VListR

Torben Bilbo" Maciorowski"

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

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VListR

1.1   VIRUSES - R

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

Red October

Rene

Revenge

Revenge, The

Revenge 1.2G

Revenge Bootloader

Revenge LoadWB

Revenge of the Lamer

Revenge of the Lamer 1

Revenge of the Lamer 2

Rimednac

Ripper

Riska

Rob Northern

Rude Xerox 2.0

1.2 red-october

```
Name          : Red October

Aliases       : ?

Type/Size     : Link/1296

Incidence     : ?

Discovered    : ?

Way to infect: When trying to call a  infected file

Rating        : Dangerous

Kickstarts    : 1.2  1.3  2.04

Damage        : Add 1296 bytes to files. In the infected files you
                can read:"Timer.Device, Dos.library, Ram, Ram: 1"

Manifestation: None

Removal       : Some virus killers can remove the virus and repair
                the files (eg. VT)

 General comments: Always remember to write protect your disk !
```

JN 08.93

1.3 rene

```
Name          : Rene

Aliases       : Lamer Exterminator 5

Type/Size     : BB/1024

Incidence     : ?

Discovered    : 04-89 Elmshorn Germany

Way to infect: Over bootblock

Rating        : Less Dangerous

Kickstarts    : 1.2 1.3 (2.04)

Damage        : Destroy Bootblock and after 6 resets and 3 infections
                fast format the disk

Manifestation: ?
```

```
    Remowal        : Install the disk
                     If the disk has been fast formated the try to undelete
                     with a disk tool prg. (eg. quaterback tool)

  General comments: Always remember to write protect your disk !
```

JN 08.93

1.4   revenge

```
    Name           : Revenge

    Aliases        : Sendarian

    Type/Size      : BB/1024

    Incidence      : ?

    Discovered     : 08-09-89 Elmshorn Gemany

    Way to infect: Over bootblock

    Rating         : Less Dangerous

    Kickstarts     : 1.2

    Damage         : Destroy Bootblock

    Manifestation: After one minute the mouse pointer will become a penis

    Remowal        : Install the disk

  General comments: Always remember to write protect your disk !
```

JN 08.93

1.5   the_revenge

```
    Name           : The Revenge

    Aliases        : -

    Type/Size      : Bootblock

    Incidence      : ?

    Discovered     : ?

    Way to infect: Boot from an infected disk.
```

```
      Rating       : ?

      Kickstarts   : ? (does not work with fastmem)

      Damage       : Overwrites bootblock.

      Manifestation: ?

      Removal      : Install new bootblock on infected disk.

         General comments:
```

PAT 08.93

1.6   revenge-1.2g.txt

```
===== Computer Virus Catalog 1.2: REVENGE 1.2G Virus (5-June-1990) ====
Entry...............: REVENGE 1.2G 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.....: 1.2/33.180
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 2000B
-------------------- Attributes ------------------------------------
Easy Identification.: typical text:'fuck','off','Revenge V1.2G','Count:'
                      virus feature: holding down the joystick button
                         (port 2) during system reboot will shut down
                         the virus (red screen); pressing the joystick
                         button and the mouse button (port 1) will
                         remove the virus from RAM and turn the screen
                         blue
Type of infection...: self-identification method: 5th longword
                         ($ 49443932 = ascii 'ID92')
                      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: after infecting a disk and the
                         next reset the mouse pointer will become a
                         penis after one minute
Damage Trigger......: permanent damage: reset
                         operation: any disk access
                      transient damage: infecting a disk with following
                         reset and 1 minute
Particularities.....: a resident program using the CoolCaptureVector is
```

```
                              shut down; uses DoIOVector; counts vertical
                              blanks until it's time to bring up his new
                              pointer; virus detects BYTE BANDIT, SCA and
                              SCA clones.
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'; own suicide function
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 REVENGE 1.2G Virus =========================
```

1.7 revenge-bootloader

```
    Name        : Revenge Bootloader

    Aliases     : (Byte Bandit Clone)

    Type/Size   : BB/1024

    Incidence   : ?

    Discovered  : ?

    Way to infect: Over bootblock

    Rating      : Less Dangerous

    Kickstarts  : ?

    Damage      : Destroy Bootblock

    Manifestation: Text in Bootblock:Revenge Bootloader

    Removal     : Install the disk

  General comments: Always remember to write protect your disk !
```

JN 08.93

1.8 revengeloadwb

```
Name          : Revenge LoadWB

Aliases       : -

Clone         : KaKo

Type/size     : Trojan/2804

Symptoms      : -

Discovered    : ?

Way to infect: No infection

Rating        : Dangerous

Kickstarts    : 1.2/1.3/2.0

Damage        : -

Manifestation: Pretend to the LoadWB-command

Removal       : Delete file.

Comments      : If you are starting the trojan, it installs the
                T.F.C. Revenge V1.03 virus in memory and
                execute the normal LoadWB.
                For further information read the
                T.F.C. Revenge V1.03 - info.
```

