ThunderBYTE Anti-Virus for Windows

Contents

Press F1 if you wish to learn how to use this Help information.

Congratulations! By purchasing the ThunderBYTE Anti-Virus utilities you have taken the basic step in building a massive anti-viral safety wall around your precious computer system. Setting up the appropriate defense, using the TBAV utilities, is a personal matter. Therefore, we highly recommend to read the manual thoroughly, so you are well aware of all different kinds of security measures you may take.

This help file contains the following chapters:

Introduction to TBAV for Windows 95

The basic parts of TBAV for Windows 95 is described in this section together with the product strategy followed by TBAV for Windows 95. Furthermore, the license agreement is described and all addresses of the ThunderBYTE international agents are listed here.

If you wish to contact ThunderBYTE Sales or Technical Support, you will find ThunderBYTEs address information here.

Installing TBAV for Windows 95

This part of the TBAV for Windows 95 Setup help file treats the installation and setup of TBAV for Windows 95 extensively. You are strongly advised to become familiar with the contents of this topic.

Using TBAV for Windows 95

The user interface of TBAV for Windows 95 is explained extensively in this chapter. Reading this chapter is indispensable in order to get the most out of TBAV for Windows 95.

Using the Scan Module

The operation of TbScan, the Scan Module of TBAV for Windows 95 is described in this chapter. All options and settings are explained, together with some information about detection of viruses.

Using the Setup Module

TbSetup is an indispensable tool when you want to maximize the functionality of TBAV for Windows 95. The Setup module calculates fingerprint information of all executable files located on your computer. This chapter of the TBAV for Windows 95 help file introduces you to the Setup Module.

Using the Background Scan Module

You can configure TBAV for Windows 95 as a background task, in which case, it periodically scans specified disks, directories, or files for viruses. All information about this feature, called the Background Scan Module, can be obtained by reading this section of the manual.

Using the File I/O Monitor

The File I/O monitor module performs a virus check on every file you copy, extract, download, etc. Consult this topic if you want to know more about the File I/O monitor.

Addressing Special Topics

Some special topics that are not related to any of the above are discussed in this section. They include: the virus information database, general configuration, the network interface and the automatic update feature.

Double-click this icon to start TBAV for Windows 95.

Double-click this icon to read the last-minute notes concerning TBAV for Windows 95.

This is the TBAV for Windows 95 menu bar. Use the submenus to configure TBAV for Windows 95.

This is the TBAV for Windows 95 drive bar. You can use it while editing or creating so-called targets.

This status message only shows up when TBAV for Windows 95 cooperates with TBAV for Networks.

This button should be pressed to initiate a scan operation.

This button should be pressed to initiate the calculation of fingerprint information of executable files.

Use this button to configure the File I/O Monitor, Application Execution Tracker and Background Scan Modules.

The virus information database can be accessed by pressing this button.

You can obtain online help by pressing this button.

This is the listbox that contains predefined target items, or (when editing a target) a representation of your directories and files.

This so-called "target window" lists the items in the currently selected or edited target.

Press one of these target buttons to alter the targets listed in the left-most target window.

The bottom window gives you information about your registration of TBAV for Windows 95.

This small window initially contains some vendor information. If one or more viruses are found, this window will contain a list of all virus infections.

In this area the directory being searched for files is displayed.

This is a scrolling list of scanned files. The way of scrolling can be adjusted via the TbScan|Options menu.

This part of TbScan's window specifies the scan algorithm used for each file.

This is where TbScan displays the heuristic flags of the scanned files. Heuristic flags denote special characteristics of executable files.

The status of scanned files, either clean (marked by Ok) or infected (marked by an X) is displayed in this area.

The right-most part of TbScan's window displays general information about the scan process.

This part of the "Virus Found!" dialog represents the item being infected (eg., a pathname of a file), together with the type of infection and the name of the virus.

A list of heuristic flags of the infected item is found in this area. Heuristic flags tell a lot about the behaviour of a virus.

Select this button if you want to delete an infected item.

Select this button to kill an infected item. "Killing" means erasing an item using a secure algorithm.

To rename an infected file, select this button. The first letter of a file's extension will become the letter 'V'. Hence, "COMMAND.COM" becomes "COMMAND.VOM".

The 'Validate' option can be used to tell TbScan that this file is not infected. Use this option with care!

Select the "Quit" button to exit TbScan when a virus is found.

Selecting this button makes TbScan continue until all targets are scanned. The "Virus Found" dialog will no longer be displayed.

To continue the scan process, select this button.

Perform the action selected in the left-most window.

Obtain information about the detected virus via this pushbutton.

For online help about the "Virus Found" dialog, push this "Help" button.

Using TBAV for Windows 95

This section, and the ones that follow, describe in detail how to use TBAV for Windows 95.
This section describes how to use Targets, an extremely important feature of TBAV for Windows 95.

Understanding Targets

First, lets define Target. A target is a list of drive names, directory names or file names that either the Setup Module, Scan Module or Background Scanning Module can process. TBAV for Windows 95 initially shows all available targets in the left Target window. The example screen earlier in the TBAV for Windows 95 QuickStart chapter lists four targets: CD_ROM, DRIVE_A, FULLSCAN, and LOCAL.

During installation of TBAV for Windows 95, some predefined targets are generated depending on your system configuration. Besides these predefined targets, you can easily define your own targets. For example, you want might to create a Target called `DOWNLOAD` that contains the directory you use for downloading programs. If you downloaded some files, and want to see if they contain viruses, you would only have to select the `DOWNLOAD` target and activate the TBAV for Windows 95 Scan module.

Understanding Predefined Targets

As it examines your system, the TBAV for Windows 95 installation utility generates some predefined targets and displays them the first time you execute TBAV for Windows 95. Depending upon your system configuration, the TBAV for Windows 95 installation utility will create the following targets (if the target items are available):

```
- First floppy disk drive
- All local fixed disk drives
- All Network drives
- All CD-Rom drives
- All drives
```

The right Target window always displays the contents of the currently selected target in the left window. Thus, since in the example in the TBAV for Windows 95 QuickStart chapter the currently selected target is the `FULLSCAN` target, the right window lists the paths C:\, D:\, E:\, F:\, G:\ and H:\.. If the target `CD_ROM` had been selected, the right window would have contained H:\, which is a reference to the CD-ROM drive.

