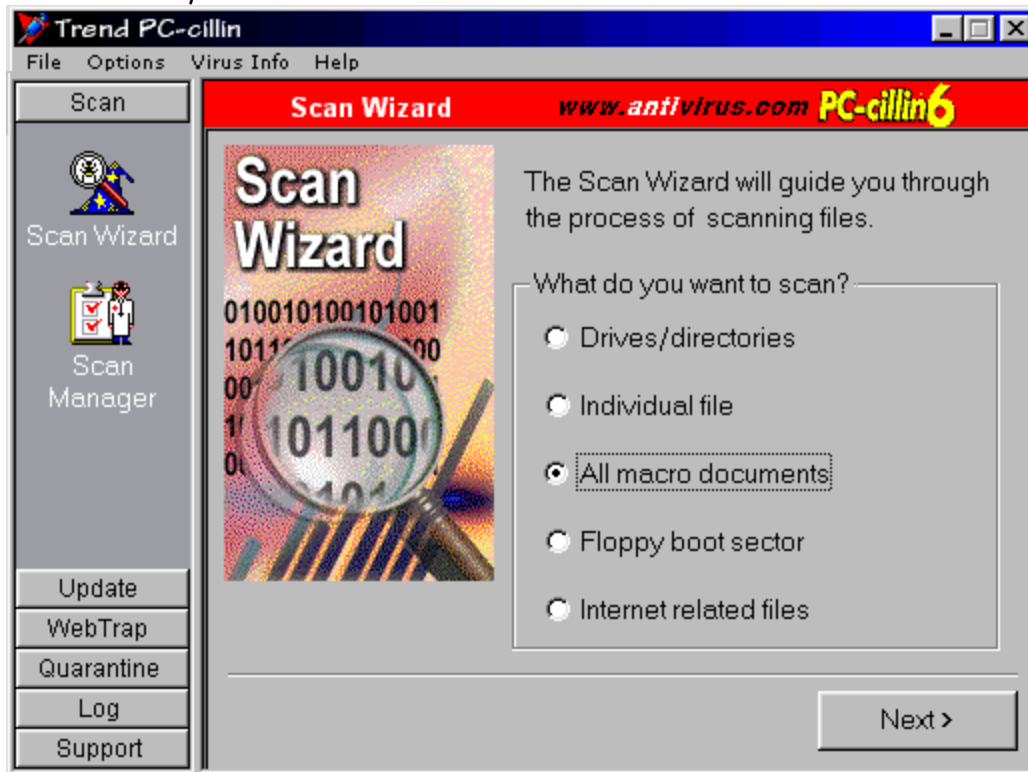


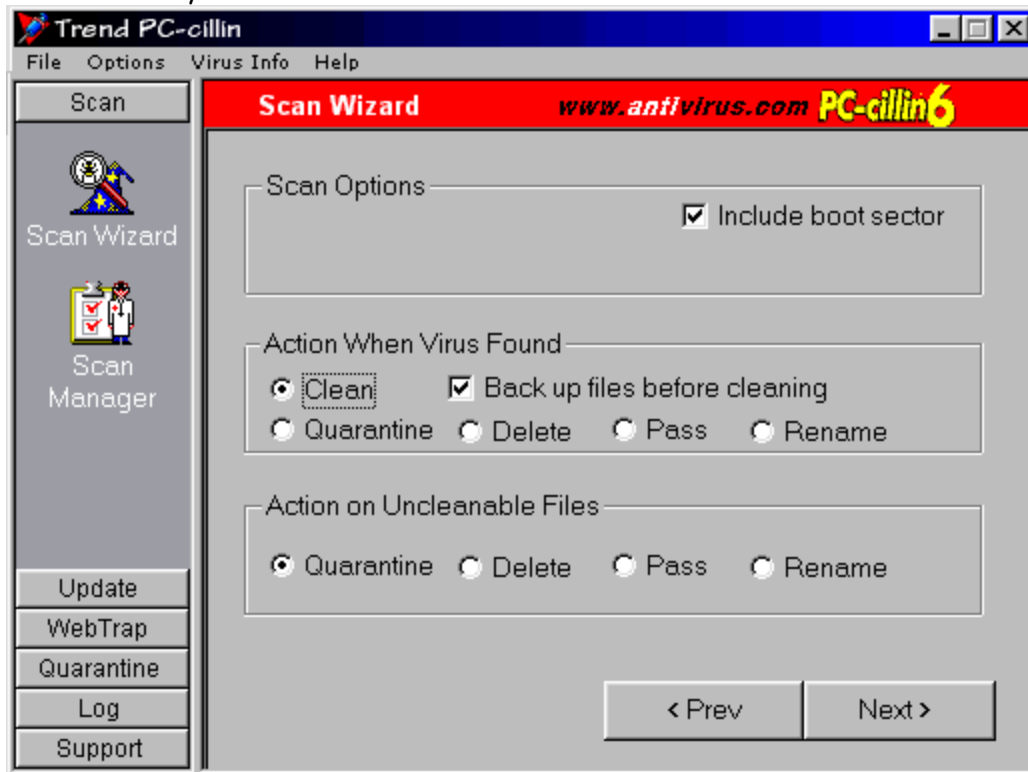
Scan Wizard Screen

Click the item you want to find out more about...



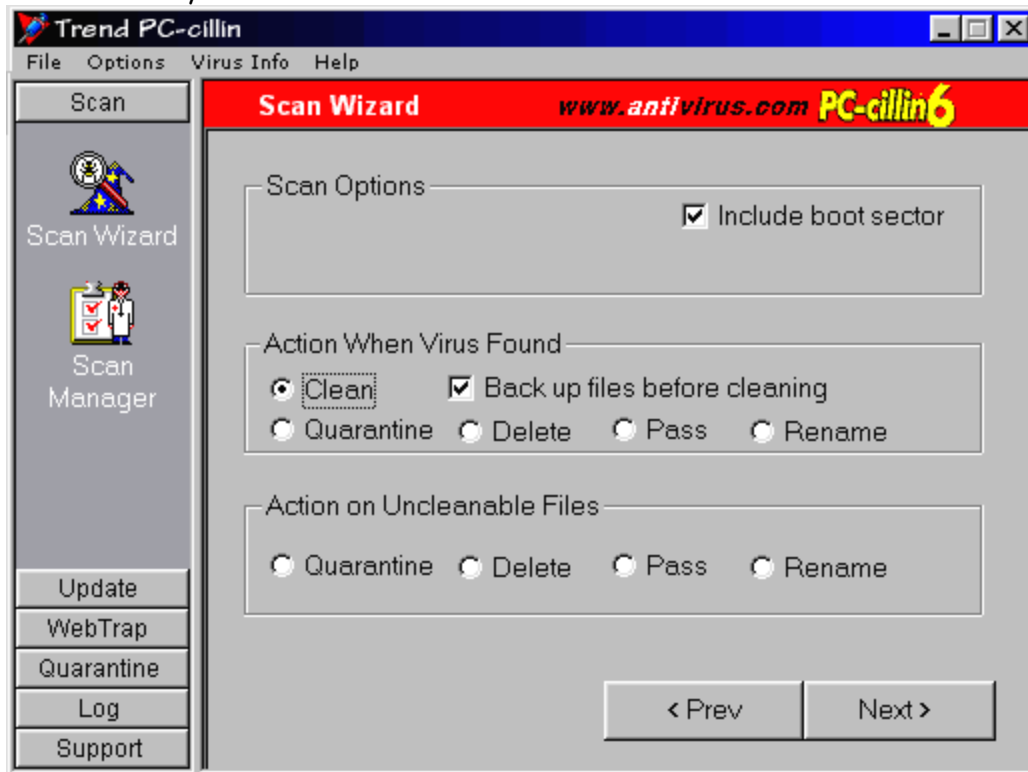
Scan Wizard Options Screen

Click the item you want to find out more about...



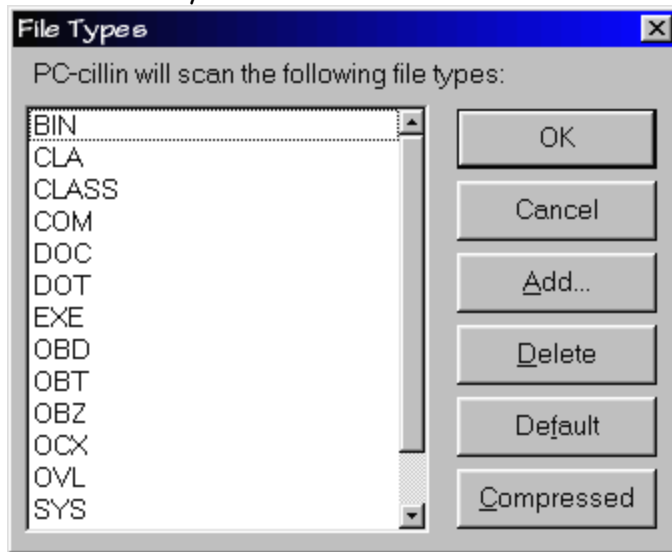
Scan Wizard Macro Options Screen

Click the item you want to find out more about...



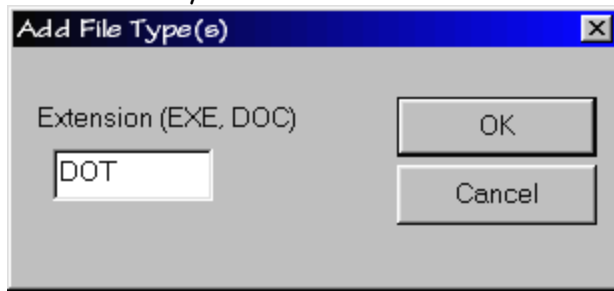
Select File Types Screen

Click the item you want to find out more about...



Add Screen

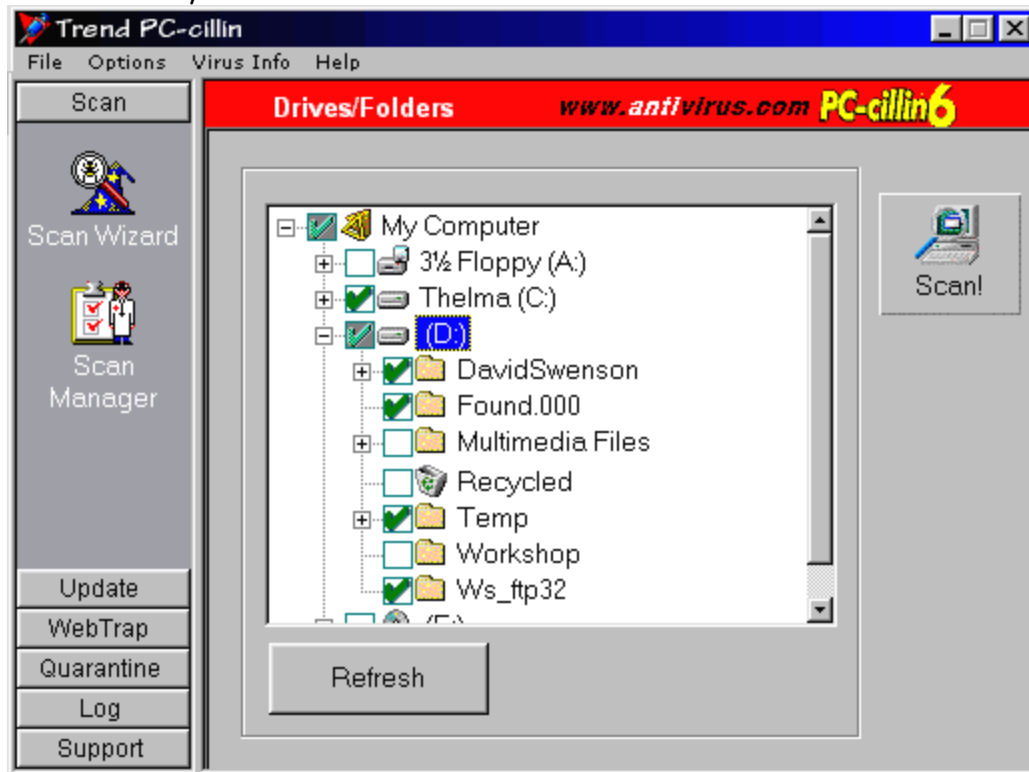
Click the item you want to find out more about...



A dialog box titled "Add File Type(s)" with a close button (X) in the top right corner. The dialog has a light gray background. On the left side, there is a label "Extension (EXE, DOC)" above a text input field containing the text "DOT". On the right side, there are two buttons: "OK" and "Cancel", stacked vertically.

Drives Folders Screen

Click the item you want to find out more about...



Scan Manager Screen

Click the item you want to find out more about...

Scan Manager www.anti-virus.com **PC-cillin6**

Run New Task Edit Copy Paste Delete

Description	Last Run	Next Scheduled Run
Complete scan after installation	1999/06/04 17:26	23:00(Monthly 1)
Scan for macro viruses	1999/06/04 17:27	23:00(Monthly 5)
Scan C: drive - weekly	1999/06/04 17:00	17:00(Weekly Friday)
Scan everything - monthly	1999/06/04 17:28	17:00(Monthly 1)
Scan Floppy A:\	1999/06/04 17:28	None
Scan Internet related files	1999/06/04 17:29	01:00(Weekly Sunday)
Scan all Word documents	1999/06/04 17:30	16:00(Monthly 20)
Scan all Excel documents	1999/06/04 17:30	19:00(Weekly Monday)
Scan program files	1999/06/04 17:32	17:00(Daily)

Update
WebTrap
Quarantine
Log
Support

New Task Screen

Click the item you want to find out more about...

Select What To Scan

The Scan Task Wizard helps you create new scan tasks.
Name your task, then choose a Scan Level .

Task Name (or description):
Scan ZIP drive

Scan Level

Scan all drives

Scan selected drive

Scan selected files/folders

E:\

C:\Aaron\Yabumi.zip
C:\Program Files

Add File...

Add Folder...

Delete

< Back Next > Cancel

Select What To Scan

Click the item you want to find out more about...

The screenshot shows a Windows-style dialog box titled "Task Configuration" with a close button (X) in the top right corner. The dialog has three tabs: "Select What To Scan" (which is active), "Choose Scan Options", and "Schedule Task".

Below the tabs, there is instructional text: "The Scan Task Wizard helps you create new scan tasks. Name your task, then choose a Scan Level."

The "Task Name (or description):" field contains the text "Scan ZIP drive".

The "Scan Level" section contains three radio buttons:

- Scan all drives
- Scan selected drive
- Scan selected files/folders

To the right of the "Scan selected drive" option is a dropdown menu showing "E:\".

Below the radio buttons is a list box containing the following items:

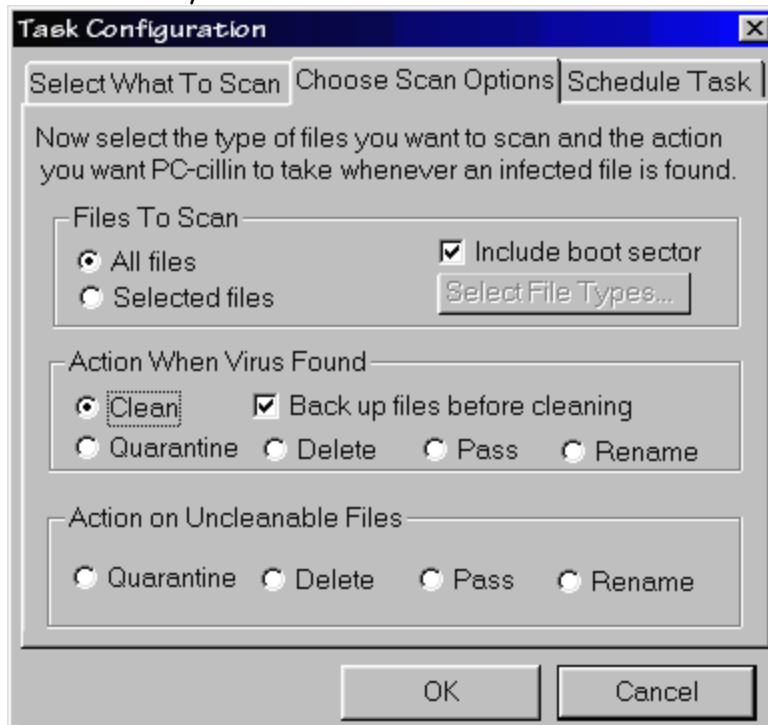
- C:\Aaron\Yabumi.zip
- C:\Program Files

To the right of the list box are three buttons: "Add File...", "Add Folder...", and "Delete".

At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

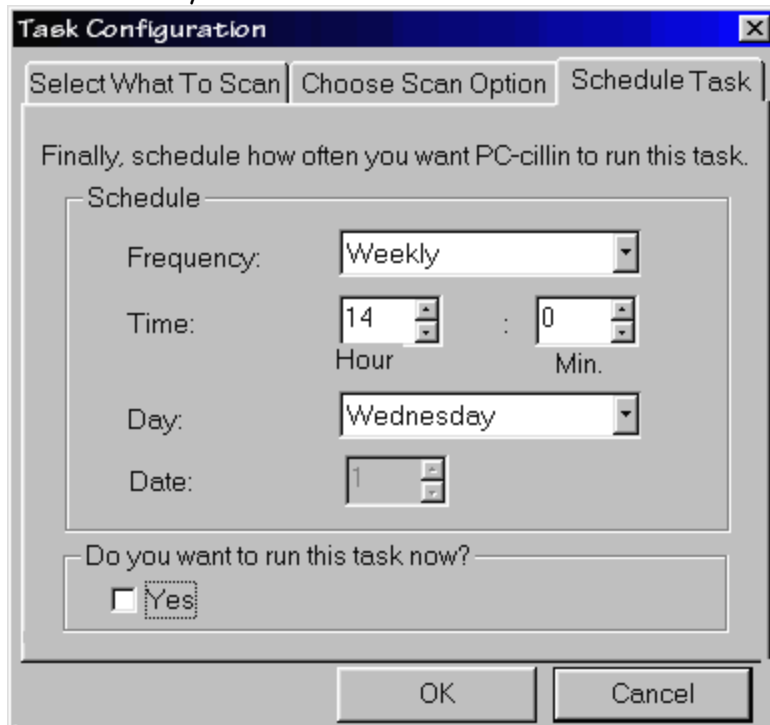
Choose Scan Options Screen

Click the item you want to find out more about...



Schedule Task Screen

Click the item you want to find out more about...



The image shows a 'Task Configuration' dialog box with three tabs: 'Select What To Scan', 'Choose Scan Option', and 'Schedule Task'. The 'Schedule Task' tab is active. The dialog contains the following elements:

- Text: 'Finally, schedule how often you want PC-cillin to run this task.'
- Section: 'Schedule' (indicated by a minus sign on the left).
- Frequency: A dropdown menu set to 'Weekly'.
- Time: Two spinners for 'Hour' (set to 14) and 'Min.' (set to 0).
- Day: A dropdown menu set to 'Wednesday'.
- Date: A spinner set to '1'.
- Text: 'Do you want to run this task now?' followed by a checkbox labeled 'Yes'.
- Buttons: 'OK' and 'Cancel' at the bottom.

Update Now Screen

Click the item you want to find out more about...



Update through Proxy Server Screen

Click the item you want to find out more about...

Updating Through Proxy Server [X]

Updating virus pattern or program files requires access to the Internet. If there is a proxy server on your network, enter its name and port. Your System Administrator will have this information.

Note: If you connect to the Internet using a dial-up connection, this option may not apply.

