Virus Detection System

This section contains the table of contents and the copyright information.

Table Of Contents

Copyright and Disclaimer

VDS (Virus Detection System) Manual

Version 3.1

Revision Date: **October 1996**

WARNING

THIS SOFTWARE AND MANUAL ARE BOTH PROTECTED BY U.S. COPYRIGHT LAW (TITLE 17 UNITED STATES CODE). UNAUTHORIZED REPRODUCTION AND/OR SALES MAY RESULT IN IMPRISONMENT OF UP TO ONE YEAR AND FINES OF UP TO $10,000 (17 USC 506). COPYRIGHT INFRINGERS MAY ALSO BE SUBJECT TO CIVIL LIABILITY.

Disclaimer

The developers and distributors of VDS make no warranty of any kind, either express or implied, with respect to this software and accompanying documentation. In no event shall the developers be liable for any damages arising out of the use of or inability to use the included programs. The entire risk as to the results and performance of this software package is assumed by the customer. We specifically disclaim any implied warranties of merchantability or fitness for any purpose. Use at your own risk.

The developers and distributors of VDS reserve the right to revise the software and accompanying documentation and to make changes in the contents without obligation to notify any person of such revision or changes.

Overview

What is VDS

VDS (Virus Detection System) is a comprehensive anti-virus package for IBM PC compatible computers running MS/PC DOS 3.0 and higher. It contains a set of well-designed tools that offer detection and easy removal of PC viruses. VDS includes many advanced features such as decoy launching, active stealth boot sector virus detection, self-recovery, and real-time virus monitoring to deal with both old and new viruses in an effective manner.

VDS is now Win95-aware

Starting with version 3.0v release, we added special features to VDS to operate better under Windows 95(tm). VDS can even remove many common boot sector viruses without even starting Windows 95 in DOS mode. In our tests, Windows 95 issued performance warnings if a boot sector infected the disk, but it could not get rid of it. VDS comes to the rescue. You can also use the icons we provide to set up shortcuts to VDS on the desktop; this is done automatically if you choose the Express installation. In addition, using Explorer, you can drag and drop folders onto the VDS icon, and it will start scanning automatically. INSTALL, starting with version 3.0y can create the shortcuts for you. Remember that preparing an emergency diskette is even more important under Windows 95 than regular DOS-based systems. Certain viruses such as **Empire.Monkey** render Windows 95 **unbootable**. VDS can now prepare a VDS emergency diskette for Windows 95 as well.

Compatibility and Network Support

VDS is Novell Netware-aware. It is not confused by dynamic drive mappings. It recognizes Netware server volumes. What this means is that instead of creating an integrity database for each mapped drive letter, you can create one for each volume. Even if the mappings change, you can still use the database for that volume. Furthermore, you can keep a copy of VDS on the server and scan each workstation as they login; and when you upgrade VDS, all workstations benefit from the upgrade without any extra effort.

Multi-Level Integrity Structure

VDS implements a sophisticated catalog system to maintain a flexible and multi-level integrity structure. You can create fingerprints for drives as well as subdirectories. And if you do not have a database for a subdirectory, you can still use an upper level database to verify the integrity of programs in that directory. In other words, if you wish to verify only the files in the DOS directory and you have created a fingerprint only for the whole drive, you can simply highlight the DOS directory and choose verify; VDS will do the rest. This approach makes sense since an upper level database contains all the integrity info for the programs that reside in the lower levels of the directory tree. VDS can track up to **32** different integrity databases easily! If you have some extended memory available, each integrity database can store up to **16000** fingerprints for programs.

Easy Installation For Networks

We have implemented a simpler installation procedure for networked environments. **System administrators need not be concerned about having to go to each workstation to install**. VDS package can be installed from the server down onto the workstation during login. It automatically determines the system parameters needed for a given workstation and loads itself onto the local hard drive if VDS is not already installed. The system administrator can further customize the operation of VDS by simply editing the default configuration file. **We supply detailed instructions for network system administrators to implement an effective anti-virus solution for their PCs using VDS**. An audit log feature is provided to facilitate tracking down an infection, should the need arise. Sample batch files for Banyan and Netware environments are provided.

Flexible Configuration

VDS provides configuration files in the spirit of Windows(tm) .INI files. This approach facilitates maintenance of several configurations to satisfy different needs. You can now keep all your integrity data on a floppy diskette, for example. Furthermore, you can specify which files are to be checked based on their extensions. VDS 3.1 can be used to verify the integrity of data files as well as programs. The operation of the scanners in the package, VDSFSCAN and VFSLITE, are also guided by a configuration file that you can modify easily. You can designate whether you wish to copy suspicious and infected programs to a quarantine directory, for example.

Object-Oriented User Interface

VDS sports one of the most functional user interfaces implemented in any anti-virus we have seen. Judge for yourself and please let us know if there are any other areas that would help make it even simpler. The main idea behind this interface is shifting the emphasis from action-oriented menus to object-oriented menus. No, we are not talking about polymorphism and all that jazz! It goes like this: There are certain objects to manipulate such as drives, directories, and files. The user concentrates on those. Then there are certain actions applied to those objects such as scanning, verification, and initialization. One-keystroke operations using the function keys are displayed at the bottom of the screen as a reminder. There is almost nothing to remember! Learn the concepts, and don't worry about the trivial details. If you
need help, just press the F1 key. By shifting the focus from actions to objects, VDS provides a more natural interface that many people seem to prefer. This is in sharp contrast to other multi-level menu interfaces that hide commonly used options.

Unusual Features

VDS includes unusual features such as **decoy launching**. You can launch a decoy in any directory you wish! If there is a file infector active in memory, there is a good chance VDS will capture a sample for you; even if it is a new virus!

VDS also provides reliable **generic virus cleaning**. This technique allows VDS to restore infected programs to their original state by using the integrity information. As the name suggests, the cleaning operation is generic and does not depend on knowing which virus attacked the file. Overwriting viruses obviously cannot be removed this way (or any other way besides restoration using originals). We had good success with most of the appender and prepender viruses that attach themselves to the programs without destroying the contents of the original file. After the restoration attempt, VDS double-checks the recovered program to see that it is exactly as the original. If this is not the case, it recommends restoration using clean backup copies, which is always the safest and the recommended solution.

VDS also attempts to **restore its own file** if it is infected. In many cases, you will have a good copy of VDS after this operation. If the recovery does not succeed, you should boot from a clean, write-protected DOS diskette, and copy the original VDS program to your hard disk.

More Modern Scanning

VDS 3.1 implements a modern scanning technique based on very sophisticated algorithms. The nice thing is that the speed is only slightly affected even if you add many new signatures. The scanners in the VDS package can be easily updated by obtaining the latest .SIG file from us and replacing the old one. This way quick updates become practical. You can also add your own virus signatures to temporarily handle a new virus infection. Using DUMPSIG program, extract a suitable signature and place it in XTERNAL.SIG file. This operation and the format of the signatures are explained in the documentation. All the scanners in the VDS package can use this external file. Note that for polymorphic viruses, it is necessary to obtain an update from us since such viruses cannot be identified using signatures. They require an algorithmic solution.

Memory-Resident Scanner

VDSTSR is a memory-resident virus scanner that checks each program before execution or copy operation for known viruses. The program weighs in at 46K, but it can be loaded high easily under DOS 5.0 and later versions as well as other popular memory managers that provide upper memory blocks. It can also swap virus information to disk to reduce its memory footprint significantly (down to about 26K). VDSTSR blocks many common viruses before they activate, and it also protects the system areas such as the MBR/BR of your hard disk. When you access the boot sector of a floppy diskette, it scans the boot sector and warns you if a virus is discovered.

More Network Support

To help out the network administrators, we are providing a utility called **ISVDSTSR** (a 17-byte program) that returns a DOS error level depending on whether VDSTSR is loaded in memory. By checking the error level in a batch file, the system administrator can implement several solutions to protect the LAN. For example, he/she can display a warning message and deny access until the user enables VDSTSR. What's even better is that he/she can load a copy of VDSTSR from the server at the time of login; this way, even if a user does not comply with the policy of having VDSTSR loaded on the workstation, the system administrator can have it his/her way!

Commitment To Quality Service And Products

VDS Advanced Research Group is committed to providing you with the state-of-the-art tools to deal with computer viruses that threaten your PCs. We develop anti-virus software and provide technical information on many topics such as polymorphic viruses (ask for a copy of our Polymorphic Engines paper). However, no solution can be effective unless it is properly used. We encourage managers to increase virus awareness among their people so that everyone stays alert. With a good dose of anti-viral software and some user-awareness, you can rest assured that your systems are well-protected against this 20th century electronic ailment.

Introduction

VDS offers a multi-layered defense against viruses. It start with scanning your disks for known viruses, removing those found, and setting up a detection and recovery database for your programs and the system areas of your hard disks. In addition, it offers to prepare an emergency diskette that you can use to recover from certain types of viruses more easily. VDS package includes a few carefully designed programs that make it easy to prevent and recover from viruses that attack IBM PC compatible computers.

VDS combines both virus-specific and generic techniques to handle both known and new viruses effectively. Today, there are several thousand viruses targeting PCs. Out of those, only a few hundred are confirmed to be in the wild. New viruses are written and distributed every day. Luckily most of them are so buggy that they do not get too far. However, there are enough of them to cause you grief and data loss. Popularity of Internet access also created a slippery medium for viruses to spread. In such a dynamic environment of threats, scanning is not adequate by itself, and it must be augmented by methods that are more generic in nature. VDS emphasizes integrity checking and recovery as its main goal. It also includes identification of thousands of viruses.

You can also supplement your antivirus defense with VDS. If your favorite scanner fails to detect a new virus, or it is unable to recover from certain infections, VDS may be able to help you solve your problem in many cases.

Tech Support and Registration

Technical Help

If you need technical assistance or have any questions, you can call **VDS-BBS at (717) 846-3873** and leave a message. Please set your communications parameters to 8,N,1. Modem speeds up to 28.8K V.34 are supported. If you are a registered user, you can also download the latest virus scan strings from the VDS-BBS. There is also an area on the BBS to upload suspected files for analysis.

How to register VDS

You can order a copy of VDS by filling out the form in **ORDER.TXT** and sending it to the authorized VDS dealer. Site licenses are available. You can e-mail any technical questions to **tyetiser@prolog.net** or leave a message on our **VDS-BBS (717) 846-3873.**

Background

Do you need anti-virus programs?

During the past years we have seen an increase in the number of viruses from a few dozen to several thousand, and many of the new viruses are becoming more sophisticated. In addition, almost every major business that uses microcomputers has experienced a virus infection on some scale. Even some shrink-wrapped software from major software developers has been infected. It is just too much of a gamble not to have anti-virus protection these days.

Will scanners protect me?

Many popular anti-virus products on the market   feature a scanner. They simply look for a sequence of identifying bytes (not necessarily consecutive) inside existing executable code such as that contained in program files and boot sectors. This approach works quite well for many viruses. The trouble is that a pattern searching approach requires fore-knowledge of specific viruses and their identifiers. This means that they are useless against new, unknown viruses. In addition, new viruses which mutate upon each infection have been developed. They make extraction of an easily discernible search pattern impossible.

How is VDS Different?

VDS Advanced Research Group would like to shift the focus from simple pattern matching to one of analyzing viral behavior. In this way, we can offer a more comprehensive solution. You must remember that scanners were first developed by well-meaning hackers who lacked a clear, long-term perspective in this matter. It was the most obvious and easiest thing to do at the time and scanners became popular over time.

If you are faced with the problem of recurring virus infections, or have data that just cannot be replaced without significant loss, you are invited to try VDS on your system. VDS ensures easy detection and eradication with little user intervention.

What is VDS?

VDS is a set of programs designed to contain the spread of computer viruses that target PCs running MS/PC DOS 3.0 or above.   VDS works by providing early detection and quick recovery. The operation of VDS is not virus-specific. In addition, the current implementation does not rely on a memory-resident program which degrades the performance of your computer by verifying programs every time they are run; however, an independent memory-resident scanner is also provided. VDS installs itself on your system using a special process which checks first for known viruses, and then creates a fingerprint of all system areas and executable files. From then on, VDS will thoroughly check the system at scheduled intervals and will notify you of any suspicious modifications detected regardless of whether the virus is a known variant or a new virus altogether.

Why VDS?

- It is NOT virus-specific.
- It does NOT need frequent upgrades.
- It does NOT require much user expertise.
- It is NOT a TSR (i.e. memory resident) with possible conflicts. This also means that it does not use up precious RAM. The An optional TSR module is provided.
- It maintains an audit log to pinpoint how a virus entered the system.
- It can use an **external virus signature database** for easy updates.

