



ParetoLogic Anti-Spyware

Security and Protection in Real-Time

Product White Paper
Aug 29, 2006



ParetoLogic Anti-Spyware

ParetoLogic Anti-Spyware offers an advanced set of tools designed to protect your computer from spyware threats.

There are two lines of defense:

Scanning and Removal

The technology behind the scan and removal process involves the use of a powerful database of known spyware items. There are frequent database updates that are free and fast. With these updates your computer is safe from the most current spyware threats. You also have several methods of scanning to choose from including automatic scans.

Active Protection

To prevent unwanted items infecting your computer, ParetoLogic Anti-Spyware provides Active Protection. Now you can monitor Internet and system activity whenever you use your computer.

To get a free scan, check out: www.paretologic.com.

ParetoLogic – The Company

ParetoLogic is an international software development company headquartered in Victoria, British Columbia, Canada. We are a member of SIIA (Software Information Industry Association) and we specialize in providing advanced security applications for enterprise, business, and personal computer users. These include custom software solutions for business and government.

Our proprietary Zheng™ technology transcends the traditional approach to online research. Offering a robust set of fully customizable, scalable, information gathering, and dissemination tools, this technology provides advanced spyware identification that drives the ever-increasing size and accuracy of our spyware database.

ParetoLogic's commitment to best-of-breed software is matched by our pledge to 100% customer satisfaction. No matter where you are in the world, our dedicated support team will respond to your questions with comprehensive technical support and troubleshooting. ParetoLogic prides itself on timely resolutions to ensure minimal downtime for our customers.



Addressed in this Product White Paper

This document provides information and recommendations related to using ParetoLogic Anti-Spyware. It is not meant for instructional purposes. We recommend using the help file that comes with the application for detailed steps and instructions.

The following topics are covered in this document:

Spyware Information	3
Protection Information	5
Scanning	5
Active Protection	8
Cycle Detection	11
Safety and Peace Of Mind	12

Spyware Information

Spyware can infect home and business computers without your knowledge simply by surfing the Internet or sharing files. Difficult to find and hard to remove, spyware can steal confidential information resulting in identity theft and credit card fraud. There are many other harmful effects to your computer system as listed and described in this section.

The term "malware", derived from the words: "malicious" and "software", is also used to describe these computer threats. Examples of common malware threats and the resulting symptoms and characteristics can be seen in the following table.

Type	Description
Popup ads	Displays advertisements in an intrusive manner
Keyloggers	Records your personal data
Browser hijackers	Changes your web browser settings
Remote influence	Influences or controls your computer remotely
Unsolicited files	Makes attempts to download and install files on your computer
Shutdown or disable	Disables programs or processes on your computer



Unauthorized phone calls	Makes calls via the phone modem
Security flaw exploits	Takes advantage of system or network flaws for remote access
Internet connection floods	Interrupts or temporarily disables an Internet connection
Threat proliferation	Spreads quickly and easily from computer to computer
Tracking	Tracks your Internet activity and can send this information remotely
Installation	Installs on your machine without your consent
Uninstallation	Makes uninstalling and removing the item difficult
Privacy and Consent	Fails to properly disclose potential privacy risks

Table 1: Types of Spyware

Harmful Effects

Along with fraudulent, unethical, and illegal activities, as described above, there are other common effects that are a result of malware activities. These can include reoccurring system errors and program failure. In many cases, spyware programs hog system resources and monopolize processing time. Results can include poor computer performance, system non-responsiveness, unexpected behaviour and program termination.

For a more complete description of spyware characteristics we recommend you follow this link: <http://www.paretologic.com/resources/characteristics.aspx>

Solution

ParetoLogic Anti-Spyware provides safeguards and protective functionality to ensure that your computer system is secure. Not only can you perform thorough scans and remove malicious files from your computer system, you can also proactively block any potential threats.

ParetoLogic Anti-Spyware puts you in control. When performing a scan, you can choose to not remove detected items or you can select these items so that they are ignored when performing upcoming scans. When an alert notice appears, you can block the item that has been detected or choose to allow it. The following sections describe this functionality.



Protection Information

The Home page is the page that is first displayed when you open the program. It contains useful information about your Active Protection level and it also provides you with the option to begin a Quick scan or a Full scan. The following table identifies these categories and describes the kind of invalid entries contained within.

