

The Anatomy of Spyware

By John McCormick

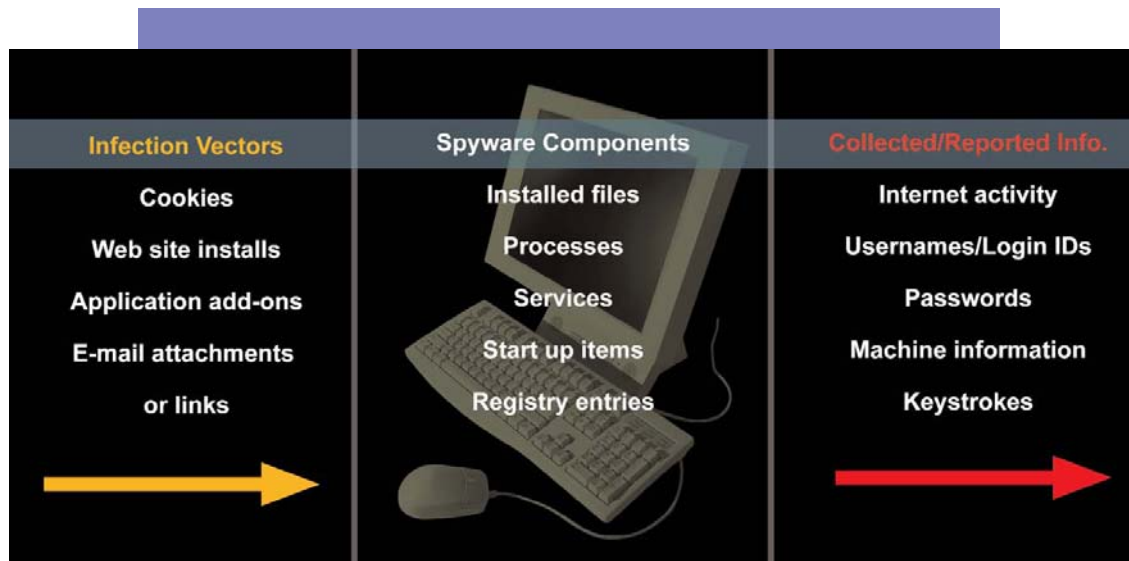


Image layout and design: Kimberly Wright

Image concept: Bill Detwiler

What spyware is

Whether malicious or benign, spyware is software secretly placed on a computer that records and reports user activity.

How you get infected

- **Cookies:** Many legitimate Web sites use cookies to function properly. Malicious Web sites can however use cookies to collect and report user activity for dubious purposes.
- **Web site installs:** Malicious Web sites often disguise spyware as a helpful utility and prompt users to install the spyware when browsing the site.
- **E-mail attachments or links:** As with viruses, spyware can propagate as an e-mail attachment or link.
- **Application add-ons:** Often bundled with popular software, such as peer-to-peer applications, free games, phony spyware removal tools, and the like; May or may not be disclosed during the host application's installation.

Copyright ©2005 CNET Networks, Inc. All rights reserved.

To see more downloads and get your free TechRepublic membership, please visit: <http://techrepublic.com.com/2001-6240-0.html>

Signs of infection

- Unexplainable, reduction in computer performance
- New toolbars appear that can't be permanently deleted
- Excessive, unexplained modem/network traffic
- Dramatic increase in pop-up ads
- Default search engine or browser home page has changed

Spyware removal

- Identify and end suspicious processes with Windows Task Manager.
- Identify and disable suspicious services with the Management Console.
- Identify and disable suspicious services and startup items with the System Configuration Utility.
- Search and delete registry entries associated with suspicious services or startup items.
- Identify and delete suspicious files.
- Install and use multiple spyware detection and removal utilities.

Note: If the above techniques fail, start Windows in Safe Mode and retry.

Spyware prevention

- Regularly apply software patches and updates.
- When possible, configure user accounts without download or install permissions.
- Prohibit the installation and use of unapproved software particularly peer-to-peer, file sharing networks.
- Use only commercial and known-safe utilities.
- Regularly scan machines with antivirus and antispyware programs.
- Use a firewall to restrict outbound traffic on all ports except those used for HTTP, POP3, and SMTP.
- Limit Web surfing to known-safe sites by using a proxy server or restricted sites list.
- Adjust IE's cookie permission settings and security zones as follows:
 - Prompt for first-party cookies
 - Block third-party cookies
 - Always allow session cookies
- Instruct users to close browser windows using the corner "X" or Alt-F4 instead of an "OK" or "Agree" dialog button.

Version 1.0
May 3, 2005

 **TechRepublic**
Real World. Real Time. Real IT.

Additional resources

- Sign up for the [Network Security NetNote](#), delivered on Mondays, Tuesdays and Thursdays
- Sign up for the [TechRepublic White Papers newsletter](#), delivered on Wednesdays
- See all of [TechRepublic's newsletter offerings](#)
- Identify potential spyware and viruses with our [Windows Service Process Identifier script](#)
- [TechRepublic Roadshow: Handling Internal Security Threats](#)

Version history

Version: 1.0

Published: May 13, 2005



John McCormick is a freelance technology writer and editor for multiple online and print publications. He is a member of The National Press Club of Washington and has been a contributing editor/writer to PC Companion, CD-ROM Review, ComputerCraft, Shareware Magazine, ID Systems, Capital Computer Digest, Computer Press (Moscow, U.S.S.R.), was the Macintosh Editor for Vulcan's Computer Monthly, and Senior Editor for both Computer Monthly and Reseller World magazines. John was a major contributor to Computer Shopper. He served as the Washington Bureau Chief for NewsBytes News Network and has also written reviews for PC Magazine.

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team