

(Alias: 1253, V1253, Thksgiving, V-1)

Dieser Virus stammt aus Österreich und trat im August 1990 erstmals in Erscheinung. Er befällt COM-Dateien und COMMAND.COM, wobei befallene Dateien um 1253 Bytes verlängert werden. Beim ersten Aufruf installiert er sich speicherresident und verringert den freien Arbeitsspeicher um 2128 Bytes. Er installiert sich im Anschluss daran sofort im Partitionssektor der Festplatte oder im Bootsektor von Disketten, sofern eine infizierte Datei auf einer Diskette aufgerufen wurde. Zu diesem Zeitpunkt befindet sich der Virus im oberen Bereich des Arbeitsspeichers, jedoch unter der 640 KB Grenze. Der Gesamtspeicher wird vom Virus nicht beeinflusst. Bei jedem Diskettenzugriff wird der Bootsektor der Diskette infiziert!

Folgende Interruptvektoren werden von Virus "1253" benützt: 08h, 13h, 21h und 60h.

Als Besonderheit des Virus gilt die Eigenschaft, dass wenn von einer verseuchten Partition einer Festplatte oder von einer verseuchten Floppydisk gebootet wird, der Virus sich im Bereich oberhalb des DOS-Kernels, jedoch unterhalb der 640 KB-Grenze speicherresident einnistet. Im Anschluss daran wird der Gesamtspeicher und der noch freie Arbeitsspeicher um ca. 77 KB verringert.

Nachdem er speicherresident geworden ist, infiziert er COM-Dateien, indem er seinen Code an das Ende der Datei anhängt. Weiterhin werden das vierte bis sechste Byte durch den Text:

V-1

ersetzt. Die Bytes eins bis drei enthalten den Sprungbefehl auf den angehängten Viruscode.

Schadensfunktion: Fällt das Systemdatum auf einen 24. Dezember und wird ein infiziertes Programm ausgeführt, so wird die gesamte Diskette/Festplatte unbrauchbar gemacht. Zerstörungen der FAT und Datenbereiche von Festplatten können ebenfalls die Folge sein.

Nebeneffekte: Wird von einer infizierter Festplatte mit dem DOS-Befehl "FORMAT" eine Diskette im Laufwerk A: neu formatiert, so kommt es auch zu Schreibzugriffen im Laufwerk B:, bzw. jedem weiteren angeschlossenen Laufwerk.

## 5.16 Tremor

In Zusammenhang mit der erstmaligen Verbreitung von Viren via TV (Channel Videodat) im Mai 1993 wurde sein Name wiederholt erwähnt: Tremor (tremor, lat = Muskelzittern). Seither will nicht so recht Ruhe einkehren an der Virenfront. Möglicherweise wurden bei der Ausstrahlung via TV durch rasche Gegenmaßnahmen eine große Verbreitung des Tremor-Virus verhindert - die Verantwortlichen strahlten kurz nach Bekannt werden das infizierte File in virenfreier Fassung noch mal aus- so ihre Stellungnahme. Auch die bereits festgestellten, vielfach verschiedenen Grundversionen des Virus legen den Verdacht nahe, dass Tremor eine weite Verbreitung in Deutschland gefunden hat. Im Januar 1995 gehörte der Tremor zu den acht am weitesten verbreiteten Viren in Deutschland!

Tremor ist nach dem intern (zusätzlich) verschlüsseltem Text

```
-=> T`R`E`M`O`R was done by NEUROBASHER / May-June'92, Germany <=-
```

```
-MOMENTS-OF-TERROR-IS-THE-BEGINNING-OF-LIFE-
```

```
-=> T·R·E·M·O·R was done by NEUROBASHER / May-June'92, Germany <=-
```

```
-MOMENT-OF-TERROR-IS-THE-BEGINNING-OF-LIFE- _
```

ein in Deutschland programmierter, hochgradig verschlüsselter polymorpher (polymorph, lat.=vielgestaltig) Virus mit (Pure) Stealth-Eigenschaften. Tremor befällt EXE- und teilweise COM-Dateien und verlängert diese um (genau) 4000 Bytes. Als Stealth-Eigenschaften bezeichnet man im allgemeinen die Fähigkeiten der amerikanischen Tarnkappen-Bomber, auf Radarschirmen nicht mehr wahrnehmbar zu sein. Dies erreicht der Virus u. a. dadurch, dass er das Dateidatum infizierter Programme um 100 Jahre erhöht (1993 -> 2093). Die Besonderheit des Virus ist eben, dass er DOS-Programme wie CHKDSK manipuliert und den im Lieferumfang von DOS 6.0 enthaltenen, residenten Virenwächter VSAFE, (auch TSAFE u. a.) ausschaltet. Seinen Namen bezieht der Virus von seiner Schadensroutine, die gelegentlich das "Bildschirmbild" zittern lässt. Der Dekoder von Tremor bietet nahezu unbegrenzte Möglichkeiten zur Mutation, weshalb ein mathematisches Näherungsverfahren

notwendig ist, um überhaupt diesen Virus erkennen zu können! Am Virus sind insgesamt nur drei Bytes konstant!

Eine Infektion erfolgt, wenn ein von Tremor befallenes Programm aufgeführt wird. Als erstes überprüft der Virus, ob DOS 3.3 oder höher vorhanden ist (Tremor benützt mehrere relativ neuere DOS-Funktionen) und ob er noch nicht aktiv ist. Anschließend untersucht der Virus, ob XMS, UMB-Speicher oder EMS Speicher vorhanden ist und installiert sich dann gegebenenfalls in den hohen Speicherbereich überhalb der 640 KB Grenze! Andernfalls installiert er sich 4 KB unterhalb des höchsten Speicherbereiches (meist um 636 KB), was aber mit Speicheranzeigeprogrammen wie MEM oder RESIDENT nicht ersichtlich ist. Anschließend wird die COMSPEC-Variable ausgelesen und das Programm infiziert, auf das die COMSPEC-Variable zeigt. Dies ist i. a. COMMAND.COM. Tremor infiziert dann jedes Programm bei Ausführung, das einen gültigen EXE-Kopf hat, auch Programme, die von EXE nach COM umbenannt wurden. Warum Tremor generell keine COM-Dateien infiziert (obwohl er dies kann), könnte an einem Programmierfehler liegen. Es gibt auch eine zweite Variante von Tremor, die zusätzlich auch COM-Programme infiziert.

Tremor überprüft ALLE DOS-Funktionen und manipuliert sie entsprechend falls ein Programm wie CHKDSK gerade abläuft. Tremor manipuliert u. a. folgende Programme:

ARJ, SCAN. CLEAN, CHKDSK, MEM, SYS, MIRROR und F-PROT

Tremor ist ein ziemlich komplexer Virus (über 48 Seiten disassemblierter Assemblercode), der meines Erachtens jedoch relativ unstrukturiert und schlampig programmiert wurde (ein frustrierter Schüler?): Verschachtelte Sprünge, wildes Abspeichern von Daten im eigenen Code usw. So konnte ich mehrmals nachweisen, dass (anhand von nicht gesicherten Registern) sich der Virus aufhängt.

Tremor ist ein 100 %-tiger Stealthvirus, der, wenn er aktiv ist, nicht auf der Platte erkannt werden kann, weil der Virus sich bei Lesezugriffen aus infizierten Programmen heraus filtert! Auch die Zunahme des Datums um 100 Jahre wird unterdrückt. Eine Verlangsamung bei Dateizugriffen ist jedoch deutlich merkbar. Die Schadensroutine (Bildschirmzittern plus Tonausgabe) wird erst nach genau drei Monaten aktiviert, nachdem das Programm infiziert wurde. Auf der Freeware Tools Diskette befindet sich ein Programm TREMOR.COM, das den Tremor-Virus simuliert!

Der Tremor-Virus kann im Arbeitsspeicher mit VirScan und CHKPC erkannt werden. Auf der Festplatte kann der Virus mit VirScan in Programmen gefunden werden, nachdem der Virus durch einen Kaltstart von einer Betriebssystemdiskette deaktiviert wurde. Entfernen können Sie den Virus mit VirScan (mit der Option /KILL). VirScan war sehr lange Zeit

der einzige Virens Scanner der den Tremor-Virus erkennen und entfernen konnte!

## 6 Beschreibung einiger Bootviren

Ein Bootvirus ist ein Computervirus, der beim Start des Rechners (Booten) aktiv wird, noch bevor das Betriebssystem komplett geladen ist. Auf Disketten sitzt der Virus zumindest teilweise im Bootsektor; selbst Disketten, die keine Dateien enthalten, können also infiziert sein. Auf Festplatten kann der Virus im Master Boot Record (MBR) oder im logischen Bootsektor sitzen.

