VW

COLLABORATORS

	TITLE : VW	

ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY		January 6, 2023	

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VW

1.1 VirusWorkshop 3.7 - 21.05.1994

VirusWorkshop 3.7

A T.R.S.I. Production in 1994
coded by Markus Schmall

It's not allowed to include VirusWorkshop/Dhunk/documentations of VirusWorkshop on any release by Safe Hex International. I am NOT a member of SHI (any more) and therefore I am not interested in any direct or indirect contact to Mr.Erik Loevendahl Soerensen, the leader of this organisation.

The following SHI (ex)members are allowed to spread VirusWorkshop on their discs: Jim Maciorowski, Lars Kristensen and Jan Bo Andersen and nobody else.

M.S.

Description of the menus

Menuerklärung

Sector Check

Sektor-Kontrolle

File/Link/Trojan Check

Datei-Kontrolle

Memory Check

Memory Kontrolle

BootBlock to File

Bootblock->File

File to BootBlock

File->Bootblock

Install

BB Installation

Make BootBlock

Erstelle BB

Show Startup

Zeige Startup

KickSave

Kickstart-Sicherung

Drive Info

Laufwerk Info

HardDisk Support

Festplatten Support

ScreenResolution Support

Aufloesungen

Preferences

Known viruses

1.2 share2

VirusWorkshop ab jetzt (24.02.1994) ShareWare:

Der vorgeschlagene Betrag ist 15 DM oder 10 USDollar. Wenn Sie VirusWorkshop regelmäßig benutzen und das Programm mögen, dann würde ich mich über diese kleine Anerkennung sehr freuen.

VirusWorkshop ist ein Produkt, welches in einem Zeitraum von über 2 Jahren entwickelt wurde und in welches sicher mehr als 500 Stunden Arbeit investiert bisher wurde. Die Entwicklung des Programmes ist ja auch noch nicht abgeschlossen....Die Weiterentwicklung eines Viruskillers kann ja nicht abgeschlossen sein.....

Ich bin Student und programmiere VirusWorkshop als mein Hobby. Mir macht diese Arbeit Spass, aber indirekt verursacht dieses Projekt immense Kosten:

- jeden Monat muß VirusWorkshop verteilt werden (sowohl über DFÜ als auch per Post)
- neue Viren/Libraries/Patches etc. müssen von Mailboxen gezogen werden
- Erfahrungsaustausch mit Freunden innerhalb von Deutschland per Telefon verschlingt auch eine nicht zu vernachlässigende Summe.

Wenn Sie mir den Betrag senden, erhalten Sie von mir die nächste Version von VirusWorkshop am Veröffentlichungstag direkt per Post.

Wenn Sie schon für eine ältere Version von VirusWorkshop eine ShareWare Gebühr bezahlt, müssen Sie natürlich nicht immer wieder diese Gebühr bezahlen.

Wenn Sie die aktuellste Version von VirusWorkshop direkt von mir haben wollen, dann senden Sie einen frankierten Rückumschlag und eine Diskette an mich. Wenn das Rückporto nicht ausreichend ist, behalte ich mir vor, diese Anfrage nicht zu beantworten, denn ich sehe es nicht ein, daß ich die Portogebühren für Sie bezahle.

Denken Sie darüber nach !

Meine Adresse:

Markus Schmall
von Graevemeyerweg 25
30539 Hannover

Dank des überragenden Sharewaregedankens hat mich 11 Wochen nach Veröffentlichung ein ganzer Brief mit der Shareware-Gebühr erreicht. Vielen Dank.

1.3 share1

VirusWorkshop is from now (24.02.1994) on ShareWare:

The suggested donation is 15 DM or 10$. If you like VirusWorkshop and use it regulary I would be very happy, if you send the suggested donation to me.

VirusWorkshop is a product, which was produced in many hours. I do not know how many hours, but I invested for sure more than 500 hours to produce it. And the development progress is still running...

I am a student and to code VirusWorkshop is my hobby. The work on VirusWorkshop makes me happy, but the costs to produce this viruskiller are very high:

- the viruskiller has to be spreaded every month.
- new viruses etc. have to be downloaded from mailboxes (mainly in nonlocal boxes).
- technical knowledge exchange by phone with friends in other sides of Germany is very high.

If you send me the donation, you will get the next version from VirusWorkshop direct from me at the releaseday by mail.

If you have already paid the Share for an older version of VW, then you need not to pay this share for a new version(but i will not stop you to do this).

If you want to get the latest version of VirusWorkshop, then please send me an envelope with stamps and a disc. If you cannot get in touch with german stamps, then send me 3 DM=2US$! I am not able to pay all the porto for you. If a letter with too low stamps arrives at my home, I will not answer or I will send it to you and you have to pay the porto !

So, please think about it !

My adress:

Markus Schmall
von Graevemeyerweg 25
30539 Hannover

Due to the really "great" opinion of the shareware idea, I recieved 1 letter with the share in a period of 11 weeks.THANKS!

1.4 prefs

VirusWorkshop Preferences Menu

AutoRamKill

AutoSpeicherKill!

The Explode Function

Imploder Funkt.

The FileID Function

New Preferencesfilestructure

Back to the mainmenu

1.5 newpref

Structure of the new preferencesfile:

1.Longword: for the screenresolution.
2.Longword
1.Byte: If "1" then the AUTOKILL function is activated.
2.Byte: If "1" then the FILEID funtion is activated.
3.Byte: If "1" then the decrunch function is activated.
4.Byte: If "1" then you will be asked at the exit, if you really want to do this.

All this functions will be first activated AFTER the RAMcheck.

Struktur des neuen Einstellungsfiles:

1.Langwort: verantwortlich fuer die Auflösung.
2.Langwort
1.Byte: Wenn dieses Byte auf "1" steht, wird die AUTOKILL Funktion aktiviert.
2.Byte: Wenn dieses Byte auf "1" steht, wird die FILEID Funktion aktiviert.
3.Byte: Wenn dieses Byte auf "1" steht, wird die Decrunch Funktion aktiviert.
4.Byte: Wenn dieses Byte auf "1" steht, werden Sie bei verlassen von VirusWorkshop gefragt, ob sie dies wirklich tun wollen.

Diese Funktionen werden erst nach dem ersten RAMcheck aktiviert.

1.6 fileid2

Wenn Sie diese Funktion aktivieren wird VirusWorkshop die FileID Library verwenden,um den Filetyp zu erkennen.Diese Library erkennt über 480 verschiedene Filetypen. Achtung:Der Speicherbedarf nimmt zu und die Geschwindigkeit beim Testen nimmt ab.

Die FileID Library wurde von Bloodrock/SDC programmiert.
Das VirusWorkshop Archiv enthält V5.1 dieser Library.

1.7 fileid

If you start this option,VirusWorkshop will use the FileID.Lib to recognizes over 480 different fileformats.The recognition results can be sometimes wrong but recognition rate is very high.Please note that this function slows down the testprocess a little bit and the memoryusage is higher.

The FileID Library was written by Bloodrock/SDC.
(Version 5.1 is included in this archive.)

1.8 intro

Introduction to VirusWorkshop:

Welcome to another new viruskiller on the AMIGA(C). This virus-killer was programmed to help you to get rid of all the viruses hanging around. VirusWorkshop handles a big number of trojan horses, which try change the AmiExpress(C) mailbox programm and it is ideal for users,who just want to check their software in a very secure way for viruses and diskerrors.

VirusWorkshop is another try to make a viruskiller for a special usergroup.I think it is good to support Kickstart 1.x but the new features should be supported.VirusWorkshop needs at least 1 MB of memory to work properly.

Some of the functions (especially DECRUNCHING) take a lot of time, but the time goes on and higher processors than the MC68000 can be found at every corner.The decrunch process needs a lot of memory. VirusWorkshop uses for decrunching the mighty XFDmaster Library by Georg Hoermann(*).

Support OS2.XX higher version and let the AMIGA get the rank in the computerbusiness,which it deserves because of it's powerfull chips and the really good operating system.

The author allows the spreading of VirusWorkshop in any form.
But don't take more than 4 US$ or 6 DM for a viruskillerdisk,which contains VirusWorkshop.

This especially counts for a big german shop, which sells a packet containing several viruskillers for more than 18 $. This is not allowed.

It's not allowed to spread VirusWorkshop on S.H.I. discs.

(Exceptions: Jim & Becky Maciorowski, Lars Kristensen
and Jan Bo Andersen)

(*) Some words about the Xfdmaster Library: This library is very well coded but contains some bugs concerning powerpacked files. In other words: It can come to problems with powerpacked files.I cannot test, if this is based on bugs in PP or in the library, but the programms itself work on my AMIGA.

1.9 einführung

Vorwort zu VirusWorkshop

Herzlich willkommen zu einem neuen Viruskiller auf dem AMIGA.Dieser Viruskiller wurde programmiert,um Ihnen zu helfen,die Virenprobleme entgültig zu vergessen.VirusWorkshop erkennt eine große Anzahl an trojanischen Pferden,die speziell auf das AmiExpress Mailboxsystem ausgerichtet sind.VirusWorkshop is ideal für User,die auf einfache Weise Ihr System auf eine sehr sichere Methode untersuchen wollen.

VirusWorkshop ist ein weiterer Versuch,einen Viruskiller für eine spezielle Usergruppe zu erstellen. Die Idee,Kickstart 1.x zu unterstützen ist generell nicht schlecht,aber OS 2.xx ist eindeutig der Stand der Dinge. VirusWorkshop braucht mindestens 1 Megabyte Speicher um zu arbeiten.

Einige der Funktionen (insbesondere das Entpacken) benötigen sehr viel Zeit und Speicher,aber die Zeit schreitet voran und schnellere Prozessoren als der MC68000 können an jeder Ecke zu angemessenen Preisen erworben werden.

Unterstützen Sie OS2.xx und neuere Version und gewährleisten Sie damit, daß der AMIGA den Rang bekommt, der ihm aufgrund seiner leistungsfähigen Chips zusteht.

Die Verbreitung von VirusWorkshop wird ausdrücklich befürwortet. Ausnahmen:

1. KEINE Verbreitung auf S.H.I. Disketten...
   (mit Ausnahme der folgenden Personen und Zentren: SHI Reginal-Center in Daenemark (nicht das Daene HQ, welches von Erik Loevendahl Soerensen geleitet wird), welches von Lars Kristensen und Jan Bo Andersen geleitet wird.

   Ich habe keinerlei Interesse in Verbindung mit Erik Loevendahl Soerensen oder S.H.I. gebracht zu werden.

2. VirusWorkshop darf nicht auf Disketten verkauft werden, die mehr als 6 DM kosten (4us$).

Dies gilt natürlich auch für Kaufhausketten und andere Anbieter. Es gibt ein erschreckendes Beispiel in Deutschland, wo ein Packet mit Viruskillern für 29 DM verkauft wird. Es ist schon dreist einen solchen Preis zu verlangen! Mall..... heißt dieser nette Laden, der solche Wucherpreise nimmt.

1.10 copyright

Copyright:

This programm was developed to help people to get rid of problems with viruses. The author takes no responsibility if damage is caused by the use of this programm.

All parts of the programm are copyrighted by Markus Schmall.

Except:
- "XfDmaster.library", which is copyrighted by Georg Hoermann (VirusZ).
- "reqtools.library", which is copyrighted by Nico François (PowerPacker).
- "FileID.library", which is copyrighted by Bloodrock/SDC.

Comment 13.03.1994: VirusWorkshop now uses intern the decrunch-routines from the great CrunchMania packer. CrunchMania is share-ware and was written by Thomas Schwarz.

All coders gave permission to include their libraries in every non commercial and free distributable production. If you want to sell this programm the final price for the customer should not be higher than $6 US dollars (this includes the costs for media and postage!).

It's not allowed to spread VirusWorkshop on S.H.I. diskettes.

Exceptions: Jan Bo Andersen and Lars Kristensen from the reginal center in Denmark.

1.11 kopierrecht

Dieses Programm wurde entwickelt um Usern zu helfen, die lästigen Viren zu vernichten. Der Autor übernimmt keine Verantwortung für Schäden, die durch die Benutzung dieses Programmes entstehen.

Auf alle Programmteile hat Markus Schmall das Copyright.

Außer auf:

- "XfDmaster.library", für welche Georg Hoermann das Copyright besitzt.
- "reqtools.library", für welche Nico Francois das Copyright besitzt.
- "FileID.library", für welche Bloodrock/SDC das Copyright besitzt.

Alle Programmierer haben die Erlaubniss gegeben,ihre Libraries in jeder nicht kommerziellen und frei kopierbaren Produktion zu ver-wenden.Wenn Sie VirusWorkshop verkaufen wollen,dann stelle ich folgende Bedingung:

Der Endpreis,welcher Porto,Verpackung etc.enthält, darf nicht höher als 6 US Dollar sein.

Bitte beachten Sie, daß VirusWorkshop NICHT auf SHI Disketten verteilt werden darf. Die EINZIGE Ausnahme mache ich bei Jan Bo Andersen und Lars Kristensen von dem regionalen Viruscenter in Daenemark, was aber nicht einschliesst, dass VirusWorkshop dann z.B. auch von Erik Loevendahl Soerensen auf seinen SHI Disketten verteilt werden darf.

Zusatz 13.03.1994: Intern werden jetzt die Entpackroutinen des CrunchMania Packers verwendet. CrunchMania is Shareware und wurde von Thomas Schwarz geschrieben.

1.12 releasenote

Release notes:

This programm should work on:

1.All AMIGA computers with the following KICKSTART versions:

-Kickstart V2.04 (V37.175 on A3000/A2000/A500(+))
-Kickstart V2.05 (V37.300)
-Kickstart V2.06 (V37.350)
-Kickstart V3.00 (V39.106)
-Kickstart V3.00a (V39.106b in the A1200)
-Kickstart V3.02 (V39.116BETA for the A4000) *
-Kickstart V3.03 (V40.9BETA for the A4000) *
-Kickstart V3.04 (V40.38BETA for the A4000) *
-Kickstart V3.1ß (V40.55 for the A4000) *
-Kickstart V3.1ß (V40.55 for the A3000) *
-Kickstart V3.1 (V40.62 for the A4000)
-Kickstart V3.1 (V40.62 for the A3000)
-Kickstart V3.1 (V40.68 for the A4000)
-Kickstart V3.1 (V40.68 for the A3000)

2. Amigas with MMUs, FPUs.
3. Amigas with 680xx prozessors (even on the MC68040).
4. All chipsets including the new AGA system.

We tested the programm with nearly all Workbench versions (including the new version 40.42) and SetPatch commands and all worked just fine.

The programm should work now on A600HDs and A600s, too. If there are any problems, then please let me know it. I have only written the OS routines and had no testmachines.

All caches etc. will be supported and the new COPYBACK mode from MC68040 is working, too.

This programm does crash, if utilities like ReKick are active. It is caused by the fact that the programm only checks the ROMs!In my opinion this is no bad fact because only some developers and hackers use such tools.

The programm was developed with the use of Kickstart 3.0x . It works with older Kickstart version in the same way. Consider buying a new Kickstart version because only the new versions (OS2.++) make the AMIGA real worth using.

The Intuition Interface was designed using GadToolsBox 37.300 by JABA Developments.

VirusWorkshop is no background viruskiller.Every writecommand from an other programm can change the directory structure and the disc information cannot (sometimes) be completely checked.

Another point is that the usage of memory is too big.

This programm needs: 1. xfdmaster.library
2. reqtools.library
3. DMS packer (only if you use DMS check!)
4. OWS packer (" OWS)
5. gadtools.library
6. FileID.library
7. AmigaGuide (*) library

How many memory needs this viruskiller?

About 270 KB mainprogramm and the memory for the libraries and for the files. This means that it needs approx. 650 KB, when you try to check files. Result:

THIS PROGRAMM REQUIRES AT LEAST 1 MEGABYTE TO WORK.

I think this is not a real big disadvantage,because every real user should have at least 1MB memory.

This viruskiller was spreaded as a LHA archive with the name "TRSIVW37.lha". It contains the following files:

VirusWorkshop
VirusWorkshop.info

```
      Virusworkshop-News
      VirusWorkshop-News.Info
      FILE_ID.DIZ
      Install
      Install.Info
      Install.script
      Pref-Edit
      Pref-Edit.info
      Vw.Displayme
      VW.prefs
      VW.prefs.README
      MagiCWb.readme
         MAGICWB/...
         LIBS/explode.library
         LIBS/reqtools.library
         LIBS/xfdmaster.library
         LIBS/fileID.library
         DOCUMENTS/Virusworkshop.Guide
         DOCUMENTS/Virusworkshop.Guide.INFO
         DOCUMENTS/VWMemmon.Guide
         DOCUMENTS/VWMemmon.Guide.INFO
         DOCUMENTS/Starterproblems.Guide
         DOCUMENTS/Starterproblems.Guide.INFO
         DOCUMENTS/Pref-Edit.Guide
         DOCUMENTS/Pref-Edit.Guide.INFO
         DOCUMENTS/NewVirus.Guide
         DOCUMENTS/NewVirus.Guide.INFO
         DOCUMENTS/DHunk.Guide
         DOCUMENTS/Dhunk.Guide.INFO
         TOOLS/Dhunk
   TOOLS/Dhunk.INFO


* = This Kickstartrelease  will  be  correctly  recognized,but  the
      the Memorykill function is not fully avaible because this is a
      BETA release and newer (official) versions are on the market.

      (*) AmigaGuide  Library  is  (C) by  Commodore. Therefore I am  not
      allowed to spread this library in the VirusWorkshop package.
```

1.13 veröffentlichung

```
                  Notizen für die Veröffentlichung
                  --------------------------------


VirusWorkshop sollte auf folgenden Rechnern arbeiten:



      1.Allen AMIGA Rechner mit folgenden Betriebssystemversionen:
      (diese Versionen müssen aber an den original ROM Adressen
      liegen. Also keine Kickstartversion bei $2000000!!!!)
```

-Kickstart V2.04 (V37.175 im A3000 und A2000/A500(+))
-Kickstart V2.05 (V37.300)
-Kickstart V2.06 (V37.350)
-Kickstart V3.00 (V39.106)
-Kickstart V3.00a (V39.106b für den A1200)
-Kickstart V3.02 (V39.116BETA für den A4000) *
-Kickstart V3.03 (V40.9BETA für den A4000) *
-Kickstart V3.04 (V40.38BETA für den A4000) *
-Kickstart V3.1ß (V40.55 für den A4000) *
-Kickstart V3.1ß (V40.55 für den A3000) *
-Kickstart V3.1 (V40.62 für den A4000)
-Kickstart V3.1 (V40.62 für den A3000)
-Kickstart V3.1 (V40.68 für den A4000)
-Kickstart V3.1 (V40.68 für den A3000)

2. Amigas mit MMU, FPU.
3. Amigas mit 680xx Prozessoren (einschließlich MC68040)
4. Amigas mit normalen,enhanced (ECS) oder AGA Chipset.

Das Programm wurde mit sämtlichen (für uns verfügbaren) Workbench-versionen getestet (einschließlich der Workbench 40.35) und alle Funktionen arbeiteten gut.

Das Programm sollte auf A600HD und A600 arbeiten.Wenn Probleme auftauchen, dann lassen Sie es mich bitte wissen. Ich habe nur die Routinen für diese Rechner geschrieben.Leider standen mir keine Testrechner zur Verfügung.

VirusWorkshop hat keine Probleme mit den Caches der Prozessoren MC68030 und MC68040.

Das Programm läuft nicht (bzw. der Vectorkiller),wenn Programme wie Rekick oder ZKick aktiv sind.VirusWorkshop testet direkt die ROMs.

VirusWorkshop wurde entwickelt unter Kickstart 3.0. Es arbeitet mit allen Betriebssystemversion größer=gleich V2.04.

Das Intuition Interface wurde entwickelt mit der Hilfe der GadTools Box 37.300,welche von JABA Developments geschrieben wurde.

VirusWorkshop ist kein Hintergrundviruskiller.Wenn Sie einen solchen Viruskiller benötigen, rate ich Ihnen zu VirusZ. Jedes Schreibkommando kann die Direktorystruktur verändern und es kann zu Fehlern beim Checken einer Diskette führen. Außerdem ist der Speicherverbrauch zu hoch.

VirusWorkshop benötigt: 1. xfdmaster.library
2. reqtools.library
3. DMS packer (nur beim DMS CHECK
4. OWS packer (" OWS)
5. gadtools.library
6. FileID.library
7. AmigaGuide Library (*)

Wiviel Speicher braucht VirusWorkshop ?

Ca.270 KB Speicher werden für das Hauptprogramm benötigt. Dazu kommen 250 KB für den Filecheck Buffer und zusätzlich noch Speicher für die Libraries und für Intuition.

Dieser Viruskiller wird in einem LHA Archiv mit dem Namen:

"TRSIVW37.lha" weitergegeben.Es enthält folgenden Files:

```
VirusWorkshop
VirusWorkshop.info
Virusworkshop-News
VirusWorkshop-News.Info
FILE_ID.DIZ
Install
Install.Info
Install.script
Pref-Edit
Pref-Edit.info
Vw.Displayme
VW.prefs
VW.prefs.README
MagiCWb.readme
   MAGICWB/...
   LIBS/explode.library
   LIBS/reqtools.library
   LIBS/xfdmaster.library
   LIBS/fileID.library
   DOCUMENTS/Virusworkshop.Guide
   DOCUMENTS/Virusworkshop.Guide.INFO
   DOCUMENTS/VWMemmon.Guide
   DOCUMENTS/VWMemmon.Guide.INFO
   DOCUMENTS/Starterproblems.Guide
   DOCUMENTS/Starterproblems.Guide.INFO
   DOCUMENTS/Pref-Edit.Guide
   DOCUMENTS/Pref-Edit.Guide.INFO
   DOCUMENTS/NewVirus.Guide
   DOCUMENTS/NewVirus.Guide.INFO
   DOCUMENTS/DHunk.Guide
   DOCUMENTS/Dhunk.Guide.INFO
   TOOLS/Dhunk
TOOLS/Dhunk.INFO
```

* =Diese Kickstartversion wird zwar korrekt erkannt, aber die VectorkillerFunktion ist nicht aktiv, da neuere Betaversionen existieren.
(*)= Auf die AmigaGuide Library hat Commodore das Copyright und daher ist es mir untersagt, diese Library mit in das VW Packet einzubinden.

1.14 menuinstruction

```
                    Description of the menus:
                    -------------------------


On the top there are two big boxes with some important information:

1a. Which Kickstart is used?
2a. Where is the VBR pointing to?
3a. Is the FILEID function activated(DEFAULT=NO)?
4a. Is the AUTOKILL function activated(DEFAULT=NO)?
      5a. Is the DECRUNCH function activated(DEFAULT=NO)?
1b. Which CPU do you use?
2b. Which FPU do you use?
3b. Which MMU do you use?


At  the  moment  I  only use the AttnFlags in Execbase (296(a6)) to
test this stuff. If my new assembler arrives I am going to write an
optimized check  routine which executes  some MMU and FPU commands.
The assembler I am using at moment, does not support their
instructions...
```

1.15 menuerklärung

```
                        Beschreibung der Oberfläche
                        ---------------------------


      Sie können 2 große Boxen im oberen Viertel erkennen,welche wichtige
      Informationen beeinhalten:


      1a. Welche Kickstartversion wird verwendet ?
      2a. Wohin zeigt das VBR ?
      3a. Ist die FileID Funktion aktiviert ? (Grundeinstellung=Nein)
      4a. Ist die Autokill Funktion aktiviert ? (Grundeinstellung=NEIN)
      5a. Ist die Decrunch Funktion aktiviert ? (Grundeinstellung=NEIN).

      Ich benutze z.Z. nur die AttnFlags aus der Execbase (296) um  diese
      Werte zu erhalten.Mein derzeitiger Assembler hat Probleme mit der
      MMU und der FPU. Sobald eine  neue  Version, die richtig  arbeitet,
      auf dem Markt ist, wird dieses Manko behoben.
```

1.16 sectorcheck

Sector Check:

Path 1:

First of all the Disk-Validator will be loaded and checked for viruses. This will be done under all Kickstarts and FileSystems. The following DOSTYPES will be supported:

1. DOS0 = old Slow File System
2. DOS1 = old Fast File System
3. DOS2 = SFS with international mode (Kick 2.00+)
4. DOS3 = FFS with international mode
5. DOS4 = SFS with international mode and Dircache (Kick 3.00+)
6. DOS5 = FFS with international mode and Dircache

Slow File System = SFS
Fast File System = FFS

At the moment there are more than 11 viruses, which can infect the Disk-Validator:

1. Saddam Hussein 1+2+3+4+5+6 (No. 2 contains a new crypt-routine and No. 3-5 are only simple editor patches!)
2. Return of the Lamer Exterminator (father of the Saddam virus?)
3. Diskval1234 (a Saddam clone)
4. Risc Diskvalidator (also Saddam clone)
5. Saddam V1.29 & Laurien (changed Saddam][/ editor patches) (several new Saddam viruses appeared!!!)

Known Damages:

All of this viruses can change the information of the tracks. The R.O.T.L.E. and the Diskval1234 Virus can completely destroy the information in the sectors. I do not own the RISC virus,so if you have it please send it to me.

The Return of the Lamer Exterminator uses the OK Flag (Offset $138 Rootblock) to be activated. VirusWorkshop deletes the virus and writes a normal validator on the disk. The changed flag will not be fixed because there can be other error on the disk, too. Simply reset your machine and load your workbench. Then insert the previous infected disk. Follow the instructions and your disk will be correct again.

Path 2:

All sectors will be loaded and checked for viruses. Damages caused by the SADDAM (+ clones) and by the LITTLE SVEN virus will be fixed. All other failures cannot be fixed. If a sector is a part of a very important file, you have bad luck. There is NO(!) way to rescue the file.

The damage caused by SHIT, Fast Eddie, Overkill, Crime92 and the Lamer Exterminator viruses cannot be fixed. All sectorbased routines cannot be 100 % secure on FFS because the sectordata can be equal to the data written by a virus! (This is not my fault!It is because of the new structures of this system!)

Saddam and it clones check the sector for the startmark "$8". Then they write their special longwords (e.g. "IRAK) at this position and code (eor) the sectors with the sectornumber. The startmark"$8" declares the sector in the SFS systems as a DATABLOCK. Please note that not all DATABLOCKs are changed! Only the first DATABLOCK of a file will be coded by SADDAM.

I have added a special routine which does not need the Disk-Validator to check a coded string. This routine does not care about the first longword in the sector. Hopy it all works fine now. All clones (e.g. Saddam][1.29) can be easily found and the damage can be repaired. I made this routine only work with DOS0 (OFS) disks because the Saddam Virus only works with this disks. This routine slows down the testprocess but it is really secure.

The Little Sven virus only exchanges the $8 with a $ABCD0008 longword. This damages can and will be fixed!

A routine is included, which checks the whole disk for invalid checksums and similar stuff. It can happen that a requester appears which says:

"SectorChecksum is not correct! Repair?"

You can now fix the block but remeber that there can appear problems, if you use FFS disks (DOS1/3/5). FFS sectors can contain the same data as the recognition mark from OFS and the viruskiller does not recognize it (a general problem!).

If your working drive is a harddisc, VirusWorkshop checks the disc only for invalid checksums. This routine was only written to use it with floppydiscs. I can happen that you have a bugfree HD and VW claims to have found an unnormal sector.

At the last point of the second path there will be loaded the ROOT-block from your drive (DFX:) and it will be scanned for a changed pointer to the BITMAPBLOCK.

The SADDAM Viruses use this method to become installed !!!

Path 3:

The bootblock will be loaded and checked for viruses and tools/intros etc. Then please press the left mousebutton to come back to the main directory. Many guys (especially some foreign members of SAFE HEX INTERNATIONAL) asked me to write a public bootblocklibrary or to include a LEARN function in this viruskiller. I do not code such things because of the danger of MISUSE. Please understand me. I have too often seen some changed extern files from other wellknown tools.

I will never include any extern files for this viruskiller (except the decrunch and reqtools Library). Even protections can be hacked and so I canceled this idea.

(Errare humanum est!)

Following programms will be recognized:

- 284+ bootblock viruses
- 460+ Utility bootblocks

The Sectorchecker has been tested with:

-GVP Serie II Controller on A4000+A2000 (MC68030+MC68000)
-Oktagon Controller on A4000/A2000
-MultiEvolution 2.2 on A500(+)
-Evolution 3.0 on A2000+A3000
-GVPs Combo 2
-normal AT controller in the A4000/A1200

For the tests were the following harddiscs used:

-Quantum ELS+LPS
-Maxtor
-HP
-Fujitsu AT
-Syquest 105 MB SCSI

1.17 sektorcheck

Sektor Check:

Schritt 1:

Zuerst wird der Diskvalidator geladen und auf Virus untersucht. Dieser Vorgang wird bei allen Kickstartversionen durchgeführt.

Folgende Dos bzw. Disktypen werden unterstützt:

1. DOS0 = altes langsames Filesystem
2. DOS1 = altes schnelles Filesystem
3. DOS2 = langsames Filesystem mit internationalem Modus (Kick 2.+)
4. DOS3 = schnelles Filesystem mit "

(Kick 3.+)

5. DOS4 = langsames Filesystem mit internationalem Modus und DirectoryCaching.
6. DOS5 = schnelles Filesystem mit internationalem Modus und Directorycaching.

Zur Zeit sind mehr als 11 Viren bekannt,die den Diskvalidator infizieren können.

Schäden:

Alle Diskvalidatorviren können die Informationen der einzelnen Sektoren verändern.Der Revenge of the Lamer Exterminator und der Diskval1234 Virus zerstören Sektoren so,daß sie nicht wieder repariert werden können.Ich suche dringend nach dem RISC Virus.

Schritt 2:

Jeder Sektor wird einzeln geladen und auf Viren und Fehlern bei den Sektorchecksummen untersucht.Schäden der Saddam Viren und des XCopy 6.5 Viruses (Little Sven) können repariert werden.Fehlerhafte Checksummen werden auf Wunsch on VirusWorkshop auch entfernt. Sektoren,deren Dateninhalt verändert wurde (z.B. vollständiges Überschreibung durch das Wort "LAMER"), können NICHT restauriert werden.

Schäden der folgenden Viren können NICHT restauriert werden:

-SHIT
-FAST EDDIE
-OVERKILL
-CRIME 92
-Lamer EXTERMINATOR
-BURN

Alle Sektorroutinen können NIEMALS 100% sicher bei FFS Disketten sein,da der Sektorinhalt den Daten eines Virus vergleichbar sein kann.

Saddam und die Clones suchen in dem ersten geladenen File nach der Sektormarke $8.Dann wird eine spezielle Sektorkennung (z.B.IRAK) an das erste Langwort des Sektors geschrieben.Die Marke $8 besagt, daß es sich bei dem Sektor um einen Datablock handelt.Nur der 1. Datablock eines Files wird von Saddam Viren codiert.

VirusWorkshop verfügt über eine spezielle Sectorroutine,die nicht auf spezielle Langworte an erster Stelle des Sektors testet. Somit brauchen Sie keine Angst vor neuen Saddam Clones zu haben.

Der Little Sven Virus ersetzt die $8 nur durch $ABCD0008.Dieser Schaden kann von VirusWorkshop behoben werden.

VirusWorkshop verfügt über eine Routine,die die komplette Diskette auf falsche Checksummen testet.Es kann passieren,daß ein Requester mit folgender Meldung erscheint :

"SectorChecksum is not correct! Repair?"

