VirusWarning

Markus Schmall Andersen

COLLABORATORS			
	TITLE : VirusWarning		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY	Markus Schmall Andersen	February 12, 2023	

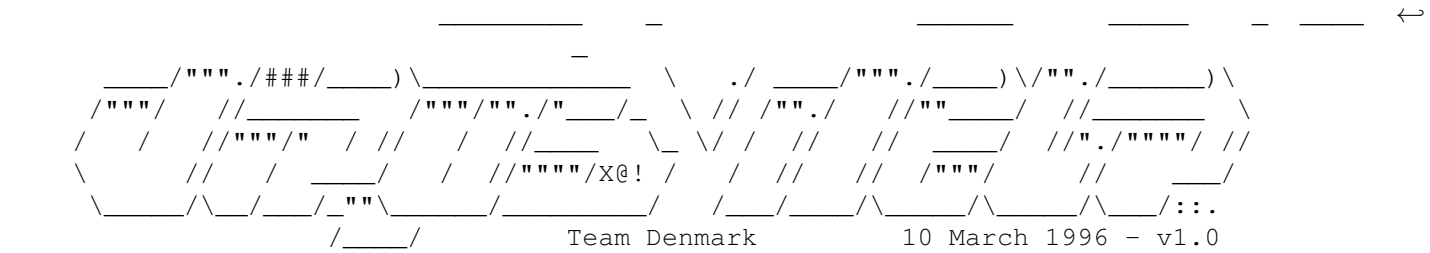
REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VirusWarning

1.1 Virus Warning's - v1.0 - 10 March 1996 - Size 113646 Unpacked



This guide was made to give you a better look of the files that we have written warnings about.

Click here to read the warnings !

Help Team Denmark using the warnings that we have been writing and send out on the Net's, with the exceptions of the virus warnings that Markus Schmall has written. But we have his permission to use them. No part of the guide may be altered in any way, without a written permission from

Virus Help Team Denmark

The newest versions of the Amiga Antivirus programs

1.2 The newest updates of the Amiga AntiVirus programs

The newest updates of the Amiga AntiVirus programs

(10 March 1996)

VirusWorkshop v5.9.... (04.02.1996) By Markus Schmall.

```
            VirusZ II v1.29........(01.03.1996) By Georg Hoermann.
            VT v2.81...............(10.03.1996) By Heiner Schneegold.
            Virus_Checker v8.04....(10.12.1995) By John Veldthuis.
            Xtruder v2.3...........(20.02.1996) By Martin Wulffeld.

Please remember to support the antivirus programmers, after all they are
helping you.......
```

1.3 Virus Help Team Denmark - Copyright © 1996 - v1.0

This Guide will be spread every 2 month, with all the new warnings by Markus Schmall and Virus Help Team Denmark. We will at that time have sent the new Warnings out on all the Nets and BBS'es, that we have access to (InterNet, FidoNet, AmyNet etc.).

If you want to use this guide or some of the warnings, please contact one of us and get a written permisssion to do it. If you want to use the warnings that Markus Schmall has written, please contact him to get his permission.

Jan Andersen	Virus Help Team Denmark's BBS
Fido... 2:235/112.0	Phone Number..: +45 4659 6867
AmyNET. 39:141/142.0	Open.....: 24 Hours
VirNet. 9:451/247.0	Modem.....: USR 33.600 V.FC

A great thanks must go to:

Markus Schmall.....: For letting us use his warnings in this guide.

Another thanks must go to: Jan-Jan, Lars, Henrik, Georg, Heiner, John, Torben, Soenke, VTC, Martin for programs and support.
Kim B., Enzo, Deliveryman, Flemming S. for collecting trojans and viruses for us.
(Sorry if I forgot you)

All the guys that is helping us collecting the new virus, and the few ones that are helping everybody, by programming a viruskiller.

1.4 Virus and Trojan warnings! - © Copyright M.Schmall & Virus Help Team DK

New warning in this guide !!!!! Name	Warning ↩
Strange Atmosphere LinkVirus ....: (Flake023.txt)	(srn-db33.lha)
VirusMemKill v1.2 Trojan ....: (Flake022.txt)	(VMK12.LHA)

```
 Old warnings in alfabetic order                                  Warning Name
-------------------------------------------------------------------------------

                Abase infected Saddam Archiv      (ABASE.DMS)
               ....: (Vhelp-15.txt)

                Achtung.exe Trojan.               (GATH95-!.LHA)
               ....: (Vhelp-05.txt)

                Addy v0.99 Trojan.                (ADDY099.LHA)
               ....: (Vhelp-02.txt)

                AmiBlank Trojan                   (ABLANK11.LHA)
               ....: (Flake021.txt)

                AmiExpress v5.0 Trojan            (PSG-AE5.LHA)
               ....: (Vhelp-18.txt)

                Callerslog v1.2 Trojan            (MST-CA12.LHA)
               ....: (Vhelp-20.txt)

                CarlingCard Hacker Trojan         (CCHACK2.exe)
               ....: (Vhelp-17.txt)

                Commander link-virus Infector.    (dpl-mam1.dms)
               ....: (Vhelp-04.txt)

                Commander link-virus Infector.    (Denistro.exe)
               ....: (Vhelp-00.txt)

                ConMan Trojan                     (hackt.lha)
               ....: (Flake006.txt)

                ConMan 1995 link-virus            (M-hac.lha)
               ....: (Flake016.txt)

                CoP Killer v1.1 Trojan            (COPKILL1.LHA)
               ....: (Vhelp-19.txt)

                Creator v1.0 Trojan               (CREATOR.LHA)
               ....: (Vhelp-12.txt)

                CygnusEd v4.00 Trojan.            (CED4.LHA)
               ....: (Vhelp-08.txt)

                DancePoolModTro.exe Infected      (SIGN.LHA)
               ....: (Vhelp-32.txt)

                DirectoryOpus v5.00.              (OPUS5.LHA)
               ....: (Vhelp-09.txt)

                DiskMaster v5.1 Trojan
               ....: (Vhelp-25.txt)
 DMS v2.06 Trojan                  (cry_206.lha)  ....: (Flake003.lha)

                dpl-dc99.lha trojan               (dpl-dc99.lha)
```

```
                ....: (Flake004.lha)

                 FileGhost 3 LinkVirus
                ....: (Flake009.txt)

                 Flake013.txt Fake                  (BIO-WARN.LHA)
                ....: (Flake014.txt)
~
                 Futuretracker Trojan               (TRSI-FT.LHA)
                ....: (Vhelp-14.txt)

                 Achtung.exe Trojan                 (Gath95-!.lha)
                ....: (Flake005.lha)

                 Happy_New_Year_96' link virus
                ....: (Flake017.txt)

                 HardDiskSpeeder v1.5 ©GVP Inc.     (GVP-HS15.lha)
                ....: (Flake012.txt)

                 IStrip v2.1 Trojan                 (Istrip21.lha)
                ....: (Flake002.lha)

                 LHA v3.0 Trojan.                   (LHA30.LHA)
                ....: (Vhelp-07.txt)

                 LZX v1.30 Trojan (CoP Type F)      (LZX130.lha)
                ....: (Flake007.txt)

                 MakeKey v1.10 For Virus_Checker    (VcKey110.lha)
                ....: (Flake013.txt)

                 NC210.LHA and NC210.LZX Infected   (NC210.LHA/LZX)
                ....: (Vhelp-31.txt)

                 NComm v3.2 Trojan.                 (NCOMM32.LHA)
                ....: (Vhelp-06.txt)

                 No Sense Diskmagazine Infected     (C!S-NS1.DMS)
                ....: (Vhelp-33.txt)

                 Pestilence Bootblockvirus 1.15
                ....: (Flake001.lha)

                 Phenomena DOS-Extender V1.1        (PHA-XMAS.lha)
                ....: (Flake019.txt)

                 Quarterback Tools Trojan           (ORS-QBD.LHA)
                ....: (Vhelp-24.txt)

                 Removcmd.lha Trojan                (Removcmd.lha)
                ....: (Flake000.lha)

                 SInfo v1.00 Trojan                 (SINFO10.LHA)
                ....: (Vhelp-11.txt)

                 Surprise Trojan at 'TP 4'.         (SURPRISE.DMS)
```

```
                ....: (Vhelp-01.txt)

                 Susi_Drive_Stepper Trojan
                ....: (Flake018.txt)

                 TMTC90.LHA Virus Infected         (TMTC90.LHA)
                ....: (Vhelp-30.txt)

                 TP-5 Andromeda Demo Trojan        (TP5-ANDR.LHA)
                ....: (Vhelp-27.txt)

                 TP-5 Parallax Demo Trojan         (TP5-PRLX.LHA)
                ....: (Vhelp-29.txt)

                 TP-5 Silents DK Trojan            (TP5-TSL.LHA)
                ....: (Vhelp-28.txt)

                 TP-5 Spaceballs Demo Trojan       (TP5-SPAC.LHA)
                ....: (Vhelp-26.txt)

                 TP-5 TRSI Trojan                  (TP5-TRSI.LHA)
                ....: (Flake020.txt)

                 TRSi Installer Trojan             (TRSI-INS.LHA)
                ....: (Vhelp-21.txt)

                 TRSi Installer Trojan             (TRSI-INS.LHA)
                ....: (Flake011.txt)

                 Virus_Checker v6.60 Trojan        (VCHCK660.lzx)
                ....: (Vhelp-23.txt)

                 VirusWorkshop v5.0 Trojan         (TRSI-VW5.LHA)
                ....: (Vhelp-15.txt)

                 VirusZ II v1.14 - Fake            (VZII_114.LHA)
                ....: (Vhelp-03.txt)

                 VirusZ II v1.19 - Fake            (VZII_119.LHA)
                ....: (Flake010.txt)

                 WireFace Trojan Type G            (chkmount.lha)
                ....: (Flake015.txt)

                 ZAP v1.1 Unpacker virus infected  (TXC-Z11.LHA)
                ....: (Vhelp-34.txt)

 ---------------------------- End of list -------------------------------
```

1.5 Commander Infector

```
  WARNING !!! WARNING !!! WARNING !!! WARNING !!!WARNING !!! WARNING !!!
       WARNING !!! WARNING !!!WARNING !!! WARNING !!!WARNING !!!

      We have nok found the file that infects your systems with the
```

Commander virus. The infector program is called:

DENISTRO.EXE

I have two versions of this file, but they both installs the virus:

1.. It has a size of 66592 bytes.
2.. It has a size of 71800 bytes.

