*Thunder*BYTE

Anti-Virus Utilities

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 information you need if you want to use the TBAVWIN utility. This program enables you to use the ThunderBYTE Anti-Virus utilities from within Microsoft Windows.

The topics of this help file are:

Topics concearning the TBAVWIN program:

What is ThunderBYTE Anti-Virus ?

ThunderBYTE Anti-Virus (TBAV) is a comprehensive toolkit designed to protect against - and recover from - computer viruses. While TBAV focuses heavily on numerous ways to prevent a virus infection, the package would not be complete without various cleaner programs to purge a system, in the unlikely event that a virus manages to slip through. The package therefore consists of a number of programs each of which help you to prevent viruses to do their destructive jobs.

Overview of the TBAV package

Collecting software information: TbSetup

TbSetup is a program that collects information from all software found on your system. The information will be put in files named Anti-Vir.Dat. The information maintained in these files can be used for integrity checking, program validation, and to clean infected files.

Enable memory resident TBAV utilities: TbDriver

TbDriver does not provide protection against viruses by itself, but must be loaded in advance to enable the memory resident ThunderBYTE Anti- Virus utilities, such as TbScanX, TbCheck, TbMem, TbFile and TbDisk to do their job properly.

Scanning for viruses: TbScan

TbScan is both a very fast signature scanner and a so-called heuristic scanner. Besides its blazing speed it has many configuration options. It can detect mutants of viruses, it can bypass stealth type viruses, etc. The signature file used by TbScan is a coded 'TbScan.Sig' file, which can be updated by yourself in case of emergency. TbScan is able to disassemble files. This makes it possible to detect suspicious instruction sequences and to detect yet unknown viruses. This generic detection, named heuristic analysis, is a technique that makes it possible to detect about 90% of all viruses by searching for suspicious instruction sequences rather than using any signature. For that purpose TbScan contains a real disassembler and code analyzer.

Another feature of TbScan is the integrity checking it performs when it finds the Anti-Vir.Dat files generated by TbSetup. 'Integrity checking' means that TbScan will check that every file being scanned matches the information maintained in the Anti-Vir.Dat files. If a virus infects a file, the maintained information will not match the now changed file anymore, and TbScan will inform you about this.

TbScan performs an integrity check automatically, and it does not have the false alarm rate other integrity checkers have. The goal is to detect viruses and not to detect configuration changes!

Automatic scanning: TbScanX

TbScanX is the memory resident version of TbScan. This signature scanner remains resident in memory and automatically scans those files which are being executed, copied, de-archived, downloaded, etc. TbScanX does not require much memory. It can swap itself into expanded, XMS, or high memory, using only 1Kb of conventional memory.

Check while loading: TbCheck

TbCheck is a memory resident integrity checker. This program remains resident in memory and checks automatically every file just before it is being executed. TbCheck uses a fast integrity checking method, consuming only 400 bytes of memory. It can be configured to reject files with incorrect checksums, and/or to reject files that do not have a corresponding Anti-Vir.Dat record.

Reconstructing infected files: TbClean

TbClean is a generic file cleaning utility. It uses the Anti-Vir.Dat files generated by TbSetup

to enhance file cleaning and/or to verify the results. TbClean can however also work without these files. It disassembles and emulates the infected file and uses this analysis to reconstruct the original file.

Restoring infected boot-sector, CMOS and partition tables: TbUtil

Some viruses copy themselves into the hard disk's partition table, which makes them far more difficult to remove than bootsector viruses. Performing a low-level format is an effective, but rather drastic measure. TbUtil offers a more convenient alternative by making a precautionary back-up of uninfected partition tables and the boot sector. If an infection occurs, the TbUtil back-up can be used as a verifying tool and as a means to restore the original (uninfected) partition table and bootsector without the need for a destructive disk format. The program can also restore the CMOS configuration for you. If a back-up of your partition table is not available, TbUtil will try to create a new partition table anyway, again avoiding the need for a low-level format.

Another important feature of TbUtil is the option to replace the partition table code with new code offering greater resistance to viruses. The TbUtil partition code is executed before the boot sector gains control, enabling it to check this sector in a clean environment. The TbUtil partition code performs a CRC calculation on the master boot sector just before the boot sector code is activated and issues a warning if the boot sector has been modified. The TbUtil partition code also checks and reports changes in the RAM lay-out. These checks are carried out whenever the computer is booted from the hard disk.

It should be noted that boot sector verification is imperative before allowing the boot sector code to execute. A virus could easily become resident in memory during boot-up and hide its presence. TbUtil offers total security at this stage by being active before the boot sector is executed. Obviously, TbUtil is far more convenient than the traditional strategy of booting from a clean DOS diskette for an undisturbed inspection of the boot sector.

Resident safeguard: TbMon

TbMon is a set of memory resident anti-virus utilities, consisting of TbMem, TbFile and TbDisk. Most other resident anti-virus products offer you the choice to invoke them before the network is loaded and losing the protection after the logon procedure, or to load the anti-viral software AFTER the logon to the network, resulting in a partially unprotected system. The ThunderBYTE Anti-Virus utilities however recognize the network software and take appropriate actions to ensure their functionality.

