VListV

Torben Bilbo" Maciorowski"

COLLABORATORS

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

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VListV

1.1 VIRUSES - V

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


            Vermin

            Virus Construction Set I

            Virus Construction Set 2

            VirusBlaster 2.3

            VirusTest Bomb 936

            Virus Fighter

            Virus Hunter

            Virus Predator

            Virus Slayer 1.0

            Virus Terminator 6.0

            Virus V1

            Vkill

            Vkill 1.0

            VTerm 6.0
```

1.2 vermin.txt

```
======== Computer Virus Catalog 1.2: VERMIN Virus (20-FEB-1992) ========
Entry...............: VERMIN Virus
Alias(es)...........: ---
Virus Strain........: VERNIM Virus family
Virus detected when.: ---
              where.: ---
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/all, 1.3/all, 2.01/all
Computer model(s)...: All models
--------------------- Attributes --------------------------------------
Easy Identification.: ---
Type of infection...: RAM resident, reset resident, bootblock
Storage media affected: All media (FD,HD)
Interrupts hooked...: ---
Damage..............: Overwriting block zero of the same device
                         (usually the bootblock)
Damage Trigger......: Read/Write-access (DoIO) on bootblock
Particularities.....: Changes DoIO vector; uses CoolCaptureVector;
                         pressing the left Mousebutton during reset
                         removes the virus and turns the screen purple
                         for approx. 2 seconds (timing only correct on
                         7 MHz-AMIGAS as this is only a CPU-loop)
Similarities:         SUPERBOY Virus
--------------------- Agents ------------------------------------------
Countermeasures.....: VirusZ 3.00, VT 2.48, BootX 5.23
Countermeasures successful: VirusZ 3.00, VT 2.48, BootX 5.23
Standard means......: VT 2.48
--------------------- Acknowledgement ---------------------------------
Location............: Virus Test Center, University Hamburg, FRG
Classification by...: Karim Senoucci
Documentation by....: Karim Senoucci
Date................: 14th DECEMBER 1992
Information Source..: ---
===================== End of VERMIN Virus ============================
```

1.3 virusconseti

```
Name         : Virus Construction Set I

Aliases      : -

Type/Size    : Boot/1024

Clone        : Michael Jordan, Coolout, Bartman...

Symptoms     : Shows an alert after 5 infections.

Discovered   : 4-5/93

Way to infect: Boot infection
```

```
     Rating       : Harmless

     Kickstarts   : 1.2/1.3/2.0

     Damage       : Overwrites boot.

     Manifestation: -

     Removal      : Install boot.

     Comments     : It patches the DoIO()-Vector and uses the Cool-
                    capture to stay resident. The virus is always
                    at the same memory-adress ($7f000).
                    There is a coded message in the file:
                    "This virus was made with the... etc."

                    ATTENTION: This bootblock was made with a programm
                    called VirusConstructionSet I. So there exist many
                    clones.


                    Under  the topic CLONES/ORIGIN there are only told
                    a  few viruses, I have got from some users near my
                    hometown.

          See the screendump of the  VirusConSetI  virus!

A.D 12-93
```

1.4 virconset2.txt

```
====== Computer Virus Catalog 1.2: VIRCONSET2 Virus (31-July-1993) =====
Entry...............: VirConSet2 Virus
Alias(es)...........: bbtest Virus
Virus Strain........: ---
Virus detected when.: ---
              where.: ---
Classification......: System virus (bootblock), memory resident
Length of Virus.....: 1.Length on storage medium: 1024 byte
                      2.Length in RAM:            1024 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.: Typical string: " > test" visible in bootblock
Type of infection...: System infection: RAM resident, reset resident,
                         bootblock infector
Infection Trigger...: Insertion of a floppy disk
Storage media affected: Only floppy disks
Interrupts hooked...: ---
Damage..............: Permanent damage: overwriting bootblock
                      Transient damage: displaying AlertBox containing
                                        silly text
```

```
Damage Trigger......: Permanent damage: insertion of a floppy disk
                      Transient damage: directly before 5th infection
Particularities.....: 1) Virus contains flag which indicates whether or
                         not to de/encode the virus.
                      2) Virus has been written with some kind of
                         generator; three versions of the virus are
                         known which only differ in a text string at
                         the begin of the virus and the content of
                         the de/encode flag.
Similarities........: ---
--------------------- 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...: Jens Vogler, Karim Senoucci
Documentation by....: Karim Senoucci, Jens Vogler
Date................: 31.July-1993
Information Source..: Reverse analysis of virus code / Heiner Schneegold
===================== End of VIRCONSET2 Virus ========================
```

See the screendump of the VirusConSetII virus!

1.5 virusblaster_2.3

```
Name         : Virusblaster v2.3

Aliases      : -

Type/Size    : File/9232

Incidence    : ?

Discovered   : ?

Way to infect: Does not spread

Rating       : ?

Kickstarts   : ?

