

Panda Anti-Virus on-line documentation.

Click on any of the options in the following graphic to go to the corresponding subject.

If you want a quick help, click here to see the [main program window](#). From this window you can access all help chapters. Click on any of the buttons to go the corresponding help subject.



When this box is checked, only the boot sector of the selected drives will be scanned.

Select the drives to be scanned by clicking on them. You can also select all drives clicking on the corresponding box.

[Click here to get this help screen.](#)

This bar displays a brief description of the option the mouse cursor is currently on.

With the menu bar you can access the program's options and functions. It consists of a series of drop-down menus where you can select what you want to do.

Click on this button to erase the file name written in the file name box.

Select the drives in which to search by clicking on them. You can also select all drives checking the appropriate box.

This option returns you to the Search String screen, after saving your changes.

This button allows adding a new string to the list. Click on it to get a window that prompts you for the string to add.

This option returns you to the String Search screen discarding your changes.

This is the list of strings where you can select the ones you want.

This button allows changing the selected string. If several strings are selected, the last one selected will be opened for editing. After clicking on this button a window will be displayed allowing you to change the string.

This button removes the selected string from the list. If several strings have been selected, only the last one selected will be removed.

Check this option to select all strings in the list.

This button returns you to the Scan screen after saving your changes.

Use this button to add an extension to the list. After clicking on it, a window will be displayed that allows entering the new extension.

Click on this button to return to the Scan screen discarding your changes.

This is the list of file name extensions that you can select from.

Click on this button to remove the selected extension from the extensions list. If several extensions have been selected, only the last one selected will be removed.

This option allows specifying all extensions, not only the ones in the list. Checking this option, ALL files on the selected drives will be scanned.

Click on this button to erase the results report. The next operation after erasing the report will be the first one in the new results report.

Here you can see the results from the operations that you have performed with the anti-virus in the various Panda Anti-Virus sessions.

This option allows printing out the results report that you are currently viewing.

Select the drives to investigate by clicking on them. You can also select all of them by checking the corresponding box.

This displays the file name selected with the "Select File" option, but you can also directly type in the file name.

Click on this button to return to the previous screen saving the selected options.

If you activate this option, the automatic process will require no user intervention if it finds any incidence. It will instead wait until the end of the scan to report about the results. If the computer is infected in many places, this makes disinfection much easier.

If the anti-virus finds a virus it cannot disinfect and this option is checked, the program will delete the infected file.

If the anti-virus finds a virus and this option is checked, the program will delete the infected file.

Click on this button to return to the previous screen discarding the selected options.

If this option is activated, the anti-virus will scan inside compressed file archives.

If this option is activated and a virus is found, the program will disinfect it.

If this option is activated, the program will enter the subdirectories contained inside the selected directory. If you select a whole drive and this option is deactivated, only the root directory of the drive is scanned.

Activate this option to have the scan results logged into the results file, so they can be later viewed through the "Reports" option.

If the anti-virus finds a virus and this option is checked, the program will not allow disinfection.

This option allows entering a message to be displayed when a virus is found. It is useful where an additional action is necessary upon a virus being found (e.g. "Please contact the system administrator").

If the anti-virus finds a virus it cannot disinfect and this option is checked, the program will rename the infected file to the .VIR extension.

If the anti-virus finds a virus and this option is checked, the program will rename the infected file to the .VIR extension.

Click on this button to return to the Investigation window after saving your changes.

Click on this button to return to the Investigation window without saving your changes.

If you check this option, the anti-virus will warn you each time it finds a compressed file archive. A compressed file archive could contain a virus in the files in it.

If you check this option, the anti-virus will warn you about all files it finds with impossible dates and/or times. Viruses usually mark infected files this way so as to avoid re-infecting them.

This three options allow choosing the degree of sensitivity of the heuristic analysis.

If this option is activated, the anti-virus warns you each time a vaccinated file is found. This allows not confusing viruses with vaccines, that have a similar program behavior (in spite of the opposite intentions of both).

The status bar offers a short help line about the program option the mouse or cursor is on.

The menu bar contains a series of drop-down menus that offer all program actions and options.

Click on this button to exit the program.

Click on this button to cancel the scan operation.

This indicates the directory currently being scanned.

This displays the action that is currently taking place.

This displays the name of the file being scanned.

Click on this button to momentarily pause the scanning process.

This displays the percentage of the scan already performed.

This indicates the drive currently being scanned..

This indicates the number of viruses found and the number of viruses removed.

This indicates how many files have been found that contain one or several of the specified strings and how many strings have been found.

Click on this button to cancel the search operation.

This indicates the directory being searched for the specified string or strings.

This indicates what is currently being done.

This indicates the name of the file in which the specified string or strings are being searched.

Click on this button to momentarily pause the search operation.

This indicates the percentage of the search that has already been done.

This indicates the drive in which the specified string or strings are being looked for.

Click on this button to cancel the heuristic analysis operation.

This indicates which directory is being analyzed using heuristic techniques.

This indicates what is currently being done.

This indicates the name of the file that is being analyzed with heuristic techniques.

Click on this button to momentarily pause the heuristic analysis operation.

This indicates the percentage of the heuristic analysis that has already been performed.

This indicates the number of suspicious files found.

This indicates the name of the drive being scanned with heuristic techniques.

Click on this button to return to the previous window accepting the directory selection done.

This displays the currently selected directory.

Click on this button to return to the previous window without accepting the selected directory.

Click on the desired directory to select it. If the selected directory has subdirectories, they will then be displayed. Click on [..] to return to the previous directory.

You can specify any directory on any drive. Use this drive list to select the desired drive.

Click on this button to return to the previous window after selecting the desired file.

Click on the desired file in this list to select it.

Click on this button to return to the previous window without selecting the file.

This displays the directory tree of the selected drive. Click on the directory you want to select. When changing directories, the file list will also change accordingly.

Here you can enter the name of the file to be selected. If you select the file name in the file list, its name will appear here.

This option allows accessing your network. This button will not be displayed if there is no network installed.

This allows selecting the type of files that will be displayed in the file list.

This allows selecting the desired drive. When changing drives, both the directory list and the file list will change accordingly.

Click on this button to get detailed information about the virus selected in the list.

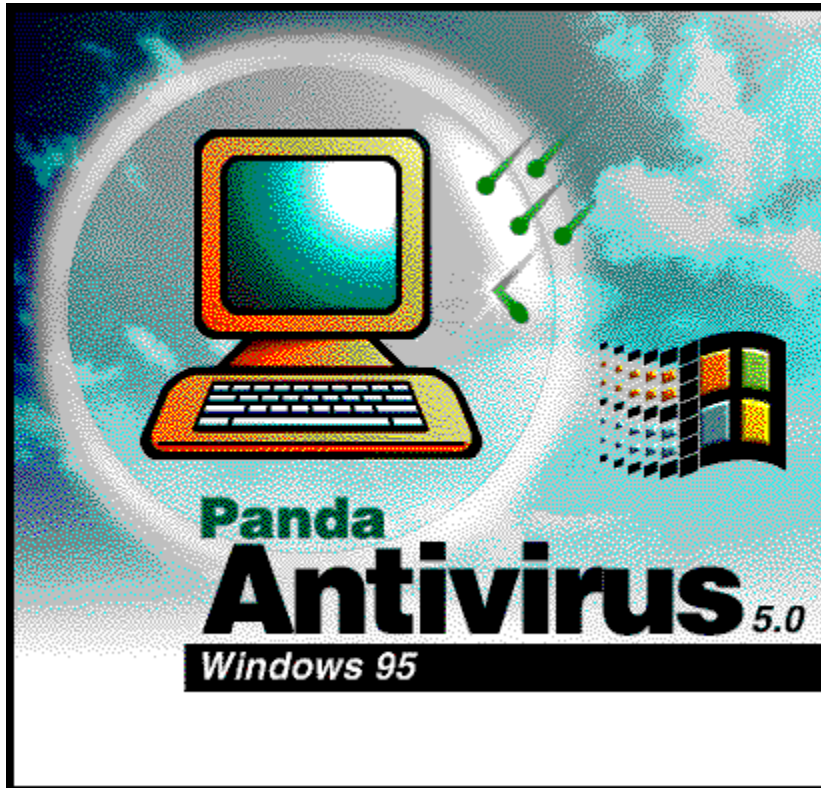
This is the list of viruses recognized by Panda Anti-Virus. For each virus you can see its name and size.