State	Description
Green (protected)	Your computer is currently protected.
Yellow (caution)	You have never done a scan, or... Active Protection is set very low. At this level, it is recommended that you raise the level of spyware protection.
Red (warning)	There are items that have been scanned and detected but not removed from your system, or... Active Protection has been turned off.

Table 2: Home Page - Protection States

With an understanding of where your protection level is set, you can take action by performing a scan or raising the Active Protection level.

Scanning

ParetoLogic Anti-Spyware provides an easy and fast scanning procedure. During the scan you can review the progress that is displayed or you can minimize the application so that it runs in the background. After the scan is complete the list of errors is displayed as can be seen in Figure 1.



ParetoLogic Anti-Spyware

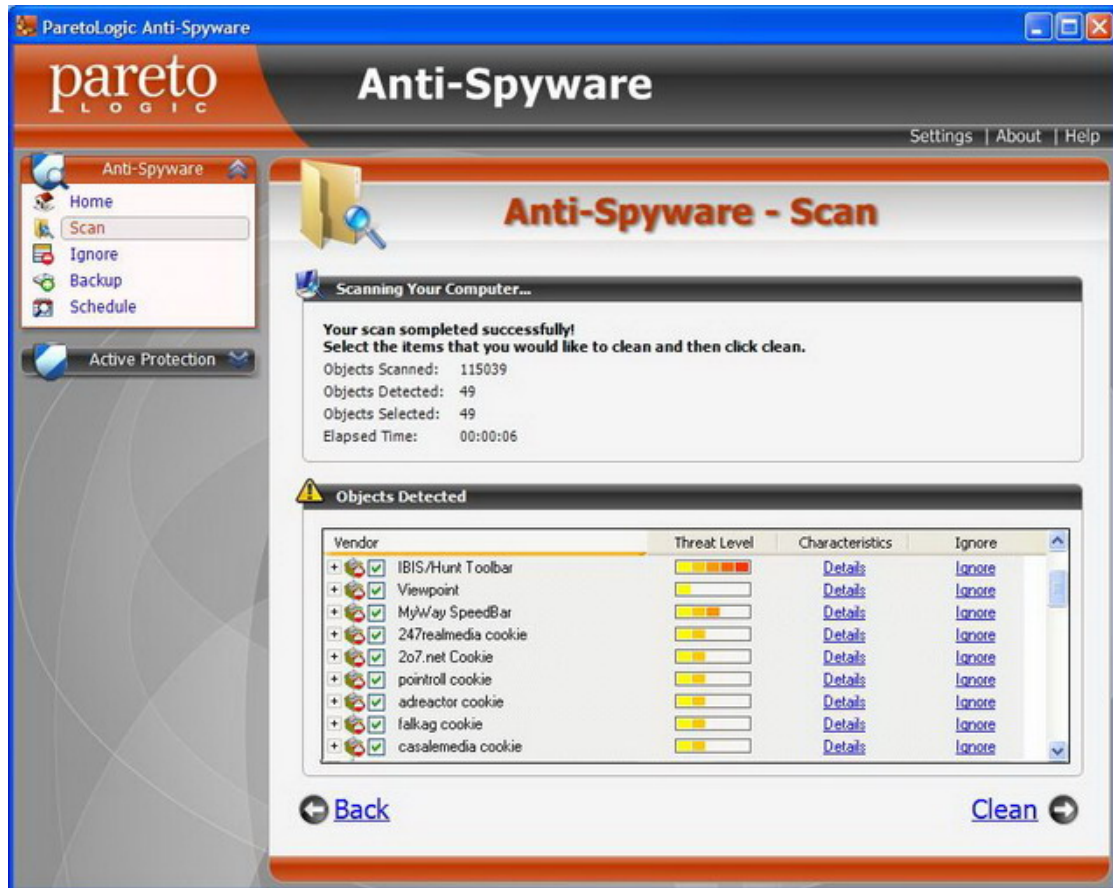


Figure 1: Scan Results

Although you may have used a number of scanning tools in the past, in most cases the first ParetoLogic Anti-Spyware scan you perform will detect numerous items. In these situations, other scanning tools are not detecting all the spyware threats that are on your computer system. ParetoLogic Anti-Spyware takes advantage of a spyware definition database that is powered by proprietary technology and dedicated service. The ParetoLogic definition database is also one of the largest in the industry.

