VListC

Torben Bilbo" Maciorowski"

COLLABORATORS

	TITLE : VListC	

ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY	Torben Bilbo" Maciorowski"	October 17, 2022	

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VListC

1.1 VIRUSES - C

```
                This is a part of the  "Amiga Virus Bible"
and is ment to be used with  - and started from -
                          AVB.Guide
```

Cameleon

CCCP Virus

Centurion

Centurion II

Challenger Trojan

Chaos

Chaos-Master 0.5

Check Filevirus

Claas Abraham (MCA)

Clist

Color Virus Carrier

Commodore Virus

Compuphagozyte 1

Compuphagozyte 2

Compuphagozyte 3

Compuphagozyte 4

Compuphagozyte 8

```
Crackright

Crime '92

Curse of Little Sven, The
```

1.2 cameleon

```
Name            : Cameleon

Aliases         : Little Sven

Type/Size       : -

Incidence       : -

Discovered      : -

Way to infect   : -

Rating          : -

Kickstarts      : -

Damage          : -


Manifestiation  : -

Removal         : -

General comments: See Little Sven
```

1.3 cccp.txt

```
========= Computer Virus Catalog 1.2: CCCP VIRUS (31-July-1993) ========
Entry..............: CCCP Virus
Alias(es)..........: ---
Virus Strain.......: ---
Virus detected when.: ---
              where.: ---
Classification.....: Bootblock and Link Virus: Overwriting Bootblock,
                        Extending Files, Resident
Length of Virus....: 1.Length: 1024 bytes Bootblock,
                               1044 bytes File extension.
                     2.Length: 1192 bytes in Chip-RAM
---------------------- Preconditions -----------------------------------
Operating System(s).: AMIGA-DOS
Version/Release....: >= Version 1.3
Computer model(s)...: All Amigas with $68000 CPU / Vectortable at $0
---------------------- Attributes --------------------------------------
```

```
Easy Identification.: Text "CCCP VIRUS" in infected bootblocks and files
Type of infection...: Self-Identification methods:
                         Disk/File: searches for special Hunklength ($FD)
                                    in first Codehunk
                         Disk/Boot: none
                         Ram: Searches for $611c(bsr.s) at VEC3 location
                         Executable File infection: extending file
                            by 1044 bytes; infection occurs if:
                              - file is readable/writable
                              - file header block contains all blocks
                                of the file (no extension block)
                              - won't infect files in directorys with
                                1st letter "l","d","f" (eg.:l,devs,fonts)
                         System infection: RAM-Resident, Reset-Resident,
                              Bootblock infection
                         Libraries/Vectors patched and action:
                              Coolcap    (Exec)  - be resetproof
                              DoIo       (Exec)  - infect preconditions,
                                                   boot infection
                              NewOpenLib (Exec)  - patch openwindow
                              Openwindow (Int.)  - start infection
Infection Trigger...: File:   Opening a Intuition Window
                      Bootblock:Any Disk-Access (DoIo on Block 0)
Storage media affected: Diskettes
Interrupts hooked...: IRQ_VEC3 ($6c) to stay in memory (against actions
                         of some antivirus-programs
Damage..............: Permanent Damage: overwriting bootblock,
                      Transient Damage: none
                      Transient/Permanent damage: virus overwrites with-
                         out allocating memory at $$6fbec-$71000, so
                         programs stored at this location my crash. Virus
                         also may have problems with some hunk-types.
Damage Trigger......: Inserting Diskette / DoIo call
Particularities.....: Very compact code (1024 Byte) with complete
                      (recursive) file and bootblock infection routine
Similarities........: ---
--------------------- Agents -----------------------------------------
Countermeasures.....: VT2.54, SnoopDos 1.7, AVM(internal)
Countermeasures successful: VT2.54,Snoopdos,AVM
Standard means......: VT2.54
--------------------- Acknowledgement --------------------------------
Location............: Virus Test Center, University Hamburg, FRG
Classification by...: Soenke Freitag
Documentation by....: Soenke Freitag
Date................: 31-July-1993
Information Source..: Heiner Schneegold, SHI, reverse analysis
====================== End of CCCP Virus==================================
```