Do not start this program, it will install the link part of Commander virus, and add 1664 bytes to your LoadWB command.

This Virus has now been around for a few month, but now we know. Over 60 BBS'es in scandinavia has now been infected with this new virus. But thanx to the AntiVirusProgrammers that has updated there killers fast, to try and stop this virus.

Thanx to:

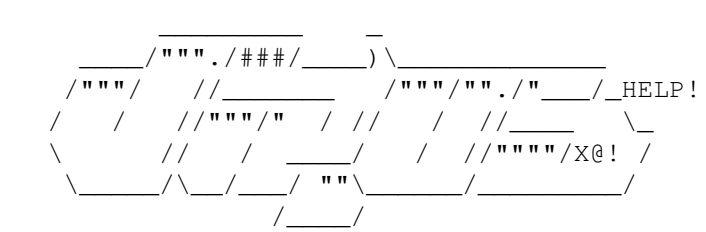
Kim B. Jensen - For sending my the 'Denistro.exe'.

The installer of Commander is now on it's way to every well known anti-virus programmer.

Regards

Jan Andersen.
Virus Help - Team Denmark.

FidoNet: 2:236/116.1
AmyNet : 39:141/142.0



1.6 Surprise Trojan at The Party 4

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

TROJAN FROM 'THE PARTY 4' CALLED SURPRISE.EXE

There 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 94' 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 :  39:141/142.0
    \XX/      TEAM DENMARK
```

1.7 Addy v0.99 trojan

```
  WARNING !!! WARNING !!! WARNING !!! WARNING !!!WARNING !!! WARNING !!!
       WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


                  DO NOT EXECUDE THE FILES FROM 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.  Spread in
 the archive 'ADDY099.LHA'.

 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.

 There is a "Readme" text in the archive, this is what is says:

 ////////////////////////// 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 can't  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 !
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

There is a FILE ID.DIZ to, here is the text:


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

------ END -------

 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 :  39:141/142.0                 \_____/\__/___/ ""\_______/__________/
                                                 /____/
```

1.8 Fake VirusZ II v1.14

```
  WARNING !!! WARNING !!! WARNING !!! WARNING !!!WARNING !!! WARNING !!!
       WARNING !!! WARNING !!!WARNING !!! WARNING !!! WARNING !!!

                          FAKE VIRUSZ II v1.14
                         ======================
```

On Thursday 2-2-95, one of my users from Sweden uploaded a new version of VirusZ II v1.14, Released 2-2-95, and it has a size of 64664 bytes. But it is a FAKE VERSION. In the doc' there was added new virus, but they was the same as in version 3.06 of the old VirusZ, and there was some new virus and here is a quote from the FAKE guide:

- Added Commander2, Saurønh, and Recycle viruses! Thanks to Markus Schmall for sending them.

- Added Big Bug, MixiMaxiMum '93, BootX Kisser and The Amiga Fucker 15.3 bootviruses. Thanks to Markus Schmall for sending them, as always!.

I have called Markus on the phone, and he has never heard of these virus, But he told me that there has been a new release of VirusZ II, but the new original release is v1.13.

Remember to check the 'ABOUT' gadget,the size of the file is stated there if the size is not right, do not use that version of VirusZ II.

Regards....

```
                                       _________   _
 Jan Andersen.                    _____/"""./###/_____)\______________
 Virus Help - Team Denmark.      /"""/   //________   /"""/""./"___/_HELP!
                                /   /   //"""/"  / //   /  //_____   \_
 FidoNet:   2:236/116.1         \       //   /  _____/   /  //""""/X@! /
 AmyNet :  39:141/142.0          \______/\__/___/ ""\_______/__________/
                                              /_____/
```

1.9 Commander Infector #2

VIRUS WARNING !!! - VIRUS WARNING !!! - VIRUS WARNING !!!
VIRUS WARNING !!! - VIRUS WARNING !!!

ANOTHER COMMANDER LINK-VIRUS INFECTOR

We have now found another program, that infects your systems with the Commander virus. The infector program is a Demo or an Intro. If someone knows the name and adress of the programmer of this program, please contact me.

The name of the second installer is:

"MY MAMA IS A VAMPIRE"

It can be found at two archives with the name:

```
Title : dpl-mam1.dms
Size  : 523162
Desc. :         DuPlO DeMo DiViSiOn PrEsEnTs:
        - --> mY mAMA iS a vAMPiRE! (aGA oNLY) <-- -
        - --- * Version 3.0 (100% working!)-[1/2]- -
        Awesome texture effect! - Released 30 Oct 94

Title : dpl-mam2.dms
Size  : 602250
Desc. : - --> mY mAMA iS a vAMPIRE! (aGA oNLY) <-- -
        - ---------- * Version 3.0 * ------------- -
        - - (100% bugfixed and fully working ----- -
        - -- version, packed in a NON corrupted -- -
        - --- archive this time!) ---------------- -
        ------------------------------------[2/2]- -
```

```
Do not start  this program,  it will install the Commander virus,
and add 1664 bytes to your LoadWB command. And infect everything
that you will try to execute.

Thanx to:
Steffen Rabenborg - For telling me about the new installer.
Peter Klein - For finding the new installer to me.

The installer of Commander is now on it's way to every well known
anti-virus programmer.

Regards....

                                        _________     _
Jan Andersen.                        ____/"""./###/____)\_____________
Virus Help - Team Denmark.          /"""/   //________    /"""/"".("___/_HELP!
                                   /   /   //"""/"  / //   /  //_____   \_
FidoNet:   2:236/116.1             \      //   /  ____/   /  //"""""/X@! /
AmyNet :  39:141/142.0              \_____/\__/___/ ""\______/__________/
                                              /____/
```

1.10 Achtung.exe trojan (09.02.95)

```
WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
     WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


      DO NOT START 'ACHTUNG.EXE' FROM THE ARCHIVE 'GATH95-!.LHA'
      ----------------------------------------------------------

 There has just been released a archive called 'GATH95-!.LHA', there are
 one dectructiv program in the archive:

 Achtung       14032 Bytes
 Achtung.exe   14032 Bytes

 The FILE_ID.DIZ looks like this:

 +-----------------------------------------+
 |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! }---+


 This has NOTHING to do with the 'Gathering 95' in Oslo....

  Do not start the program 'Achtung.exe' and 'Achtung', will search for
 DH0:, and then make a lot of files starting with this:

 LAMER.AAAAAAAA           10240 Bytes (and then change the last letter B)
```

```
LAMER.AAAAAAAB          10240 Bytes (and then change the last letter C)
LAMER.AAAAAAAC          10240 Bytes (and then change the last letter D)

 And keep doing that until your HD is full.


 I have talked to a guy in Denmark, that  has lost everything  on his DH0
drive, and there was some damage  to a lot of files, and  the name of his
system was renamed to 'LAMER:!!!!' due to this little sucker.
 And I have other reports about HD craches due to 'Achtung.exe'.

 I have tried it on floppy  disks, and the one a called 'DH0:' was filled
up with all of these 'LAMER.AAAAAAAA' 880 kb of them.

 I'm not gonna lose my HD trying to find out some more about this thing.
The most improtant thing is: DON'T START THIS SUCKER !!!!!!!!

But this little thing is on it's to every wellknown antivirus programmer.

 Thanx to Brian Overby for the help....


Regards....

                                        _________     _
Jan Andersen.                          _____/"""./###/_____)\_______________
Virus Help - Team Denmark.            /"""/   //________   /"""/"".("___/_HELP!
                                     /   /   //"""/"  / //   /  //_____   \_
FidoNet:   2:236/116.1               \      //   /  _____/   /  //"""""/X@! /
AmyNet :  39:141/142.0                \_____/\__/___/ ""\_______/__________/
                                              /_____/
```

1.11 NComm v3.2 Trojan (23.03.95)

```
WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
     WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


       DO NOT START 'NComm v3.2' FROM THE ARCHIVE 'NCOMM32.LHA'
      ------------------------------------------------------------

 There has just been released a archive called 'NCOMM32.LHA', there are
 a dectructiv program in the archive:

 NComm   121896 Bytes (Packed with Stonecracker 4.04)
 NComm   226116 Bytes (Unpacked)

 The FILE_ID.DIZ looks like this:

 ****************************************
 NCOMM V3.2 *CRACKED* KEYFILE CHECK REMOVED!
 ****************************************


 The 'Sucker' started in the S: directory replacing the data's in EVERY
 file with the text 'CIRCLE OF POWER 1995', so the startup-sequence and
```

```
rest of the files in the S dir was totally destroyed.  All .info files
will be replaced in the same way

The archive is now on it's way to every wellknown anti-virus programer.

Thanx to Jan Ravn, for sending the 'thing' to us....


Best Regards.....

