

Vx2000 Plus User Manual



USER MANUAL

Vx2000+ for WIN 95 / 98 & NT Workstations

The time to worry about viruses is before they worry you.

K7 Computing Private Limited
24 North Mada Street Srinagar Colony Saidapet
Chennai 600 015



(091) – 044 -- 235 3235

(091) – 044 – 235 0589

(091) – 044 – 235 4692

E-mail: Vx2000@md2.vsnl.net.in

Web: www.k7computing.com

K7 COMPUTING Pvt. Ltd.
SOFTWARE LICENCE AGREEMENT

This Software Is Licensed, Not Sold

This document is a legal agreement between you, the end user, & K7 Computing P.Ltd.

By using this software, you are agreeing to be bound by the terms of the agreement.

If you do not agree to the terms of the agreement, which include the software licence and limited warranty, promptly return the disks and all of the accompanying items (including documentation and packaging) to the place you obtained them for a full refund. The software contained in this package is subject to the following licence terms and conditions.

Grant of Licence - Permitted Uses

This is a single copy Software Licence granted by K7 Computing,Pvt. Ltd. licensed to you as the end user. It is not sold.

The software enclosed in this package is copyrighted material. Once you have paid the required single copy licence fee, you may use the software for the stipulated licence period, after which you are required to renew the licence. You may use the software on any computer for which it is designed so long as no more than one person uses it at any one time. If more than one person will be using it at the same time on one or more computers, you must **either** pay for additional copies of the software **or** obtain a **Site Licence** to cover the additional number of users/machines. You may not make any changes or modifications to the Licensed Software, and you may not decompile, disassemble, or otherwise reverse engineer the software. You may not rent or lease it to others.

Limited Warranty

What is covered by the Warranties K7 Computing Pvt. Ltd. warrants that the magnetic media which the software is recorded on and the documentation provided with it are free from defects in materials and workmanship under normal use.

K7 Computing Pvt. Ltd. warrants that the software itself will perform substantially in accordance with the specifications set forth in the documentation provided with it.

Duration of the Warranties The above express warranties are made for a period of sixty (60) days from the date the software is delivered to you as the first user.

Obligations of K7 Computing during the Warranty Period

Replacement K7 Computing will replace any magnetic media which proves defective in materials or workmanship, without additional charge, on an exchange basis.

In the case of an error in the documentation, K7 Computing will correct errors in the documentation without charge by providing addenda or substitute pages.

Correction of Software K7 Computing will either replace or repair without additional charge any software that does not perform in substantial accordance with the specifications of the documentation. This will be done by delivering to you a corrected copy of the software on an exchange basis.

Final Remedy If K7 Computing is unable to replace defective documentation or defective media or if K7 Computing is unable to provide a corrected of the software or corrected documentation within a reasonable time, K7 Computing will either replace the software with a functionally similar program or refund the licence fee paid for use of the software.

Exclusion of other Warranties

K7 Computing does not warrant that the functions contained in the software will meet your requirements or that the operation of the software will be uninterrupted or error free.

The warranty does not cover any media or documentation which has been subjected to damage or abuse or misapplication by you.

The software warranty does not cover any copy of the software which has been altered or changed in any way by you or others.

K7 Computing is not responsible for problems caused by changes in the operating characteristics of the computer hardware or operating system which are made after the delivery of the software.

Any implied warranties including any warranties of merchantability or fitness for a particular purpose are limited to the term of the express warranties.

K7 Computing shall not in any case be liable for special, incidental, consequential, indirect or other similar damages arising from any breach of these warranties even if K7 Computing or its agent has been advised of the possibility of such damages.

Your Obligations Under The Warranties

You must return the enclosed **Registration Card** to K7 Computing. Failure to do so may result in the inability of K7 COMPUTING to provide you with updates to the Software and you assume the entire risk of performance and result in such event.

You must call K7 Computing's customer support department for an authorisation to return any defective item to K7 Computing, during the warranty period.

If K7 Computing's customer service representative is unable to correct your problem by telephone, you will be provided with a return authorization number and an address for returning the defective item for warranty service or replacement.

You must insure any defective item being returned because K7 Computing does not assume the risk of loss or damage while in transit

Other Conditions

The warranties set forth above are in lieu of all other express and implied warranties, whether oral, written, or implied, and the remedies set forth above are your sole and exclusive remedies. Only an authorized representative of K7 Computing may make modifications to this warranty, or additional warranties binding on K7 Computing. Accordingly, additional statements such as advertising or presentations, whether, oral or written, do not constitute warranties by K7 Computing and should not be relied upon as such.

Limitation of Liability

In no case shall K7 Computing's liability exceed the licence fees paid for the right to use the licensed software.

This Licence constitutes the entire agreement and understanding between the parties and supersedes any prior agreement or understanding, whether oral or written, relating to the subject of this Licence. This agreement may only be modified by a written agreement signed by K7 Computing.

Copyright © K7 Computing 1999-2000.

Licensed material and program property of K7 Computing, 24 North Mada Street, Srinagar Colony, Saidapet, Chennai 600 015, India.

Unauthorised use, duplication, or distribution is strictly prohibited by law.

For further information:

Should you have any questions concerning this Agreement, or anything else, please contact any of the K7 Computing offices.

K7 Computing

24 North Mada Street, Srinagar Colony, Saidapet, Chennai 600 015

The Vx2000 name, the Vx2000 logo, and the K7 and K7 Computing names and logos are the trademarks of K7 Computing. All other brand and product names are trademarks or registered trademarks of their respective holders.

Contents

<u>Vx2000 Support services</u>	7
<u>Help! There's a virus in my PC</u>	8
<u>Installation</u>	
<u>Requirements for installing</u>	9
<u>Installing Vx2000Plus for Windows Platforms</u>	10
<u>Testing Vx2000 Rescue disk</u>	11
<u>Uninstalling Vx2000 Plus</u>	12
Chapter 1	
<u>About Vx2000 Plus</u>	
<u>About Vx2000</u>	13
<u>How Vx2000 Plus protects you</u>	14
<u>Offline scans</u>	14
<u>VxSentry System</u>	14
<u>Scheduled scans</u>	15
<u>Startup scans</u>	15
<u>Entrapment / MacSweep Tech</u>	15
<u>VxLive Update</u>	16
<u>Set Maximum protection</u>	16
Chapter 2	
<u>Using Vx2000 Plus</u>	
<u>Starting and Exiting Vx2000</u>	17
<u>Getting Help</u>	18
<u>Scanning for viruses</u>	19
<u>Enabling and Disabling VxSentry</u>	23
<u>Viewing Vx2000 Log</u>	24
<u>Scheduling virus scans</u>	25
Chapter 3	
<u>Removing viruses</u>	
<u>Removing viruses</u>	28
<u>Removing viruses from files</u>	29
<u>Removing viruses from Partition table</u>	30
<u>Unknown Viruses</u>	31
<u>Removing viruses through VxSentry</u>	34

If unable to clean a virus	38
Chapter 4	
Defense against newer viruses	
Automatic updates	40
Installing new update files	41
Chapter 5	
Change Vx2000 Plus settings	
Scanner settings	43
Log settings	47
VxSentry Settings	49
Exclude files from scanning	55
Internet Settings	56
Startup Scan settings	58
Right-click Scan settings	59
Setting password protection	60
Chapter 6	
Using Vx2000 Rescue Disk	
Removing viruses	62
Restoring your hard disk	63
Chapter 7	
Using Vx2000 DOS	
Starting / Exiting Vx2000 DOS	64
Removing a Virus	67
Creating Undo	70
Using Vx2000 from command line	73
Appendix A	
System Messages	
Messages and their meanings	75
Appendix B	
Trouble shooting	
Solution to common problems	80

Vx2000 Plus Service & Support

K7 computing is committed to excellent service. Our goal is to provide you with professional assistance in the use of our software and services.

Registering the Vx2000 Plus

To register the product, please complete the registration card included with your package. You can also register via our web site www.K7computing.Com.

If your address changes, you can post or fax your new address to the K7 computing office nearest to you, attention Vx2000 Registration.

Getting Technical Support

For Internet support

Connect to: <http://k7computing.com>

For Accessing Virus Lab

E-mail to: K7VL@K7computing.com

To consult Online Manuals

Download from
<http://K7computing.com/Techsupp/Manual.htm>

General E-mail:

E-mail to: Vx2000@vsnl.com

Our Contact Numbers:

Phone 91-44-235 3235 / 235 0589 / 235 4692.

Fax: 91-44-235 5921.

Help!

There's a virus in my PC.

You suspect a virus infection before the installation of Vx2000 Plus,

Or

The installation procedure has reported a virus in your computer.

What to do:

First, do not panic.

Then, take the following steps:

Boot the computer from drive A: using a clean write-protected bootable diskette.

Run Vx2000 DOS (Disk I) from drive A: by typing Vx2000.

If a virus is reported in memory again, it indicates that your bootable diskette is also infected with a virus.

Use a clean bootable disk and try again.

Scan all the hard disks and floppy diskettes.

If a virus is found, Vx2000 pops up either the **File Virus Found** or the **Boot virus found** screen.

Take appropriate action as explained in Chapter 7, Using Vx2000 DOS.

Installation

This chapter explains how Vx2000 Plus is installed in your system and how Rescue disk is created.

Installing Vx2000 Plus

When you install Vx2000 Plus exactly as directed by the on-screen messages, you will have complete virus protection as soon as you restart your system. This means:

- Vx2000 Plus Sentry loads automatically each time you start your computer.
- Rescue disk helps you in case you can't start your computer.
- An automatic scan of your disks once a week to ensure that they are virus-free.
- Protection when you copy files from other sources or download files from the Internet.
- Protection when you send and receive email.

By default the necessary files will be installed in \Program Files\K7 Computing\Vx2000Plus in drive C:.

Requirements for Installation

The minimum computer requirements are:

- 486 IBM or compatible PC with 8 MB of memory.
- Microsoft Windows 95
- 2 MB of free hard disk space to install Vx2000 Plus.

You must also have:

One 1.44 MB floppy disk and One Disk Label (for Rescue Disk)

The last step of installation asks you to create a Rescue disk. This Rescue disk is an important part of your virus protection. For example, it allows you to safely restart your computer if it is halted due to a virus in the memory. And it can be of great importance in restoring the functionality of your hard disk, in case of an emergency.

Installation

For complete protection, simply click 'Next' on all the setup panels to accept the preset option.

To start Installing:
Do one of the following

- For a CD-ROM, insert the CD into the CD-ROM Drive. Vx2000 Plus Anti-virus Setup Program starts automatically.
- For Floppy Disk, Insert Vx2000 Plus Anti-Virus Disk 1 in A: drive,
- Click start on the Windows taskbar, click Run, type A:\SETUP in the text box, then click OK.

Follow the on screen instructions.

If Vx2000 Plus cannot Install because it finds a virus, See "Removing Virus when you install " in this section.

Test your Vx2000 Plus Anti-Virus Rescue Disk. See "VX2000 Plus Rescue Disk."

Removing viruses when you install

When you install Vx2000 Plus, it scans for viruses. If it finds an active virus you will have to use Vx2000 DOS disk that comes along with the product to remove the virus before you can install Vx2000.

To Remove the Virus:

1. Shut Down your Computer.
2. Turn off your computer using the power switch.
3. Insert a clean write-protected bootable diskette in drive A:
4. Turn on your Computer.
5. When the A:\ prompt appears, insert the Vx2000 DOS disk that came along the Vx2000 Plus Anti-Virus in your A: drive.
6. Run Vx2000 DOS from drive A: by typing Vx2000. Choose the drive to scan and follow instructions on the screen to remove the virus.

Rescue Disk

On completion of installation, Vx2000 prompts you to create a Rescue Disk. Follow the instructions on the screen to create the disk. An up-to-date Rescue Disk is an important precaution against subsequent virus attacks – it can be of great importance in restoring the functionality of your hard disk in case of an emergency.

Why create a Rescue Disk?

If a virus damages the startup areas (Master Boot Record or Boot record) of your hard disk, you can use the Rescue Disk to restore this information and gain access to the system again.

If you do not have a Rescue Disk, you may be compelled to format your hard disk again to get your system working again, which means losing all the data on the hard disk.

Whenever a virus is found in memory, you can use your Rescue Disk to reboot your system. You can then run Vx2000 DOS to eliminate the virus.

If you have skipped this process during installation, see section on “To Create a Rescue Disk” later in this chapter.

Testing the created Rescue Disk

Vx2000 Plus cannot always create a Rescue disk for all hard disks. You should always test your Vx2000 Plus Rescue disk to make sure it works.

