Spyware X-terminator

User's Guide

STOMPSOFT'S TECHNICAL SUPPORT POLICY

Stomp provides unlimited telephone technical support for 30 days without charge. The 30 day no charge support period begins from the first time you call our technical support department. After the 30 day no charge period has expired, telephone support is available for a nominal charge of $20 per incident (not per call). Web based support is available without charge and is unlimited for the life of the product.

GETTING TECHNICAL SUPPORT

StompSoft is committed to customer satisfaction. If you encounter problems installing or using Spyware X-terminator, please do the following:

- Check the trouble-shooting section in this manual.
- Visit http://support.antispyware.stompsoft.com. You can view FAQ's, check for updates, and view the device support list, download manuals, and more.
- If you would like to contact StompSoft via telephone, please call 949-263-8560 Monday ~ Friday 8AM ~ 5PM PST. Please be at the computer where the software is installed when you call.

ABOUT YOUR SPYWARE X-terminator SUBSCRIPTION

Thank you for purchasing StompSoft Spyware X-terminator. When you install and register your copy of Spyware X-terminator, you will receive 12 months of spyware/adware protection in the form of automatic updates to the program's database of known spyware/ adware agents. After the initial 12 month period, you will get a message to re-new your subscription for another year for a nominal cost.

Minimum Requirements

Hardware

Pentium® 200Mhz. or faster (or equivalent) CPU with
96MB RAM and 8MB free hard disk space
CD-ROM/DVD-ROM drive for software installation

Operating Systems Supported

Microsoft® Windows® XP Home or Professional
Microsoft® Windows® 2000 Server with SP1 or later
Microsoft® Windows® 2000 Professional with SP1 or later
Microsoft® Windows® NT4 Server or Workstation with SP6 or later
Microsoft® Windows® 98/98SE
Microsoft® Windows® Millennium Edition (ME)

Installing Spyware X-terminator

Close all running programs to avoid problems with the installation. If you are running Windows NT/W2K/WinXP, you will want to be sure that you are logged in as a user with Administrator rights.

There is no need to uninstall previous versions of Spyware X-terminator. You may simply install one version "on top of" a previous one. Your old settings will be understood by your new version.

Insert the Spyware X-terminator CD. The installer should open automatically. If it doesn't, navigate to the CD and double click the file **setup.exe**.

Follow the information provided on each screen.

Uninstalling Spyware X-terminator

1. Click the **Start button** and select **Settings => Control Panel**
2. Double click **Add/Remove Programs**.
3. Select **Spyware X-terminator** from the list of programs, and click **Add/Remove**.
4. Follow the onscreen instructions.

What is Spyware X-terminator™?

Welcome to Spyware X-terminator! Spyware X-terminator is the best way to find and remove unwanted software on your computer.

Spyware X-terminator works much like a virus scanner, using "scan strings" or a "pattern file" to search for known pests. These files need to be updated regularly, but Spyware X-terminator makes that easy as well.

Often, when you find unwanted software, you may want to learn more before dispatching it. You can learn about various kinds of spyware in this manual and on our web site. If you don't wish to delete the software immediately, you may quarantine it or ignore it.

Spyware X-terminator can search for what bothers you, and skip what you want to keep. For instance, while Spyware X-terminator can find all sorts of hacker tools, you don't need to search for them. And while it can find most spyware, you can bypass detection of spyware cookies or components. And if Spyware X-terminator identifies a file you want to keep as a possible problem, you can exclude that file from further scans.

The following table identifies the Spyware X-terminator components.

Component	Description
SpywareXterminator.exe	On-demand scanning of disk(s) for pest files and spyware cookies.
SpywareXterminatorCL.exe	Command line scanning of disk(s). Especially suited for scheduling background scanning with the task scheduler.
PPMemCheck	Scans active memory for pests.
PPControl	Spyware X-terminator Controller
PPUpdater	Updates all of the Spyware X-terminator family of products. Especially useful for batch processing.
CookiePatrol	Scans cookie directory for spyware cookies. Scheduled every 30 seconds by PPMemCheck.
KeyPatrol	Scans active memory for key loggers.

Spyware X-terminator has many options, but you don't need to study them all before you begin. All defaults are "intelligent", and all you need to do is chose the area you wish to scan, and press the "Scan" button. So let's get started!

This chapter is designed to get you started quickly. Follow the instructions below to scan all of your hard drives for Spyware.

Perform the Scan:

1. Launch Spyware X-terminator, either by double clicking its icon on your desktop or by clicking the **Start** button and going to ***Programs => StompSoft => Spyware X-terminator => Spyware X-terminator***.
2. Go to the **Scan** main tab.
3. Double-click any entry in the **Selected for Scanning** window to remove each entry.
4. Click the **All Hard Drives** check box. There will be an entry for each hard drive in the **Selected for Scanning** window.

***Note**: If you had entries for individual files or directories that are on a hard drive they would be removed from the list because they are superceded by the hard drive they are on.*

5. Click the **Start** button. Spyware X-terminator will begin scanning, displaying and playing sounds when spyware is detected.

When the scan has completed you will:

- be at the ***Logs => Detected!*** Tab, viewing a detailed listing of the possible spyware detected and information about each item.
- know the number of files scanned and number of files found by checking the status bar at the bottom of the window.
- know the status of all procedures running in your computer by going to the ***Advanced => Running Processes*** tab.
- know the status of all of your startup files by going to the ***Advanced => Startup Files*** tab.
- be able to delete or safely quarantine any spyware that you wish.

Congratulations, you have just scanned all of your hard drives!

SpywareXterminator.exe Overview

We have referred to SpywareXterminator.exe to differentiate this executable from the whole product. SpywareXterminator.exe is the graphical user interface (GUI) that lets you:

- select scan options for scanning files that the user has access to on: disks, mapped drives, network neighborhood, network, or administrative shares. The user can include or exclude down to the file level when setting up the scan parameters.
- supports both standard mode scanning and through mode scanning.
- control other Spyware X-terminator components that monitor memory, monitor for cookies, check for key loggers and port activity to execute on demand or on the next boot.
- monitor scanning activity in the status line by getting constant feedback on the number of files scanned, pests found, and which file was just scanned.
- quarantine or delete any files that are detected.
- enable scan on right-click of a folder.
- control when to look for updates for all Spyware X-terminator components or just scan strings.
- set interface options such as font, date format, alarm sounds, and background color.

Whenever SpywareXterminator.exe is executed it will always scan running processes and startup files.

Using SpywareXterminator.exe

Starting SpywareXterminator.exe

SpywareXterminator.exe can be started by doing one of the following:

- From the Spyware X-terminator **Control Terminal:**
  Double-click (or right-click) icon **=>** ***Launch Spyware X-terminator***
- From the desktop:
  Double-click on the ***Spyware X-terminator icon***
  (if you elected to put a shortcut on the desktop).
- From the Start button:
  Programs => StompSoft => Spyware X-terminator=> Spyware X-terminator

Using the SpywareXterminator.exe Interface

The SpywareXterminator.exe interface has four main components:

- an action menu bar.
- start/stop scan and exit buttons which are always visible.
- five "main tabs" controlling windows for presenting information, controls and associated buttons.
- a status bar.

Start/Stop Scan Button

This button can be used regardless of which tab is selected. Whenever a scan is initiated running processes and startup files will be checked. This button is a toggle. It is initially enabled to start scanning. When a scan is started it is used to stop scanning.

Menu Reference

The SpywareXterminator.exe interface has four pull-down selections: File, Options, Logs and Help/Info.

Action Menu Bar

The SpywareXterminator.exe interface has the following pull-down selections for taking action on the items listed in the window.

• FILE PULL-DOWN SELECTIONS

Start Scan
Scan selected entries.

Save As
Save data from the following tabs:

Logs: Detected!, Master Log, Remove from Quarantined,
Advanced: Analyze a File, Running Processes, Startup Files

These files can be saved in a variety of formats depending on the data to be saved.

Save Session Log
Save the session log as a txt file. The session log is an accumulation of detections while running Spyware X-terminator

Print
Print data from the following tabs:

Logs: Detected!, Master Log, Remove from Quarantined,
Advanced: Analyze a File, Running Processes, Startup Files

Refresh
Rescan running processes or startup files if you are on one of those tabs. This selection only works when you are on the Running Processes or Startup Files sub-tab of the Advanced main tab. This performs the same function as clicking the refresh button on those tabs.

Exit
Save settings and terminate SpywareXterminator.exe.

• OPTIONS PULL-DOWN SELECTIONS

These selections take you to the tab selections under the Options main tab.

Where to Search

This tab allows you to select:

- whether to include all files or selected files
- files with specific extensions for scanning
- the granularity of the scan shell tree
- scanning method
- scan tree root

What to Search For

This tab allows you to select which types of unwanted software to scan for.

What to Exclude

This tab allows you to decide what to files or directories to excluded.

Automatic Scans

This tab controls which components will scan on boot, enables right click scanning of folders, and also allows for immediately launching the Spyware X-terminator Control Terminal (PPCT), CookiePatrol and KeyPatrol.

Interface

This tab controls the look and feel of the Spyware X-terminator interface. You can change font characteristics, background color, show startup tips, specify date format and determine if you want the alarm on detection and scanning done sounds to play.

Updates

This tab controls when and how you will do updating for files.

• LOGS PULL-DOWN SELECTIONS

Detected!

Takes you to ***Logs => Detected!*** Whenever possible spyware is detected it is shown here.

Running Processes

Takes you to ***Advanced => Running Processes***. This log will show you the status of all processes running in your machine.

Startup Files

Takes you to ***Advanced => Startup Files***. This log will show you the status of all programs executed in the startup process.

Master Log

Takes you to ***Logs => Master Log***. This is a history log of all items detected that have been quarantined or deleted..

Remove from Quarantine

Takes you to ***Logs => Remove from Quarantine***. This file points to all quarantined files and gives you the option to restore or delete them.

• HELP/INFO PULL-DOWN SELECTIONS

General Info

Takes you to ***Info => General Info***. This is a link to the "Getting Started" web page at antispyware.stompsoft.com.

Pest Info

Takes you to ***Info => Pest Info***. This gives you a local table of all known spyware pests with detailed information about them.

Spyware X-terminator Help

Navigate to this file.

Spyware X-terminator Direct

Opens a window that will allow you to navigate to various areas in the Spyware X-terminator web site.

> ***TIPS —*** *Enables the displaying of usage tips and shows the next tip. Tips can be turned off by:*
>
> unchecking the "Show this dialog next time" check box in the Tip pop-up.
>
> **OR**
>
> *Options => Interface => Show Startup Tips* No check box

About

Takes you to ***Info => About***. This tab has the version level of all key Spyware X-terminator components.

• MAIN TABS

Click on a "main tab" heading below for detailed information about that function.

Scan Main Tab

This tab gives you control over what areas to scan.

Options Main Tab

This tab gives you control over which file types to search for, type of scan to use, what to exclude, setting other Spyware Xterminator components to load on boot or execute now, enabling scan on right-click of a folder, customizing the interface, controlling updates and links to the latest spyware prevalence statistics.

Logs Main Tab

This tab gives you access to the Detected! and Master logs and the Remove from Quarantine list.

Info Main Tab

This tab has detailed information on known pests and version information on components.

Advanced Main Tab

This tab gives you a list of processes currently running in your machine, a detailed list of executables that are run at startup, and an opportunity to delete cookie history files.

• STATUS BAR

This bar is at the bottom of the interface and constantly reflects the status of Spyware X-terminator activity.

Testing SpywareXterminator.exe

If you want to test the operation of SpywareXterminator.exe run it against directories with the following "bait" file files: bait or KeyPatrolBait. The files are all harmless and can be found at:

http://downloads.stompsoft.com/antispyware/keypatrolbait.exe

http://downloads.stompsoft.com/antispyware/bait.exe

Stopping SpywareXterminator.exe

To stop SpywareXterminator.exe do the following:

- File pull-down **=>** ***Exit***

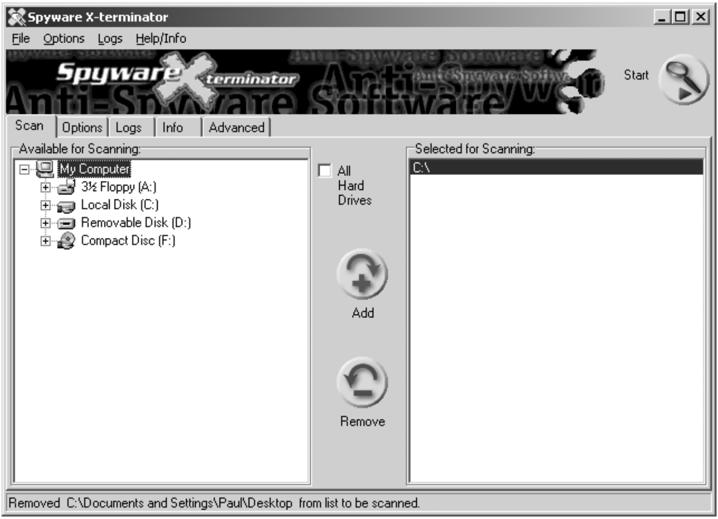
OR

- Click the window close button ***(X)***

Scan

The Scan main tab provides the interface for selecting which areas are to be scanned. The interface is divided into 3 sections:

- an Areas Available for Scanning window
- a Selected for Scanning window
- controls to facilitate the selection process



Removed C:\Documents and Settings\Paul\Desktop from list to be scanned.

Areas Available for Scanning Window

This window has a tree selection list similar to an explorer folder. What you see when you expand a selection is determined by *Options => Where to Search => Scan Shell Tree Options and Options => Where to Search => Scan Tree Root*.

Expanding an Entry in the Tree Selection List

An entry in the list has sub-entries that can be viewed if there is a "**+**" to the left of the entry. Clicking on the "**+**" or double-clicking the icon will expand (open) the entry.

Collapsing an Entry in the Tree Selection List

An entry in the list has sub-entries that can be hidden if there is a "**-**" to the left of the entry. Clicking on the "**-**" or double-clicking the icon will collapse (hide all the sub-entries) the entry.

Areas Selected for Scanning Window

This window lists each entry that has been selected for scanning.

Controls

There are three controls to aid in selecting or unselecting entries for scanning.

Add (+) Button

Clicking this button will cause any item selected in the tree selection list to be entered in the areas to be selected for scanning window.

Remove (-) Button

Clicking this button will cause any item(s) selected in the areas to be selected for scanning window to be removed from the window.

