



**By Dave Cole  
Director, Product Management,  
Security Response,  
Symantec Corporation**

### **Are You Winning the War on Spyware?**

Not long ago, most enterprises tended to treat spyware and adware as little more than network nuisances. But times have changed. Today, enterprises everywhere must take swift steps to prevent confidential information from being transmitted to outsiders.

---

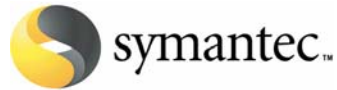
Not that long ago, most enterprises tended to treat spyware and adware as little more than network nuisances. But times have changed. Today, enterprises everywhere must take steps to proactively guard themselves against the significant and growing risk of spyware and adware. This article looks at how blocking these risks at the network level and protecting employee desktops can help prevent confidential information from being transmitted outside the enterprise.

#### **Some definitions**

Because some confusion has accompanied recent discussions of spyware and adware, let's start with some definitions. Spyware refers to programs that have the ability to scan systems or monitor activity and relay information to other computers or locations in cyberspace. Among the information that may be actively or passively gathered and disseminated by spyware are passwords, log-in details, account numbers, personal information, individual files, or other personal documents. Spyware may also gather and distribute information related to the user's computer, applications running on the computer, Internet browser usage, or other computing habits.

Spyware frequently attempts to remain unnoticed, either by actively hiding or by simply not making its presence on a system known to the user. These types of programs can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant message programs. Additionally, a user may unknowingly receive and/or trigger spyware by accepting an End User License Agreement (EULA) from a software program linked to the spyware or by visiting a Web site that downloads the spyware with or without a EULA. Symantec makes a clear distinction between malware threats such as viruses, and possibly undesirable applications such as spyware, which are categorized as "security risks."

Adware refers to programs that facilitate delivery of advertising content to the user through their own or another program's interface. In some cases, these programs may gather information from the user's computer, including information related to Internet



browser usage or other computing habits, and relay this information back to a remote computer or other locations in cyberspace.

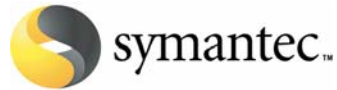
### **Risk assessment**

To help users decide what programs to keep and what to remove from their computers, Symantec designed a risk classification system for rating spyware and adware. This system scores the overall impact of applications in four different categories, providing a final designation of the application as a high, medium, or low risk. The four categories used within the risk classification system are:

- **Performance impact.** System crashes, bogged-down Internet connections, and unusual Web browser behavior all fall into the category of “performance impact,” which measures the effect of a security risk program on a system’s stability, speed, and performance. Programs that score higher in this category can produce wasted hours of troubleshooting, increased calls to the IT help desk, and/or irritating disruptions.
- **Privacy impact.** The privacy impact of a security risk application indicates the extent to which it captures information about users from their behavior for use by a third party (i.e., the spyware or adware company). The information captured by the program ranges from basic Web browsing behavior to sensitive data such as user names and passwords which might be used in conjunction with identity theft or unauthorized transfers from a victim's bank account. Once captured, this information is typically transmitted back to the third party via the Internet.
- **Ease of removal.** Behavior for this category ranges from applications that can be easily removed using a vendor-provided uninstall program to spyware and adware applications that embed themselves deep within the machine and all but refuse to be removed.
- **Stealth.** Stealth behavior ranges from a completely “silent” or unnoticeable installation and concealed operations to programs that inform a user of installation and are easily visible on the machine (i.e., users can see the program’s icons and processes and understand how it arrived on their machine).

### **Prevention and mitigation**

To safeguard themselves against spyware and adware, it is important that users continue to update their antivirus software. Security administrators should also take extra measures to ensure that client system patch levels are up-to-date. In addition, users and administrators should employ defense in-depth, including the use of a properly configured firewall, as well as integrated antivirus and intrusion detection systems. Finally, users should exercise caution when installing any software via a Web browser and never download software from sources that are not known and trusted.



Besides the deployment of defense in-depth, acceptable usage policies should be put in place and enforced. System administrators should regularly audit the system to ensure that no unauthorized software is installed or operating on the system. Furthermore, administrators and end users should read the EULAs of all software programs before agreeing to their conditions.

### **Recent legislative efforts**

Late in May, two bills focusing on spyware overwhelmingly passed the U.S. House of Representatives. The Securely Protect Yourself Against Cyber Trespass Act, or Spy Act, would outlaw the act of taking over a computer in order to send unauthorized information or code, as well as diverting a Web browser without the permission of the computer owner.

The second bill, the Internet Spyware Prevention Act, or I-Spy Act, sets jail terms of up to five years for anyone who uses spyware to access a PC without authorization and uses that computer to commit another federal crime. The I-Spy Act would allow a jail term of up to two years for anyone who uses spyware to obtain someone's personal information or to defeat security protections on a computer with the intent of defrauding or injuring the computer owner.

But as a number of experts have observed, the creation and implementation of spyware and adware will likely continue despite legislation aimed at curbing them. Indeed, such laws are not expected to be effective. The "transboundary" nature of the Internet creates serious jurisdictional issues, particularly as distribution activity may take place in locations not subject to the jurisdiction of such laws. As such, spyware could become more problematic for users, as prosecution will rely on jurisdictional cooperation, which is not always forthcoming.

### **Conclusion**

As the most recent Symantec Internet Security Threat Report noted, spyware and adware continue to be growing concerns:

"Over the last six months of 2004, the percentage of adware in the top 50 malicious code reports to Symantec increased over the first six months of 2004. Between January 1 and June 30, adware made up 4% of the top 50 malicious code reported. Between July 1 and December 31, it made up 5% of the top 50 reports."

This growing concern has put enterprises at greater risk for decreased productivity, more helpdesk calls, loss of privacy, and potential legal liability.

For these reasons, enterprises should give serious consideration to solutions that provide real-time scanning, automatic detection and removal, and integrated tools for remediating the side effects that spyware and adware can have on a user's system.



**Related links**

Spyware Protection from Symantec

<http://enterprisesecurity.symantec.com/content.cfm?ArticleID=5392>

Webcast: “Spyware and Increasing Security Risks”

<http://enterprisesecurity.symantec.com/content/webcastinfo.cfm?webcastid=146>