VListT

Torben Bilbo" Maciorowski"

COLLABORATORS

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

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VListT

1.1 VIRUSES - T

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

Taipan Chaos

Taipan Lameblame

Target

TeleCom

Telstar

Termigator

Terrorists

Terrorists 2

TFC Revenge

TFC Revenge V 1.03

TFC Revenge V 2.14

Tick

TimeBomb

TimeBomb 0.9

TimeBomb 0.9 Clone

TimeBomb 1.0

TimeBomb TG

TimeBomber

Timer Virus

TNK

Tomates Gentechnic

Traveling Jack, The

Traveling Jack 1

Traveling Jack 2

Traveller 1.0

Triplex

Trisector 911

Tristar

Turk

Turk Color Dropper

Twinz Santa Claus

1.2 taipan-chaos

Name : Taipan Chaos

Aliases : -

Type/Size : Bootblock

Incidence : ?

Discovered : ?

Way to infect: Booting from an infected disk

Rating : ?

Kickstarts : -

Damage : Overwrites bootblock, and destroys data on disk.

Manifestation: Display Alert: Chaos! by Tai-Pan....

Removal : Install new bootblock on infected disk

General comments: It waits until the counter reachs 8 and then overwrites all blocks of the disk with garbage.

PAT 06.93

1.3 taipan-lameblame

Name   : Taipan Lameblame

Aliases   : -

Type/Size   : Bootblock

Incidence   : ?

Discovered   : ?

Way to infect: Booting from an infected disk

Rating   : ?

Kickstarts   : -

Damage   : Overwrites bootblock, and destroys data on disk.

Manifestation: Display Alert: Lameblame! by Tai-Pan....

Removal   : Install new bootblock on infected disk

General comments: It waits until the counter reachs 8 and then overwrites all blocks of the disk with garbage.

PAT 06.93

1.4 target

Name   : Target

Aliases   : -

Type/Size   : Bootblock

Incidence   : ?

Discovered   : ?

Way to infect: Booting from an infected disk. Writes to disks.

Rating   : ?

Kickstarts   : -

Damage : Overwrites bootblock.

Manifestation: -

Removal : Install new bootblock on infected disk

General comments:

PAT 06.93

1.5 telecom

Name : TeleCom

Aliases : -

Clone : -

Type/size : File/756

Symptoms : -

Discovered : ?

Way to infect: File infection

Rating : Less Dangerous

Kickstarts : only 1.3 with Ranger RAM ($C00000)

Damage : -

Manifestation: -

Removal : Delete file.

Comments : The virus uses the CoolCapture to stay resident in memory. It is always at the same adress in memory ($C71000). After a reset the virus patches the DoIO(), FindResident(), and later the Open-Window() vectors. If you are booting with a disk the virus does the following:

a) It checks with the help of DoIO() if the disk is write protected. If not the virus moves a value at memory adress. This value will later be used from the OpenWindow-Patch to check if the disk was write protected.

b) The virus patches the FindResident() vector. This new patch installs some time later a new patch in the OpenWindow()-vector.

c) This new patch infects the root-dir of the disk

```
                          while it creates the virusfile ($A0) and modifies
                          the startup-sequence.

                        The string "s/startup-sequence" in the virus is
                        coded with a simple EOR-loop (eor.b #$27,(a1)+).
                        In the decoded virus you can read "TeleCom".

                        NOTE: I wonder how such a virus could spread itself.
                        ^^^^^ -> The memory Ranger RAM is rare.
                              I think this virus must be an older one.

A.D 12-93
```

1.6 telstar

```
     Name         : Telstar

     Aliases      : SystemZ 6.0

     Type/Size    : Bootblock

     Incidence    : ?

     Discovered   : ?

     Way to infect: -

     Rating       : ?

     Kickstarts   : -

     Damage       : Overwrites bootblock.

     Manifestation: -

     Removal      : Install new bootblock on infected disk

        General comments: Makes you beleive it's SystemZ 6.0


PAT 06.93
```

1.7 termigator

```
     Name         : Termigator

     Aliases      : -

     Type/Size    : Bootblock

     Incidence    : ?
```

Discovered : ?

Way to infect: Booting from an infected disk.

Rating : ?

Kickstarts : Only 1.2 because of absolute ROM jumps.

Damage : Overwrites bootblock.

Manifestation: Alert Only the TERMIGATOR VIRUS makes it possible...

Removal : Install new bootblock on infected disk

General comments: Always in memory at $7f4d0

See the screendump of the Termigator virus!