All Hard Drives Check Box

Checking this box will cause an entry for each hard drive to be placed in the areas to be selected for scanning window. Unchecking this box will remove all hard drive entries from the areas to be selected for scanning window.

Selecting Entries for Scanning

Entries can be selected for scanning by selecting them from the tree selection list or by checking the all hard drives check box.

Selecting an Entry in the Tree Selection List for Scanning

You can select an entry from the list by double-clicking the entry or by selecting it and clicking the add **(+)** button. Multiple entries can not be selected.

Note: An entry will not be selected for scanning if a superior entry has already been selected. Also, if a superior entry is selected for scanning then subordinate entries in the "selected" window will be removed.

Checking All Hard Drives for Scanning

You can select to scan all hard drives by checking the all hard drives check box.

Unselecting Entries for Scanning

Entries can be unselected for scanning by removing them from the areas to be selected for scanning window or by unchecking the all hard drives check box.

Removing Entries from the Areas to be Selected for Scanning Window

You can unselect an entry from the areas to be selected for scanning window by double-clicking the entry or by selecting it and clicking the remove (-) button. Multiple entries can be selected with the Shift or Ctrl keys in the normal Windows fashion.

Unchecking All Hard Drives for Scanning

You can unselect all hard drives for by unchecking the all hard drives check box.

Options

The Options main tab gives you control over which file types to search for, type of scan to use, what to exclude, setting other Spyware X-terminator components to load on boot or execute now, enabling scan on right-click of a folder, customizing the interface and controlling updates. This tab has the following sub-tabs.

Options Sub-Tabs

Click on a "tab" heading below for detailed information about that function.

Where to Search Tab

This tab gives you control over what areas to scan. You can select:

- all files or specific file types to be scanned.
- how much information will display in the Scan Shell Tree on the Scan Main Tab.
- which scanning methodology to use.
- which root to display in the Scan Shell Tree on the Scan Main Tab.

What to Search For Tab

This tab lets you select which types of pests to scan for.

What to Exclude Tab

This tab lets you select which directories and files to exclude from being scanned.

Automatic Scans Tab

This tab gives you control over:

- which Spyware X-terminator components to load on boot.
- immediate launching of a Spyware X-terminator component.
- enabling scan on right click of a folder.

Interface Tab

This tab gives you control over the look and feel of the Spyware Xterminator interface and whether or not to play the pest detected or done sounds.

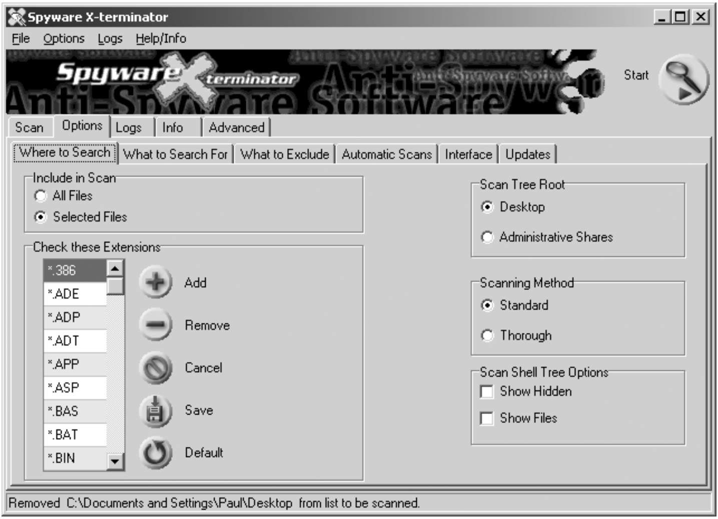
Updates Tab

This tab provides an interface to the updating processes and a quick connect to the Spyware X-terminator web site for the latest news.

Options => Where to Search Tab

The Search tab gives you control over what areas to scan. You can select:

- all files or specific file types to be scanned.
- how much information will display in the Scan Shell Tree on the Scan Main Tab.
- which scanning methodology to use.
- which root to display in the Scan Shell Tree on the Scan Main Tab.



Include in Scan
○ All Files
● Selected Files

Check these Extensions
*.386
*.ADE
*.ADP
*.ADT
*.APP
*.ASP
*.BAS
*.BAT
*.BIN

Scan Tree Root
● Desktop
○ Administrative Shares

Scanning Method
● Standard
○ Thorough

Scan Shell Tree Options
□ Show Hidden
□ Show Files

Removed C:\Documents and Settings\Paul\Desktop from list to be scanned.

The tab is divided into five sections as follows.

Include in Scan

Do you want to scan all files or selected files from the list in the Selected for Scanning window on the Scan Main Tab?

All Files check box

Scan all files. Spyware X-terminator lets you scan inside a wide range of archive or compressed file types. This is a valuable option, since many Internet downloads are compressed to improve download speed. Checking this option will have Spyware X-terminator include scanning inside archives *(such as ace, .arj, .bh, .enc, .gzip, .ha, .lha, .lzh, .pak, .rar, .tar, .xxe, .z, .zip, and .zoo files)*. Be aware, however, that scanning inside compressed files will take longer.

If you want to generally scan inside compressed files but there is one you want to exclude - for example, archived usenet messages, which are all ASCII text and cannot contain an active pest - do the following to exclude that file:

1. Rename this zip to have any extension other than those on your Selected File Types list.
2. Adjust the Selected File Types list as necessary to include the compressed file formats you to wish to scan.
3. Choose **Selected files** as your **Include in** scan option.

Selected Files check box
Scan only those files whose extensions match the list shown in the Check these **Extensions** section shown next.

Check these Extensions

This section is divided into two sub-sections: a list of file types to scan and buttons for customizing the list.

File types to scan for selection list

This list is used when you check the Selected Files check box above.

Buttons for customizing the file types to scan for selection list

Use these buttons to add, remove or use the default list.

Add

Add a new file type to the list. Click the Add button and enter 1 to 5 characters. The entry will be capitalized and added as *.*new_extension* in alphabetical sequence in the list.

Remove

Remove selected entry/entries from the list. Multiple entries can be selected using the shift key.

Cancel

Cancel changes you have made to the list.

Save

Save changes you have made to the list. If you exit Spyware X-terminator without saving you will loose your changes.

Default

Set the list back to the product default. The default extensions are:

.ADE;.ADP;*.AMM;*.ASC;*.BAS;*.BAT;*.CHM;*.CMD;*.COM;*.CPL;*.CRT;*.DO;*.DOC;*.EXE;*.HLP;*.HTA;*.INF;*.INS;*.ISP;*.JS;*.JSE;*.LNK;*.MDB;*.MDE;*.MM;*.MSC;*.MSI;*.MSP;*.MST;*.PCD;*.PIF;*.PL;*.REG;*.SCR;*.SCT;*.SHB;*.SHS;*.URL;*.VB;*.VBE;*.VBS;*.WSC;*.WSF;*.WSH;*.XL;*.XLS;

Scan Shell Tree Options

Checking these selections allows you to control the level of detail shown in the Available for Scanning window on the Scan Main Tab.

Show Files check box

If this box is checked then you will be able to select individual files for scanning.

Show Hidden check box

If this box is checked then you will be able to select hidden directories and/or files (if Show Files is checked).

Show Root check box

If this box is checked then you will be able to scan the root level for scanning. The root level is defined by the box checked in Scan Tree Root on this tab.

Scan Tree Root

These options help you to limit root item to be shown in the Available for Scanning window on the Scan Main Tab.

Desktop check box

This is your whole computer.

Administrative Shares check box

Limit the root to your administrative shares. Normally you would only want to scan your mapped drives. Scanning other areas should be left to system administrators to help keep limit activity on systems volumes.

Scanning Method

These options let you select the scanning methodology.

Standard check box

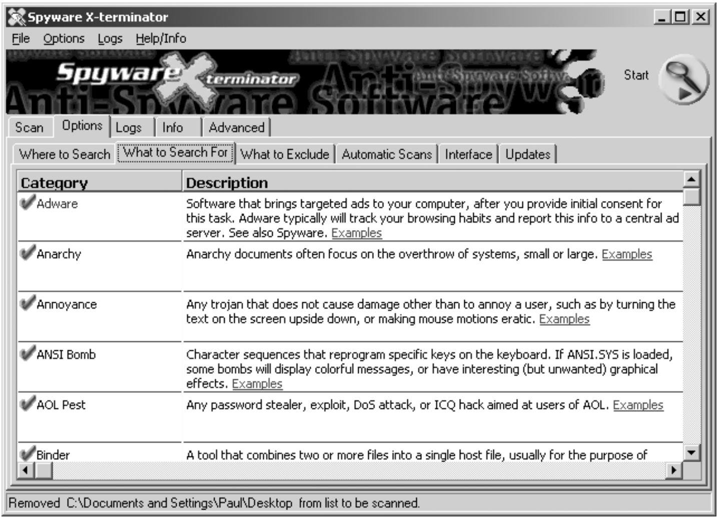
Standard mode: highest speed, no false alarms

Thorough check box

Thorough mode: a bit slower, but able to detect new variants of RAT's (Remote Administration Tools) and other pests.

Options => What to Search For Tab

The Search tab lets you select which types of pests to scan for. This tab is divided into two columns: **category**, the name of the pest with a select/no-select indicator; and **description**, a short description of the pest with a link to more detailed information at the SpywareX-terminator website.



Category	Description
✓ Adware	Software that brings targeted ads to your computer, after you provide initial consent for this task. Adware typically will track your browsing habits and report this info to a central ad server. See also Spyware. Examples
✓ Anarchy	Anarchy documents often focus on the overthrow of systems, small or large. Examples
✓ Annoyance	Any trojan that does not cause damage other than to annoy a user, such as by turning the text on the screen upside down, or making mouse motions eratic. Examples
✓ ANSI Bomb	Character sequences that reprogram specific keys on the keyboard. If ANSI.SYS is loaded, some bombs will display colorful messages, or have interesting (but unwanted) graphical effects. Examples
✓ AOL Pest	Any password stealer, exploit, DoS attack, or ICQ hack aimed at users of AOL. Examples
✓ Binder	A tool that combines two or more files into a single host file, usually for the purpose of

Removed C:\Documents and Settings\Paul\Desktop from list to be scanned.

Category

This column is comprised of two parts. The first part is either a green checkmark or a red (X) where the checkmark indicates that you want to scan for this pest and the X indicates bypass scanning. The default is to scan for all pests.

The second part is the name of the pest. You can elect to scan or not scan for the following pest types:

> Adware, Anarchy, Annoyance, ANSI Bomb, AOL Pest, Binder, Browser Helper Object, Carding, Commercial RAT, Cracking Doc, Cracking Misc, Cracking Tool, DDoS, Dialer, DoS, Dropper, Encryption Tool, Exploit, Explosives, Firewall Killer, Flooder, Hacking Tutorial, Hijacker, Hostile ActiveX, Hostile Java, Hostile Script, IRC War, Key Generator, Key Logger, Loader, Lockpicking, Mail Bomber, Mailer, Misc, Misc Doc, Misc Tool, Nuker, P2P, Packer, Password Capture, Password Cracker, Password Cracking Word List, Phreaking Text, Phreaking Tool, Port Scanner, Probe Tool, RAT, Sniffer, SPAM Tool, Spoofer, Spyware, Spyware Cookie, Theft, Trackware Cookie, Trojan, Trojan Creation Tool, Trojan Source, Virus Creation Tool, Virus Source, Virus Tutorial, War Dialer, Worm, Worm Creation Tool

Description

This column has a short description of the pest with a link to more detailed information at the Spyware X-terminator website.

Note: *When you select Spyware Cookies, you will detect a large number of such beasts. "Spyware cookies" are simply those cookies which are not used only by a single site for its private interactions with its users, but are shared across sites. When multiple sites read from the same cookie, those sites share information. Spyware cookies collect information from multiple sites, as they are visited, then share this information with multiple sites, as they are visited. Such spyware cookies include those containing the text 247media, admonitor, adforce, coremetrics, doubleclick, engage, flycast, sexhound, sextracker, sexlist, and valueclick in their names. Spyware Cookies are detected using a very different approach than Spyware X-terminator uses in detecting other pests. Because a spyware cookie will be somewhat different from one user to the next, there is no way to look it up in our PPInfo database.*

Spyware Cookies keep coming back because they are very common, and because a user normally visits the same cookie-dropping sites repeatedly.

Options => What to Exclude Tab

The Exclude tab is divided into three sections: a window that displays the list of directories and files to be excluded, buttons to add or remove entries from the list and a window that displays a list of pests to be excluded. These are all entries that you have determined are not a threat to your system's integrity and are to be excluded from all future scans.

Files and Directories to Ignore Window

This is a list of all entries (directories or files) to be excluded from scanning.

Note:

- *When a directory is selected all files and sub-directories in that directory will be excluded from scanning.*
- *Recycle folders are already in the list. We do not recommend wasting time scanning a recycle folder.*

Files and Directories to Ignore Buttons

These buttons control the adding and removing of entries in the Files and Directories to Ignore window.

Add

When you click this button you get a "Select an Area to Exclude from Scanning" dialog box. This window is an Explorer style folders selection tree that lets you keep on expanding selections down to the file level. Left-click on the check box for each item you want to exclude and then click the OK button. Your selections will be added to the list and the list saved.

Remove

First select entries (you can use the shift and Ctrl keys to select multiple entries) and then click the Remove button. The selected entries will be removed from the list and the list saved.

Select an Area to Exclude from Scanning Dialog Box

This box is made up of a selection tree, two buttons and a check box. This dialog box displays when the Add button is selected.

Selection Tree

Select the files and/or directories you which to exclude by clicking the box on the left of the entry.

OK Button

When you click this button all selections are added to the Files and Directories to Ignore window.

Cancel Button

All selections are ignored.

View Hidden Check Box

All hidden directories and files are included in the selection tree.

Excluding a Directory or File

To exclude a directory or file from future scans you must include it in this list.

To view hidden directories and files

Check this box to include hidden directories and files in the selection tree.

Note: *In some operating systems this might cause a "system volume information is not accessible" pop-up. The message can be ignored.*

To add a directory or file to the list

1. Click the Add button. A directory/file browsing window will open.
2. Expand the list as needed.
3. Select the item you want to exclude.
4. Click OK
5. Your revised list will be saved and show the full path for each entry added.

To remove a directory or file from the list

1. Highlight the name(s) of the entries you wish to delete.
2. Click the Remove button.
3. Your changes will be saved and the list will be refreshed to reflect the removal of the entries.

Pests to Ignore Window

This window lists the pests that you want to exclude by name. An entry in this list will be ignored no matter what directory it is in.

