VirusWorkshop

Markus Schmall

COLLABORATORS			
	TITLE : VirusWorkshop		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY	Markus Schmall	January 18, 2023	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VirusWorkshop

1.1   Addy099 Trojan horse

```
                    Addy099 Trojan + it's installer:
------------------------------

Addy099.exe (9584 bytes unpacked)
c/dir       (2784 PP 2.3 mastermode)
            (8284 unpacked)


The Addy099.exe file is a classical trojan. It contains some code
to write a new dircommand and to manipulate the following textfiles:

-Shell-StaRTUP (will be new created)

 Contains:

 wAiT 5
 Echo Wait 5 >>Sys:S/sTarTup-sEquEncE


-User-Startup

 Contains:

 wAiT 5

-Startup-Sequence

 Contains:

 Prompt "aFraId ?..tHe fReAk wAs hEre 2 dEvEstAtE  NDOS:>"
 wAiT 5


If VirusWorkshop detects the ADDY099 trojan, then please check this
files too and use a texteditor (e.g. the great GOLDED) to correct
the files. Thanx !
```

The new written dircommand is 2784 bytes long and was packed using
the old powerpacker 2.3 in the mastermode.

The trojan(in dircommand) searches for the file:

'S:D-TECT_DOC_DISK'

If this file is not existing, then a reset will be performed.
Otherwise some other code will be executed (via Dos EXECUTE()).

File_ID.DIZ of this file:

```
   _____
:                          :
| _____     |
| \\\\\//////////    |
|   \Addy\ver./0.99///    |
|    \\\my\FIRST////      |
|     \Release EVER/      |
|      \\\///////         |
|      ~~~~~~~~~~~         |
|     -»»bY tHe FreAk««-   |
|          SysOp at        |
|        »Money Talks«     |
|       +44 ELITE ONLY     |
¦_____:
```

                              Detection testedt 28.01.1995.

          The~document~for~this~trojan
          " link "addy-099-doc" 0}

          Warning~text~from~the~Virus~Help~Center~Denmark~!

1.2 ConMan-LoadWB+Installer

          ConMan
           LoadWB+Installer:

Needs Kickstart V37.XXX or higher to work.

Trojan: 12088 Bytes
                         (somekind of encryption tool, not packed)
new LoadWB : 2088 Bytes (packed with TurboSqueezer 6.1)
                         (unpacked 2124 Bytes)

```
    Archivname:  dpl-dc99.lha


This trojan was linked using the
        4eb9~linker
        . Euronymous/TRSi tested
this file and found the 4eb9 stuff and informed me, thanks a lot !!!
The trojan searchs for a task called "CLI(0):no command loaded" and
creates a process under this name, if it is not existing.

A new LoadWB command will be written, which contains the destruction
routine. It will be waited about $5500 ticks and after this it will
be checked for a file "s:conman". If this file is existing, the
trojan will not work. If the file is not existing, it will be tried
to format your sys: device. All data is lost, I am sorry to say this.

After the destruction process, a Intuition alert will pop up and
show show you the following text:

’
        CONMANS
         SYSKILLER MESSAGE: YOU BETTER TAKE CARE DOODIE - ’
            ’SOFTWARE-PIRACY IS A CRIME! ’.



IMPORTANT: The virus tries to install a new process called
"CLI(0): no command loaded", if this is not already existing
(from system). I could not install this task on an A500+
and on a A4000/40, so I could not write a repairroutine for
it. Result: If VirusWorkshop finds this infected LoadWB file,
THEN delete this file and reset your machine ! Thanks !
You have $5000/50/60 Minutes (+- 6 minutes) before this
destruction part will be activated !!!


                              Detection tested 26.01.1995.
```

1.3 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.
```

1.4 Commander

```
                    Commander Linkvirus:
-------------------
```

KS 3.1: yes MC68040: yes
KS 1.3: yes

- increases filelength by 1664 bytes
- Patched vectors:

 DosOpen(), DosRename(), DosLock(), DosExamine(), DosExNext(),
 DosLoadSeg(), DosSetcomment(), DosSetProt()

No resetvectors will be changed by this virus !

First appearence of this virus: Scandinavia
The virus seems to be wide spreaden in the scandinavian
countries. I have heard several reports from Sweden and
Denmark.

Approximatly 1 month after the first appearance in denmark, the
virus reached Germany and Switzerland, too.

This virus goes a similar way like the Dark Avenger viruses. It
looks for a special longword in the first hunk and replaces it
by a "JSR" command in its own code. The own code will be placed
at the end of the first hunk. The code is crypted with a simple
eor-loop, which depends of the rasterbeam.

The searched longword is a BSR or a JSR command and will be
recalculated in the virus. VirusWorkshop is able to refix all
the patched things. Special thanks at this point to Ingo
Schmidt, who really helped me a lot...

The BSR.B commands will be not touched.

Special: It looks for the task "DH0". If this task is existing,
it will be tried to infect the file "dh0:c/loadwb". The virus
infects all files, which will be accessed using the patched
functions. Possible protections from DOS will be removed by the
infected files.

The patchroutine is quite complex (or complicated in other
words).

This virus is quite similar in some routines to the Commander
bomb on PC. I got this hint from one of the members of the VTC
in Hamburg.

The following texts are double crypted and can be found at the
end of the virus:

'-<(COMMANDER)>- by Bra!N BlaSTer in 1994'
'DH0:C/LoadWB'
'DH0'
'dos.library'

`'reqtools.library reqtools 38.888'` (don't know what this is)

Detection tested 03.10.1994.
(Memoryremoval and fileremoval)

Comment 4.1.1995: Only VT, VZ and VW (from the big viruskillers)
remove the Commander virus correct. Another english speaking
viruskiller (last update 31.12.1994) is not able to repair all
the infected files.

There appeared another Commander viruskiller, which carries the
whole virus !
        Read~more~!
                Comment 03.10.1994: It already exists another special
Commander Viruskiller, but this viruskiller is not able
to recalculate the jsr commands ! (1.4 is actual at this
special thing)

Comment 19.10.1994: The repairroutine was a little bit
buggy under special circumstances. Now fixed. Sorry.

Comment 24.11.1994: After a SHI member from DK wrote about
the real Commander virus installer, I got it 2 two later from
Jan Andersen (former SHI TEAM DK). This is the intro from
RAGE and APEX. The original file is 64924 bytes long (I got
it in Germany). The "installer" is 71800 bytes long and
contains some additional CLI textroutines, which hide the
virus. This is in my opinion NEVER the original installer,
but VW 4.4 and higher will recognize it....

Comment 01.12.1994: A new installer appeared some days ago. This time
it is (again) a production from Duplo(like dpl-de99, which I urgently
need!).
This time it is a two disk AGA demo titled My mamy is a vampire. The
virus can be found in the first file from disk 1, called Vampire.exe.
The virus is included in the file and I don't know how it fiddled in
the demo. Maybe some of the Duplo programmers can say this to me ?

The infector is 875778 bytes long, packed and somekind of OS enhancer
was added before....

Comment 14.12.1994.: There seems to be guy around us, which spreads
the fuckin' Commander virus.
        But~read~for~yourself~!

1.5 Commander-Lame

                         In general I don't like to kick another viruskiller in ↩
                            this
way, but I think in this special situation, I had to go this
way !

Commander Viruskiller by Focus Design:

Filelength: 2252 bytes

This is a special viruskiller for the Commander Linkvirus,
which was first spreaded in north countries like Sweden,
denmark and other countries.

THIS VIRUSKILLER CONTAINS THE WHOLE VIRUS AND USES IT AS
A CHECK REFERENCE ! BOYS ! STOP THIS SHIT ! YOU SPREADED
A COMPLETELY WORKING VIRUS ! AN EVIL PERSON JUST HAS TO
JUMP INTO THE CODE AND ACTIVATES THE VIRUS ITSELF !

The viruskiller can't repair the damages of the Commander
virus in very large parts, cause the programmers did not
understand the inner workings of this virus ! The entry-
jump longword will be always replaced by a static longword
from the viruskiller, which is pure bullshit (another well-
known viruskiller is doing this in the same way) !

Click
        here
         to get the document for the FD killer.

The viruskiller was released on 19.10.1994. At this time
two of the major viruskillers (VT and VW) could repair
already the Commander virus. No need for a buggy late
version. Sorry guys in Focus Design, but your viruskiller
contains a FULL virus and this is very near to the
side of crime, because indirect you spread a virus in the
public !

This programm is not direct an installer for the virus,
but carries it completly and so I have no other possibility
than to kick this viruskiller !!! It will be recognized as
Commander Virus Inst. and removed ! Never seen such a bull#?&%
before. Sorry guys in Focus Design but you have chosen the
wrong way.

                              Detection tested 27.10.1994.

1.6 EL!Install

                    ELENI! Installer + ELENI! SysB file:

```
ELENI! sysb file:
-----------------


This name is based on the location of this file: "sys:b"


   This file is 1504 bytes long and contains the bootblockvirus
   and a little DOS  startprogramm for it. Please read  in  the
   bootblockvirussection for more information about this virus.



ELENI! Installer:
-----------------


Filelength: 1808 bytes (packed with
      TurboSqueezer~8.0
      )
           7100 bytes unpacked



This file pretends to be a viruskiller for the MessAngel
virus. If you start the programm, the Startup-Sequence
will be loaded and a new command will be placed in it.
Due to extremly lame programming, there will be always
saved 5000 bytes from the Startup-Sequence, even if it
was only 1000 bytes long before. Then the file "sys:b"
will be saved to disc and the following message will be
shown on the screen:


        'MessAngel killer by Docker of Twist!'
        'Checking startup-sequence...'
        'VIRUS FOUND AND REMOVED!!!'
        'Right to disable from memory!'
        '--------------------------'


This text is a pure fake. For more information about the
ELENI! virus, please read the description in the bootblock-
virussection !!!!



                          Detection tested 30.09.1994.



      Fake~document~from~the~installer
              In the document there will be mentioned two  ←
                  telephonenumber,
which you can call, if you  have  problems  with  the  fake
viruskiller. This  are , as far as I know, the numbers  from
the swedish DATOR magazine. Another hint that this virus was
created somewhere in Scandinavia....
```

```
        Comment 03.10.1994:
        -------------------


        It appeared a special MessKill Repair programm (v0.9), which
        installs a new LoadSeg patch. This patch will be removed by
        VirusWorkshop, too.



              Some~comments~to~Messkill~Repair~0.9
                      Special thanks to MFM/Skid Row for the first warning  ←
                              concerning
        this virus !
```

1.7 ELcomm

```
        Some comments from me (Flake/TRSi) to Coolorado/Corpse for
        the MessKill Repair 0.9:


        -First of all you were the first to release such a repairtool
         for the damages of the ELENI! (messkill.lha) virus.


        1.You check the DoIO vector only with 2 longwords. Too less
          in my opinion. Why don't you try to remove the patch ?
        2.You search for the DosInstaller ("sys:b") only on the
          actual sysdevice. Better give the MessKill Repairer an
          option to select a device.
        3.Argh. You install another patch for the LoadSeg vector
          instead of clearly removing the viruspatch. Your patch
          uses a direct memory access to the zeropage. Simply try
          to remove the patch like all the other killers.
        4.Your code contains a lot of relochunk entries. It should
          be possible to code such a thing without any relocentry.
          Just think: Your sourcecode is for sure not longer than
          8000 bytes, isn't it.


        If you visit the Dooms Day party, we can talk about this
        virus....
```

1.8 EL!Doc

```
        The document of this fakeviruskiller-virusinstaller:
        ---------------------------------------------------
```

```
Messangel killer.documentation

Introduction:
```

Are you having problems lately with strange files on your hd, sudden Guru
Meditation etc, then you'd better test this program since there is a virus
spreading around lately. First time (perhaps!?) found at Smaug BBS in Sweden.
From there sent to me by Jimmy Elander (thanx!) and then disassembled by me to
kill the shit!! And here it is, not the virus, but the killer!! This is the
cure for all of you who suffered from it!

How does the virus act?:

This virus is a link virus which spreads like the plague!! It's probably
mainly made to be infected to the Hd files because it doesn't respect that the
save-media might be write protected! In case you boot with a diskette after
the virus has been activated you'll very soon notice that it asks you to
remove the write protection from the diskette! If you do so then it will
infect various files on the diskette! Well, how can this virus be able to
infect almost all files?! Simple, it patches the loadseg (dos l.) so that
every file that bypasses this operation gets infected! It also copies itselft
into the startup-sequence of the active drive! Exactly what the virus does
after infection I don't know but the important thing is that you can remove
the virus from infected files!

How does this viruskiller work?:

This killer will first of all check your startup-sequence and if the virus is
present also correct it! Then it will check if the virus is in memory and ask
you to press right button to remove it! (No other option included!) Your
machine will then reboot and next time you bootup the computer will make
another Hard reset just to be 100% sure that the virus is gone! If no virus is
present in memory you will be asked if you want to perform a total scan of
files on sys:? If yes then it will scan through all files and remove possible
infections!

If you find any bugs in this killer, please report them to me by calling the
following number: +46 (0)8 6549950 or +46 (0)8 6546118

                    Now, go for the sucker!

As far as I know at the moment (02.10.1994) the mentioned telephonenumber are
from the swedish DATOR magazine. What for joke....

1.9 CMD-DOC

 Document for this cool viruskiller: ----------------------------------

*** "COMMANDER VIRUS" REMOVER ***

About one week ago, my computer suddenly started to lack memory, and attempts
at multitasking usually resulted in a system crash. A closer inquiry revealed
that this was not an infection by MicroSlug WinDoze, but the result of an
infection by a link virus called "Commander" by a lamer called "Brian
Blister".

None of our virus killers seemed to recognize the culprit, so there was no
other option than writing our own. We advise that this archive be kept in the
same dir as your usual virus killer, until it is updated to this virus, in
which case our program will probably be obsolete. You need not read any
further in the instructions, unless you run into the symptoms: – lack of
memory (the virus patches AllocMem, as far as I figure) – slow loading of
WorkBench (the virus is busy infecting everything) Be aware that if using
directory cache, the 1664 extra bytes will not be visible for dirs.. the virus
also patches dir readings etc.. and libraries, aargh!

Nevermind, should you get a RAM-sucking monster into your circuits, then..

KILL it!!

Using "Kill <fname>" will remove the virus from any infected executable file
(while leaving all other files untouched). Turn off your computer first and
boot without startup-sequence, of coz'! Remember that executing any infected
file will load the sucker, too. "Kill" was not written for user-friendliness,
so it will not respond with any error-messages.. sorry..

If you want to clean your entire harddisk, you could use our script and type
"RemoveCommander <path>" (usually hd0: etc.). You will need to clean some
commands in your c directory beforehand, check the script first.

Well. CREDZ: Research and virus remover by Coma/Focus Design. User Interface
by Bigmama/Focus Design.

*** NOTE TO MANUFACTURERS OF ANTI-VIRUS PROGRAMS, SAFE HEX, OR WHOEVER: the
source for this can be requested by writing a message to Coma at Metal
Connextion +45 74435949 (3 ndz ringdown). Also, I can supply a copy of the
damn thing, if you need it.. ok..

                        Typed by Coma on October 19th 1994

PS: We assume ABSOLUTELY NO RESPONSIBILITY for the functionality of this. It
DID, however, work fine on Coma's A1200/no fastmem/320 MB HD. We see no reason
that it shouldn't work on yours. Use at your own risk. Hope you won't be
needing this :)

There is somekind of batchfile for this "fake" viruskiller existing...

Contens of LS: --------------

.bra { .ket } .key killpath ask "Do ya want to get rid of the
Commander-virus?" if warn
 echo "Scanning dirs and sub-dirs..."
 list {killpath} pat ~(#?.info) files all lformat "kill %p%s" to
"t:virusbefængtelamerfiler!"
 echo "Checking for Commander-virus by a nice lamer called Brian Blister..."
 resident kill kill
 execute "t:virusbefængtelamerfiler!"
 delete t:virusbefængtelamerfiler!
 echo "All done!"
 resident kill remove endif echo "Have a nice day!" echo "Bye.. bye!" echo
"Well, see you later!" echo "Okay, gotta go.." echo "So.. take care of
yourself, okay?" echo "I really gotta go now, ok!" echo "So that's it baby.."
echo "Sweet dreams!" echo "I'm outta here....."

1.10 t6661

                    6661 Formatter Trojan:

       Filelength: 63140 bytes (unpacked)

       other possible names: WbPrefs-Formatter-Fake

This is a simple trojan, which uses the
        Modemcheck~(Fuck)
         virus
formatroutines to destroy data on several devices. The trojan
installs a new process with the name: amigalib.process. This
process causes this terrible damages. Many tracks will be filled
up with the longword "6661". No rescue for the data on this
damaged tracks is possible.

There must be an installer for this bastard hanging around !
If you want to help us, then search for this. Thanks a lot.

VirusWorkshop will remove this new process NOT ! It will fill it up
with NOPs. This should be ok in this way...

                                  Detection tested 26.09.1994.

1.11 Purge

Purge Installer + Purge Virus:

Purge Installer: length 9812 (imploded)
                         14862 (unpacked)

Purge Virus: length 5300 (imploded)
                         14776 (unpacked)

(VirusWorkshop recognizes all the files)

This is a simple trojan with manipulates all .info files on
the started device. The virus installs it's code on every
reachable device and changes the sequences, so if you have
found this virus, then check your User-Startup, Startup-
Sequence (the added string will be mentioned later).

If the virus installed itself completly, the later mentioned
text will appear. The virus itself is very lame coded/optimized
and was probably written in AMIGA-E.

All manipulated/new created files:

'DH0:WBStartup/Purge',0
'DH1:WBStartup/Purge',0
'DH2:WBStartup/Purge',0
'DH3:WBStartup/Purge',0
'HD0:WBStartup/Purge',0
'HD1:WBStartup/Purge',0

```
'HD2:WBStartup/Purge',0
'HD3:WBStartup/Purge',0
'DF0:WBStartup/Purge',0
'DF1:WBStartup/Purge',0
'DF2:WBStartup/Purge',0
'DF3:WBStartup/Purge',0
'A:WBStartup/Purge',0
'B:WBStartup/Purge',0
'DH0:C/Purge',0
'DH1:C/Purge',0
'DH2:C/Purge',0
'DH3:C/Purge',0
'HD0:C/Purge',0
'HD1:C/Purge',0
'HD2:C/Purge',0
'HD3:C/Purge',0
'DF0:C/Purge',0
'DF1:C/Purge',0
'DF2:C/Purge',0
'DF3:C/Purge',0
'DH0:S/User-Startup',0
'DH1:S/User-Startup',0
'DH2:S/User-Startup',0
'DH3:S/User-Startup',0
' HD0:S/User-Startup',0
'HD1:S/User-Startup',0
'HD2:S/User-Startup',0
'HD3:S/User-Startup',0
'DF0:S/User-Startup',0
'DF1:S/User-Startup',0
'DF2:S/User-Startup',0
'DF3:S/User-Startup',0
'DH0:S/Startup-Sequence',0
'DH1:S/Startup-Sequence',0
'DH2:S/Startup-Sequence',0
'DH3:S/Startup-Sequence',0
'HD0:S/Startup-Sequence',0
'HD1:S/Startup-Sequence',0
'HD2:S/Startup-Sequence',0
'HD3:S/Startup-Sequence',0
'DF0:S/Startup-Sequence',0
'DF1:S/Startup-Sequence',0
'DF2:S/Startup-Sequence',0
'DF3:S/Startup-Sequence',0


Name/Size of the new opened window:

'con:70/64/500/128/ Antipirat/NOSIZE/NODRAG/NODEPTH'

Text written in this window:

"Friend of Terminator is there !!!"
"ANTIPIRAT"
" Power of Destroying !!!"
" My ultimate answer against all the fucking"
" softwarepirats !"
```

```
" Hi Anatol,Cycledom,Primitive,Björn,Dead Homer, Brian, "
"    Gigant,Termination 8,Hardball & Slimeck"
" Worked on all available devices...!"
" Ready..."
```

The following files will be manipulated on the devices:


```
'.INFO'
'DISK.INFO'
```

The following string will be added to the sequences:

```
'Run >NIL: Purge'
```


Text at the end of the installer:

```
'FUCK=YES'
```


                              Detection tested 19.09.1994.

1.12 Fileviruses, Linkviruses, Trojans and Disk-Validator Viruses...

```
                The following viruses will be detected by Virusworkshop :
--------------------------------------------------------
```


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



```
        -z-Speed.lha~Virus

        $4EB9~Files

        6661~Formatter~trojan
                Acid Infector 1.5

        /X~Fucker~Linkvirus

        Ablank11 Trojan

        AmosAGA~Trojan

        Ahkeym-Trojan
```

```
            AAA~Enhancer~Bomb

            Addy099~Trojan~+~Installer

            ATARI

            A.I.S.F.~Virus

            AmiPatch10
                    Amiga Knight

            Alien~Trojan~Horse

            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)
                    Aibon~Installer

            AmiExpress~(ZK3.20)~Virus

            BURN~Virus~1+2
                    BBS Traveller linkvirus
Blied6

            B.E.O.L.~linkvirus
                    BGS9 5 Versions
Bret_Hawnes
Byte Parasite 1-3

            BlueSky1 (same as FLT-1996)
                    BlueSky2 (same as all the TP5 trojans)
Butonic.virus

            Bloody.Exe~Conman~1995~Installer
                    Butonic1.31

            Cryptic~Essence~Linkvirus

            COP~Trojan~Typ~A-F

            Biomechanic~Trojan

            BIO-Warn.lha~(Biomechanic~Trojan)

            Butonic3.00
```

```
            Creeping~Eel~Installer

            Cascade~2.1~Installer

            Commander~Linkvirus

            CED~4~(COP~Typ~B~Trojan)

            ComKil16~Trojan~(WireFire)

            ConDom1.5~trojan~(DaJoker)

            CheckMount~Trojan

            ConMan1995~Linkvirus~+~Installers
                    Conclip Trojan
CCCP

            Creator~V1.0~and~V1.1~trojans
                    Centurion (Smilie Cancer) 1-2

            Copy_LX~1.03~Trojan

            Compuphazygote
                    (12 different types !)

            CCHack~AmiExpress~Trojan
                    Crime
Crime++ (created by Driveinfo!)

            Christmas

            Crime92~1+2+3
                    Challenger_Trojan
Chaos Master 0.5

            Commodore
                    ConMan HD Faker + ConMan KeyM

            ConMan(Dir~Virus~Installer)

            ConMan(Dir~Virus)

            ConMan(LoadWB)+~Installer

            ConMan(LoadWB)+~Installer2

            ConMan(ARTM~2.3~fake)

            ConMan(World-Clock~1.16)

            ConMan(Hack)~Trojan~+~installer

            Combo~Loop~Trojan

            COP-Quarterback
```

```
          COPKIller~1.1~trojan~(COP~Typ~E)

          CLP_WOW.exe~Virus

          ComaVirusMaker

          DaJoker~Trojans

          Dlog~1.8

          Dialer~2.8g

          Dark~Avenger~Link~Virus~A+B
                  DiskVal1234
    DayDream 1.20 + DayDream 1.20 Server

          Devil-Zine10~BBS~Hacker

          Devil-VScan~AmiExpress~hacker

          Decompiler~Virus

          DeTag063 Trojan

          DemoManiac 2.19 Trojan

          Doom~Installer+Trojan

          Degrad~Trojan

          Diropus

          Debugger~Virus

          Digital~Dream~Installer
                  Darthvader1.1

          Disktroyer~V2.0~Virus

          Description~4.0~Virus

          Disksalv~3.01~Loader~Fake
                  DriveInfo
    DMV05.exe (see at the COP section)
    D-Structure a-c

          DAG~Installer
                  disk.info_defekt
    Disktroyer_V1.0

          DMS~2.13~Trojan

          DMS~2.06~Trojan
                  DisasterMaster2

          DisasterMaster2~Installer
```

```
            Excreminator_1

            Excreminator~Installer

            Express2.20

            Easy-E~BBS~trojan

            East~Star~Installer

            ELENI!~Installer

            Ebola~Linkvirus
                    Ebola-II linkvirus
EMWurm Logic Bomb!
ExHack Trojan

            FLT-1996 Trojan (same as BlueSky1)

            Fileghost~Virus~Installer

            Fileghost~Virus~Installer-II

            Fileghost~LinkVirus~I+II

            Fileghost3~Linkvirus

            Future~Tracker~Trojan
                    Freedom-FileVirus

            G-Zus~Packer~Bomb

            GVP-HS15.lha~Trojan
                    Gotcha_Lamer_Bomb!
Gotcha_Lamer_Bomb! Installer
Golden_Rider

            Gath95-!~(Achtung.exe)~trojan

            Hitch-Hiker 1.10 linkvirus

            HD~Toolbox~40.9~Trojan~(WireFace~Typ~C)

            Happy_New_Year_96 linkvirus
                    Infiltrator Link Virus

            Illegal~Acces~Linkvirus
                    Installer of Datalock

            Invader linkvirus

            IStrip~2.1~BBS~Trojan

            Infected~Diskrepair

            Infected~WhiteBOX
```

```
           IRQ.LINK 1+2

      Icon~(Depth~1.3)~Trojan

      JiZAnsi~1.2~Gagvirus

      Karacic~Trojan

      Kef_Ani.lha~Virus

      KAKO~Loadwb~Virus

      KidCurry~Trojan
            lamerVirusX
LSD-WHVO Trojan

      LSD-AEC1~Trojan~(AmiHacker~=~WireFace~Typ~D)

      LHA30~(COP~Typ~B~Trojan)
            LAMER_Trojan_Horse (Lamer LoadWB)

      LoadWB~Intel~GAG
            liberator.LINK (Memcheck 3.0)

      LZX~1.20T~(WireFace~Typ~C)~Trojan

      LZX~1.20T~Bugfix~(Biomechanic~Trojan)

      LZX~1.30~Trojan~(COP~Typ~F)

      LHA~Check~1.1~BBS~Trojan

      Liberator~5.01~Virus

      Liberator~3.0~Virus

      Lamerfry~1.3b~Virus

      LamerKiller~Virus

      LZ~Virus

      Labtec~Trojan

      Look!~BBS~Trojan

      LHA~V3~BBS~Trojan
                LamerExe
LamerExe TNM crunched

      LSD_Ae42.lha Trojan

      LZX~1.25~Trojan~(COP)

      Leviathan

      Lummin~Virus
```

```
M_Chat~Virus

Megalink

Master-WHO~/X~Backdoor

Merry.Exe~/X~BBS~Virus

Menems_Revenge~1+2

Mount

Mount-972~linkvirus~(=B.E.O.L.~linkvirus)
        Modem Virus Bluebox!

Modemcheck~Virus~Loadwb

Modemcheck~Virus~Installer
        Metamorphosis

M-HAC~ConMan1995~Installer

Infected~MuiGui

MST-Vec~Formatter~Viruses
        MsgTop

Mongo09.exe

Mongo05.exe
        NOGURU

NewMCI

NewAge
        NightMare (Filecheck)

Nano~][~Virus

NANo

NANo~][

NAST

NComm~3.2~Trojan~(NComm3.2-Cop~Typ~A~Trojan)

Phantom linkvirus

PStats

PHA-1994.exe

Pam-S Trojan
        Powerpacker 3.2 Logic Bomb!
```

```
              PB-Party Trojan

              PDY-SG~Installer

              Purge~Virus+Installer

              Polyzygotronifikator~Link~Virus

              PP~Bomb~Clone~(DIED)

              PP~Bomb~Clone~(Megamon)

              PP~Bomb~Clone~(MMaster~1.7)

              Promoter1~Virus~(DV)

              QRDL~V1.1

              Rastenbork~Installer
                      RetLamer
      RevLamer 1+2

              Revenge~of~NANO~I+II
                      Rob-FILEVIRUS

              Rootformatter-DV

              Red~October~1.7~Linkvirus

              Saddam~Diskvalidator~Virus~1-10

              Swiftware~0.98
                      Sepultura

              Scanlink~(Wireface~Typ~B)~Trojan

              Surprise~Virus

              Sumpf~Gag~Code

              Scansystem~Trojan

              SeekSpeed~Trojan

              Sepultura~2.26~Virus

              Susi Drive Stepper

              Stockmarket~Virus~(?)