- It works even when a stealth virus is active in memory.
- It can handle any size DOS disk.
- It is compatible with DOS 3.0 and above.
- It supports **MS Windows 3.x** and **MS Windows 95**.
- It can **capture some memory-resident viruses** to speed up diagnosis.
- It can **recover a damaged partition table** easily.
- It can fix an infected boot sector on the fly.
- It is blazingly **fast**.
- It includes an automated boot sector recovery tool.
- It works on **Novell Netware**, **Banyan**, and **Lantastic** network drives.
- It can usually **heal itself** even when infected.
- It automatically updates the baseline after additions/deletions.
- It can identify most common viruses by name.
- It can be set to run based on a user-defined schedule.
- It can remove most known and unknown viruses generically.
- It can **create an emergency diskette** for extra safety.
- It sports a very intuitive object-oriented user interface.
- It includes a **robust integrity checker** for ultimate defense against viruses.

Components of VDS

VDS package includes the following components:

VDS.EXE

An **integrity checker** that creates a fingerprint database for possible virus targets (programs, boot sectors) and verifies them later for suspicious modifications. In the case of such modifications, the integrity checker offers to restore the affected areas to their original state by using **generic disinfection** techniques, and backups (for system areas). If the restoration attempt fails, the integrity checker informs the user and requests permission to remove the damaged object by deletion. For example, some overwriting viruses do not preserve the functionality of their victims. To be able to restore such programs, one needs to use the original copies or good backups. In 95% of the cases that involve a virus that can successfully spread, restoration by generic disinfection is possible, and guarantees 100% recovery. Viruses that corrupt the operation of their victims get noticed easily and do not tend to get too far.

VDSFSCAN.EXE

A **known and heuristic virus scanner** that searches for patterns or code sequences and uses advanced algorithms to identify polymorphic and simple viruses inside executable code such as program files and boot sectors. It can also use a user-defined signature file to permit the addition of newly discovered viruses.

VDSTSR.EXE

A memory-resident (TSR) program that searches programs before they are run or optionally before they are copied. It also examines the boot sector of a floppy diskette that may have been left in drive A: before warmboot attempts. What's more, it can scan programs being unzipped or de-archived by a compression utility regardless of the version or the maker of such software. In other words, you do not need to update the TSR just because you decided to use a newer release of your favorite file compression utility. It also provides mechanisms to render some stealth viruses inoperable.

VDSMSG.EXE

A small MS-Windows(tm) program that receives messages from VDSTSR if a virus is found, and reports them to the user in a Windows-style message box following an audible alert. This program remains in iconic state until there is a message to be displayed. It should be placed in the **startup group**. INSTALL will modify **WIN.INI** and add VDSMSG to the **run=** line by default in express installation mode.

ISVDSTSR.COM

A small (17 bytes) program that **sets the DOS errorlevel to indicate the presence of the TSR component** in memory. The purpose of this program is to allow system administrators in networked environments to enforce loading TSR anti-virus protection on workstations before they are permitted to access programs on a file server.

DUMPSIG.EXE

A virus signature extraction utility. It is useful when you need to add an external signature.

VITALFIX.EXE

A **disk repair utility** designed specifically to deal with boot sector infections. It provides the user with various options to eradicate a possible virus, to save and to restore important system information such as the partition table, and to search disks for a possibly relocated copy of the boot sector. It is much safer to use VITALFIX than other disk sector editors since it performs sanity checks before overwriting important sectors on a hard drive.

INSTALL.EXE

An installation program that automates loading VDS on local and on network drives. It prepares an emergency diskette for your computer so that you can check and restore system areas and program files after booting from a clean floppy diskette. This emergency diskette is formatted as a bootable DOS diskette and the required VDS components and fingerprint and recovery information are copied over.

VDSCATCH.BIN

A device driver that implements several **anti-stealth features** and aids VDS integrity checker in maintaining reliable operation even when a stealth virus is active in memory. It also **prohibits direct writes to the master and DOS boot sectors as well as low-level format** attempts.

System Requirements

Hardware & Software

VDS has the following minimum requirements and limitations to operate correctly:

- An IBM PC or compatible computer
- MS/PC-DOS 3.0 or higher
- 384K of available memory
- A hard drive (necessary only for integrity checks)
- Up to 4000 program files per integrity database (16000 if 192K of extended memory is available)
- Up to 32 integrity databases per catalog

In addition, VDSTSR takes up about 43K of memory when loaded. It can be loaded into upper memory area under DOS 5.0 or later. With the /Diskswap option, VDSTSR uses only 26K of memory. VDSCATCH.BIN device driver takes up about 300 bytes, and it can also be loaded high.

Some systems utilize disk compression software to increase the storage capacity of drives by compressing and decompressing data on the fly. On such systems, you must have the necessary device drivers loaded before VDS. MS-DOS 6.x now includes this optional feature by providing the DoubleSpace interface. The operation of DoubleSpace is well-integrated into DOS, and works in a transparent manner. VDS is tested and found to work as expected on drives compressed using DoubleSpace.

Installation

This section contains the details on how to install VDS on a workstation under DOS and MS Windows 95.

INSTALL

A. INSTALL Command Line Options

Here is the INSTALL command line options that you can use to set up VDS.

```
INSTALL.EXE       [{-|/}BDEH?MNRUTX]    [src_path]   [dest_path]
```

-Debug	Instruct VDS to create a debug trace.
-Banyan	Install on a Banyan server.
-M	Use monochrome screen attributes.
-Help or ?	To see the command line options with examples
-Emergency <path>	Prepare an emergency diskette.
-Xpress	Install with default values.
-Uninstall <path>	Remove VDS from the given directory.
-Tsr Off	Do NOT load VDSTSR from the AUTOEXEC.BAT
-Refresh <path>	Update the VDS emergency diskette
-Network <src> <dest>	Install VDS from the server directory src to the workstation. The .INI files in the src directory will be copied over to the dest.

How to Install VDS on a Workstation

You will need the VDS installation diskette, and a blank diskette that matches the size of your A: drive. Although you can install VDS from drive B: or from a temporary directory, the blank diskette has to match drive A:. since this diskette may be needed to boot the computer in case of an emergency that renders the hard disk inaccessible. The floppy restoration process requires you to use this VDS emergency diskette.

If you have DOS 6.22 or an older version of DOS, read the section titled Installation For DOS Users. If you are using Windows 95, then read Installation For MS Windows 95 Users.

Notes About Installation

- Express installation uses the default settings to configure the operation of VDS whereas custom setup allows you to modify many parameters to suit your needs. If you choose express setup, a suitable configuration file will be created and the necessary files will be transferred to the hard disk in **C:\VDSPRO31** directory.

- On **DOS** machines, if this is the first time you are installing VDS on your computer, express setup will modify your **AUTOEXEC.BAT** and **CONFIG.SYS** to add the lines needed to load, **VDSCATCH.BIN**, **VDSTSR.EXE** and run **VDS.EXE** every time you reboot the computer. If you have **MS Windows 3.x,** the **RUN=** line in **WIN.INI** will be modified to include **VDSMSG.EXE**. This small program communicates with VDSTSR and displays any warning messages VDSTSR would like to show you in a Windows style message box.

- Custom setup will prompt you for the VDS home directory, source of VDS files, the frequency of checks, and if the config.sys, autoexec.bat, and win.ini files should be updated. You will also have the opportunity to protect more than just the C: drive. You can always do this later by highlighting a drive letter in VDS, and pressing F5 key.

- In any case, your original AUTOEXEC.BAT will be saved in AUTOEXEC.VDS, and the original CONFIG.SYS will be saved in CONFIG.VDS.

- If you enabled floppy booting in CMOS, i.e. A: then C:, you can change it back to the hard disk or C: and then A:. Even if you haven't done that before, you are encouraged to set the boot sequence to C: and then A: so that an infected diskette left in drive A: by mistake will not activate a boot sector virus and infect your hard disk. Many new motherboards with a BIOS date of 1992 seem to have this option under "Advanced Settings" in CMOS. Consult your motherboard manual about how to accomplish this.

Installation For DOS Users

Some computers have a boot sequence setting in CMOS that allows booting from the hard disk even if there is a floppy diskette in drive A:. Before starting the installation, please change this setting to boot from drive A:.

You will need a clean bootable DOS diskette, preferably the original one. You should boot your machine from this clean diskette before starting installation. Make sure the DOS version on your hard disk matches the one on the bootable diskette. You can find out the DOS version by typing **VER** at the DOS command prompt. You should also run "CHKDSK C: /F" or "SCANDISK C:" to find and fix any crosslinked files or lost clusters on your drive.

1. Turn the computer off (NOTE: It is very important that you do not perform a warmboot by holding down Ctrl-Alt-Del keys since a virus can fake a warmboot and stay in memory).

2. Put the DOS diskette in drive A: (NOTE: The version of DOS on the floppy diskette must be the same as the one installed on your hard drive). Turn the computer on. It should boot from the floppy diskette.

3. If the boot was successful, you should now see the A:> prompt. If the system asks you for time and date, just press Enter until you are at the A:> prompt.

4. Remove the DOS diskette and put the **VDS program diskette** in drive A:

5. At the DOS command prompt, type **A:\INSTALL.EXE** and press ENTER.

6. VDS installation program will offer a choice of **Express** or **Custom** setup. We recommend you use the Express setup. This creates the **C:\VDSPRO31** directory and keeps almost everything VDS needs in that directory. It also sets up shortcuts on the desktop, and arranges VDS to do its daily checks when you start Windows 95. Complete checks are performed once a day by default.

7. You will next see the list of files on the hard drive scroll by as VDS scans for infections and creates the baseline profile of all executable files on the disk. There should be lots of disk activity. If VDS finds that there are infected files, you will be asked if VDS should remove them. After the installation is complete, INSTALL will offer to prepare an emergency diskette for your system. Answer YES, and put the blank diskette in drive A: after removing the VDS installation diskette. Let INSTALL format it for you.

8. After the emergency diskette is prepared, you should remove it from drive A:, write protect it by opening the tab at the bottom left corner of the diskette, and label it **VDS Emergency Diskette**. If you have more than one computer, you should also write on the diskette the name of the computer or something you can remember that machine by. **You MUST NOT use an emergency diskette prepared for one computer on another computer**. It stores information specific to each computer that will not be useful in recovery of a different computer; and it could even cause data loss if used incorrectly in some cases.

9. Store the emergency diskette somewhere you can find it. Reboot your computer.

Installation For MS Windows 95 Users

1. Put the **VDS program diskette** in drive A:

2. Click on the **Start** button located at the bottom left corner of your screen.

3. Choose **Run** from the menu that comes up.

4. In the Open: edit box, type **A:\SETUP.EXE**

5. Click on **OK** to start the installation.

6. VDS Setup program will offer a choice of **Express** or **Custom** setup. We recommend you use the Express setup. This creates the **C:\VDSPRO31** directory and keeps almost everything VDS needs in that directory. It also sets up shortcuts on the desktop, and arranges VDS to do its daily checks when you start Windows 95. Complete checks are performed once a day by default.

7. You will next see the list of files on the hard drive scroll by as VDS scans for infections and creates the baseline profile of all executable files on the disk. There should be lots of disk activity. If VDS finds that there are infected files, you will be asked if VDS should remove them.

8. Answer YES when Setup offers to prepare an emergency diskette. Put the blank diskette in drive A:, and let Setup format it for you.

9. After the emergency diskette is prepared, you should remove it from drive A:, write protect it by opening the tab on the bottom left corner of the diskette, and label it **VDS Emergency Diskette**. If you have more than one computer, you should also write on the diskette the name of the computer or something you can remember that machine by. **You MUST NOT use an emergency diskette prepared for one computer on another computer**. It stores information specific to each computer that will not be useful in recovery of a different computer; and it could even cause data loss if used incorrectly in some cases.

10. Store the emergency diskette somewhere you can find it. You are done installing VDS, restart your Windows 95.

Uninstalling VDS

You can remove VDS from your hard drive by running the INSTALL program with the -Uninstall command line option:

```
          C:\> C:\VDSPRO31\INSTALL    -U    C:\VDSPRO31       <enter>
```

If you have performed a custom setup and specified a different directory name, then you should substitute that name in the line above. INSTALL checks to see if there were other files in the directory before VDS was installed. If there were not any, it removes all the files in VDSPRO31 directory, and then the directory itself. If there were other files, it displays a warning message and aborts without removing any files. It is up to you to delete or keep any of those files. You need to perform a "manual" uninstall. Since VDS keeps almost all of its files in its own directory, removal is a simple procedure. You should also edit your CONFIG.SYS and AUTOEXEC.BAT to remove the lines loading VDS components. Your original CONFIG.SYS is renamed to CONFIG.VDS, and the original AUTOEXEC.BAT is renamed to AUTOEXEC.VDS during installation. You could use them as well; however, if you have installed any other programs after VDS, then they might have modified your AUTOEXEC.BAT. Be careful before you copy over the CONFIG.VDS and AUTOEXEC.VDS if that is the case.

