PC Tools Software
Essential tools for your PC

ThreatFire™
User's Guide

Document Information

This documentation is Copyright 2008, PC Tools, Inc.

Trademarks

PC Tools, Inc.
5777 Central Ave, Ste. 130
Boulder, CO 80301
Ph: 303-516-1800
Fax: 303-516-1801
http://www.pctools.com
http://www.threatfire.com

Contents

Document Information

Introduction

Document Conventions

This guide employs the following document conventions:

Style	Use
Bold	To designate • responses you type in • menu names • command names • dialog box options • dialog box titles • icon names • buttons and • fields.
	 Capitalization for dialog box titles and options and commands on menus and buttons follows that of the interface. Menu names use title capitalization.
Italic	To designate guides, books, and other reference material.

This document uses the following graphics:

1. To call your attention to important information or to information that doesn't appear in the body of the document:

2. To call you attention to actions that could result in harm to your computer or information that should be carefully observed:

Welcome to PC Tools ThreatFire™ Guide

ThreatFire is patent-pending, security software for your computer. This guide covers both ThreatFire Free Edition and ThreatFire Pro.

ThreatFire guards, protects, and defends your computer by examining and monitoring the behavior of files, background tasks, and processes to block malware such as viruses, worms, trojans, spyware, adware, rootkits, keyloggers, and buffer overflows.

The purpose of this guide is to show you how to use ThreatFire: how to install it, what to do when a security threat is discerned, how to modify its options and settings.

This guide consists of eight main sections:

Introduction	This section: • outlines the purpose and describes the contents of this guide, • provides an overview of how ThreatFire protects your computer, • specifies the system requirements, and • explains the guide's conventions.
Getting Started	This section explains: • how to install ThreatFire, • the various different versions of ThreatFire, • how to uninstall ThreatFire, • how to use the ThreatFire tray icon to bring up the ThreatFire control panel, to suspend ThreatFire, to view the Tutorial, to view the Quick Start Guide, and to view your Security Status report, • how to respond to the various ThreatFire program alerts, and • a basic overview of the main ThreatFire control panel.
Security Status	This section explains: • the main **Security Status** area, including the Worldwide Detection and Protection Statistics reports.
System Scan	This section explains: • the differences between a **Quick Scan** or **Full Scan**, and • how to perform either a **Quick Scan** or **Full Scan** using the **System Scanner**
Threat Control	This section describes: • how to access the **Threat Control** area from the

	main control panel, and • what the **Allowed, Denied, Quarantined** and **Protection Log** tabs cover.
Advanced Tools	This section explains: • the **System Activity Monitor** • the **Advanced Rule Settings,** and what the **Rule Wizard** is and how to access it and use it,
Settings	This section explains: • the main **Settings** button, and • the **General, Quarantine,** and **Scheduled Scan** settings contained in the main tab.
Conclusion	The Conclusion: • summarizes some basic functions of ThreatFire, and refers you to where to look for further help.

System Requirements

Free Disk Space	Approximately 15 MB of disk space
Platforms	Windows Vista SP1 (32-bit)
	Windows XP SP1 or SP2 (Home, Pro & Media Center Editions, 32-bit)
	Windows 2008
	Windows 2003
	Windows 2000 SP4 with Update Rollup 1
Internet Connection	Some program functions require a connection to the Internet

Overview

ThreatFire protects you by intelligently blocking behavior consistent with that of malware such as viruses, worms, trojans, spyware, adware, rootkits, keyloggers, and buffer overflows.

ThreatFire vigilantly monitors any activity that might compromise the security of your computer. Technological advances allow ThreatFire to monitor your computer at very low levels to seek out even deeply hidden threats. By participating in ThreatFire's Secure Community, a network of users who continuously supply information about emerging threats by means of the software itself, you're helping PC Tools identify new threats quickly, ensuring you always have the most up-to-date protection available.

Introduction

When you install ThreatFire, it is already fully configured and no additional set up is required. ThreatFire will automatically block any known malicious threats. For indeterminate threats, or threats that *might* be a virus, it will immediately suspend the suspicious process and present you with the choice to "Allow the process to continue" or "Kill and quarantine the process." You can always undo any quarantine action through the "Restore" option in the Threat Control Quarantine tab. No critical system files will ever be quarantined even if ThreatFire has alerted on them in error and you tell it to quarantine the process. These types of critical processes will only be "denied" or terminated one time, so you're always safe. Information about the type of threat, a description of what it does, and the risk level associated with that type of threat, are always provided so that the program is intuitive and easy-to-use.

As you choose to respond to a perceived threat, the behavior of the threat and your response are relayed to PC Tools for analysis (if you have the Community Protection option set to "On"). The Secure Community, which includes all ThreatFire users who wish to participate, thus gains knowledge of new behaviors of threats, and PC Tools creates and distributes new updates as necessary to combat them.

Information collected may include the reason a program alert triggered, the history of relevant events that led to the event, your IP address, the decision you made regarding this alert, and a copy of the file that triggered the alert. This data is transmitted solely for research and analysis purposes to aid in determining whether a process is malicious in nature. Sample malware files collected may be shared with other security providers for the sole purpose of creating signatures to protect against further spread of the specific threats. All information and file samples shared are held completely confidential and are not tracked back to individual users. Each application is also associated with a unique identifier that is solely used to track the number of active users in the ThreatFire Secure Community. This unique identifier does not include any personal data and is used in lieu of requiring any program registration information such as email address, name, address, etc.

You also have the option of customizing your own rules if you wish to supplement ThreatFire's comprehensive built in protection, but you are very strongly advised not to do this unless you have expert knowledge of your computer.

Important! Improperly constructed rules can prevent your computer from running properly.

Getting Started

This section provides the basic information you need to start using ThreatFire. The topics covered in this section are:

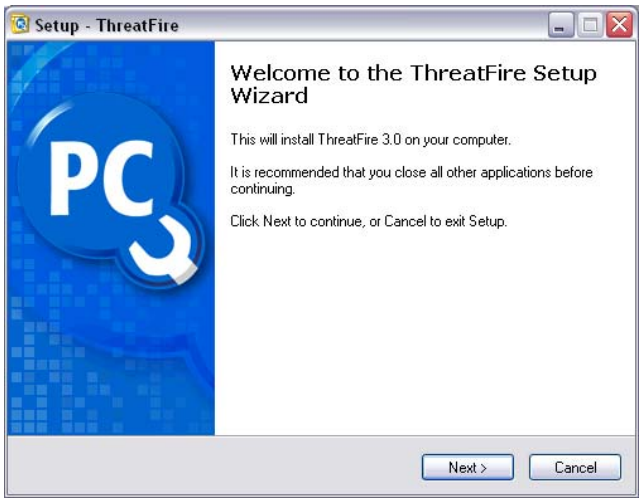
- how to install ThreatFire,
- which ThreatFire versions are included in your installation and how they are managed,
- how to uninstall ThreatFire,
- how to use the ThreatFire tray icon to bring up the ThreatFire control panel, view the introductory Tutorial, view the Quick Start Guide, suspend ThreatFire, and view your Security Status report,
- how to respond to the various ThreatFire program alerts, and
- a basic overview of the main ThreatFire control panel.

Installing ThreatFire

To install ThreatFire:

1 Insert the CD into the drive. If you are installing ThreatFire from a download, use Windows Explorer to navigate to the location on your computer where you saved the setup file and then double-click on that setup file to start the installation.

The Setup Wizard window appears:



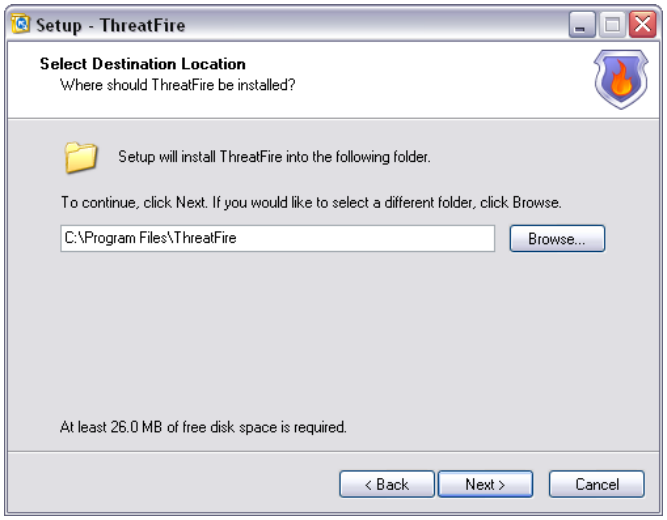
2 Click **Next** to continue; click **Cancel** to cancel the installation.

3 Read the license agreement, and if you agree with it choose to accept it.

Click **Next** to continue; click **Back** to return to the previous screen; click **Cancel** to cancel the installation.

4 The Setup Wizard indicates the destination folder for ThreatFire.

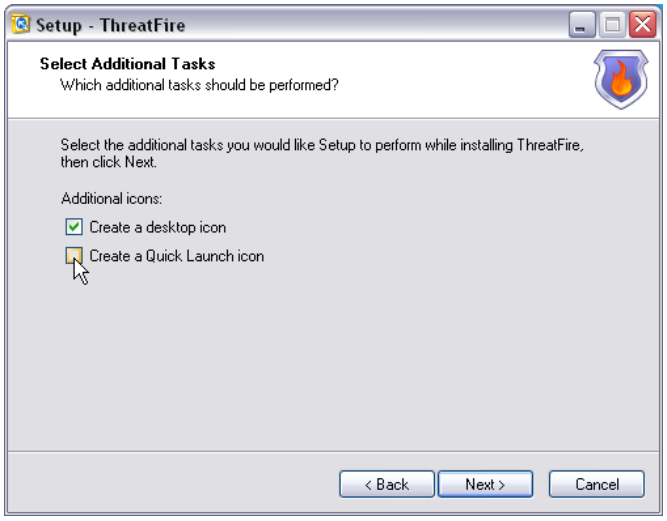
To install to a different folder, click the **Browse** button, and select another folder.



Click **Next** to continue; click **Back** to return to the previous screen; click **Cancel** to cancel the installation.

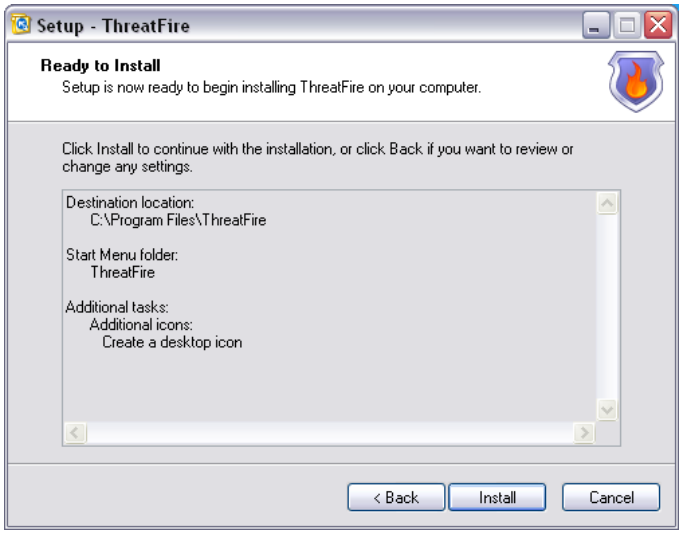
5 The Setup Wizard allows you to create a desktop icon or quick launch icon, or both. Indicate your selections by checking the appropriate boxes.

Click **Next** to continue; Click **Back** to return to the previous screen; click **Cancel** to cancel the installation.



6 The Setup Wizard displays a summary of your selections thus far.

Click **Install** to begin the installation; Click **Back** to return to the previous screen; click **Cancel** to cancel the installation.

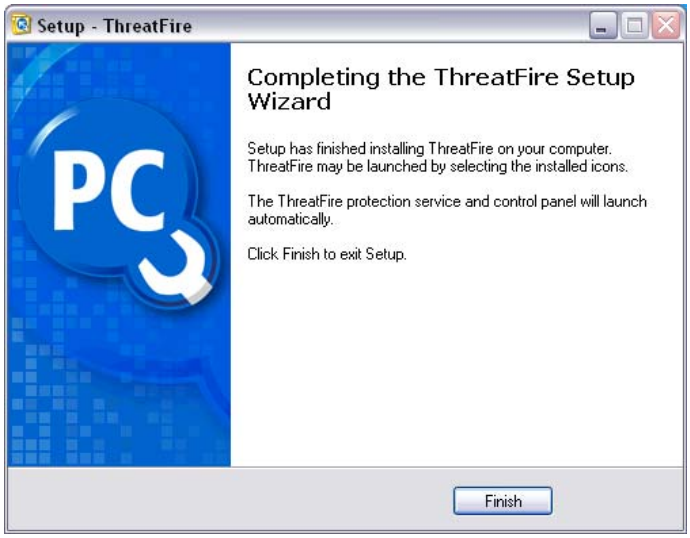


7 The Setup Wizard displays the progress of the installation.

Click **Cancel** to cancel the installation.

8 The Setup wizard indicates when the installation completes.

Click **Finish** to close the wizard.



9 The ThreatFire protection service and control panel launch automatically and the ThreatFire icon appears in the system tray.

ThreatFire will also launch your browser and direct you to the ThreatFire tutorial. It is *strongly recommended* that all new users view this tutorial to understand how ThreatFire works and why it is different from traditional antivirus products.

Different ThreatFire Versions

There are two versions of ThreatFire included in its one main installation package: ThreatFire Free Edition and ThreatFire Pro. All installations begin as ThreatFire Free Edition. To purchase or register ThreatFire Pro simply click the Upgrade Now button on the left side of ThreatFire's main control panel. This will display the ThreatFire Registration Window:

ThreatFire Registration Window

ThreatFire Pro

ThreatFire Pro is the paid (registered) version of ThreatFire which has additional configuration options and is the version available for commercial or business use. The additional options include the ability to opt out of Community Protection participation and still receive automatic updates. In the Free Edition, if you opt out of Community Protection then auto-updates are also disabled (however you may always manually update ThreatFire by running Smart Update). Also, ThreatFire Pro includes priority telephone support in addition to the web-based support system. If you have already purchased a registration code for ThreatFire Pro, simply enter that code in the field provided to convert the trial version to ThreatFire Pro.

ThreatFire Free Edition

ThreatFire Free Edition is available for personal and home use only; commercial use is prohibited. ThreatFire Free includes the very same behavior-based protection as ThreatFire Pro and also now includes the on-demand anti-virus scanning for additional protection. Consider ThreatFire Pro if you are a business or if you wish to have access to telephone support and the ability to opt out of Community Protection without having auto-updates disabled.

Upgrading to ThreatFire Pro

Purchasing and registering ThreatFire Pro is easy. Follow these simple steps to register your copy today:

Click the **Upgrade Now** link in the gold box in ThreatFire.

The Registration window appears:

Select **Purchase Online** to be directed to the PC Tools secure ecommerce store to purchase your ThreatFire Pro subscription license.

At the completion of your order you will receive your license code through email.

When you have your registration code, click the **Upgrade Now** link in the gold box in ThreatFire to again display the Registration window.

Now, before entering your code, ensure that you have an active connection to the internet.

Enter your code in the box provided and click **Register**.

Should you have any questions when purchasing or registering, please feel free to contact us: www.threatfire.com/support

Uninstalling ThreatFire

To uninstall ThreatFire:

1. Click the **Start** menu and highlight and click **Control Panel**.
2. Select **Add or Remove Programs**.
3. Under **Currently Installed Programs**, select **ThreatFire**.
4. Highlight it and click **Remove**.

