Spyware Prevention

Cyberoam Spyware Blocker offers comprehensive protection from spyware

Spyware is recognized as one of the most vexing challenges faced by corporates today. It can put the corporate information at risk, creating serious privacy, productivity and security concerns for enterprises. IDC estimates that two out of every three PCs are infected with spyware. According to new research from IDC, the need to identify and eradicate these parasitic programs will drive anti-spyware software revenues from $12 million in 2003 to $305 million in 2008. This rapidly growing market has become one of the hottest topics within the past year. The destructive effects of spyware have escalated from home PC nuisance to serious corporate dilemmas.[1]

The Trouble with Spyware

Spyware (also known as Adware, Malware, Grayware and a host of other names) is software that covertly gathers user information through users' Internet connections without their consent. Spyware applications are typically bundled with freeware or shareware programs that can be downloaded from the Internet.

Spyware can cause significant damage to legitimate software, network performance and employee productivity. Left untreated, spyware can:

- Change the system and registry settings of a computer,
- Corrupt the data,
- Trigger tons of annoying pop-up ads,
- Monitor your email,
- Enable identity theft,
- Track keystrokes,
- Steal personal information,
- Track users' online activity and sell the information to anyone willing to pay.

Adware is another application that helps in tracking, recording or reporting user information to the third party. Adware applications normally display advertising banners while the program is running.

Both these applications - spyware and adware - are sometimes similar in nature and are collectively referred to as spyware.

How Does Spyware Infect?

Spyware can infect the networks through various means. The normal modes of infection for a spyware include “drive-by downloads”, “useful free” web downloads and spyware bundled into P2P file sharing applications.

- Drive-by downloads the most common mode of infection automatically begins downloading the software on the user's computer upon a visit to the web page. Depending upon the browser's security settings, the user may be prompted with a security warning to either stop or continue the installation. The warning, however, may not offer a proper description of the program and is usually misleading or masked by other deceptive dialog boxes. In some cases, even if the user refuses to continue with the installation, “No” is not taken for an answer and repeated attempts are made to get the user to approve and download the application.

- Free Web Downloads - The distributors of spyware present the application as a useful free utility, luring users to download the application without realizing its intent. Laxity on the part of users to read the lengthy “Terms & Conditions” and “End User License Agreement” (EULA), gives such spyware an easy way to deny ownership to any liability for the problems caused.

- P2P Applications - Spyware is bundled with free P2P file sharing applications. At times it is mandatory to install the spyware component for the P2P application to function. These “free” versions generate ad revenue for publishers, causing pop-up ads and sending information to affiliate networks for data aggregation and data mining.

Protection Against Spyware : The Basic Steps

For any organization to protect itself against spyware, an effective combination of the following basic steps is essential :

- **Education:** Awareness on behalf of the users to be extra cautious while downloading and installing applications through the Internet is essential. The users should also be vigilant enough to read the fine print in the “End User License Agreement” (EULA). By doing so they would be sure of what they are downloading and won't get their hands on the extra something that they haven't bargained for.

- **Policies:** Robust company wide Internet policies have to be implemented that keep a check on the surfing pattern of the users by blocking harmful sites to prevent unauthorized and accidental downloads.

- **Technology:** Installing the latest browser and operating system patches, ensuring that browser security settings are set correctly, configuring email programs such as Microsoft Outlook to block Internet images and other external content in HTML emails and deploying up-to-date security software are some of the introductory checks that the user has to have in place.

Spyware Blocker - Cyberoam's Gateway Level Solution to Spyware

Cyberoam Spyware Blocker provides gateway level spyware and adware protection, blocking access to known spyware carrying sites and entry of spywares at the gateway level. In addition, it reports irregular traffic within the network, providing comprehensive and ongoing protection against spyware.

Prevents Access to Spyware Sites

Cyberoam's content filtering provides the first line of defense against spyware, preventing access to spyware perpetuating sites. It's WebCat web categorization engine has a comprehensive site database grouped into over 60 categories, ensuring effective surfing security.

The database contains a specific spyware category that holds sites which are known spyware generating sites. This constantly updated database offers real-time and up-to-date protection, blocking access to spyware carrying sites.

Blocks Spywares

Cyberoam Spyware Blocker identifies and blocks spyware files, preventing spyware from infecting computers within the network. The files are constantly updated, providing up-to-date enterprise protection.

As an additional measure, it automatically identifies and records URLs from where the spyware has originated for future blocking, bringing in intelligent spyware controls to the enterprise.

Blocks Applications

Cyberoam Firewall prevents traffic that does not conform to a particular application protocol from entering the network. It enables network administrators with the ability to monitor and manage the use of peer-to-peer file sharing programs from operating through the firewall, closing a potential backdoor that can be used to compromise the network.

Further, it blocks unapproved applications from sending information across the net, blocking spyware communication from infected computers to spyware originators.

Spyware Traffic Discovery : Real- Time Reporting

To combat spyware that exists within the network, Cyberoam Traffic Discovery studies current traffic patterns, identifies and reports suspicious transmissions, ensuring little time lag between origination and prevention. Through Cyberoam, administrators can identify the user and IP address from which spyware transmission is currently originating, enabling them to take steps to isolate the system and take corrective action. This provides real-time protection, preventing the spyware from spreading within the network, sending transmissions externally or causing damage to the network.

Conclusion

With the Internet set to become the default communication medium, spyware will continue to evolve. Enterprises are now coming to view it as a Grade A danger that poses a real threat to identity, privacy and information confidentiality. Cyberoam's Spyware Blocker functions with no additional effort on the administrator's part in configuring or installing new software. As an inherent part of Cyberoam, it uses Cyberoam's content filtering, firewall and spyware recognition capabilities to prevent entry of spywares within the network, thereby safeguarding privacy, bandwidth and computing resources of the organization from spyware attacks and infections.

Sources

1. www.idc.com