VListB

Torben Bilbo" Maciorowski"

COLLABORATORS			
	TITLE : VListB		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY	Torben Bilbo" Maciorowski"	October 17, 2022	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

1 VListB **1**

1.1 VIRUSES - B . . . 1
1.2 bahan . . . 2
1.3 bamiga-sector-1.txt . . . 2
1.4 bgs9.txt . . . 4
1.5 bigboss . . . 5
1.6 blackflash . . . 6
1.7 blackstar . . . 7
1.8 bladerunner . . . 7
1.9 blfvirus . . . 8
1.10 blowjob . . . 8
1.11 bluebox . . . 9
1.12 bootjob . . . 10
1.13 bootx . . . 11
1.14 brethawnes.txt . . . 11
1.15 butonic-1.1.txt . . . 12
1.16 butonic-1.31 . . . 14
1.17 butonic-3.0 . . . 15
1.18 byte-bandit.txt . . . 15
1.19 byte-bandit-2 . . . 17
1.20 byte-bandit-3.txt . . . 17
1.21 byte-bandit-4.txt . . . 19
1.22 byte-bandit-clone . . . 20
1.23 byte-bandit-error . . . 21
1.24 byte-bandit-plus.txt . . . 21
1.25 byte-warrior.txt . . . 23
1.26 byteparasite1 . . . 24
1.27 byteparasite2 . . . 24
1.28 byteparasite3 . . . 25
1.29 bytevoyager1 . . . 26
1.30 bytevoyager2 . . . 26

Chapter 1

VListB

1.1 VIRUSES - B

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

Bahan

Bamiga Sector One (B.S.1)

BGS9

Big Boss

Black Flash v2.0

Blackstar

Blade Runner

BLF Virus

Blowjob

Bluebox Trojan

Bootjob

BootX Virus (Perverse I)

Bret Hawnes

Butonics v1.1

Butonics v1.31

Butonics v3.0

Byte Bandit

Byte Bandit 2

Byte Bandit 3 (NoHead)

Byte Bandit 4

Byte Bandit Clone

Byte Bandit Error

Byte Bandit Plus

Byte Warrior

Byte Parasite 1

Byte Parasite 2

Byte Parasite 3

Byte Voyager 1

Byte Voyager 2

1.2 bahan

```
Name            : Bahan
Aliases         : Butonic 1.1
Type/Size       : BootBlock virus
Incidence       : -
Discovered      : -
Way to infect   : Via BB
Rating          : Dangerous
Kickstarts      : -
Damage          : -
Manifestiation  : Text display: 'BUTONIC'S VIRUS 1.1' and so on..
Removal         : Use a good viruskiller.
General comments: -
```

1.3 bamiga-sector-1.txt

```
=== Computer Virus Catalog 1.2: BAMIGA SECTOR 1 Virus (5-June-1990) ===
Entry..............: BAMIGA SECTOR 1 Virus
Alias(es)..........: --
Virus Strain.......: SCA Virus
Virus detected when.: October 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.....: 1.2/33.166, 1.2/33.180 and 1.3/34.20
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
--------------------- Attributes --------------------------------------
Easy Identification.: typical text: 'BAMIGA SECTOR ONE - THE BEST IN
                        BELGIUM! and, even better of some FN!! (Fuck
                        and Noise!) FN go back to the Kind-machine
                        C64! You somewhat cracked ? BS1!BS1!BS1!BS1!
                        BS1!BS1!BS1! '
                      virus feature: pressing left mouse/fire button of
                        port 1 during system reboot, causes the screen
                        to become green and the virus to shut down it-
                        self by clearing ColdCapture and CoolCapture
                        Vectors
Type of infection...: self-identification method: testing 3rd longword
                        for matching string 'CHW!'
                      system infection: RAM resident, reset resident,
                        bootblock
Infection Trigger...: reset (CONTROL + Left-AMIGA + RIGHT-AMIGA)
Storage media affected: only floppy disks (3.5" and 5.25")
Interrupts hooked...: ---
Damage.............: permanent damage: overwriting bootblock
                      transient damage: screen buffer manipulation:
                        screen becomes black, message (see above)
                        is shown by fading in and out peaces of it
Damage Trigger......: permanent damage: reset
                      transient damage: 15th infection
Particularities.....: a resident program using the CoolCaptureVector is
                       shut down, also such using the ColdCaptureVector
                       when the virus is shut down by its 'suicide'
                       function
Similarities........: SCA 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',
                                     'VIRUSKILLER 2.0', 'VIRUSX 4.0'
                      Category 4: Vaccine: 'SCA-PROTECTOR 1.0',
                                     'VIRUSKILLER 2.0'
                      Category 5: Hardware Methods: ---
                      Category 6: Cryptographic Methods: ---
```

```
Countermeasures successful: 'CHECKVECTORS 2.2', 'GUARDIAN 1.2',
                            'VIRUSKILLER 2.0', 'SCA-PROTECTOR 1.0',
                            'VIRUSX 4.0'; own suicide function
Standard means......: 'CHECKVECTORS 2.2'
--------------------- Acknowledgement --------------------------------
Location............: Virus Test Center, University Hamburg, FRG
Classification by...: Oliver Meng
Documentation by....: Alfred Manthey Rojas
Date................: 5-June-1990
Information Source..: ---
===================== End of BAMIGA SECTOR 1 Virus ==================
```

