eSafe®

PROACTIVE CONTENT SECURITY

The Spyware Epidemic: Dealing With "Legal" Malicious Code

Aladdin®

SECURING THE GLOBAL VILLAGE

Table of Contents

Part 1: Introduction to Spyware

Overview

According to a recent survey held by the National Cyber Security Alliance and America Online, 80% of home computers tested were infected with an average of 93 different types of spyware. At any given time it is estimated that around 30% of all personal computers, including home computers, are infected by at least one computer virus, and over 70% of all email messages are spam.

While computer users and organizations take measures against virus infections and spam, spyware is generally overlooked. One of the reasons is because virus infections and spam are well-established threats, are very visible, and usually easy to recognize. Spyware by nature is stealthy, devious, and unfortunately can operate in a legal grey area -- allowing many, if not most, spyware vendors to work openly as "legitimate" businesses. And they do it because, like spam, spyware is a lucrative business.

Spyware is a much bigger problem than many realize:

- *90% of all Windows PCs are infected by spyware.[1]*

- *80% of all home computers are infected by spyware.[2]*

- *88% of owners of infected systems are not aware their computer is infected.[2]*

- *75% of PC owners believe they are safe from online threats.[2]*

- *Only 24% of PC owners are actually knowledgeable about how to handle spyware.[1]*

- *65% of all PC users do not run up-to-date anti-virus software.[2]*

- *50% of all broadband users do not use a firewall. The number drops to 7% for dial-up users.[2]*

  1. According to Dell™ survey, Sep 17-19, 2004

  2. According to National Cyber Security Alliance and America Online™ survey, Oct 25, 2004

History of Adware / Spyware

- **1995: First "Freeware":** Truly free applications with no additional payload are available for download.

- **1997: "Shareware" Applications:** Free for non-commercial use. Often containing repetitive registration screens, activation timers, functionality limitation, etc.

- **2000: Some Info Collection:** "QA" reporting elements start showing up. Applications still remain relatively safe. The information collection systems are mainly used to control installation base and collect debug information.

- **2001: Adware is Born:** Slow shareware revenues and new entrepreneurs realize the potential, developing a new business model: Get "free" software - pay by exposure to banner advertisement.

- **2002: "Spyware" elements start showing up -** Get "free" software in return for submitting surfing habit information/collection. The user is given a choice to register for a non-advertising version of their favorite software or "pay" by being exposed to targeted marketing in the form of banners; first within the application and later as pop-up windows, in-browser links and more. As time went by they became more and more invasive and aggressive.

- **2002-2003: Pure "Spyware":** Spyware with no free software starts to emerge. Web site visitors' infection, vague or no EULA disclaimers, misleading ActiveX installations, browser hijacking, porn dialers and more.

- **2004-2005:** Spyware and Trojans share same capabilities. Web content security identified as critical for spyware defense. Spyware becomes illegal.

Why is Spyware a threat?

Many people believe an application that presents pop-up ads from time-to-time is nothing to worry about – a nuisance at best. In reality, however, spyware is much more insidious. A single spyware application may do one, many, or all of the following:

- Gather private / personal information
- Steal copyrighted or confidential information, as well as passwords, bank account details, social security numbers, personal/business correspondence, and credit card information
- Create irreparable system instability
- Damage or interfere with legitimate applications operation
- Open a backdoor on infected systems
- Allow a spyware operator to take over an infected system

Why is information gathering so dangerous?

In theory, the idea of a software application serving as a central depository for personal information sounds very useful and can make an online experience more convenient. Every site is personalized, and tedious form filling is spared when accessing information, shopping or doing business. In practice, however, information gathering code is almost exclusively used to maximize profit and to focus the marketing efforts of commercial sponsors. While a few applications are useful and serve only the intended purpose, many others hide their true nature using various guises and use the personal information collected usually without the user's awareness.

Home PC users are exposed daily to the threat of spyware on many of the sites they visit. Any software installed on the system can potentially be spyware if users don't take the time to read the EULA (End User License Agreement). Unfortunately, most never read it. While users may find it useful that an application stores their personal and credit card information, can they really be sure what that application does with their information? What about a "free" document editor? Who else reads the documents installed on the system except for the user? With 80% of system infected with tens of spyware components, the answer to these questions is that spyware can send any and all information to whomever it was programmed to.

> **IDC Report: Spyware a Critical Security Threat**
>
> "Today, more malicious spyware can easily infiltrate corporate firewalls," says Brian Burke, research manager for Security Products at IDC.
>
> "These programs make their way into the corporate Intranet under the guise of less-threatening network traffic and, once in, they can wreak havoc."
>
> *Enterprise IT Planet: Security.* November, 2004

In the corporate environment the problem is even more critical because users compromised by spyware are processing company information. This information can be as mundane as 'parking arrangements' but might also include sensitive business or financial documents. Classified and proprietary information is usually worth more than a company can afford to lose. In the wrong hands, this information can cause catastrophic loss to any company. As a result, any information leaks should be dealt with utmost severity. Simply put, spyware should not be allowed into such an environment. It is the responsibility of the CSO or security administrator to make sure no unauthorized information leaves the corporate network unnoticed.

At times, a user might really trust a spyware application -- that the people behind it will not misuse the information they have in their hands. Even if this trust is justified, the following should be considered: The server holding this information could be hacked; the spyware operators may decide to share their database with a third party; the spyware's company can be sold or go bankrupt, etc. Once information leaves a user's system in an uncontrolled way, there's no telling where and how that information will be used.

Adware, Spyware and In-Between

Spyware and adware are advertisement-focused applications that, much like computer viruses, install themselves on systems with little or no user interaction. While such an application may be legal, it is usually installed without the user's knowledge or informed consent. A user in an organization could download and install a useful "free" application from the Internet and in doing so, unwittingly install a spyware component. The term 'spyware' is commonly used to describe both spyware and adware applications and will be used here to that extent for convenience.