You need to edit WIN.INI file and remove the VDSMSG.EXE from the RUN= line. Otherwise, you will get a warning message every time you start Windows about VDSTSR not being loaded.

Under Windows 95, you can use the **Add/Remove Programs** applet under Settings to uninstall VDS automatically. You can also run SETUP.EXE and choose the Uninstall option.

Operation Of VDS Components

This section describes the operation of various VDS components.

Operation Of VDS

A. Operational Cycle

After VDS has been installed on a known-to-be-clean system, a complete verification of the system areas is done each time the machine is started. A daily check of the entire hard disk will also be done, unless you have selected a specific frequency in which case a complete check will only be performed when the time period has elapsed. For best results, VDS should be run from the AUTOEXEC.BAT. It can also be run, just like any other program, at the user's discretion.

The **periodic checking** requires a computer with a real-time clock that can keep track of date even after the computer is turned off. Most systems have this capability. On older machines without a real-time clock, the frequency of checks cannot be specified.

The **VDSTSR** module provides users with the ability to scan programs before they are run or copied. Once loaded, the user does not need to specify which files to scan every time. VDSTSR will intercept requests to execute a program and will search for known viruses. If it finds an infection, it will post a simple warning message and prevent execution or copying of the infected file.

VDSTSR also **traps warmboot attempts** (CTRL-ALT-DEL) and scans the boot sector of the floppy disk in drive A: if one is present. This prevents spread of common boot sector infectors such as Stoned and Michelangelo.

B. How Does VDS Work?

The first time VDS is installed, a baseline for all executable files and the system areas such as the master boot record (MBR), partition table, and the boot record (BR) is established. A unique signature is computed for all executable objects on the disk. File name, size, date, time and signature are combined to initialize the records in the database. A similar authentication scheme is also used for the VDS program itself. The MBR, partition table, boot sector, command interpreter, VDSCATCH.BIN, VDSTSR.EXE and VDS.EXE are backed up. The backups will be used if these areas need to be recovered.

When VDS is run, it verifies the integrity of its own code. If it finds that no tampering has taken place, VDS introduces **decoys** (small executable programs created at run-time) to the system to see if an active virus will take the bait. Under normal circumstances, there is no legitimate reason why these decoys should be altered by any program. If the decoys are attacked, this indicates the presence of a virus with great accuracy. If an active virus is detected with this technique, VDS will tell you whether the attacker was of STEALTH or DUMB variety. If the modifications are masked by the virus, it is considered to be STEALTH, and DUMB otherwise. VDS uses a proprietary verification mechanism to detect if the virus attempted to mask the modifications it has made.

Some viruses do not fall for decoys that easily. In fact, only memory-resident program infecting viruses will attack decoys. VDS uses different techniques to catch other types of viruses not caught by decoys. However, those viruses which do attack the decoys will be captured and placed in either **POV.CCC** or **POV.XXX** (an acronym for Prisoner Of VDS) depending on which decoy(s) they attack. POV files can later be used to analyze the captured intruder, or for legal purposes. The reason for the strange extensions (XXX instead of EXE and CCC instead of COM) is to revent someone from accidentally activating the virus by executing the POV files. If you capture an intruder, please mail it to us on a diskette for interrogation, i.e. examination! This will allow us to keep track of what viruses are in the wild, and which areas are affected by certain viruses. You will have an opportunity to place the captured intruder in a file of your choosing, preferably on a floppy diskette so that you can maintain it for further evaluation on a test system without any further risk to the computer on which the virus was found. The captured intruder also makes it simple to extract a scan string if it turns out to be a new virus VDS did not identify. You can then put the extracted scan string into an external signature database and search for it on your other disks as well.

VDS will verify the system areas and all executable files. It will generate a report of modified files and newly added files since the last time VDS was run. The user is given an opportunity to override any alarms that may be set off. If you have added new files to the machine, then VDS will scan each file for known viruses, and if clean, will ask you if you want to add the file's signature to the database. If any changes in the form of infection, software configuration or addition of files are encountered, VDS records them in **VDS-STAT.LOG** file in the C:\VDSPRO31 directory. This is an ASCII text file and can be printed or viewed easily. It contains a date and time line showing when VDS was run. It is very useful to check this log when an infection is discovered to find out how the virus was most likely introduced to the system.

If suspicious modifications appear, VDS attempts to identify any virus(es) that may be responsible for the changes. A report of all identified viruses and the victims affected as well as the date and time of operation will be appended to VDS-STAT.LOG file. **VDS looks for known viruses in all newly added files to provide early identification of viruses introduced to the system**. If no known viruses are identified, then the names of scanned files will be written to VDS-STAT.LOG. If a file is determined to be modified, the user will be given a chance to restore it. If the restoration attempt fails, then you will be able to positively erase it. **Positive erase** means that the file will be overwritten to the end of the last cluster it occupies and then deleted. This operation is necessary since DOS leaves the contents of erased files intact allowing them to be recovered by a disk utility program. VDS prevents infected files from being recovered if you allow VDS to erase them.

The user can examine reported files at his/her discretion, and take whatever action s/he deems necessary. When a possible viral attack is detected, our recommendation is to turn off the computer, boot from a clean write-protected floppy containing the same version of DOS as your computer (preferably the VDS emergency diskette prepared during installation), and replace the suspicious files with the originals. In many cases of actual virus infection, VDS restoration can easily fix program files completely. Note that this generic cleaning approach is very different from virus-specific cleaning. It has the capability to recover even from unknown virus infections. What's more, VDS checks to see if the restoration attempt resulted in a full recovery. If not, VDS will warn you about the problem.

For most boot sector viruses, VDS will restore the partition or boot sector automatically using the backup it made during installation. This approach effectively takes the guesswork out of MBR/BR recovery. Many other programs look for a relocated MBR in a specific sector on the disk and then assume that they found the original without being certain. In some cases, they cause more damage than the virus could.

If automatic restoration is not successful, VDS provides a RESTORE option that will repair the partition sector using the backup copy saved on VDS emergency diskette. If you did not prepare an emergency diskette, and the hard disk becomes inaccessible, then you should either use VITALFIX or try a manual recovery. In most cases, an experienced computer user can restore the disk by following the simple instructions which accompany VDS. As we have previously stated, we strongly suggest that you backup your master boot record on a floppy diskette so that your recovery will be simple. You can use VITALFIX to do this for you if you did not choose to backup your MBR and BR during the installation of VDS.

C. VDS Command Line Options

Here are the command line options that VDS integrity checker accepts:

VDS.EXE   [{-|/}BIRDESVY]   [Drive: | Path]   [{-|/}CX<path>]

-Batch Drive:

- Check the system areas and the files depending on frequency. This option is the default used during Express installation. It must be followed by a drive letter.

-Install Drive:

- Create fingerprint database for the system areas and the files for a given drive. This option is used by INSTALL program to start VDS during installation. It is followed by a drive letter.

-Rescue

- Use the emergency diskette in drive A: to check the specified drive.

-Scan Drive: | Path

- Scan the specified drive or path.

-Verify Drive: | Path

- Perform integrity checks on the specified drive or path.

-X<path>

- Use the specified external signature file, not the default XTERNAL.SIG.

-C<path>

- Use the specified configuration file.

-D   C: D:

- Process multiple drives specified by drive letters.

-E

- Use SCSI-compatible code.

-Y

- Create \VDS-VDS.LOG

Examples:

To check drive C: for modifications using a non-default configuration file, type the following:

```
VDS   -V   C: -Cc:\integ\vds31.ini
```

To check drive C: using the emergency diskette, type the following:

```
VDS   -R   C:
```

To scan DOS directory for viruses and use an external signature file, type the following:

```
VDS   -S    -Xc:\virus\mysigs.txt   C:\DOS
```

To scan C: and D: drives for viruses, type the following:

```
        VDS   -S    -D   C:   D:
```

To perform automatic integrity checks,   include the following line in your AUTOEXEC.BAT

```
        VDS   -B   C:
```

D. Configuration (VDSPRO31.INI) File

Many of the operational parameters for VDS are specified in a file named VDSPRO31.INI, which can be found in the VDS home directory. This is a simple text file and it can be viewed or edited easily using an ASCII text editor. Following is an explanation of each line that can be placed in this file.

VDS configuration file contains sections marked by certain keywords inside square brackets. Currently, the following sections are supported:

```
        [HOMEDIR]
        [VERIFY]
        [EXT]
        [IGNORE_DIR]
        [IGNORE_FILE]
        [TREE]
        [REPORT]
        [MSG]
        [VDSMSG]
        [FLAGS]
```

Each section has different requirements for the type of information you can enter. The INSTALL program automatically creates an appropriate configuration file for you. If you wish to change certain operational parameters such as the files that should be excluded from integrity checks, you can do so by editing the configuration file with a text editor. Refer to the explanation below for details.

```
; This configuration file specifies operational parameters for VDS Pro.

; VDS.EXE and the system backup files are located in the following
; directory.
[HOMEDIR]
C:\VDSPRO31

; Integrity database files are located in the following directory.
[VERIFY]
C:\VDSPRO31

; Files with the following extensions are processed. Adding ??? forces
; VDS to scan/check all files.
[EXT]
SCAN = COM,EXE,SYS,OVL,BOO,
VERIFY = COM,EXE,SYS,OVL,BAT,

; Following directories are NOT processed.
; This is useful in development environments where programs are modified.
[IGNORE_DIR]
```

```
; Following files are NOT processed.
; INSTALL defaults to excluding CONFIG.SYS and AUTOEXEC.BAT.
[IGNORE_FILE]
C:\CONFIG.SYS
C:\AUTOEXEC.BAT

; Directory tree(s) are stored in the following directory.
; If you set it to A: or B:, VDS does not store trees.
[TREE]
C:\VDSPRO31

; Messages are written to the following file.
; If you change it to PRN, all messages are sent to the printer.
[REPORT]
C:\VDSPRO31\VDS-STAT.LOG

; Optional message to be displayed if a virus is found
[MSG]
Call System Administrator x5112 ASAP!

; Optional message to be displayed in Windows if VDSTSR find a virus [VDSMSG]
MSG=There is a virus on this diskett or file. Call x5112.

; Operational flags
[FLAGS]
; If you wish to maintain integrity information for data files
; set the QUICK_VERIFY to No.
QUICK_VERIFY = Yes
; Look for virus-like code sequences. False positives are likely. HEURISTIC_CHECK = Yes
; Stop if an infected file is found during scan.
PAUSE = No
; You can eliminate most of the beeps by setting it to No.
BEEP = Yes
; Make sure VDSCATCH.BIN is loaded from your CONFIG.SYS.
ANTI_STEALTH = Yes
; If a modified program file is found, you will need to confirm before
; recovery.
AUTO_RESTORE = No
; Default is one complete check per day, and system area checks only any
; other time VDS is run with -Batch option.
FREQUENCY = 1
; ENTER key can be assigned to SCAN or VERIFY a file
ENTER_KEY = Scan
```

VDS As A Scanner

VDS integrity checker can serve as an easy-to-use virus scanner that works on DOS-compatible drives, including LAN server drives. It offers two modes of operation:

- Interactive
- Command line

Interactive mode is based on a simple menu system that makes it very easy to access the advanced features of VDS, and it offers context-sensitive help (F1 key). Command-line mode can also be activated from batch files. VDS accepts various options to customize its operation. Once VDS is executed, you can scan multiple diskettes easily.

VDS presents a very intuitive object-oriented interface based on simple menus. By picking the object you wish to work on, you can exploit the powerful features of VDS without any need to consult this manual at all. Function keys are assigned to activate certain operations such as scanning and verification. Each operation applies to the object currently selected.

You can move between object selections using the up and down arrow keys. Pressing ENTER explores a finer level of detail for the members of the parent object. For example, by highlighting a drive and pressing the ENTER key loads the subdirectories found on that drive. The ESC key will get you out of a menu, or it will ask if you want to stop the search or integrity check operation. The CTRL-BREAK key combination will also result in a prompt asking if you want to stop the operation.

We encourage users to start their computer with a clean, write-protected, and bootable DOS system diskette prior to using VDS to ensure that no viruses are active in memory while scanning. Some viruses manipulate file access and try to hide their existence or spread the infection to other programs. Although, VDS will attempt to check for such viruses, the only guaranteed way to do an untampered search is after booting the computer from a clean system diskette.