Proxy Server Configuration

I use a proxy server to connect to the Internet

Proxy server IP address: Port:

Proxy Server Authentication

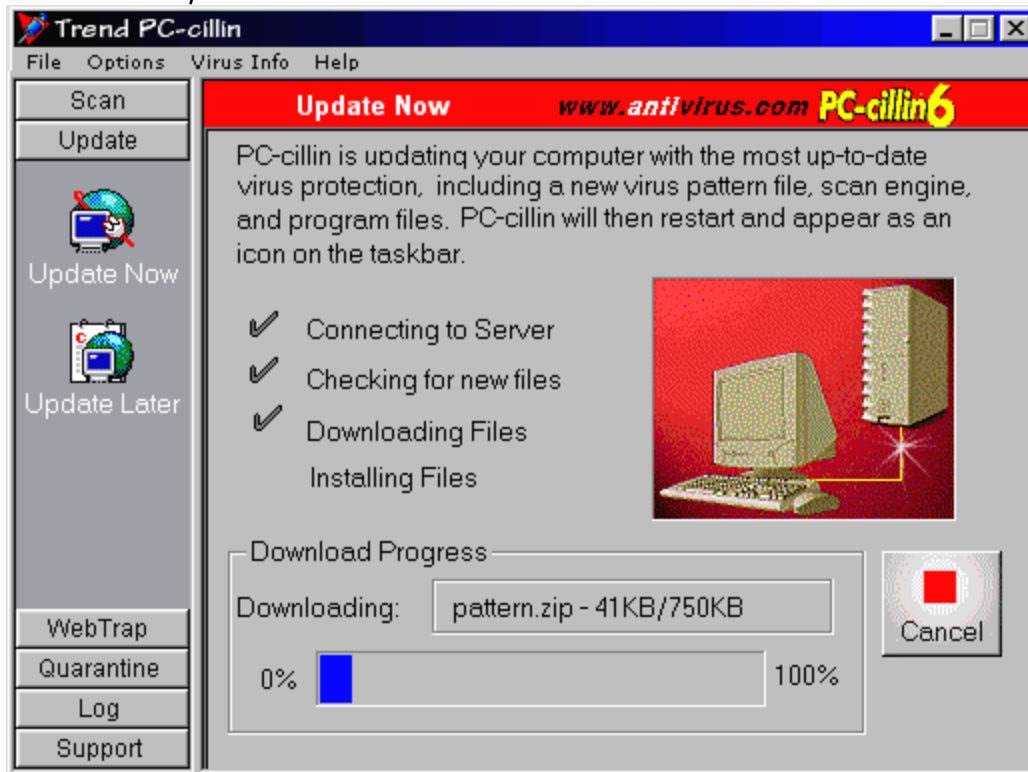
If the proxy requires a user name and password, please enter them here. Otherwise, leave this field blank.

User name: Password:

OK Cancel

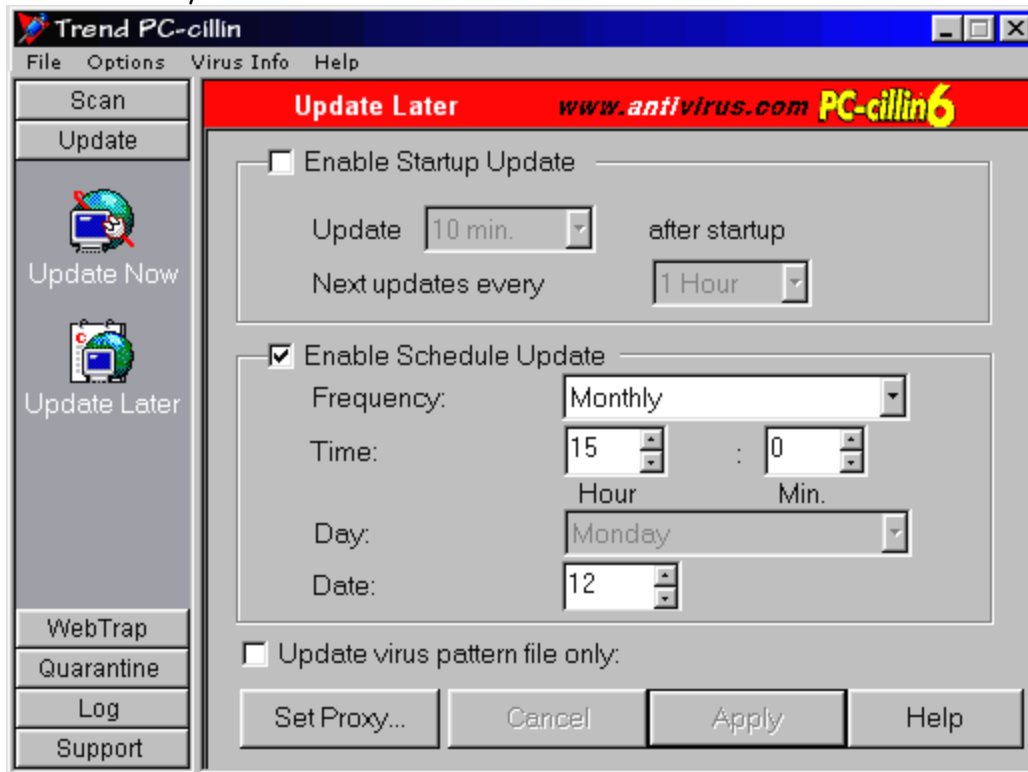
Update Now Progress Screen

Click the item you want to find out more about...



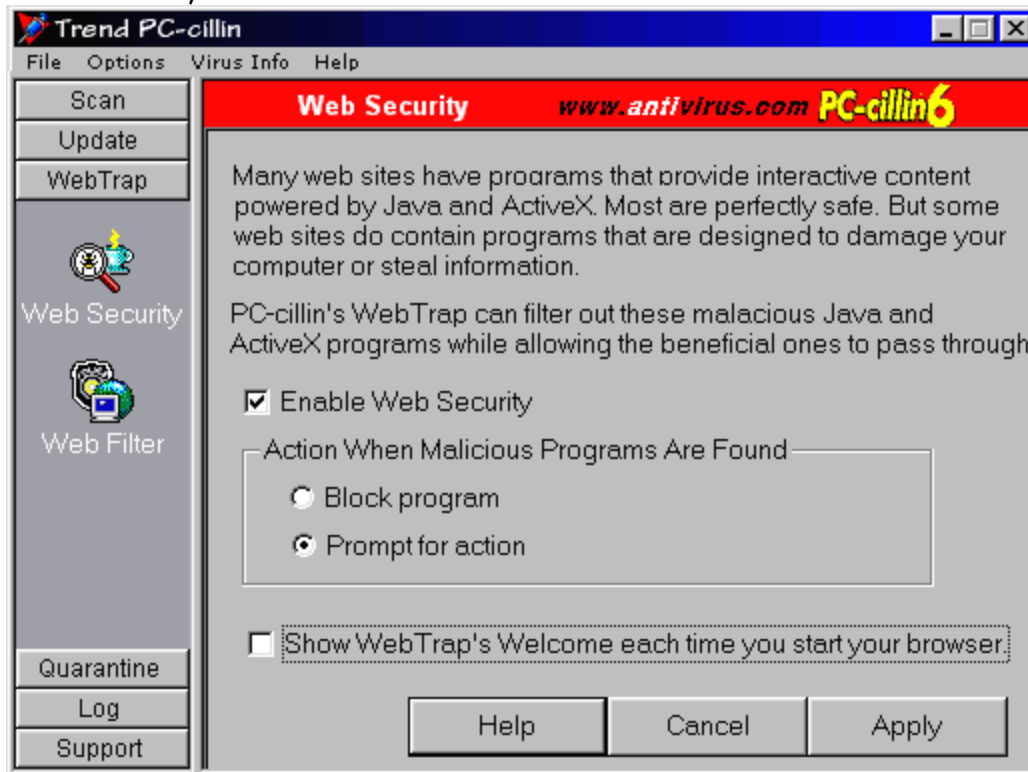
Update Later Screen

Click the item you want to find out more about...



Web Security Screen

Click the item you want to find out more about...



Enter Password Screen



Set Password

Enter password:

OK Cancel

Add Site Screen

Add Site To Restricted List [X]

Enter site's web address:

Extend to all sub-pages

Edit Site Screen

Add Site To Restricted List [X]

Enter site's web address:

Extend to all sub-pages

Set Password Screen

Click the item you want to find out more about...



A screenshot of a 'Set Password' dialog box. The title bar is blue with the text 'Set Password' and a close button (X). The dialog has a light gray background. It contains two text input fields. The first is labeled 'Enter password:' and the second is labeled 'Confirm password:'. Both fields contain a series of asterisks (*****). At the bottom, there are two buttons: 'OK' on the left and 'Cancel' on the right.

Set Password

Enter password:

Confirm password:

OK Cancel

Quarantine Screen

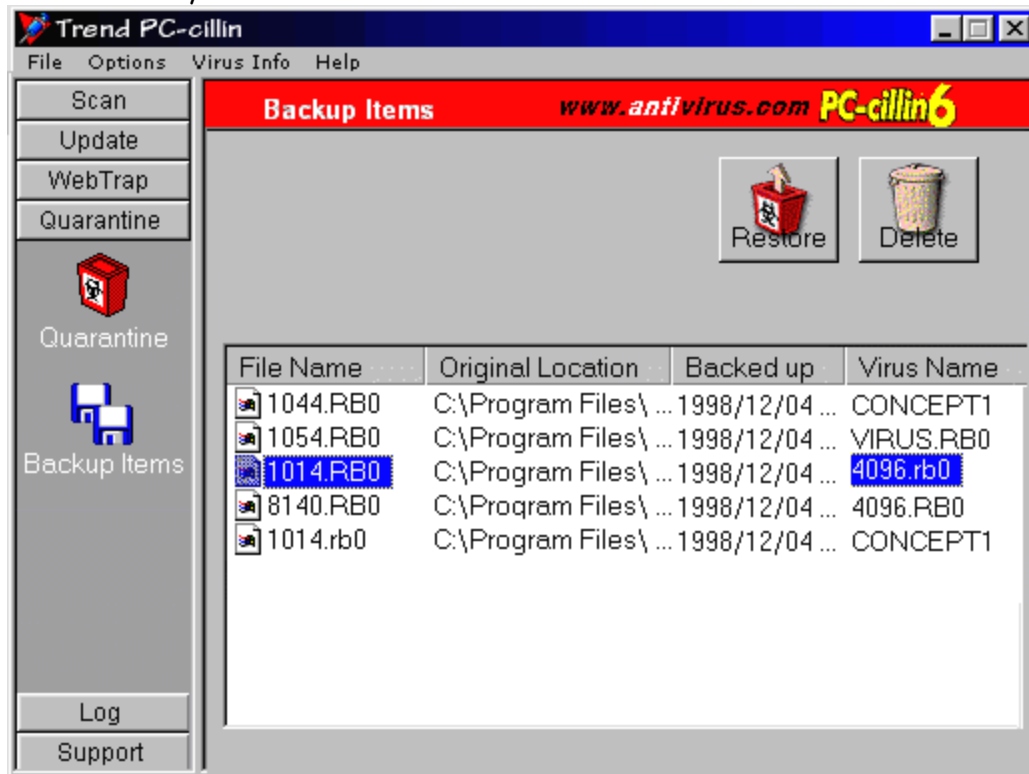
Click the item you want to find out more about...

The screenshot shows the Trend PC-cillin Quarantine interface. The window title is "Trend PC-cillin". The menu bar includes "File", "Options", "Virus Info", and "Help". The main area is titled "Quarantine" and features a red header with "www.anti-virus.com PC-cillin6". Below the header are icons for "Add", "Submit", "Clean", "Restore", and "Delete". A table lists quarantined files with columns for File Name, Original Location, Quarantined, and Status. The table contains six entries, all with a status of "Unknown".

File Name	Original Location	Quarantined	Status
neck.exe	A:\scraff\	1999/06/04 15:31	Unknown
pingpong.exe	A:\games\	1999/06/04 15:31	Unknown
Civil_war.com	A:\thesis\	1999/06/04 15:31	Unknown
bubblegum.com	A:\candy\	1999/06/04 15:31	Unknown
mammoth.exe	A:\helicopter\	1999/06/04 15:31	Unknown
important.com	A:\	1999/06/04 15:31	Unknown

Backup Screen

Click the item you want to find out more about...



The screenshot shows the 'Backup Items' window in Trend PC-cillin. The window has a menu bar with 'File', 'Options', 'Virus Info', and 'Help'. On the left side, there is a vertical toolbar with buttons for 'Scan', 'Update', 'WebTrap', 'Quarantine', 'Quarantine' (with a red box icon), 'Backup Items' (with a blue folder icon), 'Log', and 'Support'. The main area has a red header with 'Backup Items' and 'www.antivirus.com PC-cillin6'. Below the header are 'Restore' and 'Delete' buttons. A table lists backup items:

File Name	Original Location	Backed up	Virus Name
1044.RB0	C:\Program Files\ ...	1998/12/04 ...	CONCEPT1
1054.RB0	C:\Program Files\ ...	1998/12/04 ...	VIRUS.RB0
1014.RB0	C:\Program Files\ ...	1998/12/04 ...	4096.rb0
8140.RB0	C:\Program Files\ ...	1998/12/04 ...	4096.RB0
1014.rb0	C:\Program Files\ ...	1998/12/04 ...	CONCEPT1

Virus Log Screen

Click the item you want to find out more about...

The screenshot shows the 'Virus Log' window in Trend PC-cillin. The window has a menu bar with 'File', 'Options', 'Virus Info', and 'Help'. On the left side, there is a vertical navigation pane with buttons for 'Scan', 'Update', 'WebTrap', 'Quarantine', 'Log', 'Virus Log', 'Update Log', 'Web Filter Log', and 'Support'. The 'Virus Log' button is currently selected. The main content area has a red header with 'Virus Log' and 'www.anti-virus.com PC-cillin6'. Below the header are two buttons: 'Export Log' and 'Delete Log'. A table displays the log entries for the date 1999/06/04. The table has four columns: 'Time', 'Infected File Name', 'Virus Name', and 'Action On Virus'. The entries show several files infected with 'Eicar_test_file' at 15:31:37 and 15:31:38, all of which were quarantined. A 'Help' button is located at the bottom right of the window.

Log Date	Virus Log			
	Time	Infected File Name	Virus Name	Action On Virus
1999/06/04	15:31:38	A:\important.com	Eicar_test_file	Quarantine
	15:31:38	A:\helicopter\ma...	Eicar_test_file	Quarantine
	15:31:37	A:\candy\bubbl...	Eicar_test_file	Quarantine
	15:31:37	A:\thesis\Civil_w...	Eicar_test_file	Quarantine
	15:31:37	A:\games\pingp...	Eicar_test_file	Quarantine
	15:31:37	A:\scraff\neck.e...	Eicar_test_file	Quarantine

Update Log Screen

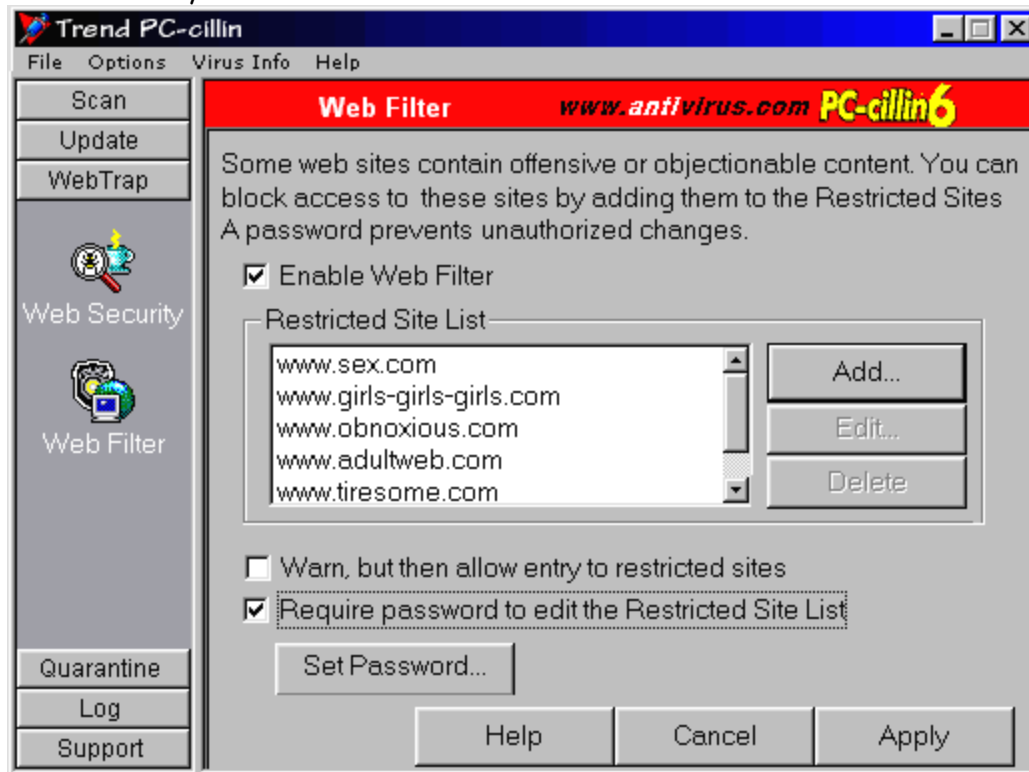
Click the item you want to find out more about...

The screenshot shows the 'Update Log' window in Trend PC-cillin. The window title is 'Trend PC-cillin'. The menu bar includes 'File', 'Options', 'Virus Info', and 'Help'. The left sidebar contains buttons for 'Scan', 'Update', 'WebTrap', 'Quarantine', 'Log', 'Virus Log', 'Update Log', 'Web Filter Log', and 'Support'. The main area has a red header 'Update Log' with 'www.antivirus.com PC-cillin6'. Below the header are icons for 'Note', 'Export Log', and 'Delete Log'. A table displays update logs for the date 1999/01/06, with columns for Time, Download, and Status.

Log Date	Update Log		
1999/01/06	Time	Download	Status
	22:31:54	Program	Updated
	22:54:31	Pattern	Updated

Web Filter Screen

Click the item you want to find out more about...



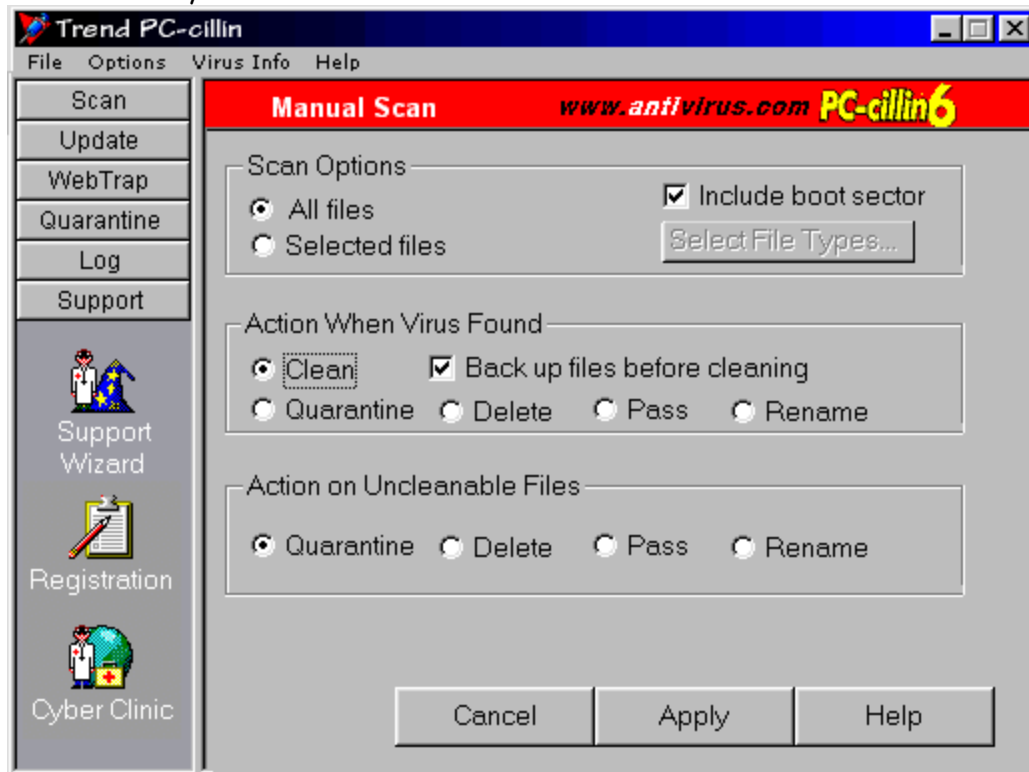
Support Wizard Screen

Click the item you want to find out more about...