              SS~Skid~Row~bomb
                      SCA Dos Kill Virus

              Show~Sysop~BBS~Trojan

              Sensible~Golf~HD~Installer
```

```
           Swifter 2.5 Trojan


           Super Nova Viruskiller


           Strange Atmosphere linkvirus
                   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


           TRSi-MEM.lha~Trojan~(IconD+Biomechanic)
                   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


           TRSi-INS~fake~trojan


           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


           VCKey110~Trojan


           VCS-I+II~Installer
                   VirusTest(TimeBomber)


           VMK~3.00~Trojan
```

```
                    Vtek22~linkvirus~Typ~A~+~Typ~B~+~installer

                    VirusMaker~1.0

                    VirusZ_II~1.02~fake~virus

                    VirusHunter~Joke

                    VirusChecker~6.4~Fake~Virus

                    VirusChecker~6.60~Fake~Virus

                    VirusWorkshop~5.0~Trojan
                            VirusBlast.2.3!
            Virus_Test_Bomb_936
            VTerminator
            WVT Trojan (LSD-WHVO)

                    WireFace~Typ~C~Trojan

                    WireFace~Typ~G~Trojan
                            Xeno
            XCopy65E
            XPRZSPEED3.2 Trojan horse
            XRipper

                    XACA~Virus

                    Zapa~Adder

                    ?~No~Name~?~+~Installer~
                            --- 314 Link/Trojan/Validator Viruses ---
```

1.13 Hitch-Hiker 1.10

```
Entry...............: Hitch Hiker 1.10
Alias(es)...........: none
Virus Strain........: -
Virus detected when.: 18.05.1996
            where.: Austria, Finland
Classification......: Linkvirus,memory-resident, not reset-resident
Length of Virus.....: 1. Length on storage medium:    ca. 1700 Bytes
                    (uses a primitiv polymorphic technic)
                    2. Length in RAM:                  3000 Bytes


-------------------- Preconditions ---------------------------------


Operating System(s).: AMIGA-DOS Version/Release.....: 2.04 and above (V37+)
Computer model(s)...: all models/processors (MC68000-MC68060)


-------------------- Attributes ------------------------------------


Easy Identification.: none


Type of infection...: Self-identification method in files:
```

```
                        - none

                        Self-identification method in memory:

                        - searches for $ABBAFAb4 at LastAlert(Exec)

                        System infection:
                        -  infects the following functions:
                           Dos LoadSeg(), Dos Write()

                        (librarychecksum will be recalculated)

                        Infection preconditions:
                         - Device must have more than 8000 sectors and
                           is smaller than $20000 bytes or file is
                           bigger than $8000 bytes
                         - HUNK_HEADER and HUNK_CODE are found
                         - device is validated
                         - 10 free blocks on the device
                         - hunk_code must contain the same
                           length as in the header.
```

Infection Trigger...: Accessing files via LoadSeg() or Write()
                      Files containing a "." or a "-" will be not
                      infected.

Storage media affected:
                      all DOS-devices

Interrupts hooked...: None

Damage.............: Permanent damage:
                      - none
                      Transient damage:
                      - none
Damage Trigger......: Permanent damage:
                      - none
                      Transient damage:
                      - None

Particularities.....: The crypt/decrypt routines are partly aware of processor
                      caches. The cryptroutine are non polymorphic and only
                      consists of some logical stuff. The virus uses some
                      special things at the fileinfection (buggy) and at the
                      library opencode.

Similarities........: Link-method is comparable to the method invented with
                      the infiltrator-virus.

Stealth.............: no stealth functions found

Armouring...........: The virus uses only a single armouring technique to
                      confuse people. It only crypts it's code and uses
                      a very simple length polymorphism code. The heuristic
                      scanner of VirusWorkshop detects this one already

as virus.

Comments............: The first infected file is probably lzx121crk.lha.
                      This is the old SHOOT version of LZX1.21r with the
                      infected file. As I got reports from Austria and
                      Finland, I suppose it has gone through internet
                      channels as this file didn't appear on scene boards.

------------------- Agents ---

Countermeasures.....: VW6.1
above Standard means......: -

------------------- Acknowledgement ------------------------------------

Location............: Hannover, Germany 19.05.1996.
Classification by...: Markus Schmall and Heiner Schneegold
Documentation by....: Markus Schmall (C)
Date................: May,19. 1996
Information Source..: Reverse engineering of original virus
Copyright...........: This document is copyrighted and may be not used
                      in any SHI publication

==================== End of Hitch-Hiker 1.10 =========================

1.14 Ebola-II = BBS Traveller linkvirus

Entry...............: BBS Traveller Virus
Alias(es)...........: Ebola-II
Virus Strain........: -
Virus detected when.: 17.04.1996
            where.: Germany
Classification......: Linkvirus,memory-resident, not reset-resident
Length of Virus.....: 1. Length on storage medium: 1536 Bytes
                      2. Length in RAM: 12000 Bytes

------------------- Preconditions --------------------------------------

Operating System(s).: AMIGA-DOS Version/Release.....: 2.04 and above (V37+)
Computer model(s)...: all models/processors (MC68000-MC68060)

------------------- Attributes ---

Easy Identification.: none

Type of infection...: Self-identification method in files:

                      - Searches for $ab1590ef at the end of the first Hunk.
                        (this longword comes from the EBOLA-I virus)

                    - Searches for $24121996 at the end of the first hunk
                       (selfrecognition)

                    - Searches for $1080402 at the end of the first hunk
                       (this is the recognition of the Strange Atmosphere
                        linkvirus)

                    Self-identification method in memory:

                    Searches for $3D385E29 at offset -6 from the Dos LoadSeg()
                    function.
                    If $1020304 will be found at this position, the destruction
                    counter will be manipulated (somekind of test for the
                    programmer of this virus ?)

                    System infection:
                    - non RAM resident, infects the following functions:
                       Dos LoadSeg(), Dos ReadARGS(), Exec Findname(),
                       Exec Findtask, Exec SetFunktion() and Exec Addport()

                    Infection preconditions:
                     - File to be infected is bigger then 2600 bytes and
                       smaller then 290000 bytes
                     - Device must have more than 6000 sectors
                     - First hunk contains a $4eaexxxx command in the 16
                       bit range to the end of the file (test for the first
                       entry)
                     - the file is not already infected (the at long of the
                       end of the hunk)
                     - HUNK_HEADER and HUNK_CODE are found

Infection Trigger...: Accessing files via LoadSeg()
                      Files starting with "v","V","." or "-" will be NOT
                      infected.

Storage media affected:
                      all DOS-devices

Interrupts hooked...: None

Damage.............: Permanent damage:
                     - Formatting the drive
                     Transient damage:
                     - none
Damage Trigger......: Permanent damage:
                     - Formatting the drive, when an internal counter reaches
                       5000.
                     Transient damage:
                     - None

Particularities.....: The crypt/decrypt routines are partly aware of processor
                      caches. The cryptroutine are non polymorphic and only
                      consists of some logical stuff. The virus uses some

```
                            simple retro technics to stop viruskillers searching
                            for itself.

Similarities........:       Link-method is comparable to the method invented with
                            the infiltrator-virus. Damage routine is taken from the
                            Strange Atmosphere linkvirus. The virus is a typical
                            mixture from the EBOLA and the Strange Atmosphere
                            linkviruses. We think that all 3 ones come from the
                            same programmer, probably in the east or north of
                            Germany.

Stealth.............:       If the viruskiller VT up to version 2.82 will be started,
                            the virus removes itself completly from memory. If one of
                            the following programms will be found in memory, no link
                            try will be started:

                            SetFunktionManager
                            VirusChecker
                            VirusZ_II
                            SnoopDos
                            SnoopDos 3
                            VW-Save!

Armouring...........:       The virus uses only a single armouring technique to
                            confuse people. It only crypts it's code based on the
                            position of the rasterbeam.

Comments............:       The name EBOLA is the name of a virus, which humans
                            can get infected with. CARO rules say, that no names
                            of persons etc. may be used to call a virus, but I
                            spoke to other persons and they already recognized
                            this virus in this way. The virus contains the string
                            "BBS Traveller", but this is just a clone from the
                            EBOLA linkvirus with some enhancements.



-------------------- Agents -------------------------------------------------

Countermeasures.....: VW6.1 beta
above Standard means......: -

-------------------- Acknowledgement ----------------------------------------

Location............: Hannover, Germany 19.04.1996.
Classification by...: Markus Schmall and Heiner Schneegold
Documentation by....: Markus Schmall (C)
Date................: April,19. 1996
Information Source..: Reverse engineering of original virus
Copyright...........: This document is copyrighted and may be not used
                      in any SHI publication

==================== End of BBS Traveller Virus =============================
```

1.15   Pam-s = Pamela Script trojan

```
Pam-S (Pamela Show) Script trojan
---------------------------------
```

This is a very simple trojan. Executed via Startup-Sequence (will be
detected and deleted by VirusWorkshop), a format command will be
activated. This format command is a little bit modified, so that
other keywords are accepted. This was probably done to irritate the
user.

The trojan seems to be appeared first in the netherlands, since
a member of Virus Help Team NL first complained about the missing
recognition in several viruskillers.

PLEASE NOTE: WHAT EVER YOU WANT TO DO, DO IT. BUT PLEASE REMEMBER,
THAT I DON'T GET SUPPORT WITH VIRUSES FROM VIRUS HELP TEAM NL.

1.16   Strange Atmosphere linkvirus

```
Entry...............: Strange Atmosphere
Alias(es)...........: SA Virus
Virus Strain........: -
Virus detected when.: 2/1996
            where.: Germany
Classification......: Link virus, memory-resident
Length of Virus.....: 1. Length on storage medium:      1232 Bytes
                      2. Length in RAM:                 $2710 Bytes


------------------- Preconditions -----------------------------------

Operating System(s).: AMIGA-DOS
Version/Release.....: 2.04 and above (V37+)
Computer model(s)...: all models/processors (MC68000-MC68060)
                      Caches may cause problems during the decoding
                      process

------------------- Attributes --------------------------------------

Easy Identification.: None


Type of infection...: Linkvirus

                      Self-identification method in files:
                      -  Searches for $1080402 at the end of the first
                         codehunk


                      Self-identification method in memory:
                      -  Checks for $3d385e29 at position -6 of the
                         LoadSeg() adress

                      System infection:
                      -  RAM resident, infects the LoadSeg() DOS function
```

```
                              – DoIO() exec function and Coolcapture will be
                                infected only under special conditions

                              Infection preconditions:
                               – File to be infected is bigger then $a28 bytes
                               – The file is not already infected
                               – HUNK_HEADER and HUNK_CODE are found
                               – HUNK_HEADER structure is valid
                               – There must be 4 free blocks on the disc
                               – File is shorter than 290000 bytes
                               – The lenght of the first hunk must be exactly the
                                 same as written in the hunkheader structure
```

Infection Trigger...: Accessing the file

Storage media affected: all DOS-devices

Interrupts hooked...: None

Damage..............: Permanent damage:
                       – Files will be trashed (depends on the Rasterbeam)
                         Devices will be overwritten (depends on the Rasterbeam)
                       Transient damage:
                       – System gets locked while reset and a new copperlist
                         will be shown. This copperlist then shows you the german
                         flag.

Damage Trigger......: Permanent damage:
                       – Internal counter
                       Transient damage:
                       – Internal counter

Particularities.....: The crypt/decrypt routines are not aware of processor
                       caches. The installer code in several files is working
                       correct with higher processors. The linkcode checks for
                       correct length of the first hunk to remove problems with
                       extra ordinary packers.

Similarities........: Link-method in the executable files is the simple "link
                       behind the first hunk" method without any special tricks.

Stealth.............: The viruses uses normal dos commands (no tunneling
                       via packets) and normal DOS call watchers like SnoopDos
                       can proof the infection behavior.
                       There are no stealth routines build in.

Armouring...........: The virus is only one armouring technique to protect
                       it's code. It uses a normal crypt routine to hide
                       the viral structures. Heuristik checkers like the one
                       in VirusWorkshop can find the dangerous parts and VW
                       gives you the rating "Virus!".

Name................: In the crypted part there is the following string:
                              '–+* Strange Atmosphere [gOOd] *+–'

                       If the internal counter reaches 50, the word "gOOd" will
                       be replaced by "eVIL" and the destructive code will be

```
                                activated.
```

```
-------------------- Agents ---------------------------------------------
```

```
Countermeasures.....: VT 2.81, VW6.0
Countermeasures successful: All of the above
Standard means......: -
```

```
-------------------- Acknowledgement ------------------------------------
```

```
Location............: Hannover, Germany 04.03.1996.
Classification by...: Markus Schmall and Heiner Schneegold
Documentation by....: Markus Schmall
Date................: March 1996
Information Source..: Reverse engineering of original virus
Copyright...........: Markus Schmall
Special note........: Virus Test Center Hamburg and Virus Help Team DK
                      are strictly allowed to use this analyse in their
                      own productions. All other groups/institutions may
                      please contact me first.
```

```
==================== End of Strange Atmosphere Virus ====================
```

1.17 ablank11

```
        ABlank11 Trojan:
        ----------------

        other possible names: KUK Crew Trojan

        Length: 1056 bytes (PP40 lib) or 1352 bytes unpacked

        Nothing tricky at all. It will be tried to initialize SYS:
        again and then to create several files (and dirs) on the
        device. Code isn't that good written, equalities to existing
        trojans can be found, but I cannot remember which one exactly.

        Thanks must go to Jan Andersen for sending me this one.

        Visible texts in the unpacked file:


         '> KUK CREW < A New and Evil Group has come t'
         'o spread TERROR and DESTRUCTiON to the Amiga'
         ' Scene! HAHAHAaaaaaaaaaaah',0
         'dos.library',0
         'SYS:',0,0
         'KUK_CREW!',0
         'KUK_CREW!:Haha!',0
```

```
'KUK_CREW!:Mr.Fitta_%ld',0,0
'KUK_CREW!:Dr.Klitta_%ld',0
'KUK_CREW!:Kuk+Fitta=Barn_%ld',0,0
'KUK_CREW!:Kiss&BajsÄrNice_%ld',0
```

1.18 LHAV3

```
                LHA V3 Trojan horse:
-------------------

Filelength 54440 bytes (unpacked)

This file will be spreaded as new LHA V3.00 version. It's a
simple 1.38e release...

This is the same mailbox hacking code as in the
        viewtek22
          (vtek22-
virus) installer. It seems to copy the userdatas and boxparameters
to the private directory from a special user.

This special user was at the upload time in holidays and cannot
be the author. This means that the account was hacked...

In the last time several boxes in the region Hannover got hacked, I
think that there is somekind of connection.

Probably against: FastCall

(Sysops, please call me, I need some information about it ! Thx)



'dos.library'
'S:HauptPfad'
'User/SysOp/UserDaten'
'BoxDaten/BoxParameter'
'User/Snoopy/.INDEX'
'User/Snoopy/.TXT'
'Absender  : xxxxxx'
'Betreff   : Dies ist ein Test'
'Datum     : 10.03.1994'
'Uhrzeit   : 20:50:58'
'Bytes     : 1024'
'Empfänger : Snoopy'
'10.03.1994 20.50.58    1 Asc Snoopy        '
'    Dies ist ein Test'


                                Detection tested 19.09.1994.
```

```
       Information to the
              Vtek22~Virus
```

1.19   VMK30

```
                  Virus Mem Kill 3.00 Trojan horse:
       ------------------------------
```

```
       Archivname: vmk30.lha
       Filename:   vmk
       Filelength: 2620 bytes (unpacked)
       File_ID.DiZ:VirusMemKill 3.00
```

```
       This is a fucking HD formatter and nothing else.
```

```
       The programm will open scsi.device at unit 0 and
       loads the RDB. It will add 1 to the third longwort
       and decrease the offset $2b of the RDB. If this value
       reaches 0, the first 100kb from your HD ,starting with
       the RDB, will be formatted using memory from adress 0.
       No rescue for the DATA is possible. Sorry. Try to restore
       the RDB and to rescue as much files as possible
       (best with DiskSalv 11.xx). The first 100 KB are lost and
       the partition datas, too. Try your harddisc software and
       restore the partition datas.
```

```
       The offset $2b in the RDB describes some of the hardware-
       abilities of the harddisc.
```

```
       The archive appeared 03.09.1994. on german and american
       mailboxsystems and on 05.09.1994. it was on nearly every
       better BBS. We published a Z-Netz warning and an ordinary
       warning text on 04.09.1994. to warn the people.
```

```
                                 Detection tested on 05.09.1994.
```

```
              Visible~texts~in~the~file
```

```
              The~document~from~the~vmk3.00~file
```

1.20   DM2INST

```
       Disaster Master 2 Installer:
       ----------------------------
```

```
       Filelength 10634 Bytes unpacked
```

This is said to be a little Intromaker, but in real it installs
using df0:s/startup-sequence a new filevirus. It will write a file
called CLS and in the Startup-Sequence you then can see "cls *"
as the first line.

The programm opens a window with the name

"Little Intromaker 1989 by TCR V1.00"

No vectors are changed !

                            Detection tested 22.05.1995.

1.21 VirusWorkshop (C) by Flake/TRSi`95

                                       VirusWorkshop

                    A Tristar & Red Sector inc. production
                                  in 1995 !
                          coded by Markus Schmall

       List of all known virus, which VirusWorkshop recognizes.

    PLEASE NOTE: IT'S NOT ALLOWED TO COPY VIRUS-ANALYSES 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.
    (Take a look at their VirusBaseCatalog, it's great ! Good work,
            Soenke, Karim and the rest from your team !)

    To be more exact: The VTC catalogue can contain some of my
    analysises. if you copy my analysises from the CMbase programm to
    your own production, this is NOT allowed.

            LINK/TROJAN/FILE~Viruses

            ~~~Bootblock~Viruses~~~~
                    What is "Intel Inside" for a lable ? A warning lable !

1.22 vmkdoc

Virus Memory Kill V3.00 © Chris Hames. (2620 Bytes) 19.04.1994

(REMEMBER! no virus can copy itself to a write-protected disk.)

This utility is different to the previous version in that it no longer
directly detects any virus. Instead it is now the most powerful tool for
detecting new viruses. It checks a heap of things that viruses use and tells
you when they have changed.

Firstly it checks CoolCapture, ColdCapture, WarmCapture, KickTagPtr
and the KeyboardReset to find anything that is trying to survive reset. If
any of these are abnormal it will alert you including a display of the area of
memory that they are pointing to. You can look for words describing was the
thing is and then decide whether to do nothing or do a cold reset(note this is
much more that just a normal reset) which should clear memory of the virus.

Secondly it checks the jump tables of all resident libraries, devices
and resources and warns you if any are not pointing to ROM. It will give you
a message describing what isn't pointing to rom and where it is actually
pointing. Most systems will get at least a few of these warnings. Setpatch
causes a few and ther legit programs do as well.

Thirdly it check for harddisk viruses. As you know some of new viruses
links to other programs. This is a new in VirusMemKill. I also added some new
features for OS3.0 but VMK STILL WORKS WITH OS1.3 !!! So as you can see VMK is
the best (I think) early virus detector for Amiga.

FOR PEOPLE WHO DON'T UNDERSTAND A WORD I AM SAYING:-

This program is very technical I agree but a general user can just
have it in their startup-sequence and notice the messages it gives. If they
change and you haven't changed your system get the latest best Virus
Killer(One that checks your disks and files) and run it to check out your
system.

ALERTS THAT ARE CAUSED BY LEGIT PROGRAMS

Please note some legit programs will cause alerts.

If a Alert/Warning is being caused by a standard workbench program or
kickstart version provide me with details and I will hopefully add it to the
list of legit patches.

Stopping Alerts/Warnings that are caused by legit programs:-

You can stop a alert/warning by giving the full cause of the alert
which is best idea

eg   -$01E(graphics.library)=$66666666 eg   KickTagPtr=$77777777

You can stop a alert/warning by giving the full cause without the
of the alert which is second best idea

eg   -$01E(graphics.library)

You can stop a alert/warning by giving just the description of the
of the alert which is the worst idea

eg   KickTagPtr eg   (keyboard.device)

Usage: VMK -cas alerts

        -c will cold reset(this should kill any virus from memory)
        -a will make library/devices/resources warnings into alerts
           with memory display.
        -s use strict mode where common changes (like setpatch stuff)
           is not ignored.

Examples of use:-

VMK -c   ; Resets your machine safely!!
                    ; (Should kill ANY virus from memory)

VMK -s -a   ; Very strict. Alerts for everything. I have this as
                    ; the first command on my kickstart 2.0 startup-sequence

VMK -a   ; Not as strict. Alerts for everything. I have this
as
                    ; the first command on my kickstart 1.3 startup-sequence

VMK KickTagPtr   ; Stops alerts about the KickTagPtr

VMK KickTagPtr=$00000700   ; Stops the specific alert at this location

VMK (dos.library)   ; Stop all warnings/alerts about the dos library

VMK (dos.library) -$01E(graphics.library)   ; no dos &
                                            ; no -$01E graphics alerts

If you find a new virus send it to:-

Erik Lovendahl Snaphanevej 10 4720 Prst Denmark

Contact the above address for more information on a $1000 REWARD for
information about virus programmers.

History: 10/ 6/91 V1.0   First release 13/10/91 V1.1   VMK now
knows about most versions of RAD: and most proper
                routine patches. ie you should now be able to put VMK
                as the first thing in your startup-sequence with
                kickstart 1.3 without getting any warnings. 12/ 8/92 V2.1
Some addons for new viruses 19/ 4/94 V3.0 OS3.0 !!! New things added but VMK
still works under OS1.3
                 and 2.0. VMK detect link viruses (usefull for harddisk
users)

        This program is provided "as is" without any warrenty or guarantee it

will do anything. All use is at your own risk.

Bye,
        Chris Hames (Available for any Amiga work)

        Internet: bytey@phoenix.pub.uu.oz.au
                          ins760z@monu4.cc.monash.edu.au

        FidoNet: 3:633/353

1.23 Visible

```
             '-$006(scsi.device)',0
             '-$228(exec.library)',0
             '-$1C2(exec.library)',0
             '-$1BC(exec.library)',0
             '-$1B6(exec.library)',0
             '-$19E(exec.library)',0
             '-$192(exec.library)',0
             '-$0C6(exec.library)',0
             '-$03C(graphics.library)',0
             '-$114(intuition.library)',0
             '-$0DE(exec.library)',0
             '-$09C(exec.library)',0
             '-$06C(exec.library)',0
             '-$018(disk.resource)',0
             '-$012(disk.resource)',0
             '-$05A(layers.library)',0
             '-$0DE(dos.library)',0
             '33mVirusMemKill V3.00 © Chris Hames'
             'ColdCapture',0
             'CoolCapture',0
             'WarmCapture',0
             'KickTagPtr',0
             'KeyReset',0
             'VMK found '
             '                                        '
             '                      .',0
             'Press LEFT mouse button to COLD RESET(Cl'
             'ear).  RIGHT to DO NOTHING.',0
             'RAW:10/20/440/150/VMK',0
             'keyboard.device',0
             'dos.library',0
             'intuition.library',0
->           'scsi.device',0              <-
```


        I have compared the old V1.10 of Virusmemkill and the only
        signifikant , visible change in the ascii text was, the the
        marked position not existed in the old released.

1.24   Alien_Trojan

```
Alien Virus:
------------


Filelength:596 unpacked
            1016 packed with powerpacker (this file was spread)


   Other possible names: Elien_virus_checker 0.1



This is a quite simple trojan, which is really not worth the
lines I am writing here.

At first it will be tried to open the file sys:MeGaSUXX.TXT.
Then a text containing 9times "a" will be written in the file.
If the writeaccess was successful, it will be tried to write
again this 9 bytes. This loop ends, if 900000 "a" stand in the
file or the writeaccess was not successfull. After this,
you can only press the leftmousebutton and the programm exits.

Better play with your joystick and don't code such a shit !

Visible texts at the end of the trojan:


        'dos.library'
        'sys:MeGaSUXX.TXT'
        'aaaaaaaa'
        '$VER:Elien_virus_checker v0.1 by zupa/T.L.X.'



                    Detection tested 24.08.1994.
```

1.25   Decompiler

```
Decompiler Virus:
-----------------

Written in AMOS

Filelength: 53990 bytes unpacked


This is a typical trojan probably spreaded as an AMOS
utility, which should be able to make a selfwritten
programm autobootable.

If you start the programm, sometimes it will appear a black
screen with red letters on it. If you then press the return
key, the directories "libs", "devs" and "fonts" will be
```

renamed. All directories will be renamed to their original
name plus an empty char.

If VirusWorkshop has detected this virus, please check your
disks for a renamed directory or so...

                         Detection testet 18.08.1994.

Comment 11.12.94.: Two viruskillers recognize a lot of normal
AMOS files as Decompiler infected. I hope this will be fixed
at one of the following updates, but I am not sure about it.

1.26 East-1

East Star Installer:

Filelength: 8340 bytes

This programm claims to be the Lazze_Zidens_Modem_Commander_V1.0,
but contains an installer for the East Star Bootblockvirus. The
$3c(a7) link method was used to link a new hunk on the file
(atleast I think so)...

The East Star bootblockvirus is just a simple clone from the
North Star virus. Better play with your joysticks instead of
creating such a bullshit...

                         Detection tested 15.08.1994.

1.27 sumpf

Sumpf Gag Virus:

Filelength: 952 bytes

This is "only" a joke, which creates an alert with the following
text:

        'Warnung !! Zuviele Befehle in den Menüs! '
        'Arbeitet da ein Hard-Virus ?! '
        '!Die Schwerkraft wird zu groß...'
        'Guru while meditating :   # 0894606021 - 08150074711 '
        '>Drücke einen Mausknopf, um den Virus zu'
        ' zerquetschen ! '

After this a new $6c interrupt will be installed and some hard-
wareregisters will be changed and tested. Nothing interesting,
better play with your joysticks and nothing more.

                                    Detection tested 14.08.1994.

1.28 JIZ

JizAnSi 1.2 Gagvirus:

Filelength 22008 bytes unpacked.

This file is spreaded as new ANSI converter for the AMIGA.
Quite nice. If you start it, a little window will be opened
and the following texts appears:

Formatting cylinder xx
Verifiying cylinder xx

The programms increases the cylindernumbers. It's probably
written in GFA Basic and the creator the the virus had access
to the original source of it, because the routines are not
simply linked on it, they are implented.

Better delete the file !!!

(I don't know, if a real JizAnsi 1.2 is existing.)

Spreaded with the following FILE-ID:

  _____/_____ _____/\ _____
  ____/   _____// /   / _____ ____/
   _/   _   \/   /\   \| |\   _/
    \ | \   \/   /| /\/   /
     __ _____/_____/ |___\ __/
  <-------\/-- GL0BAL 0VERD0SE --\/--------->
  Cracked: JiZaNSi 1.2 - IFF 2 Ansi Converter
  <--->

Here the short document:

>Released on : 08-04-94
>

```
>Files enclosed
>
>JiZANSI
>JiZANSI.DOC
>
>Limitations to the picture
>
>320 * 256, 5 bitplanes, IFF ILBM (BYTERUN1 compressed)
>
>
>The more color changes per line, the bigger the resulting ANSI-file
>will get.
>
>Limitations to the conversion
>
>You can use 1 to 5 bitplanes. No limits
>
>No "most-used-color" optimization is done... use as much color 0 as
>possible produces the smallest files...
>
>Format:  IFF32ANSI IFFPicture ANSIFile
>
>
>Note: There is no business like showbusiness.
>
>
>
>Since,
>
>Twilight Trio.
```

                      Detection tested 14.08.1994.

1.29 Look! BBS Trojan

```
                 Look! BBS (AmiExpress) Virus:
-----------------------------


Filelength: 1392 (packed with
        Turbosqueezer~6.1
        =spreaded)
            1456 unpacked



This is an ordinary AmiExpress mailbox virus, which tries to
manipulate the user.data from the system.
It will be tried to open NIL: and AUX: and a little window.
If all this was ok, a short text will be shown on the window:
```

```
         "Please wait ! Loading Data "

After this it will be tried to open/load the user.data. If it
was ok, the following text will be shown:

'SORRY MISSING DATA FILE 2 ! PLEASE  REBOOT !!! '

After this a simulated GURU will be shown and a new resetroutine,
which is not exitable, will be installed in the coolcapture.


Text from the simulated GURU:

        '          FATAL HARDWARE ERROR'
        ' Error Nr. 81000 0000A   Task Nr. 00000740'



The resetroutine is an endless loop, which changes , if you
press the left mousebutton, the background color via direct
hardware access.

This virus appeared first in Berlin/West Germany and some
say that it's made by the hacker Conman...The packer used
for this trojan was used several time by this hacker and
some parts of the code look like its handwriting...



                    Detection tested 14.08.1994.
```

1.30   Poliogonifrikator Linkvirus

```
Polyzygotronifikator LinkVirus:
-------------------------------


This is a classical linkvirus, which was send to me as
a very clever virus with polymorph routine, which should
be execellent coded. To be clear: In my opinion this virus
is quite well coded, but nothing special. A work of 4 hours
to write the complete repairroutines and testing...

Works with Kickstart 2.0 and higher based on the intern patch
routines for the LoadSeg vector from DOS. No other vectors are
changed.

At the start of the virus, it will be searched for the SnoopDos
task in memory. If it exists, the virus won't start.

The virus adds no hunk to the infected file, but increases the
first codehunk. A speciality is, that the virus contains a
little workaround for problems which appeared to other viruses
with packed files (like Infiltrator), which are not 100 %
AMIGA (no need to mention C= here) conform (Imploder Library).
```

The virus itself is 1196 bytes big and the cryptroutine, which
is polymorph, is 44 bytes long. The cryptroutine is polymorph,
but only in that way, that it put between the single commands
some garbage, some registers will be used different and nothing
else. No complicated stuff like in the Crime'92 virus.

The virus searchs for the "move.l 4,a6" command and replaces
it with an ordinary jump to its own code. The virus recognizes,
if it has already infected an file or not. This selftestroutine
tests only for one single word and is not that secure. Virus-
Workshop now uses 4 longwords to detect the virus in files.

The virus identifies itself with the word 1994 in memory and
on disk. In memory it searches for "1994" and on files it
looks for $1994 (a word). As result, this virus links only one
time on a file and nothing more. The virus does not link on
other files, if the device contains less then $1f40 sectors.

The virus contains no real destruction routine and expects as
for hunk the codehunk.

In the decrypted virus, you can read:

"Don't think about it! You're simply infected with the
Polyzygotronifikator... (Polymorph version)"

This virus comes probably from Germany, because of the "k" in the
name. A english speaking coder would have written the name like
"Polyzygotronificator" instead of "Polyzygotronifikator". This is
just some way of combination, but I think this is quite
interesting (idea by Ingo Schmidt).

VirusWorkshop is able to remove a virus and the repaired file should
work 100%. Better try it with a copy, just for security
reasons.

                                        Detection tested 05.08.1994.

Comment 11.12.1994: Another viruschecker/killer appeared, which
recognizes this virus. The repairroutine does not correct the
length of the first hunk, it only reinserts the "move.l 4.w,a6"
and nothing more. VT 2.69 and VW4.5 still detect Polygonifrikator
in file, cause it is still existing there. This is the same
viruskiller, which is not able to remove and detect the Crime'92
virus correct or in general (in a time of 14 months!!!!)
Please judge for yourself, but the german viruskiller programmers
have not the task to recorrect the bugs made by other virus-
killers ! Same problem appears at Commander linkvirus ! Please
judge for yourself !

Comment 27.02.1995: If you activated Decrunch and then checked
a file, which was first packed and then infected with this
virus, it could give Enforcerhits. Fixed now.

1.31 RootDv

```
Rootformatter Diskvalidator Virus:
----------------------------------

Filelength: 1848 bytes (like an original DiskValidator)

Works only with Kickstart 1.3 based on absolute RomJmps.

The programm does not work, so the following stuff is
just a description, how the programmer of the virus wanted
to have it:

The destruction is activated at this time.

The virus only formats 5 KB beginning with block 880, which
is at a normal DD disk the rootblock. Please try to use
diskrepair to repair as much as possible. This file can be
startet and is so a danger for users of KS2.++, too.

Based on fact, that there is no spreadingroutine, there MUST
be an installer for the file.


                                    Detection tested 28.07.1994.
```

1.32 LamerKiller

```
Lamerkiller Virus:
------------------

11512 bytes long (packed with CrunchMania normal and then
                  manipulated)

-Only Kickstart 1.x ! On higher systems: Crash !


As far as I know this virus simply writes a DiskValidator
Virus (Saddam with CodeLW "IRAK") to df0: . Nothing more.



                        Detection tested 18.07.1994.
```

1.33 DOOM

```
                DOOM Filevirus:
---------------

Kickstart 1.x: probably not working based on very high DOS Jmps.
Kickstart 2.0: working
Kickstart 3.0: working
```

```
Kickstart 3.1: working
MC68040          : working

Installer: clx_doom.exe (406012 bytes packed Stc 4.10.2)

New created files:

        -sys:c/assign (3220 bytes unpacked)
         This is the original 37.4 assign command (25.5.91)
         with the linked virus. The hunklength are manipulated,
         so don't wonder about the same lenght as the
         original.

        -sys:c/copy   (5496 bytes unpacked)
         This is the original 38.1 copy command (20.05.92)
         with the linked virus.

        -sys:libs/diskfont.library (15820 bytes unpacked)
         This is the original library V39.3 (14.07.92) with
         the linked virus.
```

The original Diskfont.library is 15340 bytes long. As a result
the virus is 480 bytes long.

This file is spreaded as AMIGA DOOM by Complex. But it not even
creates some output except from the virus.