Windows removes ThreatFire.

ThreatFire's Tray Tasks

Bringing Up ThreatFire

To bring up the ThreatFire Control Panel:

Select **Start/All Programs/ThreatFire/ThreatFire**.
Or

Right-click the **ThreatFire** icon in the system tray:
The choices are **ThreatFire, Tutorial, Quick Start Guide, Suspend** and **Status**.

Click **ThreatFire.**

The **ThreatFire** window appears.

Viewing ThreatFire Tutorial

To view the ThreatFire Tutorial:

1. Right-click the **ThreatFire** icon in the system tray.
2. Click **Tutorial**. A web page will launch for you to walk through the short web-based tutorial.
3. Close the browser window when you are finished viewing it.

Viewing ThreatFire Quick Start Guide

To view the ThreatFire Quick Start Guide:

1. Right-click the **ThreatFire** icon in the system tray.
2. Click **Quick Start Guide**. The Quick Start Guide will launch for you to view.
3. Click the **Close** box to exit when you are finished viewing it.

Suspending ThreatFire

To suspend ThreatFire:

1. Right-click the **ThreatFire** icon in the system tray.
2. Click **Suspend**. The word 'Suspend' is preceded by a check.
3. Click **Suspend** again to reactivate ThreatFire protection.

Viewing Security Status

To view your current ThreatFire Security Status:

1. Right-click the **ThreatFire** icon in the system tray.
2. Click **Status** to view the Security Status report.
3. Click **Close** when you are finished viewing the report.

ThreatFire Control Panel

The ThreatFire Control Panel has six buttons down the left side. When selected, each button will display further information for the selected option in the area to the right:

ThreatFire Control Panel

The buttons are **Security Status**, **Start Scan, Threat Control, Advanced Tools**, **Settings** and **Upgrade Now**. **Upgrade Now** is only shown in ThreatFire Free Edition. Once ThreatFire Pro is registered, then the **Upgrade Now** button is no longer displayed. All the buttons and their associated features are described in further details in the next several chapters.

ThreatFire Program Alerts

"Known Malware" Alert

When ThreatFire detects an attack on your computer by a known threat, it will immediately terminate the attack and permanently isolate the virus process in quarantine. An alert screen will appear, confirming that ThreatFire has blocked the attack. Information presented includes the file path, the name and type of threat, and its description.

All you need to do is click **Proceed** to get back to what you were doing at the time of the attack.

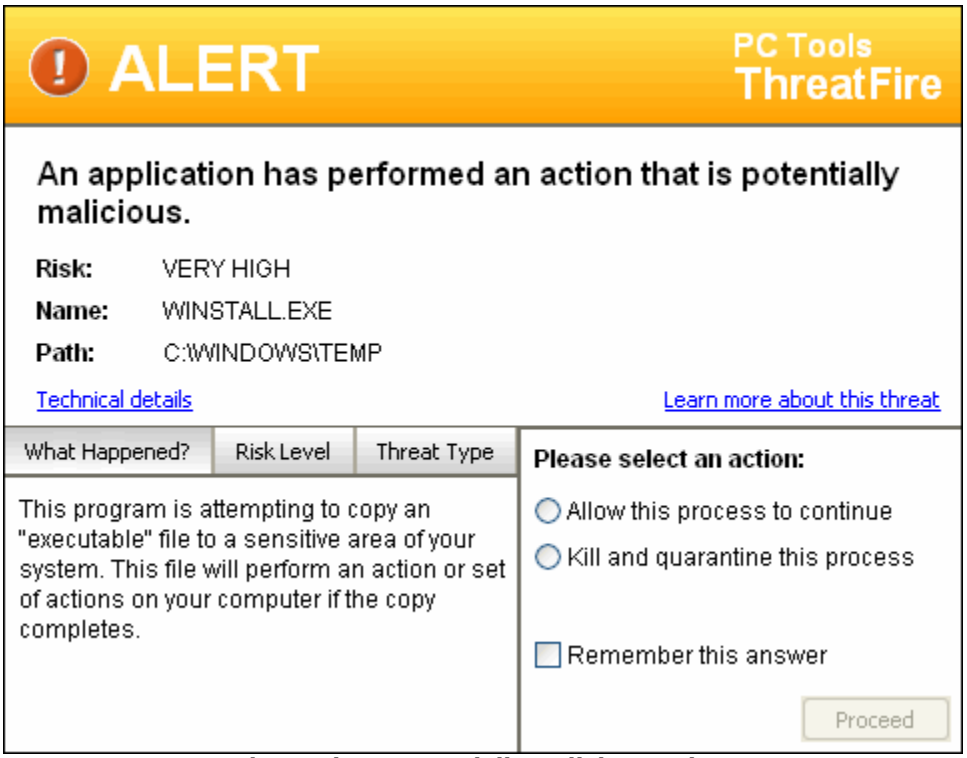
Click the **Technical details** link to view technical information about which file and/or registry objects have been quarantined. This information can also be viewed in ThreatFire's **Threat Contr**ol center under the **Quarantine** tab.

Click the **Learn more about this threat** link to launch a quick web search on the threat. The results of this web search may be of interest to you if you wish to have further information and details on the type of threat you have just avoided.

ThreatFire "Known Malware" Alert

"Potentially Malicious" Alerts

ThreatFire is always on the hunt for suspicious activity in your computer. If it detects a "potentially malicious process' that *might* be a virus attack, it will immediately suspend the suspicious process and alert you that your computer may be at risk. ThreatFire identifies the application that triggered the alert and provides its location. It also provides an overview of the type of threat, a description of what is does, and its associated risk level in order to help you make an informed decision about whether to allow or quarantine the process:



ThreatFire "Potentially Malicious" Alert

To respond to the "potentially malicious" alert:

1 Click **What Happened?, Risk Level,** and **Threat Type** for additional information about the threat.

Click the **Technical details** link for a preview of file and registry objects that will be quarantined if you select **Kill and quarantine.**

You can also click the **Learn more about this threat** link to

launch a quick web search on the threat. In many cases the results of this web search can provide a clear indication of how to proceed.

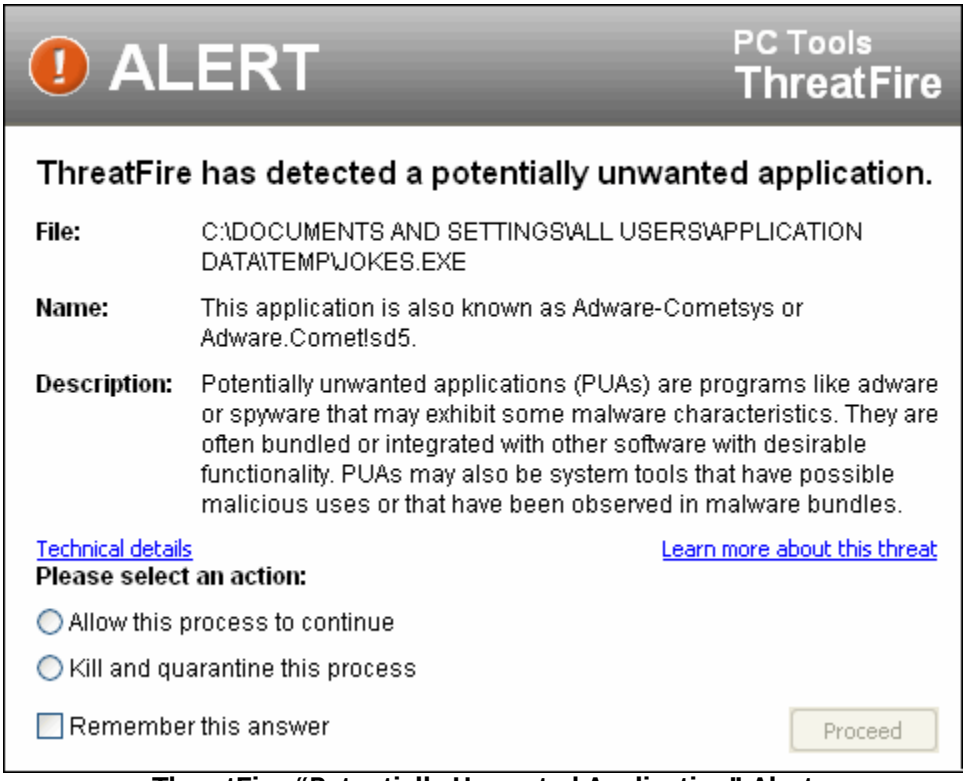
2. To allow the operation to proceed, click the **Allow this process to continue** button.
3. To disallow the operation and quarantine the process, click the **Kill and quarantine the process** button.
4. Click the **Proceed** button to perform the action you selected.

You can also choose to take the same action in future events by checking the **Remember this answer next** time box.

When you check the **Remember this answer next time** box, ThreatFire remembers to take the same action on the same process for the rule triggered. This may be helpful if you find that ThreatFire is alerting on an action that you wish to always allow because you're certain it is safe.

"Potentially Unwanted Application" Alerts

Some applications are not clearly good or clearly bad, but may fall somewhere in between as "grayware." ThreatFire refers to these programs as "Potentially Unwanted Applications" or PUAs. PUAs can include adware or system administrator tools or other classes of programs. While all adware is designed to serve you ads in some format, it is sometimes bundled with other software programs that you may actually want. It is completely your choice whether to run a PUA or not. When ThreatFire detects that a PUA is attempting to run on your computer, it will immediately halt the process and notify you with the following alert:



ThreatFire "Potentially Unwanted Application" Alert

To respond to the "PUA" alert:

1. Click the **Technical details** link for a preview of file and registry objects that will be quarantined if you select **Kill and quarantine.**

   You can also click the **Learn more about this threat** link to launch a quick web search on the threat. In many cases the results of this web search can provide a clear indication of how to proceed.

2. To allow the operation to proceed, click the **Allow this process to continue** button.

3. To disallow the operation, click the **Kill and quarantine the process** button.

4. Click the **Proceed** button to perform the action you selected.

You can also choose to take the same action in future events by checking the **Remember this answer next** time box.

When you check the **Remember this answer next time** box, ThreatFire remembers to take the same action on the same process for the rule triggered. This may be helpful if you find that ThreatFire is alerting on an action that you wish to always allow because you're certain it is safe.

"Custom Rule" Alerts

If you have created any custom rules for your system under the **Advanced Tools, Advanced Rule Settings** area, then you will see a special type of alert.

Only those advanced users who are extremely knowledgeable in all aspects of their computer's behavior should visit the Advanced Rule Settings area and use the Rule Wizard.

The Custom Rule alert will display the name for the rule that you created so you can see exactly what happened. The available actions include **Allow this process to continue, Kill and quarantine this process** and **Kill this process.**

ThreatFire "Custom Rule" Alert

The **Kill this process** option is only available in Custom Rule alerts. This action will terminate the process in question *one time only*. This option differs from the **Kill and quarantine this process** option in that the process is not automatically quarantined and may run again.

Respond to the Custom Rule alert as appropriate. The responses are logged as usual in the Threat Control Center. Any actions where you choose **Kill this process** and **Remember this answer** will be logged the Threat Control Center's Denied area.

Security Status

When you launch ThreatFire, it will always open to Security Status which shows whether **ThreatFire protection** is **ON** or **OFF** and shows the **ThreatFire Threat Detection** map and **Protection Statistics**.

ThreatFire Security Status Report

Clicking the top button will turn ThreatFire Protection **ON** or **OFF**.

The **Worldwide Detection** tab displays a sampling of some of the most recent threats that ThreatFire has detected within the ThreatFire Community. These are active threats that we are protecting our users from. Click the **Malware** tab to display recently caught malware and the **Adware** tab to display recently caught adware samples. As you click on each threat in the list the map to the right will display the threat's recent geographic distribution in red. It is interesting to see how different threats are active in different parts of the world.

Click the **Protection Statistics** tab to view the Protection Statistics report. This report shows both "Your Protection" and "Community Protection."

Security Status

"Your Protection" provides you with information on what ThreatFire is doing to protect your particular PC. "Community Protection" provides you information on what ThreatFire is doing to protect the entire Secure Community.
The following items are included in the Security Status reports:

Events Analyzed
- Number of times ThreatFire has evaluated an action to determine whether it was potentially harmful.

Programs Examined
- Number of processes that ThreatFire has monitored or examined for signs of suspicious behaviors.

Suspicious Activities Detected
- Number of times ThreatFire has flagged a potentially risky process.

Malware Blocked
- Number of times ThreatFire has discovered and blocked malware.

You can always review what these items mean by clicking the **Learn More** link at the bottom right of the window. Clicking this link will launch a web page which explains all the terms and gives you the latest statistics.

There are five date tabs across the top: **Today, Last 7 Days, Last 30 Days, Last 90 Days** and **Total**. Clicking on any of these tabs allows you to see your statistics for the relevant time period.

You may also access this report at any time through the tray icon. Simply right-click on the ThreatFire icon and choose **Status.**

System Scan

The **System Scanner** can be accessed by clicking the **Start Scan** button, which is the 2nd button down the left on the main ThreatFire control panel. The ThreatFire **System Scanner** can be configured to scan for rootkits and known.

You don't have to do anything special for ThreatFire to monitor your system for rootkits. ThreatFire is constantly on the lookout for signs of hidden processes that are running on your system that might indicate the presence of a rootkit. However, hidden processes are not the only indicators of a rootkit. A rootkit may contain several pieces and the **System Scanner** dives deeper into your system seeking out any hidden files, registry keys or other objects that may be part of a rootkit.

You can also configure your scan to look for viruses and other known threats that may be dormant on your system and thereby not detectable by ThreatFire's behavior detection (since they're not displaying any malicious behavior).

If ThreatFire finds anything, it will give you the option to quarantine the threat. From the **Quarantine** section in Threat Control you can then also choose to permanently delete the objects off your system.

Running a Scan

To run a scan:

1 Select **Start/All Programs/ThreatFire/ThreatFire**.
Or
Right-click the **ThreatFire**  icon in the system tray:
The choices are **ThreatFire, Tutorial, Quick Start Guide, Suspend** and **Status**.

Click **ThreatFire.**

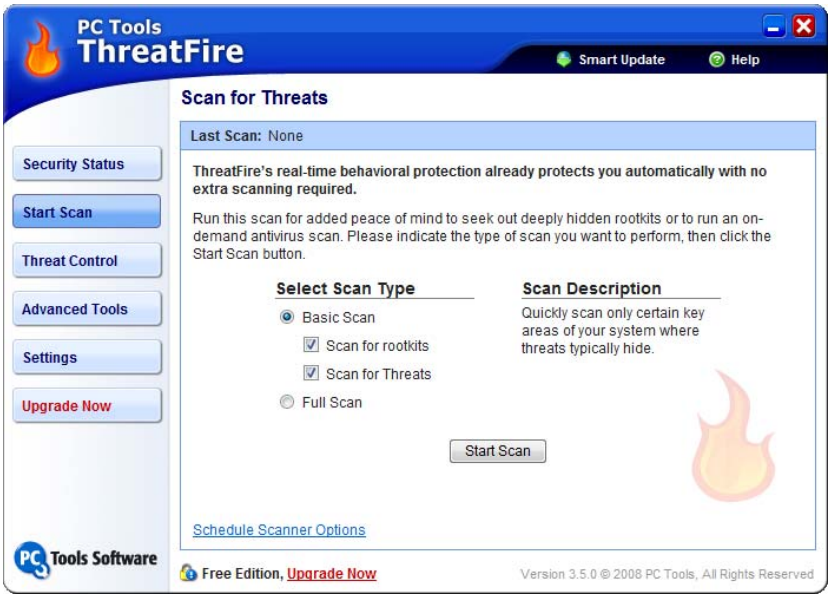
2 Select **ThreatFire**.