1.4 bgs9.txt

```
======= Computer Virus Catalog 1.2: "BGS 9" Virus (5-June-1990) =======
Entry...............: "BGS 9" (=Bundesgrenzschutz Sektion 9) Virus
Alias(es)...........: ---
Virus Strain........: ---
Virus detected when.: June 1989
              where.: Elmshorn, FRG
Classification......: link virus (renaming), resident
Length of Virus.....: 1. length on storage medium: 2608 byte
                      2. length in RAM           : 2608 byte
--------------------- Preconditions ----------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: 1.2/33.166, 1.2/33.180, 1.3/34.5
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
--------------------- Attributes -------------------------------------
Easy Identification.: typical text: 'TTV1' at the end of the virus
                         (length is 2608 byte)
                      identification on disk: a file in ROOT- and/or
                         DEVS-directory is named with the following
                         unprintable string:
                         $A0,$A0,$A0,$20,$20,$20,$A0,$20,$20,$20,$A0,
                         length of first command in startup-sequence
                         seems to be altered to 2608 byte (because the
                         file isn't the original anymore)
Type of infection...: self-identification method: virus searches for a
                         file in devs- or root directory named with
                         the following unprintable string:
                         $A0,$A0,$A0,$20,$20,$20,$A0,$20,$20,$20,$A0
                      system infection: RAM resident, reset resident
Infection Trigger...: reset (CONTROL + Left-AMIGA + Right-AMIGA)
Storage media affected: bootable floppy disks ( 3.5'' and 5.25'' ),
                         bootable ram disks, bootable hard disks
Interrupts hooked...: ---
Damage..............: permanent damage: overwriting bootblock
                      transient damage: screen buffer manipulation:
                         screen becomes black, a graphic with following
                         text is shown:
                              'a computer virus is a disease
                               terrorism is a transgression
                               software piracy is a crime
                               this is the cure     BGS9
                               Bundesgrenzschutz Sektion 9
```

```
                              Sonderkommando "EDV"        '
Damage Trigger......: permanent damage: reset (CONTROL + LEFT-AMIGA +
                                               RIGHT-AMIGA)
                      transient damage: 4 resets (have to be run until
                         initial CLI window appears )
Particularities.....: other resident programs using the system resident
                         list (KickTagPointer,KickMemPointer) are
                         shutdown; name of its resident task is 'TTV1'
                         (see string in bootblock code) when the virus
                         doesn't find a DEVS directory, it uses the
                         root.
                      first command in startup-sequence is renamed to
                         a file named with the following unprintable
                         string: '$A0,$A0,$A0,$20,$20,$20,$A0,$20,$20,
                         $20,$A0' (in DEVS- or in root directory if
                         available) and the Virus is written to the
                         directory. the command comes from using the
                         same name, next time the virus will be called
                         first before the original command is executed.
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',
                                     'BGS9-PROTECTOR', 'VIRUSX 4.0'
                      Category 4: Vaccine: 'BGS9-PROTECTOR'
                      Category 5: Hardware Methods: --
                      Category 6: Cryptographic Methods: ---
Countermeasures successful: 'CHECKVECTORS 2.2', 'BGS9-PROTECTOR'
Standard means......: 'CHECKVECTORS 2.2' (removal)
                       and creating two files named with the following
                       unprintable string '$A0,$A0,$A0,$20,$20,$20,$A0,
                       $20,$20,$20,$A0' for vaccinate disk (one file
                       has to be placed in the ROOT- and one in DEVS-
                       directory),
                      'BGS9-PROTECTOR'
--------------------- Acknowledgement -------------------------------
Location............: Virus Test Center, University Hamburg, FRG
Classification by...: Wolfram Schmidt, Alfred Manthey Rojas
Documentation by....: Alfred Manthey Rojas
Date................: 5-June1990
Information Source..: ---
===================== End of "BGS 9" Virus ============================
```

See the screendump of the BGS9 virus

1.5 bigboss

```
Name            : Big Boss

Aliases         : -

Type/Size       : BootBlock virus

Incidence       : -

Discovered      : -

Way to infect   : Via BB

Rating          : -

Kickstarts      : -

Damage          : -

Manifestiation  : -

Removal         : Use a good viruskiller.

General comments: SCA-Clone see there
```

1.6 blackflash

```
Name            : BlackFlash Virus

Aliases         : Black Flash 2.0

Type/Size       : BootBlock virus

Incidence       : -

Discovered      : -

Way to infect   : Via BB

Rating          : Dangerous

Kickstarts      : -

Damage          : Can destroy HardDisk's too, by overwriting
                  cylinder 0

Manifestiation  : Text, see below. Also readable in BB

Removal         : Use a good viruskiller.

General comments: Text, also in BB:

                 'HELLO, I AM AMIGA
                 PLEASE HELP ME !
                 I FEEL SICK !
                 I HAVE A VIRUS !
```

```
                    ! BY BLACKFLASH !'

  See the screendump of the  BlackFlash  virus!
```