```
   File ID:


        _____  /_____  _____  /\_
       /    _____ /  \/  \____   \|-/  _____\/__/
      /     |_/    |/        /  ___/|/   _|_/     \_
      _____\  /\/\__\___|\___¯_____/\   /
       ----\/-p-r-\/s-e-n-t-s------\/---\/----\/
                    Amiga Doom!
              Coded by Gengis / Complex!
```

The main programm is extremly lame coded. A DMS file can be
found in the file, whith some Mapus banners hanging around
and some IFF sound samples. At the beginning, all texts and
some other parts will be decoded using a lame cryptloop.
Then the files will be saved and some filecomments will be
set (set "RESTICTED" to bbs:user.data & to bbs:user.key).

The DMS file was uploaded to a quite known BBS on 26.05.94.
Atleast this banner can be found in the header. Another
file is in the maincode, which is an intro. In this intro
you can read some texts from Melön Dezign.

The virus checks for higher processors and read the VBR and
installs a new interrupt in the $74 vector in the vectorpage.
This is new. Nearly all other viruses only patch the vector-
page.

This new interrupt increases a variable until it has reached

30000. As long as this value is not in the variable, it will
be tried to manipulate the $dff030 register. The $dff030 will
be only changed, if a special string , which adress will be
calculated using the SerDat register($dff018)and an internal
counter, will be found(string=$6c554e69544963210d).

I think that it is something like hacking programm or a
special programm to manipulate the datatransfer from the
serial port.

No other texts were found in the virus.

                              Detection in files tested 16.07.1994.
                              Detection in memory and removal
                                            tested 17.07.1994.

Special thanks to AtomiX x for sending this virus.

        First~warning~for~this~virus

        Statement~from~Complex

1.34 DOOM1

```
   __ _____._____:  ._____ +_/  Y _/  ! _/  ___       ¦ _/
___/------+
 \_    \____ \____ \__  __| \_  |  | mYSTiC
  |  Y  |  !  |  !  ||  | |  |  !  | -----
  l__|  l__   l__    ||  | |  l__   |  1994
+-kRml__|--\__|--\__|l__|-l__|--\__|-------+ WARNING ! A file CLX_DOOM.LHA is
a trojan !! Another warning text file from EaSy RiDeR !!
```

WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING

Another fucking virus is in file CLX_DOOM.LHA After running a file
CLX_DOOM.EXE it decompress and overwrite an infected files:

ASSIGN   – to your SYS:C dir COPY   – to your SYS:C dir
diskfont.library – to your SYS:LIBS dir

so, if you have an harddrive than it is very dangerous to you. You can't boot
your HD with these infected files. After all this shitty trojan virus doesn't
do anything more ! No other damages like HD format or something like that, but
who knows... :)

So, please NUKE this CLX_DOOM.LHA file on all boards around the globe.

                                        Signed: EaSy RiDeR/MST & TRSI

Fast greets fly to: All sysops of boards where I am – Hi dudes ! :) Thanks for
ratios ! AXE/MYSTIC   – What about you ? XTD wants your real address.
Leave me a
                 note on LAST OUTPOST with your voice number coz I lost it
JARRI – When CW will be 24 hours/day ? UFOk/MST   – Jak ci sie uklada z
Januszem ? McLoud/TRSI   – What time I can page you ? KOOL FALCO   –
Call me... what about SZALONA LINIA ?

                                    Cja next time dudes !

1.35   DOOM2

 ....
.

     _____ /_____   _____   /_
   /   _____ /   \/   ____   \|-/ _____\/__/ / |_/ |/   /   ___/|/
 _|_/ _ _____\   /\/_____|___¯_____/\   /
   ----\/-p-r-\/s-e-n-t-s------\/---\/----\/
         INFO ABOUT "CLX_DOOM.LHA"
     IT'S A VIRUS NOT A COMPLEX RELEASE!

 .... CAUTION ....

 CLX_DOOM.LHA is a fake and should not be spread, it is not a COMPLEX
 release.. it is a trjoan VIRUS which fucks up your diskfont.library
 which amiexpress and s-express uses frequently, DO NOT RUN THE EXE FILE!

                    Ozone / Complex Organizer

 .... CAUTION ....

1.36   LIB30

                    Liberator 3.0 Virus:

         Filelength: 10712

         This virus patches the startupsequence and writes itself in
         it.

         Original end of the startup:

         (40.42 Startup-Sequence)

```
Resident Execute REMOVE
Resident Assign REMOVE
C:LoadWB -debug
EndCLI >NIL:
```

Modified end of the startup:

(40.42 Startup-Sequence)

```
Resident Execute REMOVE
Resident Assign REMOVE
C:LoadWB -debug
cv >NIL:
EndCLI >NIL:
```

The tests were performed with 3 drives (SYQ= Syquest 105 MB, DF0 and DF2 as normal diskdrives).

On all 3 devices the Startup-Sequence was changed in one step. If a .fastdir file, which will be created by the virus, will reach a special value (99) , then the following text will be shown:

```
' Congratulations your hard disk has been'
'    liberated of virus protection!!    '
'  Hello from the Liberator virus v3.0  '
'          - Digital Deviant            '
'  The anti-anti-virus is here again !  '
'    Lets play trash the hard disk      '
'         and ram the disk heads        '
'  Only hardcore belgi an rave can      '
'      truely liberate the mind!        '
'             The liberator 15/01/92     '
```

...

The .fastdir was not created on DF2, but on the other devices. Startvalue from this 2 byte long file is: $310a. The virus itself was not copied, but due to the filename "cv" and the startupmessage I think that the real name is Check-Vectors:

```
'Check Vectors rev 5.1 '
'All Rights Reserved '
'more TUPperware © by Mike Hansel'
'Reset vectors ok, Nothing resident'
', Trackdisk.device not intercepted, ',0
'DoIO ok, VBlank ok, dos.library not inte'
'rcepted.'
'System appears to be free of viruses and'
' trojans!'
```

```
                           Detection retested 16.07.1994.


             DosTrace~Capture~from~the~virus
```

1.37 DT_CAP

```
Leer:        =Bootdrive (DF0)
SYQ:         =Syquest
4eb9_linker:=second drive (DF2)
L3.0         =Liberator 3.0 virus


Initial CLI: Changing current directory to "Leer:".
Initial CLI: Getting shared lock (-2) on "l3.0": OK
Initial CLI: Examining "Leer:l3.0": OK
Initial CLI: Unlocking "Leer:L3.0"
Initial CLI: Loading segmented image "l3.0": OK
Initial CLI: Getting shared lock (-2) on "l3.0": OK
Initial CLI: Getting parent of "Leer:L3.0".
Initial CLI: Unlocking "Leer:L3.0"
Initial CLI: Changing current directory to "Leer:".


This is the textwriter:

l3.0: Writing 31 bytes to "32m«Unknown Object»31m": OK
l3.0: Writing 30 bytes to "32m«Unknown Object»31m": OK
l3.0: Writing 43 bytes to "32m«Unknown Object»31m": OK
l3.0: Writing 1 bytes to "32m«Unknown Object»31m": OK
l3.0: Writing 79 bytes to "32m«Unknown Object»31m": OK
l3.0: Writing 1 bytes to "32m«Unknown Object»31m": OK
l3.0: Writing 48 bytes to "32m«Unknown Object»31m": OK
l3.0: Writing 1 bytes to "32m«Unknown Object»31m": OK
l3.0: Writing 49 bytes to "32m«Unknown Object»31m": OK
l3.0: Writing 1 bytes to "32m«Unknown Object»31m": OK


Going on with the virus:


l3.0: Getting shared lock (-2) on "DF0:": OK
l3.0: Gett
```

1.38 Lib501

```
Liberator Virus V5.01:
----------------------


Filelength: 16924 unpacked
Clones: Lamerfry1.3b
```

This virus is quity tricky. It copies the file c/run and
renames it. It adds to the shell startup the commands:

';liberatorV – controlling me!'
'alias copy delete'
'alias delete "echo *"No file to delete, cant find*""'

If you have once started once such a modified shell, then
quickly load an editor and remove the three lines. Then
reset and it should work correct again.

The startup-sequence will be directly changed so, so that
the virus will be activated every time.

If you start the virus, the following message will appear
on the window:

PV(Protect Vectors) v1.02 by Peter Stuer',0
'July 22, 1992 FREEWARE'

'Reset vectors ok, Nothing resident, Trackdisk.'
'device not intercepted, '
'DoIO ok, VBlank ok, low interrupts ok, '
'dos.library not intercepted.',0

'monitoring vectors...'
'Fully Kickstartv2.xx compatible, stops all'
' viruses, checks disk-validators,',0
'Use run to push this program into the '
'background.',0

This message is only to cheat the user, Peter Stuer has
never written this programm.

In the virus you can read the names from other viruskillers,
look here:

'ZeroVirus'
'VIRUSEXPERT'
'ZeroVirus III'
'Virus_Checker'
'Master_Virus_Killer_v2.1'
'BLVC'
'Berserker'
'BerserkerV5.0'
'Virus_Checker(C)'
'Nuke!'

(Don't know, what it's really for.)

The virus installs a .fastdir file, which contains some
kind of timer. If a special value was reached,then the

following text will be printed to screen:

'   Congratulations this disk has been liberated'
                ' of virus protection!!'
'   Hello from the Liberator virus'
           ' v5.01 - Random Disaster'
       'The anti-anti-virus is here again!'
          'Lets play trash the hard disk'
'   and ram the disk heads'
         '   The piracy curse'
         'Liberator V - The future is near.'
'Look out for Liberator VI - The final nightmare ...'
         'coming soon from a lame swapper near you!'
'   Respect to the virus masters
       Lamer Exterminator,crime & Contrast.'
    'And remember - be excellent to each other!'
              'The liberator 27/07/92'
              'Virus Generation : ',0

              Detection retested 16.07.1994.

1.39 Lamerfry13b

                  Lamerfry 1.3b Virus:

Length: 8240 bytes packed (with CrunchMania and then
manipulated)

This is a simple clone from the Liberator 5.01 and
nothing more. Please note, that we recieved the virus
from a SHI member ! The file is not decrunchable, because
the crunchmania file structure was hacked.

For more information look at the
        liberator~5.1~section
         !

   Some messages etc.:

'dos.library'
'timer.device'
':c/run'
':c/',$1A,$1A
':s/.info '
':c/'

```
's/startup-sequence'
's/shell-startup'
';Lamer Fry - Says You Die !!!',
'alias copy delete',
'alias delete "echo *"No file to delete, can't find*'
's/.info '
'.fastdir',$A0,' '
'c'
'c/'
'c/run'
'c/br'
'br c:'
'.fastdir'
':s/startup-sequence'
' .',
'BackGround_Process'
'ZeroVirus'
'VIRUSEXPERT'
'ZeroVirus III'
'Virus_Checker'
'Master_Virus_Killer_v2.1'
'BLVC'
'Berserker'
'BerserkerV5.0'
'Virus_Checker(C)'
'Nuke!'


Starttext:
   ----------


'LamerFry Virus V1.3b     '
'Written For SHI                      ',
'This Test Virus Written By
       Kooky/Calypso
         For SHI'
' Tests, This IS REAL!        Please Be Very '
'Careful When Running It!                     '
'                                               '
'                                               '
'                                               '
':.fastdir',$A0,' '
':'
':.fastdir',$A0,' '


Other text, which will be displayed later:
-------------------------------------------


'      Tough luck! Your disks have been Fried Lamer,'
'      Bad luck Looser     ',
'          As you see this virus is quite sneeky '
'isn't dudes ?!?!',
'                  Next time be more careful!!'
'                                               '
```

```
'                                                    '
'              Lamerfry V2.0 – The Future Is Near,'
'          Look out for Lamerfry 2VI – The final '
'nightmare ...',
'        coming from a lame coder like kooky soon!'
'     Greets are flying out to paul browne/shi as'
' he has the only copy.',
'                   of this virus. I don't sorry ! Be'
' Kewl....',
'                         Lamer Fry – You Die....',
'                          Reproduced Nums  : '
```

```
                        Detection tested 12.07.1994.
```

```
There was lately a
        public~~announcement
         in the  AmyNet
(Virus_Amy), saying that this doc chapter would damage
the  reputation of  Kooky/Calypso, because  I  mention
his name in the  shortcut from the  file.
        Click~me
          to
read more about it !
```

1.40   Degrda

```
Degrad Trojan Formatter:
------------------------
```

```
Filelength: 5612 bytes unpacked (including the Debuginfo)
```

```
This is the lamest trojan I have ever seen so far. It will
be tried to write using the scsi.device 5 KB to  the first
sectors of the unit 0 from the scsi device. Nothing  more.
No text and the  memory, which  will  be  written  to  the
device, is an  empty block at the end of the virus. In the
BBS description  it was  marked  as a degrader tool, which
should  enable the  user  to  let  run older programms  on
modern AMIGA system with higher kickstarts, processors and
memoryexpansions.
```

```
Even the debughunk is existing ! Lame !
```

```
This trojan appeared first in the United Kingdom.
```

```
                        Detection tested 08.07.1994.
```

1.41 VCSI

```
Virus Construction Set I Installer:
-----------------------------------


Filelength: 19452 Bytes unpacked
            10192 Bytes PP2.3 packed




If you start the file, a PAL screen will be opened and a logo
will be shown.
This is the installer of the VCS I Virus. You can enter a text
and the virus will be written to disk.

Nothing more to say, except this: The handle "Max/Starlight"
was now used for more than 4 viruses. Isn't it possible to
catch this guy ?




Visible texts in the unpacked file:
-----------------------------------

'StarLight !!S'                        <-at the top of file
'BMHD',0                       <-parts of the IFF picture
'CAMG'
'BODY'
'CMAPföP'
'BODYföP'
'graphics.library',0
'intuition.library',0
'Bild',0
'VirusMaker',0
'>FORM',0
'>ILBMBMHD',0
'CMAP',0
'CRNG',0
'CRNG',0
'CRNG',0
'CRNG',0
'CRNG',0
'CRNG',0
'CAMG',0
'BODY',0
'dos.library',0
'3m              StarLight presents:  '
'0m           Virus Construktion  Set '
'Bitte Virus-Text eingeben (max.60 Zeiche'
'er Virus-Text erscheint nach 5 Infektionen'
'dos.library',0
'intuition.library',0
'Legen Sie eine Diskette ins Laufwerk DF0: ein,'
'um den neuen BootVirus zu installieren.'
'Drücken Sie dann den linken Maus-Button.'
'trackdisk.device',0
```

```
'DOS',0
'DOS',0
'Konnte BootBlock nicht schreiben...'
'Linke Maus = Nochmal'
'NuAlles klar... Viel Spaß mit dem neuen '
'VIRUS'
```

Virus Construction Set II Installer:

Filelength: 47944 Bytes unpacked
           32360 PP 3.0 packed

This is the installer of the VCS II Virus. You can enter a text
and the virus will be written to disk. The installer simply opens
a little window and nothing more.

Nothing more to say, except this: The handle "Max/Starlight"
was now used for more than 4 viruses. Isn't it possible to
catch this guy ?

Visible text in the installer:

```
'trackdisk.device',0
'dos.library',0
'CON:40/30/550/150/STARLIGHT VIRUS CONSTRUCTION SET V2.0 !'
'3mWelcome to the STR's Virus Construction Set V2.0 !'
'Please enter the Virus-Text max. 60 Chars! :'
'mPlease enter the name of the Virus max. 20 Chars! :'
'mShall the Virus code itself ? '
'F1 = YES'
'2 = NO'
'Now insert a Disk in [DF0] to write the Virus.'
'When done press LEFT-MOUSE Button...]'
'Do you want to write the Virus again ?'
'Left-Mouse = YES   |  Right-Mouse = NO'
'DOS',0
'dos.library',0
'Nuintuition.library',0
'Some greets flies over following people/Crews:'
'Evil Chuck - Tiger 1 (back on the Amiga !) - Mailman '
'Nikita (thanx for the cool parties in '
'Heilbronn) - Lion - Prof J.'
'Zombie - Garfield (where are 'ya now) - '
'Garbor (Codename ??)'
'all spreader and swaper, who are spreading'
' this disk'
```

```
            'Darkstar - HCC - Fairlight - Trinitron -'
            ' Edward (send some DISKS!)'
            'Sepultura - Death - Iron Maden - Jairo - '
            'Max (and the baby)'
            'Andreas - Chuck - Sadus - Cynic (what'
            ' about a CD from you ?)'
            'Melon Dezign/Crystal - Devils '
            '(Colors: FUCK!) - AFL'
            'Silents - Anarchy (organizing cool parties)'
            ' - Troops of Doom'
            'The rest of Guardians (fucking incident) '
            '- Roadrunner Records'
            'Skid Row and Crack inc. - Vision - SCM of'
            ' GDW (C64 - HE HE)'
            'paceballs (Tekkno-demo is wonderful !) -'
            ' Butonic ('ya still alive)'
            'Walt/Melon (have you found the extra in '
            'the demo on Civilisation ?)'
            '........ and to all the others in the sc'
            'ene ....... (MAX 23/4/93).            ',0
            'HI TO MY LOVE !!!!!!!!!!!!!!!!!!!!!!!!!!'
            '!!!!!!!!!!!!!!',0


     ...
```

You can easily see, that the coder of the installer
has some friends in the scene and knows some guys.
It should be not so hard to find him, ask Walt for
the Civilization demo and we can catch this virus-
programmer (A work for you guys in SHI!) !!!!

1.42 IGAG

```
Intel LoadWB Gag Programm:
--------------------------

3384 Bytes unpacked

no vectors are changed. A simple joke.


This is an ordinary loadwb commad, at which was added
a little graphic routine, which tries to paint a logo
on your screen. The routine is buggy like hell.

Visible texts are:


'dos.library'
'-DEBUG/S,DELAY/S,CLEANUP/S,NEWPATH/S'
'$VER: loadwb 37.1 (16.1.91)'
'workbench.library'
'Workbench is already started'
```

```
'Error while getting path'
'Could not open Workbench'
```

                                    Detection tested 08.07.1994.

1.43 DMS213

```
DMS 2.13 Trojan (HD Formatter):
-------------------------------
```

Length: 94220 bytes unpacked

This file was spreaded as new 2.13 update from DMS.

The file_id.diz file looks like this:

```
.--------------------------------------.
| GET THE REAL THING !! DMS 2.13 UNREG ! |
|   FILE_ID FIXED FOR A4000/040 NO GURU  |
|     AROUND! , FIXED BY BONESTARR/LSD   |
`--------------------------------------'
```

But there is nothing new in this version, but a hdformatter
was implented in the code. The virus will be activated first
and tries to format the DH0 device using the normal FORMAT
command:

'format drive dh0: name FuCKoFF ffs quick'

At the end of the DMS programm, you can read thw following
things:

    '   SCeNE iS LaME - SiGNeD By RoADSTaRR/LsD'
                        'dos.library'

At the spreading date of this virus (it's dated 01-06-1994)
there was DMS 2.03 actual and DMS 2.04 was released at this
day.

Nothing more to say about this VERY lame virus !

(Eine echte technische Meisterleistung ! Hoert auf mit dem
Mist und spielt lieber mit dem Joystick !!!)

                                    Detection tested 14.06.1994.

1.44 LABTEC

```
Labtec Trojan Virus:
--------------------


Filelength:      13556 bytes          (Imploder 4.0 Library imploded)
                 28840 bytes          nonpacked
```

This is a classical trojan. The file contains a special Date-
stamp routine and a special date, the files

```
c:lha,c:zoo,sys:wbstartup/virusz and sys:wbstartup/virus_checker,
c:arc,c:loadwb,s:startup-sequence,s:user-startup,s:startupii
```

will be deleted.

The following text will be printed to screen:

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

Hi there! It's probably been awhile since you've seen on of these
-a virus! Don't worry about trying to avoid the damage, it's aleady
been done. Why didn't your virus checker catch this? Because you're
a LAMER! You like it! This should be fun watching the latest mags
and seeing how long it takes for them to document this! Hey, how
about you send in a copy of this virus? Why not? Cauz you don't
where it came from...LAMER! Have a nice day!

Lets dub this one, the Labtec virus, ok?

Press ANY Key To Go Back To DOS

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

A text saying, that the OpenScreenpatch is installed and another
text saying "NoCare2.7 by..." will be printed everytime, but
the real NoCare programm seems to be not build in the virus.

Detection tested 08.06.1994.

1.45 Creinstall

```
Creeping Eel Installer:
-----------------------


Filelength: 3212 bytes
```

This programm is a patched TYPE command. The utility HUNKLAB
was used to link the virus to the file. The BB virus will be

installed in memory using a special installer, which needs
32 Bit FAstRam. This installer is comparable to the code in
the MUiGuru and Enforcer 3760 viruses.

The version information was changed and the file will be
probably spreaded as TYPE 42.x. At this time I recieved
the virus (05.06.1994), there is , as far as I know, no
Workbench V42 avaible !

Detection tested 05.06.1994.

1.46 Casinstall

Cascade 2.1 Installer:

Filelength: 3428 bytes

This programm is a patched INSTALL command. The programm
HUNKLAB was used to link the virus to the file. The BB virus
will be installed in memory using a special installer, which
needs 32 Bit FAstRam. This installer is comparable to the
code in the MUiGuru and Enforcer 3760 viruses.

The version information was changed and the file will be
probably spreaded as INSTALL 42.x. At this time I recieved
the virus (05.06.1994), there is , as far as I know, no
Workbench V42 avaible !

Detection tested 05.06.1994.

1.47 Combo_Loop

Loop Combo Trojan:

Filelength: 1848

No vectors will be changed. It's a pure destruction programm.
It will be written as a new Disk-Validtor, as a result, there
must be an installerprogramm for this. In this special case
I need YOUR help ! Many thanks !

If you start the programm (NEVER DO THIS!) a little alert
containing the following text will appear:

'MIT MIR NICHT, DU AFFE !!!!!'
'VERSUCH' LIEBER MAL EINEN LOOP-COMBO!!'
'(ODER HASCH EIN LOCH IM'

' ZELT (ZELT IM LOCH!!)'
'ICH VERABSCHIEDE MICH DANN SCHON MAL!'

This text is crypted with a simple eorloop. If you then press
one of the mousebuttons, the real destruction routine will be
started. A kopfstep will be performed and a lot of infotmation
on the disks will be lost.

To irritate the user, at the end of the virusfile, there are
several normal strings, which can be found at the end of a
normal diskvalidator, too.

Detection tested 23.05.1994.

1.48 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...

1.49 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 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 !

1.53 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!)<752#%-'48+475UR["

        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.

Comment 22.06.1994: Due to some failrecognitions with
MICROPROSE installers, I have changed the routine a little
bit again.

Thanks must go to Control/TRSi for the hints !

                                    Detection retested 22.06.1994.

1.54 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.

          Information~about~4eb9~linkers
                  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 .....).

1.55 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.

1.56 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.

1.57 LHA 3.00 BBS Hacker

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 !

1.58 AAA-Enhancer Bomb

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):
-----------------------------------------------------------


            'SHIxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'
            'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'
            'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'
            '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 (xxxxxxxxxxxxxx) 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'
' xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'

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.
```

1.59 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.
```

1.60 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 !
```

1.61 DagInst

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

Filelength: 7360 bytes

This file installs the DAG bootblock to dfx.
```

                                                  Detection tested 2/94

1.62 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.

1.63 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

1.64 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.

1.65 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.
```

1.66 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'


      Guys ! Better play with your joystick, instead of creating
      such a bullshit !



                               Detection tested on 21.1.1994.
```

1.67 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.

1.68 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 !

_

                        __   ___ __
            /X\ | ||\ || _| |
           /   \|__|| \||__||__| 1993

                        Detection tested on 25.2.1994.

1.69 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 !

Comment 26.09.1994: The linkroutine from the BURN 2(B) virus
will be used by the viewtek22 virus (vtek22).

        Information~about~the~ViewTek22~Virus!

1.70 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  <<<<<<<
```

1.71 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.

1.72 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.

1.73 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.

1.74 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 !

1.75 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.

1.76 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.

```
                   ANOTHER FILE LEECHED FROM:


    /\____/\__  /\./\_____/\___  /\___  /\___/\  _
   _/    _/ ._// |__  __/ ( |/  _ \/    \  \/ \
   \  ø /  .  \_  :./  \.| /  |  .  \ ø__/___  /
 -=_____/__||____||____|\__|__/_|__\ )  /=-
 -=====Y=================================Y=\ /==-
       :      tRiStAR - REDSECtoR      :  Y[M1]
       . .____/_____/_____.   |  .
       ; l___/  |_____  /  _____|   .  |
         /   |  __ _/.___    \_/   |   ;  :
        _/RtX |  \    |  |  /    |    .
        \  ___|___\   |____   /\  __|
         \/   :    \__|    \/  \/
        W.O.R.L.D. H.E.A.D.Q.U.A.R.T.E.R.S.



                        Detection tested on 28.12.1993.
```

1.77 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.

Comment 11.07.1994: Finally recieved the 4eb9 linker and
analyzed it. Thanks Krzystof !

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.

        Information~about~4eb9~linkers

1.78 GHOST1

                 Fileghost Virus Installers I+II:

Filelength: 8160 Bytes (first one)
            8116 Bytes (second one)

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!!)'

Both installers activate the same virus. Nothing has changed !
After the file "dh0:c/setpatch" was found, the virus will be
activated.

Differences between the first and the second installer: The
second installer crashes at WB start, due to missing startup.

Both installers try to install the Fileghost 1 virus !

                                    Detection tested 28.12.1993.

                                    Detection retested for the new
                                    installer 08.07.1994.

        Fileghost~LinkVirus~I+II

1.79 ghost2

                    Fileghost Virus I:

Works with Kickstart 3.1 and MC68040 !

Is able to overjump symbol and debughunks at the beginning
of the file.

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". -> A virustype like Infiltrator, DA and
others.

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 Virus II:

Works with Kickstart 3.1 and MC68040

Please not, that this virus will be not installed by the
recognized Installer II !!!!

This is a linkvirus, which adds NO hunk to the infected file.
It will increase the first hunk (796 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". -> A virustype like Infiltrator, DA and
others.

The $3e8 hunks will be overjumped. Caution ! Read the DHunk
documentation !

The virus changes DOSLoadseg. No resetvectors will be changed.

Selfrecognitioncode in memory: Test for the single longword:
                          $ABCD1234

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

FileGhost 2 - Merry X-Mas and a happy new year...

```
          Fileghost~LinkVirus~Installer~I+II
                                      Detection for the Fileghost2  ←
                                          tested
                                      26.09.1994.
```

Comment 11.10.1994: As far as I know this virus is very wide
spreaded in Germany. Many PD disks are infected and even a CD
was infected and NOT released.

I have just found a bug in my memorycheck routine, which I have
now fixed. Sorry guys...

1.80 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.

1.81 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.

1.82   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.

1.83   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.

1.84 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!
        .

        Information~about~4eb9~linkers

1.85 Conman2

        ConMan
         Dir Virus:

Filelength: 4004 bytes (using TurboSqueeze 6.1" link "Document_0" 0})
          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.

1.86 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.

1.87 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.

1.88 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.

1.89 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

        ****

1.90 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.

1.91 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.

            Information~about~Jeff~Butonic~3.00

1.92 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.

1.93 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 !!!

1.94 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.

1.95 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
'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...

1.96 Commodore

Commodore Virus:

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

1.At the start of the programm the adresss $66666 will be in-
creased 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.

1.97 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.

1.98 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.

1.99 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.

1.100 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.

1.101 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.

1.102 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.

        Information~about~4eb9~linkers
                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've a list
with lengths of all the AmiExpress releases then please let me
know it.
```

```
        Information~about~4eb9~linkers
```

1.103 XACA

```
XACA Virus = Lummin Virus
```

1.104 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.

Information~about~Jeff~Butonic~3.00

1.105 Jeff3

```
Jeff-Butonic 3.00:
------------------

Filelength: 2916 Bytes unpacked

Patched vectors: DoIO from Exec and KickTagptr from Execbase
```

This is a classic filevirus. The file will be copied as one
and written with a not visible name to the directory and
at the first position of the Startup-Sequence.

After some resets, the following text will appear:
(displayed as ordinary alert)

```
'0JEFF',27,'s speaking here...'
'<(w) by the genious BUTONIC.'
'HV 3.00/9.2.89-Gen.00000'
'ZGreetings to *Hackmack*,*Atlantic*,'
'd& Alex,Frank,Wolfram,Gerlach,Miguel,'
'Klaus,Snoopy-Data!',0
```

From time to time, some of the following texts can appear on
your screen (controlled by intuition):

```
'Ich brauch jetzt Alk',27,'!'
'Bitte keinen Wodka!'
'Stau auf Datenbus bei Speicherkilometer '
'128!'
'Mehr Buszyklen für den Prozessor!'
'Ein dreifach MITLEID für Atari ST!'
'©89 by BUTONIC'
'PC/XT: Spendenkonto 004...'
'Freiheit für den Tastaturprozessor!'
'C für Looser'
'Paula meint, Agnus sei zu dick.'
'Die CPU braucht etwas Schmieröl'
'C64 - jetzt mit Pampers im 3erPack'
'JEFF=ungefährlich+schützt vor Viren'
```

Quite nice texts, or ? The infection routine is controlled
by the patched DoIO routine, which depends on a readaccess
from the rootblock.

                        Detection retested 07.07.1994.

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.
2000ad-1.exe                ; An intro from 2000AD
2000ad-2.exe                ; Another intro from 2000AD
DAGE-cra.exe                ; An intro from Dage....
```

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)
-...

Known 4eb9 link programms are:

-Minichainer 0.3 by Dr.Who
-Filechainer 1.3 by ???

                    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.

        Information~about~the~Modemcheck~Virus

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
         .

Comment 26.09.1994: A new trojan appeared, which uses the same
formatroutine to destroy data.
For more information about this 6661 Formatter :
       Klick~me
       !

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.

Comment 23.05.1994: At the end of 1993 appeared a new clone of the
PowerPacker bomb. The infected file was the ModuleMaster 1.7. The
infected file is 20364 bytes long.

Attention: The first
        4eb9~linker
         file was the PP bomb at the
PowerPacker 3.2 infected fake. This linker is now known since more
than 3 years !

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 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 (un-
packed).

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.

1.123 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
```

1.124 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.

1.125 Crime92

Crime92 Linkviruses 1+2+3:

It's the first polymorph virus on AMIGA. I am very afraid that such
viruses now appear on AMIGA, too.

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.

As far as our tests show us, we can now say, that only VT by
Heiner Schneegold and VirusWorkshop detect ALL generations from
this very dangerous virus !

                    Routines overwritten and tested 07-07-1993.

1.126 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.

1.127 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.

1.128 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.

1.129 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.

1.130 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.

1.131 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.
```

1.132 BigBen

```
Big Ben Virus:
--------------

The virus was sent me as Big Ben virus, I cannot follow the name of
this virus, it appears only a clocktime sometimes on the screen.

Kickstart 2.x and higher is required to run this virus.

Patched vectors: Exec() CoolDoIO, Exec() Findname, Exec() Replymsg,
                 Exec() Waitport, Exec() DoIO


The virus tries to read the time from a hardware chip, which is not
located at this adress on newer machines. The virus allocates it's
memory correct and tests, if the catched DoIO call comes from the
"trackdisk.device" or not. So only diskdrives will be infected and
NOT harddrives.

The way of patching the vectors is new on AMIGA. The way of patching
will be used on Intel Windows machines in conjunction with background
programms (Thanks Ingo for this hint). This routine is buggy, but
works.



                     Detection and memory repair tested 01.12.1994.
```

1.133 BVirus

```
                                   BootVirus:
                         ----------


1024 Access Forbidden 2            1024 Asshole (not spreading)
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 European Disaster = Byte B. 3 1024 Disk Furunkel = Avenger
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
1024 Kimble                           1024 Laurine 1.0
1024 East Star                        1024 Amiga Fanatic
1024 Yaw1                             1024 Yaw2
1024 Yaw3                             1024 ELENI!
1024
          Max-Starlight'93
            1024
          Big~Ben
                                          1024
          Pestilence~V1.15
            1024 Rastenbork 1.2              1024 Rastenbork 2.0
1024
          Dynamix
                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.

Asshole (not spreading) virus:

Changes: Coolcapture, DoIo

This is said to be a virus, but infact it installs the patches
(without allocating the memory) and "forgets" to write it's
code to disc. This is for sure a laborotary virus.

Red Ghost "Virus":

This is/was probably supposed to be an antivirus bootblock. The
programming is in parts really lousy, the compare codes are to
bad, as a result, I rate this programm as dangerous. It's not
a virus, but it's a dangerous antivirus.

Access Forbidden 2 Bootblock virus:

- No patched vectors
- Kickstart 2.0x compatible

This is a very simple virus. It will be tried to allocate absolut
memory around $70000 and a copperlist will be created manually.
This stuff is quite lame coded. It will be tried to overwrite the
rootblock and the bootblock of a DD disk. The virus contains somekind
of graphic routine.

The virus needs no trackdisk device, so even your RDB can be
damaged in parts of it.

At the end of the virus you can read :

'NO VIRI!'
' DON'T INSTALL!'
'dos.library'
'graphics.library'

Detection tested 05.02.1995.

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.

Creeping Eel Bootblockvirus:
----

known clones: Executors and Kimble

Needs atleast Kickstart 2.0 to work properly. Copies its code to
$7ec00 (without allocating it before). Changed vectors:
DoiO and Coolcapture.

Damage: Destruction of Rootblock and the bootblockcode.

                                    Detection tested 06.06.1994.

