

Department of Energy

CIAC

Computer Incident Advisory Capability

Using Data Physician Plus! on DOE Computers

CIAC-2311 R.0

by the Members of the CIAC Team

February, 1995



DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

Table of Contents

The Data Physician Plus! Package	1
What is CIAC?	1
Overview	1
DPP Programs.....	1
VirHUNT	2
RESSCAN, WIN-RS, and RS-NET.....	2
VirALERT	2
Using Virus Scanners	3
Overview	3
Virus Signature Scanners.....	3
Program Change Detectors.....	3
Strategy for Scanning	4
Signature Files	4
Creating the Small Signature File.....	5
Creating the Large Signature File.....	8
Performing a Signature Scan.....	10
Automatic Scanning At Start-up	11
Disinfecting a Computer System.....	12
General Approach	12
Procedure for Disinfecting a System	12
Potential Disinfection Problems.....	15
Encrypted Viruses	15
Stealth Viruses	15
Defeating a Stealth Virus.....	18
Network Connections	18
Using Suspicious-Activity Detectors	20
Overview	20
Installing VirALERT or WIN-VA.....	21
Deactivating VirALERT.....	21
Lowering Sensitivity.....	22
Using RESSCAN as a Memory-Resident Scanner.....	23
Overview	23
Using RESSCAN	23
What You See When Your Computer Has a Virus	24
Introduction.....	24
Detecting a Virus Attack	25
Detecting an Infected Boot Record	26
Scanning with an Infected Scanner.....	26

Table of Contents, Continued

Appendix A Instructions from the DPP Installer.....	A-1
VirHUNT	A-1
RESSCAN	A-3
WIN-RS	A-5
RS-NET	A-5
VirALERT.....	A-6
WIN-VA	A-8
Recover.....	A-8

Reader Comments Form

The Data Physician Plus! Package

What is CIAC? CIAC is the U.S. Department of Energy's (DOE) Computer Incident Advisory Capability. Established in 1989—shortly after the Internet Worm—CIAC provides various computer security services to DOE's employees and contractors. CIAC services include:

- incident handling consulting
- computer security information
- onsite workshops
- white-hat audits

Overview

The Data Physician Plus! (DPP) software package is licensed by the U.S. Department of Energy (DOE) for use by DOE and its contractors. This report describes the use of DPP on DOE computers and includes some suggestions for using it efficiently.


DPP Programs

The DPP package contains two main programs plus variations of those programs. The main programs are the VirHUNT virus scanner and the VirALERT memory-resident suspicious-activity detector. The following table lists the anti-virus programs and their variations.

Program	Description
VirHUNT	Virus and program scanner.
RESSCAN	Virus and program scanner built with overlays so it can stay memory resident.
WIN-RS	Windows version of RESSCAN. Identical to RESSCAN, but contains a handler for VGA monitors in graphics mode.
RS-NET	Helper file for RESSCAN when used with networked drives.
VirALERT	Memory-resident suspicious-activity detector.
WIN-VA	Windows version of VirALERT. Identical to VirALERT, but contains a handler for VGA monitors in graphics mode.

VirHUNT

The VirHUNT program is the primary stand-alone file scanner. A stand-alone scanner scans files at one point in time to see if they have changed or if they contain viruses. The VirHUNT program can scan for known viruses and repair infected programs. In addition, the program can scan for changed files and reverse most changes caused by virus activity. VirHUNT also scans memory, boot records, and master boot records (MBR or partition table) for virus signatures or changes.

 **To scan for and repair changed files, a signature scan must be done first to create signatures for the clean, undamaged files**

RESSCAN, WIN-RS, and RS-NET

The RESSCAN program is a variation of VirHUNT that can run as a stand-alone scanner or be loaded as a memory-resident program (TSR); as a memory-resident program, RESSCAN scans files that are about to be executed or copied.

The WIN-RS program is a variation of RESSCAN that handles graphics mode on VGA monitors to display warning messages in Windows.

The RS-NET program is a helper program for RESSCAN for use with networked drives. Normally, RESSCAN is installed first, then the network drivers. RS-NET is run after the network drivers are loaded to allow RESSCAN to scan accessed files before they are used by the system.

VirALERT

VirALERT is a memory-resident program (TSR) that watches for suspicious activity, such as writing to the boot sector of a hard disk, creating executable files, or formatting a floppy disk. When a questionable event occurs, VirALERT displays a warning message that allows you to continue or abort the operation.

Using Virus Scanners

Overview

VirHUNT and RESSCAN are scanner programs that search for files infected with a virus or files with changes. Virus scanners use two different methods for detecting infected files:

- scanning for virus signatures
 - scanning for changes in executable files
-

Virus Signature Scanners

A signature scanner scans memory, the boot record, the master boot record, and executable files for strings of bytes identifying a virus infection. To work, the virus scanner must be coded with a string of bytes—or signature—that uniquely identifies a virus infection. The scanner cannot detect a virus without a known signature.

Encrypted and polymorphic viruses are difficult for scanners to detect. Encrypted viruses place a small encryption engine at the beginning of the virus code; usually using a different key for each infection; this encrypts the virus. Polymorphic viruses insert different numbers of nonsense commands between the actual virus code commands to hide the virus, making it difficult to create a unique signature.

Program Change Detectors

Program change detectors check file attributes—the create date and time, length, checksum, file header, and other properties—to determine if a file has changed. A program scanner can detect a new virus, but cannot identify the virus. Actually, a program scanner cannot determine if a file is infected by a virus; it can determine that the file has changed in some way. However, any changes in executable files should be viewed with suspicion. Few executable files rewrite themselves after installation. None of the DOS utility programs (e.g., FORMAT, ASSIGN) should ever change during normal use, so view changes there as a probable virus infection.

A program change detector is first run to create a signature file for some or all the executable files on a disk. Later, using the stored signatures, the program change detector determines if an executable file has changed. In addition, VirHUNT and RESSCAN store those parts of a program most often changed by a virus and can usually restore an infected program using those stored parts, even a program infected with a new, unknown virus.

Using Virus Scanners, Continued

Unlike a virus signature scanner that is used after an infection has occurred, a program change detector requires some forethought. A program change detector must have a baseline program signature file in order to tell that a change has occurred. Thus, you must have run the scanner before an infection occurred to create the signature file.

Strategy for Scanning

The VirHUNT and RESSCAN programs in the DPP package contain both a virus scanner and a program scanner. The virus scanner searches for known viruses in executable files, and the program scanner is the program change detector. Set the “create new signature file” option on the program scanner before you run it the first time to store the program signatures. Then run the program scanner again to scan for changes in the protected programs. You can set the installer program to run the initial program scan for you.