VDS will also check its own program file to make sure it is not modified. If it is modified, it will warn you with a message, and it may abort its operation. VDS tries to ensure that it is unmodified to ensure correct operation.

In the case of boot sector infections, VDS will ask you if you would like to remove an identified virus. This option applies to the master boot sector on hard disks and the boot sector on floppy diskettes. You should use the SYS program included with DOS to remove boot sector infectors from the DOS boot record of a hard drive or to keep a system floppy diskette bootable. When VDS removes a virus from the boot sector of a floppy diskette, it constructs a **BPB** (BIOS Parameter Block) for the diskette and adds instructions to display a message you would get from a non-bootable diskette. In any case, the viral code will be overwritten. In the case of the hard drive master boot sector, VDS keeps the partition table intact and replaces the loader code, again overwriting any viral instructions. It will also attempt to verify that the partition table actually corresponds to the disk layout.

DUMPSIG and External Virus Signatures

To facilitate keeping up with new viruses, we have added an external signature capability to VDS. This external file is a simple ASCII text file and can be viewed or edited easily. You can also use the **/V**filename.ext command line option to specify a different path for the external signature file. This file can also be used by VDSFSCAN and VFSLITE. Here is the format you should use to add a virus signature entry in this file:

```
; This virus is not stealth
Disk Muncher
; Seems to infect only COM files
COM
; Here is the signature Joe extracted yesterday
FA 00 23 75 ?? 33 40 B8 ?? 90 90 90 CD 21
```

Lines that start with a **;** (semi-colon) are treated as comments and ignored. The order of each field is important. In other words, you should place the virus name before its type, and the type before the signature. The signature is assumed to be in hexadecimal. You can use spaces to separate each byte value, or have them in sequence next to each other. The number of bytes in the string must be no more than 16, and no less than 8. Wildcard characters are accepted. To indicate a wildcard byte, simply put **??** in the string. The first byte of the string cannot be a wildcard.

The type field can have one of the following values:

```
COM
EXE
BOTH
BOOT
FALSE
```

BOTH implies that the virus signature can be found in either COM or EXE files. BOOT indicates that the virus attacks Master or DOS boot sectors. FALSE is used to temporarily deal with false alarms; it refers to the signature extracted from a program file that is known to trigger a false alarm. You should still report any false alarms to us so that we can update the internal signatures.

VDS tries to read virus information for each entry. To keep memory requirements low, only 32 external signatures can be processed.

We will usually provide an updated signature file to our customers. In some cases, you may need to add a signature yourself. For example, if a new virus infects your computer and VDS captures a sample for you, then you can extract a signature and put it in the XTERNAL.SIG. In this way you can identify the virus on your disks without upgrading the scanner program. If you cannot extract a signature, please send us a sample and we will analyze the virus and provide you with a signature and instructions on how to handle it. When you extract a signature for a virus, you should take it from the program entry point on; otherwise, you will need to specify QUICK_SCAN=NO option in the configuration file to force VDS to examine each byte of the files it scans. If a COM file starts with a JMP instruction, for example, you should go to the destination of that jump first. To simplify this process, you should use DUMPSIG utility provided in the VDS package.

Note that some viruses (polymorphic) try to defy signature scanning by encrypting and changing themselves. In such cases, it may be necessary to update the scanner program.

```
DUMPSIG   <filename>
```

You can redirect the output from DUMPSIG to a text file by using standard DOS redirection facility as follows:

```
DUMPSIG   sample.exe    >   sigfile.txt
```

DUMPSIG outputs 256 bytes from the program entry point of a given file in hex format. You can then look at the output and pick a 16-byte search pattern; you should avoid using a pattern with many repeated values. By testing the selected pattern on a few infected samples, you can verify the reliability of your string. It is also important that the selected pattern does not trigger a false alarm on common files such as those included with DOS; so it is a very good idea to test it on DOS program files as well.

VDS Device Driver

VDS creates a device driver for your computer during installation. This device driver, named **VDSCATCH.BIN**, has a very simple purpose: Providing VDS with access to the operating system in a manner that is resistant to stealth viruses. This is necessary since some viruses have the capability to subvert the operating system calls to hide the modifications they have made to the programs. When such a beast is active in memory, it will look as though none of the programs are infected. By recording operating system access points very early in the startup process, VDSCATCH.BIN enhances the reliability of VDS scanner and integrity checker.   The memory requirement for this device driver is quite frugal, about 300 bytes!

Another function of this device driver is to disallow tracing certain key interrupts. Many stealth viruses use the trace mode available on the Intel 80x86 CPUs. This way, they can bypass monitoring software and spread undetected. VDSCATCH.BIN attempts to stop such tricks. **Note that some anti-virus packages use tracing as well, and they may complain.**

VDSTSR

VDSTSR provides memory-resident virus scanning before execution or copying of files as well as floppy diskette boot sectors before a warmboot attempt. If it determines that the file that is about to be run or copied contains a known virus, it will warn the user showing the name of the virus and then deny the request.

The purpose of VDSTSR is to **prevent introduction of viruses** to PCs in a transparent manner. In other words, the user need not run a virus scanner manually every time he/she runs a program or copies new files to his/her hard/floppy disk. If there is a floppy diskette containing a boot sector virus in drive A: and the user attempts to warmboot the computer without opening the drive door first, VDSTSR scans the floppy diskette for boot sector viruses and issues a warning. This effectively prevents infections from common boot sector viruses such as Stoned and Michelangelo.

As a side effect of this type of mechanism, copy operations will be slowed down by about **50%** depending on the system configuration. The apparent time delay in program loading, however, should be negligible. Optionally, the user can specify not to scan upon copy operations but only before execution of programs. This approach is recommended since it provides most of the protection without overall performance degradation of the computer system. The default behavior is **not to scan during copy** operations.

Another side effect is the memory required to keep all virus signatures and names in RAM. Although the code is barely 5K, the signature database takes up about 40K. The good news is that, VDSTSR can be loaded high under DOS 5.0 and above, therefore not using up any of the precious 640K conventional memory.

To keep the program size to a minimum, VDSTSR only provides a simple message displaying the virus name and the program as well as producing a beep on the system speaker to get the user's attention. It does not provide any options to unload it from memory or support other fancy but rarely used features. VDSTSR does not scan for complicated polymorphic viruses, either. Following example illustrates a typical case:

```
C:\TEST\FRODO.EXE
<beep> 4096 virus found in FRODO.EXE
Access denied <pause>
```

The last message comes from COMMAND.COM since VDSTSR issued an error code as response to the request to execute the program file FRODO.EXE.
During copy operations, the following message would be displayed:

```
COPY C:\TEST\FRODO.EXE   FRODO2.EXE
<beep> 4096 virus found in FRODO.EXE
Invalid function <pause>
```

If the user hits the Ctrl-Alt-Del key combination in order to reboot, and there is a floppy diskette in drive A: with an infected boot sector, a message such as the following is displayed:

```
<beep> Stoned-2 virus found in floppy diskette boot sector.
Remove the floppy diskette from drive A: now! <pause>
```

VDSTSR scans floppy diskette boot sectors upon access. For example, if you put a diskette in drive B: and issue the "DIR   B:" command, the boot sector will be scanned. If a virus is found, you will see a message showing the name of the virus. You can disable this by specifying the **/I** option.

VDSTSR has only a few command line options and does not require any special procedure to install. It requires DOS 3.0 or higher to operate.

```
VDSTSR    [/COPY]   [/DISKSWAP]   [/IGNORE BOOT SECTOR SCAN]
```

The default is not to scan during copy operations, but only before program execution and warmboot attempts. VDSTSR should be placed in the AUTOEXEC.BAT file before any other TSRs except network drivers and disk compression drivers.

A small utility program called ISVDSTSR.COM is supplied to allow system administrators in LAN environments to check if VDSTSR is loaded on a workstation before granting permission to login. All this tiny program does is issue a request to VDSTSR and see if it is answered properly, indicating that VDSTSR is operational in memory. If everything is working fine, ISVDSTSR will set DOS error level to 1. This can be used in a batch file as follows:

```
ISVDSTSR.COM
if errorlevel == 1 goto LOADED
echo You have not loaded VDSTSR on your system. You cannot login.
logout
:LOADED
```

VDSFSCAN

VDSFSCAN is an easy-to-use virus scanner that works on DOS-compatible drives, including LAN server drives. It comes in two flavors:

- Interactive
- Command Line.

Interactive version is implemented by the VDSFSCAN.EXE, and the command-line version is provided by VFSLITE.EXE.

Both programs share a common configuration file named VDSFSCAN.INI. This is an ASCII text file that modifies the operation of the scanner. You can edit the settings in the INI file to tailor it to your needs. VFSLITE is very useful in networked environments where a post-login scan is desired. It sets DOS error level so that the result of scanning can be checked in a batch file.

Command Line Options

VDSFSCAN accepts the following command line options:

VDSFSCAN.EXE [{-|/}Lcd] [{-|/}RV<filename>]
[{-|/}ABCDEGH?NPQUYZ] [-LCD] [{-|/}Fnn] [drive: | Path]

-A	All files regardless of type
-B	Break/ESC is NOT allowed
-C	Complete file scan
-D	Scan all local drives starting with C:
-E	Erase infected files
-Fnn	Frequency of scan in days (0-30). Default is scan every time.
-G	Perform heuristic scan. Off by default.
-H or ?	Help for command line options
-LCD	Use monochrome attributes on LCD notebook computers
-N	No memory scan. On by default.
-P	Do NOT pause. Default is pause.
-Q	Quiet scan. Do not beep.
-R	Output report. If no file is given, C:\VFS-STAT.LOG is used.
-S	Recursively scan subdirectories. Off by default.
-U	Upper memory scan (as well as base memory)
-V	Virus signature file. VFSLITE always looks for XTERNAL.SIG.
-Y	Generate debug log in \VDS-SCAN.LOG
-Z	OEM DOS compatibility mode

If run without any command line parameters, VDSFSCAN offers a menu-driven interface.

VFSLITE

VFSLITE is the command-line-only edition of VDSFSCAN. It does not have the elaborate menus with different colors, context-sensitive help, and other features that the regular VDSFSCAN has. VFSLITE is light only in its user interface, not its capabilities. In fact, it detects the same number of viruses as VDSFSCAN. It is slightly faster in operation, and it makes an ideal anti-virus tool for networked environments where a post-login scan is desired. It sets the DOS errorlevel to 1 if it finds a virus, just like VDSFSCAN. You can test this in a batch file and take appropriate actions such as denying access to the file server.

Options and default settings

The command line options are almost the same for VDSFSCAN. An INI file can be used to establish a consistent set of flag settings for everyone. When VDSFSCAN or VFSLITE starts, they look for an INI file named VDSFSCAN.INI in the same directory as the program. If it is not present, they look for the same file in the current directory. If it is not found in the current directory either, they use internal default settings. Since the INI file is processed first, the command line options can still override the settings in the INI file.

The default internal flag settings for VFSLITE are as follows:

LCD screen = No
Pause = Yes
Allow Break = Yes
Memory scan = Yes
Upper memory scan = No
Beep = Yes
Frequency of scan = 0 (every time)
Quarantine infected files = No
Generate report file = No
Whole file scan = No
Multiple floppy scan = No
All files scan = No
Erase infected files automatically = No
Heuristic scan = No

Note that the frequency of scan is also new. Before, only the integrity checker component of VDS allowed this. The frequency option works by creating and updating a file called C:\VDSFREQ.TXT. This text file has one line showing the last date and time of virus scan. It is updated as necessary. For this option to work correctly, the computer must have a hard drive and a battery-backed real-time clock. Most systems are equipped with such devices. If the frequency is set to 0, VFSLITE ignores the frequency file; otherwise, it will create or update it accordingly.

Configuration (VDSFSCAN.INI) File

The VDSFSCAN.INI file is a simple text file with the following format and entries:

1. Lines that start with a ; (semi-colon) are comments, and they are ignored.
2. Each keyword should be flushed to left and followed by an = (equal) sign.
3. After the equal sign, an appropriate value should follow. The value depends on the type of the entry, such as log file name, or a YES/NO.
4. Upper or lower case can be used interchangeably. Spaces are ignored.
5. Value only entries for directories and files to be ignored.

Another convenient feature is that you can include your own message in the .INI file. This message will be displayed if a virus is discovered. For example, the number to the help desk could be displayed.