1.7 blackstar

```
Name            : Blackstar

Aliases         : Starfire 1/Northstar 1

Type/Size       : BootBlock virus

Incidence       : -

Discovered      : -

Way to infect   : Via BB

Rating          : -

Kickstarts      : -

Damage          : -

Manifestiation  : -

Removal         : Use a good viruskiller.

General comments: See Starfire 1/Northstar 1
```

1.8 bladerunner

```
Name            : Blade Runner

Aliases         : -

Type/Size       : BootBlock virus

Incidence       : -

Discovered      : -

Way to infect   : Via BB

Rating          : -

Kickstarts      : -

Damage          : -

Manifestiation  : -
```

```
        Removal         : Use a good viruskiller.

        General comments: SCA-Clone see there
```

1.9 blfvirus

```
        Name            : BLF Virus

        Aliases         : -

        Type/Size       : BootBlock virus

        Incidence       : -

        Discovered      : -

        Way to infect   : Via BB

        Rating          : -

        Kickstarts      : -

        Damage          : BB

        Manifestiation  : None, this virus doesn't show itself.

        Removal         : Use a good viruskiller.

        General comments: In decoded BB, you can read:
you have found the routine !! This is the new virus by BLF

NOTE: This text is NOT normally visible
```

1.10 blowjob

```
        Name            : Blowjob

        Aliases         : -

        Type/Size       : BootBlock virus

        Incidence       : -

        Discovered      : -

        Way to infect   : Via BB

        Rating          : -

        Kickstarts      : -

        Damage          : BB
```

```
        Manifestiation  : This BB tries to hide itself by writing (in BB):
                          Memory Allocator 3.01

        Removal         : Use a good viruskiller.

        General comments: In about 10 minutes after the infection by the
virus, the following text is displayed, using DisplayAlert (red flashing
box):
   ONCE AGAIN SOMETHING WONDERFUL HAPPENDED  (HE HE HE)
PLEASE POWER OFF  - PLEASE POWER OFF  - PLEASE POWER OFF

          See the screendump of the  BlowJob  virus!
```

1.11 bluebox

Besides listing the way the viruses work, I have included the observations I have done during the analyses.

Please note that my descriptions are purely theoretical; I haven't tried any of the viruses in practice, except one. However, I have studied them very thorough so I know what the individual virus is capable of.

```
-------------------------------------------------------------------------
                                BlueBox virus
-------------------------------------------------------------------------

Type: File (Trojan)

Origin: BLUEBOX in bluebox.lzh

Infect: LIBS:icon.library

Short: Execute commands via the serial port.


Long:

bluebox.lzh (size: 23033 bytes) contains
  BLUEBOX   (size: 5608)
  BLUEBOX.info    (size: 325)
  BLUEBOX.DOC   (size: 37271)
  BLUEBOX.DOC.info  (size: 354, Default tool: c:ced)

BLUEBOX is packed. Unpacked size is 9362 bytes.

Then the BlueBox utility is started, the virus will overwrite (protection
bit is cleared) any existing LIBS:icon.library (datestamp is copies from
original) with itself, which includes a copy of icon.library ( "icon 34.2
(22 Jun 1989",13,10,0 ). Afterwards the utility will be executed as normal.

Next time the icon.library is opened, the virus will launch a process called
"input.device " (note the space at the end!) (stack = 10000 bytes, priority
= 0) and also patch the Level5 interrupt (Serial port receive buffer full.)
```

The icon.library will function as normal.

The Level5 interrupt snoops the serial port for a carriage-return (ascii value 13) terminated string, and continues with the original interrupt. If the string is the numerical sequence {9,14,19,9,4,5,1} then it will execute the DOS command which follows immediately after. Output of this command will be collected in the file

"RAM: " (Last char is a shifted space! Ascii value 160)

This file is then read into an allocated area (max. 10000 bytes) and then sent back through the serial port.

Observations:

The core code for BlueBox and for the Timer virus is the same. Furthermore, the Level5 code is exactly the same for these two trojans.

The numerical sequence yields the word "INSIDEA".

The Level5 interrupt is accessed directly at $74, not though the Vector Base Register.

See also: Timer virus.

If you want to get in contact with me you could try the Internet (Usenet) email address

breese@imada.ou.dk

or the comp.sys.amiga.* newsgroups (probably .misc or .programmer)

Bjorn Reese.

1.12 bootjob

Name : BootJob

Aliases : --

Type/Size : Installer/1356

Incidence : ?

Discovered :

Way to infect: None

Rating : Dangerous if used with evilness in mind

Kickstarts : ?