Adware is a program that employs a targeted marketing technique. It usually monitors the user's activity on the net and displays advertisements based on this information. Adware applications connect to remote servers to download new ads and check for software updates for themselves. Users' details and online behavior are not shared or transmitted to these servers. Adware is similar to spyware in many aspects but is generally considered more "ethical".
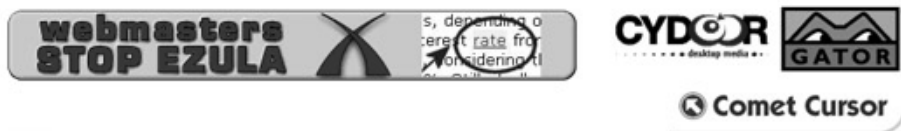
Like adware, spyware applications monitor the user's Internet activity, commonly accessed sites, surfing habits and keywords used in search engines. The main difference between the two is that spyware relays this information to an external entity. This entity will then display pop-up advertisements or redirect the user's search to display advertisements related to the search term used. Some spyware will even go as far as hijacking the infected system's default browser. This type of spyware, can shape the user's Internet surfing experience as their vendors please. On specific variant of this method referred to as "Thiefware", adds context sensitive hyperlinks to the textual content of visited web sites.

Information collected by spyware and sent to remote servers could be anything, from previously monitored activities to the user's personal information, or any confidential information, files and documents stored on the infected system.

With increased proliferation, spyware has become one of the

Thiefware example from: http://www.law.gwu.edu/facweb/claw/ezu
More thiefware information can be found at www.thiefware.com

main security concerns of many organizations. Some organizations even consider spyware to be the single greatest security threat.

Today we can say that most spyware is considered as commercial malicious code, which is openly developed, marketed and distributed without interruption and operates, at best, in gray legal areas.
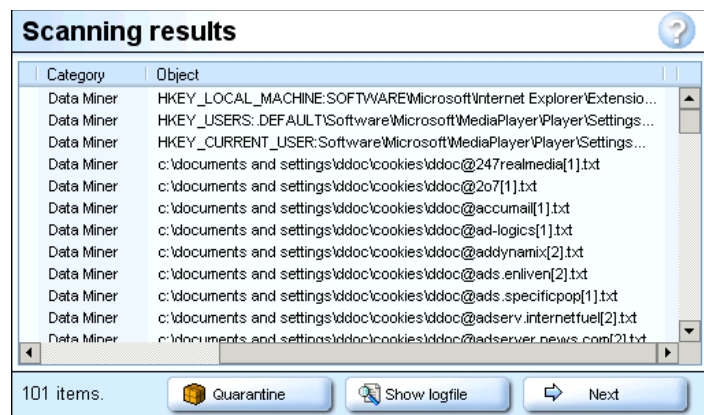
Are Cookies Spyware?

Cookies are a common component of today's browsing experience as they help site owners tailor their site to each user. Cookies can tell site operators the user's IP address and therefore, also their location on the globe. Yet, this information can be gleaned by other legitimate means – not just cookies. Some say cookies are a form of spyware. However, cookies are incapable of collecting personal information from users' PCs - there is no real impact on users' privacy. Therefore, cookies cannot be considered spyware.

Most sites today use cookies that store some preference information – are all of these websites spyware operators? Although some anti-spyware tools may identify many cookies on a certain PC as spyware, these cookies, at most, simply customize existing advertising on websites to the user's browsing habits (based on cookies collected from other sites).

Some spyware cleaning applications identify many cookies as spyware components. Are cookies really Spyware?

Cookies are also different from spyware because they do not require installation and are thus relatively invisible. Cookies are also very easy to remove, by using the 'Delete Cookies' option in one's browser. Cookies can also be blocked by the security options of the browser ('block all cookies'). The browser may also be configured to prompt the user to accept or reject certain cookies while browsing, and it can also be configured to only accept cookies from trusted sites.

The problem with cookie-control is their vast numbers on the web. Even after a fresh installation of the operating system, and even if a user only visits a handful of websites – there are bound to be several cookies already gathering information on the system. Occasionally cleaning cookies may be a good idea, not because they are dangerous or invasive in any way, but simply to free up some hard drive space and spare memory.
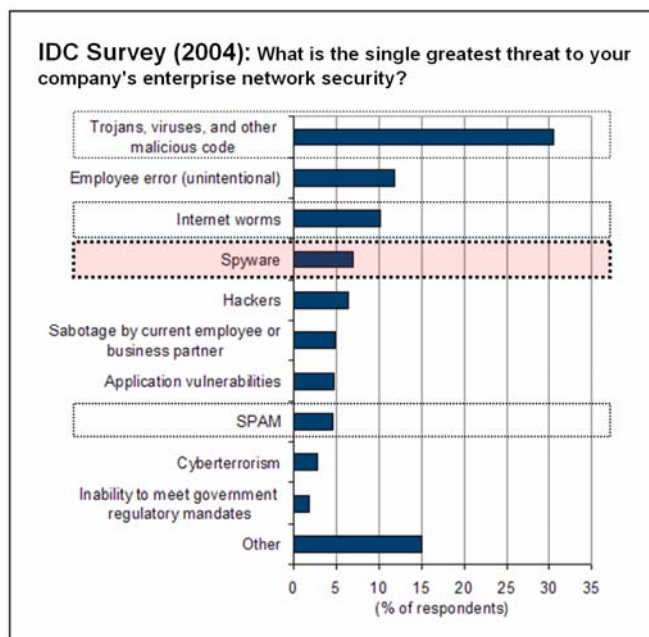
Part 2: Security Threats

Many security threats are introduced when spyware is installed on a system. When one security risk is enough to cripple a company's network, several similar risks bundled in one tight package can mean absolute disaster.