The **ThreatFire** window appears:

System Scan

3 On the left side select the **Start Scan** button.

4 The main **System Scanner** window appears.



5 Select the scan type you wish to run: **Basic** or **Full**.

A Basic scan will only search certain key areas of your system where rootkits and other threats most typically hide, whereas a Full scan will perform a comprehensive scan of your entire system.

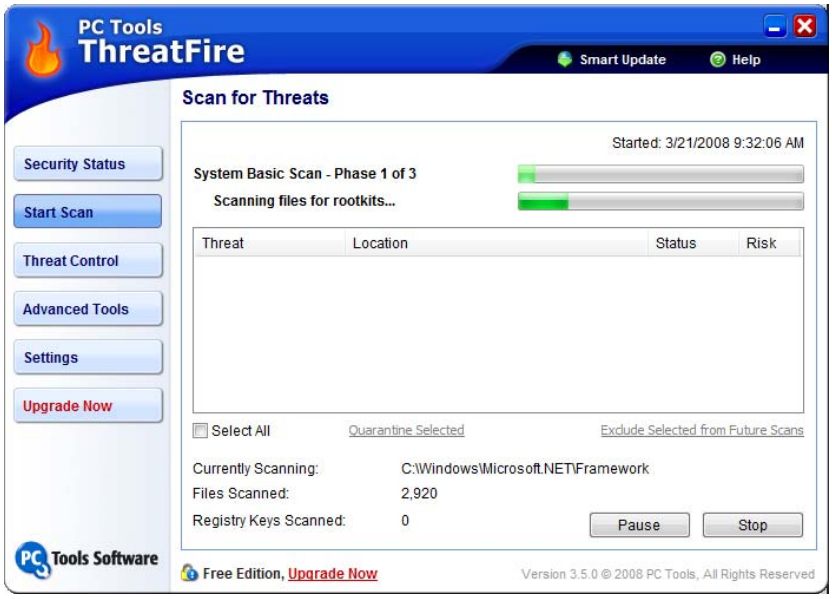
Take Note

A **Basic Scan** will not scan archive files. If you need to scan archives, please select **Full Scan.**

6 Then select the type of threats you wish to scan for: **Rootkits** or **All Threats** or **both**.

7 After selecting your scan type, click the **Scan Now** button to begin the scan.

The scan window appears and you can view the progress of your scan:



8 As the scan is running you may click the **Pause** button to temporarily stop the scan. If you choose to **Pause**, the **Pause** button changes to a **Resume** button which allows you to resume the scan when you choose.

You may also choose to **Stop** the scan by hitting the **Stop** button**.** This action will terminate the scan in progress.

System Scan

9	At the completion of the scan you will be shown the results of the scan and any rootkits or other threats found. If threats are found, select the items in the list and quarantine them by clicking the **Quarantine Selected** link.

	After quarantining, you may wish to permanently remove any rootkits. Simply visit the **Quarantine** section in **Threat Control** to manage quarantined items.

Threat Control

Threat Control is the 3rd button down the left on the main ThreatFire control panel. The Threat Control Center is where you can manage your alert actions and choices with respect to system activity. This is also where you manage any Quarantined items and where you can view the log of all ThreatFire actions.

ThreatFire Threat Control Center

The Threat Control button displays the following four tabs across the top:

Allowed

- This list displays all items you asked ThreatFire to always allow. If you no longer wish to always allow a particular item, select the appropriate entry and click **Remove** to remove it from this list. The next time that process attempts to run you will be presented with a new alert where you can then select Allow or Deny as appropriate.

Denied

- This list displays all items you asked ThreatFire to always deny, but not quarantine. If you no longer wish to always deny a particular item, select the appropriate entry and click **Remove** to remove it from this list. The next time

that process attempts to run you will be presented with a new alert where you can then select Allow or Deny as appropriate.

This list is applicable only if you have created any custom rules. Any custom rules will display a special alert with the option to **Allow the process**, **Kill and quarantine the process,** or **Kill the process** one time only. Any items that you elect to kill one time only, and also check the **Remember this answer** box, will be displayed in this Denied bin.

Quarantined

- Malware that has been automatically quarantined for your protection can be managed here. You can **Restore** or **Permanently Delete** an item by selecting it in the list and clicking the appropriate link at the bottom of the window.

Protection Log

- This section displays a log of all actions taken by ThreatFire and all processes monitored or examined for signs of suspicious behaviors.

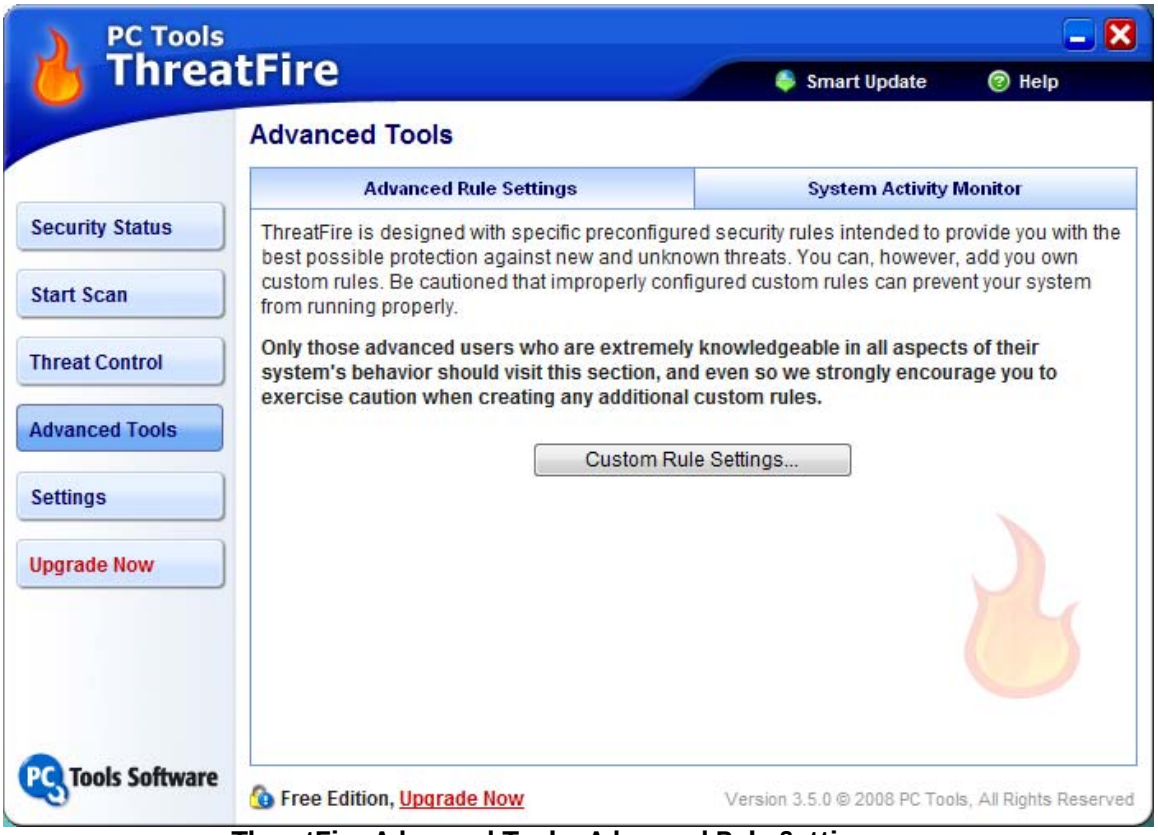
To permanently clear the contents of all log files, click the **Clear log** link in the bottom right. Please note that once these items have been removed you will no longer be able to access the data.

Advanced Tools

Advanced Tools is the 4th button down the left on the main ThreatFire control panel. This area includes advanced tools to allow advanced users to see detailed information about their system and to create custom rules for locking down their PC beyond what's included with ThreatFire's built in rules.

The **Advanced Tools** tab includes two sections: **Advanced Rules Settings** and **System Activity Monitor .**

The default display will open to **Advanced Rule Settings** tab:



ThreatFire Advanced Tools—Advanced Rule Settings

Advanced Rules: Creating and Modifying Rules with the Rule Wizard

What is the Rule Wizard?

The Rule Wizard is found on the **Advanced Rules** button, which is the 4th button down the left on the main ThreatFire control panel.

The Rule Wizard is an advanced feature used to create and modify rules.

Only those advanced users who are extremely knowledgeable in all aspects of their computer's behavior should visit the Rule Settings area and use the Rule Wizard.

The Rule Wizard takes you through four components and an action that allow you to create arguments that compose a rule ThreatFire will enforce. Let's say you know of several dangerous Internet sites. You can compose rules that keep you or other users from entering those sites. Another rule you might create, and one that is illustrated in this chapter, is to block the execution of Peer-to-Peer software (see Creating a Rule on p. 47).

The Rule Wizard contains the following four components:

- Source
- Trigger
- Options
- Exclusions

and it consists of a logical argument in this form:

If (*condition x acts this way)* **Then** (*take this action)* **Except (***when this is involved)*

The "If" clause of the argument is made up of the following components:

- Source
- Trigger
- Options

The "Except" clause of the argument consists of the following component:

- Exclusions

About the Rule Wizard

Accessing the Rule Wizard

To access the rule wizard:

1 Select **Start/All Programs/ThreatFire/ThreatFire**.
Or

Right-click the **ThreatFire** icon in the system tray:
The choices are **ThreatFire, Tutorial, Quick Start Guide, Suspend** and **Status**.

Click **ThreatFire**

2 Select **ThreatFire**.

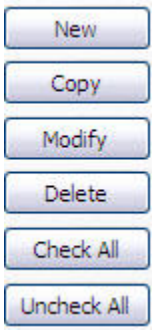
The **ThreatFire** window appears.

3 On the left side of the pane select **Advanced Tools**.

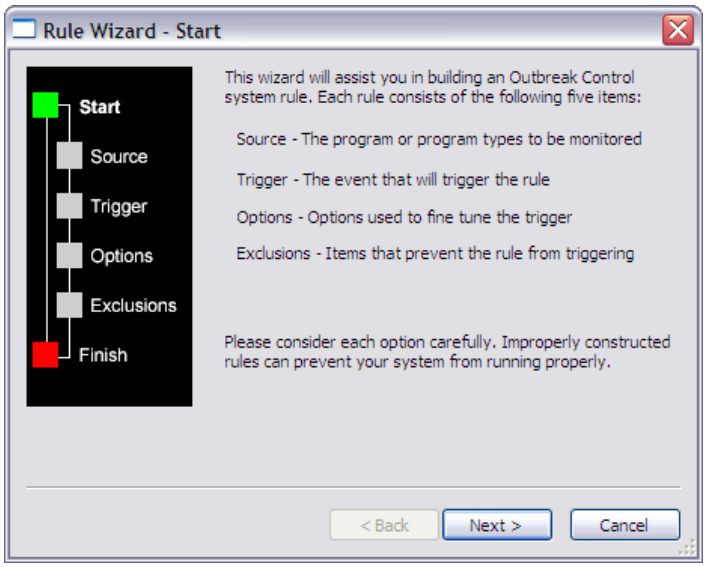
The **Advanced Tools** window displays:

4 Click the **Custom Rule Settings** button to begin.

5 On the Custom Rules window, click the **New** or **Modify button**.



The Rule Wizard appears:



Important! Improperly constructed rules can prevent your computer from running properly.

Using the Rule Wizard

To use the Rule Wizard, first bring up the Rule Wizard.

The Rule Wizard consists of four items (see What is the Rule Wizard? on p. 35).

Source

The Source is "the program or program types to be monitored."

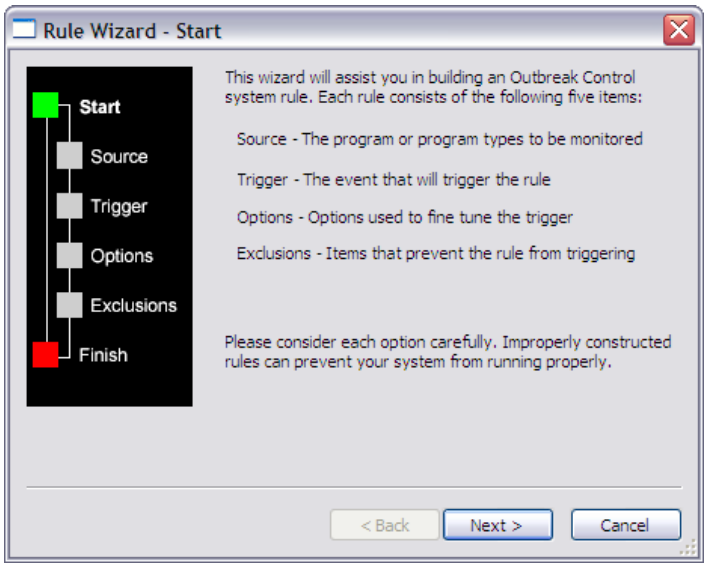
The source can be a program or application. It can be an email program or browser process, such as Internet Explorer, Firefox or Opera.

It can also be a non-interactive process, such as svchost.exe, which checks for Windows updates.

It can even be a list of specific processes, applications, or systems in which you want to prohibit certain behaviors.

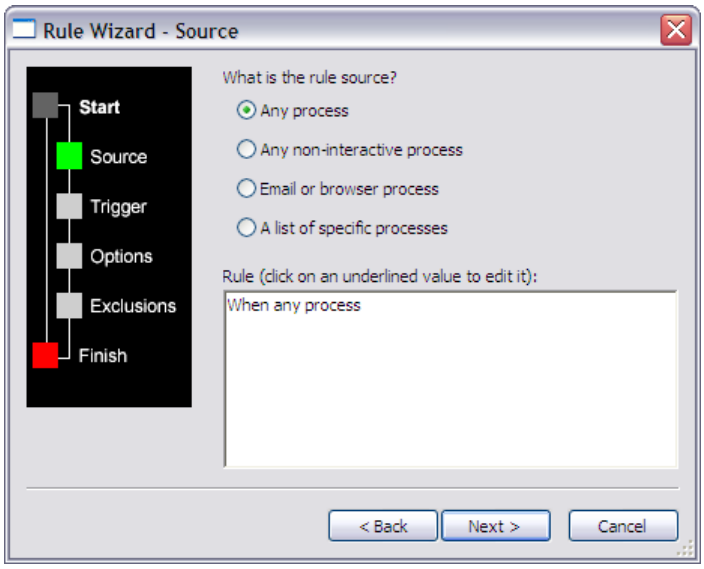
To select a source:

1 Bring up the Rule Wizard and click **Next**:



2 Select a rule source.

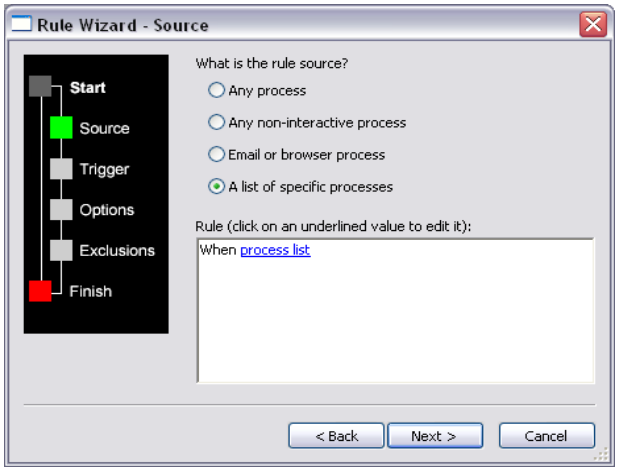
The rule sources appear at the top of the **Rule Wizard - Source** dialog box:



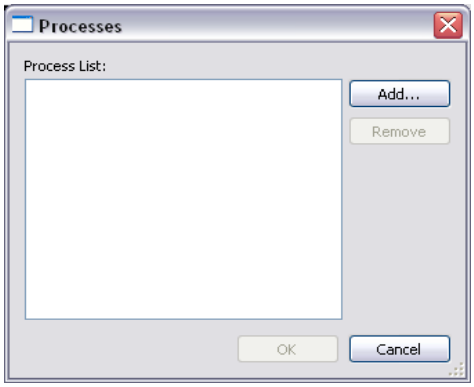
3 When you select a rule source, the **Rule** box is populated with the source of the rule.