To test your Vx2000 Plus Rescue disk:

1. Either click restart when prompted in the rescue disk creation screens or Click Start on the Windows task bar, Click on Shutdown, select Shutdown your computer from the dialog prompted and click Ok.
2. Turn off the power.
3. Insert Vx2000 Plus Rescue disk in A: drive, and restart your computer.
4. Type C: and Press Enter to change over to your hard disk.
5. When DOS prompt appears on the screen (for example, C:\>), type DIR at the prompt and press Enter. If the prompt and directory listing appear properly it indicates that Vx2000 Plus

Chapter A: Installation

rescue disk works properly. If DOS prompt does not appear, then Vx2000 Plus rescue disk does not work properly.

6. Slide the open plastic tab on the back of the disk to write protect it. This prevents you from accidentally changing the data stored in the disk.

To create a Rescue Disk

If you did not create a Rescue disk during installation, create it now. You need one 1.44 MB floppy disk and one disk label.

To create a Rescue Disk:

1. On the windows taskbar, click Start, point to the Programs, point to the Vx2000 Plus Anti-virus group, then click Rescue disk, Or Choose the rescue disk icon from the Vx2000 Plus Main window.
2. Follow the on-screen instructions.
3. Test your Vx2000 Plus Anti-Virus Rescue disk. See “Testing the Vx2000 Plus Anti-virus Rescue Disk” in this chapter.

Uninstalling Vx2000 Plus Anti-Virus

To uninstall Vx2000 Plus Anti-Virus:

On the Windows taskbar,
Click Start, point to Programs, point to Vx2000 Plus Anti-Virus group, then click on Uninstall Vx2000 Plus Anti-Virus.

Or

Click Start, point to Settings, point to Control panel group.

Click Add/ Remove programs from the icons displayed.

Choose Vx2000 Plus from the list and then press Add/Remove button to uninstall.

About Vx2000 Plus

Vx2000 Plus is a complete and comprehensive anti-virus solution designed for Windows 95 & 98 and NT Workstations. Its virus detection, prevention and removal capabilities and its file integrity checking feature have been integrated into an effective and reliable solution designed to tackle both known and unknown (or new) viruses of all kinds, including stealth, polymorphic and macro viruses.

Vx2000 provides a thorough protection for local and network drives, CD-ROMs, floppies, boot sectors, partition table, folders and files.

When you accept Vx2000 preset options your computer is safe from viruses.

By default Vx2000 Plus will

- Check boot records for viruses during system start up.
- Check programs and documents for viruses at the time you use them.
- Scan all local hard drives at a scheduled time.
- Scans files that are downloaded via the Internet.
- Scans emails that are received.
- Checks floppies for boot viruses when you use them and during system shutdown.
- Invokes the right-click scan facility in the Windows Explorer to enable easy scanning.

What you can do using Vx2000 Plus

- Scan and remove viruses from specific files, folders, or entire drives.
- Schedule virus scans at predefined times.
Fix your floppy boot in case of corruption.
- Create a rescue disk that will aid during emergencies to restore the functionality of the hard disk.
- Initiate Live Update to obtain new virus definition files.

- Configure Vx2000 Plus to block unwanted sites from being visited.

How Vx2000 Plus Works

Computer viruses in general fall into two categories:

Known viruses: The term 'Known virus' is given to a virus that has been identified by the K7 Virus Lab - where the outbreak is analyzed and virus is studied in the lab. The signature or the identity of the virus is then extracted and added to the Vx2000 Plus virus definition files. When a Vx2000 scan starts either through schedule scan or demand scan, it does nothing but search for these signatures in the files / disks. If a file is found to be infected with any virus, Vx2000 would remove the virus alone from the file according to your configuration. Every time a new virus is identified the signature is added to the definition file and this new definition file needs to be added to the product to enable detection of new viruses.

Unknown viruses: An Unknown virus is one that does not yet have a virus definition. Vx2000 uses an advanced technology to detect these viruses. The **Macsweep technology** will detect Macro viruses in Word documents. For identifying file viruses Vx2000 uses the **Entrapment Technology** by which it can detect and clean new viruses.

Different ways of protection

Offline scan



Use "Scan for viruses" button in Vx2000 Plus main window to initiate offline scan. These scans detect known viruses in specific files, folders, or drives on your computer. For information on how to scan files, folders or drives see "Scanning for viruses".

VxSentry



The Real time protection system VxSentry works in the background to protect your system in several ways:

- Detecting viruses that may already exist and remove them, preventing them from spreading further.

Chapter 1: About Vx2000 plus

- Preventing viruses from infecting your system via network, floppies, CD-ROM, Internet, Email.
- Checking for unknown viruses.
- Checking for Generic Macro virus using MacSweep Technology.

Vx2000 Plus is preset to load this real time protection whenever you start your computer. In order to load it manually choose the VxSentry icon from the Vx2000 Main window. The VxSentry would load in the background and you will see the VxSentry icon in the lower right corner of the taskbar on your Windows desktop. Refer to section "Change Sentry Options" for details on to how to configure the VxSentry.

Schedule scan



A Schedule scan is an offline scan that runs automatically at predetermined times. These scans supplement other automatic protection features to ensure that your computer is virus-free. For more information refer Chapter 2 "Schedule scans".

Startup Scan



This is an automatic scan that scans your system every time it boots. This is your first line of defense against computer viruses. This makes sure that the critical directories and the partition / boot sector are virus-free each time you start using your computer. Refer section on "Start up scan" on Chapter 5.

Entrapment / MacSweep Technology



MacSweep Technology – This will detect any macros that are present in a document. This technology rules out the question of a new macro virus infecting your system. All the macros be it new or old will be detected by this method providing 100% solution to macro virus problems

Integrity is a mechanism, which is used to detect UNKNOWN viruses, or those viruses for which Vx2000 does not yet have a signature. When Vx2000 scans a file for the first time it records critical information about it similar to taking a fingerprint. During the next

Chapter 1: About Vx2000 plus

scan Vx2000 will check the file against this integrity information for any changes. It notifies you if there are any changes that could indicate the presence of an unknown virus.

VxLiveUpdate



Virus definition files contain information that Vx2000 Plus uses during scans to detect known viruses. Vx2000 Plus depends on this updated information. Each time a new virus is discovered, its virus signature must be added to a virus definition file. You should update your virus definition files regularly so that Vx2000 Plus has the information it needs to find all known viruses.

Click on the VxLive update icon on the Vx2000 Plus Main window for these files to be downloaded automatically and installed in your system. Refer to Chapter -4 for more details.

Set Maximum Protection

To set maximum protection:

When you install Vx2000 with the preset options, your computer is automatically protected against known and unknown viruses and alerts you whenever a virus is found. However, you can increase your protection by doing the following:

Customize Scanner settings for maximum protection.

Customize Sentry settings for maximum protection.

Schedule scans.

Set the Start Up scan to check important directories.

Using Vx2000 Plus Anti-Virus

This chapter explains how to use Vx2000 Plus to protect your system, to scan and notify the presence of viruses in your system.

Starting and Exiting Vx2000 Plus

Use Vx2000 Plus Anti-Virus main window to initiate scans for viruses, schedule scans that run automatically, view or change configuration options, or update virus definitions files. VxSentry is always running. See “Enabling and Disabling VxSentry.”

To Start Vx2000 Plus Anti-Virus:

Click Start on the Windows taskbar, choose Programs, choose Vx2000 Plus Anti-Virus group, and, finally, click Vx2000 Plus Scanner. The Vx2000 Plus Anti-Virus for Windows main window appears thus:

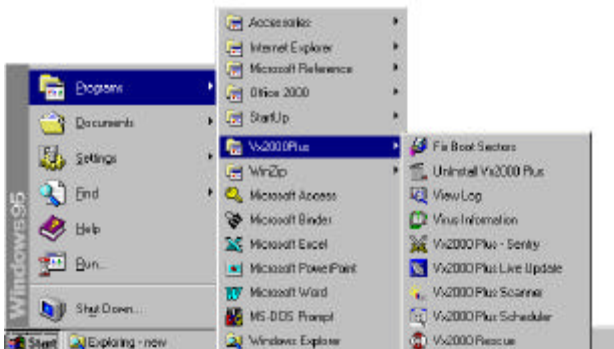


Fig 2-1: Click *Start* to
Choose Vx2000 Plus

To exit Vx2000 Plus Anti-Virus:

Choose the Scan option from the menu of Vx2000 Plus Anti-Virus main window, and select exit or use the default Window close icon.

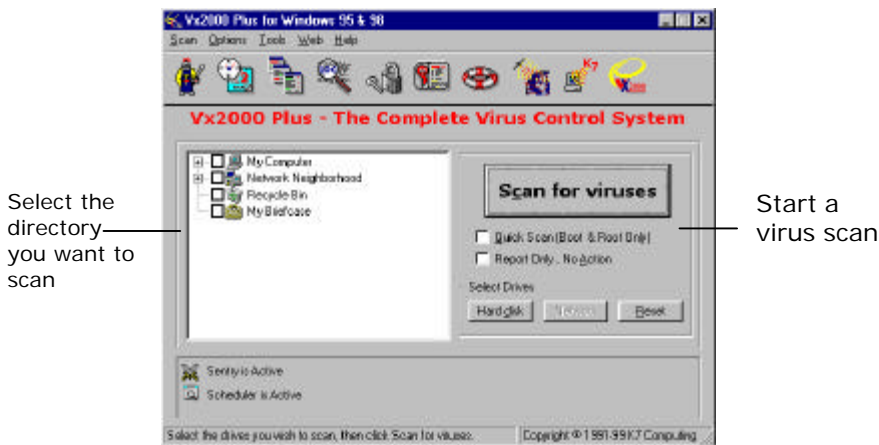


Fig 2-2:

Getting Help

Online help is provided for all capabilities of Vx2000 Plus Anti-Virus. You can get help on concepts, definitions, and procedures by:

- The Help option from the menu of Vx2000 Plus Anti-Virus main window.
- Clicking the Help button in a dialog box.

The help system includes a table of contents, and an extensive topics index. From the help window you can search for, and print, specific help topics. You can also access context – sensitive help for any option in Vx2000 Plus Anti-Virus.

Where viruses reside

A virus normally resides in a program file or the boot sector or in the partition table of your hard disk. However for the virus to spread to other locations the virus has to reside in your system memory. Vx2000 searches for the viruses in all these areas where it can reside.

Whenever you start Vx2000, by default it will automatically check the memory for viruses. If a virus is found in memory Vx2000 aborts the scanning and prompts you to boot through a Rescue disk or a clean bootable diskette then run Vx2000 DOS version to clean the virus. See Chapter 7 for more details.

Vx2000 also allows you to scan for viruses on Drive(s) or a particular folder(s) or a specific file(s).

Scanning for Viruses

You can initiate a virus scan at any time. As a general practice, scan your hard disks at least once a week or schedule a scan to occur automatically. Always scan floppy disks before you use them for the first time and always scan files downloaded from bulletin boards and other online services.

At the end of each scan, Vx2000 Plus Anti-Virus reports its results. If any problems are found, Vx2000 Plus prompts you to clean the virus (see "Removing viruses detected during scans"). After the problems are dealt with, as well as after a scan with no problems found, a detailed result of the scan is displayed.

Tip: Vx2000 Plus Anti-Virus preset options balance maximum protection with efficiency during scans. In most cases you do not need to change anything.

You can, however, customize what is scanned and what to do if a virus is found.

(see "Scanner settings" in Chapter-5)

To scan one or more drives:

Start Vx2000 Plus Anti-Virus.

In the Vx2000 Plus Anti-Virus main window:

Choose the drives or folders you want to scan in the directory tree of the Drives Selection Box in the Vx2000 Main Window.

Click on the + or – key to expand or collapse the folders. Selected Drive(s)/ Folder(s) will have a tick mark flashed in a box.

Chapter 2: Using Vx2000 Plus

To select all local hard disks click on Hard disks button on the right of the selection box.

To select all network drives click on Network button.

Note: The Network Drives option will be dimmed out if your system is not connected to a Network Server.

To reset the selected options click on the Reset button on the right of the selection box.

Click Scan for viruses button or Scan selected items from the Scan menu.

The scan dialog box reports the progress of the scan.

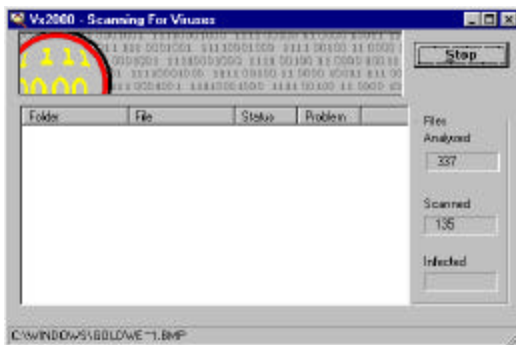


Fig 2-3:

To scan an individual file:

In the Vx2000 Plus Anti-Virus main window, choose scan files from the scan menu.