Damage : ?

```
     Manifestation: It's not hidden!

     Removal      :

  General comments: A standard program, that can save bootblocks as
        excutables. Dangeorous, because these executables can also be
        viruses, which in some cases will infect memory and there after
        other disks.


JN 07.09.93
```

1.13 bootx

```
        Name            : BootX

        Aliases         : Perverse I

        Type/Size       : BootBlock virus

        Incidence       : -

        Discovered      : -

        Way to infect   : Via BB

        Rating          : Dangerous

        Kickstarts      : 2.04 too

        Damage          : BB

        Manifestiation  : Tries to hide by text in BB: 'BootX-Viruskiller
                          by P.Stuer'

        Removal         : Use a good viruskiller.

        General comments: Reveals itself by write-protected disk giving a
requester: Read/write error. Message:
SOFTWARE_PIRATES RUINED MY EXCELLENT PROFESSIONAL DTP_PROGRAM
   I REVENGE MYSELF ON THESE IDIOTS BY PROGRAMMING VIRUSES
        THIS IS PERVERSE I  BECAUSE I LIKE ASSHOLE_FUCKING
            I PROGRAM VIRUSES FOR MS_DOS TOO
```

1.14 brethawnes.txt

```
===== Computer Virus Catalog 1.2: BRET HAWNES Virus (20-FEB-1993) ======
Entry..............: BRET HAWNES Virus
Alias(es)..........: ---
Virus Strain.......: ---
Virus detected when.: ---
```

```
              where.: ---
Classification......: Link virus (directory type), resident
Length of Virus.....: 1. Length on storage medium:  2608 byte
                      2. Length in RAM:            12608 byte
--------------------- Preconditions -----------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: 1.2/all, 1.2/all, 2.01/all
Computer model(s)...: all models
--------------------- Attributes --------------------------------------
Easy Identification.: Identification by the following entry (hex) in
                         "startup-sequence" as first entry:
                         $C0,$A0,$E0,$A0,$C0 (invisible in most ASCII
                         editors)
Type of infection...: Self-identification method: virus is searching for
                         its internal name (5 bytes) as first entry
                         in "startup-sequence"
                      System infection: RAM resident, reset resident
Infection Trigger...: first use of OpenWindow after reset
Storage media affected: all DOS-devices
Interrupts hooked...: hardware-interrupt 3
Damage..............: Permanent damage: writes it's code to disk and
                         it himself into "startup-sequence"
                      Transient damage: system shutdown after displaying
                         "guess who`s back yep, bret hawnes blops
                          your screen",
                         "i`ve taken controll over your amiga !!!!",
                         "there`s only one cure: power off, reboot !!!"
Damage Trigger......: Permanent damage: first OpenWindow after reset
                      Transient damage: 10th infection or 60,000th
                         occurence of interrupt 3 after reset (on
                         PAL-AMIGAS approx. after 20 Minutes)
Particularities.....: Changes OpenLib, OpenWindow und CoolCapture
                         vector and uses KickTagPtr; has a format
                         routine (drive 0, tracks 35 to 45) called
                         every 10th infection that doesn`t seem to work
Similarities........: Colors Virus Carrier; same infection as Lamer
                         file viruses.
--------------------- Agents ------------------------------------------
Countermeasures.....: Virus Checker 6.19, VirusZ 3.00
Countermeasures successful: Virus Checker 6.19, VirusZ 3.00
Standard means......: VirusZ 3.00
--------------------- Acknowledgement ---------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Karim Senoucci
Documentation by....: Karim Senoucci
Date................: 15-December-1992
Information Source..: Virus analysis
====================== End of BRET HAWNES Virus ========================
```

See the screendump of the Bret-Hawnes virus!

1.15 butonic-1.1.txt

```
===== Computer Virus Catalog 1.2: BUTONIC 1.1 Virus (5-June-1990) =====
Entry..............: BUTONIC 1.1 Virus
Alias(es)..........: ---
Virus Strain.......: SCA Virus
Virus detected when.: October 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.....: 1.2/33.166, 1.2/33.180, 1.3/34.20
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
-------------------- Attributes ------------------------------------
Easy Identification.: typical text: in bootblock: ---
                        in memory: "BUTONIC's VIRUS 1.1 GREETINGS TO
                        HACKMACK", "<GENERATION NR. #####>"
Type of infection...: self-identification method: unknown yet
                      system infection: RAM resident, reset resident,
                                        bootblock
Infection Trigger...: reset (CONTROL + Left-AMIGA + RIGHT-AMIGA)
Storage media affected: only floppy disks (3.5" and 5.25")
Interrupts hooked...: ---
Damage..............: permanent damage: overwriting bootblock
                      transient damage: screen buffer manipulation:
                        screen becomes light blue, following message
                        is shown: 'BUTONIC'S VIRUS 1.1
                                  GREETINGS TO HACKMACK'
Damage Trigger......: permanent damage: reset
                      transient damage: 15th infection
Particularities.....: a resident program using the CoolCaptureVector is
                        shut down; virus isn't only a clone but a
                        modification of the SCA virus
Similarities........: SCA virus
-------------------- 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: 'CHECKVECTORS 2.2', 'GUARDIAN 1.2',
                            'VIRUSX 4.0'
Standard means......: 'CHECKVECTORS 2.2'
-------------------- Acknowledgement -------------------------------
Location............: Virus Test Center, University Hamburg, FRG
Classification by...: Alfred Manthey Rojas, Wolfram Schmidt
Documentation by....: Alfred Manthey Rojas
Date................: 5-June-1990
Information Source..: --
```

```
==================== End of BUTONIC 1.1 Virus ======================
```

