VListI

Torben Bilbo" Maciorowski"

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

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VListI

1.1 VIRUSES - I

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


              Ice

              Iceman And IRQ

              Incognito

              Infiltrator

              Inger IQ

              InterLamer

              Intro-Maker by TRC

              IRQ
```

1.2 ice.txt

```
======= Computer Virus Catalog 1.2: ICE Virus (10-February-1991) =====
Entry..............: ICE Virus
Alias(es)..........: ---
Virus Strain.......: SCA strain
Virus detected when.: JUNE 1990     (when VTC received virus code)
               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: "Greets from The Iceman & The IRQ
                        The REAL Amiga hackers! hi to Red Sector Club
                        Creole, Sendarian, & SCA!! for the best
                        cracks/imports contact THE ICE BREAKERS", and
                        "INC!!INC!INC!INC!INC!INC!INC!INC!"
                      virus feature: pressing left mouse/fire button of
                        port 1 during system reboot causes screen to
                        become green and virus to shutdown itself by
                        clearing ColdCapture and CoolCaptureVector
                        (="suicide function")
Type of infection...: self-identification method: testing 3rd longword
                        for matching string "CHW!"
                      system infection: RAM resident, reset resident,
                                        bootblock
Infection Trigger...: reset (CONTROL+Left-AMIGA+RIGHT-AMIGA)
Storage media affected: only floppy disks (3.5" and 5.25")
Interrupts hooked...: ---
Damage..............: permanent damage: overwriting bootblock
                      transient damage: screen buffer manipulation:
                        screen becomes black, message (see above) is
                        displayed by fading in and out peaces of it
Damage Trigger......: permanent damage: reset
                      transient damage: 15th infection
Particularities.....: a resident program using the CoolCaptureVector
                        is shutdown; using the ColdCaptureVector
                        when virus is shutdown by its suicide
                        function
Similarities........: SCA virus strain
--------------------- 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: SCA-PROTECTOR 1.0,
                                           VIRUS-DETEKTOR 1.1
                      Category 5: Hardware Methods: ---
                      Category 6: Cryptographic Methods: ---
Countermeasures successful: CHECKVECTORS 2.2, GUARDIAN 1.2,
                            VIRUS-DETEKTOR 1.1, SCA-PROTECTOR 1.0;
                            own suicide function
Standard means......: CHECKVECTORS 2.3
--------------------- Acknowledgement --------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Oliver Meng
Documentation by....: Alfred Manthey Rojas
Date................: 10-February-1991
Information Source..: ---
==================== End of Ice Virus ================================
```

1.3 iceman-and-irq.txt

```
==== Computer Virus Catalog 1.2: ICEMAN AND IRQ Virus (20-FEB-1993) ====
Entry...............: ICEMAN AND IRQ Virus
Alias(es)...........: ICE Virus
Virus Strain........: SCA virus strain
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, 2.0/all
Computer model(s)...: All models
---------------------- Attributes --------------------------------------
Easy Identification.: Typical text: "Greets from The Iceman & The IRQ"
                                    "The REAL Amiga hackers! hi to "
Type of infection...: Self-identification method: testing 3rd longword
                                    for matching string "CHW!"
                      System infection: RAM resident, reset resident,
                                    bootblock
Infection Trigger...: Reset
Storage media affected: Only floppy disks (3.5" and 5.25")
Interrupts hooked...: ---
Damage..............: Permanent damage: overwriting bootblock
                      Transient damage: screen buffer manipulation:
                                    screen becomes black, message
                                    (see above) is shown by
                                    fading in and out pieces of it.
Damage Trigger......: Permanent damage: reset
                      Transient damage: 15th infection
Particularities.....: Any resident program using the CoolCaptureVector
                        is shut down, also when using ColdCaptureVector
                        when virus is shutdown by its `suicide` function
Similarities........: SCA virus family
---------------------- 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...: Jens Vogler
Documentation by....: Jens Vogler
Date................: 14th December 1992
Information Source..: Virus Analysis
====================== End of ICEMAN AND IRQ Virus ======================
```

1.4 incognito.txt

```
====== Computer Virus Catalog 1.2: INCOGNITO Virus (25-July-1992) =====
Entry...............: INCOGNITO Virus
Alias(es)...........: ---
Virus Strain........: ---
```