4 If your rule source is underlined, click on it to edit it.

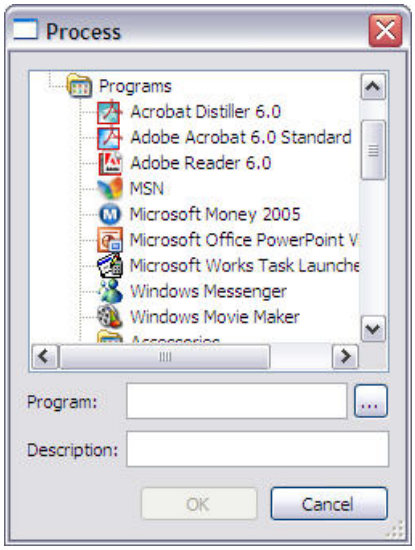
For example, if you selected **A list of specific processes**, click **process list**.



The **Processes** dialog box appears:



5 Then click the **Add** "…" button to add a process. The Process dialog box appears:



6 Highlight the program from the tree or use the ellipse to browse to the selected program.

7 Click **OK** to continue or **Cancel** to cancel.

8 After you select the source, click the **Next** button.

You can click the **Back** button to change or review items.

Trigger

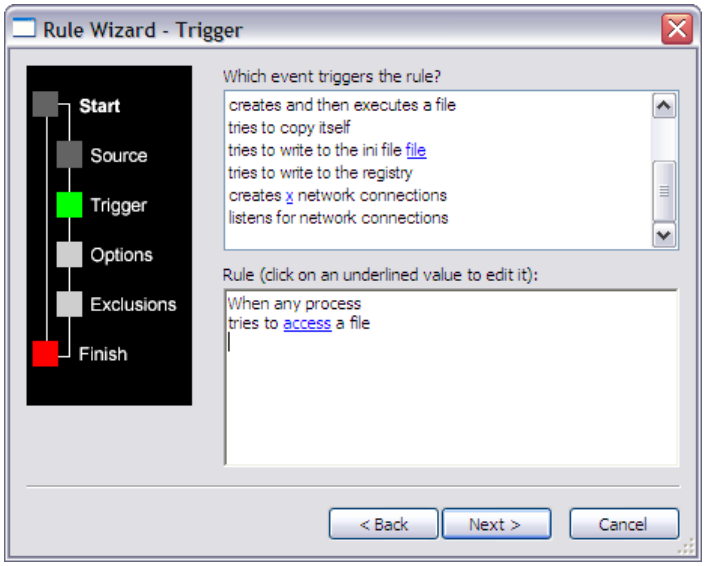
The Trigger is "the event that will trigger the rule."

Triggers are behaviors of sources, such as accessing a file, trying to rename a file, or, in the case of Internet Explorer, Firefox or Opera, even allowing access to it. You can create a rule to block Internet access completely or to block access to a particular website or domain.

To select a Trigger:

1. Click **Next** from the **Rule Wizard – Source** dialog box after you have selected a Source.
2. Select a trigger for your source by clicking it.

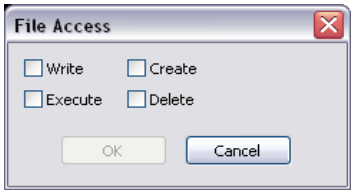
   The rule triggers appear at the top of the window:



3. When you select a rule trigger, the **Rule** field is populated with the trigger of the rule.
4. If your rule trigger has an underlined value, click on it to edit it.

   For example, if the trigger for your source is **tries to access a file**, click on **access**.

   The **File Access** dialog box appears:



   You can select any combination of these file access options. Select **Ok** to accept the options you chose or **Cancel** to close the dialog without making any selections.

5	After you select the trigger, click the **Next** button. You can click the **Back** button to change or review items.

Options

Options are "used to fine tune the trigger."

For example, for a rule thus far written:
When any process
Tries to execute a file

You can select any of these options:

- named file name
- in the folder
- that looks like an executable
- containing executable code
- with a suspicious double extension

Click underlined values to edit them.

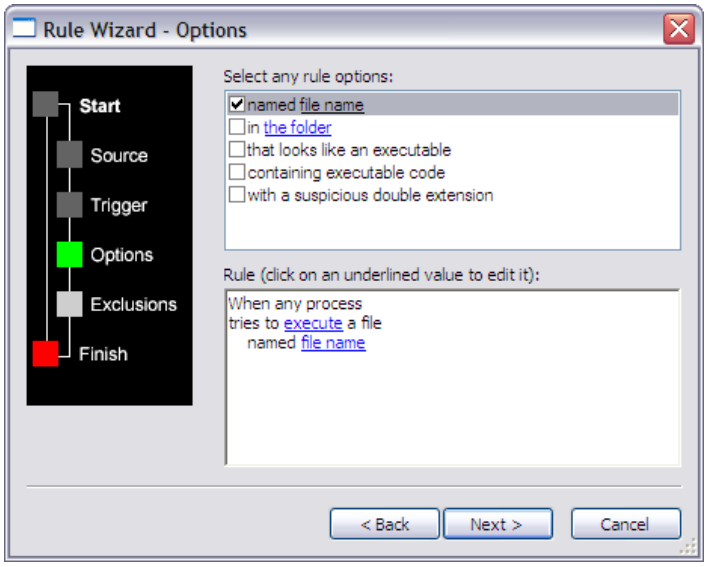
To select any rule options:

1	Click **Next** from the **Rule Wizard – Options** dialog box after you have selected a Trigger.
2	Select any rule options by checking the box in front of them. The rule options appear at the top of the window.

When you select rule options, the **Rule** field is populated with the options of the rule.

For example if you chose the trigger tries to execute a file, five options are available:

- named file name
- in the folder
- that looks like an executable
- containing executable code
- with a suspicious double extension



3 Click on underlined values to edit them.

4 After you select any rule options, click the **Next** button.

You can click the **Back** button to change or review items.

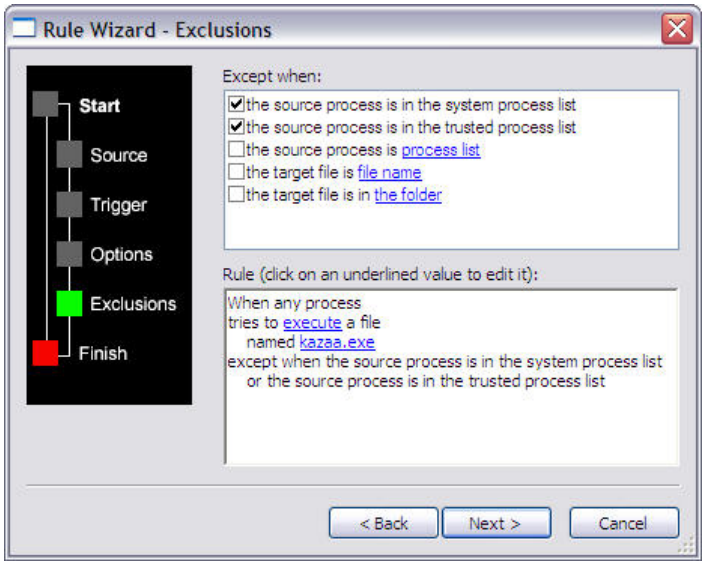
Exclusions

Exclusions are "items that prevent the rule from triggering."

To select or deselect exclusions:

1. Click **Next** from the **Rule Wizard – Options** dialog box after you have selected an Option.
2. Select available exclusions by checking the box in front of them or by accepting the selection.

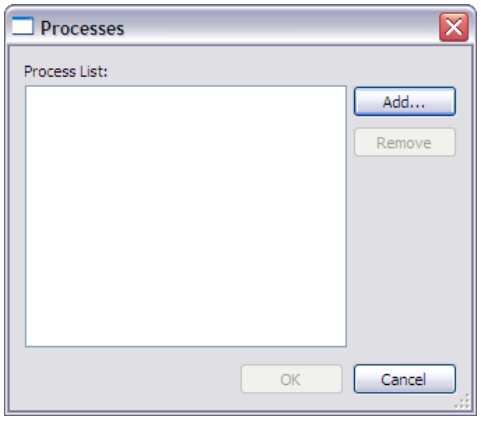
   Exclusions appear at the top of the window.



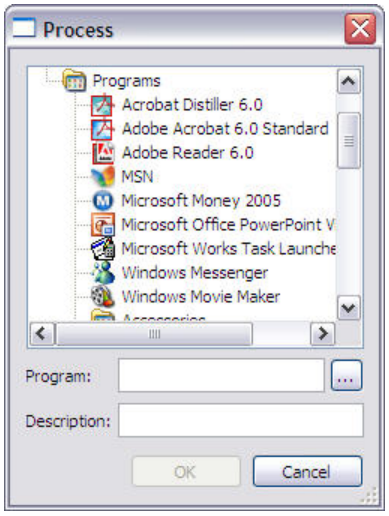
3. Deselect available exclusions by checking or deselecting the box in front of them
4. When you select rule exclusions, the **Rule** field is populated with the exclusions of the rule.
5. For example, you may wish to include the **source process is process list**.
6. Check the box in front of it.

   It appears in the **Rule** box at the bottom of the dialog box.
7. Click on underlined values to edit them.

8 If you click process list, the **Processes** dialog box appears.



9 Click the **Add...** button to add a process. The **Process** dialog box appears:



10 Highlight the program from the tree or use the ellipse to browse to the selected program.

11 Click **OK** to continue or **Cancel** to cancel.

12 After you accept or deselect exclusions, click the **Next** button.

You can click the **Back** button to change or review items.

13 Click **Finish** in the Rule Wizard to create your rule.

This guide does not show the examples with the intent that you should follow them—these examples are for informational purposes only. Only sound rules will work on your computer, and incorrectly constructed ones will cause your computer to function improperly. The examples are meant as illustrations only!

Creating a Rule

You can create rules using the Rule Wizard.

Let's say you want to create a rule to block the execution of Peer-to-Peer software.

Only those advanced users who are extremely knowledgeable in all aspects of their computer's behavior should visit the Rule Settings area and use the Rule Wizard to create or modify rules.

To create a rule:

1. Select **Start/All Programs/ThreatFire/ThreatFire**.
   Or
   Right-click the **ThreatFire** icon in the system tray:
   The choices are **ThreatFire, Tutorial, Quick Start Guide, Suspend** and **Status**.

   Click **ThreatFire.**

2. Select **ThreatFire**.

   The **ThreatFire** window appears.

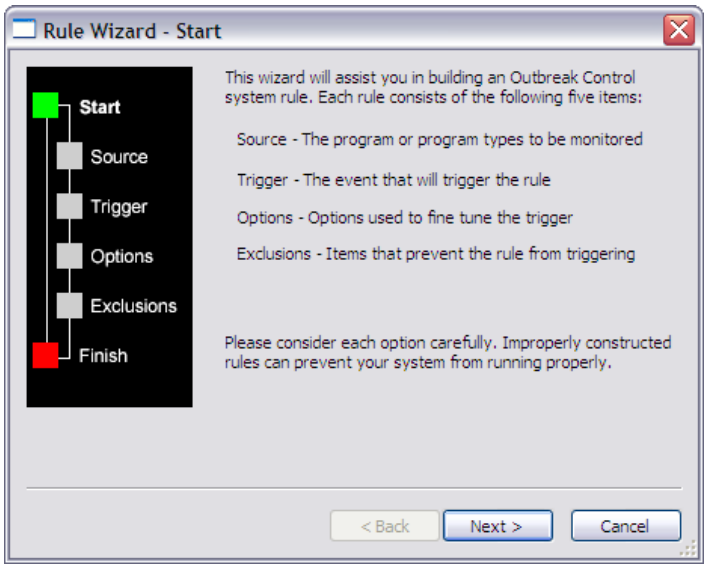
3. On the left side of the pane select **Advanced Tools**.

   The **Advanced Tools** window displays.

4. Click the **Custom Rule Settings** button to begin.

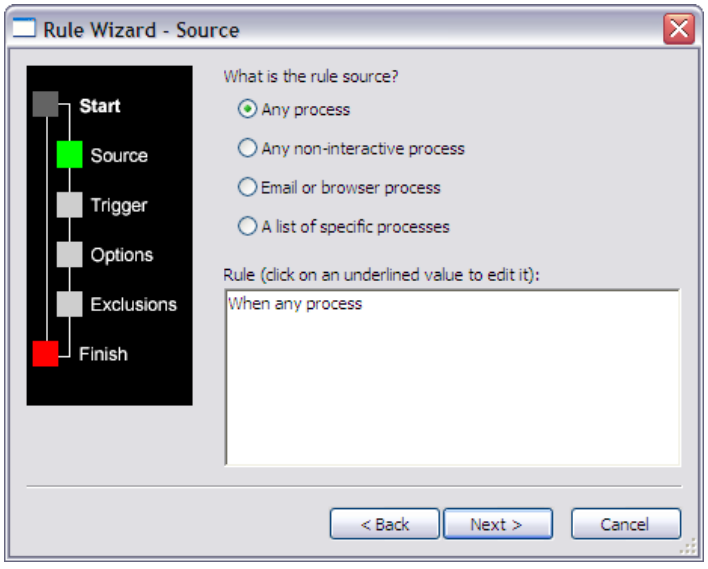
5 On the **Custom Rules** window, click **New**.

The Rule Wizard appears:



6 Click the **Next** button.

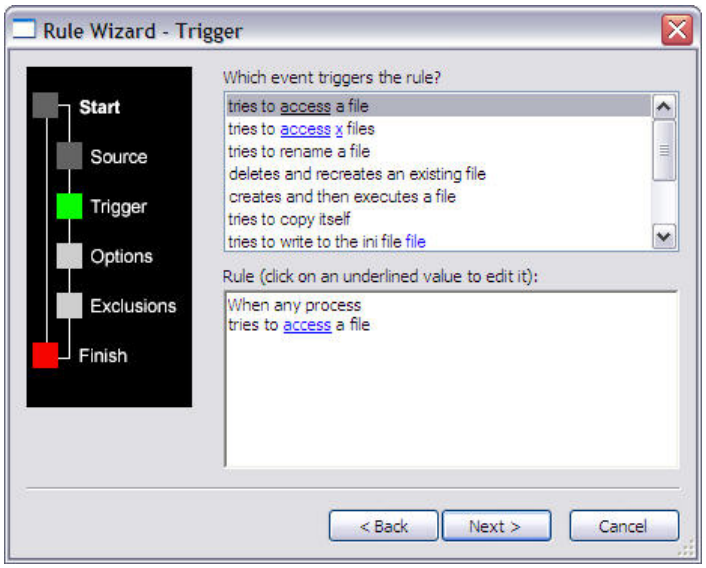
The **Rule Wizard – Source** dialog box appears.