Select the folder/file you want to scan.

Click scan.

Vx2000 Plus Anti-Virus is preset to scan program files, documents, and document templates only during a scan, because these are the only types of files from which viruses spread. Occasionally, such as after a virus attack you may want to scan all files to make sure that a file that may not appear as a regular program file gets scanned as well.

To scan all files, regardless of the file type:

In the Vx2000 Plus Anti-Virus main window, choose Options.

Choose the scan settings.

Or

Choose the Options Icon from the main window.

Click the Scanner tab.

Select All files option.

Click OK to return to Vx2000 Plus Anti-Virus main window.

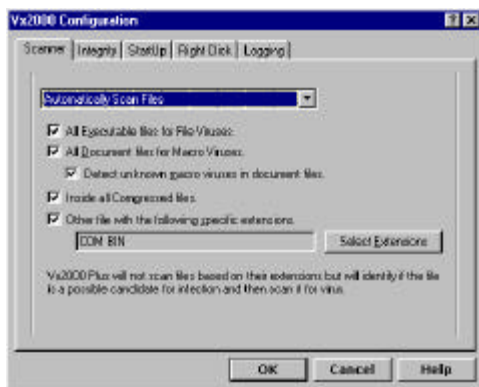


Fig 2-4:

Select the drives to scan and click Scan Now.

See "Selecting files to scan" in Chapter 5.

Quick Scan

If you wish to scan only the boot sector and the root directory of any particular drive check the Quick scan in the Main Window.

To report problems at the end of the scanning and not to prompt when problems are found check the report only in the Main Window.

Scanning results

Once the scanning starts, Vx2000 will report the status of the files being scanned.

Depending on how Vx2000 has been configured, Vx2000 will detect and take action for the following problems:

Known Virus on Partition or Boot sector

Known Virus on Files

New Strains of Viruses

File Integrity Changes

Refer Chapter 4, Removing Viruses, to take corrective measures.

Viewing Scan results

Once the scanning is completed you can browse through the report by using [Up arrow],[Down arrow],[PgUp] and [PgDn] Keys.

A detailed report of the scan is given and provides the following information:

- number of files present
- number of files scanned
- number of files infected
- number of files with missing integrity information
- files with integrity mismatches
- action taken by the user
- other relevant information.

Printing Scan results

You can take a hard copy of the scan results by choosing the "Print" button.

To take hard copy choose print to printer.

To spool the report to a text file choose print to file.

Press OK to proceed and close the dialog box.

Enabling and disabling Auto-Protect

Vx2000 Plus Anti-Virus is preset to load VxSentry– the Real time protection technology -whenever you start your computer. The VxSentry icon appears on the Windows taskbar. If the VxSentry icon does not appear on the Windows taskbar, either Auto-Protect is not loaded or Auto-Protect is configured not to display an icon on the taskbar.




Fig 2-5:

Generally, you should not disable VxSentry. It is your best protection against virus attack. There are only a few situations when you might want to disable VxSentry. For example, some times you are told to disable anti-virus protection before installing a new program.

To disable the real time protection temporarily:

1. Right click on the VxSentry Icon on the Windows taskbar.
2. Choose Disable Sentry.

The button changes to enable and the icon in the taskbar changes to 

To load Vx2000 Sentry every time you start your computer:

1. Start Vx2000 Plus Anti-Virus.

Chapter 2: Using Vx2000 Plus

2. Choose Sentry Icon in the Vx2000 Main window Or Choose Sentry Settings from the Options menu.



Fig 2-6

3. Select the General tab and check the Load VxSentry at Start Up and press OK.

Vx2000 Plus Anti-Virus would enable Real time protection every time your computer starts up thereafter.

Viewing Activity Log

The Activity Log file contains details of Vx2000 Plus Anti-Virus activities, such as when problems were found and how they are resolved. For information on specifying what is to be stored in the Activity Log, see "Customizing the Activity Log".

To view all entries in the Activity Log:

1. Choose Tools from the Vx2000 Plus Anti-Virus menu.
2. Select View Log Or Choose the View Log Icon from the Vx2000 Plus Main Window.
3. Click OK

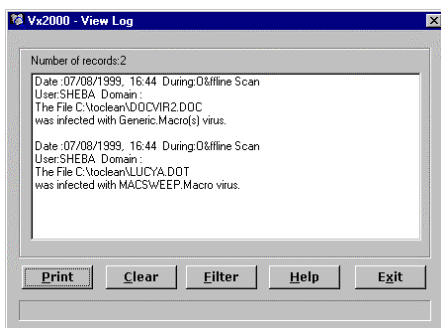


Fig 2-7:

From the Vx2000 Log dialog box you can also:

Click Print to print the activity log to a printer. Only the entries currently displayed in the list box are printed. If you filter the log, only the filtered entries are printed.

Click Filter to limit the display to specific types of events, such as all virus detections by VxSentry.

Click clear to delete all the entries in the log file.

To Filter the Activity Log entries:

1. Click Filter in the Vx2000 View Log dialog box.
2. Check the types of events you want listed. If no entries match your filter, a "No items to display" dialog box appears.

Events

- Known virus
- Integrity not found
- Integrity Mismatch

Modules

- Real time scan
- Offline scan
- Schedule scan
- Right click scan
- Start up scan

3. Click OK.

Scheduling Virus Scans

You can schedule the scanning operations, which in turn run unattended on either specific dates and times or at periodic intervals. You need not have to stop working at the time when a scheduled scan begins. You can just continue to do your work as the scanning take place in the background.

Chapter 2: Using Vx2000 Plus

To access the Scheduler, use one of the following methods:

Choose Scheduler Settings from the Options menu

Choose Vx2000 Plus Anti-Virus Scheduler Icon from the Vx2000 Main Window.

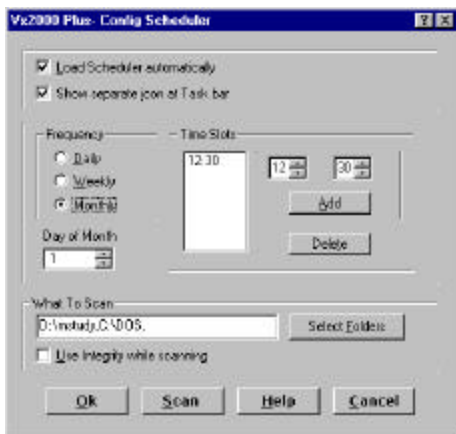


Fig 2-8:

When to Scan

In the Time Slots text boxes, enter the time or click the arrow buttons to select the time you want the scan to occur.

In the frequency group select how often you want the scan to occur: Daily, Weekly, or Once a Month.

To scan on a weekly basis, select which day of week you want the scan to occur in the Day of week selection box that would appear on selecting the "Weekly" option.

To scan on a monthly basis, in the Day of Month field enter or select which day of the month you want the scan to occur. This would appear on selecting the “Monthly” option.

What to Scan

To choose what is to be scanned, specify the path in the “What to Scan” text box separating each path with a comma or you may use the browse button to select folders.

If you would like to scan the specified path for unknown virus also, check the “Use Integrity for files”.

How to Modify/Delete a Schedule

Select the time slot you wish to delete and then choose the **{Delete}** button.

Immediate Scan– You may also invoke an immediate scan of the selected modules by choosing the **{Scan}** button.

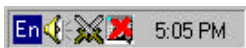
Loading and Unloading Scheduler

To load the scheduler every time you boot the system check the **[Load Scheduler at startup]**

To disable the Scheduler temporarily:

1. Right click on the Scheduler icon on the Windows taskbar.
2. Choose Disable Scheduler.

The button changes to enable and the icon in the taskbar changes to



From the same menu you can also invoke the configuration menu and also Unload the scheduler.

Removing viruses

This chapter explains how Vx2000 handles Known Viruses, Unknown Viruses and File Integrity problems.

Vx2000 Plus Anti-Virus warns you of possible virus infection in three different ways, depending upon how the virus was detected.

Virus detected during offline or on-demand scans: Vx2000 Plus Anti-Virus prompts you when a virus is found during the scan.

Virus detected by VxSentry: Vx2000 Sentry which is constantly monitoring your computer for virus displays a virus alert immediately on detection of an infected item.

Virus detected during start up or schedule scans or Right-click scans: Start up scan, which runs when you first start your computer, catch viruses that infect files and boot records which the computer itself uses for its own work. Whereas when schedule scans or Right-click scans are triggered, results are displayed at the end of the scan. You will need to use Vx2000 Plus offline scan to remove the viruses reported.

Go through this chapter to locate the relevant section title or picture that relates to the problem reported by Vx2000 Plus and follow the instructions. If the screen message is not found in this chapter please see Appendix I, System Messages.

Removing viruses from memory

If Vx2000 detects a virus in the system memory, it will pop up an alert box warning the user of the fact and also displays the name of the virus.

When a virus has been located in memory, it also means that the virus is active and may be spreading to other files or interfering with the normal operations of the system.

What is to be done:

- Switch off the system. This will remove the virus from the memory.

Chapter 3: Removing Viruses

- Boot the computer from drive A, using a clean, write-protected bootable diskette or Vx2000 Rescue Disk. After the system boots, the DOS prompt A:\ should appear on the screen.
- Run Vx2000 DOS (**Disk I**) from drive A: by typing Vx2000.
- If a virus is reported in memory again, it indicates that your bootable diskette is also infected with the virus. Use a clean bootable diskette and try again.
- Scan all the hard disks and floppy diskettes. If a virus is found, Vx2000 pops up either the **File Virus Found** or the **Boot Virus Found** screen. Take appropriate action. (Refer Chapter 7 for more details on using Vx2000 DOS).

Removing viruses from Files

When a virus has been detected the following dialog box appears.



Fig 3-1:

Below is a brief explanation of the actions associated with each button.

{Clean} – Cleans the virus from the file and continues with scanning.

{Skip} – Ignores the file and proceeds to next file. This operation will **not** remove the virus from the file.

Chapter 3: Removing Viruses

{Rename} – If the cleaning fails the file will be renamed with a .VIR extension. This prevents you from running the program accidentally and activating the virus.

{Delete} – You can eliminate the virus by deleting the file. After deletion, the file should be replaced only from your back up or from original disks.

{Apply selected action to all problems} – If this option is selected along with any of the options above, the action applies to all the following files with the same problem.

Removing Partition Table/Boot Sector Viruses

When a virus is detected in the partition table or Boot sector regions the following screen appears.

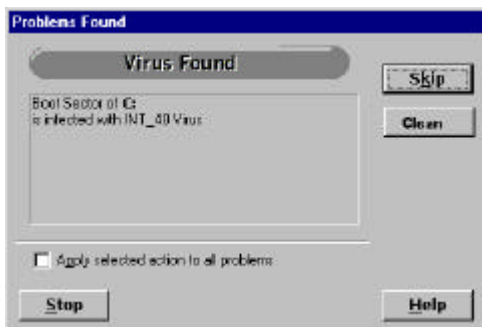


Fig 3-2:

Below is a brief explanation of the actions associated with each button:

{Clean} Cleans the virus from the Boot sector or partition table and continues scanning the drive.

{Skip} Does not clean the virus but continues scanning.

If the **{Clean}** button is dimmed, it could be due to the following reasons.

Chapter 3: Removing Viruses

- The virus cannot be removed. This may be due to corruption caused by the virus.
- Curing is not possible for this virus through Windows. In this case boot with the Vx2000 Rescue Disk and run Vx2000 DOS from Disk I and then clean the virus. (Refer the section below for more details).
- The curing routine is not available for this virus as of now. It may be a new virus or a rare strain of an existing virus. In this case contact us with sample files for assistance.

How to remove a Partition/Boot Sector Virus

Boot the machine through a clean DOS Bootable diskette or Vx2000 Rescue Disk from drive A:

Run Vx2000 DOS (**Disk I**) from the original diskette.

Select the Drive you want to remove the virus from.

Select the {Clean} button from the dialog box that appears.

For further clarification refer Chapter-7 Using Vx2000 DOS.

Unknown Viruses – How Vx2000 Plus detects them

Integrity is a mechanism, which is used to detect unknown viruses. Unknown viruses are those for which Vx2000 does not yet have a signature. When Vx2000 scans a file for the first time it records the critical information about it similar to taking a **fingerprint**. During the next scan Vx2000 will check the file against this Integrity information for any changes.

Creating Integrity Records

When Vx2000 does not find the Integrity Information for a file, the Dialog Box in Fig 3-3 appears. (This dialog box appears only if **Verify Integrity** and **Prompt for action** has been switched on in the Offline Scan settings)



Fig 3-3:

{Create} - Select this button to create Integrity Information for the file. This will help Vx2000 in detecting Unknown viruses affecting the file in future.

