# VListF

Torben Bilbo" Maciorowski"

| COLLABORATORS | | | |
|---|---|---|---|
| | *TITLE* :<br><br>VListF | | |
| *ACTION* | *NAME* | *DATE* | *SIGNATURE* |
| WRITTEN BY | Torben Bilbo"<br>Maciorowski" | October 17, 2022 | |

| REVISION HISTORY | | | |
|---|---|---|---|
| NUMBER | DATE | DESCRIPTION | NAME |
| | | | |

# Contents

# Chapter 1

# VListF

## 1.1 VIRUSES - F

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

F.I.C.A. Virus

Fast 1

Fast 2

Fast Eddie

FAT 1

FAT 2

FileGhost

Flashback

Forpib

Freedom

Freshmaker

Frity

Fuck.device

Fuck virus

Future Disaster

## 1.2 fica-virus.txt

```
========= Computer Virus Catalog 1.2: FICA Virus (31-July-1993) ========
Entry..............: FICA Virus
Alias(es)..........: ---
Virus Strain.......: ---
Virus detected when.: ---
              where.: ---
Classification.....: System virus (bootblock infector), RAM resident
Length of Virus.....: 1.Length on storage medium: 1024 bytes
                      2.Length in RAM:            2304 bytes
--------------------- Preconditions -----------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: 1.2/all, 1.3/all, 2.0/all
Computer model(s)...: All models
--------------------- Attributes --------------------------------------
Easy Identification.: The following text is found in virus/RAM:
                "Hey ROB of QUARTEX! Your mouth is getting bigger
                 every day, while your work is becoming worse
                 and worse (soon you''ll reach ABAKUSS-level) !
                 You claim to be THE VERY BEST - but you perform
                 loser cracks (look at your version of SPACE ACE)!
                 Have we EVER seen a TRAINER or an INTRO from you
                 (except the CLI-type command in combination with
                 ridiculous poems)? Fuck off, lame bastard!
                 F.I.C.A RULES!"
Type of infection...: RAM resident, reset resident, bootblock infector
Infection Trigger...: Booting from an infected disk, reset afterwards
Storage media affected: Only floppy disks
Interrupts hooked...: Following vectors are changed: KickTagPtr,
                         KickCheckSum, SumKickData and BeginIO
                         of the trackdisk.device.
Damage.............: Permanent damage: overwriting bootblock.
Damage Trigger......: Using BeginIO on Sector zero
Particularities.....: Once in action, virus tries to fool the user
                         and shows a clean bootblock, instead of
                         his infected one.
Similarities........: ---
--------------------- Agents ------------------------------------------
Countermeasures.....: VirusZ 3.06, VT 2.54, VirusChecker 6.28
Countermeasures successful: VirusZ 3.06, VT 2.54
                       (VirusChecker 6.28 diagnoses that there is no
                        standard bootblock)
Standard means......: 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 virus code
==================== End of  FICA Virus ================================
```

## 1.3 fast1

Name : F.A.S.T. 1

Aliases : No Aliases

Type/Size : Boot/1024

Clone : No Clones

Symptoms : An alert will be shown

Discovered : ?

Way to infect: Boot infection

Rating : Harmeless

Kickstarts : 1.2/1.3

Damage : Overwrites boot.

Manifestation: -

Removal : Install boot.

Comments : The F.A.S.T. 1 Virus is a very harmless virus. It always copies itself to the same memory address ($7f000). It patches the DoIO() and FreeMem()-Vector. The DoIO()-Patch is used to infect other disks and the FreeMem()-Patch sets the coolcapture always to the virusvalue.

After 16 Infections an alert will be shown:

W A R N I N G

If you pirate software you are a thief.
Thieves will be prosecuted.
Any information should be passed to:
The Federation Against Software Theft
Telephone: +44-1-240-6756

P I R A C Y I S T H E F T

You cannot read this alert in the bootblock because its always coded depending of on byte from $DFF006. The virus only infects your disk if you are trying to write a bootblock on it. In the decoded bootblock you can read the following text:

Note to Paranoimia: The early release of X-Out was no exception so stop pretending that you "help" us by delaying cracks.

