



Spyware: The Latest Trends

A Special Report by Trend Micro

In the new age of broadband, wireless, and network interconnectivity, there is no stopping the progress of information exchange. Along with connectivity, however, come numerous threats to computer productivity, data integrity, and confidentiality. It is estimated that spyware – unwanted software that invades users' privacy and productivity for monetary gain – infects a majority of all Internet-connected computers.

ISTBar, created by Canadian-based marketing company Integrated Search Technologies (IST), is an example of the powerful new tools currently affecting users. ISTBar is considered by most anti-spyware solution providers to be one of the top emerging spyware and adware threats. The name ISTBar is collectively used for three known variants of IST products: YourSiteBar (yoursitebar.com); Slotchbar (slotchbar.com); and XXXToolbar (xxxtoolbar.com). They all have a common mechanism for managing installation, download of component files, and communication with controlling servers for the execution of pop-up display.

Slotchbar provides surfers with easy and quick Web searching, using IST's search engine and instant access to sites related to dating, games, and shopping, while the Your-SiteBar and XXXToolbar are downloaded through Web sites willing to increase cash flow at the expense of their visitors privacy and productivity.

ISTBar is distributed through an ActiveX installation at different third-party Web sites that provide a variety of MP3 downloads, serials and cracks, game cheats, song lyrics, and adult material. IST forcefully installs its ISTBar IE browser plug-ins by embedding additional Javascript codes that are executed upon loading of the site resulting in automatic ActiveX installation when a surfer visits affiliate sites that distribute IST products.

Trend Micro considers ISTBar to be an unwanted application because of its surreptitious methods of installation and prominent adware behavior.

According to a recent Trend Micro study, adware (a category of overly aggressive marketing threats which includes ISTBar) infected 28 percent of computers worldwide during the period May 14 to June 10, 2006. Spyware is also becoming more pervasive because of the increase in mobile malware, particularly those based on the Symbian OS, and in new inclusions to botnets, which can glean information from various aggressive marketing software as well as long term installation of information-stealing spyware.

"The effects of spyware can be significant," explained Ed English, vice president and chief security strategist at Trend Micro. "On a system with a good deal of spyware/adware installed – there can be dozens of programs on a single system – pop-up ads can be seemingly relentless, and system performance can be brought to its knees."

The impact is clear: spyware programs are much more than a nuisance to end users. The invasion of privacy and threats to users' personal security via the possibility of identity theft caused by spyware constitute a legitimate and serious public concern.

In order to minimize the risk of infection from spyware, users need to understand safe Internet practices, and, by so doing, avoid spyware traps, according to David Perry, global director of education for Trend Micro. "By understanding the magnitude of this threat and changing their behaviors accordingly, users can enjoy a rich online experience, while taking comfort in the safety that they haven't unintentionally opened their computers – and online lives – to people they don't know," he said.

One company, Integrated Search Technologies, with its ISTBar and other spyware is responsible for just over 1% of all infections (viruses, worms, malware, & spyware) cleaned by Trend Micro Housecall – and Trend Micro is only beginning to track all of ISTBar's many third-party distributors.

Most spyware is adware, and, as such, makes its money by showing advertisements or by hijacking web browsers to pages that can generate revenue for its authors. It may be bundled with freeware, or look like legitimate software, with a corresponding End User Licensing Agreement (EULA). Computer security experts at Trend Micro recommend that users carefully read EULAs, and understand just how far-reaching certain provisions can be, prior to clicking the "Accept" button. EULAs often include terms that authorize the software supplier to download and install a range of other software on their systems, without the user's consent. Users should also equip their computers with up-to-date security products – such as PC-cillin – to protect their systems from spyware.

About **Trend Micro Incorporated**

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.