PAT 06.93

1.8 terrorists.txt

```
=== Computer Virus Catalog 1.2: TERRORISTS Virus (10-February-1991) ==
Entry...............: TERRORISTS Virus
Alias(es)...........: ---
Virus Strain........: BGS 9 virus strain
Virus detected when.: MAY 1990      (when VTC received virus code)
              where.: North Germany
Classification......: link virus (renaming), resident
Length of Virus.....: 1. length on storage medium: 2608 byte
                      2. length in RAM           : 2608 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: "TTV1" at end of virus
                                     (length=2608 byte)
                      identification on disk: a file in ROOT- and/or
                         DEVS-directory is named with following
                         unprintable string:  $A0,$20,$20,$20,$A0,$20,
                         $20,$A0,$20,$A0,$A0; length of first command
                         in startup-sequence seems to be altered to
                         2608 byte (because file isnot original anymore)
Type of infection...: self-identification method: virus searches for a
                         file in devs- or root directory named with
                         this unprintable string: $A0,$20,$20,$20,$A0,
                         $20,$20,$A0,$20,$A0,$A0
                      system infection: RAM resident, reset resident
Infection Trigger...: reset (CONTROL+Left-AMIGA+Right-AMIGA)
Storage media affected: bootable floppy disks (3.5" and 5.25"),
                         bootable RAM disks, bootable hard disks
Interrupts hooked...: ---
Damage..............: permanent damage: overwriting bootblock;
                      transient damage: screen buffer manipulation:
                         screen becomes black, a graphic with fol-
                         lowing text is displayed:
                                "a computer virus is a disease
                                 terrorism is a transgression
                                 software piracy is a crime
                                 this is the cure     BGS9
                                 Bundesgrenzschutz Sektion 9
                                 Sonderkommando 'EDV'       "
Damage Trigger......: permanent damage: reset (CONTROL+LEFT-AMIGA
                                               +RIGHT-AMIGA)
                      transient damage: 4 resets (to be run
                         until initial CLI window appears)
Particularities.....: other resident programs using the system
                         resident list (KickTagPointer, KickMem
                         Pointer) are shutdown; name of resident
                         task is "TTV1" (see string in bootblock);
                         when virus doesn't find a DEVS directory,
                         it uses the root; first command in startup-
                         sequence is renamed to a file named with
                         following unprintable string:
                         $A0,$20,$20,$20,$A0,$20,$20,$A0,$20,$A0,$A0
                         (in DEVS- or root directory if available),
                         and virus is written to directory the
                         command comes from using the same name;
                         next time, virus will be called first
                         before original command is executed
Similarities........: 100% clone of the BGS 9 virus, only name of
                         the relocated carrier (DEVS:) is different
                         (see above); problems show when other
                         resident programs suc as harddisk devices
                         are installed; same problem (=guru medita-
                         tion when started from startup-sequence)
                         also occurs with BGS 9
--------------------- Agents -----------------------------------------
Countermeasures.....: Names of tested products of Category 1-6:
                      Category 1: .2 Monitoring System Vectors:
                                     CHECKVECTORS 2.3
                                  .3 Monitoring System Areas:
                                     CHECKVECTORS 2.3, GUARDIAN 1.2,
                                     VIRUS-DETEKTOR 1.1
                      Category 2: Alteration Detection: ---
                      Category 3: Eradication: CHECKVECTORS 2.3,
                                  BGS9-PROTECTOR, VIRUS-DETEKTOR 1.1
                      Category 4: Vaccine: BGS9-PROTECTOR
                      Category 5: Hardware Methods: ---
                      Category 6: Cryptographic Methods: ---
Countermeasures successful: CHECKVECTORS 2.3, BGS9-PROTECTOR
Standard means......: CHECKVECTORS 2.3 with deletion of "no name" file
                         entry (see above) using a disk manager and
                         correction of startup-sequence (removal)
                         and creating two files named with the
                         following unprintable string "$A0,$20,$20,
                         $20,$A0,$20,$20,$A0,$20,$A0,$A0" to vaccinate
                         disk (one file has to be placed in ROOT-, the
                         other in DEVS-directory); BGS9-PROTECTOR
--------------------- 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 Terrorists Virus ========================
```

1.9 terrorists-2

```
     Name          : Terrorists 2

     Aliases       : Novi  (BGS9 clone)

     Type/Size     : File/1612

     Incidence     : ?

     Discovered    : 28-12-91

     Way to infect: Any disk with a stratup

     Rating        : Less Dangerous

     Kickstarts    : ?

     Damage        : Take name of the first file in Startup-sequence
                     the org. file is the placed after C/.Fastdir

     Manifestation: ?

     Removal       : Delete the file that is infected and replace it
                     an org. one

  General comments: Always remember to write protect your disk !


JN 07.09.93
```

1.10 tfc_revenge

```
     Name          : T.F.C. Revenge 1.03

     Aliases       : -

     Type/Size     : BootBlock

     Incidence     : ?

     Discovered    : ?

     Way to infect: Boot from an infected disk.
     Rating       : ?

     Kickstarts   : ?

     Damage       : Overwrites bootblock.

     Manifestation: Text in bootblock "THE EXTREME VIRUS..."

     Removal      : Install new bootblock on infected disk

        General comments: When the counter reachs zero alerts (DISK BAD) and
                          damages all write enabled disks in all drives.

          See the screendump of the  TFCRevenge  virus!

PAT 08.93
```

1.11 tfc_revenge_v1.03

```
     Name         : T.F.C. Revenge 1.03

     Aliases      : -

     Type/Size    : BootBlock

     Incidence    : ?

     Discovered   : ?

     Way to infect: Boot from an infected disk.

     Rating       : ?

     Kickstarts   : ?

     Damage       : Overwrites bootblock.

     Manifestation: Text in bootblock "THE EXTREME VIRUS..."

     Removal      : Install new bootblock on infected disk

        General comments: When the counter reachs zero alerts (DISK BAD) and
                          damages all write enabled disks in all drives.


PAT 08.93
```

1.12 tfc_revenge_v2.14

```
     Name         : T.F.C. Revenge 2.14

     Aliases      : -
     Type/Size    : BootBlock

     Incidence    : ?

     Discovered   : ?

     Way to infect: Boot from an infected disk.

     Rating       : ?

     Kickstarts   : ?

     Damage       : Overwrites bootblock.

     Manifestation: Text in bootblock "THE EXTREME VIRUS..."

     Removal      : Install new bootblock on infected disk

        General comments: When the counter reachs zero alerts (DISK BAD) and
                          damages all write enabled disks in all drives.


PAT 08.93
```