Bootviren sind die ältesten Computerviren überhaupt. Diese Viren waren bis 1995 die meist verbreitete Form von Viren. Ein Bootsektorvirus infiziert den Bootsektor von Disketten und Festplatten sowie den Master Boot Record (MBR) einer Festplatte. Der Bootsektor ist der erste physische Teil einer Diskette und einen Sektor (512 Byte) groß. Der Bootsektor wird von Startdisketten verwendet, um von der Diskette booten zu können, jedoch hat jede Diskette und Festplatte einen Bootsektor oder einen MBR. Bootsektorviren nutzen die Tatsache aus, dass der Bootsektor immer als erstes geladen wird. Will ein Benutzer von einer infizierten Startdiskette booten oder vergisst er eine infizierte Diskette im Diskettenlaufwerk beim Start des Computers, greift das BIOS bei entsprechender BIOS-Boot-Einstellung auf diesen Sektor zu und führt ihn aus. Der Virus versucht danach, den MBR der Festplatte zu infizieren, um bei jedem Start des Computers ausgeführt zu werden. Wenn ein infizierter Computer startet, wird der MBR geladen, der normalerweise für das Erkennen der verschiedenen Partitionen der Festplatte zuständig ist. Der Virus, das nun geladen wird, bleibt im Speicher und überwacht die Zugriffe auf andere Disketten. Wenn eine Diskette in einen mit einem Bootsektorvirus infizierten Computer gelegt wird, wird der Virus im Speicher aktiv und infiziert den Bootsektor der Diskette. Heutzutage gibt es beinahe keine Bootsektorviren mehr, da BIOS und Betriebssysteme meistens einen gut funktionierenden Schutz haben.

### 6.1 AntiCMOS

AntiCMOS ist ein einfacher Bootsektorvirus ohne Stealthfunktionen. Es existieren zwei Varianten, AntiCMOS.A und AntiCMOS.B. Beide unterscheiden sich technisch nur geringfügig, die erste Variante verändert Werte im CMOS, AntiCMOS.B erzeugt Geräusche über den PC-Lautsprecher. Der Virus verbreitet sich nur, wenn versucht wird von einer infizierten Diskette zu booten, d.h. wenn eine infizierte Diskette beim Starten des Computers im Laufwerk A: liegt bzw., wenn auf einem



infizierte Computer eine nicht schreibgeschützte Diskette gelesen oder geschriebene wird.

Größe (auf Disk): 512 Byte = 1 Sektor; Größe (im Speicher): 2 KB, die ersten 512 Byte sind mit der Virusroutine belegt, die 2. 512 werden als Puffer genutzt (darin wird der zu infizierende Bootsektor geladen)

Vorgehen: Zuerst merkt sich der Virus die Einsprungsadresse den INT 13h (Disketten-/Festplatteninterrupt), indem er die Interrupt-Vector Tabelle ausliest. Danach verringert er den zu Verfügung stehenden DOS-Speicher um 2 KB indem er die entsprechende BIOS-Variable [0:413h] um 2 verringert. Der Virus errechnet nun den Einsprungspunkt des nun für ihn reservierten Speichers und kopiert sich selbst (512 Byte) dorthin. Daraufhin springt er zum Segment des Einsprungpunktes, Offset 88h mit Hilfe eines 'RETF'-Befehls, womit die 1. Phase der Installation abgeschlossen ist.

Nun liest der Virus den Bootsektor der Festplatte in seinen Puffer und überschreibt ihn mit seinem eigenen Bootstrap-Loader. Für diese Lese+Schreiboperationen wird die vorher ermittelte Einsprungsadresse des INT 13h verwendet Diese Aufgabe übernimmt eine Subroutine. Nachdem der Virus sich also auf die Festplatte kopiert hat, installiert er seinen eigenen INT 13h - Handler, welcher sämtliche INT 13h - Aufrufe abfängt und versucht Disketten zu infizieren. Danach versucht der Virus die physikalisch 1. Dateien auf dem Datenträger zu lesen, welche unter DOS immer io.sys und msdos.sys darstellen. Da aber die meisten Disketten keine solche Dateien enthalten hängt der Computer beim Bootversuch von einer infizierten Diskette fast immer in einer Endlosschleife.

Wird der Computer aber von einer startfähigen infizierten Festplatte gebootet so wird der Virus diese Dateien dort finden wo er sie erwartet und das System wird fehlerfrei hochgefahren!! Achtung: Es wird keine Kopie des Partitionssektors oder Bootsektor angelegt, der Virus kann also nicht hundertprozentig entfernt werden wenn die Partition nicht mit FDISK /MBR einwandfrei zu reinigen ist. MBRKILL kann diesen Virus jedoch ohne Probleme entfernen.

Während der Aktivierung führt der Virus ein Test durch ob seine Schadensfunktion ausgelöst werden soll. Dieser Test basiert auf einer Abfrage des Systemzeitgebers und einem im Viruscode abgespeicherten 8-Bit Wert. Jedoch hat der Programmierer ein Fehler gemacht, die Bedingung für die Schadensfunktion kann nie erfüllt werden und die Schadensfunktionen werden somit nie aktiviert.

Die Schadensfunktion von AntiCMOS.A würde das Diskettenlaufwerk A: ausschalten und die Festplatten abmelden, AntiCMOS.B hingegen spricht nur den PC Lautsprecher an. Die B-Variante des Virus enthält den Text:

In der A-Variante ist kein Text enthalten. Diese Analyse wurde von Jochen Tuchbreiter und Ralph Roth erstellt (24.10.95).

## 6.2 AntiExe

Alias D3, NewBug oder CMOS4

Dieser Boot- und Partitionssekturvirus (MBR) wurde zum ersten Mal im Frühjahr 1993 in Russland entdeckt und isoliert. AntiExe ist in Deutschland inzwischen stark verbreitet.

VirScan Plus kann nach Booten von einer Systemdiskette diesen Virus von Festplatten und Disketten entfernen. Die Programme ChkPC und QMS können diesen Virus ebenfalls auf Disketten, der Festplatte und im Arbeitsspeicher erkennen.

Infizierung: Der AntiExe Virus wird durch Booten von einer infizierten Diskette aktiv. AntiExe installiert sich dann 1 KB (mit MEM ersichtlich) unterhalb des höchsten Speicherbereiches (z.B. bei 639 KB) und infiziert dann den MBR der Festplatte. Von diesem Zeitpunkt an wird der Disketteninterrupt vom Virus überwacht und entsprechend manipuliert.

Der Virus AntiExe ist in der Lage, den Bootsektor von Disketten und den Partitionssektor der Festplatte zu infizieren. AntiExe kann Diskettenformate von 180 KB bis 1.44 MB (= alle Standarddisketten) in allen Diskettenlaufwerken infizieren. Eine Infektion erfolgt, wenn das Betriebssystem versucht, den Bootsektor zu lesen (DIR A: genügt!). Eine weitere Eigenschaft ist, dass er zu den Stealthviren (Tarnkappenvirus) gehört, weshalb er für den normalen Benutzer unsichtbar ist. Ein Zugriff auf infizierte Datenträger wird vom Virus entsprechend manipuliert, mit dem Erfolg, dass bei einem aktiven Virus selbst ein Virensuchprogramm ausgetrickst wird. Ferner wird der original Interruptvektor 13h auf den Interrupt 0D3h umgelegt, mit dem Erfolg, dass die meisten Antivirenprogramme umgangen werden, die den Interrupt 13h tracen. Dieses "umlegen" des Interrupts ist so effektiv, dass die erste Version von MBR-Kill nicht den AntiExe Virus erkennen oder reinigen konnte.

Schadensfunktionen: Bei Disketten kann es zu Datenverlust (mindestens 1 Sektor) kommen, wenn der Virus den original Bootsektor verschiebt und abspeichert. Laut Anwendern soll das Vorhandensein des Virus auch zu zerstörten FAT's und zerstörten Datenfiles führen, was ich aber nicht bestätigen kann. Ferner kommt es mit Windows im 386'er Modus zu Inkompatibilitäten, weshalb Windows auf das Vorhandensein eines eventuellen Virus hinweist. AntiExe sucht nach einem unbekannten EXE-

Programm, welches die Größe 200256 Bytes hat. Wird auf dieses Programm zugegriffen, wird es vom Virus zerstört. Das Umlegen des Interrupts kann in den seltensten Fällen zu Inkompatibilitäten mit anderer Software führen, die diesen Interruptvektor benötigt.

Entfernung: VirScan Plus kann den Virus von Festplatten und Disketten entfernen. Hierzu benötigen Sie jedoch eine virenfreie Bootdiskette. Weiteres Vorgehen siehe VIRKILL.TXT. Alternativ kann der Virus auch mit dem Programm MBR-Kill entfernt werden. Hierzu wird keine Bootdiskette benötigt. Vorgehensweise siehe MBR-KILL.DOC.

### 6.2.1 Telecom Boot

Telecom Boot stammt vom Anti-Tel Virus ab, jedoch mit dem Unterschied, das Disketten nicht infiziert werden.