                                        _________    _
Jan Andersen.                          ____/""".//###/____)\_________________
Virus Help - Team Denmark.            /"""/   //________   /"""/"".//"___/_HELP!
                                     /   /   //"""/"  / //   /  //_____   \_
FidoNet:   2:236/116.1               \      //   /  ____/   /  //"""""/X@! /
AmyNet :  39:141/142.0                \_____/\__/___/ ""\______/__________/
VirNet :   9:451/247.0                              /____/
```

1.12 LHA v3.0 Trojan (27.03.95)

```
WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
    WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


      DO NOT START THE 'LHA v3.0' FROM THE ARCHIVE 'LHA30.LHA'
     ---------------------------------------------------------

There has just been released a archive called 'LHA30.LHA', and there are
a dectructiv program in the archive:

"LHA3.0    69888 bytes (Packed with Stonecracker 4.04)"
"LHA3.0   105808 bytes (Unpacked)


The FILE_ID.DIZ looks like this:

LHA 3.0 FROM STEFAN BOBERG


The "Sucker" started  in the S: directory  replacing the  data's in EVERY
file with  the text  'CIRCLE OF POWER 1995:', so the startup-sequence and
rest of the files in the S dir was totally destroyed.

The LHA3.0 looks a lot like the fake 'NComm 3.2', it does the same things
to your HD and disk's.

The archive is now on it's way to every wellknown anti-virus programer.

Thanx to Kim B. and Flemming S., for sending the 'thing' to us....


 Best Regards.....

                                        _________    _
 Jan Andersen.                         ____/""".//###/____)\_________________
 Virus Help - Team Denmark.           /"""/   //________   /"""/"".//"___/_HELP!
                                     /   /   //"""/"  / //   /  //_____   \_
```

```
 FidoNet:   2:236/116.1          \       //   /  _____/   /  //"""""/X@! /
 AmyNet :  39:141/142.0           \______/\__/___/ ""\_______/__________/
 VirNet :   9:451/247.0                          /_____/
```

1.13 CygnusEd v4.00 - CoP Trojan - (27.03.1995)

```
WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
     WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


        DO NOT START THE 'CED4' FROM THE ARCHIVE 'CED4.LHA'
     ------------------------------------------------------------

There has just been released a archive called 'CED4.LHA', and there are
a dectructiv program in the archive:

CED4     174500 bytes (Unpacked)


The FILE_ID.DIZ looks like this:

CYGNUS EDITOR V4.0 (MAIN)


The "Sucker"  started  in the S: directory  replacing the  data's in EVERY
file with  the text  'CIRCLE OF POWER 1995:',  so the startup-sequence and
rest of the files in the S: dir was  totally destroyed.  This goes for all
files in your 'DEVS:' directory to.

The CED4 looks a lot like the fake 'NComm 3.2' and 'LHA30.LHA' it does the
same things to your HD and disk's.

Please take care,  there is a  lot of fake programs around, that does this
thing. Checke everything before you start it.

The archive is now on it's way to every wellknown anti-virus programer.

Thanx to Kim B., for sending the 'thing' to us....


 Best Regards.....

                                      _________     _
 Jan Andersen.                    ____/""".//###/____)\_____________
 Virus Help - Team Denmark.      /"""/   //________   /"""/"".//___/_HELP!
                                /   /   //"""/"  / //   /  //_____   \_
 FidoNet:   2:236/116.1         \       //   /  _____/   /  //"""""/X@! /
 AmyNet :  39:141/142.0          \______/\__/___/ ""\_______/__________/
 VirNet :   9:451/247.0                          /_____/
```

1.14 DirectoryOpus v5.00 - CoP Trojan - (29.03.1995)

```
                WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!  ↩
                   WARNING
      WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


        DO NOT START THE 'OPUS5' FROM THE ARCHIVE 'OPUS5.LHA'
     ------------------------------------------------------------

There has been released a archive called 'OPUS5.LHA', and there are a
dectructiv program in the archive:

I have not seen the archive yet, but I have talked to some people that
used this 'thing', and had there data files replaced,

It does the same things that 'NCOMM32.LHA', 'CED4.LHA' and 'LHA30.LHA'
it will replace the data's in EVERY file with the text:

'CIRCLE OF POWER 1995:'

Please take care,  there is a  lot of fake programs around, that does
this thing. Checke everything before you start it.

If you find this program, please send it to me, or send it to all the
well known antivirus programmers.


Regards....

                                        __________     _
Jan Andersen.                          ____/""".//##/____)\_______________
Virus Help - Team Denmark.            /""""/   //________   /"""/"".//"___/_HELP!
                                     /   /   //"""/"  / //   /  //____   \_
FidoNet:   2:236/116.1               \       //   /  ____/   /  //""""/X@! /
AmyNet :  39:141/142.0                \_____/\__/___/ ""\______/__________/
VirNet :   9:451/247.0                              /____/


                More information about the 'OPUS5.LHA' Trojan
```

1.15 More information about the 'OPUS5.LHA' Trojan (04.04.95)

```
 WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING
      WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!

Hi All !!!

I now know some more about the FAKE Opus v5.0, it has a size of 347308
bytes.  The archive 'OPUS5.LHA' has a size of 464397 bytes, and in the
FILE_ID.DIZ you can read:

-----------------------------------------
           DIRECTORYOPUS v5.0
-----------------------------------------
* Uses multiple processes for windows.
```

```
* Full REXX support
* Faster dir-routines.
* Better archive handeling, supports LZX!
-----------------------------------------
```

No anti-virus program can find this trojan yet, but I have tested it on all the wellknown killers, and there are only 2 that detects something yet, but this trojan is now on it's way to every wellknown anti-virus programmer

VirusWorkShop v4.9, can not find it yet, but will give you a requester saying that:
"$3f0/$3f1/$3e8 Hunk at the beginning found"

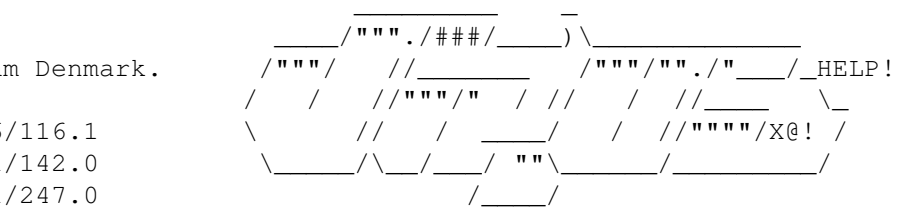
VT v2.71 can not find it yet, but will give you a requester saying that:
"3E8-Hunk am anfang ist im file"

Thanx to Kim B. for uploading this 'thing' to our BBS.

Regards....

Jan Andersen.
Virus Help - Team Denmark.

FidoNet: 2:236/116.1
AmyNet : 39:141/142.0
VirNet : 9:451/247.0



1.16 About SInfo v1.0 - CoP Trojan - (11.04.1995)!

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

DO NOT START THE 'Sinfo v1.0' FROM THE ARCHIVE 'SINFO10.LHA'

There has been released a program called 'SInfo v1.0', do not start that program it will replace every file in your S:, Libs: and C: with a new file, with a size of 5 bytes, in this file you can read 'cop!'. This is another program from 'CIRCLE OF POWER!', the same lamer that has written 'NComm32.LHA', 'OPUS5.LHA', 'LHA30.LHA' and 'CED4.LHA'.

There is another thing, SInfo v1.0 will ask for 'SINFO.library', and the library is in the archive, BUT it is not 'Sinfo.library', it is the reel 'Bootblock.library v3.1' from SHI, why this ????????

SInfo v1.0 is spread in a program called 'SINFO10.LHA', and has a size of 4432 bytes

The main program has a size of 2552 bytes.

In the FILE_ID.DIZ you can read:

```
  .-----------------------------------------.
  | SYSTEMINFO V1.0 BY JURGEN HUNSMANN 1995! |
  | A VERY GOOD REPLACEMENT OF THE INFO CMD! |
  `----------------------------------(baron)-'
```

In the DOC you can read this:

```
---------------------------- QUOTE START ---------------------------------

 TYPE: SystemInfo ala INFO
 DESC: Will list all devices available on you're system.
 AUTH: Jürgen Hünsmann
 DATE: 01-Apr-95
 MAIL: jh@grafix.xs4all.nl
 FIDO: 2:286/407.19

                              SInfo v1.0 DOC!
                             ~~~~~~~~~~~~~~~~~
 It works just like the WorkBench Info command, but has some features not
 found in the default INFO command.

 1) It will show Meg/Kilo/Bytes left on the device instead of blocks.
 2) It is ALOT faster
 3) It shows assigns
 4) Can force devices to be validated!

 Contact me at the addresses above!

---------------------------- QUOTE END -----------------------------------
```

This new 'CIRCLE OF POWER!' thing, is on it's way to every wellknown anti-virus programmer.

And to the 'COP!' programmer, STOP the shit you are doing, you must have a big problem somewere.

Thanx to Kim B. for uploading this to my BBS.

Regards...