NOTE: Creation of an Integrity Record for a file is also referred to as **Inoculation**.

{Skip} - Select this button if you do not wish to create Integrity Information for the file.

{Apply selected action to all files} -If this option is selected along with any of the options above, the action applies to all the following files.

Integrity Mismatches

When Vx2000 finds that a file has changed from its previous state, the Dialog Box as shown in Fig 4.4 appears. Vx2000 will also report the number of bytes by which the file size has increased or decreased. Please read confirming the presence of a new virus at the end of this chapter.

{Update} - Select this option only if you have upgraded your program to the next version. For example you could have copied a new version of Microsoft Word (Winword.exe). Selecting this option will update the existing Vx2000 information with the new integrity information.



Fig 3-4:

{Clean} - Select this option to restore the file to the state before it was modified. However if the file is truncated or beyond rectification Vx2000 will accordingly report and it is best to restore the file from the original copy.

{Skip} - Select this option to ignore the file and proceed.

{Apply selected action to All Files} - If this option is selected along with any of the options above the action applies to all the following files.

Suspecting a New virus

When Vx2000 reports that a file has changed and shows an increase in file size, this could mean the presence of a new virus, unless you have copied a new version of the file.

Confirming the presence of a new virus

To confirm please adopt the following procedure:

Select **{Apply selected action to All Files}** button from Fig 3.4 along with **{Skip}**. This combination makes Vx2000 proceed with the scanning without prompting for such changes. When scanning is complete, and if a new virus has actually been present, changes in

Chapter 3: Removing Viruses

several files would be reported. The report will look similar to that shown below:

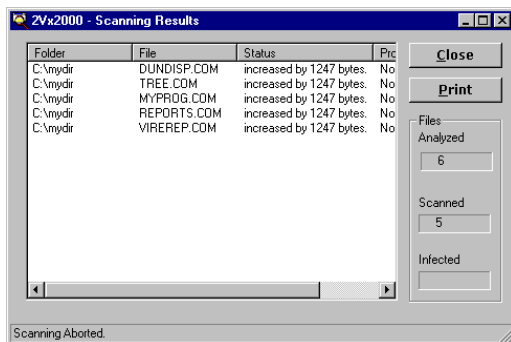


Fig 3.5:

In the above report it is clear that all files have increased in size by 1247 to 2016 bytes. This is a confirmation of the presence of a new virus.

What to do with a new virus

Please Exit Vx2000 Plus now and copy a few of these files to a clean floppy diskette.

Send this diskette to K7 Computing Pvt. Ltd. It will help us to provide you with a proper cure for the virus.

Now load Vx2000 Plus again and scan the files.

Clean the virus using the Integrity Information in a couple of files.

Exit Vx2000 Plus and check if the cured files are running normally.

If they do so proceed with cleaning for the rest of the files.

Removing Viruses detected by VxSentry

VxSentry constantly monitors for viruses, and immediately displays an alert dialog box whenever an event concerning a virus occurs. These alerts are displayed in character-based modes because all processing, including display processing, comes to a halt until the problem is resolved.

You are warned when:

- A virus is found in a program you are trying to run or a program file you are trying to copy.
- A virus is found in the memory.
- An inoculation issue is detected (either a file has not been inoculated or a file has changed since it was inoculated).
- Boot virus detected in floppy when you try to access it.

When VxSentry alert appears on your screen:

1. Read the message in the alert box to understand the type of problem that was found.
2. Refer to the appropriate section for instructions on how to proceed:
 - "Responding to VxSentry virus found alerts".
 - "Responding to VxSentry integrity alerts".
3. If you see a different message that you do not understand, see "Appendix-A" - "System messages".

Responding to VxSentry virus found alerts

There are two ways to remove a virus from your computer:

1. Clean the infected file, boot record, or master boot record.
2. Delete the infected file from the disk.

Note: Files once deleted by Vx2000 cannot be recovered even with special file recovery utilities.

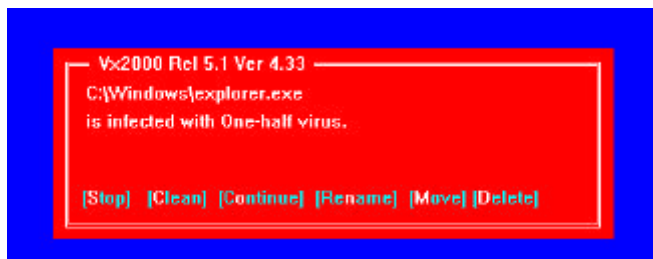


Fig 3-6:

To repair an infected file or boot record:

{Clean} Press C for Clean in the alert box.

If the Clean button is not displayed, either VxSentry is configured not to enable it or the item cannot be cleaned.

After cleaning infected files or boot records, scan your drives and floppy disk with Vx2000 Offline Scanner to verify that there are no other files or boot records which may contain viruses.

To delete the infected file:

{Delete} Press D for Delete in the alert box.

If the Delete button is not displayed, either VxSentry is configured not to enable it or the item cannot be deleted.

After deleting the infected files or boot records, scan your drives and floppy disk with Vx2000 Plus to verify that there aren't any other files or boot records that contain viruses.

Once you are certain that your system is virus-free, replace the files you deleted with uninfected copies. Make sure you scan the replacement files before copying them to your hard disk.

TIP: If your forgot which file needs replacing, look at the Vx2000 Log for the name of the file.

{Rename} or {Move}

You may also choose N to Rename the file or M to Move it to another directory. This will avoid executing the file again accidentally and spreading the virus.

Responding to VxSentry integrity alerts

When Integrity Not Found

You can configure VxSentry in the Integrity options to automatically inoculate files when it encounters un-inoculated files.

By default VxSentry prompts you when an un-inoculated file is encountered. You have the following options to resolve the integrity not found alert.

{Stop} – Press S to halt the current operation. For example, if you are trying to open the file through Ms-Word, access is denied.

{Continue} – If you want to continue without taking any action, Press O for Continue. This response does not prevent Vx2000 Plus Anti-Virus from notifying you about this file again in the future.

{Create} – Press C to create the integrity information for the file. If you inoculate a file, Vx2000 Plus Anti-Virus will notify you whenever there is a change in the file. Changes in a file can sometimes indicate the presence of an unknown virus. Inoculation does not make any changes to the file itself, but integrity data file of Vx2000 gets updated.

{Inoculate All} – To create the integrity information of all the files that are accessed subsequently, choose A. Hence forth VxSentry will not prompt you for creating integrity but will automatically create it, until the next reboot.

When Integrity Changes

Integrity changes in a file occur for the following reasons:

The file has changed for legitimate reasons since the last time you inoculated it. For example, you may have installed a new version of the software and not yet inoculated the program file.

The file contains a virus that is not in the Vx2000 definition file (perhaps because you don't have the most recent virus definitions or because it is a new virus for which Vx2000 Plus Anti-Virus does not yet have a definition).

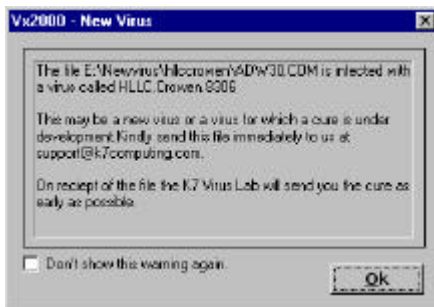


Fig 3-7:

To respond to the changes:

{Update} - If you are certain the file has changed for legitimate reasons, press U for a new Integrity information to be generated.

{Clean} – If you suspect a virus, Press C for Clean to return the file to the way it was when you last inoculated it.

{Delete} - If you suspect a virus in a program file and have an uninfected backup copy of the file, Press D for delete; then replace it with the uninfected copy. Files deleted by Vx2000 Plus Anti-Virus cannot be recovered.

When is a cure not possible

Disk is write protected

In order to remove a virus, the disk should not be write-protected. Hence before cleaning a floppy disk make sure the write-protect tab is removed. If you are cleaning files on a network drive make sure that you have write permission for the directory or drive.

File Corruption

In some cases of virus infection Vx2000 Plus Anti-Virus will report **File Corrupted**. This means that the virus has corrupted the file and the file cannot be restored to its original state. The only way to restore such files is to copy the files from the original diskette or backup.

Cure Not Available

If Vx2000 detects a virus and reports "Vx2000 cannot clean this virus" it indicates a new strain of the virus. As this virus has not surfaced before, a cure has not been provided. Please send samples of the infected files to K7 Computing Pvt. Ltd. to enable us to provide a solution.

Unable to clean floppy boot

If Vx2000 was unable to clean a boot record of a floppy disk, you can still copy important data from the floppy disk to another disk. But make sure you scan all the files as the source is infected. Use the Boot fix tool to fix the boot sector.

Choose the Fix Boot sectors from the Tools menu of the Vx2000.

Follow instructions prompted to fix the boot sector.

Defense against the newer viruses

Vx2000 Plus uses information in its virus definition files to detect viruses during scans. As new viruses are discovered, their virus definitions are added to the virus definition files. To prevent newly discovered viruses from invading your computer, you should update your virus definition files regularly. Updated virus definition files are available every month.

Automatically updating virus definitions

To ensure that you have current virus protection always, Vx2000 Plus can update the virus definition files on your computer automatically. All that is required on your part is one of the following:

- An Internet connection
- A properly connected modem

Make it a practice to update your virus definitions once every month.



Fig 4-1:

To update virus definitions automatically:
Make sure that you are connected to the Internet.

Chapter 4: Defense against newer viruses

In the Vx2000 Plus Main Window, Click the VxLive Update icon.

Choose the method of updating.

Press OK to start the update process.

Appropriate files get downloaded and installed on your computer. When the update is complete, a summary with the information of the latest enhancement is displayed.

Manually updating virus definitions

You can also manually download virus definition files provided by K7 computing Pvt. Ltd.

To download updates manually:

Access www.K7computing.com

Click on Updates

Follow instructions on the screen to download the file.

Installing new virus definition files

Use the new files you downloaded to update the product installed in your computer.

To install the new virus definitions:

In the Vx2000 Plus Main Window, Click the VxLive Update icon.

Choose the method of updating as Local Path.

Click on Settings.

Click on the Local Path tab to bring it to the front.



Fig 4-2:

Specify the path where you have saved the downloaded update files.

Press OK to start the update process.

Follow the prompts displayed by the update program.

The update program will install the new virus definition files in its proper folder automatically.

Unload and reload the VxSentry so that it begins using the new virus definition files.

If prompted to reboot, restart the computer for the new files to take effect.

Read the new text documents, if available, for more information on the latest additions to the product.

Note: In case, you are in a network and saved the files in the network then choose the network in the updating method and specify the path in the space provided in the Network tab settings.

Change the Vx2000 Plus settings

This chapter explains how to customize Vx2000 Plus Anti-Virus to meet your needs.

Vx2000 Plus Anti-virus is a powerful tool in the fight against computer viruses. The preset options of VX2000 Plus installation are designed to provide excellent protection for all computing environments. Unless you are a computer professional with special implementation requirements, most likely that you would not need to modify your Vx2000 Plus Anti-virus configuration.

Configure Scanner Settings

The manual scan options affect scans you initiate when you click the Scan for viruses button in the Vx2000 Plus Anti-Virus main window or when scheduled scans occur.

To customize what to scan:

Choose Options in Vx2000 Plus Anti-Virus main window

Choose the scan setting

OR

Choose the Options Icon in the Vx2000 Main Window and click the Scanner tab to bring it to front.

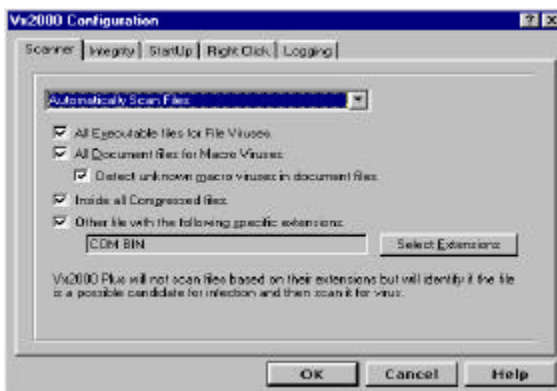


Fig 5-1:

Chapter 5: Change the Vx2000 Plus settings

From this window you can configure the types of files to scan:

Press the drop down list to choose the options.