Bekannte Varianten:

- Kampana.A
- Kampana.B
- Kampana.C

## 6.3 Anti-Tel

### 5.1 Anti-Tel

Auch bekannt als Telecom Boot, Kampana

Anti-Tel ist ein verschlüsselter Bootvirus mit Tarnkappeneigenschaften, der Disketten und Festplatten infiziert. Der Anti-Tel-Virus wird aktiv, indem er von einer infizierten Diskette gebootet wird. Er installiert sich dann 1 KB (mit MEM sichtbar) unterhalb des höchsten Speicherbereichs. Ab diesem Zeitpunkt überwacht und manipuliert der Virus den Disketteninterrupt.

Anti-Tel ist in der Lage, den Bootsektor von Disketten und den Partitionssektor der Festplatte zu infizieren. Er kann Diskettenformate von 360 KB bis 1,44 MB (= alle Standarddisketten) in allen Diskettenlaufwerken infizieren. Eine Infektion tritt auf, wenn das Betriebssystem versucht, den Bootsektor zu lesen (DIR A: reicht!). Eine weitere Eigenschaft ist, dass er zu den Stealthviren (Tarnkappenviren) gehört, weshalb er für den normalen Benutzer unsichtbar ist. Ein Zugriff auf infizierte Datenträger wird vom Virus entsprechend manipuliert. Selbst ein Virenskanprogramm wird von dem aktiven Virus getäuscht, weshalb vor der Entfernung des Virus ein Kaltstart von einer virenfreien Diskette durchgeführt werden muss.

Der Anti-Tel-Virus verfügt über eine Schadensfunktion, bei der er sich selbst auf den letzten Sektoren der FAT auf Disketten speichert. Dadurch

kann es bei sehr vollen Disketten zu verlorenen Dateien kommen. Intern führt der Virus einen Zähler mit, der bei jedem Bootvorgang erhöht wird. Nach 400 Bootvorgängen wird folgende Nachricht angezeigt:

#### VIRUS ANTITELEFONICA (BARCELONA)

und die ersten beiden Festplatten werden komplett überschrieben! Dies bedeutet, dass alle Daten auf den ersten beiden Festplatten unwiederbringlich gelöscht werden.

Es ist äußerst wichtig, den Anti-Tel-Virus zu bekämpfen, um Datenverluste und die Beschädigung des Systems zu verhindern. Um den Virus zu entfernen, ist es notwendig, einen Kaltstart von einer virenfreien Diskette durchzuführen. Anschließend sollten geeignete Virensuchprogramme verwendet werden, um das System gründlich zu überprüfen und sicherzustellen, dass der Virus vollständig entfernt wurde.

## 6.4 ASBV

Dieser Boot- und Partitionssektorvirus (MBR) wurde vom Programmautor am 19.01.1995 entdeckt und isoliert. Zu diesem Zeitpunkt war noch kein Virensuchprogramm auf dem Markt, welches diesen Virus entdecken konnte. VirScan Plus kann nach Booten von einer Systemdiskette diesen Virus von Festplatten und Disketten entfernen. Das Programm ChkPC kann ab Version 2.38 diesen Virus ebenfalls auf Disketten, der Festplatte und im Arbeitsspeicher erkennen.

Dieser Virus weist starke Ähnlichkeiten zum Parity Check Virus auf. Wahrscheinlich hat dieser Virus als Vorlage gedient.

Infizierung: Der ASBV Virus wird durch Booten von einer infizierten Diskette aktiv. ASBV installiert sich dann 1 KB (mit MEM ersichtlich) unterhalb des höchsten Speicherbereiches. Von diesem Zeitpunkt an werden Disketten- und Keyboardinterrupt vom Virus überwacht und entsprechend manipuliert.

Der Virus ASBV ist in der Lage, den Bootsektor von Disketten und den Partitionssektor der Festplatte zu infizieren. ASBV kann Diskettenformate von 180 KB bis 1.44 MB (= alle Standarddisketten) in allen Diskettenlaufwerken infizieren. Eine Infektion erfolgt, wenn das Betriebssystem versucht, den Bootsektor zu lesen (DIR A: genügt!). Eine weitere Eigenschaft ist, dass er zu den Stealthviren (Tarnkappenvirus) gehört, weshalb er für den normalen Benutzer unsichtbar ist. Ein Zugriff auf infizierte Datenträger wird vom Virus entsprechend manipuliert, mit dem Erfolg, dass bei einem aktiven Virus selbst ein Virensuchprogramm ausgetrickst wird. Als weitere Eigenschaft ist zu erwähnen, dass der "Affengriff" (booten mit Strg-Alt-Entf) vom Virus überwacht wird und gegebenenfalls

simuliert wird, weshalb vor der Entfernung des Virus ein Kaltstart von einer virenfreien Diskette durchgeführt werden muss. VirScan verwendet ein spezielles Verfahren, um eventuelle AKTIVE! Stealthviren auf Disketten entdecken zu können. Wenn Sie laufend den ASBV Virus auf Disketten finden, aber nicht auf der Festplatte, liegt es daran, dass Sie keinen Kaltstart von einer virenfreien Diskette durchgeführt haben!

Weitere bemerkenswerte Eigenschaften: Der Virus hat in seinem Code folgenden Text unverschlüsselt abgespeichert:

```
I'm ASBV  
No System!
```

Der Virus ist sehr trickreich programmiert, er verwendet u. a. 80286 Befehle zur Codeoptimierung. Ferner besitzt er die Fähigkeit tunnelnde Wächterprogramme teilweise zu blocken, weshalb der aktive Virus auch nicht mit FDISK /MBR entfernt werden kann! Weiterhin interessant ist die Rebootroutine, sie überprüft, ob DOS 6.xx aktiv ist, um dann einen Warmstart durchzuführen. Andernfalls wird der Warmstart vom Virus simuliert. Die Abkürzung ASBV könnte für folgendes stehen:

A = Advanced, Amored oder Anti; S = System oder Stealth; BV = Bootvirus

Schadensfunktionen: Intern führt der Virus einen Zähler mit, der zählt, wieviel Lese- und Schreibzugriffe erfolgt sind. Ist der Zähler gleich 1995 (hexadezimal) und es erfolgt ein Diskettenzugriff, wird die Diskette komplett überschrieben. Bei Disketten kann es zu Datenverlust (mindestens 1 Sektor) kommen, wenn der Virus den original Bootsektor verschiebt und abspeichert. Laut Anwendern soll das Vorhandensein des Virus auch zu zerstörten FAT's und zerstörten Datenfiles führen, was ich aber nicht bestätigen kann.

## 6.5 Boot-437

Typ: Bootvirus  
Gefunden: März 1994  
Alias: Bath

Boot-437 war ein häufig verbreiteter, harmloser, einfach aufgebauter, speicherresidenter Bootvirus. Wenn der Rechner von einer infizierten Diskette gestartet wird, kopiert sich der Virus in den DOS Boot Sektor der Festplatte (im Gegensatz zu den meisten Bootviren, die sich stattdessen in den MBR schreiben) und in den Arbeitsspeicher. In weiterer Folge werden alle Disketten befallen, auf die zugegriffen wird.

Schadensfunktion: Boot-437 enthält keine Schadensroutinen oder andere Auswirkungen.

Entfernen: SYS A: und SYS C: oder NoForm.bat von ROSE\_SWE

Siehe auch mein Artikel in Wikipedia:  
<http://de.wikipedia.org/wiki/Boot-437>

## 6.6 DrDemon

Dr Demon (manchmal geschrieben als DR-Demon oder einfach Demon) ist ein klassisches Boot-Sector-Virus, das Anfang der 1990er Jahre auftauchte und MS-DOS-Systeme angriff, die noch von Disketten gestartet wurden. Es gehört zu den „Boot-Viren“, die sich im ersten Sektor einer Festplatte – dem Master Boot Record (MBR) – festsetzen, sodass der schädliche Code ausgeführt wird, bevor das Betriebssystem überhaupt startet.

Der Virus verbreitet sich, wenn eine infizierte Diskette zum Booten verwendet wird oder wenn eine saubere Diskette in einen bereits infizierten Rechner eingesteckt wird. Er kopiert seinen Code in den MBR jedes beschreibbaren Mediums, das er findet, und bleibt bestehen, weil der MBR bei jedem Systemstart ausgeführt wird. Das bedeutet, dass das Virus aktiv bleibt, selbst wenn das Betriebssystem neu installiert wird, solange das infizierte Medium weiterhin angeschlossen ist.

Die meisten Varianten sind relativ harmlos – sie zeigen lediglich eine kurze Textnachricht (oft „Demon“) an und setzen dann den normalen Bootvorgang fort. Einige spätere Versionen fügten jedoch eine destruktive Nutzlast hinzu, die nach einem bestimmten Datum oder nach einer festgelegten Anzahl von Starts Teile der Festplatte überschreibt. Frühe Versionen setzten keine ausgefeilten Tarntechniken ein, sodass die Infektion mit üblichen Festplattenprüfungsprogrammen erkannt werden konnte (z.B. BootVir), die eine abnormale MBR-Größe oder Prüfsumme bemerkten.