A.D 02-94

See the screendump of the FAST virus!

## 1.4 fast2

Name : F.A.S.T. 2

Aliases : No Aliases

Type/Size : Boot/1024

Clone : No Clones

Symptoms : An alert will be shown

Discovered : ?

Way to infect: Boot infection

Rating : Harmeless

Kickstarts : 1.2/1.3

Damage : Overwrites boot.

Manifestation: -

Removal : Install boot.

Comments : The F.A.S.T. 2 Virus is very similar to the F.A.S.T. 1 Virus. Only the viruscode was changed a little bit. Please read F.A.S.T. 1 for further information.

A.D 02-94

## 1.5 fasteddie

Name : Fast Eddie

Aliases : Some of the code are very like the Glastnost virus

Type/Size : BB/1024

Incidence : ?

Discovered : 17-07-91 Copenhagen, Denmark by Bo Krohn

Way to infect: Over Bootblock

Rating : Less Dangerous

```
    Kickstarts   : 1.2  1.3

    Damage       : Destroy Bootblock and block 100 on disks

    Manifestation: The processor stops after 15 or 20 minutes.
                   The Fast Eddie virus writes its own BB and writes
                   in block 100: "Fast Eddie". This block is
                   permanently damaged. The infected disk is renamed to:

                   "This disk is infected (HE-HE)".


                   Decode in memory you will find :
                   "Call 43-444304 and ask for HENRIK HANSEN (FAST EDDIE)".

                   In fact I know this man and can say, that he had never
                   done this virus because he can't code al all. Proably
                   the virus is done like a revenge or malice of the man,
                   who is a very wellknown "swapper" from the "Paradox"
                   demo group.


                   ATTENTION: This virus is a mutation virus, that means
                   that the code are changing every time, when a new disk
                   is infected.


    Removal      : Install the bootblock


 General comments: Always remember to write protect your disk !


ELS 11.93
```

## 1.6 fat1

```
    Name         : FAT 1

    Aliases      : Stinkbomb 1

    Type/Size    : Boot/1024

    Original     : Time Bomb

    Symptoms     : No Symptoms

    Discovered   : ?

    Way to infect: Boot infection

    Rating       : Dangerous!

    Kickstarts   : 1.2/1.3/2.0
```

```
     Damage       : Formats Root-Block.

     Manifestation: -

     Removal      : Install boot.

     Comments     : The FAT 1 virus is a Timebomb-Clone.
                    So please look there for further information.

A.D 02-94
```

## 1.7 fat2

```
     Name         : FAT 2

     Aliases      : Stinkbomb 2

     Type/Size    : Boot/1024

     Original     : Extreme

     Symptoms     : No Symptoms

     Discovered   : ?

     Way to infect: Boot infection

     Rating       : Dangerous!

     Kickstarts   : 1.2/1.3

     Damage       : Damages Disk(s)

     Manifestation: -

     Removal      : Install boot.

     Comments     : The FAT 2 virus is a EXTREME-Clone.
                    So please look there for further information.

A.D 02-94
```

## 1.8 fileghost

```
     Name         : FileGhost

     Aliases      : Friend (?)

     Clones       : -

     Type/Size    : Link/872
```

```
Symptoms     : -

Discovered   : 11/93

Way to Infect: Link infection

Rating       : Less Dangerous (Many Infections !!)

Kickstarts   : 2.0/3.0 with & without cachet !

Damage       : -

Manifestation: -

Removal      : Use good viruskiller or delete infected programms.

Comments     : It uses the LoadSeg and the NewLoadSeg
               to get the names of all executed programms.
               Then it links itself behind the 1. Hunk by
               searching a RTS. (Just as Crime)

               The virus just infects files which are:

               - executeable
               - smaller than 100000 bytes
               - don't have a "-" or a "." in their names.

               The virus doesn't infect libraries and handlers
               In the virus there is a coded message:

               "Hi Friend! Don't worry... it's only the FileGhost"

               The virus isn't resident.
               A trojan is spread around which installs this virus.
               (HardSpeeder - please look there !!)
               ATTENTION: HD-Users! Be careful with this virus.
               ^^^^^^^^^  It infects files VERY FAST !!!
                          And because of the short length, the virus
                          doesn't conspicuous.
```