1.16 butonic-1.31

```
Name         : Jeff Butonic 1.31

Aliases      : -

Type/Size    : File/3408

Incidence    : Spread

Discovered   : 08-03-91

Way to infect: every non-write-protected disk
               which contains a Startup-Sequence
               It uses twelve different filenamenes
               to camouflage itself on disk !
               The following entries we can find in
               the 'Startup-Sequence':
               - 'AddBuffers 20'
               - 'Add21K'
               - 'Fault 106'
               - 'break 1 D'
               - 'changetaskpri 5'
               - 'wait'
               - 'Arthus'
               - 'Helmar'
               - 'Aloisius'
               - $A0A0A020
               - $A020
               - $2020

Rating       : Less dangerous

Kickstarts   : only 1.2

Damage       : None

Manifestation: After some time, a DisplayAlert with this text
                "Einen ganz wanderschnen good Tag!"
      "* I am JEFF - the new Virus generation on Amiga *"
                "(w) by the genius BUTONIC."
         "V 1.31/05.11.88 - Generation Nr.00037"
   "Greetings to * Hackmack *,* Atlantic *, Wolfram, Frank,"
  "Miguel, Alex, Gerlach, and to the whole Physik-LK from MPG!!"

   In the menu bar on some messages will be displayed:

    "Ich brauch jetzt'n Bier!"
    "Stau auf Datenbus bei Speicherkilometer 128!"
    "Mehr Buszyklen fr den Processor!"
    "Ein dreifach MITLEID fr Atari ST!"
    "BUTONIC!"
    "Schon die Steinzeitmenschen benutzten MS-DOS...einige sogar heut
```

```
          noch!"
         "Schon mal den Sound vom PS/2 gehrt???"
         "PC/XT-AT: Spendenkonto 004..."
         "Unabhngigkeit & Selbstbestimmung fr den Tastaturprozessor!"
         "Paula meint, Agnus sei zu dick."
         "IBM PC/XT: Ein Fall fr den Antiquittenhndler..."
         "Sag mir, ob du Assembler kannst, and ich sage dir, wer du bist."

     Removal      : Delete the file with the virus in,
                    and remove it's name from the startup-sequence

  General comments: Always remember to write protect your disk !


JN 07.09.93
```

1.17 butonic-3.0

```
     Name         : Jeff Butonic 3.0

     Aliases      : -

     Type/Size    : File/2916

     Incidence    : Spread

     Discovered   : 18-11-92

     Way to infect: All booted disks

     Rating       : Less dangerous

     Kickstarts   : ?

     Damage       : Writes a file with hex number A0A0A0 (invisible)
                    and also in the startup-sequence 1st line A0A0A0209B41

     Manifestation: Some text:
                             Hi.JEFF`s speaking here...
                             (w) by the genius BUTONIC.
                              etc. in total over $270 Bytes Text

     Removal      : delete 1st line in startup
                    and delete the invisible file

  General comments: Always remember to write protect your disk !


JN 07.09.93
```

1.18 byte-bandit.txt

```
===== Computer Virus Catalog 1.2: BYTE BANDIT Virus (5-June-1990) =====
Entry...............: BYTE BANDIT Virus
Alias(es)...........: ---
Virus Strain........: BYTE BANDIT Virus
Virus detected when.: January 1988
              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.....: 1.2/33.166, 1.2/33.180 and 1.3/34.20
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
                      (and only with those memory expansions of
                        $0C000000 type)
---------------------- Attributes --------------------------------------
Easy Identification.: typical text: 'Virus by Byte   Bandit in  9.87.
                                     Number of       copys :'
Type of infection...: self-identification method: ---
                      system infection: RAM resident, reset resident,
                         bootblock
Infection Trigger...: reset (CONTROL + Left-AMIGA + Right-AMIGA)
                      operation: any disk access
Storage media affected: only floppy disks (3.5" and 5.25")
Interrupts hooked...: vertical blank interupt
Damage..............: permanent damage: overwriting bootblock, maybe
                         killing opened files when the screen and the
                         keyboard are shut off and the user has to
                         restart the computer using
                         CONTROL + LEFT-AMIGA + RIGHT-AMIGA keys.
                      transient damage: screen buffer manipulation:
                         screen becomes dark, keyboard seems to mal-
                         function, transient damage may only be inter-
                         rupted by pressing a special key combination:
                         LEFT-ALT+LEFT-AMIGA (on newer AMIGAS the
                         COMMODORE key)+SPACE+RIGHT-AMIGA +RIGHT ALT
                         (but the virus is still active)
Damage Trigger......: permanent damage: reset
                         operation: any disk access
                      transient damage: only under following condition:
                         2 resets AND 6 infections AND execution of
                         BYTE BANDIT's own interrupt routine 5208 times
                         (about 7 minutes)
Particularities.....: uses StartIOVector
                      other resident programs using the system resident
                         list (KickTagPointer, KickMemPointer) are shut
                         down
                      copy counter: 19th word
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: 'CHECKVECTORS 2.2', 'GUARDIAN 1.2',
                            'VIRUSX 4.0'
Standard means......: 'CHECKVECTORS 2.2'
-------------------- Acknowledgement -------------------------------
Location............: Virus Test Center, University Hamburg, FRG
Classification by...: Alfred Manthey Rojas & Joerg Kock
Documentation by....: Alfred Manthey Rojas
Date................: 5-June-1990
Information Source..: ---
====================== End of BYTE BANDIT Virus ======================
```