1.13 tick

```
     Name         : Tick

     Aliases      : Julie

     Type/Size    : Bootblock

     Incidence    : ?

     Discovered   : ?

     Way to infect: Booting from an infected disk

     Rating       : ?

     Kickstarts   : ? - Malfunction with 1MB chip

     Damage       : Overwrites Bootblock

     Manifestation: Always $7f800, cool, DoIo, BeginIo and  $20
                    Doesn't work correctly with 1MB Chip
                    tests a few pointers and 3 values (e.g. at $7ec00)
                    spreads: without warning over (only bootable) BB's
                    Decoded with not.b (a0)+ you can read (in memory):
                    `  VIRUS PREDATOR  (4-88-SPAIN)  ID: 027798336  `
                    which goes to show that the name Julia is wrong.
```

PAT 08.93

1.14 timebomb

```
Name         : TimeBomb

Aliases      : -

Type/Size    : Bootblock

Incidence    : ?

Discovered   : 8-Sep-89 Elmshorn, FRG

Way to infect: Booting from an infected disk

Rating       : ?

Kickstarts   : 1.2; 1.3 (and up?)

Damage       : Overwrites Bootblock

Manifestation: typical text: 'YOU CAME ALL THE WAY FOR SHIT!
               HAVE A NICE DAY SUCKER', 'TIMEBOMB V1.0 CODED
               BY ARKON MEMBER OF AVIREX. IDEA BY THE WIZARDS
               INC. NOTE : IT SEEMS THAT THEY WERE NOT
               INTERESTED BECAUSE I DID NOT GET ANY ANSWER
               OF THEM' (not used by TIMEBOMB 1.0)

Removal      : To remove, install a new bootblock on the disk.

   General comments: blocks boot procedure after
                     3rd infection of disk; destroys root directory
                     after 2nd infection
                     Uses a counter on which action type depends:
                      counter < 2 : increase counter and rewrite
                                    TIMEBOMB 1.0 to disk, normal boot
                                    procedure
                      counter = 2 : display alert box containing text
                                    #1 (see above), overwrites root
                                    directory now (22 blocks)
                      counter > 2 : GURU MEDITATION because of a bug  ↩
                                                                    the  ↩
                         programmer(s) made: dos
                                    library isn't initialized, else
                                    the alert box containing test #1
                                    would be displayed
```

PAT 08.93

1.15 timebomb_0.9.txt

```
====== Computer Virus Catalog 1.2: TimeBomb_09 Bomb (31-July-1993) =====
Entry...............: TimeBomb_09 Bomb
Alias(es)...........: .info Time Bomb
Virus Strain........: ---
Virus detected when.: ---
              where.: ---
Classification......: Time bomb
Length of Virus.....: Length of file: 7840 bytes (+1 byte in "pic.xx")
--------------------- 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.: There is a "startup-sequence" entry called
                         ".info", and there is always a 2nd file called
                         "pic.xx" with 1 byte length in root directory
                         (serving as counter).
                      If diskette is write protected, bomb writes to
                         Shell: "User Request: Please remove write
                         Protection and press left Mouse Button to
                         continue.."
Type of infection...: None (damage-only)
Infection Trigger...: ---
Storage media affected: Floppy disks only
Interrupts hooked...: ---
Damage..............: Permanent damage: formating floppy disks
Damage Trigger......: Starting this program when the specific byte in
                         "pic.xx" counted down to zero.
Particularities.....: ---
Similarities........: VirusTest bomb (seems to be an "older version")
--------------------- Agents ------------------------------------------
Countermeasures.....: VirusZ 3.06, VT 2.54, VirusChecker 6.28
Countermeasures successful: VirusZ 3.06, VT 2.54, VirusChecker 6.28
Standard means......: Delete files ".info", "pic.xx" and 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 analysis of virus code
===================== End of TimeBomb_09 Bomb ==========================
```

1.16 timebomb_0.9-clone

```
Name          : TimeBomb 0.9 Clone

Aliases       : .info

Type/Size     : Trojan/1584 (PPacked)

Incidence     : ?

Discovered    : ?
```

```
     Way to infect: ?

     Rating       : ?

     Kickstarts   : ?

     Damage       : Formats disk

     Manifestation: If disk isn’t write enabled; "Please remove write
                    protection and press left mouse button to continue"

     Removal      : -

        General comments: Exists in two parts in SubDir c and Root:
           in c: .info     = Virus  Length PPacked: 1584 bytes
           in Root: setmap = Counter (startvalue=FF)  Length: 1 byte
           In the first line in startup-sequence: c/.info
           Damage: by each restart the value in setmap goes down 1. When
           0 is reached, the disk is formatted (Track 0-150). Then there’s
           a textdisplay:
                    Hey Looser ! Boot again !
           To be able to change the value in df0:setmap the disk has to
           be write-enabled. If write-protected, you’ll get this requester:
                 User Request : Please remove write Protection and press
                        left Mouse Button to continue..
           The startup-sequence can’t continue without write-enable.
           In Cli you’ll read:
                    DISC SPEEDER BY BUD


PAT 08.93
```