```
 Jan Andersen.                        _____/""".//###/____)\_______________
 Virus Help - Team Denmark.          /"""/   //________   /"""/"".//___/_HELP!
                                    /   /   //"""/"  / //   /  //_____   \_
 FidoNet:   2:236/116.1             \      //   /  _____/   /  //"""""/X@! /
 AmyNet :  39:141/142.0              \______/\__/___/ ""\_______/__________/
 VirNet :   9:451/247.0                          /_____/
```

1.17 Creator v1.0 - Trojan - (18.04.1995)

```
                WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!  ↩
                   WARNING
       WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
```

DO NOT START THE 'CREATOR' FROM THE ARCHIVE 'CREATOR.LHA'

In the last day or two, a lot of people have uploaded a small program to 'Virus Help BBS' with the name 'cREATOr v1.0', it is stated in the doc that it is a program, that will you choose how fast your HD shall run after every reset. BUT if you run it, it will start to format your hard-disk. The doc says nothing about this.

Here is some info about the program:

```
Archive name......: CREATOR.LHA
Archive size......: 2757 bytes
Files in archive..: CREATOR.DOC    1124 bytes
                    FILE_ID.DIZ     484 bytes
                    C:CREATOR.SCR    40 bytes
                    S:CREATOR.DAT  2880 bytes
```

The FILE_ID.DIZ looks like this:

```
*****************************************
*        cREATOr V1.0 (C) 04-10-95        *
*                                         *
* Thiz Powerful Tool Will Let You Choose  *
* How Fazt Your HD (Mili Seconds) Shall   *
* Run After Every Reset !!! Normally Thiz *
* Is Only Possible With SCSI-2 HD's And A *
* Fazt CPU (020/030/040) But After 1 Year *
* Of Hard Coding I've Developed This Good *
* Product Which Should Run On All AMIGAS! *
*****************************************
```

So DO NOT start this thing, you will loose your HD.

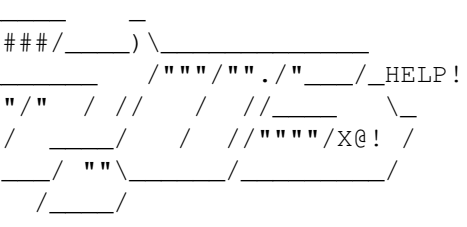
This thing is on it's way to every wellknown antivirus programmer, who will accept new virus from 'Virus Help'.

Thanx to everybody that has uploaded this thing to our BBS.

Regards....

Jan Andersen.
Virus Help - Team Denmark.

FidoNet: 2:235/112.0
AmyNet : 39:141/142.0
VirNet : 9:451/247.0



More about the 'Creator' Traojan

1.18 More about the Creator trojan - 18.04.1995)

```
Hi All......

Hmmmmmm, there has been another release of the CREATOR trojan, but there
is something wrong  again.  Again the doc' states  that it  will let you
choose how fast your HD  shall run after every reset.  But if you try to
start the program, you will asked to write 'FORMAT' in a shell, and that
would be a stupid thing to do, right ???.

This 'new' update will NOT work at any of my Amiga's, so there for I can
not tell you what it will do, but I have people testing it right now.

Here is some info about the program:

Archive name......: CREAT_11.LHA
Archive size......: 2757 bytes
Files in archive..: CREATOR.DOC    1124 bytes
                    FILE_ID.DIZ     484 bytes
                    C:CREATOR.SCR    40 bytes
                    S:CREATOR.DAT  2880 bytes

The FILE_ID.DIZ looks like this:

*****************************************
*        cREATOr V1.1 (C) 04-11-95        *
*                                         *
* Thiz Powerful Tool Will Let You Choose  *
* How Fazt Your HD (Mili Seconds) Shall   *
* Run After Every Reset !!! Normally Thiz *
* Is Only Possible With SCSI-2 HD's And A *
* Fazt CPU (020/030/040) But After 1 Year *
* Of Hard Coding It Works Very Fine !!!   *
* FIX VERSION - FIXED VERSION - FIXED VER *
*****************************************

This thing is on it's way to every wellknown antivirus programmer, who
will accept new virus from 'Virus Help'.

Thanx to everybody that has uploaded this thing to our BBS.


Regards....

Jan Andersen.
```

1.19 FutureTracker - CoP Trojan - 19.04.1995)

```
 WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING
      WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


    DO NOT START THE 'FUTURETRACKER' FROM THE ARCHIVE 'TRSI-FT.LHA'
    ---------------------------------------------------------------
```

Okay there is another 'Circle Of Power' trojan around. This time it is in a fake ProTracker called 'FutureTracker'. It will do the same thing as the other trojans that 'CoP' has released in the last month, only this time it will rewrite every file in DEVS:, L:, and S:, with another file where you can read this:

[cOp]: Khanan / Circle Of Power :[cOp]

This time the 'thing' will show a text on the screen (See the Iff.Pic in this archive). Here is what it says:

```
- - - - - - - - - - - - - - - - START - - - - - - - - - - - - - - - - -

.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp

                          cIrcle of pOwer'95

.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp.cOp

--[==========================================================================]--

Sweden's no.1, "CIRCLE OF POWER" rammed yer arse again!! Have phun retyping
             all those valueble config's. haha! Fuck you all!

          -^( THE TERROR WILL NEWER STOP, PHEAR THE MIGHTY COP! )^-

--[==========================================================================]--
                                                                  [kHANAN/cOp]

- - - - - - - - - - - - - - - - - - END  - - - - - - - - - - - - - - - - - -
```

This text will come to your screen when 'FutureTracker' is replacing the files on your harddisk.

Here is some info about the program:

```
Archive name......: TRSI-FT.LHA
Archive size......: 278290 bytes
Files in archive..: FutureTracker      317608 bytes
                    FILE_ID.DIZ           360 bytes
                    FutureTracker.cfg    1065 bytes
                    FutureTracker.doc      90 bytes
```

The FILE_ID.DIZ looks like this:

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

```
This thing is on it's way to every wellknown antivirus programmer, who
will accept new virus from 'Virus Help'.

Thanx to Kim B. for uploading this thing to our BBS.

Regards....

                                        _________    _
Jan Andersen.                        ____/""".//###/____)\_______________
Virus Help - Team Denmark.          /"""/   //________   /"""/"".("___/_HELP!
                                   /   /   //"""/"  / //   /  //_____   \_
FidoNet:   2:235/112.0             \      //   /  ____/   /  //"""""/X@! /
AmyNet :  39:141/142.0              \_____/\__/___/ ""\______/__________/
VirNet :   9:451/247.0                        /____/
```

1.20 VirusWorkshop v5.0 - CoP Trojan - 21.04.1995

```
WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING
     WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


  DO NOT START THE 'VIRUSWORKSHOP' FROM THE ARCHIVE 'TRSI-VW5.LHA'
  ---------------------------------------------------------------

There has just been released a FAKE  version of 'VirusWorkShop v5.0',
when you try  to run the program,  some music will start, and that is
all that I can find out.  I can not se that it writes anything to any
drives. But I'll let some others, test it on there systems.

I can tell you, that Markus Schmall has never made a version 5.0, and
that he never will release VirusWorkShop with the version string v5.0

This is  said to  be antoher  'COP' (Circle Of Power) release,  but I
can not get it to infect my system.


Here is some info about the program:

Archive name.........: TRSI-VW5.LHA
Archive size.........: 221737 bytes
VirusWorkShop Size..: 135744 bytes


The FILE_ID.DIZ looks like this:

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


This thing is on it's way to every wellknown antivirus programmer, who
```

```
will accept new virus from 'Virus Help'.

By the way.. The newest version of VirusWorkShop at this date is v4.9,
and the size is 136556 bytes.

Thanx to Kim B. for uploading this thing to our BBS.

Regards....

                                        _________     _
Jan Andersen.                          _____/"""./###/_____)\_______________
Virus Help - Team Denmark.            /"""/    //________    /"""/"".("___/_HELP!
                                     /    /    //"""/"   / //    /   //_____    \_
FidoNet:   2:235/112.0               \       //    /  _____/    /   //"""""/X@! /
AmyNet :  39:141/142.0                \______/\__/___/  ""\_______/__________/
VirNet :   9:451/247.0                                  /_____/
```

1.21 ABase - Saddam Infected Archive - (22.04.1995)

```
 WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING
      WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


       THE ARCHIVE 'ABASE.DMS' IS INFECTED WITH SADDAM VIRUS
       ----------------------------------------------------

There has been spread a demo version of a program with the name 'ABASE',
it is an adress base from Poland. This archive contains the Saddam virus
which is inside the 'l:Disk-validator'.
This info is for the Amiga user that still runs with KickStart 1.3, that
is because that Saddam Virus can not run under kickstart 2.0 -> 3.1.


Here is some info about the program:

Archive Name.......: ABASE.DMS
Archive Size.......: 222609 Bytes
ABase program......: 83096 Bytes, PowerPacked (138332 Bytes Unpacked)
Saddan Virus.......: L:Disk-Validator (1848 bytes).


Again thanx to Kim B. (Great Virus-Hunter).....

Regards...

                                        _________     _
Jan Andersen.                          _____/"""./###/_____)\_______________
Virus Help - Team Denmark.            /"""/    //________    /"""/"".("___/_HELP!
                                     /    /    //"""/"   / //    /   //_____    \_
FidoNet:   2:235/112.0               \       //    /  _____/    /   //"""""/X@! /
AmyNet :  39:141/142.0                \______/\__/___/  ""\_______/__________/
VirNet :   9:451/247.0                                  /_____/
```

1.22 CarlingCard Hacker - Trojan - 02.05.1995

```
WARNING !! WARNING !! WARNING !! WARNING !! WARNING !! WARNING !! WARNING
     WARNING !! WARNING !! WARNING !! WARNING !! WARNING !! WARNING


               DO NOT START THE PROGRAM 'CCHACK2.exe'
               --------------------------------------

There has been released a program that is said to be a CallingCard Hacker,
if you  start the program it  will look for a BBS: assign,  and  then read
the user.data file. This textstring is coded in the the file. Why a hacker
program for CallingCards, want to read the 'BBS:User.Data', I do not know,
but do not trust this program....