Automatically Scan Files - When this option is chosen Vx2000 Plus will not scan files based on their extensions but will identify if the file is a possible candidate for virus infection and would scan the file. You may specify what type of candidate is to be checked – Files that are susceptible to file virus infection or Macro infection. You may configure this by choosing the following settings:

All Executable files – Vx2000 Plus looks for viruses in all the executable files. Vx2000 Plus does not go by the specified extension but scans file by their type. Thus you can be sure that all executable files that are susceptible to file virus infection is scanned for viruses.

All Document files - Vx2000 Plus looks for viruses in all the Microsoft Office Document files irrespective of their extensions. All files that are susceptible to macro virus infection is scanned for viruses.

Inside all Compressed files – Vx2000 Plus checks within compressed files for viruses.

Other files with Extension - You may specify here files that cannot be identified as executable but are possible candidates for infection. By default the COM and BIN files fall in this category. All other executables like EXE, SYS, DLL are covered in the Executable files set.

Scan All files - Choose this if you want Vx2000 Plus to scan all the files irrespective of their extensions. If you want the document files to be checked for Unknown or new macros viruses then check the “Detect any macros in Documents”.

User defined file Set - By default, this option is switched ON. Choose this if you want Vx2000 Plus to scan files with the specified extensions only. The files are identified with a set of extensions, which you can configure. Press on the Select extensions button to configure this list. If you want the document files to be checked for unknown or new macro viruses then check the “Detect any macros in Documents”.

Chapter 5: Change the Vx2000 Plus settings

Even after scanning and cleaning all the program files, if the symptom of the virus presence still persists, then it is advisable to scan for [All files]. Once virus presence has been ruled out, it would be proper to consider other aspects, like hardware malfunctions, etc.

Detect any macros in Documents

Macro viruses are the most widely spreading viruses as of date. New viruses are being created almost every day. You need to protect your system from both known and unknown macro viruses. This feature of the product will help you detect any macros that are present in the document. This may or may not be a virus macro. As there can be genuine macros that you have created to make your work easier, it is left for you to decide the authenticity of the macro before using the file. Certain Microsoft's default templates do contain macros. In such cases you could ignore this message and proceed.

Choose this option when you want Vx2000 Plus to check for any macros in documents.

Verify Integrity

Choosing this option will help you detect unknown viruses in your system.

When Vx2000 scans a file for the first time it records the critical information about it, called as Checksum, similar to taking a fingerprint.

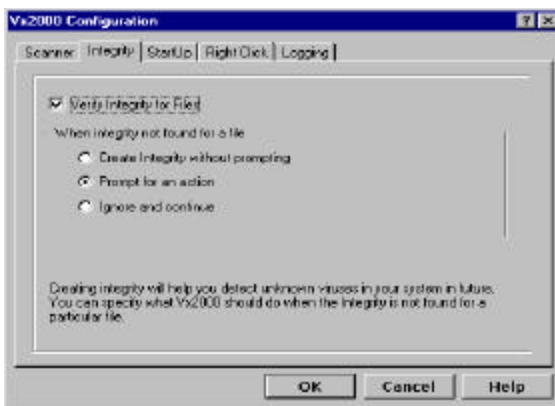


Fig 5-2:

Chapter 5: Change the Vx2000 Plus settings

Choose the Integrity tab in the Scanning Option properties to bring it to front.

Check the verify Integrity for files on for Vx2000 Plus to check for You can specify what Vx2000 should do when the Integrity/Checksum is not found for a particular file.

Add Automatically - Without user intervention Vx2000 Plus will create the necessary information for any file while scanning.

Prompt for action - Will prompt for confirmation when an integrity information is not found for any particular file. You may choose to create the integrity when prompted.

Ignore and continue - Ignores the problem and proceeds with scanning without creating the integrity information.

Please note that by creating this Integrity information Vx2000 Plus does not tamper or write to the original file. The information is collected and written into Vx2000 Plus Integrity file "VxChksum.Vx2".

Specifying File Extensions

Vx2000 Plus uses a set of extensions while scanning for viruses. You can modify this list by choosing the Extension button in the respective options in the scan settings tab.(fig 5-1)

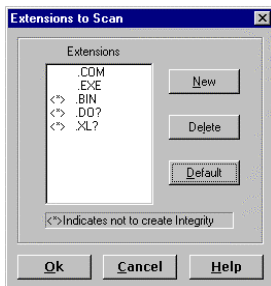


Fig 5-3:

Use the file extension dialog box to add new extensions, delete extensions, and reset the extensions to the original list installed with Vx2000 Plus.

Chapter 5: Change the Vx2000 Plus settings

The default file extension list contains the majority of extensions used for program files. Included is the document file extension that is to be scanned for macro viruses.

Add Extension:

In order to scan for applications with a unique file extension, Click **New** to display a dialog box where you can add them to the list. Once added to the list Vx2000 Plus will scan the files with that extension for viruses. In case you do not want to include that particular extension for checking of unknown viruses you need to choose the "Do not create integrity".

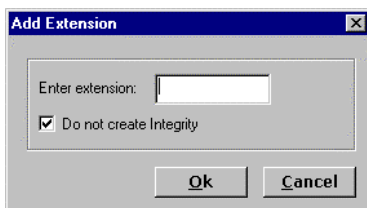


Fig 5-4:

Delete an Extension:

Click **Delete** to remove a highlighted file extension. Removing extensions from the list reduces the protection against viruses.

Reset the default Extension list:

Click **Default** to return the file extension list to the preset options.

Configure Log settings

The Vx2000 Plus log file contains details of the Vx2000 Plus activities, such as when problems were found and how they were resolved. The preset options instruct Vx2000 Plus to log detection of known viruses and Integrity Mismatch and what action was taken on these infected files. You can customize the Vx2000 Plus log to record the details of what is to be logged.

Chapter 5: Change the Vx2000 Plus settings

Click on the Options in the Menu.
Choose the Log Setting item.
Or

Choose the Options Icon in the Vx2000 Plus Main Window and click the Logging tab to bring it to front.

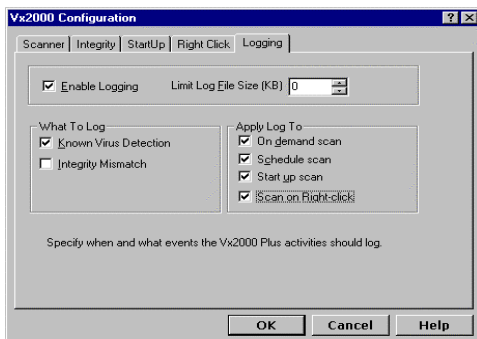


Fig: 5-5:

Check the Enable logging to start logging the activities.
In the "What to Log" group box, check the event you want Vx2000 to record.

Known virus detection: Records the detections of known viruses.
Integrity Mismatch: Records the detections of unknown viruses using Integrity.

In the "Apply to" group box, check the scan during which you want Vx2000 to record the said events.

You can also limit or increase the size of the Vx2000 Log file. When the log reaches the maximum size, it begins to overwrite the earliest entries.

Click OK to save changes and close the dialog box.

Configure VxSentry Settings

To configure the VxSentry or the Vx2000 Real Time Scanning module

Choose the VxSentry Icon from the Vx2000 Main Window.
.OR.

Click on the Options in the Menu.
Choose the Sentry Setting item.



Fig 5-7:

Detection

When to perform a scan

This allows you the flexibility to decide when and how the Real Time Scanner should function.

On Files

The Scan Files group allows you to specify when VxSentry should scan files.

[On Access] Scans a program file each time it is accessed

Chapter 5: Change the Vx2000 Plus settings

[On Creation] Scans files when they are created on your drive by an installation program, Uncompressing files, downloading via the Net or by any other means.

[On Renaming] Scans a file when it is being renamed or overwritten.

On Disks

The Scan Disks group allows you to specify when VxSentry should scan floppies.

[On Access] Scans floppy disks each time it is accessed

[On Shutdown] Scans the floppy disk in A: drive for virus before the system shuts down. This will prevent the virus entry during the subsequent boot.

Types of files to scan

Under the group "What to scan" you can specify what files VxSentry should scan.

All files - Choose this if you want VxSentry to scan all the files irrespective of their extensions.

Selective Files - By default, this option is switched ON. Choose this if you want VxSentry to scan for files with the specified extensions only. Viruses normally infect executable files and Document files only. These are identified with a set of extensions, which you can configure. Press on the Extensions button to configure this list. (Refer section on Specifying File Extensions for more details).

Detect any macros in Documents

This feature of the product will help you detect any macros that are present in the document. This may or may not be a virus macro. Choose this option when you want Vx2000 Plus to check for any macros in documents.

Action to be taken on detecting a known Virus

Select the "Actions" tab from fig 5.6 to specify how VxSentry should respond to virus detection.

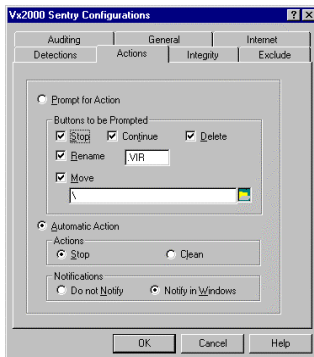


Fig 5.8:

Prompt for Action

Whenever Vx2000 detects a virus it can either prompt you for an action or you may configure it to automatically take action.

[Prompt for Action] If this option is switched on, every time VxSentry detects a Virus it will present you with a Virus Alert dialog box. It will allow you to choose how to respond. This provides more control over what happens to an infected file. You can specify what are the buttons that have to be prompted.

[Stop] - Will stop the file from being accessed

[Continue] - Allows you to continue accessing the file. If you select the continue button you may activate the virus.

[Clean] - Allows you to clean the file or boot record

[Delete] - Allows you to delete the file.

[Rename to] - Files that can not be cleaned can be renamed to the extension specified in the text box provided. Renaming the file prevents you from running the program accidentally and activating the virus.

[Move To] - Infected files can be moved to a separate directory. You may specify the directory you would like the files to be moved into for isolating the files.

Automatic Action

If you have decided on what action to take on the infected files, then you can opt for one of these actions on all the infected files accessed.

[Stop] - Will deny access to any infected file

[Clean] - Will automatically clean any infected file that is accessed as and when it is being used.

Notification Option

The prompting of the problems found messages could be configured.

[Do not notify] - When you have chosen to take automatic actions the problems found will not be prompted to you. The action will be taken silently.

[Notify In Windows] - All the messages from the VxSentry will be prompted to you through the Windows GUI. This will ease your working process.

Configuring Vx2000 to detect Unknown Viruses

Select the Integrity tab, see Fig 5.6, to specify how Vx2000 should respond to unknown viruses.

Verifying Integrity Records

When you scan a file for the first time Vx2000 Plus creates an Integrity Record for the file. This is used for detection of new or unknown viruses during the subsequent scans.

Chapter 5: Change the Vx2000 Plus settings

Any kind of modification done to the file can be detected using the information in the Integrity Record. Thus any modification done to the file by the new virus can also be spotted. The Integrity record is created for every file for which the extension is specified in the File Extensions set.

Integrity records are stored in a file named "VXCHKSUM.VX2" which is created for every directory. You can scan your hard disk using the Vx2000 Plus offline scanner and create integrity records initially.

For VxSentry to monitor for unknown viruses using the Integrity method, select the Integrity tab.

[Verify Integrity] - Set this option On to enable Vx2000 to check for unknown viruses on your system.

After choosing to Verify Integrity records on the hard disk, you will have to decide what VxSentry should do, whether the relevant integrity records are missing or have been changed.

When Integrity not found

There are three choices in this box. Only one type of action can be selected.

[Add Automatically] - Selecting this particular action cause VxSentry to create an integrity record for the file without notification.

[Continue] - Does not create the integrity record for the files and continues scanning, ignoring the problem.

[Prompt For Action] - When a file without an integrity record is found, Vx2000 will pop up a Integrity Not Found window allowing you to choose how to respond.

It is advisable to select the [Add Automatically] option.

When Integrity Mismatch

There are two choices in this box. Only one can be selected.

[Continue] - Vx2000 will ignore the problem and will continue monitoring files.

Chapter 5: Change the Vx2000 Plus settings

[Prompt For Action] - When a file with an integrity mismatch is found, Vx2000 Plus will pop up Integrity Mismatch window and allows you to choose the action to be taken.

Auditing Vx2000 Scanning activities

Select the "Audit" tab in fig 5.6 to configure what Vx2000 is to record.

The following screen will appear

Select the "Enable Logging" option to activate Logging.

What events to Log

In the "What to Log" group box, check each type of event you want Vx2000 to record.

[Virus Found] records the detection of a known virus found and the action taken

[When Integrity Not found] records the detection of a file when integrity not found

[When Integrity Mismatch] records the detection of a file when there is an integrity mismatch.

