Putting a Stop to Spyware

The Rising Tide of Spyware

Spyware threats are on the rise and pose a significant security concern to organizations. In a recent Harris poll, 92% of IT managers thought their organizations were infected with spyware and had approximately 29% of workstations infected. Spyware has the ability to capture all workstation activity – from monitoring keystrokes to interrogating the system for confidential files or network passwords. A single successful spyware attack can cost an organization a fortune in profits and lost productivity when considering the value of corporate intellectual property and the time spent disinfecting the network.

What is Spyware?

Spyware includes software applications that gather information about a user without their knowledge and subsequently transmits this information to another machine via the Internet. Spyware can gather information as diverse as e-mail addresses, credit card numbers, and data from within files. Spyware can also perform functions such as snooping on other applications or installing additional spyware. Spyware is often installed as the result of clicking on a deceptive Web site, through a file attachment or URL link within an e-mail, or through an "auto-install" application that makes its way to the desktop.

Spyware Uses Multiple Attack Points

The various types of spyware have quickly become more sophisticated and now are typically transmitted using blended threat techniques that attempt entry through multiple network points.

With so many potential entry points, it is critical for today's corporate networks to deploy anti-spyware protection at each attack layer in order to ensure comprehensive and proactive spyware defense. An enterprise class solution is needed at the network gateway to manage both Web and e-mail traffic and at the desktop to manage end point behavior.

How SurfControl Stops Spyware

SurfControl Prevents Spyware from Reaching the Desktop

The SurfControl Enterprise Protection Suite™ integrates best-in-class Web, E-mail and End Point security solutions to protect against ever-changing spyware threats that increasingly exploit multiple threat vulnerability points. SurfControl's unified approach simplifies protection across these multiple threat entry points. (e.g., Web browsing, e-mail, IM, P2P, portable media, mobile workers). This multi-layered solution is highly relevant as blended attacks find new ways to render conventional anti-spyware security measures obsolete.

SurfControl's Enterprise Protection Suite shields organizations against emerging threats by using Adaptive Threat Intelligence from its Global Threat Experts. These researchers continuously analyze and research Internet threats and provide automatic security updates to protect customers.

Enterprise Protection Suite Consists of three key anti-spyware defense layers:

- Web Threat Protection (SurfControl Web Filter, SurfControl Mobile Filter)
- E-mail Threat Protection (SurfControl E-mail Filter, SurfControl RiskFilter)
- End Point Protection (SurfControl Enterprise Threat Shield)

Web Threat Protection

SurfControl Blocks Sites that Host Spyware
The URL Category list in Web Filter contains a 'Spyware' category, allowing administrators to set up a simple set of rules to block access to sites that are known spyware hosts.

SurfControl Blocks Sites Hosting IM and P2P Applications
The same easy-to-use rules interface also allows rules to be created to block "Remote Proxies" and "Web-based E-mail" related sites in order to prevent access to P2P file sharing and IM client applications. These applications are one of the most common sources of spyware infection.

SurfControl Blocks File Downloads
Administrators can stop the downloading of spyware related applications (as well as other harmful content) by choosing to block types of file downloads. SurfControl provides administrators with the ability to block users from download sites or block specified file types. This further prevents users from downloading and installing IM and P2P applications, as well as protects the network from "suspect" files with extensions such as .exe or .vbs.

E-mail Threat Protection

SurfControl Blocks Spam, Phishing, Spyware E-mails
The Anti-Spam Agent database in E-mail Filter and RiskFilter contains multiple techniques, such as digital fingerprints, heuristics, and lexical analysis rules, to proactively detect and stop an e-mail borne spyware attack at the gateway.

SurfControl Blocks Spyware Links in E-mails
The URL Category list in E-mail Filter contains 'Hacking/Spyware' and 'Phishing/Fraud/Criminal' categories, allowing administrators to block e-mails that include links to sites that host spyware.

SurfControl Removes Active HTML from E-mails
Spyware writers often install spyware at the desktop through active HTML code transmitted to the desktop through e-mail blasts. SurfControl's HTML Stripper can detect and remove harmful code, such as ActiveX, Java applets, and VBS scripts from e-mails at the network gateway.

SurfControl Detects and Cleans Viruses Within E-mails
The Anti-Virus Agent in E-mail Filter and RiskFilter a gateway virus scanner that protects an organization's e-mail server and network from virus and spyware infested e-mails.

SurfControl Removes Executable and Other Harmful Attachments from E-mails
Spyware attacks can be transmitted through executable file attachments in e-mails. Harmful attachments, such as .vbs or .exe files can be stripped from e-mails at the gateway before they transmit through the network to the employee's desktop.

End Point Threat Protection

Multi-Layered Spyware Protection at the Desktop
Other products can scan and remove spyware, but that's only half the solution. Only SurfControl Enterprise Threat Shield scans, removes *and* prevents spyware from infecting machines before it has a chance to jeopardize the organization.

The SurfControl Enterprise Threat Shield prevents malicious applications and services, such as spyware, keyloggers, instant messaging, P2P downloads and games from ever reaching the desktop. It also scans and removes any unwanted applications that are already there.

Three Layers of Protection:

- WriteWatch stops malicious files from infecting a users machine in the first place.
- .exeWatch stops existing malicious applications from executing
- FileWatch finds and removes existing malicious applications

To learn more about how SurfControl can stop spyware from entering your network, visit
www.surfcontrol.com