- Entries may be keyed in or included with the add button.
- The name must be entered exactly as it appears in the Detected! log.
- Names are case sensitive.
- For example: to exclude eicar.com you must enter:

==> EICAR test file. Not a Pest — Just a Test File <==

Pests to Ignore Buttons

These buttons control the adding and removing of entries in the Pests to Ignore window.

Add

Whenever you do a scan and get entries in the Detected! log, the pest names are available to you for exclusion by using the add button. When you click the add button you will get a dialog box with a list of the current pest names in the Detected! log. Select the pests you want to ignore and click OK. Multiple entries can be selected by using the standard cntl+left-click combination or by left-clicking and dragging across the selection list.

Remove

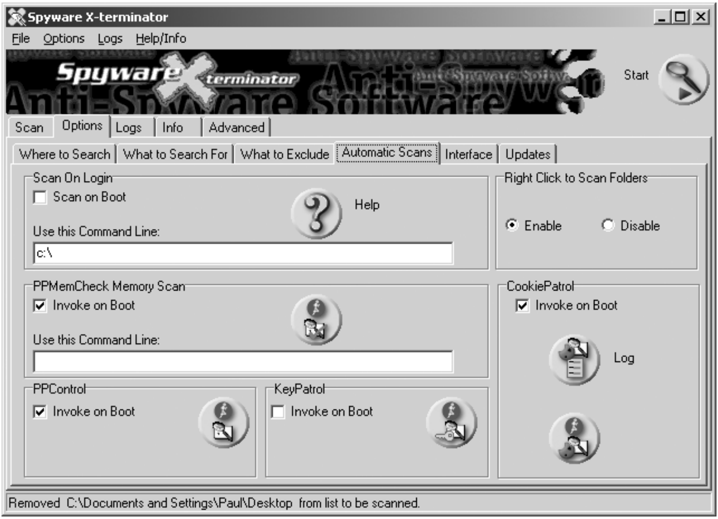
Entries in the Pests to Ignore Window can be removed one-at-a-time by selecting an entry and clicking the remove button.

Options => Automatic Scans Tab

The Automatic Scans tab gives you control over:

- which Spyware X-terminator components to load on boot.
- immediate launching of a Spyware X-terminator component.
- enabling scan on right click of a folder.

This tab is divided into seven sections.


Spyware X-terminator
File Options Logs Help/Info
Start
Scan Options Logs Info Advanced
Where to Search What to Search For What to Exclude Automatic Scans Interface Updates
Help
Log

Scan On Login
□ Scan on Boot
Use this Command Line: c:\

Right Click to Scan Folders
● Enable ○ Disable

PPMemCheck Memory Scan
☑ Invoke on Boot
Use this Command Line:

CookiePatrol
☑ Invoke on Boot

PPControl
☑ Invoke on Boot

KeyPatrol
□ Invoke on Boot

Removed C:\Documents and Settings\Paul\Desktop from list to be scanned.

Scan On Login

Scanning disks on login is accomplished by executing SpywareXterminatorCL.

- Check the Scan on Boot check box.
- Fill in program control parameters (switches) in the Use this Command line input area.
- For more information on the command line parameters click the Help button.

PPControl

You can set the Spyware X-terminator Control Terminal to startup at boot by checking the Invoke on Boot check box. Click the Launch button to start the Spyware X-terminator Control terminal on demand.

PPMemCheck Memory Scan

Scanning memory on login is accomplished by executing PPMemCheck.

- Check the Scan on Boot check box.
- Fill in program control parameters (switches) in the Use this Command line input area.
- For more information on the command line parameters see the chapter on PPMemCheck.
  Click the Launch button to start the PPMemCheck on demand.

CookiePatrol

You can set CookiePatrol to startup at boot by checking the Invoke on Boot check box. Click the Launch button in this section to start CookiePatrol on demand.

If you wish to view the CookiePatrol log then click the Log button in this section.

KeyPatrol

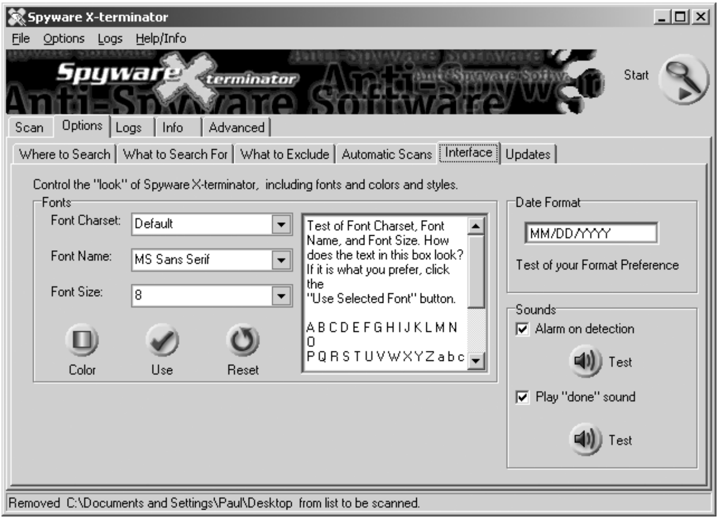
You can set KeyPatrol to startup at boot by checking the Invoke on Boot check box. Click the Launch button in this section to start KeyPatrol on demand.

Right Click to Scan on Folders

Checking the Enable check box will set the “Scan the Directory with Spyware X-terminator” right click folder option.

Options => Interface Tab

The Interface tab gives you control over the look and feel of the Spyware X-terminator interface and whether or not to play the pest detected or done sounds. This tab is divided into five sections.


Spyware X-terminator
File Options Logs Help/Info
Spyware X-terminator Anti-Spyware Software
Start
Scan Options Logs Info Advanced
Where to Search What to Search For What to Exclude Automatic Scans Interface Updates
Fonts
Color
Use
Reset
Date Format
Sounds
Test
Test

Control the "look" of Spyware X-terminator, including fonts and colors and styles.

Font Charset: Default

Font Name: MS Sans Serif

Font Size: 8

Test of Font Charset, Font Name, and Font Size. How does the text in this box look? If it is what you prefer, click the "Use Selected Font" button.

A B C D E F G H I J K L M N O
P Q R S T U V W X Y Z a b c

MM/DD/YYYY

Test of your Format Preference

☑ Alarm on detection

☑ Play "done" sound

Removed C:\Documents and Settings\Paul\Desktop from list to be scanned.

Fonts

This section allows you to change the character set used and change different characteristics of the font.

Font Charset selection list

Change the character set selection to be used. If you do not have the selected character set installed it will remain unchanged. This defaults to the default character set for your machine.

Font Name selection list

Select a font name. The default is MS Sans Serif.

Font Size selection list

Select font size. The default is 8 points.

The charset, font name, and font size settings will be retained for your use, but because you might accidentally elect a font color that was unreadable, this setting is discarded when you exit.

Color button

Clicking this button causes a color selection palette window to dialog box. Pick a color and click OK. The default is black.

Test changes window

This window dynamically reflects the selections you make above. Use it to check your selections before clicking the Use or Reset buttons.

Use button

Clicking this button applies the font selections you have made and changes Spyware X-terminator interface.

Reset button

Clicking this button resets all of the characteristics to the product defaults and applies them to the interface.

Date Format

Change the way the date is presented.

Date format input field

There are two different elements you can use to format the date, characters (d, m, y) and blanks, commas, periods or "/"s. The characters are not case sensitive.

For **Monday, September 30, 2002 8:30PM (20:30)**

C Displays the date using the format given by the ShortDateFormat global variable, followed by the time using the format given by the LongTimeFormat global variable. The time is not displayed if the date-time value indicates midnight precisely. **(09/30/2002 8:30PM)**

e Displays the year in the current period/era as a number without a leading zero (Japanese, Korean and Taiwanese locales only).

ee Displays the year in the current period/era as a number with a leading zero (Japanese, Korean and Taiwanese locales only).

g Displays the period/era as an abbreviation (Japanese and Taiwanese locales only).

gg Displays the period/era as a full name. (Japanese and Taiwanese locales only).

D or **DD** is the numeric day of the month **(30)**
- If you use D, numbers greater than 9 will display as two digits.
- If you use DD, numbers less than 10 will display with a leading zero.

DDD is the abbreviated day of the week **(Mon)**

DDDD+ is the day of the week spelled out **(Monday)**

y or **yy** is the two digit year **(02)**

yyy+ is the four digit year **(2002)**

M or **MM** is the numeric month of the year **(9 or 09)**
- If you use M, numbers greater than 9 will display as two digits.
- If you use MM, numbers less than 10 will display with a leading zero.

MMM is the abbreviated month **(Sep)**

MMMM+ is the month spelled out **(September)**

You can separate the D, M, Y with any combination of a blank, comma or a slash. Or you can run the characters together (YYYYMMDD). The default is mm/dd/yyyy

Watch the line below this window. It dynamically reflects the data you are entering.

Date format presentation
This field is formatted dynamically as you make your entry in the input field.

Sounds

Alarm on Detection check box
When a pest is detected an alarm will sound.

Alarm on Detection Test button
Test the alarm on detection sound.

Play "Done" sound check box
When Spyware X-terminator is through scanning it will make this sound.

Play "Done" sound Test button
Test the Spyware X-terminator done sound.

Options => Updates Tab

The Updates tab provides an interface to the updating process. Use this tab to control how you will manage the regular updating of Spyware X-terminator and its components. This tab is divided into three sections.

Check for latest Updates

PPUpdater is used to update all Spyware X-terminator components. This section gives you the following options for controlling when you do updates. Check one of the following boxes:

- Launch of Spyware X-terminator
- On Exit of Spyware X-terminator
- I'll do this myself...

Note: *PPUpdater can also be run in batch as part of a scheduled operation. See the Updating Spyware X-terminator chapter for more information.*

Update Now

Click the Update Now button to update to the latest software from our servers.

If you have a Proxy Server…

If you have a firewall you can select the proper settings so that the firewall will not block data flow for PPUpdater from the Spyware X-terminator web site. There are three input areas to collect the information needed to configure PPUpdater for use with your firewall and a test button to check your settings. Most home users do not have proxy servers: ask your network administrator if you need help.

Proxy Address and Port

The name or IP address of the proxy server and the port. This must be blank if a proxy server is not being used

Proxy User ID

The userid to gain access through the firewall.

Proxy Password

The password associated with the firewall userid.

Skip Internet Connection Text check box

Check this box, if you do not want to run the internet connection test.

Note: *Proxy information can also be specified on the **PPUpdater => Options** tab.*

Logs

The Logs main tab gives you access to the Detected! and Master logs and the Remove from Quarantine list which can be accessed with the following sub-tabs.

Logs Sub-Tabs

Click on a "tab" heading below for detailed information about that function.

- Detected! Tab
  This tab gives you detailed information on pests detected during a scan.
- Master Log Tab
  This tab gives you a log of pests deleted or quarantined.
- Remove From Quarantine Tab
  This tab gives access to quarantined pests with the option to delete a pest or remove it from quarantine.

Logs => Detected! Tab

The Detected! tab gives you detailed information on pests detected during a scan. This tab is divided into two sections. The log of pests detected and action buttons for determining what to do with the files.

Pests Detected Log

The information in this log is reported in the following columns:

Pest: Name of the pest.

Pest Info:
Category: Pest classification.
Description: Description of the pest.
Author: Name of author if available.
Release Date: Date of the module.

File Info:
In File: one of the following:

In Registry: exact registry location

In File: the full file path

Directory: the name of the Pest Directory

PVT: Pest Verification Token

MD5: MD5 calculation for this file.

File Analysis: Recommended course of action to check this pest. Follow links to Spyware X-terminator web site for more thorough analysis.

Action: In this column, you will get advice to help you make a decision on what to do with this pest.

Certainty: Confidence level of Spyware X-terminator analysis.
Confirmed: This detection is exact.

Suspected: The result of Spyware X-terminator's inference engine.

Threatens: Provides a hint as to what is at risk.
Confidentiality, Integrity, Availability, Productivity, and/or Liability.

Risk: Risk provides one of these suggestions:

None: This is a Spyware X-terminator test file.
Low, Moderate: This file can be executed!
High!: This file is now running!

Advice: Advice suggests what might be a sane course of action. Options here are typically **Delete**, **Quarantine** or **Ignore.**

Please do not use this advice as a substitute for your good judgment.

Note: *If you delete or quarantine a pest this column changes to the action taken.*

Scan Progress Bar

This bar monitors the percent completion progress of the scan and appears at the bottom of the Pests Detected Log during the scan.

Note: *Initial scans will not usually show a correct percentage. As you do more scans the progress bar will more accurately reflect the scanning progress.*

Buttons

The following buttons allow you to take action on the listed pests.

Select All
Select (highlight) all entries in the log.

Deselect All
Unselect all entries in the log.

Delete
Delete all selected entries. For any file that you delete, you will surely want to learn more about the pest. For this purpose, go to Analyze a File *(Advanced => Analyze a File)* before making a Delete decision, or go to the Spyware X-terminator web site,
http://antispyware.stompsoft.com/, using our search engine.

Note: *Spyware X-terminator will detect pests in an archive. If you elect to delete the infested file, you will be reminded that you will be taking the action on an archive and given the choice of canceling or continuing the operation.*

Quarantine

Quarantine all selected entries. For any file that you quarantine, you will surely want to learn more about the pest. For this purpose, go to Analyze a File ***(Advanced => Analyze a File)*** before making a Quarantine decision, or go to the Spyware X-terminator web site, http://antispyware.stompsoft.com/, using our search engine.

Note: *Spyware X-terminator will detect pests in an archive. If you elect to quarantine the infested file, you will be reminded that you will be taking the action on an archive and given the choice of canceling or continuing the operation.*

Del Cookies

Delete all pests that are cookies. They do not have to be selected. Deleted cookies are not recorded in the Master log.

Exclude

Put all selected pests in the exclude list. This can also be managed by going to ***Options => What to Exclude => Files and Directories to Ignore***.

Note: *You can also exclude pests from scanning by name rather than in a specific directory. Refer to* ***Options => What to Exclude => Pests to Ignore****.*

Clear Log

Clear all entries from the log.

Sorting

The log can be sorted on any column by left clicking the column header.

Adjusting Row Height

Row height of all rows can be adjusted by left clicking the border (in the gray column on the left) of any row and dragging the border up or down.

Adjusting Column Width

The width of a column can be adjusted by left clicking the border (in the column header) of the column and dragging the border left or right.

Selecting Multiple Rows

Standard windows multiple row selections can be made with shift and left click for a range of rows and cntl and left click for individual rows.