Here is a sample .INI file:

```
; This is an INI file for VDSFSCAN-Lite 3.1
; It contains entries for flag settings that guide the program operation

; On laptops, set the following to Yes for easier-to-read screen output.
LCDSCREEN = No

; Message to display when a virus is found. Leave blank after = if none. ALERTMSG=Call
system administrator x5112 ASAP! You have a virus.

; Report should be sent to the following file. Leave blank after = if
; none.
REPORT=C:\VFS-STAT.LOG

; File for the user-defined signatures. Leave blank after = if none. EXTSIGS=C:\XTERNAL.SIG

; Quarantine directory where the infected/suspicious files are copied QUARANTINE=C:\VDS-
CELL

; Ignore the following directories
IGNOREDIR=1
C:\CODE

; Ignore the following files
IGNOREFILE=2
C:\CONFIG.SYS
C:\AUTOEXEC.BAT

; Frequency of scanning in days. Must be between 1-30. 0 means scan
; every time.
FREQUENCY=0

; Files are scanned entirely or partially. Leave it at partial (No)
; normally.
FULLSCAN=No

; Which files to scan. Normally, set it to No.
ALLSCAN=No

; Scan all local drives starting with C: if no command line parameters
; are given.
LOCALSCAN=No

; Scan base memory.
MEMSCAN=Yes

; Scan upper memory.
UMBSCAN=No

; Pause if a virus is discovered or an error has occurred.
```

```
PAUSE=Yes

; Allow user to stop scanning.
ALLOWBREAK=Yes

; Beep if a virus is discovered or an error has occurred.
BEEP=Yes

; Remove infected files. If PAUSE is set to No above, it is automatic.
ERASEFILE=No

; Heuristic scan is on by default. Set it to No if causes false positives HEURISTICSCAN=Yes
```

Command Line Options

VFSLITE accepts the following command line options:

VFSLITE.EXE [{-|/}R|V<filename>] [{-|/}ABCDEGH?LMNPQUYZ] [{-|/}Fnn]
[drive: | Path]

```
-A      All files regardless of type
-B      Break/ESC is NOT allowed
-C      Complete file scan
-D      Drives to scan follows. If no drives given, scan all local drives starting with C:
-E      Erase infected files
-Fnn    Frequency of scan in days (0-30). Default is scan every time.
-G      Perform heuristic scan. Off by default.
-H or ? Help for command line options
-L      LCD screen attributes should be used not color
-M      Multiple floppy diskettes will be scanned. Ask for the next disk.
-N      No memory scan
-P      Do NOT pause. Default is pause.
-Q      Quiet scan. Do not beep.
-R      Output report. If no file is given, C:\VFS-STAT.LOG is used.
-U      Upper memory scan (as well as base memory)
-V      Virus signature file. VFSLITE always looks for XTERNAL.SIG.
-Y      Generate debug log in \VDS-VFSL.LOG
-Z      Zoo-test. Log both infected and clean files during scan.
```

Examples:

To scan drive D:

```
VFSLITE   D:
```

To scan drive C once every three days:

```
VFSLITE   -F3   C:
```

To scan drives C: and D:

```
VFSLITE   -D   C: D:
```

To scan all local drives starting with C:

```
VFSLITE   -D
```

To scan all files on drive C:

```
VFSLITE   -A   C:
```

To scan C:\DOS directory:

```
          VFSLITE   C:\DOS
```

To scan multiple diskettes in drive A::

```
          VFSLITE   -M   A:
```

To scan entire contents of files on C:

```
          VFSLITE   -C   C:
```

To erase infected files on C:

```
          VFSLITE   -E   C:
```

To disable beep sound and scan drive C:

```
          VFSLITE   -Q   C:
```

To scan drive C: without pause (useful during "zoo" testing):

```
          VFSLITE   -P   C:
```

To specify a non-default external signature file:

```
          VFSLITE   -Vf:\vds31\mysigs.sig   C:
```

To specify a non-default report file:

```
          VFSLITE   -Rc:\results.vds   C:
```

To scan drive C: and put the results in VFS-STAT.LOG file:

```
          VFSLITE   -R   C:
```

To skip memory scan and scan drive C:

```
          VFSLITE   -N   C:
```

To scan base and upper memory and drive C:

```
          VFSLITE   -U   C:
```

To see this help message:

```
          VFSLITE   -H
```

DOS Errorlevels Returned

To facilitate use of VFSLITE in batch files, DOS errorlevel is set as follows:

errorlevel = 0	No viruses found
errorlevel = 1	Infected/suspicious files found
errorlevel = 2	Self-check failed

Here is an example batch file:

```
VFSLITE   C:
if errorlevel = 2 goto PROBLEM
if errorlevel = 1 goto VIRUS

goto END

:VIRUS
echo You might have a computer virus. Call help desk at 5112 ASAP!
```

```
pause
goto END

:PROBLEM
echo Virus scanner is damaged. Call help desk at 5112 to get a new copy! pause

:END
```

Differences between VDSFSCAN and VFSLITE options

There are a few command line options that work differently in VDSFSCAN. Some of these options are available only in one or the other; while others have a completely different purpose.

-M

- Instructs VFSLITE to scan multiple floppy disks, asking for the next disk after each one. VDSFSCAN does not have this option.

-S

- Instructs VDSFSCAN to recursively scan subdirectories within directories. VFSLITE interprets this option as "use SCSI-compatible" code on this machine.

-D

- VFSLITE allows drives to be specified following this option. VDSFSCAN interprets it as "Scan all local drives". Note that VFSLITE will also scan all local drives if no drives are specified.

-Z

- Instructs VDSFSCAN to use compatibility mode for decoy launching. VFSLITE interprets it as "Zoo-test" option, which forces every scanned file to be reported in the log. This option is for testing purposes only.

VDS Shell For Windows 95

VDS Pro 3.1 includes a Win32 application that serves as a central access point for the programs in the VDS package. In addition, it allows you to modify numerous settings for the VDS programs using the all-familiar tabbed dialogs.

You can activate each program by clicking on the corresponding button or using the pull-down menus. Here are the buttons and their functions:

Integrity Check

This button runs the VDS integrity checker, VDS.EXE.

Scan

This button runs the VDS interactive scanner, VDSFSCAN.EXE.
The shareware release does not include VDSFSCAN.EXE. Instead,
this button will bring up a folder selection dialog. Once you
pick a folder, VFSLITE will be run to scan that folder.

VITALFIX

This button runs VITALFIX disk utility. The shareware release
does not include VITALFIX.EXE.

User Manual

This button displays the VDS user manual in Windows 95 help format.

Emergency Disk

This button runs INSTALL.EXE with the -E option to prepare an
emergency diskette for your computer.

Configuration

This button brings up a 3-page tabbed dialog that allows you to
configure numerous options for VDS programs. They are:

1. General
   - Make An Audible Beep
   - Pause
   - Allow break/cancel
   - Use LCD/Mono Attributes
   - Use SCSI-compatible Code
   - Enable Antistealth Capability
   - Location of Internal Signatures
   - Location of External Signatures
   - Quarantine Infected Items in
   - User-defined Message

2. Scanner
   - Scan Entire File
   - Scan All Files
   - Zoo Scan
   - Delete Infected Files
   - Scan Upper Memory
   - Scan Memory
   - Use Heuristic Scan
   - Scan All Local Drives
   - Clean Automatically
   - Scan Subdirectories

- Generate Debug Log
- Ask for Next Diskette
- Generate Report Log
- Advanced
  - Exclude These Directories
  - Exclude These Files
  - Executable File Extensions
  - Scan Frequency (Days)

3. Integrity Checker
   - Verify Entire File
   - Delete If Recovery Fails
   - Recover Files Automatically
   - Verify All Files
   - Initialize Records For New Files Automatically
   - Generate Debug Log
   - Generate Report
   - Advanced
     - Exclude These Directories
     - Exclude These Files
     - Files To Verify By Extension
     - Frequency of Checks (Days)

View Log

This button loads the VDS audit log into notepad for easy viewing/printing.

Register

This button loads the VDS order form into notepad if you wish to purchase a registered copy.

Exit

This buttons exits the VDS Shell

SETUP for Windows 95

VDS Pro 3.1 includes a Win32-based setup program that makes it easier to install VDS under Windows 95. When you run SETUP.EXE, it displays a window with the following fields:

Source

You can type in the directory where the original VDS files are located, such as the A:\   where the VDS diskette is. Optionally, you canuse the Browse button to the right of the edit field, to pick the directory.

Destination

You need to enter the directory where you wish to install VDS. By default, this is set to C:\VDSPRO31.

Express Setup

This is the default mode of operation for setup. It uses C:\VDSPRO31 as the VDS home directory.

Custom Setup

You can use custom setup to change certain options. You will see another dialog with the following options to change:

Scan Frequency (in days)

You can change the scan frequency by using the up-down control to the right of the field to a value between 0 and 31.

Verify Frequency (in days)

You can change the frequency of complete integrity checks using the up-down control to the right of the field to a value between 0 and 31.

Show the Following Message If A Virus Is Found

If this is checked (has an X in the box), then VDS programs will show the message shown in the field shown below.

Message to Display

This is the message displayed when a virus is identified. You can change it to suit your needs.

Quarantine Infected Files

If this is checked (has an X in the box), then VDS programs will copy the infected files to the directory shown below.

Quarantine Directory

This is the directory where the infected programs are copied to.

Create Shortcuts

This option instructs SETUP to create shortcuts to VDS Shell on the desktop, and arrange for VDS to run automatically every time you restart Windows 95.

Prepare Emergency Diskette

This option instructs SETUP to ask you if you wish to prepare a VDS Emergency Diskette for your computer at the end of the installation.

Remove Old VDS

This option instructs SETUP to remove the old copy of VDS if it was installed on your system. Note that only the default installation will be removed. If you installed VDS in a non-default location, you will need to remove it manually.

Copy Program Files

This option instructs SETUP to copy the required VDS programs to the VDS home directory.

Initialize Database

This option instructs SETUP to run VDS.EXE and have it initialize a detection and recovery database for your computer. This has to be done at least once to be able to use the VDS integrity checker.

Create Debug Logs

This option instructs SETUP to create diagnostic logs in the root directory. Both VFSLITE and VDS will be run with a special option so that they also generate diagnostic logs. These files are useful when we are trying to determine if there was a compatibility problem on your system if VDS does not install properly. We recommend that you always generate debug logs during installation, and if something goes wrong, please send us these files. If everything goes as expected, then you can delete the debug logs. The files are named: VDS_VFSL.LOG, VDS-VDS.LOG, VDS31DBG.LOG. They are placed in the root directory of drive C:.

Install

This button starts the installation process

Help

This button loads the help file for SETUP

Uninstall

This button removes VDS from your drive. If you used custom setup, then please make sure the Destination field has the correct location of the VDS home directory.

Exit

This button exits SETUP.

VITALFIX

VITALFIX is a utility program designed to automate recovery from an MBR (master boot record) infection, and to allow the user to perform low level operations on a hard disk such as sector editing. It can place a fresh copy of MBR code without disturbing the existing partition table. It can backup an MBR to a file on a floppy diskette. It even allows you to take a clean MBR from one computer, and a partition table from an infected one, combine them together and put it back on the infected system, effectively replacing the viral code while leaving the partition table intact. This is possible since most computers partitioned using the same FDISK program will contain similar code, and differ only in the contents of their partition tables.

If you simply let VITALFIX construct an MBR for you, you will have our MBR code placed on your disk. Since this piece of code has to do standard stuff, there should not be any problems. Please let us know if it does not work on your system. We have tested it on several IBM computers and compatibles with a variety of hard disks.

VITALFIX is a menu-driven program. You simply highlight the option you are interested in and press enter. You could also press the first letter of an option to activate it. Context-sensitive help is available by pressing the F1 key.

VITALFIX has some interesting features such as the capability to search for a relocated MBR all over a hard disk and to view the contents of any given sector. You can also write contents of a file to a sector and vice versa. It also allows you to edit sectors. Please be very careful when doing any write operations since a simple mistake could damage your data.

You should always boot the computer from a write-protected, clean system diskette before using VITALFIX. This will eliminate any memory resident viruses or programs that may interfere with disk operations.

Command Line Options

VITALFIX has the following command line options:

VITALFIX [{-|/}X | LCD | H | ?]

-X	Compatibility mode. Use INT 13h.
-LCD	Use monochrome attributes.
-H or ?	Display command line options.

A. VDS Messages and Explanations

Message:

Partition sector modified. Will attempt to restore.

Reason:

There is a good chance that either a partition sector infector has entered the system, or some other damage to the partition sector has occurred.

Action:

VDS will attempt to restore the partition sector and reboot the system. If the verification fails again, VDS will abort the restoration attempt and recommend a floppy recovery using the VDS emergency diskette.

Message:

No message, VDS simply hangs the machine.