```
Virus detected when.: Unknown
              where.: Unknown
Classification......: System virus (bootblock), resident
Length of Virus.....: 1. Length on storage medium: 1024 byte
                      2. Length in RAM:            1172 byte
--------------------- Preconditions ---------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: 1.2/33.166, 1.2/33.180
Computer model(s)...: All models
--------------------- Attributes ------------------------------------
Easy Identification.: ---
Type of infection...: RAM resident, reset resident, bootblock
Infection Trigger...: INT[5] = Vertical Blank Interrupt
Storage media affected: Only floppy disks (3.5" and 5.25")
Interrupts hooked...: INT[5] = Vertical Blank Interrupt
Damage..............: Overwriting bootblock
Damage Trigger......: INT[5] = Vertical Blank Interrupt
Particularities.....: Changes DoIO vector; de/encrypts string
                         "trackdisk.device" by longword-addition
                         and subtraction with #$90154354
Similarities........: ---
Particularities.....: First AMIGA virus using encryption techniques,
                         though not very complex.
--------------------- Agents ----------------------------------------
Countermeasures.....: GUARDIAN 1.2, VIRUSX 4.0, VIRUSCONTROL 2.0
Countermeasures successful: GUARDIAN 1.2, VIRUSX 4.0, VIRUSCONTROL 2.0
Standard means......: VIRUSCONTROL 2.0
--------------------- Acknowledgement -------------------------------
Location............: Virus Test Center, University Hamburg, FRG
Classification by...: Karim Senoucci
Documentation by....: Karim Senoucci
Date................: 7-July-1992
Information Source..: ---
====================== End of INCOGNITO-Virus ========================
```

1.5 infiltrator

```
     Name         : Infiltrator

     Aliases      : Klein virus

     Type/Size    : Link/1052 bytes

     Incidence    : Used to infiltrate a BBS?

     Discovered   : By mr Peter Klein, Denmark 20-06-92

     Way to infect: When you are executing a infected program

     Rating       : Dangerous

     Kickstarts   : 2.04 - ?

     Damage       : Links to other programs.
```

```
     Manifestation: Decoded you can read: This is the Infiltrator!

     Removal      : Delete the infected program or link part

  General comments: Infected files are increased by 1052 bytes. This link
                    virus have been very fast spreaden in Sweden and
                    Denmark. I have got report by at least 6 infected
                    harddisks whithin 2 days 20-06-92. The origin virus
                    is spreaden by a fake DiskMaster 2.0+ (DM2.0+lha).


                    The Infiltrator virus patches the 2.0 DOS LoadSeg
                    vector and infects any files loaded by this routine;
                    fonts, libraries and executables. Infected fonts or
                    libraries can't be opened. The Infiltrator link
                    virus cann't patch the 1.3 LoadSeg.


                    The Infiltrator virus also scans for a file called
                    'user.data' and upon finding it performs some
                    (presumably) horrid action, watch out for this file
                    on your harddisk or bulletin board and tries to
                    infect: libs, devices and so on

                    NOTE. The virus is able to link the same file
                    additional times too!!! by the consequence: NOT ALL
                    infected files are able to run !!!


                    (I haven't had time to find out what it really does).


                    The virus does not survive a reset, so it's not very
                    dangerous to floppy users, but it is also very hard to
                    detect for for example Action Replay, though you will
                    get a report a suspicious LoadSeg vector (dos.library
                    offset -150).


 ELS 11.93
```

1.6 inger-iq.txt

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

Entry..............: INGER IQ 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: "---Inger IQ Virus - Esmark 1953
                                     ---  copy it"
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 disks (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 a 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 shut down
                      Copy counter: 19th word
Similarities........: BYTE BANDIT 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 INGER IQ-Virus ==========================
```