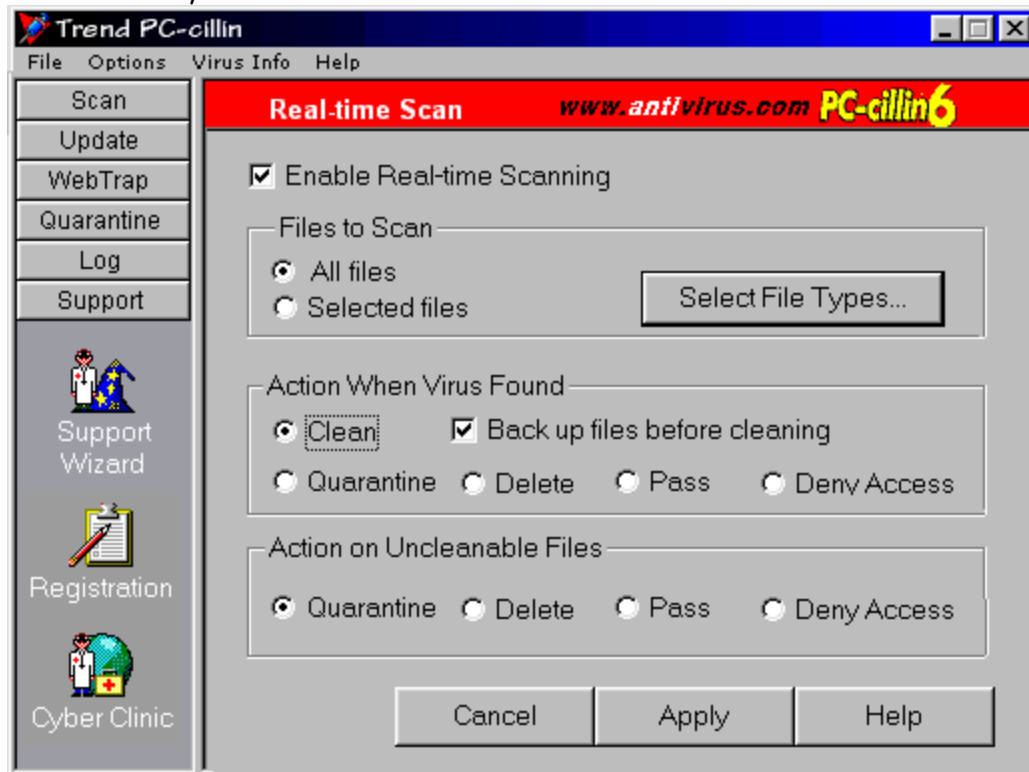
Manual Scan Screen

Click the item you want to find out more about...



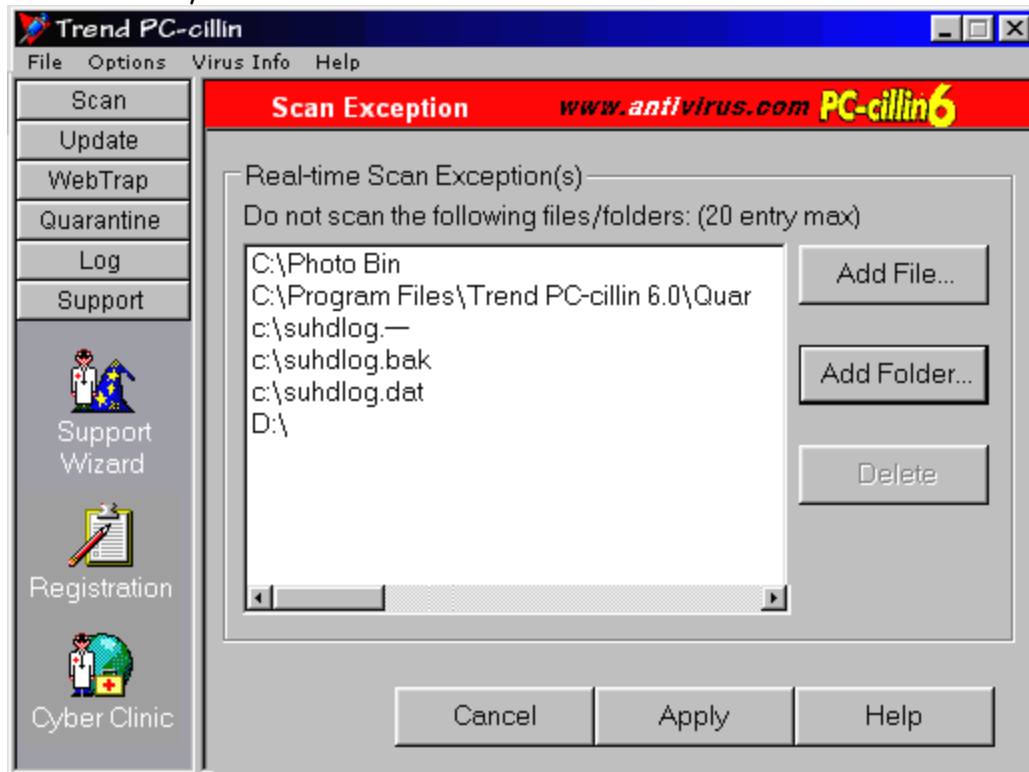
Real time Scan Screen

Click the item you want to find out more about...



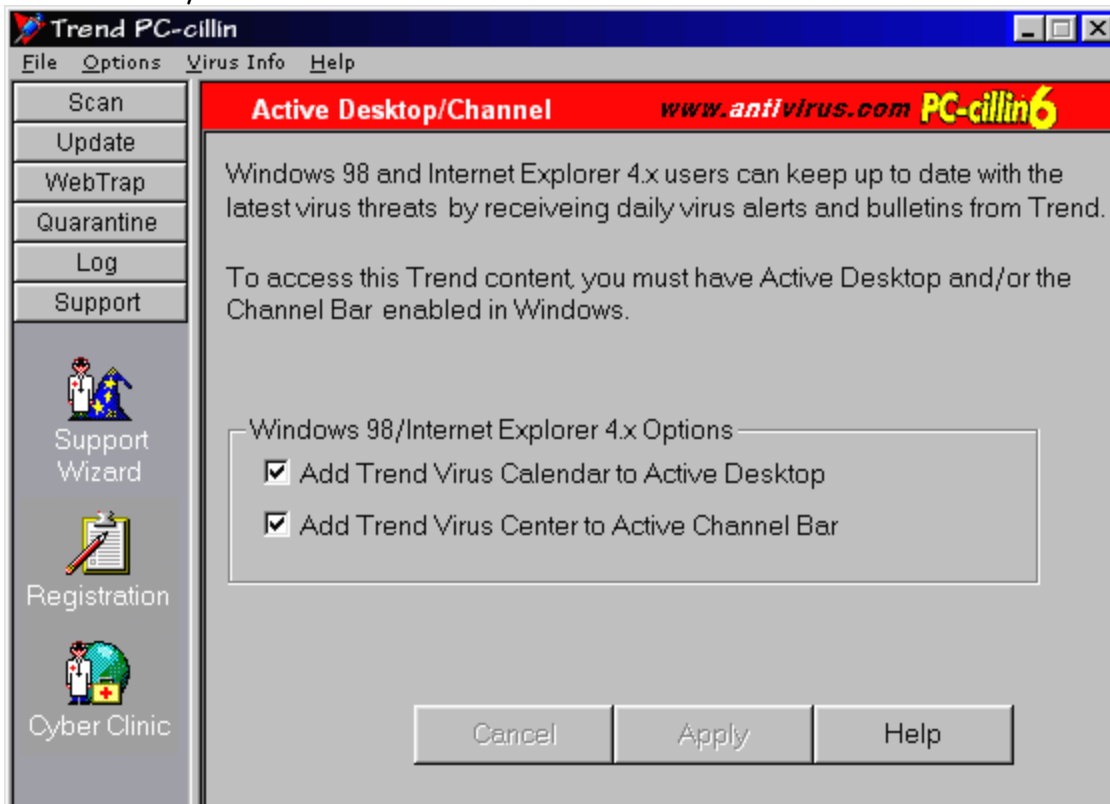
Scan Exceptions Screen

Click the item you want to find out more about...



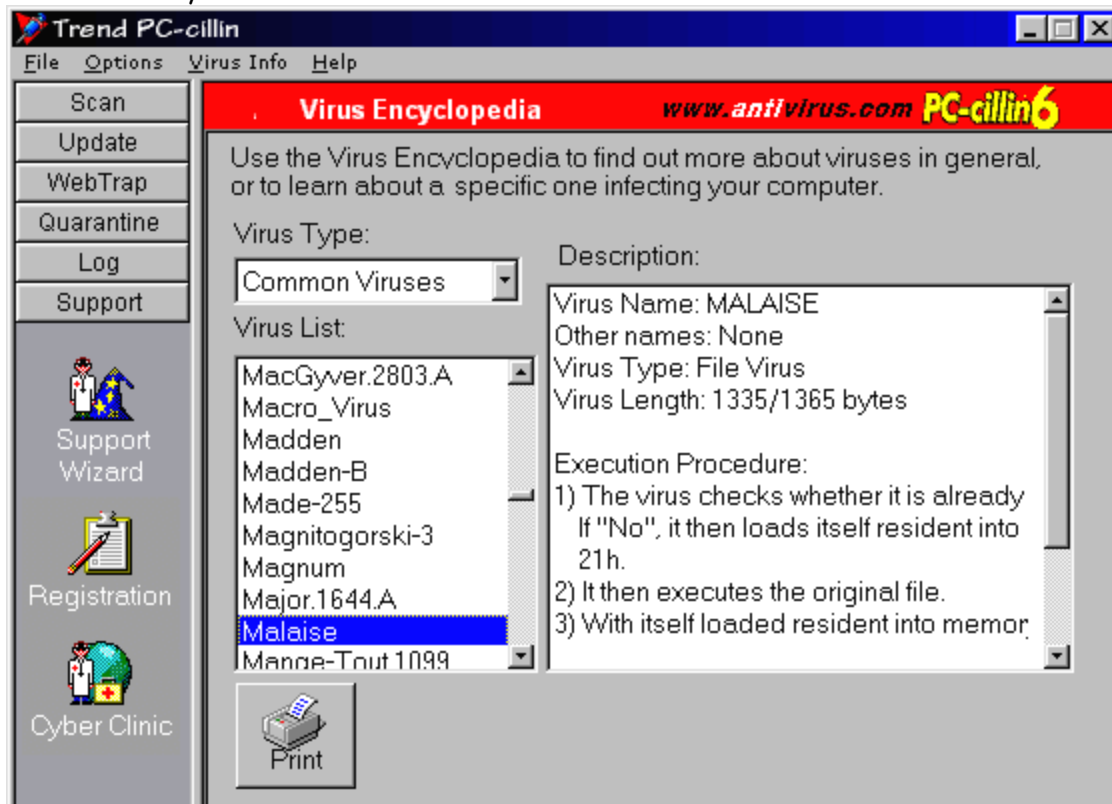
Active Desktop Screen

Click the item you want to find out more about...



Virus Encyclopedia Screen

Click the item you want to find out more about...



Virus List Screen

Click the item you want to find out more about...

Detectable List www.antivirus.com **PC-cillin6**

PC-cillin is capable of detecting many thousands of viruses.
The Detectable List shows the most common.

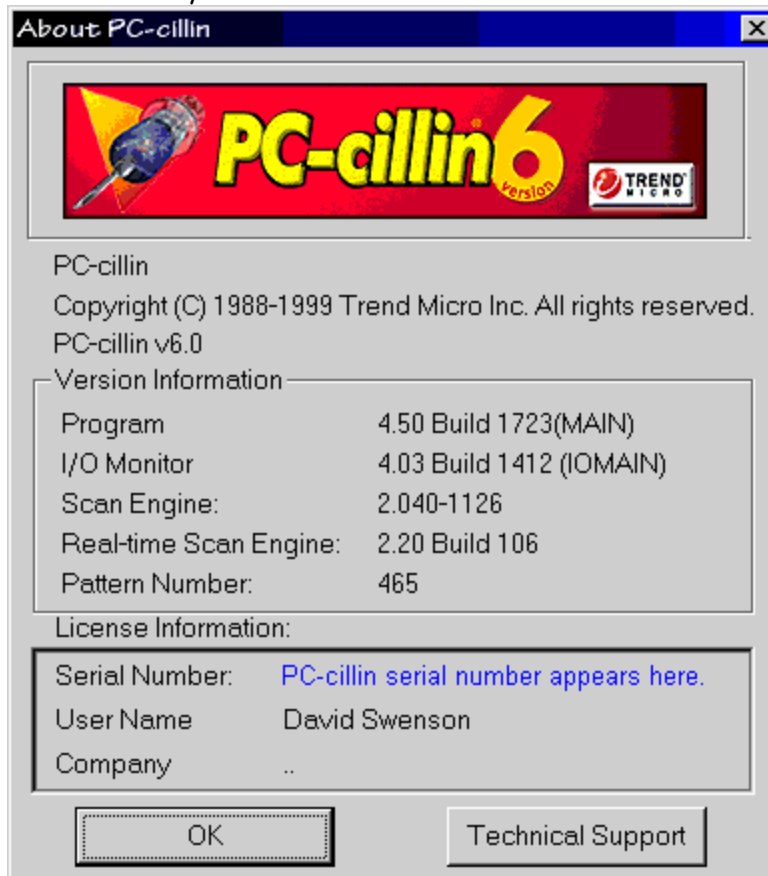
Detectable List:

5917.OLENSKA.6144-E	5918.OLEXY	5919.Olivia
5920.OLK.4275	5921.OLNG.1086	5922.OLO
5923.OLY	5924.OLYA_CAV.390	5925.OLYAEXE.O
5926.OLYMPIC	5927.OMEGA.440	5928.OMINOUS.184
5929.OMT.413	5930.OMUD	5931.ON2043
5932.ONE_HALF.3544	5933.ONE_HALF.3544-M	5934.ONEHALF.351
5935.ONEHALF.3518-E	5936.ONETHIRD	5937.ONETHIRD.11
5938.ONKELZ.527	5939.ONTARIO	5940.ONTARIO-1
5941.ONTARIO-2	5942.ONTARIO-A	5943.ONTARIO-C
5944.ONTARIO-S	5945.ONTARIO.1024	5946.ONTARIO.102
5947.ONTARIO.2052	5948.ONTARIO.B	5949.ONTARIO3
5950.OOHLALA.1895	5951.OOHLALA.1895-1	5952.OOLONG
5953.OOLONG-1	5954.OOOPS	5955.OOOPS

Print

About Screen

Click the item you want to find out more about...



Task Bar Menu Screen



Active Channel Screen



Active Desktop Example



Store Proxy Settings

Click the item you want to find out more about...

Updating Through Proxy Server [X]

Updating virus pattern or program files requires access to the Internet. If there is a proxy server on your network, enter its name and port. Your System Administrator will have this information.

Note: If you connect to the Internet using a dial-up connection, this option may not apply.

Proxy Server Configuration

I use a proxy server to connect to the Internet

Proxy server IP address: Port:

Proxy Server Authentication

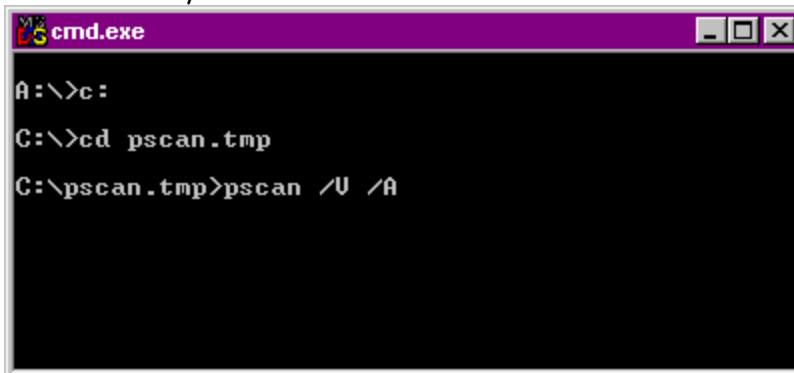
If the proxy requires a user name and password, please enter them here. Otherwise, leave this field blank.

User name: Password:

OK Cancel

DOS Screen

Click the item you want to find out more about...



```
cmd.exe
A:\>c:
C:\>cd pscan.tmp
C:\pscan.tmp>pscan /U /A
```

Taskbar Icon Screen



Web Filter Log

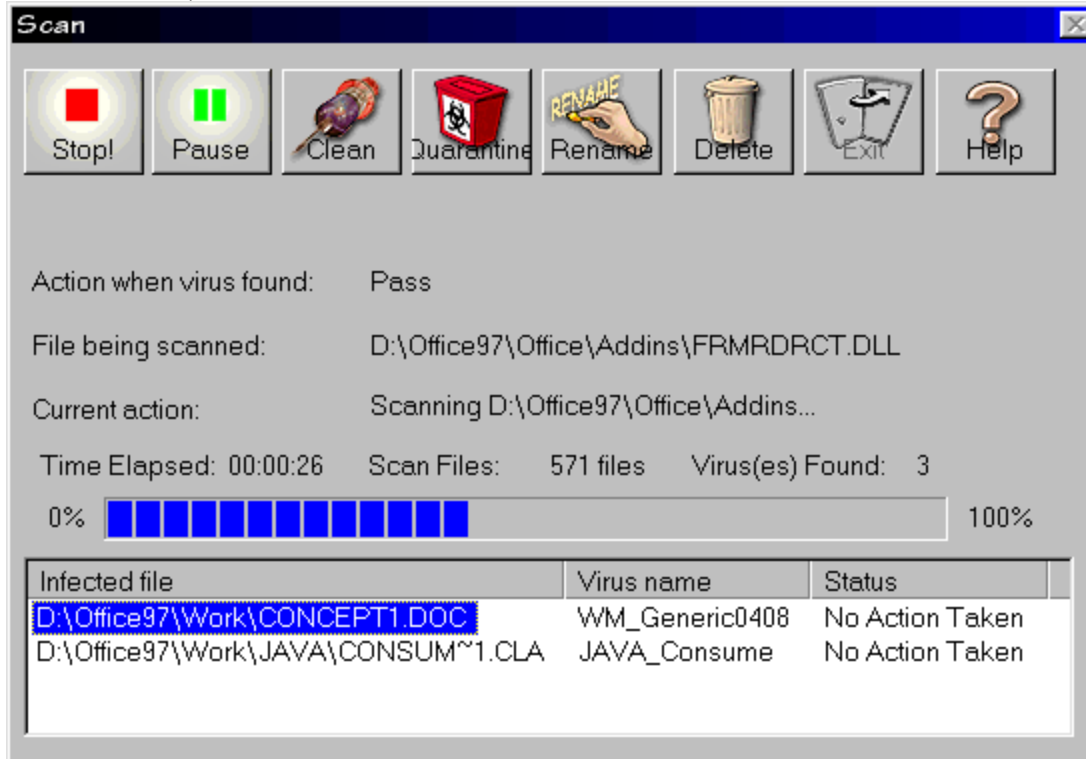
Click the item you want to find out more about...