Make sure that **Any process** is selected.

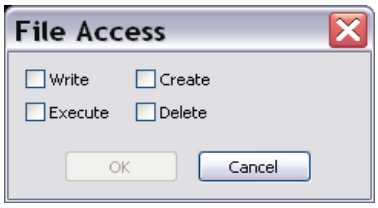
7 Click the **Next** button.

The **Rule Wizard – Trigger** dialog box appears. Select **tries to access a file**.



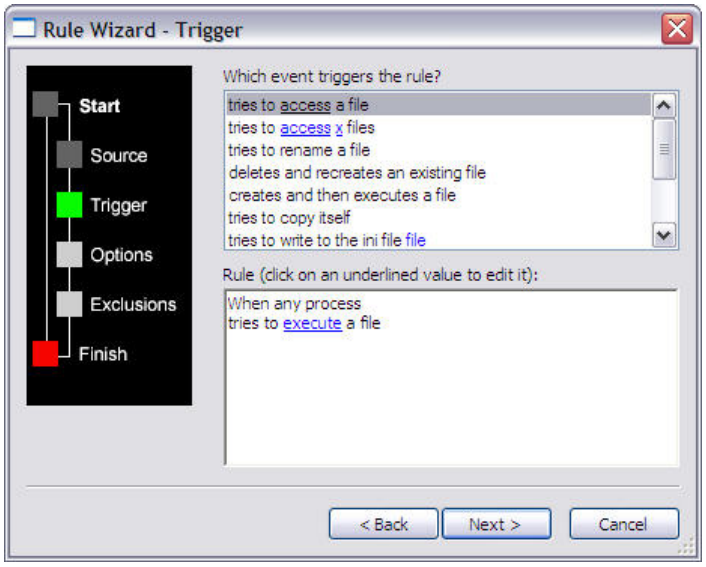
8 Click the underline value **access** in the **Rule** box.

The **File Access** dialog box appears. Check the **Execute** box:



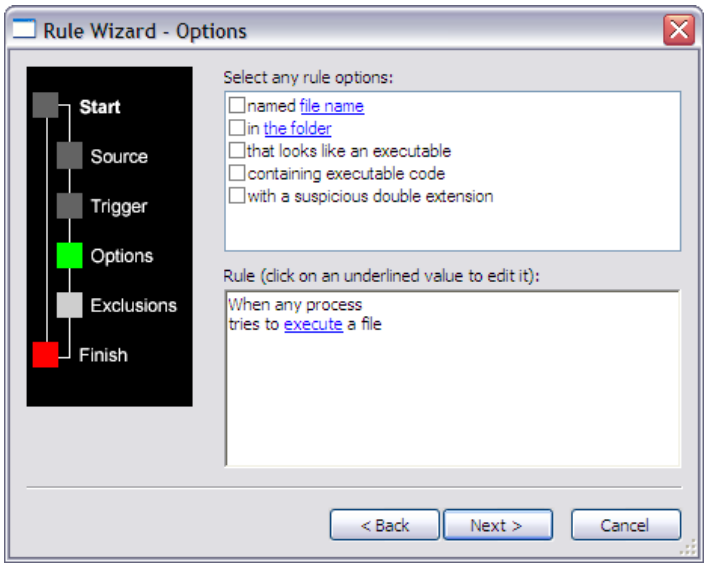
9 Click **OK**.

The trigger **Execute** appears in the **Rule** box:



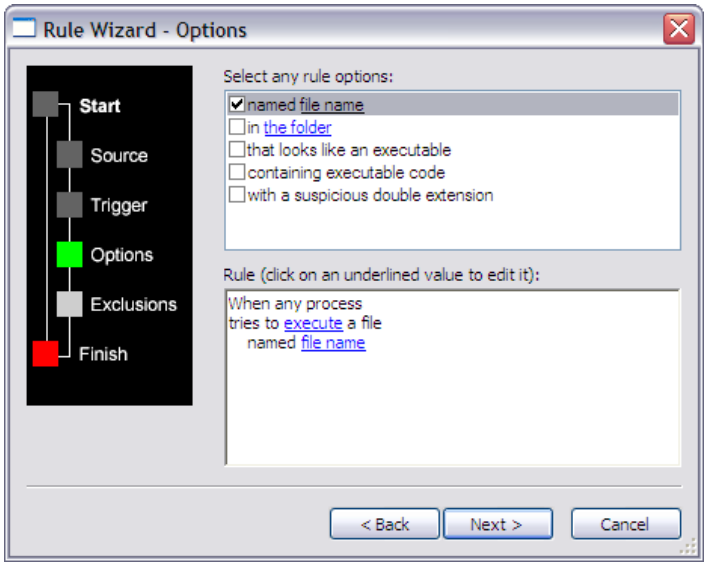
10 Click **Next**.

The **Rule Wizard – Options** dialog box appears.



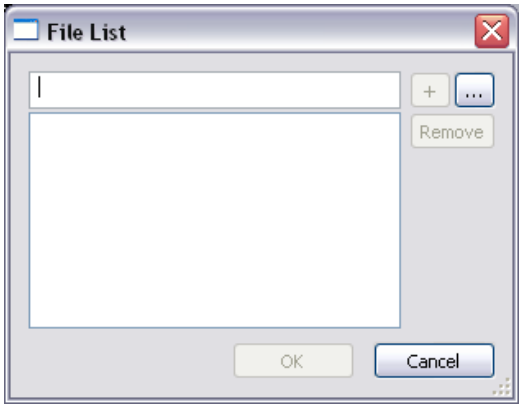
11 Check the box in front of **named file name**.

The **named file name** option appears in the **Rule** box:

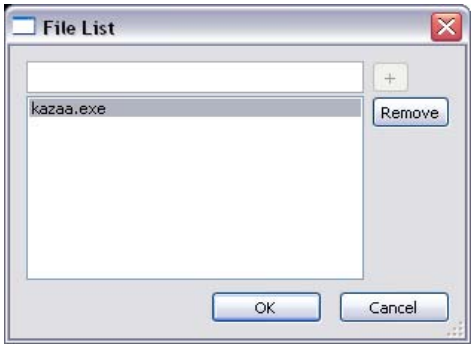


12 Click the underlined value **file name** in the **Rule** box.

The **File List** dialog box appears:

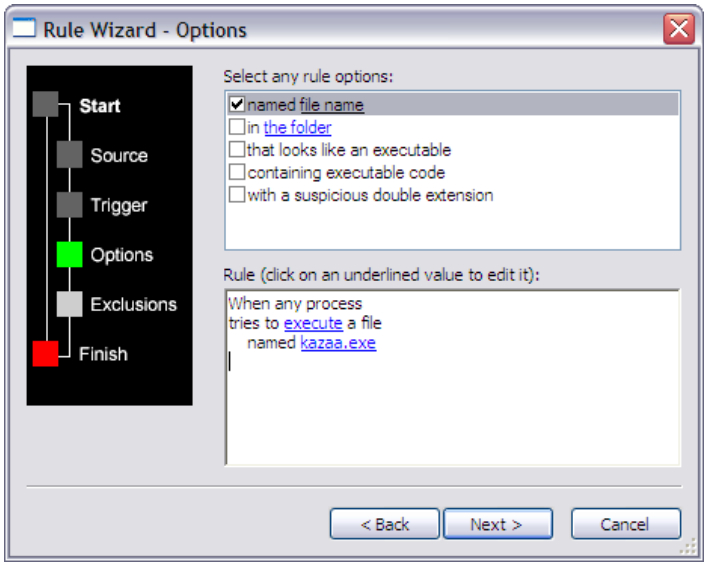


13 Type **kazaa.exe** and click the **+** button to add it to the list of executable files to block.



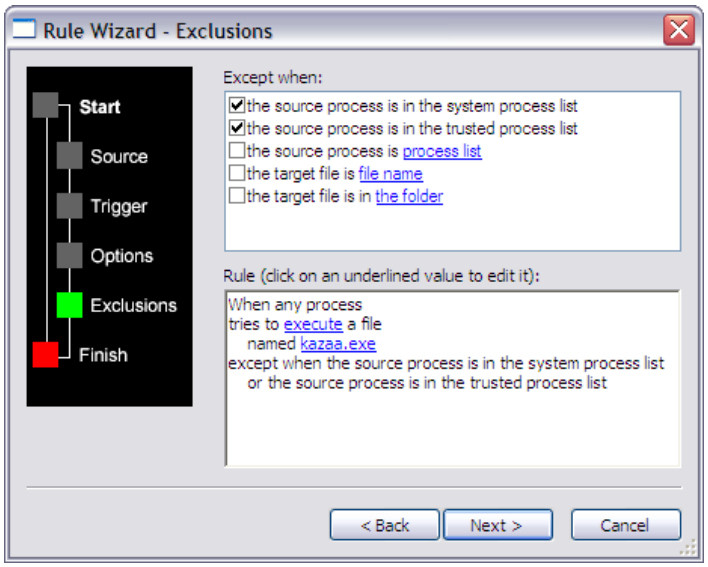
14 Click **OK**.

The value typed appears as part of the rule in the **Rule** box:

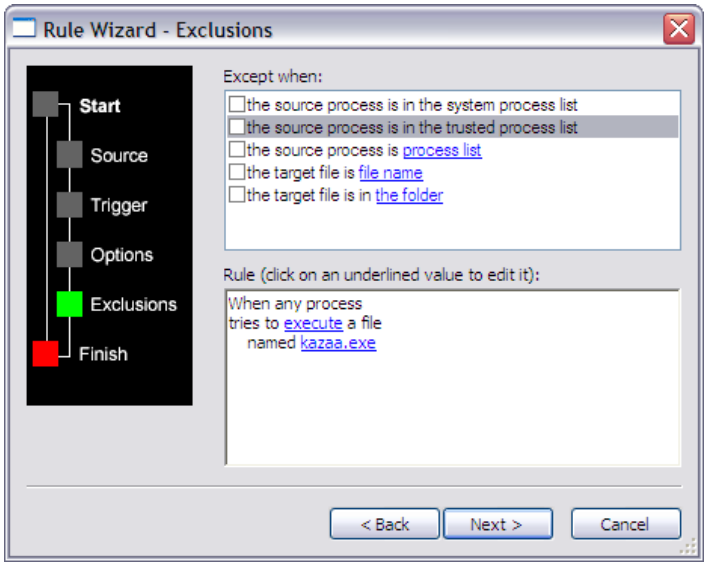


15 Click **Next**.

The Rule Wizard – Exclusions dialog box appears:

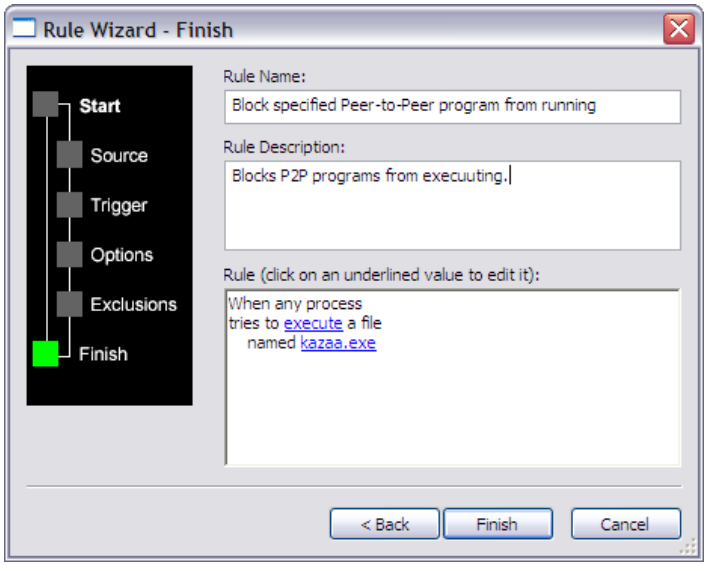


16 Uncheck **the source process is in the system process list** and **the source process is in the trusted process list**.



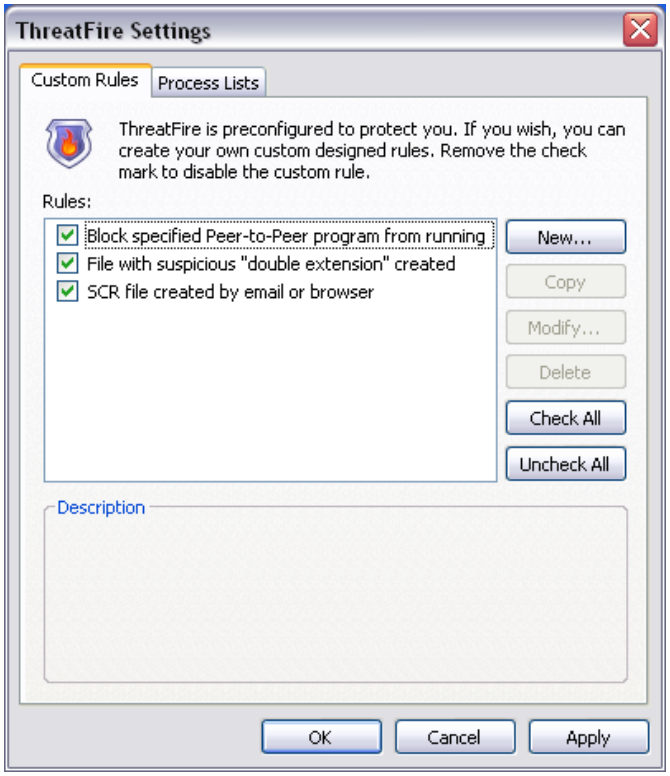
17 Click **Next**.

18 Type in the rule name and description. Be as descriptive with both as you want.



19 Click **Finish**.

The rule appears in the **Rules** box:

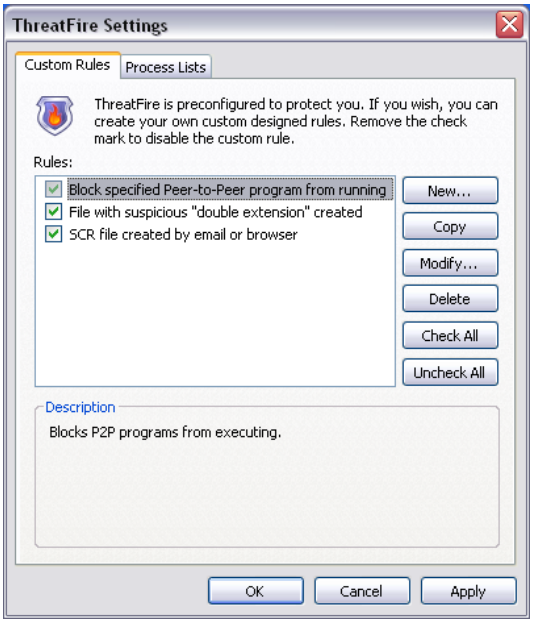


Modifying a Rule

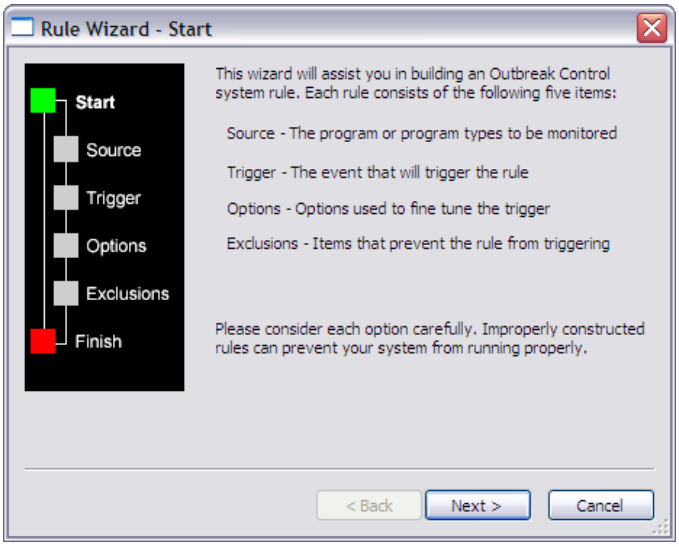
We are now going to modify the rule we just made.

