Article 7727 of comp.sys.amiga:
Path: ethz!cernvax!mcvax!uunet!husc6!hao!ames!oliveb!amiga!cbmvax!bill
From: bill@cbmvax.UUCP (Bill Koester CATS)
Newsgroups: comp.sys.amiga
Subject: Amiga VIRUS
Keywords: VIRUS
Message-ID: <2758@cbmvax.UUCP>
Date: 13 Nov 87 19:32:05 GMT
Reply-To: bill@cbmvax.UUCP (Bill Koester CATS)
Organization: Commodore Technology, West Chester, PA
Lines: 139

THE AMIGA VIRUS - Bill Koester (CATS)

When I first got a copy of the Amiga VIRUS I was interested to see how such a program worked. I dissassembled the code to a disk file and hand commented it. This article will try to pass on some of the things I have learned through my efforts.

1) Definition.
2) Dangers.
3) Mechanics
4) Prevention

1. - Definition.

The Amiga VIRUS is simply a modification of the boot block of an existing DOS boot disk. Any disk that can be used to boot the Amiga (ie workbench) has a reserved area called the boot block. On an Amiga floppy the bootblock consists of the first two sectors on the disk. Each sector is 512 bytes long so the boot block contains 1024 bytes. When KickStart is bringing up the system the disk in drive 0 is checked to see if it is a valid DOS boot disk. If it is, the first two sectors on the disk are loaded into memory and executed. The boot block normally contains a small bit of code that loads and initializes the DOS. If not for this BOOT CODE you would never see the initial CLI. The normal BOOT CODE is very small and does nothing but call the DOS initialization. Therefore, on a normal DOS boot disk there is plenty of room left unused in the BOOT BLOCK.

The VIRUS is a replacement for the normal DOS BOOT CODE. In addition to performing the normal DOS startup the VIRUS contains code for displaying the VIRUS message and infecting other disks. Once the machine is booted from an infected disk the VIRUS remains in memory even after a warm start. Once the VIRUS is memory resident the warm start routine is affected, instead of going through the normal startup the VIRUS checks the boot disk in drive 0 for itself. If the VIRUS in memory sees that the boot block is not infected it copies itself into the boot block overwriting any code that was there before. It is in this manner that the VIRUS propagates from one disk to another. After a certain number of disks have been infected the VIRUS will print a message telling you that Something wonderful has happened.

2. - Dangers.

When the VIRUS infects a disk the existing boot block is overwritten. Since some commercial software packages and especially games store special information in the boot block the VIRUS could damage these disks. When the boot block is written with the VIRUS, any special information is lost forever. If it was your only copy of the game then you are out of luck and probably quite angry!!

3. - Mechanics.

Here is a more detailed description of what the virus does. This is intended to be used for learning and understanding ONLY!! It is not the authors intention that this description be used to create any new strains of the VIRUS. What may have once been an innocent hack has turned into a destructive pain in the #$@ for many people. Lets not make it any worse!!

a.) Infiltration.

This is the first stage of viral infection. The machine is brought up normally by reading the boot block into memory. When control is transferred to the boot block code, the virus code immediately copies the entire boot block to $7EC00, it then JSR's to the copied code to wedge into the CoolCapture vector. Once wedged in, control returns to the loaded boot block which performs the normal dos initialization. Control is then returned to the system.

b.) Hiding Out.

At this point the system CoolCapture vector has been replaced and points to code within the virus. When control is routed through the CoolCapture vector the virus first checks for the left mouse button, if it is down the virus clears the CoolCapture wedge and returns to the system. If the left mouse button is not pressed the virus replaces the DoIO code with its own version of DoIO and returns to the system.

c.) Spreading.

The code so far has been concerned only with making sure that at any given time the DoIO vector points to virus code. This is where the real action takes place. On every call to DoIO the virus checks the io_Length field of the IOB if this length is equal to 1024 bytes then it could possibly be a request to read the boot block. If the io_Data field and A4 point to the same address then we know we are in the strap code and this is a boot block read request. If this is not a boot block read the normal DoIO vector is executed as if the virus was not installed. If we are reading the boot block we JSR to the old DoIO code to read the boot block and then control returns to us. After reading, the checksum for the virus boot block is compared to the checksum for the block just read in. If they are equal this disk is already infected so just return. If they are not equal a counter is incremented and the copy of the virus at $7EC00 is written to the boot block on the disk. If the counter ANDed with $F is equal to 0 then a rastport and bitmap are constructed and the message is displayed.

d.) Ha Ha.

```
< Something wonderful has happened >
< Your AMIGA is alive!!! >
< and even better >
< Some of your disks are infected by a VIRUS >
< Another masterpiece of the Mega-Mighty SCA >
```

4. - Prevention.

How do you protect yourself from the virus?

1) Never warm start the machine, always power down first.
   (works but not to practical!)

2) Always hold down the left mouse button when rebooting.
   (Also works, but only because the VIRUS code checks for
    this special case. Future VIRUS's may not!)

3) Obtain a copy of VCheck1.1 and check all disks before use.
   If any new virus's appear this program will be updated and released
   into the public domain. VCheck1.1 was posted to usnet and will
   also be posted to BIX.
   (Just like the real thing the best course of action is
     education and prevention!)

--

Bill Koester -- CBM >>Amiga Technical Support<<
UUCP ...{allegra|burdvax|rutgers|ihnp4}!cbmvax!bill
PHONE (215) 431-9355

Pleese desrigard eny spealing airors!!!!!!!!!!