Security Policy Breach

Some spyware is bold enough to disable security measures, like firewalls. Even partial interference with these programs can expose the system to extreme danger. A disabled firewall may allow hackers to gain control over the compromised system. It may also make the system vulnerable to viruses that look for open ports on the web. Add to that the fact that many spyware applications can be updated from a remote server by a party unknown to the user, contributing to potential future security breaches of unknown extent. More about spywares' ability to launch automatic updates is discussed below.

IDC Survey (2004): What is the single greatest threat to your company's enterprise network security?

Threat	% of respondents
Trojans, viruses, and other malicious code	~31
Employee error (unintentional)	~12
Internet worms	~11
Spyware	~7
Hackers	~6
Sabotage by current employee or business partner	~5
Application vulnerabilities	~5
SPAM	~5
Cyberterrorism	~3
Inability to meet government regulatory mandates	~2
Other	~15

Browser Tracking

Usually only considered a nuisance rather than an actual security risk, this activity can be dangerous to corporate networks. A browser that was hijacked by spyware may send collected logs of visited web page to its headquarters. While most websites visited may be mundane, some may contain confidential information.

Information aggregation and data-mining technologies could also be applied on the collected data , profiling all Internet, Intranet and Extranet content visited by certain IPs which can easily be matched to the organization and could even point to internal MIS structures. Collected information could be compiled into some very 'informative' intelligence reports.

Information Theft

Not only browsing habits can be gathered by spyware. It may also look for 'useful' material found on the infected system. As corporate PCs hold information that is critical to both the organization and the employee, stolen information may include a vast range of data. It could be anything from personally identifying information to source code, business plans, financial information, usernames, passwords, copyrighted material or other intellectual property.

Confidentiality Breach

Another form of information theft: Some of the information stolen from a corporate environment may contain confidential information that should not be released to the public. Falling into the wrong hands, this information can be used against the company in various ways. It can be used to embarrass, discredit, extort and otherwise financially damage those

affected by the loss. One of the worst things that can happen to a company is to lose the trust of its customers.

Key Logging

As previously discussed, this is another form of information theft. A key logger runs in the background and logs each key stroke as it happens. Practically any information can be gathered this way.

Dialers

Some spyware types, also called "dialers" or "porn dialers", install new modem dial-up connections and will attempt to connect to paid services or international numbers. While many users have moved on to broadband Internet connections, many still have dial-up modems plugged in as backup, for faxing or just because they didn't bother disconnecting it. Mobile users frequently connect by modem when on the road and some spyware can even transparently disconnect existing connections and connect with their own.

Automatic Code Updates

Perhaps the most disturbing aspect of spyware is the ease with which spyware is able to update its own code. This code is usually only an updated version of the spyware installed. However, the persons or systems behind the update may upload and execute any code they want. This can include any malicious invasive code like a virus or a backdoor. In essence, spyware can be used by its operators to take over a system or network. The *Activity Monitor* spyware, for example, opens a backdoor on infected systems. This allows access to these systems similar to the one provided by Microsoft's Remote Desktop.

Spyware Security Holes

Spyware, just like any other software, can be prone to poor programming practices and code security vulnerabilities. There are documented cases of faulty spyware code, exposing systems to hacker and malicious code attacks beyond those originally intended by the spyware developers.
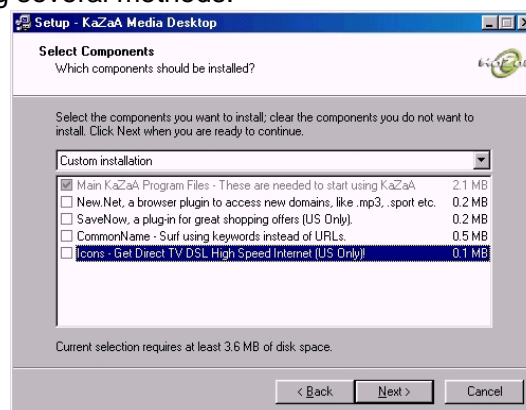
See: http://www.securiteam.com/windowsntfocus/5QP0Q1P6AU.html

Part 3: Technical aspects of Spyware

Where do they come from?

Spyware and adware usually install themselves using several methods:

1. The spyware might arrive bundled with "free" applications, available for download or otherwise distributed. The spyware component is installed as part of the installation process. The user is usually prompted for permission and asked to agree to an elaborate, long and usually tedious legal disclaimer or EULA (End User License Agreement). This message will include a great deal of "fine-print" that few will actually bother to read.

Spyware dropping can be part of some applications' installation process.

2. The spyware might ask to install itself when the user visits certain web sites. The spyware will usually be part of an ActiveX package that will display a Security Warning window. Many legitimate browser applets and add-ons install themselves in this fashion. As a result, many users are fooled by this generic message into installing spyware on their system. In many cases, spyware may also attempt to entice the user into downloading and installing it on the system by giving its setup file a tempting name such as "Free_Porn.exe", "Make_Money_Online.exe" or "Free_Warez.exe".

Many legitimate browser applets and add-ons install themselves after showing a dialog box like this.

3. Some spyware arrive bundled with a computer virus, worms or Trojans. When the virus is executed, part of its payload will be dedicated to installing the spyware components. Well-known examples are variants of the TrojanDownloader which installs several spyware components.

Spyware is usually installed on systems in a way that will ensure their operation whenever the system is online. This is done by having the system automatically load them at startup, as done by many viruses, worms and Trojan horses. Spyware can also ensure it is always on by integrating itself with other applications. The most common method would be by attaching itself to the system's Internet browser(s) as a toolbar. This type of spyware is called a Browser Helper Object (BHO, or a Browser Hijacker). Every time the user connects to the Internet, the spyware will be there, ready to share the user's information with its servers.