1.4 centurion

```
        Name            : Centurion

        Aliases         : The Smily Cancer

        Type/Size       : -
```

```
        Incidence       : -

        Discovered      : -

        Way to infect   : -

        Rating          : -

        Kickstarts      : -

        Damage          : -

        Manifestiation  : -

        Removal         : -

        General comments: See The Smily Cancer
```

1.5 centurion-ii

```
     Name         : Centurion II

     Aliases      : SMILY CANCER II

     Type/Size    : File/4676

     Discovered   : 01-04-91

     Incidence    : Very rare, since no spreading

     Way to infect: Infects first file of startup-sequence

     Rating       : Dangerous

     Kickstarts   : ?

     Damage       : Adds 3916 Bytes to infected files
                    writes at the file end:
                    CENTURIONS STRIKES BACK: THE SMILY CANCER II

     Manifestation: None

     Removal      : Delete infected files
                    (Most Virus Killers will do this)

  General comments: Always remember to write protect your disk !

JN 07.09.93
```

1.6 challengertrojan

```
Name            : Challenger Trojan

Aliases         : -

Type/Size       : Trojan Horse/126336 bytes

Incidence       : -

Discovered      : -

Way to infect   : Copies the Setclock command to DEVS:keymaps/a, and
                  creates a new file called c/setclock. It then
                  creates a file called DEVS:keymaps/rca

Rating          : Pretty harmless

Kickstarts      : -

Damage          : Locks up your system on the 24th of July

Manifestiation  : See message below

Removal         : Delete the file, c/setclock, and copy the file
                  DEVS:keymaps/a to c, and rename it to setclock.
                  Then delete the file called rca in DEVS:keymaps,
                  and also delete the file called guy in the same
                  directory

General comments: Message shown on the 24th of July:
       "Guten Tag, hier is der Guru Ihres
       Amiga-Computers. Laut Arbeitsvertrag
       habe ich das recht auf einen Medita-
       tionstag pro Jahr. In meinen Fall ist
       das der 24. Juli jeden Jahres. Da wir
       heute dieses Datum schreiben, stehe ich
       Ihnen erst morgen wieder zur Verfuegung.
       Bitte haben sie verstaendnis dafuer, denn
       auch wir Gurus muessen einmal ausruhen".
```

1.7 chaos

```
Name            : Chaos (Lameblame)

Aliases         : -

Type/Size       : BootBlock virus

Incidence       : -

Discovered      : -

Way to infect   : Via BB

Rating          : Dangerous
```

```
Kickstarts      : -

Damage          : As soon as a counter reaches 8, the disk is
                  filled with garbage = UNUSEABLE!

Manifestiation  : DisplayAlert (red flashing box) :"Chaos! by
                  Tai-Pan!" etc.

Removal         : Use a good viruskiller.

General comments: -
```

1.8 chaos-master

```
Name            : Chaos-Master

Aliases         : -

Type/Size       : Filevirus/16676 bytes

Incidence       : -

Discovered      : -

Way to infect   : Via the c/dir command, you ask for: dir df3: and
                  the dir command in df3:c is overwritten by the
                  virus. You ask for: dir prefs, and a file
                  (disk.info, length: 370 bytes) is written after
                  prefs, you click on prefs, and sorry, because of
                  the fault in disk.info, the computer hangs, and
                  you have to reset.

Rating          : Dangerous

Kickstarts      : -

Damage          : Overwrites the c/dir command, see above

Manifestiation  : See above

Removal         : Delete the file, c/dir, and copy a new one from
                  org. WB

General comments: -
```

1.9 check-filevirus

```
Name         : Check Filevirus

Aliases      : --
```

```
     Type/Size    : Trojan/18644

     Incidence    : ?

     Discovered   : 02-10-91

     Way to infect: None, "just" damaging!

     Rating       : Very dangerous, in case you have a harddisk that
                    uses the harddisk.device

     Kickstarts   : ?

     Damage       : Destroys something on harddisk

     Manifestation: Something with pictures (a skull) and sound

     Removal      : Delete it.

  General comments: SHI do not have any info on this virus !
                    if you have the virus or info about it
                    please send it to you regional SHI center.


JN 07.09.93
```