1.19 byte-bandit-2

```
        Name            : Byte Bandit 2

        Aliases         : No Name 1

        Type/Size       : BootBlock virus

        Incidence       : -

        Discovered      : -

        Way to infect   : Via BB

        Rating          : Dangerous

        Kickstarts      : -

        Damage          : BB

        Manifestiation  : -

        Removal         : Use a good viruskiller like VT

        General comments: See No Name 1
```

1.20 byte-bandit-3.txt

```
= Computer Virus Catalog 1.2: BYTE BANDIT 3 Virus (10-February-1991) =

Entry...............: BYTE BANDIT 3 Virus
Alias(es)...........: ---
Virus Strain........: BYTE BANDIT strain
Virus detected when.: July 1990     (when VTC received virus copy)
              where.: North Germany
```

```
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.....: 1.2/33.166, 1.2/33.180 and 1.3/34.20
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
                         (and only with those memory expansions of
                          $0C000000 type)
--------------------- Attributes ------------------------------------
Easy Identification.: typical text: in bootblock: 'Virus by Byte
                        Bandit in 9.87.Number of copys :'
Type of infection...: self-identification method: ---
                      system infection: RAM resident, reset resident,
                                        bootblock infection
Infection Trigger...: reset (CONTROL+Left-AMIGA+Right-AMIGA)
                      operation: any disk access
Storage media affected: only floppy disks (3.5" and 5.25")
Interrupts hooked...: vertical blank interrupt
Damage..............: permanent damage: overwriting bootblock; open
                         files may be destroyed when screen and key-
                         board are shut off and the user has to re-
                         start the computer using CONTROL+LEFT-AMIGA
                         +RIGHT-AMIGA; virus allocates 65536 Byte at
                         every system reboot
                      transient damage: screen buffer manipulation:
                         screen becomes dark, keyboard seems to mal-
                         function; transient damage may be repaired
                         by pressing the key combination: LEFT-ALT
                         +LEFT-AMIGA (on new AMIGAS: COMMODORE key)
                         +SPACE+RIGHT-AMIGA+RIGHT ALT, but the virus
                         is is still active
Damage Trigger......: permanent damage: reset
                         operation: any disk access
                      transient damage: if condition holds: 2 resets
                         AND 6 infections AND execution of BYTE
                         BANDIT's own interrupt routine 5208 times
                         (about 7 minutes)
Particularities.....: uses StartIOVector; other resident programs using
                         the system resident list (KickTagPointer,
                         KickMemPointer) are shut down;
                      copy counter: 19th word
Similarities........: clone of BYTE BANDIT with some new code instead
                         of bootblock text; manipulates background
                         color; steels 65536 byte of system memory
                         every time the system is rebooted
--------------------- Agents ----------------------------------------
Countermeasures.....: Names of tested products of Category 1-6:
                      Category 1: .2 Monitoring System Vectors:
                                     CHECKVECTORS 2.3
                                  .3 Monitoring System Areas:
                                     CHECKVECTORS 2.3,GUARDIAN 1.2,
                                     VIRUS-DETEKTOR 1.1
                      Category 2: Alteration Detection: ---
                      Category 3: Eradication: CHECKVECTORS 2.3,
                                               VIRUS-DETEKTOR 1.1
                      Category 4: Vaccine: ---
```

```
                     Category 5: Hardware Methods: ---
                     Category 6: Cryptographic Methods: ---
Countermeasures successful: CHECKVECTORS 2.3, GUARDIAN 1.2,
                            VIRUS-DETEKTOR 1.1
Standard means......: CHECKVECTORS 2.3
---------------------- Acknowledgement --------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Alfred Manthey Rojas
Documentation by....: Alfred Manthey Rojas
Date................: 10-February-1991
Information Source..: ---
====================== End of BYTE BANDIT 3-Virus ====================
```