The screenshot displays the 'Web Filter Log' window in Trend PC-cillin. The window title is 'Trend PC-cillin' and it features a menu bar with 'File', 'Options', 'Virus Info', and 'Help'. The main area is titled 'Web Filter Log' and includes a red header with 'www.antivirus.com PC-cillin6'. Below the header are three buttons: 'Note', 'Export Log', and 'Delete Log'. A table titled 'Web Filter Logs' shows a log date of '1999/01/06' and two time entries: '22:31:54' and '22:54:31'. The left sidebar contains buttons for 'Scan', 'Update', 'WebTrap', 'Quarantine', 'Log', 'Virus Log', 'Update Log', 'Web Filter Log', and 'Support'. A 'Help' button is located at the bottom right of the main area.

Log Date	Web Filter Logs		
	Time	URL Address	Web Filter A...
1999/01/06	22:31:54		
	22:54:31		

Scanning Screen

Click the item you want to find out more about...



The screenshot shows a 'Scan' utility window with a toolbar at the top containing icons for Stop!, Pause, Clean, Quarantine, Rename, Delete, Exit, and Help. Below the toolbar, the following information is displayed:

- Action when virus found: Pass
- File being scanned: D:\Office97\Office\Addins\FRMRDRCT.DLL
- Current action: Scanning D:\Office97\Office\Addins...
- Time Elapsed: 00:00:26
- Scan Files: 571 files
- Virus(es) Found: 3

A progress bar shows 0% completion, with a blue bar extending from the left. Below the progress bar is a table of infected files:

Infected file	Virus name	Status
D:\Office97\Work\CONCEPT1.DOC	WM_Generic0408	No Action Taken
D:\Office97\Work\JAVA\CONSUM~1.CLA	JAVA_Consume	No Action Taken

Copyright



Trend Micro Incorporated makes no representations or warranties with respect to the contents or use of this document or the product described herein and specifically disclaims any express or implied warranties as to the merchantability and fitness for any particular purpose. Furthermore, Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without any obligation to notify any person or entity of such changes.

Trend PC-cillin is a registered trademark of Trend Micro Incorporated. All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Copyright © 1987-1999 Trend Micro Incorporated. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

See also:

[Year 2000 Compliance Statement](#)

[Warranty](#)

Year 2000 compliance



PC-cillin is certified by Trend Micro to be year 2000 compliant.

Trend Micro Year 2000 Compliant software will:

- Accurately process prior to, during and after the year 2000, all date related data before, on and after January 1st 2000, including but not limited to accurately inputting, storing, manipulating, comparing, calculating, updating, recording, displaying, outputting, transferring and sequencing such data.
- Accurately interface with other software and hardware that uses the standard 4-digit format to represent the year.



Correctly process calendar dates for leap year as defined by the Gregorian calendar.



Not adversely affect system performance due to changes added to provide Year 2000 compliance.



Enable users to readily identify and use the century in any date fields without special processing.



Accommodate 4-digit year and century input in all date-related data fields and in all date related functions.

Trend Micro Year 2000 Corporate Policy



Definitions: "Current Products" are current products that will continue to be updated and upgraded.



Year 2000 Testing: All Current Products will be run through a complete set of test cases to determine the effect, if any, of the transition into the 21st century. This includes the capability of the products, as applicable, to perform date and data functions from, into and between the 20th and 21st centuries.



New Products and Product Versions after June 30th 1998: All new products and product versions delivered after June 30th 1998 are Year 2000 Compliant.

See also:

[Warranty](#)

Warranty



Trend Micro warrants that the software delivered shall be able to accurately process date data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the 20th and 21st centuries, including leap year calculations, when used in accordance with the product documentation provided by Trend Micro, provided that all products (e.g. hardware, software, firmware) used in combination with such software properly exchange date data with it. The duration of this warranty and the remedies available for breach of this warranty shall be as defined in, and subject to, the terms and limitations of Trend Micro's standard commercial warranty

See also:

[Year 2000 Compliance Statement](#)

Pattern Matching



Using a process called “pattern matching,” the PC-cillin draws upon an extensive database of virus patterns to identify known virus *signatures*, or tell-tale snippets of virus code. Key areas of each file scanned is compared against the list of thousands of virus signatures that Trend Micro has on record.

Whenever a match occurs, PC-cillin takes the action you have configured: [Clean](#) , [Delete](#) , [Quarantine](#) , [Pass](#) , or [Rename](#) / [Deny Access](#) .

See also:

[Virus Pattern File](#)

Virus Pattern File



To detect and clean viruses PC-cillin consults an extensive database of virus “signatures,” (inert snippets of virus code) that holds the signatures of thousands and thousands of viruses. As new viruses are written, released onto the public, and discovered, Trend collects their tell-tale signatures and incorporates the information into the virus pattern file. Obviously, it is very important to keep the virus pattern file up to date. By some estimates, thousands of new viruses are created each year, a rate of several each day. In fact, virus making has gotten so easy that free “virus kits” are even available over the Internet from rouge web sites.

To keep up with the onslaught of viruses, Trend publishes a new virus pattern file weekly (available for download from our web site). Home users probably don't need to update the file any more often than monthly. If you're an office user, consider scheduling weekly updates. Virus pattern file updates are available *free* for a year to registered PC-cillin users.

The virus pattern file is located in the `\Trend PC-cillin` folder of your computer and will have a name such as `Lpt$vpn.465`. The number represents the pattern version. If more than one virus pattern file exists in the directory, the scan engine knows to use only the latest.

How PC-cillin Detects Polymorphic Viruses



For polymorphic, or mutation viruses, PC-cillin's scan engine permits suspicious files to execute in a temporary environment. When the file is run, any encrypted virus code embedded within it is decrypted. PC-cillin then scans the entire file, including the freshly decrypted code, and identifies the code strings of the mutation virus. Once the cat is out of the bag, so to speak, PC-cillin takes whatever action you have deemed appropriate-- [Clean](#) , [Delete](#) , [Quarantine](#) , [Pass](#) , or [Rename](#) / [Deny Access](#) .

MacroTrap



Trend's MacroTrap® performs a rules-based, line-by-line examination of all Macro code that is saved in association with a document. This code analysis is called a "heuristic," or "intelligent" search because it allows the virus engine to detect new viruses that have not been included in the virus pattern file.

Macro virus code is typically contained as a part of the invisible template (.dot, for example, in Microsoft Word) that travels with many documents. The MacroTrap checks the template for signs of a Macro virus by seeking out key instructions that perform virus-like activity--instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).

Macro viruses are perhaps the most common type of viruses, responsible for the greatest number of infections, because they are relatively easy to produce, they spread easily (for example via e-mail attachments), and they are platform independent. Any computer running Word, for example, can become infected with the Concept virus -- regardless of whether the Word document is opened on a PC, an iMac, or another platform.

What is a Computer Virus?



Simply put, a computer virus is a program that replicates. To do so, it will need to attach itself to other program files (for example, .exe, .com, .dll) and execute whenever the host program executes. Beyond simple replication, a virus almost always seeks to fulfill another purpose: to cause damage.

Called the damage routine, or payload, the destructive portion of a virus can range from overwriting critical information kept on your hard disk's partition table to scrambling the numbers in your spreadsheets to just taunting you with sounds, pictures, or obnoxious effects.

It's worth bearing in mind, however, that even without a "damage routine," left unabated viruses will continue to propagate--consuming system memory, disk space, slowing network traffic and generally degrading performance. Besides, virus code is often buggy and can also be the source of mysterious system problems that take weeks to understand. So, whether it was written to be harmful or not, a virus on your system can lead to instability and should not be tolerated.

Some viruses, in conjunction with "logic bombs," do not make their presence known for months. Instead of causing damage right away, these viruses do nothing but replicate--until the preordained trigger day or event when they unleash their damage routines across the network.

To learn more about any particular virus, or about viruses in general, you can access Trend Micro's on-line Virus Encyclopedia that comes with the program or visit the Internet Antivirus Center at:

<http://www.antivirus.com>

Resources Available over the Internet



Comprehensive antivirus information is available over the Internet at our free antivirus center <http://www.antivirus.com>. From there, find out about:

- ✓ What to do if you think you have a virus
- ✓ Where you can send especially pernicious viruses for special treatment



Which viruses are currently "in the wild," or active



Trend's product and virus White Papers

Types of Computer Viruses



Tens of thousands of viruses are known to exist with more being created each day. Although most common in Windows and Dos, computer viruses also exist in OS/2, System7, and other environments as well.



Boot Viruses



Parasitic, or File Viruses



Macro Viruses

Other virus types include:



Multi-partite Viruses



Polymorphic, or Mutation Viruses



Stealth Viruses

Macro Viruses



Macro viruses are perhaps the newest type of virus. The first macro virus, written in Microsoft's Word macro language, was discovered in August, 1995. Now, more than a thousand macro viruses have been discovered, including viruses written in the macro scripts of Microsoft's Excel, Word, Access and Ami Pro applications.

Macro viruses tend to spread quickly and over a wide area via e-mail attachments. Since a macro virus is written in the language of an application, not an OS, it is platform independent and can be spread between DOS, Windows, MACs, and even OS/2 systems. That is, Macro viruses can be spread to any machine that runs the application the virus was written in. Any machine running Word, for example, whether it's a PC, Mac, or something else, is vulnerable to Word documents that contain a Macro virus. To address the special threat of Macro viruses, Trend Micro has developed a new antivirus technology, called [MacroTrap](#).

File Viruses



File viruses, also known as parasitic viruses.

File viruses attach themselves to executable files and are at least partially activated whenever the host file is run. File viruses are typically TSR (terminate-and-stay-resident), direct action, or companion programs.

TSR viruses, which are among the most common of viruses, reside in memory and attach themselves to executable programs that are run. It is in this way that the TSR viruses then spread to other programs on the hard drive, floppies diskettes, or network.

Direct Action Virus



A Direct Action virus loads itself in to memory to infect other files and then unloads itself, while a companion virus acts to fool an executable file into executing from a `.com` file. For example, a companion virus might create a hidden `pgm.com` file so that when `pgm` command is executed, the fake `pgm.com` runs first. The `.com` file invokes its virus code before going on to start the real `pgm.exe` file.

Boot Viruses



Boot sector viruses, the most common type of virus, move or overwrite a disk's original boot sector data and replace it with the infected boot code of their own design. Floppies and hard drives are the most susceptible to being overwritten by a boot sector virus. Then, whenever the infected system is powered on (boots up), the virus loads into memory where it can gain control over basic hardware operations. From its place in memory, a boot virus can also quickly spread to any of the other drives on the system (floppy, network, etc.).

Multi-partite Viruses



Multi-partite viruses share some of the characteristics of boot sector viruses and file viruses: They can infect `.com` files, `.exe` files, and the boot sector of the computer's hard drive. On a computer booted up with an infected diskette, the typical multi-partite virus will first make itself resident in memory then infect the boot sector of the hard drive. From there the virus may infect a PC's entire environment. Not many forms of this virus class actually exist. However they do account for a disproportionately large percentage of all infections.

Polymorphic, or Mutation Viruses



Polymorphic (mutation) viruses are unique in that they are designed to elude detection by changing their structure after each execution--with some polymorphic viruses, millions of permutations are possible. Of course, this makes it harder for normal antivirus programs to detect or intercept them. It should be noted that polymorphic viruses do not, strictly speaking, constitute a separate category of virus; they usually belong to one of the categories described above.

Stealth Viruses



Stealth viruses, or Interrupt Interceptors, as they are sometimes called, take control of key DOS-level instructions by intercepting the interrupt table, which is located at the beginning of memory. This gives the virus the ability to do two important things: 1) gain control of the system by re-directing the interrupt calls, and 2) hide itself to prevent detection.

Virus Writers



In the typical scenario, it is an individual, working alone, who writes a virus program and then introduces it onto a single computer, network server, or the Internet. Why? Ego, revenge, sabotage, and basic disgruntlement have all been cited as motivations. Recently, do-it-yourself “virus kits” have been popping up on the Internet, and Macro scripts are becoming both easier to learn and more powerful, putting the capacity to engineer viruses in the hands of nearly everyone. In other words, no single, likely profile exists by which virus writers can be described or understood.

So whatever the reason one may have for writing a virus, the important thing is to make certain your company is not victimized, that your data you are responsible for is safe, and that precious time is not wasted hunting down (and cleaning up after) viruses.

How Viruses Spread



There are many ways for a virus to enter your system:

▶ E-mail attachments



World Wide Web (WWW) sites



FTP traffic from the Internet (file downloads)



Shared network files & network traffic in general



Demonstration software



Pirated software



Shrink-wrapped, production programs (rare)



Computer labs



Electronic bulletin boards (BBS)



Diskette swapping (using other people's diskettes for carrying data and programs back and forth)

The most likely virus entry points are e-mail, Internet and network connections, floppy disk drives, and modems or other serial or parallel port connections. In today's increasingly interconnected workplace (Internet, intranet, shared drives, removable drives, and e-mail), virus outbreaks now can spread faster and wider than ever before.

Methods of Virus Detection



Three main methods exist for detecting viruses: integrity checking (also known as checksumming), behavior monitoring, and scanning. PC-cillin is scanning based, with further buttressing from Trend Micro's MacroTrap and WebTrap technologies. A short description of each of the methods is available.

Integrity Checking



Integrity checking antivirus programs begin by building an initial record of the status (size, time, date, etc.) of every application file on the hard drive. Using this data, checksumming programs then monitor the files to see if changes have been made. If the status changes, the integrity checker warns the user of a possible virus.

This method has several disadvantages, however, the biggest being that false alarms are altogether too common. The records used by checksumming programs are often rendered obsolete by legitimate programs, which, in their normal course of operations, make changes to files that appear to the Integrity checker to be viral activity. Another weakness is that these programs can only alert the user after a virus has infected the system.

Behavior Monitoring



Behavior Monitoring programs are usually TSR and constantly monitor requests that are passed to the interrupt table. These programs are on the lookout for the type of activity a virus might engage in--requests to write to a boot sector, opening an executable program for writing, or placing itself resident in memory. The behavior these programs monitor is derived from a user-configurable set of rules.

“Rule-based” virus traps have one a strong advantage: they can prevent any kind of malicious program from damaging your system including viruses, Trojan Horses and Logic bombs. But they also have a significant disadvantage: these programs are unable to identify or clean the virus or rid your system of the threat. To identify a virus and eliminate it from the system, only a virus scanner will work.

Scanning



Scanning: Virus scanning programs rely on a virus pattern file for detecting and locating viruses. Key areas of suspect files are examined for tell-tale virus code and compared against the virus pattern file. For polymorphic viruses, the scanning engine permits suspicious files to execute in a temporary environment. To detect macro viruses in e-mail attachments, Trend Micro provides a [MacroTrap](#) which employs a rules-based, line-by-line examination of all macro code that is saved in association with a document. When suspicious code is identified, it is removed and both the e-mail sender and recipient can be notified of the action.

Test Virus



The European Institute of Computer Anti-virus Research, along with antivirus vendors, has developed a test file that can be used in checking your installation and configuration.

The file is not an actual virus; it will cause no harm and it will not replicate. Rather, it is especially created file whose “signature” has been included in the Trend Micro virus pattern file and as such, can be detected by the virus engine.

You can download this file from:

<http://www.antivirus.com/vinfo/testfiles/index.htm>

You may need to disable real-time scanning before downloading the file. Once on your machine, you can use the test virus to see for yourself how PC-cillin's various scanning features work.

False Positives



Like any antivirus program, PC-cillin 6 may report an infected file when in fact no virus exists (but this is very seldom -- average users just aren't likely to ever have it happen). In the industry, these errors are known as "false positives."

If you encounter what you believe to be a false positive, you can do two things:

1. Confirm it.
2. Send the file to the Trend virus doctors for special analysis.

How do you confirm it? [Update](#) to the latest version of the virus pattern file and run the scan again.

How do you send a suspect file to the Trend Virus Doctors? **Quarantine** it, then click the [Submit](#) button.

In the meantime, you can add the file or directory to a special [Scan Exceptions](#) list, which PC-cillin uses to determine which files, if any, should be skipped when running a scan.

Compressed Files



PC-cillin recognizes 19 types of file compression including PK-ZIP and LZEXE, and four types of file encoding, including UUencode and MIME.

When multiple layers of compression are encountered, PC-cillin recursively decompresses each, up to a limit of 20. In other words, if an archive contains .cab files that have been compressed using PK-ZIP, and LZEXE, PK-LITE, Microsoft Compress, etc., PC-cillin will decompress each layer until no more compressed files are found or the limit of 20 layers has been reached.

Note: Infected files that are part of a compressed file are not automatically acted upon.

To have PC-cillin **Clean, Delete, Rename, Deny access, Pass, or Quarantine** a compressed file, decompress it first. If you have **Real-time Scan** enabled, decompressing the file will trigger the action. If you're not using **Real-time Scan**, right click the infected file after it is decompressed and then choose [Virus Properties](#). Be sure to delete the compressed file, as it will still contain a copy of the infected item.

Compressed file types



PC-cillin will detect viruses in files compressed using any of the following formats:



PKZIP



ZIP to EXE



ARJ



ARK to EXE



LHA



LHA to EXE



MSCOMP



Cabinet files (.CAB)



LZEXE



PKLite



TAR



GZIP (.gz)



Diet



UNIX LZW compress (.Z)



UNIX pack (.z)

Encoding formats



PC-cillin will also detect viruses in files encoded with any of the following formats:



BINHEX



UUencode



Base64



MIME

Macro File Types



The following file types are included in the **Scan Macro Files** task:

- .doc
- .dot
- .xls
- .xlt
- .xla
- .mdb
- .vbs

Viruses have been discovered that can infect all these file types. In fact, the most common viruses nowadays are *Macro* viruses.

Internet File Types



The following file types are included in the **Scan Internet Files** task:

- .htm
- .html
- .cla
- .class
- .ocx
- .cab
- .jar
- .zip

Viruses have been discovered that can infect all these file types. In fact, one of the most common "routes of infection" is the Internet.

Risky Files



The **most dangerous** files types are:

.exe, .com, .xls, .doc, .mdb

because they don't need any special conversion to infect a computer -- all they've got to do is run, or be opened, and bang! the virus spreads. Trend virus doctors estimate that 99% of all viruses are written for these file formats.

Possible virus carriers include:

EXE - (Executable file)
SYS - (Executable file)
COM - (Executable file)
DOC - (Microsoft Word)
DOT - (Microsoft Word)
XLS - (Microsoft Excel)
XLA - (Microsoft Excel)
XLT - (Microsoft Excel)
MDB - (Microsoft Access)
ZIP - (Compressed file, common in the USA)
ARJ - (Compressed file, common in the USA)
DRV - (Device driver)
OVL - (Windows overlay file)
BIN - (Common boot sector image file)
SCR - (Microsoft screen saver)



Most of these file formats, .drv, .ovl, and .bin for example are not dangerous in and of themselves; they must be converted in order to be executed.

Features



Simplicity. Perhaps the greatest feature of PC-cillin is the one you don't see or notice: it's so simple to use that you really don't *have* to do anything. Straight out of the box, you get comprehensive, reliable, and robust virus protection!



Self-installing virus pattern updated and program upgrades can be downloaded over the Internet from Trend. That's right. PC-cillin is self-rejuvenating, and that's pretty darn cool.