Storing Targets

Targets are an essential part of TBAV for Windows 95, but can also use them in TBAV for DOS. For that purpose, you should store the targets in simple ASCII file, using SCN for the file extension. The target file FULLSCAN.SCN, for example, contains the following lines:

```
C:\
D:\
E:\
F:\
G:\
H:\
```

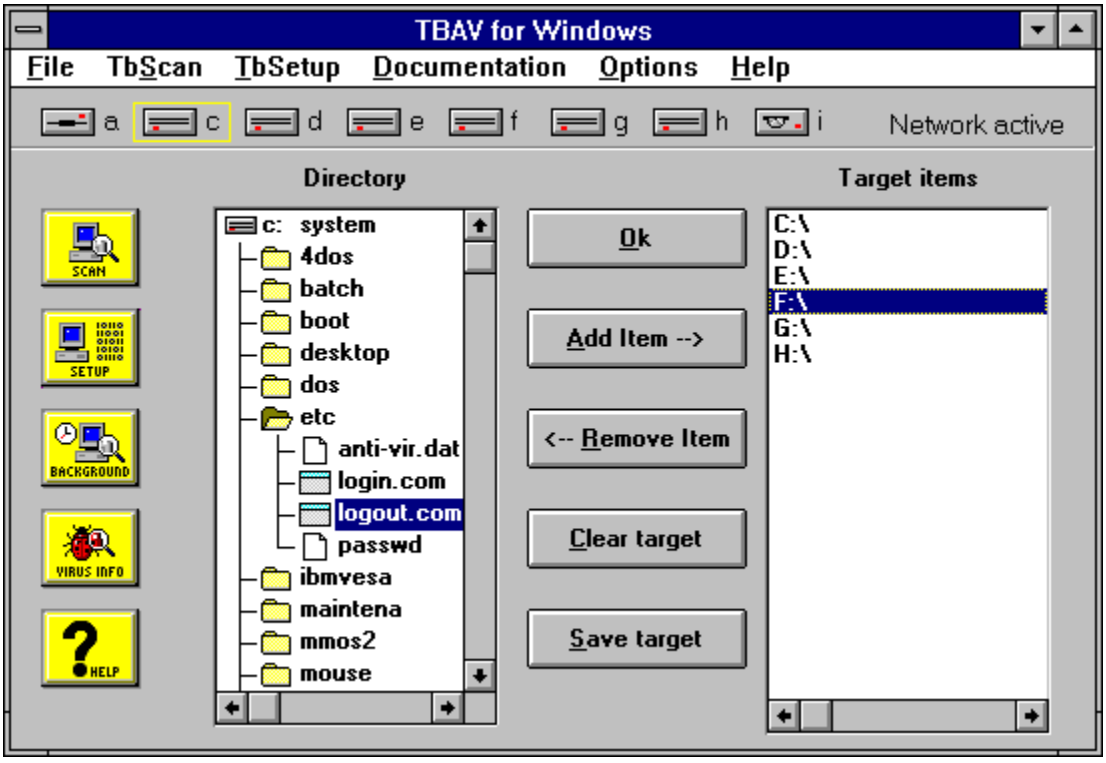
NOTE: You must store Target files in the ThunderBYTE Anti-Virus directory (C:\TBAV, for example).

Editing Targets

You can easily change an existing target by following these steps:

1. Select the Target you want to change, and then select the Edit target button. Notice that the left Target window changes to a Directory window, which graphically represents the directory structure of

the default drive, and the action buttons change, as in the following figure:



In this example, the directory structure of the default drive C: appears in the left window. The first line of the window displays the drive name and its volume label (in this case, C: and system). The window displays all subdirectories and files in that particular drive. TBAV for Windows 95 distinguishes directories, files and executables by placing a different icon next to the name of the item:

- The folder icon [] denotes subdirectories, such as DOS.
- The window icon [] denotes executable files (such as LOGIN.COM).
- The file icon [] denotes ordinary files (in the example, the file called PASSWD).

2. Double-click a folder icon or subdirectory name to open the folder and display the contents of that particular subdirectory. In this example, the ETC directory is open (notice the open folder icon []). Double-clicking an opened folder closes the subdirectory (the icon changes into a normal folder icon, and the contents of that subdirectory disappears).

3. To select a directory or a file to include in the Target, simply select it. By clicking the left mouse button on the item, you can select one or multiple items. Selected items appear in reverse color. In our example, LOGIN.COM is selected.

TIP: If you want to clear the current selection(s) in the directory window, simply double-click the first line of the directory window (the line where the grey drive icon appears). Notice also the vertical and horizontal scroll bars in the Directory window, which enable you to scroll to data that is not currently visible.

4. After selecting directories and/or files in the current Directory window, click on another drive icon in the upper left corner to change to another drive, and then select other directories and files. Targets often consist of several drive names, or directory names located on different drives.
5. After selecting one or more items, select the Add item button to copy the items from the Directory window to the Target Items window. A couple of guidelines are in order here:
   - You cannot add an item that already exists in the Target Items window. If you try, TBAV for Windows 95 simply ignores it.
   - If you set the Include subdirectories option in either the Scan module (TbScan, Options) or the Setup module (TbSetup, Options), both of which are set by default, TBAV for Windows 95

includes all subdirectories of a given pathname in the Scan or Setup process whenever that pathname is set up or scanned. If you set this option, you cannot add a subdirectory of a target item to the Target Item window. For example, if the Target Item is C:\, adding the DOS directory to the Target Items window is redundant because the DOS directory is already included.

- You cannot add an open folder to the Target Items window. You should close the folder (by double-clicking on it) before selecting and adding it to the target.

6. To remove an item from the Target Item window, thereby excluding it from a Target, simply select the item(s), and then select the Remove Item button. To remove *all* the items in the Target Item window, simply select the Clear Target button (you do not have to select the items first).
7. After editing an existing Target or creating a new Target, you will most likely want to save the Target for future use. Select the Save Target to display a dialog box which contains a list of existing target files.
   If you are editing a Target, the default name for the edited target is its original name. If you are creating a new target, be sure to type in a new name. You could also select one of the existing targets, in which case TBAV for Windows 95 displays a dialog box warning you that it will overwrite the existing target file with the new target file. Be sure this is what you want to do.
8. Select the OK button restores the left window to the Predefined Targets mode. Note that the contents of the Target Items window does not change, unless you select another target out of the list of predefined targets. CAUTION: The contents of any unsaved target is lost when you select another target in the Predefined Targets window.

Creating New Targets

Creating a new target is virtually identical to editing an existing target. The only difference is that after selecting the New Target button, the Target Items window is completely empty. Simply define and save the new Target in the same way you edit an existing Target.

Removing Existing Targets

TBAV for Windows 95 not only enables you to create new Targets and edit existing Targets, but it also enables you to remove existing Targets. You might want to do this, for example, when the layout of your fixed disk(s) has changed or a when the directory tree has changed.
To delete a Target, simply select it, and then select the Remove Target button. TBAV for Windows 95 displays a message asking you to confirm the removal of the target. Select the Yes button to delete the Target or No to cancel.

These buttons can be used to add or remove items to a target. You can also clear and save a target file. By pressing "Ok", the list of predefined targets is displayed.

This window show the directory and file tree of the currently selected drive. Select files or directories here to add them to the target being edited or created.

Using the Scan Module

This section describes the most important and probably the most frequently used part of TBAV for Windows 95, namely, the Scan module. The Scan module detects both known and unknown viruses in files and special areas of disks. You can configure the Scan module using several options, all of which you can access via the TbScan menu.