Sie können diesen Schaden beheben,aber bei FFS Disketten besteht keine 100% Sicherheit.

Als letzter Teilschritt wird er Rootblock der Diskette geladen und auf Veränderungen des Saddam Viruses untersucht.

Schritt 3:

Der Bootblock wird geladen und untersucht.VirusWorkshop verwendet keine externen Bootblockbibliotheken!!!!

(Errare humanum est!)

Folgende Programme werden erkannt:

- 284+ Bootblock Viren
- 460+ Bootblöcke mit kleinen Hilfsprogrammen.

Der Sektorchecker wurde getested mit:

-GVP Serie II Controller im A4000+A2000 (MC68030+MC68000)
-Oktagon Controller im A4000/A2000
-MultiEvolution 2.2 im A500(+)
-Evolution 3.0 on A2000+A3000
-GVPs Combo 2
-normaler AT controller in dem A4000/A1200

Folgende Festplatten wurden verwendet:

-Quantum ELS+LPS
-Maxtor
-HP
-Fujitsu AT
-Syquest 105 SCSI

1.18 unnamed.1

```
                          Sector Check:
                          -------------


Path 1:
-------
First  of  all  the  Disk-Validator will  be loaded and checked for
viruses.   This  will be done under all Kickstarts and FileSystems.
The following DOSTYPES will be supported:

1. DOS0 = old Slow File System
2. DOS1 = old Fast File System
3. DOS2 = SFS with international mode                  (Kick 2.00+)
4. DOS3 = FFS with international mode
5. DOS4 = SFS with international mode and Dircache     (Kick 3.00+)
6. DOS5 = FFS with international mode and Dircache


                            Slow File System = SFS
                            Fast File System = FFS



At   the   moment   there  are  more than 11  viruses  known, which
      can  infect  the Disk-Validator:

1. Saddam Hussein 1+2+3+4+5+6 (No. 2 contains a new crypt-routine
         and No. 3-5 are only simple editor patches!)
2. Return of the Lamer Exterminator (father of the Saddam virus?)
3. Diskval1234 (a Saddam clone)
4. Risc Diskvalidator (also Saddam clone)
5. Saddam V1.29 & Laurien (changed Saddam ][ / editor patches)


Known Damages:
--------------
All  of this viruses can change the information of the tracks.  The
R.O.T.L.E.  and  the Diskval1234  Virus can completely  destroy the
information in  the  sectors. I do not own the Diskval1234 and RISC
viruses, so if you have them please send them to me.

The  Return of the Lamer Exterminator uses the OK Flag (Offset $138
Rootblock)  to  be  activated.  VirusWorkshop deletes the virus and
writes  a  normal validator on the disk.  The changed flag will not
be fixed because there can be other error on the disk, too.  Simply
reset  your  machine  and  load  your  workbench.   Then insert the
previous infected disk.  Follow the instructions and your disk will
be correct again.


Path 2:
-------
All sectors will be loaded and checked for viruses.  Damages caused
by  the  SADDAM  (+  clones)  and  by the LITTLE SVEN virus will be
```

fixed. All other failures cannot be fixed. If a sector is a part of a very important file, you have bad luck. There is NO(!) way to rescue the file.

The damage caused by SHIT, Fast Eddie, Overkill, Crime92 and the Lamer Exterminator viruses cannot be fixed. All sectorbased routines cannot be 100 % secure on FFS because the sectordata can be equal to the data written by a virus! (This is not my fault!It is because of the new structures of this system!)

Saddam and it clones check the sector for the startmark "$8". Then they write their special longwords (e.g. "IRAK) at this position and code (eor) the sectors with the sectornumber. The startmark"$8" declares the sector in the SFS systems as a DATABLOCK. Please note that not all DATABLOCKs are changed! Only the first DATABLOCK of a file will be coded by SADDAM.

I have added a special routine which does not need the Disk-Validator to check a coded string. This routine does not care about the first longword in the sector. Hopy it all works fine now. All clones (e.g. Saddam][1.29) can be easily found and the damage can be repaired. I made this routine only work with DOS0 (OFS) disks because the Saddam Virus only works with this disks. This routine slows down the testprocess but it is really secure.

The Little Sven virus only exchanges the $8 with a $ABCD0008 longword. This damages can and will be fixed!

A routine is included, which checks the whole disk for invalid checksums and similar stuff. It can happen that a requester appears which says:

"SectorChecksum is not correct! Repair?"

You can now fix the block but remeber that there can appear problems, if you use FFS disks (DOS1/3/5). FFS sectors can contain the same data as the recognition mark from OFS and the viruskiller does not recognize it (a general problem!).

If your working drive is a harddisc, VirusWorkshop checks the disc only for invalid checksums. This routine was only written to use it with floppydiscs. I can happen that you have a bugfree HD and VW claims to have found an unnormal sector.

At the last point of the second path there will be loaded the ROOT-block from your drive (DFX:) and it will be scanned for a changed pointer to the BITMAPBLOCK.

The SADDAM Viruses use this method to become installed !!!

Path 3:

The bootblock will be loaded and checked for viruses and tools/intros etc. Then please press the left mousebutton to come back to the main directory. Many guys (especially some foreign members of SAFE HEX INTERNATIONAL) asked me to write a public bootblocklibrary or to include a LEARN function in this

viruskiller. I do not code such things because of the danger of MISUSE. Please understand me. I have too often seen some changed extern files from other wellknown tools.

I will never include any extern files for this viruskiller (except the decrunch and reqtools Library). Even protections can be hacked and so I canceled this idea. The whole VirusWorkshop code is much harder to crack than a 50 KB nonpacked bootblocklibrary.

(Errare humanum est!)

Following programms will be recognized:

- 284+ bootblock viruses
- 460+ Utility bootblocks

1.19 dateicheck

Die LinkViren Suchfunktion:

Zuerst wird das angwählte Laufwerk getestet:

1. Ist die Diskette bzw.die Harddisk validiert ?
2. Schreibschutz ?
3. Ist der BitmapZeiger korrekt? (Saddam virus...)

Es kann passieren,daß folgende Mitteilung erscheint:

"Use TrackCheck and DriveInfo first. Dir is not correct!"

Diese Mitteilung erscheint nur,wenn der BitmapZeiger und/oder das Validierungsflag des Rootblockes nicht korrekt ist.Ein falscher Bitmapblockzeiger kann repariert werden.

Danach wird jedes File geladen und auf Viren getestet.Wenn ein Virus gefunden wurde,erscheint eine Mitteilung,die Ihnen die Wahl läßt den Virus zu entfernen oder fortzufahren.Es werden mehr als 115 Linkvirus/trojanische Pferde etc. erkannt.

Wenn Sie den Filetest abbrechen wollen,dann drücken Sie bitte die linke Maustaste.Die letzten Files laufen dann sehr schnell durch (ohne Test etc.) und VirusWorkshop stoppt.

Wenn ein Virus gefunden wurde,dann müssen Sie möglicherweise die Startup-Sequence ändern,da ein Virus unter Umständen in dem File eingetragen war und jetzt,da er nicht mehr vorhanden ist,zu einem Abbruch führen kann.

DMS Check

Diese Funktion ermöglicht es dem User ein DMS Archiv auf das aktuelle Laufwerk zu entpacken und die Diskette danach gründlich zu testen.

Nichts Außergewöhnliches ? Sie müssen nur einmal am Anfang den DMS Pfad einstellen und dananch nur noch das geünschte Archiv auswählen.Gedacht für Sysops oder Trader,die Ihren neuen Programme nur schnell testen wollen.

Achtung ! Für diesen Vorgang benötigen Sie den DMS Packer. Damit ist nicht die DMSWIn Oberfläche gemeint , sondern nur der eigentliche Packer. VirusWorkshop stellt dem Packer ein eigenes Fenster zur Verfügung.Sollte der Speicher knapp werden, wird das normale Ausgabefenster benutzt.

VirusWorkshop arbeitet auch mit gesplitteten Archieven. Diese dürfen nur in 2 Teile geteilt sein (Wer teilt seine Archive in größere Teile ?)

Das File wird von VirusWorkshop immer als komplette Diskette gesichert.Bentuzen Sie danach einen DMS Splitter...

Comment 16.11.1993: VirusWorkshop arbeitet sauber mit den neuen DMS Updates von BLACKHAWK/PDX !!!

Leider arbeitet VirusWorkSHOP nicht mit den DMS Versionen oberhalb V2.0, da eine Eingabe im Fenster erwartet wird, die ich nicht liefern kann.

Filereq

Wenn Sie eine einzelne Datei testen wollen,dann ist dies die richtige Funktion für Sie.

1.Convert : Bootjob 1.3 Dateien werden in normale Bootblöcke zurück konvertiert.

2.SingleF : Wenn Sie eine Datei selektieren,wird diese untersucht. Wenn Sie nur ein Verzeichniss auswählen,wird dieses Verzeichniss untersucht.Es wird nur dieses Verzeichniss untersucht und keine Unterverzeichnisse.

* Mit Bootjob können Sie normale Bootblöcke in normale Files umwandeln.

1.20 filecheck

The File/Link/Trojan Check:

First of all the choosen device will be checked:

1. Is it validated?
2. Is it write enabled?
3. Is the BitmapPtr correct? (Saddam virus...)

It can happen that the following message appears:

"Use TrackCheck and DriveInfo first. Dir is not correct!"

This message only appears if the BitmapPtr and/or the VALIDflag ($138) is not correct. A wrong Bitmap pointer caused by Saddam can be fixed , of course.

Every file will be loaded and scanned for viruses. If a virus was found a little message appears on your screen. You can destroy/fix all known link viruses and trojan horses. Over 115(!) species will be recognised. What do you want more?

If you want to stop the filetest, then simply press the left mousebutton. The last files of your directory become printed very fast on the screen and then the programm stops.

If a virus was found, please check the startup-sequence because it can be possible that you have to fix it: A line has to be deleted...

This function includes a multicheck. Wait, I will explain it to you:

The virus "Revenge of the Lamer Exterminator" (a species, which is not a real link virus like IRQ -> it does not add a hunk etc. to the infected file!) is infected 5 times by the IRQ-II virus. VirusWorkshop will ask you 5 times to kill the "IRQ" virus and as a last step it'll ask you to kill the "Revenge of the Lamer Exterminator" virus. It should work all correct by now. If you have problems, call me!

The Repairroutine for viruses, which add a hunk to the file, is a standart routine. Some viruses (CCCP,QRDL etc.) have wrong infect routines. That means that many files, which are infected with the above listed viruses, does not work. VirusWorkshop is not able to make this programms work again.

DMS Check

This option enables you to depack a DMS archive to a disk and to check the disk for viruses.Nothing special you may say.BUT you have only to specify the file you want to check and the dest. drive.At the start you have (only at the first start) to specify where the original DMSpacker can be found !Very usefull for SYSOPs and other person, who just want to check their new files and does not want to leave the VirusWorkshop.

ATTENTION: The DMS packer (and not DMSwin) is needed.This packer is not included in the VirusWorkshop archieve.VirusWorkshop has been tested with DMS1.11, DMS1.11+, DMS 1.53 and DMS 2.02.
The output window for the DMS information is a special CON window, if you have enough free memory.If your free memory is too low, then the original WB output window will be used(or the CLI window, if you start the VirusWorkshop from your CLI).

VirusWorkshop recognizes both,splitted and complete archieves.If it detects a splitted archive it will ask for a second time for a name from an archive.I think this is enough.Who splits a normal DMS archieve in more than 2 parts ? Nobody I think.

The corrected and repacked archive will contain the whole disk and not only the splitted disc.Use a splitting archive after working with VirusWorkshop.

Comment 23.07.1993.:I have added an OWS checker,too.OWS is a diskwarper like DMS.This routine does not support singlediscs or such comfortable stuff.If you have once selected the DMS archiever it is too late.The DMS archiever will be used always.OWS is not often used on BBSs (at least I did not see one packed OWS file) but some users asked me to include this.

OWS is copyrighted by M.Pendec (Creativ Productions).
The actual version of OWS is 1.2c (08.08.1993.)

Comment 08.08.1993: I heard about problems with decrunching DMS files.I am using the DMS V1.11 Turbo Generic and it is working perfect.

Comment 16.11.1993: VirusWorkshop works perfect with the new DMS updates by BLACKHAWK/PDX. I am very sorry, but the new DMS 2.0x versions can't be used at the moment, because DMS wants to have an answer in the window, which I cannot produce.

Filereq

If you just want to test a single file, this is your right funtion. You can select, what to do.

1.Convert : Bootjob 1.3 files will be reconverted to normal boot-blocks and you can save the bootblock as a normal 1024 byte long file.

2.SingleF : You select a filename and this file will be scanned for viruses. If a virus was found, you can repair/delete the file,if you want to do this.

2a (VW2.4 and higher!): SingleF: You select only a directory and all files in the directory will be checked.

* Bootjob is a tool which can write bootblocks to disks as files, sectors and as a normal executable file.A virus can be saved as a normal file and can be given to other person and no viruskiller will find it.USE IT WITH CAUTION !!!!

1.21 memorycheck

Die Speicher-Kontroll Funktion:

Folgende Pointer werde untersucht:

- fast alle Offsets der Exec & Dosbase
- die komplette Zeropage & Vectorpage
- Interrupts und Server

Sie können weiterhin Devices,Ports,Libraries,Tasks, Resourcen und Semaphoren testen. Diese Funktionen sind sind NICHT in der eigentlichen Speicher-Kontroll Funktion eingebaut,sondern müssen extra gestartet werden.

Weiße Schrift bedeutet IMMER,daß in Ihrem System einige Vektoren NICHT in ihrem normalen Zystand sind.Zögern Sie nicht,verbogene Vektoren zu löschen.Es werden zwar auch alle Patches entfernt, aber Sie können auch fast sicher sein,daß sich kein Virus im SPeicher befindet.

! VirusWorkshop erkennt die Viren nicht mit Namen im SPeicher !

Erkannte Patches (englisch)

1.22 ramcheck

The Memory Check Function:

The following things will be checked:

- everything in ExecBase (library)
- everything in DosBase (library)
- Interrupts and Servers

You can also check devices, ports, libraries, tasks, resources and semaphores. This functions are not included in the RamCheck, however, in the same menu. The RamCheck function is the most important thing. All vectors in white letters are important. If you use SetPatch or similar stuff do not wonder about the high amount of changed vectors in Exec and Intuition. This functions are not printed in white letters!

IF WHITE LETTERS APPEAR, YOU SHOULD USE VECTORKILL!!!

If only one white text appears which says "Caused by explode.libs", then don't worry. It is the caused by the explode.library, a decrunching library for the great Turbo Imploder. Make sure that you only use version 6 and higher. Many bugs have been fixed and the accelerator card problems does not exist anymore.

All interrupts will be shown (zeropage and vectorpage). Several viruskillers only test the zeropage. There are some clever viruses, which do not touch the zeropage but modify the vectorpage. VirusWorkshop will show you both types!

VirusWorkshop does not know all viruses by name in RAM. If you see some white letters, just kill it. It does not destroy your system.

Attention:

Comment 24.01.1993: I have included a little "REKICK" test. All kickfiles should be detected by now. Note that I cannot give you in this way the 100% security because nearly all vectors point in the memory.

THIS FUNCTION CAUSES ENFORCERHITS BECAUSE IT READS THE ZEROPAGE & THE VECTORPAGE. THERE IS NO WAY TO SOLVE THIS PROBLEM. LIVE WITH IT

OR LET THE VIRUSES STAY ALIVE. ALL OTHER VIRUSKILLERS CAUSE SUCH ENFORCER HITS, TOO.

If the ENFORCER is running, you $64 vector in the vectorbase is not correct. You can kill it but then is ENFORCER dead,too.

Comment 31.03.93: I have heard some rumors that a new Enforcer (37.36) is on the market right now. This version does not touch the $64 vec.!!

Comment 18.04.93: I have finally recieved Enforcer V37.36 and my Enforcer does touch the $64 vector. Two versions in circulation ?

Recognized patches

1.23 patches

The following patches will be recognized from VW:

- CPUClr 3.1 by P.Simon: It is patch for a GFX BLIT function, which makes the processor (only usefull for 68030&68040) make the work, because it is a lot faster than the good old BLITTER.

- Switch NTSC by M.Kamper: This is a patch for the Int.OPENSCREEN function under Kickstart 2.xx.

- PatchAsm 1.0 by Flake/D-TECT: It is patch which changes a special byterow, which will be written from the ASM-One 1.15 release (TFA).

- Enforcer V37.28/36/39/49/52 by M.Sinz :Nothing more to say about this great debugger tools. The recognition code takes the $64 vector in the vectorpage, which will be changed by ENFORCER.

- Explode Library by J.A.Brower : This library patches the LOADSEG and in newer releases the NEWLOADSEG vectors in the Doslibrary. All with IMPLODER crunched files will be automatically decrunched.

- Segtracker by M.Sinz : This is a special tool for the ENFORCER friends of you. Changed offsets are (NEW)loadseg and Unloadseg. Segtracker 37.55 will be detected now, too (37.55).

- Selfdefender 0.900 by ?? : This programm is mainly used by BBS owners.It patches some vectors which can (will) be used at a system failure (GURU). The GURU does not appear because the SELFDEFENDER resets your machiene.All programms,which use the normal system requester routines crash.VW does not crash because of the use of the reqtools.library.

- Action Replay IV Software Update by Blackhawk/Paradox.This is a software update from the AR-III eprom software.Now it works with the A1200/A4000.
NOTE: This programm is not a real update by Datel. When will come

your update ?

- DosTrace 1.0 & 2.0 by Peter Stuer: This is a programm like SnoopDos.It requires at least 512 KB memory and Kickstart 2.04. Over 10 vectors will be patched as default from DosTrace .VW re-writes the complete librarievectors and not only the 10 patched vectors.

- DosTouch 1.x : This is a SnoopDosclone like DosTrace.This patch will be removed correctly and only the patched vectors will be re-stored.

- NewAlert by Brian Gontowski: This patch installs a new ALERT-routine,which shows the user more informations than the real ALERT routine.Many Errors etc. will be shown.This tool is Kick2.++ only . The following vectors will be changed by this tool:
Kicktagpointer,Kickmempointer & Kickchckpointer...

- Degrader 1.60 by Chris Hames: This tool enables the user to run many systemfriendly programms,which does not want to work with AGA Amiga computers.You can emulate the PAL mode and other very interesting things.
The changed Coldcapture Vector will be rewritten...

- Virus Interceptor 1.14 by J.Eliasson: An antivirustool,which patches the LOADSEG & NEWLOADSEG vectors.Works with Kickstart 3.0.

Comment 16.11.1993: Fixed for version 1.15 !

- PPLoadseg 1.4 by Nico Francois: This tool patches the LOADSEG-vector and enables the user to use transparent PP data files.VW can rewrite the original LoadSeg vector.

- PowerData 38.200 by Mr.Berg: This tool makes the PP data files completely transparent.The datafiles can be loaded and decrunched. On the other hand the normal datafiles can be crunched while saving them.The following Dos vectors will be changed:
DOS Open,DOS Close,DOS Examine,DOS Write ...
VW can only rewrite ALL vectors...

- Dircache 1.02 by L.Wolf:This tool is a diskcaching programm. It patches the BeginIO Vector of the specified device.Sometimes VW can recover the original value.In all other cases,VW tries to recover all vectors.

- RT Patch 1.1 & RT Patch 1.2:You should only use the newer&better version 1.2 of this programm.It patches several library,so that the REQTOOLS Library will be used.

- Syndicate Coder Patcher 37.18: This is a little tool, which installs a little patch in DosRead& DosWrite to (de)code the file, which is going to be accessed. Very positiv that this tool can remove itself by the "r" option.

1.24 scsupport

Supported Screen Resolutions

IMPORTANT: If you have an AMIGA 4000 with a 1084 monitor or a similar monitor, which does not work with higher AGA modes then please clear all monitordrives (except PAL and NTSC) in your directory sys:devs/monitors.
You cannot use other resolutions ! Think about buying a better monitor ! This "bug" appears with other programms, too.
(This text was copied from the great VT docfile !)

The following resoltions will be supported:

1.PAL HIGHRES (all chipsets / activated by default)
2.PAL HIGHRES INTERLACE (all chipsets)
This mode can be selected by starting VW with the option "i0".
3.PAL EURO72 (only ECS/AGA=640*400 with 69 Hz)
This mode can be selected by starting VW with the option "i0 1".
4.PAL Multiscan (only ECS/AGA=640*480 with 59 Hz)
This mode can be selected by starting VW with the option "i0 2".
5.PAL Super72 (only ECS/AGA=800*300 with 73 Hz)
This mode can be selected by starting VW with the option "i0 3".
6.NTSC Highres Interlace (all chipsets 640*400 with 25 hz)
This mode can be selected by starting VW with the option "i0 4".
7.DBLNTSC Highres Interlace (all chipsets 640*400 with 50 hz)
This mode can be selected by starting VW with the option "i0 5".
8.Picasso-2 640*480 (only with monitorfile 2.14+)
This mode can be selected by starting VW with the option "i0 6".
9.Picasso-2 800*600 (only with monitorfile 2.14+)
This mode can be selected by starting VW with the option "i0 7".

The PICASSO-2 is a very powerfull graphiccard for the AMIGA. Starting with the monitorfile 2.14 Commodore have given Village Tronic new monitorids, which should be the final words....

The modes 3-5 should work on all AA and ECS AMIGAS with a multisync monitor. I am not responsible for a damaged monitor caused by the use of VW,because I do not test for the connected monitor. It is your fault,if you trash your monitor.

You should should only use the "i0" option, if you have a multisync monitor.All other monitors should have problems with it or can be destroyed.

If you want to start VW from the Workbench then you have the possibility to create a preferences file.
The file must be in the s-directory of your bootdevice(SYS) and has to be named "sys:s/VW.prefs".The file has to contain the normal CLI parameters.

Example:

Simply enter "i0 1" (for Euro72) and save the file from your text-editor.If you have created a preferencesfile and want to use a different resolution just this time,then you can use the normal CLI parameters (they have priority).For the normal PAL HIGHRES mode then start VW from the CLI with the option "AA".

COMMENT: The Super72 mode is supported since the release of VirusWorkshop 2.5.

New Preferencesfilestructure

1.25 screenmodi

Unterstützte Screenauflösungen:

Wichtig: Wenn Sie einen A4000 mit einem 1084 Monitor (oder einem ähnlichen Gerät) benutzen, dann löschen Sie bitte alle Monitor-treiber aus dem devs/monitors Ordner bis auf PAL und NTSC. Andere Modi können Sie mit einem solchen Monitor so oder so nicht benutzen !
(Diese Textpassage wurde vondem großartigen VT Dokument kopiert!)

Folgende Auflösungen sind verfügbar:

1.PAL HIGHRES (alle Chipsätze/voreingestellt)
2.PAL HIGHRES INTERLACE (alle Chipsätze)
Dieser Modues kann mit dem CLI Argument "i0" gewählt werden.
3.PAL EURO72 (nur ECS/AGA=640*400 mit 69 Hz)
Dieser Modues kann mit dem CLI Argument "i0 1" gewählt werden.
4.PAL Multiscan (nur ECS/AGA=640*480 mit 59 Hz)
Dieser Modues kann mit dem CLI Argument "i0 2" gewählt werden.
5.PAL Super72 (nur ECS/AGA=800*300 mit 73 Hz)
Dieser Modues kann mit dem CLI Argument "i0 3" gewählt werden.
6.NTSC Highres Interlace (alle Chipsätze 640*400 mit 25 hz)
Dieser Modues kann mit dem CLI Argument "i0 4" gewählt werden.
7.DBLNTSC Highres Interlace (alle Chipsätze 640*400 mit 50 hz)
Dieser Modues kann mit dem CLI Argument "i0 5" gewählt werden.
8.Picasso-2 640*480 (nur mit dem Monitorfile 2.14 oder hoeher !!!)
Dieser Modues kann mit dem CLI Argument "i0 6" gewählt werden.
9.Picasso-2 800*600 (nur mit dem Monitorfile 2.14 oder hoeher !!!)
Dieser Modues kann mit dem CLI Argument "i0 7" gewählt werden.

Die Modi 3-5 können nur mit AGA Amigas (oder auch ECS?) betrieben werden.Ich bin nicht verantwortlich für beschädigte Monitore,die durch VirusWorkshop entstanden sind.

VW unterstützt ein Preferencesfile.Es heißt: "SYS:s/VW.PREFS" und enthält die normalen CLI Optionen.

(Sehen Sie sich bitte auch das Beispiel in dem Archiv an !!!!)

New Preferencesfilestructure

1.26 boot->file

Die Bootblock zu File Funktion

Achtung ! Das aktuelle Laufwerk MUß DFx sein !

Der Bootblock wird geladen und danach als File auf Diskette gesichert.Diese Funktion arbeitet unabhängig von der DOS Version und kann sowohl 1024 als auch 2048 Byte lange Bootblöcke bearbeiten.

Normalerweise sind Bootblöcke 1024 Byte lang.Wenn Sie eine Disk haben,die direkt aus dem Bootblock startet (z.B. Pinball Fantasies oder fast alle Spiele von Psygnosis oder das Demo "Voyage" von Razor),kann es ganz sinnvoll sein,2048 Bytes zu sichern.Viren, wie z.B. der OVERKILL Virus überschreiben nähmlich auch die Sektoren 2-3 und der Lader versagt und es kommt in den meisten Fällen zu einem Systemabsturz.

1.27 boot_to_file

The Bootblock to File Function:

Note: The working drive must be DF0:, DF1:, DF2: or DF3:!

The bootblock (BB) will be loaded and then saved to disk. This function supports all FileSystems and works with 1024 / 2048 byte long bootblocks.

The normal situation is that you only have to save 1024 bytes. If you have a disk, which loads directly from the bootblock (e.g. all Psygnosis games or trackloader demos e.g. Voyage/Razor 1911) it could be useful if you save 2048 bytes. If a virus like 'OVERKILL'

copies the first 1024 bytes into sector 2-3, the data in this sectors are destroyed and the loader can crash.

1.28 file_to_boot

The File to Bootblock function:

Note: The working drive must be DF0:, DF1:, DF2: or DF3:!

A chosen file will be loaded and checked for DOSx. If everything is correct, the bootblock will be written to disk.

1.29 file->boot

Die File zu Bootblock Funktion

Achtung ! Das aktuelle Laufwerk MUß DFx sein !

Das selektierte File wird geladen und auf "DOS " gecheckt.Wenn es korrekt ist,wird es als Bootblock auf die Diskette geschrieben.

1.30 bb_install

Die Bootblock Installierungsfunktion:

Bitte beachten Sie,daß das aktuelle Laufwerk DFX sein MUß!

Sie haben die Möglichkeit einen normalen Bootblock und einen sog. MYSTIC Bootblock zu installieren.Danach werden Sie nach dem gewünschten Filesystem gefragt.

ACHTUNG! Wenn Ihre Diskette im FFS formatiert ist,müssen Sie natürlich auch FastFileSystem (FFS) wählen, da sonst das Betriebs-system nach dem nächsten Reset von einer falschen Filesystem-version ausgeht und es zu folgenschweren Fehlern kommen kann.

Wenn Sie ein Kickstart 3.xx System verwenden, dann werden Sie noch gefragt,ob Sie den internationalen Modus (mit Dircaching) benutzen möchten.

1.31 install

The Install function:

Note: The working drive must be DF0:, DF1:, DF2: or DF3:!

You have the choice to install a normal Bootblock and "MYSTIC" bootblock. Then you will be asked for the filesystem. If you have a disk, which is formatted in FFS, you should use the FastFileSystem (FFS).

If you have the new Kickstart 3.xx system then you will be asked if want to use the international mode. This mode is an improved filingsystem(better errorcorrections/blockstructure).

The "D-TECT" bootblock enables you to kill all viruses in memory. This bootblock was especially written for the use with the older Kickstart 1.x versions. Under Kickstart 2.x and higher you should only use the normal bootblock because the "D-TECT" bootblock uses a direct ROMjump ($fc0000),which crashes under Kickstart 2.x.

Comment 25.07.1993.: The "D-TECT"bootblock was replaced by a MYSTIC bootblock with the same functions.It's new that the BB clearly performs a RESET on OS2.x & OS3.x AMIGAs. Due to the fact that I don't have a hardware register listing of the AGA chips, the BB will have a non complete Copperlist and shows you only garbage.If it happens, at least one of your vectors is changed.

Comment 26.07.1993.: The new "MYSTIC" bootblock contains no direct hardware access.It uses only INTUITION Library functions and it perfectly works on all MC680X0 and on ECS,AGA and on the normal chipset.

1.32 bb_erstellung

Die Bootblock Erstellungsfunktion

Bitte beachten Sie,daß das aktuelle Laufwerk DFX sein MUß!

Stellen Sie sich folgende Situation vor:

Sie haben eine kleine Datie (max.954 Bytes lang),die zudem auch noch komplett PC relativ programmiert ist und Sie wollen nun dieses Programm aus dem Bootblock heraus starten.

Was tun ?

Benutzen Sie einfach diese Funktion !!! Ein Dateirequester erscheint und Sie können das zu ladende File aussuchen.Danach wird der Datei der nötige Bootblockcode hinzugefügt und auf Diskette gespeichert.Fertig.

Diese Funktion ist sinnvoll für Personen, die kleinen Utilities im Bootblock unterbringen wollen (als Beispiel).

1.33 makebb

The Make BB function:

Note: The working drive must be DF0:, DF1:, DF2: or DF3:!

Just imagine the following situation:
You have a little file (max. 954 Bytes long), which is completly PC relativ and you want to start this programm in the bootblock.

What to do?

Simple use the "MAKE BB" function. A file requester appears and you can choose the file to load. You need not to write any routines, which execute the bootcode. This function makes all for you. Simply follow the given instructions.
This routine only supports the 1024 byte long bootblocks because it is to dangerous to write 2048 bytes, if you not know, what is on the blocks 2-3.

1.34 show_startup

The Show S.Seq. function:

You can show the Startup-Sequence. It can be very important in some cases. Example: Viruses like the Disaster Master 2 Virus write "cls *" in the first place of the Startup-Sequence. This virus can easily detected by this function. I have missed this function in most other viruskillers.

1.35 zeige_startup

Die Anzeigefunktion für die Startup-Sequence:

Diese Funktion zeigt Ihnen die Startup-Sequence.Dadurch können Sie in vielen Fällen leicht Viren erkennen.

So schreibt der Disaster Master 2 Virus folgenden String an die erste Stelle der Startup-Sequence:

"cls *"

1.36 kickstart

Die Kickstartsicherungsfunktion

Diese Funktion erlaubt dem User die wichtigsten Vektoren aus Dos Library,IntuitionLibrary, Zeropage, ExecLibrary und aus dem TrackDisk Device herauszusichern.Jeder Block ist 2 Kilobyte lang.
Mit anderen Worten: das komplette File ist 10 Kilobyte lang.

Auf diese Weise kann ich VirusWorkshop schnell an neue Kickstart-versionen anpassen.

Speicherblock:

```
dos.library       -$400 - +$400 = $800 bytes
intuition.library   -$400 - +$400 = $800 bytes
zeropage       $000 - +$800 = $800 bytes
exec.library      -$400 - +$400 = $800 bytes
trackdisk.device    -$400 - +$400 = $800 bytes
            ----------
            $2800 (10240)
```

Wenn Sie diese Funktion benutzen wollen,stellen Sie sicher,daß keine Vektoren verbogen sind !!! Sehr wichtig !!!