Real-time scanning keeps you safe by watching over your computer, quickly checking files before they are used. With real-time scanning, you don't need to worry about infected e-mail attachments, Internet downloads, or viruses buried deep within a compressed file. PC-cillin catches them all.



Uses Trend's **32-bit, multi-threading scan engine**. Yep. This is the same engine that many of the Fortune 500 use. In addition to catching and cleaning all known macro, signature, and other viruses, InterScan will also detect unknown, polymorphic viruses, macro viruses, and malicious web contents.



Friendly, knowledgeable, easy-to-access technical support specialist and our team of Virus Doctors can be contacted live Internet chats, e-mail, and, of course, and over the phone.



PC-cillin's **Web Security** protects against malicious Java applets and ActiveX controls which can be inadvertently downloaded from Internet web sites -- these programs can destroy data and steal your private information.



Web Filtering lets you block access to any web site you find objectionable



Easy automation of all routine tasks, for example:

- ◆ Virus pattern updates
- ◆ Infected file processing



Keeps **detailed log files** that can be viewed using either a spreadsheet or text editor.



Provides **red-hot macro virus detection**, keeping you safe from the most common virus threat: macro viruses. Trend's rules-based MacroTrap™, both detects and cleans macro viruses, and will analyze suspect macro code to determine if it's harmful.



Smart architecture, cool interface. PC-cillin is task-based, and comes pre-configured to perform all sorts of tasks straight out of the box.



Fast, Reliable Detection. Trend's lightning-fast scan engine consistently detects all viruses known to be in circulation (i.e., "in the wild"), as well as thousand of other, less common ones.



PC-cillin detects tens of thousands of viruses, including all viruses known to be "in the wild," or actively circulating.

System Requirements



Minimum recommended system requirements for PC-cillin® 6 are:



OS: Microsoft Windows 95/98 or Windows NT 4.0 (Workstation or Server)
with SP3 or SP4



CPU: Intel 486, Pentium, or 100% compatible



Memory: 16 MB RAM



Disk Space: 15 MB hard disk space



Monitor: 800x600 or higher resolution; 256 or more colors



CD-ROM: 2x or faster for program installation



Internet: 28.8 or faster modem for virus pattern and program updates (14.4 is possible but slow)

Optional:



Internet Explorer 4.0 or later to support the [Active Desktop](#) & [Active Channel](#) options

Getting Started



What do you want to do?

Click the topic you want step by step instructions for:



Scanning



[I want to scan a file or directory...](#)



[I want to scan my hard drive...](#)



[I want to turn on/turn off real-time file scanning...](#)



[I want to modify my default scan settings ...](#)



[I want to start/stop PC-cillin from doing a scan every time my computer starts...](#)



Infected Files



[I want to submit a file to the Trend Virus Doctor...](#)



[I want to un-quarantine an infected file...](#)



[I want to scan Internet file downloads on the fly...](#)



[I want to see how many viruses PC-cillin has caught...](#)



Internet



[I want to start/stop Web filtering...](#)



[I want to start/stop Web security...](#)



[I want to check to see if anyone has tried to access one of my restricted web sites...](#)



Active Desktop/Web Channel



[Show me what Active Desktop looks like](#)



[Show me what Channel Bar looks like](#)



[I want to add/remove PC-cillin from my desktop...](#)



[I want to add/remove PC-cillin from my Channel bar...](#)



Updating Files



[I want to automate virus pattern file updates](#)



[I want to update the virus pattern file...](#)



[I want to see whether PC-cillin has updated the program or virus pattern file...](#)



Rescue Disk



[I want to update my rescue disks...](#)



[I want to create rescue disks...](#)



[I want to make a Windows Startup disk...](#)



Virus Information



[I'd like to find out more about viruses...](#)



[I want to check my Real-time Scan settings...](#)



Contacting Trend Micro



[I want to chat with the virus doctor...](#)



[I want to contact technical support...](#)

Welcome to PC-cillin



Welcome to PC-cillin 6, Trend Micro's award-winning antivirus software.

Here's what PC-cillin will do "straight out of the box":



Checks for viruses every time you **Open, Copy, Move, or Save** a file



Protects against downloading infected files from the Internet or FTP sites



Guards against nasty Java applets and ActiveX controls while web surfing



Monitors your Word and Excel sessions for macro viruses, using [MacroTrap™](#)



Scans and cleans all files on your hard drive every Friday



Scans all program files for viruses every month



Checks all your saved documents for macro viruses

Here's what you can do with just the click of a button:



Scan every file on your system and clean any infected files



Scan any file from Windows Explorer or My Computer by right-clicking it!



Scan floppy diskettes and clean any infected files



Check of all your Word and Excel document(s) for macro viruses

No Limits

Of course, if you're a person who *likes* to customize your software, there is no limit to the

Scan tasks you can have PC-cillin perform.

You can "set and forget" as many tasks as you see fit. For each task, you can select the file types you want scanned for viruses, the action PC-cillin takes upon finding a virus (Clean the infected file, Delete it, Quarantine it, Pass it, or Rename / Deny Access to it), and other program details.


Scan Engine

Virus are detected using Trend's 32-bit, multi-threading scan engine and a process called pattern matching. In addition to catching known signature viruses, PC-cillin detects and intercepts previously unknown polymorphic, or *mutation*, viruses.


MacroTrap

Additional layers of protection come from MacroTrap™, Trend's macro virus scanning engine, which detects and removes both known and unknown macro viruses.

Drives_directories

 Choose this option and then click **Next** to have the PC-cillin Scan Wizard scan the individual drives and/or directories you select.

Individual file

 Choose this option and then click **Next** to have the PC-cillin Scan Wizard scan a particular file.
Other ways of scanning an individual file are:



Right-click the file in Explorer and choose Properties




Right-click the file in Explorer and choose PC-cillin



Drag the file from Explorer to an open PC-cillin screen

All macro documents

 Choose this option and then click **Next** to have the PC-cillin Scan Wizard check all macro-containing file types on your c:\ drive for viruses.

Floppy boot sector



Choose this option and then click **Next** to have the PC-cillin Scan Wizard check a the boot sector of a floppy disk in the a:\ drive for viruses (this scan *does not check files* on the disk).

Internet related files



Choose this option and then click **Next** to have the PC-cillin Scan Wizard check all Internet file types on your c:\ drive for viruses.

Next button



After choosing *what* you want scanned (Drive/directory, Internet files, etc.), click this button to specify the file types (if applicable) and action you want PC-cillin to take upon detecting a virus.

Scan all file types



For the highest level of security, select **All file types**.

Note: There is some trade off between speed and safety. On the one hand scanning all files takes longer than scanning only specified files types. On the other hand, most file types, for example .jpg, .avi, .hlp, .pdf, etc., are not known to host or spread viruses and probably do not require scanning. But then until August, 1995, document files (.doc, .xls, etc.) had never been known to carry viruses either. And now macro viruses are the most prevalent.

One compromise is to set your scheduled scans to scan all files, and choose a time when you will be away from the computer for 20-30 minutes. Then, for your real-time scanning, choose to scan selected file types only.

Selected file types



Choose this option to have PC-cillin examine only those file types listed under the **Select File Types** button. Any files whose extension does not appear on the list will not be scanned.

Note: “Zip” and other [compressed file types](#) must be specified to be included in the scan. Click the **Compressed...** button or **Add...** to include compressed files in the scan list.

One compromise is to set your scheduled scans to scan all files, and choose a time when you are usually away from the computer for 20-30 minutes. Then, for your real-time scanning, choose selected file types only.

Add button



Click this button to include additional file types to the list of those that are scanned. You don't need to include the "dot," quotes, or any other characters. For example: zip not .zip or "zip".

Extension



The three (or sometimes four, i.e., .html) letter "suffix" that identifies the file type. For example: annual report.doc, 4th quarter sales.xls, win.com, calculator.exe. For **Add File Type**, no "." need be specified.

Delete button



Click this button to remove the selected file type from the list of those that are scanned. File types removed from the list are no longer be scanned under the **Selected file types** option.

Default button



Click this button to reset the list of file types to the Trend defaults. Any file types added/deleted from the list will be lost.

The defaults are: BIN, CLA, CLASS, COM, DOC, DOT, EXE, OBD, OBT, OBZ, OCX, OVL, SYS, XLS, and XLT.

Note: compressed file types are not, by default included. See [Compressed... button](#).

Compressed button



Click this button to add compressed file types to the list of those scanned under **Selected file types**.

The defaults are: ARJ, CAB, CO_, DO_, EX_, LZH, XL_ and ZIP.

Scan Options Area



This area appears blank when either the **Scan all macro documents** or **Internet related files** options are selected. See [Macro Documents](#) or [Internet related files](#) for a list of file types included in these scans.

Include Boot Sector



Check this option to have PC-cillin check the boot sector, usually on the `a:\` drive or `c:\` drive, when it is scanning files. Use **Include boot sector**, for example, if PC-cillin has detected (and cleaned!) a boot sector virus on your `c:\` drive and now you are going to check every bootable floppy, ZIP drive, etc. that you use to ensure that the infection is not re-introduced.

Boot Sector



The boot sector is critical to the proper start up of your computer. On startup, the computer checks the master boot record (MBR) for instructions on how to start the operating system and loads much of this data into memory. The boot sector is special, and usually off-limits to most programs -- they can't touch it. Nor can you see the boot sector using Explorer, for example. Any boot viruses that are infecting the computer are loaded into memory along with the valid data during boot up (system start-up). It's from their perch in memory that they infect files on the hard drive whenever they are opened, closed, etc.

But the thing about boot viruses that makes them especially nasty is that even if all the files on the system are cleaned, and the memory is cleaned, the next time the computer is restarted, the whole infection will come back -- unless and until the boot sector itself has been cleaned. And besides cleaning the c:\ boot sector, if you ever have a boot virus, be sure to clean *every* floppy, ZIP, and other removable, bootable disk that you have.

You may also want to run a quick scan of the boot sector of any floppies or disks before using them to start your computer (including game disks!).

Save



Click this button to apply your new configuration settings.

Cancel



Click this button to quit the configuration screen without saving your the changes.

Action when virus found



PC-cillin will take whatever action you specify whenever a virus is detected. Generally, it's a good idea to have PC-cillin **Clean** files, and, for critically important files, to **Back-up before cleaning**.

Clean



Choose this option to have PC-cillin open the infected file(s) and remove the virus code. Not all infected files can be cleaned; for example, when the virus destroys some of the original code when infecting the file.

Back up files before cleaning



Choose this option to have PC-cillin rename and back-up the to the `\Trend PC-cillin 6\Quarantine` directory the original, *infected* file(s) before cleaning. View backed up by clicking the **Quarantine** button, then **Backup Items**.

Backed up files *should be deleted* once you've determined whether it is usable. If not, and the file is mission critical, you can send it to Trend for further analysis. (Even if the virus itself can be completely removed, i.e., the file cleaned, some viruses can damage the original file code beyond repair.)

Quarantine



Choose this option to have PC-cillin move infected files to the \Trend PC-cillin 6\
Quarantine directory.

In most cases, it's best to have PC-cillin clean infected files and be done with it. Files that cannot be cleaned, however, can be quarantined. But remember, infected files are *not cleaned* and the virus will remain in the quarantined file.

Note: Infected files that are part of a compressed file are not automatically quarantined -- you must first decompress the file to have PC-cillin take the action specified.

Delete



Choose this option to have PC-cillin erase infected files. Infected files are *not cleaned*, and they will not appear in the Windows Recycle Bin. **Note:** Infected files that are part of a compressed file cannot be deleted. Decompress the file and run the scan again.

Pass



Choose this option to have PC-cillin take no automatic action on infected files. **Pass** is available for **Manual Scans**; **Deny Access** is the corresponding choice for **Real-time Scans**.



For Scan Wizard and "on-demand" Scan Manager tasks, you can choose to **Quarantine**, **Delete**, **Rename**, **Pass** infected files on a case-by-case basis.



For [Virus Property](#) scans and automatically scheduled scans, no action is taken. A record of any viruses detected appears in the [Virus Logs](#).

Rename



Choose this option to have PC-cillin rename infected files with the .VIR extension. The file 3rd Quarter.xls would be renamed 3rd Quarter.VIR. Renamed files are *not cleaned*.

Note: Infected files that are part of a compressed file are not automatically renamed. Decompress the file to have PC-cillin take the action specified, e.g., **Rename**.

Deny access



Choose this **Real-time Scan** option to have PC-cillin "lock" infected files so they cannot be opened, copied, or otherwise used by any person or program. Files that have been denied access are *not cleaned*.

Note: Infected files that are part of a compressed file cannot be denied access. Decompress the compressed file and run the scan again to have PC-cillin act upon the individual infected file(s).

Action on uncleanable files



Sometimes PC-cillin can detect, but not clean a file. This occurs, for example, if the virus has corrupted the file, if the virus is of an "uncleanable" type, or if the file is contained within a compressed file. **Note:** Infected files that are part of a compressed file cannot be cleaned. Decompress the file and run the scan again.

Drives Folders



Select (by clicking) drive(s) and folders you want PC-cillin to scan and click **Scan**. PC-cillin will scan all files of the type specified in the Scan Wizard screen and take the action specified.

Scan button



Click this button to have PC-cillin begin scanning files of the type specified in the Scan Options and Drives/Folders Wizard screens.

Refresh



Click this button to have PC-cillin take another "read" of your directory structure and update the drives/folders it shows.

Stop



Click this button to have PC-cillin terminate a scan in progress. **Note:** scanning may continue to occur for several seconds after clicking stop while buffered operations are completed.

Pause_Continue



Pause: click this button to have PC-cillin temporarily suspend a scan in progress. **Note:** scanning may continue to occur for several seconds after clicking stop while buffered operations are completed.

Continue: click this button to have PC-cillin resume scanning. This button is only visible after Pause has been clicked

Help



Click this button to start **Point & Click Help**. Comprehensive, indexed, and searchable on-line help is available from the main PC-cillin menu. Click **Help** and then **Contents** to run a Help query.

Close



Click this button to shut the Scan window and return to the Drive/Folders screen. If **Close** is grayed out, click **Stop** to halt a scan in progress and then click **Close**.

Current action



When PC-cillin is performing a scan of selected drive/folders and file types, this field shows the status. Typically, this is scanning.

File being scanned



Shows the current file, directory included, that is being scanned. Watch this line to get an idea of how fast PC-cillin can check a given file. Zipped files and documents containing macros may take longer to scan.

Elapsed time



This "stop watch" shows how long PC-cillin has been scanning selected drive/folders and file types. If you feel the scan is impossibly fast, check whether you are scanning *all files*, or only *selected file types*.

Virus found



Displays the total number of viruses found during the current scan.

Files scanned



Displays a running total of the number of files scanned thus far.

Progress bar



Provides a graphical indication of how much of the total drives/folders have been scanned and how much remains. Use the progress bar to "guesstimate" how long the scan task will take.

Infected file list



Shows the name of any file found to be infected with a virus during the current scan, the name of the virus, and the action taken. Statuses include "No Action Taken," (when the Manual Scan action is set to **Pass**), "Quarantined," "Deleted," "Renamed," and "Cleaned." Files for which no action has been taken can be "Quarantined," "Deleted," "Renamed," and "Cleaned." on a case by case basis by highlighting the infected file, then clicking the button for the action you want to take.

Note: When PC-cillin encounters an infected file that is part of a compressed volume, the **Status** will read "Unable to ...". In this case, you can delete the entire compressed file, or decompress the infected file -- if **Real-time Scan** is enabled, PC-cillin will detect the virus and then take whatever action has been configured.

Last Run



The **Last Run** field shows the last time a task was run, either manually or automatically. No time appears if the task has not yet been run.

The **Next Scheduled Run** field indicates when next the task will run. A value of *None* in the **Next Scheduled Run** field indicates that the task is not scheduled -- it will only run if you highlight it and click the **Run** button.

Scan tasks



Scan Manager tasks are a quick and easy way to perform a variety of scans. For example, to scan all the files on all your drives, highlight **Complete scan after installation** and then click **Run** to start the task.

For more information, click any of the links below to find out what that task does.

[Complete scan after installation](#)

[Scan for macro viruses](#)

[Scan C:\ drive weekly](#)

[Scan everything monthly](#)

[Scan floppy A:\](#)

[Scan Internet related files](#)

[Scan all Word documents](#)

[Scan all Excel documents](#)

[Scan Program files](#)

Complete scan after installation



Run this scan task to do complete check of *all* files on *all* drives, for example just after installing PC-cillin. The boot sector of your `c:\` drive will be scanned. Run the scan by clicking the task name and then the **Run** button.

Infected files are backed up before cleaning. Uncleanable file are quarantined (i.e., renamed and moved to the `\Trend PC-cillin 6\quarantine` directory).

Scan for macro viruses



Run this scan task to check Word and Excel documents on all drives. Specifically, the file types scanned are Word (.doc, .dot) and Excel (.xla, .xls).

Run the scan by clicking the task name and then the **Run** button.

Scan C drive weekly



This scan task is scheduled to run automatically every Friday at 5:00 p.m. (provided your computer is on at time). Highlight the task name, click **Edit**, and then click the **Schedule The Task** tab to change the time, day, or frequency of the task. It will do complete check of *all* files on your c:\ drive, including the boot sector. Infected files will be backed up before cleaning. Uncleanable files will be quarantined (i.e., renamed and moved to the \Trend PC-cillin 6\quarantine directory).

Scan everything monthly



This scan task is scheduled to run automatically at 5:00 p.m. on the first of every month (provided your computer is on at time). Highlight the task name, click **Edit**, and click then the **Schedule The Task** tab to change the time, date, or frequency of the task. It will do complete check of *all* files on *all* drives, including the boot sector. Infected files will be backed up before cleaning. Uncleanable files will be quarantined (i.e., renamed and moved to the \Trend PC-cillin 6\quarantine directory).

Scan floppy A:



Run this scan task to do complete check of *all* files and the boot sector of the floppy in your a:\ drive, for example if you are doing a batch cleaning of a bunch of floppies. Run the scan by clicking the task name and then the **Run** button.

Infected files will be backed up before cleaning, and uncleanable files will be quarantined (i.e., renamed and moved to the \Trend PC-cillin 6\quarantine directory).

Scan Internet related files



Run this scan task to check all Internet-related files on all drives. These files types are .cab, .cla, .class, .jar, .ocx, and .zip. Run the scan by clicking the task name and then the **Run** button.

Infected files will be backed up before cleaning, and uncleanable files will be quarantined (i.e., renamed and moved to the \Trend PC-cillin 6\quarantine directory).

Scan all Word documents



Run this scan task to check all Microsoft Word documents and templates on *all* drives. These files types are .doc and .dot. Highlight the task name and click **Edit** if you want to specify a particular directory. Run the scan by clicking the task name and then the **Run** button. Infected files will be backed up before cleaning, and uncleanable files will be quarantined (i.e., renamed and moved to the \Trend PC-cillin 6\quarantine directory).

Scan all Excel documents



Run this scan task to check all Microsoft Excel documents and templates on *all* drives. These files types are `.xla`, `.xls`, and `.xlt`. Highlight the task name and click **Edit** if you want to specify a particular directory. Run the scan by clicking the task name and then the **Run** button. Infected files will be backed up before cleaning, and uncleanable files will be quarantined (i.e., renamed and moved to the `\Trend PC-cillin 6\quarantine` directory).

Scan program files



This scan task is scheduled to run automatically at 5:00 p.m. on the first of every month (provided your computer is on at time). Highlight the task name, click **Edit**, and click then the **Schedule The Task** tab to change the time, date, or frequency of the task. It will do complete check of *all* program files on *all* drives, including the boot sector. Infected files will be backed up before cleaning, and uncleanable files will be quarantined (i.e., renamed and moved to the \Trend PC-cillin 6\quarantine directory).

