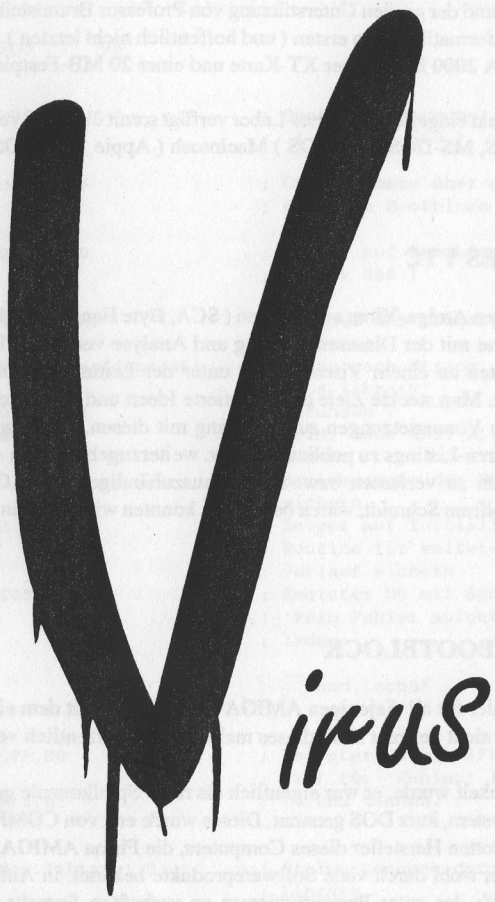
Viren auf dem Amiga



VIREN AUF DEM AMIGA - VTC Universität Hamburg

DAS VTC UND DIE AMIGA-GRUPPE

Sommer 1988 - Professor Dr. Klaus Brunnstein gründet mit ca. 20 Studenten des Fachbereichs Informatik an der Hamburger Universität ein bis zu diesem Zeitpunkt in Deutschland einzigartiges Projekt: das Virus Test Center.

Diesem Viren-Projekt und der großen Unterstützung von Professor Brunnstein ist es zu verdanken, daß der Fachbereich Informatik seinen ersten (und hoffentlich nicht letzten) AMIGA erhält. Ausgerüstet ist der AMIGA 2000 B mit einer XT-Karte und einer 20 MB-Festplatte.

Das eigens für das Projekt eingerichtete Viren-Labor verfügt somit über drei verschiedene Betriebssysteme: AMIGA-DOS, MS-DOS (PC-DOS) MacIntosh (Apple) und TOS (Atari).

GESCHICHTE DES VTC

In einer Zeit als die ersten Amiga-Viren auftauchten (SCA, Byte Bandit), und wir teilweise bereits in unserer Freizeit privat mit der Disassemblierung und Analyse von Viren begannen, wurde ein Treffen der Interessenten an einem Viren-Projekt unter der Leitung des Informatik-Professors Brunnstein veranstaltet. Man steckte Ziele ab, diskutierte Ideen und Ansichten zum Thema Viren und ethisch-moralische Voraussetzungen zum Umgang mit diesen. Als Essenz einigte man sich darauf, weder Viren/Viren-Listings zu publizieren bzw. weiterzugeben, noch Anleitungen zur Programmierung von Viren zu verfassen bzw. Dritten auszuhändigen. Wir, Oliver Meng, Alfred Manthey Rojas und Wolfram Schmidt, waren begeistert, konnten wir doch nun Studium und Hobby kombinieren.

DER STANDARDBOOTBLOCK

Zunächst einmal, soll hier für all diejenigen AMIGA-Besitzer, die mit dem eigentlichen Sinn und Zweck des Bootblocks nicht vertraut sind, dieses mal kurz und hoffentlich verständlich erklären.

Als der AMIGA entwickelt wurde, er war eigentlich als reine Spielkonsole geplant, besaß er kein Disketten-Operationssystem, kurz DOS genannt. Dieses wurde erst von COMMODORE, nachdem diese den nahezu bankrotten Hersteller dieses Computers, die Firma AMIGA, aufkaufte, bei METACOMCO, fast jedem wohl durch viele Softwareprodukte bekannt, in Auftrag gegeben. Diese programmierte mit Hilfe der unter Programmierern so verhaßten Sprache BCPL, das heutige AMIGA-DOS als einen Ableger des Multitasking-Betriebssystems TRIPOS. Mit anderen Worten, das DOS wurde dem AMIGA angeflickt und war nicht wie das restliche Betriebssystem in C oder Assembler programmiert.

Diesem Flickwerk ist es zu verdanken, daß heute im Standard-Bootblock einer bootfähigen Diskette ein Programm stehen muß, das das Vorhandensein der DOS-Library abprüft, und falls die Suche positiv verlaufen ist, das DOS initialisiert, während andere Libraries entweder längst initialisiert sind, oder aber erst bei Bedarf nachgeladen werden (siehe LIBS-Verzeichnis auf der WORKBENCH-Diskette).

Hier nun zunächst einmal der Standard-Bootblock einer bootfähigen Diskette als Assembler-Listing im MC 68000-Standardcode sowie als ASCII-Dump, wie ihn der CLI-Befehl 'INSTALL' erstellt:

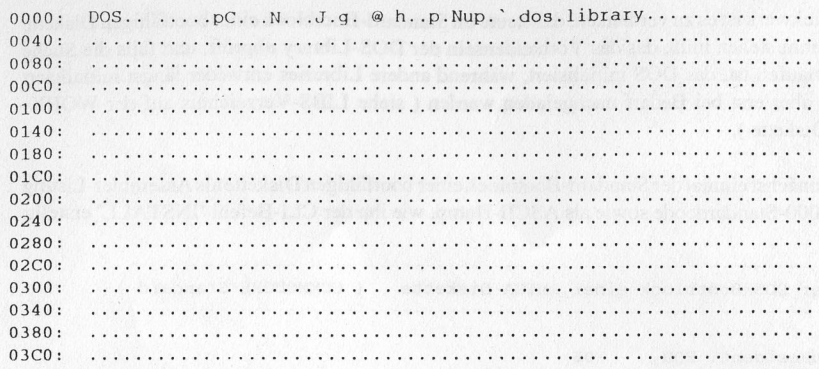
```
------------------------------------------------------------------------
Normaler DOS-Bootblock einer AMIGA-Diskette   ( COMMODORE-Standard )
------------------------------------------------------------------------

LVOFindResident: EQU     -96

DOS:
        dc.b    'DOS',0                 ; Bootblock-Kennung
                                        ;  ( 'DOS' + $00 )
BootChkSum:
        dc.l    $c0200f19               ; Check-Summme über den
                                        ; gesamten Bootblock
RootPointer:
        dc.l    $00000370               ; Zeiger auf Rootblock
                                        ;( Block 880 )
DOSTest:
        lea     DOSName,A1              ; Adresse des Library-Namen
                                        ; ermitteln
        jsr     LVOFindResident(A6)     ; Suche nach String
                                        ; 'dos.library'
        tst.l   D0                      ; gefunden ?
        beq.s   ResError                ; Nein, dann EXIT mit Fehler
                                        ; sonnst
        move.l  D0,A0                   ; Basisadresse der DOS-Library
                                        ; sichern
        move.l  22(A0),A0               ; Zeiger auf Initialisierungs-
                                        ; Routine für weiteren Boot-
                                        ; verlauf sichern
        moveq   #$00,D0                 ; Register D0 mit $00 für
                                        ; 'kein Fehler aufgetreten'
                                        ; laden
Return:
        rts                             ; ...und tschüß...

ResError:
        moveq   #$FF,D0                 ; Register D0 mit $FF ( dez.
                                        ; -1 ) für 'Fehler' laden
        bra.s   Return                  ; ...und tschüß...

DOSName:
        dc.b    'dos.library',0         ; String-Kennung der DOS-
                                        ; Library
```



Daß das Entwickler-Team nun aber gleich zwei Sektoren a 512 Byte, auch Blöcke genannt, reservierte, ist eigentlich rätselhaft, denn einer hätte es auch getan, um die 50 Byte, die die Bootblock-Routine belegt, aufzunehmen. Viren-Programmierer hätten es heute ungleich schwerer, so kurze Bootblock-Viren zu realisieren. Nun ja, Viren waren damals noch kein Thema...

Bootblock-Viren haben deswegen die Eigenschaft diese Such-Routine in sich zu beinhalten, was in den weiter unten abgedruckten ASCII-Dumps an den Strings 'dos.library' zu erkennen ist.

Bootblock-Viren verbreiten sich, wie der Name schon sagt, über den Bootblock einer Diskette, während Link-Viren Programm-Files befallen, wie zum Beispiel der IRQ-Virus. Dieser Typ von Viren ist deshalb so gefährlich, weil er nicht mehr so eindeutig und einfach zu lokalisieren ist, wie seine im Bootblock beherbergten 'Kollegen'.

Dank des komplexen AMIGA-Betriebssystems mit seinen Multitasking-Eigenschaften, sind wir bisher lange Zeit von dieser Virenart verschont geblieben. Die Programmierung solcher Viren erfordert nämlich schon eine Menge mehr an Wissen und Können, als die von Bootblock-Viren, wo es keine Probleme wie die Berücksichtigung von Hunks gibt (das sind Informationstabellen vor, im und hinter dem eigentlichen Programm, die dem Betriebssystem Auskunft über den Programmtyp, die zu benutzende Speicherart, usw. geben). Es ist aber so gut wie sicher, daß es immer wieder Programmierer geben wird, die, aus reinem Geltungsbedürfnis heraus, neue spitzfindigere Viren erstellen werden. Viele dieser Programmierer sollten ihre Fähigkeiten lieber durch nützlichere Programme unter Beweis stellen, als anderen Computerbesitzern das Leben schwer zu machen.