A.D 12-93

1.9 revenge-o.t.-lamer.txt

```
= Computer Virus Catalog 1.2: REVENGE OF THE LAMER EXTERMINATOR Virus
                                     (10-February-1991)=======
Entry...............: REVENGE OF THE LAMER EXTERMINATOR Virus
Alias(es)...........: ---
Virus Strain........: LAMER link virus strain
Virus detected when.: ---
             where.: Australia
Classification......: link virus (directory type), resident
Length of Virus.....: 1. length on storage medium: 4448 byte
                      2. length in RAM          : 4412 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) in startup-sequence as first entry:
                         "$A0,$A0,$A0,$A0,$A0,$00" (hex);
                      identification by using a disk manager: existing
                         file entry in the root directory "no name"
                         (invisible) with length=4448 byte;
                      identification by an alert message (3 pages)
                         after destroying a disk:


  "Page 1

                              RED ALERT


          It has come to my attention that the person using this
                       computer is a LAMER. (*)
              We the people, who are responsible for the
              "Revenge Of The LAMER EXTERMINATOR" Virus,
           believe that only intelligent folk are fit to use
                      the AMIGA Personal Computer
          Since you were apparently not smart enough to prevent
          infection of your computer and software by this virus,
                    (You should have used a condom),
            we must assume that you are a LAMER (a.k.a LOSER)
            and therefore we had no alternative but to erase
           your floppy disk(s), in order to get your attention.


                       - Press Any Mousebutton -


      Page 2

               We are eagerly looking forward to the First Amiga
               magazine that explains the inner workings of this
                       brilliant (at least we think so) virus.
                However, we are not very confident, since the
              three versions of the original "LAMER EXTERMINATOR"
                Virus have never really been properly analysed
                          in any Amiga magazine

             We have made this virus a little bit more aggressive
             so that more people will recognize it and hopefully
             will learn something so as to overcome the dreadful
                          disease of LAMERism

                By the way, the A in LAMER is pronounced
                like the A in DAY. (LAMER people do not
                know proper English in our experience )


                       - Press any Mousebutton -


      Page 3

                              Signed:
              Foundation for the Exterminator of LAMERS. (**)

              (*) You can recognize a LAMER or LOSER as someone
              who can only use the Ctrl-Amiga-Amiga keys on his
```

                     Amiga, and might even know how to load X-Copy...

                 (**) Due to the primitive and violent nature of some
                 LAMERS, we have decided against revealing our real
                      identities, so as to prevent unnecessary
                        visits to the hospital on our part !

                         Coming soon to a theatre near you:
                  *** The LAMER Exterminator – A New Beginning ***

                  – Press any Mousebutton To Continue Being a LAMER –"
                             (end of 3 pages text)
Type of infection...: self-identification method: virus searches for
                             following entry in startup-sequence:
                             "$A0,$A0,$A0,$A0,$A0,$00"(invisible in ASCII)
                             system infection: RAM resident, reset resident
Infection Trigger...: using unprotected disk-like devices
Storage media affected: all disk-like devices
Interrupts hooked...: vertical blank interrupt (VBI)
Damage..............: permanent damage: formatting disk-like devices;
                             transient damage: alert message after destroying
                             a disk (see above)
Damage Trigger......: permanent damage: 6 resets after infection or
                             8 minutes and 11.52 seconds (via VBI);
                             transient damage: formatting device after 6
                             infections
Particularities.....: other resident programs using system resident
                             list (KickTagPointer, KickMemPointer) are
                             not shutdown, because virus installs itself
                             correctly to the system's resident list;
                             name of resident task is "clist.library";
                             trying to format a disk after 6 infections
                             with a protected device causes virus to
                             force a reboot;
                          virus patches the following system entries:
                             KickSumData (virus inserts itself to the
                             system's resident list when deleted by
                             managing this routine which is used to
                             correct checksum over resident list);
                             AvailMem (free memory seems to be ok when
                             asked for because the virus handles this
                             routine);
                             OpenWindow (every file read is misused to
                             check whether startup-sequence of requested
                             device is already changed by virus or not;
                             if not, virus is copied to disk and startup-
                             sequence is modified; OpenWindow is used
                             also to count number of resets since virus
                             infection;
                             DOSRead (used by OpenWindow routine of
                             virus: an OpenWindow demand followed by a
                             DOS Read command causes virus to act as
                             described above: see OpenWindow);
                             DoIO (tests whether a blockblock is affected
                             by a DoIO or not; if not, normal DoIO is
                             executed; if yes, CloseDevice routine is

