VListW

Torben Bilbo" Maciorowski"

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

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VListW

1.1 VIRUSES - W

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


               WAFT

               Wahnfried

               WarHawk

               Warshaw Avenger

               Wizard TimeBomb
```

1.2 waft.txt

```
======== Computer Virus Catalog 1.2: WAFT Virus (5-June-1990) =========
Entry...............: WAFT Virus
Alias(es)...........: ---
Virus Strain........: ---
Virus detected when.: 8th 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, 1.3/34.5
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
---------------------- Attributes -------------------------------------
Easy Identification.: typical text: in bootblock: ---
                                    in memory:
                                       '==== oderint dum metuant ====',
                                       '! ! W A F T ! !'     and
```

```
                                    'Quality made in West Germany'
Type of infection...: self-identification method:
                      system infection: RAM resident, reset resident,
                          bootblock
Infection Trigger...: reset, any disk access
Storage media affected: floppy disks (3.5" and 5.25"),
Interrupts hooked...: ---
Damage.............: permanent damage: overwriting bootblock
                      transient damage: screen buffer manipulation:
                         alert box with following text:
                         '    oderint dum metuant
                                ==  W A F T ==
                         Quality made in West Germany'
                         eventcounter dependent activities:
                           ec  <   5: message is shown as alert
                                      (see above)
                           ec  <  65: window structure is manipulated,
                                      so gadgets can't be accessed
                                      in future
                           ec  < 130: mouse pointer disappears
                           ec  < 195: screens gets dark
                           ec >= 195: actions via mouse are disabled,
                                      no icon, no window and no gadget
                                      can be accessed
Damage Trigger......: permanent damage: reset
                         operation: any disk access
                      transient damage: status of CIA-A event counter
                         (bits 0 to 7) (see above)
Particularities.....: simulation of a standard bootblock by examining
                         with disk tools; allocates 1100 byte of memory
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 2.0',
                                     '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 WAFT Virus ================================
```

See the screendump of the Waft virus!

1.3 wahnfried

Name : Wahnfried

Aliases : -

Type/Size : Boot virus/ 1024 bytes

Incidence : ?

Discovered : 27-07-87

Way to infect: See below

Rating : Not very dangerous

Kickstarts : 1.2/1.3 and 2.04 too!

Damage : Overwrites bootblock

Manifestation: DisplayAlert

Removal : Install the virus bootblock

Comments : The name Wahnfried is to read in the bootblock. This virus can infect at Kickstart 1.2, 1.3, and later versions. ATTENTION..be careful this virus can infect your harddisk too!

All written Wahnfried infected bootblock don't work because a checksum error. A counter will start, and when this counter reach 0 a DisplayAlert will come at your monitor with the following text:

"Hardware Failure Press left mouse button to
continue Guru Meditation #00000015.00C03L12
Hooligen-Bits randalieren im Datenbus!
Gruß Erich!"

See the screendump of the Wahnfried virus!

1.4 warhawk.txt

```
======= Computer Virus Catalog 1.2: WARHAWK Virus (5-June-1990) =======
Entry..............: WARHAWK Virus
Alias(es)..........: ---
Virus Strain.......: ---
Virus detected when.: 23th 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.....: 1.2/33.180, others unknown yet
Computer model(s)...: AMIGA 1000, AMIGA 2000A
--------------------- Attributes --------------------------------------
Easy Identification.: typical text: in bootblock:
                        'WARHAWK SAYS : KILLING YOUR DISKS WITH OUR
                        VIRUS IS A WONDERFUL THING ! CONTACT : UCS,
                        PLK 000257-A, 3457 STADTOLDENDORF ! HEY BAD!
                        FUCK OFF'
Type of infection...: self-identification method: ---
                      system infection: RAM resident, reset resident,
                        bootblock
Infection Trigger...: ---
Storage media affected: floppy disks (3.5" and 5.25")
Interrupts hooked...: ---
Damage..............: permanent damage: overwriting bootblock
                      transient damage: ---
Damage Trigger......: permanent damage: ---
                      transient damage: ---
Particularities.....: ---
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...: Oliver Meng
Documentation by....: Alfred Manthey Rojas
Date................: 5-June-1990
Information Source..: ---
==================== End of WARHAWK Virus ============================
```

1.5 warshaw-avenger.txt