Das zum Thema Viren-Programmierer...

Ein weiterer wichtiger Punkt in Sachen 'Viren', ist das gleichgültige Verhalten der Firma COMMODORE, die trotz der Tatsache, daß der AMIGA prädestiniert ist für einen Virenbefall, auch mit der WORKBENCH 1.3 und neuerdings auch 2.0 nichts unternommen hat, um dem AMIGA-Neuling ein wenig unter die Arme zu greifen. Während eine Vielzahl von mehr oder weniger guten 'Virenkillern', die teilweise viel zu teuer und oft absolut unzuverlässig sind, existiert, erachtet COMMODORE es anscheinend nicht für nötig mal etwas in dieser Richtung zu unternehmen. Es gibt kein Programm auf der WORKBENCH- oder der AMIGA-Extras-Diskette, mit dem man den Bootblock betrachten kann, oder das eine Veränderung der System-Vektoren meldet. Warum nicht ? Das Wort 'Virus' selbst taucht z.B. nur einmal völlig nichtssagend im Workbench 1.3-Handbuch zum AMIGA-DOS auf. Dort steht auf Seite 2-22, in der Erklärung des 'Install'-Befehls, folgendes Zitat:

'INSTALL CHECK liefert den Fehlercode 5, wenn der Boot-Block keinen Neustart-Code enthält, und den Fehlercode 10, wenn ein (virusverdächtiger) Nicht-Standard-Boot-Block vorgefunden wird.'.

Was ist aber nun mit Viren, die einen Standard-Bootblock nur vortäuschen, oder solche, die sich nach dem Installieren des Bootblocks sofort wieder in diesen hineinschreiben ? Was ist mit den zig AMIGA-Besitzern, die aus reiner Unwissenheit ihre Disketten nie schreibschützen und eines Tages mit Entsetzen feststellen, daß ihre Original-Software nicht mehr funktioniert, oder daß ihr Rechner plötzlich häufiger ohne Grund abstürzt ?

Nun, aus genau diesem Grunde haben wir uns dazu entschlossen, Viren auf dem Amiga zu erforschen, zu katalogisieren und dieses der Öffentlichkeit zugänglich zu machen.

VERBREITUNGSARTEN EINIGER BOOTBLOCK-VIREN

Die erste Kategorie von Bootblock-Viren reproduziert sich 'nur' bei einem Reset mit ungesicherter Diskette im Boot-Laufwerk, in der Regel DF0:, falls keine Veränderungen vorgenommen wurden, z.B. durch Einsatz eines software- oder hardwaremäßigen Boot-Selektors, und auch 'nur' auf bootfähige Disketten.

Beispiele:

AEK	BAMIGA SECTOR ONE	BUTONIC 1.1
GADDAFI	GYROS	LSD
NORTH STAR 1	NORTH STAR 2	OBELISK
SCA	SYSTEM Z 3.0	SYSTEM Z 4.0
SYSTEM Z 5.0	SYSTEM Z 5.1	SYSTEM Z 5.3

Die zweite Kategorie reproduziert sich wie die erste Kategorie von Bootblock-Viren, und zusätzlich bei jeder Schreib-/Lese-Operation eines angeschlossenen Laufwerks auf ungesichert eingelegte Disketten, selbst, wenn die Diskette weder bootfähig noch formatiert ist.

Beispiele:

BYTE BANDIT	BYTE BANDIT PLUS	BYTE WARRIOR
CLAAS ABRAHAM	DISKDOKTORS	JOSHUA
LAMER 1.0	LAMER 2.0	LAMER 3.0
PARAMOUNT	PENTAGON CIRCLE	REVENGE 1.2
VKILL 1.0	W.A.F.T.	

An dieser Stelle der Hinweis, daß bereits das Einlegen einer Diskette in ein Laufwerk eine Lese-Operation hervorruft.

Das Betriebssystem des AMIGA prüft nämlich alle zweieinhalb Sekunden, ob eine Diskette in ein leeres Laufwerk eingelegt wurde. Ist das der Fall, dann wird unter anderem der Name der eingelegten Diskette, der verbleibende Disketten-Speicherplatz, sowie die Anzahl der Fehler auf der Diskette, eingelesen. Nun wird alle halbe Sekunde überprüft, ob die eingelegte Diskette aus dem Laufwerk entfernt wurde. Trifft das zu, so beginnt der eben beschriebene Vorgang erneut.

Folglich nützt bei der zweiten Fortpflanzungsmethode weder ein Installieren eines neuen Bootblocks (mittels CLI-Befehl 'Install'), noch das Formatieren einer Diskette, noch ein erneutes Über-Kopieren der verseuchten Diskette, solange der Virus aktiv ist. Die Original-Diskette braucht nicht einmal verseucht zu sein, es reicht schon, daß der Virus sich im Speicher befindet. Nach dem Installieren, Formatieren oder Kopieren einer Diskette, schreibt der Virus sich sofort auf den Bootblock derjenigen Diskette, die gerade nicht schreibgeschützt ist, und das muß bei jedem der drei Vorgänge mindestens eine Diskette sein (Formatieren einer schreibgeschützten Diskette funktioniert ja bekanntlich nicht...). Beim Kopieren einer Diskette mit ungesicherter Original-Diskette kann es somit zu einer Infektion derselben kommen, und das kann fatale Folgen haben. Nämlich dann, wenn es sich bei der Diskette um eine mit Bootblock-Lader handelt.

Was ist ein 'Bootblock-Lader' denn nun schon wieder ?

Bootblock-Lader sind Programme, die im Bootblock 'liegen' und die Aufgabe haben, irgendwelche Daten irgendwoher von der Diskette zu laden. Dabei wird meist auf das AMIGA-Diskettenformat verzichtet, d.h. es gibt anscheinend keine Programme und Verzeichnisse auf so einer Diskette. Solch eine Diskette wird beim Einlegen nach dem Starten der WORKBENCH, vom Betriebssystem als 'NOT A DOS DISK' moniert, sie ist ja nicht im AMIGA-Diskettenformat beschrieben. Nur durch diesen speziellen Bootblock mit dem gewissen Ladeprogramm ist es möglich, etwas mit der Diskette anzufangen, und das auch nur, wenn mit dieser Diskette auch gebootet wird. Ansonsten wird das Ladeprogramm im Bootblock ja nicht ausgeführt !

Wird nun ein solcher spezieller Bootblock durch einen Virus überschrieben, so besteht keine Möglichkeit mehr an die Daten auf der Diskette ranzukommen, außer man besitzt noch ein unverseuchtes Original, von dem man dann erneut, nach Eliminieren des Virus' (wie auch immer), eine Kopie macht. Wehe, wenn es das Original war, das verseucht wurde. Wehe, wenn keine Kopie bestand...

'Ich habe keine Viren, weil ich keine Raubkopien besitze.'

So etwas hört man immer wieder. Wie kann man nur so blauäugig sein ? Ein Virus unterscheidet nun mal nicht zwischen Raubkopie und Original. Ja, es sind schon Fälle bekannt geworden, bei denen namhafte Software-Firmen unwissentlich virenverseuchte Produkte auslieferten, und woher weiß man, daß die 50 Public Domain-Disks, die man neulich aus 9. Hand erstanden hat, nicht auch virenbefallen sind ?

Alles klar ?!?!

Es folgt nun eine Übersicht einiger uns bekannter Viren mit einer kurzen Beschreibung und dem ASCII-Dump zur Veranschaulichung. Dabei sollte aber auf jeden Fall berücksichtigt werden, daß einige Viren anhand eines Dumps kaum zu erkennen sind, weil sie kodiert vorliegen.

MERKMALE DER BEKANNTEN VIREN

HINWEIS:
Alle unten aufgeführten Viren sind nach einem Reset weiterhin aktiv, also infektiös, da sie mit Hilfe verschiedener System-Vektoren (dem ColdCapture- und/oder dem CoolCapture-Vektor und/oder dem KickTagPointer) dem Betriebssystem angelagert, und als resident, d.h. als resetfest, gekennzeichnet werden. Ein Entfernen ist nur mit speziellen Programmen, sogenannten Virus-Detektoren oder aber, zuverlässiger, durch Ausschalten des Rechners möglich. Letztere Methode zieht aber zwangsläufig einen totalen Datenverlust nach sich.

Leider haben wir es nicht geschafft alle Virenbeschreibungen fertigzustellen. Dies wird bei Gelegenheit nachgeholt werden. Bis dahin kann unter der am Ende dieses Artikels aufgeführten Adresse des VTC unser englischer Virenkatalog unter Einsendung von Rückporto angefordert werden. Für weitere Informationen, lesen Sie bitte die letzten Absätze dieses Artikels.

AEK-VIRUS

Eine besonders einfallslose Modifikation des SCA-Virus': Irgendein besonders ''fähiger Programmierer'' nahm sich den SCA-Virus mit Hilfe eines Disketten-Monitors vor und änderte mit einer programmiererischen ''Glanzleistung'' den Text (!!!), wobei er aber nicht in der Lage war das Kürzel des Programmierers (''CHW!'') zu entfernen. Außerdem ist in der Virus-Meldung davon die Rede, der Virus sei von 'ihnen' programmiert worden, es sei 'ihr großer Virus' ! Wenn das keine Dreistig-keit ist !!!

Dieser Virus ist bis auf den geänderten Text mit dem weiter unten beschriebenen SCA-Virus identisch und wird in einigen Veröffentlichungen auch 'Micro-Master'-Virus genannt.