Here is some info about the trojan:

Name.....: CCHACK2.exe
Size.....: 11216 Bytes (unpacked)


If you start the program this will be displayed:

MCI CallingCard Hacker by ByTePaCkEr/Finland 1995

Usage: CChack2.exe <CALLINGCARD.NR.>


VT v2.72 will find this 'thing', but in the doc to VT, Heiner states that
the file has a size of 11368 Bytes (unpacked), so maybe there is an other
version of this trojan,  and maybe the name of this is 'CCHACK.EXE', I do
not know.

This 'thing' is on it's way to every wellknown antivirus programmer, that
will accept new virus from us.

Thanx again to Kim B. a great virushunter, for uploading it to us.....
And to Markus Schmall for the first info about this 'thing'...

Regards....

                                    _________     _
Jan Andersen.                      ____/"""./###/____)\_______________
Virus Help - Team Denmark.        /"""/   //________   /"""/"".("___/_HELP!
                                 /   /   //"""/"  / //   /  //____   \_
FidoNet:   2:235/112.0           \      //   /  ____/   /  //"""""/X@! /
AmyNet :  39:141/142.0            \_____/\__/___/ ""\______/__________/
VirNet :   9:451/247.0                         /____/
```

1.23 AmiExpress v5.0 - CoP Trojan - 03.05.1995

```
WARNING !! WARNING !! WARNING !! WARNING !! WARNING !! WARNING !! WARNING
     WARNING !! WARNING !! WARNING !! WARNING !! WARNING !! WARNING


         DO NOT START THE 'Acp' FROM THE ARVHIVE 'PSG-AE5.LHA'
         -----------------------------------------------------
```

```
There has been released  a program that is said to be a new version of the
BBS program AmyExpress v5.0,  but it is another  'Circle Of Power' trojan,
it will replace every file in DEVS: and S: dir,  with a textfile where you
can read:

[cOp]: Khanan :[cOp]

Inside  the fake  'AmiExpress v5.0'  file 'Acp',  you can read this is the
ASCII text:

$VER: ACP V5.0 (C)-95 JOSEPH HODGE


In the File_ID.Diz, you can read:

AmiExpress v5.0


If you start the program,  a shell window will pop up,  where you can read
this:

[cOp]:              The Circle Of Power did it AGAIN!               :[cOp]
[cOp]:                                                              :[cOp]
[cOp]:      THE TERROR WILL NEVER STOP, PHEAR THE MIGHTY COP!       :[cOp]


Here is some info about the archive it is spread in:

Archive Name..: PSG-AE5.LHA
Archive Size..: 71982 Bytes (Striped For BBS adds)
Trojan Name...: Acp
Trojan Size...: 71904 Bytes


Someone must  know this 'Khanan' or other  members of 'COP'.  If you know
anything about these stupid guy's, please contact us....

This 'thing' is on it's way to every wellknown antivirus programmer, that
will accept new virus from us.

Thanx again to Kim B. for uploading this 'sucker' to our BBS.....

Regards....

                                        _________     _
Jan Andersen.                          ____/"""./###/____)\_______________
Virus Help - Team Denmark.            /"""/   //________   /"""/"".("___/_HELP!
                                     /   /   //"""/"  / //   /  //____   \_
FidoNet:   2:235/112.0               \      //   /  ____/   /  //"""""/X@! /
AmyNet :  39:141/142.0                \_____/\__/___/ ""\______/__________/
VirNet :   9:451/247.0                              /____/
```

1.24 CoP Killer v1.1 - CoP Trojan - 20.05.1995

```
 WARNING !! WARNING !! WARNING !! WARNING !! WARNING !! WARNING !! WARNING
      WARNING !! WARNING !! WARNING !! WARNING !! WARNING !! WARNING


     DO NOT START THE PROGRAM 'Copkiller' FROM THE ARCHIVE 'COPKILL1.LHA'
     ---------------------------------------------------------------------

 Okay there is another 'Circle Of Power' trojan on the loose. This time
 it will rewrite the  files in DEVS:,  and in the new file you can read
 this:

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

 Here is some info about the file it is spread in:

 Archive name: Copkill1.LHA
 Archive size: 9801 Bytes
 Cop Trojan  : Copkiller (8428 bytes)

 In the FILE_ID.DIZ you can read this:


>--------- FILE_ID.DIZ START --------------<

     _____ _______ ___  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{}

>--------- FILE_ID.DIZ END ----------------<

 But this is not a release from SHI.....

 This 'sucker is now on its way to every antivirus programmer, that will
 accept new virus from 'Virus Help Team Denmark'.

 Thanx to Bahrat Asar for uploading this 'sucker' to our BBS.


 Regards.....

                                      _________    _
 Jan Andersen.                  ____/""".###/____)\_____________
 Virus Help - Team Denmark.    /"""/   //________   /"""/"".("___/_HELP!
                              /   /   //"""/"  / //   /  //_____   \_
```

```
FidoNet:   2:235/112.0          \      //   /  ____/   /  //""""/X@! /
AmyNet :  39:141/142.0           \_____/\__/___/ ""\______/_________/
VirNet :   9:451/247.0                          /____/
```

1.25 Callerslog v1.2 - CoP Trojan - 30.05.1995

```
WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
     WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


 DO NOT START THE PROGRAM 'CALLERSLOF.SFX' FROM THE ARCHIVE 'MST-CA12.LHA'
 ------------------------------------------------------------------------
```

There has been found a new 'COP' trojan in a fake program. It was released about the 28'th of May. Here is some info about the trojan:

```
Archive Name: MST-CA12.LHA
Archive Size: 19349 Bytes (Ripped for BBS add's)
Trojan Name : cALLERSLOG.SFX
Trojan Size : 8428 Bytes (Is not a SFX. Archive)
```

Here is what the File_ID.DIZ will tell you:

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

This new trojan will replace everything in your DEVS: dir. With a text 41 bytes long, where you can read this:

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

This new 'COP' trojan is now on it's way to every wellknown antivirus programmer that will accept new virus from Virus Help Team Denmark.

Thanx again to KIM B. for uploading this our BBS.

```
    Regards....
     __
__  ///       Jan Andersen         FidoNet:   2:235/112.0
\\///       --------------           AmyNet :  39:141/142.0
 \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.26 TRSI Installer - CoP Trojan - 10.06.1995

```
                WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!  ↩
                   WARNING !!!
     WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


There has just been released another  Trojan. It was uploaded to a BBS in
Sweden by Gryzor (Member of Circle Of Power). The name of the archive is:

TRSi-INS.LHA
(Size about 40000 bytes)

The FILE ID.DIZ says that this is an installer for several games.

But TRSI has nothing to do with this sucker.

We can at  this time not say anything  more about this trojan, bacause we
have written this warning out of a phone call from Markus Schmall, but we
will here more when Markus has tested this thing.


    Regards....
     __
__  ///       Jan Andersen         FidoNet:   2:235/112.0
\\///       --------------            AmyNet :  39:141/142.0
 \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0


               Click here
               to read Markus Schmall's test of the archiv.
```

1.27 Virus_Checker v6.60 - Trojan - 27.07.1995

```
WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
     WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


Hi All.....

There has just been found a fake Virus_Checker v6.60. Do not use this trojan
at all.  The VC.guide is just a rewritten v6.57. Here is some info about the
sucker:

Archive name... : VCHCK660.lzx
Archive Size... : About 122.000 bytes (Ripped for BBS adds)
VC v6.60 Size.. : 52400 bytes

The newest version of Virus_Checker is at this time v6.58 (Brain v1.20)

This new trojan is on its way to every wellknown antivirus programmer, that
will accept new virus and trojan from us.

     Regards....
```

```
    __
__  ///       Jan Andersen         FidoNet:   2:235/112.0
\\///       --------------            AmyNet :  39:141/142.0
 \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.28 QuarterBack Tools Diamond - CoP Trojan

```
WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
     WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


Hi All...

There has been released a new COP trojan. This time it is a fake
'QuaterBackTools'. This thimg will replace everything in your S:,
LIBS;, BBS:, m.m with a text string of 75 bytes.

The file_id.diz of this trojan looks like this:


 _____  ___   _____   _   ___  ___  _____
::::: / . \_/ ___)_/_)/ .__)(___)/ ___)::::.
:::::/  ª  \___  \   \  ª  \/   \___  \:::::
:::::\_____/___  /_  /__|   \_  /___  /:::::
 '--[RD10/CodX]¼\/--\/--¼ª____\/---¼\/---'
        QUARTER BACK TOOLS DIAMOND
 SUPPORTS AFS FILE SYSTEM, XPK PARTITIONS,
 REORGANIZES BETTER THEN REORG, AND USES A
 SAFETY DISK WHEN REORGANIZING! NO CRASH!
 RELEASED BY : ERICO / OSIRIS


Info about the trojan:

Archive name: ORS-QBD.LHA
Archive Size: About 128654 Bytes
Trojan Name : QBTools3
Trojan Size : 227716 Bytes

This new trojan is on its way to every wellknown antivirus programmer
that will accept new virus from Virus Help.