```
=== Computer Virus Catalog 1.2: Warshaw Avenger Virus (31-July-1993) ===
Entry...............: Warshaw Avenger Virus
```

```
Alias(es).....: Warshaw! Virus
Virus Strain.....: Lamer Virus Strain
Virus detected when.: ---
              where.: ---
Classification......: System Virus (BootBlock), memory resident
Length of Virus.....: 1.Length on storage medium: 1024 bytes
                      2.Length in RAM:            1024 bytes
--------------------- Preconditions -----------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: 1.2, 1.3, 2.04, 3.0
Computer model(s)...: All Amigas (problems with timing!)
--------------------- Attributes --------------------------------------
Easy Identification.: Text teadable in Bootblock and Ram:
                         "Warshaw!", "Warshaw Avenger presents!!!"
Type of infection...: Self-Identification methods: searches for $ABCD
                         in Bootblock (similar to some Lamer viruses)
                      System infection: RAM-Resident (Adress=SysStack-
                         Lower+RND-Value), Reset-Resident (KickTag),
                         Bootblock
                      Hooked library/Device calls:
                         SumKickData (exec) - To bypass some antivirus
                         BeginIo     (Trackdisk) - infection / damage
Infection Trigger...: Any disk access
Storage media affected: Floppy disks only
Interrupts hooked...: ---
Damage..............: Permanent Damage: overwriting bootblock,
                         overwriting random sectors with "Warshaw!"
Damage Trigger......: Permanent Damage: Random (Rasterbeam)
Particularities.....: ---
Similarities........: Lamer Virus Strain
Stealth.............: Virus attempts to bypass antivirus-products by
                         producing a "clean" bootblock.
--------------------- Agents ------------------------------------------
Countermeasures.....: Names of tested products of Category 1-6:
                      Category 1: .1 -
                                  .2 Xooper, AVM (internal)
                                  .3 VT2.54,AVM (internal)
                      Category 2: VT2.54, BootX, VirusZ, AVM
                      Category 3: VT2.54, AVM (int.)
                      Category 4: -
                      Category 5: -
                      Category 6: -
Countermeasures successful: VT2.54,Xooper,BootX,VirusZ,AVM
Standard means......: VT2.54
--------------------- Acknowledgement ---------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Soenke Freitag
Documentation by....: Soenke Freitag
Date................: 31-July-1993
Information Source..: Reverse analysis of virus code/H.Schneegold, SHI
===================== End of Warshaw Avenger Virus ==================
```

1.6 wizard-timebomb.txt

```
====== Computer Virus Catalog 1.2: WIZARD TIMEBOMB (5-June-1990) ======
Entry..............: WIZARD TIMEBOMB
Alias(es)..........: --
Virus Strain.......: --
Virus detected when.: November 1989
              where.: Elmshorn, FRG
Classification.....: timebomb, non-resident
Length of Virus.....: 1. length on storage medium: 7840 byte
                      2. length in RAM           : 7840 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: 'User Request : Please remove write
                        Protection and press left mouse Button to
                        continue..', ' RAM CHECKED - NOVIRUS FOUND.',
                        'Hey Looser ! I hate you ! ', 'df0:pic.xx'
Type of infection...: self-identification method: ---
                      system infection: transient
Infection Trigger...: every execution of WIZARD TIMEBOMB
Storage media affected: bootable storage medium containing the WIZARD
                        TIMEBOMB
Interrupts hooked...: ---
Damage..............: permanent damage: ---
                      transient damage: ---
Damage Trigger......: permanent damage: ---
                      transient damage: ---
Particularities.....: seems to format after its eventcounter becomes
                        a special value; seems to handle a picture
                        on drive df0:, manner unknown yet; suggests
                        users to be an antivirus;
                      WIZARD TIMEBOMB covers itself by using the name
                        '.info', normally a file created by the
                        operating system, when handling icons and
                        windows under 'workbench', this file is
                        located in the c-directory, which normally
                        isn't accessable from workbench, '.info'-file
                        has to be invoked in the 'startup-sequence',
                        otherwise the timebomb can't act;
                        other particularities are unknown yet
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: ---
Standard means......: ---
```

```
---------------------- 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 WIZARD TIMEBOMB ========================
```