Controlling memory: TbMem

TbMem detects attempts from programs to remain resident in memory, and makes sure that no program can remain resident in memory without permission. Since most viruses remain resident in memory, this is a powerful weapon against all those viruses, known or unknown. Permission information is maintained in the Anti-Vir.Dat files.

Preventing infection: TbFile

TbFile detects attempts from programs to infect other programs. It also guards read-only attributes, detects illegal time-stamps, etc. It will make sure that no virus succeeds in infecting programs.

Protecting the disk: TbDisk

TbDisk is a disk guard program which detects attempts from programs to write directly to disk (without using DOS), attempts to format, etc., and makes sure that no malicious program will succeed in destroying your data. This utility also traps tunneling and direct

calls into the BIOS code. Permission information about the rare programs that write directly and/or format the disk is maintained in the Anti-Vir.Dat files.

Notify virus behaviour all over the network: TbLANMsg

TbLanMsg is a program that forwards TBAV messages to other machines. Its purpose is to notify helpdesks or supervisors automatically of a possible virus. If one of the resident TBAV utilities detects a virus, an on-line message will be send to the specified machine. Also TbScan sends a message to the specified machine or user if it detects a virus.

TbLanMsg currently only works on Lantastic networks. Versions for other networks will be available soon!

Keep record of all ThunderBYTE messages: TbLog

TbLog is a TBAV log file utility. It writes a record into a log file whenever one of the resident TBAV utilities pops up with an alert message. Also when TbScan detects a virus a record will be written.

This utility is primarily intended for network users. If all workstations have TbLog installed and configured to maintain the same log file, the supervisor is able to keep track of what is going on easily. When a virus enters the network he is able to take determine which machine introduced the virus, and he can take action in time.

A TbLog record consists of the timestamp on which the event took place, the name of the machine on which the event occured, and an informative message about what happenend and which files were involved. The information is very comprehensive and takes just one line.

Define your own signatures (in case of an emergency): TbGensig

Since TBAV is distributed with an up-to-date, ready-to-use signature file, you do not really need to maintain a signature file yourself. If, however, you want to define your own virus signatures, you will need the TbGensig utility. You can use either published signatures or define your own ones if you are familiar with the structure of software.

Remove infected files: TbDel

The DOS 'DEL' command does not actually erase a file. It simply changes the first filename character in the directory listing and frees up the space by changing the disk's internal location tables. TbDel is a small program with just one but important purpose: it replaces every single byte in a file with zero characters before deleting it. The entire contents are therefore obliterated and totally unrecoverable.

An effective stack manager: StackMan

To avoid problems with memory resident software ('TSR' programs) DOS is able to maintain a stack pool and to switch to a dedicated stack if a hardware interrupt occurs. The "Stacks" statement in the Config.Sys can be used to control this stack pool. The DOS stack switching however, has some drawbacks. TBAV StackMan offers important additional functionality above the DOS "Stacks" command.

Overview of the TBAVWIN program

TBAVWIN is a front-end interface utility for use with the ThunderBYTE Anti-Virus utilities. TBAVWIN requires Microsoft Windows 3.0 or above and, of course, the ThunderBYTE Anti-Virus utilities package, version 6.05 or above. TBAVWIN is the MS-Windows equivalent of the TBAV program, which operates solely with the MS-DOS operating system.

When you have executed the TBAVWIN program, you will see several menu options. From the File menu item, you are able to configure the TBAVWIN program. Beware, that if you cange the configuration of either the TBAV or TBAVWIN program, it effects **both** programs.

The TbSetup menu item enables you to setup and configure your computer system for use with the ThunderBYTE Anti-Virus utilities. For instance, when you have installed a new program on your harddisk, you can use TbSetup to extract checksum information from this program. This checksum information will be used by TbScan and TbCheck to make sure no virus will attach itself on your new program.

With the TbScan menu item of the TBAVWIN program you are able to execute the virus scanner program.

Should this program discover viruses on your system, you might want to clean the infected file(s). This can be achieved using the TbClean submenu.

This package of Anti-Virus utilities is most likely of great value to you and your computer system. So, registering TBAV is the most logical step one can take. The TBAVWIN program has a menu item Register to make registering this package easier.

License agreement

The ThunderBYTE Anti-Virus utilities and the accompanying documentation are SHAREWARE. You are hereby granted a licence by ESaSS B.V. to distribute the evaluation copy of the software and its documentation, subject to the following conditions:

1. The evaluation package of the ThunderBYTE Anti-Virus utilities may be distributed freely without charge in evaluation form only.

2. The evaluation package of the ThunderBYTE Anti-Virus utilities may not be sold or licensed. Neither may a fee be charged for its use. If a fee is charged in connecti- on with the ThunderBYTE Anti-Virus utilities at all, it should only cover the cost of copying or distribution. **UNDER NO CIRCUMSTANCES** should payment of such fees be understood to constitute legal ownership.

