

[Virus Buster Lite Help](#)



<u>Commands</u>	Reference to menu commands.
<u>Procedures</u>	Step-by-step instructions.
<u>Reference</u>	Useful information on viruses.
<u>Keyboard Guide</u>	Table of useful key combinations.
<u>Glossary</u>	Definitions of terms.

Leprechaun
SOFTWARE PTY LTD

(c) 1994 ACN 010 989 670

Tel +61 7 823 1300

Fax +61 7 823 1233

Commands

Scan Menu

Scan Memory

Scan A:

Scan B:

Scan C:

Scan Selections:

Exit

Options Menu

When virus detected

Terminate when

Generic sensitivity

Alarm enabled

Extended scan

Scan sub-directories

Data file name

Save options on exit

Save options now

Log file menu

Logging on

Extended log

Log file name

Access menu

[Set access](#)

[Change password](#)

Speedbar

Virus Buster Lite uses a speed bar to facilitate common operations. See [Speedbar](#).

Edit log window

The log file has its own menu. To get help on any item on that menu see [Log Window](#).

Related Topics

[Procedures](#)

Procedures

Scanning for viruses

Scanning new diskettes

Cleaning up an infection

Controlling use of Virus Buster Lite

Related Topics

Commands

Reference

Anti-virus strategy

Computer security

False alarms

File integrity checking

Generic vs Specific

Leprechaun Software

Operation monitoring

Symptoms of infection

Passive vs Active

Virus scanning

Related Topics

Glossary

Procedures

Scanning for viruses

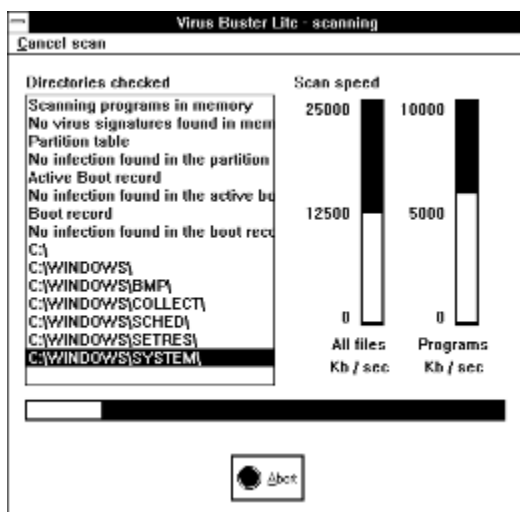
Virus Buster Lite scans program files, memory and disk boot records for viruses.

To perform a virus scan you need to follow these steps:

Select what you want to scan.

Start the scan operation.

During the scan, a display similar to that below will be shown.



The box on the left of the display lists each directory as it is scanned.

The graphs at the right of the display show the current speed of the scan. The speed (in Kb/sec) is shown for all files (including data files, which are skipped) and for program files (which are searched for signatures).

The graph at the bottom of the display shows the progress of the scan as a percentage of the complete scan.

Related Topics

Scanning new diskettes

Cleaning up an infection

Scanning new diskettes

One of the best anti-virus measures that you can take is to scan all new diskettes for viruses before you use them.

Virus Buster Lite makes it easy for you to scan new diskettes as they are used. Just set the set the Automatic diskette scan option. All new diskettes will be automatically scanned the first time another program tries to access them.

Related Topics

Scanning for viruses

Cleaning up an infection

Before beginning a clean up, take steps to stop the virus from spreading.

Clean up each machine in turn.

To clean each machine, boot from a known clean DOS diskette, run Virus Buster Lite for DOS, or Virus Buster Professional from a floppy and scan all hard drives on the machine.

Delete any infected files found. If you use Virus Buster Professional you can usually remove the virus from the file, rather than deleting the file.

Restore any deleted files from copies of the original diskettes. Some programs will need re-installation, refer to the documentation for the particular program.

Once the machine is clean, reboot normally and verify that it operates correctly. When rebooting a network, use VirusGate to prevent infected users re-infecting the server.

Complete the cleanup by scanning all diskettes which may have been used in the machine.

Controlling use of Virus Buster Lite

You may wish to limit access to Virus Buster Lite.

You can limit access in total, or limit access to some of Virus Buster Lite operations.

To limit access you need to

Set a password

Set what operations require the entry of the password

You can do this in either order. If you set the operations and the password is not set, you will be asked to enter the password.

CAUTION: The password is never displayed and cannot be discovered. If you set the password, ensure that you remember it.

Anti-virus strategy

An anti-virus strategy is the first weapon against viruses and includes issues such as backing up data, using legal software and controlling access to your system.

As well as configuring Virus Buster Lite to achieve the best level of protection for your system, a strategy should be developed and implemented. In a company situation all staff should be aware of the strategy and understand the virus danger.

Key elements of a good anti-virus strategy are:

Check all software.

Check all software and disks with Virus Buster Lite before loading them on your machine.

If possible establish a clean machine which is isolated from all other systems and does not contain critical data. The clean machine should be reserved for testing purposes and have a complete copy of Virus Buster Professional installed.

Test new software by running it on this machine. Use Virus Buster Professional to check for viruses after running the new software a number of times.

Use only legal software.

Avoid pirated software and be cautious when down-loading software from bulletin boards. Try to use only reputable bulletin boards who themselves have in place a secure anti-virus strategy.

Ensure staff do not use software or disks from home without checking them with the system administrator.

Keep a clean boot disk.

Establish a clean, bootable computer system on disk. In the event of a successful virus attack the first step is to restore the system to a virus-free state.

Write protect the system disks to ensure they will not be infected.

Add the following files to this disk: SYS.COM - FORMAT.COM - FDISK.COM (or FDISK.EXE) - CHKDSK.COM (or CHKDSK.EXE) - DISKCOPY.COM

Don't install from original program disks.

When installing software do not use the original disks (unless you have to).

Re-boot using a clean system disk, make copies of the original software then perform the installation using these copies. This ensures the original disks are never infected.

Make regular backups of data only. This avoids any programs which may be infected.

Keep enough backups.

Keep back-ups for an extended period of time.

A virus may not be noticed for some time after it has started to corrupt data. Archive disks and tapes regularly.

Watch the computer.

Monitor the operation of the computer whenever you use it.

Note normal behaviour during boot up and program loading, including time taken, screen displays and disk activity. If it behaves strangely, investigate fully.

Use network protections.

Limit user access on networks.

Many networks contain useful mechanisms to protect the system from errant users and rogue programs. If these are available to you use them.

Keep up to date.

Keep Virus Buster Lite up to date.

New virus technology is appearing all the time and this makes it important to have the latest anti-virus software available to give maximum protection.

Keep informed.

Include anti-virus seminars in staff training programs.

These seminars should be aimed at all staff and raise awareness of the virus threat. Specialist briefings should also be carried out for technical and support staff.

Keep a recovery disk.

It is good practice to maintain an emergency recovery disk for each PC.