1.37 kicksave

The Kicksave function:

This function allows you to save the most important things in the

DosLibrary, IntuitionLibrary, Zeropage, ExecLibrary and of the TrackdiskDevice. Each block is $800 bytes long. This means that the whole file is 10 kilobyte long. This function is only implented, if you use a new Kickstart version (e.g. OS41.115).

I can update the killer in this way very fast and easy.

```
Memblock:
---------
  dos.library       -$400 - +$400 = $800 bytes
  intuition.library   -$400 - +$400 = $800 bytes
  zeropage       $000 - +$800 = $800 bytes
  exec.library      -$400 - +$400 = $800 bytes
  trackdisk.device    -$400 - +$400 = $800 bytes
              ----------
              $2800 (10240)
```

If you use this function make sure that the SetPatch command is not running and tools like the explode.library are not in the system because you would get too many changed pointers and this values are not useable ! It is the best to use the programm directly after the Systemstart.

Note for Programmers: Not all the vectors will be rewritten.I save only such a high amount of bytes to have an advantage for the future viruses.

1.38 automemkill

AutoVektorkiller(Preferences Menu):

Wenn Sie diese Funktion aktivieren,wird vor den meisten Funktion erst der Speicher von Viren befreit.

1.39 autoramkill

AutoRamKill (Preferences Menu):

This Viruskiller tries to kill all vectors in RAM, when you selected a function. You can allow this by activating this. It is very important that you do this. This function is included because many guys work with Kickstart versions, which will only be loaded in the memory. In such a case your system crashes, if AutoRamKill is activated.

1.40 explode

```
                    Explode (Preferences menu):
                    ---------------------------
```

If you activate this function, the ExplodeLibrary V6 or higher will be deactivated as long as the VirusWorkshop is active.

Just imagine the following situation:

1. The Infiltrator Virus will be installed in the system.
2. The ExplodeLibrary will be installed.
3. Programms like BootX are now not able to find the virus(!).

Because of this fact I have included this function! Just start the Memorycheck function. In most times you will see that the LoadSeg Vector is changed. Now start this function and you will (hopefully) see that the LoadSeg Vector is pointing in the ROM. If not, just kill it. The ExplodeLibrary will be reinstalled with all correct values after you quit the VirusWorkshop.

```
                           Important:
                           ----------
```

This function only works with Kickstart version which are higher/equal to OS 2.04. Under older Kickstart versions there are the idiotic BCPL pointers in the RAM and I cannot give you real security if you use this function!

That means, that you cannot activate this function, if you use a RAM kickfile or the "explode.library" is not installed.
If you use a tool like "MAPROM", which uses the MMU in your A4000 to make a new Kickstart resident you can use VW, of course.

Comment 06.04.1993.: Many peoply complain about the direct way of accessing to the system (all 2.x and 3.x kickstarts ALWAYS should stay at $f80000. If you are a softwarepirate and use ZKICK etc., it is not our fault. If you have problems with it, just call me.A real Viruskiller has to go deep in the system because it has to fix a of internal adresses because many pointers can be used by a virus .

1.41 implode

Explode (Preferences menu):

Wenn Sie diese Funktion aktivieren,wird die Explode Library V6 oder höher deaktiviert.

Stellen Sie sich folgende Situation vor:

1. Der Infiltrator Virus befällt das System.
2. Die ExplodeLibrary wird installiert.
3. Viruskiller wie BootX können den Virus nicht mehr finden .

Diese Funktion arbeitet nur, wenn die Explode Library den Loadseg Vektor verändert hat.

1.42 quit

Quit (General menu):

After you've started this function, you can leave the viruskiller. At first a little security box will appear, which asks if you really want to quit the programm.

Then the buffers (from RequesterLibrary and DecrunchLibrary) will be given back to system and all the allocated memory will be given back to the system.

1.43 laufwerkinfo

Laufwerks Info (HD Tools):

Es erscheinene einige wichtige Informationen über das aktuelle Laufwerk.Wenn bei Diskstate (Status) "Problems..." erscheint,dann sollten Sie unbedingt Sectorcheck und danach den DiskDoktor bzw. Disksalv zu Rate ziehen.

Ein Weg,um an das Ziel zu kommen:

1. Take the RootNode pointer out of the DosBase (Offset 34)
2. Take the global DosInfo pointer out of the RootNode (Offset 24)
3. Take the DeviceListPtr out of the global DosInfo.

BE CAREFUL BECAUSE THERE ARE SOME bcpl POINTER HANGING AROUND!

Example in Assembler:

```
  move.l  dosbase(pc),a6
  move.l  34(a6),d0
  move.l  d0,a0     ; Pointer to the Rootnode
  move.l  24(a0),d0   ; Pointer to the global
          ; InfoStructur
  lsl.l #2,d0     ; BCPL pointer *4
  move.l  d0,a0
  move.l  4(a0),d0
  lsl.l #2,d0     ; Pointer to Devicelist*4

  move.l  d0,a0
  move.l  40(a0),d0
  lsl.l #2,d0     ; Name of the Devices /
          ; Volumes etc.*4
          ; 1.Byte = Length of
          ; string...
```

The most important values are:

HEX.	DEZ.
$200	0512
$400	1024
$370	0880
$6e0	1760

When I tried to get the DosType out of the DosEnvec structure it appeared several times (under Kickstart 3.00) that the inserted floppy disk had always the DosType=0. It seems to be a bug in the DosLibrary or in the filing system. If you try to read the Dos=DiskType then you alway get the right values...

This means that Kick3.00 is bugged in this part of the filing system, too.

Another example: You formatted a disk using Kickstart 40.55 with the following command: FORMAT DF0 NAME: Leer FFS INTL .

What happens ? Dostype ist 0 and Disktype is 3 ? Crazy,isn‘t it ? (Tested on 25.07.1993. with an A4000/040 using Kick39.106)

1.44 driveinfo

```
                    Drive Info (HD Tools):
                    ----------------------
```

Some important information will be given to the user about his actual selected drive. This routine is not written in the shortest and best way but it works and that is the most important point. If diskstate says "Problems..." then use (when using DFX) SectorCheck and afterwards the DiskDoctor from your workbench.

If you try it via DosInfo (Lock/Unlock) you can get problems. The right way:

1. Take the RootNode pointer out of the DosBase (Offset 34)
2. Take the global DosInfo pointer out of the RootNode (Offset 24)
3. Take the DeviceListPtr out of the global DosInfo.

BE CAREFUL BECAUSE THERE ARE SOME bcpl POINTER HANGING AROUND!

Example in Assembler:

```
  move.l  dosbase(pc),a6
  move.l  34(a6),d0
  move.l  d0,a0     ; Pointer to the Rootnode
  move.l  24(a0),d0   ; Pointer to the global
          ; InfoStructur
  lsl.l #2,d0     ; BCPL pointer *4
  move.l  d0,a0
  move.l  4(a0),d0
  lsl.l #2,d0     ; Pointer to Devicelist*4

  move.l  d0,a0
  move.l  40(a0),d0
  lsl.l #2,d0     ; Name of the Devices /
          ; Volumes etc.*4
          ; 1.Byte = Length of
          ; string...
```

Kickstart 1.2 has some strange bugs in the DeviceStructures. It can happen that the BootPriority is extremly high. It is caused by a bug in DOS. I will search for another way to find the right value!

Another bug: It can happen that your high cylinder is at a normal 880KB diskette $370=880. This is caused by the operating system. At this routine all adresses are given as hex values.

The most important values are:

HEX.	DEZ.
$200	0512
$400	1024
$370	0880
$6e0	1760

When I tried to get the DosType out of the DosEnvec structure it appeared several times (under Kickstart 3.00) that the inserted floppy disk had always the DosType=0. It seems to be a bug in the DosLibrary or in the filing system. If you try to read the Dos=DiskType then you alway get the right values...

This means that Kick3.00 is bugged in this part of the filing system, too.

Another example: You formatted a disk using Kickstart 40.55 with the following command: FORMAT DF0 NAME: Leer FFS INTL .

What happens ? Dostype ist 0 and Disktype is 3 ? Crazy,isn't it ? (Tested on 25.07.1993. with an A4000/040 using Kick39.106)

1.45 festplattensupport

Lese, Schreibe, Zeige den physikalischen Zylinder 0:

Es gitb einige Viren,die den RDB von Ihrer Festplatte zerstören. Warum ? Entweder mit Absicht,oder sie testen nicht,ob sie das TrackDisk.Device gepatcht haben.Was passiert,wenn Sie mit dem "scsi.device" schreibend auf Block 0 einer Festplatte zugreifen ?
Der RDB wird zerstört und die Festplatte nach einem Reset erst-einmal unbrauchbar.

Read = Erstelle eine Sicherheitskopie des RDB.
(Bitte auf eine einzelne Diskette!)
Write = Schreibe die Sicherheitskopie zurück auf die HD.
Show = ASCII Darstellung des RDB

Benutzen Sie diese Routinen nur,wenn Sie kein spezielles Programm für solche Fälle direkt von Ihrer HD Herstellerfirma haben. BSC

gibt (ALF/OCTAGON) ein sehr gutes Programm mit.

Hier eine Liste von Viren,die den RDB vernichten können:

-Crime92 1+2,Overkill,ByteBandit,Zenker1+2,Burn 1+2
und weitere...

Logfile

Diese Funktion erlaubt es, ein Protokollfile auf einem beliebigen Laufwerk anzulegen. Alle Ausgaben auf dem Bildschirm (keine Requester) werden in dieses File geschrieben. Wenn Sie das Logfile wieder schliessen wollen, einfach ein 2.mal auf LOGFILE klicken. Ansonsten wird das Logfile automatisch beim Ende von VirusWorkshop geschlossen.

1.46 hdsupport

Read, Write, Show physical cylinder 0:

There are lot of viruses hanging around which destroy the RigidDiskBlock of your HD. Why? They do not recognize that they do not use the "trackdisk.device". What happens, if they write using the "scsi.device" on the bootblock? They get the physical block of your device and destroy it. When using harddisks you surely know that the RDB is in the physical block 0. Your hd becomes unuseable. How good, if you saved the physical block 0. This function will do excatly this!

Read = Backup physical cylinder 0 to a safe disk.
Write = Restore physical cylinder 0.
Show = Comparable to the 'ASCII Dump' but you have more sectors to watch.

Especially the Read/Write parts of this routine should only be used, if you have not a special programm from your HD producer company which is surely better customized for your HD. BSC (Oktagon / ALF) is for example such a company which gives you an excellent tool to save your RidgidDiskBlock block!

List of some viruses, which can detroy the physical block 0:
-Crime92 1+2,Overkill,ByteBandit,Zenker1+2,Burn 1+2

and more...

Logfile

Do you want to have a logfile containing all actions of VW, which will be printed on the screen ? We want it. Simply start this option and select a filename. The logfile will be closed by starting again the logfile option or at the end of VirusWorkshop.

1.47 viruses

VirusWorkshop recognition list

I have to thank the following persons for their big support with new viruses in the last months:

- J.Walker/TRSi
- VirDown !
- AtomiX x/N.A.S.A. Team
- Georg Hörmann (VirusZ)
- Ingo Schmidt (Nice meeting WOC92 !!!)

PLEASE NOTE: IT'S NOT ALLOWED TO COPY VIRUS-ANALYSISES FROM THE VW DOCUMENT TO USE IT IN YOUR OWN PRODUCTIONS. THE ONE AND ONLY EXCEPTION IS THE VIRUSTEST CENTER FROM THE UNIVERSITY OF HAMBURG.

LINK/TROJAN/FILE Viruses

Bootblock Viruses

1.48 fvirus

```
                The following viruses will be detected by Virusworkshop 3.7  ↩
                   FINAL:
-------------------------------------------------------------------


Fileviruses, Trojan horses and link viruses:
--------------------------------------------


               -z-Speed.lha Virus

               $4EB9 Files

               AAA Enhancer Bomb

               ATARI

               A.I.S.F. Virus

               AmiPatch10

               Antichrist(Jack Clone)

               AeReg 3.9 Virus

               BootX Recoqfile Updater fake virus

               Bossnuke 1.5+Formatter

               Bestial Devastation
                       Beethoven

               Butonic 4.55

               Aibon 1+2(created by Express 2.20)

               AmiExpress (ZK3.20) Virus

               BURN Virus 1+2
                 BGS9 5 Versions
Bret_Hawnes
Byte Parasite 1-3
Butonic.virus
Butonic1.31
Butonic3.00
CCCP
Centurion (Smilie Cancer) 1-2

               Compuphazygote
                 (12 different types !)
Crime
Crime++ (created by Driveinfo!)
```

```
               Christmas

               Crime92 1+2+3
                 Challenger_Trojan
Chaos Master 0.5

               Commodore

               ConMan(Dir Virus Installer)

               ConMan(Dir Virus)

               ConMan(ARTM 2.3 fake)

               CLP_WOW.exe Virus

               ComaVirusMaker

               Dlog 1.8

               Dialer 2.8g

               Dark Avenger Link Virus
                       DiskVal1234

               Diropus

               Debugger Virus

               Digital Dream Installer
                 Darthvader1.1

               Disktroyer V2.0 Virus

               Description 4.0 Virus

               Disksalv 3.01 Loader Fake
                       DriveInfo
D-Structure a-c

               DAG Installer
                 disk.info_defekt
Disktroyer_V1.0
DisasterMaster2

               Excreminator_1

               Excreminator Installer

               Express2.20

               Easy-E BBS trojan
                 EMWurm Logic Bomb!

               Fileghost Virus Installer

               Fileghost LinkVirus
```

```
                Freedom-FileVirus

              G-Zus Packer Bomb
                Gotcha_Lamer_Bomb!
Gotcha_Lamer_Bomb! Installer
Golden_Rider
Infiltartor Link Virus
Installer of Datalock

              Infected Diskrepair

              Infected WhiteBOX
                IRQ.LINK 1+2

              Kef_Ani.lha Virus

              KAKO Loadwb Virus
                lamerVirusX
LAMER_Trojan_Horse (Lamer LoadWB)
liberator.LINK (Memcheck 3.0)

              LHA Check 1.1 BBS Trojan
                Liberator 3.0 & 5.01 Viruses

              LZ Virus
                LamerExe
LamerExe TNM crunched

              Leviathan

              Lummin Virus

              M_Chat Virus

              Megalink

              Master-WHO /X Backdoor

              Merry.Exe /X BBS Virus

              Menems_Revenge 1+2

              Mount
                Modem Virus Bluebox!

              Modemcheck Virus Loadwb

              Modemcheck Virus Installer
                Metamorphosis

              Infected MuiGui

              MST-Vec Formatter Viruses
                      MsgTop

              Mongo09.exe
```

Mongo05.exe
  NOGURU

NewMCI

NewAge
  NightMare (Filecheck)

Nano][Virus

NANo

NANo][

NAST

PStats

PHA-1994.exe
  Powerpacker 3.2 Logic Bomb!

PP Bomb Clone (DIED)

PP Bomb Clone (Megamon)

QRDL V1.1
  RetLamer
RevLamer 1+2
Rob-FILEVIRUS

Saddam Diskvalidator Virus 1-10

Swiftware 0.98
        Sepultura

SeekSpeed Trojan

Sepultura 2.26 Virus

Stockmarket Virus (?)
  SCA Dos Kill Virus

Show Sysop BBS Trojan
  SnoopDos 2.1 Virus

SPEEDCHECK

SnoopDos 1.6 Virus

SnoopDos 1.9 Virus

SmBX
        SCSI ($e741)

TAI 10 Installer

ToolsDaemon 2.2 Fake

```
               Telecom

               TROJAN 3.0

               Topdog Trojan Horse
                 Travelling Jack 1+2
(There are only 2 version! Jack 3 is not existing! Some people did
not recognize that the Jack viruses are able to change their
length!)
Timebomb_Info_Bomb_7840

               Timer_Virus

               Installer of Timer_Virus

               T.F.C._Revenge
                 Terrorists
Timebomber
Trabbi
TurkCarrier.virus

               UaDialer 6.2 Virus

               Ulog 1.8
                 Vkill 100 Virus
      VirusTest(TimeBomber)

               VirusMaker 1.0

               VirusZ_II 1.02 fake virus

               VirusHunter Joke

               VirusChecker 6.4 Fake Virus
                 VirusBlast.2.3!
Virus_Test_Bomb_936
VTerminator
Xeno
XCopy65E
XPRZSPEED3.2 Trojan horse
      XRipper

               XACA Virus

               Zapa Adder
                       --- 193 Link/Trojan/Validator Viruses ---
```

1.49 newage

```
NewAge Linkvirus:
      -----------------
```

Works not with Kickstart 1.x. An infected files becomes 668 bytes longer. This virus will only change the DosWrite() vector and is not resident.

After some hours of trying to infect some testfiles, 2 files were infected. Thanks Ingo for this really exhausting work !

The virus put his code in the first hunk & changes the $3ec hunk. Due to some buggy routines in this virus, the infected files become not executable and VirusWorkshop cannot remove this virus.

At the end of the virus, you can read
"NewAge by Evil Jesus".

Due to thousand of bugs in the routines, I decided to write no repairroutine. My routine worked fine for 1 hunkfiles, but if the file had more hunks, the routine crashed.

Comment 15.05.1994: Sorry Ingo, my first success was on the DHB file. The infected cmon could not be recoverd.

The german viruskillerprogrammers recieved this virus as sourcecode(written with Asm-One ?)together with the Debugger virus. As far as I understood the whole thing, the virus-programmer released an LHA file containing source and the infected file for Debugger94 and this LHA file was send from a carefull user to Jan Bo Andersen, who send this LHA file to me.

> Only deletion is possible ! <

Detection tested 14.05.1994.

1.50 easy-e

Easy-E BBS trojan:

Filelength: 38860 bytes unpacked

This is an ordinary BBS hacking programm. A new user will be added to the user.data, as far as I have understand it.

The "user.data" file will be searched on the "dh0" device.
In my opinion this virus works only on older AmiExpress systems, because the new one are crypting the user.data and such lame hacks are not possible anymore.

In the file you can read:

```
'dos.library'
'sys:'
'sys:paradox'
'EASY-E'
'dh0:bbs/user.data'
```

Detection tested 01.05.1994.

Special thanks to MOK! for sending this virus !

1.51 debug_me

Debugger (04191994) Virus:

An infected file becomes 1088 bytes long.
Changed vectors: DosWrite and DosLoadSeg
Kickstart: 2.04 and higher
other possible name: Fjpg Virus 1.11 (based on the first infected programm)

The virus does not work on Kickstart versions under 2.0, because of the patchroutines. A new way to infect files:

186 bytes from the first hunk will be copied in a new created $3f1 hunk behind the file and a part of the virus will be copied at this position in the first hunk. The length of the first hunk will be not changed but the length entries in the hunkheader will be changed (probably to irritate antivirus-programmers and resourcers). This will be done with a random value !!!

The virus contains a destruction routine ! No format but a destructive WRITE command !

VirusWorkshop can remove the virus completely. Please make a backup before repairing such a file !

A normal hunkheader looks like this:

```
$3f3
0
number of hunks
number of starthunk
number of endhunk
n longwords containing the lengths of the hunks
```

$3e9 (hunk_code)
length for this hunk

ATTENTION: Some crunchers (Turbo Imploder e.g.) write 2 different lengths in the table of hunklengths and behind the $3e9 ! I expect in this special case problems !

At the end of an infected file you can read the string "DEBUGGER". The whole virus looks like the work of a better coder (in my opinion).

This virus was send to me by Jan Bo Andersen of SHI Denmark. The sending contained the whole documantated source and a little text from the author of this virus:

Anarchy Unlimited - Virus Technology Centre - +358-0-PRIVATE

Amiga & PC viruses online

==========

Thank you for downloading Debugger V2 virus package!

Debugger02.s.asc - PGP signed asm source of Debugger virus
EvilJesus.asc - Public PGP key
FJPEG111.lha - Infected fjpeg, version number bumped up to 1.11
NewAge.s.asc - PGP signed asm source of NewAge virus

Upload fjpeg only to systems which do not have networks! Those systems will have lowest information level and sysop are mostly dummies who bought modem week ago and decided to run bbs because "It's so cool" :)

With this kind of approach virus will have best chance to reach users who want to upload it immediately. There is also a big chance that such users will trash their hd's in no time. So nice...

So no network system as information about infection will spread very fast degrading overall chance of succesful destruction.

Sincerely yours, Evil Jesus

==========

Even more irritating is, that PGP keys are in the package, too. I cannot understand this. The virus is dated 19.04.1994.

Detection tested 27-28.04.1994.
(again a night with only 3 hours

of sleep)

1.52 sysop

Show Sysop Trojan (?):

Filelength: 7860 bytes unpacked.

A tool to show username and accessmodes. I have only a newer user.data, which is crypted so I could not test it. This is for sure not such a lame thing, which simply adds a user to to this file.

At least be carefull with it...

1.53 mcioratt

NewMCI (?) trojan:

This a PP (crypted) file which contain a protected part in which is jumped. I had no time to crack the PP protection and had no real motivation to do this. At least be carefull with this thing !

1.54 g-zus

G-Zus Packer Bomb:

Filelength: 15016 bytes (unpacked)

This is a trojan, which claims to be a packer with fantastic packrates. If you start the packer, the following will happen:

df0:g-zus df0:Copy (Copy=5188 bytes long)

Creating df0:Copy.god (Copy.god=36 bytes long)
Deleting df0:Copy

The new created file with the extension "god" is always 36
bytes long and contains the following:

"ThisIsMagic!)?<75?2#%-'4?8+475???UR["

So don't use this programm.

Here a shortcut from the document:

```
-------------------------------------------------------------------------
The G-Zus compactor/decompactor: v0.01
-------------------------------------------------------------------------
   Public release: May 9, 1993.
         Function: Compress and decompress any file VERY efficiently.
         Comments: clemj00@dmi.usherb.ca
-------------------------------------------------------------------------
G-Zus: Copyright 1993
-------------------------------------------------------------------------
This is freely redistributable, so, you can distribute it!.



Here are some typical compression example you can attain with G-zus:

Flex.lzh                  251123 ----rwed 15-Apr-93 23:11:33
FoCo.lzh                   30887 ----rwed 17-Jan-93 12:05:43
gadlayout-1.5.lha          41401 ----rwed 08-Apr-93 13:29:53

Flex.god                      30 ----rwed Today     10:01:35
FoCo.god                     -17 ----rwed Today     10:05:12
gadlayout-1.5.god            -22 ----rwed Today     10:10:55

-------------------------------------------------------------------------



                Detection tested on 09.04.1994.
```

1.55 mountie

Mount Virus:
----

other possible names: Gremlins or Xcopy faker
Eleni Wirus 2.2

Some other viruskillers detect a Gremlins virus in memory and crash due to wrong values. In this way the name "Gremlins" was founded for this virus.

It's pure bullshit to say, that this virus performs a LOW-level format of your harddisc.

The installerfile is a version of a wellknown copyprogramm.
The virus was linked together with a little installer using the wellknown 4eb9 linker, which was used for many BBS viruses in the past.

Installer : 66424 bytes (4eb9 linked on a XCopy version)
Loader(c/mount): 208 bytes
Virus (BB&File): 1024 bytes

The virus works with Kickstart 2.x and higher. Using older Kickstart versions with this virus is not possible.

SumKickData, Doio and Coolcapture will be patched. The orig. values will be stored in the low memory region around $100.

VirusWorkshop can remove both Coolcapture and Doio, but the SumkickData Function is NOT recoverabel because of a bug in virus.

The virus is an ordinary bootblockvirus with a new little feature: If a counter reaches -$67 (starting by 1), two new files will be written to disk. In this way the virus can be spread on harddiscs, too.

The virus does not need the trackdisk.device. Therefore your HDs (exactly the RDB) can be destroyed, too.

The virus contains NO formatroutine. I saw a text saying this. It's not possible with this thing !

In the virus you can read "MOUNT". That's the reason, why I have choosen this name.

Detection tested 02.04.1994.

Comment 01.05.1994: I got the hint from another viruskiller to decrypt a string, which can be found at the top of the bootblock. The virus itself does not touch this string. In the bootblock it look like this: "FMJOJ XJSUT V2.2". If you decode it:

```
  lea string,a0
  move.l  #10,d7
.loop move.b  (a0),d0
  subq  #1,d0
  move.b  d0,(a0)
  dbf d7,.loop
        rts
```

Now you will be able to read the following string:
ELENI WIRUS V2.2. The "w" in wirus is not a bug in my english, it stands in this way in the virus ! I am sure that this is not the ELENI virus, which will be detected by SHIs BootX.

```
Special thanks to J.Walker/TRSi for the fast supply with this
      virus !

Some messages:

Metal Force/Anthrox'94: NEVER release resourced viruses ! So
      you force clones !

      Quite interesting ! TRSi released the first real technical
      infos about his virus and several other known crews
      released their warnings after us (partly with such wrong
      things like: Lowlevel format .....).
```

1.56 menems

```
Menems Revenge Virus 1+2:
      ------------------------

Typ 1:
      -Linkvirus
      -an infected file becomes 3076 bytes longer
      -two hunks will be added
       $3e9 hunk ($2b6)
       $3ea hunk ($23)

      Typ 1:
      -Linkvirus
      -an infected file becomes 3124 bytes longer
      -two hunks will be added
       $3e9 hunk ($2c2)
       $3ea hunk ($23)

 Only some bytes were changed from the first version to the
       next version. The first version appeared (I think) 1992 and
       the new version appeared 1994.

       The virus contains a checkroutine for files, which are longer
       than 60000 bytes. LoadSeg will be patched. No resetvectors
       will be touched. A new process with the name of a normal
       BLANK will be started.

       On some testconfigurations the files could not be repaired,
       because they contained pure garbage. Sorry.

       Sometimes a DisplayAlert routine shows you a text saying
       "Argentinia still lives..:". This text is crypted in the
       file with a asr command. No real destruction routine
       (except for the linking itself) was found in the virus.



      Detection tested 19.03.1994.
```

1.57 mst-vec

```
MST-VEC Formatter Viruses:
--------------------------

The virusname comes from the name of the archive in which the both
viruses were found:


          File 1 (MST-INTE.exe):
                ----------------------

      Filelength: 51256 bytes non packed


      This is a simple destroying programm, which scanns all files in the
      S drawer and overwrite the first bytes with the "FUCK..." string.
      Such viruses and nearly excat the same routines have been seen by
      approxmetly 10 viruses in the christmas time.

      Readable text at the beginning of the virus:


'dos.library'
'S:'
'FUCK BOBO AND JEWISH AXE! SIEG HEIL! GAS'
' ROOLEZ! BEEEAVERS!'

        File 2 (Exe_this_first!.exe):
              ----------------------------

      Filelength: 15308 bytes non packed


      This is nearly the same formatter routine like in the MChat Virus
      and the Anthrox Chat 3.0. This time the formatterthings were put
      in the beginning. Come on guys ! Stop producing this shit !


      (For more infos read at the MChat chapter)



        Detection tested 07.03.1994.
```

1.58 lhatrojan

Lha Checker 1.1 BBS trojan horse:

Filelength: 3836 bytes (not crunched)

This is supposed to be a LHA checker (for AmiExpress). At the end of the file there can be found a BBS trojan, which scans the user data and handles with the files "ram:m1.dax" and "God-fbtr.lha".

If the SnoopDos Task is found, the virus will do nothing. All important texts are crypted. It seems that no ordinary linker was used for this virus. Probably someone resourced the original LHA Checker and added the viruscode. The virus is written in assembler(at least I think so).

Detection tested on 06.03.1994.

Special thanks to VirDown! for this virus !

1.59 tripplea

AAA-Enhancer Bomb 4.8:

Filelength: 3984 (not crunched)

Patches the DosWrite() vector.

Works with Kickstart 3.x.

This programm claims to be a programm that activates the new AAA modes in the latest update of the AA chips. Pure bullshit. If you start it, the DosWrite Vector will be changed and strings will be exchanged. As a result many programms do not work, because strings (or commands) are not valid etc.

The writeaccess will be very strong slowed down and so you can recognize this virus.

The programm tries to damage the reputation of SHI.

VirusWorkshop is not abel to find the damaged files, because I know no way to distinguish between a normal and a damaged file in this special case because of no recognition code string !

Exchange Tables for the patched DosWrite routine:

```
'perverse'      'reliable'
  'Computer'        'vibrator'
  'sexual'      'actual'
  'friend'      'bugger'
  'pocket'        'vagina'
  'follow'                'Computer'
  'stroke'        'randy'
  'ready'       'blood'
  'sperm'       'bitch'
  'woman'       'head'
  'hole'          'rich'
  'poor'        'warm'
  'cold'        'open'
  'lock'        'love'
  'hate'        'meet'
  'fuck'        'lift'
  'drop'        'girl'
  'wife'        'kill'
  'kiss'        'look'
  'piss'        'nice'
  'shit'        'soft'
  'hard'        'ball'
  'hand'        'cock'
  'nose'        'dear'
  'dead'        'skin'
  'cunt'        'egg'
  'lip'         'car'
  'ass'         '0'
  '9'         '1'
  '8'         '2'
  '7'         '3'
  '6'         '4'
  '5'

  'vibrator'        'actual'
  'sexual'        'bugger'
  'friend'        'vagina'
  'pocket'        'stroke'
  'follow'        'ready'
  'randy'       'sperm'
  'blood'       'woman'
  'bitch'       'hole'
  'head'        'poor'
  'rich'        'cold'
  'warm'        'lock'
  'open'        'hate'
  'love'        'fuck'
  'meet'        'drop'
  'lift'        'wife'
  'girl'        'kiss'
  'kill'        'piss'
  'look'        'shit'
  'nice'        'hard'
  'soft'        'hand'
  'ball'        'nose'
  'cock'        'dead'
```

```
'dear'        'cunt'
'skin'        'lip'
'egg'         'ass'
'car'         '9'
'0'         '8'
'1'         '7'
'2'         '6'
'3'         '5'
'4'
```

Text in the virus, which will be never printed out to the window(names have been erased to protect the innocence):

```
'SHIxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'
'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'
'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'
'xxxxxxx, I thought of him as my friend, '
'offered me (xxxxxxxxxxxxx) 100$ Dollar '
'for writing a new kind of virus, he said'
', this would be necassary to control the'
' development of future viruses. After fi'
'nishing the virus and sending to xxxx, I'
' had to promise to destroy all my data a'
'bout this virus, so that xxxx is the onl'
'y person owning this virus. Now I found '
'out, that xxxx is contacting all Amiga-M'
'agazines and offers a hot story about a '
'brand new and very dangerous virus, xxxx'
' demands 100$ for this information, by t'
'his way xxxx gets rich and famous and is'
' respected as a great fighter against vi'
'ruses. But as you see there is some huge'
' perversity inside, because not able to '
'program his own viruses, xxxx hires viru'
'sprogramers and tries to make profit of '
'the resulting viruses. Really pervers!! '
'I (xxxxxxxxxxxxx) did this virus only f'
'or testing-purposes, and nobody except x'
'xxx got this virus from me. So if this v'
'irus should become public, then xxxx is '
'to be held responsible for it. Blame him'
', not me, Yes Blame him, because xxxx is'
' a shameful and deceitful person! '
```

Name of the window:

```
'RAW:0/0/640/200/AAA-Enhancer 4.8 by xxx'
' xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'
```

Text printed on the window:

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

    'Activates the hidden AAA-features in A120'
    '0 and A4000, because Beta-AAA-Chips'
    'are used instead of AA-Chips since June '
    '93 !!!'
    'The new revolutionary AAA-graphics-chi'
    'ps with a maximum of 3072 * 1536'
    'Pixels are nearly finished. '
    'They come with a so called'
    'AA-compatibility-mode, in which they'
    ' behave 100% like the old'
    'AA-graphics-chips. The AA-compatibili'
    'ty-mode works fine, and therefore'
    'Commodore can use the actual Beta-AAA-'
    'Chips for AA-Chips, because this is'
    'cheaper than producing two diffe'
    'rent graphics-chip-sets. The new'
    'AAA-graphics-modes are not yet 100'
    '% implemented, but the greatest'
    'AAA-feature is already working. It is '
    'called MaxMode and offers you 3072 *'
    '536 Pixels. AAA-MaxMode is not ye'
    't supported by Kickstart3.0, so'
    'AAA-Enhancer patches the Write()-vector'
    ' to set MaxMode-Bit. Now MaxMode is'
    'activated and can be selected in ScreenMode-Prefs.'
    'If you have an older A1200,A4000 with the'
    'Original-AA-Chips, than of course'
    'ScreenMode-prefs cannot offer you MaxMode,'
    ' because setting MaxMode-Bit has'
    'no effect with AA-Chips.'
    'but AA-Enhancer is useful for AA-Amigas '
    'too, because it cures the following'
    'bug. AA-Chips access memeory four '
    'times faster than ECS-Chips, some'
    'AM-chips are driven to their limits to'
    ' follow this speed and have no more'
    'time to refresh their banks. So, esp'
    'ecially in a heay multitasking load,'
    'its can change, a very hard to reproduce'
    ' bug, so if your Amiga often gurus,'
    'than always run AA-Enhancer (startup-ser'
    'quence or WBstartup), it will help !'