                          modified, so that every CloseDevice command
                          is extended [see below]); DoIO is extended
                          to set the KickCheckSum's MSB);
                          CloseDevice (extended to clear the KickCheck-
                          Sum's MSB);
                          DoIO and CloseDevice -> virus killer's do
                          not registrate modification of KickCheckSum;
                          BeginIO (patched to format disks when other
                          commands like CMD_READ, CMD_WRITE or boot-
                          block access are demanded);
                          VBI routine (misused to count VBIs, 6000
                          passes =8 minutes and 11.52 seconds)
Similarities........: ---
------------------- 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 startup-sequence
------------------- Acknowledgement --------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Alfred Manthey Rojas, Brian Logan (Australia)
Documentation by....: Alfred Manthey Rojas
Date................: 10-February-1991
Information Source..: ---
==================== End of REVENGE OF THE LAMER EXTERMINATOR Virus ==

1.10   revenge-of-lamer-1

    Name   : Revenge of Lamer 1

    Aliases   : DosSpeed

    Type/Size   : File/4560

    Incidence   : ?

    Discovered   : 29-03-91

    Way to infect: Writes to S/Startup-sequense
                   "$A0,$A0,$A0,$A0,$A0,$00" (asci)
                   Writes to root "$A0A0A0A0A0"

    Rating   : Dangerous

```
   Kickstarts   : 1.2  1.3  2.0

   Damage       : Format device after 6 resets

   Manifestation: After destroying a disk:
"Page 1
                          RED ALERT


         It has come to my attention that the person using this
                       computer is a LAMER. (*)
              We the people, who are responsible for the
               "Revenge Of The LAMER EXTERMINATOR" Virus,
            believe that only intelligent folk are fit to use
                       the AMIGA Personal Computer
         Since you were apparently not smart enough to prevent
         infection of your computer and software by this virus,
                   (You should have used a condom),
            we must assume that you are a LAMER (a.k.a LOSER)
            and therefore we had no alternative but to erase
           your floppy disk(s), in order to get your attention.


                       - Press Any Mousebutton -


   Page 2
                 We are eagerly looking forward to the First Amiga
                 magazine that explains the inner workings of this
                        brilliant (at least we think so) virus.
                  However, we are not very confident, since the
                 three versions of the original "LAMER EXTERMINATOR"
                  Virus have never really been properly analysed
                             in any Amiga magazine

             We have made this virus a little bit more aggressive
             so that more people will recognize it and hopefully
             will learn something so as to overcome the dreadful
                             disease of LAMERism

                By the way, the A in LAMER is pronounced
                like the A in DAY. (LAMER people do not
                know proper English in our experience )

                       - Press any Mousebutton -


   Page 3
                                    Signed:
                  Foundation for the Exterminator of LAMERS. (**)

              (*) You can recognize a LAMER or LOSER as someone
             who can only use the Ctrl-Amiga-Amiga keys on his
              Amiga, and might even know how to load X-Copy...

             (**) Due to the primitive and violent nature of some
             LAMERS, we have decided against revealing our real
                    identities, so as to prevent unnecessary
                     visits to the hospital on our part !
```

```
                 Coming soon to a theatre near you:
           *** The LAMER Exterminator - A New Beginning ***


           - Press any Mousebutton To Continue Being a LAMER -"

    Remowal       : Use a disktool prg. to delete the file "$A0A0A0A0A0"
                    in the root,
                    and correct the startup-sequence

  General comments:

        See the screendump of the  RevengeOfLamer1  virus!

JN 08.93
```