A.D 12-93

## 1.9 flashback

```
Name         : FLASHBACK

Aliases      : No aliases

Type/Size    : Boot/1024

Original     : Glasnost

Symptoms     : No Symptoms
```

```
     Discovered   : ?

     Way to infect: Boot infection

     Rating       : Dangerous!

     Kickstarts   : 1.2/1.3

     Damage       : Overwrites Boot, destroys sectors.

     Manifestation: -

     Removal      : Install boot.

     Comments     : The Flashback virus is a Glasnost-Clone.
                    So please look there for further information.

A.D 02-94
```

## 1.10 forpib.txt

```
====== Computer Virus Catalog 1.2: FORPIB Virus (31-January-1992) =====

Entry..............: FORPIB Virus
Alias(es)..........: ---
Virus Strain.......: BYTE BANDIT Virus Strain
Virus detected when.: JANUARY 1990
               where.: Elmshorn, Germany
Classification.....: System virus (bootblock), resident
Length of Virus.....: 1. Length on storage medium: 1,024 byte
                      2. Length in RAM           : 1,024 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: " - FORPIB - 09.88 - No 197102 - "
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
Media affected......: only floppy disk (3.5" and 5.25")
Interrupts hooked...: vertical blank interupt
Damage..............: Permanent damage: overwriting bootblock, maybe
                         destroying opened files when screen and key-
                         board are shut off and the user has to restart
                         system using CONTROL+LEFT-AMIGA+RIGHT-AMIGA
                      Transient damage: screen buffer manipulation:
                         screen becomes dark, keyboard seems to mal-
                         function; transient damage may be interrupted
                         by pressing special key combination:
```

```
                        LEFT-ALT+LEFT-AMIGA (on newer AMIGAS the
                        COMMODORE key)+SPACE+RIGHT-AMIGA+RIGHT ALT
                        (but the virus will still be active)
Damage Trigger......: Permanent damage: reset; 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 (approx. 7 minutes)
Particularities.....: uses StartIOVector; other resident programs using
                        the system resident list (KickTagPointer,
                        KickMemPointer) are shutdown
                      Copy counter: 19th word
Similarities........: BYTEBANDIT virus strain
--------------------- Agents ----------------------------------------
Countermeasures.....: Names of tested products of Category 1-6:
                      Category 1: .2 Monitoring System Vectors:
                                          CHECKVECTORS 2.2
                                  .3 Monitoring System Areas:
                                     CHECKVECTORS 2.2,GUARDIAN 1.2,
                                        VIRUSX 4.0
                      Category 2: Alteration Detection: --
                      Category 3: Eradication: CHECKVECTORS 2.2,
                                               VIRUSX 4.0
                      Category 4: Vaccine: ---
                      Category 5: Hardware Methods: ---
                      Category 6: Cryptographic Methods: ---
Countermeasures successful: CHECKVECTORS 2.2,GUARDIAN 1.2,VIRUSX 4.0
Standard means......: CHECKVECTORS 2.2
--------------------- Acknowledgement -------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Wolfram Schmidt
Documentation by....: Wolfram Schmidt
Date................: 1-NOVEMBER-1991
Information Source..: ---
===================== End of FORPIB-Virus ============================
```