Print/Save

The Detected! information can be printed or saved by going to the File pull-down.

Logs => Master Log Tab

This is the log of all Spyware X-terminator sessions, by all users, and reports information for all pest deleted or quarantined. If you have ignored a pest then it will not be entered. The log can be simultaneously opened by multiple users.

Master Log

The Master log has the following columns:

M/D/Y: Date
Seq #: Each entry is sequentially entered in the log and numbered.
MAC Address: Mac Address
User: User's login user id.
Location: Fully qualified address of the pest file.
Pest: Pest name
PVT: Pest Verification Token
Action: This will be Deleted, Quarantined or Ignored.
MD5: MD5
ComputerName: Name assigned to this computer.

The log can be manipulated in several ways:

Deleting

To delete it from Windows Explorer, go to:
\Spyware X-terminator\Logs\ , highlight **MasterLog.csv**, and press delete.

Editing

The Master log can be edited as follows:

1. Open Windows Explorer
2. In the ... **\Spyware X-terminator\Logs\** directory, double-click on **MasterLog.csv**. This action will open an application that can recognize .CSV files (in a Windows environment, this is likely to be Excel)
3. You can then edit the file as required.
4. Be sure to save it under the **MasterLog.csv** name if you wish Spyware X-terminator to use this edited version.

Exporting

To export the Master Log so that you can, for example, incorporate the data into reports or manipulate it further to create graphs or charts, do the following:

1. From the session log screen, click Export
2. Give the file a name and click **Save**.
   The default file format is .csv (Comma Separated Values), and the default directory is ... **\Spyware X-terminator\Logs**. You may change these if you wish.

Sorting

The log can be sorted on any column by clicking the column header.

Print/Save

The Master log can be printed or saved by going to the File pull-down.

Logs => Remove from Quarantine

Placing a file in quarantine essentially isolates it from the rest of your system so that it cannot cause any damage. The Quarantine function is intended for use when you are not absolutely certain that you want to delete or ignore a pest that is found during a scan. Files are moved to the ... **\Spyware X-terminator\Quarantine\** directory when you click the Quarantine button ***(Logs => Detected! => Quarantine).***

Once quarantined, a file cannot cause any damage to your machine, or any other problem — unless you deliberately run it from the Quarantine directory. So it is perfectly safe to leave a file in the Quarantine directory forever.

But, if when you reboot you get an error about a missing file — one that you have just quarantined — we know that some setting somewhere was expecting that file to run at boot time. This doesn't mean that it should be run: only that your computer was configured to try to run it.

The Remove from Quarantine tab is divided in to two sections.

Remove from Quarantine Log

The information in this log is reported in the following columns:

M/D/Y: Date
Seq #: Each entry is sequentially entered in the log and numbered.
MAC Address: Mac Address
User: User's login user id.
File: Fully qualified address of the pest file.
Pest: Pest name
PVT: Pest Verification Token
Action: This will be Deleted or Quarantined. Pests that are ignored are not entered in the master log.
MD5: MD5
ComputerName: Name assigned to this computer.

Buttons and Input Area

Files can be either deleted or restored with the following controls**.**

Sequence # input area
Enter the sequence number of the file you want to restore or delete.

Restore button
Clicking this button restores the file identified by the sequence #.

Delete button
Clicking this button deletes the file identified by the sequence #.

Sorting
The log can be sorted on any column by clicking the column header.

Print/Save

The Remove from Quarantine log can be printed or saved by going to the File pull-down.

Info

The Info main tab has detailed information on known spyware, version information on components, and a link to the Spyware X-terminator home page. The tab is divided into two sub-tabs.

Info => Pest Info Tab

When you select this tab Spyware X-terminator will load information on over eleven thousand types of spyware. Depending on your computer this might take a few minutes. This tab is divided into 3 sections.

Pest Name window
This contains the list of Pest Names. Clicking on the column heading will reverse the sort order of the list. Clicking on an entry in the list will bring up the pest information window.

Pest Information window
This window has detailed information on the pest. The following is an example for "AOL Password Stealing Trojan 103".

Category: AOL Pest

Threatens: Confidentiality, Integrity, Availability, Liability

Description: An AOL Pest is any password stealer, exploiter, DoS attack, or ICQ hack aimed at uses of AOL. ICQ is a favorite service among many hackers, and ICQ features are built into many trojans (such as stealing user's passwords, UINs, or notifying the hacker).

Creation Date: 3/7/1998

Buttons
There are two buttons for finding information in the Pest Name window.

Find (search the Pest Name list)
Clicking this button will give you a Find dialog box to enter your search criteria. This window has the following fields and buttons.

Text to Find window
Enter text to search for here.

Case sensitive check box
Check this if your search is case sensitive.

Whole words only check box
Check this if you are only searching on whole word matches.

Regular Expression check box
Check here if you are using characters in the search string to make regular expressions:

- ***** - substitute any characters
- **?** - substitute one character
- **>** - text must be alphabetically higher
- **<** - text must be alphabetically lower
- **!** - negation of the condition
- **&** - and two conditions
- **^** - or two conditions

OK button
Click to start the search.

Cancel button
Click to return without searching.

Help button
Click to get help on regular expressions

Find next
Clicking this button will search for the next entry based on the search criteria you entered in the Find dialog box.

Info => About Tab

When you need to know which version of the product components you have, use this tab.

There is also a link to the Spyware X-terminator home page ("Visit Our Web Site").

Advanced

The Advanced main tab gives you a function for detailed pest analysis of a file, a list of processes currently running in your machine and a detailed list of executables that are run at startup which can be found on the following sub-tabs.

Advanced Sub-Tabs

Click on a "tab" heading below for detailed information about that function.

Analyze a File Tab
This tab allows you to analyze a file to see if it is a pest. If it is a pest you will get detailed information about the pest.

Running Processes Tab
This tab gives you a log of all processes currently running in your machine with a determination of whether or not they are pests.

Cookies Tab
This tab gives you an opportunity to delete cookie history files.

Advanced => Running Processes Tab

The Processes tab gives you a log of all processes currently running in your machine with a determination of whether or not they may be spyware.

Running Processes Log

The information in this log is reported in the following columns:

Identifier: Sequence number.

Status: OK! if not a pest.

Process ID: Id assigned by the operating system.

Path: Full path to the file.

Size: Number of bytes in the file.

MD5: MD5 calculation for this file.

Date: Date of the file.

Company Name: Name of the company who wrote the file.

File Description: Description of the file. This comes fro text in the file.

Version: Version number of the file.

Internal Name: Internal name.

Copyright: Copyright date and company.

Orig. Filename: Original filename.

Product Name: Name of the product that this is a component of.

Product Version: Version of this component.

Refresh

Click the refresh button to get current log of processes running in storage.

Sorting

The log can be sorted on any column by clicking the column header.

Print/Save

The running processes data can be printed or saved by going to the File pull-down.

Advanced => Startup Files Tab

The Startup tab gives you log of all files that are executed at startup with a determination of whether or not they are pests.

Startup Files Log

The information in this log is reported in the following columns:

Area Checked: Startup file or registry entry

Reference: Registry key or full path to file

Status: OK! if not a pest.

Path: Full path to the file.

Size: Number of bytes in the file.

MD5: MD5 calculation for this file.

Date: Date of the file.

Company Name: Name of the company who wrote the file.

File Description: Description of the file. This comes fro text in the file.

Version: Version number of the file.

Internal Name: Internal name.

Copyright: Copyright date and company.

Orig. Filename: Original filename.

Product Name: Name of the product that this is a component of.

Product Version: Version of this component.

Refresh

Click the refresh button to get the analysis of startup files. If this is different than a run done earlier than some process has changed information on files to be run at startup. This could be the result of legitimate actions of a product installation.

Sorting

The log can be sorted on any column by clicking the column header.

Print/Save

The startup files data can be printed or saved by going to the File pull-down.

Advanced => Cookies Tab

The Cookies tab gives you a log of spyware cookie history data that is stored in the index.dat file.

Cookies Detected Log

The information in this log is reported in the following columns:

Address: Target URL.

Hits: Number of times this cookie has been accessed.

Modified: Last date and time that the entry was modified.

Expires: Date that this cookie expires.

Full Address: Userid (login name) and target URL.

Buttons

These buttons allow you to take the following actions:

Refresh: Click the refresh button to reanalyze the index.dat file for spyware cookie history.

Select All: Check all entries in the log.

Deselect All: Uncheck all entries in the log.

Delete: Delete all checked entries.

CookiePatrol Overview

CookiePatrol was created to address a pressing need of our users: to detect "Spyware cookies" the moment they landed on the computer, and silently blast them away.

Features and Benefits

- No need to block all cookies just to block some, the way your browser would have it. And no need to block blindly, disabling your ability to access certain sites, the way some personal firewalls would have it. CookiePatrol allows the cookie to be created, satisfying the web site that gave it to you. And then it destroys the cookie, satisfying your need for privacy.
- Complete transparency. You won't be annoyed every time a cookie is blasted. No blinking, popping or snorting. Just quiet death to cookies.
- Easy assessment of what's been blasted, and when you got it. Just check the logs, and you'll see the cookies that have been blasted, and the time they came in (and died!).
- No conflict with other software or security settings.
- Need not be loaded at boot time. When run, finds all spyware cookies, blasts them, then keeps them gone.
- Easy management through the Spyware X-terminator Control Terminal.

Using CookiePatrol

Starting CookiePatrol

CookiePatrol can be started by doing any of the following:

- From the Spyware X-terminator Control Terminal,
  Double-click (or right-click) ***icon => CookiePatrol => Start CookiePatrol***
- From SpywareXterminator.exe,
  Options tab => Automatic Scans tab => CookiePatrol - Invoke on Boot check box

OR

- ***Options tab => Automatic Scans tab => CookiePatrol - Invoke CookiePatrol Now button***

How CookiePatrol Works

When CookiePatrol detects a cookie it will:

- delete the cookie.
- will play ... \Spyware X-terminator\CookieCrunch.wav.
- log the date and time of deletion and the name of the cookie in the log.

CookiePatrol will not do any interactive processes with the user. The only option the user has is to view the log to see what actions were taken.

The CookiePatrol Cookie Crunching Sound

Whenever CookiePatrol deletes a cookie it plays ...
\Spyware X-terminator\CookieCrunch.wav.

To hear the sound, go to the Spyware X-terminator directory (...\Spyware X-terminator\) and double-click on CookieCrunch.wav. You can substitute your own wav file if you wish; if you delete CookieCrunch.wav then you will hear the default Windows sound.

If you do not want any sounds played when CookiePatrol deletes a cookie then:

- Download a silent version of CookieCrunch.wav from http://downloads.stompsoft.com/antispyware/cookiecrunch.zip.

OR

- Execute ...\Spyware X-terminator\CookiePatrol.exe /NoSound from the command line, batch file or login script.

Note:

- The /NoSound option can be reset by ***PPControl* => *CookiePatrol* => *Enable Sound*** refer to Using Spyware X-terminator Control Terminal.
- The sound setting is not reset when you reboot.

Viewing the CookiePatrol Log

If you want to see what cookies have been detected then you can view the log by doing the following:

- From the Spyware X-terminator Control Terminal ,
  Double-click (or right-click) ***icon => CookiePatrol => View Log***
- From the Start button,
  Programs => Stompsoft => Spyware X-terminator => CookiePatrol Log Viewer

The CookiePatrol log is stored in
...\Spyware X-terminator\Logs\user_id_COOKIEPATROL.LOG, where ***user_id*** is your login user id.

Using the CookiePatrol Interface

The CookiePatrol interface has two main components: a window for presenting log data and buttons for taking action on the log contents.

CookiePatrol Log Window

If CookiePatrol has just been run, you will likely see a list of all the cookies found, along with the moment of deletion. If CookiePatrol has been running for several hours, and you've been surfing, then the dates and times of deletion will be the actual time you received the cookie. You'll see some cookies come back over and over and get killed just as often.

CookiePatrol Log Window Buttons

The CookiePatrol interface has the following buttons.

Refresh - Show any new activity in the log.

Clear - Delete all current log entries.

Exit - Close the CookiePatrol log viewer.

The CookiePatrol log is a text file that can be found in the ...
\Spyware X-terminator\Logs directory.

Disabling the Log

To disable the CookiePatrol log: execute ...
\Spyware X-terminator\CookiePatrol.exe /NoLog from the command line, batch file or login script

Note: *Whenever CookiePatrol is stopped and restarted, logging will be reinstated.*

Stopping CookiePatrol

To stop CookiePatrol: from the Spyware X-terminator Control Terminal Double-click (or right-click) ***icon => CookiePatrol => Stop CookiePatrol***

KeyPatrol Overview

KeyPatrol detects Key Loggers using both behavioral and pattern-matching algorithms. Behavior-detecting algorithms are able to detect a Key Logger simply because it has hooked the keyboard, and is watching your typing. Pattern-matching algorithms compare thousands of bytes of every running file with a database of 58,269 pests to determine if the running program is a "known" Key Logger.

Features and Benefits

- Process can be run on-demand or run on access.
- No conflict with other software or security settings.
- Easy management through the Spyware X-terminator Control Terminal.

Using KeyPatrol

Starting KeyPatrol

KeyPatrol can be started by doing any of the following:

- From the **Spyware X-terminator Control Terminal** (on-demand scanning): Double-click (or right-click) **icon => Launch KeyPatrol**
- From the **Start button** (on-demand scanning): *Programs => Stompsoft => Spyware X-terminator =>KeyPatrol*
- From PPMemcheck (on-access scanning): KeyPatrol is launched by PPMemCheck when PPMemCheck is loaded, providing that PPMemCheck is launched with the switch /KP. It is then launched every 30 minutes if, and only if, a process exists whose name differs from any process running at the time of the last KeyPatrol scan.

Using the KeyPatrol Interface

The KeyPatrol interface has two main components: a window for presenting log data and buttons for taking action on the log contents.

KeyPatrol Log Window

KeyPatrol presents a list of running processes in your machine with information on the name of the pest, the pest file, Spyware X-terminator's analysis of the threat, and the path of the file. You may click on any of these column headers to sort in ascending or descending order on that column. The column headings are:

Name: Pest selection check box.
In the left most position of each row there is a check box for selecting the disposition of the pest. Disposition of the pest is controlled by the buttons at the bottom of the window.

Icon

After the selection check box and before the pest name is an icon. This icon reflects Spyware X-terminator’s analysis of the safety of the pest.

A green checkmark icon means that the file is known to be safe.

A warning Icon (yellow exclamation mark) means that the file is not known to be safe, but not known definitively to be a pest, either. It is simply “unknown” and should be treated with care.