To modify a rule:

1. Highlight the rule you want to modify.

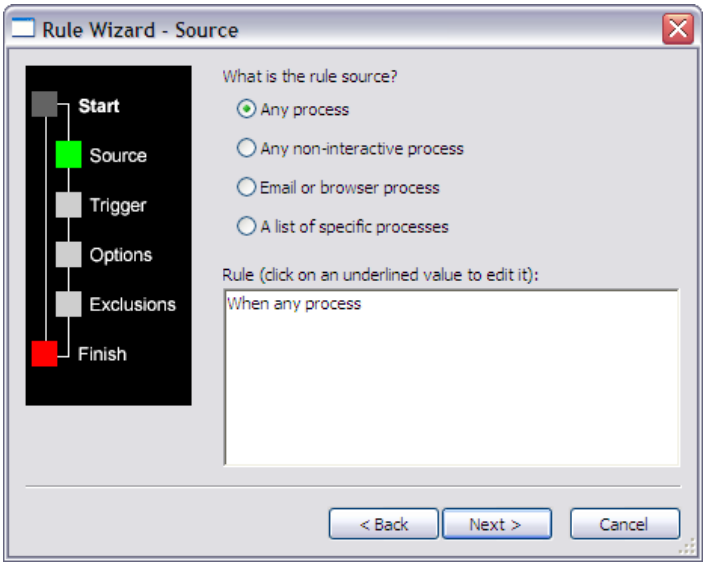


2. On the **Custom Rules** window, click **Modify**.
   The Rule Wizard appears:



3 Click the **Next** button.

The **Rule Wizard – Source** dialog box appears.

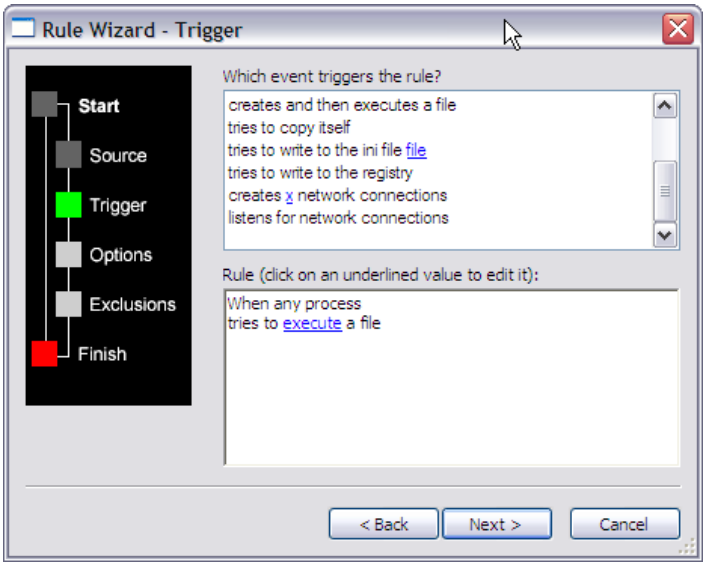


The Rule Wizard shows you the choices you made in making your rule, and you can make any modifications to

- Source
- Trigger
- Options
- Exclusions

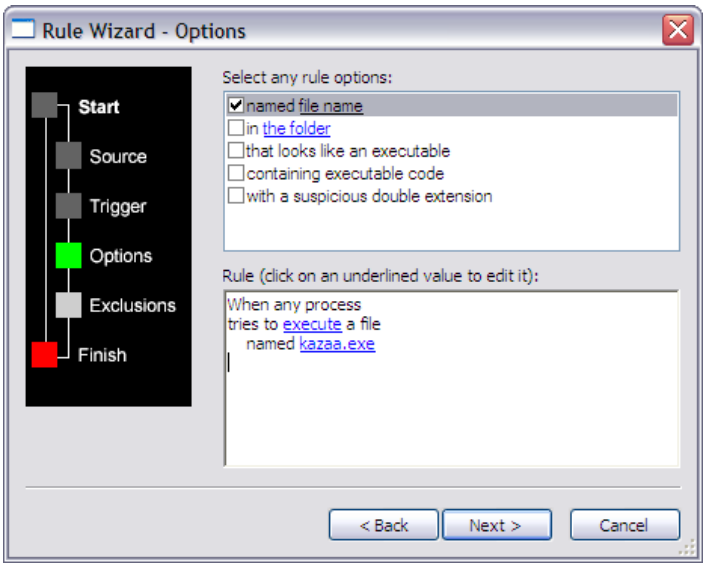
4 Click the **Next** button.

The **Rule Wizard – Trigger** dialog box appears with the choice you made:

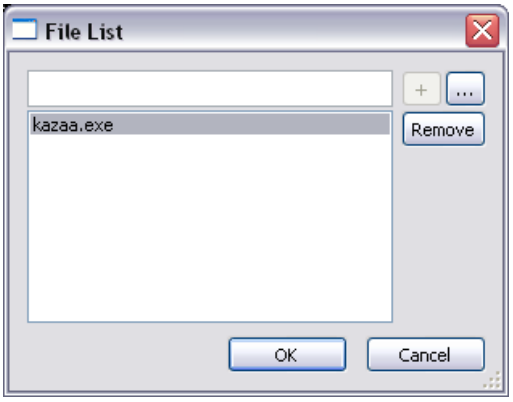


5 Click **Next**.

The **Rule Wizard – Options** dialog box appears with your selection.

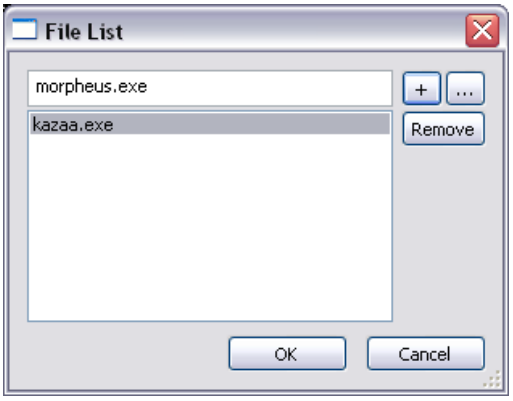


6 Click **kazaa.exe**.



The **File List** dialog box appears with the choice you made:

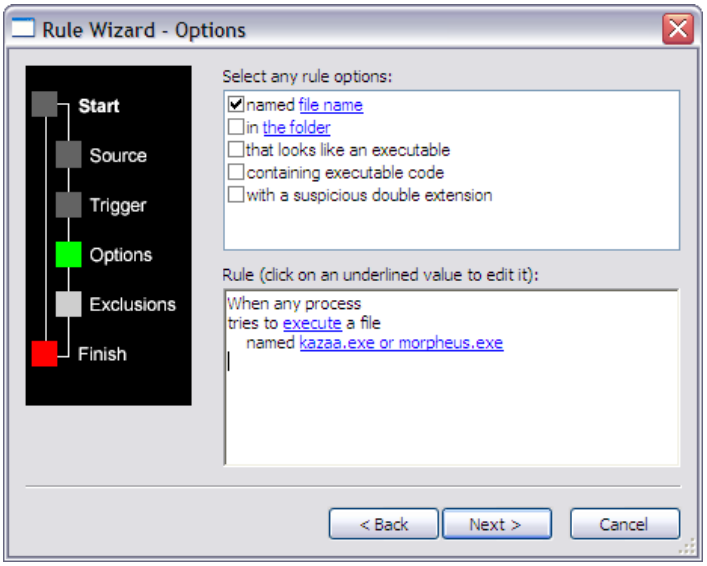
7 Type **morpheus.exe** in the text box.



8 Click the **+** button to add it to the list of executable files to block.

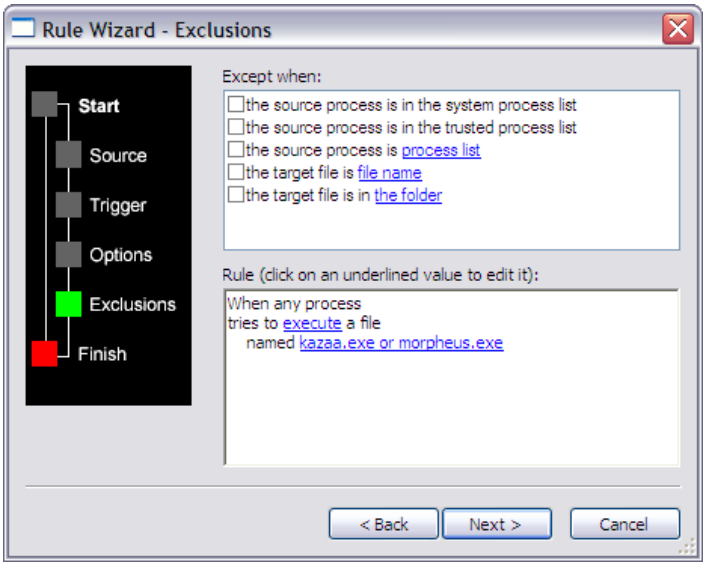
Click **OK**.

The modified rule appears in the **Rule Wizard – Options** dialog box:



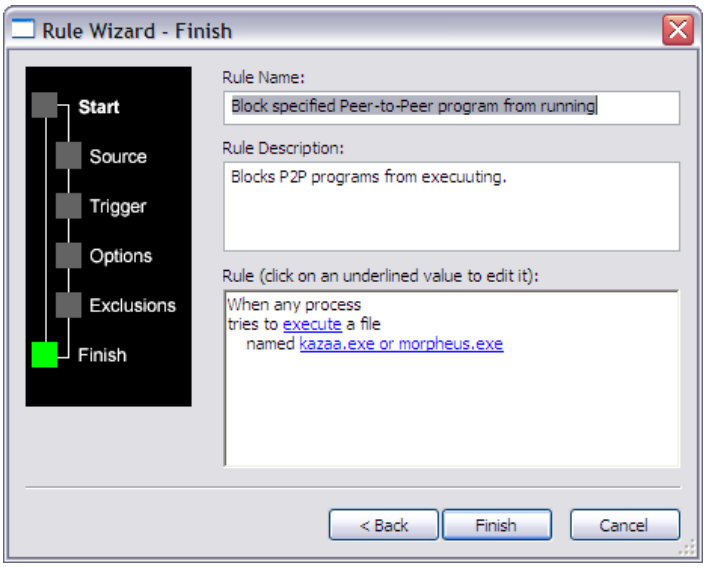
9 Click **Next**.

The **Rule Wizard – Exclusions** dialog box appears:

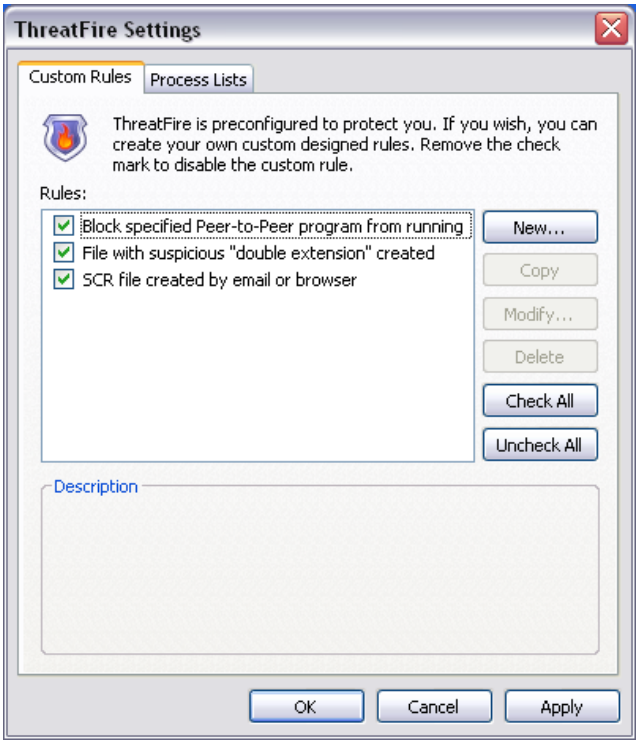


10 Click **Next**.

11 Click **Finish**.



The rule appears in the **Rules** box:



Viewing Rules

ThreatFire is meant to work interactively and yet autonomously. When you participate in the Secure Community, actions you take against behaviors are anonymously sent to the Secure Community. This provides information to PC Tools about new threats and the behavior manifested by these threats, allowing PC Tools to create new rules to combat them.

ThreatFire warns you: Only those advanced users who are extremely knowledgeable in all aspects of their computer's behavior should visit this section, and even so we strongly encourage you to exercise caution when making any changes.

If you want to view rules you have created:

1. Right-click the **ThreatFire** icon and select **ThreatFire**.

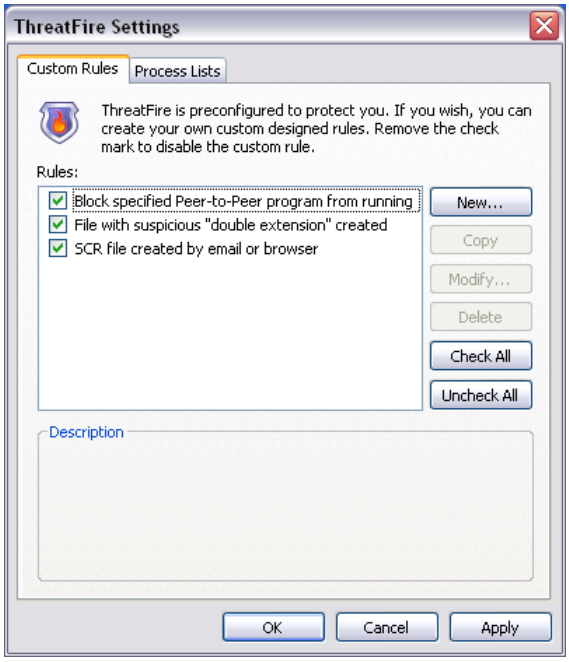
   The **ThreatFire** window appears.

2. Select the **Advanced Tools** option on the left side of the pane.

   Then select the **Advanced Rules Settings** tab on the right.

3 Click the **Custom Rule Settings** button on that pane.

The **ThreatFire Settings** window appears:



4 Highlight a rule to see the description at the bottom of the window.

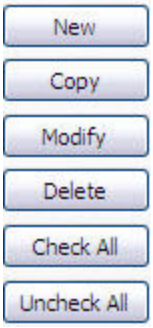
5 Remove the check in the box in front of the rule to disable it.

The Custom Rules Tab

Under the **Custom Rules** Button, you'll find two examples of rules you can create, plus any new rules you create. In the default configuration, the sample rules do not have a check in the box in front of them. To have ThreatFire enforce a rule, just click the box in front of the rule to add a check. To disable a rule, remove the check by clicking the appropriate box.