Activating the Scan Module

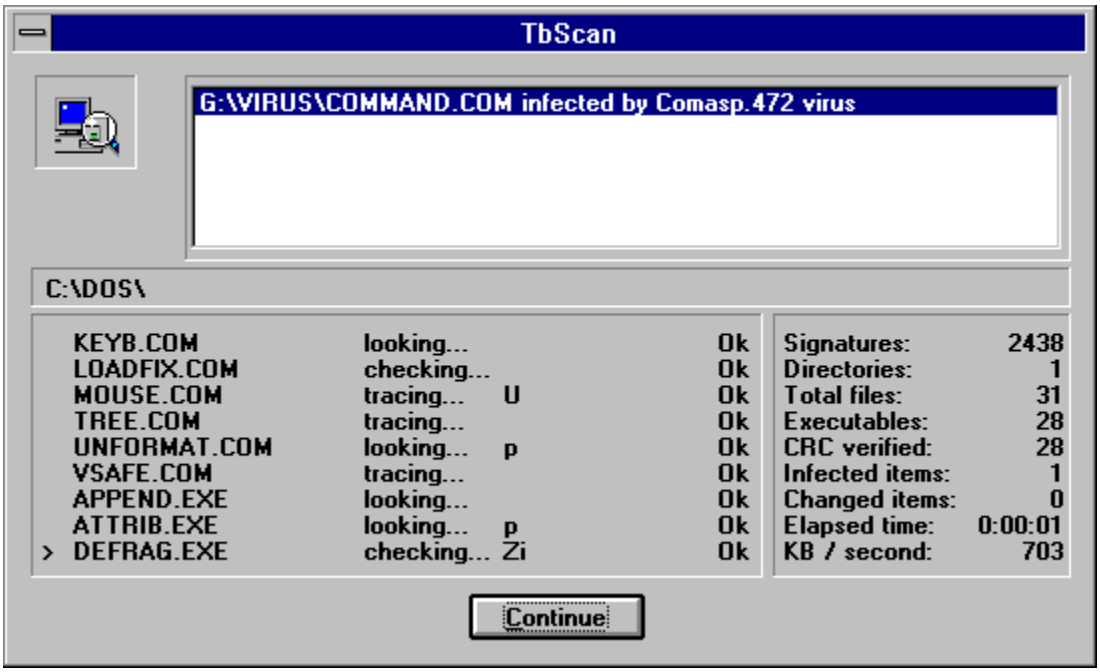
The Scan module uses a Target, as described in a previous section, as its input. You should, therefore, select or create a target before activating the Scan module. NOTE: The Scan module always uses the current contents of the Target Items window as a target. Refer to **Using TBAV for Windows 95** for more information about using TBAV for Windows 95.
You can activate the Scan module in one of two ways:

1. Select a Target in the Predefined Targets window, and then select the scan button.
2. Double-click on a Target in the Predefined Targets window.

The Scan module immediately starts processing the items listed in the Target Items window immediately.

Using the Scan Module

Activating the Scan module displays the following dialog box:



This dialog box, which is very similar to the one in the Setup module, consists of four parts:

1. The message window at the top of the box for displaying information on infected or changed files. In this example, the message window contains a reference to a virus. By default, this window displays some vendor information.
2. The directory window under the message window display the name of the currently processed directory.
3. The file window in the bottom-left corner of the box display the files that have already been scanned for viruses, along with some status information concerning those files. This status information

consists of the scan method used, heuristic flags that describe the file contents (and, if the file is an executable file, its behavior), and an indication whether or not the file is infected by a virus.

4. The statistics window to the right of the file window displays information concerning the scan process.

The Stop or continue button at the bottom of the box for aborting a scan or continuing an operation. If TBAV for Windows 95 is scanning one or more files, the Stop aborts the scan. It is also possible that TBAV for Windows 95 is waiting for user input (for example, when youve set the Prompt for pause option). In this case, selecting the Continue continues the scanning process.

Scanning for Viruses

Depending upon what options you specify, the Scan module processes a number of files each time you activate it. It scans each file separately for both known and unknown viruses. During the scan process, it displays the scan results for each fill in the file window. For example, the file window might contain the following line:

```
NLSFUNC.EXE checking...     FU      Ok
```

The first field in this line specifies the name of the file just scanned (NLSFUNC.EXE).
The second field describes the scan method used on the file. The TBAV for Windows 95 Scan module distinguishes five scan methods: *looking*, *checking*, *tracing*, *scanning* and *skipping*.
The third field, which in this case consists of the capital letters F and U, displays one or more warning characters, or heuristic flags, concerning the scanned file. During virus scanning, the Scan module checks the behavior of the file being scanned. TbScan summarizes the result of this behavior checking using several uppercase characters, each denoting a special behavioral characteristic of the file. Since the behavior checking, of course, detects common virus behavior, the uppercase warning flags *might* indicate a virus. It is quite likely, however, that your system contains a few files that are not infected by a virus at all, but which still trigger one or two heuristic flags. There is little to worry about in such a case.
CAUTION: You can ignore the heuristic flags if only a few files trigger heuristic flags. If your computer system behaves strangely and a large number of files display the same serious heuristic flags, it is quite well possible that these files are infected by a yet unknown virus.
TbScan also uses the warning characters to indicate illegal or incorrect file formats, special files, etc. In these cases, it displays the characters in lowercase, indicating a non-serious file characteristic.

In case TbScan detects a virus, you are referred to **Detecting a Virus**.

Configuring the Scan module

You can configure the Scan module via the TbScan command on the menu. Please select one of the following topics to obtain more information about the TbScan menu items.

TbScan Options

TbScan Advanced Options

What If a Virus Is Found ?

TbScan Log File Options

View Log File

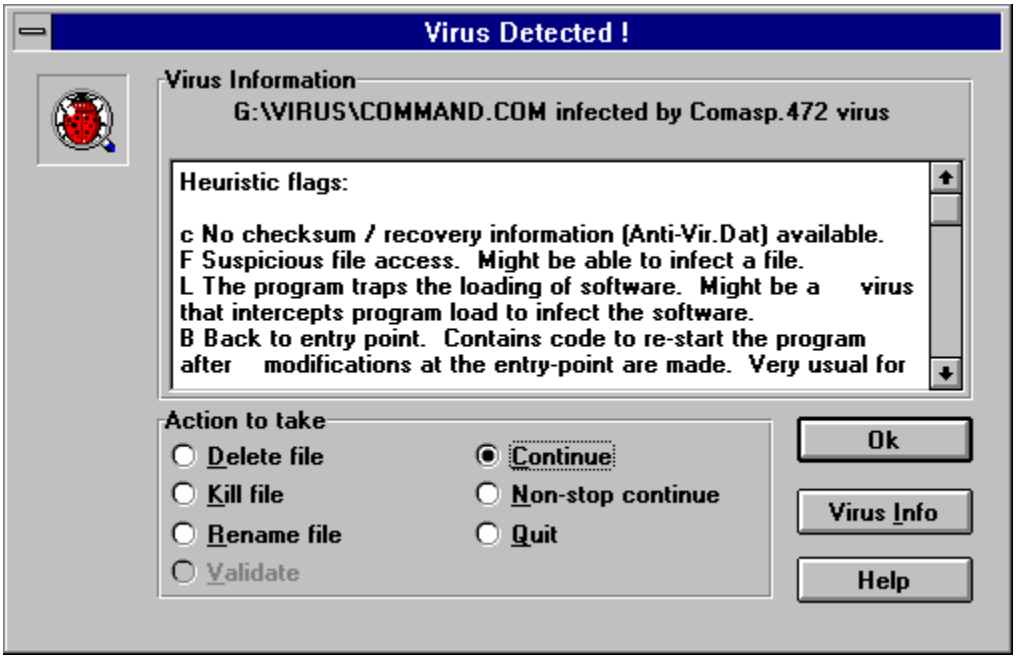
Detecting a Virus

When the Scan module detects the presence of a virus, it displays a message in the message window concerning the infected file. The Scan module distinguishes six types of messages:

1. **[Name of file] is infected by [name of virus] virus.** The file is infected by the virus mentioned.
2. **[Name of file] is Joke named [name of Joke].** Some programs simulate that the system is infected by a virus; such a program is a joke. A joke is completely harmless.
3. **[Name of file] is Trojan named [name of Trojan].** The file is a Trojan Horse, a carrier program for viruses. A Trojan Horse itself is not a virus, but it installs a virus onto your computer system when it runs. Do not execute the program; delete it.
4. **[Name of file] damaged by [name of virus].** Unlike an infected file, which carries the virus itself, a damaged file has only been damaged by the virus.
5. **[Name of file] dropper of [name of virus].** A dropper is a program that has not been infected itself, but which does contain a boot sector virus and is able to install it into your boot sector.
6. **[Name of file] garbage: (not a virus) [name of garbage].** Unlike an infected file, which contains the virus itself,.an overwritten file has been overwritten with garbage.

The TBAV for Windows 95 Scan module might at some point use the prefix Probably or Might before one of the above messages. For example, you might see the message, C:\SOMEFILE.COM probably infected by an unknown virus. Such messages appear in case of yet unknown viruses after the Scan module applies heuristic analysis to the file. If the prefix is Probably, it is most likely the specified file is infected by an unknown virus. If the prefix is Might, the probability that the file is really infected by a virus is a lot smaller, but is still possible.

By default, if TbScan detects a virus, it displays a dialog box similar to the following:



The first line in the dialog contains a reference to the infected file, together with the type of infection and the virus name. The list of heuristic flags and their textual description appears below this line.The dialog box then lists at the bottom of the box the actions you can perform:

- The default action is to continue the virus scan process, without doing anything.
- The second action is the Non-stop continue action. When you select this action, the Scan module

continues scanning and without stopping, even if it finds additional virus infections.

- You can abort the scan process by selecting the Quit option.
- The Delete file option simply deletes the infected file.
- The Rename file option renames the infected file, replacing the first letter of the extension with the letter V. EXE, for example, become VXE.
- The Kill file option is the same as the Delete file option, except you cannot undelete a killed file using a file undeleting utility (such as the DOS UNDELETE command).
- The Validate option enables only when the fingerprint information of the specified file stored in ANTI-VIR.DAT no longer matches the real contents of the file. In this case, the Scan module informs you that the file has changed. Now, if you are absolutely sure that the file cannot be infected by a virus, you might want to select the Validate option. By doing so, the Scan module no longer pops up the dialog if it scans that particular file and finds the fingerprint information does not match. Please note that virus infections are still detected, even if a program has been validated!

Notice the two buttons at the right side of box labeled Virus information and Help. The latter provides on-line help for the dialog box. The other pops up another dialog box the displays some information on the detected virus. This information, for example, consists of the file types the virus infects, the length of the viral code, the action the virus actually performs, and some information about how to remove the virus from your computer system.

Once you select an action, then select the OK button on the right side of the dialog box to carry it out.

TbScan Options

Selecting Scan Options in the TbScan menu displays the TBAV for Windows 95 Scan Options dialog box. This contains several options that you are likely to want to change. These options include the following:

Prompt for pause.
If you set this option, the Scan module waits for user input before redrawing the file window. This enables you to examine the scan results without having to consult a log file. This option is off by default.

Quick scan.
The Scan module usually scans each file for viruses. If you set this option, however, the Scan module checks only the fingerprint information (in the form of ANTI-VIR.DAT files generated by the Setup module) of files, if available. It scans files normally in cases where the fingerprint information no longer matches the real file contents, or if the fingerprint information is not available. This option is off by default.

Non-executable scan.
If you select this option, the Scan module scans for viruses in all files. Normally, it scans only executable files. We recommend that you leave this option off, since a virus must execute to perform what it is programmed to do, and to execute a virus you first need to execute an executable program. So, since the computer cannot run non-executable files, it makes no sense for viruses to even infect those files. Some viruses do write to nonexecutable files, but this is simply a result of incorrect programming. And while they do contain corrupted data, they still will not harm other program or data files.

Repeat scan.
This option is particularly useful for scanning multiple diskettes. If you enable this option, when the Scan module finishes checking a disk, a small dialog window appears asking you whether or not you want to repeat the scan process. If you disable this option, the Scan module simply quits after scanning a disk.

Boot sector scan.
Each disk, either a floppy disk or a hard disk, contains a small area called the boot sector, which is used for booting the computer. Some viruses infect that particular area of disks so that they activate each time you boot from the infected disk. If you enable this option, the Scan module searches for viruses in this area. This option is on by default.

File scan.
If the option FILE SCAN is enabled, the Scan module will search for viruses in files. This option is enabled by default. However, suppose you have been struck by a boot sector virus, and want to search the boot sector of all your floppy disks for that virus. In such cases you might want to disable scanning of files; hence, deselect the FILE SCAN option.

Subdirectory scan.
By default, the Scan module automatically searches and scans files in subdirectories of a given target item. If you scan a certain directory that contains subdirectories, the Scan module not only scans files in the directory, but scans files in the subdirectories as well. If you instruct the Scan module to scan only a single file, it does not scan subdirectories. Clear this option if you do not want the Scan module to automatically scan subdirectories.

Fast scrolling.
By default, the Scan module makes use of a special scrolling algorithm when displaying processed files. We designed the algorithm to consume the least overhead in the course of the virus scan process. The scrolling method is somewhat unusual, however. By clearing this option, TbScan uses conventional scrolling.

TbScan Advanced Options

For novice users we recommend that you do not alter the settings from the Advanced Options in the TbScan menu, but as your knowledge and experience grow, you might want to experiment. The advanced scan options include:

High heuristic sensitivity.
While TbScan always performs a heuristic scan on processing files, it reports a file as being infected only if it is very probable that the file is infected. If you select this option, on the other hand, TbScan is somewhat more sensitive. In this mode, TbScan detects 90% of the new, unknown viruses without any signature. Be aware, however, that some false alarms might occur.

Auto heuristic sensitivity.
By default, TbScan automatically adjusts the heuristic detection level after it finds a virus. In other words, when TbScan finds a virus, it then proceeds as if you had selected High heuristic sensitivity. This option provides you maximum detection capabilities in case you need it, while at the same time keeps false alarms at a minimum.

Low heuristic sensitivity.
In this mode TbScan almost never issues a false alarm. It still, however, detects about 50% of the new, unknown viruses.