## 1.11 freedom

```
Name         : Freedom

Aliases      : No Aliases

Type/Size    : Bomb/10876

Clones       : No Clones

Symptoms     : No Symptoms

Discovered   : ?

Way to infect: Boot infection

Rating       : Less Dangerous

Kickstarts   : 1.2/1.3
```

```
Damage       : Damage tracks.

Manifestation: Pretend to be viruskiller.

Removal      : Delete file.

Comments     : If you are starting the Freedom-Virus it gives
               out the following CLI-Message :

               Freedom!  By Steve Tibbett
               Checking df0: for 126 viruses.

               In fact the virus destroys tracks on the disk.
               (Block 5, 10, 15, 20...). Such damaged tracks
               CANNOT be repaired.
               After delays the virus gives out:

               SADDAM-Virus removed !
               or
               SMILY CANCER-Virus removed !
```

A.D 02-94

## 1.12 freshmaker

```
Name         : Freshmaker

Aliases      : No Aliases

Type/Size    : Boot/1024

Clones       : No Clones

Symptoms     : An alert message appear.

Discovered   : ?

Way to infect: Boot infection

Rating       : Less Dangerous

Kickstarts   : only Kick 1.3 with RangerRAM ($c00000)

Damage       : Overwrites boot.

Manifestation: -

Removal      : Install boot.

Comments     : This is another simple bootblockvirus. It
               uses the coolcapture-vector to stay resident in
               memory. Furthermore the Findresident(),
               Supervisor() and the DoIO() vectors are changed.
               Just as always, the DoIO()-Vector is used to
```

```
                    infect other disks. After 10 infections, the virus
                    gives out the following alert:

                    ES IST WIRKILCH NICHT ZU GLAUBEN.
                    DU BOOTEST MIT EINER UNGESCHÜTZTEN DISK !
                    ES IST WIRKLICH SCHADE (!), DAß ES SOLCHE
                    LAMER (!) NOCH GIBT. DU HAST WOHL KEINE
                    ANGAS VOR VIREN ??? ICH WÜNSCHE DIR
                    NOCH VIEL SPAß (!) MIT DEINEM AMIGA...
                    UNTERZEICHNET: THE FRESHMAKER IN 1991 !

A.D 03-94
```

## 1.13 frity

```
     Name          : Frity

     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 Frity Virus is another FORBIP-Clone.
                     So please look there for further information.

A.D 02-94
```

## 1.14 fuck.device

```
     Name          : Fuck.Device

     Aliases       : No Aliases

     Type/Size     : Boot/1024
```

```
     Clones       : No Clones

     Symptoms     : No Symptoms

     Discovered   : ?

     Way to infect: Boot infection

     Rating       : Dangerous

     Kickstarts   : 1.2/1.3/2.0

     Damage       : Overwrites boot.

     Manifestation: -

     Removal      : Install boot.

     Comments     : The Fuck.Device virus uses the coolcapture
                    vector to stay resident in memory. It changes
                    the DoIO()-Vector to infect other disks.
                    Depending of a value the virus infects other disks
                    OR destroys Block 0+1 and 2+3 with the string
                    "fuck.device".

A.D 02-94
```

## 1.15 fuck-virus

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.

```
------------------------------------------------------------------------------
                                  FUCK virus
------------------------------------------------------------------------------

Type: File (Trojan)

Alias: MODEMCHECK

Origin: Modemchecker in MCheck.lha

Infect: C:LoadWB

Short: Destroys contents of harddisks


Long:

MCheck.lha (size: 16772 bytes) contains
```

```
  Modemcheck.doc  (size: 2227)
  Modemchecker    (size: 15516, version: V1.1 (07.05.93))
```

Modemchecker is packed with CrunchMania. Unpacked size is 22252 bytes.

Modemchecker is a phony. It pretends to check various modem lines (CTS, CD, DTR, RT, TXD, RXD, RTS), but it reports success no matter what (even if no modem is attached.) When Modemchecker is started it will write the virus to C:LoadWB (new size is 3604 bytes.) Next time C:LoadWB is started (typical at startup) the virus will become active.