● A red “Stop” icon means that the file is known to be not safe, and that one or more pests have been detected in the folder.

Name of the key logger pest.

If an unknown key logger is detected, the pest name will be recorded in the log as “Generic_KeyLogger”.

File: Name of the key logger file.

Pest(s) in : Spyware X-terminator analysis of the safety of this pest.

Path Fully qualified path.

KeyPatrol Log Window Buttons

The KeyPatrol interface has the following buttons for taking action on the pests listed in the window.

Mark checked as Safe - Any pests marked as safe will be shown as safe in future KeyPatrol scans.

Mark checked as Unsafe - Any pests marked as unsafe will be shown as unsafe in future KeyPatrol scans.

Quarantine checked - Quarantine of any active pest is done by KeyPatrol and is done at reboot.

Delete checked - Deletion of any active pest is done by KeyPatrol and is done at reboot. If you elect to delete a key logger, you get a pop-up with the following information:

“Deleting these files may cause applications on our computer to no longer function correctly. Are you sure you want to remove these possible key loggers?”

If you answer the above question “Yes” then you will see this pop-up:

“The selected key loggers will be deleted when you next reboot your computer. Press Yes to reboot now.” Either click on the yes or the no button.

KeyPatrol writes to the masterlog.csv when a user deletes or quarantines a key logger. To do this, it invokes SpywareXterminatorCL with appropriate flags, such as [file] **/Delete /NoLogAfter /NoSound /Pest=[pestname]**

If SpywareXterminatorCL is not found, it is not invoked to write to the log. Deletion or quarantining of keyloggers will still be done by KeyPatrol.

Invert checkboxes - Mark all checked boxes unchecked and all unchecked boxes checked.

Exit - Terminate KeyPatrol.

Testing KeyPatrol

If you want to test the operation of KeyPatrol, we have created a "bait" file for you to use. This file is detected as a pest by KeyPatrol, but is absolutely harmless. It runs, notifies you that it is a bait file, and does nothing. You need two files to make this operational. They can be retrieved from:

http://downloads.stompsoft.com/antispyware/keypatrolbait.exe

http://downloads.stompsoft.com/antispyware/keypatrolhook.dll

Stopping KeyPatrol

To stop KeyPatrol from the Spyware X-terminator Control Terminal
Double-click (or right-click) ***icon => KeyPatrol => Stop KeyPatrol***

PPMemCheck Overview

PPMemCheck detects pests in memory, and both removes them from memory and (optionally) deletes them from disk.

Features and Benefits

PPMemCheck:

- detects any of 4,000+ pests in memory (see list), including keyloggers, RATs, password capture tools, trojans, and spyware.
- launches KeyPatrol, when PPMemCheck loads. KeyPatrol is also launched every 30 minutes if, and only if, a process exists whose name differs from any process running at the time of the last KeyPatrol scan.
- detects a pest whose file has been bound to some innocuous application, such as Notepad.exe, in a way that prevent Spyware X-terminator — or any other product — from detecting this variant of this pest.
- detects a pest that came into your machine as a polymorphic and/or heavily encrypted file, and which foiled the efforts of every other anti-virus and anti-trojan product to detect it as a file.
- cleans up whatever reference automatically invoked the pest. There are many ways that a pest can re-configure your machine to automatically run itself each time you boot. MemCheck examines every possible method of automatic invocation — 21 in all — and automatically removes such references when found. No more annoying error messages about "file not found" after you clean your system and reboot.
- removes from memory any pest that is running, immediately stopping its effects on your system.
- deletes any file which is the source of this active, resident pest, without requiring a reboot.
- uses the same pest names as other Spyware X-terminator modules, so you can look up any pest in our databases.
- does not slow machine performance at all.
- requires a perfect match on over 4,000 bytes of an active pest, so there is simply no chance for a false alarm. Compare this with an anti-virus product, which might alarm on just 9 bytes or so!

Using PPMemCheck

Starting PPMemCheck

PPMemCheck can be started by doing any of the following:

From the Spyware X-terminator Control Terminal:
Double-click (or right-click) ***icon => MemCheck => Start Memory Scanner***

From SpywareXterminator.exe:
Options tab => Automatic Scans tab => PPMemCheck Memory Scan - Launch button

OR

Options tab => Automatic Scans tab => PPMemCheck Memory Scan - Invoke on Boot check box

Refer to PPMemCheck Switches for information on switches that you can use for PPMemCheck when invoking on boot.

Using PPMemCheck in Login Scripts

PPMemCheck allows invocation of SpywareXterminatorCL as a complement to, or in replacement of, PPMemCheck's pest detected dialog in order to clean, record, and take additional action upon the detection of a pest. You may run it from a login script or scheduled the same way that you run SpywareXterminatorCL. Refer to PPMemCheck Switches for information on switches that you can use when executing PPMemCheck from a login script.

Using The PPMemCheck Interface

When PPMemCheck finds a pest in memory, it will display "A pest has been found in memory!" popup window with the following information and instructions:

Do You Wish to Terminate This Pest?

Click on one of the following three buttons.

- **Yes**
  Stop this pest from running, and remove it from memory, simply click **"Yes."** If you check the *"Delete the file on disk too"* option, you will also remove this file from your machine.
- **No**
  Do not terminate the execution of this pest and do not tell me about this pest anymore until the next time I logon.
- **Ignore Forever**
  Do not terminate the execution of this pest and never flag it as a pest again.
- If you click the close button (the **"x"** in the upper right-hand corner of the window) then the pest will remain executing and the PPMemCheck interface window will close.

Detection Summary

Process:	Name of the process executing
File:	Fully qualified path and name of the file. The exact location of the file.
PVT:	Pest Verification Token
Pest:	Name of the pest.

Show pest information button

Clicking this button will give you a Pest Information pop-up window with detailed information concerning this pest. Click OK when you are done.

Delete the File on Disk too Checkbox

If you check this box then the file will be deleted from the disk.

Testing PPMEMCheck

If you want to test the operation of PPMemCheck, we have created a "bait" file for you to use. This file is detected as a pest by PPMemCheck, but is absolutely harmless. It runs, notifies you that it is a bait file, and does nothing. You may obtain a copy of bait.exe from **http://downloads.stompsoft.com/antispyware/bait.exe**.

Stopping PPMemCheck

To stop PPMemCheck do the following:
From the Spyware X-terminator Control Terminal: double-click (or right-click) *icon => PPMemCheck => Stop Memory Scanner*

Unloading PPMemCheck

To unload PPMemCheck do the following:
From the Spyware X-terminator Control Terminal: double-click (or right-click) *icon => MemCheck => Unload MemCheck*

PPMemCheck Switches

PPMemCheck accepts the following command line parameters:

/Auto

Do not display MemCheck's pest detected dialog, immediately invoke SpywareXterminatorCL when pest found. This switch implies the SpywareXterminatorCL command line parameters "/NoLogAfter" and "/NoPause". PPMemCheck will invoke KeyPatrol, if found, unless PPMemCheck is run with this switch. Since automatic processing of generically-detected key loggers is risky business, KeyPatrol will simply not be invoked when the /Auto switch is used here.

/Delete

When a pest is detected, and the user chooses to terminate the pest, or if the "/Auto" parameter is given, SpywareXterminatorCL will delete it. The pest will be cleansed from memory before invoking SpywareXterminatorCL.

/Quarantine
When a pest is detected, and the user chooses to terminate the pest or the "/Auto" parameter is given, have SpywareXterminatorCL quarantine it. The pest will be cleansed from memory before invoking SpywareXterminatorCL.

/Ignore
When a pest is detected, have PPMemCheck ignore it. The pest will NOT be cleansed from memory before invoking SpywareXterminatorCL when the "/Auto" switch is given. Otherwise, the pest will be cleansed in accordance with user response.

/KP
PPMemCheck will invoke KeyPatrol, if found. It will also launch KeyPatrol every 30 minutes if, and only if, a process exists whose name differs from any process running at the time of the last KeyPatrol scan.

Anything else …;
All other parameters (such as "/EmailTo"), will be passed verbatim to SpywareXterminatorCL in all cases where it is launched.

When the user chooses to take no action upon detection of a pest, SpywareXterminatorCL is launched for the sole purpose of logging the detection, or performing additional action as indicated by parameters above. The command line parameters: "/Ignore", "/NoLogAfter", and "/NoPause" will be appended to SpywareXterminatorCL's command line.

In all cases where SpywareXterminatorCL is launched, it is provided with the fully qualified path of the pest executable.

Since only one instance of SpywareXterminatorCL can be running on the system at once, in all cases where MemCheck launches SpywareXterminatorCL, it waits until any existing instances of SpywareXterminatorCL have exited.

Updating Spyware X-terminator

Because new pests are being created every day, it is important to keep your detection up-to-date by using the latest versions of the scan strings. And because we are constantly making improvements in the Spyware X-terminator executables, you will want to keep these components up-to-date as well.

We try to update the strings at least twice a month, on about the 15th and 30th. But in reality, they are updated more often, when some scary new pest makes the news or a user reports a false alarm, for instance. We recommend that you update about once a month. Updates are free and fast so you might want to update it each time you use it. You can do an update with a simple click from the menu, or set the AutoUpdate function and never worry about this again.

Spyware X-terminator uses PPUpdater to keep components up-to-date.

PPUpdater Overview

PPUpdater is a tool for updating Spyware X-terminator.
PPUpdater can run manually or automatically.

Features and Benefits

Speed

- Finds fastest server to do download. All available servers are tested for transmission speed and the fastest is selected.

Reporting

- Creates an on-screen log, explaining what is happening.
- Writes a comprehensive log of its activity on exit (**...\Spyware X-terminator\Logs\PPUpdaterLog.txt**). This log includes product version number, connection method, product type (Licensed, evaluation, etc.), and a report on each file that it has checked. Errors, if any, are detailed in this report.

Configurability

- May be configured to show the on-screen log or to exit without showing the log. This allows both automatic use (as in login scripts) and manual use, with browsing of actions performed. See Using PPUpdater for more information.
- Works with all proxy servers. Enter Host, UserID, and Password for your http proxy server.

Security

- Stores Proxy UserID and Proxy Password in encrypted form.

Efficiency

- Does not retrieve any file that you already have the correct version of.
- Files are maximally compressed during transfer, to minimize transfer time.

Self-Configuration

- For any file that is an appropriate part of your Spyware X-terminator product suite, but which is missing, PPUpdater simply fetches a new copy.

Using PPUpdater

Manually Updating Spyware X-terminator

When you want to update the Spyware X-terminator components on-demand, you need to run PPUpdater in attended mode. All this really means is that you are specifically launching PPUpdater rather than have it run as part of a scheduling process.

PPUpdater can be manually started by doing one of the following:

- From the **Spyware X-terminator Control Terminal**, *double-click (or right-click)* ***icon => Update***
- From **SpywareXterminator.exe**, ***Options tab => Updates tab => Update Now button***
- From the **Start button**, ***Programs => StompSoft => Spyware X-terminator => PPUpdater***

Automatically Updating Spyware X-terminator

- To schedule PPUpdater either before or after each SpywareXterminator.exe execution, execute Spyware X-terminator and select the Options/Updates tab and select either "Update on Launch of Spyware X-terminator" or "Exit of Spyware X-terminator".

Update Log

PPUpdater always creates a comprehensive log in ...
\Spyware X-terminator\Logs. View it to see what actions PPUpdater took.

Using PPUpdater in Unattended Mode (ADVANCED)

When you want to make sure that the Spyware X-terminator components are updated on a regularly scheduled basis without any human intervention then you want to execute PPUpdater in unattended mode.

Overview

PPUpdater is designed to be run at boot, as part of Spyware X-terminator execution, unattended in batch mode or from a scheduler.

- PPUpdater can be configured to run at system boot by selecting the Do automating updates at boot option.
- PPUpdater can also be configured to run automatically either before or after every SpywareXterminator.exe execution.
- In its unattended mode, invoked by a scheduler, it will exit after completing its work, provided that you have invoked it with /autoexit.
- When not invoked with the switch /autoexit, you will need to select exit from the interface menu.

PPUpdater always creates a comprehensive log in PPUpdaterLog.txt in ...**\Spyware X-terminator\Logs**. View it to see what actions PPUpdater took. This log is initialized in every run. If you want to keep a copy of the log you must rename it or copy it into a different directory.

Execution at Systems Boot

- PPUpdater can be scheduled to execute to run the first time your PC is booted every day. Execute PPUpdater and check *Options => Do automatic daily updates at boot check box***.**

Configuring PPUpdater for Batch

- Uses whatever proxy info is stored in the registry by Spyware X-terminator or PPUpdater. Refer to the PPUpdater Options tab.
- Command line execution options:

  /autoexit - Exit PPUpdater when it has finished.
  /wait=sss - where sss is the number of seconds to wait before launching PPUpdater.

/RunAfter=application_name - When PPUpdater terminates it will start application_name.

Scheduling Updates

You can schedule updates using the Windows Task Schedule under Windows 9x, or the AT command under Windows NT/2000.

Scheduling Updates Under Windows 9x

1. *Double-click* on the **Add Scheduled Task** item at the bottom of the list of **Scheduled Tasks** to invoke the wizard.
2. Use the **Browse** button to locate PPUpdater.exe (normally in `c:\Program Files\Spyware X-terminator`)
3. **Enter a name** for the task, for example PPUpdate.
4. **Select the frequency** for the task to take place.
5. **Set the start date and time** for the first instance of the task. The wizard presents a summary of your scheduled activity.
6. Click **Finish** to accept the scheduled task, or **Back** to go back and edit your choices.

Scheduling Updates Under Windows NT/2000

Windows NT has a built-in scheduler, which you can control by using the AT command. You can use it to automatically run PPUpdater in the background (invisible mode) or in the foreground (interactive mode).

Make sure that the **Schedule** service is turned on:

1. Go to the Control Panel
2. Double-click on the Services icon
3. Select Task Scheduler
4. If the Task Scheduler service's startup is not set to Automatic, do so by clicking on the Startup... button
5. If the Task Scheduler service is not started, do so by clicking on Start.

Run Command Prompt
Add programs to the scheduler using the following command syntax:

```
AT <time> /INTERACTIVE /EVERY:<dates> “<command>”
```

Example:
To run PPUpdater every Monday at 6:00 AM, enter at the command prompt:

AT 6:00 /interactive /every:M “[path to PPUpdater\]PPUpdater.exe /autoexit

Spyware X-terminator Control Terminal Overview

The Spyware X-terminator Control Terminal provides an easy and convenient point to control the execution of different Spyware X-terminator components from an icon in the Systems Tray. The Spyware X-terminator Controller manages the execution of the following components when they are installed on your computer:

SpywareXterminator.exe, PPMemCheck, CookiePatrol, KeyPatrol, and PPUpdater

Using the Control Terminal

Starting the Control Terminal

The Spyware X-terminator Control Terminal can be started two different ways.