1.17 timebomb-1.0.txt

```
===== Computer Virus Catalog 1.2: TIMEBOMB 1.0 Virus (5-June-1990) ====
Entry...............: TIMEBOMB 1.0 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.....: 1.2/33.166, 1.2/33.180, 1.3/34.5
Computer model(s)...: AMIGA 500, AMIGA 1000, AMIGA 2000A, AMIGA 200B
---------------------- Attributes -------------------------------------
Easy Identification.: typical text: ’YOU CAME ALL THE WAY FOR SHIT!
                         HAVE A NICE DAY SUCKER’, ’TIMEBOMB V1.0 CODED
                         BY ARKON MEMBER OF AVIREX. IDEA BY THE WIZARDS
                         INC. NOTE : IT SEEMS THAT THEY WERE NOT
                         INTERESTED BECAUSE I DID NOT GET ANY ANSWER
                         OF THEM’ (not used by TIMEBOMB 1.0)
```

```
Type of infection...: self-identification method: ---
                      system infection: bootblock of one disk
Infection Trigger...: reset
Storage media affected: floppy disks (3.5" and 5.25")
Interrupts hooked...: ---
Damage..............: permanent damage: blocks boot procedure after
                         3rd infection of disk; destroys root directory
                         after 2nd infection (see below)
                      transient damage: depending from it’s counter
Damage Trigger......: permanent damage: blocking boot procedure after
                         3rd infection of disk (see below)
                      transient damage: counter (see below)
Particularities.....: uses a counter on which action type depends:
                       counter < 2 : increase counter and rewrite
                                     TIMEBOMB 1.0 to disk, normal boot
                                     procedure
                       counter = 2 : display alert box containing text
                                     #1 (see above), overwrites root
                                     directory now (22 blocks)
                       counter > 2 : GURU MEDITATION because of a bug  ↩
                                                                        the  ↩
                          programmer(s) made: dos
                                     library isn’t initialized, else
                                     the alert box containing test #1
                                     would be displayed
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: witout restrictions: ’CHECKVECTORS 2.2’,
                                                 ’VIRUSX 4.0’
                            with restrictions:   ’GUARDIAN 1.2’
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 TIMEBOMB 1.0 Virus ======================
```

1.18 timebomb-tg.txt

```
= Computer Virus Catalog 1.2: TOMATES_GENTECHNIC Virus (31-July-1993) ==
Entry...............: Timebomb_Vir.Tomates_Gentechnik Virus
```

```
Alias(es)...........: ---
Virus Strain........: TimeBomb_Vir.1_0 BootBlock Virus
Virus detected when.: ---
              where.: ---
Classification......: System virus (bootblock), memory 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: "TOMATES-GENTECHNIC-V I R U S !"
                                    "FUCK YOURSELF, FREAK"
Type of infection...: Bootblock infector
Infection Trigger...: Booting from an infected diskette
Storage media affected: Only floppy disks (3.5" and 5.25") in drive 0
Interrupts hooked...: ---
Damage..............: Permanent damage: Overwriting bootblock+rootblock
                      Transient damage: ---
Damage Trigger......: Permanent damage: Booting from an infected disk
                      Transient damage: ---
Particularities.....: ---
Similarities........: ---
--------------------- Agents ------------------------------------------
Countermeasures.....: VirusZ 3.06, VT 2.54, BootX 5.23,VirusChecker 6.28
Countermeasures successful: VirusZ 3.06, VT 2.54, BootX 5.23,
                      VirusChecker 6.28
Standard means......: VT 2.54
--------------------- Acknowledgement ---------------------------------
Location............: Virus Test Center, University Hamburg, FRG
Classification by...: Jens Vogler
Documentation by....: Jens Vogler
Date................: 31-July 1993
Information Source..: Reverse analysis of virus code / Heiner Schneegold
===================== End of TOMATES_GENTECHNIC Virus =================
```

1.19 timebomber

```
     Name         : TimeBomber

     Aliases      : -

     Type/Size    : Trojan/936

     Incidence    : ?

     Discovered   : ?

     Way to infect: ?

     Rating       : ?

     Kickstarts   : ?
     Damage       : Formats disk

     Manifestation: -

     Removal      : -

        General comments: made using the program TimeBomber
           consists of 2 parts in RootDir:
           virustest         = Virus   length: 936 Bytes
           virustest.data    = counter (Start value=5)  length: 1 Byte
           in 1st line of startup: virustest
           not resident, no copy routine in virustest
           Features: decreases counter in virustest.data with 1 at
           every start.
           As soon as 0 is reached, the disk gets formatted.
           To change value in virustest.data, the disk may not be
           write protected.
           If it is, the message appears:
              User Request : Please remove write Protection and press
                             left Mouse Button to continue..
           Further use of startup-sequence without write enabling the disk
           is impossible.
           in CLI always :
           RAM CHECKED - NO VIRUS FOUND.
```

PAT 08.93

1.20 timer-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.

```
-----------------------------------------------------------------------------
                                Timer virus
-----------------------------------------------------------------------------
```

Type: File (Trojan)

Origin: (I don’t know the original name) (size: 4812)

Infect: :c/SetMap or :system/SetMap

Short: Execute commands via the serial port.

Long:

When this clock utility (V1.1) is executed, the virus does the following

1) Checks if current directory is ok and writable.
2) Removes protection bits of
:c/SetMap
:system/SetMap
3) Write the virus to the files above. New length is 1712 bytes.