9-22

Indication of Infection

Unlike more stealthy malicious code, spyware tends to be quite obvious given their main purpose of displaying advertisements. This can be as obscure as advertisements displayed in local (especially non-English) language on visited websites, to pop-up messages urging to try certain products or services, even with no apparent browser window open.

Here are some common symptoms in spyware/adware infected systems:

1. Excessive number of pop-up windows even when using pop-up blocking tools.

2. Website redirection. The browser does not go where the user wants it to. This could happen always or sometimes.

3. New toolbars, menus or buttons, users don't recall installing, are added to the browser.

4. The browser's home page is not what the user set and keeps returning to the same page even after changing it.

5. The default search engine changed. Whenever a site the user looks for is not found they are directed to unknown search pages, with plenty of marketing content.

6. New taskbar icons and applications appear without user installation. Common ones allow time synchronization and weather information.

7. New links and folders were automatically added to the Favorites.

8. Excessive additional hyperlinks are visible in all visited web pages, sometimes with different underline color, highlighted, etc.

9. Significant increased network activity even when the system is supposed to be idle.

10. Significantly decreased PC performance. This includes increased startup or login times and general "sluggishness."

11. Strange, non-Microsoft dialog boxes, belonging to applications the user did not install, ask suspicious questions.

12. New modem dialup connections appear in the system to adult sites, pirate software, etc. appear in the system. Unexpected modem connection initiation (dialing) or "surprises" when the phone bill arrives.

13. System instability including frequent crashes, crippled application functionality, and unexplained error messages.

Inside the System

Many software developers work hard to get their products to work with minimal interruption to the system and to other installed applications. Spyware, however, is not so considerate. Many of them create dozens, sometimes hundreds of registry entries, directories and files. Their effect on the system is significant and may cause unexpected problems, sometimes beyond repair. Cleaning infected systems can be a complicated procedure, even for an expert. Cleaning times and effort are usually in direct proportion to the intrusiveness of the specific spyware. Some of the more insidious ones will even hook themselves into the

TCP/IP communication stack (Windows sockets) in a way that will make network connections dependant on their presence on the infected system. By removing the spyware, the user will also damage the system's communication capabilities.
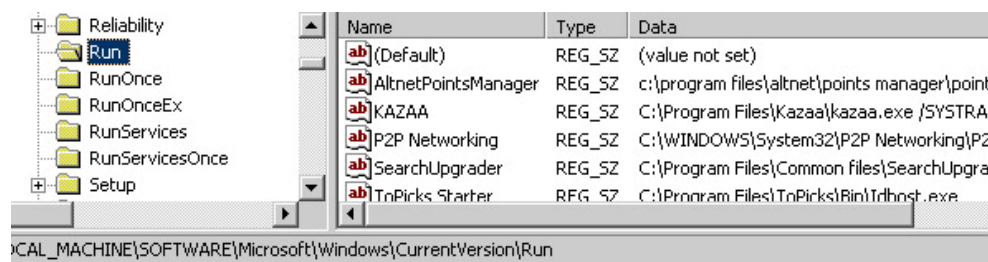

Many spyware create dozens, sometimes hundreds of registry entries, directories and files. Above we see the Windows Registry showing many spyware components designed to run in every system startup.

Modes of Operation

The dozens of different spyware applications out there share many similar features with one another. There are a few common basic elements present in the way most spyware operate. These are divided into information gathering (also referred to as enumeration) and advertising methods.

Information Gathering:

1. **User activity monitoring:** This is the most common method of information gathering. The spyware logs the user's personal details stored on the system, such as the user's full name, virtual and actual address, contacts, financial information, secret or copyrighted information etc. Sometimes, even the user's system hardware is logged. Internet browsing habits and preferences are also commonly tracked; details such as commercial products viewed by the user as well as news items and hobbies pursued – even search terms used in search engines.

2. **Key logging:** This is considered as one of the most intrusive and objectionable methods, and probably the most legally ambiguous. The spyware logs all keystrokes performed by the user and stores them in a log file. The file is periodically sent to a central server for analysis. While this method may gather information that will help personalize advertisements for that specific user, no one guarantees it will not be used for other purposes. The log files are also likely to contain usernames and passwords, credit card numbers, bank account information, personal emails and confidential documents – everything that is keyed by the user while the spyware is running on the system!
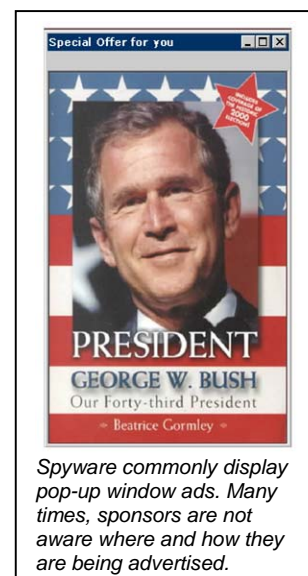
Advertising:

3. **Banners:** This is the least intrusive and most common advertisement method that most adware employ regularly. It displays a rotating banner somewhere within the application window, usually at the top of the window This behavior is usually accepted by users as it helps certain applications maintain their 'free' status without interfering with the user's

Spyware commonly display pop-up window ads. Many times, sponsors are not aware where and how they are being advertised.

everyday activity and without exposing the user to negative elements used by spyware. In themselves, the banners are not dangerous – as long as they are not combined with other advertising or information gathering methods.

4. **Display pop-up screens:** This is simply done by opening windows which display an advertisement. Pop-up screens are the most common method spyware applications use to expose their target to content of their choosing. The messages may appear in reaction to something the user does – like open a certain document, or they may appear at random intervals.