The default setting is to load the Spyware X-terminator Control Terminal icon into the System Tray.

Set Spyware X-terminator Control Terminal to invoke on boot.
Spyware X-terminator => Options => Automatic Scans => PPControl Control Panel for your Systray - Invoke on Boot check box

From the Start button
Programs => StompSoft =>Spyware X-terminator=> Control Center
(You would need to do this if you had previously unloaded the Spyware X-terminator Control Terminal.)

Using the Control Terminal

The Spyware X-terminator Control Terminal allows you to do the following when the Spyware X-terminator Control Terminal icon is in the System Tray:

For Spyware X-terminator

- Start Spyware X-terminator
  Double-click (or right-click) ***icon => Launch Spyware X-terminator***

For PPMemCheck

- Start Memory Scanner when it is loaded in memory but stopped
  Double-click (or right-click) ***icon => MemCheck => Start MemCheck***
- Stop Memory Scanner
  Double-click (or right-click) ***icon => MemCheck => Stop MemCheck***

For CookiePatrol

- Start CookiePatrol:
  Double-click (or right-click) ***icon => CookiePatrol => Start CookiePatrol***
- Stop CookiePatrol:
  Double-click (or right-click) ***icon => CookiePatrol => Stop CookiePatrol***
- View CookiePatrol log:
  Double-click (or right-click) ***icon => CookiePatrol => View Log***
- Enable CookieCrunch sound:
  Double-click (or right-click) ***icon => CookiePatrol => Enable Sound***

Note:

- Enable sound can be reset by CookiePatrol /NoSound, refer to Using CookiePatrol.
- The sound setting is not reset when you reboot.
- Disable CookieCrunch sound:
  Double-click (or right-click) ***icon => CookiePatrol => Disable Sound***

For KeyPatrol

- Start KeyPatrol: *double-click (or right-click)* ***icon => Launch KeyPatrol***

For PPUpdater

- Spyware X-terminator Help:
  Double-click (or right-click) ***icon => UPdate***

For Help

- Spyware X-terminator Help:
  Double-click (or right-click) ***icon => Help***

Stopping the Spyware X-terminator Control Terminal

The Spyware X-terminator Control Terminal can be stopped by doing the following:

Double-click (or right-click) ***icon => Unload Spyware X-terminator Controller.***
You will get the following dialog box

> *"One or more Spyware X-terminator components are running in the background. Would you like to terminate them?"*

…with a choice of yes or no buttons.

yes Terminates Spyware X-terminator Control Terminal controlled components running in the background and then terminates the Spyware X-terminator Control Terminal.

no Terminates the Spyware X-terminator Control Terminal.

Frequently Asked Questions

When I Update, should I Uninstall the Previous Version?

There is no need to do this. You may simply install one version "on top of" a previous version. Your old settings will be understood by your new version.

On-Demand v. On-Access

Does Spyware X-terminator provide protection continuously or must I initiate a scan in order to determine if a pest has shown up? If I download a pest file, will Spyware X-terminator automatically detect it or must I initiate a scan?

Spyware X-terminator is an on-demand scanner (you demand, it scans), and does not include a resident on-access (you access a file, it scans) scanner. On-access scanning can be done with PPMemCheck.

Is Spyware X-terminator able to find a hidden pest?

Yes. You can try this experiment: Using Windows Explorer, if I hide a directory containing pest files, and hide those files as well, Spyware X-terminator is still able to list them in its explorer shell on the left of the main screen, and still detects the (hidden) pest files.

Will Spyware X-terminator detect viruses?

Spyware X-terminator is not an anti-virus product and will not remove viruses. We strongly urge you to run an anti-virus program along with Spyware X-terminator for maximum coverage.

Spyware X-terminator is ***like*** an antivirus program in that it goes after unwanted software. One important category of such software is viruses, and protection for this problem is well-covered by anti-virus software. Unfortunately for users, that leaves the entire world of trojans, Spyware, hostile ActiveX, hacker tools, and more largely undetected. It is that unwanted, non-virus software that Spyware X-terminator specializes in.

There are other differences between antivirus software and Spyware X-terminator, besides "subject matter".

- Antivirus software generally looks for software within software — that's what a virus does — adds itself to other software. Spyware X-terminator looks for entire unwanted files.
- Because of the rate of proliferation of viruses, antivirus software was forced to add "heuristics" — the ability to sometimes detect a virus that it had never seen before. Spyware X-terminator uses very limited heuristics, and then only when searching for spyware. This is not due to the primitive nature of the product, but rather due to the risk of false alarming. As you know, a false alarm is usually more expensive to everyone than the real thing.

- Spyware X-terminator is able to be "generic" — detecting an infinite number of variants of the SubSeven Server version 2.2, for instance— while still being precise. Our precision is much greater than an antivirus product, because we use several thousands of bytes from a file to make our identification, whereas an antivirus product might use just 9 or so.

Spyware X-terminator has some interest in viruses: we detect some droppers, some polymorphic and encryption engines, some virus writing tutorials, some virus source code. But we do not want to try to compete with an antivirus product. Anyone entering the antivirus world at this late date cannot achieve the high detection rate of entrenched products, and so would always do their users a disservice. Recognizing that users need an antivirus product as well as something more, Spyware X-terminator has been written to assure compatibility with other antivirus products. You'll find that we work quite well with any antivirus product you use.

I can't believe there are so many Trojans!

There might be some misunderstanding about Spyware X-terminator's mission. While Spyware X-terminator is designed to find Trojans the way an anti-virus product finds viruses, it is also designed to find software that might fall into "gray" areas. A network analysis tool is usually a good thing, but if a disgruntled employee uses such a tool to find a weakness in the organization's network, it is now not a good thing. A network administrator might be properly interested in whether such a tool was out on some employee's machine.

We use the word "pest" simply because there is no other term in the language that seems to cover the broad gamut of unwanted software. Spyware X-terminator finds Trojans. But it also finds pests that are not Trojans.

Why would we call a help file a pest? Because the network administrator who is looking for inappropriate software can use such a file as an indicator that the program itself has been here... And why would a password cracking word list be a problem? If you place it on your own machine, it is not a problem at all, of course. But if a network administrator finds a number of password cracking word lists on a user's machine, then a different inference might be worth considering. Exactly what a network administrator does when they find instructions on how to build a bomb or break into an ATM or forge a credit card is something that is best left to them and their good judgment.

In a typical user's machine, Spyware X-terminator might find some spyware — which the user didn't know they had, and are glad to be rid of. Typical users don't seem to have copies of network analysis tools or password cracking word lists. So the alarms in a typical user's machine are "real".

Spyware X-terminator includes an option to exclude any file from further scanning. If Spyware X-terminator finds something in your machine that you trust, and you want it to bypass something in subsequent scans, simply use this option.

Does Spyware X-terminator ever False Alarm?

The perfect product detects everything you want to detect, and nothing else. This is not an easy position for a developer, since no two people seem to agree on what should be detected. Network administrators, for instance, will have different concerns about what is lurking on a user's machine than a user might have. If you want to maximize your detection rate, use either an anti-virus product or Spyware X-terminator. Other trojan-specific products don't seem to have the high detection rates that you demand.

If you want to eliminate certain alarms, then use any product that permits you to exclude certain individual files, such as Spyware X-terminator. We are always willing to listen to users who believe we have false alarmed. We'll revise our scan strings promptly if you'll write and send either the PVT or your log. Please let us know about any problems you have with the product at our website.

How can I test detection?

EICAR

If you don't have a pest handy, and want to test what happens when Spyware X-terminator detects a pest, there is a simple test file that you can create for this purpose. It is called the EICAR test file. The file is a legitimate DOS program, and produces sensible results when run (it prints the message "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!").

It is also short and simple - in fact, it consists entirely of printable ASCII characters, so that it can easily be created with a regular text editor. Any anti-virus product which supports the test file should "detect" it in any file which starts with the following 68 characters:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

To keep things simple, the file uses only upper case letters, digits and punctuation marks, and does not include spaces. The only thing to watch out for when typing in the test file is that the third character is the capital letter "O", not the digit zero. You are encouraged to make use of the test file. Simply copy the string above to Notepad, and save with some name such as EICAR.COM Check your work: the file must be exactly 68 bytes in size. Now scan with Spyware X-terminator (be sure that the file has a file extension that you have included in your "selected files" list.)

Bait

This harmless Spyware X-terminator pest will be detected by Spyware X-terminator, SpywareXterminatorCL and PPMemCheck.

It can be downloaded from
http://downloads.stompsoft.com/antispyware/bait.exe

KeyPatrolBait

KeyPatrolBait is made up of two components that test as pests but so no harm. It is detected by SpywareXterminator.exe, SpywareXterminatorCL, PPMemCheck, and KeyPatrol.

The components can be downloaded from:

http://antispyware.stompsoft.com/Downloads/Components/keypatrolbait.exe
http://antispyware.stompsoft.com/Downloads/Components/kpbaithook.dll

Does Spyware X-terminator recover from Pest Damage?

The answer to this question is "it depends".

- Spyware X-terminator does remove spyware references in the registry, if spyware is found.
- Spyware X-terminator does remove entries in win.ini, system.ini, autoexec.bat, the registry, and other places in your system that invoke a trojan or other pest.
- Spyware X-terminator cannot undo more general damage, such as restoring files that the pest might have deleted or damaged.

Our goal in pest removal is to be able to remove every pest found, no matter where it is located or how it has locked itself into your system, and to leave your system functioning properly, with no boot messages concerning "file not found."

Every Time I surf, I get more pests!

If your pests are identified as "AdMonitor Spyware", "ValueClick Spyware", "Flyswat Spyware" and the like... with file names such as "C:\Windows\Cookies\xx@admonitor[1].txt, then you have spyware cookies creeping back into your machine as you browse the Internet. Such cookies are reasonably harmless but of absolutely no value to you. Deleting them is completely harmless. Their only "harm" is in their compromise of your privacy, as your browsing habits and other info may be passed on to others without your awareness or permission.

The problem is the result of browsing to a site that gives you these cookies. In most browsers, you can turn off cookie support, which would prevent their acquisition...

SpywareXterminatorCL Overview

SpywareXterminatorCL is the command line version of Spyware X-terminator. If you are a systems administrator or advanced user, you will probably want to use this program, as it offers more flexibility in terms of configuration and settings than the GUI version, SpywareXterminator.exe. SpywareXterminatorCL can be invoked from a batch file, from your scheduler, or when you right-click on a folder.

Features and Benefits

- Process can be run on a prescheduled basis.
- No conflict with other software or security settings.

Using SpywareXterminatorCL

SpywareXterminatorCL is the command line version of Spyware X-terminator. If you are a systems administrator (or a home user who just likes to be able to automate your scanning for pests), you will probably want to use this program, as it offers more flexibility in terms of configuration and settings than can be accommodated in the GUI version, SpywareXterminator.exe. SpywareXterminatorCL can be invoked from a batch file, from your scheduler, or when you right-click on a folder.

Invoke on Boot

SpywareXterminatorCL can be set to invoke on boot by doing the following:

From SpywareXterminator.exe:
Options tab => Automatic Scans tab => Scan on Login - Scan on Boot check box

Information on switches that you can use for SpywareXterminatorCL are discussed below.

Running from Another Directory

To run SpywareXterminatorCL from a directory other than the installation directory do the following:

- Copy PPServer.dll into the directory.
- Copy PPEngine.dll into the directory.
- Use the /dat switch (see below) to point to the location of the PPFile.dat, PPInfo.dat and spyware.dat files or copy those files into the new directory. You don't need to copy PPInfo.dat if you do not use the /info switch.
- If you use /spycookie then spyware.dat should be copied into the new directory or the file path needs to be pointed to by the /dat switch.

Syntax

- Command format:
- ...\Spyware X-terminator\SpywareXterminatorCL.exe <Drive>or<Drive:\Directory_path> /switches
- If a directory path has blanks then the whole path must be included in double quotes (").
- All switches, shown below, may be provided in any case (/Append, /APPEND, /append, /aPPEND, etc.).
- Switches may be provided in any order. Any amount of space may separate switches on a command line.

Testing SpywareXterminatorCL

If you want to test the operation of SpywareXterminatorCL run it against directories with the following "bait" file files: bait or KeyPatrolBait. The files are all harmless.

Latest Help information

Execute C...\Spyware X-terminator\SpywareXterminatorCL.exe /?

Command Line (Switches "/", Return Codes)

- WHAT TO SCAN
- WHEN TO START
- HOW TO RUN
- LOGS
- UPON DETECTION
- NOTIFICATIONS
- UPON EXIT
- MISC
- Return Codes

====== WHAT TO SCAN ======

"<Drive> or <Drive:\Directory>"

specifies a location to automatically scan.

- Default is to scan all local (non-network) fixed disks.
- At least one such location must be specified for SpywareXterminatorCL to operate in Command-line mode.
- The second and third characters must be ":\" or the first two characters must be "\\"
- Any number of locations may be specified.
- Areas will be scanned in the order specified. In the example below, drive D: will be scanned first.
- Subdirectories will always be scanned.
- If the path contains a space, then enclose it in "double quotes"

example:
d:\ "c:\Program Files\" F:\

The example below will scan the \critical directory on C:, all of drive D:, E:, and X:, and the Program Files Directory of machine Boris using an Administrative share C$.

c:\critical\ /nopause /nosound d:\ e:\ "\\Boris\C$\Program Files\" x:\

/shares

scan all administrative shares found.

/extensions=ALL or /extensions=<list>

specifies what files should be scanned.

- preface each extension with *. Separate extensions with a semi-colon.
- default is
.ADE;.ADP;*.ASC;*.AMM;*.BAS;*.BAT;*.CHM;*.CMD;*.COM;*.CPL;*.CRT;*.DO;*.DOC;*.EXE;*.HLP;*.HTA;*.INF;*.INS;*.ISP;*.JS;*.JSE;*.LNK;*.MDB;*.MDE;*.MSC;*.MSI;*.MSP;*.MST;*.PCD;*.PIF;*.PL;*.REG;*.SCR;*.SCT;*.SHB;*.SHS;*.URL;*.VB;*.VBE;*.VBS;*.WSC;*.WSF;*.WSH;*.XL;*.XLS
- to scan all files; provide the switch /extensions=ALL

example of scanning only files with the .EXE or .COM or .DLL extension:
/extensions=*.EXE;*.COM;*.DLL

/SpyCookie

specifies to also scan for Spyware Cookies. Default will include detections in pest count, send email if so requested.