Run



Highlight a scan task in the list above and click this button to start the scan immediately.

New task



Click this button to initiate a new scan task.

Edit



Highlight a scan task in the list above and click this button to check or change task details such as what drives/folders to scan, which file types to scan, the action to take, and the frequency of the scan.

Delete task



Highlight a scan task in the list above and click this button to remove the scan task.

Copy task



Highlight a scan task in the list above and click this button to copy the details of the scan task to memory. **Copy** is used with **Paste** to base a new task on an existing one.

Paste task



Highlight a scan task in the list above and click this button to paste a scan task you have *copied*. **Paste** is used with **Copy** to base a new task on an existing one -- for example, after pasting, you can click **Edit** and then change one or two details to create a new task.

Scan Task Wizard



Use the PC-cillin Scan Task Wizard to create any number of scan tasks, designed, for example, to scan only compressed files, all files on a removable disk drive, or only files located in a particular directory.

Task Name



Give the task you are creating a name. Names are usually descriptive and will summarize what the task is designed to do.

Scan All Drives



Choose this option to have PC-cillin scan all drives, including an mapped network drives (office users only).

Scan Selected Drive



Choose this option to specify a single drive that you want PC-cillin to scan.

Available Drives



Click this drop-down box to display a list of local drives. If you are on a network, remove network volumes that are mapped to your local computer will also appear in this list. Click the drive you want PC-cillin to scan.

Scan Selected Files/Folders



Choose this option to specify which individual files and/or folders you want to scan, then click **Add File**, **Add Folder**, or **Delete** to edit the list below.

- ◆ Click **Add File** if you just want to set up a routine check of an individual file. Then, in the Open window that appears, use **Look in:** to locate each file you want scanned.
- ◆ Click **Add Folder** if you want to set up a routine check of an individual drive or directory. Then, in the Open window that appears, use **Look in:** to locate and select the folders you want scanned.
- ◆ Click **Delete** to remove a drive, folder, or file from the list to be scanned.

Set Task Schedule



You can have PC-cillin automatically run the tasks you create at the frequency you specify, or you can set the frequency to "Not Scheduled" to start the task only when you click the **Run** button.

Frequency



Update Later scheduling choices include "Daily", "Weekly", and "Monthly". For **Scheduled Tasks**, all of the above apply. In addition, you can use "Not Scheduled" to run the task manually.

Time



Time is on a 24 hour clock. P.M. hours are converted below:

24-HR 13 14 15 16 17 18 19 20 21 22 23 24

12-HR 1 2 3 4 5 6 7 8 9 10 11 12

A.M. hours, of course, are the same for both clocks.

Day



This options is available when Weekly is selected as the frequency.

Date



This options is available when *Monthly* is selected as the frequency.

Do you want to run this task now?



Click **Yes** and then the Finish button to run an immediate scan of the task you just created. Another way to run immediate scan of a given task is to click the **Run** button on the Scan Manager page.

Update Wizard



Use the Update Wizard to update the virus pattern file PC-cillin uses to detect viruses and to perform automatic program upgrades. Alternatively, you can schedule PC-cillin to automatically dial into the Internet and download the necessary files. These updates require no user intervention (i.e., you don't need to do anything special to install the files). Once the update is complete, PC-cillin will close to the taskbar.

Last Update



Tells the date of the last program/pattern file update.

Virus Pattern File Update Wizard



Shows the date of the last virus pattern file update. If this date is more than one month old, we recommend that you do update the files as soon as possible (to keep current with newly released viruses).

Program



Shows the date of the last program file update. Program files include the main PC-cillin module and scan engine. If this date is more than a few months old, we recommend that you do update the files as soon as possible (to keep current with an program enhancements that are available).

Current Pattern No



Shows the virus pattern file number, or version, that is currently being used on your computer. Virus pattern files are named as follows: `lpt$vpn.465` and are kept in the `\Trend PC-cillin 6` directory. If multiple virus pattern file are in the directory, only the one with the highest number is used.

Update Now



Perform an immediate update of the virus pattern file, either from the root directory of a local drive, or via Internet.

From Drive



Click this option, then the **Next** button if you have a current copy of the virus pattern file on a floppy disk (for example the computer you are using PC-cillin on does not have Internet connection), or in the *root* directory the `c:\` or another drive (that is, not in a folder or subdirectory). Only the virus pattern file can be updated from a drive.

Select Drive



Select a drive from the drop-down list. Only the virus pattern file can be updated from a drive (not the program files), and then only if it is located in the root (for example, choose **[a]** if you have a copy of the virus pattern file located in a:, for example, a:\lpt\$vpn.465 -- not a:\temp\lpt\$vpn.465.)

Use this option, for example, if you download the virus pattern file from Trend's web site using the Internet at work, then take the file home on a floppy drive.

From Internet



Click this option, then the **Next** button to have a PC-cillin download the latest virus pattern and program files from Trend. If you are already connected to the Internet, the download begins immediately. If you are not connected, PC-cillin will start your dial-up connection if you are using the Window 98 dialer.

Proxy Server Configuration



A proxy server is an intermediate server that typically sits between the end user (you) and the main server. It can be used to provide some forms of security and to speed download times. Most home users do not use a proxy server, but many offices, schools, and some Internet Service Providers do. If you are having trouble downloading virus pattern files and/or program updates, it may be because you do you a proxy server but it has not been identified or there is an error in the address/credentials.

See also:

[How Can I Tell If I Am Using A Proxy Server?](#)

How can I tell if I am using a proxy server?



If there is a proxy server between your computer and the Internet, chances are that your web browser will be configured to make use of it.

The procedure for checking the proxy settings (if any) of three browser are listed below:

[Netscape Navigator 3.x](#)

[Netscape Navigator 4.x](#)

[Internet Explorer 4.x](#)

Check the on-line help that came with your browser for complete details.

Netscape 3.x Proxy Settings

1. With the browser open, click **Options** in the main menu, then **Network Preferences...**
2. Make the **Proxies** tab active.



If **No Proxies** is checked, you probably don't use a proxy to connect to the Internet.



If **Manual Proxy Configuration** is checked, click the **View** button and jot down the numbers you see for **HTTP proxy** and **Port**.



If **Automatic Proxy Configuration** is checked and a web address specified, check with your ISP or network administrator to find out your proxy settings. If you see a domain name (e.g., www.trend.com) and port number, jot these down.

3. In the **PC-cillin Updating through Proxy Server** screen, enter in the **Proxy Server Configuration** fields the numbers (e.g., 123.12.12.123 for **HTTP** and 80 for **port**) you jotted down in the last step.

Netscape 4.x Proxy Settings

1. With the browser open, click **Edit** in the main menu, then **Preferences...**
2. Click **Advanced** in the list of **Categories** and then **Proxies**.



If **Direct connection to the Internet** is checked, you probably don't use a proxy to connect to the Internet.



If **Manual proxy configuration** is checked, click the **View** button and jot down the numbers you see for **HTTP** and **Port**.



If **Automatic proxy configuration** is checked and a web address specified, check with your ISP or network administrator to find out your proxy settings. If you see a domain name (e.g., www.trend.com) and port number, jot these down.

3. In the PC-cillin **Updating through Proxy Server** screen, enter in the **Proxy Server Configuration** fields the numbers (e.g., 123.12.12.123 for **HTTP** and 80 for **port**) you jotted down in the last step.

Internet Explorer 4.x Proxy Settings

1. With the browser open, click **View** in the main menu, then **Internet Options....**
2. Make the **Connection** tab active.
3. If the **Access the Internet using a proxy server** box is checked, click the **Advanced** button. If it is not checked, you probably don't use a proxy to connect to the Internet.
4. Jot down the numbers you see for **HTTP** and **Port**.
5. In the PC-cillin **Updating through Proxy Server** screen, enter in the **Proxy Server Configuration** fields the numbers (e.g., 123.12.12.123 for **HTTP** and 80 for **port**) you jotted down in the last step.

My Internet Connection Is Through A Proxy Server



Check this option if you use a proxy server to connect to the Internet. Typically, larger offices, schools, and some Internet service providers will use a proxy. Users who dial into the Internet from home probably don't use a proxy.

[How Can I Tell If I Am Using A Proxy Server?](#)

Proxy Server Authentication



This option will not apply unless you connect to the Internet using a proxy server. If you've determined that you do use a proxy server, enter the IP address (or domain name) and port in the appropriate field. PC-cillin will go through the proxy specified here to complete the downloads.

[How Can I Tell If I Am Using A Proxy Server?](#)

Pattern Update: HTTP Proxy



If you use an HTTP proxy server on the network (for example, you use PC-cillin in an office, school, or your Internet Service Provider requires a proxy, enter the IP address (number) and port of this HTTP proxy in the fields provided.

In many cases, you can check whether you have a proxy server connection by checking the Advanced, or Options settings of your web browser.

[How Can I Tell If I Am Using A Proxy Server?](#)

Username and Password



If you use an HTTP proxy server on the network and users are required to log on, supply the appropriate log in credentials in the fields provided.

Pattern Update Status



If you are not connected to the Internet and use Windows 95 or Windows 98 for your Dial up connection, PC-cillin will start a dial up connection and prompt you to begin downloading the virus pattern file and/or program file updates. The combined file size is about 2 MB, which typically take from 5 to 15 minutes to download depending on the speed of your modem.

Process



Shows the current status of the virus pattern file update. Process statuses include:



Connection failure- indicates that a dial up connection could not be made (check your dialer, modem, and phone line. A good test is to try to connect with your ISP without using PC-cillin.)



Active update via Internet- indicates that the modem has been dialed and a connection is being made with your ISP



Version.ini -OKB/OKB-indicates that your computer has connected with the Trend Web site. At this point, PC-cillin should prompt you to continue with the update. If no prompt is made, and there is no activity on the progress bar, check your proxy server settings. Release.zip, pattern.zip, and other files will be downloaded to your computer, automatically decompressed, and installed.

Stop Update



Click this button to halt or interrupt a download, then click **Update Now** in the PC-cillin bar to return to the Update Wizard screen.

Enable Startup Update



This option is most useful for people who maintain a constant connection to the Internet, or those who only occasionally turn on their computer (and so would be unlikely to benefit from the periodically scheduled virus pattern updates).

With **Startup Update** enabled, PC-cillin will dial out to the Internet *X* minutes after the computer is started, and every *X* hours thereafter.

Update after startup



After starting your computer, PC-cillin will wait the specified number of minutes and then automatically contact Trend's web site to check whether a newer version of the virus pattern file exists. If so, the new pattern file will be downloaded and installed on your machine.

Trend publishes a new virus pattern file weekly; only if the pattern file on the website is newer than the one on your computer will it be downloaded.

Next updates every



Use this option to schedule how often PC-cillin will poll Trend's web site to see if there is a newer version of the virus pattern file. A setting of 24 hours is usually sufficient. Trend publishes new virus pattern files weekly unless a significant threat is discovered that warrants immediate protection.

Enable Scheduled Pattern/Program Updates



Check this box and schedule a frequency and time for PC-cillin to automatically download program and virus pattern updates. For home users we recommend that you update the virus pattern file no less often than monthly to stay current with newly released viruses. Office users, or those who frequently download file from the Internet and/or receive abundant e-mail attachments should consider scheduling weekly updates.

After updating the files, PC-cillin will shut down and restart -- minimized, as an icon on your Windows taskbar.

If you are not connected to the Internet and use Windows 95 or Windows 98 for your Dial up connection, PC-cillin will start a dial up connection and prompt you to begin downloading the virus pattern file and/or program file updates. The combined file size is about 2 MB, which typically takes from 5 to 15 minutes to download depending on the speed of your modem.

Update Virus Pattern File Only



Check this box to have PC-cillin download only the virus pattern file, about 800KB to 1 MB in size. This download typically takes from 3 to 8 minutes. Although download time will be faster, please note that you will miss out on PC-cillin's free program enhancements.

Enable Web Security



Select this option to enable/disable PC-cillin's filtering of harmful Java and ActiveX applets. You can also toggle (turn on/off) Web Security by right-clicking the PC-cillin icon in the Windows taskbar and clicking Web Security (a check means ON, no check mean OFF). Web security operates silently in the background. You don't need to configure anything.

Java and ActiveX applets (small programs) are automatically downloaded to you computer along with web page you are visiting. Hackers seeking to exploit this potential vulnerability have written applets that enter your computer in this way, then destroy data or steal information such as account number and passwords. With Web Security enabled, PC-cillin will monitor all applets downloaded to your computer and warn you whenever it encounters a suspicious one.

Action When Malicious Programs Are Found



When PC-cillin detects a potentially malicious Java or ActiveX applet being downloaded to your computer, you can have it block the applet or prompt you for a case by case decision on what to do.

Block Program



Choose this option for the most security. With **Block Program** selected, PC-cillin will prevent any applet it suspects of being harmful from being downloaded onto your computer and running.

Prompt For Action



Choose this option for the most leeway in choosing whether to block a suspect applet or allow it to be downloaded to your computer and run. PC-cillin will let you make the decision on a case by case basis. If you trust the web site where the applet was encountered, you may choose to accept the applet. If you are suspicious, or know nothing about the web site where the applet was encountered, you may decide that you want the applet blocked.

Show The Web Trap Welcome Screen Each Time You Start Your Browser



Select this option to have PC-cillin show a brief reminder whenever you start your web browser with PC-cillin's Web Security enabled. Remove the check to receive no such reminder.

Enable Web Filter



Select this option to enable/disable PC-cillin's filtering of web sites you consider offensive or objectionable. The Web Filter is completely user configurable, and only those sites you add to the list will be blocked.

Note: You can also toggle (turn on/off) the Web Filter by right-clicking the PC-cillin icon in the Windows taskbar and clicking Web Filter (a check means ON, no check mean OFF).

Restricted Site List



A list of the sites you have restricted is shown in this window. Restricted sites can be entered as follows: `www.xxx.com` and `http://www.xxx.com`. They are the same.

There are two ways to add web sites to the **Restricted Sites List**:

1. Click **Add**, then type the site's URL in the web address field that appears.
For example, `www.sex.com` or `http://www.sex.com`
2. If you currently are at a web site that you want to block access to, open PC-cillin and make the Web Filter page active. Click **Add**, and PC-cillin will automatically add the current URL to your Restricted Site List.

Delete URL



Highlight the restricted site you want to remove from the list and click the **Delete** button.
Note: the list is grayed out, or inactive, if **Enable Web Filter** is not checked.

Warn Before Entering A Restricted Site



Check this option to allow access to a restricted site, but only after popping up a warning, or reminder, that you have flagged the site as objectionable. Note: This option is grayed out, or inactive, if the **Enable Web Filter** options is checked.

Use Password



You can restrict access to this Restricted Site List page by creating a password. Only those who know the password can access the list. Click the **Set Password** button to create or change the password you use.

Enter Password



Enter a password, then retype it to confirm that it is what you expect. Capitalization, spaces, etc. are significant.

Caution! Use a password that you will remember. Lost or [forgotten passwords](#) cannot be replaced.

See also:

[Password problems](#)

Password Problems



Password doesn't work. Check if the **Caps Lock** key on the keyboard is engaged. If it is (the **CAPS LOCK** light is on) press the **Caps Lock** key to toggle it off. You may also want to toggle **Caps Lock** on and try entering your password again, in case it was on at the time you created the password



Password disappears every time you click Set Password. This is by design. Clicking the **Set Password** button clears out your old password. Once you leave the Web Filter screen and then return, the last password entered is the one that is used.

See also:

[I forgot my password](#)

Forgot Password



If you forget your **Web Filter** password, you will be unable to open the Web Filter screen. The filter itself, and other portions of PC-cillin, will continue function normally but you will not be able to edit the **Restricted Site List**. Your only alternative it to uninstall and reinstall PC-cillin, then recreate you **Restricted Site List**.

File Name



Lists the original file name of the infected file, before it was moved to the quarantine directory. PC-cillin renames the file and gives it a `.tmp` extension, while keeping track of the original name and location in a special database file. You won't be able to identify the file by its `.tmp` name. Nor should you open these files, as they will contain "live" viruses and may re-infect your system.

Original Location



Lists the original location of the infected file, before it was moved to the quarantine directory.

Quarantined



Lists the time and date that the infected file was moved to the quarantine directory.

Status



Lists the status of currently quarantined files, for example "cleaned," "unable to clean," or "No action taken" (occurs when Manual Scan's **Action When Virus Found** is set to **Pass**).

A quarantined file may not be cleanable if the virus has corrupted the file, or if the infected file is part of a compressed volume (such as .zip file or .arj. To clean the file, decompress it (scanning will automatically occur if Real-time Scan is enabled.)

Add Quarantined



You can directly move suspect files to the quarantine folder by clicking the **Add** button, then locating the file from the directory browser that appears. The file will be scanned before being added to the quarantine directory.

Clean Quarantined



Use this option, for example if you have set **Quarantine** as the action for PC-cillin to take upon detecting an infected file. Alternatively, if your virus pattern file has gone months out of date, you can download the most current version and click **Clean** to see if PC-cillin is able to clean it using the new pattern file.

Restore From List



Select a file from the **Quarantined** list and click this button to have PC-cillin revert the file back to its original name and return it to the directory of origin.

Note: if the original directory was renamed or deleted, PC-cillin will not be able to restore the file. Recreate the directory according to the information available from the **Original Location** field and click **Restore** again.

Delete From List



Select a file from the Quarantined list and click this button to have PC-cillin delete the file. Files deleted from the Quarantine are removed from the hard drive, not sent to the recycle bin.

Submit Quarantined



If you have quarantined a file you think is suspicious, click this button to submit a copy of it to the Trend Virus Doctors for analysis.

Submitted files will be cleaned, if possible, and returned (usually the next business day). Files that cannot be cleaned are not returned, in which case you can delete or restore the file.

Backed Up Items Overview



You can have PC-cillin back up infected files before attempting to clean them, for example if you want to ensure against possible data loss (viruses can corrupt a file and destroy both code and data; ridding the file of the virus may render the file unusable, although this is rare). Backed up files can be **Restored** or **Deleted**. Both the cleaned file and the backed up copy, which has been renamed with the `.VIR` extension, can be found in the original directory, as specified in the [Backup Item](#) screen.

Note: *backed up files are infected files!*

Backed Up



Lists the time and date that the infected file was backed up before cleaning.

Virus Name



Shows the name of the virus found to be infecting the file. **Note:** Backed up files will still contain this virus and should be deleted!

Virus Log



PC-cillin keeps a running log of its activity. New logs are created whenever a virus is detected and represent a valuable source of system information. Examine log entries by clicking a **Log Date** to find out:



The **time** the virus was detected



The **name** of the file infected



The name of the **virus**



The **action** PC-cillin took on the infected file



The **user name** of the person logged in at the time of the scan



The **type of scan** -- Real-time or a Scan Task -- that turned up the virus

Log Date



List the various days on which PC-cillin detected one or more viruses. Logs are only created when a virus is detected. Click the date to show the individual details for each virus incident.

Export Log



PC-cillin can export its log data to the standard CSV (comma separated values) format used by most spreadsheets and databases. For example, if you have Microsoft Excel 97 installed, simply double the .csv file you saved to open it as a spreadsheet.