```
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)
-DoIO (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 $1800 bytes under the
maxlocmem area !

                              Detection tested on
                                        19.12.1993.

Special thanks must go to Ingo Schmidt for supporting this
virus.

East Star Virus:

A simple North Star 1 clone. Look there !

Executors Bootblockvirus:

A simple clone from the Creeping Eel Virus. Look there !

NOTE ! There is a differences between Eleni and ELENI!

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 init-
ialized 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.

        An~interesting~text~appeared~about~this~virus
                  ELENI! Bootblockvirus:
----

    other possible names: -Messangerviruskiller-Virus
                          -Eleni V3

Patched vectors: Coolcapture, DoIO() and LoadSeg()

The bootblock virus works with Kickstart 2.04 and higher.
It uses the memoryregion around $120 to save some important

values from DoIO calls. Due to no "trackdisk.device" test-
routine, this virus is able to kick the RDB from your
harddisc.

The virus is extremly lame coded and contains lot of direct
memory access routines, without allocating the stuff.

The virus compares a value (1) in a special hardwareregister
(dc002d). This is the clockregister on some machines. If
the condition is true, it will be tried to load the file
ELENI! via LoadSeg(). This routine is buggy, too.

 Due to lame coding, the virus uses the memory from $70000-
$88600 without allocating it. I expect strong problems with
machines, which have only 1 MB memory !

The patched DoIO is just for the bootblockinfections. The
LoadSeg() part is much more dangerous. It will be searched
in all loaded files <=100000 bytes for the special command
"jsr -552(a6)". This is the NewOpenLib entry (if Execbase
is in A6). This command will be replaced by "jsr -$1400(a6)".
As a result, if this virus is in memory, it will be called
by such a changed file. But what happens, if the virus is
cleared in memory and such a file will be activated ? It
causes a crash. There is no secure way to recognize such a
manipulated file.

Manipulated files must be shorter equal than 100 KB and
the whole filename (including path) must be shorter
than 26 chars !

The VirusWorkshop tool called "ELrm" will be able to try
to repair such files. Please read the documentation for
this tool very carefull.

At the first virusstart, only the CoolCapture vector will
be patched. Then a reset will be performed and DoIO will
be patched.

If this virus is in memory, every loaded process will need
much more time, this is maybe a little hint for you to use
a good viruskiller to check your system.

Special thanks to MFM/Skid Row for the first warning for
this virus !

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.

Kimble Bootblockvirus:

A simple clone from the Creeping Eel Bootblock Virus. Look
there. Some visible texts have been changed. Nothing else.

                        Detection tested 06.06.1994.

At the end of the virus you can read:

"Antivirus: Kimble comes back ... use it ....Kimble"

Khomeini Bootblockvirus:

Simple MAD clone. Only the texts have been changed.

Detection tested on 28.12.1993.

Leviathan Bootblockvirus:
----

look in the Linkvirus section...

Laurine 1.0 Bootblockvirus:

- Kickstart 2.0x needed (based on patch routines.

This bootblockvirus is not resetproof and kills ColdCapture,
Coolcapture and the KickTagPointer. To spread itself it patches
the DoIO vector from Exec (quite strange way of patching).

The virus uses the memory from $6e800+1024 bytes to place its
code. The memory will be not allocated and so every programm
can trash it and as a result your computer goes to India. I
have tested it with VW on an A500+ with 1MB Chip and I had very
often a complete systemcrash.
After 35 infections a little message will be displayed
using DisplayAlter from the intuition lib.:

        'The Laureline Virus V1.0'
        'Code by Cat Lord'
        ',Report: 30.05.93'
        'Sex: Male'
        'Number of copy: 0002'
        'Laureline Male Found: 0000'
        'Laureline Female Found: 0000'
        'Girl Maked: 0000'
        'Disk Found: 0002'
        'Dos Boot Found: 0000'
        'Other Virus Found: 0000'
        'Amiga V1.2: 0000'
        'Amiga V1.3: 0001'
        'Amiga V2.0: 0000'
                'Amiga V3.0: 0000'

The values for "Amiga V... 000x" will be changed by the virus
itself and it really contains the code to check for various
Kickstart versions. Other destruction routines are not placed

in the virus.

General comment: Better play with your joystick ! Some routines
are extremly strange...

                                    Detection tested 07.07.1994.

        Max-Starlight'93~Virus...
                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!'

RAF Bootblockvirus:

Simple WarHawk clone. Only the texts have been changed.

Detection tested on 28.12.1993.

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. Sphinx is no member of SHI.

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. Better play with your joystick instead of making
such shit !

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.

Yaw1 Virus:

A simple Amiga Fanatic clone. Come on guys ! Better play with
your joystick or programm something productive and not such
a shit !

Yaw2 Virus:

Ein einfacher Fuck Device Clone. Eine technische Meister-
leistung.

Wir sind alle "stolz" auf den "tollen" Programmierer !

Yaw3 Virus:

A simple LameGame clone. Only visible texts have been changed.
Lamer !

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
Germany

Tel.:0511 / 514944

1.134 Elame

-> In my opinion is this text a pure FAKE <-

**** WARNING ! WARNING ! WARNING ! ********* * * * * * * * * THIS TEXT
COMES DIRECTLY FROM THE CODER * * OF THE ELENI VIRUSES! READ ALL ABOUT IT! * *
* ***

Well, sorry folks but I can't tell you who I am because you would probably
kill me! Im the coder of all the Eleni viruses! The meaning of this letter is
to let you know why I coded those viruses and how you can help other people
and yourself in the future! Now, is this true! Am I, the coder of the virus,
going to help you, the victim of the virus!? Yes! You probably think I'm the
bad guy in this nightmare, but that isn't true! Seek deeper! Let me put it
this way... One rainy day you're walking in the street far away from home.
Suddenly it begins to rain. Damn, you say, but, you're also greatful that you
brought an umbrella. Oh yes, you think you're very smart but then you find out
the umbrella has got a whole bunch of holes, through which the raindrops fall
onto your head! What a shit umbrella you think! You really get pissed on the
umbrella! That's the biggest mistake! You have many things or persons to
blame, but you should not blame the umbrella! Why ?! Think deeper! If it never
had started to rain your day wouldn't have been wasted! If you would have
checked the umbrella before leaving your day wouldn't have been wasted! Am I
right or wrong! I'm right!!! Well, it's the same with my virus. I'm not the
bad guy! I have a reason why I code viruses. The REASON is the bad guy! Who
the hell is the reason? My reason is a girl!! Blame her if you have to blame
someone! If I wouldn't have coded this viruses, someone else would! Now you
know why I coded the virus but you still don't know what I want! What I want
is the most important thing! I will continue coding viruses until I get what I
want! It's simply your choice! What I want is very simple! I just want at
least one big computer mag to write something impressing about my virus! I
don't mean a little invisible advert that nobody reads, I want at least half a
page! It has to be published in Sweden's biggest computer magazine called DMZ!
Otherwize forget it!! One more important thing!! The headline MUST include the
name ELENI VIRUS, and in the text people must understand that Eleni's
familyname begins whit L! Ex. The coder wrote this virus to avenge a girl
called Eleni L. Then, what you choose to write about it is up to you! Now, why

should you do this for me, I mean you probably still thinking that I'm the bad
guy! No I'm not yet the bad guy, but just wait until soon if I don't get what
I want!!! Yes, call it blackmail or whatever you want!!! Some hints:

Somewhen in the month of june 1994 (very soon!) a new version will get life!
The installer of the virus is spreading around the world right now! It's a
very smart one, bacause it depends of your computer's internal clock. IF you
don't have any clock it will never activate! If you have, then some day in
june you'll get a nice surprise!! Not to count with all old features it will
include the following:

1> Better memory allocation=not so many bugs that make you wonder what's going
on!

2> Immortality= once it has been installed on the bootblock of a disk you will
not get rid of it unless you ... guess what!!! This due to a verify error that
it will cause!!!

3> Resistance= if you try to kill it with a hard reset the virus will program
itself to destroy your HD, and it WILL NOT be killed!!

4> Monitor burn= when your clock has backed up enough much you monitor will
blackout, perhaps FOREVER, because the virus includes a routine to change the
hz freq of your monitor/tv to a value that they can't resist!! Lucky you
because this doesn't work on all tv's/monitors!!! But stay calm, I've got
something nice to tell you in the end of this textfile!!!!

5> Hd totally fucked up!!= This time the virus will not only format your HD's
first cylinder but EVERY cylinder starting from 0.

6>Hd hardware errors= I don't really know if this one works but if it does
then you can say bye bye!!! It's based upon the same system that makes the
bootblock unremovable!! Your HD might get verify errors and since most
software that come with the HD to format it isn't very good, perhaps you will
not be able to reformat it= no HD!!!

That's all folks!!!

Well, before I end I'm gonna tell you about the little surprise!! I know my
viruses don't work on Amiga version under 2.0 but the next viruses might!! So
what, you think!! Well, how about a virus that passes through write-protection
on the 1.3 ROM!!??? Eat this !!!! Now, why shouldn't I possibly could be
joking with you!! Be my guest and ask Commodore about hardware errors in the
1.3 ROM!!!! Now, I can promise you that I will not release any more viruses if
you follow the mentioned rules!! Remeber that YOU decide if this virus will
make the scene suffer!! I have two more things to say before I quit!! To all
those who know my identity (if there are any!!), this virus is nothing
personal against you, so if you want the cure just touch me!! The last thing I
have to say is that if you follow my rules then I will personally spread the
anti-virus that cures all infected disks/files before they have caused any
damage!!!

T H E   C H O I S E   I S   Y O U R S !!

PS.. Send this text to both DMZ and SHI because I haven't!! DS

1.135 Max/STL`93

Max of Starlight'93 Virus:

Kickstart 1.x: NO
MC68040   : YES

Patched vectors: Exec-GetMsg(), Exec-DoIO(), Intuition-Displayalert
and Kicktagptr.

This is an ordinary crypted bootblockvirus. The crypt-routine is an
ordinary eor-loop which depends of the rasterbeam register.

The memory will be allocated and there is no check for the calling
device-> I destroyed a 40 MB scsi drive with it. The RDB was over-
written by this virus.

The virus clears Coolcapture and Coldcapture, probably to make sure,
that it's the only code resident in memory !

The displayalertpatch is buggy or idiotic. No backjumpadress will be
saved. Only a zero will be given back and no jump to the original
routine.

The infection and destruction routines will be only activated, if

1. access to Rootblock (880)
2. access to bootblock (0)
3. read(2) or write(3) command

The destructive routine tries to overwrite a random block with
the double-longword :"INSANE!!". Only datablocks (recognition
longword 8) will be affected by it. This means less destruction
on FFS.

The virus contains no textroutine....

At the end of the virus you can read (after decrypting it):

'The Max of StarLight Virus'93'
'intuition.library',0

1.136 SS-II Bomb

SS-II Trojan:

```
Filelength: 57449 bytes
```

This is supposed to be a megatrainer for Silent Service II by Skid
Row. In reality this is a trojan, which clears the listed files
(see shortcut). In general I don't like to check for textfiles, but
this is highly dangeous and so I decided to check for it.

After all the files are cleared, the original Skid Row loader will
be activated.

Shortcut from the text:

```
;Buzz Bomb MKI, on the Attack... Flying Straight outa Reallity Control
;Coded 9-12-91 by The Christening Man, if your reading this, Congrats...
;BBBBBBBBBBBBBBBBBBBBBBBBBBBBBZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
;BBBBBBBBBBBBBBBBBBBBBBBBBBBBBZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
;BBBBBBBBBBBBBBBBBBBBBBBBBBBBBZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
Delete Sys:c/cd ;BBBBBBBBBBBBBZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
Delete SYS:c/loadWb ;BBBBBBBBBZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
Delete SYS:c/Assign ;BBBBBBBBBZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
Delete SYS:s/Startupii ;BBBBBZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
Delete SYS:Libs/Mathieeedoubbas.library ; your reading this, Congrats...
Delete SYS:Devs/mountlist ;BBZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
Delete Sys:Devs/Serial.device ;ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
Delete Sys:L/Newcon-handler; ... Flying Straight outa Reallity Control
```

Detection tested 8.12.1994.

1.137 Pestilence V1.15

Pestilence Bootblockvirus 1.15:

Kickstart 1.x : not working
Kickstart 3.1 and MC68040 : working

Patched vectors:

Exec-Disable
TD's BeginIO
Exec-Coldcapture
Exec-KicksumData   (not repairable)
Intuition-DisplayAlert (not repairable)

First appearance (as far as I know): Heilbronn/Germany

This is a new bootblockvirus with some nasty inner workings:

The last both patched vectors cannot be repaired, because the
virus does not store the original value. Sorry guys ! All other

patched vectors can be corrected by VirusWorkshop.

The virus checks before patching, if it's already installed
or not. The BeginIO routine only catches TD-READ and TD-WRITE
commands. The routine checks, if the loaded bootblock is the
virus. If yes, the bootblockcode will be manipulated (probably
to hide the code for viruskillers!!!!)

Under special circumstances (compare longword must be "DEAD"),
the blocks 2-3 will be filled with some garbage. The information
on this blocks cannot be recoverd...

If a pointer reaches a special value, the whole disc will be
formatted using memorygarbage. This routine is buggy, because
the memoryblock, which should be written, is out of REAL
memory and the system travels to india.

It crypts all read blocks (T-DATA) with an eor-loop. If the
virus is active in memory, all crypted blocks will be decrypted
online. If you remove the virus from memory, several checksum-
errors will appear on your screen. VirusWorkshop 4.6 and higher
are able to repair the crypted blocks, because there is no magic
in this cryptroutine.

Such routines (online-(de)crypting) were first seen on the AMIGA
in the "Saddam" diskvalidator viruses and then in "The Curse of
little Sven" bootblockvirus.

The first longword of a crypted block looks like this:$AFFE0008.

The whole virus is crypted with a simple eor-loop and looks like
the work from a quite sober'n clean programmer. At the end of
the virus you can read (after decrypting it):

'trackdisk.device'
'intuition.library'
'PESTILENCE v1.15 (c) 14/05/94!'

                        Detection and repair tested 11.12.1994.

1.138 CommanderWarn

THIS WARNING APPEARED ON THE FAST GERMAN SYSTEMS AROUND 10.12.1994. (-ed)

  WARNING! WARNING! WARNING! WARNING! WARNING! WARNING! WARNING! WARNING!
 -~-

Today Some Lame Dude That Called Himself " Nike/sKID rOW'94 " Logged In To My
Board... He Claimed To Be A Skid Row Member... He Also Claimed That He Was A
Coder,GFX-Artist And Trader! Ok...So Far So Good....BUT!...He Claimed That He

Was Calli'n From ENGLAND! I Thought That It Was Quite Strange To Call A New
Opened Swedish Board.. So I Jumped Into A Chat And Asked Him What He Wanted...
He Says That He Wanted Me To BETA-TEST A New NUKE-DOOR.... Well, Well...Ain't
It Quite Strange To Call All The Way From ENGLAND To SWEDEN To A Little New
Opened Board Just To BETA-TEST A New Door... Especially When He Was In Such A
Big Group As SKID ROW!!! Well... He Got Some Access And Uploaded The Whole
Thing... I Unarchieved It And Started A VIRUSWORKSHOP Scan... GUESS
WHAT!!!....The Archieve Contained 2 COMMANDER LINKVIRUSES!!!

SO LOOK OUT FOR THIS FILE: EXE4.7.LHA In That Archieve These Files Contains
COMMANDER VIRUSES: ---.
                                                                |
                  SkidRow/doors/ex/Ex!_Task <----------------|
                  SkidRow/doors/ex/Ex!_UpdateSLog.x <--------'

          The Door Is A So Called Exorcist!.x

SO WATCH OUT FOR THESE FILES....

I Can't Really Understand How It Can Be So FUCKI'N FUN To Trash New Boards
Maybe It Is You'r Fucki'n Ego That Tells You That You Are SOOOO ELITE!!! Well
I'll Say One Thing, And I Will Also Stand For It! I Don't Think That You
Become More Elite If You Manage To Get A Virus In Someones Harddrive... The
Scene Are Going Down The Drain If We Must Keep Draging On Such CRAP! That
Can't Do Anything Except To Try To Get Elite By Destroying Others Work! I
Don't Know If There Is Someone Called " Nike " In Skid Row, But If There Is
And He Have Nothing To Do With This, I Appologize.... If It Really Is A Door
Made By SKID ROW And That They Really Wanted Me To Test It But Did Not Know
About The Virus I Appologize To Them To, But I Don't Think That Is
True!...... Anyway I Advice You To Scan You'r HD If You Have These Files.
Maybe It Is A Mistake Made By Skid Row,...TRUE OR FALSE..You Tell Me!

Ok...End Of Text, But Let Us Get Rid Of Those So Called " ELITE " That Does'nt
Know Anything Better Than To Destroy Other Peoples Hard Work!!!

                                        CLAUDiA SCHiFFER/NEXUS^SRE

 ACHTUNG! ACHTUNG! ACHTUNG! ACHTUNG! ACHTUNG! ACHTUNG! ACHTUNG! ACHTUNG!
-˜
-

1.139 LamerFry_Comment

 Paul_Browne%39:138_14.4@GH_AMIGA.INSIDER.SUB.DE benutze seine Tastatur am
01.01.1995 um 17:58:46 Uhr, um folgenden Text unter dem Betreff "Public
Announcement" zu erzeugen:

(Comment: PB is Paul Browne, SHi England
          other texts are from me)

PB> I had a phone call today from Mark Pemberton, also known as Kooky of
Calypso. PB> He used Virus Workshop 4.3 to delete the Commander virus from his
system but PB> was very upset and annoyed to find himself listed in the VW
docs as a virus PB> programmer. PB>

    I have only listed the visible texts in this virus and nothing more. This
    virus is a clone from the Liberator virus and was crunched and then
    manipulated the headers/routines. It's his own fault, if he makes such
    stuff. In the doc I only mention the visible ASCII texts and this should
    be ok, or ?

    Shortcut: "This virus written by Cooky/Calypso for SHI test" or
    something like that. If he writes something like this, it is his
    own fault and he has to be sure, that someone will read this.

PB> Several months ago he hacked some existing viruses to demonsrate a means
by PB> which viruses can be crunched and still evade detection when libraries
such as PB> the decrunch.library and unpack.library are used by virus killers.
He gave me PB> the only copy of the virus which I passed on to SHIMain in
Denmark and from PB> there it was sent only to SHI anti-virus programmers. It
was never released. PB>

    It reached some german antivirusprogrammers. I clearly state in the docs
    that this virus was send to me by a SHI member. There can be everywhere
    some not so secure places and the virus could be out.

PB> Mark is very concerned that the VW docs might harm his reputation and has
PB> asked me to invite anyone who doubts him to contact him at his address
which PB> I'll include below. Personally I find it surprising that a test
virus PB> intended only for SHI programmers and which was only passed through
internal PB> SHI channels could find its way to a programmer who bans SHI from
distributing PB> his killer.

    For my person: I don't think that he is something like a virusprogrammer.
    His fault was to clone a virus (producing clones is not legal ?!?) and
    to write his name in it. HE wrote his name in the file and now HE has to
    read his handle in my docs. This is his problem, not mine.

    Programming viruses in any form is prohibited and I personally wonder
    a little bit, that SHI owns a special manipulated testvirus-clone.

    To the internal SHI stuff: VT, VZ and VW know this virus. There are/were
    some persons in SHI, who understand, why several viruskillers are not
    allowed to be distributed by SHI , but on the other hand see, that they
    can support us with a new and unrecognized clone.

1.140   DMS_2.06_Trojan

               DMS 2.06 Trojan:

 Filelength 45732 Bytes (partly packed)

This trojan was spreaded around 2-3.01.1995. in Europe. The
                4eb9
                 linker was used to link an additional code on a normal DMS ←
                    version.
DMS 2.06 is at this time NOT released. The linked programm contains
a FastCall hacking system, which is a little bit more advanced in
comparison to the code in the
                LHAV3
                 or in the
                Vtek22
                 trojans. The
trojan tests for the SnoopDos task and skips, if this task was
found.

The mailbox hacker is crypted with a quite nice eor-loop. The main-
part is packed with something different, but I was too lazy too
check this out, because it's for the virus quite irrelevant.

Shortcut from the decrypted file:

      'S:HauptPfad'
      'User/SYSOP/Userdaten'
      'User/Slayer/.index'
      'User/Slayer/.txt'
      'Absender : SLAYER'
      'Betreff   : Test'
      'Datum   : 16.11.1994'
      'Uhrzeit   : 22:02:41'
      'Zeilen   : 2'
      '16.11.1994 22.02.41   1 Asc Slayer   '
      '   Test'
      'SnoopDos'
      'dos.library'
      'User/Slayer/lesemeldung'

File-ID description of this trojan:


```
ø-==--==--==--==--==--==--==--==-ø
|     __  ___¡___                 |
|    /  \ \  |: / /\    - DMS 2.06 ---  |
|   / _ \ \ ! / / ·\                .|
|  // | \/   \// \/\  -cRACKED     :|
| /· ¦  ·\:¡ ·\    \ \       vERSION :|
|/____|_____\|_____\          .:|
|            !                   ::|
|                             .:::|
|                     ......:::::::|
ø-==--==--==--==--==--==--==--==-ø
```


This warning appeared first on the fast european systems:

```
>Probably virus in file dms206.exe of archive dms206.lha
>                         45732 Bytes
>
>Virus Workshop reports $4EB9 File wich means probaly BBS-Virus
>inside!!!! Former version of DMS did not contain this $4EB9 (Hunk?)...
>Also packed with an unknown packer...
>
>I have not very much knowledge about these things, but check it out
>it looks a little bit strange.....
>
>The program-name is 2.06 but the last REAL version was 2.04!
>
>Better don´t use this shit till someone checked it!


Without this warning I would have never had checked this file for a
possible infection. Special thanks to ¿nfiltr/\to®.
```

Comment 11.01.1995:

Some guys thought it would be funny to re-release this trojan again. This
time it's name is cry_206.lha.

File_ID.Diz of it:

```
:::_____    _____::
::/   __/__  \  \   /   /  __ \__   ____/\:
:/\   /\   \_\   \  \_/   / /_/ /\/   /\___\/:
:\ \ \ \_\    _   /\       / ____/ /   / /:::::
::\ \___\_//\ \ \     /_/\___\/__/ /:::::::
:::\/__/_/:\/_/\/    /\_\/::: \__\/:::::::::
::::::::::::::::/___/:::::::::::::[PRESENTS]
::DMS V2.06 (FaSt) [CrAcKeD VeRsIoN]:::::::
::::::::::::::::::::::::::::::::::::::::::::::
```


                         Detection tested 04.01.1995.

Comment 05.01.1995:

VH Team NL (Jan Hendrik Lots) produces tests of viruskillers and claims
that VirusWorkshop isn't able to recognize this 2.06 trojan. That is
simply wrong. JHL is testing a manipulated one and I cannot give you a
letter saying that a viruskiller would recognize all deactivated viruses,

```
too.
```

1.141 Surprise Trojan

```
                    Surprise Virus:
---------------

Filelength: 39296 Bytes (unpacked)

The name for this virus comes from the person, who send it to me.
There is no sign, why this virus was called in this way.

This is a simple RDB formatter for all harddrives on Unit 0 from the
SCSI device (e.g. all A4000/A1200 systems). The code looks partly
quite good. The first 2048 bytes will be overwritten and there is no
rescue, except you made a backup of the RDB before. The name of the
device is "Suck me Organizers" and the volumename is "FuckOffe".

Kids, stop finally playing around with this shit !

At the end of the virus you can read:


'RDSK'
'Suck Me Organizers             '
'PART'
'FuckOffE'
'DOS'
'scsi.device'



                            Detection tested 04.1.1995.


Comment 12.01.1995: A warning text concerning this virus caused
some misunderstanding(?).
        Click~me
          to read it.


Another text from the "authors" of the virus appered. Judge
for yourself !
        Click~me
          !
```

1.142 TurboSqueeze 6.1

The TurboSqueezer is a not very often used Packer nowadays. It was used several
times for BBS viruses (probably based on the reason, the some unpacker
librariers did not recognize it).

Mainly BBS viruses against AmiExpress were packed with it.

1.143 Copy_LX

Copy_LX 1.03 Trojan:

Filelength 6932 Bytes (unpacked)

This is a classical trojan horse. Installer is probably a modified
LX 1.03 programm (I still search for it. The file I got from the
AmiNet was clear). It will write a new COPY command.

This copy command searches for the file "s:save". If this file
exists, the trojan will not work and the original copy command
(V38.1), which is linked behind the trojan, will be activated.

Then the virus checks the actual date: If the date is 5961 or
more days after the 01.01.1978, the virus will start, otherwise
it will skip. This date was somewhen in 1994. Then a longword
"scsi" will be decrypted and via globaldoslist and the known
routines, it will be tried to get a device, which starts with
the long "scsi". If such a device was found, it will be tried
to get the rootblocknumber and then it will be tried to
read from the rootblock.

Problem: I got the Copy command itself and the resourcefile.
In the copyfile only the READ command will be used, in the
resourced file the WRITE command will be used. I wonder a
little about this.

If the write command is used, all reachable devices (beginning
with scsi) will loose it's rootblock. Try to recover the
data using things like Quarterback and/or Disksalv.

                    Detection tested 07.01.1995.

1.144 Party94_Comment

Original Text from Jan Andersen / Virus Help: (Filename: vhelp-01.txt)

```
*** Omr.: VIRUS_AMY                          Dato: 31 Dec 94 11:37:55 ***
Fra : Jan Andersen (39:141/127.1) *** Til : All *** Emne: Virus Warning !!!!
```

Hi All !!!!

The is a new warning about a demo that damages your RDB Boot. (Great way of
starting the new year) :-((((((((((

This demo is called 'SURPRISE.exe', and has a size of 39296 bytes. It makes
all your partitions on your HD into, one partition and calls it 'SUCK ME
ORGANIZERS'. We think that it only makes damages on SCSI devices, but we are
not sure about that.

The demo was made at the 'PARTY 95' in Herning, Denmark. And was given to the
organizers to compeat in the contest of the best demo. It did do some damage
to there HD, but a guy (Benny) did restore there HD.

We do not know if it was spred at the party. But if it was, please take care
of this demo.

This demo is on it's way to every wellknown antivirus programmer.

            Regards....

       __
  __   ///   Jan Andersen   FidoNet: 2:236/116.1
  \\///   VIRUS HELP   AmyNet : 39:141/127.1
   \XX/   TEAM DENMARK   BBS   : +45 3672 6867

Reply by Lector / The Party:

We (the organizers) wanted to reply to this text to confirm / disprove any
rumours / speculations.

First of all, it is true that we recieved a intro (not demo) that did some
damage on the computer we tested the intro on. However, this was NOT a virus.
A virus stays resident in memory, can infect other disks or change existing
files on the harddrive. It was 'simply' a program that, as Jan Andersen
explains, destroys your RDB and all info about your partitions. (Whick of
course is bad enough)

However, the program ONLY works in AT/IDE devices, in other words, it will NOT
do any damage to SCSI devices. (According to a representative from SHI)

Finally, the intro was NOT spread at The Party 94 (!) (at least not by us) but
we have no knowledge of whether the author distributed if personally or not.

The Party

1.145 IStrip 2.1 BBS Trojan

```
IStrip 2.1 BBS Trojan:
----------------------

Filelength 1156 Bytes (unpacked)
Filename: Istrip/S/Istrip.bin

This is a classical BBS trojan, which tries to read the user.data
file from AmiExpress systems and write it into the uploaddirectorie
under the name: eatme.lha. This way of hacking boards was performed
by Zonder Kommando some months ago. The code looks quite good and
the programmer of this shit is no beginner in assembly-language.

File_ID.Diz:

---- - -- - -- --- - --- ----- - --- - -- -
       TAS / MEDELLiN UK PRESENTS
---- - -- - -- --- - --- ----- - --- - -- -
--> ISTRIP 2.1 beta LhA turbo stripper! <--
--> There is no other stripper! Doesn't <--
--> use LhA for stripping, custom 680x0 <--
--> code! - Can kill #?#? & *.* banners <--
--> As well as delete protected files + <--
--> Ansi Analyzing improved with 60 %   <--
-->                                      <--
-->    WORLD BEST/FASTEST STRIPPER!      <--
------[..SSF..]-dANCE-wITH-mE-[..5D..]-----

I think it exists a real IStrip and someone just resourced it and
put a new routine additional in it. VirusWorkshop only recognizes
the virus itself, not the loader.


Detection tested 17.1.1995.
```

1.146 ADDY-099-Doc

```
///////////////////////// Addy Ver. 0.99 \\\\\\\\\\\
                         --------------
```

WHAT THE FUCK IS IT ?

A small BBS Add maker, for you guys to put in your .lha's :)

This Programme is made by me, if you like it, tell me cause i've JUST

started learning how to do make small programmes, if there are any bugs

in it, please let me know, i can be found at the coolest bbs'es in Sw.

(Sorry about the lame doc, but i just cant wait to release my

first programme).

Usage:

If you cant figure this one out, you never will.

Simply double click And follow the instructions. Easy Huh ?

Known Bugs: NONE.. at all.. tested very well.. Wouldent want my first

release to be crap.. would I ?

Written By The Freak !

