CYBER SECURITY INDUSTRY ALLIANCE

Spyware: Get the Facts

August 2006

Spyware: Get the Facts

What is spyware?

The Anti-Spyware Coalition (ASC) defines spyware and other potentially unwanted technologies as technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:

- Material changes that affect their user experience, privacy or system security;
- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use and distribution of their personal or other sensitive information.

How does a computer user become infected by spyware?

Spyware occurs through a number of ways, mainly through the user or through software vulnerabilities. This malicious software can be installed on a computer if a user clicks on pop-up windows, downloads free software from unknown sites or clicks on a link in spam to download anti-spyware software. In addition, spyware can often piggyback on legitimate software, installing itself while the legitimate software is downloading. Unlike viruses and worms, spyware does not replicate itself. However, like these malicious threats, spyware exploits computers.

Symantec’s March 2005 Internet Security Threat Report states that “nine of the top 10 reported spyware programs were bundled with other software.”

What is the difference between spyware and adware?

Adware, a threat that is similar to spyware, is defined by ASC as a type of Advertising Display Software that delivers advertising content potentially in a manner or context that may be unexpected and unwanted by users. In addition to displaying numerous annoying ads, many adware applications also perform tracking functions.

What are the symptoms of a spyware infection?

Anyone with an internet connection is at risk of being affected by spyware. In fact, IDC estimates that nearly two-thirds of consumer PCs harbor some form of spyware. While spyware can sometimes reside on a computer with no symptoms, most users will experience some form of interruption. Signs of spyware can include an increase in pop-up advertisements, slowed PC performance and system instability, new search toolbars, hijacked homepage and search results, new items added to the favorites menu, an increase in unwanted network activity and increased disk usage.

What can computer users do to prevent spyware?

To prevent spyware, OnGuard Online, a website that provides practical tips from the federal government and the technology industry, recommends that users:

- Update their operating system and Web browser software, and set their browser security high enough to detect unauthorized downloads.
- Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.

- Download free software only from known and trusted sites. Enticing free software downloads frequently bundle other software, including spyware.
- Do not click on links inside pop-up windows.
- Do not click on links in spam that claim to offer anti-spyware software; users may unintentionally be installing spyware.

What is the impact of spyware on the victims?

A recent survey by the Cyber Security Industry Alliance found that 67% of voters feel that spyware is a serious problem facing consumers today.

There are serious security implications of spyware, or spyware masquerading as adware. Unknowingly, these programs can disable security software and leave users exposed to hackers, viruses and worms. Ramifications of spyware include identity theft, adware, hijacking and many others. Key examples include:

- While downloading an application containing icons for popular IM clients, some bundled adware programs terminate the customer's antivirus and firewall applications, leaving them wide open to viruses and other attacks.

- There are spyware programs that automatically install search toolbars on a user's computers using standard technical mechanisms. The problem is that when users try to manually or programmatically remove the search toolbars, instead of deleting the program's own registry keys, it deletes virtually the entire registry. This renders the entire operating system unusable.

- While installing a supposed IE browser toolbar, a spyware program is installed on the user's computer that hides any files or folders that begin with the same letters as the name of the toolbar such that they are invisible from Explorer, even if Show Hidden Files and Folders is checked under Folder Options.

In many cases, adware programs download and install a host of other adware and spyware programs without the users' consent or knowledge, which leaves computers open to attack.

What legislation has been proposed to address the problem of spyware?

The House of Representative has passed two measures that would protect Internet users from the unknowing transmission of their personally identifiable information through spyware programs. One requires software companies to obtain consent from a consumer before installing software that aggregates information and distributes it to third-parties. The other identifies specific acts as criminal offenses in an effort to discourage spyware.

The Senate passed out of Committee a similar measure that provides the Federal Trade Commission (FTC) with the resources necessary to protect users of the Internet from the unfair and deceptive acts and practices associated with spyware as well as increasing criminal penalties for publishers of potentially unwanted technology.

What does CSIA believe the federal government should do to address spyware?

The Industry has made great strides in addressing spyware through the Anti-Spyware Coalition. However, CSIA encourages Congress to pass legislation to ensure that spyware makers are penalized. CSIA also supports the role of the Federal Trade Commission in protecting consumers from spyware through enforcement actions as well as raising awareness and educating consumers.

In addition, CSIA is working closely with both the public and private sectors to ensure that all issues are explored and discussed before legislation is finalized around these topics.

About the Cyber Security Industry Alliance

The Cyber Security Industry Alliance is the only advocacy group dedicated exclusively to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. Led by CEOs from the world's top security providers, CSIA believes a comprehensive approach to information system security is vital to the stability of the global economy. Visit our web site at www.csialliance.org.

Members of the CSIA include Application Security, Inc.; CA, Inc. (NYSE: CA); Citadel Security Software Inc. (CDSS:OTC); Citrix Systems, Inc. (NASDAQ: CTXS); Entrust, Inc. (NASDAQ: ENTU); F-Secure Corporation (HEX: FSC1V); Fortinet, Inc.; Internet Security Systems Inc. (NASDAQ: ISSX); iPass Inc. (NASDAQ: IPAS); McAfee, Inc. (NYSE: MFE); Mirage Networks; PGP Corporation; Qualys, Inc.; RSA Security Inc. (NASDAQ: RSAS); Secure Computing Corporation (NASDAQ: SCUR); Surety, Inc.; SurfControl Plc (LSE: SRF); Symantec Corporation (NASDAQ: SYMC); TechGuard Security, LLC; and Vontu, Inc.

Cyber Security Industry Alliance
2020 North 14th Street, Suite 750 • Arlington, VA 22201 • (703) 894-CSIA • www.csialliance.org