Virus Info Base

COLLABORATORS			
	TITLE : Virus Info Base		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY		July 1, 2022	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

Virus Info Base

1.1 Mallander V1.0

```
Name          : Mallander Virus

Aliases       : Derk

Type/Size     : Boot/2048

Clones        : No Clones

Symptoms      : No Symptoms

Discovered    : 29-03-92

Way to infect: Boot infection

Rating        : Dangerous

Kickstarts    : 1.2/1.3/2.0

Damage        : Overwrites boot + block 2,3 !

Removal       : Install boot.

Comments      : The Mallander-Virus works like the Digital Dream
                Virus: It saves the Original-Bootblock in block
                2,3 to execute it even after infection. If you are
                booting with an infected disk the virus does the
                following:

                 1) Checks for memory from address $7F800 if you
                    have not free memory there, the virus gives
                    you a RESET.

                 2) Copies itself to address $7F800 and loads the
                    original bootblock to $7FC00 and executes it.

                 3) After the execution of the Org.BB the virus
                    changes the KICK-Vectors to stay resident in
                    memory.
```

After the next reset the virus patches the DoIO() Vector for infection. Imagine you are booting with a clean, uninfected and unprotected disk:

1) The virus loads the original bootblock to $7FC00 and checks for the word "DERK" in the bootblock.

2) The virus calculates the new checksum and saves 2048 bytes. -> Block 2,3 = UNREPAIRABLE DAMAGED

By the way:If The Mallander virus is active in memory and you show the bootblock of an infected disk with e.g. a Bootblock-Utility, the virus ALWAYS shows you the original bootblock and NOT the virusboot.
->>> KILL THE VIRUS FIRST IN MEMORY !!!

If AMIGA-DOS accesses a block with the help of DoIO() the virus decreases the chip-memory by 16348 bytes , this will be done as long as there isn't any chip memory anymore. Then the virus gives out an alert:

"J.D. MALLANDER VIRUS V. 1.0"
"I need lots of money - buy my cool pd serie 'action power'"

Click on this gadget if you want to see a Demo of the Mallander virus. Push left mouse button to return.

This text is crypted, you CAN'T read it in the BB.

A.D 07-94