Bootblock:

```
0000:  DOS.k.t.CHW!A...C.....0<..".Q...N.....C...,y....N... @ h..p.Nu,y
0040:  .....9......f.B...a..<K.....;|.`..p2a..F`.a...A........:g.#..:..
0080:  ..-H.:Nu-|...>..A.."B@r..XQ...F@0.Nu.......$f....(g.N.....B.N...
00C0:  ....DOS.f0-y.....:B.....H...K.....A..... .....g.(Ia...L.?.Nu.y..
0100:  .....y......09.....@...@..f.a..R"L3|....,y....N..8"L3|....#|....
0140:  .$#|.....(#|.....,,y....N..8"L3|....,y....N..8Nu"LB..$3|....,y..
0180:  ..N..8G.....C.....B.,y....N...#.....",y....N..:A.....'H..p.2<.@
01C0:  4<..,y....N..z+|......;|....pda...E.....A.....#.....0<..B.Q...;|
0200:  .u..;|....;|.8..;|....B...;|....B...;|...."KB...rQ,y....N..."KB.
0240:  ......gP JE...,y....N...t.2<..p.a..J;A...A."Q...B...a..6t.p.a...
0280:  .A.";A..Q...B...a...`..R y....+h.&..;|....Nu.@.-....f..-....g.Q.
02C0:  ..Nu........p......bt.......u.............Q.............D....gr
0300:  aphics.library.dos.library..  Another Future of programming  ..-
0340:  .has begun on Amiga !!!!..A.   Don't worry ....PP..  about our g
0380:  reat V I R U S !!! 2Z. Spread by ....x2. Micro-Master of CCW  .2
03C0:  2. and Odie from AEK !!!.n..N.....A.@..%.................,..%G...
```

BYTE BANDIT-VIRUS

Der BYTE BANDIT-Virus läuft auf 512 KB-AMIGAS einwandfrei, auf solchen mit Speichererweiterung nur, wenn es sich dabei um sogenannte C000000-Erweiterungen handelt, wie z.B. die Original-COMMODORE-Erweiterungen. Auf einem AMIGA 1000 mit 2 MB-Golem-Erweiterung lockte dieser Virus lediglich den Guru hervor, mit dem Effekt, daß ab und zu die Exec-Struktur so zerstört ist, daß nur ein erneutes 'Hochfahren' der KICKSTART-Diskette übrig bleibt.

Fortpflanzung:

Bei jeder Schreib-/Lese-Operation eines angeschlossenen Laufwerks mit ungesicherten Disketten.

Effekt:

Bildschirm wird nach einer gewissen Zeit abgeschaltet, der Rechner scheint blockiert. Durch Drücken einer Tasten-Kombination (Left-ALT, Left-AMIGA, SPACE, Right-AMIGA, Right-ALT) wird diese Blockade wieder aufgehoben und ein Weiterarbeiten mit dem Computer ist wieder möglich. Der Virus ist aber weiterhin aktiv !!! Hierbei handelt es sich offensichtlich um ein Hintertürschen des Programmierers, falls er selbst einmal in die unangenehme Situation kommen sollte.

Bootblock:

```
0000:  DOS.8=#...>``..>Virus by Byte   Bandit in  9.87.Number of
0040:  copys :....{H...,x..3.@.........&0.........|..f..@A..B P"h..*I
0080:  A...E..H....f.A..p .A..".....N.A..,B. . .a..>a...C...N...J.g..$
00C0:   @ h.......&l.3....... <....L...Nu <....`.3.@.........&H... <..
0100:  .."<....N..:A... .A..'C...N...J.g. @I...K...*.A...(. ...A... .A.
0140:  ..-H.......&l.3.......L...NuA...C... .B...-H.&2.J.#I..E...#J...|
0180:  .....|.!...|.....|....G...#K..#|......G...#K..N...-@.*Nu ).,....
01C0:  ..f....)...<..g..2.<..f.../. i...(.A _.......9........g.......g.
0200:  ..H.@.,x..3.@.........&.|....&i.($K.......$g.. &z..#K.(#|.....$
0240:  A...C.......f.$KA...C..x....f. K2<..B...d...R.Q...F."+....d.....
0280:  ....'A..A..D.P..g....P..0..|..e...0...A.............&l.3.......
02C0:  L... z..N.K....U..f..&K....U..f...K.............R.e...a...*z..N.
0300:  3.@.........&H...3.......K...B.K....9........g..9.....9.@....F.
0340:  ..2<..3.......Q....9.........f.....g...`.3.......L........&l.3.
0380:  ......NuA..F0..|..d....P..,x..a..JNu0...`.df@ge.trackdisk.device
03C0:  .dos.library.....................................................
```

BYTE WARRIOR-VIRUS

Der BYTE WARRIOR-Virus, in einigen Zeitschriften auch 'DASA'-Virus genannt, was wohl an der zufälligen Zeichenkombination im Bootblock liegt, ist als einer der ersten Versuche zu werten, ein Anti-Virus-Programm zu schreiben, das sich selbst reproduziert. Fragt sich nun was besser ist, ein Virus, der meine Disketten verseucht und eventuell Disketten mit Bootblockladern zerstört, oder ein Anti-Virus, der denselben Schaden anrichtet...

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

Der BYTE WARRIOR-Virus legt übrigens nach seiner Aktivierung von Speicheradresse $0007FC00 bis $0007FC95 folgenden Text ab:

```
Virus detector by the mighty Byte Warrior!!!  Please, please,
please don't install this disk, coz I want to travel!  Spread
the bootblock and the word!
```

Fortpflanzung:

Bei jeder Schreib-/Lese-Operation eines angeschlossenen Laufwerks mit ungesicherten Disketten.

Effekt:

Man muß in folgende zwei Fälle unterscheiden:

1. BYTE WARRIOR befindet sich bereits im System:

   Flimmern der Power-LED und Tonfolge beim Einlegen einer Diskette, in deren Bootblock sich ein Virus befindet, der den ColdCapture- und/oder den CoolCapture-Vektor verändert, wie z.B. der SCA-, der AEK-, der OBELISK-, der NORTH STAR I-, der NORTH STAR II- und der GYROS-Virus.

2. BYTE WARRIOR befindet sich noch nicht im System und wird vom Bootblock geladen:

   Nun erkennt er lediglich noch den SCA-Virus und dessen Abkömmlinge. Der GYROS-, OBELISK-, NORTH STAR I- und NORTH STAR II-Virus werden nicht mehr erkannt.

ACHTUNG !!!

Aufrund eines Programmierfehlers unterscheidet der BYTE WARRIOR nicht, ob es sich bei einer Schreib-/Leseoperation um eine Operation eines Diskettenlaufwerks (hierfür zuständig: das TRACKDISK.DEVICE) oder um eine Operation eines anderen 'Devices' handelt. Dadurch, daß fast alle Peripherie-Geräte des Amiga über diese sogenanntem Devices angesteuert werden (Programme, die die Kommunikation mit den Peripherie-Geräten übernehmen), führt auch dazu, daß der BYTE WARRIOR die ersten Sektoren einer Festplatte überschrieben kann, was bei nicht-autobootfähigen Festplatten dazu führen kann, daß wichtige Daten überschrieben werden. Diese Daten können die Einteilung der Festplatte u.ä. enthalten. Da es hierfür keinen Festplatten-Standard gibt, geht jeder Festplattenanbieter seinen eigenen Weg diese lebenswichtigen Daten irgendwo auf der Platte unterzubringen. Manche Anbieter benutzen dazu den bei nicht-autobootfähigen Festplatten unbenutzten Bootblock.
Sollte nun eine Infektion durch den BYTE WARRIOR oder einen anderen Virus stattfinden, so ist es durch etwas Aufwand und Wissen jedoch durchaus möglich, den Original-Bootblock, der allerdings keine 'Bootblock-Daten' enthält, zu restaurieren.

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

Bootblock:

```
0000:  DOS.d.m....YH...a...L...C...N...J.g... @ h..p.Nup.Nudos.library.
0040:   |....C...0<.. .Q... |...f"|....0<...........Q...J..*f...J...g.
0080:  ..N.....,y.....|...L.&N...-@.*-|...n.:NuB..*B...0<..A.."BA.XQ...
00C0:  DASA0.2<..........0<0.Q...........0<0.Q...Q...#....b....3.......
0100:  3..?....3.......0<..N....R0<..N....R0<..N....R0<..N....R0<..N...
0140:  .R3.......Nu...T....J....T.....!.............TJ..*f...J...g...N.
0180:  .....)....g....)....f..........$g..........$f...J..,f...J..(g...
01C0:  3.......#..(....#..,....#..$....#.. .... i.....A.....9......g..N
0200:  #|.....(3|....#|.....$#|.....,N.....3y......#y.....(#y.....,#y..
0240:  ...$#y..... N.....3.....0<..Q...Nu....M.lTd...\..\.l..4.\.......
0280:  \4..4\..E.ll..l....}...d...|...d...|...d.....\...d\....\..d...d
02C0:  .....,...D..\.\..\l.L....e|l....\......\..........\...D.l.......
0300:  ................................................................
0340:  ................................................................
0380:  ................................................................
03C0:  ................................................................
```

DISK DOKTORS-VIRUS

Fortpflanzung:

Bei jeder Schreib-/Lese-Operation eines angeschlossenen Laufwerks mit ungesicherten Disketten.