3. The evaluation package of the ThunderBYTE Anti-Virus utilities must be presented in its complete form. It is not allowed to distribute the program and its documentation files separately.

4. Neither the software nor its documentation may be amended or altered in any way.

5. By granting you the right to distribute the evaluation copy of the ThunderBYTE Anti-Virus utilities, you do not become the owner of these utilities in any form.

6. ESaSS B.V. accepts no responsibility in case the program malfunctions or does not function at all.

7. ESaSS B.V. can never be held responsible for damage, directly or indirectly resulting from the use of the ThunderBYTE Anti-Virus utilities.

8. Using the ThunderBYTE Anti-Virus utilities means that you agree to these conditions.

Any other use, distribution or representation of the ThunderBYTE Anti-Virus utilities is expressly forbidden without the written permission of ESaSS B.V.

Registration

THIS IS NOT FREE SOFTWARE! If you paid a 'public domain' vendor for this program, you paid for the service of copying the program, and not for the program itself. Proceeds from such transactions would never reach the makers of this product. You may evaluate this product, but if you decide to make use of it, you should register your copy.

To register: run the REGISTER program, and return the resulting form to a ThunderBYTE shareware registration site.

We offer several inducements to you for registering. First of all, you are entitled to support for the ThunderBYTE Anti-Virus utilities, which can be quite valuable at times.

Some very enhanced features (like the TbScan option 'extract') are only available to registered users. Once you have become a registered user, these advanced options will be made available to you. Your registrations allow us to enhance our products and to keep them up to date!

The registration key

Registered users receive the information and instructions to generate their TBAV.KEY. The key file will contain important information such as the licence number and the name of the licensee. The key file TBAV.KEY is NOT to be sold or transferred in any way. The ThunderBYTE Anti-Virus utilities do search for the key file in the current directory. If they do not find it there, they search the same directory where the program file itself resides.

If the key file is corrupt or invalid, the ThunderBYTE Anti-Virus utilities continue without error message although your version of the ThunderBYTE Anti-Virus utilities will then be treated as an unregistered SHAREWARE version. If your key is only valid for some of the ThunderBYTE Anti-Virus utilities, the other utilities will ignore it when run.

Although you are allowed to evaluate the ThunderBYTE Anti-Virus utilities for a reasonable period of time, it is **ILLEGAL** to use them in combination with a key, produced without authorization of ESaSS B.V., or generated by any software not distributed by ESaSS B.V..

Disclaimer, Trademark and Copyright

Disclaimer of warranty and limited warranty

ESaSS BV warrants that (a) the software will perform substantially in accordance with the accompanying written materials and (b) the software is properly recorded on the disk media. This warranty extends for ninety (90) days) from the date of purchase. There is no warranty after expiration of the warranty period.

Neither ESaSS BV nor anyone else who has been involved in the creation, production or delivery of the ThunderBYTE Anti-Virus utilities or the documentation grants any other warranties with respect to the contents of the software, the written materials and each specifically disclaims any implied warranties of merchantability or fitness for any purpose.

Except as stated herein, in no event shall ESaSS BV or its suppliers be liable for any damages whatsoever, whether direct, indirect, consequential, or incidental damages (including damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss, arising out of the use of or inability to use such product even if ESaSS BV has been advised of the possibility of such damages. Because some states do not allow the exclusion of limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

ESaSS BV reserves the right to revise the software and the written materials and to make changes from time to time in the contents without obligation to notify any person.

Trademark

The ThunderBYTE Anti-Virus utilities are registered trademarks of ESaSS BV. All other product names mentioned are acknowledged to be the marks of their producing companies.

Copyright

 The diskettes provided with the ThunderBYTE Anti-Virus utilities are not copy protected The ThunderBYTE Anti-Virus utilities are protected by copyright law, which applies to the computer software as well, except for that you may make copies of the software solely for backup or archive purposes and transfer the software to harddisk disk provided that the software is used as specified herein.

The File menu item

The File menu item contains three entries: Configure TBAV, Quit and Exit. If you want to quit TBAVWIN, and choose Quit, all changes that you have made in the configuration of TBAVWIN will be saved to the ini-file (TBAV.INI). If you don't want the contents of this file to be changed, you should choose Exit to quit the TBAVWIN program.

There is one submenu with which you are able to make some configuration changes in the TBAVWIN menu shell. If you want to read more about it, please select the line below.

Configure TBAV

The TbSetup menu item

Some information about TbSetup

TbSetup is an indispensible tool, adding support to the rest of the ThunderBYTE Anti-Virus utilities, even though it does not take an active part in actual virus detection or cleaning itself. TbSetup organizes control and recovery information giving extra power to the other utilities. The information is gathered, mainly from program files, into a single reference file called Anti-Vir.Dat, one each per directory.

The TbSetup program recognizes some files that need special treatment. An example of such a file is a disk image file of a network remote boot disk. - Such a file that actually represents a complete disk - should be scanned completely, and for all viruses. TbSetup will put a mark in the Anti-Vir.Dat file to make sure that TbScan scans the complete file for all viruses.