The database consists of spyware definitions that are current. ParetoLogic is committed to accurately identifying new spyware threats by adding new spyware entries in the database on a daily basis. Frequent database updates are then sent to your computer as part of the dedicated security service. An Internet connection is required to receive updates.



Removal of Detected Items

By default, all the detected items are selected for removal. You can view these items and the location of each, you can modify which of these are selected, you can send items to the Ignore list, or you can remove them with the knowledge that you have backup capabilities. To assist you in deciding what items to remove, ParetoLogic Anti-Spyware displays information related to each detected item including the threat level.

Scheduling Scans

ParetoLogic Anti-Spyware comes equipped with scheduling functionality so that your computer is scanned automatically on a regular basis. You can set up one or more schedules to automate the scanning process. When complete, the results are displayed for you and you can decide on what action to take.

Ignore List

After a scan you can add detected items to the Ignore list. In these instances, ParetoLogic Anti-Spyware does not remove the item and it will be ignored during upcoming scans. By clicking the Ignore link, as seen in Figure 2, you are sending the item to the Ignore list.

Vendor	Threat Level	Characteristics	Ignore
<input type="checkbox"/> IBIS/Hunt Toolbar		Details	Ignore
<input type="checkbox"/> Registry Values			
<input type="checkbox"/> software\microsoft\windows\currentversion\sharedlls\C:\WINDOWS\downloaded program files\qdown_as2.dll			

Figure 2: Details of Invalid Entries

If you decide you want to scan and remove the item at a later time you can do so by going directly to the Ignore list. ParetoLogic Anti-Spyware offers the ability to view and manage the list of ignored items.

Backup and Restore

With ParetoLogic Anti-Spyware you can easily restore items that were removed during the scan and removal stage. Every time you remove detected items a backup file is created. ParetoLogic Anti-Spyware saves these backups so that deleted items that were removed can be restored. There is also an option to restore one or more backup files at a time.



Active Protection

Active Protection is designed to detect and block spyware attacks and threats as they happen in real-time. ParetoLogic Anti-Spyware uses monitors that are designed to stay on the alert for any malware intruders. It provides you with the highest level of protection while being as un-obtrusive as possible. You can set the security level of the monitors to determine what actions Active Protection will take when intercepting a threat or detecting a change.

Monitors

The monitors are at the heart of the Active Protection technology. These components are designed to detect particular system changes. There are seven monitors that can be classified in two main categories: Internet and Windows.

Active Protection monitors watch file system, registry, and process components. In determining a suitable protection level, it is useful to know something about what is being monitored. Monitored item information is provided in the following table.

Type	Description
Internet Monitors	Web browsers are a popular target for malware as they are usually the most popular point of interaction between a user and the World Wide Web. This interaction is crucial as it provides the makers of malware a chance to gain revenue. Browsers are highly configurable and offer a large range of options which provides malware with many target areas. For example, Internet Explorer allows customization of security settings for individual web sites through their use of security zones. Some malware add their parent web sites to the trusted zone thereby allowing the web sites to install malicious components.
Browser Hijack	A common action that malware takes is to change the browser home and search pages to point to a malicious web site. The Browser Hijack monitor watches your web browser settings to prevent hijacking of your home page and other settings.
Browser Helper Object	Internet Explorer (IE) allows application developers to extend the IE interface almost indefinitely through toolbars, ActiveX, menu items, modification of favorites, and generic add-ins called browser helper objects. These items are monitored through registry entries.
Browser Modification	This monitor checks for any modification to your web browser menus, toolbars, and other settings.
Network	Malware can employ numerous methods to change network



	related settings. Some examples are: Windows Messenger service, dialup connections, DNS entries, hosts file, LSPs, bad web sites, and protocols.
Windows Monitors	There are a plethora of attack points for malware. The monitors for the Windows category includes: Startup and Shell.
Startup	The Startup category contains methods by which executables can ensure that they will run after a reboot. Malware needs to execute after a reboot to function successfully and Windows provides many different mechanisms to accomplish just this. These mechanisms include, but are not limited to: registry locations, folders, initialization/batch files, services, and the task scheduler.
Shell	The Shell contains many different points of attack and is a prime area of interest for monitoring malware attacks. It includes: certificates, key logging, hidden processes, running processes, and alternate data streams.