Effekt:

Erstellt einen eigenen Task, den er zu Tarnzwecken 'clipboard.device' nennt und verhindert somit, durch einen Virus-Protektor, der im Multitasking-Betrieb arbeitet, aus dem System 'geworfen' zu werden. Außerdem setzt er im 'WarmCapture'-Vektor eine Marke, die einen gewissen 'Viruskiller' veranlaßt anzunehmen, das System sei virenfrei.
Nach 2000 erfolgreichen Infektionen formattiert er die eingelegte ungesicherte Diskette !

Bootblock:

```
0000:  DOS.@.U.....,y....N...B....6.......40<..Q....y......f. <....S.f.
0040:  .......4`xN... n.*.hBM..gh,y.... <....."<....N..:A..` .gJ"P$IA...
0080:  0<.."..Q...N...A...C..."..A..."..A..."..A..4"..A..."..A..PB.B.a..4A...
00C0:  R.C...,y....N... @ h..p.NuH...,y....a...m\A...R. :........g.....
0100:  _.fBN..........`m4f..........9.u....f.N..... :..B..9......H@J@g.
0140:  L.?.NuL.?.N.....N.....H...a..P$i..$j....tracf...J..,f..x.i....g.
0180:  ...i....g..i....g.`..Z,y....3|....N.....J.. f@A...R. .....H@J@f.
01C0:  a2an3|....A..4#H.(#|.....$#|.....,,y....N.....L.?.Nua...m`3|....
0200:  #|.....$#|.....,#|.....(,y....N............$f..h`.A... .....E...
0240:   <...."<....D...$...Q... .Nu,y....-z.,.*-z.*..N.BM,y.... <...."z
0280:  .PN..4A..zR.......m. ...(."<....N..:A..`B.`B-z...*-z.....|...2-z
02C0:  ...:a.m.-z....A.."B@r..XQ...F@0.NuA.........Nu,y....C...E..t#J.:
0300:  E..`#J.>#J.6.|.....|....E...#J..E...G.....N...`..|,y.... z.fN. <
0340:  ...."<....N..:J.g.A..P . @C..."<.... ...Q...C... z.2N..FG..2J.g.
0380:  N... z..N.....`....<...R...0..........[.........dos.library...cl
03C0:  ipboard.device.........} (C)rackright by Disk-Doktors      ......
```


(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

GADDAFI-VIRUS

Der GADDAFI-Virus ist ein direkter Nachkomme des BYTE WARRIOR-Virus, allerdings mit mehr oder weniger großen Änderungen. Die Meldung, das Verbreiten sei verboten steht im Gegensatz zum angebotenen Update-Service unter der dort aufgeführten Telefonnummer, oder ???

Nein, nein, diese Nummer ist ein Witz: Es handelt sich hierbei um die Telefonnummer der österreichischen Lottozentrale, was den Rückschluß auf die Nationalität des Programmierers erlaubt...

Fortpflanzung:

Bei jeder Schreib-/Lese-Operation eines angeschlossenen Laufwerks mit ungesicherten Disketten.

Effekt:

Nach 7 Resets produziert der GADDAFI-Virus mit Hilfe der Schreib-/Leseköpfe der angeschlossenen Laufwerke Geräusche, indem er diese vibrieren läßt. Nicht besonders gesund für's Laufwerk... Dieser Zustand kann nur durch einen Reset verlassen werden, wodurch der GADDAFI-Virus sich selbst zerstört, d.h. danach ist er nicht mehr aktiv.

Bootblock:

```
0000:  DOS..F.....pa...C...N...J.g... @ h..p.Nup.Nudos.library.
0040:  GADAFFI VIRUS ! Spreading strictly forbitten !!!(c)88 JG
0080:                  For UpdateSevice call:0222/1597 Have FUN...
00C0:   |....C..80<.. .Q...3.......a...a..FNuB..*-|.....2<..A.."B@.XQ.
0100:  ..D@.@..0.-|...$.&N...-@.*-|...F.:Nu...,....J....,...(.!........
0140:  ......N............$g..........$f...J..,f..xJ..(g..p.)....g....)
0180:  ....f..\3.......#..(....#..,....#..$....#.. ....a..6N.....3y....
01C0:  ..#y.....(#y.....,#y.....$#y..... N..... i.....A.....9......g...
0200:  #|.....(3|....#|.....$#|.....,Nua...`....y.......y......b...Nu,y
0240:  ....N..|3.@.....3.......,y....3.......-|...X.*-|...X..2<..A.."B@
0280:  .XQ...D@.@..0.....................2<.................NqNqNq
02C0:  NqNqNq........0.Q...................NqNqNqNqNqNq........0.Q.....
0300:  .........`.......................................................
0340:  ................................................................
0380:  ................................................................
03C0:  ................................................................
```

GYROS-VIRUS

Dieser Virus wurde wohl mit der Absicht programmiert, einen Freund (?) zu ärgern, wie der Text im Bootblock vermuten läßt.

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

Fortpflanzung:

Bei jedem Reset des Rechners mit ungesicherter Diskette im Boot-Laufwerk

Effekt:

Blockiert den Bootvorgang nach einer Weile, d.h. anstatt von einer Diskette zu booten, blockiert der Virus die Ausführung des Bootblocks, der Bildschirm wird auf schwarz geschaltet, die Disk-LED erlischt. Ein erneuter Reset des Rechners schafft keine Abhilfe. Es kann sein, daß es diesen Virus auch in einer lauffähigen Version gibt, die uns vorliegende jedoch läßt vermuten, daß sich um eine Art Vorversion handelt. Zumindest steckt im Wirkteil, übrigens wohl eine Grafikspielerei mittels Blitter-Chip, ein grober Fehler.

Bootblock:

```
0000:  DOS....x.... 9......DOS.g...A...C.....0<..".Q...N.....C...,y....
0040:  N... @ h..B.Nudos.library.`...Nu,y....a...A..L...:g...K...+n.:..
0080:  -H.:Nu,y.... <....".|....N..4C...-I..A.."B@r..XQ...F@0.Nu.......$
00C0:  f......(g...N..ZB.N..T..DOS.f..HH...,y....K..<-m...:B...K....U..
0100:  K...:...a..t(IK....U..k...`...a...L.?.NuN....."L3|....,y....N..8
0140:  "L3|....#|.....$#|.....(#|.....,y....N..8"L3|....,y....N..8Nu#.
0180:  ........K.....B."<......d.........Q..."<......#.....Nu....,y....
01C0:  "L3|....#|.....$N..8A.....................1|....1|....1|....1|..
0200:  ..F.'.N.....N.....Dear Arnd! Your Amiga is fucked from a nice GY
0240:  ROS. Many greetings to you from Goeblodiel!!...................
0280:  .....................................\........I.............p....
02C0:  .......p...t...t.............8..J...........8..D...D...J.....
0300:  ...........4...t...t...L...\...b...@..Ml..K...C...\h............
0340:  ..C...G........P..........f..........V...@......H0..G.PRT..P.P
0380:  ........................................................................
03C0:  ....................8..<..<....0.............................
```

LAMER-VIRUS 1.0, 2.0, 3.0

Der LAMER-Virus...

Was ist ein LAMER ? Als LAMER, übrigens ein bitterböses englisches Schimpfwort, werden diejenigen Leute in der AMIGA-Szene bezeichnet, die andere Ansichten haben als man selbst. Oder sie haben Intros von Crackern als ihre eigenen ausgegeben. Oder lassen sich ihre Intros von fremden Leuten gegen Geld programmieren, um vorzugeben, sie seien die größten. Oder sie geben Raubkopien, die sie selbst kostenlos erhalten haben, nur gegen Geld weiter. Und so kann man das ganze endlos weitertreiben; Leute die einem auf die eine oder andere Art und Weise nicht passen, werden kurzerhand als LAMER 'gebrandmarkt'.

Fortpflanzung:

Bei jeder Schreib-/Lese-Operation eines angeschlossenen Laufwerks mit ungesicherten Disketten.

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

Effekt:

Täuscht einen Standard-Bootblock vor, wenn mit Hilfe eines Disketten-Monitors oder ähnlichem, der Bootblock einer Diskette untersucht wird. Der LAMER-Virus kodiert sich ständig neu, so daß sein Aussehen sich bei der nächsten Infektion schon wieder geändert hat.
Lediglich die ersten 78 Byte des LAMER 1.0 bleiben stets gleich. Beim LAMER 2.0 lediglich die ersten 52 Byte. Bei beiden ändern sich in diesen ersten Byte natürlich die Byte 5 bis 8, welche die Bootblockprüfsumme darstellen. Bei einer Neukodierung des LAMER's entsteht somit eine neue Prüfsumme...

Dieser LAMER-Virus, Version 2.0, formattiert nach einer gewissen Zeit die Diskette, während LAMER 1.0 'lediglich' wahllos Sektoren mit dem Text 'LAMER' vollschreibt. Diese beiden Versionen simulieren bei einer Infektion einen Standard-Bootblock, wenn dieser mit einem Hilfsprogramm, z.B. Guardian, DiskX, etc., untersucht wird.

Beide LAMER-Versionen sind an den Byte 12 und 13 zu erkennen: Beim LAMER 1.0 steht dort 'pa', beim LAMER 2.0 'pp'.

Übrigens habe wir den Virus in einer weiteren Variante aufgefunden: Neben der Bootblock-Version existiert noch ein Trägerprogramm, der 'LoadWB'-Befehl des CLI, vor den ein LAMER-Installationsprogramm 'gehängt' wurde. Dieses installiert nun den Virus im System, ohne daß der Anwender etwas davon bemerkt ! Bootblock-Wächter, z.B. 'Guardian 1.2' werden durch den im RAM simulierten Bootblock getäuscht. Allerdings handelt es sich bei dieser LAMER-Variante NICHT um einen Link-Virus, sondern um ein sogenanntes 'Trojanisches Pferd', also um ein Programm, das nur die Aufgabe hat den Virus unbemerkt ins System zu schleusen.