After the SetMap command is infected the utility executes the real clock utility.

The new SetMap sets the required KeyMap (just as the original SetMap would have done) and then it searches for ramdrive.device (exit if found). Then it allocates 1030 bytes (exit if unsuccessful) and copies the actual virus into this area. Then it starts the actual virus as a process with the name ramdrive.device (stack = 10000 bytes, priority = 0) and exits.

The actual virus patches the Level5 interrupt (Serial port receive buffer full) by accessing the absolute address $74, not through Vector Base Register. This new interrupt snoops the serial port for a carriage-return (ascii value 13) terminated string, and continues with the original interrupt. If the string is the numerical sequence {7,5,12,12,5,18,1} then it will execute the command which follows immediately after the sequence. Output of this command will be collected in the file

RAM:Command-00-T01

This file is then read into an allocated area (max. 10000 bytes) and sent back through the serial port.

Observations:

The core code for Timer and for the BlueBox virus is the same. Furthermore, the Level5 code is exactly the same for these two trojans.

To emulate the SetMap command, the virus copies the name of the required KeyMap (usa1, d, dk, or similar) to a string with a preceding path name. The default of this is

:devs/keymaps/d

This could very well mean that the origin of the virus is Germany. Furthermore KeyMaps are found by using the path name ":devs/keymaps/" instead of the more approriate "DEVS:keymaps/" (similar for ":c/SetMap" and ":system/SetMap")

Take another look at the sequence mentioned above. If you add 64 to all values you get the word "GELLERA". Comparing with the sequence from BlueBox it should probably be "GELLER". Does anybody know what this word means? (a name?) Contact SHI if you have got a clue.

The stack size (of 10000 bytes) is unnecessary big; 1000-2000 bytes should be sufficient. Judging from the programming style the virus coder is not very familiar with neither the OS nor the M68000 (2-3 years of experience at most.)

See also: BlueBox virus

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.

1.21 tnk

Name   : TNK

Aliases   : - (SCA clone)

Type/Size   : BB

Incidence   : ?

Discovered   : ?

Way to infect: Booting from an infected disk

Rating   : Not really dangerous

Kickstarts   : ?

Damage   : Overwrites bootblocks

Manifestation: Scrolling Text in screen

Removal   : Install new boot block

General comments: In the BB you can read "This was The New Kid"

PAT 08.93

1.22 tomatesgentechnic.txt

```
== Computer Virus Catalog 1.2: TOMATES GENTECHNIC Virus (20-FEB-1993) ==
Entry...............: TOMATES GENTECHNIC Virus
Alias(es)...........: ---
Virus Strain........: ---
Virus detected when.: ---
              where.: ---
Classification......: System virus (bootblock)
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 texts: "TOMATES-GENTECHNIC-V I R U S !"
                                     "FUCK YOURSELF, FREAK"
Type of infection...: Bootblock
Infection Trigger...: Booting from an infected disk
Storage media affected: Only floppy disks (3.5" and 5.25") in drive 0
Interrupts hooked...: ---
Damage..............: Overwriting bootblock and rootblock
Damage Trigger......: 2nd boot from an infected disk
Particularities.....: ---
Similarities........: ---
--------------------- 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..: ---
===================== End of TOMATES GENTECHNIC Virus ==================
```

1.23 the_traveling_jack

```
     Name         : The Traveling Jack

     Aliases      : -

     Type/Size    : Link/198

     Incidence    : ?

     Discovered   : ?

     Way to infect: Executing infected program

     Rating       : ?

     Kickstarts   : ?

     Damage       : Links to other programs

     Manifestation: a) writes a file to disk VIRUS.xy length always 198 Bytes
                       x and y are HexNumbers, chosen using $BFE801.
                       Text in VIRUS.xy:
                         The Travelling Jack....
                         I'm travelling from town to town looking for respect,
                         and all the girls I could lay down make me go erect.
                                 -Jack, 21st of September 1990
                    b) links to other programs

     Removal      : Reset and delete infected program. Use a virus killer.
```

```
        General comments:
           Conditions:
           DOS0-Disk, Disk validated, 12 Blocks free on disk, File length
           at least 2000 Bytes, Filename at least 5 chars, Filename
           contains no chars with value lower than $40,
           no Info.File
           Type A:
           LinkHunklengthnCalculation:
           $24C + value from $DFF006
           decoded in memory $909+1 Bytes
           Type B:
           LinkHunklengthnCalculation:
           $25B + value from $DFF006
           decoded in memory $945+1 Bytes
           Travelling Jack 3 is it not, it is type B, I Think. Many
           Viruscheckers have a bug, because they know this one as
           something other than type B;
           maybe they are right. (28.09.91)



PAT 08.93
```