This diskette should contain copies of critical system areas such as the partition table, boot record, FAT table and root directory.

Computer security

Defending your system against virus attack can be done in many ways. Most of the available methods can be categorised as one of these;

virus scanning,

integrity checking,

activity monitoring.

Virus Buster Lite uses two methods of virus scanning. Virus Buster professional uses all the above methods to provide a comprehensive defence system.

In addition, you may implement methods to allow recovery from virus and other disasters, such as taking regular backups, and physically isolating your machine from unauthorised users.

Virus Buster Professional will enable you to take additional measures, to allow recovery of information which can not be recovered with normal utilities.

False alarms

When Virus Buster Lite is scanning for viruses, false alarms occur when the software detects a virus in a file which, in fact, is clean.

This is a rare occurrence, but with the explosion in numbers of new viruses and the advent of the mutating type of virus, this phenomenon may become a little more common.

To avoid false alarms you need to apply judgement in your use of Virus Buster. Virus Buster will help by providing guidance when a warning is given, and indicating whether the warning is critical, or only to be considered if other associated warnings occur.

File integrity checking

All viruses have one common characteristic. This can be exploited to detect viruses.

In order to spread, a virus must make some change to executable code on a storage device. In simple terms, a virus must change program files on disk in order to survive.

File integrity tools provide the means to regularly audit all executable code on a disk in order to detect any changes made. Because executable code is rarely changed in a typical office PC, any changes should be treated as suspicious signs of a possible virus infection.

In PCs where code is regularly changed, such as software development houses, valid changes are generally limited to specific directories which are excluded from the audits.

Virus Buster Professional and BootChecker are file integrity checkers.

Advantages

- o Will reliably detect any virus, provided the operating system is reliable.
- o Is fast.

Disadvantages

- o May generate false alarms when legitimate changes to executable code are made (such as upgrades to application packages.)
- o Only detects viruses after an infection has occurred.

Generic vs Specific

Generic virus defences are often touted as being superior to the older, specific methods. Here is a comparison of the two methods.

Generic

A generic defence is designed to be effective against all viruses. It therefore does not rely upon the characteristics of known viruses, but exploits a general characteristic of viruses, in order to detect and/or prevent virus activity.

Naturally, a generic defence will not provide identification of a virus by name, but will issue warnings of a general nature, such as "program attempted to format hard disk - virus suspected".

Just because a virus defence is generic by nature does not mean that it will successfully stop all viruses. It is only as good as the techniques and assumptions used in constructing it. Many generic virus defence tools are only useful against simple viruses.

Specific

A specific virus defence is designed to detect viruses by the specific characteristics of the virus. It relies on a sound analysis of each particular virus leading to a reliable identification method for each virus.

A specific virus tool will usually identify a virus by name. The identification method may allow for some variation in the expected virus form, and then indicate that these are possible viruses which appear "similar to" a known virus.

A specific virus defence tool is generally useless against new viruses, but will sometimes detect a new virus which has been written using code from an old virus.

Virus Buster Lite uses both specific and generic virus detection.

Leprechaun Software

Leprechaun Software is dedicated to bringing you the best in security software.

We have a complete range of anti-virus tools including:

Virus Buster Professional for DOS and Windows A complete anti-virus solution.

Virus Buster Lite for DOS and Windows This is it!

VirusGate for Netware servers Guards your server against infected users.

The Anti-virus Toolkit including FAB, CATCH and FINDSIGN.

Leprechaun Software also produces security software for medium security applications, including DiskLok and KeyLok, both of which are fully Windows compatible.

Operation monitoring

An operation monitor "watches" the PC and provide an alert and/or blocks actions which are defined as virus-like or simply dangerous.

Virus Buster Professional provides activity monitoring.

Advantages

- o Can prevent viruses spreading and/or activating.
- o Can prevent disastrous accidental actions be users.

Disadvantages

- o May generate false alarms.
- o May prove unduly restrictive to normal operations.
- o May cause system slowdown as resources are utilised in monitoring activities.

Symptoms of infection

Computer viruses produce a wide range of different effects.

The first sign that a virus might be present could be disappearing files or a slowing of computer speed.

Other effects could be unusual screen messages, strange memory readings, changes in the boot record of a partition table, bad sectors appearing on the hard disk, application programs failing to run or not running properly, changes to file sizes, disk writes or format commands which occur by themselves.

As a general rule, if it has any of these symptoms, it's probably a virus:

- o Your machine exhibits the same symptoms as your friends machine
- o The machine plays tunes by itself
- o A "dir" after booting from the hard drive displays different file sizes to the same directory after booting from a clean DOS diskette.
- o Program files grow in size or have their date changed

If it has any of these symptoms, it may be a virus:

- o The machine runs slower than normal
- o The hard disk light and/or the diskette lights come on more than usual
- o Unusual messages are displayed on the screen, or the screen behaves oddly
- o Programs suddenly stop running because of insufficient memory (and you haven't added any new memory resident utilities).
- o The keyboard locks up or behaves badly

Passive vs Active

Anti-virus tools can be categorised as either passive or active.

The best type of tool depends upon your particular needs and risks. Virus Buster Lite uses a passive scan. Virus Buster Professional utilises both types to provide you the maximum flexibility.

Passive

A passive defence tool has to be run each time you want to check for viruses. It is generally a "standard" DOS or Windows application.

Active

An active defence tool provides continuous protection.

It may be loaded into memory and become part of the operating system or it may be resident in an independent processor which "watches" the main PC.

Virus scanning

Scanning a file for virus signatures and signs is the oldest method of virus defence. It has a place in any defence but should not be the principal or only defence method.

Advantages

- o Can provide a positive identification of a virus by name, allowing you to gain information about the virus from other sources, such as VInfo.
- o Can quickly locate files which have been infected during a virus outbreak.
- o Can detect known viruses in new programs before the programs are introduced to the system.

Disadvantages

- o Can only detect known viruses.

Virus signatures

A virus signature is a sequence of instructions taken from the actual virus.

The sequence is chosen carefully to ensure that it is sufficient to uniquely identify the virus. Sometimes the sequence may just happen to occur in a legitimate (un-infected) program. This is called a false alarm. Sometimes the sequence may also occur in a similar virus. This leads to mis-identification of the virus.

Code analysis

Virus Buster Lite scans for viruses using two methods. Code analysis and signature scanning.

Code analysis involves tracing the execution of each program scanned and comparing the actions performed by the program with actions 'typical' of a virus. If a program is found to contain sufficient of these actions then it is flagged as being suspect.

Code analysis is also termed generic detection, artificial intelligence and black magic.

Automatic diskette scan

Virus Buster Lite is able to detect whenever a new diskette is being read by any other program, and can scan the diskette automatically.

To do this you need to turn on the Automatic scan option in the Options dialog. You can then minimize Virus Buster Lite and go about your normal work. Whenever a new diskette is accessed, Virus Buster Lite will spring into action, scanning the diskette and warning you if the diskette contains a virus.