Damage       : Destroys disk in df0:

Manifestation: By loading in Cli you will see a prompt
               as Antivirus Killer from M & T 7/91

Removal      : -

   General comments:
```

PAT 08.93

1.6 virustest_bomb_936.txt

```
== Computer Virus Catalog 1.2: VirusTest_bomb_936 Bomb (31-July-1993) ==
Entry...............: VirusTest_bomb_936 Bomb
Alias(es)...........: ---
Virus Strain........: ---
Virus detected when.: ---
              where.: ---
Classification......: Bomb
Length of Virus.....: 936 bytes (+ 1 byte in "virustest.data")
--------------------- Preconditions ------------------------------------
Operating System(s).: AMIGA-OS
Version/Release.....: 1.2/all, 1.3/all
Computer model(s)...: All AMIGA models
--------------------- Attributes ---------------------------------------
Easy Identification.: There is a "startup-sequence" entry called
                         "virustest", and there is always a 2nd file
                         called "virustest.data" with 1 byte length in
                         root directory. If diskette is write protected,
                        bomb will write to Shell:
                        "User Request : Please remove write Protection
                         and press left Mouse Button to continue.."
Type of infection...: --- (damage only)
Infection Trigger...: ---
Storage media affected: Floppy disks only
Interrupts hooked...: ---
Damage..............: Permanent damage: formating the floppy disk
Damage Trigger......: Permanent damage: starting this program with the
                         byte in "virustest.data" counted down to zero.
Particularities.....: Calling DosFunction with Dosbase in A5 Register
                         can crash recent Operating System versions.
Similarities........: TimeBomb V0.9 (seems to be a new version)
--------------------- Agents -------------------------------------------
Countermeasures.....: VirusZ 3.06, VT 2.54, VirusChecker 6.28
Countermeasures successful: VirusZ 3.06, VT 2.54, VirusChecker 6.26
Standard means......: Delete the files "virustest", "virustest.data",
                         and "startup-sequence" entry, or use VT 2.54.
--------------------- Acknowledgement ----------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Jens Vogler
Documentation by....: Jens Vogler
Date................: 31-July-1993
Information Source..: Reverse analysis of virus code
==================== End of VirusTest_Bomb_936 =======================
```

1.7 virus_fighter

```
     Name         : Virus Fighter V1.0

     Aliases      : VKill-Clone

     Type/Size    : B

     Incidence    : ?
```

```
Discovered   : ?

Way to infect: Booting from an infected disk

Rating       : ?

Kickstarts   : 1.2; 1.3; 2.x; 3.x??

Damage       : Overwrites Bootblock

Manifestation: ?

Removal      : Install a new bootblock

   General comments: Prg. code = VKill
                     DecoderLW changes: "1991"
                     Decoded Text for requester:
                        VIRUS FIGHTER V1.0 etc.
```

PAT 08.93

1.8 virus_hunter

```
Name         : Virus Hunter

Aliases      : -

Type/Size    : B

Incidence    : ?

Discovered   : ?

Way to infect: Booting from an infected disk

Rating       : ?

Kickstarts   : 1.2

Damage       : Overwrites Bootblock

Manifestation: ?

Removal      : Install a new bootblock

   General comments: KickTag $7F300, KickCheckSum $7F307
                     always at $7F300
                     Were an antivirus BB for KS1.2.
                     Adviceable to delete to day.
                     It contains direct ROM-jumps
```

```
PAT 08.93
```

1.9 virus_predator

```
     Name         : Virus Predator

     Aliases      : Julie

     Type/Size    : B

     Incidence    : ?

     Discovered   : ?

     Way to infect: Booting from an infected disk

     Rating       : ?

     Kickstarts   : ? (Does not work OK with 1MB CHIP)

     Damage       : Overwrites Bootblock

     Manifestation: ?

     Removal      : Install a new bootblock

        General comments: always $7f800, cool, DoIo, BeginIo and  $20
                          tests a few pointers and 3 values
                          (e.g. at $7ec00)
                          spreads: without warning over bootable BB's
                          Decoded with not.b (a0)+ you can read
                          (in memory):
                           VIRUS PREDATOR  (4-88-SPAIN)  ID: 027798336


PAT 08.93
```

1.10 virus_slayer_1.0

```
     Name         : Virus Slayer 1.0

     Aliases      : -

     Type/Size    : B

     Incidence    : ?

     Discovered   : ?

     Way to infect: Booting from an infected disk
```

```
Rating       : ?

Kickstarts   : 1.2

Damage       : Overwrites Bootblock

Manifestation: ?

Removal      : Install a new bootblock

   General comments: Cool, DoIo, in memory always $7FA00
                     only KS1.2 because of absolute ROM-DoIo old
```

PAT 08.93

1.11 virus_terminator_6.0

```
Name         : Virus Terminator v 6.0

Aliases      : -

Type/Size    : Trojan/1880

Incidence    : ?

Discovered   : ?