1.24 travelingjack1.txt

```
== Computer Virus Catalog 1.2: Traveling Jack 1 Virus (18-Jan-93) ======
Entry...............: Traveling Jack 1 Virus
Alias(es)...........: Jack 1 Virus
Virus Strain........: Traveling Jack Virus Strain
Virus detected when.: 1991
              where.:
Classification......: Linkvirus(Extending), Not Resident,
                         variably self-encrypting.
Length of Virus.....: 1.Length on medium: variable, at least 2368
                      2.Length in RAM:    $940=2368 Bytes
--------------------- Preconditions ------------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: 1.2/1.3/2.04
Computer model(s)...: A500,A500+,A1000,A2000,A2500,A3000
--------------------- Attributes ---------------------------------------
Easy Identification.: Text in RAM, in file "VIRUS.XX" (where XX
                         are random numbers created through event
                         counter in CIA-A) and in root-directorys:
                         "The Traveling Jack....",$A,$A,$D
                         "I'm traveling from town to town looking for r"
                         "espect,",$A,$D
                         "and all the girls I could lay down make me go "
                         "erect.",$A,$A,$D
                         "                              -Jack, 21st of "
                         "September 1990",0
                      Length of File in root-directory: 198 bytes
Type of infection...: Self-Identification methods:
                         Checks for $4cfa6400 (=movem.l (PC)+,a2/a5/a6)
                         at DOS-Library ROM-Call-pointer
                      Infection:
                         -$20(DOS-Library node) (=pointer to
                         dos.library ROM-calls = dosbase+$2e)
                      File Infection:
                         Extends files by at least 2368 bytes
                         (+random value from rasterbeam-register)
                      Cannot handle following file (hunk)-types (skips):
                         HUNK_OVERLAY, HUNK_BREAK,  HUNK_RELOC8
                      Infection starts if the following conditions hold:
                         - random (rasterbeam) matches comparevalue
                           (see below)
                         - DOS,0 Disk (old filesystem)
                         - Disk validated
                         - Path to the file is smaller than 38 chars
                         - Virus is able to allocate 8000+280 bytes
                           in memory
                         - file is executable
                         - file is larger than 2000 Bytes
                         - last 4 chars of filenameare in (a-z,A-Z)
                         - last 4 chars of fn. are not "INFO"
                           (UPPER/LOWECASE)
                         - filename is longer than 4 chars
                         - file does not consist of one of the above
                           hunk-types
                         - file is writeable.
Infection Trigger...: Random (VPOS,VHPOS=$dff004)
Storage media affected: Media formatted with Old-Filesystem
Interrupts hooked...: ---
Damage.............: Permanent Damage: Writes files "VIRUS.XX" into the
                         current root directory of ANY disk
                      Transient/Permanent damage: Potentially, some files
                         wont run after infection (due to hunk-check-
                         routines)
Damage Trigger......: Random ($dff004.l and #$1ff) < $80 -> infection
                                             > $b0 < $e0 -> damage
Particularities.....: Virus checks at address $ffffffe8 for
                         #$fdfe6c48 and does not install itself if this
                         value is found. On normal Systems this adress is
                         a ROM-adress at $ffffe8, on turbo-32-bit Amigas
                         this could be a RAM-address.
                      Virus is encrypted and modifies its encryption
                         routine code every new generation.
Similarities........: ---
--------------------- Agents -------------------------------------------
Countermeasures.....: Names of tested products of Category 1-6:
                      Category 1: .1 SnoopDos
                                  .2 AVM0.237
                                  .3 ---
                      Category 2: vt2.48,lvd
                      Category 3: vt2.48,virusz,vc6.03,lvd
                      Category 4: ---
                      Category 5: possible (see partic.)
                      Category 6: possible (not tested)
Countermeasures successful: vt2.48,virusz,vc6.03,avm0.237
Standard means......: vt2.48
--------------------- Acknowledgement ----------------------------------
Location...........: Virus Test Center, University Hamburg, Germany
```

```
Classification by...: Soenke Freitag
Documentation by....: Soenke Freitag
Date................: 18-January-1993
Information Source..: Reverse-Engineering of Virus Code
===================== End of "Traveling Jack"-Virus====================
```