Table 3: Monitored Items

At the right protection level, Active Protection is designed so that the monitor can detect a threat and, if it is an unknown threat, the monitor presents an alert to get input from you as to what action to take.

Alert Notification

You can receive alerts when Active Protection detects a potential threat or a change in one of the areas it monitors. Alert notification can be set at a level that you choose so as to be working on an automated level or to be working at a high alert level.

The Alert window includes:

- The name of the monitor that detected the malware threat or the event change.
- A description of the threat and what was detected.
- Buttons to determine what actions you would like Active Protection to take (for Full Protection only).



The alert popup notice appears as follows:



Figure 3: Alert Notification

In some situations, you could receive repetitive alerts even though you are choosing to block an item. In such cases, Cycle Detection is activated in order to end the loop and provide a solution. See Cycle Detection on page 11.

Custom or Predefined Levels

Active Protection settings can be instance specific (custom) or generic (predefined). With instance specific settings you can set any monitor at a level separate from the other monitors. In this way, the monitor will act to block, allow, or log the detected item or event. For example, you could set your Network monitor to “Log Only” and have the Windows Shell monitor set at “High” so that you can intercept any potential malware from hijacking your computer.

There are several levels available for you to choose from so that you can decide to be given notification of all Active Protection activities (the highest level of protection) or you can simply review the logs that are created to examine detected items and changed events.



The following table identifies the levels of protection that are available.

Level:	Alert:	Log:	Action:
Full	Yes	No	<ul style="list-style-type: none">- Alerts you to any unknown changes.*- Blocks all known malware.
Medium	No	Yes	<ul style="list-style-type: none">- Logs any unknown changes.- Blocks all known malware.
Low	Yes	Yes	<ul style="list-style-type: none">- Logs any unknown changes.- Alerts you to any known malware.
Log-Only	No	Yes	<ul style="list-style-type: none">- Logs all known and unknown changes.
Off	No	No	<ul style="list-style-type: none">- Ignores all changes.- Active Protection is off.

Table 4: Protection Level

* The term “changes” refers to any detected modifications made in an area that Active Protection is monitoring. The terms “known” and “unknown” are based on comparisons of the change with all entries in the ParetoLogic spyware database. For more information about the database see page 6.

Cycle Detection

ParetoLogic Anti-Spyware is the first to offer Cycle Detection – the ability to detect when a loop occurs. An alert loop can occur when you have selected to block a detected threat but a new notice continues to appear for the same item. In these cases it is likely that the malware item is able to recreate itself.

Spyware is blocked automatically depending on your Protection level or when you choose to block it after a popup alert appears. In certain instances the detected item is blocked but, due to its malicious design, it is still able to write a new entry to the computer registry causing another popup alert to be displayed. This pattern will repeat until a Cycle Detection alert appears.

The Cycle Detection alert is similar to the alert notice that can be seen in Figure 3. However, the option to block the item is disabled in order to stop the reoccurring loop. The alert warns you that your system may be infected with malware and you should run a scan to remove it.



Safety and Peace of Mind

Dealing with computer performance and security issues is of prime importance from a business, financial, and personal home-use perspective. Being exposed to spyware threats can result in hardships, frustration, loss of time, and even loss of personal information. At ParetoLogic we make your safety a priority.

Having the necessary equipment to provide a safe and reliable computing experience is essential. ParetoLogic Anti-Spyware is designed to be fast and it offers a friendly, easy-to-use interface with a step-by-step process that puts you in control. Once you have the confidence of a secure computing environment, you can automate the process and have your system running at optimal levels of performance. ParetoLogic Anti-Spyware is a dedicated software solution that provides security and protection and gives you peace of mind.

All information contained in this document is the proprietary information of ParetoLogic Inc. and is protected by international copyright treaties. This document contains information that is privileged and confidential. Any disclosure, distribution or copying of this document without the prior written consent of ParetoLogic is strictly prohibited under applicable law. ParetoLogic and ParetoLogic Anti-Spyware are registered trademarks or trademarks of ParetoLogic Inc. in Canada, the United States, and in other countries. All other trademarks are the property of their respective owners.

Copyright © 2006 ParetoLogic Inc. All rights reserved.