Virus signature scanners and program change detectors both take several minutes to scan a large hard disk. If the scanner is set up in the AUTOEXEC.BAT file to run every time you boot your computer, your computer will take longer to boot up. Scanning the entire hard disk for viruses or for program changes every time you boot is probably unreasonable for all but the “front door” and “open” computers in your organization. A “front door” computer is reserved specifically for scanning disks coming into an organization and should not be attached to any network. “Open” computers are available for anyone to use; because of their uncontrolled nature, they are very susceptible to viruses.

Rather than scanning all resident files each time a computer is booted, scan the entire hard disk at times convenient to the user (e.g., at night, at lunch) and scan only a few particularly sensitive files at boot-up. By always scanning those files most likely to be infected by a new virus, you should catch most new infections before they have gone very far. The root directory of the C: drive and the DOS directory are the most likely places for a new infection to occur.

Because of a new development in the One_half virus, you may want to scan any heavily used directory on a networked drive. The One_half virus infects the boot record on the C: drive and files on a networked drive, but it does not infect other files on the C: drive. Of course, you should always scan any floppies brought into your area, including those in shrink-wrapped containers and any new executable files copied onto your hard disk.

Signature Files

To use the signature scanner efficiently, make two program signature scans:

- the small signature of the directories you are going to scan whenever you boot up your system
- the large signature file of the entire hard disk

Using Virus Scanners, Continued

3. Select **A: Set signature options**. This menu displays:

```
A: Signature scan
B: Scan, find Newfiles
C: Scan and Remove
D: Scan, Remove, Newfiles
E: Scan in FAST mode
F: Scan FAST, Newfiles
G: Create signatures
H: Create in FAST mode
I: NO signature scan
```

4. Select **G: Create new signatures**. This menu displays:

```
A: Set signature options
B: Set signature filename
C: Set exclude list filename
```

5. Select **B: Set Signature filename**. This dialog box displays:

```
Please enter the signature file to use, or a
blank for VIRHUNT.SIG
>> <<
```

Using Virus Scanners, Continued

6. Type a file name for the program signature file (e.g., VIRHUNT1.SIG), then press **<Return>** + **<Esc>** to return to the Options menu.
7. Select **A: Directory to scan**. This dialog box displays:

Path(s) to search, or blank for the default E:\	
>>	<<
Hard drives: C: or (ALL)	
Other drives: A: B:	

8. Type the names of the directories you want to scan at every boot-up, then press **<Return>**. For example, if you type C:\C:\DOS, you will scan the root directory on the C: drive and the DOS directory every time you boot up your computer.
9. On the Options menu, **D: Scan subdirectories** must be set to "No." If it is not, select it, then press **<Return>** to select a "No" value from the list of options displayed.
10. On the Options menu, **B: Scan what** must be set to "Memory/Boot/Files." If it is not, select it, then press **<Return>** to select this value from the list of options displayed.
11. Select **do virus Scan** on the Scan menu. Your small group of files will be scanned and a signature file named VIRHUNT1.SIG will be created.


Using Virus Scanners, Continued

12. If no viruses are detected, your screen will display similar to this screen:

```
=====
#      ««««« Virus Hunt and Destroy V4.0E (c) DDI 1989-94 »»»»» #
#              Sandy Sparks (CPPC), (510)422-6856, CIAC      #
# Summary of virus scan on 10/24/94 at 14:46:37              #
# Scanning: Memory                                          #
# Scanning: Boot Record C:                                 #
# Scanning: Files                                           #
# Scanning Boot Record C:                                  #
# Scanning: Files                                           #
#                                                            #
# Scan Complete!   NO VIRUSES FOUND                        #
#                                                            #
# Files:   89 scanned,   135 total,   2 directories        #
#                                                            #
#                                                            #
#                                                            #
#                                                            #
#                                                            #
#                                                            #
#                                                            #
#                                                            #
# Press any key to continue                                #
=====
```

Creating the Large Signature File

Follow these steps to create the large signature file for the entire hard disk.

 **If you have already run an initial, small signature file, many of the options for the large file scan will already be set to the correct values.**


Using Virus Scanners, Continued

1. Start VirHUNT.
 2. Select **F: Signature mode** on the Options menu.
 3. Select **A: Set signature options**.
 4. Select **G: Create new signatures**.
 5. Select **B: Set signature filename**.
 6. In the dialog box, type a file name for the program signature file (e.g., VIRHUNT2.SIG), then press **<Return>** + **<Esc>** to return to the Options menu.
 7. Select **A: Directory to scan**.
 8. Type ALL in the dialog box, then press **<Return>**.
 9. On the Options menu, **D: Scan subdirectories** must be set to "Yes." If it is not, select it, then press **<Return>** to select a "Yes" value from the list of options displayed.
 10. On the Options menu, **B: Scan what** must be set to "Memory/Boot/Files." If it is not, select it, then press **<Return>** to select this value from the list of options displayed.
 11. Select **do virus Scan** on the Scan menu. Your entire hard drive will be scanned and a signature file named VIRHUNT2.SIG will be created.
 12. When this process completes, you may want to save a copy of this signature file on a floppy disk, in case the original gets overwritten or damaged.
-

Using Virus Scanners, Continued

Performing a Signature Scan

Follow these steps to perform a signature scan.

 **This procedure assumes the default values are the same as those set for the signature file.**

1. Start VirHUNT.
2. Select **F: Signature mode** on the Options menu.
3. Select **A: Set signature options**.
4. Select **B: Scan, find New files**.
5. Select **B: Set signature filename**.
6. In the dialog box, Type VIRHUNT1.SIG, then press **<Return>** + **<Esc>** to return to the Options menu. Running VIRHUNT1.SIG scans only the files in the C:\ and C:\DOS directories.

To scan the entire hard disk, use VIRHUNT2.SIG as the filename instead of VIRHUNT1.SIG.

7. Select **A: Directory to scan** on the Options menu.
8. In the dialog box, type C:\ C:\DOS. To scan the entire drive, type ALL, then press **<Return>**.
9. On the Options menu, **D: Scan subdirectories** must be set to "No." If it is not, select it, then press **<Return>** to select a "No" value from the list of options displayed.
10. On the Options menu, **B: Scan what** must be set to "Memory/Boot/Files." If it is not, select it, then press **<Return>** to select this value from the list of options displayed.
11. Select **do virus Scan** on the Scan menu. Your files will be virus and signature scanned.

Using Virus Scanners, Continued

The program scanner follows this order for scanning:

- It first scans memory for a virus signature.
- The scanner then scans the boot record on the C: drive and all the files in C:\ and C:\DOS directories for known viruses.
- Next, the scanner does a program signature scan on the boot record and then for all the files in the VIRHUNT1.SIG signature file (or VIRHUNT2.SIG, if you are scanning the whole disk).
- Finally, the scanner checks the C:\ and C:\DOS directories again and lists any executable files that were not in the signature file.

If these executable files are legitimate, create a new signature file that includes these files.