1.25 travelingjack2.txt

```
== Computer Virus Catalog 1.2: Traveling Jack 2 Virus (20-FEB-1993) ====
Entry...............: Traveling Jack 2 Virus
Alias(es)...........: Jack 2 Virus
Virus Strain........: Traveling Jack Virus Strain
Virus detected when.: 1991
              where.:
Classification......: Linkvirus (Extending), Not Resident,
                        variable self-encryption.
Length of Virus.....: 1.Length on medium: variable, at least 2428 Bytes
                      2.Length in RAM:                  $97c=2428 Bytes
--------------------- Preconditions ------------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: 1.2/1.3/2.04
Computer model(s)...: A500,A500+,A1000,A2000,A2500,A3000
--------------------- Attributes ---------------------------------------
Easy Identification.: Text in file "VIRUS.XX" (where XX are random
                         numbers created through event counter in CIA-A)
                         in root-directorys:
                         "The Traveling Jack....",$A,$A,$D
                         "I'm traveling from town to town looking for r"
                         "espect,",$A,$D
                         "and all the girls I could lay down make me go "
                         "erect.",$A,$A,$D
                         "                               -Jack, 21st of "
                         "September 1990",0
                         Length of File in root-directory: 198 bytes.
                         Sometimes generates Write-Protect requester.
Type of infection...: Self-Identification methods:
                         Checks for $4cfa6400 (=movem.l (PC)+,a2/a5/a6)
                         at DOS-Library ROM-Call-pointer
                      Infection: -$20(DOS-Library node)
                         (=pointer to dos.library ROM-calls=dosbase+$2e)
                      File Infection: Extends files by at least
                         2368 bytes (+ random value from rasterbeam-
                         register)
                      Cant handle following file (hunk)-types (skips):
                         HUNK_OVERLAY, HUNK_BREAK, HUNK_RELOC8
                      Infection starts if the following conditions hold:
                         - Random (rasterbeam) matches comparevalue
                           (see below)
                         - DOS,0 Disk (old filesystem)
                         - Disk validated
                         - Path to the file is smaller than 38 chars
                         - Virus is able to allocate 8000+280 bytes
                           in memory
                         - File is executeable
                         - File is larger than 2000 Bytes
                         - Last 4 chars of filenameare in (a-z,A-Z)
                         - Last 4 chars of fn. are not "INFO"
                           (UPPER/LOWECASE)
                         - Filename is longer than 4 chars
                         - File does not consist of one of the
                           above hunk-types
                         - File is writeable.
Infection Trigger...: Random (VPOS,VHPOS=$dff004)
Storage media affected: Media formatted with Old-Filesystem.
Interrupts hooked...: ---
Damage..............: Permanent Damage: Writes files "VIRUS.XX" into the
                         current rootdirectory of ANY disk
                      Transient/Permanent damage: Potentially some files
                         won't run after infection (due to hunk-check-
                         routines)
Damage Trigger......: random ($dff004.l and #$1ff) < $80 -> infection
                                             > $b0 < $e0 -> damage
Particularities.....: Jack 2=Jack 1 + code routine for the infection/
                         damage routine + texts
                      Virus checks at adress $ffffffe8 for #$fdfe6c48
                         and doesnot install itself if this value is
                         found. On normal Systems this adress is a ROM-
                         adress at $ffffe8, on turbo-32-bit Amigas this
                         could be a RAM-adress.
                      Virus is encrypted and modifies its encryption
                         routine code every new generation.
                      Some Virus code is encrypted in RAM and will only
                         be decrypted when executed.
Similarities........: ---
--------------------- Agents -------------------------------------------
Countermeasures.....: Names of tested products of Category 1-6:
                      Category 1: .1 SnoopDos
                                  .2 AVM0.237
                                  .3 ---
                      Category 2: vt2.48,lvd
                      Category 3: vt2.48,virusz,vc6.03,lvd
                      Category 4: ---
                      Category 5: possible (see partic.)
                      Category 6: possible (not tested)
Countermeasures successful: vt2.48,virusz,vc6.03,avm0.237
Standard means......: vt2.48
--------------------- Acknowledgement ----------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Soenke Freitag
Documentation by....: Soenke Freitag
Date................: 18-January-1993
Information Source..: Reverse-Engineering of Virus Code
===================== End of "Traveling Jack 2"-Virus ==================
```

1.26 traveller-1.0.txt

```
=== Computer Virus Catalog 1.2: TRAVELLER 1.0 Virus (25-July-1992) ===
Entry...............: TRAVELLER 1.0 Virus
Alias(es)...........: ---
Virus Strain........: ---
Virus detected when.: Unknown
              where.: Unknown
Classification......: System virus (bootblock), memory resident
Length of Virus.....: 1. Length on storage medium: 1024 byte
                      2. Length in RAM:            3072 byte
--------------------- Preconditions -----------------------------------
Operating System(s).: AMIGA-DOS
Version/Release.....: all versions
Computer model(s)...: all models
--------------------- Attributes --------------------------------------
Easy Identification.: Typical text: "The Traveller 1.0"
Type of infection...: RAM resident, reset resident, bootblock
Infection Trigger...: Message with #$6E000 at offset $2C and
                         with #2 (Read) at offset $1C recieved dy DoIO
Storage media affected: All device-driven systems
Interrupts hooked...: Interrupt-vector 3
Damage..............: Permanent damage: overwriting block zero of
                                        the same device
                      Transient damage: screen buffer manipulation:
                                        screen becomes red, green
                                        and blue; message "never heard
                                        of virus-protection ??? -
                                        lamer !!!" is shown in black;
                                        system stops working
Damage Trigger......: Permanent damage: message with #$6E000 at offset
                                        $2C and #2 (Read) at offset
                                        $1C recieved dy DoIO
                      Transient damage: 45,000th occurence of
                                        interrrupt 3 after last in-
                                        fection
Particularities.....: A resident program using the CoolCaptureVector
                         is shut down; changes DoIO vector; uses
                         KickTagPtr; restores DoIO vector
Similarities........: ---
--------------------- 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................: 14-July-1992
Information Source..: ---
===================== End of TRAVELLER 1.0 Virus =====================
```

1.27 triplex

```
Name          : TRIPLEX

Aliases       : -

Type/Size     : BB

Incidence     : ?
```

```
     Discovered   : ?

     Way to infect: Booting from an infected disk

     Rating       : ?

     Kickstarts   : 1.3, 2.04 (and up?)

     Damage       : ?

     Manifestation: -

     Removal      : Install new boot block

        General comments: You can read in the BB: "This nice little Virus
           was written in 1990 and so on
```

PAT 08.93

1.28 trisector_911

```
     Name         : TRISECTOR

     Aliases      : -

     Type/Size    : BB

     Incidence    : ?

     Discovered   : ?

     Way to infect: Booting from an infected disk

     Rating       : ?

     Kickstarts   : 1.3, NOT with 2.04 (and probably not with more than K2.04)

     Damage       : ?

     Manifestation: -

     Removal      : Install new boot block

        General comments: Do NOT require trackdisk.device
```

PAT 08.93

1.29 tristar

```
     Name         : TRISTAR-Viruskiller V1.0

     Aliases      : -

     Type/Size    : BB

     Incidence    : ?

     Discovered   : ?

     Way to infect: Booting from an infected disk

     Rating       : ?

     Kickstarts   : ?

     Damage       : ?

     Manifestation: -

     Removal      : Install new boot block

        General comments:


PAT 08.93
```