VBL.INI

Virus Buster Lite has many options to enable you to configure it to operate exactly the way you prefer.

All option settings are recorded in the INI called VBL.INI. This file is located in the WINDOWS directory.

Although the file is a simple text file, it is recommended that you not edit it manually as Virus Buster Lite may not recognise the changes you make.

Title bar

The title bar shows the name of the application.

The active window (the one in which you are working) has a different color to other windows.

Minimize icon

Click on the minimize icon to reduce the window to an icon.

Select `RestoreCONTROL_RESTORE` to return the window to its normal size.

Stopping virus spread

These comments apply to resident viruses, but can safely be used for non-resident viruses.

To prevent a virus spreading you must firstly turn the computer off to remove it from memory. If a network is infected, take the server down.

Take steps to contain the problem. Stop any further transfer of programs by modem, network or diskette. Notify any clients or associates that may have been infected.

Now boot from a known clean boot diskette. (Ensure that drive A: is turned on in the BIOS first).

Take backup copies of all data. **This is essential.** Removal of the virus from program files may prevent access to data files.

See the section on Virus cleanup for more information.

Edit log window

The edit log window displays the logfile. You can also edit the log and save it to disk.

The edit log window has a menu and a speedbar.

You can leave the log open and switch back to the application window if required.

Access settings

You can password protect access to some Virus Buster Lite operations.

These settings are available:

- | | |
|-----------------------|--|
| Run program | The password must be given before Virus Buster Lite will open. |
| Change options | The password must be given to change any of Virus Buster Lite's options. |
| Delete files | The password must be given before Virus Buster Lite will delete an infected or suspect file. |

Press the OK button to set the access control to the displayed settings. Press Cancel to leave the settings as they were.

Related Topics

[Controlling use of Virus Buster Lite](#)

All options

This allows you to set most of Virus Buster Lite's scanning options in one convenient dialog box.

The dialog box has these settings:

Action when virus is found Define what Virus Buster Lite does when an infection is found.

Generic detection sensitivity How sensitive Virus Buster Lite is to programs which have some virus characteristics.

Alarm sounds Alarm sounds when an infection is found.

Extended scan Brief or detailed scan of some files.

Scan sub-directories Scan for program files within sub-directories.

Terminate scan if... Terminate the scan is a number of files are checked and no infection is found.

Automatic diskette scan Automatically scan new diskettes as they are accessed by other applications.

Press the OK button to set the options to the displayed settings. Press Cancel to leave the options as they were.

Related Topics

Options menu

Diskette is clean

The diskette scan is complete and no virus infections were found.

If you want to immediately scan another diskette in the same drive, replace the diskette and press the OK button.

If you want to quit scanning diskettes in this drive, press Cancel.

Related Topics

[Scanning for viruses](#)

Diskette is suspect

The diskette scan is complete but at least one suspect file was found.

If you want to immediately scan another diskette in the same drive, replace the diskette and press the OK button.

If you want to quit scanning diskettes in this drive, press Cancel.

Related Topics

Scanning for viruses

Code analysis

Diskette is infected

The diskette scan is complete but at least one infection was found.

If you have not already removed the infected file, you should set the diskette aside and re-format it.

If you want to immediately scan another diskette in the same drive, replace the diskette and press the OK button.

If you want to quit scanning diskettes in this drive, press Cancel.

Related Topics

[Scanning for viruses](#)

[Virus signatures](#)

[Cleaning up an infection](#)

Quit Virus Buster Lite

Whenever you exit from Virus Buster Lite the program checks that you really wanted to exit before it actually quits.

Press OK to quit, or press Cancel to return to Virus Buster Lite.

Generic sensitivity

Virus Buster Lite scans for viruses in two ways, by signature and by code analysis. Code analysis is a generic detection method.

This setting determines how 'paranoid' Virus Buster Lite is when it analyses programs.

At high sensitivity, Virus Buster Lite will report any program which looks like it may possibly be a virus as being suspect. You can expect a few false alarms at this setting.

At low sensitivity, Virus Buster Lite will only report programs that have a strong resemblance to a virus. It is possible, but unlikely, that you still have a couple of false alarms at this setting.

In automatic mode, Virus Buster Lite begins in low sensitivity mode, but will switch to high sensitivity mode if any viruses are positively identified during the scan. This helps it to detect all file infections.

You can turn off the code analysis feature if you want to rely solely on the signature scanning.

You can also change this setting from the Options dialog box by pressing the Options button on the speed bar.

Related Topics

Generic vs Specific

Code analysis

Enter the password

The operation you are attempting to perform has been password protected.

To continue, you must enter the current password, then press the OK button.

Press the CANCEL button if you do not know the password.

Log file settings

Set the log file to operate the way you want it.

Log to file Turns the logging of scan operations and results on or off. When ticked, a log file is written each time a scan is performed.

Type of log When extended logging is enabled, the log file records the filename of every file scanned.

Press **Set file** to change the log file used. Press **OK** to use the displayed settings. Press **Cancel** to leave the settings as they were.

Action when a virus is found

This option allows you to specify what automatic action Virus Buster Lite will take when a virus is detected. You can choose from the following actions.

- | | |
|---------------------------------|--|
| Ignore the virus warning | Virus detections are ignored. You would normally use this only when you are logging the results and when you already know that you have a virus infection. |
| Delete the suspect file | Any file found to contain a virus will be immediately deleted. Normally you would only use this during the clean-up operation after a virus infection is discovered. |
| Abort the scan | The scan will halt immediately any virus infection is detected. You might use this to prevent the virus infecting other files during the scan. |
| Prompt for action | If a virus is detected, the scan is immediately halted and a dialog box prompts you for what action to take. This is the normal setting. |

You can also change this setting from the Options dialog box by pressing the Options button on the speed bar.

[Virus in partition table](#)

A virus signature has been found in the partition table or boot record of the disk being scanned.

If the virus is found in the C: disk, or the diskette that you have booted from, the situation is very serious. Seek professional help.

If the virus is found in another diskette, you can use FORMAT to remove the virus (this will also destroy all data on the diskette).

Virus Buster Professional will remove almost all boot sector viruses. FAB (also from Leprechaun Software) can be used to remove all other viruses, and to recover disks which have been damaged by a virus.

Related Topics

[Scanning for viruses](#)

[Virus signatures](#)

[Cleaning up an infection](#)

Set new password

Type in your new password in the top line.

Press the TAB key, and type the password again, exactly as you first typed it.

Press the RETURN key, or click the OK button.

Press the CANCEL button to leave the password unchanged.

To turn the password off, set a new password of no characters (leave each line empty).

If you make a mistake entering the password, an error message will appear and you will be able to try again.

Scan complete

The requested scan is complete.

Press the OK button to return to the main window.

Press the Stats button to review the scan statistics.

Press the Log button to edit the log from the scan. This button will not appear if logging is turned off.

Scan statistics

This shows brief statistics for the last scan performed.