General Real Time Scan Settings

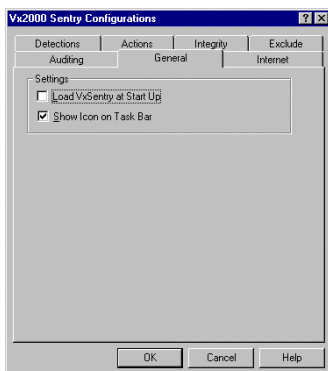


Fig 5.11:

Startup option

[Load Vx2000 at startup] – The VxSentry will get loaded into memory every time you boot the system.

Taskbar option

[Show Icon on Task Bar] – The Real Time Scanner Icon will be displayed on the task bar. Through the Icon you can invoke the Configuration menu.

By clicking the right mouse button on this Icon you will get a menu. From this menu you can **[Disable]** the Real Time Scanner temporarily by selecting the disable option.

Unloading the Real Time Scan

The **[Unload]** option can be used to remove the Real Time Scanner from memory.

Exclude files from scanning

To exclude files from being checked for known or unknown viruses:

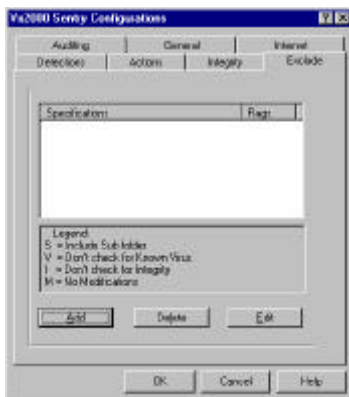


Fig 5.12:

Click the Exclude tab to bring it to the front.
Click Add.

Chapter 5: Change the Vx2000 Plus settings

Do one of the following

Use the browse button to display a folder selection dialog box from which you can choose a folder that will be displayed in the Entry to exclude text box.

.Or.

Enter a folder in the item text box. You should check Include Subfolders if you want to ensure that all files within that folder are excluded.

Check "Don't check for Integrity" if you do not want the folder to be scanned for the detection of unknown viruses.

Check "Don't check for known virus" if you do not want to scan the folder for known virus.

Be careful! Excluding files reduces your level of protection.

Check "No modifications" if you do not want the file to be tampered with either by a virus or any other source.

You could use this option to protect certain important files from tampering.

Internet Settings

Select the Internet tab in Fig 5:6, to specify the Internet security protection of Vx2000.

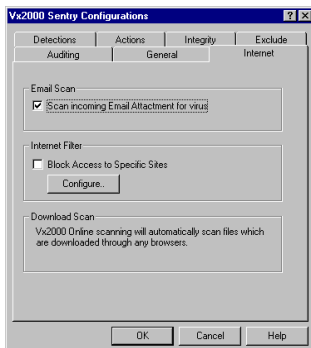


Fig 5.13:

Scan Email for viruses

To scan the emails as and when they land in your mail box check the "Scan Incoming Email attachment for viruses."

The attachments will be scanned for viruses and will be prompted to you immediately.

Block IP Addresses

In order to block access to specific sites check the Block Access to Specific Sites option.

Click on the Configure button to specify the Addresses to be blocked.

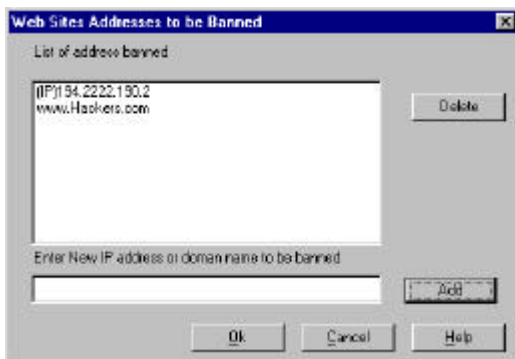


Fig 5.14:

To Add an address

Enter the IP Address in full or the domain name in the text space provided under the heading "Enter New IP address or domain name to be banned".

Click on Add button next to it to add the address to the list. Vx2000 will not allow access to the specified sites.

To Delete an address

Choose the address to be deleted from the displayed list and click on Delete.

Startup Scan settings

Checking for viruses during system startup is an important step in preventing virus from activating or spreading. If a system file is infected, the virus will activate when you start up your computer and may infect other programs you run during the day.

To configure the startup scan:

Click on the Scanning Options Icon from the Vx2000 Main window.

Click on the start up scan tab to bring it in front.

. Or.

You may choose the Start up Settings item from the Options menu.

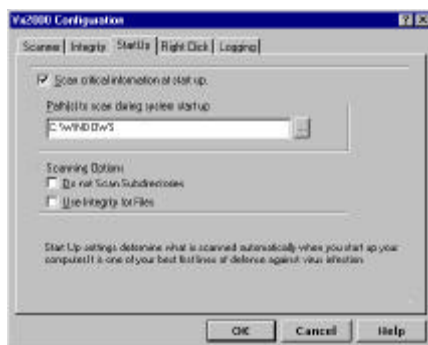


Fig 5.15:

Check the Scan critical information at start up to enable the start up scan option.

Enter the drive letter or pathname for the drive, folder, or file you want scanned during system startup in the Path to scan text box. To scan more than one item, use a comma between them. For example:

C:\windows,D:\Myporgs

Chapter 5: Change the Vx2000 Plus settings

You can also use the browse folder next to the text to add to the list.

Check the 'Do not scan sub directories' if you want only the root directory of the specified path to be scanned.

Check the 'Use integrity for files' if you want the files to be checked for Integrity during startup.

We recommend that you perform a start up scan for critical directories. It is one of your best first lines of defense against virus infection.

Configure Right-click Scan settings

To set the right-click scan facility in the explorer interface:

Click on the Scanning Options Icon from the Vx2000 Plus Main window.

Click on the Right-click Scan tab sheet to bring it in front.

. Or.

You may choose the Right-click Settings item from the Options menu.

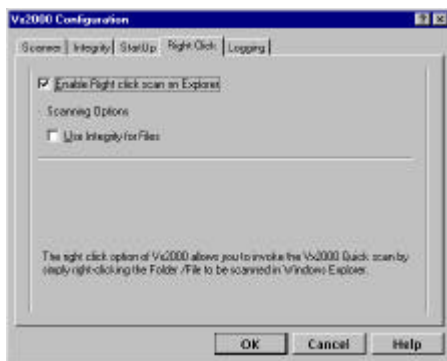


Fig 5.16:

Check the Enable Right click scan on Explorer to start this option. When enabled, this option Vx2000 allows you to invoke the Vx2000 Plus Scan by simply right-clicking the Folder / Files to be scanned

Chapter 5: Change the Vx2000 Plus settings

and choosing the Vx2000 scan on the menu displayed in Windows Explorer.

Setting password protection

Password protection guarantees that your Vx2000 Plus configuration will not be modified. You can protect selected features or all configurable options.

To password-protect features:

Click on the Password Icon in the Vx2000 Main Window.

Check the Enable Password to turn on the password protection feature.

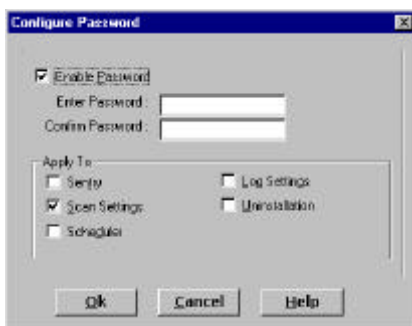


Fig 5.17:

Check the features you would like to protect with the password in the 'Apply to' group box.

Enter the password you want to use in the 'Enter Password' text box. The same password applies to all the selected features. You will have to retype the same password correctly in the Confirm Password text box.

Passwords can be from 1 to 16 characters in length and are case-sensitive. As you type, Vx2000 Plus replaces the characters on the screen with asterisks (*) for security.

Chapter 5: Change the Vx2000 Plus settings

Vx2000 also asks for the password before allowing changes to the password protection options.

To change your password:

Click on the Password Icon ON the Vx2000 Plus Main Window.

Enter the existing password in the 'Confirm Password' box.

Click OK.

Enter the new password in the Enter Password text box, then type it again in the Confirm password text box.

Click OK.

To remove password protection:

Click on the Password Icon on the Vx2000 Plus Main Window.

Enter the existing password in the 'Confirm Password' box.

Click OK.

Do one of the following:

To remove password protection completely, uncheck 'Enable Password'.

To remove password protection for some of the protected features, remove the check for the features from the 'Apply to' group.

Click OK.

Using Vx2000 Rescue Disk

A Vx2000 Plus Rescue disk simplifies certain operations during virus emergencies.

If you have not yet created a Vx2000 Plus Rescue disk, do it now. See "Creating Rescue disk" in Chapter-A.

Removing viruses from a shutdown computer

How to remove viruses using Vx2000 Plus Rescue disk:

If your computer is running, choose Shutdown from the Start menu on the Windows taskbar to shut down the computer.

Switch off your computer using the power switch. Turning off the power removes any viruses that might be present in memory.

You MUST switch off the power. Selecting Restart or pressing Ctrl+Alt+Del is not sufficient to remove certain viruses from memory.

Place the disk labeled as Vx2000 Plus Rescue disk in drive A: , then switch on the computer. Your computer will start from the Rescue disk.

When A: prompt appears insert Vx2000 DOS disk I in drive A: and type Vx2000.

Vx2000 scans the partition table and boot sector of the hard drive and informs you when a virus is found. Press C for Clean to eliminate the virus.

Choose all drives in the hard disk from the select drives options shown in screen and press scan so that Vx2000 will scan your entire disk. If any virus is prompted Press C to clean it.

Once all viruses have been eliminated, remove any floppy disk left in the drive and reboot your computer by switching the power switch OFF and then ON to return to Windows.

Try to find the source of the virus. Use Vx2000 Plus and scan all hard drives again. Scan floppies as well.

Restoring your hard disk

If a virus has damaged the startup areas of your hard disk, you can use the Rescue disk to restore this information and gain access to the system again.

- Insert the Rescue disk of your system in Drive A:. Make sure that the disk belongs to the **specific system** for you will cause damage if you use the rescue disk prepared in any other system.
- Type VxRescue at the prompt.
- Follow instructions on the screen.
- Reboot the system when prompted.

If the system does boot again contact your Hardware maintenance engineers as there could be some other problem.

Using Vx2000 DOS

This chapter helps you to use Vx2000 DOS to check for viruses and remove them when found in your system.

Starting & Exiting Vx2000 DOS

To Start Vx2000

Insert the original Vx2000 Plus diskette in drive A: or B: and type Vx2000.

Insert Disk II when prompted.

Vx2000 main window appears as shown below:



Fig 7-1:

On how to Scan Drives refer to Chapter 2 Scanning For Viruses.

To Exit Vx2000

To Exit Vx2000 and return to DOS prompt select the Exit option from scan menu or press [ESC].

Where to Scan

A virus can normally reside in a program file or the boot sector or in the partition table of your hard disk. However for a virus to spread to other locations the virus has to reside in your computer memory.

Chapter 7: Using DOS

Vx2000 searches for the viruses in all the areas where they can reside.

By default whenever you start Vx2000, it will automatically check the memory for viruses. If a virus is found in memory Vx2000 aborts the scanning and returns to the DOS prompt.

Vx2000 allows you to search for viruses on Drive(s) or on a particular subdirectory or a specified file.



Fig. 7-2:

Scanning Drives

To scan one or more drives choose the Select Drives option from the Scan Menu ([Alt D]). This is also the default screen of Vx2000.

To scan a drive move the highlight bar to the drive to be scanned and press [Spacebar] to select or un-select.

To scan all Floppy drives press [Alt D], all Hard Disks press [Alt F], all Network Volumes [Alt N].

When the selections are complete, press the [Enter] key to start scanning of the selected drives.

Scanning Directories/File(s)To scan either a Directory or File(s) choose the Scan Directory option from the scan menu ([Alt F]).



Fig 7.3:

Enter the full path of the directory or file name, which is to be scanned. You can also include wild cards in the input. Typing C:\Accounts\bin will result in Vx2000 scanning all program files in the subdirectory Bin and also the subdirectories in it.

Typing C:\Accounts\Bin\MyProg.Exe will make Vx2000 Plus to scan the specified file Myprog.Exe only. A group of files can also be specified by using the DOS wildcards (* and ?).

Once the path to the files to be scanned is specified, press [Enter] key to start scanning.

Scanning Results

When scanning starts Vx2000 will report the status of the files being scanned.

Depending on how Vx2000 has been configured, Vx2000 will detect and take actions for the following problems

- Known Virus on Partition or Boot sector
- Known Virus on Files
- New Strains
- File Integrity changes

Viewing Scan Results

Once the scanning is complete you can browse through the report by using up, down, [PgUp], [PgDn] Keys.



