VListE

Torben Bilbo" Maciorowski"

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

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VListE

1.1 VIRUSES - E

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


                EastStar

                EastStar Installer

                Electro Vision

                EM-Wurm

                Euromail

                Excrement

                Excrement Installer

                Excreminator 1 Bomb

                Executors

                Exorcist

                Express 2.20

                Extreme
```

1.2 eaststar

```
     Name          : EastStar

     Aliases       : No Aliases
```

```
    Type/Size    : Boot/1024

    Original     : NortStar

    Symptoms     : No Symptoms

    Discovered   : ?

    Way to infect: Boot infection

    Rating       : Harmeless

    Kickstarts   : 1.2/1.3

    Damage       : Overwrites boot.

    Manifestation: -

    Removal      : Install boot.

    Comments     : The EastStar virus is a NorthStar clone.
                   So please look there for further information.

A.D 02-94
```

1.3 eaststarinstaller

```
    Name         : East Star Installer

    Aliases      : No Aliases

    Type/Size    : File/8340

    Clone        : No Clones

    Symptoms     : No Symptoms

    Discovered   : ?

    Way to infect: No infection

    Rating       : Less dangerous

    Kickstarts   : 1.2/1.3

    Damage       : Installs the East Star Virus im memory.

    Manifestation: -

    Removal      : Delete File

    Comments     : The EastStar Installer was linked together
                   with NComm. This Link was created by using
                   Hunklab. If you are now starting the file
                   it first installs the EastStar virus in
```

```
                    memory.
A.D 02-94
```

1.4 electrovision

```
     Name         : Electro Vision

     Aliases      : No Aliases

     Type/Size    : Boot/1024

     Original     : FORBIP

     Symptoms     : No Symptoms

     Discovered   : ?

     Way to infect: Boot infection

     Rating       : Less Dangerous

     Kickstarts   : 1.2/1.3

     Damage       : Overwrites boot.

     Manifestation: -

     Removal      : Install boot.

     Comments     : The Electro Vision Virus is another FORBIP-Clone.
                    So please look there for further information.

A.D 02-94
```

1.5 em-wurm

```
     Name         : EM-Wurm

     Aliases      : (Source:QuickInt PP-crunched length: 3196 Bytes)

     Type/Size    : Trojan/3888

     Incidence    : ?

     Discovered   : 23-05-91

     Way to infect: None, doesn't even survive reset

     Rating       : Very dangerous with  EM, EUROMAIL or EUROSYS devices
                    Else  harmless

     Kickstarts   : all
     Damage       : Overwrites euromail files
                    add one line in the startup-sequence
                    that calls a new program in the c: directory.
                    writes in c:$A0 length: 3888 Bytes ASCII-Textavailable
                    writes in 5th Byte of c:protect (when available) $01
                    Result: protect useless

     Manifestation: None

     Removal      : Delete it and check you startup-sequence

  General comments: Always virus check New files with more than one
                    Virus killer


JN 07.09.93
```

1.6 euromail

```
     Name         : Euromail

     Aliases      : EM-Wurm, AnitEuromail

     Type/Size    : Trojan/3888

     Clone        : No Clones

     Symptoms     : No Symptoms

     Discovered   : ?

     Way to infect: No infection

     Rating       : Dangerous

     Kickstarts   : 1.2/1.3/2.0

     Damage       : Damage Files.

     Manifestation: -

     Removal      : Delete file.

     Comments     : The Euromail virus is a dangerous virus. It
                    only becomes active, if one of the following drawers
                    exists: EM, EUROMAIL, EUROSYS.
                    If you are starting the virus, it tries to damage
                    the file c:protect. After that the virus creates
                    a file c:$A0 and modifies the startup-sequence
                    with $A0, $0A. The virus starts the process
                    "clipboard.device". All files in the above mentioned
                    drawers will be damaged. Such damaged files CANNOT
                    be repaired.
```

A.D 02-94

1.7 excrement

```
Name          : Excrement

Aliases       : No Aliases

Type/Size     : Boot/1024

Clone         : Sentinel

Symptoms      : The POWER-LED begins to behave strange.

Discovered    : ?

Way to infect: Boot infection

Rating        : Less dangerous

Kickstarts    : 1.2/1.3

Damage        : Overwrites boot.

Manifestation: -

Removal       : Install Boot.

Comments      : The Excrement-Virus uses the coolcapture-vector
                to stay resident in memory. Further the virus
                uses the DoIO()-Vector from the EXEC.library to
                infect other disks. The virus copies itself
                always to the same memory-adress ($7f400).
                In the bootblock you can read:

                "EXCREMENT"

                Depending of infections the POWER-LED begins to
                flash.
```

A.D 02-94

1.8 excrementinstaller

```
Name          : Excrement Installer

Aliases       : No Aliases

Type/Size     : File/1180

Clone         : No Clones
```

```
     Symptoms     : No Symptoms

     Discovered   : ?