    Regards....
     __
__  ///       Jan Andersen         FidoNet:   2:235/112.0
\\///       --------------            AmyNet :  39:141/142.0
 \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.29 Diskmaster v5.1 - CoP Trojan - 04.11.95

```
WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
     WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
```

```
Hello everybody.....

The mad guys from 'Circle Of Power' is back. This time it is a faked program
called 'DiskMaster v1.4'. It will replace files in LIBS:, DEVS:, S:, with a
new file with the length of 41 bytes, and in this file you can read this
text:

FausT / cIRCLE oF pOWER'95 - TRUE POWER!

The file_id of this program look's like this:


       __________     _
  _____/""".//###/_____)\_________________
 /""""/    //________     /"""/"".//"___/_
/    /    //""""/"   / //    /   //_____    \_
\       //    /   _____/    /   //"""""/X@!/
 \______/\__/____/ ""\_______/___________/
-->><!VIRUS!<><</_____/->><>-!WARNING!-<><><--
Brought To You Diskmaster V5.1 Debugged
And Updated With VirusX2.4 VirusKiller!!
>>>-----------------------------------<<<

This is nothing that Virus_Help has anything to do with. But I'm sure that
you all know that by now.

This littel 'sucker' is on it's way to every wellknown anti-virus programmer
that will accept new virus from Virus Help Team Denmark.

     Regards....
      __
 __  ///       Jan Andersen          FidoNet:   2:235/112.0
 \\///       ---------------            AmyNet :  39:141/142.0
  \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.30 TP-5 Spaceballs Demo - CoP Trojan - 29.12.1995

```
 WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
      WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


Hi All !!!!!

There is a lot of trojans comming right now from 'The Party 5', but I'm
pretty sure that the files are from the 'COP' idiots.

The archive 'TP5-SPAC.LHA' with a size about 45000 bytes (ripped from all
BBS adds) the mainfile 'TP5_Spaceballs.exe' has a size of 38060 bytes.

The program is trying to lock on NComm:, just like tha old COP trojan's.

Here is the FILE_ID from the archive:

.-----------------------------------------.
|        DIRECTLY FROM THE PARTY 5         |
```

```
`-----------------------------------------'
.-----------------------------------------.
|                                         |
|       Spaceballs 40k intro called       |
|              'Ice Frontier'             |
|                                         |
`-----------------------------------------'
```

Please do not start the program. The archive is on it's way to every wellknown anti-virus programmer that will accept virus from us.

Thanx to 'Tauno Pinni' for bringing this to us......

Regards....

```
  __
__  ///       Jan Andersen         FidoNet:   2:235/112.0
 \\///       --------------           AmyNet :  39:141/142.0
  \XX/    VIRUS HELP TEAM DENMARK         VirNet :   9:451/247.0
```

1.31 TP-5 Andromeda Demo - CoP Trojan - 29.12.1996

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

Hi All !!!!!

There is a lot of trojans comming right now from 'The Party 5', but I'm pretty sure that the files are from the 'COP' idiots.

The archive 'TP5-ANDR.LHA' with a size about 47000 bytes (ripped from all BBS adds) the mainfile 'TP5_Andromeda.exe has a size of 40216 bytes.

The program is trying to lock on NComm:, just like tha old COP trojan's.

Here is the FILE_ID from the archive:

```
.-----------------------------------------.
|        DIRECTLY FROM THE PARTY 5        |
`-----------------------------------------'
.-----------------------------------------.
|                                         |
| Andromeda's 40k intro called 'feelings'. |
|                                         |
`-----------------------------------------'
```

Please do not start the program. The archive is on it's way to every wellknown anti-virus programmer that will accept virus from us.

Thanx to 'Tauno Pinni' for bringing this to us......

Regards....

```
 __  ///       Jan Andersen         FidoNet:   2:235/112.0
 \\///       --------------            AmyNet :  39:141/142.0
  \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.32 TP-5 Silents DK Demo - CoP Trojan - 29.12.1995

```
 WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
      WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


Hi All !!!!!

There is a lot of trojans comming right now from 'The Party 5', but I'm
pretty sure that the files are from the 'COP' idiots.

The archive 'TP5-TSL.LHA' with a size about 46000 bytes (ripped from
all BBS adds) the mainfile 'TP5_SilentsDK.exe' has a size of 39440 bytes.

The program is trying to lock on NComm:, just like tha old COP trojan's.

Here is the FILE_ID from the archive:

.-----------------------------------------.
|        DIRECTLY FROM THE PARTY 5        |
`-----------------------------------------'
.-----------------------------------------.
|                                         |
|      Silents DK's 40k intro called      |
|              'Byte Kitchen'             |
|                                         |
`-----------------------------------------'

Please do not start the program. The archive is on it's way to every
wellknown anti-virus programmer that will accept virus from us.

Thanx to 'Tauno Pinni' for bringing this to us.......


     Regards....
      __
 __  ///       Jan Andersen         FidoNet:   2:235/112.0
 \\///       --------------            AmyNet :  39:141/142.0
  \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.33 TP-5 Parallax Demo - CoP Trojan - 30.12.95

```
 WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
      WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


Hi All !!!!!
```

There is a lot of trojans comming right now from 'The Party 5', but I'm
pretty sure that the files are from the 'COP' idiots.

The archive 'TP5-PRLX.LHA' with a size about 41000 bytes (ripped from
all BBS adds) the mainfile 'TP5_Parallax.exe' has a size of 39980 bytes.

The program is trying to lock on NComm:, just like tha old COP trojan's.

Here is the FILE_ID from the archive:

```
.-----------------------------------------.
|        DIRECTLY FROM THE PARTY 5        |
`-----------------------------------------'
.-----------------------------------------.
|                                         |
|   Parallax's 40k intro called 'Cubic'.  |
|                                         |
`-----------------------------------------'
```

Please do not start the program. The archive is on it's way to every
wellknown anti-virus programmer that will accept virus from us.

```
     Regards....
      __
 __  ///       Jan Andersen         FidoNet:   2:235/112.0
 \\///       --------------            AmyNet :  39:141/142.0
  \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.34 TMTC90.LHA archive infected with virus - 30.12.1995

```
 WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
      WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
```

Hi All...

A new archive is now spread with an 'old' virus in it. The archive name is
'TMTC90.LHA'. The virus in the archive is 'Disaster Master 2', and it is in
the C: dir. in the cls command.

Every wellknown viruskiller can find this virus. Just make sure that you
don't use or install the 'cls' command on your HD.

The FILE_ID.DIZ look's like this:

```
____________________+ Ti/\/\eTr/\cE
\_______   _______/____________________
     |    _|__  +\_______   _______/
 +   |   |    \+ ______|     |
   + |___|     \/     /     |
         |_____/     /|_____|
     Released /_____/ Today
 Chicago 90  HD and AGA Fixed
 Done by >TORCH< Leader of TmT
```

```
That is all for now.... Happy new year everybody....

     Regards....
      __
 __  ///       Jan Andersen         FidoNet:   2:235/112.0
 \\///       --------------            AmyNet :  39:141/142.0
  \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.35 NC210.LHA/LZX infected with HappyNewYear Virus

```
 WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
      WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


   Hi All...

   A new archive is now spread with a virus in it.  The archive name is
   'NC210.LZX' or 'NC210.LHA'. The virus in the archive is the new link
   virus called 'Happy New Year 96'.


   At this time only 3 viruskillers can find this 'sucker'.

   VirusWorkshop v5.8... By Markus Schmall
   VT v2.79.............. By Heiner Schneegold
   VirusZ II v1.27...... By Georg Hoermann


 The FILE_ID.DIZ look's like this:

   Get file description from comprograms +
   Name: NC210.lha
   Path: Aminet/comm/misc
   Best: Aces High SW, 5 Ndz

That is all for now.... Happy new year everybody....

Thanx to 'ENZO' for saving this for us.......

     Regards....
      __
 __  ///       Jan Andersen         FidoNet:   2:235/112.0
 \\///       --------------            AmyNet :  39:141/142.0
  \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.36 DanceModPoolTro.exe Virus infected - 05.02.1996

```
 WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
      WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!

   Hi All...
```

```
   A new archive is now spread with a virus in it.  The archive name is
   'SIGN.LHA'.  The virus in  the archive is  the new link virus called
   'Happy New Year 96'.

   Archive Name.....: SIGN.LHA
   Size.............: 25261 bytes (Ripped for BBS adds).
   Infected file....: DancePoolModTro.exe (25484 Bytes Packed with STC)


   At this time only 3 viruskillers can find this 'sucker'.

   VirusWorkshop v5.9... By Markus Schmall
   VT v2.80............ By Heiner Schneegold
   VirusZ II v1.27...... By Georg Hoermann


 The FILE_ID.DIZ look's like this:

.-----------------------------------------.
|              f¡GHt AGA¡NSt              |
|                 FASC¡SM.                |
|                                         |
|           fR¡ENDSh¡P RUlEZ...           |
|               WORlDW¡DE !!              |
`-----------------------------------------'
              !!sIGn&sPREAd!!

That is all for now.... Happy new year everybody....

Thanx to 'Morten Johan Leerhoy' sending the archive to us...


     Regards....
      __
 __  ///       Jan Andersen         FidoNet:   2:235/112.0
 \\///       --------------            AmyNet :  39:141/142.0
  \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.37 No Sense Magazine - Ebola Infected

```
  WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
       WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!


 Hi All...

 A new archive is now spread with a virus in it. The archive name is
 'C!S-NS1.DMS'. The virus in the archive is the 'Ebola' Link virus.

 Archive Name.....: C!S-NS1.DMS
 Size.............: 546381 bytes (DMS Packed)
 Infected file....: No_Sence1 (60048 Bytes Packed with STC)


 At this time only 3 viruskillers can find this 'sucker'.
```

```
VirusWorkshop v5.9... By Markus Schmall
VT v2.80.............. By Heiner Schneegold
VirusZ II v1.27...... By Georg Hoermann


The FILE_ID.DIZ look's like this:
 ____________________________________________
          _   _    ,  __   _  ,  __
         | ) (_)   ) (_/_ | ) ) (_/_

          n   o    s   e   n  s  e
    m a g a z i n e  -  d i s k   p u b l.

       a   C - L O U S   diskmagazine

   The First Issue of No Sense Magazine -
 Disk Publication (Includes Swedish chart.)
 ____________________________________________


Well, that is all for now.....

Thanx to 'Kim B.' sending the archive to us...

