



realtimepublishers.com™

The Definitive Guide™ To

Controlling Malware, Spyware, Phishing, and Spam

McAfee®
Proven Security™

Dan Sullivan

| | |
|---|----|
| Chapter 4: Spyware and other Potentially Unwanted Programs..... | 66 |
| Varieties of PUPs..... | 67 |
| PUPs..... | 67 |
| Adware..... | 68 |
| Spyware..... | 69 |
| Keyloggers..... | 69 |
| Password Stealers..... | 71 |
| Tracking Cookies..... | 72 |
| Defining Spyware..... | 76 |
| Installation Methods and Effects..... | 77 |
| Concealment..... | 77 |
| Injection..... | 77 |
| Payload Types..... | 78 |
| Spyware and other PUP Behaviors..... | 79 |
| File Scanning..... | 79 |
| Reading Cookies..... | 79 |
| Changing Browser Settings..... | 80 |
| Installing Browser Help Objects..... | 81 |
| Malware vs. Malware..... | 82 |
| Impact of Spyware..... | 82 |
| Reduced Computing Performance..... | 82 |
| Performance Effects of Monitoring..... | 83 |
| Number of PUPs..... | 83 |
| Loss of Proprietary and Confidential Information..... | 84 |
| Help Desk Costs..... | 84 |
| Summary..... | 85 |

Copyright Statement

© 2006 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.


[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimerepublishers can be found at <http://nexus.realtimerepublishers.com>.]

Chapter 4: Spyware and other Potentially Unwanted Programs

Spyware is a type of Potentially Unwanted Program (PUP) that monitors users' online behavior as well as performs other tasks, which this chapter will explore. As with other forms of malware, the use of spyware has increased and studies have shown it affects large numbers of Web users. The pervasiveness of spyware is not limited to a particular segment of the population or to particular types of Web users; it is a problem for home users as well as businesses and other organizations that support large numbers of users.


In the case of home users, a 2004 survey by America Online (AOL) found that 80 percent of the systems survey contained at least one known spyware program. (It also found that 20 percent of those systems hosted a virus). Compounding the problem is a lack of understanding about the issue.

In the AOL survey, two-thirds of respondents felt their computer was safe from online threats. A 2005 survey from the Pew Internet and American Life Project found similar confidence in users' ability to stop potentially unwanted programs. The Pew survey found that 61 percent of home users felt very or somewhat confident that they could keep malware, as well as spyware, off their computers.

 For more details about the AOL and Pew surveys, see "AOL Survey Finds Rampant Online Threats, Clueless Users" at <http://www.computerworld.com/securitytopics/security/story/0,10801,96918,00.html> and "Spyware Survey" at http://www.pewinternet.org/pdfs/PIP_Spyware_MayJune05_Qs.pdf.

The spread of spyware in corporate environments is comparable to that found in home users. Leading anti-spyware vendors are finding increasing numbers of spyware getting installed on users' systems. For example:

- The McAfee Anti-Virus Emergency Response Team (AVERT) Labs witnessed a 12 percent rise in spyware incidents from the first quarter to the second quarter of 2005 and a 60 percent increase since the first quarter of 2004.
- According to a WebRoot survey of enterprise clients, 88 percent of enterprise computers had instances of spyware on them in 2005.
- The problem is also manifesting itself at the Help desk. Twenty percent of support calls to Dell in late 2004 were spyware related, which is an increase of 12 percent from earlier in the year.

 For more information about the state of spyware in corporate environments, see "McAfee AVERT Reports Top 10 Threats for 2004 and Advises on Future Threats and Trends" at http://www.mcafee.com/us/about/press/mcafee_enterprise/2005/20050103_093758.htm, "Spyware: A Customer Relations Problem" at <http://www.technewsworld.com/story/40419.html>, "Dell Spyware Decision Spurs New Trend" at <http://www.crbuyer.com/story/37668.html>, and "First State of Spyware Report Shows Bad Guys Winning" at <http://www.technewsworld.com/story/42844.html>.

Fortunately, there appears to be more awareness of PUPs in organizations than among home users. According to an *Information Security* survey, countering spyware is a top security priority for the next 18 months for more than two-thirds of respondents.