Configure executable extensions.
By default, TbScan scans only those files that have a filename extension that indicates that the file is a program file. Viruses that do not infect executable code simply do not exist. Files with the extension EXE, COM, BIN, SYS, and OV? (note the wildcard, the OV? specification includes files such as OVR and OVL) are considered executable. There are, however, some additional files that have an internal layout that makes them suitable for infection by viruses. Although it is not likely that you will ever execute most of these files, you might want to scan them anyway. Some filename extensions that might indicate an executable format include: .DLL (MS-Windows Dynamic Link Library), .SCR (MS-Windows screen saver file), .MOD (MS-Windows file) and .APP. While infection of such files is not likely, you might want to scan them once in while. To force TbScan scan these files by default, select this option and fill out the extensions you want TbScan to scan. For example, you can specify .DLL.SCR.CPL (with no spaces in between). You can use the question mark wildcard.
WARNING: Be careful what extensions you specify. Scanning a non-executable file causes unpredictable results and can result in false alarms.

Extract signatures.
This option is available to registered users only. See the Using TbGensig section in Chapter 4 for more information.

What If a Virus Is Found ?

The If virus found menu item of the TbScan menu enables you to specify the action the Scan module takes when it detects a virus:

Present action menu.
This option (the default) instructs TbScan to display a menu listing three possible actions if it detects a virus: just continue, delete, or rename the infected file.

Just continue (log only).
By default, if TbScan detects an infected file, it prompts you to delete or rename the infected file, or to continue without action. If you select this option, however, TbScan always continues. We highly recommend that you use a log file in such situations, since a scanning operation does not make much sense if you dont read the return messages (see the Log File Menu option below for further information).

Delete infected file.
By default, if TbScan detects a virus in a file it prompts you to delete or rename the infected file, or to continue without action. If you select this option, however, TbScan deletes the infected file automatically, without prompting you first. Use this option if you know your computer is infected by a virus and you want to erase all files the virus has infected. Make sure you have a clean backup and that you really want to get rid of all infected files at once.

Kill infected file.
This option is almost the same as the Delete infected file option with one major difference. The DOS UNDELETE command enables you can recover a deleted file, but if you delete the infected file using this Kill option, recovery is no longer possible.

Rename infected file.
By default, if TbScan detects a file virus it prompts you to delete or rename the infected file, or to continue without action. If you select this option, however, TbScan renames the infected file automatically, without prompting you first. By default, TbScan replaces the first character of the file extension by the character V. It names an .EXE file, to .VXE, for example, and a .COM file to .VOM. This prevents the execution of infected programs and thereby spreading the infection. This also enables you to keep the files for later examination and repair.

TbScan Log File Options

The TBAV for Windows Scan module can create a log file of the scan procedure, containing complete filenames, virus names and heuristic flags. To reduce the size of the log file, you can configure its contents in several ways, using the Log File Options item of the TbScan menu:

Log only infected file.
This logs infected files, that is, files infected by either a known or unknown virus.

Log summary too.
This is the same as the first option, but adds a short summary of the scan process to the log file.

Log suspected too.
Use this option if you also want to keep track of files that trigger the default heuristic level (so-called suspected files).

Log all warnings too.
This option lists in the log file files that trigger one or more heuristic warnings.

Log clean files too.
This option Includes an entry in the log file for each file being processed.

Output to log file.
Setting this option instructs the Scan module to create the log file. You then use the options above to specify the exact contents of the log file.

Append to existing log file.
In some cases, you might want to keep the current contents of the log file, and add new entries at the end of the file. This option enables you to do this.
NOTE: You still must set the Output to log file option to write the scan results to the log file.

No heuristic descriptions.
By default, the Scan module specifies the heuristic flags triggers for each entry in the log file using the warning character itself and a small description. For example, if some file triggers the # flag, the description Found a code decryption routine or debugger trap. This is common for viruses but also for some copy-protected software is added to the log file. Since the size of the log file might become rather large because of these descriptions, you might not want to include these descriptions. By setting this option, TbScan omits these descriptions the log file.

Log file button.
Selecting this button enables you to choose a filename for the log file. You can either choose an existing file or type the name of a non-existing file. In the latter case we recommend you use the extension .LOG for the file name, since this corresponds to the more or less standard naming convention. The Scan module uses the specified name during all subsequent Scan operations until you change the name again. By default, the log file name is TBSCAN.LOG and resides in TBAV for Windows 95 directory.

View Log File

This option enables you to view the log file created by the Scan module. Selecting this option displays the contents of the log file in the Scan module internal viewer (see the picture below for an example). If a log file does not already exist, a warning appears. You can also print the contents of the log file from within the file viewer by selecting the File menu and then selecting Print.

NOTE: You can use your favorite file viewer instead of the internal TBAV for Windows 95 file viewer by using the TBAV for Windows 95 configuration item on the Options menu.

Using the Setup Module

The Setup module of TBAV for Windows 95 collects fingerprint information of all the executable files on your system. The Scan module uses this fingerprint information, which it stores in special ANTI-VIR.DAT files (one in each directory), to check whether a certain executable file has changed (which might indicate a virus infection). The virus cleaning utility (which is part of TBAV for DOS) then uses this information to recover the original contents of an infected file.

CAUTION: We recommend that you use the Setup module only during first-time installation of the ThunderBYTE Anti-Virus utilities or for new applications. Suppose you apply the Setup module after a virus has infected some executable files. The setup module in this case validates the infected programs! We recommend that you first scan the target you want to apply the Setup module to for viruses. In this case you ensure that infected files are not validated by accident.

The Setup module of TBAV for Windows 95 uses a separate data file to recognize special program files. Such files demand special attention. For example, when the Scan module processes them, it lists them in TBSETUP.DAT data file. The data file is part of the standard TBAV package.
NOTE: The TBSETUP.DAT file itself also contains a lot of information concerning its purpose and the list of special program files. Since the data file is a normal readable file, you can load it into your favorite ASCII text editor and view it. TBAV for Windows 95 even offers you the possibility to view the data file (please refer to the section on configuring the Setup module).

The following ThunderBYTE Anti-Virus utilities use the information gathered by the Setup module:

TBAV for DOS

- TbScan. In this case, the information is used for integrity checking.
- TbClean. TbClean uses the information to reconstruct the original contents of an infected file.
- TbScanX, TbCheck, TbFile, TbMem. All these programs use the fingerprint information to maintain permission information.

TBAV for Windows 95

- Scan module. In this case, the information is used for integrity checking.
- Background Scan module and Application Execution Tracker module. These modules use the fingerprint information to maintain permission information.