Typische Symptome:

- Unerwartete Bootmeldungen – ein kurzer Text erscheint kurz vor dem Laden von DOS.
- Längere Bootzeiten wegen des zusätzlichen Codes im MBR.
- Beschädigte oder fehlende Dateien, falls die destruktive Nutzlast ausgelöst wird.

## 6.7 EDV-Virus

Infiziert alle Floppy-Disk-Bootsektoren und Festplatten-Partitionen. Er kopiert sich 20 KB unter das Speicherende, verringert aber den von DOS oder BIOS gemeldeten Speicher nicht. Der Virus speichert den Original-Bootsektor an Track 39, Head 1, Sektor 8.



Solange der Virus im Speicher ist wird jede saubere Festplatte/ Diskette infiziert. Wie beim Brain-Virus leitet dieser Virus Zugriffe auf den Bootsektor auf das gespeicherte Original um. Zugriff auf infizierte Festplatten ist erst nach dem Entfernen des Virus möglich.

## 6.8 Form-Virus

Der Form-Virus ist der weltweit verbreitetste Bootvirus. Neben dem Parity\_Check.B dürfte Form der am weitesten verbreitetste Bootvirus in Deutschland sein. Seinen Ursprung hat der Form-Virus in der Schweiz (Kanton Zug?). Form infiziert Festplatten- und Disketten Bootsektoren. Im Gegensatz zu den meisten Bootviren infiziert Form nicht den Master Boot Record (MBR) sondern den gerade aktiven (angewählten) Bootsektor der Festplatte, in der Regel also den DOS Bootsektor. D. h. konkret, dass, falls Sie OS/2 oder LINUX "aktiv" installiert haben, der Form sich blind in deren Bootsektor einklinkt, was meistens zu einem Absturz beim Booten oder zu Datenverlust führt.

Infizierte Disketten enthalten einen als BAD-Track markierten Sektor (1 KB), der den Virus-Code und den Original-Bootsektor enthält. Diese Daten werden bei der Festplatte auf dem letzten Track, Sektor und Kopf abgelegt. Der freie Arbeitsspeicher wird - wie beim Stoned-Virus - ebenfalls um 2048 Bytes verringert. Solange der Virus im Speicher ist, wird jede saubere Diskette infiziert. Im Virus (nicht im Bootsektor) erscheint folgender Text:

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

Vom Form-Virus existieren derzeit vier Varianten:

- Headcrash
- Form 18 (2x)
- Form 24

wobei nach meiner Erfahrung der Form 18 (Form.A) der am weitesten verbreitetste ist.

Schadensfunktion: Am 18. bzw. 24. ten jeden Monats (je nach Variante) hängt sich der Virus zusätzlich in den Keyboardinterrupt (nur bei CMOS gepufferter Uhr). Jeder Tastenanschlag wird dann mit einem Ton begleitet. Bei neueren MS-DOS Versionen wird jedoch der Keyboardinterrupt von MS-DOS "abgehängt", so dass man das typische Klicken nicht mehr hört!

Da heutzutage nur noch selten Disketten benötigt werden, ist der Virus so gut wie ausgestorben. Moderne BIOS-Varianten sind zusätzlich mit einem Schutz für das Überschreiben des Harddisk-Bootsektors ausgerüstet.



### 6.8.1 Form.Headcrash

Der Headcrash Virus ist eine veränderte Variante des Form 24-Virus, wird aber von der meisten Virenschanner noch nicht erkannt. Die Schadensfunktion wird am 31. ten ausgelöst! Der Virus wurde um etliche Maschinenbefehle geändert, weshalb ihn nicht alle Virenschanner erkennen! Als Nachricht enthält der Virus jetzt in etwa folgende Meldung:

```
... Headcrash - Harddisk failure at Track 0, Sector 0. No System Disk ...
```

Das Programm CHKPC kann zuverlässig die verschiedenen FORM Varianten erkennen und unterscheiden! Mit dem Programm NOFORM.COM kann der Form-Virus und dessen Varianten von der Festplatte und mit BOOTKILL.EXE von Disketten entfernt werden.

FORM kann mit folgenden Befehlen sehr einfach entfernt werden. Hierzu benötigen Sie eine leere Diskette:

```
format a: /s
a:
sys c:
```

[Diskette entnehmen und Rechner ein/ausschalten]

```
format a:
[Fertig, Virus ist entfernt!]
```

## 6.9 Joshi

Wird eine infizierte Festplatte oder Diskette gebootet, lädt der Virus sich in den Arbeitsspeicher und fängt die Serviceaufrufvektoren (Interrupts) für Tastatur, Zeitgeber, Platte und (ein wenig später) für DOS ab. Der Virus infiziert den MBR bzw. Diskettenbootsektoren der Laufwerke A, B und die ersten zwei physischen Festplatten, wenn auf diesen Laufwerken Eingabe/Ausgabe erfolgt. Der infizierte MBR ist bei normalen Lesezugriffen nicht sichtbar, da das Abbild des ursprünglichen MBR ausgegeben wird (Tarnkappenvirus). Die Tastaturroutine wird vom Virus verwendet, um im Hauptspeicher erhalten zu bleiben, wenn ein Warmstart (Strg+Alt+Entf) durchgeführt wird. Die DOS Serviceaufrufroutine wird verwendet, um am 5. Januar den richtigen Zeitpunkt für die Aktivierung auszuwählen. Am 5. Januar wird auf infizierten Systemen die folgende Nachricht angezeigt: "Type Happy Birthday Joshi!", Es kann erst weitergearbeitet werden, nachdem "*happy birthday joshi*" über die Tastatur eingegeben wurde.

Auf infizierten Disketten befindet sich der Virus im Diskettenbootsektor

und in einer speziell formatierten Zusatzspur, die vom Virus erstellt wird. Mit Hilfe von DISKCOPY oder anderen üblichen Hilfsprogrammen wird kein wahres Abbild der infizierten Diskette erstellt (der größte Teil des Virus und der ursprüngliche Bootsektor fehlen). Von Hilfsprogrammen zur Virusidentifizierung wird dann teilweise angezeigt, dass die Diskette nicht mit dem normalen Virus infiziert ist.

Schadensfunktion: Wird eine Festplatte infiziert, die mit einer früheren Version von FDISK als DOS Version 3.0 partitioniert wurde, überschreibt der Virus einen Teil der FAT mit sich selbst. Dabei spielt es keine Rolle, welche Version von DOS zum Zeitpunkt der Infizierung tatsächlich installiert ist. Ausschlaggebend ist nur, welche Version von FDISK zuletzt zum Partitionieren des Laufwerks verwendet wurde. Ist auf der Festplatte noch genügend freier Speicherplatz verfügbar, werden zunächst keine bemerkbaren Symptome festgestellt. Ist die Festplatte voll, kommt es zu umfangreichen Dateiüberlagerungen und -beschädigungen.

## 6.10 MusicBug

Alias Musican

Ursprung: Taiwan

Der Virus enthält einige Texte:

```
MusicBug v1.06 Macrosoft Corp.
```

und

```
-- Made in Taiwan --
```

Der Virus wurde, ähnlich wie der Azusa Virus, mit einer Treiberdiskette für eine VGA-Karte eines Herstellers aus Taiwan importiert. Die Disketten waren versiegelt und waren schreibgeschützt.

Vier Monate nach der Installation spielt der Virus Musik. Anschließend steuert ein Zufallsgenerator, wann eine Melodie gespielt werden soll. Die Wahrscheinlichkeit liegt bei etwa 14%. Zur Verfügung stehen 8 Töne. Jeweils 38 Töne werden ausgegeben, die zufällig aus den 8 Tönen ausgewählt werden. Der Autor wollte offensichtlich durch die Verzögerung von vier Monaten erreichen, dass der Virus sich stärker ausbreitet.

Der Virus infiziert den Bootsektor von 5,25"-Disketten. Er unterscheidet zwischen 360 KB und 1,2 MB Disketten. 3,5"-Disketten werden ebenfalls infiziert. Der Virus nimmt in jedem Fall an, dass die FAT Einträge 12 Bit lang sind. Festplatten, die FAT Einträge mit 16 Bit langen Einträgen benutzen, können dadurch zerstört werden.

## 6.11 Orge/Disk Killer

Der Disk-Killer ist ein Bootsektor Virus, der sich durch Kopieren in drei Blöcke der Datenträger vermehrt. Dabei ist es dem Virus gleichgültig, ob die Blöcke, in die er sich kopiert, schon von Programmen oder Daten belegt wurden. Diese Blöcke werden in der FAT als schlecht markiert.