IMPORTANT: Virus Help Team DK BBS, new phone number +45 4659 6867.

    Regards....
     __
__  ///       Jan Andersen         FidoNet:   2:235/112.0
\\///       --------------            AmyNet :  39:141/142.0
 \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.38 ZAP v1.1 Unpacker - Ebola Infected

```
 WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
      WARNING !!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!

Hi All...

A new archive is now spread with a virus in it. The archive name is
'TXC-Z11.LHA'. The virus in the archive is the 'Ebola' Link virus.

Archive Name.....: TXC-Z11.LHA
Size.............: 197233 bytes (LHA Packed)
Infected file....: UnARJ.... ( 9100 Bytes)
                   UnRAR.... (24176 Bytes)
                   Install.. ( 4132 Bytes)

At this time only 3 viruskillers can find this 'sucker'.

VirusWorkshop v5.9... By Markus Schmall
VT v2.80.............. By Heiner Schneegold
VirusZ II v1.28...... By Georg Hoermann
```

```
 The FILE_ID. look's like this:
   __ _______  __._____________
  \//  _).\ensuremath{\lnot}\( \ensuremath{\lnot}|  )__) .__)
.--/  /  ¦  \     \  | ¦ \ensuremath{\lnot}\----------------.
| /   \_____/  |__/__|____/TOXiC GIVES YA: |
|-\___/-----\ensuremath{\lnot}\_|---------------------------|
|             ZAP V1.1 *FREEWARE*           |
| EXTRACTS LHA/LZH/LZX/DMS/ARJ/ZIP/ZOO/RAR |
|   EASY GUI, PREFS EDITOR + SAVE PREFS     |
|    FILE/DIRECTORY/DEVICE REQUESTERS       |
|  ALL EXTRACTORS INCLUDED,STATUS DISPLAY   |
|  NEW MANUAL + NEW INSTALLER + NEW ICONS   |
|      PLAY MUSIC WHILE EXTRACTING          |
|    FASTER SOURCE CODE, FASTER PROGRAM     |
`----TOXiC'S-2:ND-RELEAS-DOWNLOAD-&-TRY----'


 Well, that is all for now.....

 Thanx to 'Torben Danoe' sending the archive to us...

 IMPORTANT: Virus Help Team DK BBS, new phone number +45 4659 6867.

     Regards....
      __
__  ///       Jan Andersen         FidoNet:   2:235/112.0
\\///       --------------            AmyNet :  39:141/142.0
 \XX/    VIRUS HELP TEAM DENMARK          VirNet :   9:451/247.0
```

1.39 Amiblank Trojan - (Markus Schmall)

```
 Warning ! Warning ! Warning ! Warning ! Warning ! Warning ! Warning !

      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 and Flemming Slabiak 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! HAHAHAaaaaaaaaaah',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


        Greets Markus Schmall (Programmer of VirusWorkshop)!!!!!

       (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
       IN ANY RELEASE OF THEM !)
```

1.40 TP-5 TRSi Demo - CoP Trojan - 28.12.1995)

```
  Warning ! Warning ! Warning ! Warning ! Warning ! Warning ! Warning !

Hi !

Warning ! The file "TP5-TRSI.lha" contains a COP trojan and it is NO
TRSI release. In the file_id it's said that this is a 40K intro from
TRSi. It's the same code as found in the pha-xmas.lha trojan.

The file didn't appear up to now (28.12. 19.00 o'clock) on german
systems. The file was on some boards in Denmark. I have informed in
a public letter the Aminet moderators, so that this thing will be
hopefully not uploaded to it.

The File_Id looked like this:

.-----------------------------------------.
|        DIRECTLY FROM THE PARTY 5        |
'-----------------------------------------'
.-----------------------------------------.
|                                         |
|   TRSI's 40k intro called 'Domination'  |
|                                         |
'-----------------------------------------'

Special thanks must go to Jan Andersen of Virus Help DK and Kim B.
for the support. Thanks !

Greets

         Markus Schmall.  (Programmer of VirusWorkshop)

       (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
       IN ANY RELEASE OF THEM !)
```

1.41 Phenomena DOS-Extender V1.1 - CoP Trojan - 24.12.1995)

```
Hi ! Back in the street...

Warning ! Warning ! Warning ! Warning ! Warning ! Warning ! Warning !

The archiv "PHA-XMAS.lha" contains a new trojan. The code looks like
the COP trojans, but this time no word from them. Via the access of
DosLists it will be tried to access the files and overwrite them with
a $1f byte long string, which look like this:

"+46-620-13141 - DUNGEON OF DOOM"

A swedish number, I suppose.

If the sys partition is protected, the following text will be up:

'Phenomena DOS-Extender V1.1 ',$A9,'1993 by Photon'
'Unable to write Swapfile. Remove write-protection and retry'
'Creating new Swapfile. Please hold...'

Of course Photon has nothing to do with it.

The FileID of this files looks like this:

.-----------------------------------------.
: Phenomena presents ' merry x-mas ! '     :
: Pha's very last production on the Amiga! :
:                                          :
: Code & Graphics : Photon, Color & Twins  :
: Music           : Tip & Mantronix        :
`-----------------------------------------'

But it`s only a little lame trojan.

The archive already popped up in Germany on 24.12., but the archive
was corrupted. 2 days later I found it as intact archive on the
D-o-E BBS, where I want to thank Mercury for his freedl, otherwise
I wouldn`t have been able to analyse this one.

Some people had real luck. E.g. Hitpoint downloaded the corrupted
archive and could so not start the shit (hi Dieter !)...

Ok, that is all for now, it`s morning time and I want to sleep...

Greets

      Markus Schmall (Programmer of VirusWorkshop)

     (IT`S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
     IN ANY RELEASE OF THEM !)
```

1.42 Susi_Drive_Stepper Trojan - (Markus Schmall)

```
Warning ! Warning ! Warning ! Warning ! Warning ! Warning ! Warning !
```

```
Hi ! I just recieved a new (old?) trojan, here the
analyse of it:

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'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
IN ANY RELEASE OF THEM !)


A special hello and thanks goes out to Jan Andersen for
his really great help all the time and all his work. He sended
me this trojan. Thanks Jan.


- Merry X-mas to all of you - Have a nice christmas celebration time -

Greets
        Markus Schmall (Programmer of VirusWorkshop)
```

1.43 VirusMemKill v1.2 Trojan - (Markus Schmall)

```
Warning ! Warning ! Warning ! Warning ! Warning ! Warning ! Warning !
```

```
vmk12.lha (a file which came from an eastern country), which
is said to be VMK 1.2 contains a new lame bootblockvirus.
The maincode is 3452 bytes long and contains the old vmk +
the installer for this little bb virus.

Next versions of VT, VZ and VW will surely recognize it.

signed
         Markus Schmall (Programmer of VirusWorkshop)

  (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
  IN ANY RELEASE OF THEM !)
```

1.44 Happy_New_Year_96' Link-Virus - (Markus Schmall)

```
Hi #?

A new little linkvirus appeared yesterday on the gobal stations. It's
called HNY96 (Happy_New_Year_96) and is 540 bytes long and infects
normal executable files. The infection is done via LoadSeg(). We
recieved this virus from the US, Holland, Switzerland and Germany. It
seems to be on the wild, so there will be an update of VT very soon
to kick the bastard. VW 5.7 is too new to stress the users with a
600 kb release again. Since the installer isn't known, I will release
a blockersystem in the coming days.

Greets

          Markus Schmall (Programmer of VirusWorkShop)


P.S.: Ebola linkvirus is found in dvd!-def.lha. Don't start it...

      (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
      IN ANY RELEASE OF THEM !)
```

1.45 ConMan 1995 link-virus - (Markus Schmall)

```
Warning ! M-hac.lha and Bloody.exe contain LINKVIRUSES ! BE CAREFULL !

Here a first BETA ANALYSE of it:

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.

Greets
```

```
          Markus Schmall (Programmer of VirusWorkShop)

  P.S.: This analyse is copyrighted and strictly forbidden to be used
        in any SHI production....
```

1.46 Strange Atmosphere Link-Virus (02.03.96) - Markus Schmall

```
                  Warning ! Warning ! Warning ! Warning ! Warning ! Warning ! ↩
                     Warning !


  The archiv 'srn-db33.lha' is a  possible  installer  of a new linkvirus
  called Strange Atmosphere.  We have here the first infected files.  The
  files become 1232 bytes longer and the linkvirus contains a destructive
  routine, which is able to format harddiscs. We will give you as soon as
  possible a viruskiller update, which can kill this little bastard !

  Thanks to RD10/ORS  for the testsamples  and to Maestro for his general
  great work !

  Greets

          Markus Schmall   (Programmer of VirusWorkshop)

       (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
       IN ANY RELEASE OF THEM !)


                 Analysis made by Markus Schmall
```

1.47 Analysis of Strange Atmosphere link-virus

```
 THIS IS A BETA ANALYSIS, WHICH BE CHANGE UNTIL THE FINAL RELEASE OF THE
 NEXT VIRUSWORKSHOP VERSION !

 KNOWN INSTALLERS OF THE LINKVIRUS ARE: SRN-DB33.LHA AND TCR-RESC.DMS !



Entry...............: Strange Atmosphere
Alias(es)...........: SA Virus (as called in VW)
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.

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.....: VW6.0ß (VT follows soon)
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 ==================
```

1.48 WireFace Trojan Type G - 09.08.1995 - (Test By Markus Schmall)

```
      A short beta analyse of the chkmount.lha trojan !

      THIS IS COPYRIGHTED MATERIAL ! NOT ALLOWED TO BE USED IN ANY SHI
      PRODUCTION !


      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 39 first sectors are going to be cleared:

’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)


Greets..

   Markus Schmall   (Programmer of VirusWorkshop)

(IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
IN ANY RELEASE OF THEM !)
```

1.49 Flake013.txt Warning FAKE!! - 18.07.1996 - Markus Schmall

```
                Warning !

It is said to be trojan in "BIO-WARN.LHA". This is spreaded under
the name of Virus Help Team Denmark and contains a file called flake013.txt
and flake_killer_bio.exe and advertisements from the ASYLUM bbs.

The text flake013 is a analyse/warning from me, which was spreaded under
the name of Virus Help Team DK some days ago. The executable file is not
known to me.

The upload user of the archiv is known (the handle) and we will force the
sysop of Asylum to close this account.

Greets
         Markus Schmall   (Programmer of VirusWorkshop)

      (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
      IN ANY RELEASE OF THEM !)


                Click here
                to read the reel Flake013.txt
```

1.50 MakeKey v1.10 For Virus_Checker - 08.07.1995) - Markus Schmall

```
Warning !

VcKey110.lha is a trojan ! DON~T START IT ! YOU HAVE BEEN WARNED !
Here is my BETA analyse of the file.

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.
~~~~~~

"

Greets
Markus Schmall (Programmer of VirusWorkshop)

(IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
IN ANY RELEASE OF THEM !)