Der Virus dekodiert nach einer Infektion folgenden Text in den Speicher: 'The LAMER Exterminator!!!'. Dieser Text ist im 'Trojanischen Pferd' 'LoadWB' noch unverschlüsselt enthalten, und kann mit jedem beliebigen File-Monitor angeschaut werden.

Tja, und dann ist da noch der LAMER 3.0, ein ganz fieser Vertreter der Bootblock-Viren: Er kopiert den Original-Bootblock, egal ob dort etwas steht oder nicht auf die Sektoren 2 und 3 der Diskette und schreibt sich selbst in die Blöcke 0 und 1, also in den Bootblock. Wird nun von dieser Diskette gebootet, so erfolgt zuallererst eine Infektion des Rechners. Dann führt der Virus (!) selbstständig den auf die Blöcke 2 und 3 ausgelagerten Original-Bootblock aus.

Während bei den ersten beiden LAMER-Versionen dem Benutzer beim Betrachten des Bootblocks mit Hilfe von verschiedenen Bootblock-Programmen immer ein Standard-Bootblock vorgegaukelt wurde, erscheint nun der 'echte'; nur daß dieser nicht im Bootblock steht...

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

Bootblock:

```
0000:  DOS........pp.a"N...J.g. @ h..p.Nup.`.dos.library.H...N...A....:
0040:  .a4<.R....Q....h..J............z.....(. `..(.(`..(.$_...B:B9.:`.
0080:  B:.:.:...:..].l.......9..bBa........)...HMY.9.......F.W.;..fHM.(
00C0:  . _.....9...;.......:..%B. .V......9....B..9..0.B..H..v%:.$9.....
0100:  .x9..H%B.x............H...9..n.z9..8;..HH....:;..V....;..>.A..H.
0140:  .|9..JD._.+.H...Z.9..^.(. _...._.'..:<....7.....:..%B. '...HM....
0180:  ...&_..RD..&`....!...._.!....`...B.ZJ9.......Y..P.!...._,.a."..
01C0:  ....`....".<.T.R`........V;.....!...:.....$<.)..........._....a
0200:  ..."...:`...J.Y..F.V.....V.......T...D."9..O....._...,j9.../"..
0240:  ."........)....T.Z.B...H......i...`.....L..T.>.B.r^.,y)...@y....
0280:  ^.,y.9..Y..v9.. D"..._.+"..D*`0.....V.....V.......T..."......y..
02C0:  .....:.&Y6.T..."....`........FYe]..L.).........V....Y.J.Y^F...HM.!
0300:  ....`*Y..a."."...T.n`......a."<.)...HMF.....B..<Y../&R.....V`..!
0340:  ....`.H...Z.H..  F.<.HM'...HM9...=..RDz_..DJ...)...HMNLY[c^aKc(^]
0380:  Pa[]...b].F9E=,.=RN]LeahYNgL.....................................
03C0:  ................................................................
```

NORTH STAR I-VIRUS

Fortpflanzung:

Bei jedem Reset des Rechners mit ungesicherter Diskette im Boot-Laufwerk.

Effekt:

Tarnt sich als bootblockansäßiger Virus-Detektor, erkennt BYTE BANDIT- und SCA-Virus, sowie SCA-Abkömmlinge, wie den AEK-Virus, wobei der Erkennungsmechanismus sehr dürftig ausgefallen ist (Viren werden nur an Zeichenketten erkannt, nicht an Programmsequenzen). Gibt eine entsprechende Meldung aus ("VIRUS detected on this Disk. Reset,WriteProt OFF.Re-Insert") und blockiert den Bootvorgang solange, bis die eingelegte Diskette entsichert wird, und er sich in den Bootblock kopieren kann.

Der NORTH STAR I-Virus kann durch Drücken der linken Maustaste in Port 2 erkannt werden (die Power-LED des Amiga flimmert).

Neben den eben genannten Viren, erkennt der NORTH STAR I-Virus auch eine andere Version seiner selbst, auf die er mit der Meldung "OLD AntiVirus Please RESET and INVERT WriteProt for UPDATE" reagiert, sowie eine weitere Anti-Virus-Variante eines anderen Autors ("My AntiVirus is Better! STARFIRE/NORTH STAR").

Bootblock:

```
0000:  DOS........`.`.North Star............Nort....f...Star....f..y..
0040:  ....m.`"A...C.....0<.."..Q...N.....y......#.STAR....C.....,y....
0080:  N... @ h..B.Nu.9.....f.0<...y.....2<`.Q...Q...,y....a...A.....
00C0:  ...:g.#..:.....H.:Nu.|.....A..."B@r..XQ...F@0.Nu.......$f....(g.
0100:  N.....B.N.......DOS.f0a0al.y.....:B.......C.....f.H...K.....(Ia.
0140:  ..L.?.Nu.......Hf..y.....``..Band. f..y.....`L........f..y....
0180:  ."`8Nu..Nort..f...Star..f..l....g.m.Nua............g.a...`.a..t
01C0:  .........g.a...`.N.....a..X"L3|....,y....N..8"L3|....#|.....$#|
0200:  .....(#|.....,y....N..8"L3|....,y....N..8#.....NuB....."<....A.
0240:  ....B...d.........Q..."<......#.....NuH...,y....#.....B.C.....N.
0280:  ..#.....,y....B.A....."<...2N...,y...."y....N..bL...B.NuH...,y..
02C0:  ..#.....B.C.....N...#.....,y....B.A....p`.intuition.library.....
0300:  .......VIRUS detected on this Disk. Reset,WriteProt OFF.Re-Inser
0340:  t.....#AntiVirus (C)1988 STARFIRE / NORTH STAR.....OLD AntiVirus
0380:  . Please RESET and INVERT WriteProt for UPDATE. ....#AntiVirus (
03C0:  C)1988 STARFIRE / NORTH STAR......dos.library.N.................
```

NORTH STAR II-VIRUS

Fortpflanzung:

Bei jedem Reset des Rechners mit ungesicherter Diskette im Boot-Laufwerk.

Effekt:

Tarnt sich als bootblockansäßiger Virus-Detektor, erkennt BYTE BANDIT- und SCA-Virus, sowie SCA-Abkömmlinge, wie den AEK-Virus, wobei der Erkennungsmechanismus sehr dürftig ausgefallen ist (Viren werden nur an Zeichenketten erkannt, nicht an Programmsequenzen). Gibt eine entsprechende Meldung aus ("VIRUS Detected on Disk! STARFIRE/NORTH STAR") und blockiert den Bootvorgang solange, bis die eingelegte Diskette entsichert wird, und er sich in den Bootblock kopieren kann.

Der NORTH STAR II-Virus kann, wie auch der NORTH STAR I-Virus,durch Drücken der linken Maustaste in Port 2 erkannt werden (die Power-LED des Amiga flimmert).

Neben den eben genannten Viren erkennt der NORTH STAR II-Virus auch eine ältere Version seiner selbst (NORTH STAR I-Virus), auf die er mit der Meldung "OLD AntiVirus STARFIRE/ NORTH STAR" reagiert, sowie eine weitere Anti-Virus-Variante eines anderen Autors ("My AntiVirus is Better! STARFIRE/NORTH STAR").

Bootblock:

```
0000:  DOS........`.`..xNorth Star.............Nort....f...Star....f.
0040:  .y......m.`"A...C.....0<..".Q...N......y......C.....,y....N... @
0080:   h..B.Nu.9......f.0<...y......2<`.Q...Q...,y....a...A........:g.
00C0:  #..:....-H.:Nu-|......A..."B@r..XQ...F@0.,y..........&g...B..&`.
0100:  ............f...B.....`...Nu.......$f....(g.N.....B.N.......DOS.
0140:  f2a2a...-y.....:B.......C.....f.H...K.....(Ia...L.?.Nu.......Hf.
0180:  .y.....  `t..Band. f..y....."``........f..y.....$`L..otec.$f..y..
01C0:  ...&`ZNu..Nort..f...Star..f..l....g.m.Nua..v..........g.a..$`.a.
0200:  .`..........g.a...`.#.........N@a..>..........g.a...`.a..X"L3|..
0240:  ..,y....N..8"L3|....#|.....$#|.....(#|.....,,y....N..8"L3|....,y
0280:  ....N..8#.....NuB....."<....A.....B...d..........Q..."<......#...
02C0:  ..Nu,y....#....\B.C....FN...#....X,y...XB.Nu"<....N...,y...\"y..
0300:  .XN..bB.NuH...a.A....`a.L...NuH...a.A.....a.L...NuH...a.A.....a.
0340:  L...Nuintuition.library...I....v.P.VIRUS Detected on Disk! STARF
0380:  IRE/NORTH STAR.....OLD AntiVirus.  STARFIRE/NORTH STAR...P.My An
03C0:  tiVirus is Better! STARFIRE/NORTH STAR.....dos.library.N.......
```

OBELISK-VIRUS

Fortpflanzung:

Bei jedem Reset des Rechners mit ungesicherter Diskette im Boot-Laufwerk.

Effekt:

Sieht aus, wie einer der auf dem AMIGA üblichen Bootblock-Vorspanne, die unmittelbar nach Einlegen der Boot-Diskette erscheinen: schwarz-rot-gelber Hintergrund mit einem Hinweis auf die Programmierer im Vordergrund ("OBELISK CRACKING CREW"). Erscheint unmittelbar nach Einlegen einer bootfähigen Diskette nach einem Reset. Dieser Virus blockiert in keinster Weise den Rechner, sondern hat lediglich die Aufgabe sich fortzupflanzen.