(This text is pure bullshit, so don't care about it !!!)


      Detection tested on 23.02.1994.
```

1.60 ddream

```
Digital Dream Installer:
      ------------------------

      Packed filelength:6496 Unpacked length:9960

      The file is packed with PP2.x !  It installs the Digital Dream
      Virus. Read in the bootblock section !
      It pretends to be a viruskiller for an old filevirus.
```

1.61 tool22

```
ToolsDaemon 2.2 Fake Virus:
      ---------------------------


      Filelength of the mainprogramm: 7128 bytes
      Filelenght of the new written file: 784 bytes


      The mainprogramm, a ToolsDeaemon with linked virus, installs
      a  process  ("Background_Process") and  writes a  new  file
      ("S:mount") to disc.  This  file and the  process contain  a
      very strong routine, which reduces all filelengths from  the
      devices df0,hd0,sys,ram,df1,df2 to 42 bytes ( You  remember:
      Douglas Adams "Hitchhikers Guide through Gala...").

      Such destruction routines have been seen in the public at eg.
      PP bomb and so on. So think about a good and actual backup !
```

1.62 daginst

```
DAG Virus Installer:
      --------------------

      Filelength: 7360 bytes

      This file installs the DAG bootblock to dfx.


                Detection tested 2/94
```

1.63 execb

```
Excrement Bootblockvirus Installer:
      ----------------------------------
```

Length: 1068 bytes

This file simply installs the EXCREMENT bootblockvirus to
memory. The coolcapture will be changed. VirusWorkshop repairs
the changed vector and can kill the fucking virus !

Detection tested on 24.01.1994.

1.64 excre

Excreminator Virus 1:

Filelength: 2392

This is a very lame trojan horse. It changes NO vectors
in memory. It simply loads at each call the file
"df0:libs/exec.library" and works with this 4 byte long
file. The counter will be set to 5. If the value reaches
0 (by counting -1), all drives will be formatted using a
very lame hardware routine, which does not work on faster
processors because of timing problem. The virus tries to
cheat the user. It writes messages, that it is searching
for virus etc. But it does not search, it simply uses the
DOS delay routines to wait some seconds.

Remember: This was a work of beginners. Some words to
you: Better play with your joysticks !!!

This virus looks like a work of one hour. The formatroutine
looks very similar to a routine published in a big german
book company and the rest code is lame....

```
      "intuition.library"
"df0:libs/Exec.library"
      "df0:Libs"
"-*- Excreminator V1.0 -*-"
"Written by ',27,'The Lame Trio (TLT)',27,' in 1991"
"Memory Check ..."
"Checking BootBlock for Virus ..."
"  OK! No Virus found!"
"ALL DRIVES FUCKED UP! LAME SUCKER !!!"
"#Use a better Viruskiller next time!"
"-e.g. Excreminator II HAHAHA"
```

Detection tested:

Somewhen in 1993

1.65 muigui

Filelength: 15140 bytes

This programm, which is linked before MuiGui, tries to
install a virus. The installer is very lame coded and
contains direct memory access routines in the 32 BIT
fastram(is the programmer a user of a TURBOboard?).

Some exaples for direct memory access:

```
MOVE.L  D0,$07EC125C.L
MOVE.L  #$07EC124C,$000E(A1)
```

Detection tested on 22.1.1994.

1.66 tai10

TAI 10 Installer:

Filelength: 12952 bytes
other possible name: Enforcer 37.76 Fake Virus

This programm, which is linked before Enforcer, tries to
install a virus. The installer is very lame coded and
contains direct memory access routines in the 32 BIT
fastram(is the programmer a user of a TURBOboard?).

Some exaples for direct memory access:

```
MOVE.L  D0,$07EC125C.L
MOVE.L  #$07EC124C,$000E(A1)
```

Visible texts in the installer:

```
'trackdisk.device'
'Nudos.library'
'Don^t change or delete ! '
'This is a resident viruskiller  !  '
'press the left mouse to kill bootvirus..'
```

```
'!',27,'TAI 10'
'_'
'SUSPICIOUS BOOTBLOCK FOUND...'
'.M.:VIRUSKILL'
'R.M. : GO ON '
```

P.S. At the testdate there is , as far as I know, NO Enforcer 37.76 on the market.

Detection tested on 22.1.1994.

1.67 vcheck

Virus-Checker 6.4 Fake Virus:

This is a simple Compophazygote Clone.

Only the visible texts have been changed:

```
':c/Virus_Checker',0
':c/Virus_Checker',0
':c/Virus_Checker',0
'This is a SHI Antivirus , use this great'
' utility'
'They have the best viruskillers of the world,'
', join SHI !'
' Only SHI has all virii for the amiga computer,'
'mputer, nobody else  !'
'Virus_Checker V6.4 by John Veldthuis  '
'Checking DF0: For Viruses'
```

Detection tested on 21.1.1994.

1.68 mongo05

Mongo05.exe BBS Trojan:

Filelength (PP4.0): 1464
not crunched : 2260

This is a quite clever hacking programm produced by a so called Mongo of Zonder Kommando. The user.data will be made avaible

under a new name in the upload directory, so that the hacker
only need to download the file from the bbs. The name of the new
file will not appear in the BBS dirlist, so that only the hacker
can download it.

The name of the user.data in the download directory is

"ATX_NADA.dms".

Detection tested on 15.2.1994.

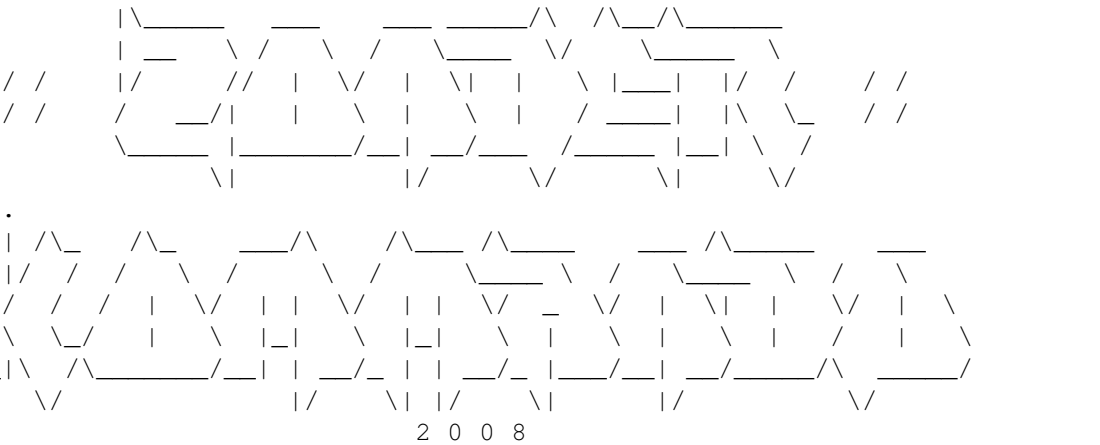
1.69 mongo09

Mongo09.exe BBS Trojan:

Filelength (PP4.0): 1708
not crunched : 3368

This is a quite clever hacking programm produced by a so called
Mongo of Zonder Kommando. The user.data will be made avaible
under a new name in the upload directory, so that the hacker
only need to download the file from the bbs. The name of the new
file will not appear in the BBS dirlist, so that only the hacker
can download it.

Shortcut from the text spreaded together with this trojan horse:



2 0 0 8

Hack Mania is DEAD !

Soo what' next ?

Mongo is here to rule !

So MONGO the HERO , has made the NEW Great util

MONGO MANIA V0.8

Mongo Mania is better than hackmania from stalin and Mongomania take Amiexpress 1.x 2.x (3.x).

It can take ami 3.x if the sysop forgot to Delete the ACP file for 2.x, and he havn't changed any paths !

And the new features are:

New Hackfile name > FLT_DSQ.DMS (1993 bytes)

Decode with >

```
        Lea.l       $50000,a0
        Moveq       #1993,d0
Zk:     Add.b       #$3,(a0)+
        dbra        d0,zk
        rts
```

Load in FLT_DSQ.DMS with Seka,Asm1 etc in memory at $50000

Write the Small assembler prg and start it!

Use: H or N $50000 and you can see text.

New protection > xxxx (user name in user.data)

Snoopdos can eat shit won't find anything or Mongo M. Don't do anything if snoopdos is there !

Bugs are: NOT TESTED if Protection works (it shall work)
NOT TESTED if 1.x hacker works 100% but there shoule be no probb !

Detection tested on 25.2.1994.

1.70 virusz2

BURN Virus 1(or TYP A like in VT):

Increases filelength: 2412

This virus is quite clever. It adds 2 hunks to the file. The first hunk will be linked before the file and the other hunk will be added behind the file. The first hunk creates a process with the data of the last hunk.DOSWRITE will be changed.

I could not manage to spread the virus. Everything was tried but I could not figure out how to spread it. A real repairroutine was not included in VirusWorkshop, because I think that only one testfile is too less. VW now only deletes the infected file.

The linkroutine only knows a very low amount of hunks and is not the state of the art.

The installed process has always another name,because the Exec Tasklist will be used to create the Procname.

The virus contains a DATESTAMP routine. On 07.2.1994. the virus will start to destroy all DATA and no spredtry will be performed.

The memorykill routine fills up the process with 1037 * "RTS". All routines will be overwritten and no damage can be caused by this process. Other viruskillers try to rem. the process, but it's much easier only to deactivate the thing.

A formatroutine is in this file. The mainfile is about 3000 bytes longer than the real VirusZ version and contains at the end of the file the virus-code. The DOSlist will be scanned and several sectors will be overwritten via EXECs DOIO and the blocks will be filled up with "BURN"s. The string "BURN" cannot be read as in the Bossnuke Virus("DOS3"s).

The longword will be created in this way:

```
move.l  #$5171c5c8,d1
eori.l  #$13249786,d1 ="BURN"
```

The routine is very similar to another formatroutine,which appeared in the last weeks. This was the Bossnuke Virus.

Detection tested on 18.1.1994.

Special thanks go to Cranc/LOGIC for supplying me with the info about a virus in a fake version.

BURN Virus 2(or TYP B like in VT):

Increases an infected file by 2428 bytes.

Differences to Version A:

A different time routine, but still the pure destroying-code will be activated at 7.Feb 1994. A little bit changed cryptroutine for the formatlw "BURN". Some changes in the infection(spread) routine. Due to a strong bug in the cryptroutine for the longword "BURN", this word will be never created(Thanks must go to Ingo Schmidt for this hint:You really not needed to trash a SYQUEST to test it).

Version A did not spread ! Version B can be easily spread.

Many mistakes in the code (hunks!). VirusWorkshop can fix (hopefully) all bugs made by this virus. It corrects the HUNK RELOC32. Make a copy before repairing this file !

Many links are possible. I have stopped counting at 20 links.

Detection in RAM and file tested
09.02.1994.

Special thanks must go J.Walker/TRSi for the really hyper-fast supply with this virus. Thanks again !

1.71 ax320

Hacked AmiExpress version 3.20:

This should be a cracked AmiExpress version. I have heard that it contains several backdoors. Be carefull...

The file was spread under the name : zk-320.lha. In this special case I can only say, that I heard it from several sides that this file contains many backdoors.

Shortcut from the document:

```
  /        #######  #######  ##   ## #######   ###############      /
  \ /\          ##  ##   ##  #### ##       ##  ##            ##     \ /\
   X       #######  ##   ##  ## ####  ##   ##  #####   ######       X
 \/ \      ##       ##   ##  ##  ###  ##   ##  ##      ##   ##    \/ \
    /      #######  #######  ##   ##  ######   ######  ##   ##       /

##   ##  #######  ##########  ##########  #######  ##   ## #######   #######
##  ##   ##   ##  ##  ##  ##  ##  ##  ##       ##  #### ##       ##  ##   ##
#####    ##   ##  ##  ##  ##  ##  ##  ##  #######  ## ####  ##   ##  ##   ##
##  ##   ##   ##  ##  ##  ##  ##  ##  ##  ##   ##  ##  ###  ##   ##  ##   ##
##   ##  #######  ##      ##  ##      ##  #######  ##   ##  ######   #######
                                                                    [ML/ZK]
                    ######     #####    #####    #####
                         ##   ##  ###  ##  ###  ##   ##
                       ####   ## # ##  ## # ##   #####
                      ##      ###  ##  ###  ##  ##   ##
                     #######    #####    #####    #####
```

```
.-------------------------------------------------------.
|    One World..One People..White People.. SIEG HEIL!   |
`-------------------------------------------------------'
.---------->>> PRESENTS -  AMI EXPRESS v3.20 <<<----------.
|                                                         |
|               /X 3.20 contains NO BACK DOORS            .
|          100% working with File_id.diz and Sent!        |
|                BEST VERSION  FUCK THE REST!             |
|                                                         :
:      Great Supply by : AUX                 of ZK2008    |
|      Hacked^Cracked  : FAGLIGHT            of ZK2008    |
|      Ascii           : MONALISA            of ZK2008    |
|      This info txt   : FAGLIGHT^MONALISA   of ZK2008    |
`-------------------------------------------------------'

.---Members in Zk2008: AuX,Faglight,Stefan,Leif,Mongo---.
|  HEIL HITLER!!     RoseMarie,Titti,MonaLisa....       |
`-------------------------------------------------------'


 >>MUSIC SUPPORT: NO REMORSE - SKREWDRIVER - IAN STUART
                  DIRLEWANGER
 >>GREETINGS TO: COMBAT 18 - HACK INC - VAM - JAEGERKOMMANDO

 >>>>>>> FAGLIGHT ^ MONALISA ^ AUX / ZK2008  <<<<<<<
```

1.72 stck

```
Stockmarket BBS Virus(?):
-------------------------


I saw several warnings concernig this 75476 bytes long file.

Shortcut from the first warning:


WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
-----------------------------------------------------------------------

I Just wanna inform all of you /X sysops, than a file -L-STOCK.LHA (a door
game for /X) has a fucking BACKDOOR !!!!

If you enter BUY option and write a number highest than possible (for
example a number 20 or 100 or any more than allowed than your Upload Status
will be restored to 0 !!!!! 0 bytes !!!!! All your uploads will be canceled!

Oh what a fucking lamers are in LEGEND !!! Shit !!!

         Discovered by EaSy RiDeR/MYSTIC
                                    -------------------------------



I don't know, if it's a real backdoor or only a programming
bug (I don't have /X). So be carefull with it.



           Detection tested 12.1.1994.
```

1.73 pha

```
Fake Phenomena Intro Virus (?):
      -------------------------------

      Filelength: 57508

      This file is crunched with Spike 1.6 and claims to be an intro
      by Phenomena. BUT if you start this file, an endless loop will
      be activated. A file will be opened ( always with oldmode  and
      the with newmode). This procedure does not stop. You  have  to
      reset the computer. If the opening process fails, the computer
      crashes.

      It was uploaded to the fast german BBSs at 1.1.1994.
```

```
  PHA-1994.EXE N  57508  01-01-94
  P H E N O M E N A  ' 9 3 - SWEDISH ELITE!
        BRINGS YOU : 1994! HAPPY NEW YEAR [-K¡T!]

        On Cauldron the following warning was spread:


FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE!


   THE SO CALLED "PHENOMENA - HAPPY NEW YEAR DEMO" IS A FUCKING FAKE! IT

    WILL FUCK YOUR HARD DISK AND CHANGE A LOT OF FILES IN THE S: DIREC-

       TORY! MOST OF YOUR FILES IN THIS DIRECTORY BECOME UNREADABLE!

              IF YOU GO INTO THESE FILES YOU CAN SEE A TEXT:

   ".. DR WHO WISHS YOU A HAPPY NEW YEAR .. PHUCK THESE GUYS (some names

                are listed) .." FUCK THIS FUCKING ASSHOLE!

                                FAITHFULLY,

                                CAP/SUPPLEX


FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE! FAKE!
                           /\      .____:_ _
```

```
  I could not resource this file because of timeproblems (VW had to
        be  released). I  have tested  it  on  my  harddisk, but  nothing
        happened (only this nasty fileopen/close). Files  in the S-Direc.
        were at my AMIGA not changed. But for  sure, this is not  a  demo
        from Phenomena.


            Detection tested 5.1.1994.
```

1.74 kef_ani

```
        Kef_Ani BBS Virus:
        ------------------

        Filelenght: 1795068 bytes
```

This programm claims to be a preview from a demo by Kefrens, which should be released at THE PARTY III in Denmark. This very short LHA archive (170KB) only contained this very long file, which contains the virus. The virus is the CLP_Wow.exe virus (read this docs,too). The virus is VERY lame coded and seems to work nowhere. I have tested it on several computers, but always a crash. I resourced the file and found lots of bugs. Lame work. Stop doing this and code some usefull programms !!!

In the first 1024 bytes you can read:

```
'BBS:'
'dR.WHo oF ALiEN LiFE FoRM (A.L.F) DESTRoYS AGAiN'
'! HAHAH! ;)'
```

This text should be written to all files in the BBS: directory.

Detection tested on
1.1.1994.

NOTE: This virus was linked with the 4eb9 linker !!!

Thanks must go to AtomiX for supplying me with the information that this virus is in circulation.

1.75 ua62

UA Dialer 6.2 Fake Virus:

Filelenght: 26868 bytes

This claims to be a new update of the famous UADialer. If you start this programm, the files BBS:user.data and BBS:user.keys will be read and the first 54 bytes will be replaced by

```
'dR.WHo oF ALF (ALiEN LiFE FoRM) WiSHES U A MERRY'
' X-MAS!'
```

(This is the sysop account !)

Shortcut from the document:

! B R A I N S T O R M !

UA-DIALER V6.2

>NO DOX NEEDED! JUST FIND IT OUT! THE DIALER WILL TRY TO CONVERT<
>THE OLD CONFIGS THE FIRST TIME YOU START IT! MAY TAKE AWHILE SCANNING!<

JHON/BRAINSTORM -93!

I have only heard that BRAINSTORM is dead.

Detection tested on 29.12.93.

Thanks must go AtomiX for sending this virus. Thanks again pal !

1.76 joke

VirusHunter 3.2 Gagvirus Fake:

Length: 4528

This programm claims to be a viruschecker. It checks your memory and says always that it found a Lamer9 and simulates a Reset. It's relly lame because on a A4000 with Kick3.1 the "hand" from Kickstart 1.x comes back. I don't like such jokes and therefor VirusWorkshop offers you to kill this programm.

This text you can see at the bottom of the file:

```
'intuition.library',0
'graphics.library',0
'CON:0/10/640/190/Hardware-Virus-Hunter',0
'Welcome to Hardware-Virus-Hunter'
'Version 10.20 on 21.07.92 by Tobias Eckert'
'This program is ShareWare. If you like it,'
'please send me : 20,00'
'Self-Checking for Virus-Infektion ... '
'Virus-Checker is healthy'
'Checking Batterie backed up clock ... '
'Your clock is healthy'
```

```
'Checking Monitor ... '
'Your Monitor is healthy'
'Checking Rom-Vektors '
'Rom is infected!!!'
'Scanning type of Virus ... '
'Found Lamer9-Exterminator-Virus'
'Checking for damage ... '
'Agnus Sound-Registers are destroyed'
'You have to replace your Agnus!!!'
'Please check doc-file for adress of your '
'local dealer.'
'Rom-Virus-Killing in progress...'
'Delete Kick-Rom ... '
'done'
'Rebooting Kickstart...'
'HA!ASSHOLE!...'
```

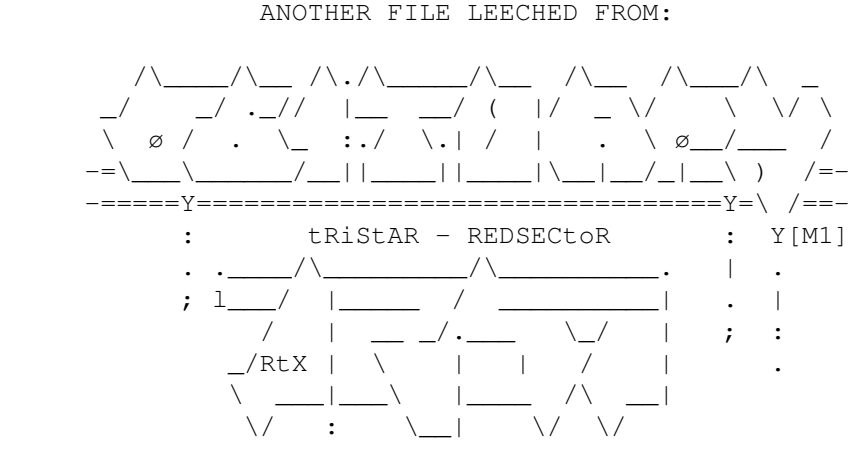
Detection tested on 29.12.1993.

1.77 merry

Merry.Exe BBS Virus:

This virus creates an am empty file PCA in the BBS directory and I was told that it formattes mailboxes. It's a old Kefrens intro and the virus was linked with the 4eb9 linker.

The file is about 60 kb long. There is another merry.exe file with about 265 kb in circulation (hi KARAM). This file only contains a "WEISSWURST Feiertags" intro by KAMPFgruppe.



W.O.R.L.D. H.E.A.D.Q.U.A.R.T.E.R.S.

Detection tested on 28.12.1993.

1.78 m-who

Master-WHO /X Backdoor:

Filelength: 4844 bytes

This is (again,,bah) a lame /X backdoor, who writes a new user to the system. Great work. Not to mention that this virus was again made with the help of the 4eb9 linker. I am searching for this linker since the last 4 months !!!!

VT and VirusWorkshop recognizes this file as 4eb9 file. I have included a special recognition routine for this virus.

Shortcut from the Master-Who.doc file:

```
*****************************
*                           *
*      MASTER-WHO V1.1      *
*                           *
*****************************
```

Featuring

-Automatically determines how many nodes are running (<= 9 nodes).
-Shows Node number , Name , Location and Action.
-The fastest who door available (100% 68000 Assembler).
-The shortest who door available.
-Tracks even loss of carriers.
-Show full action in your Kickstart workbench 1.3 2.0
-Show download files

I don‘t know, if this utiltie is existing in real, too...

Detection tested 28.12.1993.

1.79 ghost1

```
                  Fileghost Virus Installer:
--------------------------

Filelength: 8160 Bytes.

This file claims to be a speedup system for loading files. In
the text it‘s said that the LOADSEG und NEWLOADSEG vectors will
be changed. Yes, that‘s true, but only the virus will be installed
and nothing else.

Quite intelligent.

The file which was in my archiv, is not startable, because the file
was changed by 1 byte.


’ find DH0:C/SETPATCH!’
’» Can‘t load Setpatch.Maybe read-protected’
’HardSpeeder © by Christian Neumann.’
’Patch installed....’
’This Utility was written for HardDisk-’
’Users.’
’Especially for Sysops.’
’The HardSpeeder installs a Patch in the’
’LoadSeg and NewLoadSeg - Vektor.’
’After the installation it will load ALL P’
’rograms faster than usually.’
’HardSpeeder needs SETPATCH installed ’
’in DH0:C !!!’
’© by Christian Neumann (Public Domain - ’
’USE IT!!)’


        Detection tested 28.12.1993.


             Fileghost LinkVirus
```

1.80 ghost2

Fileghost Virus :

This is a linkvirus, which adds NO hunk to the infected file. It will increase the first hunk (876 bytes) and changes the "RTS" at the end of the hunk or tries to go back several steps and searchs for a "RTS". This "RTS" will be replaced by a "BRA XYZ".

The virus changed DOS(NEW)Loadseg and Exec Forbid. No reset-vectors will be changed.

At the end of the file you can read:
(this text ist mostly decrypted by a "eor.b d0,(0)+" routine. Nothing special...

```
'dos.library'
'Hi Friend! Don't worry... It's only the '
'FileGhost.'
```

Fileghost LinkVirus Installer

1.81 bootx

BootX Recoqfile Updater Fake Virus:

Filelength: 2052

This file appeared on an american BBS system and was spreaded as BootX updater. This is a trojan horse containing only a formatterroutine. I think the purpose of this programm is to damage the reputation of SHI.

The virus opens a window with the following text:

```
'RAW:0/0/640/200/BootX-Updater by SHI Safe'      <Winname>
'Hex International, Erik Loevendahl Soerensen'
'dos.library'
'This program updates the BootX-Recognition-'
'Files, so BootX will know 87 new'
'viruses. Sometimes the update-procedure fails'
' and your (hard)disk will be'
'quick-formatted, but this is not a big bug'
', simply use an undelete-tool like'
'quaterback-tools or disksalv. But mostly'
' updating works fine and the result'
```

```
'is a new powerful BootX-Version! Even '
'better, some people think of the'
'quick-formatting-bug as a great feature, '
'because by quick-formatting all'
'viruses get destroyed, so everybody should'
' use BootX-Updater!!'
'You can become a member of the famous SHI-'
'organization, if you supply SHI'
'with at least one virus per month. Self-'
'-programming of viruses is very'
'welcome, by this way we will learn about'
' future virus-techniques and we'
'can control anything, both viruses and '
'antiviruses. It is absolutely legal'
'to program viruses, because SHI doesn't '
'spread these viruses.'
'Only programmers of antivirusprograms can'
' get these new viruses from SHI,'
'Either by exchanging viruses or by paying'
' 5$ for each 1 KB Virus. I think'
'this is a fair price for all the idealistic'
' work, SHI is doing. So if you are'
' able to supply us with at least one new'
' virus per month, join SHI'
'                       SHI     Safe Hex '
'International'
'Erik Loevendahl Soerensen (also known as '
'the master of the virus-universe',27,')'
'            Snaphanevej 10, 4720 Praestoe'
' Denmark - Europe'
'sys:system/format  ......         '    <Formatcommand>
```

Detection tested 30.12.1993.

1.82 clp_wow

CLP_WOW.exe Virus:

The warning that a destroyerfile called "CLP_WOW.exe" is in circulation appeared 21.12.1993. I started searching for this virus like hell. But I did not find it on the german systems.

On the 24.12.1993. at 21.00 o'clock I found a file called "clpvirus.txt" on a fast german BBS system. The file came from the USA (Planet X) and contained a complete dissassembly of the virus and a warning.

A big sorry to all friends, who I nerved with always calling and asking for this virus.

The sourcecode was complete and so I assembled it with 4 assemblers (OMA 2.05 (opt,nonopt) ASM-ONE (opt,nonopt)) and included the recognition routines for this virus.

I hope that the original file will be recognized. Due to the case that the whole source was in this file, it‘s very possible that clones appear.

Inner workings of this virus:

The S: directory will be scannned and all files will be loaded. Then the loaded will be overwritten (ca. the first 200 bytes) by a lame text and the file will be written back. No rescue for executable files is possible.

Another point: The virus is so buggy that it crashes at all of my systems and no danger is caused. The LAMERS made several mistakes.

This file seems to be spread together with the archive "bullet.lha".

At the end of the file can be read:

"Isn’t CUTE LITTLE PONNIES just a nice group!?... hahahaha!"
" Fuck off... Next time we will be even MORE nice... "
" MONO oF CUTE LITTLE PONNIES! HAHAHAHAH! Oups."
".. Hope we didn’’t destroy any valuable configs in ure "
"S-drawer... ahahhHHAHAHAHAHH!!!!!!! Ok, have fun, anbd"
" don’’t 4get to call again! HAHA! ’

Comment 29.12.1993.:

A cracked version of /X 3.19 appeared on the boards. This version was cracked by Mono of Cute little Ponnies. Same name. I saw a warning that this /X release contain a backdoor.

NOTE to the man who dissassembled this virus:

Never spread a complete sourcecode of a virus ! Some lame guys could assemble and spread the file again. You are right if you say that this virus is VERY lame coded but the damage is too big....If you have the original virusfile, I would be happy, if you could send it to me. Or upload it to one of TRSi‘s Boards

and ask the Sysop to post it to me....

I have tried to start the new assembled files, but the programm failed.

Comment 12.03.1994: A lot of such based programms have serious problems.

1.83 atari

ATARI Virus:

This virus is a simple BSG9 clone. Nothing more to say about it. Kids, play with your joysticks but do not produce such lame virusclone, which every better viruskiller recognizes(or should recognize!) !

Detection tested on 7.12.1993.

1.84 levis

Leviathan Virus (Bootblock+File):

This virus is a quite tricky combination between BB and file virus. It can be written as a normal bootblock to disk and it can write a file in the first position of the Startup-Sequence.

The virus uses the memory from $7f000-$7e000 direct.
At first the viruscode will be copied and after this, the memoryblock will be allocated.

ColdCapture, OldOpenLibrary and DoIO will be changed.
The Coldcapture Routine initializes the DoIo and the Old-Openroutines.

I have tested this virus with a normal A500+ and an A4000 but the ResetRoutine of this virus does not work on this computers. You have to coldreset your machine.

At the end there is a crypted textblock:

```
'YOU ARE THE OWNER OF A NEW GENERATION OF'
' VIRUS! IT FUCKS YOUR STARTUP-SEQUENCE! '
'HAVE FUN.... '
```

In this virus was no special destroy routine found (except the BB write command).

Detection tested 6.12.1993.

1.85 conman3

ConMan Dir Virus Installer:

Filelength: 20980 (packed with TurboSqueeze 6.1) bytes
24340 (unpacked) bytes.

This is the installer for the ConMan Dir virus. At the start it checks for the taskname "CONMAN-Virus". If this name is existing, the virus will be not activated. The virus was linked using the 4eb9 linker to an USR modemsetter. After this progress, the virus was packed with the Turbo-Squeeze 6.1 packer, which was used at the Dir Virus, too.

If you depack the file (using Xfdmaster Library, Decrunch Library does not recognize it), you can read the "normal" texts like "Snoopdos" or "dos.library".

The above mentioned "CONMAN-Virus" task will be not installed by the installer. I think, that it‘s somekind of selfprotection.

The installer crashes on 68040 machines with activated caches.

Detection tested 10.04.1994.

For more information concerning the ConMan Dir Virus simply

click me!
.

1.86 conman2

ConMan Dir Virus:

Filelength: 4004 bytes (using TurboSqueeze 6.1)
8456 bytes unpacked

This virus creates a new process with the name "Workbench ". It writes a new Dir Command and tries to damage several other files (L:RAM-Handler,Devs:System-Configuration,C:Loadwb).

No spreading was possible on a normal (not accelerated) A500+.
On an AMIGA 4000/40 the virus could be started and wrote a new dircommand. The virus does not work with activated caches. It will simply crash.

VirusWorkshop removes the process NOT. It simply fills up the whole process with "RTS". Sorry guys. I have tried to remove the task, but after some crashes (mainly on slower machines), I stopped this project.

The virus will sometimes display an alert and after you have pressed a mousebutton, the value $fa0 will be written to the interrupt enable register. All disk/keyboard actions will be disabled.

Alerttext:

THIS IS NOT A SYSTEM ALERT! THIS IS THE NEW CONMAN-TROJAN VIRUS!

ALL DISK ACTIVITIES WILL BE DISABLED!

GREETINGS TO JOE/DEFJAM BRUCE/DEFJAM NATAS/DEFJAM ALEX/DEFJAM AND DOC!

CONTACT ME xxx-xxx-xx-xx USR 14.4 NO STUFF! ONLY VIRUS-PROGRAMMER AREA!

Detection tested 30.03.1994.
Ramdetection tested 31.03.1994.

1.87 conman

ConMan Virus:

This is a trojan horse against the AmiExpress mailbox system. It tries to work with the User Files from the /X System, but it's so lame coded, that it has several problems with it.

This virus probably appears as the ARTM2.3 fake Virus because the virus is linked at ARTM.

The viruses uses memory at $4f000 to decode a little string saying: "CONMAN/HACKMASTER/93/TROJAN-Virus".

The whole virus looks like a work from a beginner, who once read an article about /X ! Better play with your joystick !

The virus does not work on an AMIGA with MC68000 processors,
because the virus decodes a string at a nonequal adress!

Other possible name: ARTM BBS Virus

Comment 19.12.1993.: Today I got the message on Diabolo to take care of my pws, because ConMan tried to hack mailboxes in the last days. It seems to be an active hacker ....

Detection tested 6.12.1993.

1.88 vmaker

ComaVirusmaker by TAI-Pan and VirusMaker 1.0 Installer:

Both programms offer the user the possibility to install various viruses (Lameblame,Chaos,Gadaffi,Ass,ByteBandit, Sca....). The programms are only simple installers, but I decided to include this both files.

The files are VERY old and I think that nearly nobody uses this crap but who knows.

Detection tested on 20.11.1993.

1.89 sep2.26

Sepultura 2.26 Virus:

Works with MC68040 (without caches) and Kickstart 3.0

It patches:
- DosLoadseg()
- DosRename()
- DosDelete()
- DosLock()
- DosOpen()

No resetvectors will be changed !

The virus writes a not visible file to drive df0. It makes the Startup-Sequence 5 bytes longer and inserts its own filename at the top of the Startup-Sequence.

At the bottom you can read (after decoding it):

```
'Wer schaut mich an in dieser Eil sind '
'wir etwa nötig geil? Bitte, bitte laß mich'
'da, sonst sag ichs meinem Großpapa.'
' (w) Sepultura (V2.26)'
```

The adress $7fff0.l will be accessed without allocating it ! The virus will be crypted with a value out of $dff006 (VBI).

Detection tested on 17.11.1993.
Ramkill tested on 17.11.1993.

1.90 boss

Bossnuke 1.5ß Trojan horse virus:

Bossnuke is one of the best (maybe the best) nuker for the AmiExpress mailbox system. The "new" bossnuke release contains a virus !!!

The programm ULOG.X (length 18560 bytes) writes to files on your drive:

```
'BBS:COMMANDS/BBSCMD/L.info' ( 1060 bytes long)
'doors:scan.x'               ( 712 bytes long)
```

The second file contains a formatroutine, which writes only "DOS3s" to your drive. It will scan the devicelist and write via CMD_Write. No chance to rescue a file, which contains such a buggy block.

Detection tested on 17.11.1993.

Special thanks go to No Limit/TRSI for keeping this virus for me...

****

Comment from BIGBOSS to the fake release:

BOSSNUKE v1.5 is totally FAKE and never has been released by me (BIG BOSS). I have released v1.0 and have included v2.0 in the utility package available on Mirage or any amiexpress support bbs. If you are running BOSSNUKEv1.5, remove it immediately!

For all of you out there running BossNuke v1.0, I will *NEVER* update the ulog.x file. It is the same one that was being used in v1.0 that can still be used now for v2.0. In my utility package is a version of ULOG.X that is different than the bossnuke version, but this contains the special FILE_ID.DIZ extraction routines and also BOSSTOP weekly routines. This will never be released in any version of BOSSNUKE.

If you ever get a new version of bossnuke, make sure that you do not install a new ulog.x. You can use the one out of the old v1.0. If you have purchased the bossutility package, then the ulog.x in there is with the extra features and can be trusted.

Do not trust any BOSSUTILS that you do not download off MIRAGE or any amiexpress support bbs.

Big Boss/Author of BossNuke

****

1.91 megalink

Megalink Virus:

This virus works like the old IRQ Team linkvirus. A hunk will be added (length $fd*4) and the file will be 1044 bytes longer. The virus contains no routine, which makes it reset proof. The virus does not patch a library.

Detection and Repairroutines tested on
14.11.1993.

1.92 seekspeed

SeekSpeed Trojan Horse:

This is a Jeff Butonic 3.00 linked together with SeekSpeed 37.10 by R.Waspe. The used linker was the Hunklab by United Forces (Cachet).

Due to the case that everyone can get the original SeekSpeed programm, this time no repairroutine.

Thanks must go to KARAM for sending this virus.

Detection tested on 20.10.93.

1.93 nast

The NasT Virus is 2608 bytes long and can be seen as a clone from the BGS9 etc. familie. Nothing more to say about it.

1.94 darkavenger

Dark Avenger Link Virus:

Type A:

This virus is a linkvirus like the Infiltrator Virus. It changes the first longword in the first hunk and activates itself in this way.
The first hunk will be 1128 bytes longer. The virus itself is crypted and the code changes every time. That is a new technique on the AMIGA. You can not test at special adresses....

The virus patches the DOSOPEN vector and is not resident. All files longer than $186a0 and shorter than $7d0 bytes will be not infected. The virus allocates $18c7c bytes memory for all actions.

Sometimes (after infections) the virus changes the the window-title to "-=- The Dark Avenger -=-".

It should work on all OS2.0 Kickstart systems and works with the MC68040 (all caches avaible).

Detection and repairroutine tested
on 8.10.1993.
Memorycheck & DosOpenrescue tested
on 9.10.1993.

Please make always a backup of the infected file and then try to repair the file !!!

Typ B:

This virus is a linkvirus like the Infiltrator Virus. It changes the first longword in the first hunk and activates itself in this way.
The first hunk will be 1072 bytes longer. The virus itself is crypted. The first LW is in the crypted part of the virus. It patches the DOSOPEN vector and changes no resetvectors at all.

The virus itself works on MC68040 but take care of the caches !!

Detection and repairroutine tested
on 9.10.1993.
Memorycheck & DosOpenrescue tested
on 9.10.1993.

It is not possible that each type links 2 times behind on a file. But it is possible that a file will be infected by Typ A then by TypB and again by Typ A. I have made a file containig 20 links !!!!

Please make always a backup of the infected file and then try to repair the file !!!

1.95 zapa-dms

The Dms 1.12 Turbo Fake Virus (Zapa-Adder):

Filelength: 7636 Bytes

This is a patched version of DMS 1.11 Turbo Generic. It contains a little backdoor, which patches the files:

-BBS:User.Data
-BBS:User.Keys
-BBS:Config1

and adds a user "ZAPA" to this files, which has a very high

level and a very good acount.

Due to the fact that everyone can get new DMS releases, VW will only delete the file.

1.96 loadwb

T.F.C. Revenge LoadWb 1.3 = KAKO Loadwb Virus:

Filelength (unpacked): 2804

This is a patched loadwb command, which installs an Extreme Clone BB in memory. The Kako LoadWB is only a simple editor clone. It should work on all systems.

The following texts can be found in the T.F.C. Revenge LoadWb:

'T.F.C. Revenge LoadWB ... © by The Fanatic Crew ...'
' Don't try to check this out ... coz we've got the power ...' ↩
,x??N®ÿN^1????Aú?ZCú? <
'The Fanatic Crew???ø0proudly presents T.F.C. Revenge Virus V1.03
'Swapping disk for disk ... is always a great risk ...so better '
'use a condom next time ...signed The Fanatic Crew, 06.06.1991'
'We've got the power ...dos.library intuition.library'

The KakO LoadWb contains only different the string "KAKO LoadWB". A work of a real "hero". Stop this and play with your joystick...

1.97 commodore

Commodore Virus:

This is a simple destroyerprogramm.The file is 1752 bytes long and contains the following stuff:

1.At the start of the programm the adresss $66666 will be increased by 1.It depends on the value in this adress, what happens.A work of a beginnner (I think) because the string "dos.library" can be found 4 times in this short file.
2.The destroypart: It simple deletes the file "s/startup-sequence" and creates an empty directory with the name "Commodore war hier !!".

The following texts can be found in the virus (non crypted!):

```
'Commodore war hier !!',0
'  Ihr Computer ist Überhitzt !!!'
'-Wenn es nach dem Reset ein absturz gibt'
'  SCHALTEN IHN SIE BITTE AUS'
'   Commodore 1987'
'Please remove the Write-Protection'
'And Press Mouse-Button to Continue'
' KEIN VIRUS IN DRIVE DF0:  '
'      GEFUNDEN !!         '
'    Commodore 1987'
'You have found the Routine !'
'This is the new Commodore-Virus !`
'BY STARLIGHT ENTERPRISES 1992'
```

Simply delete this virus file and check your Startup-Sequence.

1.98 mchat

M_Chat Virus:

Filelenght:13492 (unpacked)

Spreaded on the german boards on 24.9.93.

This is a destroyer programm for the /X BBS system.It claims to be a bugfixed version of MULTICHAT.
If you start this programm,the following devices will be quick-formatted:

-dh0:,system2.0:,df0:,df1:,dh1:,dh2:,dh3:,dh4:,df2: and hd:

After this actions the simple text

"Sorry,the BBS is not registred" will be printed.

At the end of the file you can read:

`MULTINODE CHAT DOOR VERSION V2.3 [BUGFIXED] by Portax of Wibble`

```
‘copy c:format ram:ff‘
‘copy sys:system/format ram:ff‘
‘ram:ff drive dh0: name HAHAHA noicons quick < ram:cr‘
‘ram:ff drive system2.0: name HAHAHA noicons quick < ram:cr‘
’ram:ff drive work: name HAHAHA noicons q’
’uick < ram:cr’
’ram:ff drive dh1: name HAHAHA noicons quick < ram:cr’
’ram:ff drive bbs: name HAHAHA noicons quick < ram:cr’
’ram:ff drive df0: name HAHAHA noicons quick < ram:cr’
’ram:ff drive df1: name HAHAHA noicons quick < ram:cr’
’ram:ff drive dh2: name HAHAHA noicons quick < ram:cr’
’ram:ff drive dh3: name HAHAHA noicons quick < ram:cr’
’ram:ff drive dh4: name HAHAHA noicons quick < ram:cr’
’ram:ff drive df2: name HAHAHA noicons quick < ram:cr’
’ram:ff drive HD: name HAHAHA noicons quick < ram:cr’
’ram:ff drive df0: name HAHAHA noicons quick < ram:cr’
’ Sorry, the BBS is not registred’
```

A shortcut of the (very) short document:

What is it?!

Well M_Chat Is a MultiChat Node Door , Quite simple actually.

Installation!

M_Chat is VERY easy to install!
Make sure you have you boards main dir. assigned as BBS:
And your doors dir. assigned as: DOORS:
Just copy the actual proggie: M_Chat to your DOORS: dir.
Add the following line to your BBS:COMMANDS/CUSTOMCOMMANDS or
BBS.CMD file like this:

```
----------------------------cut here!
*CHAT     XM010DOORS:M_Chat
----------------------------cut here!
```

This is a great Multi_Node chat door for Amiexpress

In the states at least one BBS (Planet X) was formatted with this tool.

Detection tested on 25.9.93.

```
 Comment 07.03.1994: On some german boards there appeared a file
       called ATX-chat.lha. This file contains exactly the same virus.

       A shortcut of the (very) short document:

           MULTINODE CHAT DOOR VERSION V3.0 FROM TRASH/ANTHROX

  WELL THIS IS THE NEW 32 MULTICHAT DOOR FROM TRASH/ANTHROX.YOU NEED /X
                             3.32 OR HIGER.

INSTALATION:

COPY:
------------------>
ATX-CHAT  ---> BBS:DOORS
CHAT.INFO ---> BBS:COMMANDS/BBS.CMD
------------------>

-.-.-.-.-.-.-.-.-.-.-.-SORRY FOR THIS MINIDOC.FILE-.-.-.-.-.-.-.-.-.-.-.--.-.-


                                                          TRASH/ANTHROX


         Detection retested 07.03.1994.
```

1.99 aereg

```
       Aereg 3.9 Virus:
       ----------------


       Length (packed with Imploder 4.0 in Lib.mode): 656 bytes
       Length unpacked:                               664 bytes

       Appeared 11.09.1993  on  the german mailboxes  with  the
       following name: "aereg`em.lha".

       It claims to be a registrator for the cracked version of
       AmiExpress 3.9.I have heard that AmiExpress 3.9 does not
       need a keyfile.So what`s this ?

       Oh,a new little very LAME destroyerprogramm for the  /X-
       system.
       It destroys following files:


         bbs:user.data
                                      bbs:user.key
                                      bbs:utils/express
```

The programm works with all processors and Kickstarts.

At the end of the decrunched file you can see the following text:

```
'Registrator for Ami-Express'
'Startup /X 3.9 Crack As Normal'
'Run Registrator v0.1'
'To Update 3.9 to a Registation /X'
'Registration LRA-11.0089'
'This is an un-registered version of Expr'
'ess'
'Registration UOB-09.0493'
'Registration version of Express v3.9'
```

The document for this virus looks like this:

```
"Note:

This Stuff is quite easy to install...
extract all stuff to ram: and copy the dir contents into your own..
first run AeRegist.exe after that run convertdb to convert the old
ami-express conf.db into the V3.9 conf.db
(this will clean up the msg base also)

Thx for your attention, have fun !!"
```

Detection tested on 12.09.1993.

NOTE: This virus will be recognized packed and nonpacked.

1.100 aisf

A.I.S.F. Virus:

Length: 8708 Bytes

This virus will be probably spreaded as a faked VirusChecker update.The file works with all kind of Kickstarts and memory-configurations and has no problems with faster processors.

This file opens a window ith the following name:

```
'VIRUS-CHECKER V6.72'
```

'by A.I.S.F. !!!'

The window has no funtion.It's only a trick to irritate the users.

The $6c Vector in the Zeropage will be patched. Following routine will be installed in the vector:

1.Decrease a counter by 1
2.Compare if it $50000
3.If not,do nothing
4.If $50000 is reached,then display the following alert,which will be decrypted first:

```
'!! CRIME DO NOT PAY !!!'
'WHY ARE YOU SWAPPING ILLEGAL SOFT ?'
'BECAUSE YOU ARE A CRIMINAL !!!!'
'AND BE SURE:'
'WE (A.I.S.F.) WILL GET YOU !'
'(A)NTI'
'(I)ILLEGAL'
'(S)WAPPING'
'(F)OUNDATION'
'-PRESS MOUSE TO CONTINUE-'
```

If you then press a mousebutton,then the destroyroutine will be started.Your drivemotorhead steps around on the disk.

I am only wondering,why the value $50000 was chosen.If you count only the VBI interrupt then the virus would start its work after nearly 2 hours.

At the end of the file (which is not crunched),you can see a non-crypted text,which says several times:

```
' THE A.I.S.F. INTERLAMER-VIRUS  '
```

VirusWorkshop removes the useless and the patched $6c vector.

Thanks must go to Ingo Schmidt for sending me this virus.

Detection tested on 11.09.1993.

1.101 descr4.0

Description 4.0 Virus:

Filelength=7016 Spreaded at 05-07-1993.

This virus appeared first at 05.07.1993. on the german BBSs.It's a patched version of Description 3.0 by SBS!.This is a utilitie,which is only usefull for AmiExpress boards.It was released as version 4.0

but in the file the original 3.0 messages appear.Then it claims to load "SNAP" in the memory but it loads the delete command and clears all files.The viruscoder must have Kickstart 2 but is for gods sake not very well informed about the new functions....

You can see the command as an ASCII string in the code:

"delete :#? all".
Protect all important files on disc and the virus should not clear them,because "delete" searches for the PROTECTIONbits"....

The virus is completely implented in the programm.No linker etc. was used in my opinion.The virus works only if all programms needed by the original DESCRIPTION 3.0 are avaible.I forgot to copy the file: "S:Descriptions.TXT" and the virus did not work.

Special thanks must go to Atomix for the warning and Ronny for keeping that virus for me.Thanx pals.Two days after the first appearance of this virus,I got it from you....

Detection tested on 07.07.1993.

At the end of the file you can see a text saying:Your HD is deleted. Happy Birthday MCI/DCS Hahahahah.....

Comment 28.07.1993:

The -z-speed.lha Virus is the DESCRIPTION 4.0 virus.Thanks Marcel ! This virus claims to speed up your USR HST 14.4 modems.This is pure garbage.

The original document:

>Just RUn Speeder.exe From Ram And Watch YER CPS CLIMB On
>You Next Transfer Mine Increased from 1600 to 1800
>On normal 14.4 HST
> SAMIR ZENITH LEADER
Y
>Watch For Our releases!!!!!

-> This is a damm fake.Samir has nothing to with it (at least I heard it).

Detection tested on 01.08.1993.

1.102 dtroy2

Disktroyer V2 virus:

This is not a virus.It's only a file,which has the job to kill the information on your drives.The diskregisters ($bfdxxx) will be directly used.

The routine does not work correct on AMIGAs with higher processors because of some timing problems.

Some parts of the resourced code:

```
L_1EC MOVE.W  #$0800,D0
  BRA.B L_1F4
L_1F2 MOVEQ #-1,D0
L_1F4 NOP
  DBRA  D0,L_1F4    ;Some kind of waitloop
  RTS
        ......
```

Detection tested on 6.7.1993.

1.103 bbsvirus

Infected Diskrepair BBS Virus:

Again another trojan horse for the AmiExpress BBS system. This virus is linked BEHIND a new version of DISKREPAIR.The used linking system is the $4eb9 linker as used in many other trojan horses against AX. The new thing in this virus is that is not linked in front of the file.

In this case the viruspart is imploded and is decrunched 10244 bytes long.

The directories BBS and BBS:Utils/ will be scanned for a special filelength(ca.200000 bytes) and the SNOOPDOS task will be searched. I cannot say what this virus exactly makes because I have no AmiEx release.

Some resourced virusparts:

```
Snoopdos_Search
  PEA snoopname(PC)
  JSR FindTask(PC)
NoSnoopDos
  ...
```

```
snoopname DC.B  'SnoopDos',0
bbsname1  DC.B  'BBS',0
bbsname2  DC.B  'BBS:',0
bbsname3  DC.B  'BBS:',0
bbsname4  DC.B  'BBS',0
bbsname5  DC.B  'BBS:',0
bbsname6  DC.B  'BBS:Utils/',0
```

A utilitie, which does not work,if SnoopDos is active ? Not normal.

Detection tested on 29.05.1993.

Infected WhiteBox BBS Virus:

This virus is very similar to the virus linked behind Diskrepair. The viruscode is more optimized and it will be searched for some more filelengths.The used linker is the $4eb9 linker.Who does have such a linker ?

If a Sysop with the AmiExpress system finds such a virus please reinstall the AmiExpress mainfile.

Detection tested on 06.06.1993.

The "Whitebox" and the "Diskrepair" viruses does only work with some versions of AmiExpress(ca.5 releases).I do not think that they touch AmiExpress 3.03 or AmiExpress 3.04.If you have a list with lengths of all the AmiExpress releases then please let me know it.

1.104 xaca

XACA Virus = Lummin Virus

1.105 beton

Butonic 4.55 Virus:

This is a simple Butonic 1.31 clone.Only the texts were changed. Due to the case that I did not explain the older Butonic,I will describe this one:

Changed vectors : $68 (only in the Zeropage)
-454(DOIO / EXEC)
Kicktagpointer(Exec)
Length:3408 bytes

The virus copiers itself with a filename,which will be one of the names listed,to a disk and changes the Startup-Sequence. The name of the virus will be copied at the first position of the Startup-Sequence.The length will be not increased.As a result the last entry in the file will be cutted and works in many not.

Intuition Displayalert Text:

```
' hoffentlich stoere ich sehr !',0
'* I am JEFF - the old Virus family for '
'an Amiga * (w) by the nicely  BUTONIC.',0
'HV 4.55/29.02.93 - Generation Nr.00001',0
'ZKillings goto* BootX    *,* VirusZ   *,'
' Virus_Checker ,',0
'Viruscope, Maus , Virus-Checker , Virus'
' Control and big VT !!',0
```

Texts for the Windowname:

```
'Hallo gib die Cola her !',0
'Lass die Chips roesten und nicht rosten '
'!!!!',0
'Nimm die Birne weg sonst krachts!',0
'Wenn Du nicht spurst dann gibts $!',0
'BoTiNuC!',0
'Schaem Dich Du Banause lass es sause Jun'
'ge  ...aber nicht schlappi...!',0
'Willst Du Nachhilfe oder was is los  ?',0
'Gib es auf Du lahmer socke...',0
'Wer andern eine Grube graebt faellt selb'
'st in dieselbige !!!',0
'Wo willste den jetzt wieder hin',0
'Kannst Du mal Ruhe geben Du alter Knoche'
'n-Kerl ...',0
'Liebst Du Viren, dann weiss ich auch, we'
'r Dich am meisten hasst',0
```

```
Names for the virusfiles:

  'LoadWB       ',0
  'Mount  ',0
  'Cls      ',0
  'VirusY   ',0
  'setclock opt i ',0
  'info ',0
  'Obelix ',0
  'Idefix ',0
  'Asterix  ',0


          Detection tested on 31.07.1993.

                (Remember to fix the Startup-Sequence !)


Comment 05.08.1993: It appeared a file called "sd-tv",which  claims
      to be SnoopDos 1.9.I cannot say,if this is a real update or a fake,
      but this file installs the "Butonic 4.55" virus in the memory.

                 This file was created by the use of Hunklab.


    Detection tested on 05.08.1993.
```

1.106 4eb9

```
      $4EB9 Files:
      ------------

      This type of linked file(Is there a  utilitie in  circulation,which
      creates such files ?)  was  several  times detected in BBS  viruses
      like SWIFTWARE 0.98.

        ! The viruses are not always linked at the front of the file !

      The basic structure of the fileformat looks like this :


      ; Hunktable

      jsr $0  = $4eb900000000
      jsr $0  = $4eb900000000
      moveq #0,d0 = $7000
      rts             = $4e75

      ; Hunk which fixes the two jumps.
```

Detection tested on 30.05.1993.

Note: MANY BBS viruses are spreaded in such files ! If you find such a file please send it to me ! Thanks a lot ! SnoopDos is not the right way because the SNOOPDOS task will be (sometimes) deactivated.

List of known 4eb9 files:

GoD-CLT1.exe ; Global Overdove +12 Trainer
; for CLYSTRON.

In this file there is no virus.Only the TRAINERmenu was linked with the 4eb9 Linker.

Comment 12.12.1993: A new 4eb9 clone appeared. A virus was linked on a faked ARTM version. This new code looks like this:

```
; Hunktable

movem.l d0-d7/a0-a6,-(sp)
jsr $0
movem.l (sp)+,d0-d7/a0-a6
jmp $0

; Hunktable
```

Comment 31.03.1994: I got a call from a person, which did not want to say his name, which said, that CONMAN programmed the linker and several other viruses (see Conman Dir).

Some $4eb9/$4ef9 files:

-Master Who 1.1
-Uadialer 2.8
-ConMan Dir Installer
-Xcopy (Mount Virus)
-...

Detection tested on 12.12.1993.

1.107 nano

```
NANo Virus + NANo ][ Virus:
---------------------------

This virus copies itself with a not visible name at the  first  pos.
of the Startup-Sequence (at least it tries to do this ).There  is  a
little  Intuition  routine included, which shows you a  little  text
with the greetings from the "hero",who created this simple virus.

The other version of NANO shows a germanflag at the reset.

The following vectors are changed:

    $2e(execbase)
                                          -$1c(DOSBASE)
                                          -$54(DOSBASE)
                                          -$1c6(Execbase)
                                          -$94(DOSBASE)



NANO filelenghts:  NANO1 = 1484
                   NANO2 = 1472


The viruses does not work correctly on the A4000 with MC68040.

                 Detection tested on 23.05.1993.
                                  & on 06.07.1993.
```

1.108 compu

```
          Compuphazygote 7 LinkVirus:
---------------------------

      Several vectors will be changed. I got an infected echo file,
which was not executable and the hunkstructure was totally
      damaged.

      I tested this virus against VT 2.62 and it proofed my analysis:
      - Hunkstruktur defect !

      I wrote a repairroutine for this virus but I cannot say, that
      this is a 100% proof  one. I could  only  test  it  on  a not
      repairable and executable file. So, if you have this virus,
      please send me a copy, so that I can check my routines.

      An infected file becomes 1760 bytes longer (at least I hope
      this !).
```

Compuphazygote 8 Virus:

This virus contains many parts of the NANO virus (or should I better say that the NANO viruses contain big parts from the Compuphazygote virus?).

Exactly the same vectors are changed and the whole structure looks very familiar.

The Compuphazygote virus tries to trick out the user with this text at the top of the file:

```
'     :AmigaDOS Datafile @ 1988 by CBM.This file contains important'
      '     disk data for Block Allocation ! '

'     >>> WARNING:  Deletion  of this file  could  destroy all disk'
      '     datas !!! <<<'
```

This is pure bullshit.

Detection tested on 07.07.1993.

Compuphazygote 2 Virus + VirusZ_II 1.02 virus

1.109 virusz

Compuphazygote 2 & VirusZ_II 1.02 Viruses:

Filelength: 1148 bytes

Damage: On every inserted disk (via ICDMP flag) will be the new file "c:VirusZ" or "c:virusx" with a length of 1148 bytes written. The virus waits for the diskinserted flag and for the closewindow flag. At the bottom of the file there somekind of hardware read/write code, which will be only accessed if the files could not be opened correctly.

Simply copy the viruskillers back to c:

Text, which can be read at the end of the VirusZ II 1.02 virus:

```
'intuition.library'
':c/VirusZ'
':c/VirusZ'
'This is a new Utility for your amiga computer ! '
'It gives you safety to all new virii in future!'
'No vectors can changed anymore so your computer'
'is safe ! ! ! '
      'VirusZ II 1.02 Georg Hörmann',0
```

Text, which can be read at the end of the Compuphazygote 2 Virus:

```
':c/VirusX'
'intuition.library'
':c/VirusX'
':c/VirusX'
'The CompuPhagozyte has attached to your '
'system !'
'Wait for  new virus in other computer-systems'
'The CompuPhagozyte in 9.91 by The Emperor'
' Of Trillion  Bytes !'
'VirusX 5.00 by Steve Tibbett'
```

Detection tested (VirusZ Virus)
26.12.1993.

1.110 dltdsv

Diskvalv 3.01 Loader Fake Virus:

Length: 3604 bytes

This is a simple Modemcheck Virus clone, which only writes a new destruction longword and some ASCII texts have been changed.

For more information read at
Modemcheck Virus
.

Other possible name: Disksalv 3.01 Fake. DLT ...

Detection tested 27.02.1994.

1.111 modemcheck

```
                  Modemcheck Virus:
-----------------

This virus installs a new "c:loadwb" command,which needs OS2.++.This
new "c:loadwb" command starts a new process with the name
"Diskdriver.proc".After waiting some minutes (ca.3) a routine will
be started, which kills a single cylinder on a device by writing a
memoryblock filled up with the longword "FUCK". This damage cannot
be fixed.What makes VW, if it detects the virus in memory ?It simply
fills up all DOIO commands with NOPs and the virus is not able to
the destroying diskaccess.The process itself will not be touched.
What to do ? Simply check your disk for viruses and afterwards reset
your AMIGA. All should work correct by now.

VT goes a different way and removes the complete process.As stated
in the VT-Kennt document it is very complicated to remove the full
process. I just searched for the easier way of disabling the virus.



    Memorycheck routine tested on 17.5.93.
   Modemcheck Install detect routine tested on 16.5.93.
  Modemcheck "c:loadwb" detect routine tested on 16.5.93.


Comment 06.06.1993.:In the Fidonet the virus is called "FUCK" Virus.
There appeared a special Fuckvirus killer on the boards,which claims
that other viruskiller would not detect it in memory.Just run VT2.53
or VW2.0b (both released more than one week earlier) and you will
see that the virus is recognized and deactivated.



Known clones:
          Disksalv
          .
```

1.112 bestial

```
Bestial Devastation:
--------------------

First of all I could at first not spread the virus. God knows why it
failed.

The virus adds 1124 bytes to the first hunk and copies itself at the
beginning of the file. Some hunkroutines in the virus are not correct
and it is possible that many infected files does not work. The next
point: The virus uses absolut adresses and should only work on a very
```

few systems with &c00000 ram (Ranger Ram).

1.113 antichrist

Antichrist Virus:

This is a normal clone from the Travelling Jack viruses. The main-idea is to add a first hunk with different lengths. At this clone only some cryptparts and some eays other stuff was changed. VW says "TRAVELLING JACK" and is able to kill it.

Detection and termination tested on 18.3.93.

1.114 dialer

Dialer 2.8g Virus:

This is a trojan horse for AmiExpress.The SysopPW will be taken and put in the file "nocallersat300". Now the hacker can simply get the PW (when getting connected with 300 baud) and enter the BBS.
The UADialer 2.8 is a bluebox. Therefore I did not code a repair-routine for this virus. Blueboxing is a crime and I do not want to support it.
Due to the fact that it is spread in a crunched executable file,VW will only recognize the crunched file.

The crunched executable file does not work an a A4000 (MC68040) with activated CACHES.