Nach der Markierung können die als schlecht markierten Blöcke nicht mehr beschrieben werden. Der Bootsektor wird so geändert, dass beim Booten des Systems der Viruscode zuerst ausgeführt wird. Der Virus kann jede vom System benutzte Diskette infizieren. Er speichert die Aktivitäten des Datenträgers und unternimmt nichts, bis ein vordefiniertes Limit erreicht wird. Dieses Limit ist eine Virusaktivität von 48 Stunden. Da der Virus nicht immer aktiv ist, wird dieses Limit auf den meisten Systemen erst sechs bis acht Wochen nach der Infektion erreicht.

Wird das vordefinierte Limit erreicht oder überschritten und der Rechner neu gebootet, wird ein Text ausgegeben. Danach teilt der Virus dem Anwender mit, ihn jetzt bitte allein zu lassen, um die Sektoren 0 bis 055555 Hex mittels eines XOR Befehls zu ändern. Tatsache ist, dass der Virus zu diesem Zeitpunkt die auf der Festplatte gespeicherten Informationen zerstört. Die einzig wirkungsvolle Maßnahme, nachdem der Disk-Killer Virus aktiv wurde, besteht im neuen Formatieren der Festplatte. Der Text, der während der Aktivität des Virus ausgegeben wird, lässt sich auch im Virus selbst finden:

```
»Disk Killer - Version 1.00 by COMPUTER OGRE 04/01/89. Warning!! Don't turn  
off the power or remove the diskette while Disk Killer is processing! Now  
you can turn off the power. I wish you luck! « _
```

Wichtig ist, dass trotz der ausgegebenen Nachricht der Rechner sofort ausgeschaltet werden sollte. Dabei besteht eine kleine Chance, wenigstens einige Programme oder Daten zu retten.

Der SYS Befehl kann angewendet werden, um den Bootsektor der Platte oder der Diskette wieder herzustellen. Dateien und Programme auf nicht bootfähigen Disketten können durch einen simplen COPY Befehl gerettet werden. Wenn Sie versuchen diesen Virus zu löschen, denken Sie bitte an die allgemeinen Regeln:

Von einer nicht infizierten, sauberen und schreibgeschützten Diskette das System neu booten. Danach erst die Maßnahmen zur Desinfektion ergreifen. Dadurch, dass der Virus bei einer Infektion eine oder mehrere Dateien auf dem Datenträger zerstört hat, reicht es nicht, den Bootsektor einfach neu herzustellen bzw. wieder zu überschreiben. Die zerstörten Daten müssen durch Originaldateien ersetzt werden. Das kann durch Sicherungskopien geschehen, die vor der Zerstörung der drei Blöcke erstellt wurden. Nutzen Sie in diesem Falle nicht den DISKCOPY Befehl.

## 6.12 Ping-Pong

Der Ping-Pong-Virus, auch unter den Namen Boot, Bouncing Ball, Bouncing Dot, Italian, Italian-A oder VeraCruz bekannt, trat erstmals im Jahr 1988 auf und gehört zu den frühesten Computerviren, die sich auf IBM-kompatiblen DOS-Computern verbreiteten. Er wurde erstmals am 1. März 1988 an der Polytechnischen Universität von Turin (Politecnico di Torino) in Italien entdeckt. Er zählt zur Kategorie der Bootsektorviren, die den Master Boot Record (MBR) des Speichermediums infizieren.

Sobald der Ping-Pong-Virus ein System infiziert, überschreibt er den vorhandenen MBR-Code mit seinem eigenen Code. Bei einem Neustart des Computers wird der infizierte MBR in den Arbeitsspeicher geladen, und der Virus aktiviert sich.

Der markanteste Aspekt des Ping-Pong-Virus ist der visuelle Effekt, den er auf dem Bildschirm erzeugt. Ein weißer Punkt, der einem hüpfenden Ball ähnelt, bewegt sich über den Bildschirm und berührt alle vier Ecken. Diese Darstellung diente als erkennbares Zeichen für eine Infektion mit dem Virus.

Trotz der auffälligen visuellen Effekte verursachte der Ping-Pong-Virus in den meisten Fällen keine schwerwiegenden Schäden auf dem infizierten System. Es gab jedoch eine Schwachstelle im Viruscode, die auf bestimmten Prozessoren zu Systemabstürzen führte. Dieser Fehler trat auf '286-Maschinen sowie auf V20-, '386- und höheren Prozessoren aufgrund der Verwendung des Befehls "MOV CS,AX" auf, der nur von '88er und '86er Prozessoren unterstützt wird.

Es ist erwähnenswert, dass in Israel eine Variante des Ping-Pong-Virus aufgetaucht ist, die sich in ihrem Verhalten von der ursprünglichen Version unterschied. Statt eines hüpfenden Balls führte diese Variante typografische Fehler in allen an den Drucker gesendeten Texten ein. Diese Abwandlung verdeutlicht die Anpassungsfähigkeit und Evolution von Computerviren im Laufe der Zeit.

Der Ping-Pong-Virus verbreitete sich zu seiner Zeit schnell und richtete erheblichen Schaden an. Um sich vor dem Ping-Pong-Virus und ähnlichen Bedrohungen zu schützen, war es wichtig, Sicherheitsmaßnahmen zu ergreifen, wie beispielsweise das Vermeiden des Einsatzes unsicherer Disketten oder das regelmäßige Scannen von Speichermedien mit aktualisierter Antivirensoftware.

In der heutigen Zeit ist der Ping-Pong-Virus in den meisten modernen Systemen nicht mehr aktiv, da Sicherheitsmaßnahmen und Antivirensoftware erheblich verbessert wurden, um solche Bedrohungen

zu erkennen und zu beseitigen. Dennoch bleibt der Ping-Pong-Virus ein historisches Beispiel für einen frühen und weit verbreiteten Bootsektorvirus, der sowohl visuelle Effekte als auch spezifische Systemschwachstellen aufwies.

## 6.13 Parity Check/Parity Boot

Alias Quandary, Parity.enc, Parity.Boot.Enc, IHC, Newboot, Newboot\_1, WeRSilly, Quandry, Parity Boot, P-Boot oder Generic Boot

Dieser Boot- und Partitionsvirus wurde vom Programmator am 12.11.1992 entdeckt und isoliert. Zu diesem Zeitpunkt war noch kein Virensuchprogramm auf dem Markt, welches diesen Virus entdecken konnte. VirScan Plus kann nach Booten von einer Systemdiskette diesen Virus von Festplatten und Disketten entfernen. Das Programm ChkPC kann diesen Virus ebenfalls auf Disketten, der Festplatte und im Arbeitsspeicher erkennen.

Zur Zeit existieren drei Varianten von diesem Virus (A, B1 und B2). Anhand der gemeldeten Infektionen (Parity B2) nehme ich an, dass dieser Virus der inzwischen am weitesten verbreitetste Bootvirus in Deutschland ist! Seinen Ursprung soll er in Deutschland haben, entdeckt wurde er jedoch in Australien!

Infizierung: Der Parity Check Virus wird durch Booten von einer infizierten Diskette aktiv. Parity Check installiert sich dann 1 KB (mit MEM ersichtlich) unterhalb des höchsten Speicherbereiches. Von diesem Zeitpunkt an werden Disketten- und Keyboardinterrupt vom Virus überwacht und entsprechend manipuliert.

Der Virus Parity Check ist in der Lage, den Bootsektor von Disketten und den Partitionssektor der Festplatte zu infizieren. Parity Check kann Diskettenformate von 180 KB bis 1.44 MB (= alle Standarddisketten) in allen Diskettenlaufwerken infizieren. Eine Infektion erfolgt, wenn das Betriebssystem versucht, den Bootsektor zu lesen (DIR A: genügt!). Eine weitere Eigenschaft ist, dass er zu den Stealthviren (Tarnkappenvirus) gehört, weshalb er für den normalen Benutzer unsichtbar ist. Ein Zugriff auf infizierte Datenträger wird vom Virus entsprechend manipuliert, mit dem Erfolg, dass bei einem aktiven Virus selbst ein Virensuchprogramm ausgetrickst wird. Als weitere Eigenschaft ist zu erwähnen, dass der "Affengriff" (booten mit Strg-Alt-Entf) vom Virus überwacht wird und gegebenenfalls simuliert wird, weshalb vor der Entfernung des Virus ein Kaltstart von einer virenfreien Diskette durchgeführt werden muss. VirScan verwendet ab der Version 9.33 ein neues Verfahren, um eventuelle AKTIVE!!! Stealthviren auf Disketten entdecken zu können. Wenn Sie laufend den Parity Check Virus auf Disketten finden, aber nicht auf der Festplatte, liegt es daran, dass Sie keinen Kaltstart von einer

virenfreien Diskette durchgeführt haben!