Zu erkennen ist der OBELISK-Virus nur an der zufälligen Zeichenfolge 'GURU', da die oben genannte Meldung als Grafik im Bootblock vorliegt.

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

Bootblock:

```
0000:  DOS........p/........:e.A..."n.:0<..".Q...A..PN.a...X.!.GURU.`C.
0040:  ..N... @ h..p.NuA...-H..C.."p.r..YQ...F@2.Nu,x..a.C......:g.!n.:
0080:  .D-I.:Nu.......$f.J..,f....(f..i....g..i....g.N.....B.a...DOS.ft
00C0:  H... :.>....gb L0<...XN.f..P..g.Q...`JA.........d>-P.:B.(I3|....
0100:  N..83|....#|.....$A...#H.(B..,N..83|....N..8a..>L.?.NuH..."o.<3|
0140:  ....B..$N..8N..|C...N..h/.,@/..2A..HC... .1@.2H@1@..-H.23.......
0180:  ><..N....9......W...-_.2"N,_N..bN..vL.?.Nu...................8..
01C0:  ..........d.............................graphics.library.dos.l
0200:  ibrary....?.....9...8...........?.8...........8?.......;...8?..
0240:  ........................8?.......;...8?.........................8
0280:  8.....8.;...p8.8.....8.......8.....;...88.....8.;....?.8.....8..
02C0:  .....?.........88...?...;....?.......8.....?.?.........88.......
0300:  9............8.....?...........88.....8.8.;..........8.....8....
0340:  .......88.....8.8.;.p........=.............[...x?...........8?..
0380:  .....?.............;....?...........8?.........?...........;.....
03C0:  ..?.........8?...8.......8.........9.............................
```

(leider etwas dürftig...)

PARAMOUNT-VIRUS

Beim PARAMOUNT-Virus handelt es sich um einen direkten Abkömmling des BYTE WARRIOR-Virus', einen sogenannten Clone, im Gegensatz zum oben beschriebenen GADDAFI-Virus, der wesentlich mehr eigenständige Elemente enthält.

Fortpflanzung:

Bei jeder Schreib-/Lese-Operation eines angeschlossenen Laufwerks mit ungesicherten Disketten.

Effekt:

Wie der BYTE WARRIOR-Virus auch, enthält der PARAMOUNT-Virus neben seiner im Klartext vorliegenden Bootblock-Message (siehe ASCII-Dump) auch noch die kodierte Nachricht des BYTE WARRIOR-Virus', die im Speicher von Adresse $0007FC00 bis $0007FC95 abgelegt wird:

```
Virus detector by the mighty Byte Warrior!!!  Please, please,
please don't install this disk, coz I want to travel!  Spread
the bootblock and the word!
```

Lediglich die schnelle Tonfolge des BYTE WARRIORS und die Eigenschaft diverse Viren zu erkennen wurden entfernt (siehe Beschreibung des BYTE WARRIOR-Virus').

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

ACHTUNG !!!

Aufrund eines Programmierfehlers unterscheidet der auch der PARAMOUNT-Virus nicht, ob es sich bei einer Schreib-/Leseoperation um eine Operation eines Diskettenlaufwerks oder um eine Operation eines anderen 'Devices' handelt.
Näheres ist weiter oben der Beschreibung des BYTE WARRIOR-Virus' zu entnehmen.

Bootblock:

```
0000:  DOS.7.....{.H...a...L...C...N...J.g... @ h..p.Nup.Nudos.library.
0040:   |....C...0<.. .Q... |...f"|....0<............Q...J..*f...J...g.
0080:  ..N.....,y....-|...L.&N...-@.*-|...n.:NuB..*B...0<..A.."BA.XQ...
00C0:  PSWC !!...........0<0.Q...........0<0.Q...Q...#....b....3.......
0100:  3..?....3.......0<..N....R0<..N....R0<..N....R0<..N....R0<..N...
0140:  .R3.......Nu...T....J....T.....!.............TJ..*f...J...g...N.
0180:  .....)....g....)....f..........$g..........$f...J..,f...J..(g...
01C0:  3.......#..(....#..,....#..$....#.. .... i.....A.....9......g..N
0200:  #|.....(3|....#|.....$#|.....,N.....3y......#y.....(#y.....,#y..
0240:  ...$#y..... N.....3.....0<..Q...Nu....M.lTd...\..\.l..4.\.......
0280:  \4..4\..E.ll..l....}...d...|...d...|...d......\...d\....\..d...d
02C0:  .....,...D..\.\..\l.L....e|l....\......\..........\...D.l.......
0300:  ................................PARAMOUNT SOFTWORKS CREW 1988 :
0340:  Greetings to : Napoleon ,Obelisk, Idefix, Asterix Hamburg ...
0380:  ................................................................
03C0:  ................................................................
```

SCA-VIRUS

Der SCA-Virus, der Urvater aller AMIGA-Viren wurde, von einem Cracker der 'Swiss Cracking Association' (SCA) programmiert, um zu beweisen, daß es durchaus möglich ist, Viren auf dem AMIGA zu realisieren. Bis zu diesem Zeitpunkt gab es noch keine sogenannten Bootblock-Lader, so da dieser Virus keinerlei Schaden anrichten konnte.

Der Programmierer des SCA-Virus' selbst war erstaunt, wie schnell sich dieser Virus ausbreitete. Damals hatte ja kaum einer von Viren gehört, geschweige denn welche in Aktion gesehen. Also schrieb er einen Virusdetektor, den 'SCA-Protector 1.0', welcher den SCA-Virus erkennen und einen Bootblock so schützen konnte, daß sein Virus einen solchen Bootblock nicht infizierte. Dieser Bootblock war dann aber nur gegen den SCA-Virus geschützt ! Nur schade, daß der 'Protector' selbst sich nicht so schnell verbreitete, wie der Virus selbst...

Der SCA-Virus war der am weitesten verbreitete Virus. Später war man ja gewarnt; viele AMIGA-Besitzer untersuchten fortan die Bootblöcke ihrer Disketten bevor sie sie starteten. Auch wir gehörten zu diesen... Damals mag so ein Virus ja noch ganz witzig gewesen sein, weil es etwas Neues war, heute kann fast jeder Hans und Franz einen solchen Virus programmieren, genügend Literatur, um sich zu informieren gibt es ja schon. Das geht soweit, daß Software-Firmen sogar schon Bücher mit Viren-Listings veröffentlichen, damit auch ja jeder so etwas nachmachen kann. Das ist eine beispielslose Verantwortungslosigkeit gegenüber dem Computer-Anwender ! Aber diese Firma ist wohl nur auf hohe Verkaufzahlen aus, so wie es aussieht ! Na ja, wer's halt nötig hat...

Übrigens: Auf dem Atari-Markt geht das soweit, daß sogar schon ein 'Virus Construction Set' käuflich zu erwerben ist, mit dem jeder seinen 'persönlichen' Virus kreieren kann, mit ganz persönlichen Eigenschaften. Sch...-Spiel...

Fortpflanzung:

Bei jedem Reset des Rechners mit ungesicherter Diskette im Boot-Laufwerk.

Effekt:

Horizontaler Text auf schwarzem Hintergrund in der Mitte des Bildschirms ("Something wonderful has happened"), meldet sich nach jeder 15. erfolgreichen Infektion einer Diskette. Nach Ende der Virus-Meldung führt der Rechner seine Aufgaben (Beenden des Boot-Vorgangs, 'Startup-Sequence' abarbeiten) normal fort, der SCA-Virus ist aber weiterhin aktiv !!!
Drückt man während des Bootvorgangs den linken Mausknopf, so verfärbt sich der Bildschirm grün, und der Virus entfernt sich eigenständig aus dem System ! Auch hier wieder ein Programmiererhintertürchen...

Bootblock:

```
0000:  DOS.7...CHW!A...C.....0<..".Q...N.....C...,y....N... @ h..p.Nu,y
0040:  .....9......f.B...a..<K....;|.`..p2a..F`.a...A........:g.#..:..
0080:  ..-H.:Nu-|...>..A.."B@r..XQ...F@0.Nu.......$f....(g.N.....B.N...
00C0:  ....DOS.f0-y.....:B.....H...K.....A..... .....g.(Ia...L.?.Nu.y..
0100:  .....y......09.....@...@..f.a..R"L3|....,y....N..8"L3|....#|....
0140:  .$#|.....(#|.....,,y....N..8"L3|....,y....N..8Nu"LB..$3|....,y..
0180:  ..N..8G.....C.....B.,y....N...#.....'K,y....N..:A.....'H..p.2<.@
01C0:  4<..,y....N..z+|......;|....pda...E.....A.....#.....0<..B.Q...;|
0200:  .u..;|....;|.8..;|....B...;|....B...;|....'KB...rQ,y....N..."KB.
0240:  ......gP JE...,y....N...t.2<..p.a..J;A...A."Q...B...a..6t.p.a...
0280:  .A.";A..Q...B...a...`..R y....+h.&..;|....Nu.@.-....f..-....g.Q.
02C0:  ..Nu........p......bt.......u.............Q.............&....gr
0300:  aphics.library.dos.library.. Something wonderful has happened..-
0340:  .Your AMIGA is alive !!!..A.and, even better...PP..Some of your
0380:  disks are infectedn2Z.by a VIRUS !!!.x2.Another masterpiece of.2
03C0:  2.The Mega-Mighty SCA !!.n..N.....A!SCA!SCA!SCA!SCA!SCA!SCA!SCA!
```

SYSTEM Z-VIREN

Hier handelt es sich um einen Sonderfall. SYSTEM Z-Viren sind eigentlich keine Viren im eigentlichen Sinne, sondern vielmehr Anti-Virus-Viren, die sich nicht eigenständig verbreiten.