The virus in LoadWB launches a new task using CreateProc. The new task is called Diskdriver.proc (stack = 4096, priority = 0). Afterwards it proceeds with the original LoadWB ("$VER loadwb 38.9 (30.3.92)",10,13,0).

The Diskdriver.proc task is the malicious part. It waits for 30000 ticks (ticks/50 seconds for PAL, equals 10 minutes, ticks/60 for NTSC), when it fills an internal buffer of 150000 bytes (allocated by a BSS section (HUNK_BSS)) with FUCKFUCKFUCK... It tries to open a file called S:HORSE. If it was successful the virus will gracefully exit, if not it will cause havoc. It will examine all physical devices (dn_Type = DLT_DEVICE), and pick out all where

```
  (de_numheads > 2) OR (de_uppercyl >= 90) OR (de_blkspertrack > 22)
```

Then it will write the content of the internal buffer (FUCKFUCK...) on all track from the lowest cylinder (de_lowcyl) to the highest cylinder (de_yppercyl) of all selected devices (typical harddisks). When it exits.

Observations:

The programming style is pretty clean which indicates a rather experienced programmer. He’s probably from Europe (30000 ticks yields exactly 10 minutes by 50Hz powersupplies.)

S:HORSE seems to be a safety line for the programmer (and his friends (if he has any :-))

It doesn’t destroy ordinary floppy disks.

Destruction is performed at exec.library level (using DoIO)

Notes:

Some uncorrect things have been said about the FUCK virus.

```
 "The ’LoadWB’ that contains the virus is the 2.1 version, so the virus
  isn’t danger for any machine with 1.2 or 1.3."
  [1]
 "Before the infection begins a couple of tests is run:
  - execversion = 37.132 = KS2.04 . If no there’s NO infection. The program
    just stops. This means no danger to owners of A600, A600HD and so on."
  [2]
```

Deadly wrong! Even though LoadWB will fail because it requires at least V36

(dos.library) it has already at this point launched the virus, which doesn't require any particular version of the OS. I tested this on 1.2, and the Diskdriver.proc was running.

"Once installed at the boot Fuck Virus will wait patiently and if not IDCMP message of any type is registered [...] 10 minutes, it will proceed..." [1]
"7. This trojan "loadwb" will start the horrible damage, if you don't use your keyboard 10 minutes." [3]

The havoc start (provided S:HORSE wasn't found) after approx. 10 minutes (30000 ticks) no matter what IDCMP messages is registered. It doesn't care about user interaction.

Casual filling of the tracks [4]

Data isn't destroyed randomly, but very systematically. From the lowest cylinder to the highest. The reason why it seems random is probably due to the fragmentation of the harddisk.

[1] FuckVirus.doc by Gabriele Greco, author of FuckChecker (Fuckchck.lha).
[2] VT.Knows by Heiner Schneegold, author of VT.
[3] VirWarn-1b by Erik Loevendahl Soerensen.
[4] Everybody, except me ;-)

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.

## 1.16 futuredisaster

Name : Future Disaster

Aliases : No Aliases

Type/Size : Boot/1024

Clones : No Clones

Symptoms : No Symptoms

Discovered : ?

Way to infect: Boot infection

Rating : Dangerous

```
Kickstarts   : ONLY 1.2

Damage       : Overwrites boot/ Damages RootBlock.

Manifestation: -

Removal      : Install boot.

Comments     : The Future Disaster-Virus is a simple boot-
               blockvirus. It uses the coolcpature vector to
               infect other disks. Furthermore the BeginIO()-
               and DoIO() vector is used to infect other disks.
               If a value reaches 7 it destroys the RootBlock
               (880 only DD-Disk.) of the current disk by
               writing the memorycontens of $7FB00.

               Advice from me : Try Disksalv2 or 1. Most of
               ^^^^^^^^^^^^^^   the damaged DATA will be repaired.
```

A.D 03-94