1.51 HardDiskSpeeder v1.5 ©GVP Inc. 1995 - Markus Schmall

Warning ! The archive "gvp-hs15.lha" contains a new trojan !

Here is my first analyse:

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"'


   Greets

         Markus Schmall   (Programmer of VirusWorkshop)

      (IT`S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
      IN ANY RELEASE OF THEM !)
```

1.52 TRSi Installer Trojan - Markus Schmall

```
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).

Here is my first analysis of the virus, which is a little bit short, but
I ran totally out of time. Sorry dudes..
```

```
Biomechanic Trojan
------------------

other possible names: TRSI-INS Trojan
Type: Destruction only
Destruction caused by: simple bytemodification

This is NO TRSi release ! 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:

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 virus is looking for a special enviroment and then manipulates the
files:

Here a original PGP signed message:

0000: 89009502 05002FCF 1B5220F5 BA1075CB    ....../I.R o°.uE
0010: 69450101 C11D03FF 7ED659E1 39C4AD2C    iE..A...~ÖYß9Ä-,
0020: CED29280 21FCEB79 5CF3B9A0 AADB5C14    IO..!üëy\ó1 ªU\.
0030: D2B35295 5FFBE735 4E8070E1 A8C2C909    O3R._ûç5N.pß"AÉ.
0040: 2235ABB5 BE37E843 79CCD140 7AA2ACA5    "5«$\mathrm{\mu}$ 7èCyIÑ@z¢\ ↩
   ensuremath{\lnot}$\yen$ <-

Here the manipulated one:

0000: 89009502 05002FCF 1B5220F5 BA1075CB    ....../I.R o°.uE
0010: 69450101 C11D03FF 7ED659E1 39C4AD2C    iE..A...~ÖYß9Ä-,
0020: CED29280 21FCEB79 5CF3B9A0 AADB5C14    IO..!üëy\ó1 ªU\.
0030: D2B35295 5FFBE735 4E8070E1 A8C2C909    O3R._ûç5N.pß"AÉ.
0040: 2235ABB5 BE37E843 79CC0002 B37800A5    "5«$\mathrm{\mu}$ 7èCyI..3x.$\yen$  ↩
   <-

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 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).


Greets
         Markus Schmall   (Programmer of VirusWorkshop)

      (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
      IN ANY RELEASE OF THEM !)
```

1.53 VirusZ II v1.19 FAKE - Markus Schmall)

```
Warning !

A faked VirusZ_II 1.19 is going around. The filename is 'vzii-119.lha'
and contains some parts of the actual vzii-118.lha release from Georg
Hoermann. The mainprogramm seems to be an older version of VirusZ with
a filelength of 64664 bytes. I found no trojan in it. Please just
delete the file. I called Georg and he told me, that he not released
VirusZ_II 1.19 !

File ID of the fake:

       _________     _
  ____/""".//##/____)\_____________
 /"""/   //________   /"""/"".//___/_HELP!
/   /   //"""/"  / //   /  //____   \_
\       //   /  ____/   /  //"""""/X@!/
 \_____/\__/___/ ""\_____/_________/
--><><><><><><></____/-><>- Presents-<><--
      VirusZ II v1.19 - (09.06.95)
>>>-----------------------------------<<<

Probably just again somebody, who wants to destroy the good reputation
of Virus Help and Georg Hoermann.


Greets
         Markus Schmall   (Programmer of VirusWorkshop)

      (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
      IN ANY RELEASE OF THEM !)
```

1.54 FileGhost 3 linkvirus - (06.1995) - Markus Schmall

```
 WARNING !

 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. So the relochunks
will stay unchanged.

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 virus is, in my opinion, not from the author of the last Fileghost
viruses. This one has display routines and will be recognized by the
infected user in this way very fast. The last versions of Fileghost just
worked around in the background.


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 !’
```

```
 Greets
         Markus Schmall   (Programmer of VirusWorkshop)

       (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
       IN ANY RELEASE OF THEM !)
```

1.55 LZX v1.30 Trojan - 09.06.1995 - Test By Markus Schmall

```
Warning !

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.


Greets
         Markus Schmall   (Programmer of VirusWorkshop)

       (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
       IN ANY RELEASE OF THEM !)
```

1.56 ConMan Trojan - Test By Markus Schmall

```
Warning to all :
----------------

Packing type: Turbo Squeezer

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

packed:   12692 Bytes
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 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.

Due to no viruskiller for this bastard it is best for the infected
users to do the following: Boot from the orginal WB disks and
simply copy a new IPREFS to your HD and it should work again !

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.

Sorry for this short analysis, I just got the thing packed in a
warning from RD10/Osiris (NEVER SPREAD THE VIRUS IN A WARNING MAN !
IF YOU WANT TO DO SOMETHING GOOD, THEN DON'T SPREAD IT IN THIS
WAY !) and wanted to give you some information than RD10. It is
weekend for me now, too and I want to go to a party, so wait for
the first viruskillers to recognize this bastard.


Greets

    Markus Schmall   (Programmer of VirusWorkshop)

    Special hellos to IXXy and Simone....

 (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
 IN ANY RELEASE OF THEM !)
```

1.57 Achtung.exe Trojan - 11.02.1995 - Test by Markus Schmall

```
 VirusWarning ! VirusWarning ! VirusWarning ! VirusWarning !
```

The archiv Gath95-!.lha contains a trojan ! DELETE IT !

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! }---+
```

Greets
Markus Schmall (Programmer of VirusWorkshop)

(IT‘S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM IN ANY RELEASE OF THEM !)

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

1.58 27.02.1995 - Test by Markus Schmall

```
Warning !

Caution ! The file "dpl-dc99.lha" contains a trojan, which can format
your SYS: device. If you have started this one, then check your loadwb
command. If it is 2088 Bytes long, replace it ! It is a new written
command from the virus !!!

Greets
         Markus Schmall   (Programmer of VirusWorkshop)

      (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
      IN ANY RELEASE OF THEM !)
```

1.59 DMS v2.06 Trojan - 11.02.1995 - Test by Markus Schmall

```
Warning !

The file cry_206.lha is a trojan ! It contains the DMS 2.06 fake
trojan like the DMS206.lha archiv in the last week !!!! It's a FastCall
hacker ! Don't start it !

Greets
         Markus Schmall   (Programmer of VirusWorkshop)

      (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
      IN ANY RELEASE OF THEM !)
```

1.60 Istrip v2.1 Trojan - 17.02.1995 - Test By Markus Schmall

```
 Warning !!

 Caution ! The file "Istrip21.lha" is a trojan and contains a BBS hacker !
 Be careful and delete this file !

 Greets
         Markus Schmall   (Programmer of VirusWorkshop)

      (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
      IN ANY RELEASE OF THEM !)
```

1.61 Pestilence Bootblockvirus 1.15 - 09.12.1994- Markus Schmall

```
   Warning !

   (This analyse was made in a hurry and is still beta!!!)
```

```
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.

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 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!'


Greets

       Markus Schmall   (Programmer of VirusWorkshop)

    (IT'S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM
    IN ANY RELEASE OF THEM !)
```

1.62 Removcmd.lha Trojan - 26.10.1995 - Markus Schmall

```
Warning !

Warning ! The archive "removcmd.lha" contains an installer for
the Commander Linkvirus ! This installer appeared around the
```

globe around 24.10.1994. and is descriped as follows:

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!  Have you got probs. with the COMMANDER !
!! virus by Brian Blister? It's a link-vir !
!! that eats your mem like hell.. brand new!
!! and not killable with VirZ or VirKiller !
!! or any other killer.. Except this one   !
!! brought to you by Coma/FD and Bigmama/FD!
!! Download and be happy!!!!!!!!!!!!!!!!!!!
```

Don‘t start this file ! It‘s a installer for the fucking Commander Linkvirus, which can be removed 100% from VT 2.68 and VW4.3.

The archive contains the file "kill" with the filelength 2252 bytes ! This is the installer !

The virus first appeared in scandinavia and it‘s spreading was nearly stopped by some motivated members of SHI (special hi in this case to Jan Andersen and Bo Krohn). Now the Commander virus is spreaden worldwide......

Greets

Markus Schmall (Programmer of VirusWorkshop)

(IT‘S HEREBY PROHIBIT, THAT SHI USES THIS ANALYSE IN ANY FORM IN ANY RELEASE OF THEM !)