Fortpflanzung:

Nur wenn ein Virus im Bootblock erkannt wird und der Anwender die Frage, ob der Bootblock installiert werden soll, mit 'JA' beantwortet. Hier wird dann eine Kopie des SYSTEM Z-Anti-Virus' auf die Diskette geschrieben, was der unbedarfte AMIGA-User jedoch nicht weiß.

Effekt:

Produziert eine schnelle Tonfolge, um zu signalisieren, daß SYSTEM Z noch aktiv ist. Der Bildschirm verfärbt sich hellblau, wenn kein Virus erkannt wurde, andernfalls grün.

Diese beiden Anti-Viren erkennen den BYTE BANDIT- ,den SCA-Virus und dessen Abkömmlinge sowie BYTE WARRIOR-Virus und den LAMER-Virus 1.0.

Bootblock:

```
0000:  DOS.PVL....p`.." SYSTEM Z VIRUS  PROTECTOR V3.0 A...C.....0<..".
0040:  Q...,y....B...-|.....&N...-@.*3.......3.......C...N... @ h..p.Nu
0080:  dos.library.H....9......g,A.....2<..B...d.R.Q...F."9......d.R...
00C0:  PVL.g4B..&N...-@.*L...Nu........J..........!.............3.....
0100:  ..3.......3.......C..n#.....3..@....3..?....3.......A..B2<..NqQ.
0140:  ..3.....f.3........,y...........:g.#.:.....|......:L...Nu.....R.@
0180:  ...........$f....(g.N.....B.N.......DOS.ffH... y.....:.........f.
01C0:  a...A..zaHJ.g.a....lJ..pf.a.A...a0J.g.a....lJ...f.af.9......f.aZ
0200:  al.lJ...f.aNL...NuH.../.C...B.N...,@"<...<B.  N.../."N,y....N..b
0240:   .L...Nuintuition.library.&LE.....0<....Q...NuR.....S.....*I3|..
0280:  ..N..8"M3|....#|.....$#|.....(B..,N..8"M3|....N..8S.....R.....Nu
02C0:  .&.Warning: This disk is infected with the ByteBandit-Virus!....
0300:   Left MouseButton: Kill the Virus, Right MouseButton: Continue..
0340:  .4.Warning: This disk is infected by the SCA-Virus.... Left Mous
0380:  eButton: Kill the Virus, Right MouseButton: Continue............
03C0:  ..............................................................B.JSN.
```

(Die anderen Viren-Dumps sparen wir uns der Ähnlichkeit wegen...)

VKILL-VIRUS 1.0

Es handelt sich beim VKILL 1.0-Virus um einen weiteren Vertreter der virulenten Anti-Viren.

Fortpflanzung:

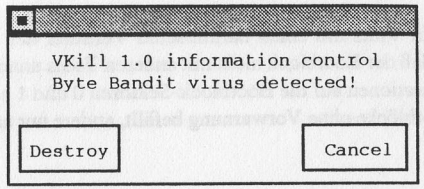
Bei jeder Schreib-/Lese-Operation eines angeschlossenen Laufwerks mit ungesicherten Disketten, solange es sich bei dem jeweiligen Bootblock um einen Standard-Bootblock handelt, oder aber, wenn der Anwender die unten gezeigten Requester mit Destroy beantwortet.

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

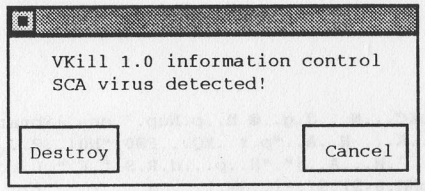
Effekt:

Gibt nach der Infektion, bei jedem Versuch den Bootblock zu untersuchen, sei es durch einen Virus-Detektor oder einen Disketten-Monitor, vor, da es sich bei dem untersuchten Bootblock um einen Standard-Bootblock handelt.

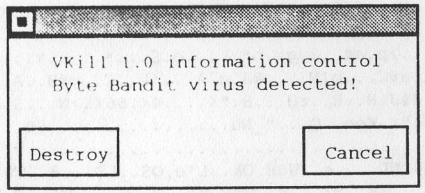
Bei Erkennen eines Nicht-Standard-Bootblocks durch den Virus, taucht ein Requester mit folgendem Aussehen auf:



beim BYTE BANDIT-Virus,



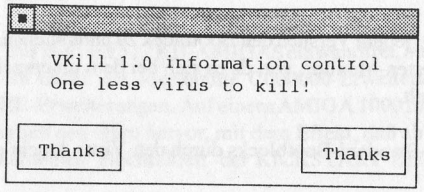
beim SCA-Virus und



bei jedem anderen Nicht-Standard-Bootblock.

Wird nun 'Cancel' angeklickt, so passiert nichts, der jeweilige Bootblock bleibt unverändert, bei 'Destroy' wird der VKILL 1.0-Virus auf den Bootblock geschrieben, und folgender Requester erscheint:

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91



Es handelt sich bei diesem Virus um einen harmloseren Vertreter der Bootblock-Viren, wobei lediglich der Effekt stört, daß der Bootblock nicht mit anderen Tools untersucht werden kann, weil dieser Virus alle Lese-Operationen auf die Bootblock-Sektoren 0 und 1 abfängt, harmlos deshalb, weil er 'nur' Standard-Bootblöcke ohne Vorwarnung befällt, andere nur nach einer etwas dubiosen Rückfrage (siehe oben).

Um einen Virus handelt es sich bei diesem deshalb, weil er sich ohne irgendwelche äußeren Anzeichen auf einen Standard-Bootblock schreibt.

Bootblock:

```
0000:  DOS.AQ/....pa&C...N...J.g. @ h..p.Nup.`.dos.library.H..0E..."n.:
0040:  &Ip.".S.f.Rk..A...-H..A.."p.r..XQ...F@0."N0|..E... .N..\'@..L...
0080:  NuH..0&n.:,x..`.H...A..j"."H..p...d.R.S.f.F.".L...Nu/.$h.....t$_
00C0:  fZ ).,.......bNH.8<$).$(.*i.($M.)....g....)....f(J.g.....a.f&&:.:
0100:  ..c.#B.$..#J.(#C.,3|....L.<.N....4L.<.Nu3|....a(J.. f.#|.....$/.
0140:  E...#J.($_B..,3|....a..:H...a.L...N..&J.`..Da.f.(). .)..J.g.B.S.
0180:  f.#D. .C..B)..N...`.G..j..f...DOS.g...CHW!g0G....Kgh...>Vig..bp.
01C0:  .JV...f.a..*`NI...p.`.I...`.I...p.a.abg.a..>g.I...`.B..$3|....a.
0200:  .XNuI..]J.g.I..>p.a4`.J.g..h":....e.$...*.. ..*...G...p%..Q...r2
0240:  .. .`..6H...&.avC...p!N...,@J.g`A...!L..C..v#H..A...#H..A..m$HR.
0280:  g.A..TE..X#H.4#J.H..E..rG...B."<....4<.66<.>N...$.a."N,x..N..bJ.
02C0:  L._.Nu/.A..fp4"< Ken..Q..."_Nu.................0..............
0300:  ..............................................v...LkT@.k..F...
0340:  I$.NC$..R$.no%.NL....=..U8E.Ok..L'e,O$..L$...%..T9..I1.. .&/.=..
0380:  U8E.E?..T..O ...Ek'.N/...=..U8E.E?..T..O ...T)..C E.O/.NN$.NN$..
03C0:  A'e*I8.NW9..Ek..O?..T..nd...R$.ni,..R.e:H*..SK..T>..I$.@L"..A9.n
```

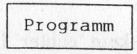
LINK- UND COPY-VIREN

Nun kommen wir zum zweiten bereits erwähnten Typ von Viren, den Link-Viren:

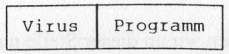
IRQ-VIRUS

Er heißt 'IRQ-Team-Virus V41.0', der Kürze wegen von uns als 'IRQ-Virus' geführt, und war lange Zeit der wohl nervigste Amiga-Virus. Er hängt sich vor Programme und installiert sich beim Starten eines infizierten Programms im System. Dazu mißbraucht er den 'KickTagPointer', um sich resident zu machen, und den Vektoreinsprung für die Betriebssystemfunktion 'OldOpenLibrary', um sich zu verbreiten.

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91



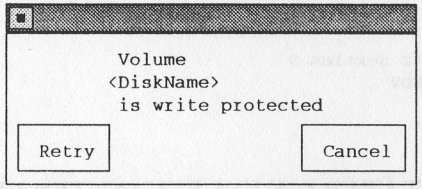
nicht infiziertes Programm



infiziertes Programm
(Virus wird zuerst ausgeführt)

Hier liegt die Gefährlichkeit des IRQ-Team-Virus': Er puffert selbstständig den Originaleinsprung für diese Betriebssystemfunktion und setzt dafür eine auf den Virus zeigende Adresse ein, d.h. bei jederBenutzung der Funktion 'OldOpenLibrary' wird zunächst in den Virus verzweigt, und erst danach in die eigentliche Betriebssystemroutine. Der IRQ-Virus infiziert grundsätzlich den Befehl 'DIR', weil dieser wohl den am häufigsten benutzten CLI-Befehl darstellt, sowie den ersten Befehl der zuletzt ausgeführten Startup-Sequence. Dabei achtet der Virus natürlich darauf, da er ein infiziertes Programm nicht ein zweites Mal verseucht. Ein infiziertes Programm wird um 1096 Byte länger, als das nicht verseuchte Pendant. Sieht man sich mit Hilfe eines geeigneten Programms, z.B. 'FileZap', 'NewZap' oder 'Type' ein befallenes Programm an, so ist für den Laien eigentlich nichts Ungewöhnliches festzustellen, denn die Programmierer haben den virulenten Teil 'geschickterweise' codiert, so daß keine verdächtigen Meldungen bzw. Texte erkennbar sind.