This allows entering the name of the virus to find. As you type letters of its name the list will advance to the most similar name in the list, starting with these letters.

Click on this button to return to the main Panda Anti-Virus screen. The selected options, if any, will not be lost.

About.

This window invites you to register. After registering you will be able to use our client service and you will also receive timely information about updates.



Start Scan.

This button starts scanning with the selected options. After clicking on it, the scan status window will be displayed.

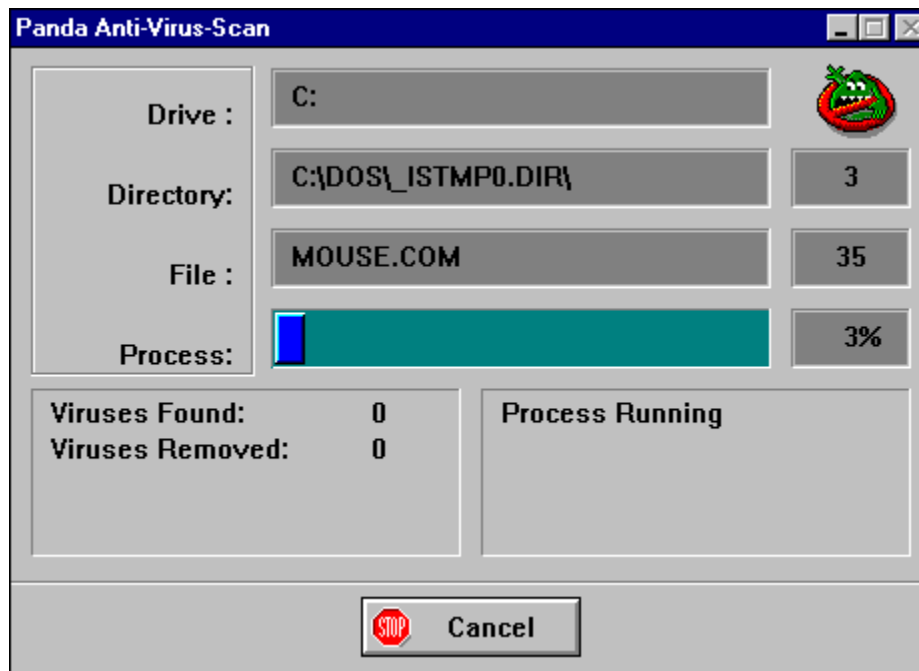
During this process Panda Anti-Virus will scan the areas you selected, searching for viruses. This is the most usual scan option and with it Panda Anti-Virus will search for any of the viruses it knows about. This scan allows disinfecting the viruses found.

Independently from the extensions you add to the search, files with .COM and .EXE extensions will always be scanned.

If you select the option of scanning inside compressed file archives, Panda Anti-Virus will scan all files that are located inside the compressed archive, as if they were regular files.

We recommend you scan all your computer's drives regularly (about once per month). You should also scan all programs that your are going to install, both the installation diskettes and the program itself once it has been installed onto the hard disk.

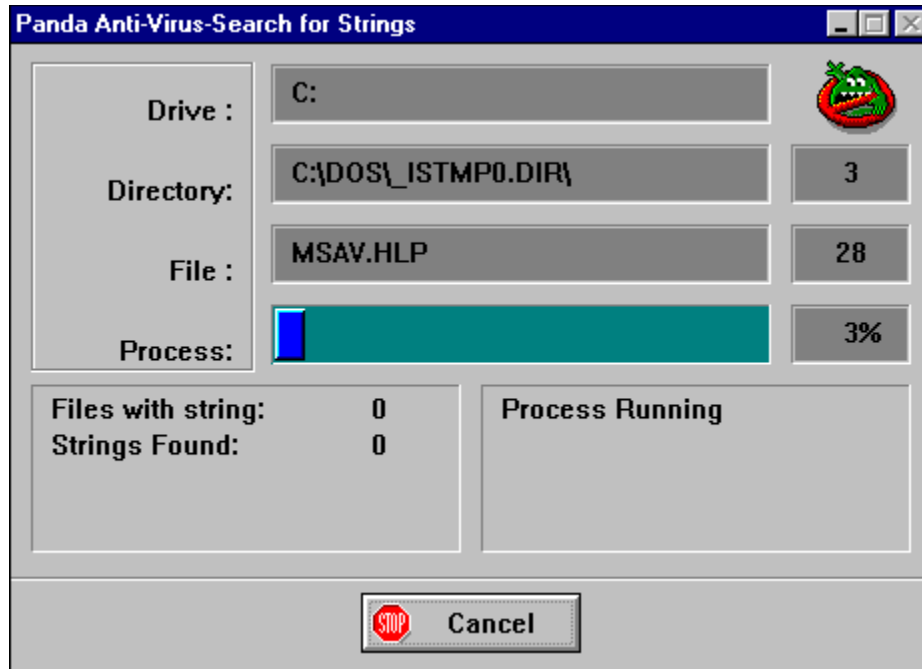
The scan status screen comes next. Click with the mouse to see a description of its components.



Start Search on Disk.

Click on this button to start searching for the selected strings on disk. After clicking on it, the disk search status screen will be displayed.

Next comes the disk search status screen. Click with the mouse to see a description of the window's components.



Start Search in Memory.

This button starts searching for the selected strings in memory. After clicking on this button, a bar will indicate the percentage of the task that has already been completed and afterwards a partial results window will be displayed, that then allows accessing the program results window.

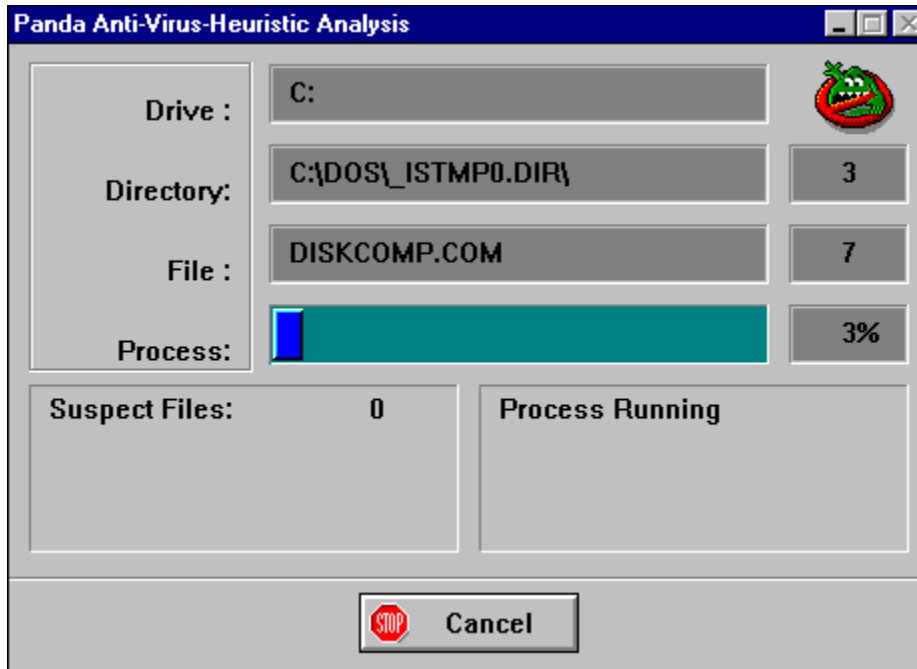
Next comes the partial result window for searching in memory.



Start Investigation.

This button starts the investigation process using the selected options. After clicking on this button, the investigation status window will be displayed.

Next comes the investigation status window. Click with the mouse to see a description of any part of the window.



Updates.

Every day new viruses appear on the scene, and if anti-virus programs are not updated regularly, they will not be able to detect and remove them. Therefore, it is vital to have a permanent anti-virus update service, to always be protected.

You can get a periodic update service directly from Panda Software. This service gives you the possibility to have your anti-virus constantly being updated.

Just for registering, you will receive timely information about new versions of Panda Anti-Virus.

Ñeàìèðíààìéà.