\\\\\\\\\\\\\\\\\\////////////////////////////////

1.147 VHD-Warning-Addy

```
              _____   _                        _____     _____      _    ____       _
   ____/"""./###/____)_____       \   ./  ____/"""./____)\/"".
./_____)\
  /"""/    //_____    /"""/"".
/"___/_   \ //  /"".
/   //""____/   //_____   \ / /
 //"""/"   / //   /   //____    \_ \/ /   //    // ____/    //"./""""/  // \ //   /
 ____/ / /  //"""""/X@!/    /  //    //  /"""/       //    ___/
  _____/\__/___/_""_____/_____/    /___/____/\_____/\_____/\___/:
:.
                  /____/
                            Team Denmark
    >>>>>>>>>>>>>>>>>>>>>>>>>>>--------------<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

     WARNING !!! WARNING !!! WARNING !!! WARNING !!!WARNING !!! WARNING !!!
          WARNING !!! WARNING !!!WARNING !!! WARNING !!!WARNING !!!

                   WATCH OUT FOR THE ARCHIVE "ADDY099.LHA"

 Do NOT start the 'ADDY0.99.Exe', it will replace your startup-sequence
 and shell-startup, and add 656 bytes to your c:Dir command.

 It will change your startup.sequence with a new small one:

 Prompt "AfraId ?..tHe fReAk wAs hEre 2 dEvEstAte NDOS:>"

 Every time you run a shell it will add a line in your user-startup
 "Wait 5" and you will the the text above when you are rebooting.

 I do not know what it does to your C:Dir command, but if you have

started this program up, the replace the c:Dir command, with a new
clean one, form your WB disk's.

It will work under KS 2.0 and 3.0, have not tested it under KS 1.3 yet.

The archive is on it's way to every well known antivirus programmer
in the world, thanx guys for the great job you are doing.....

Thanx to Morph, for sending me this new 'Thing'.

Regards
                                         _____ _
Jan Andersen.   _____/""". /###/_____)_____
Virus Help - Team Denmark.   /"""/   //_____   /"""/"". /"___/_HELP!
                                 /   /   //"""/" / //   /   //____   _
FidoNet: 2:236/116.1   \   //   / _____/   / //""""/X@!/
AmyNet : 39:141/127.1   _____/__/___/ ""_____/_____/
BBS   : +45 3672 6867   /____/

1.148 Some texts concerning the Surprise Virus

The text below appeared on the known systems at the beginning of febuary 1995.
This seems to be a text from the programmers of the Surprise Trojan. The text
is a fake in my opinion and/or contains some logical errors...

Here the text is:

  The truth about the Party virus called:
          - SURPRISE.EXE -
  [written by the authors of this virus!]

                 SURPRISE.EXE - is it really a virus?

 Dear Amiga owners!   [date:30/01/94]

 All of the AUTHORS wanna excuse for this file, but it was made in respect to
the behaviour of the organizers at the Party 4... Lots of them thought to be
GOD and did like that! for example: - They could drunk! alcohol, in spite of
not being allowed for us! - They made lots of people waking up at 7 o'clock in
the morning! (just
  for fun! - to show us they were the organizers) - If they wanted to,they
searched for anything illegal in our PRiVATE stuffs!

(in spite of the fact we didn't have anything illegal – and we even told it
  them!) Is it fair to search in our PRiVATE stuffs? – even the price of
xeroxing was different man by man (the first one copied
  a sheet for 2 dkk, somebody else for 3 dkk and there was one who did
  that for FREE! – it depended on the mood of the organizers!) But these were
just some minor problems, however, they managed to fuck up our mood and the
atmosphere with their behaviour... We travelled more than 2000 km to get this
party, but unfortunately we met with narrow-minded and pigheaded organizers
there...

NOBODY (I mean from the programmers) spread this file at all! All we wanted to
do is just to strike back to the organizers because of their annoying
behaviour... We didn't want to harm anybody! (expect for the organizers) ...

We are really sorry if you got (and run) this file... IT's NOT a VIRUS!!!!! It
doesn't infect anything and it even not spread itself neither!

                        DELETE AND DON'T RUN IT!

All we wanted to express was our misunderstanding with the organizers....

Comment To: *** Omr.: VIRUS_AMY   Dato: 31 Dec 94
11:37:55 *** Fra : Jan Andersen (39:141/127.1) *** Til : All *** Emne: Virus
Warning !!!!

You needn't afraid... It's not virus, just a small file... If you don't run
this file, then nothing is happening! It ONLY? damage the partition-table!

        WE ARE ALSO AGAINST THE VIRUS-PROGRAMMERS!

        AND WE REALLY SORRY FOR HAVING SPREAD THIS FILE!

                                [authors of the SURPRISE-intro]
                                 ^^^^^^^^^^^^^^^

1.149 Gath95-! Trojan

Gath95-! Trojan:

Filelength: 14032 bytes unpacked (crypted with a simple loop)

other possible names: Achtung(.exe) trojan

This is a very simple trojan. It tries to format your dh0: using quick-
format and afterwards it will be tried to fill your dh0: using files
with the following names: dh0:lamer.aaaaa. The filesnames can differ in
the last chars (possible to really fill up the drive).

The trojan writes a new file with the name:

"ram:verwirrung" (a german word, which means irritation)

The the executecommand for the quickformat will be started. The new name

of the dh0: device is then LAMER.

This trojan is much more dangerous than the ordinary quickformat stuff,
because of the high amount of new written files (lamer.aaaax), the intern
structures of the qickformatted directory will be changed and a data loss
is in most cases not to prevent.

This trojan was spreaded as intro for the Gathering'95 party in Oslo.

File_ID.DIZ:


```
+----------------------------------------+
|Virtual Dreams, Melon and Rage's New Intros
+----------------------------------------+
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 THE GATHERING PARTY INVETATIONS. 3 OF THEM
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
+----------------------------------------+
|The BEST CODE of 1994/95. Defintly! Get it!
+-----------------------{ cSo/Ç(¿'g5! }---+
```


                                    Detection tested 11.2.1995.

 Special thanks to Mario/TRSi for keeping this virus for me !
                  Euronymous/TRSi for the warning !
                  Ixxy/TRSi for calling Mario

1.150 Red_October_17_Linkvirus

 Red October 1.7 Linkvirus:

 -Kickstart 3.x: Yes
 -MC68040   : Yes

 -Infected files become 1296 bytes longer
 -No changed vectors

 The virus allocates the memory for the to be infected file. It does
 not path a DOS vector, it simply tries to infect files via EXNext etc.
 The virus recognizes itself using the first codehunk and the first
 longword in this hunk ($4e714e71).

 The virus does not correct any Relochuncs and most infected programms
 crash. It simply copies its codehunk before the first codehunk and
 increases the length. The virus is very simple, but I decided to

recognize this one, too. This virus is very old.

Around offset 1100 in the first hunk, you can read:


```
'timer.device'
'dos.library'
'ram:'
'ram:1'
```


The original first infected file is 1296 bytes long and will be
cleared completely ('cause there is nothing more to fix').

To this virus, there exists a documentation, which was spread years
ago together with this virus:

The Red October Virus 1.7 (901029)

This virus program is for demonstration and testing purpose only.

The Red October virus is a non-overwriting virus and was developed
and tested under AmigaDOS 1.3.

The following points influenced the development of the program:

1. The virus should infect other programs only when system clock
   seconds are evenly divisible by three.

2. All of the infected files should continue to work properly.

3. The manipulation task in the virus causes a system crash when
   the system clock seconds are 16, 32 or 48 (evenly divisible
   by sixteen).

4. The virus only infects files which are shorter than 50000
   bytes in the current directory.

Delete the virus and the infected programs on the computer when
you are done. WORK WITH COPIES ONLY.

                                        Detection tested 12.2.1995.

1.151 Promoter1-Virus


```
Promoter 1 Virus:
-----------------
```


```
Filelength 1848 Bytes (unpacked)
```

This one seems to be a little trojan, which tries to copy itself
from disc to disc using the disc-validator. It will be tried to
write a new file called "df0:l/disc-validator". The virus contains
no real destructive routine and is only interesting for KS <2.04.
The virus contains a little intuition routine to display some
texts. This routine is buggy, because a cachefault will be made.
Pure code from a beginner.

You can read the following texts in the virus:

'Learn from the great master about the my'steries of BCPL'
'FUCKFUCKn.library'
'dos.library'
'df0:l/disk-validator'
'   I am the Kickstart 2.0 - PROMOTER - Virus'
'   Please stop using Kickstart 1.2/1.3'
'   and I will stop bothering you'
' This masterpiece of brilliant software was designed by'
' the marvellous VaginaMan, always deep inside the mysteries'
'   sponsored by Commodore Australia for remembering'
'   you to switch over to Kickstart 2.0 !!'
' This is PROMOTER 1, coming soon PROMOTER 2, which won't be such
' nice as Number 1'
'   So this is your last chance to switch'
' to Kickstart 2.0 with all',0
' your data, because Number 2 will be very'
' destructive and infectious,',0
' of course only for Kickstart 1.2/1.3-Users, because our motto is'
'   PROMOTE AMIGA',0
'   PROMOTE Kickstart 2.0'
'»   PROMOTE AMIGA'

                                        Detection tested 18.2.1995.

1.152 World-Clock 1.16 Fake-Trojan

                    World-Clock 1.16 /X Trojan:

Filelength: 21396 Bytes unpacked
Used method: linking with 4eb9 (advanced version)

World-Clock is an AmiExpress utility written by Siegel/TRSi
(AmiExpress section). Using the wellknown 4eb9 linker, a
little BBS trojan was linked. This trojan is packed 1952
and unpacked 1380 bytes long. The used packer was the

        TurboSqueezer~6.1

```
        packer, which will be NOT recognized by
XfdMaster library.

VT and VW detect the
        4eb9~file
         and let pop up a requester.

The trojan itself is very lame coded and even contains some
so bad code, that the enforcer will report it. It just
changes User.Data and user.Keys. Nothing more. A user under
the name Hyper will be activated and get a account.

Some ways of programming (e.g. the routine, which checks, if
the virus is in system) are comparable to the /X-Fucker
linkvirus and probably out of the same source, called
CONMAN.

At the end of the unpacked viruspart you can read:

'BBS:USER.DATA'
'BBS:USER.KEYS'
'dos.library'
'AE.Master'
'CONMAN'
'HYPER'
'BERLIN'
'110'
'HYPER'
```

```
            Some~words~from~Siegel/TRSi~to~this~trojan.
                Special thanks to Siegel for keeping this trojan for me  ←
                    !!!
```

```
                        Detection tested 20.2.1995.
```

1.153 Siegel_Comment_World-Clock1.16

```
 _____        _____
| _____    _____. _____ _____|_    _____|_    _/
| \   _____/_____(_____:/   __     /___  ___/____/_   _    /___ |
| _/_____    /        :   _____/   /  \__      /  _____/   / |
| \ _ _____/_____:_____/_____/  Mo!  /_____/  |
|  \ /                              /_____/          l_____|
|   \/   SIEGEL/TRSI (/X·INNOVATION) iNFORMS    |
|     ----------------------------------    |
|                        |
| aBOUT tHE fUCKIN' lAMER wHICH cREATES fAKES |
|                        |
| rEAD tHIS tEXT cAREFULLY sO U sHOULD kNOW tHE |
|                        |
| \            T R U T H !            |
```

```
 | \                                                        |
  `-------------------------------------------------'
```

Berlin, 18.02.1995 ~~~~~~~~~~~~~~~~~~ Well, one of my Beta-Testers has given
me today a Version of World-Clock, which includes a BackDoor!!!!!!! This Tool
enables every time you start it after an reset the wellknown User 'HYPER' and
reactivate him...this is NO FAULT FROM ME! I have checked this fake version
(V1.16) with the Virus Terminator (VT) and he reports an $4EB9-$4EF9-Link,
which will be produced by this fuckin EXECUTABLE-LINKERS, which allows poor
lamers to add their code to existing Programs...to do this, this
linker-programs have to change the Hunkinformations in the desired Program to
allow the linking of their own shitty code and of course the executing of
their linked code...as an example, i have written down the first line of both
versions, the infected and the original one, and here you could see the
changings:

ORIGINAL: ~~~~~~~~~ 00000000: 000003F3 00000000 00000002 00000000
.... 00000010: 00000001 00000C05 00000A93 000003E9
.... 00000020: 00000C05 48E77EFE 24482400 49F90000
....H.~.H.I...

...

AND THE FAKE-VERSION: ~~~~~~~~~~~~~~~~~~~~~ 00000000: 000003F3 00000000
00000007 00000000 .... 00000010: 00000006 00000005 0000007C
0000015A ....|...Z 00000020: 00000154 00000A13 00000A40 00000022
...T.......@..."

...

I think a blind man could see the difference between this two examples.

I'm very afraid that I can't do anything against such fuckin' Lamers, which
are only able to destroy other's work instead of writing their own Doors, and
I could - of COURSE - give no gurantee that the public versions of my doors
are NOT infected by this lamer, I could only say :

I'm not interested to spend many hours of coding only to built in such back-
doors! My personal goal is it to write user-friendly doors which should be a
great help for all users when using the Amiex-BBS, not to destroy others
BBS-Systems by infiltrating such users like HYPER.

The best gurantee to avoid such fuckin' shit is to register yourself and get
the Tools direct from me...but that's your own decision....for number/PW of my
BBS take a look to the end of file...

Signed:SieGeL (tRSi/X-iNNOVATiON) - FUCK YOU HACKER, ONE TIME I'LL GET YOU...

PS:Last Public Version is V1.18 - Length : 22348 Bytes....

1.154   ConMan-LoadWB-Installer2 (Quartex)


```
            ConMan
            -LoadWb-Installer 2:
```

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

Length: 24596 Bytes unpacked

This is supposed to be a new intro from the legendary Quartex,
but this is just a trojan, which writes a new LOADWB command
and installs a new task into system, which is named:

```
        CLI(0): No command loaded
```

```
  (This types of tasks exists in clean systems, too)
```


The new LoadWB command is 2088 bytes long and packed with
TurboSqueezer 6.1, like all other productions from ConMan in
the past. The unpacked file is about 2124 bytes long and
more information can you read about this virus in the
section about the first
```
        ConMan-LoadWB-Installer
```
```
            .
```


                            Detection tested in Feburary/95

P.S.: Some unpacking systems have problems with this packed
File, probably based on unpackroutines without security stuff.

1.155 Rastenbork-Installer

```
Rastenbork Installer:
--------------------
```


Packed: 5220 bytes (PP 4.0)
unpacked: 8640 bytes

This is just a little lame installer for two bootblockviruses.
The work looks pretty lame and the texts in the installer sound
for me like a work of a little boy trying to get famous by
writing such shit.

To this little lame guy: If I get you, you have a serious problem.
To the polish organizers of TRSi: If I were you, kick this guy
very fast.

The installer just writes via TDdevice 2 viruses on the
bootblock and is even in this part buggy.

Visible text in this installer:


```
        ' need reqtools.library! Sucker!'
```

```
                'Panic! I can',27,'t open trackdisk.device!'
                'reqtools.library'
                'intuition.library'
                'trackdisk.device'
                'ThE rASTenbOrk iNsTAller by PePe/tRSi'
                'VirusInfo'
                'About installer...'
                'WhAt tHE hEll ?!'
                'Oh no...the CoolCapture vector seems to '
                'be changed!!!'
                'If you have virus in memory,installing will'
                ' not work'
                'resident virus will reinstall itself!!!'
                'but it doesn',27,'t have to be a virus.'
                'QUiT|prOCEEd'
                'Back to menu'
                'vIRUs->dF0|vIRUs iNFo|<---|--->|aBoUt|QUit'
                'vIRUs->dF0|vIRUs iNFo|--->|aBoUt|QUiT'
                'vIRUs->dF0|vIRUs iNFo|<---|aBoUt|QUiT'
                '--------------------------------------'
                '----------------------------'
                'rASTenbOrk vIRUs liBraRy                 '
                '       Last update: 1994.11.29'
                '--------------------------------------'
                '----------------------------'
                'Virus name.......Rastenbork Virus'
                'Version..........1.2'
                'Born.............1994.04.28'
                'Action...........writes rubbish to the '
                'root block after 10 times disk'
                '               changed in any drive '
                'since last soft reset'
                'Help.............use any disk repairing '
                'program (eg.FixDisk)'
                'recognization....$f0f screen while bootin'
                '               included text ',27,'Boot Vir'
                'us Protector v5.4',27
                '               and ',27,'A NPS production.',27
                'Notes............one of first releases o'
                'f Rastenborg and therefore'
                '               with some bugs (get Viru'
                'sInfo).'
                '--------------------------------------'
                '----------------------------'
                '01 of 02                         kEE'
                'p oUT oF tHE rEaCh Of lAMerS !'
                '--------------------------------------'
                '----------------------------'
                'Information on Rastenbork Virus 1.2:'
                'This is the first release of Rastenbork, '
                'and contains some bugs, which'
                'may  be  found as one  of destructive ac'
                'tions  of virus, however  they'
                'haven',27,'t been planned. Here are some techn'
                'ical informations:'
                'auto memory alloc at every reset'
                'new DoIO handler for all actions'
```

```
'installs on every unprotected disk at '
'disk changing'
'-after changing  disk 10 times (any driv'
'e)  since last reset exchanges'
'next read  DoIO operation  to write, so '
' usually the  rootblock (880)'
$A
' is destroyed,then writes intuition aler'
't.'
'includes coded text'
'-includes not coded text suggesting  tha'
't bootblock is a Vir Protector'
'And the most important bugs:'
'does not check  if disk is in AmigaDOS, '
'so booting from HD with virus'
$A
' in memory equals  babbling the HD 0  bl'
'ock (funny?). This hasn',27,'t been'
'planned but may be used against HD users'
'!'
'-does not  check if  disk has already  b'
'een installed  with the virus,'
'so the  disk changing  operation takes s'
'ome more  time on every disk,'
' but  this doesn',27,'t  cause any  troubles '
' for the virus  bootblock data'
'isn',27,'t self-changing.'
'----------------------------------------'
'---------------------------'
'rASTenbOrk vIRUs liBraRy                '
'       Last update: 1994.11.29'
'----------------------------------------'
'---------------------------'
'Virus name.......Rastenbork Casher Virus'
'Version..........2.0'
'orn.............1994.11.28'
'ction...........codes directory blocks a'
'fter 10 boots from'
'                 infected disk'
'Help.............decoding possible'
'ecognization....$fff screen while bootin'
'g'
'                 included text ',27,'Panzer t'
'otal anti virus system',27
$A
'Notes...........latest release so far,b'
'ut who knows what the future'
'                 will bring...'
'----------------------------------------'
'---------------------------'
'2 of 02                             kEEp'
' oUT oF tHE rEaCh Of lAMerS !'
'----------------------------------------'
'---------------------------'
'Information on Rastenbork Casher Virus 2'
'.0:'
'his is  the second  release  of Rastenbo'
```

```
'rk and  is a little  improved'
'comparing to the previously one. Has als'
'o other destruction idea.'
'Technical informations:'
'-auto memory alloc at every reset'
'-new DoIO handler for self-copying actio'
'n'
'-installs on every unprotected disk at d'
'isk changing'
'each boot from infected disk  increases '
'internal counter and rewrites'
' bootblock'
'after ten boots from the same infected d'
'isk, the sectors of directory'
' block are being coded,so fix disk isn',27,'t'
' enough to restore data.'
'Anyway,this can be done.'
'includes coded text'
'-includes not coded text suggesting  tha'
't bootblock is a Vir Protector'
'checks if disk has been previously insta'
'lled with this virus; if yes,'
' leaves it alone'
'checks if disk is in AmigaDOS,if it is n'
'ot,it should not proceed with'
' installing disk with virus.This ought t'
'o keep hard disks free from'
' destroying their 0&1 blocks,but I haven'
't tested this yet.'
'This little program allows you  to insta'
'll two versions of Rastenbork'
'irus.The question remaining is what for?'
' I don',27,'t know.Coding viruses'
'ive much fun, so that is why I coded tho'
'se.  And what is use of this'
'nstaller for you?  Is there any sense? I'
' don',27,'t think so, but you can'
'end virus to any of your enemies and wat'
'ch him carefully.Treat it as'
' test of my work.'
'Please, spread this installer only to  y'
'our friends and use it within'
'any lamer you know.'
'If my viruses have caused any troubles t'
'o any scene dudes,please take'
'my deepest apologies.They weren',27,'t meant '
'in this way.'
'If you want  to contact the  author, for'
' any reason or  just for  new'
'friendship (no swap), please write to:'
'           PePe/tRSi,'
'400 Ketrzyn,POLAND'
'Greetings to anyone I have ever met on m'
'y way, and to those I haven',27,'t'
'had pleasure to know...'
'os.library'
'intuition.library'
```

```
          'Boot Virus Protector v5.4'
          'Vectors wrong!'
          'Boot contains SCA (or similar) virus !'
          'Cold'
          'Cool'
          'DoIO changed!'
          'A NPS production.'
          'DOS'
          'dos.library'
          'intuition.library'
          '    Panzer total anti virus system'
          'Virus destroyed!'
```

                          Detection tested 26.02.1995.

1.156 ConMan-Hacker

```
ConMan-Hack trojan:
-------------------
```

Packing type: Turbo Squeezer

The archiv "hackt.lha" contains a fucking CONMAN trojan ! The archiv
contains the file Hackt.exe, which is Turbo Squeezed.

```
hackt.exe packed:   12692 Bytes
hackt.exe unpacked: 12312 Bytes
```

It installs a new process with the name CLI(0):console.device and
writes a new file called C:Iprefs. This Iprefs is packed several
times and uses the 4eb9 linker method to unlink some strange stuff.

```
packed:    10820 Bytes
unpacked:  14216 Bytes
```

The "CLI(0):console.device" process will reset your machine after
it wrote the new IPrefs file.

The file itself contains an very old IPrefs and an, again packed,
destructive virus from a guy called CONMAN. It will try to destroy
many sectors by filling them with the word "CONMAN 1995". There is
no rescue for such sectors. The destructive routine is just looking
for "trackdisk.device", so no danger for harddiscs or so.

The IPrefs file will install a new process called conman.device. This
process contains the destruction routine. VirusWorkshop is able to
remove the dangerous DOIO() calls.

The ConMan viruses were mostly BBS hackers, now this guy reached a
new dimension. I got yesterday a phonecall from an irritated user
(someone of Krypton or so ?) and he told me about his file. He got
it from a BBS in Berlin, which is thought to be the homeplace
of CONMAN. This guy told me that he had downloaded it around 6.4.1995,

so this virus is on the wild.

                                        Detection tested 9.4.1995.

Special comment to RD10 of Osiris: It is pure bullshit to release a
warning like yours and to include the whole virus ! Try to think next
time a little bit more !

1.157   VTek22 LinkVirus (Typ A+B)

VTek22 Linkvirus and it's installer:

Around March 1995 there was a new version of VTek22 found, which
has some inner changes and increases the file with another length.

Warning ! In the file "viewtek22.lha" there is a new linkvirus !
The virus was uploaded to a box in Hannover around 24.08.1994. We
got around 29.08.1994. the first phonecalls concerning this virus
and spreaded short warning texts in Hannover and some days later
a warning appeared in the german Z-Netz. The description of this
archive says that it contains a new update of the wellknown viewtek
programm by tek. If you depack the whole archive, you will find a
guidefile and the viewtek mainfile. The mainfile is 93844 bytes long
and contains the installer for the new linkvirus.

The virus itself is located in the second hunk. The first hunk is
848 bytes long and contains some crazy texts:

'dos.library'
'S:HauptPfad'
'User/SysOp/UserDaten'
'BoxDaten/BoxParameter'
'User/xxxxxxxx/.INDEX'
'User/xxxxxxxx/.TXT'
'Absender : KFUserCheck'
'Betreff   : Bitte lesen >NEUERUSER.TXT<'
'Datum   : 10.08.1994'
'Uhrzeit   : 20:50:58'
'Bytes   : 1024'
'Empfänger : xxxxxxxx'
'09.08.1994 23.45.16   1 Asc SYSop'
'Neueintraege'

The archiv contains only one mailbox advertisement from a box
in Hannover. I meet the sysop of this box and got the
name from the uploader of the file. The username is xxxxxxxx.
(The same as in the ASCII text of the installer).
The installer is a modified viewtek 2.1.378 version dated
17.02.1994. In my opinion the first hunk is something like

a FASTCALL hacking system, which is maybe able to modify userdata
and some other boxparameters. It's possible that this file was
not uploaded by xxxxxx, but by somebody else and the sysop of this
board activated this virus and the userdata etc. were completely
changed.

But now to the exact description of this virus:

Linkmethod: adds a new hunk to the file ($3ed longwords=Typ A)
                                        ($462 longwords=Typ B)

Increases filelength by: 4036 bytes (Typ A)
                            4504 bytes (Typ B)
Kickstart version required: KS V37.xx or higher

The virus itself is not resident and creates only a new process.
The nodeentry will be in the way changed, that the nl_type flag
says that it is a task. The process has always the same name:
"trackdisk.device" and has the same priority as a normal trackdisk.-
device task. Many parts of this virus are crypted. The crypt-
routines are static, no polymorph or in other way "intelligent"
cryptparts could be found. The DOS routines are quite clever. There
are no direct DOS jsr's (e.g. jsr -36(a6), to close a file). This
routines a hidden or in other words another technic will be used
for it (global). Due to this special effect, all DOS function scanning
programms like SpyDos, HackDos or SnoopDos will be cheated and no
output is made by this programms.

The virus only links itself on other files, if the following
conditions are true:

-more than 9 sectors free
-device must be validated
-no file longer than 143360 bytes will be infected
-file must be executable
-filename is one of the following:

 c:zoo , c:shrink , c:iprefs , c:mount , c:dms , c:setpatch,
 c:version, c:lharc, c:arc, c:fastgif, c:vt, c:show, c:ppshow,
 c:ed, c:iconx

This virus contains many cryptroutines, which are not used as far
as I can see up to now. A displayroutine or something like a text-
writer seems to be not in the virus. The virus contains a crypted
block, maybe this block contains a name for this little bastard.
We are working on it...
The virus contains a routine, which manipulates the controll-
register B from CIA-B and the controllregister for the synchro-
nisation from the blitter with the screen. I don't know exactly
what this will affect exactly.
The hunk routine recognizes the following hunks: $3ec and $3eb.
I expect some problems with programms with some other special

hunks. VIRUSWORKSHOP 4.1 will be able to remove this virus and
the infected programms will be working, even if they were not
working, when they were infected.

The way of manipulating the hunks is quite similar to the method,
which the Burn Viruses use.

Detection tested 05.09.1994.

Detection of Typ B tested 20.3.1995.

1.158 AX-Fucker

                    /X Fucker Linkvirus:

Kickstart 2.x only based on the DOS patchroutines.
MC68040: yes (without caches)
Increases filelength by 928 bytes

This is an ordinary linkvirus, which adds its code to the first
hunk and does only work on the following conditions:

- file contains only 1 hunk
- no reloc hunk at the beginning

It puts an additional $3f1 hunk in the beginning containing the
string /X Fucker. The virus patches the DosOPEN() and DOS LoadSeg()
vectors and is not resetproof.

Based on the $3f1 file at the beginning, better viruskillers could
atleast say that a $3f1 hunk is at the beginning. The virus itself
is coded quite bad and seems to be spreaded bad.

The first infected archive was the "axripii.lha".

The LoadSeg() routine is only thought for the infection of loaded
files. The DosOPEN() routine contains a destruction routine, which
is timebased. Starting with 24 Feb '95 all opened files will be
opened using the NEWMode (they will be cleared), if the access is
to the BBS: directory.

Hexdump of parts of this virus:


```
0000: 000003F3 00000000 00000001 00000000    ...ó............
0010: 00000000 000000E5 000003F1 00000003    .......å...ñ....
0020: 2F582046 75636B65 72000000 000003E9    /X Fucker......é
0030: 000000E5 48E7FFFE 2C780004 43FA02F8    ...åHç.þ,x..Cú.ø
0040: 4EAEFE68 41FA02EC 20800C39 005A0000    N®þhAú.ì ..9.Z..
0050: 00006700 03046104 4AFC02FE 13FC005A    ..g...a.Jü.þ.ü.Z
0060: 00000000 2C780004 2A7A02C8 203C0000    ....,x..*z.È <..
0330: 351D0001 12F0646F 732E6C69 62726172    5....ðdos.librar
0340: 79000000 03F10000 00032F58 20467563    y....ñ..../X Fuc
```

```
   0350: 6B657200 00000003 4CDF7FFF 41FA0004     ker.....Lß..Aú..
```


                         Detection tested 12.3.1995.

    There appeared a quite bad description of this virus, which is
    nearly in all points wrong.
                    Click~me
                     to read it.

1.159   AX-Fucker warning by SHI Main

                                                         03-03-95
                        SAFE HEX WARNING

The archive axripii.lha 120046 bytes is a trojan and contains a harddisk
damage program called Fucker virus. The dangerous files is the following:

        AmiBBB .... 2092 bytes unpacked
        AmiRip .... 1348 bytes unpacked
        RipCon. Device .. 4324 bytes unpacked

This trojan will overwrite your hardisk in no time with a lot of garbage
and all your files will be lost. No salvage is possible. Check out that you
don't spread or run this nasty ones.

                                      Kind Regards

                                   Erik Loevendahl
                                SAFE HEX INTERNATIONAL

1.160   NComm32_Trojan

                    COP Typ A Trojan:
    ----

    other possible names: NComm 3.2 Trojan

    Length: 121896 (StoneCracker 4.04 packed)
            226116 (unpacked)

    This is a typical lame trojan. It contains a routine to scan every file in
    the S: and BBS: assigns and to overwrite it with the a new file, which only
    contains the text "
                CIRCLE~OF~POWER~1995!
                ". The code of
    the trojan looks not like a beginners work, it will be used some indirect

adressing and several other stuff.

The file is 2 times modified using the wellknown
                4eb9~linker
                 and visible
texts in the virus are "s:", "dos.library" and "CIRCLE OF POWER 1995!".

                          Detection tested 25.03.1995.

COP Typ B Trojan:
----

other possible names: CED4, LHA30 or OPUS5

found in CED4 (filelength 174500 powerpacked and protected)
found in LHA30 (filelength 69888 packed with StoneCracker 4.04)
found in OPUS5 (filelength 347308 powerpacked and protected)

Nearly the same routines, but a lot of more assigns will be infected
(devs: libs: ncomm: bbs:) and the new written text is "Circle of Power'95".

The file OPUS5 is again a little bit different. The string is only COP'95
and there will be destroyed e.g. no ncomm: assigned files. The protection
in CED4 and OPUS5 is the same. Due to a additional hunk at the beginning of
the file, no unpacker can recognize the packed stuff. Nothing tricky for a
profi....

The additional hunk is a so called HUNK_NAME and only contains the string
"*Art". I know this string as a sign for a programmer some time ago, but
don't remeber his name.

                          Detection tested 28.3.1995.

COP Typ C Trojan:

Possible other names: SinFo Trojan
Filelength 2852 bytes

Same behavior as the last ones.

              Click~me~to~read~some~crazy~stuff~about~SHI~and~COP~!
                COP Typ D Trojan:

Found in VirusWorkshop 5.0 fake: 135744 bytes unpacked
            FutureTracker fake: 317608 bytes unpacked
       AmiExpress 5.0 ACP fake: 71904 bytes unpacked

This trojans only contain the destructive routines, a 4eb9 linker in a
quite new generation, a music player and a little routine to display
some texts about COP.

The archivname of the fake VirusWorkshop 5.0 was: trsi-vw5.lha. First I
heard about this fake from a textfile called Hack Report by SHI. No warning
appeared from this guys until now.

In the faked virusworkshop archiv all documents including the newfiles were
missing and the idiots used a VW 4.9 archiv to create it.

File_ID.DIZ from the fake VirusWorkshop 5.0 archiv:

```
_____  _____
\  .    ___.___._\ensuremath{\lnot}\/  ____/_____)  TRiSTAR &
 \/|  .|   |  \ensuremath{\lnot}| _/_____\ensuremath{\lnot}\|    \ensuremath{\ ←
    lnot}|
    |  ||   |   : \ensuremath{\lnot}\   \ensuremath{\lnot}V \    ||     RSi
    |___|  |___|_____/_____|
·+*#*+·^·TRN!·|____\·+*#*V·^·+*#*+·PRESENT!·
            VIRUS-WORKSHOP 5.0
```

(looks like the original archiv descriptions)

File_ID.DIZ from the fake FutureTracker archiv:

```
        _ _ _____ _ __.
.--------\\_   ___/___    /  _____/--^-|.
|  bACk tO  |    |   __/  _/_____   \    |:
| tHe rOOTs l____|___/     _____||
|------------------/_____\----------cDr-|
| FutureTracker - ProTracker Clone by PSI! |
| 6 channels, 256 samples, full MIDI port! |
`------------------------------------------'
```

Click~me~to~see~a~picture~of~the~COP~trojans~!
(This picture was taken out of a warning from VH-Denmark !)

 COP Typ E Trojan:

 Detected in Copkiller 1.1 : 8428 bytes unpacked
          MST-CA12   :   same length

 Changes in the code: Now it is assemblycode and the existence of an
 infoblock will be checked. The rest of this trojan is the work of a
 bad coder. The pointerstructures will be modified incorrect and the
 damage will be only caused in devs:.

There is a crypted part in the file, which is crypted using a logical
loop. All overwritten files ($29 bytes long) contain the string:

                [cOp]: Scotch & Khanan on tour '95 :[cOp]

In the crypted part you can read:

                '[cOp]: Scotch & Khanan on tour '95 :[cOp]devs:'
                's:'
                'bbs:'
                'L:'
                'NCOMM:'

Normal readable text in the file:

                'dos.library',0
                'CoppKiller v1.1 by Jolle / SHI © 1995'
                'Attention: File %s may be infected with a'
                ' cop trojan, do you want to run this file anyway?'
                'LBs:Trojan.Log',0
                '"LMore than 5 Mode Newfile in last 2 sec'
                'onds terminating orginating process'

(Even this texts appears to be a little bit suspicious, but I think
 I saw a real 1.0 version of the Copkiller flying around, which was
 spreaded by SHI, too)

File_ID.DIZ of the spreaded file:

         _____ _____ ___   DIRECT UPLOAD FROM
      __/ ___// / // /\   SAFE HEX
      ___ // _/ // / /   INTERNATIONAL
      / / // __ // / /   -------------
     /____//__/__//__/ / AGAIN A NEW TOP-HIT!
     _____\/   -------------

        ->> PRESENTS C.O.P. Killer v1.1 <<-
     An excellent trojankiller that recognises
     the new encoding system used by C.O.P.
     Also read about the SHI reward >$5000<
     for the name of a virus programmer.