Directories	This is the total number of directories scanned. It includes all sub-directories.
Files	This is the total number of files found in all directories. It includes data files. Data files do not need to be scanned for virus signatures.
Executables	This is the total number of executable files found in all directories.
Infected	This is the total number of executable files which were identified as being infected by a virus.
Suspect	This is the total number of executable files which were identified as being suspect.
Started	This is the time of day when the scan was started.
Elapsed	This is the total number of seconds taken to complete the scan. Because Windows is a multi-tasking system, the elapsed time can vary dramatically even when scanning the same disk.

File may be infected

A number of virus like characteristics have been detected in the file shown.

A virus has not been positively identified. This is a tentative identification of a new, unknown virus.

If the file is new, or has not been used, you should take this warning rather seriously. Do not run the file until it has been checked further and cleared.

If the file is old and has been used in the past, it is probably safe to ignore the warning if only a few files on the disk give this alarm. A real virus spreads widely and you can expect many files to give a warning.

Press the **Ignore** button to leave the virus in the file. Use this option if you know that you can isolate the virus and wish to keep a copy of it for later research.

Press the **Delete** button to delete the named file. This will destroy this copy of the virus. You should search all disks for further copies of the virus.

Press the **Abort** button to leave the file alone and terminate the scan. Use this option if you think that the virus may be active in memory.

Related Topics

[Code analysis](#)

Terminate scan if...

This allows you to automatically terminate the virus scan if a number of files have been checked and no virus infections have been found.

If a virus is detected during the scanning of these first files, then this setting is ignored for the rest of the scan. (All files will be scanned.)

To change the setting, type in the required maximum number of files to scan. You can also use the scroll bar to increment or decrement the current setting.

To always scan all files, set the number of files to zero (0).

Related Topics

[Options menu](#)

Virus detected in file

The signature of the named virus was found in the file shown.

Press the Delete to delete the named file. This will destroy this copy of the virus. You should search all disks for further copies of the virus.

Press the Ignore button to leave the virus in the file. Use this option if you know that you can isolate the virus and wish to keep a copy of it for later research.

Press the Abort button to leave the file alone and terminate the scan. Use this option if you think that the virus may be active in memory.

Related Topics

[Scanning for viruses](#)

[Virus signatures](#)

[Cleaning up an infection](#)

[Virus in memory](#)

The signature of the named virus was found in memory.

THIS IS A CRITICAL SITUATION.

You should save all work and power down the machine.

Clean up the machine after booting from a known clean DOS diskette. Do not run any programs from the hard disk until you have scanned them and found them to be clean.

Related Topics

[Scanning for viruses](#)

[Virus signatures](#)

[Cleaning up an infection](#)

Directory

This shows the currently selected directory to scan.

You can change to another directory using the arrow at the right end of the directory.

To scan a directory, select the directory, make sure that the Directory radio button is on, then use the Scan selections menu command, or press the Scan speed button.

Related Topics

All local hard disks

Scanning for viruses

Selected disks

Select directory

Press this button to use the drop down directory box.

You can select a directory from the drop down box by double-clicking on a directory in the box. All directory names are listed within square brackets.

Select the [..] directory to move to the parent directory. For example, if the Directory is set to C:\WINDOWS\SYSTEM, selecting [..] will change to C:\WINDOWS.

Select another drive using the [d], where "d" is the drive required.

Related Topics

Directory

All local hard disks

This selects all local hard drives. These are those drives that are not removable and not network drives.

The selected drives are shown in the Disks panel. You can click on that panel to select further disks to scan, or to remove some from the selection.

To scan the disks, make sure that the All local radio button is on, then use the Scan selections menu command, or press the Scan speed button.

Related Topics

Scanning for viruses

Directory

Selected disks

Selected disks

This allows you to select disks by name.

All disk drives detected on the system are listed in the display. Click on a disk button to select or de-select a disk. When a disk is scanned, all files in the root directory are scanned. If the Scan sub directories option is on, then all files on the disk will be scanned.

To scan the disks, make sure that the Selected disks radio button is on, then use the Scan selections menu command, or press the Scan speed button.

Related Topics

Scanning for viruses

Directory

All local hard disks

Also scan memory

When this is set, a scan of all program memory is performed prior to the file scan.

It is recommended that the memory scan be left turned on, as it is much safer to perform a memory scan prior to a file scan, and the extra time taken is usually irrelevant.

You may wish to turn this off if you are scanning many diskettes. Once a memory scan has completed, it is safe to proceed with diskette scans.

Related Topics

[Scanning for viruses](#)

[Scan Memory](#)

Also check Boot + MBR

When this is set, a scan of the disk boot record (and partition table for hard drives) is performed prior to the file scan.

It is recommended that the boot scan be left turned on, as it is much safer to perform a boot scan prior to a file scan, and the extra time taken is usually irrelevant.

Related Topics

[Scanning for viruses](#)

[Boot sector virus](#)

[Also check sub directories](#)

When this is set, all files in sub-directories of the nominated scan area will be done.

Related Topics

[Scanning for viruses](#)

[Scan sub-directories](#)

Check disk A:

Check this to include a disk in the A: drive in the scan.

You can scan a diskette in A: directly using the Scan A: speed button or menu command.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk B:

Check this to include a disk in the B: drive in the scan.

You can scan a diskette in B: directly using the Scan B: speed button or menu command.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk C:

Check this to include the C: drive in the scan.

You can scan the C: drive directly using the Scan C: menu command.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk D:

Check this to include the D: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk E:

Check this to include the E: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk F:

Check this to include the F: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk G:

Check this to include the G: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk H:

Check this to include the H: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk I:

Check this to include the I: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk J:

Check this to include the J: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk K:

Check this to include the K: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk L:

Check this to include the L: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk M:

Check this to include the M: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk N:

Check this to include the N: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk O:

Check this to include the O: drive in the scan.

To scan the disk,make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk P:

Check this to include the P: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk Q:

Check this to include the Q: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk R:

Check this to include the R: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk S:

Check this to include the S: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk T:

Check this to include the T: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk U:

Check this to include the U: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk V:

Check this to include the V: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk W:

Check this to include the W: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk X:

Check this to include the X: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk Y:

Check this to include the Y: drive in the scan.

To scan the disk, make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Check disk Z:

Check this to include the Z: drive in the scan.

To scan the disk,make sure that the Selected disks button is on, then use the Scan selections menu command, or press the Scan speed button.

Control menu

The control menu includes commands to change the location of the application window, minimize and restore it, and to switch to other Windows applications.

For more information, see the individual commands below.

<u>Restore</u>	Restore the window to normal size after it has been minimized.
<u>Move:</u>	Use the keyboard to move the window to another position.
<u>Minimize</u>	Reduce the window to an icon.
<u>Close</u>	Close the window.
<u>Switch to</u>	Switch to another running application.

Restore

Restore the application to its normal size after you have minimized it to an icon.