Activating the Setup Module

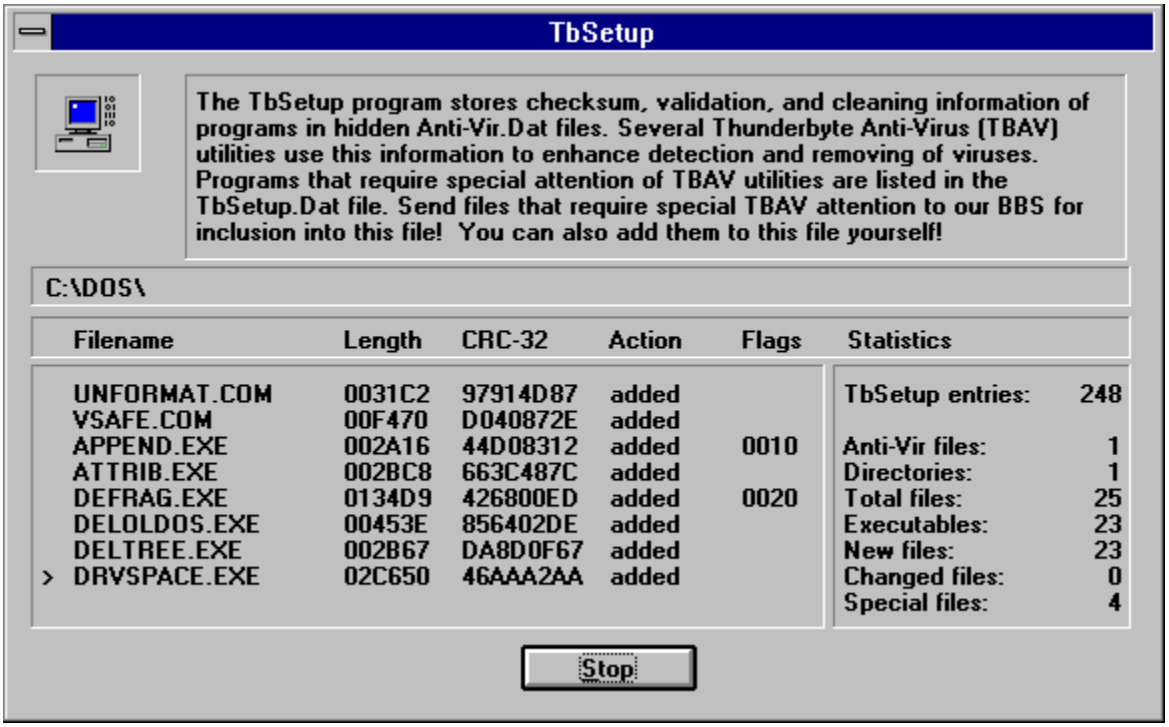
The Setup module uses a Target (described earlier in this chapter) as its input. You should, therefore, select a Target before activating the Setup module. The Setup module always uses the current contents of the Target Items window as a Target.

You activate the Setup module by selecting the second easy-access button at the left-hand side of the main TBAV for Windows 95 window:

The Setup module immediately begins processing the items listed in the Target Items window

Using the Setup Module

When you start the Setup module, it displays the following dialog box:



This dialog box, which is very similar to the Scan modules box, consists of five parts:

1. The Message Window. Located at the top of the window, this contains some information regarding the Setup module. The contents of this message window does not change throughout the setup process.
2. The Directory Window. Located beneath the message window, this displays the name of the currently processing directory.
3. The File Window. Appearing in the bottom-left corner of the dialog box, this displays the files for which the fingerprint information has been or is being calculated, together with some status information concerning those files. This status information consists of the length of the files, a checksum number, the action applied on the file, and some flags that indicate special files.
4. The Statistics Window. Located right next to the file window, this displays information concerning the setup process.
5. The Stop or Continue button. If the Setup module is processing one or more files, the button has a Stop label, which enables you to abort the setup operation. If TbSetup is waiting for user input (for example, as a result of setting the Prompt for pause option), the button has a Continue label while the setup process suspends. Selecting the Continue button continues the process.

Depending on the selected options, the Setup module processes a number of files each time you activate it. During the process, it displays the results for each file in the file window. For example, the file window might contain the following line:

```
NLSFUNC.EXE 003D86      9BAE1A00    added *      0010
```

NOTE: Do not be concerned if the information flies too fast for you to read, or if it puzzles you. You will probably never need these details anyway.
The first field in this line specifies the name of the file just processed, in this case NLSFUNC.EXE. The second field contains the length of the file, printed in hexadecimal numbers. The third field is a special 32-bit checksum. TbSetup obtains this checksum through an algorithm that computes this checksum by

taking the contents of the file into account. The fourth field specifies one of tree actions that TbSetup performs:

- **Added.** Indicates that ANTI-VIR.DAT does not yet list the processed file. TbSetup adds a new entry for this file in the ANTI-VIR.DAT file.
- **Changed.** Indicate that the ANTI-VIR.DAT file contains an entry for the file but the fingerprint information no longer matches the real file contents, so TbSetup updates the record.
  CAUTION: Keep in mind that a change in fingerprint information might indicate a virus infection.
- **Updated.** Indicates that the ANTI-VIR.DAT file contains an entry for the file. The Setup module has, however, changed the permission flags of that entry. The earlier obtained fingerprint information still matches the file contents.

The fifth field, specifies the permission flags of the file. TbSetup obatains these flags either from the TBSETUP.DAT file (the file that lists special program file), or from the manually settings set or reset by the user.
NOTE: For novice users, the exact meaning of the permission flag number is not very important. We refer users who do wish to know the meaning of the flags to the TBSETUP.DAT file, which contains a brief description of each flag.

Configuring the Setup module

You can configure the Setup module by means of the TBAV for Windows 95 menu bar. Clicking the Setup entry displays a menu with the following items. To obtain more information about configuring the Setup module, select one of the listed items.

TbSetup Options

TbSetup Flags

Data File Pathname

View Data File

TbSetup Options

The Setup module of TBAV for Windows 95 has several options that you are likely to want to change. These options can be accessed via the Options item of the TbSetup menu.

Prompt for pause.
When you specify the this option, TbSetup stops after it processes the contents of one window. This enables you to examine the results.

Only new files.
Use this option if you want to add new files to the ANTI-VIR.DAT database but prevent the information of changed files from being updated. Updating the information of changed files is dangerous because if the files are infected, the information to detect and cure the virus is overwritten. This option prevents the information from being overwritten but still allows adding information of new files to the database.

Remove ANTI-VIR.DAT files.
If you want to stop using the ThunderBYTE utilities you do not have to remove all the ANTI-VIR.DAT files yourself. By using this option TbSetup neatly removes all ANTI-VIR.DAT files from your system.

Test mode (Dont change anything).
Use this option if you want to see the effects of an option without the risk of activating something you dont want to activate. This option instructs the program to behave as it normally would but not change or update anything on your hard disk.

Hide ANTI-VIR.DAT files.
The ANTI-VIR.DAT files are normally not visual in a directory listing. If you prefer them to be normal, visible files, disable this option. NOTE: Be aware that this option applies only for new ANTI-VIR.DAT files.

Make executables readonly.
Since TbFile permanently guards the read-only attribute, we highly recommend that you make all executable files readonly to prevent any modifications on these files. TbSetup automatically does this job for you if you enable this option. TbSetup recognizes files that you should not make readonly.

Clear readonly attributes.
Use this option to reverse the Make executables readonly operation. If you enable this option, TBAV clears all readonly attributes on all executable files.

Include SubDirectory scan.
By default, TbSetup searches subdirectories for executable files, unless you specify a filename (wildcards allowed). If you disable this option, TbSetup does not process sub-directories.

