VListJ

Torben Bilbo" Maciorowski"

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

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VListJ

1.1 VIRUSES - J

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


            Jeff Butonic 1.31

            Jeff Butonic 3.00

            JITR

            Joshua
```

1.2 jeffbutonic1.31

```
Name          : Jeff Butonic 1.31

Aliases       : No Aliases

Clone         : Aids, Jeff V4.55

Type/size     : File/3408

Symptoms      : Shows an alert

Discovered    : ?

Way to infect: File infection

Rating        : Less Dangerous

Kickstarts    : 1.2/1.3/2.0 BUT: only DD-Disks !!!

Damage        : No Damage.
```

```
Manifestation: Pretend to be useful cli-command.

Removal      : Delete file.

Comments     : When you are starting the JeffV1.31 virus it
               first decodes itself with a eor-loop. After
               that it tries to allocate 3500 bytes memory,
               makes itself resident by changing the kick-vectors,
               installs a patch in $6c.s (Zero-Page!) and
               finally patches the DoIO()-Vector from EXEC.LIB.
               The DoIO()-Vector is used to infect other disks.
               If you are inserting an unprotected disk, the
               virus scans the root-block of it ($6E000 = only
               DD-Disks!!!) and tries to create the virusfile
               and to modifiy the startup-sequence. No DOS-functions
               , like Open(), write() and so on
               are used (!!). The virus creates the virusfile
               with different names:

               "AddBuffers 20"
               "Add21K"
               "Fault 206"
               "break 1 D"
               "changetaskpri 5"
               "wait"~~~
               "Arthus"
               "Helmar"
               "Aloisius"

               Sometimes the widow-title changes and following
               messages will appear:

 Ich brauch jetzt'n Bier!
 Stau auf Datenbus bei Speicherkilometer 128!
 mehr Buszyklen für den Prozessor!
 Ein dreifach MITLEID für Atari ST!
 BUTONIC!
 Schon die Steinzeitmenschen benutzten MS-DOS...einige sogar heut
 noch!
 Schon mal den Sound vom PS/2 gehört???
 PC/XT-AT: Spendenkonto 004...
 Unabhängigkeit & Selbstbestimmung für den Tastaturprozessor!
 Paula meint, Agnus sei zu dick.
 IBM PC/XT: Ein Fall für den Antiquitätenhändler...
 Sag mir, ob du Assembler kannst, und ich sage dir, wer du bist.

               Depending of $DFF006 , the virus gives out the
               following alert:

       Einen ganz wunderschönen guten Tag!
 * I am JEFF - the new Virus generation on Amiga *
            (w) by the genious BUTONIC.
      V 1.31/05.11.88 - Generation Nr.00053
Greetings to * Hackmack *,* Atlantic *, Wolfram, Frank,
Miguel, Alex, Gerlach, and to the whole Physik-LK from MPG !!
```

```
                    *  There have come a new Jeff Butonic 1.31 clone
                       too (the same lenght 3408 bytes), but with a
                       changed display alert:


                       Es tut mir leid es ihnen zu sagen !
                       *Ihr computer hat AiDS ein neuer Virus*
                       Gemacht von Donald & Micky
                       IM Jahre 1992 - Generation Nr.05426
                       Grüße gehen an : Metalwarrior - Mozart -
                       Tiger 1 - Poge
                       Außerdem noch an : Meinen Virus-Freund David
                       Hasselhoff !

                       AND THE FOLLOWING TEXT ON THE SCREEN:

                       Tina zeig mir deine Votz
                       Hey du Depp am Computer ! was is ?
                       Hilfe die NFL-Kappen Kommen !
                       Redskins - Fickt euch alle !!!
                       Evil C !
                       Der Vorkotzer er will nicht kotzen !!
                       Rechtfertige er sich !
                       Easy and fast-- Schnebber-Pax !!
                       Burger du Drecksack !!
                       Popper überfährt man mit einem Chopper !!
                       Rod Grod Med Flod !!
                       Fuck for oil And for NLF-Deppen !!
                       Ihr Assigen NFL-Ficker ihr seid alle schwul
                       und dumm !!

          See the screendump of the  JeffV1.31          virus!

ELS 11-93/
A.D 02-94
```

1.3 jeff-butonic-3.txt

```
== Computer Virus Catalog 1.2: JEFF BUTONIC 3.0 Virus (10-Feb-1991) ==

Entry..............: JEFF BUTONIC 3.0 Virus
Alias(es)..........: ---
Virus Strain.......: ---
Virus detected when.: ---
              where.: North Germany
Classification.....: link virus (directory type), resident
Length of Virus.....: 1. length on storage medium: 2916 byte
                      2. length in RAM           : 2876 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: ---
```