Ìðè íàæàðèè èíííè "Ñeàìèðíààìéà", ìíγàèγàòñγ íàìρ ñeàìèðíààìéγ. Ñeàìèðíààìéà - γòì ìñííáíγ è íàèáíéää +àñòì èñííèγçòáíγ ðóíèðèγ Àìèèèðòñà Ìáíàà. Ñeàìèðíààìéà ñçíà+ààð èññeàáíààìéà Ààøááí èíííòρòàðà ñ òàèòρ àùγñíèðòù, íà çàðàæáí èè ìí àèðòñíì.

Àñòù ààà ààðeàíðà àíñòòíà à ðàæèì ñeàìèðíààìéγ. Àù ìíæàðà íàæàðòù íà èíííèò "Ñeàìèðíààìéà" à èííí+ííé çííà èèè àùáðàòù ììèèρ "Ñeàìèðíààìéà" à çííà ìáìρ.

Àìèèèðòñ Ìáíàà ìðááìðèíèìààð ñeàìèðíààìéà ìáìγðè ðíèùèí ìðè ìà+àèà ðááíðòù àèγ ðíáí, +òíáù òáíñòòíààðèòùñγ à òíì, +òì ìðìðáññ ñeàìèðíààìéγ ìíæàð àúòù ìñòùáñòàèáí ááç ìíáð ìí àèíà àèðòñà.

À γòì ìéíà Àù ìíæàðà àùáðàòù ðíð àèñé, èìðìðúé Àù àèèèààðà ìíàáàðáíòòù ñeàìèðíààìéρ. Àù ìíæàðà òàèèà àùáðàòù àèγ γòíáí àèðàèòìðèρ èèè ààæà ìòáàèùíúé òàèé.

Àìèèèðòñ Ìáíàà ìðáàèèàááàð Àáì áàà ðèíà èññeàáíàíéγ ñeñòáíù. Òì ñeàìèðíààìéà, ì èìòìðì Àù ñáé+àñ +èðáàðà - γòì ìáù+íúé ìðìòáññ, ììèì èìðìðíáí ñòùáñòàóáð òàèèà γáðèñòè+áñéíà èññeàáíààìéà.

Àìèèèðòñ Ìáíàà áñáááà ñeàìèðòáð òàèéù ñ ðáñòèðáíéáì .COM è .EXE. Àù ìíæàðà òàèèà ìáíçíà+èòù àðòáèà ðáñòèðáíéγ è ììèè ñeàìèðíààìéγ, à òàèèà, ìðè ìáíáðíàèìñòè, òéàçàòù, +òì Àù ðìðèðà ìíàáàðáíòòù ñeàìèðíààìéρ èèòù ìáèáñòù ìà+àèùííé çàððòçèè.

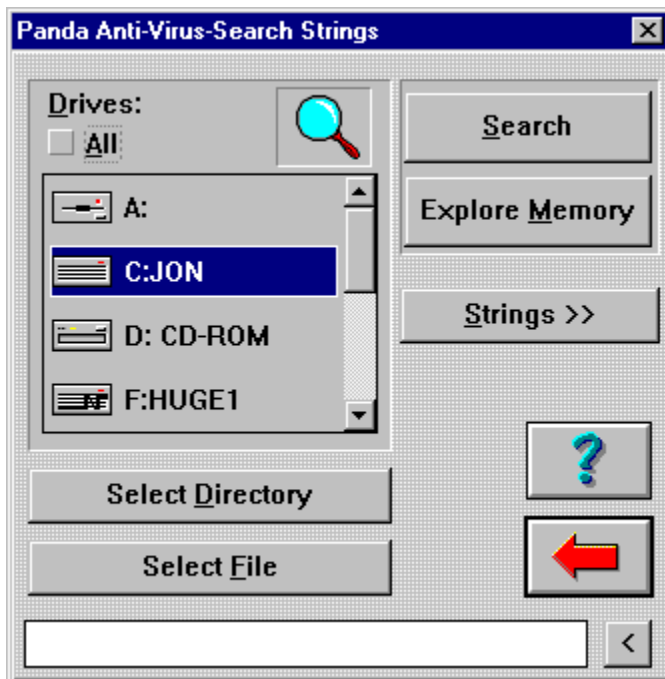


Search.

This option allows searching for a certain string in memory or in any of the disk drives. You can search for any string, but the goal of this option is searching for strings given by our technical service to identify new viruses not yet recognized by this version of Panda Anti-Virus.

Click on the "Search" button to display the search window. From this window you can select the drive or drives in which to search. You can also select a directory or even a specific file to search on it.

The search window can also be accessed both clicking on the "Search" button in the button bar and selecting the "Search for String" option in the "Investigation" menu from the menu bar.



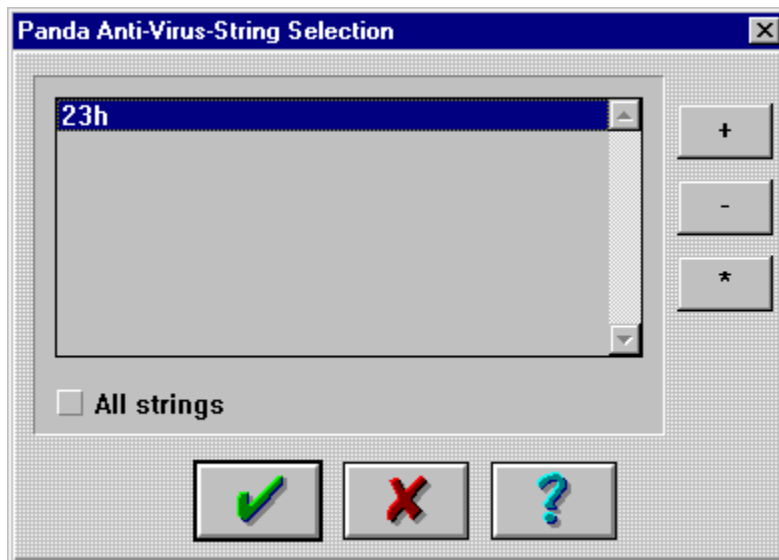
Selecting Strings.

The search for strings is an accessory function that allows simultaneously searching for one or several strings in memory and also in any of the files on your disk drives.

Strings can be specified in ASCII, decimal or hexadecimal. Numbers entered are presumed to be decimal. To specify a hex number, just add an "h" after it.

You can search for any string you want, but this function is normally used in conjunction with some string provided by the Panda Software technical service, so as to identify viruses that are unknown to this version of Panda Anti-Virus.

Once the string (or strings) has (have) been selected, you can specify, in the search window, where to look for it, if on disk (search) or in memory (explore memory).



Load Configuration.

This option allows loading all program options that were previously saved into the configuration file.

Extensions.

This window allows selecting which files the anti-virus should scan, by selecting the file name extensions of the files to scan. The anti-virus always scans files with .COM and .EXE file name extensions.

To select the additional files types to be scanned by the anti-virus, click on the desired file name extensions. The selected extensions indicate which files will be scanned.

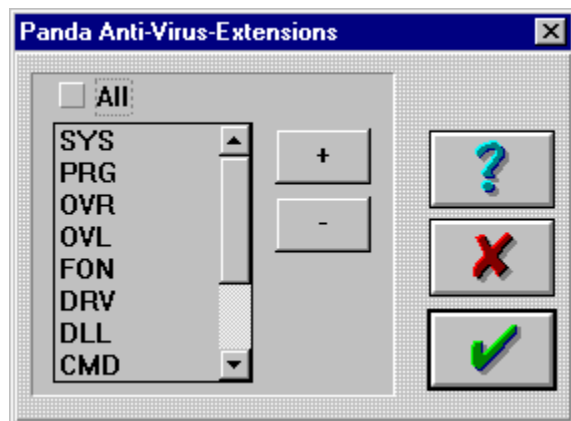
To deselect an extension, just click on it again.

Please remember that you can select all extensions in the list by clicking on the "All" option. A check mark on it indicates that this option is active.

If you want to add an extension to the list, click on the "+" button. A window will be displayed prompting you for the extension. Once entered, the new extension will have been added to the list.

To remove any extension from the list, click on it and press the "-" button. The extension will then be removed from the list.