TbSetup is the one program where the rule applies: The less you use the program, the better your protection against viruses! Why? Keep in mind that an Anti-Vir.Dat file stores vital information needed to detect a virus, as well as data for subsequent recovery and for cleaning. But consider what would happen if you were to execute TbSetup after a virus entered the system: the information in the Anti-Vir.Dat file would be 'updated' to the state of the infected file, wiping out all traces of data needed to reconstruct the file of the original, uninfected state. Never use TbSetup when there is the slightest evidence of a virus in your system. Once the Anti-Vir.Dat files have been generated as part of the initial setup, any subsequent usage of TbSetup should be confined to directories with new or changed program files.

The TbSetup Menu

The TbSetup menu consists of six items. The first of them is the Start TbSetup item, which enables you to actually execute the TbSetup program. The next item is Files/Paths to Setup. You can enter the files and paths here, that you want TbSetup to process. TbSetup can use a special file to recognize files that need special treatment. The name of this file can be entered by choosing Data file pathname. To view this file, choose View data file.

There are two submenus to set or clear some options of the TbSetup program. To read more about them, please select one of the two lines below.

TbSetup options
TbSetup flags

The TbScan menu item

Some information about TbScan

TbScan is a virus scanner: it has been specifically developed to detect viruses, Trojan Horses and other such threats to your valuable data. Most viruses consist of a unique sequence of instructions, called a signature. Hence through checking for the appearance of such signatures in a file we can find out whether or not a program has been infected. Scanning all program files for the signatures of all known viruses helps you to find out quickly whether or not your system has been infected and, if so, by which virus.

TbScan is the fastest scanner on the market today, therefore it invites users to invoke it from within their AUTOEXEC.BAT file every morning. Thanks to its design, TbScan will not slow down if the number of signatures increases. It doesn't matter whether you scan a file for 10 or a 1000 signatures.

TbScan can detect yet unknown viruses. The built-in disassembler is able to detect suspicious instruction sequences and abnormal program layouts. This feature is called 'heuristic scanning' and it is partially enabled by default. Heuristic scanning is performed on files and bootsectors.

The TbScan Menu

The TbScan menu item consists of seven topics, of which four items are submenus. To execute the scanner, you should choose Start TbScan. To tell TbScan where it should perform its scanning operation you can choose Files/paths to scan. TbScan offers you the possibility to make a log-file while scanning. In order to view this file, you must select the View log file option.

The options that TbScan offers can be enabled or disabled by using one of the following submenus:

TbScan options
TbScan advanced options
If virus found
Log file options

The TbClean menu item

Some information about TbClean

TbClean isolates viral code in an infected program and removes it. From then on it will be safe to use the program again, as the risk of other files being infected or damaged by it will have been securely eliminated.

Generic Cleaners

TbClean works completely different compared to 'conventional cleaners. First of all, it does not recognize any virus. Its disinfection scheme is completely different and it works with almost any virus. Actually, the TbClean program contains two cleaners: a 'repair' cleaner, and a 'heuristic' cleaner. The repair cleaner needs an Anti-Vir.Dat file that is generated by the TbSetup program before the infection occurs. In this Anti-Vir.Dat file essential information is stored, like the original file size, the bytes at the beginning of the program, a cryptographic checksum to verify the results, etc. This information enables TbClean to disinfect almost every file, regardless of the virus it has been infected with, known or unknown.

No information available?

In the heuristic cleaning mode TbClean does not need any information about viruses either, but it has the added advantage that it does not even care about the original, uninfected state of a program. This cleaning mode is very effective if your system is infected with an unknown virus and yo neglected to let TbSetup generate the Anti-Vir.Dat files in time.

In the heuristic mode, TbClean loads the infected file and starts emulating the program code to find out which part of the file belongs to the original program and which to the virus. The result is successful if the functionality of the original program is restored, and the functionality of the virus has been reduced to zero. *Note that this does not imply that the cleaned file is 100% equal to the original.*

It is possible that the infected file is infected with multiple viruses, or multiple instances of the same virus! Some viruses keep on infecting files, and in such case the infected files will keep growing. If TbClean used its heuristic cleaning mode, it is very likely that TbClean removed only one instance of the virus. In this case, it is necessary to repeat the cleaning process until TbClean reports that it can not remove anything anymore.

The TbClean Menu

After tracking one or more viruses, all you should do is select the Start cleaning option in the TbClean menu. After specifying the relevant filename, TbClean will come into action. By using the submenu Options you can tell TbClean to make a list file of a chronological disassembly of the virus being removed. The name of this list file can be entered using the List file name option.

TbClean allows some additional parameters. These parameters can be enabled or disabled using the following submenu:

TbClean options

The TbUtil menu item

Some information about TbUtil

TbUtil provides a defense against partition table and bootsector viruses:

TbUtil copies the partition table, bootsector and CMOS data area into a file. On a regular base you can use TbUtil to compare both the current and the copied versions of the partition table, bootsector and CMOS data area. After a (virus) accident you can restore the copy with the TbUtil program.