1.11 revenge-of-lamer-2

```
    Name          : Revenge of Lamer 2

    Aliases       : ?

    Type/Size     : File/4448

    Incidence     : ?

    Discovered    : 29-03-91

    Way to infect: Writes to S/Startup-sequense
                    "$A0,$A0,$A0,$A0,$A0,$00" (asci)
                    Writes to root "$A0A0A0A0A0"

    Rating        : Dangerous

    Kickstarts    : 1.2  1.3  2.0

    Damage        : Format device after 6 resets

    Manifestation: After destroying a disk:
   "Page 1
                         RED ALERT

        It has come to my attention that the person using this
                    computer is a LAMER. (*)
             We the people, who are responsible for the
             "Revenge Of The LAMER EXTERMINATOR" Virus,
          believe that only intelligent folk are fit to use
                    the AMIGA Personal Computer
         Since you were apparently not smart enough to prevent
         infection of your computer and software by this virus,
                 (You should have used a condom),
          we must assume that you are a LAMER (a.k.a LOSER)
           and therefore we had no alternative but to erase
          your floppy disk(s), in order to get your attention.
```

```
                              – Press Any Mousebutton –


     Page 2
                      We are eagerly looking forward to the First Amiga
                      magazine that explains the inner workings of this
                             brilliant (at least we think so) virus.
                      However, we are not very confident, since the
                      three versions of the original "LAMER EXTERMINATOR"
                       Virus have never really been properly analysed
                                    in any Amiga magazine

                      We have made this virus a little bit more aggressive
                      so that more people will recognize it and hopefully
                      will learn something so as to overcome the dreadful
                                    disease of LAMERism

                         By the way, the A in LAMER is pronounced
                         like the A in DAY. (LAMER people do not
                         know proper English in our experience )

                               – Press any Mousebutton –

     Page 3
                                     Signed:
                      Foundation for the Exterminator of LAMERS. (**)

                      (*) You can recognize a LAMER or LOSER as someone
                      who can only use the Ctrl-Amiga-Amiga keys on his
                       Amiga, and might even know how to load X-Copy...

                      (**) Due to the primitive and violent nature of some
                       LAMERS, we have decided against revealing our real
                           identities, so as to prevent unnecessary
                             visits to the hospital on our part !

                           Coming soon to a theatre near you:
                        *** The LAMER Exterminator – A New Beginning ***


                      – Press any Mousebutton To Continue Being a LAMER –"

     Removal       : Use a disktool prg. to delete the file "$A0A0A0A0A0"
                     in the root,
                     and correct the startup-sequence

  General comments: Revenge of Lamer 2 is similat to Revenge of Lamer
                    only some Write-Test-Routines removed

         See the screendump of the  RevengeOfLamer2  virus!
                            and the  RevengeOfLamer3  virus!

JN 08.93
```

1.12   rimednac

```
      Name          : Rimednac

      Aliases       : ?

      Type/Size     : BB/1024

      Incidence     : ?

      Discovered    : ?

      Way to infect: Over Bootblok

      Rating        : ?

      Kickstarts    : ?

      Damage        : Destroy Bootblock ?

      Manifestation: ?

      Remowal       : Install the disk !!

  General comments: SHI do not have any info on this virus !
                    if you have the virus or info about it
                    please send it to you regional SHI center.
```

JN 08.93

1.13 ripper

```
      Name          : Ripper

      Aliases       : Rip The Ripper (North Star 1 clone)

      Type/Size     : BB/1024

      Incidence     : ?

      Discovered    : 05-02-91

      Way to infect: Over Bootblock

      Rating        : Less Dangerous

      Kickstarts    : ?

      Damage        : Destroy Bootblock

      Manifestation: ATARI KILLS COMMODORE! RIP! RIP THE RIPPER etc

      Remowal       : Install the disk

  General comments: Always remember to write protect your disk !
```

JN 08.93

1.14 riska

```
Name          : Riska

Aliases       : (Byte Bandit 1 clone)

Type/Size     : BB/1024

Incidence     :

Discovered    : 31-05-91

Way to infect: Over bootblock

Rating        : Less Dangerous

Kickstarts    : ?

Damage        : Destroy Bootblock

Manifestation: ?

Remowal       : Install the disk
```

  General comments: Always remember to write protect your disk !

JN 08.93

1.15 rob-northern

```
Name          : Rob Nothern

Aliases       : (BGS clone)

Type/Size     : File/2616 bytes

Incidence     : Very rare

Discovered    : 26-04-92

Way to infect: When executed

Rating        : Less Dangerous

Kickstarts    : 1.2  1.3

Damage        : The virus take name of the first command in the
```

```
                    S/startup-sequence and move the org. command to
                    Devs and/or Root directory under the name:
                    $A0,$A0,$A0,$20,$20,$20,$A0,$20,$20,$20,$A0
                    Destroy Bootblock.

   Manifestation: The text: a computer virus is a disease
                    terrorism is a transgression
                    software piracy is a crime

   Removal        : Delete the file with the virus and install the disk

General comments: If a disk is re-infected with Rob Nothern virus.
                    the startup-sequence stops because of a programming
                    error.
```

JN 07.09.93

1.16 rude-xerox-2.0

```
   Name           : Rude Xerox 2.0

   Aliases        : (Forpib clone)

   Type/Size      : BB/1024

   Incidence      : ?

   Discovered     : ?

   Way to infect: ?

   Rating         : Less Dangerous

   Kickstarts     : ?

   Damage         : Destroy Bootblock

   Manifestation: ?

   Removal        : ?

General comments: SHI do not have any info on this virus !
                    if you have the virus or info about it
                    please send it to you regional SHI center.
```

JN 08.93