TbSetup Flags

The Setup module includes some options that only advanced users should use. These options allow you to change the permission flags of files manually. After clicking the Flags item in the Setup menu, a dialog box pops up and you can choose to set flags manually, reset flag manually or use normal flags.

You can specify the flags you wish to set or reset by selecting one or more items from the window at the lower half of the dialog box.

Use normal flags.
This is the default setting, which you should probably use until you acquire more experience.

Set flags manually.
This option is for advanced users only. Using this option, you can manually set permission flags in the ANTI-VIR.DAT record. This option requires a hexadecimal bit mask for the flags to set; for information about the bit mask, consult the TBSETUP.DAT file. The Define flags to be changed box lists the flags you can change.

Reset flags manually.
This option is for advanced users only. Using this option, you can manually reset permission flags or prevent flags from being set in the ANTI-VIR.DAT record. This option requires a hexadecimal bit mask for the flags to reset; for information about bit mask, consult the TBSETUP.DAT file. The Define flags to be changed box lists the flags you can change.

Data File Pathname

The Data File Pathname option of the TbSetup menu enables you to specify the filename of the TBSETUP.DAT file and its location. By default, the file is TBSETUP.DAT and appears in the TBAV for Windows 95 directory.

NOTE: The filename you specify must really exist.

You can view the data file with the **View Data File** item in the TbSetup menu.

View Data File

Selecting the View Data File item from the TbSetup menu displays a new window, which contains the contents of the TbSetup data file. You can print the contents of the TBSETUP.DAT by selecting File, Print.

NOTE: You can use your favorite file viewer instead of the internal TBAV for Windows 95 file viewer, by using the Options, TBAV for Windows 95 configuration command.

This is where TbSetup shows the special flags of a file to indicate certain characteristics of that file.

The TbSetup statistics are collected in this window.

The CRC (the result of a special mathematical algorithm) of files processed by TbSetup, is written here.

The action performed by TbSetup (e.g., "added" or "changed") is displayed in this area.

The length of the file being processed in displayed here, in hexadecimal notation.

This area of the TbSetup window holds the name of the current directory.

This part of the TbSetup window always contains some information about TbSetup.

The names of the files being processed by TbSetup are displayed here.

Using the File I/O Monitor

The File I/O monitor module performs a virus check on every file you copy, extract, download, etc. Some of the most common actions of computer users are creating and copying files, extracting compressed files, modifying files, or downloading files. Furthermore, most users regularly put some diskette in the disk drive(s) of the computer they are using. Since computer viruses are likely to become active whenever a file is changed, created, modified, etc., you really should scan each file you process.

The File I/O Monitor Module automatically scans newly created or modified files written to your hard disk. It also automatically checks diskettes inserted in a disk drive.

Activating the File I/O Monitor Module

By default, the File I/O Monitor Module is active in all TBAV for Windows 95 modes. You can disable the module by using the configuration dialog box of the Background Scan module. You can access this dialog by using either the Options, Background Scan configuration command, or by selecting the third easy-access button at the left-hand side of the TBAV for Windows 95 main window.

Please refer to the Configuring the File I/O Monitor Module later in this chapter for configuring, enabling, and disabling the File I/O Monitor Module.

Using the File I/O Monitor Module

If you use TBAV for Windows 95 in normal mode (that is, not minimized or iconized), the File I/O Monitor module uses the title bar to indicate its actions. Each time the File I/O Monitor scans a file or diskette for viruses, the tile bar reads Scanning...

The status window, which appears after you minimize TBAV for Windows 95, also displays the activity of the File I/O Monitor. The first line displays the status of the File I/O Monitor. The second line of the status window displays the file being processed by the File I/O Monitor.
NOTE: See the **Using the Background Scan Module** section earlier in this chapter more information about the status window.

Configuring the File I/O Monitor Module

You can disable the File I/O monitoring by using the configuration dialog box of the Background Scan module. You can access this dialog by using either the Options, Background Scan configuration command, or by selecting the third easy-access button. Checking the box enables file I/O monitoring, and clearing the box disables it.
CAUTION: If the Enable File I/O Monitor option is grayed-out so that you cannot access it, this means that the driver that ships with TBAV for Windows 95 (this driver notifies TBAV for Windows 95 of changes in the internal DOS/Windows file system) is not correctly installed. You should reinstall TBAV for Windows 95 (choose First time installation !) in this case.

Using the Background Scan Module

The Background Scan module is an extremely valuable of TBAV for Windows 95. It enables you to scan disks, directories, or files periodically.

The benefit of an operating system such as Windows or OS/2 is its ability to run applications in the background. In other words, such operating systems are able to run several tasks simultaneously; the task that requires user input is the foreground task, while tasks that are able to run without user interaction are background tasks. You can configure TBAV for Windows 95 as a background task, in which case, it periodically scans specified disks, directories, or files for viruses. How often it does is totally up to you.

There are really two advantages to this background scanning:

1. Background scanning checks for viruses while you are doing your normal work. In other words, scanning your computer for viruses does not cost you any time!
2. You can never forget to perform a virus scan, since TBAV for Windows 95 automatically scans your system.

When active, the Background Scanning module of TBAV for Windows 95 uses only idle time for virus scanning. For example, when you are typing some letter in a word processor, there will be little idle time between two key presses. The Background Scan module exploits this idle time. Thanks to this mechanism, you can be absolutely sure that activating the Background Scan module will either not cause system performance to decline at all or very little.

Activating the Background Scan Module

Before activating the Background Scan module, you should make sure you enable and correctly configure it. You can access the configuration dialog box by using either the Options, Background Scan Configuration command, or by selecting the third easy-access button at the left-hand side of the main window of TBAV for Windows 95.

See the Configuring the Background Scan Module section later in this section for configuring, enabling, and disabling the Background Scan Module.

You activate the Background Scan Module by minimizing TBAV for Windows 95. TIP: To minimize a Windows 95 application, click on the small down arrow in the upper right corner of the window. To maximize the application, click on the up arrow. When you minimize TBAV for Windows 95, the main window disappears, and a small window containing some status information becomes visible at the bottom of the screen.

If you do not wish to see this status window, you can iconize TBAV for Windows 95 by also minimizing the status window. If you maximize the status window, the normal TBAV for Windows 95 window appears.

Using the Background Scan Module

After you activate the Background Scanning module, the status window appears. The first line of the status window displays the status of the Background Scan module. For example, it informs you about the period of time after which Background Scan will start. If you disable the Background Scanning module, the first line reads Background Scan is disabled.

The second line of the status window specifies the target for background scan. You can select a target using the **Background Scan Configuration** dialog box. The last line displays the date and time of the

last scan of the system (by either background scan or normal scan).

You will probably want to keep track of the actions the Background Scan module takes. If you are using an application that runs in full-screen mode, however, the status window disappears behind that application. To make the status window always visible, you can configure it as being always on top. In other words, the status window will always be the top-level window. To do this, activate the Control menu by clicking the box in the upper left corner of the window. When the system menu appears, click the Always on top item to make the status window the top-level window.

NOTE: Be aware that the system menu is accessible only when the Background Scan module is not currently scanning. If it is scanning, you can use the system menu to abort the background scan. If you click the system menu (or the title bar) of the status window while the Background Scan module is scanning the specified target, a dialog box appears and asks you if you want to abort or continue the background scan.