TbUtil removes a partition table virus without having to low-level format the hard disk, even if there is no backup of the partition table.

TbUtil removes bootsector viruses.

TbUtil creates a partition table that has some first-line virus defenses built-in.

TbUtil replaces the infected or clean bootsector by a safe TBAV bootsector.

The TbUtil menu contains some useful programs to prevent bootsector virus infection or to remove these viruses.

Immunize/clean diskette

You can use the 'immunize' program to clean diskettes infected by a bootsector virus or to replace the standard bootsector by a bootsector which has advantages over the original one.

It has virus detection capabilities: it can detect even 'stealth' and bootsector viruses.

The TBAV bootsector is able to load the system files if they are available on the disk, but if the DOS system files are not on the disk the TBAV bootsector will present a small menu and offers you two possibilities: retry the boot operation with another diskette, or to boot from the harddisk. If the user selects the latter, it is not required to open the diskette drive door.

Immunize/clean partition code

This is a very powerful option, which can be used to clean an infected partition table if there is no TbUtil data file. It replaces the existing partition table code by a new partition routine containing some virus detection capabilities. The original partition code will be saved in a file. You have to execute TbUtil from a floppy drive or you have to specify the name of the file (the specified drive should be a diskette drive) to store the original partition code.

If the original partition table is completely damaged and cannot be used to build a new one, TbUtil will scan the entire disk for information about the original disk layout. TbUtil will also search for TbUtil data files on the hard disk. It is however recommended to store the data file on a diskette, although it is a good idea to keep a copy of it on the hard disk. Just in case!

If your system configuration changes, i.e. you update your DOS version, or change the amount of memory, you need to update the information stored in the immune partition as well. You can do this by using this option.

In the unlikely event that the system does not boot properly, you can restore the original partition table using the TbUtil 'restore' option or by using the DOS 5+ 'FDISK /MBR' command (which will create a new partition table).

Other options of the TbUtil can be accessed via the submenu

System maintenance

The Register menu item

If you select the Register menu item, the REGISTER.EXE program will be loaded, to assist you in registering the ThunderBYTE Anti-Virus package. If you want to know more about the license agreement or registration of TBAV, please choose one of the topics shown below.

The File|Configure TBAV ***submenu***

Execute programs in full screen

By enabling this option, TBAVWIN will execute all programs in full screen instead of executing them in a sizeable DOS-box.

Wait after program execution

By enabling this option, TBAVWIN will display the message: "Press any key..." after executing an external utility.

Display command line before executing

Enabling this option will force TBAVWIN to display the DOS command, which will load the external utility. This option comes in handy in order to see the command(s) you specified before. After pressing <Enter> TBAVWIN will execute the DOS commands.

Edit command line before executing

If enabled, you may change the DOS command, which will load the external utility.

File view utility

TbSetup and TbScan generate a datafile and a logfile respectively. By default, you can view these files from the TBAVWIN menu using an internal file view utility. By using this option you are able to attach your favorite external file view utility. Enter the complete path and the file name, including the extension.

The TbSetup|Start TbSetup ***dialog***

You're about to start the TbSetup utility. Now is the time you can view or edit the commandline, depending on your configuration. If you press the OK button, TbSetup will be executed. Pressing the CANCEL button will bring you back to the TBAVWIN menu shell.

The TbSetup|Files/paths to setup ***dialog***

With the 'Files/paths to setup' dialog you can specify the files that TbSetup should process when executed. For instance, if you installed a new program in the directory C:, you might want to enter this pathname, so that TbSetup can create the Anti-Vir.Dat file.

If you press the OK button, the pathname you entered is used the next time you execute TbSetup. If you press the CANCEL button, the pathname you entered will be discarded, and the pathname you saw when you first opened this dialog, will be used.

The TbSetup|Data file pathname ***dialog***

TbSetup uses a data file for all special program files on your disk that need special treatment. The pathname of this file can be entered using this dialog box. Pressing OK will cause the pathname you entered to be used. If you press CANCEL all changes will be discarded.

The TbSetup|Options ***submenu***

Prompt for pause

When you enter option 'pause' TbSetup will stop after it has processed the contents of one window. This gives you the possibility to examine the results.

Only new files

If you want to add new files to the Anti-Vir.Dat database, but prevent the information of changed files from being updated use option 'newonly'. Updating the information of changed files is dangerous because if the files are infected, the information to detect and cure the virus will be overwritten. Option 'newonly' prevents the information from being overwritten but it still allows information of new files to be added 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 will neatly remove all Anti-Vir.Dat files from your system.

Do not change anything

If you want to see the effect of an option without the risk that something is activated you do not want, use option 'test'. If that options is specified the program will behave as it would normally, but it will 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 to have normal - i.e. visible - files disable this option. *Note that this option only applies for new Anti-Vir.Dat files.*

Make executables read-only

As TbFile guards the read-only attribute permanently it is highly recommended to make all executable files read-only to prevent any modifications on these files. TbSetup will do the job if you enable option 'read-only'. Files that should not be made read-only are recognized by TbSetup.