An example virus log in CSV format, as seen when opened with Notepad:

Detected Virus List

Time,Infected File Name,Virus Name,Action On Virus,User Name,Scan Type

23:12:11,C:\swenson\backup.zip, ,Unable to clean. File quarantined.,David,Task Scan

23:12:11,C:\swenson\backup.zip (4096.COM),FRODO_FRODO.A-C,Unable to clean or quarantine,David,Task Scan

23:12:11,C:\swenson\virus.lzexe, ,Unable to clean. File quarantined.,David,Task Scan

23:12:11,C:\swenson\virus.lzexe (LZEXE),2144-1,Unable to clean or quarantine,David,Task Scan

21:18:09,C:\swenson\backup.zip, ,Unable to delete,David,Wizard Scan

21:18:09,C:\swenson\backup.zip (4096.COM),FRODO_FRODO.A-C,Unable to delete,David,Wizard Scan

21:18:09,C:\swenson\VIRUS.COM,FRODO_FRODO.A-C,Deleted,David,Wizard Scan

21:18:09,C:\swenson\CONCEPT1.DOC,WM_Generic0408,Deleted,David,Wizard Scan

Delete Log



Highlight the date you want to remove and click this button to have PC-cillin delete that day's logs from the computer.

Note



After downloading and then updating the virus pattern and/or program files (fully automatic), click this button to view the release note. Release notes contain pattern- and program-specific information.

Update Log



PC-cillin keeps a running log of its virus pattern and program file updates. New logs are created whenever a download is performed and represent a valuable source of system information.

Examine log entries by clicking a **Log Date** to find out:



The **time** the virus was detected



What file(s) were **downloaded** and installed from Trend Micro



The **status**--Success or Failure--of the download

Web Filter Logs



PC-cillin keeps a running log of its Web Security activity. New logs are created whenever a web site is blocked or harmful web content encountered. Examine log entries by clicking a **Log Date** to find out:



The **time** the virus was detected



The **URL**, or web address, that was blocked



The **Action** the web filter took: either *Deny Access* or *Warn*



The **user name** of the person making the URL request

Virus List



The Detectable Virus list contains a complete record of all viruses, variants, and malicious Java/ActiveX applets that the virus pattern file can detect. Currently, *PC-cillin* is capable of detecting well over 10,000 viruses and malicious codes, including more than 3,000 different macro viruses and their variants.

But most importantly, *PC-cillin* detects all viruses found to be "in the wild," or actively infecting people's computer files. The contents of the **Detectable List** will vary according to the version of the virus pattern you are using.

Version Information



PC-cillin optimizes performance by using a function-specific modular architecture. Version information tells the version and specific build of each module being used on the system. These components may be individually upgraded during a program and virus pattern file [Update](#). PC-cillin ships with following:

Version Information

Program: 4.50 Build 1723
(automatic upgrades, PC-cillin core files)

I/O Monitor: 4.03 Build 1412
(automatic upgrades, used for Real-time Scan)

Scan Engine: 2.040-1126
(automatic upgrades, used for Manual Scans)

Real-time Scan Eng. 2.20 Build 106
(automatic upgrades, used for Real-time Scanning)

Pattern Number: 465
(updates available, Internet)

License Information

Serial Number: Front cover of User's Guide,
none for the 30-day trial version

User Name: As entered during installation

Company: As entered during installation

Active Desktop



Microsoft's Active Desktop is an optional feature of both Internet Explorer 4.x and Windows 98 that allows you to display things on your desktop the same way they appear in your web browser. For example, you can run Java/ActiveX animations and accept real-time information streams from the web (as long as you are connected). It must be installed to display Trend's Active Desktop content.

Registered users of PC-cillin are entitled to download Trend's antivirus-related content for free.

Infected Files



What should you do if PC-cillin detects a virus? Kill it. That is, clean the file, kill the virus.

Here's how:

1. If you're running one of PC-cillin's pre-set tasks, any infected files are cleaned automatically. In this case you don't have to do anything except, perhaps, check the virus log and see the results.
2. If you're doing an immediate scan using the **Scan Wizard**, you can have PC-cillin take one of the following actions on any virus(es) that it turned up:



Clean infected files (you can also make a back up copy of infected files before it is cleaned)



Quarantine the infected file



Delete the virus, file and all



Pass over the file; you can then Quarantine, Delete, etc. on a case-by-case basis



Deny Access to the infected file so it cannot be used



Rename the file so it has a .VIR extension

Whatever action PC-cillin takes, a note of it is written to the log file .



We recommend that you *clean* infected files. If the file cannot be cleaned, for example because it is corrupted or because of the nature of that particular virus, then the safest thing to do is quarantine the file.

Files that turn out to be Uncleanable are usually program files (.exe, .com, .sys) rather than document files (.doc, .xls, etc.) and so are more easily replaced. You can just copy the file in question from the original program original disk(s) to the appropriate directory.

Scan Exceptions



You can set exceptions to PC-cillin's **Real-time Scan** so that certain files or directories are ignored. For example, **Quarantined** files are never included in real-time scanning-- it just wouldn't make sense (you know they're infected, that's why they've been quarantined!) You may have other files that you don't want real-time scanning to consider.

Real time Scanning



Real-time scanning provides constant protection against viruses. With real-time scanning turned on, you can dramatically reduced the chances of you computer even becoming infected with a virus in the first place.

Because it is so powerful (and because it operates imperceptibly in the background), we recommend that you always keep real-time scanning turned on.

The real-time scanner checks files for viruses whenever they are used, for example each time a file is opened, copied, moved, saved, compressed or decompressed, downloaded from the Internet, and, in the case of e-mail attachments, read.

Internet Virus Protection



Besides monitoring file operations, real-time scanning offers protection against viruses entering your system from the Internet via file downloads (HTTP and FTP) and through infected e-mail attachments. It even monitors compressed files such as ZIP as they are decompressed. Real-time scanning does not check every file, however. It monitors only those file types that are known to be the most susceptible to infection by a virus. Whenever a virus is detected the real-time scanner takes the action specified in the Real-time Scan Options screen.

Startup Scan



PC-cillin can run a quick scan of your critical system files before loading Windows. This is useful because Windows runs, opens, and closes hundreds of files during the course of normal operation. If any of these files are infected, the virus can be quickly spread throughout your system.

Note: Startup Scans can take anywhere from several seconds to several minutes to complete. Windows will not load until the scan is completed.

Virus Encyclopedia



PC-cillin includes a desktop version of Trend's virus encyclopedia, organized by name and virus type. Use it to find out about tens of thousands of individual viruses, including the typical symptoms of a given virus, its infection procedure, and the damage routine.

With the growing prevalence of Macro viruses, we've bolstered the number of Macro virus descriptions included in the encyclopedia to well over 2000.

Of course, PC-cillin, which uses Trend's award-winning, 32-bit, multi-threading scan engine, is capable of detecting all viruses that are known to be in circulation, plus the many thousands more that exist as "proof of concept" only in researcher's virus labs and on hacker's computers.

Channel Bar



A "Channel" is a Web site designed to deliver content from the Internet to your computer. It is similar to subscribing to a favorite Web site, in this case Trend's. As a part of the Trend Channel, you get a rich map of the Trend web site that allows you to quickly select and view any content you want.

You can use the Channel bar to quickly open Trend's web sites from your Active Desktop without first opening the browser. The Channel bar can be displayed on your desktop whether you have installed the browser-only version of Internet Explorer or the browser with the new desktop.

Viewing The Detectable Virus List



PC-cillin can detect tens of thousands of viruses. A complete description of the most common viruses can be found in the [Virus Encyclopedia](#) . You can also look up a particular virus in the Detectable List to check whether your current [virus pattern file](#) can detect it.

Here's how:

1. Click **Log** in the PC-cillin bar, then the **Virus Log** icon.
2. Click **Virus Info** on the main menu.
3. Click **Virus List** from the menu options that appear.
4. Click **Print** to make a hard copy of the list, or scroll the text box.

Note: for detailed virus information, please see the on-line Virus Encyclopedia, or visit our web site at <http://www.antivirus.com> for additional antivirus information and resources.

If a particular virus does not appear in the list, try updating to the latest virus pattern file. Trend publishes new virus pattern files weekly for download.

Making a Rescue Disk



A "**rescue disk**" is a bootable floppy disk that PC-cillin can create. Rescue disks should be checked for viruses and write protected. In addition to this disk, PC-cillin backs up some critical systems files and copies them to two additional floppies. We strongly recommend that you have PC-cillin create rescue disks for you during installation. If you choose to defer, however, please be sure to make them as soon as possible.

Note: Do not restart your computer using a rescue disks that was created for PC-cillin II or PC-cillin 97 -- data loss can result.

Here's how:

1. Label your three floppies **PC-cillin Rescue Disk 1, 2, & 3**, then insert the first into the a:\ drive.
2. Click the Windows **Start** button, then **Programs** and **Trend PC-cillin 6.0**.
3. Click **Create rescue disk**, then the **Start** button in the windows that appears.
4. As each floppy is finished, remove it and immediately write protect it by sliding *up* the plastic button that is in the upper left hand corner of the back of the disk. The disk is write protected when you can see through both squares in the upper corners. Creating the **rescue disks** takes about 10 minutes.

Note: You cannot make rescue disks on a machine infected with a boot virus. Be sure to clean (or delete) any viruses that have been detected. See below for details on recovering from a boot virus.

See also:

[If You Have A Boot Virus](#)
[Updating Rescue Disks](#)

Updating Rescue Disks



If you've already got a set of rescue disks from a previous version of PC-cillin, you should nevertheless create a new set after installing PC-cillin 6. Likewise, if you created your rescue disks under Windows 95 and have subsequently upgraded to Windows 98, you need to create a new set of rescue disks. Of course, you can re-use your old floppies for the new disks. All data on the old disks will be lost in the creation of the new disks.

Note: *Do not restart your computer using a rescue disks that was created for PC-cillin II or PC-cillin 97 -- data loss can result.* Nor should you boot from rescue disks created for Windows 95 if you are running Windows 98 (and vice versa).

See also:

[If You Have A Boot Virus](#)

Using Scan Wizard



PC-cillin's [Scan Wizard](#) makes it easy to check a given drive, directory, or file type for viruses. A selection of pre-configured scan tasks is also available via [Scan Manager](#) .

Here's how:

1. Click **Update** in the PC-cillin bar, then the **Scan Wizard** icon.
2. Click the **Description** that identifies what you want to scan, then click **Next**.
3. Depending on the **Description** you have selected, the Scan Wizard will guide you through a series of scan options or do a quick scan of the individual file or floppy.
4. Click the **Scan** button to begin scanning or **OK** to finish the Wizard.

Using Scan Manager



One especially convenient feature of PC-cillin is that it comes pre-configured to automatically run a variety of scans -- you don't *have* to *do* anything to protect your computer against viruses. You can also control which scans to run and when -- just highlight the **Description** of the Scan Manager task you want to run and click **Run**. Or, you can create your own tasks.

Here's how:

1. Click **Scan** in the PC-cillin bar, then the **Scan Manager** icon.
2. Click **New Task**, then type in a name for your task in the **Task Name** field, for example, **Scan ZIP Drive**.
3. Choose the items that you want PC-cillin to scan, then click **Next** and select the options you want. For example, **All file types**, **Clean**, and **Quarantine**.
4. Click **Next** again. In the **Schedule** window, specify how often you want the scan task to run and fill in the time/date option as appropriate.
Note: If you don't want PC-cillin to automatically run the scan, choose **Not Scheduled** for the **Frequency**.
5. Click **Finish** to save your scan task and add it to the list of Scan Manager tasks.
 - ◆ You can also select **Yes** before clicking **Finish** to run the scan immediately.

Using Update Now



Use **Update Now** to connect to Trend's web site and start downloading the [virus pattern file](#) and/or program file upgrades. The download will occur only if the files on your computer are older than those available at the web site.

Here's how:

1. Click **Update** in the PC-cillin bar, then the **Update Now** icon.



Choose **From drive** if you have a copy of the virus pattern file on a floppy disk, for example, or in the root directory of you hard drive or a network drive.



Choose **From Internet** to download both the virus pattern file and any program upgrades from Trend.



Click **Use Proxy Server** to specify (or confirm) [your proxy server settings](#) .

2. Click **Next** to have PC-cillin contact Trend and begin downloading the files or reading the file from the root directory of the drive specified. Installation is automatic, and occurs immediately upon download.

Note: If you use the Windows' **Dial Up Networking** to connect to the Internet, PC-cillin will start your dialer automatically. If you use different Internet connection software, you need to make the connection first, before using **Update Now**.

Only registered users are eligible for virus pattern updates.

Using Update Later



Update Later allows you to automate the task of keeping your virus pattern file up-to-date. It is especially practical for users with a constant Internet connection, or those who use their computer often.

1. Click **Update** in the PC-cillin bar, then the **Update Later** icon.
2. If you have a permanent connection to the Internet, *or* if you very seldom turn your computer on, click **Enable Startup Update to have PC-cillin** connect to the Internet *X* minutes after the computer is started, and every *X* hours thereafter. Typical settings for these options are 30 minutes and 24 hours, respectively.
3. Next, click **Enable Scheduled Update** and choose how often you want PC-cillin to update the pattern file.

Trend publishes virus pattern updates weekly, but unless you are a heavy user of the Internet, frequently send and receive file via e-mail, or are connected to a network, biweekly or monthly virus pattern updates are most likely sufficient. Microsoft [Active Desktop](#) users can stay abreast of the latest virus news by adding the Trend Virus Calendar to their desktop.

4. Check **Update virus pattern file only** to skip program updates (this can reduce download time by 30 to 50 percent, but you risk missing valuable program upgrades as a result).
5. If you use a proxy server, click the **Set Proxy...** button and enter your [proxy information](#) as appropriate.

Using Web Security



Web Security protects against malicious Java and ActiveX applets. Although most web sites are completely harmless, it is possible, and it does happen, that someone will create a small program and set it to run, invisibly, whenever their web page is accessed. These programs may destroy data, steal your passwords, financial data, etc. PC-cillin's Web Security protects you against these threats.

Here's how to use Web Security:

1. Click **WebTrap** in the PC-cillin bar, then the **Web Security** icon.
2. Next, put a check in the **Enable Web Security** box and click **Prompt for action** to have PC-cillin inform you of the potentially harmful web program. Otherwise, check **Block programs** to have PC-cillin perform the action automatically.

With Web Security enabled, PC-cillin will monitor all Java and ActiveX applets that are silently downloaded to your computer whenever you are browsing the Web.

Using Web Filter



For protection against offensive web contents, PC-cillin also offers **WebTrap**, Trend's user-configurable utility that let's you make whatever web sites you want "off limits" to other users of the computer.

Here's how:

1. Click **WebTrap** in the PC-cillin bar, then the **Web Filter** icon.
2. Put a check in the **Enable Web Filter** box.
3. Add one or more URLs to the **Restricted Sites** box.
 - ◆ If your web browser is currently opened to an objectionable site, click **Add** to automatically add the URL to the **Restricted Sites** box.
 - ◆ If you want to enter a lot of different URLs, click **Add** for each URL. Be sure to include the `http://www` prefix if appropriate.
4. Check **Extend to all sub-pages** to have PC-cillin block the entire web site, not just the specified page.

Access to your list of URLs can be password protected. Check **Enable password** and enter a password to have PC-cillin prompt for this password the next time the **Web Filter** screen is opened.

Using Quarantine



Let's say you've got a file that you suspect is infected but your not sure. Or, let's say you have an infected file that, for whatever reason, PC-cillin couldn't clean but you are reluctant to delete it. In these cases, we say "Quarantine it."

Here's how:

1. Click **Quarantine** in the PC-cillin bar, then the **Quarantine** icon that appears.
2. Click **Add**, then browse your directory to find the file you want to quarantine and then double-click the file you want to quarantine. PC-cillin will perform a quick scan and tell you whether it appears to be infected.



PC-cillin finds a virus: **Clean it**, or move it to the **Quarantine** directory without cleaning



PC-cillin doesn't find a virus: **Quarantine** it anyway, or leave it alone.

Using Backup Items



Before cleaning a file, you can have PC-cillin make a back-up copy (backed up items are infected files that have been cleaned) You might choose to back up files before cleaning, for example, if you are concerned that the virus, or the process of removing it, may damage the file. **Note:** The backed file will still contain the virus! Be sure do delete it once you know the cleaned copy is fine (not corrupted).

Here's how to enable Backup :

1. Click **Options | Manual Scan** in the PC-cillin menu.
2. Under **Action when Virus Found**, choose **Clean** and click **Back up files before cleaning**.

This will set the default for all new Scan Wizard scans to include backing up. For the existing Scan Manager tasks, files are already backed up before cleaning.

Here's how to Delete or Restore backed up files:

1. After you've tested the cleaned file, click **Quarantine** in the PC-cillin bar, then the **Backup Items** icon that appears.
2. A list of currently backed up files appears. Highlight the file you want to **Delete** or **Restore** and click the appropriate button.

Note: Backed up files can contain live viruses. In most cases, you should delete the backed up files rather than restore. Use **Restore**, for example, if the cleaned file is a data file and has become corrupted and you must recover the data it contains. If you do restore an infected file, *DO NOT OPEN IT USING THE DEFAULT APPLICATION!* For example, to open an infected Word document, use a hex editor or try using the Notepad program -- the word macro virus will not find the environment it needs to spread.

Using Virus Log



PC-cillin keeps a running record of all the viruses it detects and the action that was taken. These logs can be viewed from **Virus Log**.

Here's how:

1. Click **Log** in the PC-cillin bar, then the **Virus Log** icon that appears.
2. One log appears for each day that virus activity was detected. If multiple virus incidents occurred on the same day, you'll notice an associated list on the right.

Virus log information includes the following:



Time: States the time and date that the virus was detected.



Infected File Name: Shows the name of the file in which the virus was detected.



Virus Name: Shows the name of the virus that was detected.



Action On Virus: States the action that PC-cillin took on the infected file (as specified in the [Scan Options](#)).



User Name: Indicates the Windows profile, if any, that was being used at the time the virus was detected.



Scan Type: Shows the type of scan (real-time, manual, etc.) that detected the virus.

Using Update Log



PC-cillin keeps a running record of each time it contacts Trend to update the virus pattern file or upgrade its program files. These logs can be viewed from **Update Log**.

Here's how:

1. Click **Log** in the PC-cillin bar, then the **Update Log** icon that appears.
2. One log appears for each day that virus activity was detected. If multiple virus incidents occurred on the same day, you'll notice an associated list on the right.

Using Web Filter Log



PC-cillin keeps a running record of all the viruses it detects and the action that was taken. These logs can be viewed from **Web Filter Log**.

Here's how:

1. Click **Log** in the PC-cillin bar, then the **Web Filter Log** icon that appears.
2. One log appears for each day that virus activity was detected. If multiple virus incidents occurred on the same day, you'll notice an associated list on the right.

Using Support Wizard



The Support Wizard will guide you through the process of contacting technical support.

Technical Support

Trend Micro provides free technical support, virus pattern downloads, and program updates to all registered users. You can contact technical support via e-mail, on-line chat, or by phone.



Trend Technical Support

2171 Campus Drive, Suite 370

Irvine, CA 92612

E-mail: Support@trendmicro.com

URL: <http://www.antivirus.com>

Phone: (949) 387-7800

Fax: (949) 387-7801

Hours: 8:00 AM to 5:00 PM Monday – Friday (Pacific Standard Time)

Using On-line Chat



On-line chat is available from 7:00 A.M. to 11:00 P.M. Pacific Standard Time. You can use chat to converse, live and in real-time, with Trend's technical support and/or Virus Doctors.

E-mailing Technical Support



E-mail support is free and available 24-hours a day 7 days a week. In most cases, you will receive a response within one business day.

E-mail address: ts-support@trendmicro.com

Cyber Clinic



The Trend Cyber Clinic is free and available 24-hours a day 7 days a week.

Using Active Desktop



Active Desktop is a feature of Microsoft's Internet Explorer version 4.x (when used with Windows 95). It can also be installed as a part of Windows 98. For details, see Microsoft's IE 4.x or Windows 98 documentation.