1.7 interlamer

```
Name          : INTERLAMER

Aliases       : A.I.S.F., Virus-Chcker V6.72

Clone         :

Type/size     : Bomb/8708

Symptoms      : An alert will be shown

Discovered    : ?

Way to infect: No infection

Rating        : Very Dangerous

Kickstarts    : 1.2/1.3/2.0

Damage        : Steps Drive.

Manifestation: Pretend to be a Virus-Checker Version

Removal       : Delete file.

Comments      : When you start the trojan, a window appeares with
                the title "VIRUS-CHECKER V6.72" this is a FAKE!!!
                The Window is USELESS!! The trojan installs a new
                routine in $6c (Zeropage). Which shows after a
                delay an alert:

                            !!! CRIME DO NOT PAY !!!

                        WHY ARE YOU SWAPPING ILLEGAL SOFT ?

                         BECAUSE YOU ARE A CRIMINAL !!!!

                                    .... etc

                 After pressing any mouse button your drives are
                 beginnig to step. This steping can cause HARDWARE-
                 ERRORS, so be careful !!!
                 In the end of the file you can read:
                 "THE A.I.S.F. INTERLAMER-VIRUS"

                 NOTE: If you are starting the trojan with the para-
                 ^^^^^ meter "*" a CLI-message appeares:

                 "WOW! YOU GUY MUST BE ELITE !!!"
```

A.D 12-93

1.8 intro-maker

```
     Name         : Intro-Maker by TCR

     Aliases      : -

     Clone        :

     Type/size    : Trojan/10624

     Symptoms     : -

     Discovered   : ?

     Way to infect: No infection

     Rating       : Less Dangerous

     Kickstarts   : 1.2/1.3/2.0

     Damage       : -

     Manifestation: Pretend to be an Intro-Maker

     Removal      : Delete file.

     Comments     : When  you start the trojan, a window appeares with the
                    following  window-title:  "Little  Intro-Maker 1989 by
                    TCR V1.00"


                    Now  you  can  enter a headline, a scrolltext and save
                    the  intro.  But  in  fact  this programm installs the
                    DisasterMaster V2-Virus in memory.


                    For  further  informations look at "DisasterMaster V2"

          See the screendump of the  Intro-Maker  virus!
```

A.D 12-93

1.9 irq.txt

```
========== Computer Virus Catalog 1.2: IRQ Virus (5-June-1990) ========
Entry..............: IRQ Virus
Alias(es)..........: ---
Virus Strain.......: ---
Virus detected when.: January 1989
              where.: Elmshorn, FRG
```

```
Classification......: link virus (extending), resident
Length of Virus.....: 1. length on storage medium: 1060 byte
                                                   + 36 byte (hunk)
                      2. length in RAM           : 1060 byte
                                                   + 36 byte (hunk)
---------------------- 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: ---
                      others: allocates 100.000 byte of workspace
                         during infection of files
Type of infection...: self-identification method: $fffe6100 at 2nd word
                         of virus (without hunk table)
                      system infection: extending executable file,
                          RAM resident, reset resident, EXEC library
Infection Trigger...: usage of OldOpenLibrary routine of exec library
Storage media affected: any available storage medium
Interrupts hooked...: ---
Damage..............: permanent damage: causes some overlay programs to
                         malfunction because of altered offsets in hunk
                         table; DIR command of CLI is infected (stan-
                         dard file); 1st file used in startup-sequence
                         of inserted disk is infected (random file);
                         use of a nearly full disk may cause a
                         read/write error when the infected file won't
                         fit on disk, this disk may not be repaired.
                      transient damage: screen buffer manipulation:
                         changes window title of actual window:
                         'AmigaDOS presents:a new virus by the
                         IRQ-Team V41.0'
Damage Trigger......: permanent damage: usage of OldOpenLibrary routine
                         of exec library
                      transient damage: by random
Particularities.....: only infects files with a maximum length of
                         99.999 byte; uses SetFunction routine of exec
                         library to modify entry of the OldOpenLibrary
                         routine; other resident programs using the
                         system resident list (KickTagPointer,
                         KickMemPointer) are shut down.
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',
                                     'RemIRQ', 'KV', 'IRQKILLER',
                                     'LINKKILLER', 'VIRUSX 4.0',
                                     'DVICE PLUS'
                      Category 4: Vaccine: ---
                      Category 5: Hardware Methods: ---
                      Category 6: Cryptographic Methods: ---
```

```
Countermeasures successful:  'CHECKVECTORS 2.2' with 'RemIRQ', 'KV',
                                    'LINKKILLER' or 'IRQKILLER',
                                    'VIRUSX 4.0', 'DVICE PLUS'
Standard means......: 'CHECKVECTORS 2.2', 'IRQKILLER'
--------------------- 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 IRQ Virus ================================
```