Automatic Scanning At Start-up

To automatically perform the same run of VirHUNT each time you boot your computer, place the following command in the AUTOEXEC.BAT file:

```
C:\DDI\VIRHUNT.EXE C:\ C:\DOS SCN SFC:\DDI\VIRHUNT2.SIG  
LIC:\DDI\SCAN.OUT SISN QU
```

This command assumes the files VIRHUNT.EXE, and VIRHUNT1.SIG are all in the C:\DDI directory. If you start up with this command, VirHUNT scans the C:\ and C:\DOS directories. The command performs the following functions:

- The SCN option sets the VirHUNT “Scan subdirectories” option to “No”.
 - The SISN option performs a program signature scan and reports new files not included in the signature file.
 - The QU option commands the program to quit upon completion of a successful scan.
 - The SF option sets the file name of the program signature file.
 - The LI option sets the file name used to store the results of the scan.
-

Disinfecting a Computer System

General Approach

To disinfect a disk infected with a memory-resident virus such as the Satan Bug, you must remove the virus from memory, then scan the disk with an uninfected copy of VirHUNT. To remove the virus from memory, boot your computer with a clean, locked boot disk. Then you can scan the hard disk using VIRHUNT on a clean, locked disk. The procedures in this section are also applicable to nonmemory-resident program viruses, as well as most boot-sector and partitionable viruses.

Procedure for Disinfecting a System

CAUTION: Before following these procedures, you must have a clean, locked emergency boot floppy disk containing:

- an up-to-date (less than six-months old) virus scanner
- FORMAT.EXE, SYS.COM, and FDISK.COM
- any disk management software such as DiskManager needed to access your hard disk
- simple CONFIG.SYS and AUTOEXEC.BAT files to bring up your system
- any backup/restore software you usually use

Create this disk before your system becomes infected, or on another uninfected computer.

Disinfecting a Computer System, Continued

Follow these steps to disinfect a system infected with a memory-resident virus:

1. Boot the infected computer with the locked, uninfected floppy.
2. Run the virus scanner on the uninfected floppy and scan the hard disk on the infected computer.
3. Once the scan has completed, repair or delete any infected files the scanner found and scan the disk again. If possible, replace infected files rather than letting the scanner fix them. While scanners do a very good job of fixing infected files, they may not fully repair all the damage in a file. Replacing the file from a clean, locked master disk ensures the file is not damaged.
4. Repeat step 4 until no more infected or changed files are found. Sometimes a disk is infected with more than one virus, and fixing the damage done by one virus may reactivate a previous infection. Eliminate that possibility by rescanning until the scanner does not detect any more infections.
5. When the scanner indicates that the hard disk is clean, insert your emergency backup system disk and restore the system using the SYS command. This step replaces the invisible system files, COMMAND.COM, and the boot sector.
6. Restore any deleted executables from your locked master disks or backup sets.
7. Scan the disk again with your virus scanner. Note that at this point, the scanner may detect changes in some files because you have copied in new versions. If the scanner detects a virus, then delete the infected file. Later you should scan your source disk for the infected file.
8. Remove the emergency floppy and reboot the computer. Your computer should boot up correctly.
9. Insert the emergency floppy and run the scanner again just to be sure you have detected every infected file.

Disinfecting a Computer System, Continued

CAUTION: Some of the newer viruses make a disk unmountable without the virus in memory (Monkey) or encrypt the disk, making it unintelligible without the virus in memory (One_half). If one of these viruses is detected:

- Restart your computer from the hard disk, letting the virus take control again.
- Copy any important files onto a floppy disk before removing the virus. Copy only document files if possible and assume that the floppy is infected with the virus after copying those files.
- Then disinfect the hard disk.
- When you finish disinfecting the hard disk, scan the floppy and note any infected files.
- Insert the floppy into your disk drive A: and copy any uninfected files back onto your hard drive.

WARNING: DO NOT reboot your system with an infected floppy disk in drive A:. Your system can be reinfected by a virus if you run an infected program or boot up with the infected floppy in disk drive A:.

10. Scan any floppy disks that may have been infected by your computer. Keep in mind that the virus could have been active for months before you discovered it.
11. Inform anyone with whom you shared floppy disks that their system may have been infected by your computer, and suggest that they scan their system.

Potential Disinfection Problems

Encrypted Viruses

Encrypted viruses such as the Satan Bug are particularly difficult to remove from an infected program. Most viruses of this type attach themselves to the end of a program, remove a small piece from the beginning of the program, and insert code at the beginning that causes the virus code run before the program. When the virus code completes its run, it executes the small piece of program code it removed from the beginning of the program; then the virus continues with the original program. Therefore, when you run an infected program, you only notice a slight hesitation at the beginning when the virus code runs; then the infected program runs like normal.

Encrypted viruses often store the small piece of the normal program within the virus code and then encrypt the virus code. For an anti-virus program to be able to patch an infected program, the anti-virus program must be able to decrypt the encrypted virus to find the piece of missing code to return it to its original location. The Satan Bug virus has up to nine levels of encryption, and it uses a different level for each infection. Decrypting this much code is a very difficult process, so most anti-virus programs are not set up to repair programs infected with the Satan Bug virus.

However, some file signature scanning programs may save enough of the scanned files to be able to repair an infected program. The DPP package does save a sufficient amount of information to be able to repair a program infected with the Satan Bug virus, but you must have created the program signature file before your system was infected. Again, if at all possible, you should always replace infected files rather than repairing them to ensure you have undamaged copies.

Stealth Viruses

Stealth viruses are a special problem for virus scanners and program change detectors. An effective stealth virus hides its presence on a disk by diverting low-level disk read requests to different sectors; in this scenario, when a scanner examines a file, the file appears to be uninfected when, in fact, it is infected with a virus.

Potential Disinfection Problems, Continued

For example, this screen shows the master boot record (MBR) of a hard drive with the One_half stealth 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...|iÛP P., #
#00000010: BF 00 06 B9 00 01 F2 A5 - EA 1D 06 00 00 BE BE 07 ..... Ñ..... #
#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 .uô..î.îL.îôâ... #
#00000040: CB 74 1A 80 3C 00 74 F4 - BE 8B 06 AC 3C 00 74 0B .t ç<.tÛ.î..<.t. #
#00000050: 56 BB 07 00 B4 0E CD 10 - 5E EB F0 EB FE BF 05 00 V .....^..ÿ..... #
#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. ....}ù= #
#00000080: 55 AA 75 C7 8B F5 EA 00 - 7C 00 00 49 6E 76 61 6C U.u.îi..|..Inval #
#00000090: 69 64 20 70 61 72 74 69 - 74 69 6F 6 020 74 61 62 id partition tab #
#000000A0: 6C 65 00 45 72 72 6F 72 - 20 6C 6F 6ÀÛ64 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 ..... #
#<Error
#  Hard Disk 1                               Offset 0, hex 0 #
=====

```

Potential Disinfection Problems, Continued

This screen shows the same sector with the virus removed by booting with a clean, locked boot disk:

```
=====
#                               Disk Editor                               #
# Object Edit Link View Info Tools Help                               #
#Physical Sector: Cyl 0, Side 0, Sector 1                               #
#00000000: 33 DB FA BC 00 7C 8E D3 - FB 8E DB 83 2E 13 04 04 3α...|Ä. Äpâ.... #
#00000010: B1 06 CD 12 D3 E0 BA 80 - 00 8E C0 B9 0B 00 B8 07 .....†.Ç.Ä..... #
#00000020: 02 06 CD 13 B8 D3 00 50 - CB 7E 03 1C 83 C6 10 FE .....P.~.â... #
#00000030: CB 75 EF CD 18 8B 14 8B - 4C 02 8B EE 83 C6 10 FE .uô..i.iL.ióâ... #
#00000040: CB 74 1A 80 3C 00 74 F4 - BE 8B 06 AC 3C 00 74 0B .t Ç<.tÛ.i."<.t. #
#00000050: 56 BB 07 00 B4 0E CD 10 - 5E EB F0 EB FE BF 05 00 V .....^.ÿ..... #
#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. ....}ù= #
#00000080: 55 AA 75 C7 8B F5 EA 00 - 7C 00 00 49 6E 76 61 6C U.u.i1..|..Inval #
#00000090: 69 64 20 70 61 72 74 69 - 74 Ò9 6F 6E 20 74 61 62 id partition tab #
#000000A0: 6C 65 00 45 72 72 6F 72 - 20ÀÛÇ 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 ..... #
#<Error
# Hard Disk 1                               Offset 0, hex 0 #
=====
```

The block at the very beginning of the sector is the boot program that mounts the disk and starts MS-DOS. In an infected disk, the boot program contains a block of code that loads the virus into memory and runs the virus. The virus then runs the original boot code to start MS-DOS. To hide itself, the virus intercepts attempts to read the sectors containing the virus and replaces these sectors with images of uninfected sectors.

Potential Disinfection Problems, Continued

Defeating a Stealth Virus

A stealth virus cannot function if it is not in memory. Follow these steps to defeat a stealth virus:

1. Boot the system using a clean, locked floppy.
2. Use your scanner program to find and remove any virus.
If there is any chance that your scanner program on the hard disk is infected (you will usually receive a message if it is infected) have another copy of the scanner program on the clean, locked floppy to perform the scan.
3. If the scanner program on your hard disk is infected, shut down your system completely by turning the power off, then reboot to remove the virus from memory.

Pressing <Ctrl+Alt+Del> to reboot is not sufficient to remove most memory-resident viruses.

Unfortunately, some virus-infected hard drives cannot be mounted by a system without the virus in memory. Because a virus such as Monkey moves the partition table to a different location, the virus must be in memory for the system to access that moved table. Luckily, most virus scanners know how to locate and remove these viruses.

Network Connections

Most corporate PCs are attached to a network and many users worry that an infected file server could spread an infection to every computer on a net. While this is not impossible, infections of networked file servers are usually limited to the files in an infected user's partition, i.e., those files accessible for change by the user with the infected computer. If you can write or delete a file, you can infect it. Since you can not write or delete files in another user's partition, you cannot infect their files

The biggest risk with servers is posed to the files in the server's system and shared resources such as a word processor with a network license. These files cannot be infected by normal users, but they can be infected by the local system operator while he or she is performing maintenance on the system. If this occurs, every computer that uses the infected resource will be infected.

Potential Disinfection Problems, Continued

For example, CIAC is aware of a case where the LOGIN.EXE program in a Novell server was infected with a virus. As each workstation logged into the server, that workstation was infected with the virus. The entire network became infected rapidly. If the users had installed a suspicious-activity detector (refer to the section entitled "Using Suspicious-Activity Detectors"), the infection would have been prevented.

CAUTION: If you know your file server is infected with a virus, contact your system operator for assistance with disconnecting your computer from the network before turning on your computer.

Using Suspicious-Activity Detectors

Overview

The VirALERT and WIN-VA programs are suspicious-activity detectors. A suspicious-activity detector is a small TSR program that is loaded into memory at bootup and then watches over a system for virus-type activities. Suspicious activities include writing to the boot blocks of a disk, changing or creating an executable file, or going memory resident. When such an activity occurs, the suspicious-activity detector pauses the activity and displays a dialog box similar to this:

```
VirALERT: Warning!      Attacking program: INSTALL.EXE
      Attempt to create the file VIRHUNT.EXE!
Options:  Continue, Fail, Abort, Inactivate viralert or Reboot?
```

The dialog box allows you to continue or halt the activity (Fail or Abort options). Since some suspicious activity is normal, you must decide whether to stop or continue it. For example, this alert occurred when the installer copied the file VIRHUNT.EXE onto the hard disk. Since this is a normal activity, you would allow it to continue. However, when you start up your word processor and the suspicious-activity detector detects an attempt to change the executable file for your spreadsheet program, you should prevent the activity from occurring by using the Abort option, because an attempt on the spreadsheet program is not a normal activity for a word processor.

Using Suspicious-Activity Detectors, Continued

Installing VirALERT or WIN-VA

Load VirALERT or WIN-VA as a device driver in your CONFIG.SYS file. Normally, the DPP installer program will install the program for you. VirALERT has several options that allow you to set the type of suspicious activity. Each of the options is explained in the installer program and in Appendix A of this document.

In general, you should not set the options to detect all suspicious activity. If the suspicious-activity detector generates many alarms, you may not take close notice when a suspicious activity alarm indicates a virus is present. A reasonable setup for the CONFIG.SYS file is:

```
DEVICE=C:\DDI\VIRALERT.SYS TV Z=RESSCAN.COM, WIN-RS.COM
```

With this setup, VirALERT:

- checks for any attempts to write an executable file (T)
- watches for other TSR programs attempting to install themselves (V)
- warns you when VirALERT is off
- ignores the TSR programs RESSCAN.COM and WIN-RS.COM (Z=...)

In general, the installer completes this setup for you. When you boot your system, VirALERT may warn you of system programs such as MOUSE.COM going memory resident. If these programs are supposed to go resident, add their names to the list of files following the “Z=” option and VirALERT will ignore them.

Deactivating VirALERT

If you are performing an activity that sets off the suspicious-activity detector, (e.g., copying a directory full of executable files), you will probably be inconvenienced by having to continue pressing **C** (Continue) every time the dialog box displays. You can turn VirALERT off for a short time.

Using Suspicious-Activity Detectors, Continued

To disable VirALERT:

1. Press **I** (Inactivate) to turn VirALERT off for the duration of this copy command. VirALERT automatically turns back on again when the command completes.

OR

To toggle VirALERT off:

1. Press **<Alt+V>** to see the VirALERT dialog box.
2. Press **<Space bar>** until "OFF" displays, then press **<Esc>** to continue.
3. Repeat this sequence to toggle VirALERT on again.

Lowering Sensitivity

The average user probably does not want an alarm to go off every time he or she copies an executable file. It has been CIAC's experience that if the alarms are activated many times, the average user stops checking to see if infections are valid and just presses **C** (Continue) every time they display. To lower the sensitivity of VirALERT so it does not check accesses to executable files, use this setup for the CONFIG.SYS file:

```
DEVICE=C:\DDI\VIRALERT.SYS TV X=* .EXE,* .COM Z=RESSCAN.COM,  
WIN-RS.COM
```

CAUTION: With this setup, VirALERT will not detect a virus infecting a program. VirALERT will detect attacks on the boot sector and system (.SYS) files and any attempt by a program to go memory resident. You must decide if the decreased alarm rate is worth the slightly increased risk of infection.

This setup works exactly the same as the full enabling setup, except attempts to create or modify .COM and .EXE files are ignored.

Using RESSCAN as a Memory-Resident Scanner

Overview

In addition to its capabilities as a virus scanner for disks and files, the RESSCAN program can function as a memory-resident program to check executable files as they are used. RESSCAN uses most of the same scanning options as VirHUNT and requires about 24K of memory when it is loaded.

Once RESSCAN is in memory, it performs these functions:

- When you run or copy executable files, RESSCAN checks the files for known viruses.
- RESSCAN checks the boot sectors of floppy disks.
- RESSCAN checks file signatures to see if a file has changed.

RESSCAN runs much slower than VirHUNT; therefore, unless you require the program's specific memory-resident capabilities, use VirHUNT for these functions.

Using RESSCAN

Follow these steps to prepare RESSCAN, have it go resident, and have it scan files for viruses and changes:

1. Perform a scan with VirHUNT, and save the configuration.
2. Use the following command line in your AUTOEXEC.BAT file:

```
C:\DDI\RESSCAN.EXE SWN
```

The SWN option sets the program not to scan, but to read the configuration file and then go resident. Any files you checked with VirHUNT will now be checked by RESSCAN as you use them.

What You See When Your Computer Has a Virus, Continued

Detecting a Virus Attack

Clearly, at this point you would not run either of the two files (CONTLIN1.EXE and CONTLIN2.EXE). Thus, the virus cannot get into memory and no other files will be infected. You should delete these files and replace them with uninfected copies. To demonstrate the infection process, however, this section assumes you run CONTLIN1.EXE, triggering the following events.

1. This VirALERT warning displays:

```
VirALERT: Warning!      Attacking program: CONTLIN1.EXE
                        Trace into DOS/BIOS call (a virus STEALTH technique)!
                        Options:  Abort, Continue, or Reboot?
```

The warning indicates that CONTLIN1.EXE is tracing the execution into the BIOS, probably to see where to patch into the system.

2. Normally, you would press **A** (Abort) to stop this activity, boot with a clean floppy, and use your virus scanner to start scanning disks.
3. However, if you press **C** (Continue) this alert displays:

```
VirALERT: Warning!      Attacking program: CONTLIN1.EXE
                        Attempt to write to boot record on drive C!
                        Options:  Continue, Fail, Abort, Inactivate viralert or Reboot?
```

This alert indicates the program CONTLIN1.EXE is attempting to write to the boot record of the hard drive. At this point, you could still press **A** (Abort). The virus is in memory, but it has not yet infected the boot record.

4. If you press **C** (Continue) again, your boot record is infected.
-

What You See When Your Computer Has a Virus, Continued

Detecting an Infected Boot Record

The next time you boot up your computer, the virus is loaded into memory before anything else.

1. In this example, when VirALERT loads during the boot process, it detects that system interrupt 21 has been diverted for some reason. This screen displays:

```
=====
#                                                                 #
#                                                                 #
#Windows-VirALERT V4.0E (c) 1989-94 by DDI.  All Rights Reserved. #
#                                                                 #
#                                                                 #
#WARNING!                                                         #
#                                                                 #
#System interrupt 21 is pointing to a "non-existent" block of memory, #
#a common virus signature.                                         #
#                                                                 #
#If you are aware of this, press any key to continue.              #
#                                                                 #
#If this is a problem, the suggested action is to turn off the machine, #
#leave it off for a minute, then re-boot from a trusted floppy.   #
#Cleanup action may then be taken.                                  #
#                                                                 #
#=====
```

2. VirALERT allows you to turn off your computer and get out your anti-virus tool kit.
3. If you continue activity instead of shutting down, your operation appears normal, except the virus is quietly infecting executable files whenever you access them.

Scanning with an Infected Scanner

Your system is now infected and the One_half virus is in memory. In this example, you run VirHUNT, disinfect it, and check the memory for infection.

What You See When Your Computer Has a Virus, Continued

1. If you run the VirHUNT program to check the disk, this screen displays:

```
=====
#                                                                 #
#E:\>cd ddi                                                    #
#                                                                 #
#E:\DDI>virhunt                                                #
#                                                                 #
#Security prefix Copyright 1991 by DDI                          #
#                                                                 #
#                                                                 #
#VIRHUNT.EXE, protected on  9-14-94                             #
#                                                                 #
#Security analysis in progress...                               #
#                                                                 #
#Virus detected: do you wish to attempt removal (Y/N)?         #
#=====
```

This screen shows VirHUNT completed its self-check, determined that it was infected, and now allows you the option to remove the infection. Here is another point where you should shut down, get out your anti-virus tools, and go to work disinfecting your disk.

2. However, in this example, you press **Y** to disinfect VirHUNT and then run VirHUNT to scan the hard drive, including a memory scan. This screen displays:

```
=====
#          <<<<<<  Virus Hunt and Destroy V4.0E (c) DDI 1989-94  >>>>>>          #
#                                                                 #
#                                                                 #
#                                                                 #
#                                                                 #
# WARNING!  One Half                                           #
#                                                                 #
# This virus can infect files during a virus scan, or hide from a #
# virus scan.                                                  #
# Virus scanning should NOT continue.                          #
#                                                                 #
#                                                                 #
# The action you must take now is to turn off your system, wait #
# 1 minute# and reboot from a write-protected floppy disk. Then, #
# use a clean copy                                             #
# of VIRHUNT (from a write-protected floppy) to clean up the system. #
#                                                                 #
# PLEASE TURN OFF YOUR SYSTEM NOW!                             #
#=====
```

At this point, VirHUNT locks up your computer. Your only choice is to reboot.

What You See When Your Computer Has a Virus, Continued

In this example, you scan the disk without scanning memory first. Thus, the scanner cannot detect that the virus is in memory.

1. Run VirHUNT without scanning memory. When the scan completes, this screen displays:

```
=====
#          ««««« Virus Hunt and Destroy V4.0E (c) DDI 1989-94 »»»»» #
#          Sandy Sparks (CPPC), (510)422-6856, CIAC #
# Summary of virus scan on 10/24/94 at 15:07:23 #
#  INSTALL.EXE      One Half #
#  ARR.EXE          One Half #
#  ARRLITE.EXE     One Half #
#  ARRGLFIX.EXE    One Half #
# Directory: E:\BAD #
#  INSTALL.EXE     One Half #
# Directory: E:\ZIP204 #
#  PKUNZIP.EXE     One Half #
#  PKUNZJR.COM     One Half #
#  PKZIP.EXE       One Half #
#  PKZIPFIX.EXE   One Half #
#  ZIP2EXE.EXE    One Half #
# Directory: E:\ZIP204\ZZAP #
#  MAKECRC.EXE    One Half #
#  ZZAP.EXE       One Half #
# # #
# Scan Complete! 45 viruses found! #
# # #
# Files: 59 scanned, 177 total, 14 directories, 45 viruses #
# # #
#          Press any key to continue #
=====
```

The screen indicates most of the scanned files are infected with the virus. When the scanner opened the file to scan it, the memory-resident virus took control and infected the file, then the scanner scanned the file and found the new infection. Thus, running the scanner gave the virus access to every file scanned.

What You See When Your Computer Has a Virus, Continued

REMEMBER: If you scan a disk with a program-infecting virus in memory, every executable file you scan will be infected with the virus. Where initially you had only a few infected files, you now have an entire infected disk.

To scan an infected computer, you must ensure no virus is in memory before initiating the scan. If a virus is present in memory, you will either miss the virus because it is using stealth techniques to hide, or you will infect all your executable files.

To ensure that you do not have a virus in memory:

- Create a clean, locked boot-up floppy disk from a clean (uninfected) computer.
 - Turn your computer off for 30 seconds before rebooting.
 - **DO NOT** use Ctrl-Alt-Del to reboot.
 - Boot your system with the clean bootup disk.
 - Then, use your virus scanner to scan for viruses.
-

Appendix A

Instructions from the DPP Installer

This section presents text copied from the Data Physician Plus! installer program. The text describes how to install the programs in the package and what the various options mean.

VirHUNT

««««« VirHUNT/RESSCAN Installation V4.0E (c) DDI 1990-94 »»»»»

The VirHUNT program searches memory, boot records, and files for known viruses. When found, VirHUNT can optionally remove these viruses.

The default operation is to enter the program and go to the main menu, where an options menu, an information menu, and a virus scan are available.

The default scan consists of memory, the boot record(s) of the current disk and the executable files on the current disk. Although viruses can be removed, the default is to report viruses only, not remove them.

All VirHUNT options are available as command line options, so that VirHUNT may be run without operator intervention (such as from AUTOEXEC.BAT).

VirHUNT can also create and use signature files, which contain information on your boot record(s) and files. Later, VirHUNT can do a signature scan, which compares the current state of your system to the information saved in the signature file. This allows VirHUNT to find, and often remove, previously unknown viruses (although DDI would appreciate a copy of any viruses you find for analysis).

The command line options for VirHUNT are:

DI : drive and/or directory to scan. DEFAULT: current drive
If the path starts with a drivename, forwardslash, or backslash, the DI is not needed, just the pathname.

US : user specified virus parameters for search/remove. DEFAULT: None

SW : scan what: all Memory, Real memory, Boot, Files (ie SWBF = Boot, Fil all Memory is 1Meg, Real memory is DOS memory (usually 640K).
Only 1 memory option can be specified. DEFAULT: MBF

FI : files scanned, All, Executable only, executable plus extension list. (FI.ext.ext ...) DEFAULT: Executable only

SC : scan subdirectories of given directory, Y or N. Default Y (yes).

VA : virus action, Remove, Wipefile, Halt system. DEFAULT: report only

VO : variations option, Yes (treat as virus) or No. DEFAULT: Yes

BA : backup on virus remove, Force, Ask, No. DEFAULT: No

PA : Pause on full screen, Yes or No. DEFAULT: No

PR : print scan output, Yes, No, LPT1, LPT2, LPT3 DEFAULT: No

LI : scan output to list file. DEFAULT: None

DE : Describe viruses found, Text or pop-up Window. F1/F2 toggle

Instructions from the DPP Installer, Continued

Text/Window descriptions on and off during a scan. DEFAULT: None

SI : Signature scan mode. Scan, Create, Fast, Remove, report Newfiles.
legal combinations S, SF, SR, SN, SFN, SRN, C, CF DEFAULT: None

SF : signature file to use. DEFAULT: \VIRHUNT.SIG on default drive

EX : Exclude list for signature scan. Files in this list may change
without causing a signature changed message. DEFAULT: None

QU : quit to DOS after scan. DEFAULT: stay at VirHUNT main menu

QZ : quit to DOS after scan without pause, even if viruses found. Must
be used with the LI parameter. DEFAULT: stay at VirHUNT main menu

HD : scan all local hard drives (not network or ramdrives or...). This
allows same BAT or CFG on system with different hardware setups.

-C : force VirHUNT to use monochrome colors. If a monochrome display
is detected, monochrome colors are used by default.

-L : use Left hand mouse (left button is Esc, right button is Enter
instead of the default left button is Enter, right button is Esc)

-D : if not at target date for dated running (see configuration file
information below), quit to DOS.

-N : do not process VIRHUNT.CFG file(s) except for color information.
This is useful for setting up batch files to do specific tasks.

-S : Skip removal warning message. User assumes risks of bad removal.

EXAMPLES of VirHUNT command lines:

VIRHUNT C: D: FI.PIF.DLL QU

Scan memory, boot, all executable files, and all files with a .PIF
or .DLL extension on the C: and D: drives, quit to DOS when done.
If no viruses were found, VirHUNT will run without needing anything
(like a keypress) from the user.

VIRHUNT FIA DI\SCRIBBLE

Scan memory, the boot record of the current disk, and all files in
the \SCRIBBLE directory of the current disk.

VIRHUNT SIS SF\MYDISK.SIG

Do a normal scan of the current disk, and scan signatures for changes
using the signature file MYDISK.SIG in the root dir of the current disk

VIRHUNT SIS EX\EXCLUDE.LST DET

Do a normal scan of the current disk, and scan signatures for changes
using the default signature file VIRHUNT.SIG in the root dir of the
current disk. Do not report changes to files listed in \EXCLUDE.LST,
and describe viruses found as text in the scan report.

VirHUNT can also use an optional configuration file, VIRHUNT.CFG, which can
contain custom information such as special messages, a custom color scheme,
dated run, and command line parameters.

The easiest way to create a configuration file is to use the options and
configuration menus in VirHUNT until the program is setup the way you want,
and then have VirHUNT save the current configuration.

Instructions from the DPP Installer, Continued

Also, note that VirHUNT tries to process 2 configuration files when it is run, one in your current directory and one in the source directory for VIRHUNT.EXE. This allows network users to have both global parameters (such as custom messages, dated runs, or noabort) and local options (such as the local disk setup or custom colors).

RESSCAN

««««« VirHUNT/RESSCAN Installation V4.0E (c) DDI 1990-94 »»»»»

The RESSCAN program has two functions. The first is as a stand-alone virus scanning program, and as such it can scan memory, boot records, and files for known viruses.

RESSCAN can also create and use signature files, which contain information on your boot record(s) and files. Later, RESSCAN can do a signature scan, which compares the current state of your system to the information saved in the signature file. This allows RESSCAN to find previously unknown viruses (DDI would appreciate a copy of any viruses you find for analysis).

The second function is as a TSR (Terminate and Stay Resident) program, which watches the programs being run, and files being copied and manipulated, for infected files. If an infected file is found, a warning window is popped up on the screen, and the user must verify that the operation is to continue. Another module, installed by default, checks for boot viruses when floppies are used and when a reboot is tried. If signatures are used another module, installed by default, checks files being run/copied/manipulated against their stored signatures, and pops up a warning if any changes are found.

As a TSR, RESSCAN takes between 19K and 24K of memory, depending on which modules are installed.

RESSCAN can also use an optional configuration file, the same VIRHUNT.CFG file used by VirHUNT. RESSCAN will use the custom messages, command line parameters, and noabort information. The colors, and command line parameter specific to VirHUNT will be ignored, as they are not appropriate for RESSCAN

Also, note that RESSCAN tries to process 2 configuration files when it is run, one in your current directory and one in the source directory for RESSCAN.COM. This allows network users to have both global parameters (such as custom messages or noabort) and local options (such as the local disk setup).

RESSCAN uses overlay files for virus (RESSCAN.VIR) and memory (RESSCAN.MEM) scanning, and they must be present in the source directory for RESSCAN.COM. If they are not present or corrupt, RESSCAN will give an appropriate message. When resident, if RESSCAN finds its overlay to be missing it will periodically give a warning message (not every time, to cut down on annoying messages), and will always warn of a corrupt overlay file.

Instructions from the DPP Installer, Continued

Since RESSCAN now needs an overlay, it is not permitted to run from removable disks. To over-ride this (for emergencies or disks like Bernoulli drives), the -I command line parameter tells RESSCAN to ignore removable disk status

The command line options for RESSCAN are:

- R : do not attempt to remain resident. Options: S (do not install signature scan), B (do not install bootrecord check).
DEFAULT: try to install all modules TSR
- D : if not at target date for dated running (see configuration file information below), quit to DOS.
- N : do not process VIRHUNT.CFG file(s). This is useful for setting up batch files to do specific tasks.
- I : Ignore removable disk, run anyway.
- Opath : Alternate path to Overlays if RESSCAN source does not have them.
- E : Executables (COM/EXE) only checked when resident.
- DI : drive and/or directory to scan. DEFAULT: current drive
If the path starts with a drivename, forwardslash, or backslash, the DI is not needed, just the pathname.
- HD : scan all local hard drives (not network or ramdrives or...). This allows same BAT or CFG on system with different hardware setups.
- VA : Action to take if virus detected. Affects both virus scan and TSR operation. Legal value: Halt on virus detected.
DEFAULT: continue (initial scan), ask user (if memory resident).
- SW : scan what: all Memory, Real memory, Boot, Files (ie SWBF = Boot, Files) all Memory is 1Meg, Real memory is DOS memory (usually 640K).
Only 1 memory option can be specified. DEFAULT: MBF
- FI : files scanned, All, Executable only, executable plus extension list. (FI.ext.ext ...) DEFAULT: Executable only
- SC : scan subdirectories, Yes or No. DEFAULT: Yes
- SI : Scan signature file. Also: SISF fast scan, SIN scan and newfiles, SIC create signature file. DEFAULT: No signature scan
- SF : name of signature file to use. DEFAULT: \VIRHUNT.SIG on default drive
- EX : Exclude list for signature scan. Files in this list may change without causing a signature changed message. DEFAULT: None
- US : filename of user-defined virus signatures. DEFAULT: None

EXAMPLES of RESSCAN command lines:

```
RESSCAN C: D: FIA -R
```

Scan memory, boot(s) and all files on the C: and D: drives. Do not install RESSCAN as a resident program.

```
RESSCAN FI.PIF.DLL
```

Scan memory, boot(s), executable files, and files with .PIF or .DLL extensions on the default drive. Install RESSCAN as a resident program.

```
RESSCAN SWN VAH
```

Do not scan for viruses, but install RESSCAN to watch file execution and copy/manipulations, boot viruses, and signature changes. Halt system if a virus is detected.

Instructions from the DPP Installer, Continued

```
RESSCAN -RSB SIS SF\MYDISK.SIG EX\EXCLUDE.LST
Scan memory, boot(s) and files on current disk. Scan signatures for
changes using MYDISK.SIG in the root directory of the current disk.
If signatures changes are found, do NOT report them if the file is in
the list of excluded files. Install RESSCAN as a TSR to watch for
file viruses ONLY (do not install boot checking or signature checking).
```

WIN-RS

```
««««« VirHUNT/RESSCAN Installation V4.0E (c) DDI 1990-94 »»»»»
```

The Windows-RESSCAN program is the same as RESSCAN, except that it contains additional code to manipulate VGA cards, so that graphics programs and environments, such as Microsoft Windows, are properly handled when a warning box pops up.

However, this ability and the additional data to be saved when a warning box pops up requires an additional 8.5K of resident memory, and so this ability has been placed in a separate program. Note that if you do NOT have a VGA, additional data space is not reserved, and Windows-RESSCAN only takes approximately 1K more than the normal RESSCAN.

Otherwise, Windows-RESSCAN is the same as the normal RESSCAN.

For information on the RESSCAN program, press Enter, else press Esc to exit about.

RS-NET

```
««««« VirHUNT/RESSCAN Installation V4.0E (c) DDI 1990-94 »»»»»
```

RS-NET is a "helper" program for RESSCAN and Windows-RESSCAN when running with a network.

If RESSCAN is loaded before the network software (typically done in your AUTOEXEC.BAT file), when the network software takes over, RESSCAN may not see the DOS requests it is looking for.

To overcome this problem, there are two solutions:

- 1) load RESSCAN after your network software is loaded
- 2) run RS-NET after RESSCAN and your network software are loaded

Note that RS-NET is NOT a resident program itself, it simply instructs RESSCAN to make sure it is in the command chain.

Also, be sure to run RS-NET BEFORE you log into the network server, to protect yourself from anything that may be on the server.

Instructions from the DPP Installer, Continued

VirALERT

««««« VirHUNT/RESSCAN Installation V4.0E (c) DDI 1990-94 »»»»»

The VirALERT program is a device driver (an extension to DOS installed by means of a DEVICE= command in your CONFIG.SYS file) that monitors your system for suspicious activity. This watch includes looking for programs that try to modify the boot record of a disk and programs that try to obtain write access to executable (.COM or .EXE) or system (.SYS) files.

VirALERT also watches for programs that try to install themselves as resident programs and gives you the option of removing them from your system before they can do any damage.

In addition, VirALERT will check for suspicious memory blocks (possibly viruses in the boot sector of your disk) every time your system boots. When VirALERT is installed in your CONFIG.SYS file, there are several command line options that may be used. The format of the command line is:

```
DEVICE=VIRALERT.SYS d: W Q V T F I H X=list Y=list Z=list
```

The first parameter, d:, tells VirALERT the name of the first hard disk in your system, with the d replaced by the appropriate letter (i.e. C: or D: or E: or...). If it is not given, it defaults to C:.

The second parameter, W, tells VirALERT to warn the user of writes to executable or system files that use FCBs. FCBs can, in certain cases, access files without opening them, which this option will catch. This is a rare occurrence, and need not be used unless you suspect something is happening.

The third parameter, Q, tells VirALERT to watch for questionable writes to disk. Questionable writes are those that come from an executable program and are directed at the DOS area of the disk. Although they will not directly infect a file and may be legitimate, the user may wish to know about them. Again, this option only needs to be used if you suspect that something is happening.

```
DEVICE=VIRALERT.SYS d: W Q V T F I H X=list Y=list Z=list
```

The fourth parameter, V, tells VirALERT to warn you when it is off. It does this by displaying a green, blinking V in the upper-right corner of your screen when VirALERT has been toggled OFF (see the Alt-V hotkey, discussed below), to warn you that you are not being protected.

The fifth parameter, T, tells VirALERT to warn the user of TSR (resident program) installation. This warns the user of viruses that attempt to install themselves in memory.

The sixth parameter, F, tells VirALERT to watch for format calls that affect floppy disks, as well as watching the hard disk. This is needed only if you suspect that something is causing problems on your floppies. Also, note that the DOS FORMAT command does not truly format a hard disk, like it does to a floppy, so that VirALERT will not stop an accidental DOS FORMAT to the hard disk.

Instructions from the DPP Installer, Continued

The seventh parameter, I, tells VirALERT to skip the initial check for disconnected memory blocks. Although they can be signs of a virus, some machines reserve blocks of memory for use by BIOS, which can confuse VirALERT.

The eighth parameter, H, changes VirALERT's hotkey from Alt-V to Ctrl-Alt-V. This helps avoid conflict with programs that use the Alt-V combination internally.

The ninth parameter, X=list, tells VirALERT to exclude the associated list of files from being watched. For example:

```
X=MYFILE.EXE,*.SYS,AB?.COM
```

will make VirALERT ignore any files named MYFILE.EXE, any file with a .SYS extension, and .COM files with 3 character names starting with AB. Note that there is NO associated pathname, so that any file with the correct name will be excluded, and there is a maximum of 9 files in a list, which must be given without spaces.

The tenth parameter, Y=list, tells VirALERT to include the associated list of files in its protection. For example:

```
Y=*.OVL,MYFILE.TXT
```

will make VirALERT watch all files with a .OVL extension, and the file MYFILE.TXT. As for the include list, there is no associated pathname. Note that a file can be specified in BOTH the include and exclude lists. When this happens, the exclude list takes precedence, so that a command line like:

```
X=AUTOEXEC.BAT Y=*.BAT
```

will include all .BAT files EXCEPT for AUTOEXEC.BAT.

The eleventh parameter, Z=list, tells VirALERT to exclude the associated list of files from its TSR watch. For example:

```
Z=SK.COM,CED.COM,MYTSR*.EXE,MYTSR*.COM
```

will allow the programs SK and CED, and any programs starting with MYTSR to go resident without warning the user.

Note that T parameter must be specified before Z becomes useful.

When VirALERT gives a warning, there are several available options:

Continue - The operation is OK, so let it go.

Fail - Do nothing, and return an error to the caller.

Abort - Terminate the program and return to DOS. Since no cleanup is done, it is possible that this could later crash DOS.

Inactivate VirALERT - The operation is OK, and you want to turn VirALERT off for the duration of the current program.

Delete it - Remove the program attempting to stay resident.

Reboot - Force the computer to reboot, so the program is GONE.

Not all options will be available at any warning, as not all are appropriate at one time.

Instructions from the DPP Installer, Continued

VirALERT also has an associated hotkey, Alt-V, which can change the status between active (VirALERT is on duty), inactive (VirALERT will be quiet until the current program is finished or another program is run), and OFF (VirALERT will not watch until Alt-V is used to change its status). The default is that VirALERT is active.

WIN-VA

««««« VirHUNT/RESSCAN Installation V4.0E (c) DDI 1990-94 »»»»»

The Windows-VirALERT program is the same as VirALERT, except that it contains additional code to manipulate VGA cards, so that graphics programs and environments, such as Microsoft Windows, are properly handled when a warning box pops up.

However, this ability and the additional data to be saved when a warning box pops up requires an additional 8.5K of resident memory, and so this ability has been placed in a separate program. Note that if you do NOT have a VGA, additional data space is not reserved, and Windows-VirALERT only takes approximately 1K more than the normal VirALERT.

Otherwise, Windows-VirALERT is the same as the normal VirALERT.

For information on the VirALERT program, press Enter, else press Esc to exit about.

Recover

««««« VirHUNT/RESSCAN Installation V4.0E (c) DDI 1990-94 »»»»»

Recover allows the user to save the boot records of their hard drive(s) and CMOS setup information in a file on a floppy disk, as disaster recovery insurance, and restore it later if the need arises.

A reboot is forced after a recover, so that the new parameters will be in effect. If you have a serious system problem, you may need to restore your CMOS only, then restore your boot records, otherwise the program may not be able to identify the recovery file as belonging to your system.

While saving this information is a good piece of insurance, restoring it to your system is a "last-ditch" attempt to revive a dead system, and DDI cannot be responsible for any problems that arise from its use.

If you make any hardware changes to your system (add or remove drives or expansion boards) it is a good idea to create a new recovery file, so that its contents match the current state of your system.

Reader Comments

CIAC updates and enhances the documentation it produces. If you find errors in or have suggestions to improve this document, please fill out this form. Mail it to CIAC, Lawrence Livermore National Laboratory, P.O. Box 808, Mail Stop L-303, Livermore, CA, 94551-9900. Thank you.

List errors you find here. Please include page numbers.

List suggestions for improvement here.

Optional:

Name _____ Phone _____

Department of Energy

CIAC

Computer Incident Advisory Capabili

*Technical Information Department • Lawrence Livermore National Laboratory
University of California • Livermore, California 94551*