Way to infect: Executing the trojan.

Rating       : ?

Kickstarts   : ?

Damage       : Installs Cheater Hijacker

Manifestation: Pretends to be a Virus Killer

Removal      : Install new bootblock on infected disk.

   General comments: KS2.04 too!!
                     Tries to hide by the text:
                           Virus Terminator v6.0
                           by Rudolf Neiber (1992).
                     But the truth is that this Trojan
                     installs the Cheater Hijacker virus
   (a bootblock virus, see that for more info!)
                     The Virus Terminator is found in memory by VT,
                     and is found by running the VT "FileTest".
                     Advice: Remove the virus and check for the
                     Cheater Hijacker virus!!!
```

PAT 08.93

1.12 virus_v1

```
Name         : Virus V1

Aliases      : -

Type/Size    : Bootblock

Incidence    : ?

Discovered   : ?

Way to infect: Booting from an infected disk

Rating       : ?

Kickstarts   : 1.2; 1.3; 2.x; 3.x??

Damage       : Overwrites Bootblock

Manifestation: As soon as the counter get $F:
               Text Graphics-Routines, dark background:
                   1. Virus V1 (red)
                   2. Wir sind wieder da ahaaa.. (gruen), is to
                      read in the bootblock too.

Removal      : Install new bootblock on infected disk.

   General comments: always $7EC00  Cool $7ec62, DoIo $7eca8
                     Doesn't need trackdisk.device !!!
```

PAT 08.93

1.13 vkill

```
Name         : VKill

Aliases      : Aids

Type/Size    : Bootblock

Incidence    : ?

Discovered   : ?

Way to infect: Booting from an infected disk

Rating       : ?

Kickstarts   : ?

Damage       : Clears bootblock.
```

```
     Manifestation: ?

     Removal      : Install new bootblock on infected disk.

        General comments: changes PutMsg
              with FastMem:
              (clears every write enabled Bootblock
        without warning!!!,
              also when it’s an Org. Bootblock!! )
              with ChipMem only:
              (writes own BB without warning)
              DecodeLongWord: " KEN"


PAT 08.93
```

1.14 vkill-1.0.txt

```
====== Computer Virus Catalog 1.2: VKILL 1.0 Virus (5-June-1990) ======
Entry...............: VKILL 1.0 Virus
Alias(es)...........: ---
Virus Strain........: ---
Virus detected when.: March 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, 1.3/34.5
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
--------------------- Attributes --------------------------------------
Easy Identification.: typical text: --
                      virus feature: ’VKILL 1.0’ requester before
                         opening CLI and detecting a virus or a non-
                         standard bootblock (see below)
Type of infection...: self-identification method: ---
                      system infection: RAM resident, reset resident,
                         bootblock
Infection Trigger...: reset (CONTROL + Left-AMIGA + RIGHT-AMIGA)
                      operation: on bootable standard bootblocks:
                         any access on bootblock sectors (blocks 0,1)
                         created using normal file system and new fast
                         file system;
                         on nonstandard bootblocks: when detecting a
                         virus or a nonstandard bootblock AND
                         ’VKILL 1.0’ request AND positive answer
Storage media affected: only floppy disks (3.5" and 5.25")
Interrupts hooked...: ---
Damage..............: permanent damage: overwrites bootable standard
                         bootblocks; simulates bootable standard boot-
                         blocks when examined with any tool
                      transient damage: screen buffer manipulation:
                         ’VKILL 1.0’ requester before opening CLI and
                         detecting a virus or a nonstandard bootblock
```

```
                          (see below)
Damage Trigger......: permanent damage: reset
                         operation on bootable standard bootblocks:
                         any access on bootblock sectors (blocks 0,1)
                         operation on nonstandard bootblocks: when
                         detecting a known virus or a nonstandard boot-
                         block (see below) AND 'VKILL 1.0' request
                         AND positive answer
                      transient damage: when detecting a known virus
                         or a nonstandard bootblock (see below)
Particularities.....: a resident program using the CoolCaptureVector is
                         shut down; detects BYTE BANDIT, SCA (and SCA
                         clones) and nonstandard bootblocks; detects
                         standard bootblocks of the new fast filing
                         system ('DOS' + $01); virus encodes itself
                         using ascii characters ' Ken' as key
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 VKILL 1.0 Virus =========================
```

1.15 vterm_6.0

```
  Name          : Virus Terminator 6.0

  Aliases       : - (Installer of Cheater Hijacker, perhaps?)

  Type/Size     : Trojan/1880

  Incidence     : ?

  Way to infect: None, but installes the Cheater Hijacker BB virus

  Rating        : Dangerous
```

```
Kickstarts   : ?

Damage       : None (except for the overwriting of the existing BB)

Manifestation: Text: Virus Terminator v6.0 by Rudolf Neiber (1992)

      General comments: A simple trojan that installs the Cheater Hijacker
      virus. Check it out for more info.
```