Clear read-only attributes

This option can be used to reverse the operation of option 'read-only'. If you enable this option all read-only attributes of all executable files will be cleared.

Sub-Directory scan

By default TbSetup will search sub-directories for executable files, unless a filename (wildcards allowed!) has been specified. If you disable this option, TbSetup will not process sub-directories.

The TbSetup|Flags ***submenu***

Use normal flags

This is the default setting for TbSetup. However, if you're an experienced user, you might want to set or reset flags manually.

Set flags manually

This option is for advanced users only. With this option you can manually set permission flags in the Anti-Vir.Dat record. This option requires a hexadecimal bitmask for the flags to set. For information about the bitmask consult the TbSetup.Dat file. The flags you can change are the ones listed in the 'Define flags to be changed' box.

Reset flags manually

This option is for advanced users only. With this option you can manually reset permission flags or prevent flags to be set in the Anti-Vir.Dat record. This option requires a hexadecimal bitmask for the flags to reset. For information about the bit mask consult the TbSetup.Dat file. The flags you can change are the ones listed in the 'Define flags to be changed' box.

The TbScan|Start TbScan ***dialog***

You're about to start the TbScan utility. Now is the time you can view or edit the commandline, depending on your configuration. If you press the OK button, TbScan will be executed. Pressing the CANCEL button will bring you back to the TBAVWIN menu shell.

The TbScan|Files/paths to scan ***dialog***

With the 'Files/paths to scan' dialog you can specify the files or paths that TbScan should process when executed. To search both disks C: and D: you should enter:

C:\ D:

When no filename has been specified but a drive and/or path instead, the specified path will be used as top-level path. All its subdirectories will be processed too. If a filename is specified, only the specified path will be searched. Subdirectories will not be processed.

If you press the OK button, the pathname(s) you entered will be used the next time you execute TbScan. If you press the CANCEL button, the pathname you entered will be discarded, and the pathname you saw when you first opened this dialog, will be used.

The TbScan|Options ***submenu***

Use TBAV.INI file

TbScan searches for a file named TBAV.INI in the TbScan directory. By enabling this option, the TbScan configuration values, saved in the TBAV.INI file, will also be valid when loading TbScan from the command line. Be careful, since options specified in the TBAV.INI file can not be undone on the command line. See chapter I-2 ('Configuration') of the manual.

Prompt for pause

When you activate the 'pause' option TbScan will stop after it has checked the contents of one window. This gives you the possibility to examine the results without having to consult a log file afterwards.

Quick scan

TbScan will use the Anti-Vir.Dat files to check for file changes since the last time. Only if a file has been changed (CRC change) or is not yet listed in Anti-Vir.Dat it will be scanned. Normally TbScan will always scan files.

Non-executable scan

With this option TbScan will scan non-executable files (files without extension COM, EXE, SYS or BIN) too. If TbScan finds out that such a file does not contain anything that can be executed by the processor the file will be 'skipped'. Otherwise the file will be searched for COM, EXE and SYS signatures. TbScan however will not perform heuristic analysis on non-executable files. Since viruses normally do not infect non-executable files it is not necessary to scan non-executable files too. We even recommend not to use this option unless you have a good reason to scan all files.

A virus needs to be executed to perform what it is programmed to do, and since non-executable files will not be executed a virus in such a file can not do anything. For this reason viruses do not even try to infect such files. Some viruses however will write to non-executable files as a result of 'incorrect' programming. If so, these non-executable files will never harm other program or data files, but do contain corrupted data.

Maximum compatibility

If you select this option, TbScan attempts to be more compatible with your system. Use this option if the program does not behave as you would expect, or even halts the system. This option will slow down the scanning process. Therefore, it should only be used if necessary. *Note that this option does not affect the results of a scan.*

Bootsector scan

Enabling this option will force TbScan to scan the bootsector as well.

Memory scan

Enabling this option will force TbScan to scan the memory of the PC.

HMA scan forced

TbScan detects the presence of an XMS-driver, and scans HMA automatically. If you have an HMA-driver which is not compatible with the XMS standard you can use the 'HMA' option to

force TbScan to scan HMA.

Upper memory scan

By default TbScan identifies RAM beyond the DOS limit and scans that too. This means that video memory and the current EMS pages are scanned by default. You can use this option to enable the scanning of non-DOS memory.

Subdirectory scan

By default TbScan will search sub-directories for executable files, unless a filename (wildcards allowed!) is specified. If you disable this option, TbScan will not scan sub-directories.

Repeat scanning

This option is very useful if you want to check a large amount of diskettes. TbScan does not return to DOS after checking a disk, but it prompts you to insert another disk in the drive.

Abort on Ctrl-Break

If this option is enabled, TbScan will abort scanning when Ctrl-Break is pressed.

Fast scrolling

TbScan shows the processed file in a scrolling window. There are two methods of scrolling: fast scrolling where the files are displayed on top of the previous ones if the window becomes filled, and the conventional slow method of scrolling where the files at the bottom 'push up' the previous ones. By default TbScan uses the faster but less attractive method of scrolling.