You can also perform this operation by double clicking on the icon, or by pressing ENTER when the icon is selected.

This command is not available when the window is at its normal size.

Move

Use the keyboard to move the application to another position.

When this command is used, the mouse pointer changes to a four headed arrow. Now use the arrow keys to move the window. Press ENTER to place the window in the selected position.

To move the application with a mouse, drag the title bar to the new position.

Size

Use the keyboard to change the size of the log edit window. (The application window cannot be resized.)

When this command is used, the mouse pointer changes to a four headed arrow. Now use the arrow keys to move the cursor to the border you want. Use an arrow key to move the border. Press ENTER when the window is the size you want.

To resize the log edit window with a mouse, drag a corner or a border to the required size.

Minimize

Reduce the application to an icon.

You may want to do this if you have finished using Virus Buster Lite, but want to keep it ready for later use.

If you want to use the automatic diskette scan feature you need to keep Virus Buster Lite either as a normal application, or as an icon.

You can also minimize the application by clicking on the minimize button in the top right of the window.

Maximize

Enlarge the edit log window to full screen. (The application window cannot be maximized.)

You can also minimize the edit log window by clicking on the maximize button in the top right of the window.

Close

Closes the application window, quitting Virus Buster Lite.

You can also exit the application in other ways, see the [exit](#) command.

Switch to

Opens Task List, which allows you to switch to another running application and to rearrange the windows on the desktop.

You can also switch to other applications by pressing ALT-TAB, or by clicking on another application window.

Scan menu

The scan menu includes commands that allow you to scan for viruses in the computer memory, in drives A:, B: and C:, and the current selected disk areas. You can also access the exit command here.

For more information, see the individual commands below.

<u>Scan Memory</u>	Scan the memory of the computer for viruses.
<u>Scan A:</u>	Scan the diskette in drive A: for viruses.
<u>Scan B:</u>	Scan the diskette in drive B: for viruses.
<u>Scan C:</u>	Scan the C: drive for viruses.
<u>Scan Selections:</u>	Scan the currently selected areas for viruses.
<u>Exit</u>	Close Virus Buster Lite for Windows.

You can use the speed bar for most of these commands.

Scan memory

Use this command to scan only the memory of the computer for viruses.

To improve speed, only memory allocated to executable code is scanned. Viruses cannot safely reside in unallocated memory, so all viruses will still be detected.

If a virus is detected in memory you should take great care in preventing spreading of the virus.

Memory is scanned when you:

- o Select the Scan memory command from the Scan menu.
- o Select the Scan A:, Scan B:, Scan C: or Scan selections commands from the Scan menu and the Also scan memory box is checked.
- o Press the Scan A:, Scan B: or Scan speed bar buttons and the Also scan memory box is checked.

Scan disk A:

Use this command to scan a diskette in drive A: for viruses.

You can scan a diskette in three ways:

- o Select the appropriate Scan command from the Scan menu.
- o Press the appropriate Scan button on the speed bar.
- o Set the Automatic diskette scan option and access the diskette with any other program.

Unless this is an automatic scan, when the scan is complete you will be asked if you be given the opportunity to immediately scan another diskette in the same drive.

If a virus was found or was suspected on the diskette, you will be reminded of this at the end of the scan.

Scan disk B:

Use this command to scan a diskette in drive B: for viruses.

If your PC does not have a second diskette drive, this option will not be available.

You can scan a diskette in three ways:

- o Select the appropriate Scan command from the Scan menu.
- o Press the appropriate Scan button on the speed bar.
- o Set the Automatic diskette scan option and access the diskette with any other program.

Unless this is an automatic scan, when the scan is complete you will be asked if you be given the opportunity to immediately scan another diskette in the same drive.

If a virus was found or was suspected on the diskette, you will be reminded of this at the end of the scan.

Scan disk C:

Use this command to scan the C: drive for viruses.

You can scan the C: drive in three ways:

- o Select the Scan C: command from the Scan menu.
- o Select the Scan selected command from the Scan menu when either:
 - Directory is ticked and the directory name is set to C:\, or
 - All local hard disks is ticked, or
 - Selected disks is ticked and the C: box is ticked.
- o Press the Scan selected button on the speed bar when any of the above are true.

When the scan is complete you can review the log file.

Scan selections

Use this command to scan the current selected areas for viruses.

The current selected areas are shown in the main window. You can define the disk areas to scan, whether or not to scan memory, disk boot records, and whether or not to scan sub-directories.

To scan one particular directory, click on the Directory button near the top of the main window.

To scan all the hard drives on the PC, click on the All local hard disks button.

To scan particular disk drives only, click on the Selected disks button. (Only available drives are shown.)

To scan the boot record and MBR (for hard disks) of all disks before scanning of any files, tick the Boot record + MBR checkbox.

Exit

Use this command to exit Virus Buster Lite for Windows.

You can exit from Virus Buster Lite in four ways:

- o Select the Close command from the Control menu.
- o Double click on the system menu button.
- o Select the Exit command from the Scan menu.
- o Click on the Exit button on the speed bar.

Whenever you exit from Virus Buster Lite the program checks that you really wanted to exit before it actually quits.

Press OK to quit, or press Cancel to return to Virus Buster Lite.

Options menu

The options menu provides commands to configure Virus Buster Lite to operate exactly the way you want.

For more information, see the individual commands below.

<u>When virus detected</u>	Define what action the program will automatically take when a virus is detected.
<u>Terminate when</u>	Set an optional maximum number of files to scan before aborting the scan.
<u>Generic sensitivity</u>	Set the sensitivity of the generic virus detection algorithms.
<u>Alarm enabled</u>	If a virus is found the program can sound an audible alarm.
<u>Extended scan</u>	Change the current password.
<u>Scan sub-directories</u>	Automatically scan any sub-directories found.
<u>Data file name</u>	Select the virus signature data file to use.
<u>Save options on exit</u>	Automatically save the current configuration when you exit from Virus Buster Lite.
<u>Save options now</u>	Save the current configuration immediately.

You can use the speed bar to start a dialog box which allows easy access to most of the options.

When virus detected

This option allows you to specify what automatic action Virus Buster Lite will take when a virus is detected. You can choose from the following actions.

- | | |
|---------------------------------|--|
| Ignore the virus warning | Virus detections are ignored. You would normally use this only when you are logging the results and when you already know that you have a virus infection. |
| Delete the suspect file | Any file found to contain a virus will be immediately deleted. Normally you would only use this during the clean-up operation after a virus infection is discovered. |
| Abort the scan | The scan will halt immediately any virus infection is detected. You might use this to prevent the virus infecting other files during the scan. |
| Prompt for action | If a virus is detected, the scan is immediately halted and a dialog box prompts you for what action to take. This is the normal setting. |

You can also change this setting from the Options dialog box by pressing the Options button on the speed bar.

Terminate when...

This allows you to automatically terminate the virus scan if a number of files have been checked and no virus infections have been found.