Some spyware employs information gathering methods which can also immediately act upon the collected information to display advertisements:

5. **Homepage and default search engine hijacking:** The spyware may permanently change the browser's homepage and default search engine to a web page of its choosing. The user is forced to view the new web page whenever the browser is opened and whenever attempting a search using the browser search bar. Attempting to replace the homepage address by the user will usually only work temporarily or even fail completely.
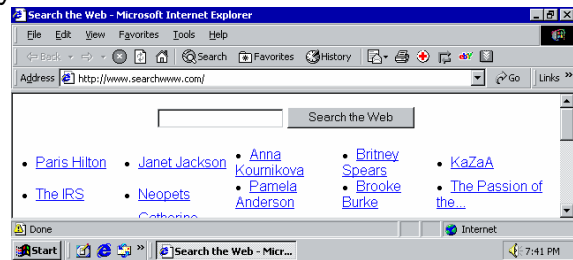

Spyware may hijack the browser's home and search pages.

6. **Redirection:** The common search redirection spyware monitors search engines entries, redirecting the search to display related commercial results. For example, searching for "Angelina Jolie" in a search engine would display links that were mostly, or even solely, sponsored sites offering celebrity merchandise of the movie star, DVDs, or other Hollywood products, such as magazines, entertainment news websites (with paid subscription options of course) and so on.

7. **Browser Helper Objects (BHO):** This type of spyware integrates directly with the web browser. Usually, BHOs they can use most of the methods mentioned above as they have complete control over the user's ability to browse the web.
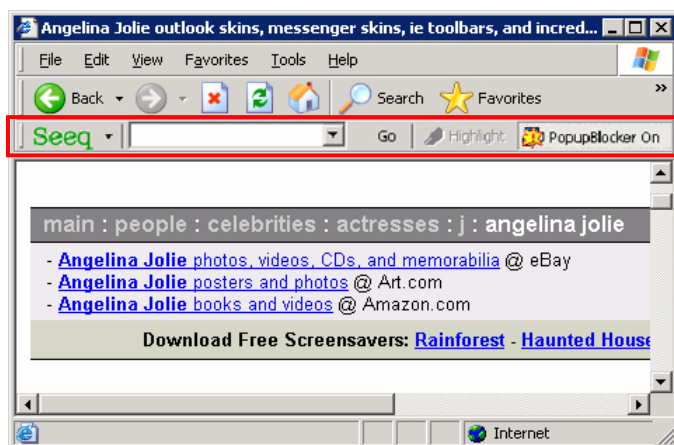
Toolbar spyware such as *Seeq* are very common and integrate directly with the browser. This one, very cynically, even imitates the

8. The Cynical "Anti-Spyware" Spyware: Some spyware vendors are just shameless. Knowing the concern about spyware and combining their Internet promotion and marketing expertise, they have put two and two together and created the "Anti-spyware" spyware…
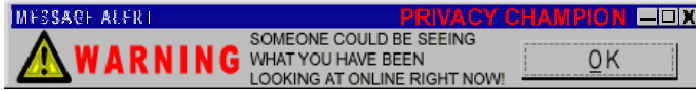
Unfortunately, dozens of these already exist. These applications typically use aggressive, false, and manipulative advertisements to convince and sometimes automatically install themselves. Some even cost money or offer a paid "upgrade" that will only show less advertisements. They claim to clean infected systems but will do so, if at all, only partially and allow their own advertisements and information gathering to work uninterruptedly. This type of spyware is especially dangerous because it provides a false sense of security.

Part 4: Spyware Blocking Challenges

Many security experts agree that, like computer viruses, spyware is very difficult to block since it comes in all sizes and shapes – employing a single technique against spyware is simply not enough. While many products can block certain types of spyware, few solutions, if any, are air-tight.

Due to many reasons, legal and technical, blocking spyware may not always be as straightforward as blocking a virus. The fact that spyware creators are mostly legitimate, if sometimes dubious, businesses allow them to operate openly, hire talented programmers, and improve their software. They come up with new ways to integrate deeper into the system and collect more information with more details.

Unlike viruses and worms, spyware does not yet use self-propagation methods, so infected machines are not going to infect other machines. But, of course this could change in the future as spyware creators look for new hunting grounds.

And finally, spyware does not receive the appropriate attention; the same attention as other serious threats. While practically everyone knows a thing or two about computer viruses, statistically, only one in four people regard themselves as knowledgeable about how to handle spyware infestation. In reality, however, around 80% of all computers are infected by spyware.

Spyware Legal Issues

Unlike computer viruses, spyware is usually installed on the system *with* the user's consent, or at least partial consent. Spyware is often bundled with desirable applications that users install, so making the separation could be problematic, even impossible. Removing some spyware prevents the associated applications from working. Therefore, treating spyware exactly like a virus may be a problem. For example, while a vendor may remove a virus even without notifying the user, deleting a program installed by the user may not be a desirable action. In addition, many spyware applications are not illegal by definition. Even just calling them "spyware" may enrage their vendors who consider themselves legitimate. Such vendors have been known to file slander lawsuits against offenders whom they claim damaged their reputation.
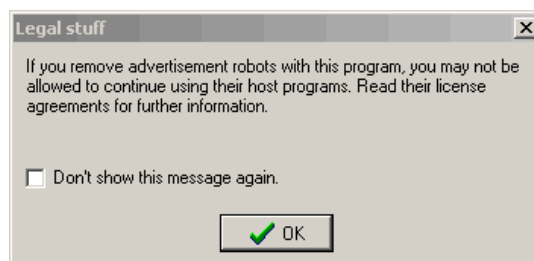
Existing Solutions and Associated Problems

The common line of defense against spyware in recent years has been to passively try avoiding it and the random use of desktop products to clean the system. This approach might be appropriate for consumers but is clearly not enough in the corporate environment. Until recently there have been no efficient spyware perimeter security measures or centrally managed desktop solutions.