This chapter will delve into the details of PUPs—how they threaten information security and what can be done about it. The discussion is divided into three areas:

- Varieties of PUPs
- PUP behaviors
- Impact of PUPs

Let's begin with a look at examples of PUPs before developing a more formal definition.

Varieties of PUPs

PUP is a general term for a broad class of programs that include:

- Adware
- Spyware
- Monitoring programs
- Keyloggers
- Password stealers
- Tracking cookies

Although these types of PUPs are distinct, some features may overlap. Just as viruses and worms have evolved into multifaceted threats, known as blended threats, a single spyware application may contain multiple components. To better understand these various types of programs, let's look at an overview of the broader class of PUPs.

PUPs

The Internet is a distributed computing platform that allows relatively easy access to a wide array of information and services. It also provides a direct line into vulnerable systems that can become infected with a variety of PUPs. PUPs are programs written for a seemingly legitimate purpose that alter the security or privacy posture of a computer on which it is installed. PUPs may be distributed as standalone programs or may be included with popular types of applications and file types. For example, PUPs can be:

- Peer-to-peer file-sharing clients
- Screensavers
- Utilities, such as clock synchronization programs
- Browser toolbars


These vectors, or methods of distribution, can be used to carry a number of different types of PUPs.

Adware

Adware is a common type of PUP whose primary function is to derive advertising revenue for a third party. Adware can deliver pop-up and pop-under advertisements and banner ads in addition to tracking Web activities. Widely deployed adware programs include:

- Gator
- 180SearchAssistant
- BonziBuddy
- GAIN

Gator from Claria Corporation is one of the best-known programs in the area of “online behavioral marketing,” in which the online habits of users are tracked and used to profile user interests and target advertising to those interests. If users knowingly agree to allow the installation and use of monitoring programs on their computers, the application may be categorized as adware.

 No one likes to read End User License Agreements. They are long, legalistic, and often incomplete; but they are worth reading if you are downloading a freeware or shareware program that may be used to install adware. This type of download can include just about any utility or popular program, but not all free programs are spyware. When in doubt, read the End User Agreement or pass on the program and do not download it.


In addition to the behavioral marketing monitoring programs, homepage hijackers also fall into the adware category of PUPs. These programs modify home page settings to redirect browsers to a particular page, thus boosting the number of hits on that page. In general, manually resetting the home page property in a browser only works temporarily because the home page hijackers will change it back again.

One of the ways home page hijackers work is by adding an entry to the Run registry keys in Windows. In Windows NT 4.0, Windows 2000 (Win2K), Windows XP, and Windows Server 2003 (WS2K3) the keys are:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Every time the system starts, the commands listed in the \Run registry setting are executed. The home page hijacker inserts a command into the entry that causes the home page setting to be reset. Home page hijackers can be overcome by deleting those registry entries.

In other cases, hackers have exploited a vulnerability in Internet Explorer (IE) whereby they use HTML Application files (.hta) to install ActiveX components when a user browses a site. When an .hta-based home page hijacker infects a system, users can search for and remove any unauthorized .hta files to clean up the problem.

 HTML Application is a Microsoft proprietary protocol and works only with IE. Other browsers, such as Mozilla Firefox and Opera, are not vulnerable to this threat. Microsoft has provided a patch for this vulnerability.


Of course, home page hijackers can enter a computer as part of the payload in a blended threat and use injection methods commonly seen by viruses as well.

Spyware

Spyware is software that gathers personally identifiable information about a computer's user and delivers that information to a third party. Spyware is often distributed with adware, but may also be downloaded while browsing sites that download unwanted software along with Web content.

In some cases, software distributors openly admit to deploying data collection software or programs that utilize computing resources on client machines. Companies, such as Brilliant Digital Entertainment, have openly admitted to downloading programs for the purpose of using computing and storage resources of users of the company's program.

For example, in their 2002 SEC filing, the company described an installer that would be downloaded along with the popular Kazaa peer-to-peer file-sharing system client as "components [that] help facilitate the delivery of files—ad banners, music files, documents, software files, etc.—across the network. Apart from facilitating Altnet SecureInstall connectivity, the Installer is a full-fledged software installation system, with key features including file compression, file patching, and file encryption." Spyware can be a component in a more sophisticated distributed application.