Reason:

If VDS has been running just fine, but stopped functioning now, then VDS.EXE may be corrupted either by accident or by an overwriting virus which failed to preserve its victim's operation. It is also possible that some TSR program caused a conflict. Assuming VDS runs as the first program in your AUTOEXEC.BAT file, and CONFIG.SYS is not modified, you should assume the worst case: a virus attack.

Action:

Reboot the computer from VDS emergency diskette or a write-protected known-to-be-clean system diskette. If you have prepared the VDS emergency diskette, then run VDS from A drive with the REPAIR option:

```
A:\VDS   -R   <enter>
```

* You can simply run **REPAIR.BAT**

Message:

VDS requires DOS 3.0 or higher to run.

Reason:

The version of DOS installed on your computer was below 3.0.

Action:

You need to upgrade to DOS 3.0 or above. VDS will not run on systems with a lower DOS version.

Message:

Error occurred during installation.

Reason:

This is a generic message that indicates a malfunction during installation.

Action:

You should see some other error messages come up before this one. The cause can be determined based on those. Go back and check if you followed all the steps in the installation procedure.

Message:

Different DOS version. If you upgraded DOS, reinstall VDS.

Reason:

DOS version during installation was different from the current one. Action: The system floppy used during installation should have the same DOS version you have on the hard disk.

Message:

Need one megabyte free space on hard disk to install VDS.

Reason:

VDS found that there is not enough space on the hard disk.

Action:

You should delete some files to free up space and then run INSTALL again.

Questions and Answers

This section addresses some common questions about VDS.

Q - Do I have to know a lot about viruses to be able to use VDS on my system?

A - Not at all. One of the design goals was to create a program that can be easily used by novice computer users. Viruses present some unique complexities even to the experienced computer security experts. VDS can alleviate most virus-related problems automatically. You are, however, encouraged to become familiar with general guidelines to deal with computer viruses.

Q - Can I run VDS under MS Windows 3.x?

A - Yes, you can. We recommend that you either create a PIF file with full window option on, or shell to DOS first. Do not try to switch tasks while VDS.EXE is running. VDSFSCAN can run in the background in 386 enhanced mode. VITALFIX should never be run from inside Windows since it accesses the hard disk directly.

Q - VDS found and removed 'Stoned-2' virus off my hard drive. Now what should I do?

A - Many boot sector viruses such as this one infect hard drives only if you boot off of an infected floppy. Therefore, you probably have one or more infected diskettes. You should run VFSLITE on your diskette immediately and let it clean them for you.

Q - It seems that VDS captured a new virus in a POV.CCC file. But should I do with it?

A - You should forward us a sample for analysis. There are several ways to contact us. The preferred method is uploading the sample to our tech support **BBS (717) 846-3873**. You can also send it electronically via Internet e-mail to **tyetiser@prolog.net**. You should first encrypt the sample either using **PGP** (send us a message and request our public key) or PKZIP with the password option. The password should be sent separately. We will contact you in this case. You can always send us a diskette via surface mail.

Q - Is VDS compatible with DOS 6.x?

A - Yes, it is. We have tested VDS on various systems running MS/PC DOS 3.0. 3.1, 3.2, 3.3, 4.01, 5.0, 6.0, 6.20, 6.21, 6.22. We did not encounter any problems. Please let us know if you do.

Q - Can I run VDS under OS/2?

A - You can run it in OS/2 DOS box in a limited fashion. Extensive testing under OS/2 has not been done. The scanners in the VDS package seem to work fine under OS/2. If you use dual boot or boot manager features of OS/2, don't install the VDS integrity checker.

Q - I have a program that requires to be run before other programs in AUTOEXEC.BAT. Since VDS should be the first program to run, how can I resolve this conflict?

A - There is no conflict from a technical point of view. The other programs that force you to run them first usually re-vector several interrupts to their memory resident code. If another program grabs these interrupts, then they would not be able to guarantee proper operation.

Running VDS as the first program does not affect these programs since VDS is not memory-resident and it does not hook any interrupts. If you run other resident programs, however, they may conflict with the operation of VDS. The solution is to run VDS as the very first program in AUTOEXEC.BAT. Remember that the other programs need protection against viruses as well. If VDS runs first, it can check them before a possibly infected program is run. If VDS itself is infected, it will notice that fact and warn you.

Q - My computer is infected with a virus already. How can I use VDS to deal with this problem?

A - The approach to this problem depends on what kind of a virus you are dealing with. VDS can help you locate which parts of the system are affected if it is a virus that can be identified using our search strings. If it is a boot sector infector, you can simply turn off the computer, boot from a write-protected floppy diskette and run SYS program to put a clean boot sector onto your hard drive. If it is a program file infector, you need to replace the infected files from the original distribution diskettes. In the case of partition sector viruses, we recommend that you use VITALFIX.EXE. This utility automates locating MBR, and even constructs one if necessary.   You may be able to get the original partition sector back, if the virus relocated it to another sector on track 0, head 0 (as some do). You need to fire up a low-level disk editor, and look through head 0, track 0. The first sector contains the Master Boot Record (partition sector), and may have been replaced by the virus code. Look at each sector (17 of them on an MFM drive), and see if any one has AA55 as the last two bytes in the sector. These identification bytes are present on all legitimate partition sectors as well as boot sectors. Remember that this is a trial-and-error process, so it may not work. You may want to seek assistance from a local computer "guru" if necessary. Make sure you save the current copy of the partition sector on a floppy diskette first. If the hard disk is accessible after booting from a floppy diskette, then the partition table (64 bytes near the end of the master boot record) may still be valid. The code that loads the active boot sector may belong to the virus. If you can extract the partition table information from the current copy of the partition sector, you may even be able to place it into a good partition sector you get from a similar computer with a similar disk. You can then place this combination of partition table from the infected system and partition sector code from the clean system on top of the current partition sector on the infected system and reboot. This might just do the trick. Be very careful, however, and backup all your data files before starting this surgical operation. You might end up clearing the MBR and repartitioning the disk as a last resort.

Q - I found out that my computer is infected with a boot sector virus. How can I use VDS to scan and clean my floppy disks?

A - Run VFSLITE on the infected diskette, and let it remove the virus for you. If you have bootable disks, removal will preserve the booting capability only if MS-DOS or IBM PC-DOS is installed. Cleaning other DOS variants may not result in a bootable diskette. At any rate, the virus will be removed. You should use the SYS command to remove boot sector viruses from bootable disks formatted under a DOS variant OS.

Q - Does VDS have a TURBO mode versus a SECURE mode?

A - Yes. If you set QUICK_VERIFY=YES in the configuration file, VDS will operate in TURBO verification mode, which is faster but less accurate than VERIFY mode. Turbo mode is not recommended for data integrity.

Q - How secure is VDS encryption scheme?

A - Our purpose was not to come up with an unbreakable (if there is any such scheme) encryption method, but to use something more secure than good old XOR. Contrary to popular belief, the robustness of an anti-virus integrity system cannot be measured by the sophistication of the encryption algorithm it uses. Some people even believe that they can deal with stealth viruses easily if they use an encryption scheme that cannot be forged. That is not so. The stealth viruses intercept the verification routine's attempts to access the modified executables on the disk, and present them with a clean copy. No matter how sophisticated the algorithm used to generate a signature is, it will be fooled every time since the verifier is getting clean (the same as the original) input. While these people are perfecting the technique to compute a one-way cipher of extreme complexity, stealth viruses are having a ball on the disk they choose to invade. Of course, if a direct attack is a concern, then more secure encryption methods are very useful. In the DOS environment, manipulating the disk access is much easier and works in most cases. So, if someone tells you they got a superior multi-stage encryption routine that can come up with secure keys for their anti-virus product, just ask them why they chose to waste their time on such an endeavor!   Viruses are not an attack to the secrecy but to the integrity and availability of computer systems. Unfortunately, many self-proclaimed experts seem to confuse these separate issues.

Q - I heard some programs create hidden files on the disk. Does VDS create any hidden files?

A - Absolutely not. We have nothing to hide from the end-users!   Almost everything VDS creates is restricted to the VDS home directory. Decoys and report files may be created in the root directory as well.

Q - Does the VDS authentication scheme eliminate the possibility of a trojan version of the program?

A - To some extent. "Trojanization" has been a problem with many software packages in the market. VDS authentication scheme provides a reasonable amount of assurance that the copy you have is actually created by the original developers. It is possible to circumvent this mechanism and display a fake message. This can be considered a direct attack. Remember, a direct attack against any program is possible (you can safely ignore those who claim otherwise). The purpose is to provide another layer of security. If every software product in the market put in as much effort as VDS does, there would be less incidents of trojans. You should get your programs from reliable sources. If you see a program claiming to do major database work, and it is only 4K long, you should double-check on it!

Q - I backup my hard disk regularly. Do I still need an anti-virus program to be safe?

A - Yes, you still need a program such as VDS. Backups can help when recovering from damage. The problem is by the time you notice that the system is infected, the virus may have been transferred to the backup media. When you restore the system, you may very well restore the virus too!   In some cases, the virus may corrupt the backup diskettes and render them useless. One person reported that Stoned virus corrupted all his backup diskettes while he tried to backup his hard disk to be able to perform a low-level format. Unfortunately, the Stoned virus was active in memory at the time. By the way, when was the last time you verified that you can actually restore from your backups?

Q - What are "POV" files?

A - POV stands for "Prisoner Of VDS". These files are created by VDS when it detects an active virus in memory that attacks upon file access. When VDS introduces decoys into the system, some viruses immediately attack them. VDS notices this fact and captures the intruder in a   file. VDS will also capture a modified boot or partition sector in POVBOOT.BBB or POVPART.PPP file in the VDS home directory. This feature speeds up the diagnosis process. In other words, you will have the captured virus stored in a file that you can analyze (or have someone analyze it since this would require familiarity with the 80x86 assembly language). Remember that not every virus can be caught this way. If you catch a virus, you are encouraged to mail it on a diskette to us for analysis.

Q - Is it possible for a data file to become infected by a virus?

A - The criteria for a virus to do anything at all is that it must gain control of the CPU. An ordinary data file will never have such control. The possibility exists for macro or script files that some application software packages provide to automate certain operations. There are no common viruses that exploit this feature. Another possibility is to cause damage as a side effect, for example, by redefining a key sequence as a substitute for a destructive command, assuming a driver such as ANSI.SYS is loaded. Again, these are very limited ways that a virus can propagate, if at all. Batch files can also be used to activate a program that contains a virus. The problem is that it is too obvious and will be detected easily.

Q - How do I prepare an emergency diskette after installation?

A - You can run the INSTALL program with the -E option to have it repeat the emergency diskette preparation step. To do this, type:

```
INSTALL.EXE   -E   C:\VDSPRO31
```

Q - How can I get rid of "VDSTSR no loaded" message that comes up every time I start Windows?

A - Edit WIN.INI located in the C:\WINDOWS directory. Delete the VDSMSG.EXE from the line RUN= near the beginning of the file. Save WIN.INI and restart Windows.

Q - What is C:\VDS-CELL directory for?

A - VDS puts any suspicious or infected files in that directory. This directory can be changed by editing the QUARANTINE entry in VDSFSCAN.INI file. The programs copied to the quarantine directory are renamed to non-executable extensions for safety. You should send us the files in the C:\VDS-CELL directory so that we can analyze them.

C. Known Problems and Conflicts

This section addresses various conflicts or problems with the operation of VDS that we are aware of. You are encouraged to report any problems you discover.

1. SETVER.EXE that comes with MS/PC DOS 5.0 causes false alarms.

SETVER.EXE program modifies itself to keep track of programs and the version of DOS they should get as a result of INT 21h, function 30h call. Many consider such self-modifying programs "ill-behaved". Until developers of DOS come up with a better way to accomplish the same task, you are likely to get false alarms. We do not intend to accommodate use of such a questionable practice.

2. When scanning a Netware volume, VDS reports an ERROR condition on some files.

Certain files such as NET$OBJ.SYS are open and locked by the Netware operating system. They contain bindery information. Any attempt to open them will result in an error condition. You should not be concerned since this is a feature not a bug!

3. Some programs are reported to be suspicious when I enable the HEURISTIC_SCAN.

Heuristic scan is a method that allows early recognition of viral code. Certain coding techniques are common to many viruses. By looking for such indications, VDS is able to recognize some new viruses. The problem is that there may be legitimate programs that also use such code. The only guaranteed way to establish whether a virus is present is by performing an analysis of the suspected program.   We try to minimize such false alarms, and we would be interested in hearing from you if you come across a suspicious file.

Viruses

This section contains information about viruses.

What is a Virus?