```
VirusStart:
dosbase   DC.B  0
    DC.B  0
    DC.W  0
filehandle  DC.W  0
    DC.W  0
destfilehandle  DC.W  0
    DC.W  0
memblock
    dcb.l 40,0
dosname   DC.B  'dos.library',0
username  DC.B  'bbs:user.data',0
desttext  DC.B  'bbs:node1/NOCALLERSAT300',0
```

A little script,made with DosTouch,which shows us the inner workings of the Dialer28g:

```
  Load   ram:dialer
->  Open   bbs:user.data     Openmode:OLD
->  Open   bbs:node1/NOCALLERSAT300     Openmode:OLD
  CProc  DIALER-TASK
  Open   s:UADial.pref     Openmode:OLD
  Open   s:UADial.prefs     Openmode:OLD
  Open   s:UADial.conf     Openmode:OLD
```

Detection and Termination tested on 18.03.93.

This virus (like most BBS trojans) should only work with AmiExpress 1.x and 2.x because the structures of AmiExpress 3.x are a little bit different,aren't they ?

Comment 08.08.1993: In the last days there appeared a BETA release of UADialer4.0b.Only use the official releases !

1.115 saddam

Saddam Clones 2+4+7:

This Saddam clone viruses use a different crypting routine, which is 4 byte shorrter than the other.

Detection tested 10.02.1994.

Saddam Clone Laurien:

This is a very lame editorpatch from the orignal Saddam Virus.Only the string "Saddam Virus" has been changed to "Laurien Virus".

Detection and Termination tested on 07.03.93.

Saddam Virus V1.29:

How intelligent! An AMIGA user started his monitor and changed the sectorcode routine a little bit. What for an exhausting work! Play with you joystik but do not make such shit.

The virus will be found as Saddam][and the changed sectors will be found, too.

Detection and Termination tested on 01.01.1993.

1.116 pclone

PP Bomb Clone (Died&Megamon):

You remember the old Powerpacker bomb build in the release version 3.2 from the original PP ? This virus part was taken and put in the DIED and MEGAMON utilitie programms. VW offers you only the possibility to clear the file because a repairroutine is much stronger to code than to get a new version of DIED or from MEGAMON.

1.117 log

Ulog/Dlog V1.8/MsgTOP BBS Viruses:

PLEASE NOTICE THAT THE ULOG/DLOG Viruses have the same filelength are many parts of the routines are equal. I am calling this viruses "Devil" viruses because I have heard that this viruses were created by/for a sysop in the south of Germany with this name.

Comment 08.04.1993.: I met a friend of him and he told me that more than 60 files are infected with the BBS virus from the same author. The last version,which I got, was release V11. Most files will be recognized by VW as $4eb9 files.

Due to the fact that I met this person only one time, I could not get any further information.

This viruses change the "user.data" File from the /X mailbox system in the following way: The counter(value) for the account editing and the SYSOP downloads will be reduced so that most users can play with the system.
This viruses are only dangerous for sysops. They cannot destroy the information on the disk.

The MsgTOP virus will be only recognized, if it is packed with the Imploder(V1.x-V3.x).

Detection and Termination tested on 02.02.1993.

1.118 swift

Swiftware 0.98 Virus:

A very special kind of virus. It is copying the sysoppassword from an AmiExpress BBS system into a little file, which can only be read if you enter the system with 300 baud (NOCALLERSAT300). Nearly all users have at least 2400 baud(in most cases this is too slow for the BBS and you get no access) and so nearly nobody reads it. The hacker just have to call the BBS with 300 baud and he gets the sysop password.

I heard that all this programms(the virus) was created by one coder in the south of GERMANY, who runs a big BBS but I cannot give more detailed informations this time.

Comment 19.04.93.: I spoke with one of the coders of the viruses and he said that the virus is now avaible in version 16.00 .The last virus I recieved was version V11.0. He told me that more than 70 infected file exist.Lots of work to do for us...

Many $4eb9 files are trojan horses. The coder of this viruses (or his friend=an Assembler expert) use very often a special linker, which creates such files.

1.119 pstats

PStats BBS(?) Virus:

This virus damages some files, which are needed from the the PhobOS mailbox system. I heard that PhobOS is a "scene" mailbox programm, which is very wide spread in the south of Germany.
The PStats programm was written in GFABASIC. As a result I think, the author of the virus has the sourcecode of the PStats programm. Is it maybe spreaded together with the PhobOS system? This time I need your help. I have heard that this system is wide spread in the south of GERMANY.

Detection and Repairroutine tested on 19.01.1993.

1.120 amipat

AmiPatch 1.0 Virus (?):

This programm opens the file "BBS:user.data" and a file called "011011".If you start the programm, an optimization progress will be started.What becomes optimized ? I do not know. You can see a little counter on the screen counting from 0-100. But nothing special happens.For normal users not dangerous but I would like to hear from some Sysops, what happens on their BBS system.

Detection tested on 14.5.1993.

1.121 lz

LZ Linkvirus:

This virus can be(in my opinion) seen as the father of the CRIME viruses. The infected file becomes 400 bytes longer and the virus does not add a new hunk to the file. The virus implents itself at the end of the first hunk and changes 2 bytes at the real end of the hunk.

Detection and Repairroutine tested on 24.01.1993.

1.122 smbx

SmBX Virus:

This file is a trojan horse. The file (the shell-command from the SMBX mailbox system) contains an additional part, which installs the MOUNT virus. The file is 65488 bytes long.

Comment 19.02.1993.: I have heard that there exists 2 versions of this shell. Only one version should contain this virus.

1.123 telecom

Telecom Virus:

This virus works like the old Jeff viruses. It adds a "$a00a"string at first position in the startup-sequence and writes itself with the name "$a0" in the rootdir. The file is only 756 bytes long (unpacked).

This virus uses direct memoryadresses and expects RANGER RAM and Kickstart 1.3.

Some resourced parts of the virus:

```
MOVE.L  #$00C71082,$002E(A6)
MOVE.L  #$00C710B0,$00C00218.L
MOVE.L  #$00C710CA,$00C000B0.L
MOVE.L  #$00C71126,$00C03C5A.L
MOVE.L  #$00FC0AFC,$00C00218.L
```

Detection tested on 17.01.1993.

1.124 dopus

Diropus BBS Virus:

This virus becomes only dangerous, if you have a mailbox running with the AmiExpress mailbox programm. The viruses tries to work with the "bbs:user.data" and the "bbs:user.keys". It does not clear any data. Simply clear this file on your disc.

Detection and Repairroutine tested on 14.01.1993.

A little part of the virus:

```
  MOVEA.L #newuser,A0     ; new BBS user info
  MOVE.L  #MODE_OLDFILE,D2
  JSR _LVOOpen(A6)      ; User.Data will be
           ; opened
  MOVE.L  D0,handle0
  MOVE.L  handle0,D1
  MOVE.L  memblock,D2
  JSR _LVOClose(A6)
  rts

newuser DC.B  'ANDY/DECADE',0
  DC.B  '----------------30',0
  DC.B  0
  DC.W  0
L_75E DC.W  1
  DC.W  $61
  DC.B  'dding----------19',0
```

1.125 christmas

```
Christmas Linkvirus:
--------------------
```
The infected file becomes 1056 bytes longer. The virus adds a hunk to the infected file. The virus does only work, if you have Ranger memory from $C00000-$C80000 because the virus uses direct memory adresses in this range and at the end of the first 512 kbyte chip memory.

Example:

```
  cmpi.l  #$0007E07A,$00C002A4.L  ; 2 Direct memory adresses
          ; in one assembler command
  beq.b L_2
  nop
  lea L_8C(pc),a0
  lea $0007FB84.L,a2
  move.w  #$0400,d0
.loop move.b  (a0)+,(a2)+   ; The CopyLoop
  dbra  d0,.loop
  move.l  #$0000633A,$0007FE80.L
L_2:
```

The only visible text in the virus is: > Generation: 0000 <. Other textparts are not visible.

```
    DC.B  'Nu > Generation: 008 <',0
```

The repair routine was only tested with one file because I did not succeed in spreading the virus on my test disks. Does anyone has an infected file which is longer then 2000 bytes? I need now your help/support.

Detection and Repairroutine tested on 01.01.1993.

1.126 crime92

```
Crime92 Linkviruses 1+2+3:
--------------------------
```
This virus adds no hunk to the infected file. It changes the end of the first hunk and implant itself there. There are some special facts about this virus.

It uses 2 ways to infect a file:
1. possibility: "RTS" stands at the end of the first hunk. Then the viruscode starts at this point.
2. possibility: "RTS" stands not at the end of the file. Then the virus searchs for the next "RTS" in the code.

The infected file becomes 1800 bytes longer. The name "CRIME92" comes from an ASCII string found in the virus.

Works with Kickstart 3.0 and MC68040 (without cache!).

It is possible that this viruses kills the RidigDiskBlock of your harddisk (physical block 0). Make sure that you saved the block 0.

Routines tested on 5.12.92.

Comment: There is a new CRIME92 clone on the market,which uses a different cryptroutine.This virus will be recognized and completely removed,too. This virus will be only spreaded as the original Crime92.

Comment 07.07.1993.: Again a new cryptroutine was found in the virus.I am not quite sure but slowly I start thinking that someone only writes new crypting routines for this virus.

Comment 20.10.1993: I recieved a PM letter from the Z-NETZ saying, that VW us not able to detect the Crime92 virus in different files. I have checked this out but I found no bug in the routine and all tests were ok....

Comment 17.12.1993: I found several files, which could not be found by VirusWorkshop. I have fixed the problem (hopefully). Special thanks go to Soenke Freitag from the german VTC located in Hamburg.

Routines overwritten and tested 07-07-1993.

1.127 qrdl

QRDL V1.1 Linkvirus:

This virus makes an infected file 2300 bytes longer. It creates an own first hunk (like the "classic" viruses like CCCP, Smilie Cancer).

The CoolCapture is set sometimes. The following pointers will be used:
- Exec: DoIO / NewOpenLibrary
- Intuition: OpenWindow (-$CA)
- $78 (Exec)

Called this way because of a little ASCII text in the virusfile.

Sometimes the bitmap of the just inserted disk will be filled with $FFFFFF. This routine will only be started if an old filesystem disk (DOS0) will be used. The result is that the OS thinks that the disk is empty and if you write on the disk, all other files on disk became cleared.

Disassembled code:

```
  move.l  #$00000370,d0   ; 880 = Rootblock
  move.w  #$007F,d1
.loop move.l  #$FFFFFFFF,(a0)+  ; fill with -1
  dbf d1,.loop
  move.l  #$0000007F,(a3)
  move.w  #$0002,$001C(a1)  ; TD " WRITE "
  jsr -$01a8(a6)
  move.l  #$00000200,d0
  jsr -$00D2(a6)
  rts

sector: move.l  #$00000200,$0024(a1)
  mulu.w  #$0200,d0
  rts
```

It is possible that infected files will not work anymore because of a bad hunk detection routine in the virus. I cannot rescue such files at the moment.

WARNING:
The repair routine has only been tested on one file because I could not spread the virus on my disks!

Detection and termination tested on 21.11.92.

1.128 ax

AmiExpress 2.20 fake version virus:

This virus was spreaded in an archive called d-aex220.lha with the length 135400 bytes. This archive contains the file Express2.20 (194046 bytes long). This is no official AmiExpress release version! The trojan bomb writes a short file called AIBON (776 bytes) to disk and fixes the startup-sequence so that this file will be called at first. Now the desaster begins: All files on disk will be shortened to 42 bytes and the keyboard will be disabled.

Detection and termination tested on 16.09.1992.

Comment 1.10.1993: It appeared a file called DWEdit1.62, which contains an "aibon" clone.Let us call it aibon2.It is 784 bytes long. The mainfile is linked with Hunklab by UFO/CHT.VW calls this mainfile AIBON3.

1.129 timer

```
Timer_Virus with installer:
---------------------------
The  installer is 4812 bytes long and writes a new "setmap" command
to  disk.  This command is 1712 bytes long and contains a original
"Setmap" command and the real virus.  The installer "seems" to be a
simple clock with a display of free chip/fast ram.

The  written  "Setmap" command installs an $74 interrupt, opens the
ConsoleDevice  and  search for a task called "ramdrive.device".  If
this  task  is  aktive,  all  actions  will  be skipped.  If know a
special  byterow  is  transmitted  to  a BBS, on which the virus is
active,  the  user  can use all avaible shell commands and can hack
the  BBS!  The  sysop  does  not the the actions of the user.  His
keyboard is disabled.

For  gods sake this virus is really lame coded.BUT In my opinion it
is the best hacking programm at the moment!  Be careful!

Works with Kickstart 3.0 and MC68040.

          Detection and termination tested on 2.10.1992.
```

1.130 trojan3

```
Trojan 3.0 and Speed Check Viruses:
-----------------------------------
Both viruses become only dangerous, if AmiExpress is installed.  On
the  one  hand the BBS directory will be formatted and on the other
hand a file "DEMO99.lha" will be created in your download directory
which contains the "user.data".  Nothing special indeed.

Works with Kickstart 3.X and MC68040.

           Detection and Termination tested on 23.10.92.
```

1.131 snoopdos1.9

```
SnoopDos Version 1.6 Virus:
---------------------------
It is the normal Snoopdos1.5 version which contains some additional
bytes  (the  virus).  This little bastard is a trojan horse against
the AmiExpress directories.  Such tools seem to become popular.

Works with Kickstart 3.0 and MC68040.

In  the  last  days  (at  the  end  of  1992) there appeared a real
SNOOPDOS 1.7 update.  Delete all SnoopDos 1.6 releases and use only
the V1.7 release. Please notice that the SNOOPDOS 1.7 is not crash-
```

```
proof on a A4000 with Kickstart 3.X (SnoopDos 1.4 works fine !!!).

          Detection and termination tested on 24.10.1992.


      Comment 23.3.93. In the last days there appeared a Snoopdos 2.0
                       version.Use this version !


Comment 05.08.1993: It appeared a file called "sd-tv",which  claims
      to be SnoopDos 1.9.I cannot say,if this is a real update or a fake,
      but this file installs the "Butonic 4.55" virus in the memory.


    Detection tested on 05.08.1993.
```

1.132 topdog

```
TopDog Trojan Horse:
--------------------

Just  another  tool  that  kills the BBS:user.data and writes a new
user  in this file.  This time only this user can get access to the
mailbox.   The userdata is only 66 bytes long and contains only one
user.



ASCII dump:
dc.b  $0C,$EB,$EA,$E5,$EA,$A0,$F4,$E9,$E9,$E9
dc.b  $F4,$E7,$B4,$A0,$E9,$F7,$ED,$F6,$E5,$F7
dc.b  $E5,$F7,$E9,$A0,$E9,$F2,$E5,$F7,$E7,$E5
dc.b  $F7,$A0,'grewg ee  ',$0A
dc.b  ' The Three Musketeers ',$0A
dc.b  $00

          Works with Kickstart 3.0 and MC68040.

          Detection and termination tested on 02.11.1992.
```

1.133 bvirus

```
                          BootVirus:
                          ----------


1024 16BitCrew                      2048 ABC.Virus! (all 4 blocks)
1024 AEK                            1024 Aids
```

```
1024 Alien.New.Beat                 1024 AmigaDos.............08-04-92
1024 Amigafreak                     1024 AmigaMaster...........02-04-92
1024 AmigaMaster...........02-04-92 1024 Ass.Virus
1024 ASV.(Data_Crime).....02-04-92  1024 ASV_Virus............02-04-92
1024 Australian.Parasite            1024 Avirex_Timebomb
1024 BamigaSectorOne                1024 Big.Boss
1024 BlackFlash                     1024 Blade_Runner.Virus
1024 BLF-Virus                      1024 BlowJob
1024 Butonic-Bahan                  1024 Byte.Voyager.I
1024 Byte.Voyager.II                1024 ByteBandit.1
1024 ByteBandit.2                   1024 ByteBandit.3
1024 ByteWarrior.1                  1024 ByteWarrior.2
1024 Byte_Bandit_Error              1024 Cameleon
1024 CCCP.Virus.                    1024 CheaterHijacker.......08-04-92
1024 CheaterHijacker.......08-04-92 1024 Claas-Abraham.(MCA)
1024 CList                          1024 Coder.Virus
1024 CrackRight.1.01                1024 CrackRight.1.02
1024 CrackRight.1.03                1024 CrackRight.1.04
1024 Dag.Virus                      1024 Data_Crime!...........12-04-92
1024 DAT_89_Virus                   1024 Deniz.SCA.Strain
2048 Derk-MALLANDER........08-04-92 2048 Derk-Mallander........08-04-92
1024 Derk_1.0_Virus........02-04-92 1024 Destructor.Virus
1024 Digital.Emotion                1024 Dirty.Tricks
1024 Diskguard.1.0                  1024 Divina.I
1024 Divina.II                      1024 Dotty_virus
1024 Dr.Mosh1..............20-06-92 1024 Dr.Mosh2..............20-06-92
1024 DumDum_virus..........12-04-92 1024 Exterminator_2!.......15-04-92
1024 Extreme                        1024 F.A.S.T.I
1024 Fast.I.Virus                   1024 Fast.II.Virus
1024 Fastload.ByteWarrior           1024 Fast_Eddie
1024 FICA.Virus                     1024 Forpib.Virus
1024 French Kiss                    1024 Frity(Riska.Clone)
1024 Future_Disaster                1024 Gadaffi
1024 Gadaffi-Mad.II.Virus           1024 GeneStealer...........23-04-92
2048 Glasnost(File-Boot)            1024 Graffiti
1024 Gremlins                       1024 GXTeam.Virus
1024 Gyros                          1024 Hauke
1024 Hauke_ExterminatorI            1024 HCS4220.I.Virus
1024 HCS4220.II.Virus               1024 Heil_Virus............13-05-92
1024 Hilly.Virus                    1024 Hoden_V33.17
1024 ICE                            1024 Ice_Breakers.2
1024 Incognito                      1024 Inger.IQ.Virus
1024 JITR_virus                     1024 Joshua.2.1
1024 Joshua.2.2                     1024 Julie.
1024 Kauki                          1024 Kefrens.N
1024 LADS.Virus(Gremlin)            1024 LameBlame.............08-04-92
1024 Lamer Exterminator!            1024 LamerExterminatorI
1024 LamerExterminatorII.1          1024 LamerExterminatorII.1a
1024 LamerExterminatorII.1b         1024 LamerExterminatorII.1c
1024 LamerExterminatorII.2          1024 LamerExterminatorIII
1024 LamerExterminatorIV            1024 Lamer_10..............02-04-92
1024 Lamer_10..............02-04-92 1024 Lamer_Decoded.........02-04-92
1024 Lamer_Decoded.........02-04-92 1024 LameStyle.UK
1024 Loverboy..............02-04-92 1024 Loverboy..............02-04-92
1024 LSD                            1024 MAD.I
1024 LSD-II           1024 "UHR"
1024 Mad.II                         1024 Mad.III
```

```
1024 MAD.IV                          1024 Megamaster
1024 Metamorphosi_1.0......02-04-92  1024 Mexx.Virus
1024 MG.Virus.............08-04-92  1024 MG.Virus.............08-04-92
1024 Microsystems                    1024 Morbid_Angel
1024 Nasty-nasty.virus               1024 NorthStar.1
1024 NorthStar.2                     1024 NorthStar.3
1024 Obelisk                         1024 Obelisk.Crew.II
1024 Obelisk2format                  1024 Opapa
1024 Paradox.I                       1024 Paradox.II
1024 Paramount                       1024 Paratax.I
1024 Paratax.II                      1024 Paratax.III
1024 Pentagon.Virus.Slayer           1024 Pentagon.Virus.Slayer.1
1024 Pentagon.Virus.Slayer.2         1024 Phantastograph
1024 Powerbomb                       1024 Rene.Virus
1024 Revenge                         1024 RevengeBootLoader
1024 Ripper                          1024 Riska
1024 Rude.Xeroxx.2.0                 1024 Sachsen_1.............02-04-92
2048 Sachsen_3                       1024 Saddam.Hussein
1024 SCA-2001.Virus                  1024 SCA-Kefrens
1024 SCA-Paratax.Virus               1024 Sca-XCopy.Strain!
1024 SCA.1.Virus                     1024 SCA.2.Virus
1024 Scarface                        1024 Scarface.II
1024 Sendarian                       1024 SinisterSyndicate
1024 SS_Virus.............17-05-92  1024 Starfire2.............02-04-92
1024 Starlight_II..........02-04-92  1024 Starlight_Warhawk.....02-04-92
1024 Suntronic                       1024 SuperBoy.Virus
1024 Supply.Team                     1024 Switch.Off.Virus
1024 T.F.C.Revenge_2.14....02-04-92  1024 T.F.C._Revenge_1.03...02-04-92
1024 TaiPan_Chaos                    1024 TaiPan_LameBlame
1024 Target                          1024 Target.Virus
1024 Termigator.Virus                1024 The Cure!.............07-04-92
1024 The.Incognito                   1024 Timebomb
1024 TomatesGentechnicService        1024 Traveller.1.0
1024 Triplex..............22-04-92  1024 TriSector_911
1024 Turk                            1024 Twinz_Santa_Claus_Virus
1024 U.K..Lamerstyle                 1024 ULDV_8_Virus
1024 UltraFox                        1024 Vermin.Virus
1024 Viruskiller_Virus               1024 Virus_Fighter!........12-04-92
1024 Virus_Slayer_V1.0               1024 Virus_V1(Wieder_da)...02-04-92
1024 VKill.I                         1024 Vkill.II
1024 Waft                            1024 Warhawk
1024 Warsaw                          1024 Xcopy-Sca..........NEW_virus??
1024 Zaccess.I                       1024 Zaccess.II
1024 Zombi.1                         1024 Germany..............29-09-92
1024 Republikaner..........29-09-92  1024 Asylant..............29-09-92
1024 Sonjas_Virus.BB                 1024 Overkill.............14-10-92
1024 Adam Briely BB........20.10.92   1024 Cobra 21.10.92.
1024 Killed.BB                       1024 Executors
1024 Angel                           1024 Influenza
1024 Detlef           1024 Fuck.Device
1024 Disk Terminator                 1024 Suicide Machine
1024 Ingos Return                    2048 Zenker
1024 Multilator                      1024 Payday
1024 Cascade 2.1          1024 Creeping Eel
1024 USR492(SENTINEL)                1024 Wahnfried
1024 XCOPY2(a form of antivirus ?)   1024 KAKO 28.07.1993
1024 VIPHS 25.9.93.          1024 SS Virus
```

```
1024 Starcom 1                      1024 Starcom 2
1024 Starcom 3                      1024 Starcom 4
1024 Starcom 5                      1024 Starcom 6
1024 Prima Vera         1024 Irak 3
1024 Grim Heaper                    1024 ABC_Viruskiller1.0
1024 Electro Vision         1024 Exorcist (Satan)
1024 LameGame           1024 MAD 3B
1024 PVL                            1024 Microsystems CBM
1024 SCA-666                        1024 TFC 47.11
1024 SCA-KarlMarx                   1024 SCA-Karl Marx 2 (TAI)
1024 Atomix SCA Clone               1024 AIFS
1024 Tai2                           1024 Tai3
1024 SHI                            1024 VirConSet 1
1024 VirConSet 2                    1024 VirConSet 2b
2048 Zenker 2 (Ingo)                2048 Digital Dream
1024 Fred Cohen         1024 Leviathan
1024 Pal            1024 PKK
1024 Assasin            1024 DTL(MTD)
1024 TAI-4                          1024 Bad Bytes 2
1024 Bad Bytes 4                    1024 Bad Bytes 1
1024 Bad Bytes 3          1024 Bad Bytes 5
3072 Dum<II>Dum                     1024 RAF
1024 Khomeini                       1024 Datalock 1.01
1024 Baltasar                       1024 Datalock 1.02
1024 Shit(=Nuked007)                1024 Jinx
1024 Sphinx           2048 TAI-13
1024 Mount (look at Fileviruses!)   1024 Mosh 1.0
```

AIFS Bootblock Virus:

This virus only patches the DOIO vector in the execlibrary. It is not resident and uses memory at $7xxxx (without alloc.) for it's code.

It should work properly on all Kickstarts and processors.

The virus never sends a message or similar stuff and it is remarkable that it only needs the first block.

Detection tested on 27.10.1993.

Assassin Bootblockvirus:

Simple SCA Clone (better play with your joystick !).

Only the text has changed.

```
  ' Something NEW has happened      '
  ' Your COMPUTER are   !!!'
  'INFECTED BY THE    '
  'ASSASSIN VIRUS    '
  'HA-HA-HA-HA-HA'
  'THANX TO ME YOUR      '
  'BOOTBLOCK IS SMASHED!!Ün'
  '  DTL!DTL!DTL!DTL!DTL!DTL!DTL!'
```

Bad Bytes inc 2 Bootblockvirus:

A Lame Game clone (what a hard work: Stop doing this and produce instead USEFULL utilities and programms, which make the AMIGA more powerfull!). Only the texts have been edited.

To produce viruses is never a good thing.

```
  'Software Failure - We hate you! You are g'
  'oing to DIE!',0
  'Anti-Harald Paulsen and Twins virus done '
  'by TTS and Nighthawk  of BadBytesInc., U'
  'FO and Zax of Hollywood Team! Stay cool,'
  ' be nofool - coz',27,' the DataKuKluxKlan is '
  'getting bigger! TTS signing...'
```

Bad Bytes inc 2 Bootblockvirus:

Simple SCA Clone (better play with your joystick !). Only the text has changed. To the "hero", who "produced" thus stuff: In my opiniion YOU are the lamer !

```
  ' Parasite of Bad Bytes Inc presedting'
  ' AntiLamer virus! '
  ' Spread the virus to'
  ' every fuckin hated LAMERS! Im '
  ' fed up with 'em!'
  ' The only way for total'
  ' perfection...BBI!!! '
  ' BBI!BBI!BBI!BBI!BBI!BBI!BBI!'
```

Bad Bytes 1 Virus:

This is a simple Warhawk Clone. Only the texts have been changed.

```
'TTS VIRUS IS ON THIS LAMERS WORK !!!!! '
' AND DON',27,'T THINK ABOUT KILLING ME BECAUSE'
' I KILLED THE VIRUS-KILLER !!!!! TTS!TT'
'S!TTS!TTS!TTS!'
```

Possible other name: TTS Virus

Bad Bytes 3 Virus:

This is a simple Backflash Clone. Only the texts have been changed.

```
'Every 13th copy - you will always get the'
' feeling of being hated! BBI rules!!'
' DIE IN HELL!!!! '
'Done by Bad Bytes Inc - Thanx to BlackFl'
'ash for the code!       '
```

Bad Bytes 5 Virus:

This is a simple Coder Clone. Only the texts have been changed.

```
'Your computer is stoned! Legalize mariuhana!'
'Parasite of BBI! '
```

Baltasar Bootblockvirus:

This is a simple SCA-II Clone. Only the visible texts has been changed.

```
'graphics.library',0
'dos.library',0
'Hello lamer ! you have a virus   '
'Use pampers not amiga  '
'  its better !  ...PP'
'You are so lame shame you      n2Z'
' Christmas  , '
'Baltasar-Virus 1994   '
```

Detection tested on 22.1.1994.

Cobra bootblock virus:

Does not work with Kickstart 2.X. A virus which is not resident. It installs an interruptroutine to $94(execbase). Should not work with RAM Kickstarts.

The virus itself causes an ENFORCER hit when testing for a special byterow at the end of the chipram. I reassembled this routine and use it in VW, too.That is the reason for the ENFORCER hit at the begin.

Disk Terminator bootblock virus:

This virus is a simple SCA 1 virus clone.The "author" was so tricky to overtake the original "CHW!" string in the virus.Only the ASCII-texts are changed.Stay away and play with your joysticks instead of making such lame clones....

Datalock 1.01 and Datalock 1.02 viruses :

Both viruses are VERY agressive and contain very powerfull destructionroutines.

Both viruses use direct adress accessing to $7fXXX and do not need the "trackdisk.device". I have killed two of my harddiscs (one including my WHOLE VirusWorkshop sources) but I had luckily made a backup 4 days ago. Phew.

DoIo always at $7f858
Kicktag always at $7fade

Very tricky new decoding routine, which will be changed before. Nice... The viruses killed my RDB on a SCSI-II harddisc and killed some sectors by overwriting it with some stuff.

The bootblock and another 1024 bytes (V1.02) will be written. At V1.02 there will be 4 KB written to the bootblock. A very wide destruction.

The V1.01 has an additional destruction routine, which kills the sectors 890-893. At sector 880 there is on normal DD discs the ROOTBLOCK (directory). It's therefore possible that very important directory blocks will be killed by this virus.

The V1.02 has a different destruction routine. 4 blocks, which

will calculated using a random routine will be killed by over-
writing some memorygarbage.

At the end of the virus, you can read (decrypted):

"Datalock 1.1 (C) ‘94 ALL (?) code by Deathcode."

Detection tested on 08.02.1994.

Digital Dream Bootblockvirus:

This virus loads the original bootblock and puts it into the two sectors directly behind the bootblock (sector 2&3). All ! datas in this sectors are destroyed and cannot be repaired ! The virus codes itself with a little eor routine and patches
-030 (EXEC)
-408 (EXEC).

The virus was probably programmed by Max of Starlight, who programmed a lot of viruses. Isn‘t is possible to catch such a person ? I cannot understand it. This guy programmed more than 5 viruses !

Detection tested on 28.11.1993.

DTL Bootblockvirus:

A simple MICROSYSTEMS clone, which only contains some new texts. Nothing special about it.

```
’DTL!DTL ’
’YOUR DISK IS INFECTED BY ’
’ NEW VIRUS MADE IN      ’
’ N O R W A Y         ’
```

DumIIDum Bootblockvirus:

Uses blocks 0-5 and works with Kickstart 3.0 and 2.04. The virusmaincode is located in block 2 and 3. The first both blocks only contain a simple loaderroutine (trackdisk).

All data in the blocks 2-5 will be destoyed (sorry no rescue possible). If a file was in this blocks, it cannot be used anymore.

Changed vectors:

Cool, Doio, DosRead, DosOpen, DosWrite.

If a counter reached $50, a destroyroutine will be started and e.g. the rootblock will be changed.

In the 4.virusblock you can read 2 time "dos.library" and "DUM<II>DUM".

The virus will be installed $1800bytes under the maxlocmem area !

Detection tested on

19.12.1993.

Special thanks must go to Ingo Schmidt for supporting this virus.

Eleni Bootblockvirus:

Length: 1024 bytes

Patched vectors:-Coolcapture (always patched to $7f296)
-SumKickData (always patched to $7f32a)
-DoIO (always patched to $7f2da)
The original value of the DoIO vector will be stored at $7fa02.

The original bootblock will be stored at sector 1738 and will be loaded from the virus and the virus jumps directly in the original bootcode. The virus contains a write routine, which writes the text "ELENI" (via DOIO). The writeroutine uses not the dos.library, pure DOIO action !

At the start of the virus, the viruscode will be copied to $7f144 (without allocating the memory before). On system with low memory, it can happen very often, that the system crashes. The viruses uses the adress $60000 as a flag for the textwriteroutine. The area $70000 and higher will be used from the virus without allocating the memory.

The text "*ELENI*" is visible at the end of the file. In the middle you can read something about "Version 1.6".

If the virus has read several times from sector 1738 and a counter (hardware) reached the value 1 , it will overtake the control of the drive(s) and manipulates CIA and the drivecontrol register.

If the counter reached the value 4, the writeroutine for the "*ELENI*" string will be started. The counter is located at $dc002d. I don't know, what is this for a register and I could not find out, if it is always initialized with the same value. On my AMIGA it contained the byte $f2.

If a DoIO read access was caught, the infection routine will be started. If a DoIO write access was caught, the writeroutine will be started. In the NewDoIO routine, the virus handle with the CIA-A registers (powersupply ticks and interrupt control).

Due to no checkroutine for Trdevice, the virus can destroy (in my opinion) the RDB.

The infection routine reads the original bootblock to $70000, tests it and at success, the virus writes the original bootblock to the sector 1738 and copies itself to sector 0. The bootblock at sector 1738 will be saved non crypted.

Detection in BB & memory tested
18.05.1994.

Jinx Bootblockvirus:

Patches Kickchecksum,KickTagPointer,KickSumData,TD BeginIO, Exec VBI.

Works with Kickstart 2.0

This is a very tricky bootblockvirus, which looks for me like a Lamer Exterminator virus but more tricky (Hi Soenke).

VirusWorkshop can remove ALL changed vectors and your system should work again.

If the bootblockvirus is on your disk and you boot with this writeprotected disc, a requester appears, which says, that your the disc is a non DOS disc. If you remove the write-protection everything is allright again.

The read access will be patched and the bootcode will be hidden. Little bug: Even if you read the directory via TD device, the original bootblock will be shown.

The bootblock will be crypted randomly and in the end of the decoded bootblock you can see the text:

"JINX....trackdisk.device....".

Detection tested on 24.2.1994.

RAF Bootblockvirus:

Simple WarHawk clone. Only the texts have been changed.

Detection tested on 28.12.1993.

Khomeini Bootblockvirus:

Simple MAD clone. Only the texts have been changed.

Detection tested on 28.12.1993.

Leviathan Bootblockvirus:
---

look in the Linkvirus section...

Mosh 1.0 Bootblock virus:

(Caution: There are 2 viruses with the name Dr.Mosh in
circulation, this are different ones!!!)

Patched vectors: DOIO, KickTag, -$58(dos)

Doio is alway pointing at $7f964 and the Kicktag pointer is
also always pointing to $7fbde.

This virus works only under Kickstart 2.0 and higher, caused
by BCPL.

This virus copies its code to $7f800 (without allocation) and
overwrites the original bootblock. Caused by a missing checking
routine for "trackdisk.." the virus is able to destroy to RDB
of your HD, too. After 5 infections the sector 880 will be
trashed (exactly this block). At normal DD disks, this is the
location for the rootblock. As a result your disk is not
useable anymore. Try to use DiskSalf etc. to recover your data.
In the same process the block $2800/$200 will be trashed.
A file, which is located in this block, is not repairable
anymore. Sorry.

Caution: Due to the missing memoryallocation, it can happen,
that the patched DOIO routine will be overwritten and the
system crashes.

Example: VirusWorkshop crashed on an A500+ based on this
reason.

The virus contains some texts at the end, which are crypted:

'dos.library'
'intuition.library'
'HEY ! I'M MOSH version 1.0'
'FIRST SILESIAN VIRUS' <- other possible Name !?!
'F2'
'Written by the best M.G.F'
'<x2Special greetings to: C.I.A. and K.GARLEJ'
'FFd<Biiig fucking to: KAZIO STEINHOFF and'
' D.K.BIT'
'AND now SERIOUS I LOVE BEATA B my BEST girl'
'Friend have you AIDS ? if have it fiine'
'i olso have one'

Detection tested 24.04.1994.

Special thanks to MOK! for sending this virus !

(This doc sounds like the VT2.63 doc, but it's not copied. This
text was written before VT2.63 was released.)

PAL Bootblockvirus:

A simple SCA clone. Only the texts have been changed.