If a virus is detected during the scanning of these first files, then this setting is ignored for the rest of the scan. (All files will be scanned.)

To change the setting, type in the required maximum number of files to scan. You can also use the scroll bar to increment or decrement the current setting.

To always scan all files, set the number of files to zero (0).

You can also change this setting from the Options dialog box by pressing the Options button on the speed bar.

Generic sensitivity...

Virus Buster Lite scans for viruses in two ways, by signature and by code analysis. Code analysis is a generic detection method.

This setting determines how 'paranoid' Virus Buster Lite is when it analyses programs.

At high sensitivity, Virus Buster Lite will report any program which looks like it may possibly be a virus as being suspect. You can expect a few false alarms at this setting.

At low sensitivity, Virus Buster Lite will only report programs that have a strong resemblance to a virus. It is possible, but unlikely, that you still have a couple of false alarms at this setting.

In automatic mode, Virus Buster Lite begins in low sensitivity mode, but will switch to high sensitivity mode if any viruses are positively identified during the scan. This helps it to detect all file infections.

You can turn off the code analysis feature if you want to rely solely on the signature scanning.

You can also change this setting from the Options dialog box by pressing the Options button on the speed bar.

Alarm enabled

Virus Buster Lite scans for viruses in two ways, by signature

You can also change this setting from the Options dialog box by pressing the Options button on the speed bar.

Extended scan

Virus Buster Lite normally scans some files, which are considered unlikely to be infected, very briefly. Setting the extended scan ON will mean a more thorough scan of these files, but it will also slow the scan.

You can also change this setting from the Options dialog box by pressing the Options button on the speed bar.

Scan sub-directories

When you scan a disk or a directory, Virus Buster Lite can be set to either:

scan just the files in the root or nominated directory

or

scan all files in all sub-directories.

Normally you will want to always scan all sub-directories.

You can also change this setting on the main window.

Data file name

Virus Buster Lite uses a database of virus signatures.

This database contains the signatures of thousands of viruses. Virus Buster Lite always scans for all signatures in every file checked. If a signature match is found Virus Buster Lite notifies you that a virus has been positively identified.

Regular updates of the database file are available.

Virus Buster Lite can also detect unknown viruses using code analysis.

You can also change this setting on the main window.

Save options on exit

Virus Buster Lite has many options to enable you to configure it to operate exactly the way you prefer.

All option settings are recorded in the file VBL.INI.

When this option is set, all option settings are saved each time you exit from Virus Buster Lite. This means that the program will run exactly as you left it last time it was used.

Related Topics

Save options now

Save options now

Virus Buster Lite has many options to enable you to configure it to operate exactly the way you prefer.

If you don't want the options saved automatically each time you exit, you might use this after you have finished configuring the program.

Related Topics

[Save options on exit](#)

Log file menu

The log file menu provides commands to configure the log file.

For more information, see the individual commands below.

<u>Logging on</u>	Turns recording to the log file on and off.
<u>Extended log</u>	Turns recording of all results, rather than just recording virus infections, on and off.
<u>Log file name</u>	Allows you to define the file used as the log.

You can use the speed bar to start a dialog box which allows easy access to these options.

Logging on

This turns the logging of scan operations and results on or off. When ticked, a log file is written each time a scan is performed.

You can also change this setting in the Log options dialog box, accessed by clicking the Log button on the speedbar.

Related Topics

[Extended log](#)

[Log file name](#)

Extended log

The log records the results of scan operations.

Normally the log file records only the names of directories scanned, and the filenames of any infected files.

When extended logging is enabled, the log file records the filename of every file scanned.

You can also change this setting in the Log options dialog box, accessed by clicking the Log button on the speedbar.

Related Topics

[Logging on](#)

[Log file name](#)

Log file name

The log records the results of scan operations.

Use this command to change the name of the log file. Normally the log file is overwritten each time a scan is performed. If you want to save the results of a scan permanently, use this option to start logging to a new file.

You can also change this setting in the Log options dialog box, accessed by clicking the Log button on the speedbar.

Related Topics

[Logging on](#)

[Extended log](#)

Access menu

The access menu provides commands to set password control on the use of Virus Buster Lite.

For more information, see the individual commands below.

Set access Set the program operations for which password access will be set.

Change password Change the current password.

You can use the speed bar to start the Set access dialog box.

Set access

Set the program operations for which password access will be required.

You can password protect:

Running of Virus Buster Lite password required to start the application.

Change options password required to modify any option settings.

Delete files password required to delete infected files.

The password is common for all restrictions.

Related Topics

Change password ACCESS_CHANGE_PASSWORD

Change password

Change the current password. A dialog box allows you to enter a new password.

You will not be able to see the letters of the password as you type them (for extra security) so you are asked to enter the password twice, just to make sure the password is recorded correctly.

If you make a mistake entering the password, an error message will appear and you will be able to try again.

To turn the password off, set a new password of no characters (leave each line empty).

Related Topics

Set accessACCESS_SETACCESS

Speedbar buttons

The scan menu includes commands that allow you to scan for viruses in the computer memory, in drives A:, B: and C:, and the current selected disk areas. You can also access the exit command here.

For more information, click on one of the buttons below.



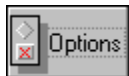
Scan the diskette in drive A: for viruses.



Scan the diskette in drive B: for viruses.



Scan the currently selected areas for viruses.



Change program options.



Change log file settings.



Change access control settings.



Close Virus Buster Lite for Windows.

You can use the menu for these commands.

Scan A: button

Use this speedbar button to scan a diskette in drive A: for viruses.

This button will not appear if an A: drive is not detected on your machine. The button will contain a picture of a 3 1/2 inch or 5 1/4 inch diskette as appropriate.

When the scan is complete you can press the OK button to immediately scan another diskette in the same drive.

If a virus was found or was suspected on the diskette, you will be reminded of this at the end of the scan.

Related Topics

[Scan disk A:](#)

Scan B: button

Use this speedbar button to scan a diskette in drive B: for viruses.

This button will not appear if an B: drive is not detected on your machine. The button will contain a picture of a 3 1/2 inch or 5 1/4 inch diskette as appropriate.

When the scan is complete you can press the OK button to immediately scan another diskette in the same drive.

If a virus was found or was suspected on the diskette, you will be reminded of this at the end of the scan.

Related Topics

[Scan disk B:](#)

Scan button

Use this button to scan the current selected areas for viruses.

The current selected areas are shown in the main window.

Related Topics

[Scan selections](#)

Options button

This allows you to see and change the most commonly changed program settings in one convenient dialog box.

You can change the following settings:

Automatic action when a virus is found

Generic detection sensitivity

Alarm sounds, on or off

Extended scan, on or off

Scan sub-directories, on or off

Number of files to scan before terminating the scan

Automatic diskette scan, on or off

When the options are set to suit your needs, press the OK button. Options will not be saved to disk until you exit (if enabled) or you choose the Save now command.

You can also use the menus to make changes to most of these settings.