```
                        identification by the following entry (invisible
                           in ASCII editors) in startup-sequence as 1st
                           entry: "$A0,$A0,$A0,$20,$9B,$41";
                        identification using a disk manager: a file
                           $A0,$A0,$A0 (invisible) exists in root
                           directory, with length=2916 byte;
                        identification by text in memory: "Hi. Jeff's
                           speaking here... (w) by the genious BUTONIC...
                           V3.00/9.2.89 - Gen.0026 Greetings to
                           *Hackmack*,*Atlantic*, & Alex,Frank,Wolfram,
                           Gerlach,Miguel,Klaus,Snoopy-Data!"; this
                           text is displayed as alert message after
                           destruction of a disk structure;
                        identification by transient damage: window
                           titles are changed to following ones: "Ich
                           Brauch jetzt Alk!", "Bitte keinen Wodka!",
                           "Mehr Buszyklen fuer den Prozessor", "Paula
                           meint, Agnus sei zu dick"
Type of infection...: self-identification method: virus searches for
                           the following entry in startup-sequence:
                           $A0,$A0,$A0,$A0,$9B,$41 (invisible in ASCII
                           editors);
                        system infection: RAM resident, reset resident
Infection Trigger...: using unprotected disk-like devices
Storage media affected: all bootable and disk-like devices
Interrupts hooked...: ---
Damage..............: permanent damage: destroys directory structure;
                        transient damage: manipulation of window titles;
                           alert message after destroying the structure
                           of a bootable device
Damage Trigger......: permanent damage: (to be analysed)
                        transient damage: (to be analysed)
Particularities.....: DoIO vector and KickTag pointer are misused
Similarities........: author of this virus evidently knows BGS virus
---------------------- Agents ----------------------------------------
Countermeasures.....: Names of tested products of Category 1-6:
                        Category 1: .2 Monitoring System Vectors:
                                       CHECKVECTORS 2.3, VT 1.94
                                    .3 Monitoring System Areas:
                                       CHECKVECTORS 2.3, GUARDIAN 1.2,
                                       VIRUS-DETEKTOR 1.1, VT 1.94
                        Category 2: Alteration Detection: ---
                        Category 3: Eradication: CHECKVECTORS 2.3,
                                    BGS9-PROTECTOR, VIRUS-DETEKTOR 1.1
                        Category 4: Vaccine: BGS9-PROTECTOR
                        Category 5: Hardware Methods: ---
                        Category 6: Cryptographic Methods: ---
Countermeasures successful: CHECKVECTORS 2.3, VT 1.94
Standard means......: CHECKVECTORS 2.3 or VT 1.94 with deletion of
                        "no name" file entry (see above) with a disk
                        manager and correction of the startup-sequence
---------------------- 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 JEFF BUTONIC 3.0 Virus ================

          See the screendump of the  JeffV3.00  virus!
```

1.4 jitr.txt

```
====== Computer Virus Catalog 1.2: JITR Virus (10-February-1991) =====

Entry..............: JITR Virus
Alias(es)..........: ---
Virus Strain.......: ---
Virus detected when.: AUGUST 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
--------------------- Attributes ------------------------------------
Easy Identification.: typical text: "JITR" at 3rd bootblock longword,
                        and "Copy count :", "I'm a safe virus! Dont
                        kill me! I want to travel! And now a joke :
                        ATARI ST   This virus is a product of JITR"
                        at the end of bootblock
Type of infection...: self-identification method: testing 2nd longword
                        (=>bootblock checksum for matching own one);
                      system infection: RAM resident, reset resident,
                                        bootblock
Infection Trigger...: every access to unprotected disks
Storage media affected: only floppy disks (3.5" and 5.25")
Interrupts hooked...: ---
Damage..............: permanent damage: overwriting bootblock
                      transient damage: ---
Damage Trigger......: permanent damage: every access to unprotected
                                        disks
Particularities.....: a resident program using the CoolCaptureVector
                        is shutdown, DoIO is modified and points to
                        virus DoIO routine first;
                      JITR seems to be shortest AMIGA virus, occupying
                        only 498 byte of bootblock, though 1024 bytes
                        are allocated in RAM;
                        copy counter at offset $017A
Similarities........: ---
--------------------- 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-KILLER 1.1
                      Category 2: Alteration Detection: ---
                      Category 3: Eradication: CHECKVECTORS 2.2,
                                               VIRUS-DETEKTOR 1.1
```

```
                      Category 4: Vaccine: ---
                      Category 5: Hardware Methods: ---
                      Category 6: Cryptographic Methods: ---
Countermeasures successful: CHECKVECTORS 2.2, 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 JITR Virus ============================
```

1.5 joshua.txt

```
======== Computer Virus Catalog 1.2: JOSHUA Virus (5-June-1990) =======
Entry...............: JOSHUA Virus
Alias(es)...........: ---
Virus Strain........: ---
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.: ---
Type of infection...: self-identification method: testing value of
                        adress the vertical blank interrupt vector
                        is pointing to plus 480 byte, if matching
                        hex. $2029002C (MOVE.L 44(A1),D0 ) -> start
                        of the infection part of the virus
                      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 (IV 5)
Damage..............: permanent damage: overwriting bootblock
                      transient damage: unknown yet
Damage Trigger......: permanent damage: reset
                        operation: any disk access
                      transient damage: 6th infection
Particularities.....: other resident programs using the system resident
                        list (KickTagPointer,KickMemPointer) are shut
                        down; uses BeginIO() routine.
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...: Wolfram Schmidt (still working on it)
Documentation by....: Alfred Manthey Rojas
Date................: 5-June-1990
Information Source..: ---
====================== End of JOSHUA-Virus ============================
```