     Way to infect: No infection

     Rating       : Less dangerous

     Kickstarts   : 1.2/1.3

     Damage       : Installs the Excrement Virus

     Manifestation: -

     Removal      : Delete File.

     Comments     : If you are starting the file, it installs the
                    Excrement virus in memory. Nothing more to say
                    about it.

A.D 02-94
```

1.9 excreminator_1-bomb.txt

```
==== Computer Virus Catalog 1.2: Excreminator_1 Bomb (31-July-1993) ====
Entry...............: Excreminator_1 Bomb
Alias(es)...........: ---
Virus Strain........: ---
Virus detected when.: ---
              where.: ---
Classification......: Bomb (=destructive program)
Length of Virus.....: Memory and media: 936 bytes
                      Media: 4 byte in "df0:Libs/Exec.library"
--------------------- 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.: 1) Typical text found in code:
                     dc.b 'ALL DRIVES FUCKED UP! LAME SUCKER !!!',0,1
                     dc.w $AA
                     dc.b $23,'Use a better Viruskiller next time!',0,1
                     dc.w $AA
                     dc.b $2D,'e.g. Excreminator II HAHAHA',0,0
                      2) There is a "startup-sequence" entry called
                         "Excreminator", and there is always a file
                         "Libs/Exec.library" with 4 byte length in
                         root directory.
Type of infection...: ---
Infection Trigger...: ---
Storage media affected: Floppy disks only
Interrupts hooked...: ---
Damage..............: Permanent damage: overwriting all floppy disks
                         with meaningless data.
Damage Trigger......: Starting this program when the byte in
```

```
                         "Libs/Exec.library" is zero.
Particularities.....: Programming the drive hardware directly.
Similarities........: ---
--------------------- Agents ------------------------------------------
Countermeasures.....: VirusZ 3.06, VT 2.54, VirusChecker 6.28
Countermeasures successful: VirusZ 3.06, VT 2.54
Standard means......: Delete the following files: "Excreminator" and
                         "libs/Exec.library", as well as the
                         "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 engineering of code
===================== End of Excreminator_1 Bomb ======================

          See the screendump of the  Excreminator1  virus!
```

1.10 executors

```
     Name         : Executors

     Aliases      : No ALiases

     Type/Size    : Boot/1024

     Original     : Disk Herpes

     Symptoms     : No Symptoms

     Discovered   : ?

     Way to infect: Boot infection

     Rating       : Dangerous

     Kickstarts   : 1.2/1.3/2.0

     Damage       : Overwrites boot/Overwrites Root-block.

     Manifestation: -

     Removal      : Install boot.

     Comments     : The Executors Virus is another Disk Herpes clone.
                    Only the texts were changed. For further informations
                    please look there.

A.D 02-94
```

1.11 exorcist

```
Name         : Exorcist

Aliases      : No Aliases

Type/Size    : Boot/1024

Original     : Alien New Beat

Symptoms     : No Symptoms

Discovered   : ?

Way to infect: Boot infection

Rating       : Dangerous

Kickstarts   : 1.2/1.3

Damage       : Overwrites boot.

Manifestation: -

Removal      : Install boot.

Comments     : The Exorcist Virus is another Alien New Beat Clone.
               Only the texts were changed. For further informations
               please look there.
```

A.D 02-94

1.12 express2.20

```
Name         : Express2.20

Aliases      : No Aliases

Type/Size    : AIBON Installer 194064 bytes
               Aibon (DestroyProgram) 776 bytes

Clone        : No Clones

Symptoms     : No Symptoms

Discovered   : ?

Way to infect: No infection

Rating       : very DANGEROUS !

Kickstarts   : 1.2/1.3/2.0/3.0

Damage       : Damage files.

Manifestation: -
```

Removal : Delete File.

Comments : If you are starting the virus it tries to copy Aibon to ":s". Then the virus modifies the startup-sequence with the virusname. After all changings were successful all files in "sys:" will be cut to 42 bytes.
This files CANNOT be repaired. The virus checks for "bbs:", too. If existing ALL files will be first destroyed there.

ADVICE:

a) Delete s/Aibon

b) Delete Express2.20

c) Change your Startup-Sequence (!)

A.D 02-94

1.13 extreme

Name : Extreme

Aliases : No Aliases

Type/Size : Boot/1024

Clone : ZACCESS 3, PRIMAVERA, FAT2

Symptoms : No Symptoms

Discovered : ?

Way to infect: Boot infection

Rating : Dangerous

Kickstarts : 1.2/1.3

Damage : Overwrites boot/Destroys Disk(s).

Manifestation: -

Removal : Install boot.

Comments : The Extreme virus uses the kick vectors to stay resident in memory. To infect other disks the virus uses the DoIO()-Vector from the exec.library. When a special value reaches 0 the virus start a quickformat routine and shows the following alert:

```
                    THE EXTREME ANTI-VIRUS  HA HA !!!
                       BACK TO LIVE BACK TO REALITY
               SICO DE MOEL  BERGERWEG 100  CALL 072-114816

A.D 02-94
```