The new extensions list (if you have modified the original one) will automatically be saved and the anti-virus will from that moment on operate with the selected extensions, until you change them again.



HOTLINE and Virus SOS services.

What is the HOTLINE?

The HOTLINE service is a personalized technical support service. If you have any problem regarding computer viruses, real experts with much experience will help you for free, just for being registered.

How can I register?

To register you only need to send us the registration card with your data on it.

What should I do before calling?

Before calling, you should have read all documentation, both the written one and the on-line documentation you are currently reading. Many problems can be solved just by reading the documentation.

If you cannot solve your problem from the documentation, please have the following information ready before calling:

- Type and make of the computer you have: processor, video card, installed peripherals, if you are connected to a network, ...
- Operating system version.
- Available memory. (from the MEM command).
- Space available on disk (gotten with the DIR command)
- Contents of the AUTOEXEC.BAT and CONFIG.SYS files.
- Recovery diskette or boot diskette.
- DPS utility program.
- Manual of the Panda Anti-Virus.

You should be close to the computer when you call us, so you can follow our expert's instructions directly.

Then explain the problem in detail, indicating the steps you did to get it. Describe as exactly as possible what you observed, avoiding as much as possible giving the technician your interpretation, as this may mislead him. If you found a virus, note the name of the virus and the file where it was found. Take note of all possible details, so that it is easier for us to help you.

How can I contact the HOTLINE?

You can contact the HOTLINE by phone, fax, mail, through the Panda Software BBS or through our Internet Web Site.

Consult your manual for more information.

What is the Virus SOS service?

If you find a virus that the current version of Panda Anti-Virus does not detect, you can send us the file with the virus for a detailed study. If it is a new virus, we will send you a revision of the program

that detects and disinfects the new virus.

Before sending a file you suspect contains a virus, you should contact our technical service to learn about the possibility of it really being a virus and, in that case, how to capture it to diskette.

In 24 HOURS we will send you the updated version.

Language.

This option allows specifying the (human) language used by the program. The window displays all available languages. When selecting one of them, this language immediately becomes the active one.



Virus List.

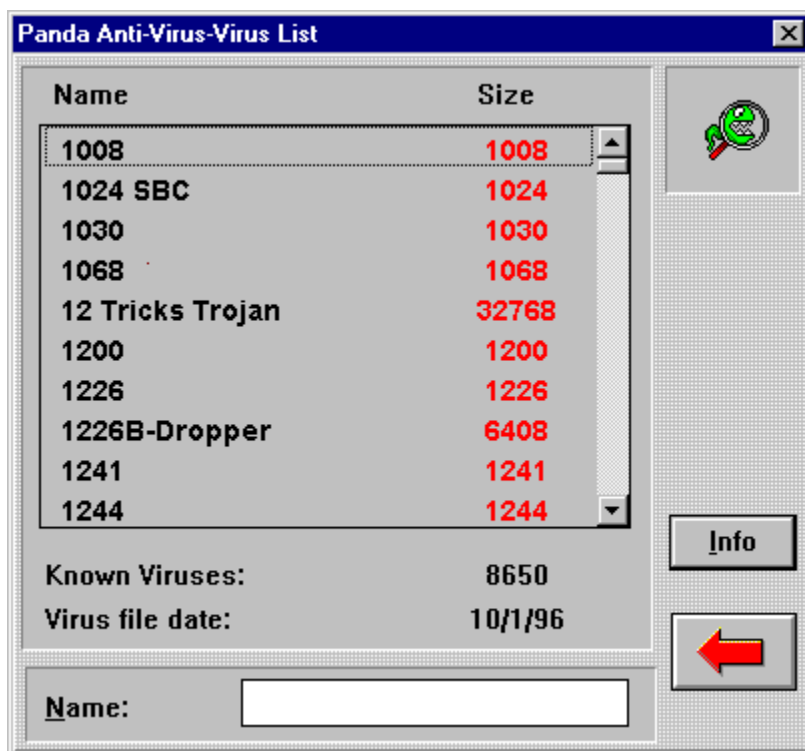
This virus list is an alphabetically ordered list of all viruses that are recognized by the current version of Panda Anti-Virus.

There are two ways to access the virus list. You can click on the "Virus" button in the button bar or select "Virus report" from the "File" menu in the menu bar.

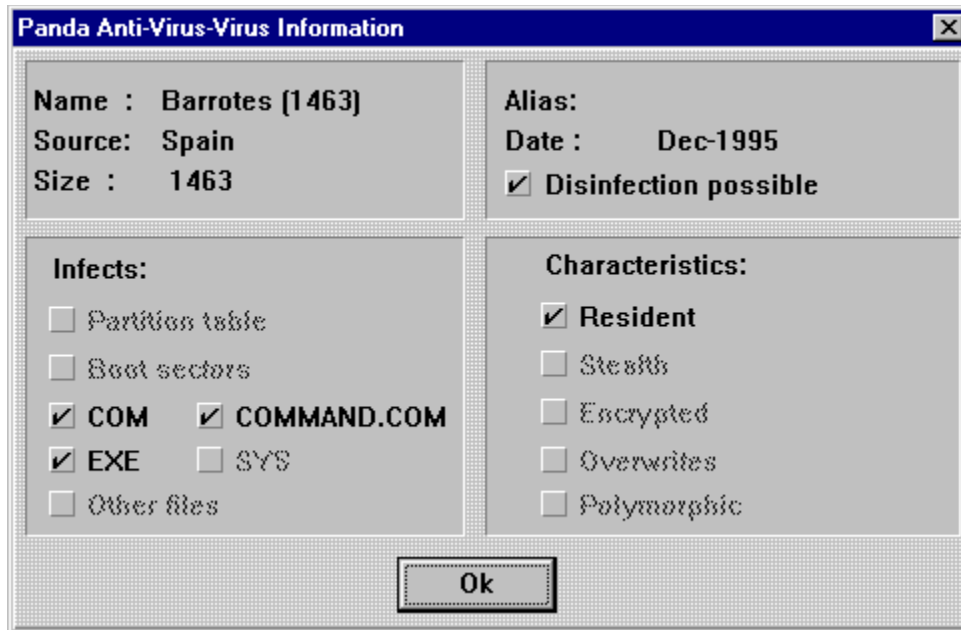
Each of the entries in the list displays the common name for the virus and its size. To get more information on a specific virus, just press the "Info" button or double-click on the virus name.

The detailed information consists of: the alias, country of origin, date it appeared, size in bytes, if Panda Anti-Virus can disinfect it, areas it infects and advanced virus characteristics.

There are two ways to search for a specific virus. Pressing the initial of the virus, the list will jump to the first virus whose name starts with that letter. From that point on you can finish looking for it. The second way consists of positioning the cursor into the blank editing field in the lower part of the window and start typing in the virus name. As you enter the name, the list will keep advancing to show you the option that best suits your entry up to that moment.



The following screen is an example of the information that is displayed when clicking on the "Info" option in the virus list.



The following gives a detailed description of all characteristics a virus can have:

- **Resident:** When run, the virus reserves a small amount of memory to install itself into it and infect from there.
- **Stealth:** This is a technique some resident viruses use, which consists of hiding the changes the virus makes to the files it infects. When someone tries to get one of the characteristics of the file the virus has modified, the virus, being resident in memory, intercepts the call and returns instead the data previous to the change.
- **Encryption:** The viruses that have this characteristic are capable of encrypting themselves in a different way each time they infect a file. Therefore, the virus cannot be found with a string search. Luckily, the virus needs a decryption routine and this always has to be the same. Therefore the virus can be identified by its decryption routine.
- **Overwrites:** Viruses that overwrite, resident or not, overwrite the file they infect. This file is then therefore unusable. The file size does not change, unless the size of the virus is greater than the size of the file. The only way to disinfect these viruses is to erase the infected file and substitute it by a non-infected copy of it.
- **Polymorphic:** Polymorphic viruses are advanced versions of encrypted viruses. Polymorphic viruses are able to change the encryption method from generation to generation. Therefore, no part of the virus remains unaltered. What is then needed is an algorithmic search method for each of these virus "races."

Internet.

Sentinel VxD allows you being protected against viruses that might enter through the Internet.