The TbScan|Advanced options ***submenu***

High heuristic sensitivity

Auto heuristic sensitivity

Low heuristic sensitivity

TbScan always performs a heuristic scan on the files being processed. However, only if a file is very probably infected with a virus, TbScan will report the file as being infected. If you use option 'High heuristic sensitivity', TbScan is somewhat more sensitive. In this mode 90% of the new, unknown, viruses will be detected without any signature, but some false alarms may occur. If you use option 'Low heuristic sensitivity', TbScan will report an unknown virus in only a few cases. If you choose 'Auto heuristic sensitivity', TbScan automatically adjusts the heuristic detection level after a virus has been found. This provides you maximum detection capabilities in case you need it, while the amount of false alarms due to heuristics remains small in normal situations. In other words: as soon as a virus has been found, TbScan will anticipate and proceed as if option 'High heuristic sensitivity' has been specified.

Extract signatures

This option is available to registered users only. See the chapter 'TbGensig' (IV-5) of the manual on how to use the option 'extract'.

Configure executable extensions

By default, TbScan only scans file with a filename extension which indicates that the file is a program file. Viruses which do not infect executable code simply do not exist. Files with the extension EXE, COM, BIN, SYS, OV? are considered to be executable.

However, there are some additional files which 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 may want to scan them anyway.

Some filename extensions that may indicate an executable format are: .DLL.SCR.MOD.CPL.00?.APP The first four extensions indicate Windows executable files. They normally display "This program requires Microsoft Windows" when you try to execute them, so you probably won't run these files often under DOS. Even when they are infected by a DOS virus they are not likely a threat since you don't execute them. Therefore TbScan does not scan them by default. To make TbScan scan these files by default, select this option and fill out the extensions you want to have scanned. The question mark as wildcard is allowed.

Warning! Be careful about which extensions you specify: scanning a non- executable file causes unpredicatble results, and may result in false alarms.

The TbScan|If virus found ***submenu***

Present action menu

If TbScan detects a virus, the program will display a menu containing the possible actions to be taken: just continue, delete, kill or rename the infected file.

Just continue (log only)

If TbScan detects an infected file it prompts the user to delete or rename the infected file, or to continue without action. If you select this option, TbScan will always continue. We highly recommend you to use a log file in such situations, as a scanning operation does not make much sense without the return messages being read (see 'Command line options').

Delete infected file

If TbScan detects a virus in a file it prompts the user to delete or rename the infected file, or to continue without action. If you specify the 'delete' option, TbScan will delete the infected file automatically, without prompting the user first. Use this option if you have determined it is a virus infection. Make sure that you have a clean back-up, and that you really want to get rid of all infected files at once.

Kill infected file

This option is nearly the same as the 'delete' option. However, with the DOS 'undelete' program you can recover a deleted file, but if a file has been deleted with the 'kill' option, recovery is not possible anymore.

Rename infected file

If TbScan detects a file virus it prompts the user to delete or rename the infected file, or to continue without action. If you select the 'rename' option, TbScan will rename the infected file automatically, without prompting the user first. By default, the first character of the file extension will be replaced by the character 'V'. An .EXE file will be renamed to .VXE, and a .COM file to .VOM. This prevents the infected programs from being executed, spreading the infection. At the same time they can be kept for later examination and repair.

The TbScan|Log file options ***submenu***

Log file path/name

With option logname you can specify the name of the log file to be used. TbScan will create the file in the current directory unless you specify a path and filename after selecting this option. If the log file already exists, it will be overwritten. If you want to print the results, you can specify a printer device name rather than a filename (logname=lpt1). *Note: you have to combine this option with option 'log'.*

Output to logfile

When you use this option, TbScan creates a log file. The log file lists all infected program files, specifying heuristic flags (see: appendix B of the manual) and complete pathnames.

Append to existing log

If you use this option, TbScan will not overwrite an existing log file but append the new information to it. If you use this option often, it is recommended to delete or truncate the log file once in a while to avoid unlimited growth. *Note: you have to combine this option with option 'log'.*

No heuristic descriptions

If you enable this option TbScan will not specify the descriptions of the heuristic flags in the log file. The heuristic flag descriptions are listed in appendix B of the manual.

Loglevel

These levels determine what kind of file information will be stored in the log file. The default log level is 1. You may select one of five log levels:

0 Log only infected files. If there are no infected files do not create or change the log file.

1 Log summary too. Put a summary and timestamp in the log file. Put only infected files in the log file.

2 Log suspected too. Same as loglevel=1, but now also 'suspected' files are logged. Suspected files are files that would trigger the heuristic alarm if option 'heuristic' had been specified.

3 Log all warnings too. Same as loglevel=2, but all files that have a warning character printed behind the filename will be logged too.

4 Log clean files too. All files being processed will be put into the log file.

The TbClean|Start TbClean ***dialog***

You're about to start the TbClean utility. You're asked to enter the name of the infected file you want to clean, and the name of the cleaned file. If you press the OK button, TbClean will be executed. Pressing the CANCEL button will bring you back to the TBAVWIN menu shell.