PC-cillin uses Active Desktop as a means of keeping up with the latest in virus news. With Active Desktop, you can turn web elements from Trend's award-winning web site, <http://www.antivirus.com>, into desktop elements and update them at any time.

Adding or removing PC-cillin from an Active Desktop...

1. In the main menu, click **Options | Active Desktop**.
2. Click the **Add Trend Virus Calendar To Active Desktop** option to enable content streaming.

Starting or stopping Active Desktop...

Provided that **Active Desktop** has been installed with Windows 98, turn it on/off as follows:

1. Right-click a spot on your desktop where there are no icons, open windows, etc.
2. In the menu that pops up, **Active Desktop** will appear if the feature is installed.
3. Check (or Uncheck) the **View as Web Page** option to turn the feature on or off.

See also:

[How do I know if I have Active Desktop Installed?](#)

How do I know if I have Active Desktop Installed?



Active Desktop is a feature of Internet Explorer 4.x (with Windows 95), or it can be optionally installed as a part of Windows 98. To receive the Trend Virus Calendar, Active Desktop must be installed. Here's how you can find out:

1. Click the Windows **Start** button.
2. Click **Settings**, then **Active Desktop**.
3. If **Active Desktop** does not appear, chances are it is not installed.

Another way to tell if Active Desktop is installed is by right-clicking a spot on your desktop where there are no icons, open windows, etc. In the menu that pops up, **Active Desktop** will appear if the feature is installed. (You can then check (or uncheck) the **View as Web Page** option to turn the feature on or off.)

For instructions on installing Active Desktop, see your Microsoft Windows 98 or Internet Explorer 4.x documentation.

Using Channel Bar



There are two ways to display the channel bar, depending on whether you installed only Internet Explorer or Internet Explorer and a new desktop.

There are also two ways to display a Channel within the bar. All are explained below.



To display the Channel bar if you installed only Internet Explorer:

1. Click the **Start** button, then **Programs | Internet Explorer | Channel Bar**.



To display the Channel bar if you installed the new desktop with the browser:

1. Click the **Start** button, then **Settings | Active Desktop | Customize my Desktop**.
2. Make the **Web** tab active, then click **View my Active Desktop as a web page**.
3. Choose **Internet Explorer Channel Bar**.

(**Note:** close the Channel bar by clicking the top of the Channel bar, then the **Close** button that appears.)



To display a Channel in the *browser*

1. Click the **Channels** button on the toolbar.
2. In the **Explorer** bar, click the channel or category you want to view.

(**Note:** hide the Explorer bar by clicking the **Channels** button on the toolbar again.)



To display a Channel on the *desktop*

1. Right-click the desktop, then click **Properties**.
2. Make the **Web** tab active, and then **New**.
3. Click **No**, then type in Trend's web address: www.antivirus.com in the dialog box that appears.

Using the Virus Encyclopedia



To use the Virus Encyclopedia,

1. In the main menu, click **Virus Info**, then **Virus Encyclopedia**.
2. Choose a **Virus Type** (Common Viruses, Boot Sector, Parasitic, Macro, or All), then select a virus from the list that appears in **Virus List:** box.

Note: Because of the enormous number for viruses the PC-cillin can detect and the rate at which new viruses are created, a **Description** may not be available for a given virus.

Using Manual Scan



The configuration settings specified in the Manual Scan screen are used by default for new Scan Wizard tasks and for Virus Property scans.

Here's how:

1. In the PC-cillin menu, click **Option | Manual Scan** to bring up the Manual Scan configuration screen.
2. Choose the configuration options you want uses in manual scans, for example **All file types**, **Clean**, and **Quarantine**, and click **Apply**.

Using Real-time Scan



When enabled, PC-cillin's Real-time Scan provides constant protection against viruses by doing a quick check of each file as it is used. Real-time scanning takes place in the background and requires no user intervention, so you don't really have to do anything to "use" Real-time Scan -- just be sure it is enabled.

Here's how:

1. Click **Options | Real-time Scan | Scan Options** from the main menu.

From this screen, you can toggle [Real-time scanning](#) and set global scanning properties (including **Scan Options** and the **Action When Virus Found**) that in use for all [real-time scanning operations](#).

An even faster way:

2. A faster way to do the same thing is by right-clicking the PC-cillin icon on the Windows taskbar. In the pop-up menu that appears, a check will appear before **Real-time Scan** if it's enabled.

Using Startup Scan



You can have PC-cillin run a **Start-up Scan** to check critical system files for viruses each time you start your computer, before loading Windows.

This scan can take anywhere from a few seconds to a minute or so, depending on your system configuration (CPU speed, memory, the commands in your `config.sys` and `autoexec.bat`, etc.)

To turn on/off the Start-up Scan,

1. From the PC-cillin main menu, click **Options**.
2. Click **Startup Scan**. A check indicates that Startup Scan is enabled.

PC-cillin performs a **Startup Scan** by default, unless you disable the options.

Setting Default Scan Wizard Values



From the Manual Scan screen, you can set the default scanning properties (including **Scan Options** and the **Action When Virus Found**) used by the [Scan Wizard](#) for the Drives/Directories option.

Here's how:

1. From the main menu, click **Options | Manual Scan**.
2. Select the options you want, for example, **All file types**, **Clean**, and **Quarantine**.
3. Click **Apply** to save your configuration.

Of course, you can also configure new Scan Wizard tasks individually, on a case-by-case basis.

Uninstalling PC-cillin



Before uninstalling PC-cillin, be sure to stop Real-time scanning. You can do this by right-clicking the PC-cillin icon on the [Window taskbar](#) and then clicking **Real-time Scan** to remove the check, if any. The icon appears as a white lightning bolt when real-time scanning is disabled. During uninstall, PC-cillin deletes all quarantined files. These files may contain “live” viruses and should not be left on your computer. If you must preserve them, we suggest that you copy the entire directory to a safe location such as a specially marked floppy disk.

There are two ways to run uninstall,

1. Click the Windows NT **Start** button, then **Programs | Trend PC-cillin and Uninstall Trend PC-cillin**.
2. Double-click **My Computer**, the **Control Panel** and then **Add/Remove Programs**. Choose **Trend PC-cillin** from the list that appears.

See also:

[Upgrading From A Trial Version](#)

[Registering PC-cillin](#)

Cleaning Boot Viruses



Boot sector viruses are especially troublesome (and dangerous) viruses because they occupy a sensitive part of the hard drive, the boot sector, and load into memory whenever the system is started. From memory, they spread easily to any files that are subsequently opened and floppy disks that are used.

So, a boot virus is no ordinary virus and some special steps are required.

Dealing with a boot virus

1. The first thing you need to do is get a *clean*, bootable floppy disk (for example the Startup disk you made when installing Windows 95 or 98).

If you don't have one, borrow one -- it's too late to make one on the infected machine. If you have another computer with the *same* OS (Windows 95 or 98), you might be able to make a [Windows Startup disk](#) , but be sure that machine is not also infected, and be sure to [write protect](#) the disk before using it.

2. Then, when prompted by PC-cillin, insert the floppy into the a:\ drive and restart your computer.
3. When the computer restarts, you'll see a [DOS prompt](#) . Enter the following, commands, pressing the enter key after each line:

```
c:                                     [press enter]
cd pcscan.tmp   [press enter]
pcscan /V /A    [press enter]
```

The last command tells PC-cillin to scan and clean all files on all drives, including the boot sector.

Be aware: boot viruses spread easily. If PC-cillin detected a boot virus, it is very likely that one or more of your floppy diskettes are also infected. Be sure to run the [Floppy Scan task](#) and check *all* your floppies for viruses.

Making a Windows Startup disk



You can use a Startup disk to boot (i.e., start) your computer in the event of a boot virus infection or other fundamental problem. If you don't already have a Startup disk, you can create one.

Note: Do *NOT* create a Startup disk from a computer that is infected with a boot virus!! If you must, relocate to another computer (for example one at work or at a friend or neighbor's) and create the disk from that machine. Alternatively, you can borrow a Startup disk to use for booting your computer -- but be sure that it is write protected!!

Here's how:

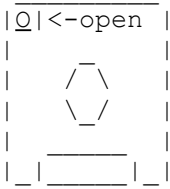
1. Click the Windows **Start** button, then choose **Settings**, and **Control Panel**.
2. Click Add/Remove Programs.
3. Click the **Startup Disk** tab to bring it forward.
4. Insert a (non-write protected) floppy disk into the a:\ drive.
5. Click the **Create Disk** button.

When using a Startup disk to boot your computer, be sure to use one created with Windows 98 to start a Windows 98 machine, or one created with Windows 95 to start a Windows 95 machine.

Write Protecting a Disk



In a write-protected disk, the plastic switch in the upper left-hand corner is up, so you can see through it.



(Look at the back of the disk, the side opposite the label, with the sliding panel at the bottom. The slider in the upper left corner should be in the UP position.)

The reason you want the disk write protected is because boot viruses always try to infect the boot sector of any floppy that is used to start the computer. Write protecting the disk makes it impossible for the virus to transfer a copy of itself from your hard drive to the floppy. You should also write protect your rescue disks one they are made.

Dealing with Infected Files



If PC-cillin detects a virus you can have it take one of the following actions:



Clean infected files (you can also make a back up copy of infected files before it is cleaned)



Quarantine the infected file



Delete the file, virus and all



Pass over the file



Deny Access to the infected file so it cannot be used



Rename the file so it has a .VIR extension

Whatever action PC-cillin takes, a note of it is written to the log file .

Checking A File For Viruses



PC-cillin can run a quick check of any file, for example if you want to double check a compressed file before e-mailing it to someone.

Here's how:



If you're using Explorer, right click the file or folder you want to scan. Then, in the menu that appears, choose the **PC-cillin** option. PC-cillin will scan the file according to the preferences you have selected for [Manual Scan](#).



The fastest method, available whenever you are using Windows Explorer, is to right-click on the file in question. Choose **Properties** from the pop-up menu that appears, then click the **Virus Properties** tab. PC-cillin will run a quick scan of the file and let you know the results.



Another way to run a quick check of a file is by starting the **Scan Wizard** and selecting **Individual file**. In the window that appears, choose the file you want to scan and click **Open**. PC-cillin immediately gives you the results of the scan.



Finally, you can "drag" the file(s) in question over to the open PC window. Zap! That's it. As soon as you release the mouse button, PC-cillin checks the file for viruses and reports the status back to you.

Checking All Files For Viruses



Immediately after installing PC-cillin, and then periodically thereafter, we recommend that you run a complete scan of every file on every drive on your computer. Depending on how many files you have, such a scan can take from 10 minutes to an hour to complete.

Here's how:

1. Double-click the PC-cillin icon on the Windows taskbar.
2. Next, click the **Scan** button, then double-click the **Scan Manager** icon to bring up the list of tasks.
3. Select the first task on the list, **Complete scan after installation**, and click **Run**.

Viola! That's it. As easy as one, two, three.

Sending Trend Your Viruses



You can send trend your viruses. More specifically, if you have a file you suspect is infected with a virus but the scan engine doesn't detect it or can't clean it, send an e-mail with the file attached to the Trend Virus Doctors.

Here's how:

1. Click the **Quarantine** button in the PC-cillin bar, then the **Quarantine** icon that appears.
2. Select a file from the list and click **Clean** to try cleaning the file.
3. If it cannot be cleaned, you can click **Submit** to send the suspicious file to the Trend Virus Doctors for analysis.

Files may also be placed in your quarantined directory (the default is `c:\Program Files\Trend PC-cillin 6.0\Quarantine`) as a result of the [Action](#) selected for viruses detected during routine tasks or scans run via the Scan Wizard.

Our team of Virus Doctors (i.e. computer scientists) will "dissect" the file to identify and characterize any virus(es) it may contain. We will then contact you via e-mail to let you know what we've found.

Keeping Your Computer Virus Free



PC-cillin is already set up to keep you system virus-free. After installing, you don't *have* to do *anything* to ensure that your system stays virus-free. PC-cillin gives you this certainty using three layers of protection:



Scheduled Scans check the files most likely to be infected by viruses. These include Internet files and document files. Monthly files scans will check every file on the system.



Real-time scanning watches over your system and will detect a virus as soon as it arrives at your computer. Each time you **Open**, **Copy**, **Save**, or **Move** a file, the real-time scanner performs a quick check of the file. Because it work invisibly, in the background, you probably won't even know it's there.



Automatic virus pattern updates. If you are using your computer when a scheduled update is set to go off, PC-cillin will automatically dial-in to the Internet. The download occurs "silently," if you are already connected to the Internet.

Guarding Against New Infections



PC-cillin is already set up so that every month, when you are connected to the Internet, it will automatically contact Trend Micro and download the latest virus pattern file and any PC-cillin program updates. Both are free and automatic for one year after registration. If you are using a 28.8 Kbs modem to connect to the Internet, expect the downloads to take about 10 minutes. You can also download the pattern file whenever you see fit.

Here's how:

1. Click **Update** in the PC-cillin bar, then the **Update Now** icon that appears.
2. Choose whether you will access the file from a floppy disk or the Internet (most common)
3. If you use a dial-up connection, you can probably skip the **Use Proxy Server** option and just click **Next**. If you are at an office and connect to the Internet using a LAN, you may need to check the **Use Proxy Server** option and enter your proxy information (your system administrator will know).
4. Finally, click **Next**.

Setting Scan Exceptions

To set scan exceptions,

1. Click **Options | Scan Exceptions** from the main menu.
2. Click **Add File** or **Add Folder**, as appropriate.
3. Select the file/folder that you want PC-cillin to ignore for during real-time scanning.
4. Click **Apply** to save your changes.

Note: No more than 20 exceptions should be created. If you must include more, consider moving individual files/folders to a subdirectory of a folder already on the list. PC-cillin extends the exception status of any folder on the list to all its sub-directories.

Registering PC-cillin

To register PC-cillin,

1. Click **Support** in the PC-cillin bar, then the **Support Wizard** icon that appears.
2. Choose **On-line registration...** and click **Next**.
3. Enter your name and e-mail address.
4. Click **Register Now**. Only registered users are eligible for virus pattern updates and free technical support.

Serial Number



To install the complete version of Trend PC-cillin 6.0 you need a serial number, which can be found on the outside front cover of the User's Guide that accompanies the program CD-ROM. Alternatively, you can install the [free 30-day trial version](#) of PC-cillin. In this case, no serial number is required.

Trial Version



The 30-day free trial version of PC-cillin 6 is fully functional and can be installed without entering a serial number. After 30 days, however, the virus scanning services will be disabled and no longer function.

If you decide to purchase PC-cillin, you do not need to reinstall the software. Instead, click the **Order Screen** that appears and choose **Click Here** to start your web browser and open the following web site:

<http://www.antivirus.com/products/pcc/buy.htm>

You will be sent a special "unlock" program which you can use to restore your PC-cillin protection.

Alternatively, call (800) 656-05443 (orders only, please).

Files not being scanned



Are you receiving the following error message? "*No file to scan or error in scanning.*"

Try this test:

1. Open Windows Explorer (double-click **My Computer**, then right-click a drive letter and choose **Explorer** from the pop-up menu that appears).
2. Right-click the file, drive, or directory that you want to scan.
3. Choose **PC-cillin** from the pop-up menu that appears.

Does PC-cillin scan the file? If it does, check to see whether **All file types** or **Selected file types** is selected for **Scan Option** for your **Scan Wizard** or **Manual Scan**.

Chances are that your Scan Wizard is only scanning certain file types -- for example macro files (.dot, .xla, etc.), or system files (.exe, .sys, etc), but that there are no files of that type in the target location. If **Selected file types** is selected, choose **All file types** and run the scan again.

Downloading Infected Files



With **Real-time Scan**, PC-cillin protects you against downloading infected files from the Internet. If a file you are downloading turns out to be infected, PC-cillin can detect the virus even if it is hidden in a compressed file.

In addition, through **Web Security**, PC-cillin provides specific protection against malicious Java applets and Active X code.

Hint: You can check whether you are using **Real-time Scan** by right-clicking the PC-cillin icon in the task bar. A check mark will appear before the **Real-time Scan** option if it is enabled. Click **Real-time Scan** to turn the feature on or off.

E-mail Attachments



With **Real-time Scan**, PC-cillin protects you against saving infected e-mail attachments. If an e-mail attachment you received is infected, PC-cillin can detect the virus even if it is hidden in a compressed file.

Hint: You can check whether you are using **Real-time Scan** by right-clicking the PC-cillin icon in the task bar. A check mark will appear before the **Real-time Scan** option if it is enabled. Click **Real-time Scan** to turn the feature on or off.

Checking Compressed Files



PC-cillin will check the contents of a compressed file for viruses. To clean the file, first decompress it (this will automatically occur if real-time scanning is enabled.)

For example, let's say there are five files, A.doc, B.doc, C.doc, D.doc, and E.doc compressed into a single file called docs.zip. Let's further say that C.doc is infected with a macro virus.

PC-cillin will detect the virus in C.doc, issue an alert, and write the event to the virus log. If you want to clean C.doc, use WinZip, or whatever compression program you have to decompress docs.zip. When the individual files have been decompressed, right-click C.doc and choose PC-cillin from the pop-up menu that appears. PC-cillin will take the [Action When Virus Found](#) you have set for **Manual Scans**.

Virus Properties



Use **Virus Properties** to do a quick scan of a file from a My Computer, Windows Explorer, or Find window.

Here's how:

1. From the Windows Explorer screen, locate file you suspect and right-click it.
2. Choose **Properties** from the pop-up menu that appears.
3. Make the **Virus Properties** tab active by clicking it.

PC-cillin will do a quick scan if the file and report the results.

Alternatively, you can choose PC-cillin from the pop-up menu that appears to launch PC-cillin automatically run the scan from there.

Recommended settings



Although there are no hard and fast recommendations for what program settings you should use, the Trend Virus Doctors do suggest the following guidelines:



Scan [All file types](#) , and use the **Include boot sector** option



Choose to **Clean** files and select **Backup before cleaning** -- be sure to check the [Virus Log](#) and delete any backup up copies one the cleaned file has been tested.



[Quarantine](#) files that cannot be cleaned



Leave [Real-time Scan](#) on



Leave [Web Security](#) on



Leave [Startup Scan](#) on



Schedule Weekly or Monthly automatic [virus pattern updates](#) (depends on how much you exchange files, install software, download files, receive e-mail attachments, etc.)



Use **e-mail** or the live [chat](#) for your technical support questions. (This tends to be more convenient than calling.)



Use [Active Desktop](#) to keep abreast of the latest virus developments and stay current with important news

Replacing Corrupted Files



If you have a file that has been corrupted by a virus (i.e., it can't be cleaned) there are several ways to attack the problem, depending on what kind of file it is.



Document Files - Delete the file. Scan and then use your backup copy, if have one. If the document contains irreplaceable data and no backup exists, you may be able to recover data by opening the file with Notepad or another simple editor -- **DO NOT OPEN THE DOCUMENT USING THE ORIGINAL APPLICATION OR THE VIRUS CAN SPREAD!** Ignore the strange characters that appear -- it will be mostly machine-readable formatting data for the document, and macro viruses will not work in the Notepad environment. In patches throughout the document, you will likely find your data which you can then cut and paste into an new doc. It's not pretty, but this method is often better than recreating



Program Files -- Note the file name and location, then delete the file. You will need to replace the corrupt file with one from the original program disk(s).



Internet Files -- Delete the infected file and download another copy, preferably from a different site.




E-mail Attachment -- Delete the e-mail, attachment and all. Tell the sender about the virus, and ask him/her to send another copy.

Help Contents



Click this option to search or browse the PC-cillin on-line help.

PC-cillin Help

 This file. You can access context specific help by clicking the Help button on the screen in question, or search the help file by clicking Contents menu option.