If you receive from the Internet an executable file, a compressed file or a file whose file name extension is in Sentinel's list of extensions to scan (e.g. DOC files), Sentinel VxD will scan it immediately, warning you if a virus is detected.

If, for example, you receive a virus-infected e-mail message, Sentinel VxD will not detect the virus when the e-mail is received, but when you try to open or manipulate the file you have received via e-mail.

With **Panda Anti-Virus** your are always protected against viruses, even from the Internet.

Investigate.

The investigation option allows performing an heuristic analysis that allows detecting new viruses, that are not yet being recognized by this version of Panda Anti-Virus. The heuristic analysis complements the regular scan.

You can access the investigation screen either by clicking on the "Investigation" button in the button bar or selecting the "Unknown Virus" option of the "Investigate" menu in the menu bar.

This very powerful tool detects all files that have virus-like characteristics. Therefore, it is not completely infallible and can indicate a file as suspicious, while it is not really infected. Using the various options, you can set the analysis sensitivity to a minimum, intermediate or maximum level.

The heuristic scan recognizes common virus characteristics, but does not look for a specific virus. Therefore, if the heuristic analysis detects a virus, it will not be able to disinfect it.

The heuristic method can indicate several grades of virus suspicion. If it indicates that a file is "very suspicious" it most probably is virus infected. It is normal to find one or two files that are minimally suspicious, and that does not indicate a virus presence. But if many suspicious files are found, it is a sign that a virus may have infected them.

In the options part you can also select the events you want the program to warn you about. These can be:

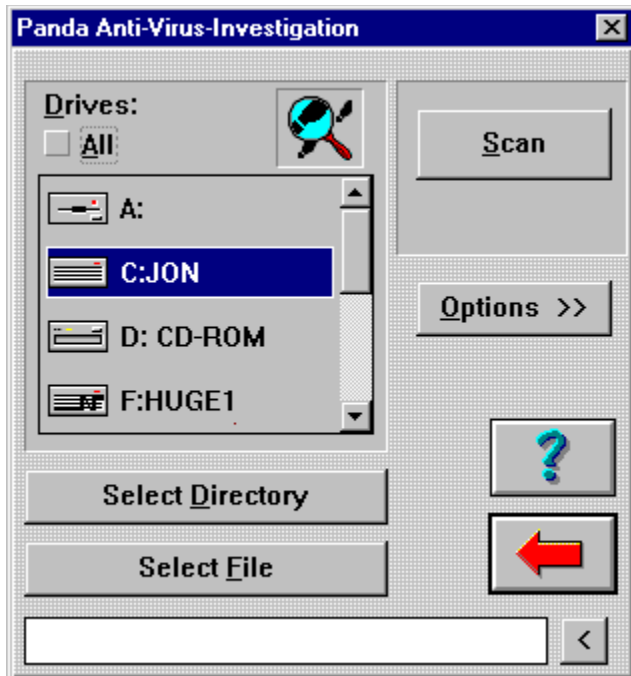
- Incorrect dates and times.
- Compressed files.
- Vaccinated files.

Changed dates and times are usual signs of virus presence. The change consists of setting the date and/or time to an impossible value. Viruses usually tag files this way to know that they have already been infected and to avoid infecting them again.

The warning about compressed files is interesting as it tells the user about the possibility of this compressed file archive having a virus in some of the files it contains.

The warning about vaccinated files is important, so as not to confuse this files with virus infected files. This is due to the fact that vaccines, protections against viruses, behave in part as the viruses themselves.





Button Bar.

Description.

The button bar is an easy to use graphical user interface element that provides a fast access to the main functions of Panda Anti-Virus. These same functions can also be accessed through the program's main menu.



Introduction.

What is a virus?

A virus is a computer program that installs itself into the computer without user knowledge and without his consent, so as to perform a series of actions that are damaging to the computer.

This program spreads to all programs on the hard disk of the infected computer and to the diskettes used while the virus is active. In this way, through diskettes is how the virus propagates to other computers. It can also infect other computer through any of the PC's input/output ports, as the serial port (if the computer is connected to other computers through it), a modem or a network.

As a virus is a computer program, it can only start acting and infecting when the computer is running.

What can a virus do to your computer?

The two most important actions of a virus in a computer are: infecting and destroying.

Virus infections follow a geometric progression, so that in very little time (hours, but sometimes minutes or even seconds) all your computer can be infected.

The destructive activities of a virus always target the hard disk. They can inhibit all user access to the hard disk or corrupt the data it contains or erase it totally or in part.

Additionally, viruses try to hide from anti-viruses and occasionally perform some other non-destructive activities aimed usually at drawing the user's attention to the fact that they have infected the computer, as beeps, strange messages, music or strange behavior on screen.

What is an anti-virus?

An anti-virus is a program that has three basic goals:

- Detecting the presence of viruses in files.
- Disinfecting all files that contain viruses.
- Protecting the computer against future virus attacks.

What is Panda Anti-Virus ?

Panda Anti-Virus is an anti-virus program, the result of years of development by a very experienced team of programmers. Its goal is keeping your computer safe from the various type of viruses that exist, preventing them from infiltrating your computer and removing them if they succeed in it.

Panda Anti-Virus is one of the best virus detection and removal programs on the market, but you still have to remember that you need to be cautions with the diskettes you receive. Remember that before installing a program onto your hard disk, you should scan all diskettes it comes on with Panda Anti-Virus. Once the program has been installed, scan again the program in its installed location on the hard disk. Also remember to periodically scan your computer with Panda Anti-Virus. This is the only way to keep your system virus free.

We hope you will like this product and it will help you keep your computer safe and virus free.

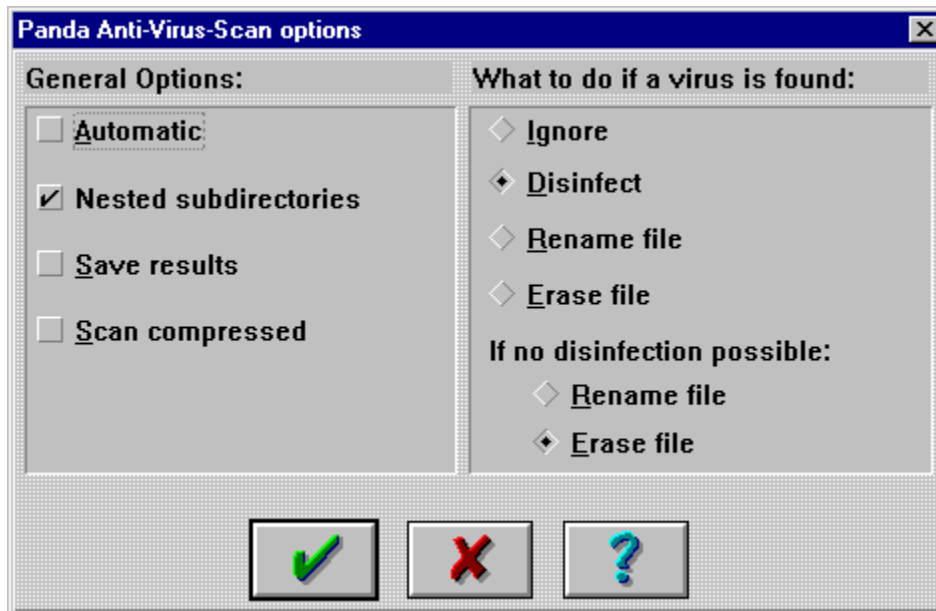
Scanning Options.

This window allows selecting the desired scan options. To get detailed information on any of these options, please click on it below.

To activate an option, click on it. Then the small box next to the option will have a mark to indicate that it is active.

To deactivate an option, just click on it again. The mark in the box will disappear to indicate that the option is deactivated.

Remember that you can save your desired option configuration selecting "Save Configuration" in the Configure option of the main menu.