```
\textdegree{}\textdegree{}\ensuremath{\pm}\ensuremath{\pm}$^2$$^2$Û$^2$$^2 ←
    $\ensuremath{\pm}\ensuremath{\pm}\textdegree{}\textdegree{}  Update ←
    18-05-95 \textdegree{}\textdegree{}\ensuremath{\pm}\ensuremath{\pm}$^2 ←
    $$^2$Û$^2$$^2$\ensuremath{\pm}\ensuremath{\pm}\textdegree{}\textdegree ←
    {}
```

The document for this trojan is faked and contains some bullshit
information like "COP guys are good programmers, why don't you
programm other things like viruskiller".

The MST-CA12 contains the following ID:

```
 .--------[_____ mYSTIC _____]--------.
 |__ _____\   \____   /   /_____|____
 /   |  \    /   /___/_/  ___/_____/  ___/__
/         \___  /____  \   \   /   \   \    /
\___\/   /____/   /   /_____/_____/_____/
  | /___/   _____/AdN!          _|_
  |                                 \_/
  |   cALLERSLOG 1.2 fOR lOGIC bBS    |
  | 100% fIXED - iNC iFF sCREENsHOT   |
  |                                   |
  '-[LoGIC DeVELOPeMENT]-[/X cOMPAT]-'
```


Same code as in Copkill1, nothing more to say about it ! Circle of Power
nowadays seem to become a little bit $%%$% Why do they pack an iff-
picture into this archiv with a little lists of mailbox users like
Fury, 2fast and Antichrist ? I cannot understand it.

                    Detection tested 21.05.1995.

COP Trojan Typ F:

The file lzx130.lha with the File ID:

LZX Version 1.30 (Evaluation) Jun 5, 1995

and the following files:

```
LZX_68040              65384 ----rwed Gestern    07:55:44
LZX_68020              64896 ----rwed Gestern    07:55:34
LZX_68000EC            67680 ----rwed Gestern    07:55:20
```

contains a COP trojan ! Don't start it, it will trash your HD !
It tries to fuck up the following dirs:

```
"ncomm'
'bbs'
'devs'
's'
'envarc'
'libs'
```

All files will be overwritten with the following text and NO rescue is
possible:

```
                          =CIRCLE OF POcER=
             [ THE RETURN OF THE POcER PEOPLE! PHEAR US! ]
```

The destruction routine is the same as in the last one and does not
seem to be from a prof. coder.

This time it was added a history file to cheat the user.

A special thanks goes at this point to Apollo for the warning ! Sorry
for your HD....

Another LZX version got infected by COP, too. This time it is lzx125.lha.

```
LZX_68040                    65456 ----rwed
LZX_68020                    65708 ----rwed
LZX_68000EC                  68492 ----rwed
LZX.guide                    92373 ----rwed
```

In the File ID stands:

LZX 1.25 (NO FAKE)

All executables are infected by the COP trojan !

NOTE: Another COP trojan appeared at the end of October'95. It was in a
fake of a new AmiExpress version (LSD_AE42.lha). Functions like in the
previous COP versions, but this time the decoding fails and there CAN't
be a damage. A warning popped up, but how it can happen, if no visible
string , even not the dos.library, can be seen.

Comment 05.11.1995: Another COP trojan appeared in the file DMV05.exe.
It's just a small COP trojan as always. No new functions, only another
text and some changed directories...

1.161   Some words about COP...

Some words about Circle of Power (short: COP)

This seems to be a scandinavian hackergroup, which hacks/formats
mailboxes for money or simply just for fun.

Here a shortcut from a formatcapture, which they spreaded on the boards:

                    [-+-] PHEAR THE CIRCLE OF POWER!! [-+-]

Whatever: ~~~~~~~~~ If u wanna hack/format yer enemies for a small fee, lets
say some cards or $$$, contact us. This service is only available for swedes
tho. The phone number to our VMB will be stated in the next release, ofcuz a
toll-free 020 number. (no shit. heh)

                                        -[·k·H·A·N·A·N·]- / -$\div$C$\ ←
                                            div$O$\div$P$\div$-

Members: ~~~~~~~~ Khanan - Scotch - Iconxpert

1.162 ahkeym_Trojan

AhKeym-Trojan:
----

filelength: 2160
other possible name: Heavne-Master-Key-Maker Trojan

Possibly programmed in Arexx and then made executable via a Arexx compiler.
All texts are crypted, only the normal access to the rexx#? libraries will
be shown. This is a virus, which tries to kill the following stuff:

- Many files in the prometheus: directory (Prometheus is a german mailbox
  programm)
- All files in the directories sys:c/ sys:l/ sys:libs/ sys:l/

Then it tries to kill various RDB via the KillRDB command. Accessed devices
are oktagon.device and scsi.device.

The whole stuff is programmed very lame, but effective.

After decoding you can read a lot of text in the file:

Heaven-Master-Key-Maker V1.1
fuer die neuen sichereren Keys :
Serien#.fuer.Tools.. :
Serien#.fuer.Checker :
Serien#.Sec. Abfr... :
'Key fuer Checker, Tools oder Beide.. :
delete >NIL: sys:s/startup-sequence'

```
sys:c/delete Prometheus:pmbs.key');
sys:c/delete Prometheus:daten/#?')
'Fetich =;-)))
'Das Key liegt in RAM:T....... have fun ( drueck ne Taste )'
sys:c/reboot'
 call ciao;
```

Original File_ID.Diz of this file:

```
    ____/\____:__/\ _ ____/\_____
   \:::.    \ensuremath{\lnot}:    Y  \     .:::/
    \_::. _____    | __\___.:__/
    /    __) /    l/ \ensuremath{\lnot}\./   Y   FAiRLiGHT
 .::\    | .\   /    .    |.:. .::.:::\
     ___!:.::\ _____:____NeB::..
================\/======:==================
         A-Heaven Master keymaker
           for the NEW key's
```

                                   Detection tested 25.03.1995.

1.163   Devil-Zine10-BBS-Hacker

```
Devil-Z10 BBS Trojan:
---------------------
```

other possible names: Devil-Zine10 Hacker

```
3 files: l/disk-validator (1848  bytes unpacked)
         ../.fastdir     (840   bytes unpacked)
         c/.fastdir      (9800  bytes Turbo Imploder packed)
                         (16696 bytes unpacked)
```

This virus was found on a LSD CD in the ZINE10 diskmag directory. I have
the original ZINE10 from BRS and this does not contain the virus, so I
expect a later infection. All kind of the code look like the work of a
guy called Devil, who coded in earlier days a lot fo this shit.

../fastdir file:

This is just somekind of installer. It reads the 880 block from trackdisk.
device unit 0 and set the validate flag illegal. Due to this routine, all
kickstart 1.x systems will try to load the disk-validator to repair the
"failure".

Readable texts in this file:

```
'dos.library'
'ZINE10:'
'FTSCNU'
'trackdisk.device'
```

l/disk-validator

This is just a loader routine for the file c/.fastdir. It loads via LoadSeg()
the code and starts a new process with the name "Filesystem". Nothing more.
The codes is partly crypted. It looks for the task/process "SnoopDos" to
make sure, that the old SnoopDos is not in memory active. SnoopDos 3 will
be not detected.

Readable texts in this file:

```
'dos.library'
'ZINE10:'
'FTSCNU'
'File System'
'SnoopDos'
```

c/.fastdir

This is the "main" file of the bbshacker. It contains a lot of directory-
pathes to several BBS (AmiExpress) dirs. This file scans through this
dirs and looks for special files, which will be just recognized at their
filelength. Then the code will be manipilated. Probably in the past some
security doors or stuff like this had this filengths and the virus/hacker
tried to hack it in this way. This part checks the existence of
SnoopDos,too.

After decryption you can read the following texts in this file:


```
'BBS'
'DH0'
'DH1'
'HD0:'
'HD1:'
'DH0'
'DH1'
'HD0'
'HD1'
'BBS:'
'DH0:BBS/'
'DH1:BBS/'
'HD0:BBS/'
'HD1:BBS/'
'DH0:'
'DH1:'
```

```
'HD0:'
'HD1:'
'SnoopDos'
'dos.library'
```

Detection tested 27.3.1995.

1.164 Revenge of NANO fileviruses

```
Revenge of NANO I Virus:
------------------------
```

```
Type = Filevirus
Length = 1412 Bytes
Kickstart 3.0 : yes
Patched vectors: CoolCapture and OldOpen ()
```

This is a quite simple filevirus. It simply patches the Exec OldOPEN()
and the Coolcapture to stay resident. The virus writes itself as an
invisible file with the name "$a0a0" to disk and inserts this name in
the first position of the startup-sequence.

The new written Startup-Sequence is always $bc0=3008 bytes long and
can contain several garbage, if the original startup-sequence was too
short. If the original startup-sequence was longer, then the last entries
will be lost and no rescue is possible.

Under special conditions the virus will open a requester saying some
stuff or will change the title of the actual window. All in all a harmless
virus without any special dirty tricks inside.

Visible texts in this virus are:

```
'dos.library'
':s/startup-sequence'
'I hate Commodore !!!'
'Revenge of NANO !!!!'
'...another masterpiece by  N A N O !!!'
'  GREETINGS TO:'
' 1 Byte Bandit, Byte Warrior,DEF JAM, DiskDo'
'ktors'
' B FANTASY, Foundation For The Extermination Of Lamers,'
' N I.R.Q. Team, Obelisk Softworks Crew, S.C.A., UNIT A ...'
```

Detection tested 8.2.1995.

1.165 ConMan-hackt.lha-trojan

```
ConMan-Hack trojan:
-------------------


Packing type: Turbo Squeezer

The archiv "hackt.lha" contains a fucking CONMAN trojan ! The archiv
contains the file Hackt.exe, which is Turbo Squeezed.

hackt.exe packed:   12692 Bytes
hackt.exe unpacked: 12312 Bytes

It installs a new process with the name CLI(0):console.device and
writes a new file called C:Iprefs. This Iprefs is packed several
times and uses the 4eb9 linker method to unlink some strange stuff.

packed:    10820 Bytes
unpacked:  14216 Bytes

The "CLI(0):console.device" process will reset your machine after
it wrote the new IPrefs file.

The file itself contains an very old IPrefs and an, again packed,
destructive virus from a guy called CONMAN. It will try to destroy
many sectors by filling them with the word "CONMAN 1995". There is
no rescue for such sectors. The destructive routine is just looking
for "trackdisk.device", so no danger for harddiscs or so.

The IPrefs file will install a new process called conman.device. This
process contains the destruction routine. VirusWorkshop is able to
remove the dangerous DOIO() calls.

The ConMan viruses were mostly BBS hackers, now this guy reached a
new dimension. I got yesterday a phonecall from an irritated user
(someone of Krypton or so ?) and he told me about his file. He got
it from a BBS in Berlin, which is thought to be the homeplace
of CONMAN. This guy told me that he had downloaded it around 6.4.1995,
so this virus is on the wild.




                          Detection tested 9.4.1995.



Special comment to RD10 of Osiris: It is pure bullshit to release a
warning like yours and to include the whole virus ! Try to think next
time a little bit more !
```

1.166 Devil-VScan-AmiExrexx Hacker

```
Devil-VScan-Trojan:
-------------------
```

Filength: 37896 bytes

other possible names: V-Scan 5.05 fake/trojan
first detected during a CD scan from a german pd compilation

This is a changed version of V-Scan by Arthur Hagen. There was linked
an additional hunk using the 4eb9 linking method (a quite old version
was used) and this hunk contains a bbs or to be more precise an AX-
bbs hacker, which modifies user.data. The code looks like the work of
a guy called Devil, so I decided to call this one Devil-VScan. it has
nothing (?) to do with the actual VScan programm by Gabriele Greco
(atleast I think so).

Shortcut from the original document:

5.03:   Works with the A3000(!). Recognizes ZKick 2.30. No longer
                 reports some odd files as (C) Steve Tibbett. Sorry, Steve!
                 Two new crunchers added (TurboImploder 3.1 and PowerPacker
                 3.0a). Will now handle overlayed programs correctly. Will
                 recognize saved bootblocks. Analyze mode much improved.
                 Works for files larger than 1Mb. Some other bugfixes.

5.04:   Nothing much, just added the Centurion file virus (yawn).

5.05:   *** WARNING *** This is a bogus version not made by myself!
                 Avoid this one at all costs!

                            Detection tested 15.4.1995.

1.167   Some more thoughts from my place

Some days before the SINFO10 COP trojan appeared, the VirusZ_II 1.16
version was released by Georg Hoermann. He mentioned in his history
file, that he added recogntion codes for new viruses and mentioned the
Circle of Power viruses. This is not 100% correct, because he only
can recognize the viruses, which he has. As said some days later the
SINFO10 trojan appeared and VirusZ could not recognize it.

The file-id.diz of the SINFO trojan looks like this:

```
.--------------------------------------------.
| SYSTEMINFO V1.0 BY JÜRGEN HÜNSMANN 1995! |
| A VERY GOOD REPLACEMENT OF THE INFO CMD! |
```

```
`------------------------------(baron)-'
```

Some days later I found on a ELITE bbs in germany a file called
vzwarn!!.lha
from SHI. As I wondered a lot about this, here is the file-id.diz from the
SHI release:

```
    _____ _____ ___    DIRECT UPLOAD FROM
  __/ ___// / // /\      SAFE HEX
  \___  // _/ // / /    INTERNATIONAL
  / / // __  // / /     -------------
 /____//__/__//__/ /    AGAIN A NEW WARNING
 _____\/       -------------
```

```
     A WARNING ABOUT VIRUSZ V1.16.
  Don't trust the cop virus recognition!
  to trust virusz's cop recog. COULD BE
  VERY FATAL!!
```

\textdegree{}\textdegree{}\ensuremath{\pm}\ensuremath{\pm}^{2}^{2}Û^2^{2}\ ←
    ensuremath{\pm}\ensuremath{\pm}\textdegree{}\textdegree{} Update 16-04-95 \ ←
    textdegree{}\textdegree{}\ensuremath{\pm}\ensuremath{\pm}^{2}^{2}Û^2^{2}\ ←
    ensuremath{\pm}\ensuremath{\pm}\textdegree{}\textdegree{}

This warning contains again the wellknown SHI contact texts and this little
text:

```
VZWARN!!.TXT   1856  04-16-95    .-------------------------------------------.
                                 |      A WARNING ABOUT VIRUSZ V1.16.         |
                                 | DON'T TRUST THE COP VIRUS RECOGNITION!     |
                                 | VIRUSZ IS SAID TO RECON THE COP VIRUS.     |
                                 |   WE TESTED IT ON THE COP VIRUS IN THE     |
                                 | ARCHIVE CALLED SINFO10.LHA AND IT DOES     |
                                 |   **NOT** RECOGNIZE THAT COP VIRUS!!!      |
                                 |    THE COP VIRUS HAS PROBABLY SEVERAL      |
                                 | GENERATIONS OF ITSELF. TO TRUST VIRUSZ'S   |
                                 |    COP RECOG. COULD BE VERY FATAL!!        |
                                 `-------------------------------(baron)-'
```

WARNING! WARNING! WARNING! WARNING! WARNING! WARNING! WARNING! WARNING!

                         ABOUT VIRUSZ 1.16

THIS IS SNAPPED FROM VIRUSZ GUIDE:
==
                      VIRUSZ II REVISION HISTORY
==

 1.16   Changes/Additions since 1.15:
         - Added patches: DosPrefs, TWA, PowerSnap and a new version of
           ToolsDaemon. Thanks to Rudolph Riedel for sending these. ***>>   -
Added viruses: Circle Of Power, /X Fucker, Rastenbork 1.2, ***
           Rastenbork 2.0, Rastenbork Installer, World Clock Fake.
           Thanks to Markus Schmall and Jan Andersen for sending them.

This version claims to recognize the "circle of power" (cop) virus, but it
does **NOT** recognize this virus in the sinfo10.lha archive!!! don't trust
virusz when it comes to the "cop" virus!!!

TO TRUST THAT VIRUSZ RECOGNIZES THE COP VIRUS COULD BE VERY DANGEROUS AND
FATAL TO YOUR VALUABLE DATA ON YOUR HD'S.

                        So take care with this!!!
                 you have been warned!!!!!!!!!!!!!!!!!!

WARNING! WARNING! WARNING! WARNING! WARNING! WARNING! WARNING! WARNING!

Signed.

The Baron The West BBS, Sweden

  The name BARON is mentioned in the virus archiv, in the SHI warning and
  in the several FILE-ID.DIZ files. The warning from the baron never appeared
  in Germany.

  If SHI warns you, because of a single fail recognition, I could give you
  several wrong recognitions of SHI killers. I think it is just a unfair
  behavior against a person (Goerg), who has no netaccess and cannot defend
  himself.

1.168   Icon Trojan = Icondepth 1.3 trojan

                  Icon Trojan:
  ----

  other possible names: IconDepth (1.3) trojan

  Filelength: 2384 bytes (packed with PowerPacker 4.x)
            4188 bytes unpacked

  Based on a third party information, the programm is in large parts
  comparable to the
              SINFO
               trojan from the
              COP
               guys.

  This is supposed to be a tool to decrease the planenumbers in Icons.
  This routine is buggy and or done by full knowledge of the destructive
  workings. Some bytes in a lot of files will be changed and cannot be
  repaired !

  The code looks like a partly optimized assembler code, but code be done
  by a ordinary C compiler, too.

  File ID Diz from the archiv:

  IconDepth V1.3! If you are using
  MagicWB then this is what you need!

```
50% faster when using WB!


The following directories will be affected from the trojan:

'sys:prefs/'
'sys:devs/'
'sys:l/'
'sys:c/'
'sys:libs/'

In this directories there are only a very few icons, so it looks even
more suspicious.

The trojan prints the following text to keep the user friendly:

'Hold on while IconDepth V1.3 is converting your icons!'



                                       Detection tested 27.04.1995.



Another virus appeared in this series. This time it appeared in an
archive called "
                TRSI-INS.lHA
                ". Be sure that we don't have anything
to do with it.

Another virus appeared from this series in the archive ORB-KC.DMS.

This virus will be called from another viruskiller: KidCurry (probably
based on the diskname).


This virus is located this time in the file hd_install.exe.

Filelength packed with PP4.0: 2756 bytes
   "   "       unpacked      : 8052 bytes


It modifies exactly the same bytes in the file and does not seem to
be coded in asm. I suppose it is coded in a new version of AMIGA-E !
```

1.169   Creator 1.0 and 1.1 trojans

```
Creator V1.0 and V1.1 trojans:
------------------------------

Spreaded in Germany around 10.4.1995.


The archives only contain a renamed and very old format command
and a little script, which executes this command. The script is
only 40 bytes long and contains only this texts and nothing more.
```

Here the short document for both of the files: (Version 1.1 is spreaded only
as update of this!!!)

```
                              ----------------------------
                              THE cREATOr V1.0 © 04-10-95
                              ----------------------------
```

What Is This Crap? ------------------

Well, with "cREATOr" you're able to choose your own ms (mili seconds) for your
harddisk. Normally it depends on which harddisk/cpu you've got into your amiga
computer! But this fantastic program shall take it all over by itself (after 1
year hard coding)...

How To Get Started? -------------------

Just copy the file cREATOr.DAT to your S: directory on your harddisk! Than
copy the file cREATOr.SCR to your C: directory on your harddisk! Now type from
SHELL or CLI "EXECUTE C:cREATOr.SCR" !!! Than you'll be prompted to start the
program when you like by hitting RETURN. After hitting RETURN the program
shall write and test some info on your harddisk and cpu !!!

The Good Results: -----------------

Well, I've tested it by a lot of friends and they were all very happy with
this litte but powerful program !!! I hope you like it and don't forget to
spread it as much as you can. It's all free ware...

Signed: CREATOR 1995

                              Detection tested 29.4.1995.

1.170 CChack2 /X Trojan

```
      CCHack2.exe AmiExpress trojan:
      ------------------------------

      Filelength: 11368 (with 2 File_ID.DIZ)
                  11216 (without    "      )
                  11056 pure file


      This is supposed to be a tool for phonephreakers to get control of
      calling cards from the amercian telephone company MCI. In real this
      is just another AmiExpress trojan, which tries to modify the
      user.data. The code is written in C and contains the suspicious
      strings a little bit crypted.
```

```
'MCI CallingCard Hacker by ByTe%s/Finland'
'Usage: %s<CALLINGCARD NR.>'
'Not Enough digits!!!'
'Too many digits!!!',0
'Usable Nr.%d : %7.7s%7.7s'
'PaCkEr'
```

File_ID.DIZ:

```
'FLIDCaLLiNg CaRd CodEr'
'ekkeR GRatIs BellUHHHHH!!!!!'
'Op KOstUUUHHHH VaN IEmaND AndErs!!!!!!'
' HEHEHEHEHEHEHHHEHEHEHEHEHEHEHEEHHHEHEHEH'
```

Detection tested 14.05.1995.

1.171 Pentagon

```
                  Pentagon Virus_Slayer Viruses 1-2a:
---------------------------------
```

```
Kickstart 3.0   : yes
Clones          :
        Dynamix~Viruskiller
                Changed vectors : Kicktag, Kickchecksum, DOIO und  ↩
                    Coolcapture
```

This bootblock pretend to be a viruskiller for several viruses
like the old Northstar and Byte Bandit viruses.

It will copy its code to $7fb00 (direct without allocating it)
and tests its existence in memory only by checking a longword
at $7fbXX.

If a bootblock access was detected, it will search for some
longwords (very unsecure) and if a virus was found, it will
be tried to overwrite the bootblock with the own code.

No tricky stuff, no crapted routine. A "virus" from the old
time.

1.172 Dynamix

```
Dynamix Bootblockvirus:
-----------------------
```

This is only a little clone from the Pentagon~Virus~Slayer~.

        The visible texts got changed. Better play with your joystick instead
        of this bullshit.

        'The DYNAMIX VIRUS KILLER V4.0 [/] by DYNAMIX 1991 !'
        'No greetings, no regards to anyone!   '
        'Z2Virus oder alter Antivirus ist auf der Disk!!!'
        'd<Entfern den Schreibschutz und drücke rechts'
        '(PLINKS kontrolliert es (Oh nein!)   RECHTS: Löschen'
        'DYNAMIX [/] in 1991! Terrorists are every where!!!!!!!!!'

1.173 Biomechanic

                    Background for this trojan:

Warning ! The file TRSi-INS.lha is no TRSi release and contains a fucking
trojan ! In the middle of the 10.6.1995. one of our members (NIKE/TRSi)
got a call on the BBS from a guy called GRYZOR, who is supposed to be the
leader of Circle of Power (COP), and this guy said to NIKE that TRSi is
lame and such things. Later he uploaded there a file called TRSi-INS.lha
to this board and NIKE wondered a little bit and contacted me and the
other TRSi guys. So this virus is now (10.6.1995. 18:30 o'clock) about
6 hours old. Let us stop this bastard and finally get a solution for
the COP problem (hi Apollo and Noise Belch).

Biomechanic Trojan
----

other possible names: TRSI-INS Trojan, TRSI-MEM Trojan, bio-warn.lha
Type: Destruction only
Destruction caused by: simple bytemodification

This are no TRSi releases ! It is just a fake !

In the File-ID it is stated that this are some hd installers for actual
games. In real this is just a trojan, which will manipulate your files
on your HD.

The contents of the archive TRSI-INS.lha:

ViroCop-HD_install.exe   5912 ----rwed 02-Sep-92 12:49:54
SWOS-HD_install.exe   9588 ----rwed 02-Sep-92 12:51:12
SensibleGolf-HD_install.exe   4776 ----rwed 02-Sep-92 12:51:24
Mortal-Kombat2-HD_install.exe   5512 ----rwed 02-Sep-92 12:50:12
MCI-CARDS4-FREE.EXE   5912 ----rwed 02-Sep-92 12:49:30
Embryo-HD_install.exe   6764 ----rwed 02-Sep-92 12:50:24

The contents of the TRSI-mem archiv:

```
1-> asylum kixx! <-1             Dir ----rwed Heute          08:43:15
2-> asylum roxx! <-2             Dir ----rwed Heute          08:43:15
3-> asylum kixx! <-3             Dir ----rwed Heute          08:43:15
File_id.diz                      380 ----rwed 02-Sep-92  12:43:28
Members.exe                     8584 ----rwed 02-Sep-92  12:50:32
trsi-mem.lha                    3423 ----rwed Heute          08:09:31


The contents of the bio-warn.lha archiv:

File_id.diz                      349 ----rwed 02-Sep-92  12:59:32
flake013.txt                    7988 ----rwed 02-Sep-92  12:59:00
Flake_killer_bio.exe            3264 ----rwed 02-Sep-92  12:55:14
1-> asylum kixx! <-1             Dir ----rwed Heute          10:15:03
2-> asylum roxx! <-2             Dir ----rwed Heute          10:15:03
3-> asylum kixx! <-3             Dir ----rwed Heute          10:15:03
```

FileUD of bio-warn.lha:

```
          _____     _
     ____/"""./###/____)_____
    /"""/    //_____   /"""/"".""/"____/_HELP!
   /    /   //"""/"  / //    /  //____    \_
   \       //    /  ____/   /  //"""""/X@!/
    \_____/\__/___/ ""_____/_____/
   -->><!VIRUS!<></____/-><>-!WARNING!-<><--
  'WARNING AND KILLER FOR BIOMECHANIC TROJAN'
   >>>-------------------------------<<<
```

FileID of TRSI-mem.lha:

```
_____  _____
\  .    ___.___._\ensuremath{\lnot}\/  ____/_____)   TRiSTAR &
 \/|  .|  |  \ensuremath{\lnot}| _/_____\ensuremath{\lnot}\|    \ensuremath{\ ←
    lnot}|
   |  ||  |  : \ensuremath{\lnot}\   \ensuremath{\lnot}V \     ||      RSi
   |___|  |___|_____/_____|
·+*#*+·^·TRN!·|____\·+*#*V·^·+*#*+·PRESENT!·
     A Small Intro Called -Schnelltro!-
If you are interrested in joining our forces
     then read the info in this intro!
```

The virus is looking for a special enviroment (a special bit combination)
and then manipulates the files:

Here a original PGP signed message:

```
0000: 89009502 05002FCF 1B5220F5 BA1075CB     ....../Ï.R õ°.uË
0010: 69450101 C11D03FF 7ED659E1 39C4AD2C     iE..Á...~ÖYá9Ä,
0020: CED29280 21FCEB79 5CF3B9A0 AADB5C14     ÎÒ..!üëy\ó$^1$~ªÛ\.
0030: D2B35295 5FFBE735 4E8070E1 A8C2C909     Ò$^3$R._ûç5N.pá¨ÂÉ. ->  0040:
2235ABB5 BE37E843 79CCD140 7AA2ACA5     "5«$\mathrm{\mu}$¾7èCyÌÑ@z¢\ensuremath{\ ←
  lnot}$\yen$
```

Here the manipulated one:

```
0000: 89009502 05002FCF 1B5220F5 BA1075CB      ....../Ï.R õ°.uË
0010: 69450101 C11D03FF 7ED659E1 39C4AD2C      iE..Á...~ÖYá9Ä,
0020: CED29280 21FCEB79 5CF3B9A0 AADB5C14      ÎÒ..!üëy\ó$^1$~ªÛ\.
0030: D2B35295 5FFBE735 4E8070E1 A8C2C909      Ò$^3$R._ûç5N.pá¨ÂÉ. ->  0040:
2235ABB5 BE37E843 79CC0002 B37800A5      "5«$\mathrm{\mu}$¾7èCyÌ..$^3$x.$\yen$
```

If you start the virus (it is in all the above listed files), a little
text will show up:

                  – b i o m e c h a n i c –

and the work begins. If the work is completed, the following text will
be printed out, too:

                  ... trashed your hd ...

and a directory named "biomechanic trashed your hd !!" will be created,
which is empty.

The file TRSI-mem.lha with the trojan members.exe is a little bit
different:

1. It will be printed

    "hi to markus schmall! catch me, if you can ! c.o.p sucks !

                  biomechanic trashed your hd"

The code looks quite good. This is not the work of a real beginner. The
guy behind has some programming knowledge. This way of programming is
better
than from the COP viruses. The programm uses indirect adressing and a lot
of stackusage, which cannot be done by a beginner (atleast I think so).

The code itself is WB startable (different to COP viruses I think) and
was probably not coded using a C compiler like the old COP trojans.

All files have the same recognition longwords, because only the end
of the files changes, the creator of it possibly only "incbind" some more
files to get different filelength.

Detection tested 11.06.1995.

A special thanks to NIKE/TRSi for all his effort and warnings ! Thanks !

In the bio-warn.lha archiv you will find the text
            Flake013.txt
            . Here a
little
            comment

about it.

Comment 5.8.1995. A new Biomechanic trojan appeared in sweden under the
name
                    LZX1.20~registered~bugfixed
                     version.

Biomechanic in VZ121 Fake:

Filelength: 80268 bytes (partly packed)
Same AmigaE code as always and packed again with Powerpacker 4.0

File_ID.DIZ of the faked one:

```
              _____     _
     _____/"""./###/____)_____
    /"""/    //_____    /"""/"".'/"___/_HELP!
   /    /   //"""/"   / //    /  //____    \_
   \       //    / ____/    /  //""""/X@!/
    _____/\__/___/ ""_____/_____/
   -->-<><><><><><>-</____/->-<>-  Presents-<><--
        VirusZ II v1.21 - (08.07.95)
   >>>----------------------------<<<
```


Faked history:

1.21   Changes/Additions since 1.20:
        - Added recognition for the following viruses:
          Circle Of Power (some new versions), TRSI-INS.LHA Biomechanic
          trojans, new version of Rastenbork link virus.

(ED: There is no rastenbork linkvirus on the wild...)

Biomechanic in VChCK659 Fake:

Filelength: 55428 bytes

(same as VZ121 Fake)

```
              _____     _
     _____/"""./###/____)_____
    /"""/    //_____    /"""/"".'/"___/_HELP!
   /    /   //"""/"   / //    /  //____    \_
   \       //    / ____/    /  //""""/X@!/
    _____/\__/___/ ""_____/_____/
   -->-<><><><><><>-</____/->-<>-  Presents-<><--
        Virus_Checker v6.59 (23-07-95)
```

```
 >>>--------------------------------<<<
```

History of this faked one:

6.59 Released 24 July 1995

Fixed some more small bugs. Fixed also a requester text looking better.

1.174 Fileghost3 Linkvirus

Fileghost 3 Linkvirus:

MC68040 and MC68060: yes
Kickstart V35 and above
Patched vectors: DOS LoadSeg()
Increases filelength by 1288 bytes
Detected: Jun'95 in the south of Germany

This is another linkvirus out of the Fileghost series. This linkviruses
just add their code to the end of the first hunk and then search for the
last "rts" and modify it to a "bsr.b" to get activated.

Differences to the previous versions of the virusfamily:

1. Some more indirect adressing
2. Test, if SnoopDos (FindTask "SnoopDos") is active
3. It will be searched for 2 longwords in the first hunk

        $53460C46 at offset $2A from the loadseg() memptr
        $2F49003C at offset $3A   "   "   "

   If you know, which programm has such longs in the first hunk, please
   let me know. Thanks.

4. The cryptroutine is a little bit advanced
5. The word $1994 will be used to check, if the virus already infected the
   LoadSeg() vector. This routine is comparable to Fileghost2 and to
   the Polygonifrikator viruses.
6. Depending on a spreading counter, the virus will set new windowtitles
   (see at the bottom of the description).

The fileghost virus contains no destructive routine. As on every type of
this type of virus, it is possible that programms, which need a 100%
correct hunkstructure (e.g. some packers) will get problems and will
not work.

The infection routine is a very lame modified version of the Fileghost2
routine. Probably the work of a beginner. A lot of files become 0 bytes
long based on a heavy bug.

I recieved several infected files, but could not spread them. The machine

always crashed. This was tested on A500+ and A4000. I can't find a big
bug in the loadseg infection routine, but I am not sure. The repairroutine
is tested with 5 files and should work properly.

New texts for the windowtitles:

'AUA! schlag nicht so auf die Tasten!'
'FileGhost3 – the nightmare continues!'
'Hallo DEPP!'
'Was machst Du denn als nächstes ?'
'Weißt Du eigentlich, daß Du dumm bist ?'
'Und schon wieder eine Datei weniger!'
'Gib mir mal 'n Bier!'
'Tötet alle Nazis + RAPER!'
'AMIGA kills PC! (HEHE)'
'INTeL Outside !'

                          Detection tested 15.06.1995.

1.175 Aibon_Installer_ACP-CTRL

Aibon Installer:
----

other possible name: ACP-CTRL
MC68040: yes
Kickstart 3.1: yes
Filelength: 56016 bytes unpacked

This is just another installer for the aibon virus. The aibon virus itself
is a destructive only virus (please refer to the aibon chapter in this
documentation). This is the installer and the especiality is, that it
starts the destructive work after writing the aibon file.

Detection tested 16.06.1995.

Visible texts from the file:

        'Nuv2.20'
        '$VER: Version v2.20 (Jul 17 1992, 14:13:'
        '54)'
        'Jul 17 1992'
        ',_Nuzmwriteport'
        'console.device'

        ...

1.176 Blieb6.exe /X Trojan

```
Blieb6.exe /X Trojan:
--------------------

Filelength: 7612 bytes unpacked

This is a quite old AmiExpress BBS trojan, which searches in a very
primitiv way for the config file from the AmiExpress system and tries
to manipulate it to give users a better access.

It will be searched on dh1 and dh0.


                         Detection tested 17.06.1995.
```

1.177 Karacic (GVP-HS15.lha) Trojan

```
        Karaçiç Trojan Virus:
        --------------------

        Filelength packed:     1460 Bytes (Rob Northern !!!)
                               1924 Bytes (unpacked)

        Other possible names: GVP-HS15 Trojan

        Works only with Kickstart 3.0 and ahead (V39 funtions will be
        used).

        Some other suspicius fact is, that the programm was packed using
        the Rob Northern cruncher, also called Propack. The file was
        afterwards modified a little bit, so that no existing depacker
        can unpack it.

        This trojan is programmed quite simple. The needed libraries will
        be opened and it will we checked for the old SnoopDos task.

        Then the file "s:nothere" will be tested. If it exists, no damage
        will be caused.

        Then a TimeDisplayAlert (timer some seconds) will pop up and show
        you:

                    LMB> Kill system RMB>Reboot


        The code analyzer behind is programmed like this:

        1.If the user gave no input in the 5 seconds and/or presses the
          right mousebutton, the system will be trashed using some basic
          format and delete routines.

        2.If the user presses the left mousebutton, then a ColdReboot
          will be performed.
```

SO DON'T START THIS AND IF SUCH A REQUESTER APPEARS, THEN RESET
YOUR AMIGA BY HAND !

The routine to show the Alert is a Kickstart V39 function. It will
be not tested, if the used system is really V39 or higher.

FileID of this archive (GVP-HS15.lha):

HardDiskSpeeder v1.5 ©GVP Inc. 1995
(a little cache program for HDs!)

...

If you start the programm, it will show you the following text:

'HardDiskSpeeder v1.5 installed ...'

If you start it using a "?", then the following text will show
up:

'HardDiskSpeeder v1.5 by GVP Inc. ©1995'

The trojan tries to destroy the following directories and devices:

dh0-dh4, hd0-hd4, l:, libs:, devs:, s: and c:

The formatted new devices will have the name:

'"Karaçiç Virus strikes back"'

                                    Detection tested 21.06.1995.

1.178 Scansystem.lha Trojan

```
Scansystem Trojan:
------------------

other possible names: none
Filelength: 10720 bytes (unpacked)
Found in  : scansystem.lha
Found     : Jun'95
```

This is another typical trojan. It pretends to be a system optimizer,
which should enable a MMU emulation (pure bullshit).

Here the FILE_ID.DIZ:

                    A Fast Optimizer For 68020-68030 Motorola
                    System +7% Faster ! Patch System Routines
                    and allow you to create a MMU Simulation!
                    Speed For ALL! Optimize your system !
                    This Famous Tool has been written in ASM
                    by CheckIn of NewIntelligent Tools Prod!

If you start it, it will open a window with the name:

        'CON:0/0/1280/1280/ SystemScan v0.6 by CheckIn ! in 1995'

Afterwards some messages appear and the directories "sys:libs","sys:devs",
"sys:c","sys:s" and "sys:L" will be investigated. The programm pretends
just to scan the files, in reality, all deletable files will be deleted.
If the programm fails to delete a file, it will give you a "FAILED..." How
nice.

As "replacement" the programm writes a file called "SYS:FUCK!" on the
disc, which probably should make it unpossible to recover the files. If
this file already exists, the programm will exit with the comment:

' System Already Scaned !'

Other messages, which appear during the scan, are e.g.:

' Scan Integrity of the System ! Please Wait ...'

The code was probably done using a highlevel compiler and not normal asm-
code (I hate to dissassemble compilercode).

                                        Detection tested 30.06.1995.

1.179 VCKey110.lha Trojan - Makekey

VCKey 1.10 Trojan:
----

other possible names: none
Kickstart: V37 and higher
Filelength: 9088 bytes (partly packed)
found in/when: VkKey110.lha/Jul95

This is said to be a cracked keyfile creator for the wellknown Virus-
Checker antivirusprogramm.

The FILE ID looks like this:

"

```
MakeKey v1.10 Keyfilemaker
for Virus Checker Cracked.
----------------------( EAGLE's NEST! )----
"
```

In reality this file contains a nasty trojan, which tries to format
your SYS: device (DOS1 bootcode) and give it the new name "Snupp!".
If I can read my autodocs correct, only a quickformat will be done.
Try to use Disksalv to recover the data on your sys: device.

In the unpacked code you can read:

"WiREFACE / dEMONS oF tHE pENTAGRAM * WHiPPED YOUR HD, SUKKAH !! We Look "
"Down Your Nose (Laughter)!"

The dangerous code was linked using the 4eb9 linking method on the normal
makekey programm from the actual VirusChecker distribution. The dangerous
code is packed with powerpacker 4.0 (5848 bytes long). This was probably
done to shorten the whole file and to crypt the visible texts. The unpacked
viruscode is 7588 bytes long.

(Do you really think that such a lame protection can stop a good antivirus-
 researcher from doing its job ????)

VT 2.74 and VW 5.2 atleast recognize a $4eb9 linker in the file. Another
viruskiller, which claims to recognize 4eb9 files, does not detect it.

There is a little document in this archive called MakeKey.readme:

```
"
MakeKey v1.00 cracked... presenting MakeKey v1.10 :)
```

This is a specially written program to allow users who have
registered to make a keyfile from the information they recieve.

*** But now you can enter any serial numbers you want ! ***
~~~~~~

It can be run from SHELL or WORKBENCH and opens a GUI.
It requires WB2.04 or better to run. Enter the data into the
gadgets and click on MakeKey and the keyfile will be generated.

"

1.180   SlinkV10 - Scanlink trojan - Wireface Typ B

```
Scanlink 1.0 Trojan:
--------------------

other possible names: Wireface Typ B
Code equalities: VCKey110.lha trojan
```

```
Kickstart: V37 and higher
Filelength: 8040 bytes (partly packed)
found in/when: slinkv10.lha/11.7.95
```

This is said to be a new kind of linkvirus/filevirus detector written by a
wellknown antivirus organisation.

The FILE ID looks like this:

```
~~~|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    ScanLink v1.0 - Latest hack in the war
    against viruses! This one can detect
    linkviruses yet unknown using new antivir
    technology. Latest from S.H.I
    |
~~~|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```


In reality this file contains a nasty trojan, which tries to format
your SYS: device (DOS1 bootcode) and give it the new name "Snupp!".
If I can read my autodocs correct, only a quickformat will be done.
Try to use Disksalv to recover the data on your sys: device.

In the unpacked code you can read:

"WiREFACE / dEMONS oF tHE pENTAGRAM * WHiPPED YOUR HD, SUKKAH !! We Look "
"Down Your Nose (Laughter)!"

The dangerous code was linked using the 4eb9 linking method. The dangerous
code is packed with powerpacker 4.0 (5940 bytes long). This was probably
done to shorten the whole file and to crypt the visible texts. The unpacked
viruscode is 7732 bytes long.

(Do you really think that such a lame protection can stop a good antivirus-
 researcher from doing its job ????)

VT 2.74 and VW 5.3 atleast recognize a $4eb9 linker in the file. Another
viruskiller, which claims to recognize 4eb9 files, does not detect it.

There is a little document in this archive called Scanlink/scanlink.doc:

  "

                              Scanlink v1.0
                              ~~~~~~~~~~~~~~

· This is a small and simple program that will scan all your
   devices for linkviruses.

   Well I can do that with any other virus program you say?

· Well what's so special about this is that the 'DOP' link
  virus / logical bomb is hardcoded into this proggy to also
  detect yet unknown versions of the virus which can't be
  placed for example in virus.library. If it finds an altered
  virus it will create LIBS:link.library and store it there
  for future use.

· This is FREEWARE, it will be implemented in future releases
  of virus killers from SHI, thus being SHAREWARE

                    The best to you all and happy hacking...

              ~~~~~~
                                S H I

                        Erik Lovendal Sorensen

                        Mon Jul 10 09:23:45 1995

              ~~~~~~

        "

The file appeared on the fast german boards at the evening of 11.7.1995. !

                                        Detection tested 22.07.1995.

1.181 WireFace Typ C Trojan

WireFace Type C Virus:
----

found in lzx120t.lha (trojan in lzx_1.20t.lha 83660 bytes long)
 and in hdtb409.lha (trojan in hdtoolsbox2 106508 bytes long)

Comment: 25.07.1995: Another WireFace Typ C trojan was found in
vchck660.lzx with the mainfile containing 52400 bytes.
This trojan seems to be based on the (at this time) old Virus
Checker 6.56 release.

Found when: night from 21.07. to 22.07. 1995 on a european mailbox
See also at: VCKey110.lha and SLINKV10.lha

Both files were created using the 4eb9 linking method and are highly
dangerous ! The linked file is 1880 bytes powerpacked and 2876 bytes
unpacked long and contains a formatroutine for several drives and
assign just like the COP trojans. It will be done via a Dos COmmand
and not via the systemcommand.

The code was enhanced in comparision to the last version and it was
probably rewritten.

The files contain a lot of text at the end of the hunk and even some
kind of nickname for me well be used. You surely know the famous
Cornflakes from KELLOGS ? Some guys in the past from my school always
called me Cornflake and now this "%/&%" viruscoder tells me this waY.

The viruscode was partly optimized since the last versions of this
virus but in general the fucking formatroutine stays.

At the end of the virus you can read:

'dos.library'
'BBS'
'BBS:'
'CHOKe'
'CHOKe:DOPisGOD%ld'
'ALFONS ÅBERG ViRUS v2.0 ßeta by WiREFACE / dEMONS oF tHE pENTAGRAM, "
"dedicated to (Corn)Flake/TRSI'
'CHOKe:GODisEViL'
'DH0'
'DH0:'
'dOP'
'dOP:aNuS%ld'
'dOP:hihihi'
'DH1'
'DH1:
'dEMONS'
'dEMONS:pENiS%ld'
'DH2'
'DH2:'
'pENTAGRAM'
'pENTAGRAM:rEVENGE!'
'DH3'
'DH3:'
'WiRELESS'
'WiRELESS:hELL%ld'
'WiRELESS:!hATe!'
'You''ve been hit by (boom) (boom), you''ve b'
'een hit by (boom) a smooth criminal (Alfons '
'that is, tihi)! – Good luck restoring your l'
'ousy hD – WE HATE YOU ALL! HA HA HA HA HA !!'
'! (echo) ha ha ha'

The file id of the hdtoolsbox looks like this:

hdtoolbox 40.9 (9.7.95)

The file id of the lzx120t fake looks like this:

```
+-------------------------------------+
|         Lzx v1.20 TURBO Version     |
`-------------------------------------'
          12% Faster Testing
```

```
        10% Faster Adding!
         3% Faster Packing (-lh5-)
  .-----------------------------------.
  |  © 1995 Data Compression Technologies   |
  +-----------------------------------------+
```

It is really surprising. At first SHI (slinkv10) and VirusChecker(vckey110)
got attacked by this crazy guys and now I seem to be the destination of
this person? . I don't know, why...

                              Detection tested 22.07.1995.

1.182   AmosAGA

AmosAGA Trojan:

Filelength 74492 Bytes (AGA-Install.exe unpacked)
Found in/archiv/when: Denmark/amosaga.lha/30.7.1995
other possible names: NONE

This is just a little nasty trojan with the following
FILE ID:

"Beta Version a Ny aga ext... til AMOS"

It is just a little deleter for all files on the sys device.
Nothing tricky at all. Probably this virus was coded in
AMOS, since it contains code to load the AMOS.Library .

It was uploaded to the dansk AMOS user group as beta version
of a new tool by a guy called John O. Jörgensen. This is the
name, which appears in the virus, too.

There are two other files supplied in the package:

1. a readme.txt file:

**************** Welcome to the Beta Release of the Amos_Pro AGA extension
v1.0b **************** ******************************** By John O. Jørgensen.
****

Just execute the installer program and press install.... The installer program
is completely automatic...

Please do not spread this to anybody... This is a Beta version...

Sign. John O. Jørgensen.

2. A file called AGA-DATA.DATA. This is a pure LHA file and nothing special at all.

Detection tested 01.08.1995.

1.183 B.E.O.L. linkvirus

Mount-972 Linkvirus:

Kickstart: 2.04 and higher (V37+)
Patched vectors: several vectors in the device basis (quite tricky)
Length: 972 bytes
Processors: MC68000-MC68040 (68060 not tested)
Discoverd: Jul'95
Linking method: Infiltrator
Other possible names: B.E.O.L. virus

This is one of the most complicated viruses on AMIGA, which I have ever seen. It's coded very well and at many constructs even a very professional resourcing system from a friend has problems with this nasty virus. It is crypted using a "normal" logical (exclusiv or) routine, only the cryptword changes (depending on $dff006). The virus itself searches from the start of the file on for a "$4eae" to replace it with a pc relative jsr (-> as a result the first hunk can have only wordsize) and links its code at the end of the first hunk. The linking method doesn't contain any other tricks, a simple hunk-copying is enough to remove it from the infected file (+ rewriting the original longword).

The virus checks for Kickstart V37+ and does not start, if the check wasn't succesfull. If the check was succesfull, then the Caches will be cleared.

The virus detects its existence in memory by testing the lastalert entry in the execbase. If -$17 is the number of the lastalert, then it will not activate.

The virus allocates 972 bytes chipmemory to secure, that it will be not overwritten.

This virus uses a lot of special commands, which are a little bit crazy and probably should irritate the resource-programms. I could not resource some parts of the virus 100%, but the VirusWorkshop recognition routine for the memory will disable all the spreading functions. The virus uses some specialities of the commands and sometimes filles up a normal 00 bytes with a crap value, so that some resourceprogramms have problems. Asm-One 1.28 beta was able to resource it in most parts.

The patches from the virus will be done very clever and I must admit
that I have only once seen a comparable routine so far on AMIGA.

If you start a normal vectorchecker, no modification is visible. The
name of the virus is based on the lengthincrease and because a text
saying "c/mount".

The virus seems to be not resetproof. If an internal counter (byte)
reaches the value 0 (by lsl.b #2), then a file called README will be
written to the actual device. The file is 1152 bytes long and a text
can be read:

©+® B.E.O.L. 1995! Don't be angry!!
©+® B.E.O.L. 1995! Don't be angry!!

(This lines will be repeated several times)

                                        Detection tested 01.08.1995.

Comment Oct/95: The Virus Test Center of the university in
Hamburg made a very good analysis of this little bastard. Soon to
appear in well selected newsgroups and CMBase...

1.184 Flake013.txt

The flakexx.txt files are simple copies from my warnings in the AMIGANET. I
release there a warning and Jan Andersen, member of Virus Help DK, put this
warning in a file with increasing number (the xx) and spreads it on
skandinavian boards.

Jan Andersen released a flake013 text but not THIS text. I will show you some
differences to my text:

```
              _____  _____
              \___ \ensuremath{\lnot}\___ \ensuremath{\lnot}\ \ensuremath{\lnot ←
                }\/¯ __\ensuremath{\lnot}\___ \ensuremath{\lnot}\  __\ ←
              ensuremath{\lnot}\___ \ensuremath{\lnot}\
              /  / _/ _/  /___¯¯\/\ /  / /_/ / _/ _/\
             /  /  ¯  /  /\__/  /\//  /   ¯  /  ¯  /\/
            /__/__/__/__/_____/ //__/__/__/__/__/ /
            _____\/ \_\_\_\_\_\/

             _____  _____  _____
              \___ \ensuremath{\lnot}\   _\ensuremath{\lnot}\___ \ensuremath{\lnot}\·NL ←
               /¯ __\ensuremath{\lnot}\   _\ensuremath{\lnot}\/¯   \ensuremath{\lnot ←
                }\___ \ensuremath{\lnot}\  _ \ensuremath{\lnot}\___ \ensuremath{\lnot ←
                }\
             / _/ _/  /_\/  /  /\ /___¯¯\/  /_\/  /___/\ /  /  /  / _/ _/\
            /  ¯  /  ___/  /  / //\__/  /  ___/  /  /\//  /  /  /  ¯  /\/
           /__/__/_____/_____/ //_____/_____/_____/ //__/_____/__/__/ /
```

```
      _____\/  _____\/  _____\/

=+\===============/\==================/\=====/\================+=
.:\_.::::::::::/\.:/.:\:::::::::::::/\.:/.:\/\.:/.:\:::::::::::::::.
.:::\:::/\::/.:\/:::\::::::::/\::/.:\/:::::\/::::\·:::::___.___.__.._
.:::::\::/.:\/.:::::::::\::/\::/.:\/::::::::::::::::\/\·:/.:::::::::::·
=+=====\/===============\/==\/=====================\/===========+=


----------------------------------------------------------------------
VIRUS WARNING! VIRUS WARNING! VIRUS WARNING! VIRUS WARNING! VIRUS WARNING!
----------------------------------------------------------------------
```

 Warning !

 As you all probably know there is a new trojan called Biomechanic, spread >
around. (lately in TRSI-INS.LHA!) It's very mean and dangerous because it >
changes all files it can get hold on. I have also found out that it patched >
loadseg() in dos.library. You should be VERY careful. I have therefore made >
a very (Sorry! No time!) fast killer for it. Use it when ever when you think >
you could be infected.

 Here is my first analysis of the virus.

 Biomechanic Trojan

> Type: Destruction and in some cases, spreading.
 Destruction caused by: simple bytemodification

> Don't think it has ended here! The virus has now infected some files which >
are just waiting to be executed so they can spread.

 to be continued. The text contains advertisements from some boxes in Denmark
 and the name of JHL will be mentioned. This was not in the original text, so
 someone has modified it.

1.185 Lzx120T-BLK

   LZX 1.20 bugfixed version (Biomechanic trojan)

   Filelength: 67504 bytes unpacked
   Linking method: 4eb9
   Linked file packed with: PP4.0

   This is just another trojan out of the BIOMECHANIC series. It tries
   to manipulate several data on the main device, but failes at my
   system. Nothing special to be said about this virus. Simple
   destructive via normal DOS access and nothing tricky in it.

   When you start the file, the following text will appear on the screen:

   '   The forces of terror.'
   '   Biomechanic and C.O.P world tour 95.'

```
'        Just writing over some files is not so cool. Improve the code!'
'          Message to C.O.P! Cool work, but make more cooler trojans.'
'            Lean back and listen to the soun'd of a writing HD.'
'          Biomechanic did it again with a new smarter trojan!'
```

As said the ordinary 4eb9 linker is used again. If you find such a file, then be very carefull ! VirusWorkshop is able to recognize a lot of different 4eb9 types.

Here the faked FILE_ID.DIZ:

LZX V1.20 bugfixed by Blackhawk.
680020 Registred version only.

This trojan comes with a readme file, with some faked text:

Hi dudez! Here's a bugfixed verion of LZX, the best archiver avalaible today. The version is 1.20 and it's also registrated. I hope that my little update won't cause more bugs, than it had before! :) But anyway, I've tested it and it worked just fine for me!

Please not that this is not a original release from the authors. It just had a annoying bug which I wanted to fix, and so I did.

signing of: BlackHawk.

                        Detection tested 4.8.1995.

1.186 Comkil16

```
Comkill1.6 trojan (WireFire)
----------------------------
```

Filelength: 4606 bytes
Linking type: 4eb9

This is said to be a new release of the Commander viruskiller Comkill by SHI. In reality this is somekind of BBS hacker for the wellknown AMiExpress mailbox system. It will be tried to copy the user.data to the download areas to gain access to the system. Nothing special, this technics are known now for years.

Visible texts in the file:

'Hihihihi'
'WIREFIRE'
'bbs:'
'bbs'
'bbs'
'SteelVision'

```
'Mnenonic'
'ThinG'
'ByteMangler'
'Darkman'
'FlashRoger'
'messenger'
'·kEWldUdE·'
'SViNOMiR'
'Darkelf'
'bbs:user.data'
'ram:test.data'
'bbs:node4/playpen/pst-for.txt'
'bbs:node2/playpen/pst-for.txt'
'bbs:node3/playpen/pst-for.txt'
'bbs:node1/playpen/pst-for.txt'
```

The user data will be made avaible under the name pst-for.txt in the user-
areas. WireFace trojans are known, WireFire is probably somekind of
namecopy.

                                        Detection tested 5.8.1995.

1.187   DaJoker

```
PDY-SG-Installer:
-----------------

Length: 42676 partly packed
other possible names: DaJoker Trojan
Kickstart: ALL versions
destructive routines: yes
```

This is just a little quite easy build trojan. It tries to delete several
files (listed at the end) and gives then a message to the shocked user.
Please try to recover the files using quarterback or disksalv. It should
be possible.


```
FILE_ID.DIZ:

_____  _____
_____ \_____ \____ _\/\_ _ /__/.____/__ / /
:  / ____/     _/  / // \ //  // /  /  /  /:
| /__/  /__/  /_____/____ /__/____ /_____/ |
|.:::::::::/___ /:::::::::\/:::::::\/:::Sk!n.|
+-----------\/P r e s e n t s -----------+
Sensible Golf HD Installer!.....

Readable texts in the coded file:


        '                             '
        'The Joker Fucked Yar Harddisk!'
        '                             '
        'dh0:c/delete dh0:libs/'
        'dh0:c/delete dh0:wbstartup/'
```

```
        'dh0:c/delete dh0:locale/'
        'dh0:c/delete dh0:prefs/'
        'dh0:c/delete dh0:devs/'
        'dh0:c/delete dh0:s/'
        'sys:c/mapus'
        'sys:c/loadwb'
        'sys:c/lock'
        'sys:c/edit'
        'sys:c/ed'
        'sys:c/Diskdoctor'
        'sys:c/ConfigOpus'
        'sys:c/amigaguide'
        'sys:c/assign'
                                Detection tested 5.8.1995.


  Condom 1.5 Trojan:
  ------------------


  Length: 2948 party packed
  other possible name: DaJoker trojan

  Exactly the same damage routine as in the Sensible Golf installer.
```

1.188 LSD-AEC1

```
  LSD-AEC1 Trojan:
  ----------------

  other possible names: WireFace Typ E
  destructive: yes
  destruction on: SYS:, DH0:, DH1:, BBS:

  All non protected files will be set to a filelength with 0 bytes.
  Nothing special, EXCEPT the way the trojan in implented in the
  AeCrack file. First the file is packed and 4eb9 linked. Then
  the whole procedure again.

  This can't stop a good programmer.

  File_ID.DIZ:

   ___/\____ ___ _/_____/_____
  _____    /__ ___   _____       \
   \/     /_____     \/     /     /
   /     /     /     /     /     /     /
  /_____      /_____      /_____     /__ __ _
  ___ _____ /___ ___ __ /_ __ _____ /__//_//
  bIS      \/          \/          \/
          /X Crack v1.0 Release 1
        CRACK AMIEXPRESS PASSWORDS
  Crack Passwords, Mail users, Many options.
  ^^^  NIFFY: AMIGASCENE's SATAN program!  ^^^
```

A little documentation is supplied in the package:

```
        ___/\____  ___  _/_____/_____
   ____     /__ __/    _____     \
    \/     /_____     \/     /     /
    /    /    /    /     /     /     /
   /____     /____     /____     /__ __ _
   ___ _____ /___ ___ __ /_ __ _____ /__//_//
   bIS     \/       \/        \/
                  presents:

           PASSWORD HACKER for Amiexpress !