 See the full text of Brilliant Digital Entertainment's 2002 SEC 10KSB filing at <http://www.sec.gov/Archives/edgar/data/1022844/000101143802000252/0001011438-02-000252.txt>.

Once a spyware program is on a computer, there are a number of methods for stealing information. One of the most dangerous is the use of keyloggers.

Keyloggers

Keyloggers are programs that record every keystroke, allowing the user of the keylogger to acquire usernames, passwords, account numbers, and other identifying information (see Figure 4.1). Because the keyboard is the primary vehicle for user data entry, virtually no application is safe from this eavesdropping mechanism. In addition, data does not even have to be saved. An email can be typed but never sent, a word processing document edited and then discarded, or a username and password entered but then cancelled—the information could still be captured by a keylogger program.

Applications that demand high security have tried countermeasures such as visual keyboards to circumvent keyloggers. With visual keyboards, a display of a keyboard appears on the screen and users click the mouse over images of the keys. As we could have expected, keyloggers have evolved to include more sophisticated features, such as capturing screenshots and recording the names of windows and Web sites visited along with timestamps for these activities.

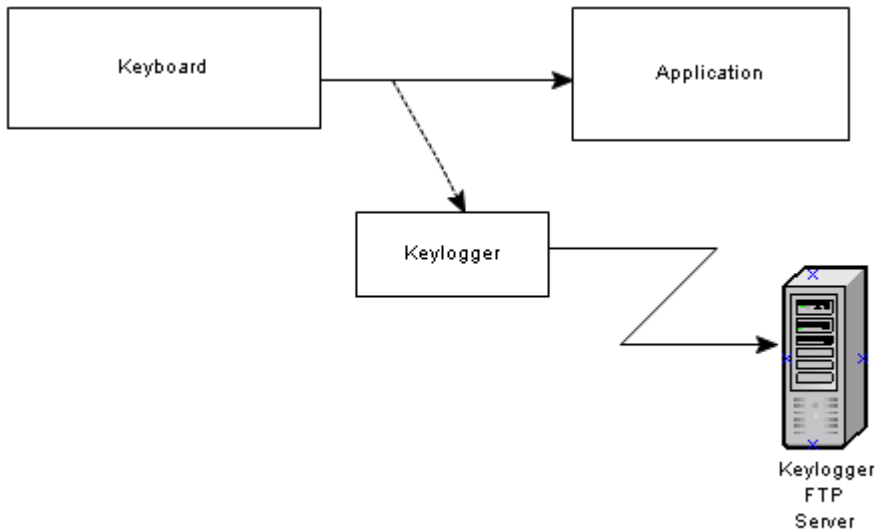



Figure 4.1: Keyloggers intercept communications between the keyboard and applications and send collected information to attacker-controlled servers, such as FTP or other collection servers.

Unlike other PUPs, not all keyloggers are used by attackers:

- Commercial keyloggers are sold to consumers as tools for monitoring children's and other family members' activities online
- Keyloggers are used by software developers to help diagnose software bugs
- The FBI has disclosed that it has developed and used a keylogging program known as Magic Lantern to retrieve encryption passcodes of suspects

 For more information about the FBI's disclosure on Magic Lantern, see "FBI Software Cracks Encryption Wall" at <http://www.msnbc.com/news/660096.asp?0na=x21017M32&cp1=1>.

 It should be noted that the keyloggers used by spyware are software-based devices. Hardware devices have also been developed as well. When they are installed between the keyboard cable and computer keyboard port, they capture and record keystrokes.

In some cases, PUPs are not designed to steal information but to use others' computing resources. One of the simplest PUPs of this type drives up the number of visits to a Web site.

Password Stealers

Password stealers are programs that read the text of passwords transmitted to applications and send them to a site where they are collected by the attacker. Hiding the characters in a password, as Figure 4.2 shows, is common but ineffective against these programs because the programs do not depend on reading what is displayed in the box, only what is transmitted from the client to the application.