1.10 claas-abraham.txt

```
==== Computer Virus Catalog 1.2: CLAAS ABRAHAM Virus (5-June-1990) ====
Entry...............: CLAAS ABRAHAM Virus
Alias(es)...........: --
Virus Strain........: --
Virus detected when.: November 1989
              where.: Elmshorn, FRG
Classification......: system virus (bootblock), resident
Length of Virus.....: 1. length on storage medium: 1024 byte
                      2. length in RAM           : 1024 byte
---------------------- Preconditions -----------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: 1.2/33.180
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
---------------------- Attributes --------------------------------------
Easy Identification.: typical text: in bootblock: --
                         in memory: '>>> Claas Abraham Virus !!! <<<'
Type of infection...: self-identification method: ---
                      system infection: RAM resident, reset resident,
                         bootblock
Infection Trigger...: reset (CONTROL + Left-AMIGA + RIGHT-AMIGA)
                      operation: any access on bootblock sectors
Storage media affected: only floppy disks (3.5" and 5.25")
Interrupts hooked...: interrupt vector 3 (IV 3)
Damage..............: permanent damage: overwriting bootable standard
                         bootblocks; formatting disks from sector 880;
                         changes reset entry (adress: $00FC00D2),
                         reason is unknown yet
```

```
                       transient damage: ---
Damage Trigger......: permanent damage: reset
                          operation: at any access on bootblock sectors
                          (blocks 0 and 1), formatting disks from sector
                          880 after 16th infection
                       transient damage: ---
Particularities.....: a resident program using the CoolCapture and/or
                          the ColdCapture vector is shut down
                       resident programs using the system resident list
                          (KickTagPointer,KickMemPointer) are shut down;
                          virus creates a resident list called
                          '>>> Claas Abraham Virus !!! <<<'
Similarities........: ---
---------------------- Agents ----------------------------------------
Countermeasures.....: Names of tested products of Category 1-6:
                       Category 1: .2 Monitoring System Vectors:
                                      'CHECKVECTORS 2.2'
                                   .3 Monitoring System Areas:
                                      'CHECKVECTORS 2.2','GUARDIAN 1.2',
                                      'VIRUSX 4.0'
                       Category 2: Alteration Detection: ---
                       Category 3: Eradication: 'CHECKVECTORS 2.2',
                                      'VIRUSX 4.0'
                       Category 4: Vaccine: ---
                       Category 5: Hardware Methods: ---
                       Category 6: Cryptographic Methods: ---
Countermeasures successful: without restrictions:
                             'CHECKVECTORS 2.2', 'VIRUSX 4.0'
                            with restrictions: 'GUARDIAN 1.2'
Standard means......: 'CHECKVECTORS 2.2'
---------------------- Acknowledgement -------------------------------
Location............: Virus Test Center, University Hamburg, FRG
Classification by...: Wolfram Schmidt
Documentation by....: Alfred Manthey Rojas
Date................: 5-June-1990
Information Source..: ---
====================== End of CLAAS ABRAHAM Virus ======================
```

1.11 clist.txt

```
======= Computer Virus Catalog 1.2: CLIST Virus (15-July-1991) =======
Entry...............: CLIST Virus
Alias(es)...........: ---
Virus Strain........: LAMER EXTERMINATOR Strain
Virus detected when.: January 1991
              where.: Australia
Classification......: System virus (bootblock), resident, encrypting
Length of Virus.....: 1. Length on storage medium: 1024 byte
                       2. Length in RAM           : 1024 byte
---------------------- Preconditions ---------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: 1.2/33.180
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
---------------------- Attributes ------------------------------------
Easy Identification.: Typical text: bootblock: ---
```

```
                                    in memory:'clist.library
                                            clist 33.80 (8 Oct 1986)'
Self-identification.: Kicktag pointer points to virus data
Type of infection...: System infection: RAM resident, reset resident,
                                         bootblock
Infection Trigger...: reset (CONTROL+Left-AMIGA+Right-AMIGA),
                      any disk access
Storage media affected: floppy disks  3.5" and 5.25")
Interrupts hooked...: ---
Damage..............: Permanent damage: overwriting bootblock;
                         simulation of standard bootblocks when
                         examined with any tool; removes expansion
                         RAM this reducing available memory; virus
                         allocates 1024 bytes in memory and
                         1096 bytes overall.
                      Transient damage: ---
Damage Trigger......: Permanent damage: reset; any disk access
                      Transient damage: --
Particularities....: uses StartIOVector; other resident programs using
                       system resident list (KickTagPointer,
                       KickMemPointer) are shutdown; virus encodes
                       itself at every new infection (bytes 54-864).
Similarities........: LAMER EXTERMINATOR virus strain
--------------------- Agents ----------------------------------------
Countermeasures.....: Names of tested products of Category 1-6:
                      Category 1: .2 Monitoring System Vectors:
                                     CHECKVECTORS 2.2
                                  .3 Monitoring System Areas:
                                     CHECKVECTORS 2.2, GUARDIAN 1.2,
                                     VIRUSX 4.0
                      Category 2: Alteration Detection: ---
                      Category 3: Eradication: CHECKVECTORS 2.2,
                                               VIRUSX 4.0
                      Category 4: Vaccine: ---
                      Category 5: Hardware Methods: ---
                      Category 6: Cryptographic Methods: ---
Countermeasures successful: without restrictions: CHECKVECTORS 2.2,
                                                  VIRUSX 4.0
                            with restrictions:    GUARDIAN 1.2
Standard means......: CHECKVECTORS 2.2
--------------------- Acknowledgement -------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Wolfram Schmidt
Documentation by....: Wolfram Schmidt
Date................: 15-July-1991
Information Source..: ---
===================== End of CLIST-Virus ============================
```