Virus Defined

A **virus** is a piece of   programming code that has the ability to replicate itself by attaching to other executable objects, either by logical or physical means. In addition to its replication task, a virus may have a manipulation task in the form of a damage routine. Most PC viruses are written in the 80x86 assembly language to keep their size small and to gain greater flexibility in manipulating the operating system and other program files.

Researchers classify PC viruses in several ways. We prefer to separate the **structure** of the implementation of viruses from the **objects they attack**. We classify them simply by their features and types.

Boot Sector Infections

A. Preliminary Information

There seems to be much confusion about the difference between a partition sector (Master Boot Record is another name for it) and a boot sector among many PC users. If you are already familiar with the organization of a typical hard disk, you can skip the rest of this section; otherwise, please read on.

The very first sector on a typical hard disk stores the partition information for the disk. Within the partition sector, a 64-byte area contains enough information to locate all physical partitions on the disk, and shows which partition is the active partition. The **active partition** is used to boot the computer. There can be **four physical partitions** on a disk. The partition sector is located outside of any partition boundaries and has enough code to determine the active partition, load the boot sector in that partition and transfer control to it. The code in the partition sector does not care which operating system it is loading. In fact, one reason for having partitions is to allow
coexistence of multiple operating systems on one hard disk. **FDISK** program that comes with DOS is used to manipulate the partition table.

Each partition has a boot sector. The **boot sector** holds certain information about that partition (in an area called BIOS Parameter Block or BPB) such as the number of sectors and number of FATs (file allocation table). In the case of the active partition, it also contains some code that loads the operating system. DOS partitions can be either **primary** or **extended** (extended partitions were added in DOS 3.3). The extended partition can be further subdivided into **logical drives**. DOS assigns a drive letter to each logical partition after it sets up all the primary partitions on all physcial drives present in the system. It then assigns letters to all of the logical partition on the first physical drive, second drive and so on until every partition has a unique drive letter. On most systems, the hard disk has only one primary partition, and it is accessed as drive C:. Any device-driven drive such as a CD-ROM is assigned a drive letter after all the hard disk partitions are processed. For example, the CD-ROM would be accessed as drive D:. To be bootable, DOS requires that the primary partition on the first physical drive is set up as the active partition.

FORMAT program with the /S option is used to make the active DOS partition bootable by setting up the necessary operating system files. FORMAT must also be run on every partition to be able store files. This is called high-level formatting. Floppy disks do not have partition sectors, they only have a boot sector. That's one reason low-level and high-level formatting is combined into one procedure in the case of floppy diskettes.

Since the partition sector contains vital information to access the drive, it is important that this information be protected. If you lose your partition sector, you might have to wipe out the MBR, and repartition the disk. Of course, this operation would make all files inaccessible. Fortunately, it is hardly ever necessary to take such an extreme step. If you have VDS in place, you should be able to restore your partition table information easily.

Nevertheless, if you cannot reconstruct the partition table so that you can backup your files, or if you just want to get rid of a virus residing in the MBR, you should know a few important facts.

1. A complete low level format of the entire hard disk is not necessary. Using a low level disk editor, you can write zeroes over the contents of the MBR and repartition the disk. This will get rid of the virus. In fact, certain types of hard drives, namely IDE, are not designed to be low level formatted by the end-user. Low level format is necessary on brand new drives that do not come pre-formatted from the manufacturer. Getting rid of

an MBR virus is just a matter of removing its code from MBR and putting a fresh copy of the standard MBR code.

2. FDISK will **not** put a fresh copy of the MBR code if the disk is already partitioned; therefore, an MBR virus can survive repartitioning by standard FDISK. This might surprise you, but it is a fact so dangerous to ignore. Worse yet, FDISK will destroy the boot records and FATs of any modified partitions. For example, if you repartition a drive with exactly the same parameters, **you will still lose access to your files**. If you have data on your hard drive, do NOT use FDISK except with the /MBR option if and only if the files are accessible after booting off of a clean diskette. It can do more damage than good if the partition table is not correct.

- MS/PC DOS 5.0 and higher includes an improved version of the FDISK program. It can replace the MBR code only, while leaving the partition table intact. Unfortunately, the DOS technical documentation did not mention this capability until recently.

The command is:

FDISK /MBR

3. If the partition table is intact, as is the case in most infections, you can recover all your data easily. To do this, you should use a utility like **VITALFIX**, or do it manually following the instructions in this document. For details, see the section titled MANUAL RECOVERY PROCEDURE under HOW TO DEAL WITH VIRUSES.

Following diagram illustrates the organization of a typical hard disk.

```
-------------------------------------------------------------------------------------
          Master Boot Record              Sec 1, Cyl 0, Head 0
-------------------------------------------------------------------------------------
usually the rest of the sectors on track 0, head 0 are not used
-------------------------------------------------------------------------------------
          Active Partition Boot Sector
-------------------------------------------------------------------------------------
          File Allocation Table 1 (FAT#1)
--------------------------------------------------------------------------------------         Partition 1
          File Allocation Table 2 (FAT#2)
-------------------------------------------------------------------------------------
          Root Directory
-------------------------------------------------------------------------------------

          Data Area for files

-------------------------------------------------------------------------------------
          Other Partition Boot Sector
-------------------------------------------------------------------------------------
          FAT #1
-------------------------------------------------------------------------------------
          FAT #2                                                   Partition 2
-------------------------------------------------------------------------------------
          Root Directory
-------------------------------------------------------------------------------------

          Data Area for files
```

B. How to recover with RESTORE option

If the partition table or the boot sector is modified, you can restore it as follows:

1. Turn off the computer.
2. Place the write-protected VDS emergency diskette in drive A.
3. Turn on the computer.
4. Run VDS.

```
A:\VDS   -R   <enter>
```

VDS will attempt to use the backup copy of the affected area to restore it. If it detects that the backup copy is also modified, it will abort the restoration attempt so as not to do more harm than good! The restoration process involves the partition sector, boot sector on the active partition, and COMMAND.COM.

5. If all goes well, VDS will ask you to remove any floppy diskettes and press a key to reboot the system. All system areas should pass the verification tests this time. If they do not, the restoration attempt was unsuccessful, and a manual recovery is necessary.

C. Manual Recovery Procedure

- This section assumes you have a standard system partitioned using FDISK, and running MS/PC DOS 5.0 or above. If you have a hard drive with a non-standard geometry, then the following procedure may be more complicated. Exercise caution during this recovery procedure, since you could accidentally render your disk unusable. If you can access the hard disk after booting the computer from a floppy diskette, you should backup all your data files first.

If you know or suspect that your hard drive is infected by a virus, you can attempt to restore it by carefully verifying that each point in the execution path during start-up is clean. To do that, you need to know what points are in the execution path. Refer to the diagram below.

First get a write-protected (preferably the original) DOS system diskette. You cannot format a diskette on a possibly infected system, and be positive that the diskette does not get infected. Some viruses stay in memory and infect the floppy diskettes whenever they are accessed. Turn the computer OFF. Place the system diskette in drive A: and close the drive door. Turn the computer ON. Never trust that a warm-boot (Ctrl-Alt-Del) will get rid of a memory resident virus. Some viruses are known to fake a warm-boot. Worse yet, some vicious viruses activate their damage routine when you press Ctrl-Alt-Del combination.

The purpose of the following procedure is to clean the system areas of a computer with a hard disk so that it is safe to boot from the hard disk. Verification of other program files are not considered in this discussion. Recommended recovery procedure for infected program files is to replace them with the originals. A utility program such as VDSFSCAN that searches for infected programs can speed up the process. Virus cleaning utilities are NOT recommended. If you know or suspect that a program is infected, copy over the original from the distribution diskette. This is the cleanest and the safest approach. If you have installed VDS integrity checker on your system, it could restore most programs to their original state easily and reliably; even new viruses can be removed with this procedure.

To attempt recovery, you will need a low level disk editor that allows you to read and write any sector on the disk. If you feel intimidated by manipulating your disk in this manner, please do not attempt a manual recovery without the help of a friend who has experience performing this type of an operation. Nevertheless, VITALFIX is very handy to do such low level manipulations.

On a standard PC, the startup sequence looks like the following:

Stage 1.

```
point A                  point B
-------------------------  --------------------------------------------------
ROM BIOS Code            Master Boot Record Code (0,0,1)
-------------------------  --------------------------------------------------
```

Stage 2.

```
point C                  point D            point E
-------------------------  ----------------  --------------------------
Boot Record Code         IBMBIO.COM       IBMDOS.COM
in Active Partition      or IO.SYS        or MSDOS.SYS
-------------------------  ----------------  --------------------------

point F                  point G                 point H
-------------------------  ----------------        --------------------------
Device drivers in        COMMAND.COM        Programs in AUTOEXEC.BAT
CONFIG.SYS
-------------------------  ----------------        --------------------------
```

Stage 1 is independent of any operating system. Point A is implemented in hardware and is not modifiable, therefore it cannot be infected. At point B, the code resides on the hard disk (head 0, cylinder 0, sector 1). The purpose of point B is to provide a mechanism to load different operating systems. You can have your disk partitioned so that one partition is for DOS, while another one is for some other operating system. By marking one of them as active in the partition table (located within the Master Boot Record), you can control which operating system will load upon bootup. The code in MBR simply locates the active partition by examining the partition table, loads the code in the boot sector of that partition and transfers control to it. The MBR is attacked by viruses such as Stoned since it provides very early control of the system. More sophisticated viruses can easily redirect BIOS disk access routines (the vector addresses reside in the first 1024 bytes of RAM and are modifiable) to evade detection.

Stage 2 is where a specific operating system comes into play. In the case of DOS, the code at point C loads the first system file (IBMBIO.COM) and transfers control to it. After initializing the DOS kernel, IBMBIO.COM processes the CONFIG.SYS file. Each device driver listed in CONFIG.SYS is loaded and initialized. IBMDOS.COM is also loaded at this time. At point G, COMMAND.COM gets control and processes AUTOEXEC.BAT file if there is one. Except for point A, all other points in the execution path are modifiable. You must assume that any modifiable code is prone to viral infections. During recovery you must assume the worst case and handle each point as if it is infected by a virus. You must also remember that a higher point depends on a lower point. In other words, if you do not clean point B, you cannot guarantee that point C will not be compromised afterwards.

The MBR code (point B) is easily replaceable. The key item at point B is the partition table which contains vital information to access the disk. If the hard disk is accessible after booting from a floppy (e.g., DIR C: works fine), then there is a good chance the partition table is intact. You should immediately extract the partition table information (64 bytes total) from the first sector on head 0, cylinder 0 and store it in a file on a floppy diskette. If you have a similar (uninfected) computer with a hard disk, you should make a copy of its MBR in a file.

The next step is to combine the partition table that you stored away with the clean MBR you have taken from the uninfected computer. The result is an uninfected MBR that can be used to replace the infected one. Make sure when you combine the two pieces, you are editing at the correct offset within the MBR sector. Our VITALFIX utility automates this whole process (except swapping diskettes, of course!). Here is a simple picture to clear things up:

Master Boot Record located at   sector 1 on head 0, cylinder 0

```
------------------------------------ 1
|         MBR code       |
|                        |
|                        |
|                        |
|-----------------------------------| 447
|-----------------------------------| Partition Table
|-----------------------------------| Entries
|-----------------------------------|
|-----------------------------------| 511
|         55             |
|-----------------------------------| 512
|         AA             |
------------------------------------
```

Note that the **partition table has four entries** making it possible to divide the disk into four distinct areas. The MBR code is the same on most PCs as long as you use the same FDISK program. The partition table depends on how the disk is set up. The last two bytes must be 55AA by convention.

Some viruses simply relocate the whole MBR sector to another location on the disk, then place their code in sector 1, head 0, cylinder 0. They also redirect disk access routines and present the original copy when someone attempts to access the MBR. This is an evasion technique used by certain viruses that target the MBR. Since you have booted from a clean floppy diskette, you do not have to worry about this. If you can find the original MBR on the disk (usually relocated to another sector on head 0, cylinder 0), then you could simply put it back to sector 1, head 0, cylinder 0 to recover. For example, one variant of Stoned virus places the original MBR to sector 7, head 0, cylinder 0. In that case, follow the procedure outlined above.

Once you restore the MBR, you can move on to point C and verify it. The easiest way to accomplish that is to use SYS.COM program included with DOS. SYS will put a fresh copy of the boot sector code as well as replacing IO.SYS and MSDOS.SYS. This operation cleans points C, D, and E (three birds with one stone).