Following are some of the anti-spyware solutions and practices available today, along with their limitations:

       14-22

Legislation

I-SPY Act: The Internet Spyware (I-SPY) Prevention Act of 2004 is one of the first anti spyware laws. Unfortunately, although it is a very important law that defines spyware and acknowledges the problem, it is likely that just like the CAN-SPAM Act, it will only throw spyware vendors to the fringes of the law or worse, have them resort to illegal activity from off-shore based spyware servers.

I-SPY Act Bill Summary and Status: http://thomas.loc.gov/cgi-bin/bdquery/z?d108:h.r.02929:

Desktop Solutions

- **Avoid Spyware** by refraining from installing such software. This method is really ineffective today. Spyware is so prevalent that even experienced users starting off with a clean system and relying only on avoidance are often surprised to find their system infected in no time. In organizations this is obviously not practical because users often do not know, care, or ask, before installing new software on their systems. In many cases users are even not aware spyware has been installed when they were visiting certain web pages.

- **Desktop Products:** these tools inspect the system and clean spyware and spyware residues. Usually spyware is identified by file signature, registry keys, hosts files and cookies. Some products also provide active protection in the background against new infections but this adds another background process that may conflict with some applications, make startup slower and create some slowdown. Most of the available tools require some computer experience, but the biggest problem for the organization is the lack of central installation and management.
  Another problem is that currently there are almost 30,000 spyware component signatures and growing. The signature method is similar to conventional anti virus signatures, requiring an extensive database that constantly updates with new spyware versions and the corresponding software in which they exist. This is a complicated and reactive solution.

Gateway Solutions

- **Gateway-based signatures**: The solutions use a signature database with the same limitations mentioned regarding the desktop products. However, unlike desktop solutions, gateway signatures are only applicable to files passing through the gateway, but not to registry keys, modified desktop host files or other desktop stored components. They are also ineffective where users with laptops install spyware-infected software when outside the organization, or if such software is otherwise brought into the organization, for example, on CD-ROM.

- **URL blocking:** This method prevents access to websites related to spyware. This method will simply not allow a user or an automated process to access certain HTTP addresses marked as unsafe.

- **Prevent unauthorized installations:** Identifying unwanted install processes, especially in infectious web pages, prevents spyware from taking over a system. This method will simply not allow any identifiable spyware from being installed via web.

- **Spyware protocol blocking:** Identifying the communications protocol used by spyware, and blocking such traffic prevents spyware from transmit collected information, downloading the advertisement content, or updating its own code.

Part 5: Blocking Spyware with eSafe

eSafe Spyware Defense Overview

eSafe Gateway is uniquely positioned to deal with the spyware security threats at the gateway due to the patented NitroInspection™ technology and its ultra-fast inline content inspection. Equipped with AppliFilter™ and the Proactive Security Engine (PSE) ™, eSafe is able to provide a comprehensive solution for spyware based on a multi-layered gateway approach:

eSafe's four layers of Spyware blocking

Layer 1: Spyware 'driveby' blocking

Layer 2: Spyware download blocking

Layer 3: Spyware signature blocking

Layer 4: Spyware communications blocking

Layer 1: Spyware 'driveby' blocking

Where: At the gateway, before the spyware can be downloaded to the desktop.

Unique to eSafe:

- Proactively block <u>exploits</u> which allow automatic spyware download and installation.
- Proactively prevent unintended spyware download by unsuspecting users after being exposed to tricky and misleading dialog boxes.

Technology: eSafe's XploitStopper™ blocks web surfing exploits which are used by many spyware. AppliFilter™ blocks some spyware content server download by pattern.

Added security: No infection even if the user clicks 'Yes' in various dialog boxes.

Note: Some of the functionality in this layer requires the AppliFilter add-on.
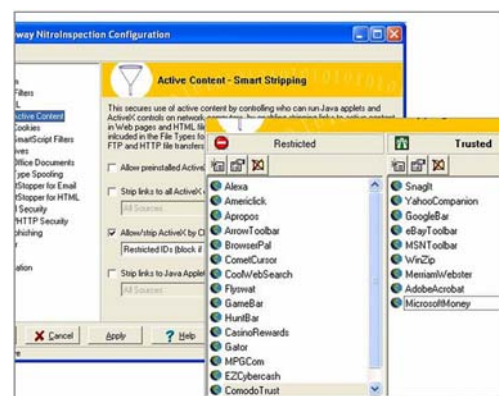
Layer 2: Spyware download blocking

Where: before spyware is downloaded or before <u>an existing ActiveX</u> is exploited.

- Block access to spyware servers using auto-updated URL lists (separate from URL filtering add-on).
- Block spyware according to Auto-updated lists of ActiveX (CLSID) identification.

Added security:

- Effective against spyware and a variety of other malicious mobile code (MMC).
- Block existing ActiveX (pre-installed) from being exploited.
- Allow predefined ActiveX and browser add-ons to be installed by users.
- Allows a white list of trusted objects such as

eSafe allows only authorized browser add-ons to download or run.

16-22

Google or MSN toolbars.
- Allows a black list of untrusted objects.
- Administrators can assign new Objects used by the organization.

Layer 3: Spyware signature blocking

Where: After spyware is downloaded and before it reaches the client.

- Uses traditional signature database – similar to antivirus technology.
  Note: Most anti-spyware vendors do not have antivirus technology.
- Smart Signatures provided by the Proactive Security Engine, use heuristics to block most spyware <u>without updates</u>!

Added security:

- This layer is effective after spyware is downloaded and before it reaches the requesting client.
- It is also effective against spyware worms traveling by email, or downloaded from web and FTP sites.

Layer 4: Spyware communications blocking

Where: at the gateway, whenever spyware traffic is identified.