1.12 color-virus-carrier

```
     Name         : Color Virus Carrier

     Aliases      : Turk Installer

     Type/Size    : Trojan/2196
```

```
     Incidence    : Very rare

     Discovered   : ?

     Way to infect: Doesn't infect, but installs the Turk virus

     Rating       : Dangerous

     Kickstarts   : ?

     Damage       : The overwriting of the bootblock
                    (The Turk Virus Destroys 880 blocks on a disk)

     Manifestation: Pretends to be some demo

     Removal      : ?

  General comments: SHI do not have any info on this virus !
                    if you have the virus or info about it
                    please send it to you regional SHI center.

JN 07.09.93
```

1.13 commodore-virus

```
     Name         : Commodore Virus

     Aliases      : --

     Type/Size    : Trojan/1752

     Incidence    : Rare

     Discovered   : 26-09-92

     Way to infect: None, a destructive program

     Rating       : Dangerous

     Kickstarts   : ?

     Damage       : Removes or changes the startup-sequence
                    creates a directory called "Commodore war hier!"

     Manifestation: DisplayAllert: Ihr Comput er ist Uberhitzt !!!.
                    Wenn es nach dem Reset ein absturz gibt ...?S
                    SCHALTEN IHN SIE BITTE AU S...xU   Commodore 1987.

                    Text display:..con:10/10/330/50/REQUEST ..1m33m
                                 KEIN VIRUS IN DRIVE DF0: GEFUNDEN !

                    Text in file:
                                 !.This is the new Commodore-Virus !
```

```
                                .BY STARLIGHT ENTERPRISES 1992

     Removal      : Remove the "virus" and to control the startup-sequence
                    you might find a program-name placed here
                    if you do, remove it by using ED or like.

  General comments: SHI NEEDS more info on this virus !
                    if you have the virus or info about it
                    please send it to you regional SHI center.


JN 07.09.93
```