```
  ' Peace Atomic League is coming to'
  ' the amiga users today !'
  ' we like you     ...'
  ' esert not to PC community ,   '
  ' the amigas    '
  ' are the best compis   '
  ' R.I.P. poor PC  !!!   '
  ' !PAL!PAL!PAL!PAL!PAL!PAL!PAL!'
```

PKK Bootblockvirus:

A simple SCA clone. Only the texts have been changed.

```
  ' Death for the killer of Moelln !!'
  ' rown Power lives today'
  ' Nothing is better..PP'
  ' Germans are infected with the  n2Z'
  ' NAZI-VIRUS !!!'
  ' Muslims take your life'
  ' in your own hands  !!!Ün'
  ' !PKK!PKK!PKK!PKK!PKK!PKK!PKK!'
```

Sphinx Bootblockvirus:

A simple SCA clone. Only the visible texts have been changed.
Please notice, that this lame clone comes not out of the rows
from TRSi.

```
graphics.library
dos.library
Cave virus, use this AntiVirus ..
Do not delete this boot
it is your cure ...
kill all known virus  use it for
protection !!!
Sphinx from TRSI     !
```

Detection tested from 13.03.1994.

TAI-4 Bootblockvirus:

A LameGame clone. I hate it to include all this simple clones. Come on, better play with your joystick instead of producing such viruses ! You don't help the AMIGA to get a better face to the public !

' Have a nice day Sorry Look for T.A.I.'
' the best..'

TAI-13 Bootblockvirus:

A simple Glasnost Clone. Only the visible texts have been changed.

Detection retested 13.03.1994.

VirusConSet 1 bootblockvirus:

This virus is quite lame coded. It patches the Coolcapture and the DOIO vector from EXEC. The memory from $7f00-$7f4XX will be used without allocation and it will be written to the following adresses: $c3af7e and $310.

Detection tested on
4.11.1993.

The SHI bootblockvirus:

This virus uses memory at $7ec00 and patches the DOIO and the Coolcapture vector from EXEC.

The memory will be not allocated !!! This virus should work with all kind of Kickstarts and prozessors....

At the bottom of the bootblock, you can read the following text:

```
'Call Canada great BBS! Is the best for v'
'irusprogrammers. We like Viri. Call VXQ-'
'BBS (416) 324 9439 .Send new viri , welc'
'ome to BBS  :'
' SHI!SHI!SHI!S'
```

Detection tested on 04.11.1993.

Comment 05.11.1993.:

This is an Australien Parasite Clone ....

SCA Clone Atomix:

Again a new SCA Clone. You may think why I write about this virus ? Simply, because I hate it to see every week new clones from the SCA virus. Come on guys ! You should better play with your Amiga instead of creating such bullshit.Every viruskiller should detect this ones. I am bored of it.

Text at the bottom of the bootblock:

```
This is the Warkill Virus Anti
done in 1993 by Atomix of NASA !!!!
Greetings go to Peacemakers:
BBS TEAM
Nuclear Desaster
Silvermoon BBS
```

Detection tested on 24.10.1993.

P.S. VirusWorkshop will only say: " SCA Clone (HAHAHHA) ".....

SCA KarlMarx Bootblockviruses:

This viruses are both SCA clones, which are changed only in 2 bytes. VirusWorkshop will only say: "SCA Clone (HAHHAHA)".

Detection tested on 23.10.1993.

Kako Virus:

This is a simple EXTREME clone.
This virus cannot reset clearly on a Kickstart 2.++ AMIGA because it uses direct memory jmp's.
The virus is able to kill the data on your disk.This routine does not work on faster Turboboards because of the TIMING problems.

Detection tested on 28.07.1993.

Payday Antivirus:

This is in generall an ANTIVIRUS but too old and useless under OS 2.x .So VW recognizes it as a virus.

XCOPY2 Virus:

I had problems to decide if this is a virus or not,but finally I say: This is not a real virus (because it does not spread it's own code) but it destroys other bootblocks by writing a normal bblock. This process can only be started by pressing the mousebuttons.

Another point is that the programm patches the DOIO vector and the Kicktagpointer.Everything very virus alike.

Let's call it a Utilitiebootblock,which should be always cleared.

```
MOVEM.L D0-A6,-(A7)
MOVEA.L 4.W,A6
MOVE.L  #$00000200,D0
MOVE.L  #MEMF_CLEAR|MEMF_CHIP|MEMF_PUBLIC,D1
JSR _LVOAllocMem(A6)
LEA Mempointer(PC),A0
MOVE.L  D0,(A0)
```

```
  MOVEA.L D0,A0
  MOVEA.L D0,A1
  MOVEA.L D0,A5
  ADDA.L  #$00000064,A5
  LEA L_8(PC),A4
  MOVE.W  #$01FF,D7
L_4A  MOVE.B  (A4)+,(A5)+
  DBRA  D7,L_4A
  ADDI.L  #$00000026,D0
  MOVE.L  D0,$000E(A1)
  MOVE.W  #$4AFC,8(A0)
  ADDQ.W  #8,A1
  MOVE.L  A1,(A0)
  ADDA.L  #$000000DE,A1
  MOVEM.L (A7)+,D0-A6

  ....
  LEA L_BC(PC),A0
  LEA L_136(PC),A1
  MOVEM.L (A7)+,D0-A6
  RTS
```

Detection tested on 07.07.93.

USR492=Sentinel Virus:

I recieved this virus under the name "USR492" but after some calls I correct me and call this virus "SENTINEL".It tests for the LW "SENT".The virus copies itself to $7f400 (without allocating the memory) and jumps in $7f49c.

The $2e(EXECBASE) and the DOIO Vectors are changed.The virus only works with the normal "DOS0"bootblock.If there is a FFS bootblock, the new bootblock will be not written.

Detection tested on 02.07.1993.

Zenker Bootblock Virus:

This virus is a new type of virus. It only uses a loaderroutine in the ordinary bootsectors and all the virusparts are put in the sec. from 896-898. The original BB will be written to the sectors 898-900. That means that the sectordata 896-900 will be destroyed 100% and cannot be fixed. What happens, if the headerblocks and other structures are in this sectors ? You can forget this files. VW offers you the possibility to rewrite the BB from 898 to sector 0. In some cases this might work(for games with bootloaders ect.) but in the most cases your disc is damaged and not useable anymore.

It can happen that the RDB block from your harddisc becomes over-

written. In this case it is too late. You can only restore the backup of your RDB sectors (you surely have one!) and hope that the information on sector 896-900 were not too important.

The virus uses some memory without allocating it.It uses $7f500 without allocating this memory space.

Detection tested on 23.3.93.
Block-0 tested on 23.3.93.

The Virus tries to look like a normal bootblockloader with the string "COMMODORE Bootblockloader ....)....

Comment 28.11.1993: It appeared a Zenker Clone called INGO. Only the visible texts were changed.
In the bootblock you can read now:

"Bootloader by Ingo(16 Feb.1993)
.....FUCKFUCKFUCK "

In the block 897 you can read:

"Now I am the 29 Generation"

In Block 989 you can read at 0-11 "== INGO!! ==".

Detection tested on 28.11.93.
Block-0 tested on 28.11.93.

Multilator Virus:

This virus only works with FAKE fastram and Kickstart 1.2. Nothing more to say about it.

Detection tested on 08.07.1993.

Overkill bootblock virus:

This virus works with all Kickstarts and even on turboboards. It writes the original bootblock to the block 2-3 and destroys in this way some possible data on this tracks.

Changed vectors: DoIO, CoolCapture, ColdCapture (always with the

same adresses).

Warning: This virus clears sometimes sectors on devices. Danger! You can loose your RigidDiskBlock of your HD or the bootsectors because of some bugs in the DoIO routines(no security check for the trackdisk device).

The "UHR" Bootblock virus:

This virus does not work with Kickstart 2.04 and higher.It checks the highest byte in the $6c vector for $fc.This is only a possible value for Kickstart 1.x .If the value was not found,a normal bootblock will be executed.

The virus is crypted on disc with a simple "EOR" loop.It patches the DOIO,the LEVEL3Interrupt and the Coolcapture vectors.

The "new" thing in this virus is,that it copies itself to a special adress,which will be calculated with the following rout.:

```
    LEA $0007F800.L,A1
    TST.L $004E(A6)
    BEQ.B Abs_Copy
    MOVEA.L $004E(A6),A1
    LEA -$0800(A1),A1
Abs_Copy  MOVE.L  A1,-(A7)
    MOVE.W  #$0398,D0
Copy_Loop MOVE.B  (A0)+,(A1)+
    DBRA  D0,Copy_Loop
```

This means that no adress exists,where this virus can be always found.The patched DOIO vector does not ask for the TRACKDISK-device.

The following adresses will be changed in the next parts of the virus:

$00BFE601.L
$00BFE701.L
$00D80002.L
$00BFEE01.L

The $d80002.L register is (I heard it only) an old register for the internal clock.The bootblock will be crypted everytime new (depending on one special register).

Detection tested on 14.6.1993.

If you have a virus which will not be detected by VirusWorkshop then please write me. You will get as fast as possible a new version which recognises the virus. Thanks a lot!

Markus Schmall
Von Gravemeyerweg 25
30539 Hannover-Bemerode
Germany

Tel.:0511 / 514944

1.134 cruncher

The following crunchers will be recognized:

(even some more but not listed)

PowerPacker 2.x	PowerPacker 3.0
Imploder 1.0-3.1	Imploder 4.0
Titanics Cruncher 1.1	Titanics Cruncher 1.2
TNM Cruncher 1.1	PowerPacker 4.0
PowerPacker 4.1	PowerPacker 4.2
PowerPacker 4.3b	PP 4.0 Library
DragPack 1.0	DragPack 2.52
Master Cruncher 3.0 R	PackIt 1.0
TurboSqueezer 8.0	Lib Imploded
CrunchMania 1.4 R/N	CrunchMania 1.4 R/S
CrunchMania 1.6	CrunchMania 1.8
Crunch O Matic 1.0 E	PP 3.0 Overlayed
PP 3.0 Password	PP 4.0 Overlayed
PP 4.0 Overlay/Lib	PP 4.0 Password
PP 4.0 Password/Lib	Black&Decker 2.0
ByteKiller 2.0	ByteKiller 3.0
CrunchMania 1.4 A/N	High Pressure Cruncher
RSI Packer 1.4	Master Cruncher 3.0 A
Time Cruncher 1.7-2.2	TFA Cruncher 1.54
Turtle Smasher 1.3	Turtle Smasher 2.00
TetraPack 2.1	TetraPack 2.1 Pro
TetraPack 2.2	TetraPack 2.2 Pro
DefJam Cruncher 3.2	DefJam Cruncher 3.2 Pro
Defjam Cruncher 3.5 & 3.6	Compacker 4.2
Crunch Master 1.0	HQC Cruncher 2.0
MaxPacker 1.2	Mega Cruncher R

```
ReloKit 1.0       StoneCracker 2.70
StoneCracker 2.70 K     StoneCracker 2.99
StoneCracker 3.00     StoneCracker 3.10
Super Cruncher 2.7      Syncro Packer 4.6
TryIt 1.01        Ultimate Cruncher 1.16
TSBs Ultimate Packer 1.1b   Imploder 1.0-3.1 P
Imploder 4.0        LHA archives-1.42e
DMS files  -1.12      ZOOM files -5.4
Powerpacker Data Files           Skid Row Warper 2.0
      Skid Row Warper 1.1     RAP!TOP!COP! V1.0-1.2
Crystal Warper 2.0ß     Phil Douglas Warper 2.0ß
      N.O.M.A.D. Warper 1.3                  N.O.M.A.D. Warper 5.1e
```

The power results mainly from the use of the faboulus "xfdmaster.Library" by Georg Hoermann. This fine piece of code is public domain. In the VirusWorkshop package is version 33.20 of the library included. Newer versions of the library bring you even more recognized crunchers.

This library is able to decrunch most above listed filetypes. I have included a function called "Decrunch" in the PREFERENCES menu to able/disable the decrunchroutines. If you have activatet this function every relocatible crunched file will be decrunched. Please note that decrunching will take some moments on slow 68000 AMIGAs .

Special note from Georg about the library and the library package:

This library and all documentation/include files are Freeware! Use it in your programs, spread it around the world, do whatever you want with it, but don't change or sell anything without asking him before. For bug reports/suggestions contact him at:

Georg Hoermann
Am Lahnewiesgraben 19
8100 Garmisch-Partenkirchen
GERMANY

If you use the decrunch.library in your own programs, please state in your documentation that it is written by Georg.

If anybody has the time and knowledge to write some 'C', Modula or whatever include files, send them to him and he'll release them together with the assembly include.

Special fileformats, which will be recognized:

TXT2Exe by Oliver Wagner:

This is a little tool, which creates from a normal textfile an executable file, which can be started from CLI/SHELL.

N.O.M.A.D. Warper 5.1e:

This is a diskcompressing utilitie like DMS.It is a lot slower but it WARPS the tracks.If necessary, the tracks will be nibbled. I think it is a tool from crackers but it appeared on some german BBS and so I decided to include it.

There is a write included in this archiv...

Testlongwords: "Warp v1.1" Position: 0-7

N.O.M.A.D. Warper 1.3:

This is a diskcompressing utilitie like DMS.It is a lot slower but it WARPS the tracks.If necessary, the tracks will be nibbled. I think it is a tool from crackers but it appeared on some german BBS and so I decided to include it.

Testlongwords: "NOMADWAR" Position: 0-7

Prorunner V1.0 & V2.00:

Prorunner is a utilitie, which converts the original Protracker format in an own format, which can be replayed a lot faster. I had only 1 checkmark (the .SNT/SNT!) and therefore it can come to some misunderstandings.

Protracker:

All normal modules from Protracker 1.1-3.00 should be detected. The support for the new fileformat from the Cryptoburners tracker (Protracker 3.0xb) will come, if I see the first module done with this tool.

Xlink 3.00:

This is a utilitie which enables the user to link 2 executable file together. A very fine tool. But imagine the following situation: One of the linked files contain a virus!

VirusWorkshop asks you if you want to delete Xlink files. If you want to be clever then do the following things:
1. Copy the XLINK file to a seperate disk and start the file. Then start the VirusWorkshop and look at the vectors. If the memory was clear before starting the Xlink file and now it is incorrect then you should clear the file because there could be a virus in it.

Such utilities should always contain a viruschecker, which checks the choosen files for linkviruses.

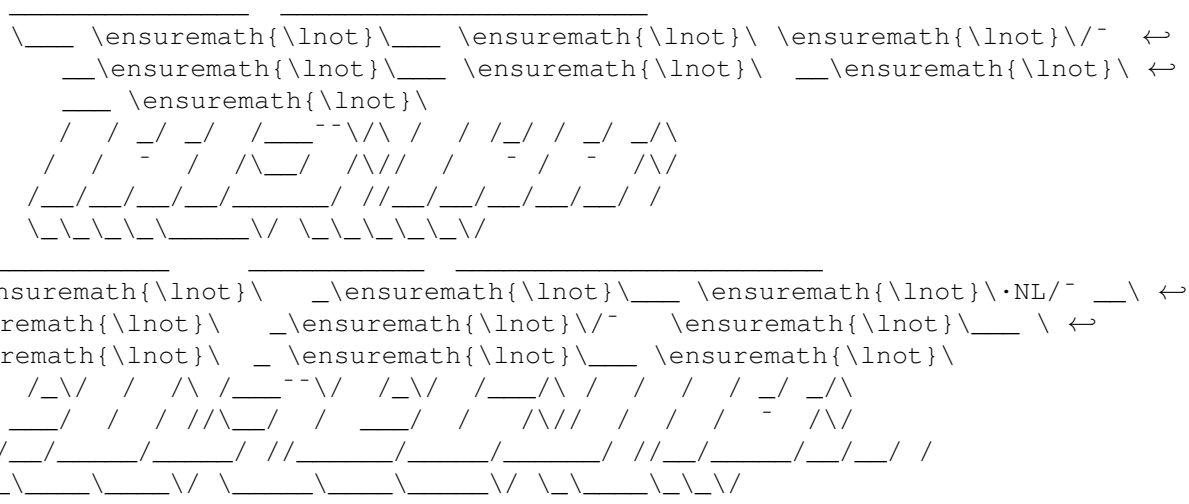
Comment 22.3.93.: The Dial2.8g Virus is a Xlink 3.00 file !!!

signed,
Markus Schmall

(23.03.1993)

1.135 history

History document for Virus Workshop 3.6



VirusWorkshop Version 3.5 final:

> VirusWorkshop 3.5 is only for Kickstart 2.04 and higher.

> It is not allowed to put VirusWorkshop on S.H.I. discs ! <
> There are two exceptions: Jim and Becky Maciorowski (ex. SHI USA) <
> and Lars Kristensen and Jan Bo Andersen (SHI Center in Denmark)

Hiermit verbiete ich, Markus Schmall, Mallander Computersoftware
VirusWorkshop zu vertreiben !!!!

Don‘t try to (de)crunch VirusWorkshop. It‘s decrunchprotected and
is already crunched !

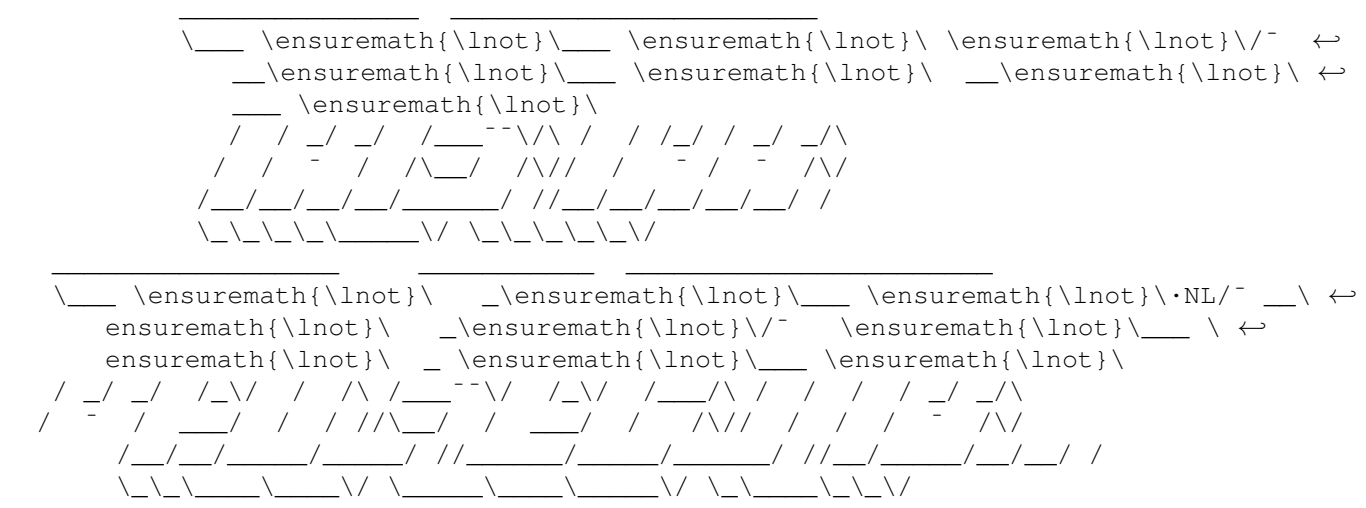
- Added LHA Checker 1.1 BBS Trojan virus. Thanks must go again to
VirDown! for this great support !
- Added MST Vec formatter viruses (2 pieces).
- Fixed Infiltrator Virus recognition routine to work together with
$3f1 and $3e8 hunks. Now it should work ! Thanks Ingo Schmidt for
the hints !
- Changed intern packerformat from ScrunchPro to CrunchMania 1.91r.
- Added TAI-13 and Sphinx Bootblock viruses. Thanks must go again
to VirDown! for his everlasting support.
- Optimized the Pref-Editor a lot ! Thanks must go to Vasco Steinmetz
for all the ideas/hints/tips...
- Added Picasso-2 support for the 640*480 mode and the 800*600 mode
(starting with the Picasso Monitorfile 2.14).
- Added recognition code for the Menems Revenge2 Virus. Thanks must
go to Jan Bo Andersen (SHI Denmark) for this virus !
- Wrote repairroutines for Menems Revenge 1+2. I forgot to do that
in the past. Sorry.
- Added Dhunk utility ! Added recognition code for the 3e8,3f0 and 3f1
hunks ! PLEASE read the manual (dhunk.guide). It‘s very important !
- Added recognition code for the ConMan DIR Virus. Thanks must go again
to Ingo Schmidt for sending me this virus.
- Added Mount ("Gremlins") Virus. Thanks must go to J.Walker/TRSi
for the support. Thanks again ! Read the manual concerning this virus !

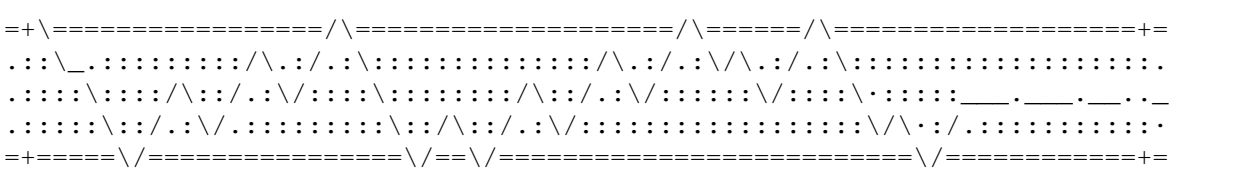
So many things were planned for this new release....
But you know all the problems, which can slow down nearly every project:
- new girlfriend
- a very good holiday job
- and a lot of cool parties...

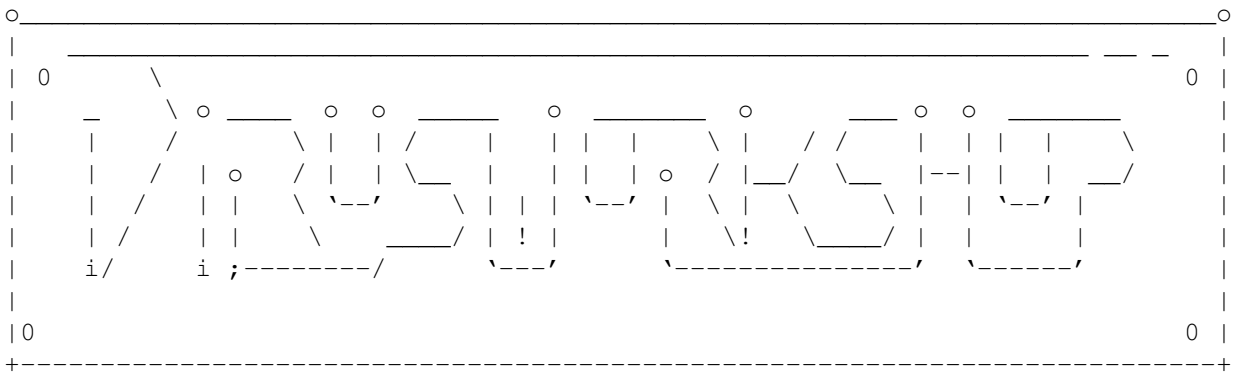
I have not forgotten all your wishes. They will be realized as soon as
the things are going normal again.

Markus

Tristar & Red Sector inc.‘94 - Back to the roots







```
 VirusWorkshop Version 3.4 final:
 --------------------------------

 > VirusWorkshop 3.4 is only for Kickstart 2.04 and higher.


 > It is not allowed to put VirusWorkshop on S.H.I. discs ! <
 > There are two exceptions: Jim and Betty Maciorowski (ex. SHI USA) <
 > and Lars Kristensen and Jan Bo Andersen ( SHI Center in Denmark )