Custom Rules Tab Buttons

On the right of the **Custom Rules** tab are six buttons:



Take Note

You must first highlight a rule for these buttons to be active. If no rule is highlighted, the buttons appear as dimmed.

Creating New Rules

Creating rules is discussed in the section The Rule Wizard - Creating and Modifying Rules.

Copying Rules

To copy rules:

1. To copy a rule, first highlight the rule.
2. Click the **Copy** button.

   The rule is copied and put on the bottom of the rules.

To copy all rules:

1. To copy all rules, click the **Check All** button.
2. Click the **Copy** button.

   Click the **Uncheck All** button to deselect them.
3. Click the **Apply** button at the bottom of the window to finalize any changes.

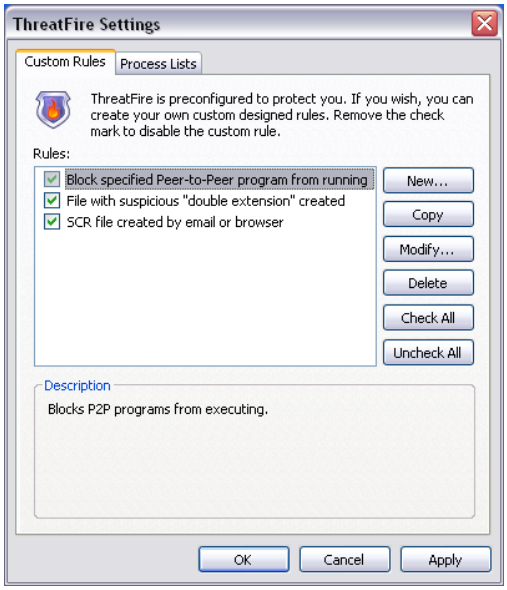
Modifying Rules

Modifying Rules is discussed in The Rule Wizard - Creating and Modifying Rules.

Deleting Rules

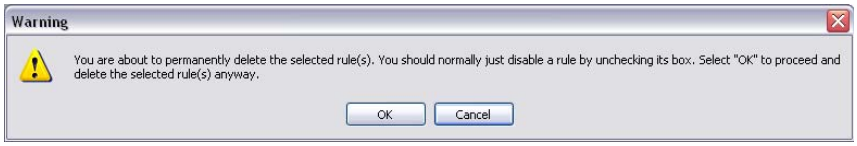
To delete a rule:

1 Highlight the rule.



2 Click the **Delete** button.

The following warning appears:



Take Note

A profile is the set of rules configured on a given computer.

3 Click **OK** to continue or **Cancel** to cancel.

4 Click the **Apply** button to finalize your changes.

Selecting and Deselecting All Rules

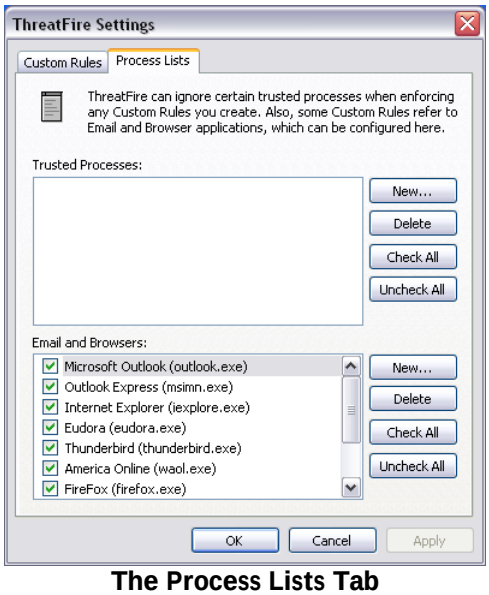
- Click **Check All** to select all rules and **Uncheck All** to deselect all rules.
- Click the **Apply** button to finalize your changes.

The Process Lists Tab

The **Process Lists** tab allows you to add exclusions to rules (see Exclusions on p. 45) and email programs and browsers to rule sources (see Source on p. 38).

The tab has two boxes:

- Trusted Processes
- Email and Browsers



The Process Lists Tab

The Rule Wizard — Exclusions

As explained in Exclusions on p. 45, Exclusions is one of the four components the Rule Wizard uses to configure a rule.

Important! Improperly constructed rules can prevent client computers from running properly.

Exclusions exempt processes that are listed in the **Trusted Processes** box. The rule will not execute when one of these processes is the source process when the rule is triggered.

Trusted Processes List

At the top of the **Process Lists** tab is the **Trusted Processes** list.

This list contains the trusted processes that are created as exceptions to custom rules.

Therefore, any processes listed in the Trusted Processes box are exempt from the rule. The rule will not fire for those processes.

Process Lists Tab Buttons

On the right of the Trusted Process list are four buttons:

Use these to create, delete, select and deselect all trusted processes.

Creating a New Trusted Process

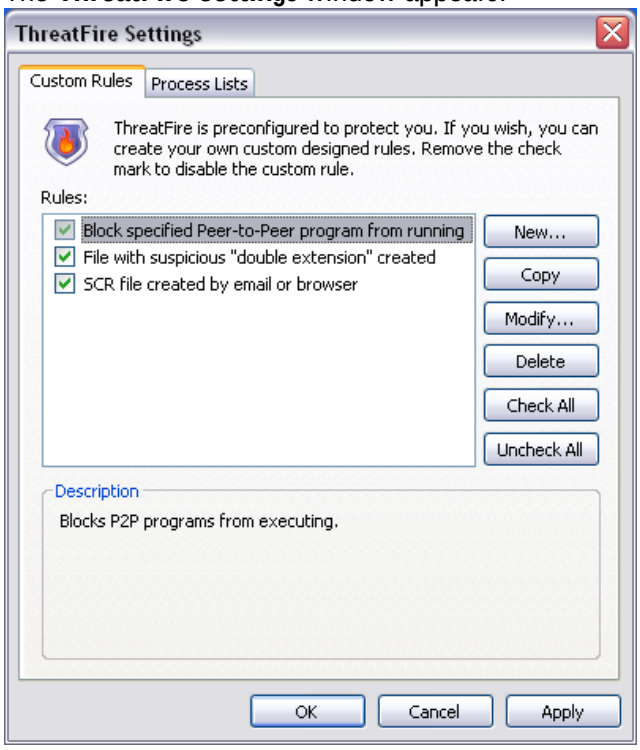
To add a new trusted process:

1. Select **Start/All Programs/ThreatFire/ThreatFire**.
   Or
   Right-click the **ThreatFire** icon in the system tray:
   The choices are **ThreatFire, Quick Start Guide, Suspend** and **Status**.
   Click **ThreatFire**.
2. The **ThreatFire** window appears.
3. Select the **Advanced Tools** tab on the left side of the pane.

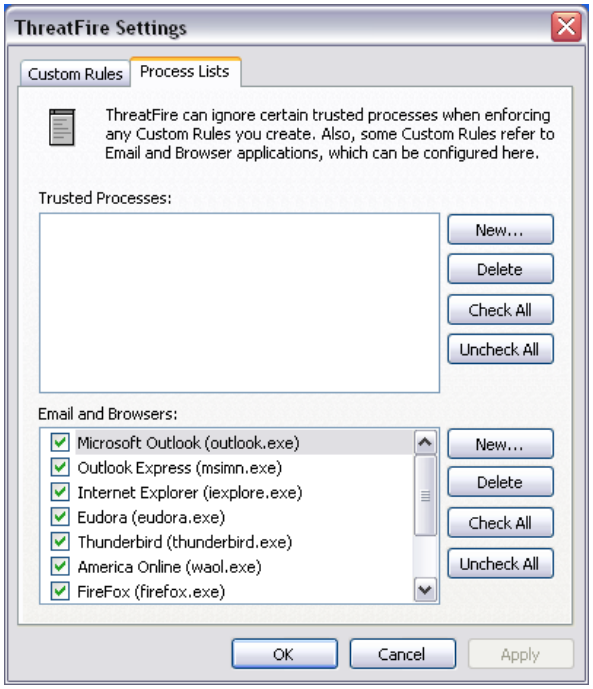
Then select the **Advanced Rule Settings** tab.

4 Click the **Custom Rule Settings** button on that pane.

The **ThreatFire Settings** window appears:



5 Click the **Process Lists** tab.

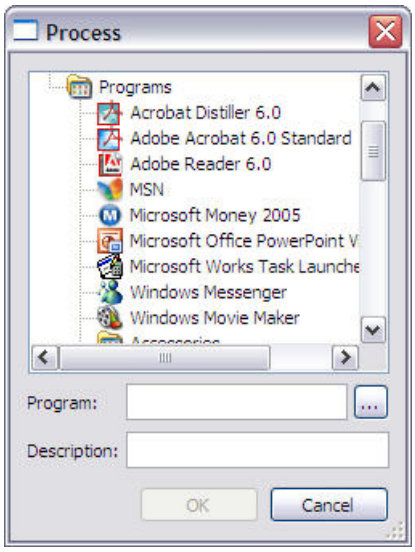


6 Click the **New** button next to the **Trusted Processes** box.

Take Note

The **New** button does not bring up a custom rule; it brings up a dialog box that allows you to add processes that will be excluded when a rule fires.

7 The **Process** dialog box appears:



8 Highlight the program from the tree or use the ellipse to browse to the selected program.

9 Click **OK** to continue or **Cancel** to cancel.

The program is added to the **Trusted Processes** list.

10 Click **Apply** at the bottom of the **Process Lists** tab to finalize any additions.

Deleting a Trusted Process

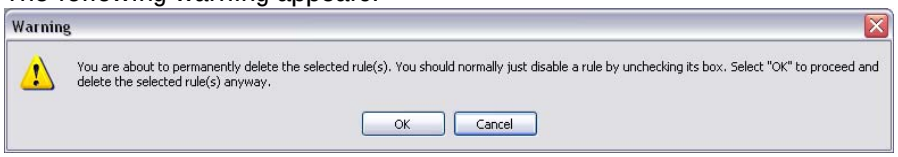
To delete a trusted process:

1 Click the **Process Lists** tab.

2 Highlight the process.

3 Click the **Delete** button.

The following warning appears:



Take Note

A profile is the set of rules configured on a given computer.

4 Click **OK** if you wish to continue or **Cancel** to cancel.

5 Click **Apply** at the bottom of the **Process Lists** tab to finalize any changes.

Selecting and Deselecting All Trusted Processes

- Click **Check All** to select all Trusted Processes and **Uncheck All** to deselect all trusted processes.
- Click **Apply** at the bottom of the **Process Lists** tab to finalize any changes.

The Rule Wizard — Source

Remember, the first item in the Rule Wizard used to construct rules (see Using the Rule Wizard on p. 37) is Source. Rule Wizard – Source has four selections:

- Any process
- Any non-interactive process
- Any email or browser process
- Any process list

The third choice is for any email or browser process, and the sources for that choice are listed in the **Email and Browsers** list on the **Process Lists** tab.

Email and Browsers List

At the bottom half of the **Process Lists** tab is the **Email and Browsers** list.

Here you would include any email and browser rule sources so that when the rule fires it is caused by one of the email programs or browsers in this list taking an action with certain options and exclusions. The action is determined by you, the user, when you respond to the choices in the dialog box that appears when a rule triggers.

The email programs or web browser that is the rule source when the rule fires are the ones included in the **Email and Browser** list.

Email and Browsers List Buttons

To the right of the **Email and Browsers** list are the following buttons:

Use these to add new email programs and browsers to the list, to delete them, and to select and deselect all email programs and browsers.

Adding a New Email Program or Browser

You can add a new email program or browser as a source to custom rules.

This action is taken for the email program and browsers specified on the **Process Lists** tab.

To add a new email program or web browser:

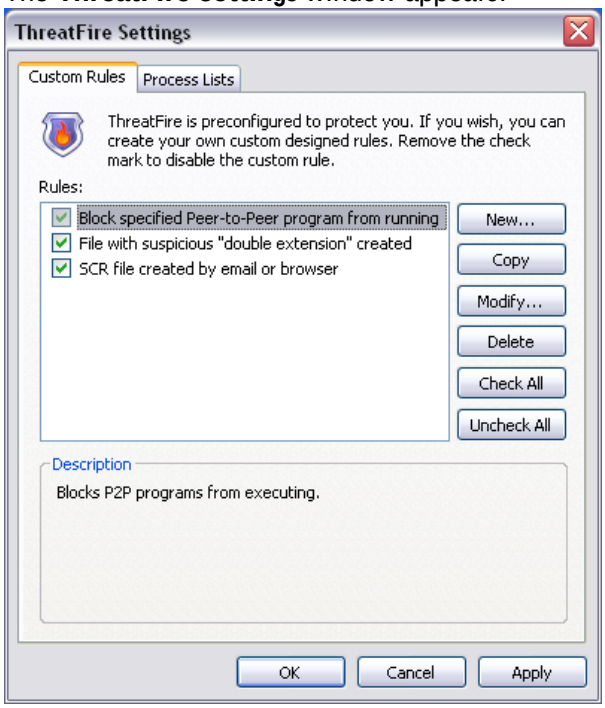
1. Select **Start/All Programs/ThreatFire/ThreatFire**.
   Or

   Right-click the **ThreatFire** icon in the system tray:
   The choices are **ThreatFire, Quick Start Guide, Suspend** and **Status**.

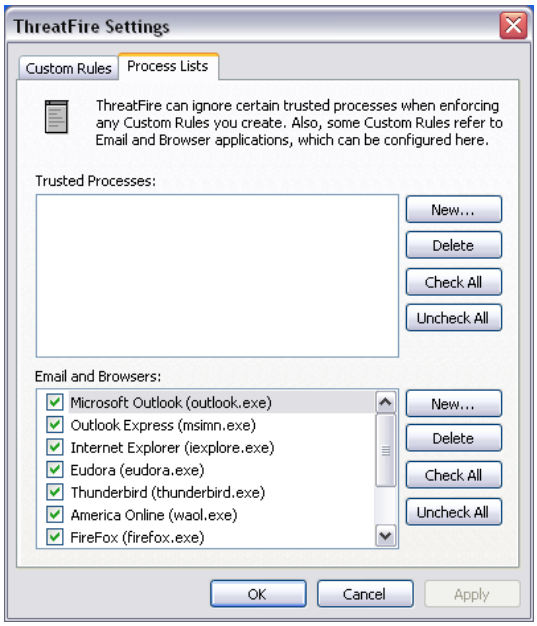
   Click **ThreatFire**.

2. The **ThreatFire** window appears.
3. Select the **Advanced Rules** option on the left side of the pane.
4. Click the **Custom Rules Settings** button on the right side of the pane.

   The **ThreatFire Settings** window appears:



5 Click the **Process Lists** tab.

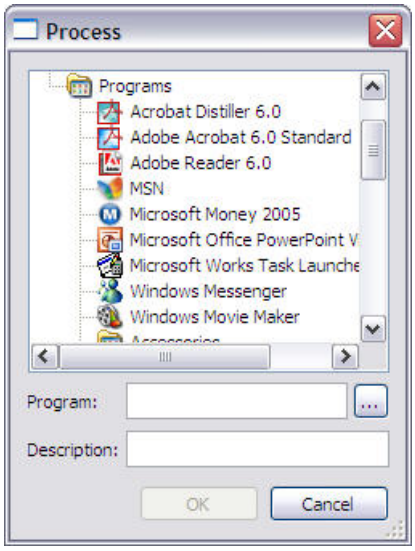


6 Click the **New** button.

Take Note

The **New** button does not bring up a custom rule; it brings up a dialog box that allows you to add processes that will be the sources when one of those rules fire.