1.14 compuphagozyte1.txt

```
=== Computer Virus Catalog 1.2: COMPUPHAGOZYTE 1 Virus (31-July-1993) ==
Entry..............: CompuPhagozyte 1 Virus
Alias(es)..........: ---
Virus Strain.......: CompuPhagozyte Virus strain
Virus detected when.: ---
              where.: ---
Classification.....: Link Virus (directory type), non-resident
Length of Virus.....: 1.Length on storage medium: 1452 byte
                      2.Length in RAM:            1452 byte
--------------------- Preconditions -----------------------------------
Operating System(s).: AMIGA-OS
Version/Release.....: 1.2/all, 1.3/all, 2.0/all, 3.0/all
Computer model(s)...: All AMIGA models
--------------------- Attributes --------------------------------------
Easy Identification.: The following text appears in infected files:
                  "The CompuPhagozyte has attached to your system !
                   Wait for much more better virus on other systems, too!
                   The CompuPhagozyte in 9.91 by The Emperor Of Trillion
                   Bytes ! Virus-Checker V4.0 by Michael Ortmanns"
Type of infection...: System infection: overwriting the file
                         ":c/virus-checker" if this exists.
Infection Trigger...: Inserting a disk-like medium while virus program
                         is active.
Storage media affected: All disk-like media
Interrupts hooked...:    None
Damage.............: 1) Writing file ":c/virus-checker" on disk.
                      2) Potentially destroying floppy disk structure
                         (see Particularities).
Damage Trigger......: Upon inserting a disk-like medium.
Particularities.....: 1) Virus pretends to be "virus-checker 4.0".
                         Virus' infectivity is small as it always tries
                         to write to current directory.
                      2) If for some reason file ":c/virus-checker"
                         could not be written to disk, some obscure
                         hardware banging routine is called which seems
                         to destroy disk structure (of floppy disk only).
                      3) If real ":c/Virus-checker" exists, it is
                         corrupted and shortened to 1452 byte (poten-
                         tially due to an error of AmigaDOS-Write
                         routine; cause not fully verified)
```

```
Similarities........: CompuPhagozyte Virus family
--------------------- Agents ----------------------------------------
Countermeasures.....: VT 2.54, VirusZ 3.06, VirusChecker 6.28
Countermeasures successful: VT 2.54
Standard means......: VT 2.54
--------------------- Acknowledgement --------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Karim Senoucci
Documentation by....: Karim Senoucci
Date................: 31-July-1993
Information Source..: Virus disassembly / SHI / Heiner Schneegold
================== End of COMPUPHAGOZYTE 1 Virus ======================
```

1.15 compuphagozyte2

```
Name            : COMPUPHagozyte 2

Aliases         : -

Type/Size       : Filevirus/Trojan, 1148 bytes

Incidence       : -

Discovered      : -

Way to infect   : Camouflages itself as VirusX V5.00

Rating          : Dangerous, it deletes VirusX V5.00

Kickstarts      : -

Damage          : Copies itself to a file in C/, called
                  VirusX V5.00. NOTE: If the file doesn't exist,
                  nothing happens

Manifestiation  : Shows a requester with the text: "VirusX
                  V5.00 by Steve Tibbett". You get the pint,
                  when you click at the requester and nothing
                  happens!

Removal         : Use a good virus-killer.

General comments: Note: NO spreading
```

1.16 compuphagozyte3

```
Name            : COMPUPHagozyte 3

Aliases         : -

Type/Size       : Filevirus/Trojan, 568/592 bytes
```

Incidence : -

Discovered : -

Way to infect : Camouflages itself as the "cls" (Clear screen) command

Rating : Pretty harmless

Kickstarts : -

Damage : Clears the screen using 30 return codes (WOW!)

Manifestiation : See above

Removal : Use a good virus-killer.

General comments: Note: NO spreading. Note: At Kickstart 2.04, it causes a GURU with reset! Note: Doesn't stay resident with 1MB

1.17 compuphagozyte4

Name : COMPUPHagozyte 4

Aliases : -

Type/Size : Filevirus/Trojan, 916/952 bytes

Incidence : -

Discovered : -

Way to infect : Writes an invisible file to root-directory

Rating : Pretty harmless

Kickstarts : ONLY KS 1.2

Damage : Only DF0:

Manifestiation : See below

Removal : Use a good virus-killer.

General comments: Note: NO spreading. Note: At Kickstart 2.04, it causes the computer to reset in some time, when reset. It overwrites the four first bytes of startup-sequence, and if any program with a name longer than 4 bytes were present, an error code is generated due to some strange signs.

1.18 compuphagozyte8

```
     Name          : Compuphagozyte 8

     Aliases       : -

     Type/Size     : File/1952

     Clones        : -

     Symptoms      : -

     Discovered    : ?

     Way to infect: File infection

     Rating        : Harmless

     Kickstarts    : 1.2/1.3/2.0

     Damage        : Because of a prgramm-error the startup-sequence
                     can be defective.

     Manifestation: In the file you can read: ":AmigaDOS Datafile... etc."

     Removal       : Delete file ($A0A0A0A0) and modify startup-sequence

     Comments      : It patches the Kickchecksum, DoIo, Lock(dos), Open(dos),
                     and the LoadSeg(dos)-Vector. And $6c !!!
                     It uses the coolcapture to be resident. Always at
                     the same adress in memory. ($7C000)
                     If one of the patched vectors are used, the virus
                     creates the virusfile in the root-dir and modify
                     the startup-sequence with the virusname.($A0A0A0A0)

A.D 12-93
```