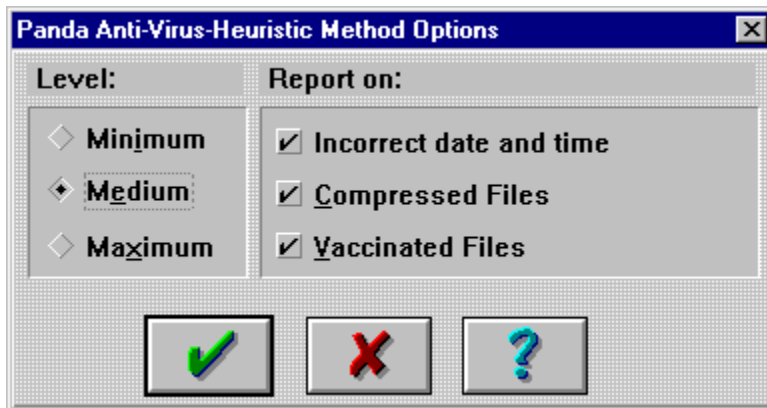
Investigation Options.

This window allows selecting the desired investigation options. To get detailed information on any of these options, click on it below.

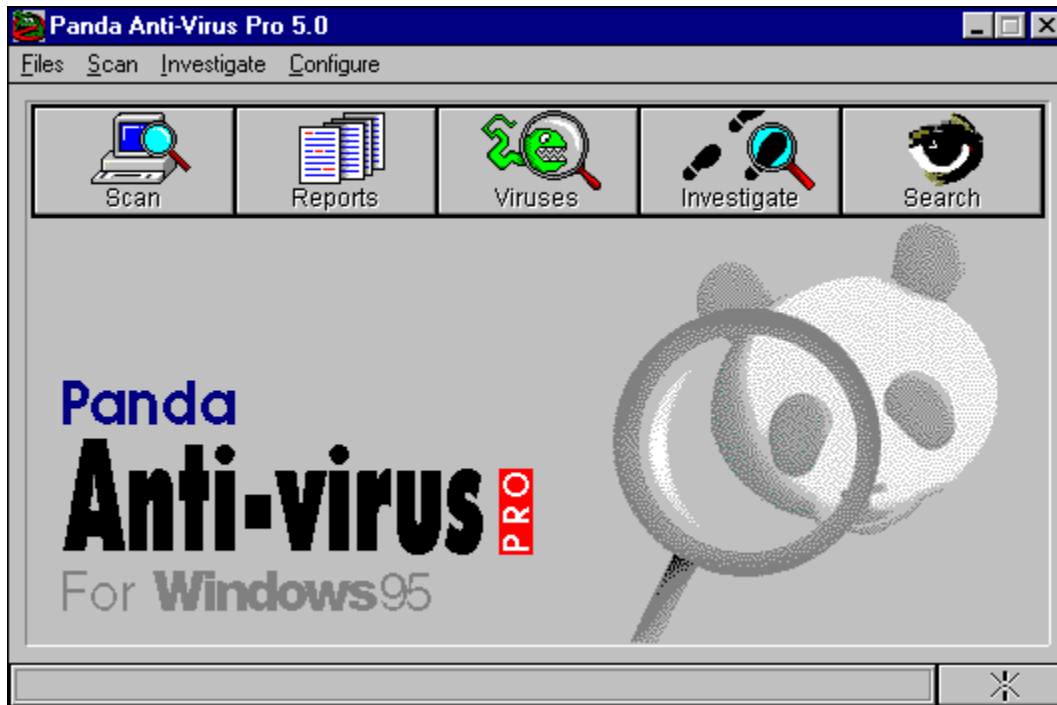
To activate an option, just click on it. This will put a mark into the box next to the option, to indicate that it is now active.

To deactivate an option just click on it again. The mark in the box will then disappear to indicate that this option is now deactivated.

Remember that you can save the desired option configuration selecting Save Configuration in the Configure option of the main menu.



Main program window.



Answers to frequently asked questions.

Can an anti-virus damage my computer?

An anti-virus is a complex program. Under certain circumstances and if the manufacturer's recommendations are not followed, it could damage your data. With Panda Anti-Virus the possibility of this occurring are nearly non-existing and when there is a greater risk, the program will warn you about it.

Older anti-viruses or those of dubious origin can more easily have this problem as they usually do not know the most recent viruses that use more elaborate techniques and which are more difficult to remove.

There is also the danger of variants of known viruses that have changed their behavior.

Answers to frequently asked questions.

What does the "BOOT sector write" message mean? The BIOS anti-virus protection.

The "BOOT sector write" or similar message means that an attempt has been made to write to the hard disk's boot sector. This message is not generated by the anti-virus, but by a write protection built into some BIOS that can usually be activated or deactivated from the computer's SETUP.

This does not necessarily mean that there is a virus trying to penetrate the system, but that an attempt has been made to write to the BOOT. The agent writing to the boot can be a virus, a regular program, as the DOS FORMAT or FDISK programs, or the anti-virus itself. This message should therefore be interpreted with caution as it often does not indicate a virus presence.

Answers to frequently asked questions.

What to do if there are errors disinfecting the BOOT

In these cases, use the /BTA and /MBR parameters of PAVCL.EXE.

These parameters should only be applied if there are problems disinfecting BOOT viruses.

Sometimes a BOOT virus cannot be disinfecting, because the original BOOT sector cannot be located, because it is defective or because the disk reports a read error. This can also be due to a bad disinfection of the virus or to the original BOOT not being correct when the infection happened.

The problem of not having the original BOOT also happens under other circumstances. When this problem happens on a diskette, the solution is quite easy: saving the files on the diskette to some other medium, usually the hard disk, formatting the diskette and copying the previously saved files back to the original diskette. No copy should be made using the DISKCOPY or any other disk duplicating command, as the virus would also be duplicated by this process.

There is no danger in working with or copying files to a diskette that is infected with a BOOT virus. You only have to be careful not to leave the diskette in the diskette drive when rebooting or when switching on the computer, so it does not try to boot from it. The moment it did, the virus would be activated and would infect the system, even if the diskette is no boot diskette.

There are some PAVCL.EXE parameters that allow overwriting any virus that is located in diskette BOOT sectors of or in the hard disk's Master BOOT. When being overwritten with some other program, the virus disappears. It is then replaced by some generic boot sector that allows removing most viruses, even if they have not yet been catalogued.

These parameters are:

/BTA	For diskettes (use /BTB for drive B:)
/MBR	For the hard disk's partition table.

Answers to frequently asked questions.

Should all extensions be scanned or only executable ones?

Ideally, all extensions that the anti-virus offers by default should be scanned, as viruses only infect executable files. The option of scanning all extensions allows scanning all files, as there can be executable files with a non-standard extension or data files that are really renamed executable files.

It is also recommended that you scan all file name extensions when the disk is infected and then has to be disinfected.

Answers to frequently asked questions.

What about files with strange dates and/or times?

Some viruses change the date and/or time of the files they infect to impossible values. In this way the virus tries to identify files that have already been infected.

The anti-virus offers the possibility of searching for these suspicious dates, which are an important hint for discovering new, as yet uncataloged viruses.

There can be however other causes for a file to have a changed date or time, without virus intervention.

- It can have been set by the program's manufacturer.
- The user can have changed it with a utility program.
- If the date is wrong when a file is written, DOS will stamp it with that wrong value.

The appearance of several executable files with changed dates should be considered specially suspicious, specially if they were correct before.

Answers to frequently asked questions.

Can a system be completely immunized against viruses?

It can be immunized partially. A total immunization is impossible, as a virus could always be manufactured that eliminated the protections. However, the task of preparing this type of virus is such that in general it can be said that an immunizer can be built that is effective in a very high percentage of cases.

Answers to frequently asked questions.

What is the worst a virus could do?

Undoubtedly, the most destructive operation a virus could perform is formatting the computer's hard disk. This means losing millions of bytes that could represent months worth of work. Restoring the contents of a formatted hard disk is very costly and sometimes even impossible.

Answers to frequently asked questions.

How many PC viruses are there currently?

New viruses are continuously being created and not all of them have yet been catalogued. Of course, not all of them have spread sufficiently to be considered frequent, but in any case, the number of viruses in the PC environment is immense and is growing day by day.

Answers to frequently asked questions.

Can viruses always be removed from an infected computer?

Yes, a hard disk can always be low-level formatted as well as all infected diskettes. The problem is that there is often data in infected areas, that needs to be saved.

Basically, if the infection is on an executable program, it just needs to be erased, as there should be backup copies of it. If the system boot has been infected, it can be replaced by a new one.

