



[Astaro Firewall](#)

**astaro**  
internet security

Network Security Whitepaper

**Complete Spyware protection:  
Blocking Incoming and outgoing  
Spyware Traffic at the Gateway**

Version: 1.00

Release date: March 2005

Author: Gert Hansen Chief Software Architect

## Table of Contents

<b>INTRODUCTION</b> .....	<b>3</b>
<b>WHAT IS SPYWARE?</b> .....	<b>3</b>
Definition.....	3
<b>HOW ARE SPYWARE THREATS HANDLED?</b> .....	<b>4</b>
<b>ASTARO'S GATEWAY SOLUTION TO TREAT SPYWARE</b> .....	<b>5</b>
<b>IDENTIFYING MALICIOUS URLS</b> .....	<b>5</b>
<b>BLOCK SPYWARE INFECTION AND COMMUNICATION</b> .....	<b>6</b>
<b>BLOCK SPYWARE INSTALLATION</b> .....	<b>7</b>
<b>MANAGING SPYWARE PROTECTION</b> .....	<b>7</b>
<b>CONCLUSION</b> .....	<b>7</b>

## Introduction

Spyware is a growing threat to privacy, security and productivity. One recent study<sup>1</sup> found 80% of surveyed computers infected, with an average of 93 spyware and adware components on each infected system. Desktop anti-spyware products help address the problem, but they are difficult to manage since every client needs to be kept up to date separately, and even with their use it may take hours to disinfect a single PC. It is also common sense that spyware won't go away. Like spam email it is a moneymaking revenue source and not just a malicious hacking challenge for programmers.

## What is Spyware?

### *Definition*

Strictly speaking, spyware is software that gathers information about a computer user and his or her Web surfing habits without the user's explicit knowledge or consent and report this information to the Internet. The term spyware also subsumes adware, malware, and other applications of that kind threatening a user's system.

Spyware is harmful to the user for many reasons:

- Decreased productivity, as PC users are constantly interrupted and spend time closing pop-ups and other ads.
- Information/data leakage and violations of privacy (a worst case scenario would be a tool recording every key stroke, eventually culminating in password cracking)
- Decreased system performance (particularly on older PCs with limited amounts of memory)
- Increase demands on help desks, as users and help desk staffs spend hours trying to remove spyware from infected systems.

A typical piece of spyware installs itself in such a way that it automatically starts up every time the computer is booted. It then runs at all times, monitors Internet usage and – in case of adware - delivers targeted advertising to the affected system. Spyware generally does not damage the user's data files; indeed, the overwhelming majority of the harm inflicted by spyware comes about simply as an unintended by-product of the data-gathering or other primary purpose. Spyware normally installs itself through one of the following methods:

- A hidden spyware component comes bundled with an otherwise apparently useful program. For instance, granting permission for web-based applications to integrate into one's system can also load spyware, e.g. certain toolbars.

---

<sup>1</sup> **AOL/NCSA Online Safety Study**, Conducted by America Online and the National Cyber Security Alliance, **October 2004**

- Unnoticed installation on a computer on the fly via a so-called *drive-by download* without prompting the user. Among those drive-by installations are often so-called browser helper objects which embed themselves as part of a Web browser, recording the user's surfing behavior in order to display user specific advertising or to collect search terms entered by the user.
- HTTP cookies for user tracking purposes. A cookie, a well-known mechanism for storing information about Internet users on their own computers, can often be used to track individual Web surfing habits not only for a particular website but for all websites a user had visited over a period of time. This can be a violation of privacy if a company is tracking surfing behaviour across multiple Web sites. A related technique is so-called Web bugs (also known as tracking bugs, pixel tags, web beacons or clear GIFs) that determine who viewed an HTML-based email message or a Web page, when they did so, how many times, and how long they kept the message open

Spyware cannot be blocked by personal firewalls, because it looks like regular Internet traffic.

## How are Spyware threats handled?

As of today the most common way to detect and disable spyware on personal computers is a client based approach. This client-side approach makes use of specially designed software which is installed on the client providing the following spyware protection measures:

- Monitoring certain aspects of the system such as browser helper objects
- Monitoring the registry
- Monitoring the host file
- Monitoring changes of the system caused by spyware, for instance, if a program has copied itself into the autostart folder, etc.

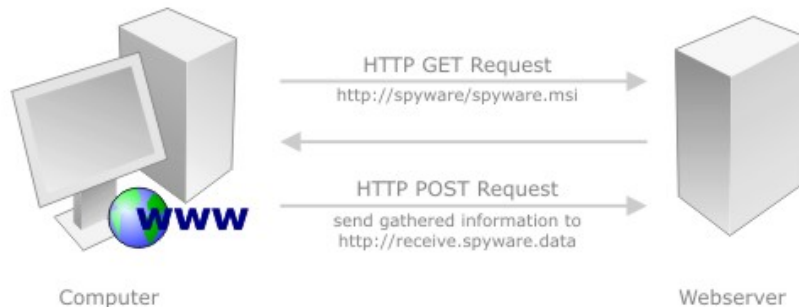
These mechanisms are useful to detect spyware on a desktop computer, however, one important drawback of this approach is that you don't have full spyware protection but rather an (immediate) de-installation of spyware that had already made its way to the system. Therefore, the quality of the spyware detection software determines if and how quickly already installed spyware will be removed from the system.

Furthermore, a client side approach may be appropriate for single home users who have the time to administrate their PCs but it is not appropriate for small, medium sized businesses or large enterprises as it is almost impossible for any administrator to check and maintain every single client. Even with automatic update features similar to those used by anti-virus software it requires every single user to make sure that his PC is protected properly, i.e. protection SW is activated and updated on a regular basis.