1.19 crackright

```
======= Computer Virus Catalog 1.2: CRIME'92 Virus (31-July-1993) ======
Entry..............: Crime'92 Virus
Alias(es)..........: Crime'92 A,B,C,D Virus (different generations of
                                              same polymorphic virus)
Virus Strain.......: ---
Virus detected when.: ---
               where.: ---
Classification.....: Memory resident Link Virus (Extending),Polymorphic
Length of Virus.....: 1.Length: 1800 Byte on storage medium
                      2.Length: 4028 Byte in RAM
---------------------- Preconditions -----------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: 1.2/1.3/2.04/3.0
Computer model(s)...: ALL AMIGAs
---------------------- Attributes --------------------------------------
Easy Identification.: String "Crime'92" is readable in RAM
Type of infection...: Self-Identification methods:
```

```
                          Memory: Checks for String "Crime'92"
                             at $204(Coolcapture). Reset resident.
                          Disk: Not really a Self-Identification, but
                              virus won't infect Files with instruction
                              movem d0-d7/a0-a6,-(SP) = $48e7
                              at specified location.
                          Executable File infection: extending files
                              by 1800 bytes at load time.
                          Preconditions: infection occurs if:
                              1) Disk is validated ("R"),
                              2) 8 blocks free on Disk,
                              3) File length < 102400($19000) Bytes,
                              4) File can be read into memory,
                              5) First Hunk is HUNK_HEADER,
                              6) HUNK_CODE found,
                              7) MOVEM-opcode ($48e7) is not found,
                              8) RTS-opcode found in hunk.
                           System infection: RAM- and Reset-Resident.
                              Virus can infect system libraries and almost
                              any file containing executable code matching
                              infection-preconditions, even printer
                              drivers.
                           Vectors hooked up to Kick1.3 (incl.):
                              ColdCapture (exec.library)
                              CoolCapture (exec.library)
                              Wait        (exec.library)
                              $2e         (dos.library) - Rom-Ptr,private
                           Vectors hooked from Kick2.0 above:
                              CoolCapture (exec.library)
                              Wait        (exec.library)
                              LoadSeg     (dos.library)
                              NewLoadSeg  (dos.library)
Infection Trigger...: Running any program from CLI and random condition
Storage media affected: All disk-like devices
Interrupts hooked...: ---
Damage..............: Permanent Damage: Overwriting random sectors
                      Transient Damage: None
                      Transient/Permanent damage: Due to some bugs,
                         virus may produce divide by zero errors on
                         startup of an infected program. During reset,
                         virus overwrites a random memory longword with
                         zero which may cause dead-end resets.
Damage Trigger......: Random and counter combination.
Particularities.....: Due to self-modifying (polymorphic) code, virus
                         won't run with processor chaches.
Polymorphism........: Virus is polymorphic in its encryption routine
                         which makes its detection with simple search-
                         strings impossible; presently, no antivirus
                         detects Crime'92 reliably! Virus may only be
                         detected reliably with algorithmic methods.
                      Several reported "variants" of Crime'92 (A-D) are
                         just different polymorphic generations.
Similarities........: ---
--------------------- Agents ----------------------------------------
Countermeasures.....: VT2.55
Countermeasures successful: No Virus-Checker detects all generations
                            of this Virus (status: July 1993). Update:
```

```
                          VT2.55 detects most(all?) variants (we sent
                          all generated variants to the author)
Standard means......: Boot from clean diskette and overwrite all sus-
                         picious executables with original clean ones.
--------------------- Acknowledgement ---------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Soenke Freitag
Documentation by....: Soenke Freitag
Date................: 31-July-1993
Information Source..: H.Schneegold, SHI, Reverse-analysis of virus code
===================== End of Crime'92 Virus ============================
```