1.21 byte-bandit-4.txt

```
= Computer Virus Catalog 1.2: BYTE BANDIT 4 Virus (10-February-1991) =

Entry...............: BYTE BANDIT 4 Virus
Alias(es)...........: ---
Virus Strain........: BYTE BANDIT strain
Virus detected when.: July 1990     (when VTC received virus code)
               where.: North Germany
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.....: 1.2/33.166, 1.2/33.180 and 1.3/34.20
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
                         (and only with those memory expansions of
                          $0C000000 type)
---------------------- Attributes ------------------------------------
Easy Identification.: typical text: ---
Type of infection...: self-identification method: ---
                      system infection: RAM resident, reset resident,
                                        bootblock
Infection Trigger...: reset (CONTROL+Left-AMIGA+Right-AMIGA)
                      operation: any disk access
Storage media affected: only floppy disks (3.5" and 5.25")
Interrupts hooked...: vertical blank interrupt
Damage..............: permanent damage: overwriting bootblock; open
                         files may be destroyed when screen and key-
                         board are shut off and the user has to re-
                         start the computer using CONTROL+LEFT-AMIGA
                         +RIGHT-AMIGA keys; same functions as in
                         original BYTE BANDIT virus, only text was
                         stripped from bootblock and has been re-
                         placed by the text "dos.library"
                      transient damage: screen buffer manipulation:
                         screen becomes dark, keyboard seems to mal-
                         function; transient damage may be repaired
                         by pressing special key combination:
                         LEFT-ALT+LEFT-AMIGA (new AMIGAS: COMMODORE
                         key)+SPACE+RIGHT-AMIGA+RIGHT ALT, but the
                         virus is still active
```

```
Damage Trigger......: permanent damage: reset
                         operation: any disk access
                      transient damage: under following condition:
                         2 resets AND 6 infections AND execution of
                         BYTE BANDIT's own interrupt routine 5208
                         times (about 7 minutes)
Particularities.....: uses StartIOVector; other resident programs
                         using system resident list (KickTagPointer,
                         KickMemPointer) are shutdown;
                      copy counter: 19th word

Similarities........: clone of BYTE BANDIT with replacement of ori-
                         ginal virus text by string 'dos.library'
--------------------- Agents ----------------------------------------
Countermeasures.....: Names of tested products of Category 1-6:
                      Category 1: .2 Monitoring System Vectors:
                                     CHECKVECTORS 2.3
                                  .3 Monitoring System Areas:
                                     CHECKVECTORS 2.3, GUARDIAN 1.2,
                                     VIRUS-DETEKTOR 1.1
                      Category 2: Alteration Detection: ---
                      Category 3: Eradication: CHECKVECTORS 2.3,
                                               VIRUS-DETEKTOR 1.1
                      Category 4: Vaccine: ---
                      Category 5: Hardware Methods: ---
                      Category 6: Cryptographic Methods: ---
Countermeasures successful: CHECKVECTORS 2.3, GUARDIAN 1.2,
                            VIRUS-DETEKTOR 1.1
Standard means......: CHECKVECTORS 2.3
--------------------- Acknowledgement -------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Alfred Manthey Rojas
Documentation by....: Alfred Manthey Rojas
Date................: 13th JANUARY 1991
Information Source..: ---
====================== End of BYTE BANDIT 4 Virus ====================
```

1.22 byte-bandit-clone

```
        Name            : Byte Bandit Clone

        Aliases         : -

        Type/Size       : BootBlock virus

        Incidence       : -

        Discovered      : -

        Way to infect   : Via BB

        Rating          : Dangerous

        Kickstarts      : -
```

```
        Damage          : BB

        Manifestiation  : -

        Removal         : Use a good viruskiller.

        General comments: Byte B... text has been removed from BB!
```

1.23 byte-bandit-error

```
        Name            : Byte Bandit Error

        Aliases         : -

        Type/Size       : BootBlock virus

        Incidence       : -

        Discovered      : -

        Way to infect   : Via BB

        Rating          : Dangerous

        Kickstarts      : -

        Damage          : BB

        Manifestiation  : -

        Removal         : Use a good viruskiller.

        General comments: When infected with this virus, the disk becomes
NOT A DOS DISK, therefore the virus can't be booted, and it can't spread! A
masterpiece of programming!!
```

1.24 byte-bandit-plus.txt

```
== Computer Virus Catalog 1.2: BYTE BANDIT PLUS Virus (5-June-1990) ===
Entry...............: BYTE BANDIT PLUS Virus
Alias(es)...........: ---
Virus Strain........: BYTE BANDIT Virus
Virus detected when.: September 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.....: 1.2/33.166, 1.2/33.180 and 1.3/34.20
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
                         (and only with those memory expansions of
```

```
                          $0C000000 type)
--------------------- Attributes ------------------------------------
Easy Identification.: typical text: ---
Type of infection...: self-identification method: ---
                      system infection: RAM resident, reset resident,
                         bootblock
Infection Trigger...: reset (CONTROL + Left-AMIGA + Right-AMIGA)
                      operation: any disk access
Storage media affected: only floppy disks (3.5" and 5.25")
Interrupts hooked...: vertical blank interupt
Damage..............: permanent damage: overwriting bootblock, maybe
                         killing opened files when the screen and the
                         keyboard are shut off and the user has to
                         restart the computer using CONTROL+LEFT-AMIGA
                         +RIGHT-AMIGA keys; allocates available memory
                         minus 86016 byte
                      transient damage: screen buffer manipulation:
                         screen becomes dark, keyboard seems to mal-
                         function, transient damage may only be inter-
                         rupted by pressing a special key combination:
                         LEFT-ALT+LEFT-AMIGA (on newer AMIGAS the
                         COMMODORE key)+SPACE+RIGHT-AMIGA+RIGHT-ALT
                         (but the virus is still active )
Damage Trigger......: permanent damage: reset
                         operation: any disk access
                      transient damage: only under following condition:
                         2 resets AND 6 infections AND execution of
                         BYTE BANDIT's own interrupt routine 5208 times
                         (about 7 minutes)
Particularities.....: uses StartIOVector
                      other resident programs using the system resident
                         list (KickTagPointer,KickMemPointer) are shut
                         down
                      copy counter: 19th word
Similarities........: clone of BYTE BANDIT with some new code instead
                         of bootblock text, using undocumented system
                         adresses, manipulates background color, seems
                         to steel 86016 byte of system memory depending
                         from a counter at memory location $0007FC00
--------------------- 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: 'CHECKVECTORS 2.2', 'GUARDIAN 1.2',
                            'VIRUSX 4.0'
Standard means......: 'CHECKVECTORS 2.2'
--------------------- Acknowledgement -------------------------------
Location............: Virus Test Center, University Hamburg, FRG
```

```
Classification by...: Alfred Manthey Rojas
Documentation by....: Alfred Manthey Rojas
Date................: 5-June-1990
Information Source..: ---
==================== End of BYTE BANDIT PLUS Virus ==================
```