Thus, the most economic and secure way to deploy and manage Anti-Spyware solutions is to place appropriate Spyware protection functionality into a perimeter device, which inspects all traffic that is exchanged between the enterprise network and the Internet.

But, regardless of where Anti-Spyware solutions are positioned in order to get full spyware protection, you need to make sure that systems are not getting infected in the first place and already infected system are not allowed to send any tracking information out to the Internet.

Every spyware uses Web traffic communication, i.e. the HTTP protocol, to either infect a system or to send data back to the Internet. Therefore, in order to protect a system from spyware, every HTTP request to the Internet must be checked if



potential spyware is downloaded. On the other hand, an infected system also makes use of the HTTP protocol to deliver its gathered user information back to the Internet. For that reason the key to any complete spyware protection solution is the accurate inspection of each URL that is referenced from the enterprise network.

## Astaro's Gateway solution to treat spyware

Astaro's security technology as incorporated within Astaro Security Linux software and Astaro Security Gateway appliances uses a server/gateway side approach in order to minimize maintenance and to provide full protection from user tracking threats.

To provide full spyware protection the following functionality is included:

- Detection of URLs from which spyware is originated and blocking of any attempts to infect computers within the enterprise network
- Interception and blocking of spyware communication from already infected computers while trying to send tracking information to the Internet

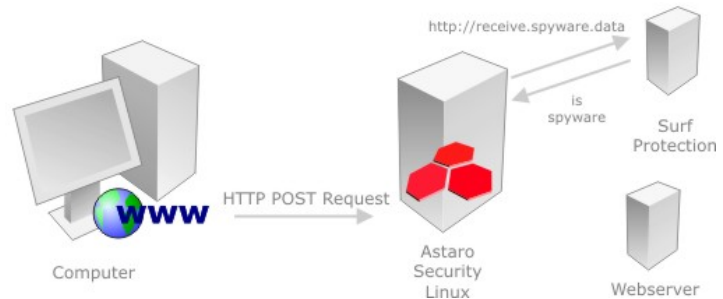
## Identifying malicious URLs

In order to inspect malicious HTTP traffic which might relate to spyware Astaro makes heavy use of a content filtering database with more than 2.6 billion Web pages and images classified into 60 categories. This database is the largest and most up-to-date database of its kind. By using fully automated web crawlers more than 120 million web pages are added to the database each month.

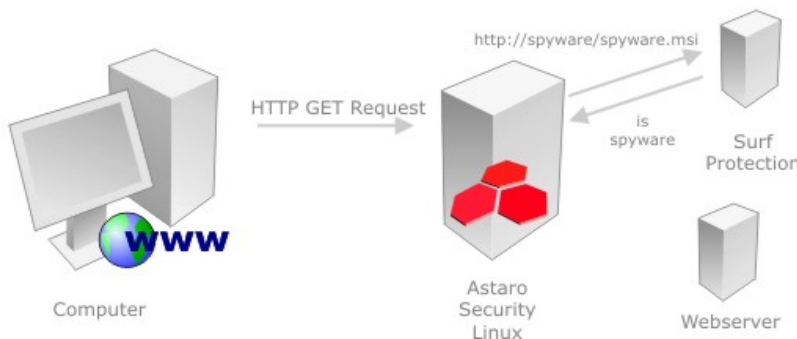
The highly sophisticated mechanisms used to categorize this content are also able to detect URLs related to spyware. A specific Spyware-category is now be used to accurately identify URLs of spyware sources or servers

## Block Spyware infection and communication

By using this web content database, Astaro's Spyware Protection solution is now able to check if the URL that is requested by the browser is a spyware URL (including Web Bug URLs), and if the server to which data is being sent is in fact a spyware server. It can then block both – Spyware infection as well as spyware communication.



To deal with those situations where Spyware writers change their servers and sources frequently, the system has a mechanism to handle spyware URLs that are not yet classified. If a user requests a web page, the URL is classified within 24 hours and updates of the new categories are distributed to Astaro customers several times a day. Thus, unknown URLs are classified within 1 or 2 days.



To be absolutely safe even during this timeframe, customers have the option to block all suspicious and unknown sites which have not yet been categorized. This option has the additional value of enhancing protection against phishing attacks by blocking communication to fraudulent links. To avoid

overly restrictive blocking of sites, customers also have the option of adding known safe sites to a whitelist that exempts them from being blocked.

## Block Spyware installation

In addition to blocking spyware related URLs Astaro's solution provides the option to filter embedded objects that might be included within so called *drive-by-downloads*. By activating this option all embedded objects like ActiveX Controls, Java, Flash or others would be removed from HTTP traffic, having the effect of protecting against installation of any active components on a user's desktop.

This functionality is part of Astaro's Content Filtering capabilities which are applicable to any type of HTTP traffic.

## Managing spyware protection

A huge advantage of Astaro's approach is the small administrative effort that has to be made to provide reasonable spyware protection at a low cost. No applications need to be installed on hundreds or thousands of client PCs. No applications need to be configured on those PCs. And there is no need to check if spyware patterns have been updated recently on those PCs.

## Conclusion

Spyware is a growing threat to a productive working environment. Treating the problem only with desktop anti-spyware tools is costly and ineffective. Now, Astaro Linux Security version 5.2 with full spyware protection can prevent the installation of spyware inside the network, and can preserve privacy by blocking spyware traffic outside of the network. And these capabilities are available as part of an award-winning, complete and effective security solution that is already known for being extremely easy to deploy and manage.