1.20 crime-'92.txt

```
======= Computer Virus Catalog 1.2: CRIME'92 Virus (31-July-1993) ======
Entry...............: Crime'92 Virus
Alias(es)...........: Crime'92 A,B,C,D Virus (different generations of
                                              same polymorphic virus)
Virus Strain........: ---
Virus detected when.: ---
               where.: ---
Classification......: Memory resident Link Virus (Extending),Polymorphic
Length of Virus.....: 1.Length: 1800 Byte on storage medium
                      2.Length: 4028 Byte in RAM
--------------------- Preconditions -----------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: 1.2/1.3/2.04/3.0
Computer model(s)...: ALL AMIGAs
--------------------- Attributes --------------------------------------
Easy Identification.: String "Crime'92" is readable in RAM
Type of infection...: Self-Identification methods:
                         Memory: Checks for String "Crime'92"
                            at $204(Coolcapture). Reset resident.
                         Disk: Not really a Self-Identification, but
                             virus won't infect Files with instruction
                             movem d0-d7/a0-a6,-(SP) = $48e7
                             at specified location.
                         Executable File infection: extending files
                             by 1800 bytes at load time.
                         Preconditions: infection occurs if:
                             1) Disk is validated ("R"),
                             2) 8 blocks free on Disk,
                             3) File length < 102400($19000) Bytes,
                             4) File can be read into memory,
                             5) First Hunk is HUNK_HEADER,
                             6) HUNK_CODE found,
                             7) MOVEM-opcode ($48e7) is not found,
                             8) RTS-opcode found in hunk.
                          System infection: RAM- and Reset-Resident.
                             Virus can infect system libraries and almost
                             any file containing executable code matching
                             infection-preconditions, even printer
                             drivers.
                          Vectors hooked up to Kick1.3 (incl.):
                             ColdCapture (exec.library)
```

```
                              CoolCapture (exec.library)
                              Wait        (exec.library)
                              $2e         (dos.library) - Rom-Ptr,private
                           Vectors hooked from Kick2.0 above:
                              CoolCapture (exec.library)
                              Wait        (exec.library)
                              LoadSeg     (dos.library)
                              NewLoadSeg  (dos.library)
Infection Trigger...: Running any program from CLI and random condition
Storage media affected: All disk-like devices
Interrupts hooked...: ---
Damage..............: Permanent Damage: Overwriting random sectors
                      Transient Damage: None
                      Transient/Permanent damage: Due to some bugs,
                         virus may produce divide by zero errors on
                         startup of an infected program. During reset,
                         virus overwrites a random memory longword with
                         zero which may cause dead-end resets.
Damage Trigger......: Random and counter combination.
Particularities.....: Due to self-modifying (polymorphic) code, virus
                         won't run with processor chaches.
Polymorphism........: Virus is polymorphic in its encryption routine
                         which makes its detection with simple search-
                         strings impossible; presently, no antivirus
                         detects Crime'92 reliably! Virus may only be
                         detected reliably with algorithmic methods.
                      Several reported "variants" of Crime'92 (A-D) are
                         just different polymorphic generations.
Similarities........: ---
---------------------- Agents -----------------------------------------
Countermeasures.....: VT2.55
Countermeasures successful: No Virus-Checker detects all generations
                            of this Virus (status: July 1993). Update:
                            VT2.55 detects most(all?) variants (we sent
                            all generated variants to the author)
Standard means......: Boot from clean diskette and overwrite all sus-
                         picious executables with original clean ones.
---------------------- Acknowledgement --------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Soenke Freitag
Documentation by....: Soenke Freitag
Date................: 31-July-1993
Information Source..: H.Schneegold, SHI, Reverse-analysis of virus code
====================== End of Crime'92 Virus ============================
```

1.21 curse-sven.txt

```
     Name         : Curse of Little Sven, The

     Aliases      : - (Cameleon)

     Type/Size    : Bootblock

     Incidence    : ?
```

```
     Discovered   : ?

     Way to infect: Become active if you start the trojan XCopyPro V6.5
                    this version is false! and is found at BBS as
                    xcopy65e.lha  Length: 25360 bytes

     Rating       : Dangerous!

     Kickstarts   : ?

     Damage       : Overwrites bootblock, and DATA BLOCKS!!!

     Manifestation: Text in memory after decoding: The Curse of Little Sven!

     Removal      : Install new bootblock on infected disk. Fix damaged files
                    with a virus killer. Use VT for instance. (Recommended)

  General comments: The virus moves the original bootblock to block 2+3
                    BUT, IF!!..... the block was used by a file, then
                    have the virus damaged the two data blocks.
                    This file is destroyed and NOT..... possible to repair.
                    The virus contains a routine, which overwrites data
                    after you have done 80 steps.


PAT 08.93
```