Schadensfunktionen: Ist der Virus aktiv, werden bei jedem Tastendruck die Interruptvektoren 01h und 03h (Debuggerinterrupts) vom Virus überschrieben. Ein Debuggen von Programmen führt beim aktiven Virus zu unvorhersehbaren Programmabstürzen. Intern führt der Virus einen Zähler mit, der zählt, wie viele Disketten erfolgreich infiziert wurden. Übersteigt der Zähler die interne Uhr, wird der Bildschirm gelöscht, die Meldung:

PARITY CHECK



angezeigt und der Rechner wird angehalten. In diesem Fall muss ein RESET durchgeführt werden, wobei der Virus wieder bei Null anfängt zu zählen. Gerade bearbeitete Daten (nicht abgespeicherte) sind somit verloren (Datenverlust!). Bei Disketten kann es zu Datenverlust (mindestens 1 Sektor) kommen, wenn der Virus den original Bootsektor verschiebt und abspeichert. Laut Anwendern soll das Vorhandensein des Virus auch zu zerstörten FAT Tabellen und zerstörten Datenfiles auf der Festplatte führen, was ich aber nicht bestätigen kann. Bei 3,5" DD Disketten wird durch einen Fehler im Virus oft die komplette Diskette zerstört!

## 6.14Quandary

Alias Newboot, Parity.enc

Quandary ist ein Bootvirus, der Tarntechniken (Stealthtechniken) verwendet. Der Virus ist 1 Sektor groß und sitzt im Bootsektor von Disketten und im Partitionssektor (MBR) von Festplatten. Es werden nur 3,5"-HD Disketten befallen. Bei zwei eingebauten Festplatten werden beide infiziert. Der Virus ist teilweise verschlüsselt. Bei der Infektion mit Quandary wird der Originalsektor gesichert im Sektor 15 bei Festplatten und im letzten Sektor des Hauptverzeichnisses bei Disketten.

Die Festplatte wird beim Booten bzw. bei einem Bootversuch von einer verseuchten Diskette infiziert. Bei aktivem Virus zeigt der CHKDSK-Befehl 1024 Bytes weniger konventionellen Hauptspeicher an. Quandary ist ein

Stealthvirus, d.h. er zeigt den original Sektor an, wenn man den Bootsektor bzw. den MBR einliest.

Quandary hat eine programmierte Schadensfunktion, die allerdings nicht ausgeführt wird: Dabei würde der Virus den BIOS -Parameterblock bei Disketten bzw. die Partitionstabelle bei Festplatten und anschließend den gespeicherten Originalsektor überschreiben. Danach hätte man keinerlei Zugriff mehr auf die Daten.

Die Infektion erfolgt über Booten (bzw. Bootversuch) von einer infizierten Diskette. Während des normalen Systemstarts über die infizierte Festplatte wird der Virus speicherresident; er versucht sich im System zu tarnen. Der CHKDSK-Befehl zeigt im infizierten System 1024 Bytes konventionellen Arbeitsspeicher weniger an. Im infizierten System versucht der Virus jede Diskette zu infizieren, auf die zugegriffen wird. Ist der Diskettenschreibschutz aktiv, so bricht der Virus den Infektionsversuch ab.

## 6.15 Stoned

Alias New Zealand, Marihuana, Donald Duck, Sex Revolution, San Diego Deunis, Smithsonia

Dieser schon etwas betagte aus Neuseeland stammende Virus wurde erstmals 1988 in Wellington analysiert und befällt Bootsektoren von Disketten und Festplatten. Er ist unter zahlreichen weiteren Namen, so unter Donald Duck, Sex Revolution, Rostov und einigen mehr im Umlauf. Er diente zig anderen Bootviren als Vorlage, weshalb heute über fünfzig Stoned Varianten existieren!

In seiner Urfassung befällt der Stoned-Virus nur Bootsektoren von 360K-Disketten, bei allen späteren Varianten werden auch Festplatten befallen. Der ursprüngliche Bootsektor wird in Spur 0, Seite 1, Sektor 3 abgespeichert, was für 360 KB Disketten nicht weiter gefährlich ist, bei 1.2 MB Disketten können dadurch allerdings Probleme auftauchen. Auf Festplatten wird der ursprüngliche Bootsektor in Spur 0, Seite 0, Sektor 7 abgelegt. Bei Festplatten können Teile der Partitionstabelle und der FAT durch Stoned zerstört werden.

Wird von einer infizierten Diskette gebootet, so nistet sich der Virus im Speicher ein und verringert diesen um 2 KB (bei Überprüfung mit CHKDSK). Falls die Festplatte noch nicht infiziert wurde, versucht der Virus sich in die Partitionstabelle der Festplatte zu schreiben. Wird von solch einer Festplatte gebootet, installiert sich der Stoned-Virus automatisch. Danach wird jede Diskette, von der eingelesen, oder die beschrieben wird, vom Stoned-Virus befallen. Von Zeit zu Zeit (Systemzeit modulo sieben) gibt der Virus beim Booten von Disketten (nicht beim Booten von der



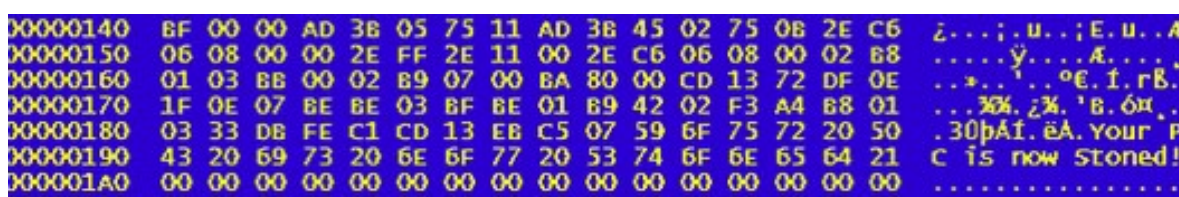
Festplatte), abhängig von der Version des Virus, eine Meldung am Schirm aus, die unterschiedlichen Textinhalt haben kann:

```
"YOUR PC IS STONED NOW!"  
"Your Computer is now stoned!"  
"Your PC is now stoned! LEGALIZE MARIHUANA!"
```

### 6.15.1 Stoned.A

Diese Variante befällt keine Festplatten und wird vielfach als der Urvirus bezeichnet. Wird von einer befallenen Diskette gebootet, erfolgt die Ausgabe folgender Meldung:

```
"Your PC is now stoned! Legalize Marihuana!"
```



00000140	BF 00 00 AD 3B 05 75 11 AD 3B 45 02 75 0B 2E C6	¿...;u...;E.u..A
00000150	06 08 00 00 2E FF 2E 11 00 2E C6 06 08 00 02 B8	....ÿ....A....
00000160	01 03 BB 00 02 B9 07 00 BA 80 00 CD 13 72 DF 0E	..*...'.°E.f.rB.
00000170	1F 0E 07 BE BE 03 BF BE 01 B9 42 02 F3 A4 B8 01	...30%.¿%. 'B.6M.
00000180	03 33 DB FE C1 CD 13 EB C5 07 59 6F 75 72 20 50	.30pAf.ëA.Your P
00000190	43 20 69 73 20 6E 6F 77 20 53 74 6F 6E 65 64 21	C is now Stoned!
000001A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Hexdump des MBRs einer modifizierte Variante

### 6.15.2 Stoned.B

Ist ähnlich aufgebaut wie Stoned-A. Im Unterschied zu Stoned-A kann es zu RLL-Kontroller-Hangs kommen, wenn von einer infizierten Diskette gebootet wird. Außerdem wird die Meldung in etwas anderer Variante ausgegeben:

```
"Your PC is now stoned! LEGALIZE MARIHUANA!"
```

Für beide Variante gilt, dass die Meldung nicht bei jedem Boot-Vorgang ausgegeben wird.

### 6.15.3 Stoned.C

Bei dieser Variante gibt es keine Meldung auf dem Bildschirm.

### 6.15.4 Stoned.D

Diese Variante kann auch Disketten vom Format 3,5" (720 KB, 1,4 MB) und 5,25" (1,2 MB) befallen. Werden diese Formate befallen, kann es zu unwiederbringlichen Schäden kommen.

### 6.15.5 Stoned.E

Ist ähnlich aufgebaut wie Stoned-B und erzeugt bei Aktivierung einen Beep-Ton.

### 6.15.6 Stoned.F

Ist ähnlich wie Stoned-E aufgebaut, erzeugt einen Beep-Ton und gibt folgende Meldung auf dem Bildschirm aus:

```
"Twoj PC jest teraz be!"
```

### 6.15.7 Stoned II

Diese spezielle Variante des Virus nützt ausgeklügelte Techniken, sich gegen Virensuchprogramme zu schützen. Es existieren davon bereits drei Varianten, wovon zwei eine Meldung in ihrem Code enthalten.

```
"Your PC is stoned now! Version 2"  
"Donald Duck is a lie!"
```

Die dritte Variante enthält keine Meldung.