The TbClean|List file name ***dialog***

If have have set the option Make list file in the TbClean Options you can enter the name of this file here. The default name is the same as the name of the infected file, with the extension replaced by '.LST'.

If you press the OK button, the filename you entered will be used as a list file. If you press the CANCEL button, the filename you entered will be discarded, and the filename you saw when you first opened this dialog, will be used.

The TbClean|Options ***submenu***

Use TBAV.INI file

By enabling this option, the TbClean configuration values, saved in the TBAV.INI file, will also be valid when loading TbClean from the command line. Be careful, since options specified in the TBAV.INI file can not be undone on the command line. See chapter I-2 ('Configuration') of the manual.

Prompt for pause

TbClean will stop disassembling information after each full screen to let you examine the results.

Use Anti-Vir.Dat

If this option is deselected, TbClean will act as if there were no Anti-Vir.Dat records available and will therefore perform heuristic cleaning.

Use heuristics

If deactivated, TbClean will not use heuristics in the cleaning process.

Expanded memory

If activated, TbClean will detect the presence of expanded memory and will use it in heuristic mode. You may disable EMS usage if it is too slow, or if your expanded memory manager is not very stable.

Show program loops

By default TbClean keeps track of looping conditions to keep an iterati- on that would be emulated thousands of times from being listed on your screen. With this option TbClean 'works out' every loop. *Note that TbClean will perform at a drastically reduced speed. Do not combine this option with the 'list' option, because the list file might grow too big.*

Make list file

TbClean will generate an output file with a chronological disassembly of the virus being removed.

The TbUtil|System maintenance ***submenu***

This menu contains the actual TbUtil program. The program takes care of saving, restoring or comparing the system configuration of your PC. The backup system configuration is stored on a diskette in a file with either a default name or a name you can specify yourself.

Warning: You can only restore a system configuration datafile on the machine which created the datafile. If not, restoring such a file will make your PC inaccessible!

TbUtil data file pathname

With the 'Save' option, the system configuration is saved in a file. You can add a description to this TbUtil data file, which makes it easier to determine which datafile belongs to which machine.

Machine description

Enter a meaningful description of the machine. Enter something like "AT 12MHz, 4Mb, room 12, Mr. Smith". You do NOT have to remember it, TbUtil will display it on the screen when comparing or restoring, but it helps you to verify that the data file belongs to the machine.

Save system configuration

This option stores the partition table, bootsector and CMOS data area into the TbUtil data file.

Attention! *Since the PC is completely inaccessible to DOS if the partition table gets damaged, it is HIGHLY RECOMMENDED to store both the TbUtil data file and the program TbUtil.Exe itself on a diskette! It is not nice if the partition table is destroyed and the only solution to the problem resides on the same inaccessible disk...*

When loading TbUtil from the command line you must specify a filename after the 'store' option. Using the TBAV menu, you may use the default filename 'TBUTIL.DAT'. If you own more than one PC, it is advisable to create one TbUtil diskette with all TbUtil data files of all your PC's on it. Use the extension of the file for PC identification, eg.:

a:TbUtil.<number>

Compare system configuration

This option enables you to check on a regular basis that everything is still OK. If you specify this option TbUtil will compare the information in the TbUtil data file against the partition table, bootsector and CMOS data area. It will also show the comment stored in the data file. And of course, if you use this option you will also be guaranteed that the TbUtil data file is still readable.

Restore system configuration

This option enables you to restore the partition table, bootsector, and CMOS data area. It will ask you to confirm that the data file belongs to the current machine. Finally it will restore the partition table, bootsector of the partition to be used to boot, and the CMOS data area.

Process Partition code/Bootsector/CMOS memory

TbUtil will by default restore the partition code, bootsector and CMOS if option 'restore' is specified. If you use one of the above mentioned options in combination with the option 'restore' TbUtil will restore just the items specified.

Who are those guys ?

The ThunderBYTE Anti-Virus utilities were developed by ESaSS B.V., a Dutch company. The products of ESaSS B.V. are mainly related to the battle against computer viruses, but ESaSS B.V. also develops products in other areas of computer security. ESaSS B.V. has gained a lot of experience with and knowledge of viruses, assembler-written system software en personal computer hardware. Of course, ESaSS B.V. has a large collection of viruses to test their products on.

The ThunderBYTE Anti-Virus utilities were written by Frans Veldman. The TBAVWIN program was written by Bartjan Wattel.

How to contact ESaSS B.V.

The address of ESaSS B.V. is stated below. Frans Veldman can be contacted by email at `veldman@esass.iaf.nl` on the Internet. ESaSS B.V. can also be contacted at `100140,3046` at Compuserve, or on the Internet at `100140.3046@compuserve.com`.

ESaSS B.V.

P.O. Box 1380 Voice: +31 (0)80-787881
6501 BJ Nijmegen Telefax: +31 (0)80-789186
The Netherlands Support BBS: +31 (0)85-212395