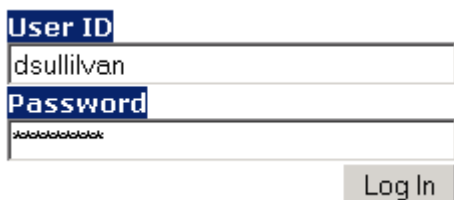


Figure 4.2: Masking the characters in passwords does not prevent password stealers, which detect characters as they are sent from the keyboard to the application.

Password stealers are specialized forms of keyloggers. Both types use hooks in the operating system (OS) to detect keyboard events and record keystrokes.

Password stealers are evolving in a cat-and-mouse fashion. To avoid keyboard vulnerabilities (such as the SetWindowsHookEx function described shortly), some applications have deployed visual keyboards. Rather than type on the keyboard, users click on an image of a keyboard on the screen. The input program then uses the position of the mouse click to determine which character was selected.

Although visual keyboards avoid the problem of intercepted key strokes, they have similar limitations. In particular:

- Mouse events can be intercepted as are key strokes
- Screenshots can be captured making a recording of the mouse position over the visual keyboard.

Password stealers are a substantial threat to information security. Comprehensive policies on using strong, difficult-to-crack passwords, changing passwords frequently, and not sharing passwords are all moot once a password stealer has captured a username and password. One way to detect unwanted programs that startup automatically is to use a startup program reporting tool, as Figure 4.3 shows.