Point F involves verifying each device driver listed in the CONFIG.SYS file. Unless you need a device driver to access the disk due to non-standard geometry, you can simply delete (or rename) CONFIG.SYS. Otherwise, you have to copy the device drivers from the original diskettes to the hard disk. Make sure you are copying over the ones that CONFIG.SYS activates.

Point G is easy to take care of by copying COMMAND.COM from the original DOS diskette to the hard disk. If you have a shell statement in CONFIG.SYS that specifies a different command interpreter, then make sure you replace that one with the original.

Point H can be handled by deleting (or renaming) AUTOEXEC.BAT since it is not required.

Now the system is ready to be booted from the hard disk without reactivating a possible virus. Of course, **the first time you run an infected program, everything you have cleaned so far might get reinfected**. Did we say dealing with viruses can be a little tricky?

Virus Attack Methods

A. Features of PC Viruses

Stealth Virus

A virus that has the capability to hide the modifications it has made to its victims to evade detection. For example, the virus may hide the file size increase when the user attempts to get a directory listing. Another example would be a boot sector virus that returns the original boot sector when a program attempts to read it. To accomplish such tricks, a stealth virus usually stays resident in memory and monitors disk access either at the DOS or BIOS level. This way, it can see each disk access request and alter the results to hide the modifications it has made. There are varying degrees of stealth capability. In other words, it may be possible to discover the presence of a virus using an alternate mechanism to examine the object that may have been affected.

Dumb Virus

A virus with no stealth capability. Such a virus makes no attempts to conceal its presence. The most apparent change is the increase in file size since the virus added its code to the program file. An alert user can notice such a change easily. This is the most common feature of PC viruses.

Encryptive Virus

A virus that keeps its code encrypted and includes a decryptor to restore itself. The purpose of encryption is to make it difficult to extract a scan string. The decryption routine is designed to contain variable sections so that it is not easily recognized. It is possible to detect such viruses using a wildcard pattern that matches the decryptor.

Polymorphic Virus

A virus that keeps its code encrypted and includes a highly variable decryptor to restore itself. It is not possible to extract a wildcard scan string to recognize the decryptor. One has to design an appropriate algorithm to detect it. We usually analyze the structure of the decryptor and identify its key features, and then use this information to implement a detection routine.

B. Types of PC Viruses

MBR/BR Virus

A virus that attacks the master boot record or the DOS boot record of a disk. This type of virus usually moves the original contents of the boot sector and replaces it with its own code. Key data structures within the boot sector (partition table or BIOS parameter block) are almost always left intact not to mess up the operation of DOS. A boot sector virus reserves memory for itself by reducing the base memory size (e.g., 640K to 638K), and copies its code to the top of memory. There are a few boot sector viruses that remain in low memory as well. Almost all boot sector viruses monitor the BIOS disk interrupt (INT 13h) to spread or to hide themselves. Every time a disk is accessed, they get control and check if the disk being accessed is already infected. If not, they can infect it before returning control to the original interrupt handler.

Program Infector

A virus that attaches to program files. There are a few subcategories for this type of viruses:

a. Simple Infector

A virus that modifies a program file physically to add its code. The program file entry point is adjusted so that the virus gets control when the program is executed.

b. Companion Virus

A virus that logically inserts itself into the search path so that it gets control when the user attempts to run a program that has the same file name. The most common variety exploits the fact that DOS runs a program file with a COM extension rather than the one with an EXE extension if both of them exist. Another possibility is to insert the virus in the search path. If the user does not specify the exact location of the program, then DOS will use the path to look for it. If the virus program comes before the actual program in the search path, then the virus will get executed. This type of virus is rare indeed.

c. System Infector

A virus that alters DOS system data structures so that it gets control instead of the program the user intends to run. For example, DIR-2 virus manipulates the directory entries to point the starting cluster to its location. When DOS reads the disk to load a program, the virus gets loaded. Another possibility is to insert the virus in a system location that DOS is known to always load.

Multi-partite Virus

A virus that can infect both program files and boot sector of a disk. Dealing with such a virus can be quite a nuisance since the first portion of the virus gets control of the system even before DOS is loaded. The virus can alter the system vectors to implement a potent stealth mechanism, for example. Removing this type of virus requires that all affected areas are restored.

C. Some Facts About Viruses

1. PC-based local area networks are NOT immune to viral attacks.

Network connections pose another question by making it easier for the virus to travel from one location to another. As long as the user has write access to the programs on a disk, it may be able to infect it. If the program file happens to be on a file server, all those that run it may cause the virus to jump to their local machines. Can you imagine what could happen if the superuser/supervisor runs an infected program on the LAN by mistake?

It is a misconception that PC-based networks are less susceptible to viruses. The boundaries of information flow are not always well-defined. Although many popular LAN operating systems provide various control mechanisms that can be used to implement robust anti-virus measures, many sites do not take advantage of them. If the users allow each other to access one another's directories, for example, the risk of infection is very high, and the rate of infection may be even higher compared to spread via floppy diskettes. Since many common viruses employ "ill-behaved" programming techniques, they cannot infect network file servers even when write/modify access is granted. This does not eliminate the risk by any means, but simply makes it less evident.

2. BBSes do not necessarily contain infected software.

There have been some extreme remarks about the dangers of downloading software from electronic bulletin boards (BBS). In actuality, the sysop (the person that maintains the BBS) has to take pains to ensure his board is free of malicious software to be able to keep a good reputation. On the other hand, there are supposedly some hacker BBSs that provide viruses, even in source code. Your chance of bumping into one of these is very little. Please do not be afraid to explore what the BBSs in your area have to offer. Many useful programs such as VDS are available for the cost of a local phone call. There is no need to be paranoid about the situation, just be aware of the possibilities. It is always a good idea to get software only from well-recognized bulletin boards such as the ones maintained by user groups. It is a good practice to search the programs you down-load for known viruses.

3. **Write-protected floppy diskettes cannot be infected by a virus as long as the floppy drive is working correctly.**

This is why you should always place a write-protect tab on all original diskettes if they are not already protected. The spread of viruses can be effectively slowed down by careful use of appropriate control mechanisms.

4. **A virus cannot infect your computer if you read your e-mail.**

For most cases, you will not activate a virus by reading your mail. However some e-mail programs try to load the application that is necessary to process a file attachment. In such cases, the program that needs to be loaded could interpret the contents of the attachment in such a way that viral instructions could be carried out.

How To Deal With Viruses

A. Recommended Guidelines

When dealing with viruses, there are a few rules to go by, all of which make good common sense. These rules are:

1. If there is a possibility that your hard drive is infected, do not use a floppy diskette on that computer unless it is write-protected.

Rationale:
If you did NOT cold-boot the computer from a clean floppy diskette, the virus may be active in memory and it can infect the floppy diskettes used in the drives. This is, after all, a common way for spreading infections among computers.

2. Do not boot a hard drive system from a floppy diskette unless you are positive that the floppy is virus-free.

Rationale:
This follows from Rule #1. The virus can infect the hard disk. The result is a hard disk that passes on the virus to other floppies. The floppy can carry a boot sector virus even if it was not formatted to be a system diskette, because all DOS diskettes have a boot sector.

3. If your PC is connected to a local area network, and you detect that your system may be infected by a virus, disconnect your PC from the network immediately.

Rationale:
The purpose is to isolate the infection in order to minimize the spread, and reduce the time required to clean the system. Make sure you know how to disconnect only your PC. Pulling out the wrong cable may bring down a whole subsection of the network.

4. If you receive new programs (especially games), test them on a machine that does not have valuable data before installing these these programs on other computers.

Rationale:
This precaution will help prevent the introduction of new viruses into the system. Even shrink-wrapped software may contain a virus. There have been some unfortunate incidents where major computer companies shipped infected diskettes to their customers by mistake.

5. If you do not feel technically competent to handle a virus attack, contact someone who can help.

Rationale:
Dealing with viruses can be a very tricky business. You cannot afford to leave a single infected file on your system. It takes only one infected program to continue the spread of the virus.

6. When you want to backup your hard disk, boot from a write-protected, clean floppy diskette. Preferably use file-by-file backup mode instead of image backup.

Rationale:
Some viruses remain active in memory and interfere with disk access. They are likely to corrupt the backup diskettes. File-by-file mode gives you a better chance to recover damaged backups.

7. Write protect all original diskettes as well as their backups before using them.

Rationale:
This would prevent infection of your program diskettes should they be used in an infected system. Besides, during recovery you can be assured that the originals are not corrupted.

8. Before using programs that came on floppy diskettes, search them for known viruses.

Rationale:
Many companies are just beginning to realize the threat the viruses pose. They may or may not have a virus-free program development environment. It is better not to take any chances and check the diskettes yourself. If you find a write-protected, original program diskette to be infected, first contact the company that sold you the disk and complain.

9. If your BIOS supports choosing a boot sequence, set it to C: and then A:.

Rationale:
This will eliminate the possibility of inadvertently booting from an infected floppy diskette left in drive A:. Some modern BIOSes offer a setup option that allows you to always boot from your hard disk, even if there is a floppy diskette in drive A:. Many common boot sector infectors like the Stoned virus can infect your hard disk only if you boot your computer from an infected floppy diskette.

How To Order VDS

This section provides contact information and order forms to register VDS.

Registration

Getting A Registered Copy of VDS

This copy of VDS you are evaluating expires after a few months as indicated by the expiration date on the program screen. It is also missing a few nice-to-have features that the registered copy has. The evaluation copy does find and remove viruses, but it is usually not as up-to-date as the registered copy.

You can order VDS by filling out the form in *ORDER.TXT* and sending it to an authorized VDS dealer. Site licenses are available. You can e-mail any technical questions to **tyetiser@prolog.net** or leave a message on our **VDS-BBS (717) 846-3873.**

By purchasing a copy of VDS, you will receive the latest and complete copy of the programs. VDSFSCAN and VITALFIX are not included in the unregistered shareware release. Your purchase will encourage us to support the product better. Please take a moment to register VDS today.

Order Form for U.S.A.

VDS Advanced Research Group
740 W Princess St, 2A
York, PA 17404, U.S.A.

BBS: (717) 846-3873
http://home.prolog.net/~tyetiser

VDS 3.1e Order Form

Date: ___/___/_____

Name:____

Address:____

________________**City**: ____________________ **State**: _____ **Zip**:_________

Phone: (   )   -   (   )   -

E-mail address: ____

Contact Person:____

License Type: ( ) Personal ( ) Academic ( ) Business

Number of Copies:______________

Total Amount: $37.00 **x** Number of Copies = ________ + $3 = _______
(shipping outside U.S.A.) + $15.00

Where did you get VDS? ____

Name one thing you like about it: ________________________________

* Fill in the blanks, include a money order (outside the U.S.) or check for
the total amount and mail it to our address at the top. Allow 2 weeks
for delivery.

==
===========

For us to serve you better, please answer the following questions

1. If any, which virus(es) infected your PCs so far? ________________________

2. Which antivirus software did you use to find/remove them? ______________

3. Do you use a disk compression program? ( ) No ( ) Yes
( ) DoubleSpace(tm) ( ) Stacker(tm) ( ) Other __________________________

4. Do you use 4DOS or NDOS instead of COMMAND.COM? ( ) No ( ) Yes

5. Do you use either QEMM or 386MAX memory managers? ( ) No ( ) Yes _______

6. What is the most common DOS version installed on your PCs? _______________

7. Do you have a local area network?   ( ) No   ( ) Yes
    ( ) Novell Netware(tm)   ( ) Banyan VINES(tm)   ( ) Other _______________

8. What is your Internet e-mail address (if you wish to be notified of
    new releases)?   e-mail: ___________________________

==

You can direct all questions/suggestions to   tyetiser@prolog.net

Order Form for Italy

=======================================
RISERVATO AGLI UTILIZZATORI ITALIANI
=======================================

Il distributore esclusivo per l' Italia di   VDS PRO e':

FINSON SRL
Via Montepulciano 15
20124 Milano (ITALY)

Tel. (02) 66.98.70.36 / Fax (02) 66.98.70.27

L' utilizzo e la distribuzione della versione shareware in Italia sono esplicitamente vietati; i trasgressori saranno perseguiti a norma di legge.
Il prezzo di vendita di VDS PRO in Italia e' di Lit. 99.000 Iva compresa, e comprende:

* manuale di 80 pagine in italiano
* software in italiano
* un aggiornamento gratuito
* la possibilita' di ricevere quattro aggiornamenti a sole L. 59.000 ivate
* servizio di assistenza telefonico gratuito

VDS PRO e' distribuito in oltre 2.200 punti vendita suddivisi tra computer shop, librerie, catene e grandi magazzini.

Per ordini diretti a mezzo telefono: (02) 66987036 (orario d' ufficio)
tramite fax: (02) 66987027