### 6.15.8 Stoned.Azusa

Alias Azusa, Hong Kong

Dieser Virus stammt vermutlich aus Hong Kong und trat im Februar 1991 erstmals in Erscheinung. Er stammt vom Stoned Virus ab. Er befällt Bootsektoren von Disketten und den Partitionssektor von Festplatten. Beim ersten Aufruf installiert er sich speicherresident am oberen Ende der 640 KB-Grenze und verringert den übrigen Arbeitsspeicher um 1024 Bytes. Der original Partitionssektor einer Festplatte wird von Azusa nicht gesichert! Bei einem Schreib-/Lesezugriff auf Disketten wird ein nicht befallener Bootsektor sofort vom Virus überschrieben. Bei 360 KB-Disketten wird der original Bootsektor auf Spur 40 abgelegt, bei High Density-Disketten (1,2 MB, 1,4 MB) und bei 720 KB-Disketten wird er in die Mitte der Diskette gelegt, was unter Umständen zur Zerstörung von Daten führen kann. Azusa führt einen internen Zähler mit, der jeden Bootvorgang von befallenen Disketten und Platten mitprotokolliert. Bei jedem 32. Bootvorgang wird der Zugang zu den Schnittstellen COM1 und LPT1 gesperrt (Druckerausgänge), der interne Zähler wird auf Null gesetzt. Beim nächsten Aufruf (Booten) wird der Zugriff zu den Ports wieder freigegeben.

Von dem Virus gibt es bereits eine Variante

### 6.15.9 Stoned.Hong Kong-2

Diese Variante von Azusa trat im April 1992 erstmals in Erscheinung und verringert den freien Arbeitsspeicher um 2048 Bytes. Im Gegensatz zu seinem Verwandten erzeugt dieser Virus beim Befall von High Density-Disketten schlechte Sektoren und Dateizuordnungsfehlern, die mit CHKDSK nachgewiesen werden können, jedoch keinesfalls mit dem

Parameter "/F" behoben werden dürfen. Weiteres kann es vorkommen, dass die Directory-Einträge auf Null gesetzt werden. Die Betätigung von <CTRL> <ALT> <DEL> oder von <CTRL> <C> kann zu Systemabstürzen führen. COM1 und LPT1 werden nach einem Zufallsprinzip gesperrt.

#### 6.15.10 Stoned.Michelangelo

Der Stoned.Michelangelo-Virus ist ein Computervirus, der erstmals im Jahr 1991 entdeckt wurde. Er ist nach dem berühmten italienischen Bildhauer Michelangelo Buonarroti benannt und erlangte Bekanntheit aufgrund seines potenziellen Schadenspotenzials. Die Verbreitung des Stoned.Michelangelo-Virus erfolgte hauptsächlich über infizierte Disketten, da zu dieser Zeit Disketten ein häufiges Medium für den Datenaustausch waren. Obwohl der Stoned.Michelangelo-Virus in den letzten Jahren an Bedeutung verloren hat, bleibt er ein historisches Beispiel für einen Computervirus, der aufgrund seines potenziellen Schadenspotenzials Aufmerksamkeit erregte.

Die Schadensfunktion des Virus wird am 6. März aktiv, dem Geburtstag von Michelangelo. Der Virus speichert sich in den Bootsektor von Disketten und in den Partitionssektor von Festplatten. Der originale Bootsektor bzw. Partitionssektor wird gesichert. Bei Disketten wird dieser Sektor am Ende des Hauptverzeichnisses abgelegt. Sind dort Verzeichniseinträge vorhanden, werden diese überschrieben; dadurch kann es zu Datenverlusten während der Infektion kommen.

Wird der Rechner am 6. März gestartet, überschreibt der Michelangelo-Virus wichtige Systembereiche und Dateien. Die Festplatte des Rechners muß dann neu eingerichtet werden, die Daten sind in der Regel verloren - vor allem dann, wenn nur eine Partition (nur C:) eingerichtet ist. Die Infektion erfolgt über Booten (bzw. Boot-Versuch) von einer infizierten Diskette. Während des normalen Systemstarts über die infizierte Festplatte wird der Virus speicherresident. Der CHKDSK-Befehl zeigt im infizierten System 2048 Bytes konventionellen Arbeitsspeicher weniger an. Im infizierten System versucht der Virus jede Diskette im Laufwerk A: zu infizieren, auf die zugegriffen wird. Ist der Diskettenschreibschutz aktiv, so bricht der Virus den Versuch ab. Disketten im Laufwerk B: ebenso 720 kByte-3,5"-Disketten werden nicht infiziert. 1,44 MByte-Disketten sind nach der Infektion nicht mehr lesbar. Der Virus Michelangelo wurde erstmals im April 1991 in Schweden und in den Niederlanden entdeckt. Der Michelangelo-Virus basiert auf dem Stoned-Virus, verhält sich jedoch anders in der Infizierung. Michelangelo befällt 5.25 Zoll-Disketten und Festplatten. Bei Festplatten wird der Partitionssektor infiziert. Der freie Arbeitsspeicher wird - wie beim Stoned-Virus - ebenfalls um 2048 Bytes verringert.

Bei 360 KB-Disketten wird der originale Bootsektor im Sektor 11 abgelegt. Bei 1.2 MB-Disketten im Sektor 28 - wo sich das root-Verzeichnis der Diskette befindet. Falls hier Daten standen, werden sie durch den Virus überschrieben!

Schadensfunktion: Am 6. März jedes Jahres wird der Michelangelo-Virus aktiv und versucht die Festplatte mit "Arbeitsspeicherabbildern" zu formatieren.

#### 6.15.11 Stoned.Rostov

Der Ursprung dieses Virus ist unbekannt. Er ist ähnlich wie Stoned-B aufgebaut und enthält folgenden Text im Code:

```
"NON SYSTEM DISK!"
```

#### 6.15.12 Stoned.Sex\_Revolution 1.1 bzw. 2.0

Dieser Virus ist analog zu Stoned-B aufgebaut und enthält folgende Meldung:

```
"EXPORT TO SEX REVOLUTION ver. 1.1"  
"EXPORT TO SEX REVOLUTION ver. 2.0"
```

### 6.16 V-Sign

V-Sign auch bekannt als Cansu und Sigalit ist ein Bootsektorvirus von 1992. Er ist leicht polymorph und zeigt ein Image nach der Infektion von 64 Disketten an.

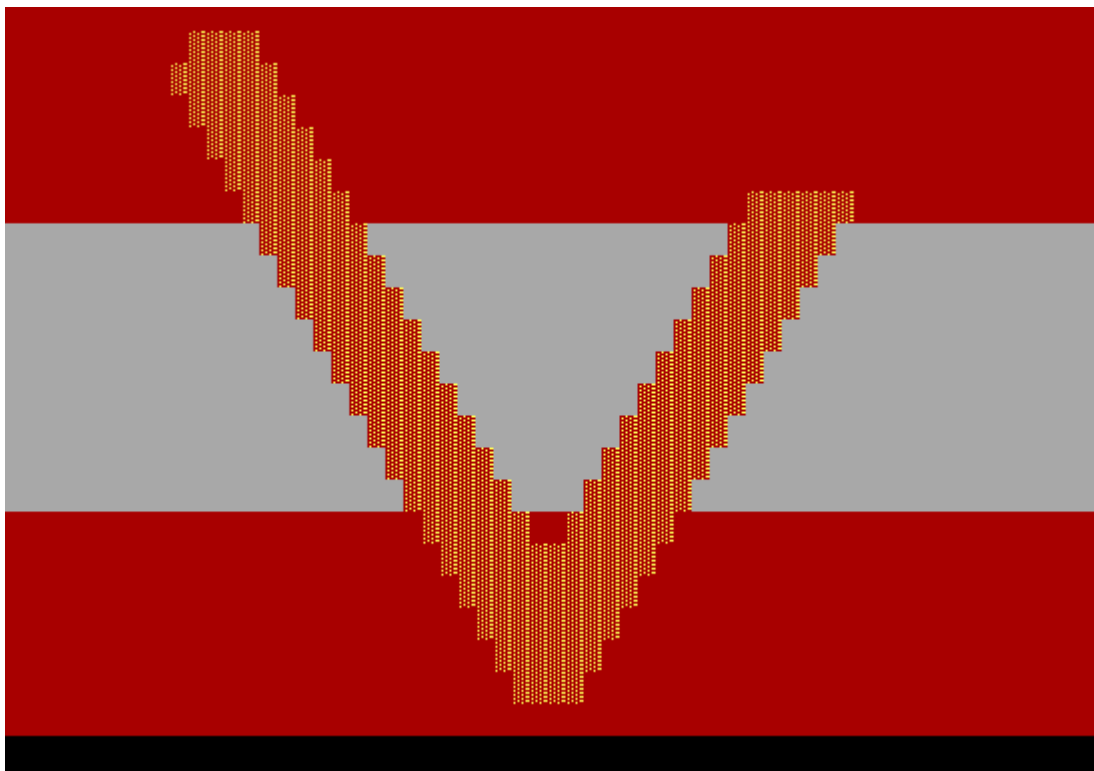
Wenn das System von einer infizierten Diskette gestartet wird, wird V-Sign speicherresident und nimmt 2.048 Bytes ein. Er installiert sich im hohen Speicher, knapp unter der DOS 640k-Grenze. Der Virus infiziert die Festplatte, sobald der Benutzer darauf zugreift.