Fig 7.4:

A Detailed report of the scan is given. The report summarizes:

- Number of files present
- Number of files scanned
- Number of files infected
- Number of files with missing integrity records
- Files with integrity matches
- Action taken by the user
- And other relevant information.

Removing a virus

How do you proceed?

Go through this chapter to locate the relevant section title or picture that relates to the problem reported by Vx2000 and follow the instructions. If the screen message is not found in this chapter please see Appendix I **System Messages**.

Removing viruses found in memory

If Vx2000 detects a virus in system memory; it will pop up an alert box warning the user of the fact and also the name of the virus.

Chapter 7: Using DOS

When a virus has been located in memory, it means that the virus is active and may be spreading to other files or interfering with the normal operations of the system.

What is to be done?

Switch off the system.

This will remove the virus from memory.

Boot the computer from drive A, using Vx2000 Rescue disk or a clean, write-protected bootable diskette. When the system boots at the DOS prompt, A:\ should appear on the screen.

Run Vx2000 from drive A, using the original write-protected Vx2000 diskette.

If virus is reported in memory again, it indicates that your bootable diskette is also infected with the virus. Use a clean bootable diskette and try again.

Scan all the hard disks and floppy diskettes. If a virus is found, Vx2000 pops up either the File Virus Found screen or the Boot Virus Found screen. Take appropriate action as explained below:

Removing Virus from Files

When a virus is found in a File the following dialog box appears. This dialog box appears only if Prompt for action has been switched On in the **Scanning options**.

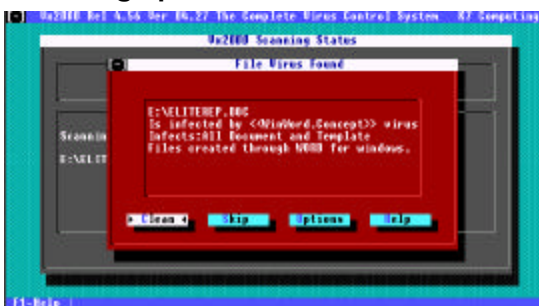


Fig 7.5:

Below is a brief explanation of the actions associated with each button.

{Clean} Cleans the virus from the file and proceeds with scanning

Chapter 7: Using DOS

{Skip} Ignores the file and proceeds to the next file. This operation will not remove the virus from the file.

{Options} This Button will provide you with more options as shown in

Fig 7.5. The Buttons themselves are self explanatory in their actions.

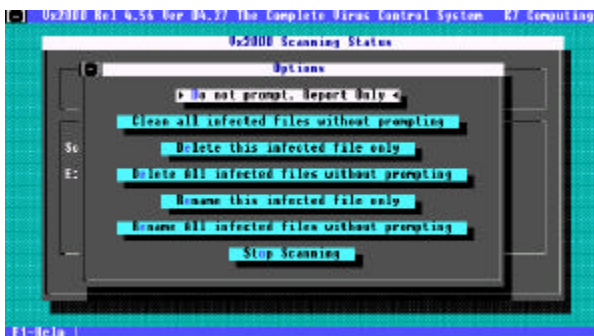


Fig 7.6:

Cleaning the file will remove the virus and restore the file to the state prior to infection.

In most of the cases of virus infection, there could be a 100% restoration to its original state. However in some cases after the file has been cured, there could be a difference in size of +16 to -16 bytes. If such files do not execute normally after curing, you have to copy the original files from the diskette.

If the **clean** button is dimmed, it could be due to the following reasons:

- The file cannot be cured. This could be due to corruption of the file by the virus.
- The curing routine is not available for this virus. In this case however Vx2000 would have already given the appropriate message.
- Vx2000 has not been loaded from the Original diskette.

Removing Viruses from the Partition or Boot Sector

When a virus is detected the following screen appears. This dialog box appears only if Prompt for action has been switched On in the Scanning Options.

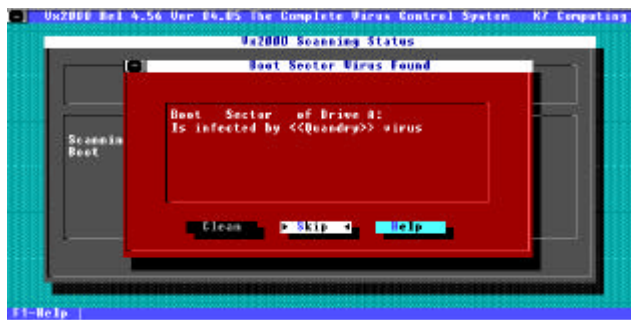


Fig 7.7:

Below is a brief explanation of the actions associated with each button:

{Clean} Cleans the virus from the Boot sector or partition table and proceeds with scanning the drive

{Skip} Does not clean the virus and proceeds with scanning.

If the clean button is dimmed, it can be due to the following reasons:

- The virus cannot be removed. This can be due to the corruption made by the virus.
- The curing routine is not available for this virus. In this case however Vx2000 would have already given the appropriate message.
- Vx2000 has not been loaded from the original diskette.

Creating Undo

The Partition Table and the Boot sector of the hard disk is very vital for any system to boot normally. Accidental corruption or damage to these areas may render the system unusable.

Hence whenever Vx2000 attempts to write in these areas to remove the virus, Vx2000 provides you with the Backup option called Undo.

Chapter 7: Using DOS

Using this option if you find that your system does not behave normally or does not boot, you can undo the change made by Vx2000 and gain access to your system again.

However it is important to note that the system is still infected with the virus.

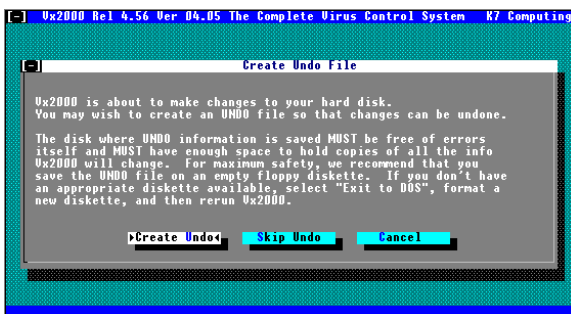


Fig 7.8:

It is always better to create the "Undo Disk" when you are attempting to clean a particular virus for the first time.

Procedure to remove the Partition or Boot sector virus:

Boot the machine through a clean DOS Bootable diskette from the drive A;

Run Vx2000 from the original diskette;

Select the Drive you want to remove the virus from;

When the virus is found. The Dialog Box as shown in Fig 7.9 appears;

Select the Clean button. The Dialog Box as shown in Fig 7.9 appears;

Select the Create Undo button. The Dialog Box as shown in Fig 7.9 appears;

Remove Vx2000 diskette from Drive A and insert a blank formatted diskette;

Press [Enter] to start cleaning;

Chapter 7: Using DOS

Once the cleaning is over, remove the diskette and preserve it carefully since the Undo information is stored here.

Once when the entire scanning and cleaning is completed Boot your system through Drive C. If you are unable to boot, it indicates that some corruption had taken place and Vx2000 was unable to fix it. It is now best to Undo the changes made and take backup of the data of your hard disk and format it.

Please refer to Appendix-2 **Trouble Shooting** to find out how to remove viruses by Formatting.

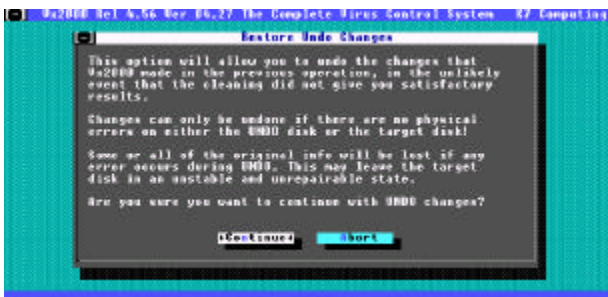


Fig 7.9:

To restore the changes made by Vx2000 do the following:

Run Vx2000

Select the **Undo Changes** from the **Utilities** option. The Dialog Box as shown in Fig 7.9 appears.

Press [Enter] or [Alt C]. The Dialog Box as shown in Fig 7.10 appears.

Insert the disk where the Undo information was saved.

After moving the Highlighted bar to the appropriate drive press the [Enter] key or [Alt O].

Vx2000 will now restore the system to its previous state.

Using Vx2000 DOS from command line

This Section explains how to use Vx2000 without invoking the user interface.

Experienced users may find this mode of operation more comfortable.

Vx2000 DOS allows you to use switches or abbreviated commands when running it from the DOS prompt.

You can thereby run Vx2000 and scan drives, directories or files according to desired and varied options, all at one go.

Some of the switches are used as it is, while others are followed with a parameter.

More than one switch and more than one parameter can be used in a command line.

When a combination of command switches are used, a space is used to separate them.

Wildcards are allowed when pathnames are specified for a group of files.

Certain switches are used alone. Others are followed by a parameter.

More than one switch and more than one parameter can be used in a command line.

DOS Command Line Switches

<Pathname >Any drive, directory, file or combination of these can be specified. Use space to separate the parameters.

(e.g. Vx2000 C: D:\GAMES E:\ACCOUNTS\MYACC.EXE)

/?	Displays the usage along with all the command line switches available.
/BOOT	Scans the boot sector and partition table only.
/CLEAN	Cleans viruses when found without prompting
/DEL	Delete the infected files if unable to clean
/NOMEM	Do not scan for viruses.

Chapter 7: Using DOS

/MONO	Force Monochrome screen.
/ALL	Checks all files.
/EXT	Check extensions (e.g. Vx2000 C: /EXT DLL 386 BIN)
/REPORT FileName	Spool report to file <FileName>
/APPEND	Append report used in conjunction with /REPORT
/NOBEEP	Do not Beep when infection is found.
/NOSUB	Do not scan sub-directories.
/NOEXPIRE	Do not warn if version is outdated.
/RENAME	Rename infected files to *.VIR if unable to clean
/MULT	Scan multiple floppy disks.
/VI	Verify & Clean using integrity information.
/AI	Add integrity information if not found without prompting.
/UI	Update integrity information without prompting
/RI	Rebuild Integrity Files.
/QUIT	Quit Vx2000 if no virus is found while scanning.
/DOS	Run Vx2000 in DOS Mode
/S FileName	Takes in all command line arguments from the FileName specified. Ignores the current configuration information. For Example if MYFILE.DAT contains the following lines. C:\ C:\DOS /NOSUB

Invoking Vx2000 /S MYFILE.DAT will scan all the files in the C: root directory and all files c:\dos directory only.

System Messages

This section contains a list of messages that you will come across while using Vx2000 Plus.

Note that the entries below use items such as **<FileName>**, **<Drive>**, etc. The actual messages you will see on the screen will have the specific filename or the drive letter or the appropriate text in them.

<FileName> has increased/decreased by n bytes

The specified File has changed since the integrity information was created. This may or may not be a virus.

In order to confirm this and to take necessary action, refer Chapter 3, *Removing Viruses*, under the Section *Confirming its presence*.

Drive not Ready - <Drive>

The specified drive could not be accessed by Vx2000 since the drive door is open or there is a problem in the drive.

Boot Sector of Drive <drive> is infected by <Virus Name>

The boot sector of the specified drive is infected with the virus. It is best to select Clean and remove the virus.

Refer to Chapter 3, *Removing Viruses*, Section on *Removing viruses from Partition Table/Boot Sector*,

<Virus Name> found in Memory

The virus specified is now active in memory. Vx2000 would not continue to scan your specified drive further. To remove the virus from memory refer to the Section on *Removing Viruses found in Memory*, in Chapter 3, *Removing Viruses*.

<File Name> Infected by <Virus Name>

The specified file is infected by the virus. To remove the virus from memory refer to the Section on *Removing Viruses from Files* in Chapter 3, *Removing Viruses*.

<File Name> No Integrity Information

The Integrity Information has not yet been created for this file. Creating this will help in detecting unknown viruses in future. Refer to Chapter 3, *Removing Viruses*, Section on *Creating Integrity Records*.

Appendix-A : System Messages

<File Name> has changed.

The file has changed since the integrity information was created but there will not be any change in file size. This may or may not be a virus. Refer to Chapter 3, *Removing Viruses*, Section on *Confirming its presence*.

Scanning Aborted by User

If, during the scanning operation, the user cancels the operation either by pressing [ESC] key or selecting the [Abort] button, Vx2000 would quit the operation and return to the Vx2000 Scanning Results.

<File Name > Unable To Access

This message will appear when Vx2000 attempts to scan a specified file that is already open. The file may have been opened by Windows, if present, or by some other TSR program. The file may be locked in a network drive also.

<File Name > Infected by <virus name> - Not able to clean
Vx2000 is not able to remove the virus from the specified file. You may delete the file and reinstall it from the original diskette. For further information on this refer to Chapter 3, *Removing Viruses*, Section on *When is a cure not possible*.