Configuring the Background Scan Module

As mentioned earlier, you can access the configuration dialog box by using either the Options, Background Scan Configuration command, or by selecting the third easy-access button. For more information about configuring the Background Scan Module, click the following topic.

Configuring the Background Scan Module

Configuring the Resident Modules

The File I/O Monitor and Background Scan Module can be configured using the Background Scan Configuration item in the Options menu.

Enable File I/O Monitor Module.
You can disable the File I/O Monitor Module by clearing this box or enable it by checking this box. It is active by default.

Enable Background Scan.
You can disable the Background Scan Module by clearing this box or enable it by checking this box. It is active by default.

NOTE: The status window always appears when minimizing TBAV for Windows 95, even if you disable the File I/O Monitor or Background Scan Module.

Show status window.
The status window will be displayed by default when you minimize TBAV for Windows 95. However, if you prefer TBAV for Windows 95 to show its icon instead of the status window, you can deselect the Show status window checkbox.

Background Scan Module - Activity period.
Specifies the period after which the Background Scan Module should starts scanning. The minimum period is 1 minute, and the maximum period is 999 minutes. The default period is 30 minutes. The countdown starts the moment you minimize or iconize TBAV for Windows 95.

Background Scan Module - Target.
This specifies the target for background scanning. If you select the Targets button, a small list with currently accessible targets appears, enabling you to choose one of these targets. The status window displays which Target will be scanned. The default target is LOCAL.SCN, i.e., all local fixed disks.

Background Scan Module - Priority.
The default priority for background scan is high - this means that the background scan operation is performed very fast, but is it possible that other applications will slow down a bit. To prevent this small decline in system performance, you might want to set the background scan priority level to low.

Addressing Special Topics

Understanding The Virus Information Database

TBAV for Windows 95 includes a comprehensive list of viruses and their descriptions. This virus information database is very useful whenever TBAV for Windows 95 detects a virus on your computer system; you can immediately access information about the behavior of the virus and (more important) how to get rid of it.

You can access the virus information database in two ways:

- Click the easy-access virus info button. This button is displayed below.
- Select the Virus Information option from the Documentation menu.

For more information about the virus information database, select the following topic:

Virus Information Database

Please note that the virus information database is only available for registered users.

Understanding General Configuration

As you probably know, the Options menu contains an item entitled TBAV for Windows 95 configuration. Selecting this item displays a configuration dialog, which enables you to change the general TBAV for Windows 95 options. For specific information about the items in this dialog box, select the following topic:

General Configuration of TBAV for Windows 95

General Configuration of TBAV for Windows 95

The items of the general TBAV for Windows 95 options are discussed next. These items can be altered via
the TBAV for Windows 95 configuration item in the Options menu.

Wait after program execution.
If you enable this option, TBAV for Windows 95 waits after either the Setup or Scan module finishes. If you do not set this option, TBAV for Windows 95 immediately returns to the main window when the Setup module or Scan module finishes. This option is enables by default.

Virus alert options.
TBAV for Windows 95 can produce some sound via the internal speaker or sound card when it finds a virus. Using the radio buttons under Audible alerts, you can specify in which cases TBAV for Windows 95 produces sound. Always specifies that TBAV for Windows 95 always uses sound when it detects a virus. Only once specifies that TBAV for Windows 95 produces sound only the first time it detects a virus. Background Scan specifies that TBAV for Windows 95 produces a sound only when it detects a virus during background scan. You can also turn off the sound option by enabling the Never option. Only once is active by default.
NOTE: Be aware that the virus counter resets every time TBAV for Windows 95 starts.

The Flash virus window option can be enabled to give an extra accent to the window that pops up when a virus is found.

File view utility.
TBAV for Windows 95 default internal viewer enables you to view and even print the Setup data file or a log file created by the Scan module. If you prefer to use another one, however, you can specify this by typing the pathname of your favorite file viewer in the edit control.
TIP: You might try using Microsoft Write as your file viewer by entering C:\WINDOWS\WRITE.EXE. As Write starts, select the No Conversion button..Another possible viewer you might prefer is Notepad (C:\WINDOWS\NOTEPAD.EXE).

Warning messages.
By default, a warning window will be displayed when TBAV for Windows 95 is being closed, since closing TBAV for Windows 95 will disable all on-the-fly virus checking capabilities of TBAV for Windows 95. If you do not want to see this warning message each time you quit TBAV for Windows 95, you can disable it via this option.

Virus Information Database

When you activate virus information, a small dialog window appears containing the names of all viruses included in the database. You can quickly locate information about a specific virus by starting to type the name of the virus in the edit box. The selection in the list box updates according to the contents of the edit box. In the example, we typed the name Smiley_Boot; Smiley_Boot, then, appears in the list box (actually, the name appeared after typing only Smiley_). Double-clicking a virus name in the list box, or clicking the View Info button at the right side of the window, displays a window containing information about the virus.

For information about the virus information window, refer to **Detecting a Virus**.

The "What's New ?" Files

When you activate the Whats new ? information, a small dialog window appears containing the names of all files residing in the TBAV directory containing update information. Each of these files has an extension that represents the version number of TBAV. For example, the Whats new ? file for version 6.35 of TBAV for Windows 95 is called TBAVWNEW.635, while the Whats new ? file for version 6.35 of TBAV for Dos is called WHATSNEW.635.

If you select one of the files, the file viewer will pop up, showing you the contents of the selected Whats new ? file.

How to contact ThunderBYTE

About ThunderBYTE

ThunderBYTE Anti-Virus Utilities represents the next generation of anti-virus detection and cleaning software against known and unknown computer viruses -- complete with 5 different security levels to help protect against viruses: signature and heuristic based scanning technology, generic decryption using real-code emulation, integrity checking plus active monitoring.

Created in Europe to combat the growing threat of intelligent and sophisticated viruses around the world, ThunderBYTE Anti-Virus Utilities have been the leaders in anti-virus computer software for several years, clearly acclaimed as the world's fastest scanner. Using a combination of traditional and proprietary heuristic "seek-and-destroy" techniques to ferret out even the newest and stealthiest viruses, trojans, and logic bombs, these utilities offer an enhanced level of anti-virus protection at speeds that are unsurpassed in the PC arena.

ThunderBYTE Sales, Support and Upgrades

For power users there is no compromise; only the best will do. In the world of anti-virus utilities, one company stands head and shoulders above the pack when it comes to power and speed: the ThunderBYTE Anti-Virus Utilities. Within ThunderBYTE is both the world's fastest and most advanced virus detection engine.

ThunderBYTE is supported world-wide by a dedicated professional team of anti-virus researchers, technical support specialists and highly trained, specifically authorized agents. Electronic support is provided 24 hours a day via CompuServe in the ThunderBYTE Forum (GO TBYTE), WUGNET/WINUTIL Forum (GO WINUTIL) and on the Windows News Forum (GO WINNEWS).

ThunderBYTE International Agents

For a comprehensive list of ThunderBYTE International Agents, select the List of Agents menu item from the Documentation menu.