Ein Hinweis auf Aktivitäten des IRQ-Virus' ist unter anderem die Requester-Meldung



unmittelbar nach Starten eines infizierten Programms, wenn die Systemdiskette, das ist die Diskette mit der gebootet wurde, schreibgeschützt ist. Andernfalls schreibt sich der Virus unbemerkt auf die Diskette. Bei kurzen Programmen fällt die Infektionszeit kaum auf, bei längeren umsomehr: Wird beispielsweise in der Startup-Sequence als erster Befehl 'NotePad' eingetragen, ein Programm mit einer Länge von über 50 KB, so lädt der Virus dieses zunächst in einen von ihm reservierten Speicherbereich, 'hängt' sich vor 'NotePad', und schreibt dann erst die infizierte 'NotePad'-Kopie zurück auf Diskette, was natürlich durch den ungewöhnlich langen Diskettenzugriff auffällt. Während der Infektion kann man übrigens mit Hilfe eines System-Monitors, wie z.B. dem 'SysMon' oder ähnlichem, die Virus-Aktivität erkennen: Erstens 'zieht' der Virus extrem viel CPU-Zeit, zweitens reserviert er temporär 100000 Byte Speicher für den Infektionsvorgang.

Der IRQ-Virus befällt deswegen auch nur Programme bis zu einer Länge von 100000 Byte.

So, das sollte reichen, um das Funktionsprinzip dieses Link-Virus' zu verstehen...

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

BGS 9-VIRUS

Den BGS 9-Virus wollen wir an dieser Stelle nur kurz skizzieren. Er ist kein 'echter' Link-Virus, denn er 'hängt' sich NICHT an Programme an ! Wird dieser Virus gestartet, so passiert folgendes: Er sucht sich den ersten Befehl der 'Startup-Sequence', z.B. 'MOUNT', benennt diesen um in eine Zeichenkette um, die wie aus Leerzeichen bestehend aussieht, und verlagert diesen in den 'devs:'-Ordner des logischen Laufwerks 'SYS:' (in der Regel die Bootdiskette). Deshalb werden Viren dieser Art auch Copy-Viren genannt.

Sich selbst kopiert der Virus unter dem Namen aus der 'Startup-Sequence' auf die Diskette bzw. Festplatte. Wird nun das nächste Mal der 'infizierte' Befehl, in unserem Beispiel 'MOUNT', gestartet, so aktiviert man ungewollt den Virus, welcher, nach erfolgreicher eigener Installation im System, den eigentlich gewünschten Befehl aus dem 'devs:'-Ordner nachlädt und startet.

Der BGS 9-Virus zeigt sich nach jedem viertem Reset, der mindestens bis zum Öffnen des Amiga-DOS-Fensters abgelaufen sein muß, in Form eines schwarzen Bildschirms mit folgendem Text:

```
a computer virus is a disease
terrorism is a transgression
software piracy is a crime

this is the cure

BGS9 Bundesgrenzschutz Sektion 9
     Sonderkommando EDV
```

GESAMTÜBERSICHT ÜBER DIE UNS BEKANNTEN VIREN

Name	Alias	Boot	Link	Copy	Time	Anti	Analyse	Klass.
16 Bit Crew		x						
AEK	SCA	x					x	x
ASS 1.0		x			x		x	x
Aids		x						
Alien		x					x	
Amiga Freak	Byte Bandit	x						
Australian Parasite		x						
Avirex Timebomb		x			x			
BGS 9	BGS 9			x			x	x
Bahan		x						
Bamiga Sector 1	SCA	x					x	x
BlackFlash		x						
Butonic 1.1	SCA	x					x	x
Byte Bandit	Byte Bandit	x					x	x
Byte Bandit 3	Byte Bandit	x					x	x
Byte Bandit 4	Byte Bandit	x					x	x
Byte Bandit Plus	Byte Bandit	x					x	x
Byte Warrior	Byte Warrior	x				(x)	x	x
CCCP		x	x					
CLI Batchfile Virus				x			x	
CList	Lamer Boot	x						
Claas Abraham		x					x	x
DAG	SCA	x					x	x

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

Name	Alias	Boot	Link	Copy	Time	Anti	Analyse	Klass.
Disaster Master			x				(x)	(x)
DiskDoktors		x					x	x
DiskHerpes		x						
Extreme		x						
Fast		x						
Gaddafi		x					x	x
Grafitti		x						
Gremlin		x						
Gyros		x					x	x
HCS	HCS	x				x		
HCS 3	HCS	x				x		
IRQ	IRQ Link		x				x	x
IRQRun	IRQ Link		x					
Ice		x					x	x
JITR		x					x	x
Jeff Butonic			x				x	x
Joshua		x					x	x
Julie		x						
Kauki		x						
LSD	SCA	x					x	x
Lamer 1.0	Lamer Boot	x					x	x
Lamer 2.0	Lamer Boot	x					x	x
Lamer 2.0 Trojan	Lamer Boot						x	x
Lamer 3.0	Lamer Boot	x					x	x
MGM 89		x						
MicroSystems		x					x	x
No Name 1		x						
North Star 1	North Star	x				x	x	x
North Star 2	North Star	x				x	x	x
Obelisk		x					x	x
Opapa		x						
Paramount	Byte Warrior	x				(x)	x	x
Pentagon Circle	Pentagon Circle	x				x	x	x
Pentagon Circle 2	Pentagon Circle	x				x		
Revenge 1.2G		x					x	x
Revenge...Lamer Ext.	Lamer Link		x				x	x
SCA	SCA	x					x	x
ScarFace		x						
Sendarian		x						
Smily Cancer			x				(x)	
Suntronic		x				x	x	x
System Z 3.0	System Z	x				x	x	x
System Z 4.0	System Z	x				x	x	x
System Z 5.0	System Z	x				x	x	x
System Z 5.3	System Z	x				x	x	x
System Z 5.4	System Z	x				x		
Target	SCA	x					x	
Terrorists	BGS 9				x		x	x
Tick		x						
TimeBomb 1.0		x				x	x	x
Trojan		x					x	
Turk		x					x	x
UltraFox		x						
UltraKill		x					x	
VKill 1.0		x				x	x	x
W.A.F.T.		x					x	x
Warhawk		x						
Wizard Timebomb						x	x	
Xeno			x				x	

(C) 1991 Amiga-Gruppe VTC Uni Hamburg - CEBIT '91

Legende:

Name:	Name des Virus
Alias:	Aliasnamen des Virus
Boot:	Typ Bootblock-Virus
Link:	Typ Link-Virus
Copy:	Typ Copy-Virus
Time:	Zeitbombe (Timebomb)
Anti:	Virus hat Antivirus-Eigenschaften
Analyse:	Virus ist vollständig analysiert
Klass.:	Virus ist klassifiziert, Eintrag im VTC-Virus-Katalog besteht

KONTAKTAUFNAHME MIT DEM VTC

Da es zeitlich fast unmöglich ist, Viren zu analysieren und diesen Artikel ständig auf dem neusten Stand der Dinge zu halten, besteht für all diejenigen AMIGA-User, die jetzt noch einen Virus in ihrer Diskettensammlung beherbergen, der nicht in dieser Übersicht auftaucht, die Möglichkeit, beim VTC der Uni Hamburg den Viren-Katalog zu bestellen. Dieser ist nur in Englisch verfügbar und kann gegen ein Rückporto von 3,50 DM bezogen werden.
Eine andere Möglichkeit ist die, eine Diskette mit dem betreffenden Virus einzusenden. Diese sollte mit der Aufschrift 'VIRUS !' versehen sein, sowie dem Absendedatum und dem Virusnamen, sofern dieser bekannt sein sollte.
Falls die Diskette zurückgesandt werden soll, so sollte ein adressierter und ausreichend frankierter Rückumschlag beiliegen, da weder die Amiga-Gruppe noch das Viren-Projekt in der Lage sind, das anfallende Porto zu tragen.
Wir hoffen, daß jeder dafür Verständnis zeigt. Eine kurze Symptom-Beschreibung darf ebenfalls beiliegen.

ACHTUNG: Es werden keine Raubkopien angenommen, bearbeitet oder beantwortet ! Kopien werden nur dann von uns bearbeitet, wenn die Original-Diskette beigeliegt ! Außerdem leisten wir weder eine Garantie für eine absolute Virenfreiheit nach einer Diskettenüberprüfung unsererseits, noch für das einwandfreie Funktionieren von uns entseuchter Programme. Anfragen und Ersuchen um Programmtests, die darauf hinauslaufen, daß in der Produktbeschreibung ein Test durch das VTC als Gütesiegel auftaucht, werden von uns rigoros abgelehnt.

Anfragen an das Viren-Projekt zum Thema Viren, egal um welchen Rechnertyp es sich auch handeln möge, aus zeitlichen Gründen bitte nur in schriftlicher Form und ebenfalls nur mit adressiertem und ausreichend frankierten Rückumschlag.

Unsere Adresse: Virus Test Center
Uni Hamburg - FB Informatik
Schlüterstraße 70
2000 Hamburg 20