/SpyCookieNoAlert

specifies to also scan for Spyware Cookies (in cookies directory), but do not trigger an alert.

- No email will be sent unless pests other than spyware cookies are found
- No popup warning will be given on Spyware Cookies.

====== WHEN TO START ======

/wait=[seconds]

specifies how many seconds to delay before scanning begins.

- default is no delay.

example of starting scan only after a 10-second delay:
/wait=10

/OnceADay

Adds entry to HKLM /software/microsoft/windows/current version/run/ with switch /onceaday and other switches found on command line. On load with this switch, checks pestpatrol.ini to see when it was last run. If run today, exits. Otherwise, updates pestpatrol.ini, and runs with whatever other switches it was invoked.

```
====== HOW TO RUN ======
/idle
            Run only when CPU is idle. This should result in maximum
            scanning speed without slowing other processes.

====== LOGS ======
/log=fullyqualifiedfilename
This switch will save scan results to this file and location, providing the
location already exists.
            - This argument is not case sensitive.
            - If the path contains a space, then enclose it in "double quotes"
            - If no log file name is specified, the log will be named
              <userid>.txt where <userid> is the user's login name.
              example: "/log=c:\Our Results\Our Log.txt"
/Info
        This switch will add pest category, description, author, and release
        date info to your log. Using the switch will slow performance.
/Procs
        This switch will add info on running processes to your log.
/Append
        This switch will will append your scan results to the existing log, if it
        exists. Default is to overwrite a prior log of the same name.
/NoLogAfter
        This switch will prevent display of the log, in Notepad, upon
        completion of the scan. By default, a log is displayed upon
        completion of a scan of a directory or drive IF a pest is found.
/NotifyAlways
        This switch will force the display of the message "Folder is Pest Free"
        upon completion of the scan of a directory, if this is the case.

====== UPON DETECTION ======
/[Action]
        This switch specifies what to do if a pest is found. If not provided,
        SpywareXterminatorCL will take no action against the pest.
            May be one of these values:
            /Ignore (default) - takes no action
            /Delete (remove the pest.)
            /Quarantine (moves pest to a Quarantine directory)
/NoSound
        This switch disables any alarm sounds that otherwise occur when a
        pest is found.
            - Default: Sound when a pest is found.
/NoPause
            This switch disables any popup warnings that otherwise occur
            when a pest is found.
            - Default: Pause.
```

====== NOTIFICATIONS ======

/EMailTo=<address>

specifies the email address to notify if a pest is detected. The message is sent with a log attached. MAPI must be supported by sending machine.

Example: /EMailTo=yourself@yourself.com

The next 3 switches are optional. Use if you wish to use a mail server inside your firewall.

/Host=<mail server name>
/UserID=<UserID with permission to send to this mail server>
/Password=<Password for UserID with permission to send to this mail server>

/ICQ=<icqnumber>

specifies the icq address to notify if a pest is detected.

Example: /ICQ=142772065

====== UPON EXIT ======

/RunAfterFile=

specifies what File should be run upon completion of operation. You must enclose the entire string within double quotes if it contains any spaces.

/RunAfterParams=

specifies what Parameters should be passed to the RunAfterFile. You must enclose the entire string within double quotes if it contains any spaces.

/RunAfterShow=

If RunAfterFile specifies an executable file, RunAfterShow specifies how the application is to be shown when it is opened. This parameter can be one of the following values:

MAXIMIZED - Activates the window and displays it as a maximized window.
MINIMIZED - Activates the window and displays it as a minimized window.
NORMAL - Activates and displays a window.

Example: /RunAfterFile=net /RunAfterParams=”use x: /delete” /RunAfterShow=MINIMIZED
Example: /RunAfterFile=c:\windows\notepad.exe /RunAfterParams=c:\alerts\notice.txt /RunAfterShow=Maximized

====== MISC ======

/DATSource=<path>
Locate PPFile.dat and PPInfo.dat in specified path. Default is same directory from which SpywareXterminatorCL is run. You must enclose the entire string within double quotes if it contains any spaces.
Example: /DATSource=d:\misc\
/Help or /?
Display Help.txt in Notepad.

Return Codes

SpywareXterminatorCL exits with these error levels.
- 0: no problem encountered in operation, and no pest detected.
- 1: trouble reading specified device or file or other error.
- 2: one or more pests found.

SpywareXterminatorCL Example

Example Command

```
“c:\program files\Spyware X-terminator\SpywareXterminatorcl.exe”
        “C:\test\Spyware X-terminator\Pseudo Bad Guy”
        /extensions=all
        /dat=C:\temp\
        /wait=3
        /spycookie
        /log=c:\temp\ppcltest.log
        /nopause
```

Example Execution Log

```
Scan of 09/04/2002 1:53:04 AM
User Name: test
MAC Address: 00-00-00-00-00-00
Computer Name: TESTRMT
Volume Name: APTIVA
File System Name: FAT32
Volume Serial No: 998460234
Windows Version: Windows 98 4.10.67766222
SpywareXterminatorCL.exe version: 4.0 8/28/2002
Scanning controlled from the command line with these parameters:
- C:\test\Spyware X-terminator\Pseudo Bad Guy
- /extensions=all
- /dat=C:\temp\
- /wait=3
- /spycookie
- /log=c:\temp\ppcltest.log
- /nopause
Pest Detected in C:\test\Spyware X-terminator\Pseudo Bad Guy\eicar.com
Pest: EICAR test file. Not a Pest — Just a Test File
PVT: 1750191932
MD5: 44d88612fea8a8f36de82e1278abb02f
User Action: ignored
Pest Detected in C:\test\Spyware X-terminator\Pseudo Bad Guy\bait.exe
Pest: Bait test file. Not a Pest — Just a Test File
PVT: -661848060
MD5: 11c4cd2c5b1c83cc05ab05136cb5c8d3
User Action: ignored
SpywareXterminatorCL scanned C:\test\Spyware X-terminator\Pseudo Bad
Guy checking 7 files in this area as well as checking for
353 Spyware registry entries, 359 Spyware files, and 51 Spyware directories.
Also checked for 48 Spyware Cookies.
Total time: about 7 seconds
Found 2 pests!
Exited with error level of 2
```

Troubleshooting Spyware X-terminator

Using debug.dat

If Spyware X-terminator behaves badly, there are some things you can do before emailing us. The most important is to run Spyware X-terminator with a debug.dat file. Then send us both the normal log that is produced (save the Detected! log if possible) and the special debug log, "DebugLog.txt".

To run with the debug.dat file:

1. **create a file** called **debug.dat** with your favorite editor
2. the content of the file does not matter
3. save the file in ...**\Spyware X-terminator**
4. **run SpywareXterminator.exe**

Run Spyware X-terminator with the same settings you used when it behaved badly. You will get a log that will help us find out what has gone wrong. It is located in **\Spyware X-terminator\Logs\DebugLog.txt**

- Having done all this, visit **http://support.antispyware.stompsoft.com**, where you can submit BOTH logs and describe your problem as best you can. Please also include the the following information:
- Applications running at the time of the Spyware X-terminator problem, including anti-virus products.

Any information on what you have done to try to troubleshoot the matter, and how urgently you need a solution.

More Information

Go to **http://support.antispyware.stompsoft.com** for more information on troubleshooting Spyware X-terminator.

Appendix I Glossary

Anarchy: In the hacking culture, there is a strong belief in anarchy, that laws should not be created for cyberspace nor can they be enforced without grievous infringement on civil liberties. Such views are not widely shared by the general public or by governments. Anarchy documents often focus on the overthrow of systems, small or large.

Annoyance: Any Trojan that does not cause damage other than to annoy a user, such as by turning the text on the screen upside down, or making mouse motions erratic.

ANSI Bomb: Character sequences that reprogram specific keys on the keyboard. If ANSI.SYS is loaded, some bombs will display colorful messages, or have interesting (but unwanted) graphical effects.

AOL Pest: Any password stealer, exploit, DoS attack, or ICQ hack aimed at users of AOL. ICQ is an instant messenger service from mirabilis.com, now AOL. ICQ is a favorite service among hackers, and ICQ features are built into many trojans (such as stealing user's passwords, UINs, or notifying the hacker). Some versions contain a built-in web-server that under Win9x can be used to access any file on the system. Some versions have a problem such that you can send a file to a victim with the filename: foo.jpg .exe This is really a program, but it appears to the user as a .jpg file, so they will simply open it, not realizing it is program. ICQ inboxes can be easily flooded; there are lots of attacks/countermeasures floating around on the Internet for this. Finding somebody's IP address given their UIN is a hot topic: Mirabilis tries to hide this, but many tools exist to discover it anyway.

Carding: Credit card fraud. Carding texts offer advice on how to make credit cards, how to use them, and otherwise exploit the credit card system.

DDoS: A Distributed Denial of Service (DDoS) attack is one that pits many machines against a single victim. An example is the attacks of February 2000 against some of the biggest web sites. Even though these web sites have a theoretical bandwidth of a gigabit/second, distributing many agents throughout the Internet flooding them with traffic can bring them down. The Internet is defenseless against these attacks. The best defense is for users everywhere to run Spyware X-terminator, and remove DDoS clients when they are found, so that their machines are not used as attack tools. Another approach is for ISPs to do "egress filtering": prevent packets from going outbound that do not originate from IP addresses assigned to the ISP. This cuts down on the problem of spoofed IP addresses. A subset of DoS attacks.

Disassembler: A software tool that takes a executable apart, revealing the code within. Disassemblers are legitimate products and often sold commercially. But they are often used by hackers who wish to reverse engineer a product or find flaws that would permit an exploit.

DoS: An exploit whose purpose is to deny somebody the use of the service: namely to crash or hang a program or the entire system. Examples of DoS attacks include flooding the victim with more traffic than can be handled; flooding a service (like IRC) with more events than it can handle bomb; crashing a TCP/IP stack by sending corrupt packets; crashing a service by interacting with it in an unexpected way; or hanging a system by causing it to go into an infinite loop. For example, the Ping of Death exploit crashed machines by sending illegally fragmented packets at a victim. A common word for DoS is "nuke", which was first popularized by the WinNuke program.

Dropper: In viruses and trojans, the dropper is the part of the program that installs the hostile code onto the system.

Exploit: A way of breaking into a system. An exploit takes advantage of a weakness in a system in order to hack it. Exploits are the root of the hacker culture. Hackers gain fame by discovering an exploit. Others gain fame by writing scripts for it. Legions of script-kiddies apply the exploit to millions of systems, whether it makes sense or not. Since people make the same mistakes over-and-over, exploits for very different systems start to look very much like each other. Most exploits can be classified under major categories: buffer overflow, directory climbing, defaults, Denial of Service.

Explosives: Any document explaining how to build or use explosives. It is hard for us to imagine any good use for explosives in the modern office.

Hacker Tools: Code that gives access to data on your machine for example: password crackers,

network sniffer, and keystroke loggers.

Hostile ActiveX: Any ActiveX program that can cause damage in a machine, or compromise confidentiality, integrity, or availability of other information in a machine.

Hostile Java: Browsers include a "virtual machine" that encapsulates the Java program and prevents it from accessing your local machine. The theory behind this is that a Java "applet" is really content — like graphics — rather than full application software. However, as of July, 2000, all known browsers have had bugs in their Java virtual machines that would allow hostile applets to "break out" of this "sandbox" and access other parts of the system. Most security experts browse with Java disabled on their computers, or encapsulate it with further sandboxes/virtual-machines.

IRC War: Internet Relay Chat.

Key Logger: (Keystroke Logger). A program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. The attacker then peruses them carefully in the hopes of either finding passwords, or possibly other useful information that could be used to compromise the system or be used in a social engineering attack. For example, a key logger will reveal the contents of all e-mail composed by the user. Keylog programs are commonly included in rootkits and RATs.

Loader: Any program designed to load another program.

Lockpicking: Any document describing how to pick locks. While such a document might be handy if you forget your keys, in most cases we think the lock is there for good reason.

Mailbomber: Software that will flood a victim's inbox with hundreds or thousands of pieces of mail. Such mail generally does not correctly reveal its source.

Misc: Anything (other than a document) not in another category, perhaps because it falls into multiple categories, such as a tool suite.

Misc Doc: Any document that we feel doesn't belong in today's office, but does not fall neatly into some other category, such as "Cats in Microwaves" or "How to Annoy Your Teacher"

NetWare Cracking: Document or tool for breaking into a NetWare system.

Network Cracking Text: Any document describing how to break into a network.

NT Cracking: Document or tool for breaking into a Windows NT system

NT Security Scanner: A tool that probes an NT server, looking for vulnerabilities. While these can be used by security managers, wishing to shore up their security, the tools are as likely used by attackers to evaluate where to start an attack. One kind of Probe Tool.

Nuker: Any program that, when run, deletes files and otherwise makes your machine unusable.

Password Capture: A variant of the Key Logger that captures passwords as they are entered or transmitted. Some password capture trojans impersonate the login prompt, asking the user to provide their password.

Password Cracker: A tool to decrypt a password or password file. Spyware X-terminator uses the term both for programs that take an algorithmic approach to cracking, as well as those that use brute force with a password cracking word list. Password crackers have legitimate uses by security administrators, who want to find weak passwords in order to change them and improve system security.

Password Cracking Word List: A list of words that a brute force password cracker can use to muscle its way into a system.

Phreaking Text: A document describing how to hack the phone system. Most of these documents apply to older phone systems, and describe techniques that rarely work on modern phone systems. See also Phreaking Tool.

Phreaking Tool: Any executable that assists in hacking the phone system, such as by using a sound card to imitate various audible tones. See also Phreaking Text.

Port Scanner: In hacker reconnaissance, a port scan attempts to connect to all 65536 ports on a machine in order to see if anybody is listening on those ports. Ports scans are not illegal in many places, in part because they don’t actually compromise the system, in part because they can easily be spoofed, so it is hard to prove guilt, and in part because virtually any machine on the Internet can be induced to scan another machine. Many people think that port scanning is an overt hostile act and should be made illegal. An attacker will often sweep thousands (or millions) of machines rather than a single machine looking for any system that might be vulnerable. Port scans are always automated through tools called Port Scanners.

Probe Tool: A tool that explores another system, looking for vulnerabilities. While these can be used by security managers, wishing to shore up their security, the tools are as likely used by attackers to evaluate where to start an attack. An example is an NT Security Scanner.