Technology: Uses AppliFilter™ to prevent existing spyware from communicating with their servers

- Provides protection <u>even when spyware is already installed on the desktop</u>
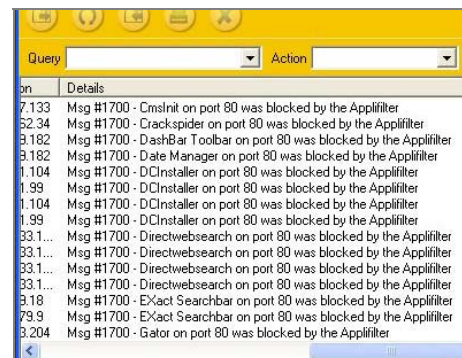- Allows administrators to identify infected machines

Added security:

- Renders spyware useless to the vendor
- Identifies spyware communications <u>by protocol</u> - on any port

Blocking communications between the desktop spyware component and the remote spyware server will render it useless to its vendor. eSafe's' AppliFilter™ searches for signs of spyware communication protocols in the raw traffic as it passes the gateway before it is even constructed into files. By working similarly to active IDS, eSafe intercepts and blocks spyware communications before it reaches desktops inside the organization. Another eSafe benefit is that unlike proxy-based gateway solutions, eSafe is not limited to blocking spyware over HTTP port 80. In fact, eSafe is not bound to specific ports at all and can inspect traffic
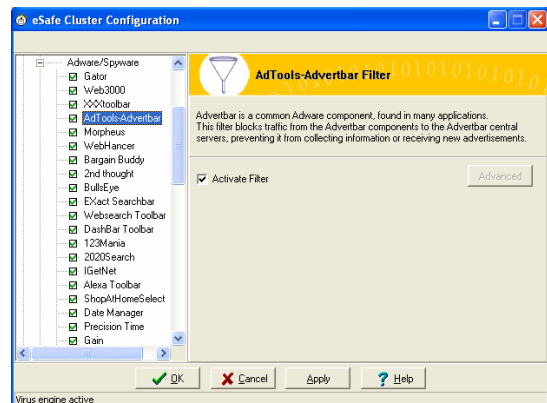
AppliFilter™ prevents existing spyware from communicating with their servers as well s downloads and "drive-by" installation attempts of new spyware.

Monitoring eSafe reports allow administrators to identify and treat individual infected workstations.

17-22

by protocol, whichever port spyware uses.

In addition to blocking communications between the spyware and its server, eSafe reports allow administrators to pinpoint infected workstations and provide them with the proper desktop cleaning tools.

Automatic Updates

All eSafe signatures and spyware attack parameters are automatically updated by the eSafe CSRT (Content Security Response Team) when new spyware is discovered. Automatic updates include:

- Spyware and malicious code signatures.
- Spyware and malicious code proactive heuristics definitions.
- Spyware and legitimate (white list) ID definitions.
- AppliFilter™ real-time spyware protocol definitions.

Summary

As we have seen, spyware is a serious security threat as well as an IT helpdesk nightmare. It is estimated the problem will grow and Spyware will become more pervasive and less legal. In order to achieve as much control as possible, it is suggested to address the problem in the same manner as other malicious code:

- Acknowledge the threat
- Prepare a spyware prevention plan for the organization
- Educate IT helpdesk
- Educate users
- Deploy the technological solutions:
    - o Use a gateway solution to block the download and installation of Spyware
    - o Use a gateway solution to block communications of infected PCs with Spyware servers
    - o Observe gateway solution reports to identify infected machines
    - o Use desktop solutions to clean infected machines and run periodical inspection

Appendix: eSafe Technologies

eSafe is an integrated solution working in parallel to access security (firewall, VPN, intrusion detection) and focusing **specifically** on SCM (Secure Content management) requirements. SCM covers:

- Email anti-virus
- Anti-spam
- Web traffic (HTTP and FTP) content inspection
- URL (web site) filtering
- Worm protection
- Instant messengers, Peer-to-peer (P2P), spyware, adware, and more
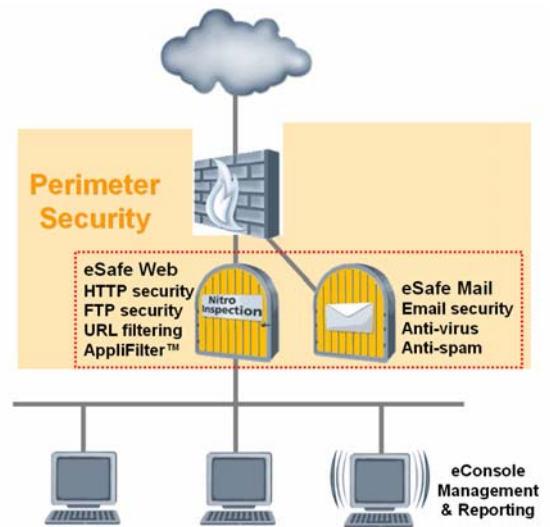
eSafe addresses all gateway content security layers

eSafe is a comprehensive, fully-integrated content security solution that addresses all content security layers. It includes:

Proactive antivirus: Proactively blocks most zero-hour malicious code, including worms and Trojans.

Signature antivirus: ICSA and Checkmark certified to block 100% of In-The-Wild viruses.

Exploit protection: Proactively blocks security vulnerability attacks in all email and on the web.
 - HTTP protocol enforcement and exploit detection.
 - HTML inspection for malicious scripts and exploits in web pages, webmail and email body.
 - Email standardization to RFC standards eliminates known and unknown exploits.

**Email Compliance** based on textual content and attached file types.

Web/URL filtering according to category, content, and files types.