V-Sign speichert 38 Bytes des Master-Boot-Records in einem eigenen Code, während es Seite 0, Zylinder 0, Sektor 1 überschreibt. Sein Code nimmt zwei weitere Sektoren auf, so dass er den Rest von sich selbst auf Seite 0, Zylinder 0, Sektoren 4 und 5 platziert.

Disketten werden beim Zugriff auf sie infiziert. Es funktioniert genauso wie beim Infizieren einer Festplatte, außer auf der Diskette, speichert er seine beiden anderen Sektoren auf den letzten Sektoren des Stammverzeichnisses der Diskette (Sektoren 10 und 11 auf 360k 5,25 Zoll Disketten zum Beispiel).

Wenn der Virus 64 Disketten infiziert hat, zeigt er sein "V-Sign" an. Zu diesem Zeitpunkt führt dies dazu, dass das System sich aufhängt.

**Name und Herkunft:** V-Sign kommt höchstwahrscheinlich aus der Türkei, aber auch Indien gilt als mögliches Heimatland dieses Virus. Es wurde jedoch erstmals in Kanada berichtet. V-Sign bezieht seinen Namen aus dem Bild, das es anzeigt. Der andere Name, Sigalit, ist hebräisch für die violette Pflanze. Cansu ist ein türkischer weiblicher Name. Fujitsu Deutschland hat den Virus versehentlich in einigen Druckerplatten installiert.



## 6.17WYX

**Wyx** (aka Polyboot, Preboot, Eek.B) ist ein ungefährlicher, speicherresidenter, verschlüsselter Boot-Virus der im November 1997 entdeckt wurde. Es existieren drei Varianten. Der Viruscode besteht aus

zwei Festplattensektoren.

Nach der Aktivierung reduziert WYX den für DOS-Anwendungen verfügbaren Gesamtspeicher um 2 KB und lädt sich dann selbst an den oberen Rand des Speichers (an die 638K Grenze). Der Virus infiziert den MBR des Festplattenlaufwerks und den Bootsektor auf Disketten. Der MBR der Festplatte wird beim Booten von einer infizierten Diskette infiziert. Um andere Laufwerke zu infizieren, greift der Virus auf INT 8 (Timer) zu und prüft mit Verzögerungen, ob andere Laufwerke in Gebrauch sind, und infiziert je nach dem entweder Laufwerk A: oder Laufwerk B:, oder den MBR des Laufwerks C:.

Während er den MBR-Sektor infiziert, deaktiviert der Virus den Virenschutz, indem er das erforderliche Feld im CMOS-Speicher zurücksetzt. Der ursprüngliche MBR, der Bootsektor des Laufwerks C: und der zweite Virussektor werden in den letzten Sektoren der ersten Spur des Festplattenlaufwerks (reservierte Spur), der ursprüngliche Bootsektor von Diskettenlaufwerken ist am Ende der Sektoren des Stammverzeichnisses gespeichert.

Der Virus macht sich in keiner Weise bemerkbar, jedoch aufgrund von Fehlern im Virus kann ein Teil des Bildschirmspeichers während der Ausführung überschrieben werden. Dies kann dazu führen, dass am oberen Rand des Bildschirms unleserliche Daten erscheinen. FAT32-Partitionen können bei der Infektion beschädigen oder zerstören werden.

Er enthält den folgenden Text:

01/09/97 WYX (Variante A)

31/03/98 WYX (Variante B)

20/01/2001 WYX (Variante Polyboot)

## 7 UEFI Bootkits

### 7.1 Windows UEFI Malware

Es gibt eine Reihe von UEFI-Malware, die Windows-Systeme angreift. Einige der bekanntesten Beispiele sind:

- **ESpecter:** Dies war einer der ersten UEFI-Bootkits, die in freier Wildbahn entdeckt wurden. Es wurde verwendet, um Spyware auf den Computern der Opfer zu installieren. ESpecter infiziert den Windows Boot Manager und kann so Malware bereitstellen, bevor das Betriebssystem startet.

- **FinSpy-Bootkit:** Ein weiteres frühes UEFI-Bootkit, FinSpy, ist ein hochentwickeltes Überwachungstool, das von Regierungen und Strafverfolgungsbehörden eingesetzt wird. Seine UEFI-Komponente ermöglicht es ihm, auf infizierten Systemen zu verbleiben und der Erkennung zu entgehen.
- **BlackLotus:** BlackLotus ist vielleicht das berüchtigtste UEFI-Bootkit und ist in der Lage, UEFI Secure Boot selbst auf vollständig aktualisierten Systemen zu umgehen. Es wurde verwendet, um Ransomware und andere Malware bereitzustellen. Es nutzt Schwachstellen in der UEFI-Firmware aus, um sich selbst zu installieren und dauerhaften Zugriff zu erhalten.
- **LoJax:** Diese Malware nutzt eine Schwachstelle in den UEFI/BIOS-Einstellungen aus, um ein bösartiges UEFI-Modul zu installieren. Dadurch kann LoJax die Neuinstallation des Betriebssystems und den Austausch der Festplatte überstehen.
- **MosaicRegressor:** Dieses UEFI-Bootkit wurde bei gezielten Angriffen verwendet, hauptsächlich gegen Regierungs- und diplomatische Einrichtungen. Es verwendete eine komplexe Infektionskette mit mehreren Komponenten.
- **TrickBoot:** Dies ist ein Proof-of-Concept-UEFI-Bootkit, das demonstriert, wie Angreifer Schwachstellen in der UEFI-Firmware ausnutzen könnten, um Hintertüren zu installieren.
- **CosmicStrand:** Dieses hochentwickelte UEFI-Firmware-Rootkit zielt auf Windows-Systeme ab und ist aufgrund seiner Fähigkeit, sich in der Firmware zu verstecken, besonders schwer zu entfernen.

Dies sind nur einige Beispiele für UEFI-Malware, die entdeckt wurde. Es ist wichtig, sich daran zu erinnern, dass ständig neue Bedrohungen auftauchen. Daher ist es wichtig, die Firmware Ihres Systems auf dem neuesten Stand zu halten und die Sicherheitsrichtlinien zu befolgen, um sich selbst zu schützen.

## 7.2 Bootkitty: Der erste UEFI-Bootkit für Linux

Bootkitty ist ein UEFI-Bootkit, das speziell für Linux-Systeme entwickelt wurde. Es handelt sich um einen Proof of Concept, der demonstriert, wie ein UEFI-Bootkit verwendet werden kann, um die Kernel-Signaturprüfung zu deaktivieren und schädliche ELF-Binärdateien zu laden.

### 7.2.1 Funktionsweise:

- Ausführung des Bootkits und Patchen des legitimen GRUB-Bootloaders
- Patchen des EFI-Stub-Loaders des Linux-Kernels



- Patchen des dekomprimierten Linux-Kernel-Images

Bootkitty kann UEFI Secure Boot umgehen, indem es die notwendigen Funktionen im Speicher patcht, die für die Integritätsprüfung verantwortlich sind. . Bootkitty patcht den legitimen GRUB-Bootloader, um die Kontrolle über den Bootvorgang zu übernehmen. . Bootkitty patcht das dekomprimierte Linux-Kernel-Image, um die Kernel-Signaturprüfung zu deaktivieren und schädliche ELF-Binärdateien zu laden. . Bootkitty lädt zwei ELF-Binärdateien über den Linux-Init-Prozess. Diese Binärdateien können verwendet werden, um weitere schädliche Aktionen auszuführen.

#### Wichtige Punkte

- Bootkitty ist der erste UEFI-Bootkit, der Linux-Systeme angreift.
- Bootkitty ist ein Proof of Concept und wurde bisher nicht in freier Wildbahn eingesetzt.
- Bootkitty unterstützt nur eine begrenzte Anzahl von Linux-Systemen.
- Bootkitty ist mit einem selbstsignierten Zertifikat signiert und kann daher nicht auf Systemen mit aktiviertem UEFI Secure Boot ausgeführt werden, es sei denn, die Angreifer-Zertifikate wurden installiert.
- Bootkitty hinterlässt Spuren im System, wie z. B. die Änderung der Kernel-Versions- und Linux-Banner-Strings.

#### 7.2.2 Gefahren und Gegenmaßnahmen:

Bootkitty stellt eine potenzielle Bedrohung für Linux-Systeme dar, da es verwendet werden kann, um die Kontrolle über den Bootvorgang zu übernehmen und schädlichen Code auszuführen. Um Ihre Linux-Systeme vor solchen Bedrohungen zu schützen, stellen Sie sicher, dass UEFI Secure Boot aktiviert ist, Ihre System-Firmware und Ihr Betriebssystem auf dem neuesten Stand sind und Ihre UEFI-Widerrufsliste ebenfalls aktuell ist.

## 8 Ende der Dokumentation