RAT: Remote Administration Tool. A Trojan that when run, provides an attacker with the capability of remotely controlling a machine via a "client" in the attacker's machine, and a "server" in the victim's machine. Examples include Back Orifice, NetBus, SubSeven, and Hack'a'tack. What happens when a server is installed in a victim's machine depends on the capabilities of the trojan, the interests of the attacker, and whether or not control of the server is ever gained by another attacker — who might have entirely different interests.

Infections by RATs on Windows machines are becoming as frequent as viruses. One common vector is through File and Print Sharing, when home users inadvertently open up their system to the rest of the world. If an attacker has access to the hard-drive, he/she can place the trojan in the startup folder. This will run the trojan the next time the user logs in. Another common vector is when the attacker simply e-mails the trojan to the user along with a social engineering hack that convinces the user to run it against their better judgment.

Ripper: In the underground culture, the word rip means to make a copy of. Often, this has the connotation of making an illegal copy of a copyrighted work. The most common examples are programs that rip music CDs, or site rippers that download a complete copy of an entire web-site.

Rootkit: A rootkit is a collection of tools that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network. The intruder installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. The rootkit then collects userids and passwords to other machines on the network, thus giving the hacker root or privileged access.

A rootkit may consist of utilities that also: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to circumvent detection.

Sniffer: A wiretap that eavesdrops on computer networks. The attacker must be between the sender and the receiver in order to sniff traffic. This is easy in corporations using shared media. Sniffers are frequently used as part of automated programs to sift information off the wire, such as clear-text passwords, and sometimes password hashes (to be cracked).

Spoofer: To "spoof" is to forge your identity. Attackers use spoofers to forge their IP address (IP spoofing). The most common use of spoofing today is smurf and fraggle attacks. These attacks use spoofed packets against amplifiers in order to overload the victim's connection. This is done by sending a single packet to a broadcast address with the victim as the source address. All the machines within the broadcast domain then respond back to the victim, overloading the victim's Internet connection. Since smurfing accounts for more than half the traffic on some backbones, ISPs are starting to take spoofing seriously and have started implementing measures within their routers that verify valid source addresses before passing the packets.

Spyware Cookies: Spyware cookies are simply those cookies which are not used only by a single site for its private interactions with its users, but are shared across sites. When multiple sites read from the same cookie, those sites share information. Spyware cookies collect information from multiple sites, as they are visited, then share this info with multiple sites, as they are visited. Spyware cookies are not dangerous, and invade your privacy very little. Nonetheless, some folks hate them, and many are glad that Spyware X-terminator can find and remove them. Such spyware cookies include those containing the text 247media, admonitor, adforce, coremetrics, doubleclick, engage, flycast, sexhound, sextracker, sexlist, and valueclick in their names.

Theft: Any documents that present methods to steal things — cars, books, cheeseburgers.

Trojan: Any program with a hidden intent. Trojans are one of the leading causes of breaking into machines. If you pull down a program from a chat room, new group, or even from unsolicited e-mail, then the program is likely trojaned with some subversive purpose. The word *Trojan* can be used as a verb: To trojan a program is to add subversive functionality to an existing program. For example, a trojaned login program might be programmed to accept a certain password for any user's account that the hacker can use to log back into the system at any time. Rootkits often contain a suite of such trojaned programs.

Trojan Creation Tool: A program designed to create Trojans. Some of these tools merely wrap existing Trojans, to make them harder to detect. Others add a trojan to an existing product (such as RegEdit.exe), making it a Dropper.

Virus: Software which adds itself to other software or "objects" in the computer, generally without the user's awareness and always without user permission. Viruses have been written to infect nearly every kind of file. Anti-virus software is designed to detect and remove viruses. Spyware X-terminator is designed to complement anti-virus software, and generally does not detect viruses. Spyware X-terminator's mission is to detect every other kind of unwanted software.

Virus Creation Tool: A program designed to generate viruses. Even early virus creation tools were able to generate hundreds or thousands of different, functioning viruses, which were initially undetectable by current scanners.

Virus Source Code: Code which can be compiled or assembled to create a working virus.

Virus Tutorial: We don't think there is much need for viruses in today's offices, so we don't think there is much need to learn how to create them. Virus Tutorials explain 'how to'.

War Dialer: (demon-dialing, carrier-scanning) War-dialing was popularized in the 1983 movie *War Games*. It is the process of dialing all the numbers in a range in order to find any machine that answers. Many corporations have desktop computers with attached modems; attackers can dial in order to break into the desktop, and thereafter the corporation. Similarly, many companies have servers with attached modems that aren't considered as part of the general security scheme. Since most security emphasis these days is on Internet-related attacks, war-dialing represents the "soft underbelly" of the security infrastructure that can be exploited.

Worm: A program that propagates itself by attacking other machines and copying itself to them. Both worms and viruses are self-replicating code that travels from machine to machine by various means. Both worms and viruses have, as their first objective, merely propagation. Both can be destructive, depending on what payload, if any, they have been given. But there are some differences: worms may replace files, but do not insert themselves into files. In contrast, viruses insert themselves in files, but do not replace them.

Startup Files Scanned

There are a number of ways to automatically start a program running when your computer starts up. Spyware X-terminator checks for spyware that attempts to use the following:

Win.ini

System.ini

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]

[HKEY_CLASSES_ROOT\exefile\shell\open\command]

[HKEY_CLASSES_ROOT\comfile\shell\open\command]

[HKEY_CLASSES_ROOT\batfile\shell\open\command]

[HKEY_CLASSES_ROOT\htafile\Shell\Open\Command]

[HKEY_CLASSES_ROOT\piffile\shell\open\command]

[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command]

[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command]

[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command]

[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command]

[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command]

‘StartUp’ folder, contained in the Start Menu

C:\Explorer.exe

END-USER LICENSE AGREEMENT FOR STOMP SOFTWARE

IMPORTANT-READ CAREFULLY: This End-User License Agreement ("License") is a legal agreement between you and Stomp Inc. dba StompSoft ("Stomp"), the republisher of the Stomp software. All Stomp software and third party software distributed by Stomp shall be referred to herein as the STOMP SOFTWARE. This License covers only the STOMP SOFTWARE. The STOMP SOFTWARE includes the computer software, the associated media, any printed materials, any "on-line" or electronic documentation, and all updates thereto. By installing, copying or otherwise using the STOMP SOFTWARE, you agree to be bound by the terms of this License. If you do not agree to the terms of this License, Stomp is unwilling to license the STOMP SOFTWARE to you. In such event, you may not use, install or copy the STOMP SOFTWARE in any way, and you should promptly contact Stomp for instructions on returning the unused product(s) for a refund of the purchase price of the STOMP SOFTWARE.

STOMP SOFTWARE LICENSE

The STOMP SOFTWARE is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. You agree to treat the STOMP SOFTWARE like any other patented and/or copyrighted material. You agree to not remove, modify or alter any patent, copyright, or trademark notice from any part of the STOMP SOFTWARE. The STOMP SOFTWARE is licensed, not sold.

GRANT OF LICENSE

This License grants you the following rights:

- **Software.** You may install and use one copy of the STOMP SOFTWARE on a single computer.
- **Storage/Network Use.** You may not use the STOMP SOFTWARE over an internal network or distribute the STOMP SOFTWARE to your other computers over any network.
- **Back-up Copy.** You may create one (1) back-up copy of the STOMP SOFTWARE. You may use the back-up copy solely for archival purposes.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

- **Limitation on Reverse Engineering, Decompilation and Disassembly.** You may not modify, reverse engineer, decompile, or disassemble the STOMP SOFTWARE in whole or in part.
- **Separation of Components.** The STOMP SOFTWARE is licensed as a single product. Its component parts may not be separated for any reason and/or used on more than one computer.
- **Single COMPUTER.** The STOMP SOFTWARE is licensed for use on a single computer. The STOMP SOFTWARE may only be installed on one computer at any given time.
- **Rental.** You may not rent or lease the STOMP SOFTWARE.
- **Software Transfer.** You may permanently transfer all of your rights under this License only as part of a sale or transfer of the software, provided you retain no

copies, transfer all of the STOMP SOFTWARE (including all copies, component parts, the media and printed materials, all versions and any upgrades of the STOMP SOFTWARE and this License), and the recipient agrees to the terms of this License.

- **Termination.** Without prejudice to any other rights, Stomp may terminate this License if you fail to comply with the terms and conditions of this License. In such event, you must destroy all copies of the STOMP SOFTWARE and all of its component parts.

COPYRIGHT. All title and copyrights in and to the STOMP SOFTWARE (including but not limited to any images, photographs, animation, video, audio, music, text and "applets" incorporated into the STOMP SOFTWARE), and all copies of the STOMP SOFTWARE, are owned by Stomp and/or its affiliates, third-party suppliers or licensors (hereinafter, collectively referred to as "Stomp") who retain all right, title, and interest in the STOMP SOFTWARE and its respective components, parts and underlying technology. All rights not specifically granted under this License are reserved by Stomp.

HIGH RISK ACTIVITIES. The STOMP SOFTWARE is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the STOMP SOFTWARE could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). Stomp specifically disclaims any express or implied warranty of fitness for High Risk Activities.

U.S. GOVERNMENT RESTRICTED RIGHTS. THE STOMP SOFTWARE and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1) and (2) of the Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Republisher is Stomp, Inc., 2302 Barranca Parkway, Irvine, CA 92606.

LIMITED WARRANTY

LIMITED WARRANTY ON CD-ROM MEDIA. Stomp warrants that for a period of ninety (90) days from the date of its delivery to you, that the CD-ROM media on which the STOMP SOFTWARE is furnished will be free from defects in materials and workmanship under normal use. This limited warranty extends only to you as the original licensee. Stomp's entire liability and your exclusive remedy will be replacement of the CD-ROM media not meeting Stomp's limited warranty and which is returned to Stomp with proof of purchase in the form of a bill of sale (containing a date verifying that the CD-ROM media is within the warranty period). Stomp will have no responsibility to replace a disc damaged by accident, abuse or misapplication. ANY IMPLIED WARRANTIES ON THE CD-ROM MEDIA, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY. SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THESE LIMITATIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

EXCLUSION OF WARRANTY ON STOMP SOFTWARE. You expressly acknowledge and agree that use of the STOMP SOFTWARE is at your sole risk. The STOMP SOFTWARE is provided "AS IS" and without warranty of any kind, and to the maximum extent permitted by applicable law, Stomp EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. STOMP DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE STOMP SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE STOMP SOFTWARE WILL BE CORRECTED, FUNCTION ERROR FREE OR WITHOUT INTERRUPTION. FURTHERMORE, STOMP DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE STOMP SOFTWARE IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY STOMP OR A STOMP AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE STOMP SOFTWARE PROVE DEFECTIVE, YOU (AND NOT STOMP OR A STOMP AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.

LIMITATION OF LIABILITY

STOMP SHALL NOT BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR BREACH OF ANY EXPRESS OR IMPLIED WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT LIABILITY OR ANY OTHER LEGAL THEORY RELATED TO THIS PRODUCT. SUCH DAMAGES INCLUDE, BUT ARE NOT LIMITED TO, LOSS OF PROFITS, LOSS OF REVENUE, LOSS OF DATA, LOSS OF USE OF THE PRODUCT OR ANY ASSOCIATED EQUIPMENT, DOWN TIME AND PURCHASER'S TIME, EVEN IF STOMP HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, STOMP'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNT ACTUALLY PAID BY YOU, IF ANY, ALLOCABLE TO THE STOMP SOFTWARE. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

For StompSoft Spyware X-terminator Software (the "STOMP SOFTWARE") Only: You acknowledge that your use of the STOMP SOFTWARE may remove, disable or otherwise change other software installed on your computer, including software that may or may not be "spyware/adware/snoopware/malware." You acknowledge that you are solely responsible for selecting which programs the STOMP SOFTWARE removes from your computer and agree that in no event shall Stomp be held liable for your use or decisions regarding the use of the STOMP SOFTWARE. While Stomp believes it uses reasonable efforts to properly identify products detected by the STOMP SOFTWARE, and regularly updates its list of such products, Stomp does not guarantee that its list is or will be complete, is accurate, or that the STOMP SOFTWARE may not remove other software that is not considered "spyware/adware/snoopware/malware". Because new and/or modified "spyware/adware/snoopware/malware" and other software are constantly being introduced, you should make sure you obtain and install all updates to the STOMP SOFTWARE. By using the STOMP SOFTWARE, it is your responsibility to ensure that you are not violating any end user license agreement you entered into regarding the installation of "spyware/adware/snoopware/malware" software on your computer. By installing and using the STOMP SOFTWARE, in addition to all other items within this License, you explicitly agree to hold Stomp harmless from any and all legal action that may result from your use of the STOMP SOFTWARE.

UPDATES AND SUBSCRIPTION

Certain STOMP SOFTWARE products are updated from time to time depending on the title of the STOMP SOFTWARE (such as updated virus definitions; updated URL lists; updated firewall rules; updated vulnerability data, etc.; collectively, these are referred to as "Definitional and/or Content Updates"). You may obtain Definitional and/or Content Updates for any period for which you have purchased a subscription for Definitional and/or Content Updates for the STOMP SOFTWARE (including any subscription included with your original purchase of the STOMP SOFTWARE). This license does not otherwise permit you to obtain and use Definitional and/or Content Updates.

MISCELLANEOUS

This Agreement shall be governed by the laws of the State of California and all parties submit to jurisdiction and venue in California.

You may not export or re-export the STOMP SOFTWARE or any underlying information, components or technology except in full compliance with this License as well as all United States and other applicable laws and regulations.

Without limiting any of Stomp's other rights, Stomp may terminate this License if you fail to comply with the terms and conditions herein. In such event, you agree to destroy any and all copies of the STOMP SOFTWARE.

If you purchased the STOMP SOFTWARE on-line via the Internet, or via any other electronic method, you may have a limited number of times that the STOMP SOFTWARE may be installed.

Your use of the STOMP SOFTWARE may be subject to additional third-party end-user license agreements. By installing and/or using the STOMP SOFTWARE, you agree to be bound by all license agreements whether from STOMP or any other third-party. Be sure to thoroughly read all licenses presented during purchase, installation and/or on-going use of the STOMP SOFTWARE, as well as all accompanying printed and electronic documentation.

Should you have any questions concerning this License or this limited warranty, you may contact Stomp by writing to: Stomp Inc. 2302 Barranca Parkway, Irvine, CA 92606 Attn: Product Marketing.