1.30 turk.txt

```
========= Computer Virus Catalog 1.2: TURK Virus (31-July-1993) ========
Entry...............: TURK Virus
Alias(es)...........: ---
Virus Strain........: ---
Virus detected when.: APRIL 1990
              where.: Australia
Classification......: System virus (bootblock), memory 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, 3.0/all
Computer model(s)...: All AMIGA models (see particularities)
--------------------- Attributes ---------------------------------------
Easy Identification.: Typical text: "TURK", "Amiga Failure... Cause:
                                    TURK VIRUS Version 1.3!"
Type of infection...: System infection: RAM resident, reset resident,
                                        bootblock
Infection Trigger...: 1) Reset (CONTROL+Left-AMIGA+RIGHT-AMIGA)
                      2) Operation: any disk access
Storage media affected: Only floppy disks (3.5" and 5.25")
Interrupts hooked...: ---
Damage..............: Permanent Damage: virus overwrites bootblock
                         and destroys 880 blocks by overwriting them
                         with unformated sequence of data from RAM
```

```
                        thus causing read/write error on affected
                        storage media.
                     Transient Damage: screen buffer manipulation:
                        alert box after formating a disk.
Damage Trigger......: Permanent damage: reset.
                     Transient damage: any disk access.
Particularities.....: 1) Resident programs using the CoolCaptureVector
                        or KickTagPointer are shutdown.
                     2) Virus overwrites autovectors 64, 192, 200
                        and 201 to store data.
                     3) Problems may arise on machines which set VBR
                        of CPU to a non-zero value as the autovector
                        addresses used in virus point to public memory.
Similarities........: See TURK.Color Dropper Trojan (dropping this virus)
--------------------- Agents -----------------------------------------
Countermeasures.....: VT 2.54
Countermeasures successful: VT 2.54
Standard means......: VT 2.54
--------------------- Acknowledgement --------------------------------
Location............: Virus Test Center, University Hamburg, Germany
Classification by...: Original entry: Oliver Meng (February 20,1990)
                     Update:         Karim Senoucci
Documentation by....: Oliver Meng, Karim Senoucci
Date................: 31-July-1993
Information Source..: Reverse analysis of virus / SHI
==================== End of TURK virus ================================
```

See the screendump of the Turk virus!

1.31 turk.color_dropper.txt

```
= Computer Virus Catalog 1.2: TURK.COLOR_DROPPER Trojan (31-July-1993) =
Entry...............: Turk.Color_Dropper Trojan
Alias(es)...........: Color Virus Carrier=Color Demo=Installer of Turk
Virus Strain........: ---
Virus detected when.: ---
              where.: ---
Classification......: TURK Virus dropping Trojan Horse
Length of Virus.....: 1.Length on storage medium: 2196 bytes
                     2.Length in RAM:            4258 bytes
--------------------- 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 (see particularities)
--------------------- Attributes -------------------------------------
Easy Identification.: Typical text, visible in file:
                        "Hope you enjoy this proggie!
                         It was put together in ten minutes ...
                         Press Left Mouse Button for the demo ...
                         **  Press Right Mouse Button to end **"
Type of infection...: System infection: bootblock, RAM resident, reset
                        resident,changes CoolCapture- and DoIO-vectors
Infection Trigger...: Bootblock infection: DoIO-call requesting read
                        or write access to bootblock
                     Other infections: executing trojan horse
```

```
Storage media affected: Only floppy disks
Interrupts hooked...: ---
Damage..............: Permanent damage: overwriting bootblock with
                                TURK boot virus (see TURK virus).
                      Transient damage: overwriting 80k Bytes of main
                                memory with the string "TURK" and
                                halting system.
Damage Trigger......: Permanent damage: DoIO-call as described above
                      Transient damage: reset
Particularities.....: 1) Uses memory at $70000 without allocating it;
                         overwrites autovectors 64, 148, 200 and 201.
                      2) Resident programs using CoolCaptureVector or
                         KickTagPointer are shutdown.
                      3) Problems may arise on machines which set VBR
                         of CPU to a non-zero value as the autovector
                         adresses used in virus point to public memory.
Similarities........: TURK Virus
--------------------- Agents -------------------------------------------
Countermeasures.....: VT 2.54, VirusZ 3.06, VirusChecker 6.28
Countermeasures successful: VT 2.54, VirusZ 3.06, VirusChecker 6.28
Standard means......: VT 2.54
--------------------- Acknowledgement ----------------------------------
Location............: Virus Test Center, University Hamburg, FRG
Classification by...: Karim Senoucci
Documentation by....: Karim Senoucci
Date................: 6-July-1993
Information Source..: Virus Disassembly / SHI / Heiner Schneegold
===================== End of TURK.COLOR_DROPPER Trojan =================
```

1.32 twinz_santa_claus

```
Name         : Twinz Santa Claus

Aliases      : CODER, Coders Nightmare (Coder Strain)

Type/Size    : BB

Incidence    : ?

Discovered   : ?

Way to infect: Booting from an infected disk

Rating       : ?

Kickstarts   : ?

Damage       : ?

Manifestation: -

Removal      : Install a new boorblock

   General comments: always $7f600, DoIo, KickTag, KickCheckSum, $68
                     Text changed to The Santa Claus Virus
```

```
PAT 08.93
```