   If you want to contact me via modem, then you should call

   BoardName: Chaos Line
```

(official VirusWorkshop Support BBS !)

USR Dual Standard 16.8 Modem

Tel.: ++49[0]572374340

Username: VW
Password: VW

The VirusWorkshop conference includes all important information for you. My user handle is "Flake/TRSI". Every user of a high-speed modem gets a very good connect (14400+).

If you want to know some other BBS numbers, read the contact chapter !

ToolManager Users please read the STARTERPROBLEMS Guide file !

VirusWorkshop NOW supports the new XFDMaster Library by Georg Hoermann. XFDMaster is the new highly optimized decrunch library !

AAARG: I got at the end of febuary (22.2) a call that a german PD-distributor sells VW and other viruskillers for 29 DM. This is not the right way. The firma sells the program at a not acceptable price. The sold version version is V2.2, which is VERY old. If you see an anouncement in big german AMIGA magazines saying : Direct out of the hackerscene etc... and the sellersname starts with Mall..... you think on the right person.

Nocheinmal in deutscher Sprache und klar verstaendlich:

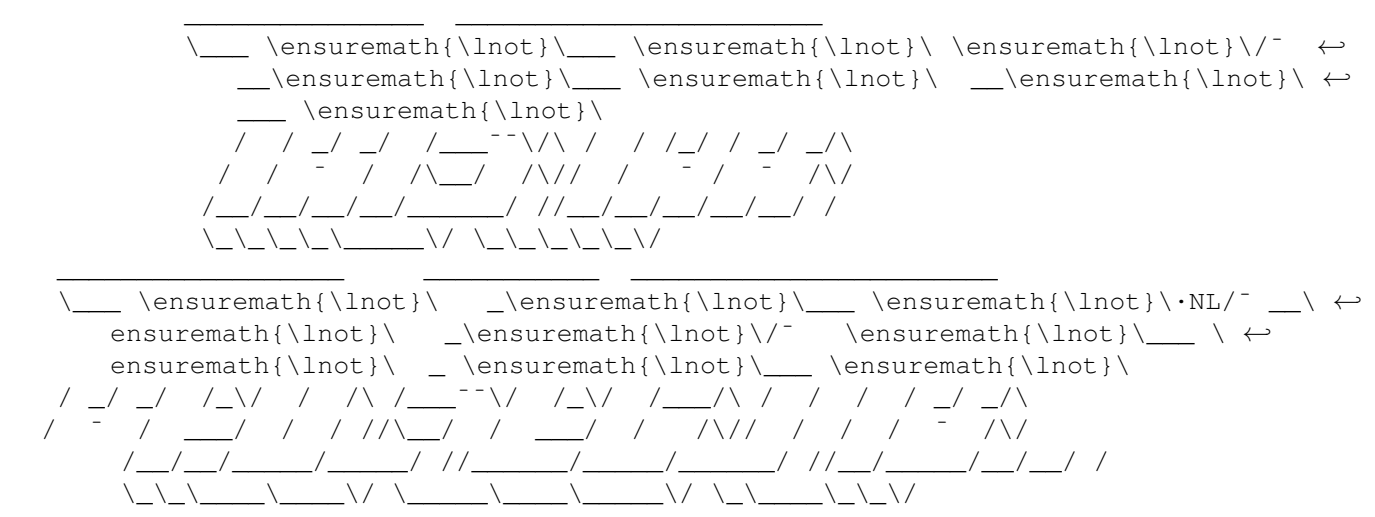
Hiermit verbiete ich, Markus Schmall, Mallander Computersoftware VirusWorkshop zu vertreiben !!!!

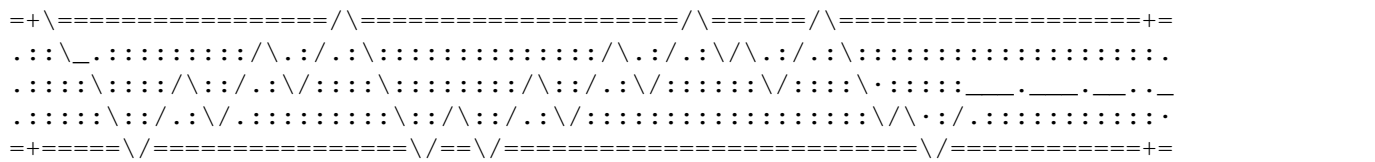
Don‘t try to (de)crunch VirusWorkshop. It‘s decrunchprotected and is already crunched !

- Optimized the intern codes: VirusWorkshop is now about 90 KB shorter ! This was caused by a totally new rewritten directory-scanroutine. Special thanks have to go to Olaf "Olsen" Barthel for some ideas for doing this job in assembler(recursive!).
- Added recognition code for DAG Installer, Datalock 1.01, Datalock 1.02 viruses. Special thanks go to Krzysztof Klos for sending this pieces.
- Added Saddam 2, Saddam 4, Saddam 7 (Saddam clones with new crypt routines !). Special thanks go again to Krzysztof Klos for sending this viruses !
- Added memorykillroutine for BURN2 ! Fixed routine for BURN1 !
- Wrote repairroutine for BURN2 virus !
- Fixed some problems with multiple links.
- Added ToolsDaemon 2.2 Fake virus ! Special thanks go to VirDown and Ingo Schmidt for supplying me with this virus !!!
- Added Mongo09.exe BBS trojan horse !
- Added Mongo05.exe BBS trojan horse !
- Added recognition code for SHIT! (=Nuked007) virus. Thanks must go again to Krzysztof Klos !

- Wrote memorycheckroutine for ToolsDaemon 2.2 fake virus !
- Added recognition code for Segtracker 37.55 by M.Sinz...
- Added recognition code for TAI-11 (Compuphazygote Clone). Thanks must go to VirDown for sending me this virus !
- Added some more german strings to the locale file !
- Added recognition code for Syndicate Coder Patcher !
- Added recognition code for the Digital Dream Installer. Thanks must go to Jan Bo Andersen for sending this virus !
- Added support for the new XfDMaster Library by Georg Hoermann. Thanks again Georg for the fast supply with the AUTODOCS...
- Added JINX bootblock virus ! Thanks must go to Soenke Freytag for sending this virus.
- Added Tripple A Enhancer Bomb. Thanks again VirDown for the really great support.
- Opimized some routines, which could cause problems, if you have activated the DECRUNCH option. Now it should be very safe (Thanks again for the GREAT xfdmaster.library to Georg Hoermann)
- Changed VirusWorkshop status to ShareWare !
- Fixed some routines again and changed the GUI a little bit (Vasco, VW3.4 WILL have more more userstyleguide-like GUI)
- Checked the Loader trojan, which is a simple clone from the Modem-check virus. VW recognizes it as the ModemCheck virus. Thanks again Adrian Guelik for this virus.
- Added a new reqtools library and a new FileID library.
- Fixed some intuition routines...
- Added installer of Datalock ! Thanks again to Krzystof Klos !
- Fixed some bugs !

Tristar & Red Sector inc.'94 - Back to the roots





What to expect in the future for VirusWorkshop ?

Maybe a special bbs checker based on the dms.device will be included in VirusWorkshop. The problem is that in the public spread DMS 2.0 version, one of the most needed commands crashes on my system and I cannot test it. I have written to M.Pendec and hope to able to test it soon....

PICASSO 2 SUPPORT :

I now got the new monitor file for this amazing gfxcard and I am working very strong on the real PICASSO support. Planned supported resolutions are: 640*480 and 800*600. This should be enough for the cardusers.

DON'T TRY TO CHANGE TO VIRUSWORKSHOP MAINFILE. IT'S ALREADY PACKED AND YOU CANNOT DEPACK IT. THE FILE BECOMES NOT SHORTER, IF YOU CRUNCH IT AGAIN !!!!

News in VirusWorkshop 3.2:

- Added support for the "new" explode library.
- Added a little preferences editor. The structure of the prefs-file has been changed. Read this part in the guidefile.
- Added Fileghost Linkvirusrecognition & repaircode and fixed the recognition code for the installer.
- Added new ReqTools Library (V2.2)
- Completely rewrote the Drivechange function. Special thanks must go to Vasco Steinmetz for his really great help with REQTOOLS. Thanks again Vasco !!!
- Fixed some internal stuff. Special thanks must go to Agent Orange/MST for the hints (intuition.library).
- Optimized the code in several parts.
- Added Stockmarket virus (?)
- Added an AmiExpress Version, which contains several backdoors...
- Added BURN Virus Virus (READ Document!)
- Added VirusChecker 6.4 (Compuphazygote Fake) Virus (Thanks KARAM!)
- Fixed CCCP Recognition code (Thanks Martin !)
- Added Baltasar BB Virus (SCA Clone). Thanks again KARAM !!!
- Added TAI 10 Installer (Enforcer 37.76 Fake?). Thanks again KARAM!

- Added infected MUIGUI (Thanks again Martin !!!!)
- Added recognition code for Enforcer 37.55 by M.Sinz
- Added new FileID Library 4.1 (Thanks Oliver !!!!)
- Added support for the A4000 version of Kickstart 40.68
- Added Excreminator Bootvirus Installer
- Fixed a major problem in the memmonitor. Now the enforcerhits do not appear, if you select a vector, which points to 0 !
- Added support for the A3000 version of Kickstart 40.68. Thanks must go to Olaf "Olsen" Barthel for letting me test VirusWorkshop on his system...
- Added some CRC checkroutines. Thanks must go to Olaf "Olsen" Barthel for the CRC32 routines !

Tristar & Red Sector inc.'94 - Back to the roots

VirusWorkshop Version 3.1 final:

> VirusWorkshop 3.1 is only for Kickstart 2.04 and higher.

> It is not allowed to put VirusWorkshop on S.H.I. discs ! <
> There are two exceptions: Jim and Betty Maciorowski (ex. SHI USA) <
> and Lars Kristensen and Jan Bo Andersen (SHI Center in Denmark)

If you want to contact me via modem, then you should call

BoardName: N.A.S.A.

USR Dual Standard (including V.Fast!) Modem

Tel.: ++49[0]572374340

Username: VW
Password: VW

The VirusWorkshop conference includes all important information for you. My user handle is "Markus Schmall". Every user of a high-speed modem gets a very good connect (14400+).

Or leave me the "c" command a commet (to FLAKE).

- Added Fileghost Virus installer. Thanks must go to Ingo Schmidt for sending this one.
- Fixed an Enforcerhit on a A3000 with a couple of installed patches and bootroms. The ZEROPAGE was completely empty and

therefor VirusWorkshop forced a LONGREAD from $0. Now it's fixed !
- Added Fred Cohen Bootblock Virus (Thanks must go to Markus Pfeiffer for sending this virus).
- Added ATARI (BSG9) filevirus. Thanks must go to Georg Hörmann for sending this virus.
- Added Leviathan (Boot+File) Virus & ARTM Virus. Thanks must go again to Georg Hörmann for sending this virus.
- Added ConMan (fake ARTM 2.3) BBS Virus. Thanks must go (again) to Georg Hörmann for sending this virus.
- Fixed the installerscript. The script aborted, when you did not already have installed an older release of it.
- Added recognition code for $4eb9 linker clone.
- Fixed a fu....ng problem with the A3000 40.62 kickstart version. I recieved some time ago a buggy (patched) Kickfile of it. I included it and on an AMIGA of a developer it crashed. Now I have taken the offsets from an official developer file ! Thanks O....
- Added Asassin BB Virus, DTL(MTD) BB Virus, PAL BB Virus, PKK BB Virus, TAI-4 BB Virus, Bad Bytes Inc 1-5 BB Viruses. Thanks must go to KARAM for the really great support. Back on the stage....
- Fixed the problem with the Kickstart 37.175 in the A3000. SPecial thanks must go to Dieter Siemens for reporting this and for the help.
- Added some additional routines for 100% secure checking for the Crime'92 viruses. Special thanks must go to Soenke Freitag (University of Hamburg/ Virus Test Center) for hints and some tips.
- Fixed a gfx problem with the Infiltrator Virus: The pointer to the text was changed and you could not see the correct text. Thanks must go to Soenke Freitag for reporting this bug !
- Added Dum<ii>Dum Bootblockvirus ! Thanks Ingo !
- Added CLP_WOW.exe Virus in 4 (!!!) Versions. Read the documents for more info.
- Added RAF and Khomeini Bootblockviruses. Special thanks go to Jan Bo Andersen (SHI Denmark) for sending this ones.
- Special thanks must got to Flemming Lindeblad for the daenish translation from the catalog file. Many thanks...
- Added VirusZ II 1.02 virus (Compuphazygote clone). Thanks again Karam !
- Added BooTX recoq update installer fake formatter virus. Thanks must go to Ingo Schmidt for sending this virus.
- Added recognition code for WARP 5.1e by N.O.M.A.D.
- Added M-WHO.lha /X backdoor. Thanks must go to Ruediger Everding for suplying me with this virus. Thanx Rudi... Moege die Schlammbowle fliessen....
- Added merry.exe /X BBS virus. Thanks must go to Karam, Warhead/TRSI and NO LIMIT/TRSI&ILS for sending this virus.
- Added XRipper (Lamerinstaller) and Vkill100 filevirus. Thanks must go to Georg Hoermann for sending this pieces..
- Added UaDialer62 Virus. Thanks must go to AtomiX for sending this virus.
- Added VirusHunter joke file. Thanks again Georg !!!
- Added Anim_demo.exe BBS virus. Read CLP_WOW.exe doc, too. Thanks again AtomiX for this really fast support....

Tristar & Red Sector'94 - Back to the roots

Enough is enough: Since many months I am searching for the so
called "4eb9" linker. The viruses: merry.exe, kairo.exe, m-who.lha
and many others are created with this programm. The group GLOBAL
OVERDOSE used this linker in their CLYSTRON trainer. Isn't it
possible that I get this linker ?

VirusWorkshop - Alive and kicking...

VirusWorkshop Version 3.0 final:

> VirusWorkshop is now a T.R.S.I. production !

> KARAM! Bitte melde Dich bei mir ! Das Board ist ja derzeit
  offline !

> VirusWorkshop 3.0 is only for Kickstart 2.04 and higher.
> It is not allowed to put VirusWorkshop on S.H.I. discs ! <

-Added SHI bootblock virus (Thanks KARAM for sending this one...)
 This is a Australien Parasite Clone....
-Added VirusConset I,II and IIB viruses (Thanks again KARAM for
 your really great support....)
-Added some patches
-Added LOCALE Support (I need translations for the following
 languages: -french,-danish ....) Feel free to
 contact me!!!
-Added recognition code for Peter Stuers LVD 1.75
-Added VIRI bootvirus (FICA clone).Thanks Karam !!!!

```
-Added some older viruses...
-Added Megalink virus (Thanks Ingo Schmidt for sending this piece..)
-Fixed some stuff...
-Hopefully fixed problems with NTSC AMIGAs. Use Virusworkshop with
 option i0 -4/5 ! Read DOCS !!! Thx Jim Maciorowski...
-Added Bossnuke 1.5 virus ! Thanks must go to NO LIMIT/TRSI !!!
-Added Sepultura 2.26 virus ! Thanks must go to Ingo Schmidt for
 sending this virus !
-Added 25 Bootblocks (utilities,intros). Thanks must go to ConTrol/TRSI
 for sending this ones !!!
-Added VirusMaker 1.0 and ComaVirusinstaller. Thanks must go again
 to Control/TRSI for sending this stuff...
-Added a little installerscript to install all the libraries...
-Added Ingo Virus (Zenker Clone). Thanks must go to Ingo Schmidt
 for sending this piece.
-Added Digital Dream Bootblock Virus. Thanks must go to Ingo Schmidt
 for sending this virus !

                              Tristar & Red Sector - Back to the roots




VirusWorkshop Version 2.6 final:
--------------------------------


> VirusWorkshop 2.6 is only for Kickstart 2.04 and higher.



 STEVE3003, please contact me ! Thanks !
 ( Not on Z-NETZ ! Voice or letter ! Or call Trade in Center or
 Nuclear Destroyer...)

-Added recognition code for PPLoadseg 1.4 by Nico Francois
-Added support for the FileID Library by Bloodrock/SDC.
 (VW is now able to recognize more than 380 different formats)
-Added recognition code for Powerdata 38.200
-Added recognitioncode for MChat Virus
-Fixed problems with the new ReqTools 2.1f Library
-Added the new reqtools Library
-Added recognition code for VIHPS and Diskval1234 viruses
 (These viruses are not new but VW did not recognize it.Thanks must
 go to KARAM for sending this pieces.)
-Rewrote Vectorkiller and Sectorchecker.It should work now with
 all HD devices etc. and the vectorkiller should do it`s work
 correct on Kicktart 2.04.
-Added Support for the A3000 version of Kickstart 40.62.
-Added support for the Commodore RAM Disk
-Added recognition code for Dircache 1.02
-Added recognition code for the new $4eb9 Linker clone.
-Added recognition code for RT Patch 1.2
-Fixed a little problem with the window:It was no backdrop window.
 (Thanks for this bugreport go to Agent Orange/MST)
-Added recognition code for N.O.M.A.D. warper 1.3
```

```
-New menus added: Document !
 You can now ,if AMIGAGUIDE.Library,enough memory is avaible and the
 textfiles stay in the same directory  like VW, read  all  documents
 from VirusWorkshop.
-Fixed problems with not giving free the memory, when starting from
 WB.Thanks must go Vasco Steinmetz.
-Added recognition/repaircode for the Dark Avenger Typ A Virus.
-Added recognition/repaircode for the Dark Avenger Typ B Virus.
-Added some clone BB viruses:Starcom 1-5,Irak 3,Mad 3B,Prima Vera
 & Grim Heaper (Thanks must go to Georg Hörmann for sending this
 viruses)
-Added ABC Virus(killer) BB,Electro Vision BB Virus, Exorcist(SATAN)
 BB Virus,Lame Game BB Virus, Starcom 6 (again thanks must got to Georg
 Hörmann for sending this ones.).
-Added aibon2 virus + the installer for it (Thanks again Georg!!!)
-Sectorchecker optimized again.It should now work with all sectorsizes
 (except 32 KB/blk).At least I hope so.
-Vectorkiller improved and fixed for COMBO-2 Kontroller (Thanks must
 go to Joachim Dort for reporting this bug and for letting me use
 his computer).
-Added a MicroSystems Clone BB (CBM) and PVL BB Virus ( Thanks must go
 to Karam for his really great support !!!)
-Added 2 SCA clones (SCA-666,SCA-KarlMarx) and a TFC BB Clone
 (TFC 47.11) Again thanks for this viruses must go to KARAM !!!



VirusWorkshop Version 2.5 final:
--------------------------------


> VirusWorkshop is now a MYSTIC release <

> VirusWorkshop 2.5 is only for Kickstart 2.04 and higher.


> To the author of the August Releasecharts: You wrote that
  Mystic would release the same utilities every month.Yes this is true,
  but a viruskiller has to be updated every month to be actual.
  P.S.: Nice charts !!!


- Added recognition code for RTPatch 1.1a by Nico Francois.
- Added REKICK test for the libraryoffsetprint (Thx Stöberhai).
- Problems with MC68881&MC68882 text print fixed (Thx to
  Mike Volland & Peter Schulz).
- Again fixed a memorycheck problem
- Added XACA Virus (=Disktest) Thanks must go to Georg Hörmann
  for sending this virus.
- The UserInterface was completely rewritten and is now styled with
  the GADTOOLS Library.Sorry Kickstart 1.x users,but VW is from now
  on a pure OS2.x programm.
  After 8 hours of coding,VW is now compatible to the C=
  User Style Guides..
- Shortened code and rewrote some blocks (again 6-10 hours).VW is
  now 17 KB shorter....
- Support for the Super72 Highres (800*300,AGA only) added.
```

- Added recognition code for Degrader 1.60 by C.Hames.
- Added checkroutine for OS versions.If you have only Kickstart 1.x,
  VW will quit automatically.
- Added recognition code for Phil Douglass 2.0ß Warper
- Added Support for the A4000 version of Kickstart 40.62
- Added recognition code for Enforcer 37.52 by M.Sinz
- Added recognition code for DosTrace 2.00 by Peter Stuer
- Added recognition code for the Cruncherformat of Siegfried Copy 1.2
- Added recognition code for VirusInterceptor 1.4 by J.Eliasson
- Added a little memorymonitor (read the single "MEMMON.GUIDE")
- Added recogntion code for the A.I.S.F. Virus (Thanx must go to
  Ingo Schmidt for sending this virus).
- Added some new intro/utilitie bootblocks
- Speeded some internal routines in the filechecker.Now you have a
  little speedadvance: On a A4000/40 VirusWorkshop previously needed
  about 50 seconds for it's work on a 8 MB partition with a lot of
  files.Now it only needs 41 seconds.You must remember that on a MC68040
  the clearroutine is running in the CACHE and is extremly fast executed.
  That means even more speed on a normal system.
- Added the Aereg 3.9 virus (Thanks must go to ATOMIX for sending this
  virus!)
- Fixed some bugs,which only occured on a MC68030 (Thanks Mike Voland)

VirusWorkshop Version 2.4 final:

> VirusWorkshop is now a MYSTIC release <

VirusWorkshop 2.4 is only for Kickstart 2.04 and higher.The next
release will be probably again for Kickstart 1.x,too.

- I have added a DISKTYPE text in the DRIVEINFO menu.DiskType is not
  always the same as DOSType.It should work on all drives with a
  normal AMIGADOS format.
- New version of DosTouch (V1.4) added.
- Added recognition code for NewAlert by Brian Gontowski.
- Fixed problems with HD drives (Sorry)
- Added -z-speed.lha Virus (Description 4.0)
  Thanx must go to Crackdown/Mystic for keeping this virus for me.
- Added KAKO Bootvirus + Installer (Thanx must go to KARAM for sending
  this stuff)
- Added new function in FILEREQ/SingleFile:If you select a file,
  only the file will be checked.If you select a directory,the whole
  directory will be checked.
- Spotted bug in the Kickstart 37.350 vectorkill option
- Changed Kickstart 37.300 vectorkiller
- Added Butonic 4.55 Virus (Thanks again,Karam !)
- Added SnoopDOS 1.9 virus (Thanks Atomix/Christian)
- Added recognition code for Enforcer 37.49

VirusWorkshop Version 2.3 final:

- WARNING: Do not use the DECRUNCH LIBRARY (DECRUNCH=ON),if you have only 1 MB memory.The library crashes at longer files.The recognition code for the PP 4.3b is not correct.Some files will be recognized as PP DATA but it are normal PP files....The same problem occures,if you have a long ANIM file (about 2mb,powerpacked) and you want to depack it with an AMIGA with 9 MB of memory.
- New version of the REQTOOLS Library added...
- New version of DosTouch added
- Bug in the HDSupport Routine partly fixed.You can now use the Filechecker without crashing your system.The sectorchecker should not be used for Harddrives.
- Bug fixed:You can now use the DMS Check for RADs,too.Thanks go to ATOMIX for the bugreport.
- Bug fixed:Example:You have a device called a and wanted to check the files in the directory Hilfe.Other file does not exist.VW2.2 stopped all actions because it thought(because of the short name), that no files existed.Fixed now.Thanx must go to ATOMIX.

VirusWorkshop Version 2.2 final:

- Sorry for the misunderstandings in version 2.1 with the 2 released archieves.There was a strange bug in the VW21.lha archive which I found some minutes after release.Sorry.
- Added DMS check.
- Added DosTouch (a little utilitie like SnoopDOS) to the archive.
- Added Nano][Virus,Payday Virus,Multilator Virus,Cascade 2.1 Virus, Wahnfried Virus,Usr492 (Sentinel) Virus and XCOPYV2 virus.
- Added Disktroyer2 virus
- Added recognition code for DosTouch
- VirusWorkshop recognizes now about 400 Utilitiebootblocks.
- Added a new detectionroutine for a new cryptroutine from a Crime92 clone (?).
- Added COMPUPhazygote 7 virus
- Added Description4.0 virus
- Added recognition code for DosTrace 1.0 by Peter Stuer
- Fixed some bugs in the Filechecker.
- Fixed some bugs in the Decrunchroutines...

VirusWorkshop Version 2.1 final:

(released at 12.06.1993)
- Final code shortened (ca. 10 Kbyte) but after crunching the file is only 1200 bytes shorter.
- Added recognition code for the Action Replay IV Software Update by Blackhawk/Paradox.
- Added new BBS Virus,which is linked behind WHITEBOX.
- Added Support for the A4000/A3000 version from Kickstart V40.55,which is (I heard it only) the final Kickstart 3.1 file.
- Added a little text in the main menu which shows the user,if the "decrunch" mode is enabled or not.
- Completly recoded the "Exec&Dos in Ram" routines.All should work now correct.Thanx must go to Hartmut Schulze.

- Shortened code again (ca.30 KBYTE).The kickstartmodules are now all packed with "SCRUNCHPRO" by 2-Cool/LSD.Thanks for the datadecrunch-routines....
- Rewrote some of the memorykill routines.If you have a A600 with Kickstart 37.300 or 37.350 then please start VW and use the funktion "KICKSAVE" and save the first 512 bytes from your ROMs.I want to write a unique memorykill routine.

I am searching for SUPPORT mailboxes & BBSs.

VirusWorkshop Version 2.0b final:

Things added:
- Checkroutine for the avaible SCREENMODES.
- LW Name does not say anymore "DF0:   6".Thanx must go to Martin Spaltner.
- SCSI Virus will now be detected correctly. All "version" commands (RELEASE 40.1) are not infected but my checkroutine was too lousy.
- Support for Kickstart V40.38 (A4000) added.
- Optimized the Sectorcheckroutine.It is still not bugfree ! (Some drives may stop and you have to reset.Sorry but I cannot find this nasty bug!).On my machines (A500 with an Evolution 2.2 controller and an A4000) the sectorchecker works. If you add an extra harddrive (for example a GVP Series II controller) to the A4000 the extra SCSI harddrive cannot be sectorchecked (It crashes!).God knows why. I hope I have found the nasty bug quite soon.
- AmiPatch 1.0 added.
- If you have a NTSC Amiga then please start the VW with the option i0.VW will start in the INTERLACE mode and you can see all information at the bottom of the screen.Thanks for reporting this "bug" must go to Jim Maciorowski.
- Modemcheck Virus added.
- Some little codeoptimizations & bugfixing.
- Diskrepair BBS Virus added.
- General $4eb9 linker search routine added.

VirusWorkshop Version 2.0a final:

Things added:
- Bestial Devastation Virus , FUCK Device Virus and DETLEF Virus added.
- Support for the beta developer versions of Kickstart 39.116 &40.9 for the A4000 added.
- Diropus virus added. Thanks must go to Martin Spaltner for sending this virus.
- OS2.0 Look added.
- Added recognition code for the FFC/Skid Row warper V1.1 and V2.0 and for the RAP!TOP!COP! utilities from A.Sander.
- Added recognition code for the OWS Packer by M.Pendec.
- VirusWorkshop now tries to get the size of the Workbench and emulates it. (Idea by Karsten Weiss)
- Shortcuts added in the menus (Thanks must go to Karsten Weiss).

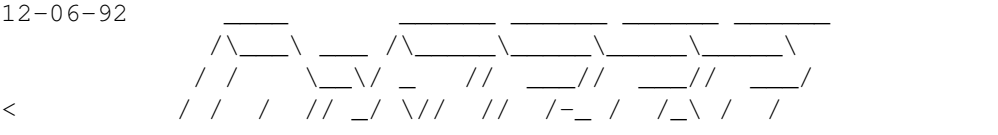
- Full HD Support in the Sectorcheck function!
- Sectorchecker searchs now for invalid checksums, too.
- Recognition code for the Turtle Smasher 2.00 cruncher.
- International Filesystem requester and Expansion Library requester added in the BootBlockInstall option.
- Crime92 should be repaired now. I have tested it with about 20 files with different cryptroutines and different structures.
  If there occure problems with your infected file, please call me....
- Four new bootblockviruses added: Angel, Influenza, Killed & Executors.
- 12 new fileviruses added: Chaos Master, Commodore, NOGURU, Christmas, SmBX trojan horse, Beethoven , PStats , Telecom , MsgTOP , 2 versions of Devils BBS virus (ULOG/DLOG) and Swiftware 0.98.
  Thanks must go to Georg Hoermann (VirusZ) for sending them.
- Code shortend about 2000 bytes.
- Recognition code for the Xlink 3.00 file linker.
- Special routine to look for future coded sectors by future Saddam Disk-validators!
- The documents were put in one file and converted to the AMIGA Guide format (but you can read it with a normal ASCII viewer, too).
- Sectorchecker improved very strong: The Overkill Sector damage routine did not work properly and is fixed now.
- LZ Virus recognition and repaircode added.

Bugs fixed:

- In MAKEBB the Requestertitel said "SELECT SAVEFILE" but it has to be "Select LOADFILE ". Fixed now.
- Megabug removed: Just try to use VirusWorkshop under OS37.175 (2.04) , OS37.300 (2.05) or OS37.350 (2.06). It crashes all the time!
  What was the reason for this crashes? There are several SCREENCLEAR routines built in. One of them crashes because of one illegal value. Kickstart 3.00, 1.3 and 1.2 does not care about it. SORRY to all Kickstart 2.0x users.
- The INSTALL function was partly broken down. Fixed now.
- Buffersize increased (about 40KB). It does not matter because the programm only works with at least 1 megabyte RAM.
- About 10 Enforcer Hits were fixed. There are still many hits in the programm but I have to check the VECTORBASE. You can deactivate the ENFORCER by using VECTORKILL. Quite easy to do....
- Blockread/write routines hardly optimized . Many bugs have been removed and all(!!!) clones of SADDAM (existing or not existing) will be kicked down !!!
- MC68882 was not correct detected.
- Better devicehandling.

06.12.1992.:Official release of Virusworkshop as VirusWorkshop 2.0a Beta!

VWBETA.LHA P 137727 12-06-92



>>> FREE DOWNLOAD <<<

```
     ---------------            \/ _____/ \/    / _// _____// _____// _/
                               --\/------------\/--\/-----\/-----\/-------
                                    presents: Virusworkshop 2.0a BETA
                               ----------------------------------------
```

Intern Version 1.9c:

- I saw ASM-One 1.09 by The Flame Arrows. Try to load a source if you have not changed the directory in the REQTOOLS.Library requester. No file can be loaded. I had the same problems. Fixed. But please always select the dir correct, because of the following problem: If you not change the directory the pure filename will be written (e.g. "TESTFILE). Sorry T.F.A.: The source I posted you isn^t working 100 %.
- When testing VirusWorkshop on a Kickstart 1.2 AMIGA 500 I discovered another bug. To come of the correct DEVICENODE, you HAVE to go over DOS ROOTNODE (see DOCfile!)

Intern Version 1.9b:

- added QRD 1.1 linkvirus RAM Check & File check routines!
- added a simple CPU/MMU/FPU Check (soon to be opimized!)
- the code was shorted & speeded a lot (about 2 KB)
- fixed some bugs which made the system refuse to work when the VBR was not ZERO under Kickstart 1.2. and Kickstart 1.3.
- fixed a silly bug which made the VirusWorkshop not detect any SADDAM Virus (at Sectorcheck) under MC68040. I forgot to use the Caches and the new COPYBACK mode correctly. Now fixed.
- VirusWorkshop now uses REQTOOLS Library 2.1. Under Workbench 2.1+ you will have now in the Filerequester your local language!
- optimized the low memory handling: The filebuffer will only be allocated, if you select the CHECK FILES function!

****

```
moveq #0,d0
rts
EOF.
```

(c) 1994 by Markus Schmall

1.136 future

Ideas for the future:

- A requester which cancels special directories from checking files (FONTS: ENV: etc.) Idea by Martin Spaltner ! THX !

Do you have a special thing which I could include ? An unknow patch

or a new virus ? Simply write to me !

1.137 hellos

Special regards and greetings go to:

Ingo Schmidt

Vasco Steinmetz

Soenke Freitag
J.Walker/TRSi Danke fuer den "0" day Support mit solchen gefährlichen Viren, wie BURN und Mount. Danke. Wenn ich doch nur Deinen richtigen Namen wuesste....

Dave de Pauw Thanx for all the viruses and the hint with OFS!

Andreas Weyert Danke für die vielen Utility-BootBlöcke und Calls....Gruess Lars !

Georg Hoermann Danke für neue Viren, für die XfDMaster Library und für die Gespräche/Briefe und .....

Michael Sinz For the megamighty ENFORCER

Ralf Thanner Hallo Ralf ! Nettes Gespraech bei der Rainbow Party. Wenn ich Deine Adresse haette, wuerde ich mich melden... Viel Erfolg mit den Projekten...

Atomix Thanks for making paint this nice ascii for Virusworkshop and for viruses...

Rüdiger"No Limit"/QTX&ILS Nice studies and thanks for the support...

VirDown Thanks for all this viruses... Without your big'n' great support VirusWorkshop would be not as powerfull as today. Thanks a lot.

Melanie For all the moral support...

Joachim Dort Thanks for BETAtestings and
your help and computer !!!

Steve3003 Nice chat on Woc‘93 !
Really cool comments in
Z-Netz/Rechner/Amiga/Viren !!!

Mike Voland For all your support and hints...

Flemming Lindeblad For the translation of VW.catalog

Kai Haseloh Depack! ist wirklich gut ! Wieso
soll ich das GUI optimieren ? Im
Vergleich zu meinem alten "STIL"
ist es doch schon ein großer
Schritt in die richtige Richtung.

Jörg Wabbel, Markus Klinge....

There’s one person I DON’T want to thank:
---

* Erik Løvendahl Sørensen

1.138 vtc

Hi Sönke ! Vielen Dank für den Support und die gehaltvollen Msgs.
im Z-Netz/Rechner/AMiga/Viren !!! Der Tag im VTC war eindrucksvoll.
Zu dem Dark Avenger: Er ist polymorph, aber halt genau die andere
Version !

1.139 contact

How to contact the author:

If you have an idea, bugreport or a virus, which is not recognized,
then please send it to me. You will get an answer as fast as
possible. To contact me just write to:

Markus Schmall
von Gravemeyerweg 25
30539 Hannover/Bemerode

Telephone: +(0)511 514944
(from 18.00 - 20.00)

I am at this time mostly at home. Otherwise one of my parents is at home. It is nearly not possible that you reach nobody from us...

To get the latest version write me. I will send you then as soon as possible the latest version. Please include postage and lettercases! I cannot afford it to pay such things for you.

! ATTENTION !

I AM NOT INTERESTED IN ANY KIND OF SWAPPING ILLEGAL WARES!
I AM COMPLETELY LEGAL CODER!

The latest versions of the VirusWorkshop and DosTouch can be found on the TIME PD discs by A.P.S. Electronic.

You should find this viruskiller in several networks. If you are a sysop who wants to spread this piece, just contact me (I own an USR Courier DST Terbo!).

This viruskiller will always be first uploaded to:

```
*****************************************************************
*                                                               *
*  BoardName: Chaos Line                                        *
*                                                               *
*  USR Dual Standard ++49[0]572374340                           *
*                                                               *
*  Username: VW                                                 *
*  Password: VW                                                 *
*                                                               *
*  Here you can download the newest version of VirusWorkshop.   *
*                                                               *
*  Chaos Line is the official VirusWorkshop Support BBS ! If you *
*  have any problems with viruses, then try to reach me on this  *
*  BBS ! The Sysop is very helpfull !                           *
*                                                               *
*****************************************************************
```

Other very fine boards are

DALLAS BBS

USR Terbo Dual Standard ++49[0]711588146

Nirwana BBS

USR Terbo Dual Standard ++49[0]511522809

another very well mailbox is the mailbox from the Virus Test Center from the University of Hamburg. There you will find all actual viruskillers:

Tel.:++[0]4054715235 (V32bis modem)

You can find the VirusWorkshop in the following BBSs(a friend of me uploads the file to them):

- sorry, no special BBS this time...

Write a message to "Flake@DALLAS.zer".

If you have access to INTERNET, then try to reach me on:

"msch0091@rz.uni-hildesheim.de".

(You can write out of nearly every net to this adress!)

If you have access to AmiXnet, then try to write to the following adress:

AX0001 Markus Schmall NetID @GR0001

The contact via INTERNET is preferred, because the Z-Netz lacks sometimes and some PMs will be somewhere "forgotten" in the system. I wrote some messages in this network, but some of them are still not routed and this after 6 months.

VirusWorkshop can be found on the TIME PD disks.At the release day of VirusWorkshop it will be mailed to A.P.S. Electronic !!!

CU l8er,
Markus Schmall

Tristar & Red Sector - The sleeping gods