<File Name > Infected by <virus name> - No write- permission

The file that Vx2000 is trying to delete/rename is on a media which is write-protected.

Unable to write Integrity record. The disk may be full or write-protected. Check and retry.

The Integrity Information cannot be created for the specified directory because this directory or the media is write-protected or there may not be enough space.

The printer is either not switched on or it is not online

This message appears when the scan report is spooled to a printer. The printer may not be connected or it may not be ready.

<File Name> is infected by <Virus Name>

File access not allowed. Use Vx2000 to scan the disk.

This message appears when the file in use is identified to have a known virus by the Vx2000 Real Time Scanning module.

Appendix-A : System Messages

<File Name> The file has changed since it was scanned last. It may be infected with a new virus

This message appears when the sentry detects a change in the integrity information. This probably means the presence of new virus. Refer to Chapter 3, *Removing Viruses*, Section on *Integrity Mismatches*.

<File Name> Integrity Information for this file has not been created. Creating it will help detect New viruses at a latter stage.

This message is displayed by Vx2000 Real Time Scanning module indicating that the Integrity Information has not been created for the file. This will help in checking for Unknown viruses in future. Refer to Chapter 3, *Removing Viruses*, Section on *Creating Integrity Records*.

**<Drive> The disk is infected with a Boot virus
Use Vx2000 to clean it**

This message is displayed by Vx2000 Real Time Scanning module indicating the presence of a Boot virus in the disk that you are currently accessing. Use Vx2000 to clean the virus. Refer to Chapter 3, *Removing Viruses*, Section on *Removing viruses from Partition Table/Boot Sector*.

Unable to create Report

The report file was not created as the disk is full or does allow write access.

Error in Critical File or File Not found.

Please reinstall Vx2000

Additional driver file Not Found. Vx2000 Additional file corrupted or error

These messages will appear when any one of the Vx2000 files is corrupted or does not exist. The only way to rectify this will be to reinstall the product.

Cannot Load Vx2000. Not enough memory.

This message would appear when there is not enough memory to load Vx2000.

Vx2000 could not load some of the critical files needed to clean.

Cleaning of files for virus will not be possible.

This message appears under two circumstances: the Vx2000 additional files are corrupted or they are not found.

Appendix-A : System Messages

Load Vx2000 from the original disk.

Unable to locate Help Info

Vx2000.msg file does not exist. Reinstall Vx2000.

Unable to get virus details. Sorry! No information is available on this virus

In addition to the indication of the presence of the virus, you will also get a brief description of the virus. This message will appear when there is no such information available.

Invalid Drive specified

The specified drive does not exist in your system.

Virus signature database - Outdated

The virus signature file has expired. It is time to get an update of the file.

Partition Table of Drive :<drive> - Read error

Boot sector of Drive :<drive> - Read error

Vx2000 was unable to read the Boot sector / Partition Table of the specified drive.

Following are the messages that you will receive in the Vx2000 Scanning Results Report.

<File Name> <Problem> - <Result>

For example ,

C:SUBST.EXE - infected with Eddie - Cleaned

The list of possible <Results> are given below

Ignored - The problem in the file has been skipped. It should be noted that the problem still exists.

Cleaned - The virus in the file has been removed.

Renamed - The specified file has been renamed with .VIR extension.

Deleted - The file has been deleted.

No Write Permission - Vx2000 does not have write access for the file to perform the cleaning operation.

Not able to clean - The virus could not be cleaned. Refer to Chapter 4 "Removing Viruses" for reasons.

False Alarm - The file is not actually infected with the virus. It is a false alarm. Hence do not panic.

Integrity Added - The Integrity Information has been created for the file.

Appendix-A : System Messages

Integrity Updated - The Integrity Information has been updated with the new data.

File Corrupted - The specified file has been damaged due to the virus. You have to restore the file from the original diskette.

No Cure - The cure has not yet been provided for this virus. Refer to Chapter 4, *Removing Viruses*, Section on *When is a cure not possible*.

Trouble Shooting

This section explains how to resolve some common problems that may arise while you are using Vx2000 Plus. Follow the procedures provided here to try to solve these problems before calling Vx2000 technical support.

Solutions to common problems

- **My Vx2000 Plus Rescue disk doesn't work**

Due to the number of product specific technologies used by manufactures to configure and initialize hard disks, Vx2000 Plus cannot always create a bootable Rescue disk automatically. If the rescue disk does not work properly, do one of the following:

If you have a special boot disk for your computer, add it to your Vx2000 Plus rescue disk set. In a virus emergency, boot from that disk (first slide open the plastic tab on the back of the disk to make sure it is write-protected). Remove the disk and insert the Vx2000 DOS disk I and type A:\Vx2000 from the DOS prompt and press Enter, then follow instructions on the screen.

Use the Disk manager program or similarly named program that came with your computer to make a bootable disk. Be sure to test that bootable disk with Vx2000 Plus.

Sometimes, the Vx2000 Plus rescue disk does not work properly because you have more than one operating system installed, such as Windows NT and Windows 95.

Startup from your hard disk, insert the Vx2000 Rescue disk in the A: drive, and, from the DOS prompt, type SYS A: and press Enter. This transfers the operating system to the rescue disk. Be sure to retest your Vx2000 Plus rescue disk.

- **I've scanned and removed a virus, but it keeps infecting my files.**

Cause: The source of infection is a floppy disk or ZIP files.

Appendix-B : Trouble Shooting

Solution: Scan all floppy disks and Zipped files. See “Scanning for viruses” in Chapter 2.

Cause: The virus may be contained in an executable file with a non-standard file extension.

Solution: Modify the scanner options to scan All files instead of Program Files. Scan all disks that you use and repair all the infected files including Zipped files. Add any infected files’ extension to the program file extensions list.

See “Change Scanner Settings” in Chapter 5 for information on how to change the selection of files for scanning.

- **The sentry does not load when I boot the system every time.**

There may be more than one reason for this. The command to load the sentry every time the system is booted may not have been chosen. Or you may have bypassed this while booting your system.

If the command is not included then click on Sentry icon from the main window.

Choose the Sentry Options.

Select the General Tab.

Check “Load VxSentry at Start up.”

Boot the system without bypassing the batch file.

- **Integrity not found errors are appearing in files for which the integrity has already been created.**

The Integrity information for every file in a directory is stored in “Vxchksum.Vx2” file. One such file is created for each directory. If the media is write protected or if there is not enough disk space while writing this file Integrity Information will not be created. Hence make sure there is enough space in the disk and that you have the write access to it.

Refer the section on “Integrity Alerts” in Chapter 3.

- **Program hangs after curing the virus.**

The virus would have damaged the file beyond rectification. Or the virus itself would have been corrupted.

Appendix-B : Trouble Shooting

You have to restore the files from the original disks only.

- **Integrity mismatches are reported in files since I have installed a new version.**

When you install a new version of a product it means that you have copied some of the modified files. Hence the integrity information will not match.

Refer to section on "When Integrity Changes" in Chapter 3 to recreate the integrity records.

To remove viruses by formatting

Follow the steps below in order to remove the virus from the partition table of the hard disk. But note all the data will be lost.

1. Boot your system with a clean bootable disk
2. From the disk execute the command
A: \ format c:

This will result in the entire C drive being reformatted. All the data here will be lost.

3. This does not mean that the partition virus was removed. In order to get rid of it completely issue the following command.
A:\fdisk / mbr

To prepare a sample disk

When your system is infected with a new virus please send us a sample of the virus in order to provide you with a cure. To take a sample do the following :

1. Insert a fresh disk in the appropriate drive.
2. Format it and transfer the system files by issuing the following command from the DOS prompt
C:\dos\format a:/s
3. Copy a few commonly used EXE and COM files into it.

Appendix-B : Trouble Shooting

Now you have a sample of the virus transferred to the disk. Send this to the following address for a remedy.

K7 Virus Lab
K7 Computing Pvt. Ltd.
9, North Mada Street
Sri Nagar Colony
Saidapet
Chennai – 600 015.

Vx2000 reports a virus in memory but none of the files or the partition table is infected

This may be a False alarm. To ensure this, do the following:

1. Boot your system with a clean bootable floppy disk.
2. Run Vx2000 from the original disk.
If Vx2000 reports a virus in memory it indicates that your bootable disk is also infected with a virus.
3. Reboot the system with a clean bootable disk and then Run Vx2000 from the original disk.
4. Now scan your C drive for virus.
5. If Vx2000 does not report a virus, boot the system through the hard disk and run Vx2000.
6. If a virus is reported in memory it indicates a False Alarm and not an actual virus presence.
Simply ignore the problem and proceed.

Network options are dimmed

When you are not attached to the server the network options will not be available to you.

When I login to my network and then scan Virus is reported. But there is no virus in my local hard disk.

When you login there may be certain files executed through your login script. Your LOGIN.EXE itself may be infected with a virus.

Proceed according to the steps given below to get rid of the virus.

1. Boot the system with a clean bootable disk
2. Run Vx2000 from the original disk
3. Scan all drives and remove virus if present
4. Boot the system through the hard disk

Appendix-B : Trouble Shooting

5. Execute the clean lan driver files individually
Do not use any batch file to get connected to your network
6. When you are connected to the network copy the LOGIN.EXE to a floppy or the C drive
7. Run Vx2000 from the original disk and clean it
8. Login with the clean LOGIN.EXE
9. Edit the login script and REM all the statements present
Scan the network with Vx2000 and clean any virus that may be present

If you still get the virus in memory it indicates that it is a false alarm. Make sure you have done the above steps properly before you come to a conclusion.

I have an infected floppy to be cleaned

To clean the virus you have to run Vx2000 from the original disk only. To clean a virus from a floppy

1. Insert Vx2000 disk in the appropriate drive
2. Run Vx2000 by typing
A:\vx2000 (Substitute a: with the appropriate drive)
3. Once Vx2000 has scanned the memory and the "Select Drives" screen appears the Vx2000 disk can be removed from the disk drive.
4. Now insert the infected floppy in the drive, scan and clean it.

Vx2000 has reported a Generic boot virus found

While checking the boot sector Vx2000 will look for certain instructions that any boot sector virus would possess. Even if Vx2000 does not have a signature any new boot sector virus that has attacked your system will be detected. Send in a sample of the virus in order to get a specific cure and more details of the virus. (See "To prepare a Sample disk" in this Chapter).

Vx2000 has reported a Generic Macro virus found

While checking for documents for viruses Vx2000 will detect any macros that are present in it. This may or may not be a virus macro. As there can be genuine macros that you have created to make your work easier, it is left to you to decide the authenticity of the macro before using the file. Certain Microsoft's default

Appendix-B : Trouble Shooting

templates do contain macros. In such cases you could ignore this message and proceed.

If this has been reported in the documents that you are normally using and you have not created any macros it indicates the presence of a virus. Please copy the files that were reported to have Generic macros to a floppy and mail it to us or send the files in a Zipped form to K7VL@K7Computing.com to enable us to study it and give you a solution.

Though I have booted my system with a bootable disk virus is reported in memory

Before you make a conclusion make sure that the system was booted with a floppy. When you boot the system through a floppy the prompt after booting should be A:

If you have confirmed that the system is booted through the A drive and Vx2000 reports a virus in memory it clearly indicates that the bootable disk is also infected with the virus. Use another clean bootable disk or clean this disk in an uninfected system and then proceed.

System does not boot

The system may not boot due to one of the following reasons

- The partition table code is corrupted
- The partition table data is corrupted
- The boot sector is corrupted
- The O/S files are missing or corrupted
- The default shell Command.com is missing or corrupted.
- The files loaded through CONFIG.SYS or autoexec.bat are corrupted or missing
- There is a hardware problem

To identify the exact problem we have to eliminate the problems one by one.

Boot the system with a clean disk from Drive A: After booting when you see the A: prompt type C:

If you get the "Invalid specification" this confirms that the Partition table data is corrupted.

Appendix-B : Trouble Shooting

If you get the C: prompt it indicates that the Partition table code had been corrupted. If there are no drivers like "Ontrack" loaded then issue the following command to replace the code

```
A:\fdisk / mbr
```

Now try booting the system through C:

If it does not boot, then boot the system through A:. Transfer the system files from the floppy by issuing the following command

```
A:\sys C:
```

Boot the system through the hard disk. While booting the system bypass the AUTOEXEC.BAT and CONFIG.SYS by pressing the [F8] function key. If the system boots normally it indicates that the driver files or any program that is being loaded while booting is corrupted. Replace these programs from the original disks and then try booting.

In spite of the above actions if the system refuses to boot it may be due to a Hardware problem or the disk might have repaired using some disk tools.