7 The **Process** dialog box appears:



8 Highlight the program from the tree or use the ellipse to browse to the selected program.

9 Click **OK** to continue or **Cancel** to cancel.

The process is added to the **Email and Browsers** list.

10 Click **Apply** at the bottom of the **Process Lists** tab to finalize any additions.

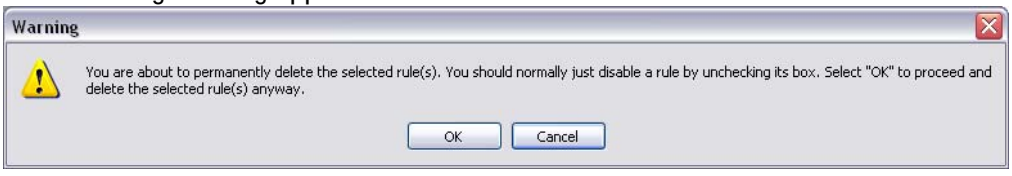
Deleting an Email Program or Browser

To delete an email program or browser:

Click the **Process Lists** tab.
Highlight the process.

Click the **Delete** button.

The following warning appears:



A profile is the set of rules configured on a given computer.

Click **OK** if you wish to continue or **Cancel** to cancel.

Click **Apply** at the bottom of the **Process Lists** tab to finalize any changes.

Selecting and Deselecting All Email Programs or Browsers

- Click **Check All** to select all Trusted Processes and **Uncheck All** to deselect all email programs or browsers
- Click **Apply** at the bottom of the **Process Lists** tab to finalize any changes.

System Activity Monitor

The **System Activity Monitor** displays detailed information on all running processes on your PC.

The processes are categorized in like groups on the left side of the display: **Applications, Other** (the category most likely to display any malware that may be running on your system)**, Autoruns, System, Services** and **Protected.**

The various categories can be collapsed or expanded by clicking the plus sign **+** next to each category name.

Under each category you will see a list of all running processes in that category. You may click on each individual process to display information about that process in the right-hand pane. In the following image ThreatFire's tray process is highlighted on the left with detailed information about it displayed on the right:

The categories of data presented in the right-hand pane may include any of the following based on the particular process being viewed: **Process Data, Properties, Program Windows, Network Actions, File Actions, Registry Actions, Program Actions** and number of **Modules.**

Advanced Tools

Right-clicking a process name on the left brings up a context menu with the following options:

Get information on [process name]
Kill [process name]

If you select **Get information on** [process name] then your browser will be launched and a web search on the process name will be performed.

If you select **Kill** [process name], then the process in question will be immediately terminated.

Please exercise caution when killing a process as any associated programs will also be closed and you may lose any unsaved data.

Settings

The **Settings** button is the 5th down the left on the main ThreatFire control panel. It has 3 tabs across the top: **General, Quarantine,** and **Scheduled Scan.**

General Settings

The items in the **General Settings** tab are:

ThreatFire Protection:

- Ensures that ThreatFire can actively monitor your computer for signs of suspicious behavior and potential attacks.

Protection Level:

- Slider setting allows you to adjust ThreatFire to your preferred level of protection. There are five available levels, with Level 3 being the default:

- Level 1-- Alerts only when a known threat is detected, so unknown suspicious activity is ignored. This level will display the fewest alerts.
- Level 2-- Alerts when a known threat is detected and for *most* unknown threats.
- **Level 3-- Recommended level.** Alerts for known threats, known PUAs and for any unknown threats. This is the default level and provides the widest range of protection with the most intelligence. While there may be some "false positives" (alerts on non-malware) at this level, ThreatFire's built-in intelligence keeps these to a minimum.
- Level 4-- Alerts on most suspicious actions, for all but the most trusted processes.
- Level 5-- Alerts on any suspicious action. This level will display the most alerts. In addition to actual malware alerts, you will see alerts on known safe programs that are exhibiting some suspicious behavior.

Default Actions:

- Allows you to set default actions for the three main ThreatFire alerts—the "yellow" potentially malicious alert, the "gray" potentially unwanted grayware alert and the "red" known malware alert.

- Choose **Prompt Me, Allow** or **Quarantine** when a suspected threat is detected. A suspected threat is one that unknown in nature and is potentially malicious. You would normally see the "yellow" ThreatFire alert dialog in these cases. The default selection is **Prompt Me.** If you choose **Allow** or **Quarantine** then no alert will be displayed. The selected action will happen automatically and the only record you will see will be in ThreatFire's Threat Control center logs—either **Quarantine** or **Protection Log.**
- Choose **Prompt Me, Allow** or **Quarantine** when a potentially unwanted threat is detected. A potentially unwanted threat may include adware or some system tools used in malware distribution. You would normally see

the "gray" alert, indicating "grayware," in these cases. The default selection is **Prompt Me.** If you choose **Allow** or **Quarantine** then no alert will be displayed. The selected action will happen automatically and the only record you will see will be in ThreatFire's Threat Control center logs—either **Quarantine** or **Protection Log.**

- Choose **Quarantine and Alert Me** or **Quarantine** for known malicious threats. These known threats would typically display the "red" ThreatFire alert. The default selection is **Quarantine and Alert Me** which will display ThreatFire's "red" alert. If you elect to automatically quarantine any detected threats, then you will not see this alert and instead you'll only see the details of the event in ThreatFire's **Quarantine** area.

- Setting alert actions to automatically **Quarantine** any threats can be helpful for those users wishing to run ThreatFire in a "silent" mode where no user interaction is required.

Important: Please use extreme caution when changing the default actions. If you elect to automatically allow all suspected or known threats then your overall protection will be greatly reduced and you may run the risk of infecting your PC.

Likewise, if you automatically quarantine all suspected threats (yellow alerts) there is a possibility that legitimate programs may be affected (false positives). If you run into any such cases, you may always **Restore** a program from ThreatFire's **Quarantine** area.

These default alert actions only apply to ThreatFire's regular program alerts. Alerts for any custom rules you create through **Advanced Tools** will always prompt you to select the appropriate action.

Settings

Check for Updates:

- Automatically checks for program updates available for download on the PC Tools servers.

Community Protection:

- Automatically reports to PC Tools information about the event when a suspect rule is triggered by ThreatFire. Participating in the Secure Community is win-win: you help identify new threats and provide better protection to all other ThreatFire users, and in turn, other members do the same for you.

In ThreatFire Free Edition, if Community Protection is ever set to Off, the Check for Updates option is automatically set to Off as well and cannot be turned back on until Community Protection is turned back on.

ThreatFire Pro does not have this restriction and allows you to turn off Community Protection without also having to turn off Check for Updates.

Settings

Please note: if you disable Community Protection then ALL internet communication on ThreatFire's part will be disabled. This can affect other areas of the program including program notices and receiving updated Worldwide Detection data for the list of threats and the map on ThreatFire's Security Status tab. If you do turn Community Protection OFF, then you will only see a cached version (or older data, in other words) of this report.

Program Language:

- Use the drop down selection box to set the program language. Click **Apply** to finalize any changes.

Notices:

- Check or uncheck the boxes to tell ThreatFire whether to display various program notices and information.

Quarantine Settings

If you are using Windows XP or later, you can tell ThreatFire to automatically set a System Restore Point before performing any quarantine action. While it is very rare that there would be any problems during quarantine, having a system restore point to revert back to is just an added safety measure to make it easy to recover from any potential problem.

To set this option, simply check the checkbox to **Set System Restore Point**. Should you decide you wish to stop setting restore points, simply uncheck the same box.

Scheduled Scan Settings

We recommend that you scan for rootkits and other threats at least once a week. Under the **Scheduled Scan** settings tab you can configure ThreatFire to conduct either a Quick Scan or Full Scan automatically for you at the time and frequency of your choice.

To schedule an automatic scan:

1. Select **Start/All Programs/ThreatFire/ThreatFire**.
   Or
   Right-click the **ThreatFire** icon in the system tray:
   The choices are **ThreatFire, Quick Start Guide, Suspend** and **Status**.
   Click **ThreatFire.**

2 The **ThreatFire** window appears.

3 Select the **Settings** button on the left side of the pane.

4 Click the **Scheduled Scan** tab on the right side of the pane.

The **Scheduled Scan Settings** window appears:

5 Check the **Run a scheduled scan** box to indicate that you wish to turn on and run automatic scans.

Use the **Time, Repeat,** and **Type** dropdown boxes to choose the scan's start time, repeat frequency and type.

Take Note

In ThreatFire Free Edition **Scan for** is automatically set to **Rootkits.**

In ThreatFire Pro you have the option to scan for **Rootkits, Viruses** or **Both.**

6 Click **OK** to confirm your scan settings.

Click **Cancel** to cancel your dropdown box selections.

Take Note

You must click **OK** to confirm that you wish to run an automatic scan with the specified scan choices.

Settings

Important: Please note that if any items are detected during an automatic scan, a message will be displayed instructing you on how to proceed. You may be asked you to run a manual scan to address any remaining threats.

Conclusion

Protecting You When Traditional Antivirus Can't

A "Zero-Day" attack occurs when your computer is infected by a Zero-Day threat – a virus, trojan or spyware which is so new that traditional antivirus programs have no "signature" to identify the threat.

Because Zero-Day attacks happen faster than traditional antivirus can react. Here is what your traditional signature-based antivirus product must do to protect you against any new threat:

1) Catch the threat.
2) Analyze the threat to understand what it does
3) Write a signature that recognizes the threat.
4) Test the signature to ensure it does not damage your computer.
5) Issue you an update with the new signature. And then…
6) *You* still have to update your software with the new signature!

It can be days before traditional antivirus companies provide the "signature update" necessary to protect your computer. And traditional signatures cannot protect you if a threat "morphs" to evade the signature.

ThreatFire does not rely on signatures in order to protect you. Its patent-pending ActiveDefense technology is the most intelligent behavioral analysis technology available today. It continuously monitors all activities on your PC at a very low system level and uses a proprietary combination of analytics, risk algorithms, program histories and tolerance thresholds to identify and shut down threats.

When ThreatFire detects an attack on your computer by a known virus, it will immediately terminate the attack and permanently isolate the virus process. An alert screen will appear to confirm that ThreatFire has prevented the attack.

If ThreatFire detects a "potentially malicious process" that *might* be a virus attack, it will immediately suspend the suspicious process and alert you that your computer is at risk. You can then choose to "Allow" or "Deny" the process based on the informative information provided in the alert.

In other words: you're fully protected, and can proceed without worry of infection!

Where to Look for Further Help

For further technical assistance, you can go to the ThreatFire Support Site and Knowledge Base at www.threatfire.com/support.

Please also view the ThreatFire Tutorial online at www.threatfire.com/tutorial.

Glossary

Background	Computers are capable of executing several tasks, or programs, at the same time. The foreground process is the one that accepts input from the keyboard, mouse, or other input device. Background processes, on the other hand, do not accept interactive input from a user, but can access data stored on a disk and write data to the video display. Spyware can run as a task in the background so that the user may not even know it is running.
Browser Helper Object (BHO)	A Browser Helper Object, or BHO, is a small program that runs automatically every time the user starts their Internet browser. Developers typically use BHOs to customize and control Internet Explorer; however, they can be used maliciously since they do not require a user interface. It is possible that the user is unaware of Browser Helper Objects installed on their systems. BHO's can be used for malware like spyware that gathers information on user surfing habits.
COM File	In MS-DOS, a COM file is a simple type of executable file.
Control Panel Applet	Mini application (applet) programs for changing the system environment or settings you use in Window's Control Panel.
Control Panel	Access by clicking Start/Control Panel. This program permits you manage many parts of your computer by allowing you to install or uninstall program, configure network connections, modify mouse sensitivity and system sounds, and perform many other functions.

Glossary

ThreatFire Secure Community	The ThreatFire Secure Community is a worldwide network of active users who volunteer to aid in identifying new threats. Any time a suspect alert is triggered in ThreatFire, information related to this event is automatically reported to PC Tools for analysis through a secure connection. Any information collected is held completely confidential and is used solely for the purposes of researching new or previously unknown threats, gaining an understanding of their behaviors, and developing new protection against them. Information collected may include the ThreatFire alert that fired, the history of relevant events leading to that alert, the decision taken, and any relevant IP address information. This immediate confidential feedback on potentially dangerous new threats allows PC Tools to advance its ActiveDefense technology to block these threats. So as threat strategies evolve and new security penetration tactics emerge, ThreatFire technology will remain at the forefront of the solutions that defeat those threats.
Disk Operating System (DOS)	An operating system that resides on a disk.
Dynamic Link Library (DLL)	A dynamic link library (DLL) is a collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL file. These files can be malicious because they can run just like an application.
Executable	An executable is a file that runs a program, or a particular kind of file that is capable of being executed or run as a program in the computer.
Extension	A file's extension describes the format as part of its name; for example, "file.doc". The file name extension helps an application program recognize whether a file is a type that it can work with and a user to recognize the type of file it is; in this case, a Word document.
File Transfer Protocol (FTP)	File Transfer Protocol (FTP) is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol.
Foreground Process	A foreground process is one that accepts input from the keyboard, mouse, or other input device.

Glossary

Host File	A host file, stored on the computer's file system, is used to look up the Internet Protocol address of a device connected to a computer network. The hosts file can also be used in malicious ways by the authors of Spyware and Viruses, where popular websites are redirected to an advertiser's server.
Layered Service Provider (LSP)	A Layered Service Provider, or LSP, is a piece of software intertwined with the networking services of a computer. When using the protocol of the internet, TCP/IP, the LSP combines itself with the TCP/IP layer of your network. As such, the LSP has access to all TCP/IP traffic coming into and leaving a computer. Spyware authors can use an LSP to spy on the habits and data of the user.
Multi-Purpose Internet Mail Extensions (MIME)	MIME (Multi-Purpose Internet Mail Extensions) is an extension of the original Internet e-mail protocol, the Simple Mail Transport Protocol (SMTP), which handles ASCII text. MIME gives users access to the protocol to exchange different kinds of data files on the Internet: audio, video, images, application programs, and other kinds, including ASCII text.
Process	A process is an instance of a program running in a computer.
Program Information File (PIF File)	A Program Information File, or PIF, is a file type that holds information about how Windows should run a non-Windows application. These instructions can include the amount of memory to use, the path to the executable file, and what type of window to use. PIF files have a .pif extension.
Registry	A collection of settings stored on the hard disk that determine how Windows appears and how it behaves, and controls applications running on the computer.
Simple Mail Transport Protocol (SMTP)	SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.
Spoofing	E-mail spoofing is the forgery of an e-mail header so that the message appears to come from someone or somewhere other than the actual source.
Transmission Control Protocol (TCP)	A communication protocol used for the exchange of information over the Internet.

Glossary

Trojan	A Trojan is a program in which malicious or harmful code is contained inside an apparently harmless file, and when executed it can get control of and damage a computer.
Trusted Processes	Trusted processes are applications that can see all protected objects; nothing is hidden from trusted processes. Users can set up certain applications as trusted processes, such as anti-virus software that needs to check protected files for computer viruses.
Uniform Resource Locator (URL)	A URL is the unique address for a file that is accessible on the Internet.
Winlogon Shell	The interactive user interface with an operating system, in this case Windows. The shell is the layer of programming that understands and executes the commands a user enters. The process "winlogon.exe" runs in the background and is a part of the Windows Login subsystem.

Index

Glossary