           /X Crack version v1.0 Release I
```

Here's a stripped down version of my /X Hacker Cracker program
that will work like SATAN on the internet. It will search
/X for backdoors and weaknesses. This is the part that cracks
the passwords on users and mails them that their password is
too easy to hack (to common?) and that they should change it!

Usage:

aecrack <user.data> <confnum>

where confnum is the number of the conference where the mail
should be posted. If your AMIGA ELITE conference is 2 type:

aecrack BBS:user.data 2

If you only want to check the passwords do like this

aecrack -o<filename>

where <filename> is the output filename for the passwords
with the format U:USERNAME, P:PASSWORD<CR>
ie.
aecrack -oRAM:Passwords

I take *NO* responsability for this program used/abused whatever.
Run it on your own risk.

                                    Fish/LSD

.....

A new textfile will be written to disc under the name -!-WiREFACE-!-:

WiREFACE / dEMONS oF THE PENTAGRAM presents... (tadaa)
'KLiA MiG PÅ NUPPEN' TROjAN (SUPER BETA RELEASE(BETA BETA CODE))
A NEW GENERATiON OF LOGiCAL BOMBS HAS ARRiVED TO YOUR LOCAL BBS
Vi ska till fajmoj o fajfaj o bada imorrn! Du er inte klok.
Tenker du skriva allt vi sege nu? Skiva. L0jligt. Smock(puss)
mmh.. Naeeeeeeehehhehehe chrhh sfhhh.. eeh skriv det her da:
Fan va t0ntig du er Andreas som haller pa o skriva saher (fisa)
det var sk0nt.. nehehhe aj.. naeee!

                              Detection tested 4.8.1995.

1.189 Illegal Access Linkvirus

Entry...............: Illegal Access
Alias(es)...........: –
VirusStrain........ : –
Virus detected when.: 7/1995
            where.: USA
Classification......: Link virus, memory-resident,
                      reset-resident Length of Virus.....:
                      1. Length on storage medium: ca.4000 Bytes
                      2. Length in RAM: 4514 Bytes

-------------------- Preconditions ----------------------------------

Operating System(s).: AMIGA-DOS Version/Release.....: 2.04 and above (V37+)
                                                    (for infection: V39+)
Computer model(s)...: all models/processors (MC68000-MC68060)

-------------------- Attributes -------------------------------------

Easy Identification.: None

Type of infection...: Self-identification method in files:
                      - Searches for $2c780004 in the first Hunk at first
                        position (normal file infection)

                      Self-identification method in memory:
                      - Checks for exception vector 3 (Illegal Opcode)
                        and for $4afc in the OpenLibrary() funtion

                      System infection:
                      - RAM resident, infects the processsor exception
                        vector, modifies 19 different functions,
                        CoolCapture, ColdCapture and post mortem resident
                        handler

                      Infection preconditions:
                       - File to be infected is bigger then $1800 bytes
                       - First hunk isn't about 4000 bytes long and does
                         not contains $2c780004 at first long in it
                         (for normal file infections)
                       - The file is not already infected

                                      – HUNK_HEADER and HUNK_CODE are found
                                      – HUNK_HEADER structure is valid
                                      – The longword 2-4 of the filename in the info-
                                        structure multiplicated in this way:
                                        m3*m2, m1*m3 (longword orientated, 68020++ command)
                                        must be less then $320000. Otherwise it's asked,
                                        if the filelength is smaller than $32000 (=200kb)

Infection Trigger...: Accessing the volume
                            Storage media affected: all DOS-devices

Interrupts hooked...: The virus infects the processorexception 3 vector
                      (Illegal Opcode)

Damage..............: Permanent damage:
                      – None
                      Transient damage:
                      – none Damage Trigger......: Permanent damage:
                      – None
                      Transient damage:
                      – None

Particularities.....: The crypt/decrypt routines are aware of processor
                      caches and cleares them if necessary. This routines
                      are polymorphic and use several tricks like symmetric
                      decoding with memoryusage to make it a little bit more
                      difficult. Some of the routines are equal to routines
                      in the B.E.O.L. virus. The way of creating a new
                      process ("keyboard.device") using the stack is in my
                      eyes comparable. The linking method searches for
                      special filetypes (e.g. libraries and devices) and
                      infects them in a different way. This files will
                      get an additional entry in their HUNK_RELOC32 table
                      containing the original pointer to Library Init().
                      This library structure makes it impossible to use
                      a kind of intelligent searchcode for the virus. "Brute
                      force" code is needed to search for the resident
                      structure.

Similarities........: Link-method in library structured file is like the one
                      of infiltrator-virus (but optimized).
                      Link-method in normal executable files is the IRQ
                      typ (just another hunk)

Stealth.............: The viruses uses normal dos commands (no tunneling
                      via packets) and normal DOS call watchers like SnoopDos
                      can proof the infection behavior. The virus restores
                      both, fileprotect flags (including the user id !) and
                      the filedate, so that except of the filelength, no
                      difference can be seen. The exception handler uses a
                      special stealth technique to differ between a normal
                      exception and a self called. It checks up for "4AFC"
                      and , if found, it changes it to "4EF9", so nobody
                      will be able to find the real problem behind.

During daily work, the virus does not change in any way the resetvectors from Exec. If a reset is performed, it will shortly init the Coolcapture and ColdCaptures to get resident. At the start of the new system (test for "dos.library") all new initialized coolcapture and coldcaptures will be removed again (-> post mortem handling)

Armouring...........: The virus uses several armouring techniques to confuse people while debugging this virus:
1. The virus uses double encryption with an polymorphic engine
2. The virus is self-modifying in several bytes (e.g. $4e71->$4e75)
3. The virus excessively uses the stack for unusual operations like:
   - creating processes
   - decrypting
   - jumps
   - pointer-replacement
   - saving structures
4. The virus refuses to run in test-suites and checks if it is running under normal conditions (system-files present)
5. Data-Reuse - the Virus uses several bytes from within code with a completely other meaning, wich makes labeling impossible (Using data from a code area)
6. Access to non equal code blocks as basis offset for further work

------------------- Agents --

Countermeasures.....: VW5.7 ,VZII1.24
                      VT 2.77 and VC 7.18 (not libraries)
Countermeasuressuccessful: All of the above
Standard means......: -

------------------- Acknowledgement ----------------------------------

Location............: Hannover, Germany 30.8.1995.
Classification by...: Markus Schmall, Georg Hoermann, Heiner Schneegold
                      and Soenke Freitag (VTC)
Documentation by....: Markus Schmall
Date................: August,30. 1995
Information Source..: Reverse engineering of original virus

============ End of Illegal Access Virus ========================

Comment 12.09.1995: A bug in my library detection code popped up with files containing only one hunk. Fixed right now. Sorry. Detected by Remko Wiersma.

Comment 15.10.1995: A bug in my autoinit library detection popped up and
so I had to refix it again.

1.190   WireFace Typ G Trojan

```
WireFace Trojan Typ G:
----------------------

Found in   : chkmount.lha
Type       : destructive trojan
Protection : *Art
Filesize   : 4672 Bytes (partly packed)
```

This is another trojan from the WireFace series. This trojan looks
in parts like Biomechanic trojans, some byterow comparecode are
for sure copied. I haven't test up to the end, but the code looks
like a comparable code as in the icond biomechanic stuff.

If you start it and a destruction is not possible (devices not
found) a text will be printed on screen saying several times:

nugget@dataphone.se

It has some visible texts at the end of the virus. The virus itself
is protected and then afterwards packed with StoneCracker 4.04. The
final filesize is 5868 bytes.

The following devices are tried to be accessed and the first 39
sectors are going to be overwritten:

'scsi.device'
'icddisk.device'
'oktagon.device'
'SoftSCSI_OktagonC9X.device'

Other visible texts are:

'(TrojanName: iLSKNA ANDREAS v1.1) WiREFACE / dEMONS oF tHE "
" pENTAGRAM strikes again with another stunning release (trojan) "
" hahaha. Send postcards, money, bugreports or COMPLAINTS'
'to me at this email adress: nugget@dataphone.se. CU in another
"relase!'
'nugget@dataphone.se'   (This is the printed text)

The programm looks like created with an old compiler. Some special
1.x programming technics are used, which won't be used nowaday
normally anymore.

VirusWorkshop and VT will give you the warning, that a $3e8 hunk is
in the file. This is the protection from the trojan. Simple, but
effective.

Something more to wonder about: I have downloaded this file from SOS

at 8.8.1995. and I have only used the name MOUNT-972 in one warning
in AMiganet and the german Z-net, so the viruscoder must read it, too.

The trojan is supplied with a little documentation:

                        Mount-972 Virus Checker
                        ----

                  by Robert Wolvestein (ao@dataphone.se)

This small checker finds and eliminates the Mount-972 virus
that resently popped up! The virus must have been spread
via Aminet or thru BBS's coz it is EVERYWHERE, almost 40% of
my 'scene-friends' had it in some way or another.

Regards Robert.

(ED: A cool fake, better play with your joystick)

                                    Detection tested 9.8.1995.

1.191 CONMAN1995-Linkvirus

ConMan 1995 Linkvirus:

Other possible names: M-Hac Virus, Bloody Virus
Detected in: M-hac.lha and Bloody.EXE
Detected when: August 1995/Germany SOS
Linking method: 4eb9 (!!!!)
Resident: NO
Length: 1836 bytes

This is a new type of linkvirus. There are 2 installers known yet.
It simply creates a new process with the known CONMAN code , but
now with different names.

Possible names are:

C:DIR
ramlib
Background_Process
RAm
L:FastFileSystem
LIBS: gadtools.library
Workbench
DF0

```
addbuffers
CON
LIB:req.library
CLI(0): no command loaded
CLI(1): no command loaded
```

Please note that several of this takss can appear in normal systems,
too.

The speciality of this virus is, that it uses a intern 4eb9 linker
to link to files. Quite tricky. Viruskillers like VT, VZ_II and
VW should so be able to detect the infected files.

The linking routine knows the following hunksymbols: $3f2,$3f3,$3ec
and $3eb. The code is a little bit dangerous, but I will implent
in VirusWorkshop a complete reverse analyzed routine, so it should
be no problem to repair even not working infected files.

The virus adds 4 hunks to the file and the linked code is partly
packed. It is packed with StoneCracker 4.04ß and then afterwards
manipulated.

The virus is not memory resident.

Some words about the installers:

m-hack.lha FILE_ID.DIZ

```
.-------------------------------.
| MASTER AMIEX ONLINE PW HACKER |
| PREVIOUS VERSION HAVE A BUG!  |
`-------------------------------'
```

The programm hack (4388 bytes long) contains the trojan.

bloody.exe FILE_ID.DIZ:

NON DOS DISK READER >>>>-BEST!

The programm is including this ID 25560 bytes unpacked long.

1.192 Ebola


```
Entry...............: Ebola Virus
Alias(es)...........: E1116 (to stay CAROconform)
Virus Strain........: -
Virus detected when.: 9/1995
            where.: Germany
Classification......: Linkvirus,memory-resident, not reset-resident
Length of Virus.....: 1. Length on storage medium:    1116 Bytes
                      2. Length in RAM:               3300 Bytes
```

-------------------- Preconditions ----------------------------------

```
Operating System(s).: AMIGA-DOS Version/Release.....: 2.04 and above (V37+)
Computer model(s)...: all models/processors (MC68000-MC68060)
```

-------------------- Attributes ---------------------------------------

Easy Identification.: none

Type of infection...: Self-identification method in files:
                      - Searches for $ab1590ef at the end of the first Hunk.

                      Self-identification method in memory:
                      - Checks for $213f at offset -2 of the loadseg()
                        function

                      System infection:
                      - non RAM resident, infects the following functions:
                        Dos LoadSeg(), Exec FindTask() and Exec
OpenResource()

                      Infection preconditions:
                       - File to be infected is bigger then 2500 bytes and
                         smaller then 130000 bytes
                       - First hunk contains a $4eaexxxx command in the 16
                         bit range to the end of the file (test for the first
                         entry)
                       - the file is not already infected (the at long of the
                         end of the hunk)
                       - HUNK_HEADER and HUNK_CODE are found

Infection Trigger...: Accessing files via LoadSeg()
Storage media affected: all DOS-devices

Interrupts hooked...: None

Damage..............: Permanent damage:
                      - None
                      Transient damage:
                      - none
Damage Trigger......: Permanent damage:
                      - None
                      Transient damage:
                      - None

Particularities.....: The crypt/decrypt routines are partly aware of
processor
                      caches. The cryptroutine are non polymorphic and only
                      consists of some logical stuff. The virus uses some
                      simple retro technics to stop viruskillers searching
                      for Draco and possible for the HochOfen (Trabbi) Virus.

Similarities........: Link-method is comparable to the method invented with

```
                              the infiltrator-virus


Stealth.............: No stealth abilities


Armouring...........: The virus uses only a single armouring technique to
                      confuse people. It only crypts it's code based on the
                      position of the rasterbeam.


Comments............: The name EBOLA is the name of a virus, which humans
                      can get infected with. CARO rules say, that no names
                      of persons etc. may be used to call a virus, but I
                      spoke to other persons and they already recognized
                      this virus in this way.



-------------------- Agents ---------------------------------------------


Countermeasures.....: VW5.5 and VT 2.76 Countermeasures successful: All of the
above Standard means......: -


-------------------- Acknowledgement ------------------------------------


Location............: Hannover, Germany 03.09.1995.
Classification by...: Markus Schmall and Heiner Schneegold
Documentation by....: Markus Schmall (C)
Date................: September,03. 1995
Information Source..: Reverse engineering of original virus
Copyright...........: This document is copyrighted and may be not used
                      in any SHI publication


==================== End of EBOLA Virus =========================
```

1.193   COP Trojan - Quarterback Deluxe

```
Entry...............: COP-Trojan
Alias(es)...........: QuarterbackD Trojan,
                      ORS-QBD.lha trojan
Virus Strain........: -
Virusdetected  when.: 9/95
            where.: Denmark
Classification......: Trojan, memoryresident,not resetresident
Length of Virus.....: 1. Length on storage medium: 227716 Bytes (unpacked)
                      2. Length in RAM:          227716 Bytes
                                              - redundant hunkdata
-------------------- Preconditions ---------------------------------


Operating System(s).: AMIGA-DOS Version/Release.....: 3.00 and above (V39+)
                      (Some functions are supposed
                      to work only on V40 ?)
Computer model(s)...: all models/processors (MC68000-MC68060)


-------------------- Attributes -----------------------------------------


Easy Identification.: Filelength
```

```
Type of infection...: Overwriting all files in the destination directories

Infection Trigger...: none
                          Storage media affected: all DOS-devices

Interrupts hooked...: None

Damage..............: Permanent damage:

                      Overwriting files in ENV, SYS, LIBS,NCOMM and S
                      with a 75 bytes long text containing the following
                      information:

                      "=CIRCLE OF POWER= [ WE ARE BACK! THE RETURN "
                      "OF THE POWER PEOPLE! / GRYZOR ]"



Damage Trigger......: Permanent damage:
                      - Start of programm
                      Transient damage:
                      - Start of programm

Particularities.....: The trojans uses the DosList to get access to
                      the various directories and then starts to
                      damage the information in this files. The code
                      uses some Kickstart 3.x functions and is so
                      not working on older systems. Some failure-
                      recognition routines were build in (in
                      comparison to older COP trojans).

                      Normal behavior blockers are able to stop
                      this trojans. No tunneling techniques are used
                      for this little bastard.



Similarities:        A lot of the routines are comparable to older
                      COP trojans found in various wide spread
                      utilities. Some codes are optimized, but still
                      the old style is recognizeable. This special
                      one contains nearly the same code as the
                      COP trojan found in PT4ß.



Stealth.............: None


Armouring...........: Important parts are crypted using a logical
                      loop, which is breakable by a normal code
                      simulator.


-------------------- Agents ---------------------------------------------

Countermeasures.....: none Countermeasures successful: All of the above
Standard means......: -
```

```
-------------------- Acknowledgement -------------------------------

Location............: Hannover, Germany 16.9.1995.
Classification by...: Markus Schmall and Heiner Schneegold
Documentation by....: Markus Schmall
Date................: September,16. 1995
Information Source..: Reverse engineering of original trojan
Copyright...........: Markus Schmall
Special.............: No use of this analyse except VTC Uni Hamburg
                      in their CMBase releases


==================== End of Quarterback3 COP Trojan=====================
```

1.194   Cryptic Essence Linkvirus

```
Entry...............: Cryptic Essence Alias(es)...........: Evil Jesus #3
Virus Strain........: -
Virus detected when.: 9/1995
             where.: Denmark Classification......: Link virus,
memory-resident, not reset-resident
Length of Virus.....: 1. Length on storage       medium:    none
                      2. Length in RAM:               $97c bytes


-------------------- Preconditions ---------------------------------

Operating System(s).: AMIGA-DOS Version/Release.....: 2.04 and above (V37+)
Computer model(s)...: all models/processors (MC68000-MC68060)


-------------------- Attributes ------------------------------------

Easy Identification.: None


Type of infection...: Self-identification method in files:
                      - None. Double infections are possible but mostly
                        result in dead samples. Tested on CVMODE as
                        testinfect file.

                      Self-identification method in memory:
                      - None

                      System infection:
                      - RAM resident, infects the DOS Write() function

                      Infection preconditions:
                       - File to be infected is bigger then 9276 bytes
                       - First hunk is a normal code hunk without
                         memory extentsion (=$3e9)
                       - This hunk must be bigger than 9276 bytes
                       - First word in this hunk is not:

                         - $4afc (ILLEGAL)
                         - $4e75

                       - Second word in this hunk is not:
```

```
                              - $4afc (ILLEGAL)
                              - $4e75
```

Infection Trigger...: Accessing the volume (by writing)
                      A normal COPY is not suitable, because COPY divides
                      longer files in little chunks and at this chunks,
                      the virus mostly cannot work correctly.
                        Storage media affected: all DOS-devices

Interrupts hooked...: None

Damage..............: Permanent damage:
                      - Changes data in files randomly. Not repairable
                      Transient damage:
                      - none
Damage Trigger......: Permanent damage:
                      - Counter reaches 0
                      Transient damage:
                      - None

Particularities.....: The crypt routines are not aware of processor caches
                      and have serious problem at some places. It can come
                      to wrong decoding and such stuff. The linkmethod is
                      new for the AMIGA computer series and is called on
                      PC Cavity linkviruses. There is no modification to
                      the relochunks needed to repair the file from the
                      virus.

                      In the virus there is found a comment to a wellknown
                      PC antivirus researcher and to a essey written by
                      this guy, which was obviously used from the virus-
                      programmer(s) as basis.

Similarities........: Cavity linkviruses on PC (such families have been
                      e.g. seen in the Netherlands). Packroutine is stolen
                      from the xpk distribution. The way of linking is
                      completly new for the AMIGA at this time (9/95).

Stealth.............: The viruses uses normal dos commands (no tunneling
                      via packets) and normal DOS call watchers like SnoopDos
                      can proof the infection behavior. The virus does not
                      restore fileprotect flags and the filedate, so that
                      this can be a proofal for a possible infection. The
                      filelength does not change. No new hunk will be added.
                      Using the RCH technic the virus searches a place
                      where to put it's own code and crunches the existing
                      data at first. The can't be found based on a normal
                      offset location search.

Armouring...........: The virus uses several armouring techniques to
                      confuse people while debugging this virus:
                      1. The virus uses double encryption with an
                         polymorphic engine (SPe)
                      2. The virus is flexible programmed and uses

```
                                  nearly no hardcoded values
                            3. Write() vector patch uses a polymorphism
                               to cheat some not flexible av-software
                            4. Polymorphism at entry jump to irritate the
                               av software
```

-------------------- Agents ---

Countermeasures.....: VT 2.77, VW 5.6
Countermeasures successful: All of the above
Standard means......: -

-------------------- Acknowledgement ------------------------------------

Location............: Hannover, Germany 28.9.1995.
Classification by...: Markus Schmall, Georg Hoermann and Heiner Schneegold
Documentation by....: Markus Schmall
Date................: September,28. 1995
Information Source..: Reverse engineering of original virus
Special.............: Some parts of this analyse have been shorted/cutted
                      not to show the public too much information about
                      things like RCH and SPe.

==================== End of Cryptic Essence Virus ======================

It's surprising that the virus seems to be uploaded from the auhtor including
FULL source at a dansk AV board. The author included even a little text:

-----BEGIN PGP SIGNED MESSAGE-----

  -=* Cryptic Essence, © 1995 Evil Jesus (maximum false positive) *=-

 Extra thanks for xxxxxxxx xxxxxxxxx giving some valueable information
 how to reach maximum damage in essee 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxx'.

 It really inspired me to write C.E.!

 - Generalized infection scheme, virus itself will not use any strings
   to avoid reinfecting same file. This should make it very hard to
   detect and also gives possibility to change visible decrypting code.
 - Random damage, impossible to repair.
 - Source code is easily modifable to use different packers and crypters.

 If you are interested about that particular essee you can write to
 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.

 Sins unforgiven, Evil Jesus

-----BEGIN PGP SIGNATURE----- Version: 2.6ui (Amiga)

iQBFAgUBMFP6ho3j8jX6L7S9AQFwuQF/TruUbFYQ5LwSBOk1SkqUp9R8tycB4m5y
bgNZh5X0wVHU9ggx285ZUOdOcM+OeRGS =Mrqg -----END PGP SIGNATURE-----

I don't know, that the virusprogrammer wanted to do with it. The xxx's are only there to stay CARO conform and not to mention a special pc av freak, which will be mentioned inside the virus, too.

VIRUSWORKSHOP WILL ONLY RECOGNIZE THIS VIRUS ON 68020 AND HIGHER SYSTEMS, BASED ON THE CODEEMULATION, WHICH IS SENSELESS ON 68000 !

1.195   Swifter 2.5 Trojan - Laboratoy trojan ?

```
Swifter 2.5 Trojan:
-------------------

Other possible names: Game-Trojan
Filelength: 003.DAT (new Startup-Sequence) 73 bytes
            002.DAT (SetKeyBoard) 1412 bytes
            001.DAT (assign) 3220 bytes
            000.DAT (new keymap) 1972
            Swifter 106496 (Imploder 4.0)
                    215448 (unpacked)

            (IFF picture in swifter is
             215018 bytes long and NOT
             used)
```

This is just another lame trojan with no special stuff in it. It will be tried to delete the startup-sequence and then to install a new one, which should delete a lot of files. After the mainfile was started, a new Keymap will be activated, containing a lot of garbage and dangerous commands like a format command. The virus itself is 430 bytes long and after it a normal IFF picture with a not youth free slogan can be found. This picture will be not accessed and was probably put there to increase the length of the file.

The file was uploaded to a swedish bbs by an unknown user and this user contacted the sysop and said that he is sorry, but he uploaded by accident a new trojan from him to his box. Make your own point of view, I am a little bit irritated.

File ID of the upload:

SWiFTER. Ett spel jag har gjort. Asfränt!

Helt klart värt en DL. Läs längre
beskrivning.

1.196 phantom

```
Entry...............: Phantom Linkvirus
Alias(es)...........: Super-Nova
Virus Strain........: -
Virus detected when.: 11/1995
            where.: Germany
Classification......: Link virus, memory-resident
Length of Virus.....: 1. Length on storage medium:  ca.688 Bytes
                      2. Length in RAM:              688 Bytes


-------------------- Preconditions -----------------------------------


Operating System(s).: AMIGA-DOS
Version/Release.....: 2.04 and above (V37+)
Computer model(s)...: all models/processors (MC68000-MC68060)


-------------------- Attributes --------------------------------------


Easy Identification.: None

Type of infection...: Self-identification method in files:
                      - Searches for $83ef19acin the first Hunk at last
                        position (normal file infection)

                      Self-identification method in memory:
                      - Checks for a longword in the LoadSeg routine
                        ($42a449fa)

                      System infection:
                      - RAM resident, infects the DOS Call LoadSeg()


                      Infection preconditions:
                       - File to be infected is bigger then 4000 bytes and smaller
                         than $2e630 bytes
                       - First hunk is a code hunk
                       - File is executable
                       - First hunk has no reloc linked behind
                       - First hunk ends not with $83ef19ac


Infection Trigger...: Accessing the volume via LoadSeg (patched)

Storage media affected: all DOS-devices

Interrupts hooked...: none

Damage..............: Permanent damage:
                      - None
                      Transient damage:
                      - none

Damage Trigger......: Permanent damage:
                      - None
                      Transient damage:
```

                              - None

Particularities.....: The crypt/decrypt routines are aware of processor
                      caches.

Similarities........: Link-method in library structured file is like the one of
                      the Commander virus (without bsr changes!)

Stealth.............: The viruses uses normal dos commands (no tunneling
                      via packets) and normal DOS call watchers like SnoopDos
                      can proof the infection behavior. The virus uses no
                      stealth weapons. The only things is it's size. 688 bytes
                      difference in files don't wake up the user so fast.

Armouring...........: The virus uses only 2 weapons:
                      1. The virus uses a cryptroutine to hide it's code.
                      2. The virusname is hidden in a block, which will be
                         normally never accessed. Just decrease the values
                         by 1 and you will see the text "let's go again...
                         PHANTOM"

Comments............: This file was sent to the dansk SHI leader from a german
                      guy. It was send to him as a new viruskiller. This happened
                      months (years?) ago and now (11/95) the virus appeared again ↩
                        .

                      In reality this is just a modified old version of VMK with
                      an installer linked before. The installer is timebased.

                      (In the BX-News.Guide in the chapter Super-Nove you
                       can find some more information, how the virus reached SHI).

------------------- Agents --

Countermeasures.....: VW5.7, BootX 5.23B with Recog 2.25 (only the installer)   ?
Countermeasures successful: All of the above
Standard means......: -

------------------- Acknowledgement -----------------------------

Location............: Hannover, Germany 05.11.1995.
Classification by...: Markus Schmall
Documentation by....: Markus Schmall
Date................: October,05. 1995
Information Source..: Reverse engineering of original virus
Copyright...........: Markus Schmall, Virus Test Center Uni Hamburg has the
                      permission to use this analyse in their catalog. SHI
                      is not allowed to use this document in ANY way.
==================== End of Phantom Virus ============================

1.197 pb-party

```
PB-Party Trojan:
----------------

Length: 161984 bytes unpacked

File_ID:

+-------------------------------------+
|         POLKA BROTHERS PRESENTS:    |
|                                     |
|     INVITASION INTRO TO PARTY V     |
+-------------------------------------+

This is just a fake. In reality this file just overwrites the BBS:User.Data
with the text:

 'tHE rEAL hACKERS fUCKED yOU iN tHE bEHIND!'


The way of programming is not advanced. Better play a good game instead
of producing such SHIT !
```

1.198 happy

```
Entry...............: H.N.Y.96. I+II
Alias(es)...........: Happy_New_Year_96
Virus Strain........: -
Virus detected when.: 11/1995
            where.: Austria, Germany, Holland, Poland and USA
Classification......: Link virus, memory-resident, not reset-resident
Length of Virus.....: 1. Length on storage medium:  540 Bytes
                      2. Length in RAM:              540 Bytes

-------------------- Preconditions -----------------------------------

Operating System(s).: AMIGA-DOS
Version/Release.....: 2.04 and above (V37+)
Computer model(s)...: all models/processors (MC68000-MC68060)

-------------------- Attributes --------------------------------------

Easy Identification.: Text at the end of the first hunk: "Happy_New_Year_96"

Type of infection...: Self-identification method in files:
                      -  Searches for $65772059 in the first Hunk.
```

```
                        Self-identification method in memory:
                        -  Checks for $2f08 in the LoadSeg function

                        System infection:
                        -  RAM resident, infects the LoadSeg() code of
                           DOS library

                        Infection preconditions:
                        - device has more than 4 free sectors
                        - file is longer than $960 bytes and shorter than
                          $1e460 bytes
                        - Hunk_Code is found in the area behind the HUNK_
                          header (NO CHECK FOR RUNAWAYS!!!)
                        - The filename contains this not a "-" and does
                          not contains ".l". This is probably to be secure
                          no to infect a library.
                        - $4e75 is found at the end of the first CODEHUNK
                          or $4e75 is in the last $3f words of this hunk.
```

Infection Trigger...: Accessing the volume

Storage media affected: all DOS-devices

Interrupts hooked...: LoadSeg() of DOS will be used for the infection code.
                      The routine is a little bit buggy and trashes the
                      a1 register.

Damage.............: Permanent damage:
                     - None
                     Transient damage:
                     - None

Damage Trigger......: Permanent damage:
                      - None
                      Transient damage:
                      - None

Particularities.....: This virus uses no encryption routines to hide it's
                      code. The LoadSeg() patch isn't 100% clear and
                      trashes the adress register A1.

Similarities........: Link-method is comparable to the Crime
                      series. End of the first hunk will be the loc.
                      for the virus and the last "RTS" will be replaced.

Stealth.............: no stealth abilities found

Armouring...........: The virus uses only some special adresscommands to
                      confuse the AV people.

Installers..........: DemoManiac 2.19 fake (dop-dm1.dms)
                      DeTag0.63 (detag063.lha)

-------------------- Agents ---

```
Countermeasures.....: VT 2.79, VW 5.8
Countermeasures successful: all of the above
Standard means......: -

-------------------- Acknowledgement --------------------------------

Location............: (C) Markus Schmall, Hannover, Germany
Classification by...: Markus Schmall
Documentation by....: Markus Schmall
Date................: November,24. 1995
Information Source..: Reverse engineering of original virus
Copyright...........: Markus Schmall, the VTC Uni Hamburg is allowed to
                      use this document in their libraries. SHI is
                      forbidden to use this document in any form.
==================== End of H.N.Y.96. Virus ==========================
```

1.199   flt-1996

```
FLT-1996 Trojan:
----------------

other possible names: BlueSky1 trojan

This is a simple trojan, which tries to overwrite SCSI.DEVICE
unit 0 completely. The code isn't that good. Nothing more to
say about it. Not linked, a trojan and no usefull code.
```

1.200   susi

```
Susi_Drive_Stepper Trojan:
--------------------------

Filelength:    904 bytes unpacked
Programmed in: Assembly language
Processors:    MC68000-MC68040(?)
               On MC68060 it did not work
Typ: Trojan


This is a very easy programmed trojan. Via the use of
Disk Resource it will be tried to access a device (0)
and some IDs will be changed. The whole new "created"
DiskResource struct is not correct and contains a lot
of not understandable code. The trojan is not reset-
proof, it just tries the above mentioned diskresource
manipulation and some little hardwarehacks.The trojan
selects unit 0 and steps with the head around. The
```

direction will be changed at every loop and the head
moves always one track. The timing is so bad managed,
that the controller gets irritated and quits work
temporarly.

The name of the new created port is "susi". You can
see at the end of the file some names, but nothing
more. All in all a simple trojan.

```
0260: 00000000 00000000 00006469 736B2E72      ..........disk.r
0270: 65736F75 72636500 73757369 00616E64      esource.susi.and
0280: 72656100 76616C65 6E74696E 6100696E      rea.valentina.in
0290: 67726964 00636872 69730000 0A000120      grid.chris.....
```

It was tried to damage a disc using this trojan, but we
didn't succeed.

1.201   Invader=Silesian linkvirus

```
Entry...............: Invader
Alias(es)...........: Silesian Virus
Virus Strain........: -
Virus detected when.: 1/1996
            where.: Poland
Classification......: Link virus, memory-resident, not reset-resident
Length of Virus.....: 1. Length on storage medium:  1200+(0..72)    Bytes
                      2. Length in RAM:           $19000 or $d6b0 Bytes
                      (depends on the returncode of availmem() )
```

-------------------- Preconditions ----------------------------------

```
Operating System(s).: AMIGA-DOS
Version/Release.....: 2.04 and above (V37+)
Computer model(s)...: all models/processors (MC68000-MC68060)
                      The virus has problems with caches of all kind.
```

-------------------- Attributes -------------------------------------

```
Easy Identification.: None


Type of infection...: Self-identification method in files:
                      -  None

                      Self-identification method in memory:
                      -  Checks for a word in the Dos Open() function


                      System infection:
                      -  RAM resident, infects the followind DOS
                         functions
```

```
                        - Open()
                        - Rename()
                        - Lock()
                        - LoadSeg()
                        - NewLoadSeg()
                        - SetComment()
                        - SetProtection()


                        Infection preconditions:

                        - File is executable

                        Please note, that there is no check for a CODE
                        hunk or such things. The virus loads the to be
                        infected file, but forgets to do a real length
                        check. It seems as the virus cuts file just as
                        it wants to.

                        Example:

                        (Memoryalloaction is $19000)

                        Infecttry of xyz (=$2a000 bytes)

                        The infected file will be $19000+$4b0+0..72
                        bytes long and not repairable anymore.
```

Infection Trigger...: Accessing the volume

Storage media affected: all DOS-devices

Interrupts hooked...: No interrupts used

Damage.............: Permanent damage:
                     - Damages files, adds bytes, copies blocks.
                     Transient damage:
                     - The Virus writes a file with the name
                     "===README===" on the ramdisk. It contains
                     some text like "Get me you lamer..." etc.

Damage Trigger......: Permanent damage:
                     - Overwriting file contents in several places,
                     especially, when the files have more hunks.
                     Transient damage:
                     - Infection-Counter

Particularities.....: The memoryallocation operations are not cache-
                     proof and should make a lot of problems. The code
                     isn't that professional written, the patch-
                     routines are very simply made. One important
                     counter is behind the first hunk, which isn't
                     that clever. The data behind the first hunk can
                     be damaged in a serious way.

Similarities........: Link-method is like the one of infiltrator-virus.

Some ideas behind (search for DH0 and then try to
infect dh0:c/loadwb first) look like stolen from
the Commander linkvirus.

The change of the last command in the to be
infected hunk is a little bit buggy. Under
circumstances the last word in the hunk will
be changed, even if there is another important
information in it. The "RTS" locater doesn't
look only for the last "RTS", it really looks for
all "RTS" in the STEP range.

Stealth.............: No stealth abilities at all. All can be seen on
                      the SnoopDos screen.

Armouring...........: No special armouring found in this virus.It just
                      uses somekind of encryption(depending on $dff006)
                      for it's code, which is static.

-------------------- Agents --

Countermeasures.....: VW 5.9, VT 2.80 (?)
Countermeasures successful: All of the above
Standard means......: –

-------------------- Acknowledgement -----------------------------------

Location............: (C) Hannover, Germany
Classification by...: Markus Schmall and Heiner Schneegold
Documentation by....: Markus Schmall
Date................: January, 16.01.1996.
Information Source..: Reverse engineering of original virus
Copyright...........: This document isn't allowed to be used in any
                      form without my permission. It's hereby allowed
                      for VTC Hamburg and Virus Help Team DK to use it.

==================== End of Invader Virus ============================