A file can also be disinfected, removing the virus, but respecting the file's data. This operation is not always successful, and sometimes creates unwanted secondary effects.

In some cases the virus destroys data or code in a way that does not allow it to be recovered.

Remember that the best security measure is keeping recent copies of all your important data and regularly scanning the whole computer with the anti-virus.

Answers to frequently asked questions.

Why do viruses stay resident?

A memory-resident program stays, to some extent, hidden to the user's view. The virus stays there, watching while the system operates and takes advantage of any occasion to infect another part of the computer and, in the worst case, to perform its destructive action.

The main reason for a virus to become memory resident is infecting more and "better".

Answers to frequently asked questions.

Viruses are found in memory but not on the hard disk. Why?

You may have previously run another anti-virus and pieces of its virus signatures may have remained in memory. Switch the computer off and back on to get rid of this message in this case.

This is due to some memory resident programs of certain anti-viruses leaving traces of virus signatures in memory. When another anti-virus is going to scan the memory, it find a series of "virus pieces" that are the signatures left over by the previous resident anti-virus. This creates false alarms.

In this case you would usually find many viruses in memory.

If they were real viruses, the system would not work at all, as the viruses would interfere with each other bringing the system to a halt.

In general, the simultaneous presence of many viruses in memory should be considered a false alarm due to the use of several anti-viruses or running an anti-virus several times in a row.

Answers to frequently asked questions.

How long do viruses take to reproduce themselves?

It depends only on the virus. In general, they try to infect as fast as possible, but in many cases they only infect under certain circumstances: specific dates or specific files. They also try to avoid infecting the same file more than once.

Answers to frequently asked questions.

Could a virus be manufactured that could not be detected by an anti-virus?

A virus can be manufactured that is very difficult to detect by an anti-virus. This is usually so due to the fact that anti-viruses suppose that the same virus always behaves in a similar way and specially, that its form is always the same. However, new viruses are appearing, that mutate while infecting. In this way they cannot be identified as known viruses. They can however be detected by other means, as by the Panda Anti-Virus Investigation Technique.

Answers to frequently asked questions.

Basic questions about viruses

[What is the worst a virus could do?](#)

[Why do viruses stay resident?](#)

[How long do viruses take to reproduce themselves?](#)

[How many PC viruses are there currently?](#)

[Can viruses always be removed from an infected computer?](#)

[Could a virus be manufactured that could not be detected by an anti-virus?](#)

[Can a system be completely immunized against viruses?](#)

[Can an anti-virus damage my computer?](#)

Questions about how the anti-virus works.

[Should all extensions be scanned or only executable ones?](#)

[What about files with strange dates and/or times?](#)

[Viruses are found in memory but not on the hard disk. Why?](#)

[What does the "BOOT sector write" message mean? The BIOS anti-virus protection.](#)

[What to do if there are errors disinfecting the BOOT](#)

Exit.

Select this option to exit the program. If you changed any of the configuration options, before exiting the program will ask you if you want to save your changes. If you choose to do so, the changes will be saved to the program configuration file. If you answer no, the changes will be discarded.

Remember you can also exit the program clicking on the button in the lower right corner of the main program window.



Save Configuration.

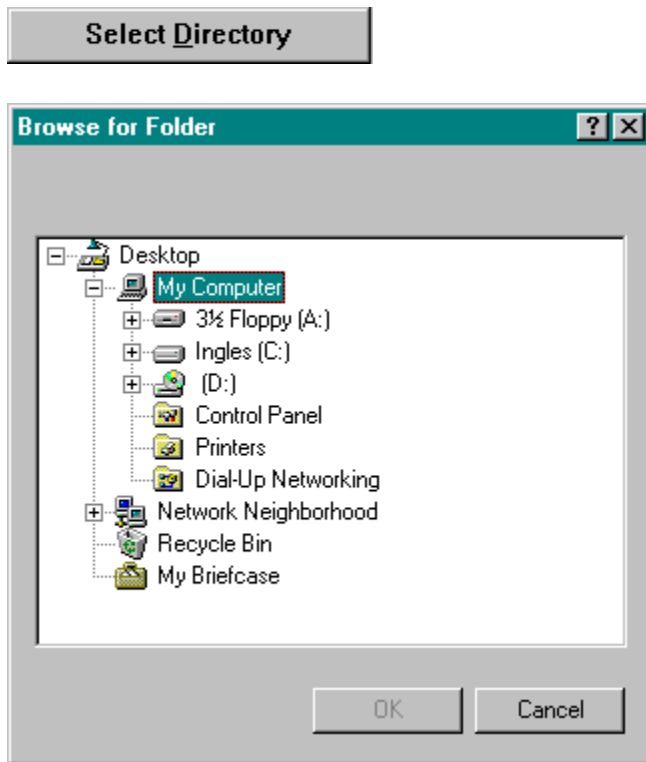
Allows saving all program configuration options into the configuration file.

Do not try to manually edit the program configuration file (with a .CFG extension). Any change to this file can produce unexpected results in the behavior of the application.

Select Directories.

This window allows selecting a specific directory.

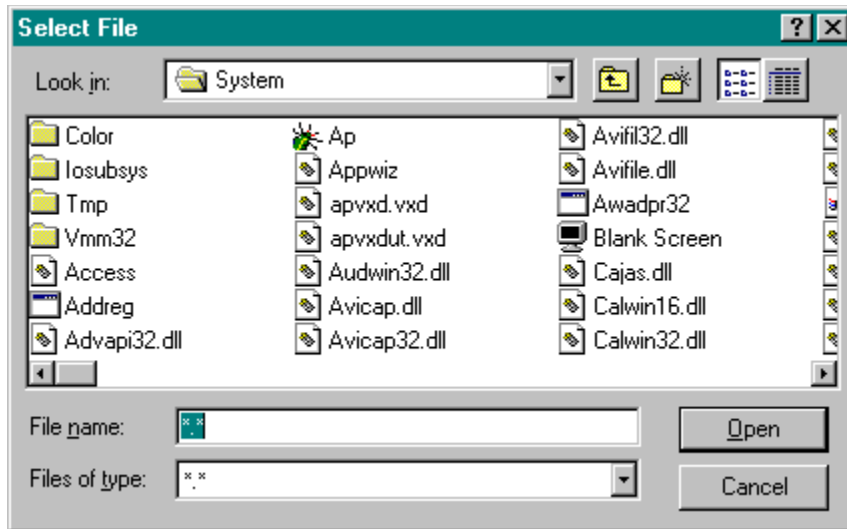
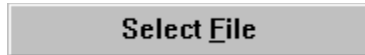
To select another drive, just click on it and then you will be able to browse all this drive's directory tree through a easy to use interface. The text box "Current directory" displays the current selection.



Select Files.

This window allows selecting a specific file.

To select another drive, just click on it and then you will be able to browse all this drive's directory tree through a easy to use interface. Once located on the desired directory you will be able to select the desired file.



Select Drive.

This option allows selecting the drives to use for a certain operation (scanning, investigation or searching). The program displays a list of all the drives available on the system. Just select the drives you want from this list.

You can select all drives clicking on the box next to the "All" option.

You can also deselect a drive clicking on it again.



Sentinel.

Sentinel VxD is a permanent watchman that supervises the operations performed on files in your operating system so as to detect viruses while you work with your programs.

Sentinel VxD is completely transparent to the user and prevents operations on infected files. When Sentinel VxD is active, virus infected files cannot be accessed. Sentinel VxD acts immediately and safely and never allows an infection or viruses moving through your system.

Sentinel VxD does not require user intervention to detect viruses, but it examines files while the user does his normal work with his applications.