Application Filtering of Internet worms, spyware, IM, P2P, remote control applications and tunneling.
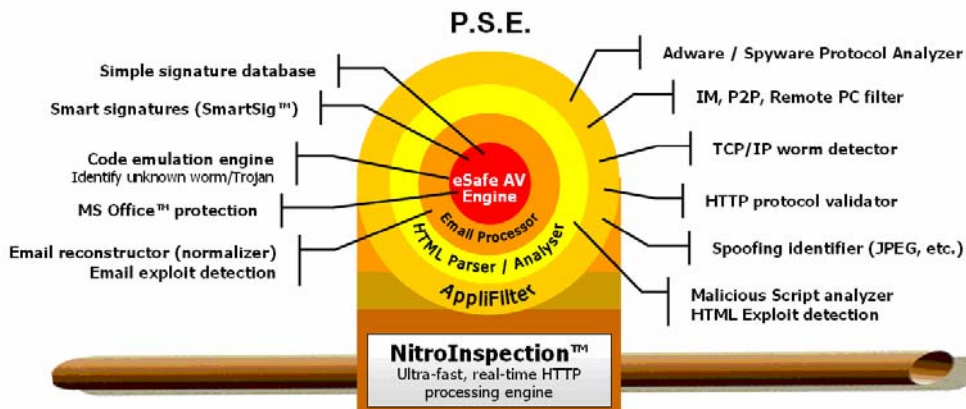
Spam Management blocks the flood of unsolicited bulk email, saving time and money.

4-Layer Spyware Blocking

Layer 1: Spyware "driveby" blocking

Layer 2: Spyware download blocking

Layer 3: Spyware signature blocking

Layer 4: Spyware communications blocking
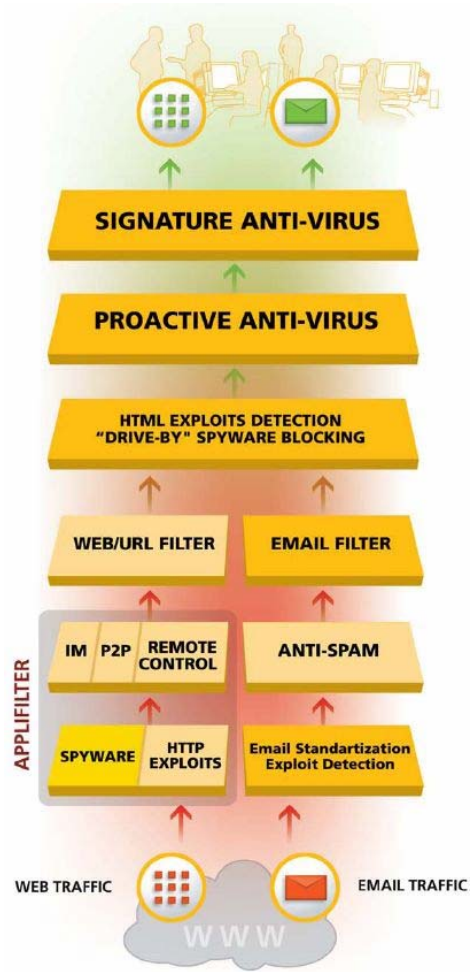
eSafe's Proactive Security Engine (PSE)™

eSafe PSE uses patented content inspection technologies to provide the most comprehensive solution without performance degradation even in very busy networks with tens of megabits of Internet connectivity speeds.

eSafe Features

- Real-time protection for all Internet born traffic - SMTP, POP3, HTTP, and FTP

- Proactive anti-virus and malicious code protection engine that is ICSA and Checkmark certified

- Exploit and worm protection against new vulnerabilities as well as protection against various hacking attacks

- Advanced Anti-spam module that utilizes multiple spam control methods including real-time black lists (RBL), DNS lookup, header verification and keyword filtering to keep spam to a minimum

- URL filtering module to keep out unwanted web content

- Web application filtering such as instant messengers, P2P and file sharing, remote access, spyware and adware

- Innovative NitroInspection™ packet collector engine which can be deployed in various configurations; mainly inline to achieve highest performance and excellent user experience

- Flexibility in network implementation

- Up to 40Mbps on standard appliance

- Integrated fail-over and load-balancing with up to 8 eSafe machines inspecting over 200Mbps of traffic

- eConsole - fully integrated management and configuration console

- Automatic on-line update for signatures, engine and new upgrades

- Extended 24 x 7 premium support service

- Check Point OPSEC and Cisco AVVID certified partner

- Smooth integration with virtually any firewall/VPN product

- Unique offering of value added services especially for the ISP and MSSP markets

Contact Information

Aladdin
SECURING THE GLOBAL VILLAGE

For more info:
Aladdin.com/eSafe

International	T: +972-3-6362222, Email: esafe@Aladdin.com
North America	T: 1-800-562-2543, Email: esafe.us@Aladdin.com
UK	T: +44-1753-622266, Email: esafe.uk@Aladdin.com
Germany	T: +49-89-89-4221-0, Email: esafe.de@Aladdin.com
Benelux	T: +31-30-688-0800, Email: esafe.nl@Aladdin.com
France	T: +33-1-41-37-70-30, Email: esafe.fr@Aladdin.com
Israel	T: +972-3-6362222, Email: esafe.il@Aladdin.com
Japan	T: +81-426-607-191, Email: esafe.jp@Aladdin.com
Spain	T: +34-91-375-99-00, Email: esafe.es@Aladdin.com

About Aladdin Knowledge Systems

Aladdin (NASDAQ: ALDN) is a leader in digital security, providing solutions for software digital rights management and Internet security since 1985, serving more than 30,000 customers worldwide.

Aladdin products include: the USB-based eToken™ device for strong user authentication and e-commerce security; the eSafe® line of integrated content security solutions that protect networks against malicious, inappropriate and nonproductive Internet-borne content; and the HASP® family of hardware- and software-based products that flexibly protect, license and distribute software and intellectual property.

Visit the Aladdin Web site at http://www.aladdin.com.

For free trial software, success stories and additional white-papers, visit http://www.eSafe.com. If you would like to obtain pricing or suggestions on eSafe for your organization's architecture, please contact one of the Aladdin offices listed above.