1.25 byte-warrior.txt

```
===== Computer Virus Catalog 1.2: BYTE WARRIOR Virus (5-June-1990) ====
Entry...............: BYTE WARRIOR Virus
Alias(es)...........: DASA Virus
Virus Strain........: BYTE WARRIOR Virus
Virus detected when.: August 1988
              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: bootblock: 'DASA'
                         in memory: 'Virus detector by the mighty Byte
                         Warrior!!! Please, please, please don't install
                         this disk, coz I want to travel! Spread the
                         bootblock and the word!'
Type of infection...: self-identification method: ---
                      system infection: RAM resident, reset resident,
                         bootblock
Infection Trigger...: reset (CONTROL + Left-AMIGA + Right-AMIGA)
                      operation: any disk access
Storage media affected: only floppy disks (3.5" and 5.25")
Interrupts hooked...: ---
Damage..............: permanent damage: overwriting bootblock
                      transient damage: power LED blinks fast when
                         ColdCapture or CoolCapture vector is occupied,
                         sequence of 5 notes is played using audio
                         channel 3.
Damage Trigger......: permanent damage: reset
                         operation: any disk access
                      transient damage: reset
Particularities.....: uses DoIOVector
                      other resident programs using the system resident
                         list (KickTagPointer, KickMemPointer), the
                         ColdCapture or CoolCapture vector are shutdown
Similarities........: PARAMOUNT virus
--------------------- 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',
                                    'VIEWBOOT 1.01', 'VIRUSX 4.0'
                      Category 4: Vaccine: ---
                      Category 5: Hardware Methods: ---
                      Category 6: Cryptographic Methods: ---
Countermeasures successful: 'CHECKVECTORS 2.2', 'GUARDIAN 1.2',
                            'VIRUSX 4.0'
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 BYTE WARRIOR Virus ======================
```

1.26 byteparasite1

```
Name            : Byte Parasite I

Aliases         : -

Type/Size       : Filevirus/2108 bytes

Incidence       : -

Discovered      : -

Way to infect   : None, faulty virus, therefore: Many GURU'S!

Rating          : NOT dangerous!

Kickstarts      : -

Damage          : None, whatsoever!

Manifestiation  : Well, a GURU?

Removal         : Use a good viruskiller.

General comments: Nice try!
```

1.27 byteparasite2

```
Name            : Byte Parasite II

Aliases         : -

Type/Size       : Filevirus/908 bytes

Incidence       : -
```

```
        Discovered      : -

        Way to infect   : Tries to copy VirusX from DF0:c to DF1:C

        Rating          : Relatively dangerous, see below

        Kickstarts      : 2.04 too

        Damage          : Overwrites org. VirusX

        Manifestiation  : Shows a requester saying: 'VirusX: Checking
                          device DF0:

        Removal         : Use a good viruskiller.

        General comments: This little virus, is meant to cause
inconvenience to an anti-virusprogrammer. You can read in the file:'But
now send me to: (An address)'
```

1.28 byteparasite3

```
        Name            : Byte Parasite III

        Aliases         : -

        Type/Size       : Filevirus/2160 bytes

        Incidence       : -

        Discovered      : -

        Way to infect   : Tries to copy Virus-Checker from DF0:c to DF1:C

        Rating          : VERY dangerous!, see below

        Kickstarts      : 2.04 too

        Damage          : Overwrites org. Virus-Checker, with empty file

        Manifestiation  : Shows a requester saying: 'Virus-Checker V3.0: Checking
                          device DF0:

        Removal         : Use a good viruskiller.

        General comments: WARNING! This virus can cause HARDWARE DAMAGE,
look at these cut-outs from letters:
1. "then I found my stepmotor of the disk drive had got hold of the
spindle, and I had to pull it back with a pair of tongs":

2. "then I had to re-adjust the disk drive heads"
```

1.29 bytevoyager1

```
Name            : Byte Voyager I

Aliases         : -

Type/Size       : BootBlock virus

Incidence       : -

Discovered      : -

Way to infect   : Via BB

Rating          : Dangerous

Kickstarts      : -

Damage          : Overwrites block 880 (root) with "Infected by
                  BYTE VOYAGER !!!!!", that is on disks, the new
                  disk-name. NOTE: HD too!

Manifestiation  : New disk name, see above

Removal         : Use a good viruskiller.

General comments: -
```

1.30 bytevoyager2

```
Name            : Byte Voyager II

Aliases         : -

Type/Size       : BootBlock virus

Incidence       : -

Discovered      : -

Way to infect   : Via BB

Rating          : Dangerous

Kickstarts      : -

Damage          : Overwrites block 880 (root) with "Another virus
                  by Byte Voyager", that is on disks, the new
                  disk-name. NOTE: HD too!

Manifestiation  : New disk name, see above

Removal         : Use a good viruskiller.
```

General comments: -