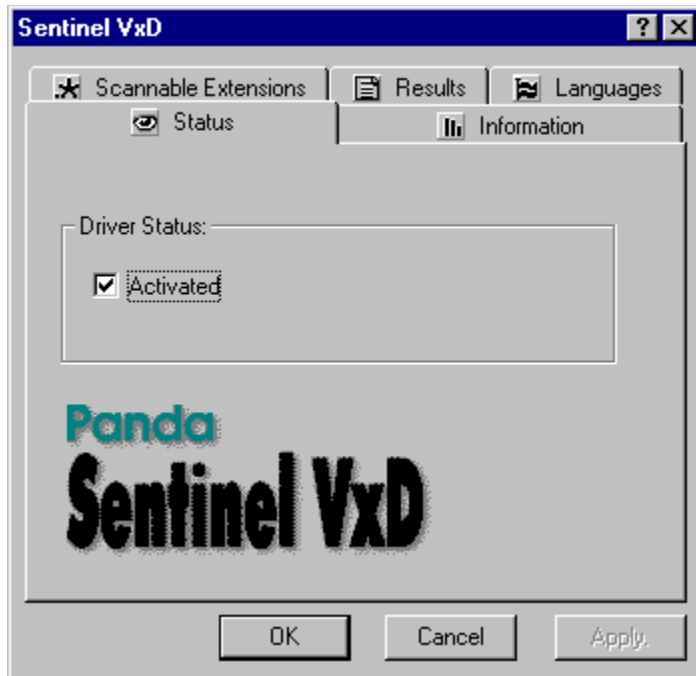
Sentinel VxD is able to detect a virus under the following circumstances:

- When a program is run.
- When a file is copied.
- When a file is moved.
- When a file is renamed.
- When a file is decompressed, whatever its compression format.
- When a file is downloaded through any communications line: a BBS, network or the Internet.
- When a file is infected by a memory resident virus
- When there is a virus in the boot of a diskette.

Sentinel is represented by the **Panda Software** icon in the taskbar. If the bear is white, Sentinel is active. If it is gray, it is inactive.



The following depicts the window that is displayed if you double-click on the Sentinel icon. On the various tabs you can configure the extensions, languages, the results file, etc.



You can activate, deactivate or eliminate Sentinel quickly using the right mouse button.

Symptoms that can indicate a virus presence.

- The computer becomes slower.
- The size of files grow.
- The available memory is reduced.
- Sometimes written messages appear.
- The system will not boot.
- The screen erases or is changed unexpectedly.
- Some files disappear.
- Some sectors or tracks on the disk are formatted.
- Some programs cannot be run any more.
- Music sounds unexpectedly.
- New files appear with the same name as other files.
- The space available on disk is reduced.
- Directories on disk appear to be damaged.
- Some files show information from other files.
- The system does not recognize a disk drive any more.

Result Report.

The result report is a document that displays a list of the various operations performed by the anti-virus, separated by lines. This allows keeping a convenient log of the operations performed with the anti-virus even over several sessions of using the program.

The result report can be accessed in two ways. You can click on the "Report" button in the button bar or select the "Results" option from the "File" menu in the menu bar.

You can also access the result report from the action window of any of the fundamental operations (scanning, investigating and searching).

For each operation, the date, time and type of operation is logged, as well as its scope. The result and incidences (e.g. if viruses were found and where) are also logged.

This document is conserved between the various executions of the anti-virus. All operations performed by the anti-virus are chronologically logged into this file.

This file can be viewed at any time. It can also be printed out and deleted. If the file is deleted, the next anti-virus operation will be the first one to be logged into the new report file.

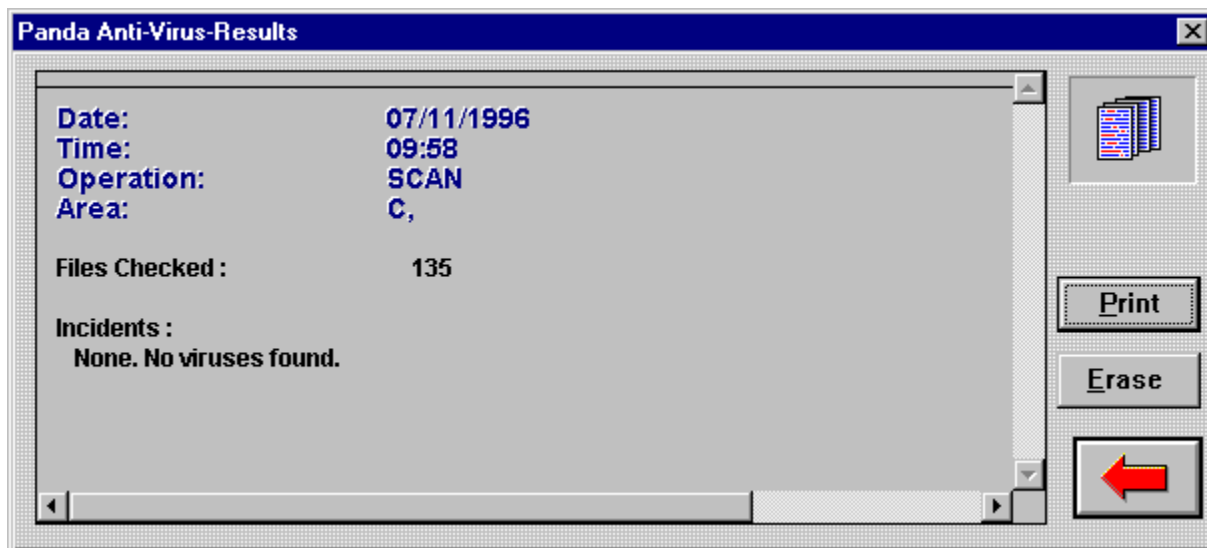


Table of Contents.

This tree represents the structure of the on-line manual. Click on each main option to drop down its contents and then click on any issue to get the corresponding help.

- [+ Introduction.](#)
- [+ Button bar.](#)
- [+ File Menu.](#)
- [+ Scan Menu.](#)
- [+ Investigation Menu.](#)
- [+ Configuration Menu.](#)

Table of Contents.

This tree represents the structure of the on-line manual. Click on each main option to drop down its contents and then click on any issue to get the corresponding help.

- [Introduction.](#)
- [Introduction.](#)
- [Button bar.](#)
- [File Menu.](#)
- [Scan Menu.](#)
- [Investigation Menu.](#)
- [Configuration Menu.](#)

Table of Contents.

This tree represents the structure of the on-line manual. Click on each main option to drop down its contents and then click on any issue to get the corresponding help.

- [+ Introduction.](#)
- [+ Button bar.](#)
- [+ Description of the button bar.](#)
- [+ Scan.](#)
- [+ Reports.](#)
- [+ Virus.](#)
- [+ Investigate.](#)
- [+ Find.](#)
- [+ File Menu.](#)
- [+ Scan Menu.](#)
- [+ Investigation Menu.](#)
- [+ Configuration Menu.](#)

Table of Contents.

This tree represents the structure of the on-line manual. Click on each main option to drop down its contents and then click on any issue to get the corresponding help.

- [+ Introduction.](#)
- [+ Button bar.](#)
- [+ File Menu.](#)
- [+ Virus Report.](#)
- [+ Results.](#)
- [+ About.](#)
- [+ Exit.](#)
- [+ Scan Menu.](#)
- [+ Investigation Menu.](#)
- [+ Configuration Menu.](#)

Table of Contents.

This tree represents the structure of the on-line manual. Click on each main option to drop down its contents and then click on any issue to get the corresponding help.

- [+ Introduction.](#)
- [+ Button bar.](#)
- [+ File Menu.](#)
- [+ Scan Menu.](#)
- [+ Scan.](#)
- [+ Investigation Menu.](#)
- [+ Configuration Menu.](#)

Table of Contents.

This tree represents the structure of the on-line manual. Click on each main option to drop down its contents and then click on any issue to get the corresponding help.

- [+ Introduction.](#)
- [+ Button bar.](#)
- [+ File Menu.](#)
- [+ Scan Menu.](#)
- [+ Investigation Menu.](#)
- [+ Unknown Viruses.](#)
- [+ Search String.](#)
- [+ Configuration Menu.](#)

Table of Contents.

This tree represents the structure of the on-line manual. Click on each main option to drop down its contents and then click on any issue to get the corresponding help.

- [+ Introduction.](#)
- [+ Button bar.](#)
- [+ File Menu.](#)
- [+ Scan Menu.](#)
- [+ Investigation Menu.](#)
- [+ Configuration Menu.](#)
- [+ Analysis.](#)
- [+ Extensions.](#)
- [+ Language.](#)
- [+ Load Configuration.](#)
- [+ Save Configuration.](#)

HOT-line

Servicio telefónico de ayuda a los usuarios.

