Commander

COLLABORATORS			
	TITLE : Commander		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY		August 24, 2022	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

Commander

1.1 Commander

```
                Name         : Commander

Aliases      : No Aliases

Type/Size    : Link/1664

Clones       : No Clones

Symptoms     : No Symptoms

Discovered   : 21-07-94

Way to infect: Link Infection

Rating       : Less Dangerous

Kickstarts   : 1.3/2.X/3.X

Damage       : Links itself to executable files.

Manifestation: Writes in comment ": "in all infected file

Removal      : Use viruskiller to remove or delete file (?!?!)

Comments     : If you`re  starting  an  Commander infected  file  the
               virus  first searches for the task "DH0". If this task
               is  in  memory  the  virus  tries  to infect  the file
               "DH0:C/LoadWB".   After  that  the  virus  patches the
               following vectors from the dos.library:

               - Open()
               - Rename()
               - Lock()
               - Examine()
               - ExNext()
               - LoadSeg()
               - SetComment()
               - SetProtection()
```

These vectors are all used to infect other files. As one result the Amiga gets little slower by disk access.

The virus just infects files which doesn‘t have the letter "V" or "v" as the first in the filename. And it only gets active if the actual drive isn‘t write protected and only if there are at last 10 free blocks on it.

For infection the virus searches for Offsetjumps or BSR.l [JSR -XXX(a6) or BSR.L XXX]. These jumps will be manipulated so that they first will activate the virus.

The virus itself is crypted by useing dff00X. In memory you can read:

"reqtools.library reqtools 38.888"

But there is another crypted message in the virus which says after decrypting:

"-<(COMMANDER)>- by Bra!N BlaSTer in 1994."

Click on this gadget
More info
to see a text how a
user describes his commander virus problems. Push left mouse button to return.

All in all a very primitive virus. I can‘t find any special routine which is very good coded. But this virus is tricky.

A.D / ELS 11-94

1.2 Commander Infection

HOW THE USER USUALLY DEALS WITH COMMANDER VIRUS
~~~~~~

The first weird thing the user encounters is that suddenly some of his programs won’t work and/or the memory isn’t set free after running a program that reserves RAM. Also some ASCII-chars in the WB-title-bar looks a bit different (like: all ’0’ is replaced with ’Ò’ and weird pixels appear in the top line of some chars).

When the user tries to find out what is going on either by getting a directory by using the "Dir" command from CLI or running DirectoryOpus, everything will seem to be normal, but - if the user is really paying attention the size of free space on his HD has shrunk. How much, depends
~~~~~~

on how long time mysterious things have been going on.

At this time the user may have guessed that a virus has taken over the control. If not he'll probably try running some disk-repair-tool, and he will find that his Amiga freezes during the process. Afterwards he'll possibly run a virus-killer and depending on the efficiency of it, this will either produce no result or the solution. If not the solution...

'Panic' is now written in the user's mind (if he hasn't recently backed up his HD). In frustration of nothing else to do he'll perhaps use the command: 'List' and find strange ': ' in the dirs right underneath the executable programs he has lately run. The ': ' means that the file listed just above has the comment ' ' (a single space). It may also occur to the user that all the files having this weird comment has grown 1664 bytes longer. And maybe 2 or 3 boots later not only almost all files in the C directory but also other exe-files (maybe never run) is infected!!

AS FAR AS I KNOW THE COMMANDER-VIRUS DOES THE FOLLOWING THINGS:
~~~~~~

When active the memory reserved by the executed prg.'s will not be released after quitting them.

It infects all the files the user executes, - not necessarily from the Startup-sequence - (e.g. the 'Dir' command), - later it also infects files not run.

'INFECTS' MEANS:

When executing a file and Commander is active - in memory, the virus links itself (1664 bytes) to the file, thereby making itself executed - if not already active - the next time the infected file is run. Copying this single file to your friends disk and inserting it in his Amiga is enough to make his life a nightmare!. Commander deletes the existing comment on the file and puts in a single space (' ') instead.

NOTES:
~~~~~~

Wether it is software-destructive or not I don't know. The only things obvioulsy affecting the user is that it won't let unnecessarily reserved RAM be released, it deletes his comments, it makes the files grow taking away free space from the HD/Disk and it makes some ASCII-chars appear different (not changing the actual font-file as far as I know).

David A. Filskov