Log button

This allows you to see and change the log file settings in one convenient dialog box.

You can change the following settings:

Logging, on or off.

Extended log recording, on or off.

The log file name.

When the log options are set to suit your needs, press the OK button.

You can also use the menus to make changes to these settings.

Access button

This allows you to see and change the access control settings. Set the program operations for which password access will be required.

You can password protect:

Running of Virus Buster Lite password required to start the application.

Change options password required to modify any option settings.

Delete files password required to delete infected files.

The password is common for all restrictions.

You can also use the menus to make changes to these settings.

Related Topics

[Change password](#) ACCESS_CHANGE_PASSWORD

Exit button

This allows you to quickly exit from Virus Buster Lite.

Related Topics

Exit

Log menu

File menu

Save

Exit

Edit menu

Undo

Cut

Copy

Paste

Delete

Clear

Search menu

Find

Replace

File Menu

The File menu allows you to save the file after making edits, and to exit from the log editor.

For more information, select the File menu command name.

Save

Exit

File Save

This saves the current contents of the log file to disk.

Use this after making edits to the log file. It is not necessary to save the log unless you make edits, the file is already saved to disk.

File Exit

This exits from the log file editor, back to the window showing the results of the scan.

Edit Menu

The Edit menu includes commands that enable you to move text to and from the clipboard, to delete text, and to undo a previous editing operation.

For more information, select the Edit menu command name.

<u>Undo</u>	Cancels a previous operation.
<u>Cut</u>	Deletes text and moves it to the clipboard.
<u>Copy</u>	Copies text to the clipboard.
<u>Paste</u>	Moves text from the clipboard to the edit window
<u>Delete</u>	Deletes highlighted text without moving it to the clipboard.
<u>Clear all</u>	Deletes all text without moving it to the clipboard.

Edit Undo

Undo reverses the last editing action if possible.

Use this if you make a mistake while editing the log.

Edit Cut

Removes the selected text from the document and puts it on the Clipboard. This command is unavailable if nothing is selected.

Edit Copy

Copies the selected text onto the clipboard. This command is unavailable if nothing is selected.

Edit Paste

Inserts a copy of the Clipboard contents at the insertion point. This command is unavailable if the Clipboard is empty.

Delete

This deletes the currently selected text. The text is not copied to the clipboard and the command cannot be undone.

Edit clear all

This deletes the entire contents of the log file.

The contents are not copied to the clipboard and the command cannot be undone. If you clear the log by mistake, exit from the log editor and then restart it.

Search Menu

The Search menu includes commands that enable you to find a particular text string, and to replace a text string with a new string.

For more information, select the Search menu command name.

Find

Find any particular text string in the log file.

Replace

Replace text with a new text string.

Next

Repeat the last Find command.

Search Find

Searches for specified text in the log file.

Enter the required text in the dialog box.

Click the Case sensitive box if you want to search for an exact match to the case of the text you entered.

Press OK to begin the search.

Search Replace

Replaces specified text with new text in the log file.

Enter the text to be changed in the top line of the dialog box.

Enter the new text in the bottom line of the dialog box.

Click the Case sensitive box if you want to search for and replace with an exact match to the case of the text you entered.

Click the All occurrences box if you want to change all instances of the text in the log file.

Click the Prompt on replace if you want to be able to check each replacement before it occurs.

Press OK to begin the replacement.

Search Next

Repeats the last search command.

If no previous search has been performed the command will fail.

Edit log speedbar

The edit log speedbar simplifies the most common commands.



This saves the log file to disk.



This will delete the currently highlighted text (if any) and place it on the clipboard. You can paste it from the clipboard back into the log, or into another application.



This will copy the currently highlighted text (if any) to the clipboard. You can paste it from the clipboard back into the log, or into another application.



This will paste the current contents of the clipboard (if any) into the log file.



Use this to search for text in the log file. See [Search find](#) for more information.



Use this to repeat the last Find command.



Close the log file.



Show the help file.

Glossary

Boot sector virus

Executable file

File infector

Known virus

Trojan file

Unknown virus

Virus

Definition

Effects of

Forms of

Hiding places

Origin of

Purpose of

Boot sector virus

A virus that replaces the boot record of a floppy disk, and/or the master boot record of a hard disk.

When a PC is booted from an infected disk, the virus takes control of the machine before the operating system loads. Boot sector viruses usually spread to every disk inserted into the machine.

Commonly the virus saves a copy of the original boot record, but this is not always the case.

Executable file

A virus needs to infect executable code in order to spread.

A computer contains executable code in three locations:

the ROM this cannot be modified.

the boot record Boot sector viruses infect this code

executable files these are program files.

Executable files are usually distinguished from other files by the file extension. Virus Buster Lite scans the files *.EXE, *.COM, *.DLL, *.386, *.SYS, *.OV?, *.BIN and *.DRV. Virus Buster Professional allows you to specify which files to scan.

Related Topics

Boot sector virus

File infector

File infector

A file infector modifies executable files by adding virus code.

When an infected file is run, it may infect other files immediately, or it may remain resident in memory after the host program terminates and then infect other files.

Related Topics

Boot sector virus `BOOT_SECTOR_VIRUS`

Known virus

Virus Buster Lite uses a database of virus signatures. A virus which appears in the database is a known virus.

This database contains the signatures of thousands of viruses. Regular updates of the database file are available.

Virus Buster Lite can also detect unknown viruses using code analysis.

Related Topics

Virus

Unknown virus

Trojan file

A trojan file is a program which performs some (usually destructive) action while the user believes it to be doing something else.

A severe trojan may format the hard drive while it displays a captivating graphic.

A trojan is not a virus. Trojans do not spread by themselves. Virus Buster Lite contains the signature of many trojans, but the best way to avoid being damaged by a trojan is to use only licenced software.

Related Topics

[Virus](#)

Unknown virus

Virus Buster Lite uses a database of virus signatures. A virus which appears in the database is a known virus. Any other virus is an unknown virus.

This database contains the signatures of thousands of viruses. Regular updates of the database file are available. Viruses which are unknown today become known tomorrow.

Virus Buster Lite can also detect unknown viruses using code analysis.

Related Topics

Virus

Known virus

Virus purpose

Viruses are created to infiltrate computer systems and perform some act of electronic vandalism.

They take many forms and will strike either immediately, repeatedly or at a specific time after entering a computer system.

Virus definition

A virus is a program capable of making copies of itself and using this ability to spread through and between computer systems.

Viruses can spread themselves from computer to computer wherever computer programs are transferred from one system to another. They attach themselves to genuine programs or disguise their presence on hard or floppy diskettes and copy themselves to any other programs or disks they encounter.

Virus forms

Viruses come in many forms, using different methods to spread themselves from disk to disk, and have a wide variety of effects.

Modified "hybrid" viruses regularly appear from original versions and completely new types have been discovered over time, including stealth, mutating and encrypting viruses.

Some forms of virus have been predicted by researchers, others have appeared as a complete surprise.

Virus hiding places

A virus can conceal its presence by attaching itself to a legitimate program file, occupying a "bad" sector on a disk, copying itself to an "illegal" part of a disk not read by the operating system or some other special means.

Once concealed within a file or on a disk, the virus monitors the system and waits for certain conditions to be fulfilled before becoming active and delivering its payload.

Virus effects

Virus effects can be virtually anything at all depending on the motive of the program's author.

They can vary from simply displaying a humorous message, subtly altering data files, consuming computer disk and time resources or formatting a disk with the loss of all data.

To be safe you should treat all viruses as potentially very dangerous.

Virus origin

All viruses are man-made. Every one of the multitude of viruses now known to exist has been designed and programmed by hand.

Viruses and computer security are a human problem as much as a technological one.

[Virus Buster Lite Keys](#)

Choose from the following list to review the keys used in Virus Buster Lite and Windows:

[Cursor movement keys](#)

[Dialog box keys](#)

[Editing keys](#)

[Help keys](#)

[Menu keys](#)

[System keys](#)

[Selecting text](#)

[Using Windows](#)

Related Topics

[Commands](#)

Cursor Movement Keys

Key(s)

Function

DIRECTION key Moves the cursor left, right, up, or down in a field.

End or Ctrl+Right Arrow Moves to the end of a field.

Home or CTRL+Left Arrow Moves to the beginning of a field.

PAGE UP or PAGE DOWN Moves up or down in a field, one screen at a time.

Dialog Box Keys

Key(s)	Function
TAB	Moves from field to field (left to right and top to bottom).
SHIFT+TAB	Moves from field to field in reverse order.
ALT+letter	Moves to the option or group whose underlined letter matches the one you type.
DIRECTION key	Moves from option to option within a group of options.
ENTER	Executes a command button. Or, chooses the selected item in a list box and executes the command.
ESC	Closes a dialog box without completing the command. (Same as Cancel)
ALT+DOWN ARROW	Opens a drop-down list box.
ALT+UP or DOWN ARROW	Selects item in a drop-down list box.
SPACEBAR	Cancel a selection in a list box. Selects or clears a check box.
CTRL+SLASH	Selects all the items in a list box.
CTRL+BACKSLASH	Cancel all selections except the current selection.
SHIFT+ DIRECTION key	Extends selection in a text box.
SHIFT+ HOME	Extends selection to first character in a text box.
SHIFT+ END	Extends selection to last character in a text box

Editing Keys

Key(s)

Function

Backspace

Deletes the character to the left of the cursor.
Or, deletes selected text.

Delete

Deletes the character to the right of the cursor.
Or, deletes selected text.

Help Keys

Key(s)


Function

F1

Gets Help and displays the Help Index. If the Help window is already open, pressing F1 displays the "Using Windows Help" topics.

Displays a Help topic on the selected command, dialog box option, or system message.

SHIFT+F1

Changes the pointer to  so you can get Help on a specific command, screen region, or key. You can then choose a command, click the screen region, or press a key or key combination you want to know more about.

Menu Keys

Key(s)

Function

Alt	Selects the first menu on the menu bar.
Letter key	Chooses the menu, or menu item, whose underlined letter matches the one you type.
Alt+letter key	Pulls down the menu whose underlined letter matches the one you type.
LEFT or RIGHT ARROW	Moves among menus.
UP or DOWN ARROW	Moves among menu items.
Enter	Chooses the selected menu item.

System Keys

Key(s)	Function
Ctrl+Esc	Switches to the Task List.
Alt+Esc	Switches to the next application window or minimized icon, including full-screen programs.
Alt+TAB	Switches to the next application window, restoring applications that are running as icons.
Alt+PrtSc	Copies the entire screen to Clipboard.
Ctrl+F4	Closes the active window.
F1	Gets Help and displays the Help Index for the application. (See <u>Help keys</u>)

Text Selection Keys

Key(s)

Function

SHIFT+LEFT or RIGHT ARROW	Selects text one character at a time to the left or right.
SHIFT+DOWN or UP	Selects one line of text up or down.
SHIFT+END	Selects text to the end of the line.
SHIFT+HOME	Selects text to the beginning of the line.
SHIFT+PAGE DOWN	Selects text down one window. Or, cancels the selection if the next window is already selected.
SHIFT+PAGE UP	Selects text up one window. Or, cancels the selection if the previous window is already selected.
CTRL+SHIFT+LEFT or RIGHT ARROW	Selects text to the next or previous word.
CTRL+SHIFT+UP or DOWN ARROW	Selects text to the beginning (UP ARROW) or end (DOWN ARROW) of the paragraph.
CTRL+SHIFT+END	Selects text to the end of the document.
CTRL+SHIFT+HOME	Selects text to the beginning of the document.

Window Keys

Key(s)

Function

ALT+SPACEBAR

Opens the Control menu.

Alt+F4

Closes a window.

Alt+Esc

Switches to the next application window or minimized icon, including full-screen programs.

Alt+TAB

Switches to the next application window, restoring applications that are running as icons.

Alt+ENTER

Switches a non-Windows application between running in a window and running full screen.

DIRECTION key

Moves a window when you have chosen Move from the Control menu.
Or, changes the size of a window when you have chosen Size from the Control menu.

Clipboard

This is a topic that describes the Windows term "clipboard". If you click the "clipboard" term within the Copying Text or Glossary topic, this Help topic will be displayed in a pop-up window.

This topic is also tagged with the keyword "clipboard," for use with the WinHelp Search option.

VirusGate

VirusGate is an NLM available from Leprechaun Software. VirusGate checks each user as they log onto the network. Infected users are locked out.

Log file

The log file keeps a record of the results of the latest virus scan.

INI file

Windows uses initialisation files to record program settings. These files commonly have the file extension of .INI.

Speed bar

The speed bar is the row of buttons at the top of the main window. You can click on the buttons for quick access to many commands.

Stealth

A stealth virus conceals itself by modifying the operating system. A simple stealth technique is for the virus to supply a TSR which modifies the operation of DOS and results in a DIR (directory listing) reporting the size of infected files as the pre-infected size.

Encrypting

An encrypting virus encrypts (scrambles with a secret code) part of itself when it infects a file. Usually a random key is used resulting in each infection 'looking' very different. Encrypted viruses are more difficult to detect.

Mutating

A mutating virus modifies part of its code when it infects a new file. Usually the changed part of the code performs no useful function. The fact that each file infection can 'look' substantially different helps the virus to avoid discovery. Virus Buster Lite 'sees through' all mutating viruses.

Boot record

The boot record is the first logical sector on a DOS disk. The boot record contains vital disk information such as the number of tracks. The boot record also contains a short program which initiates the boot-up sequence.

Suspect file

Virus Buster Lite analyses program code, looking for indicators that the program is a virus. This analysis is based on what the program does, rather than looking for known virus signatures. A file which 'looks like' it might be a virus is called a 'suspect' file.