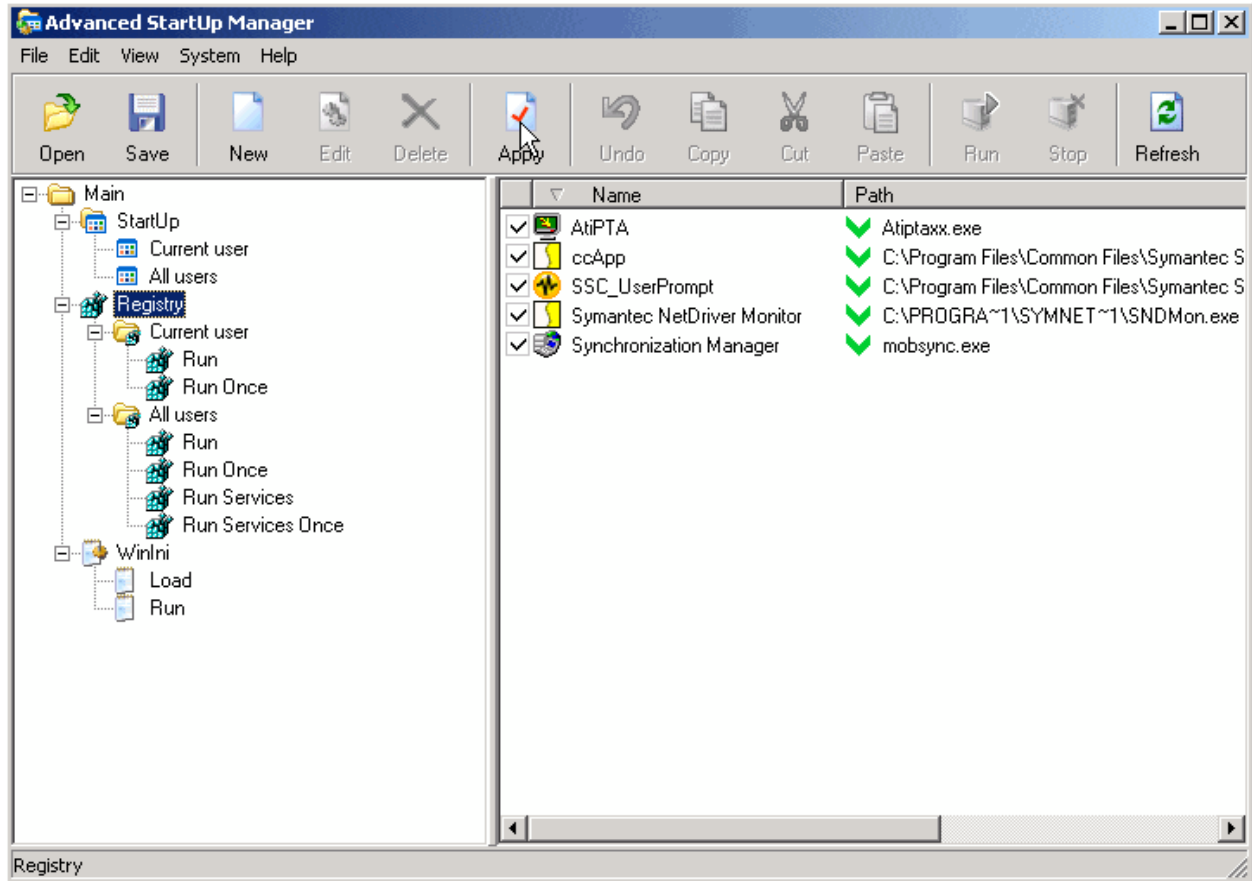


Figure 4.3: Utilities, such as a startup program reporting tool like Advanced Startup Manager, can help to identify programs set to auto start in the registry.

⚠ Be aware that some complex malware, known as root kits, can hide the existence of running processes. Less sophisticated malware can be identified with utilities.

Tracking Cookies

Cookies are text files used by browsers to record information locally. Cookies are used for a number of reasons, including:

- Personalizing preferences
- Remembering passwords
- Keeping track of a program state in Web applications
- Tracking user activities online

The first of these are legitimate uses of cookies; the final reason, tracking activities, can have legitimate uses but not always.

Personal Preferences

Personal preference cookies allow users to customize the look and feel of sites. For example:

- News sites may allow readers to rearrange the layout of news sections and can record those preferences using cookies.
- Web portals use cookies to record physical address information allowing the portals to display weather and other topics of local interest.
- E-commerce sites use cookies to remember account numbers, language preferences, and other information about cookies.

Typically, personal preference cookies are used for the convenience of the site visitors and do not collect personal information.



When in doubt about the information tracked in personal preference cookies, consult a site's privacy policy.

Remembering Passwords

Cookies are also used to remember passwords for Web sites and Web-based applications. Online newspapers, for example, often ask readers to create accounts and provide basic demographic information. For convenience, many readers will have the site save their login information.



Saving passwords in cookies is obviously a security risk and should only be used if the disclosure of the password would not compromise private information. Passwords to online bank accounts, brokerage accounts, health insurance plans, or other sites dealing with financial or confidential information should never be saved in cookies. When in doubt, do not select any option to save passwords.

Tracking Program State

One of the advantages of HTTP, the protocol underlying Web pages and many Web application interfaces, is its simplicity. It is also one of its drawbacks. A common problem in any application design is keeping track of what the user has done and where the user is in the overall process of the application. This is known as maintaining “state.”

When programmers developed applications for mainframes or client/server applications, maintaining state was relatively easy. The program would have a single channel of communication between the user and the application.

When applications moved to the Web, they no longer had a single channel of communication when using HTTP. Every message sent from a Web server or a browser was independent of other messages. Developers use cookies to save information in the browser so that it can re-use that information in later messages. For example, if a user adds an item to a shopping cart, it can be stored in a cookie and read when the user decides to check-out. The information is not lost if the user decides to browse for other items.

Tracking User Activity Online

Tracking user activity online is a commonly used technique by online advertisers. Regardless of whether the user approves, the purpose is to record events, such as visits to particular sites, and analyze patterns in usage.

This information is then used to target ads to users with particular interests. For example, if someone browses sites on hiking, mountain biking, and national parks, that person is a likely target for backpacking products. Studies have demonstrated that targeting ads based on behavioral profiling is more effective than non-targeted online advertisement, so tracking online user activity is not likely to diminish.

 For details of one study on the behavioral marketing's impact on revenue, see "Behavioral Targeting Study Reveals CPM Lift" at <http://www.clickz.com/news/article.php/3396431>.

Keeping track of cookies, and just knowing what is on a computer, can be a daunting task. Browsers have a number of tools for managing cookies, including privacy settings. A few simple steps can give users better control and information about cookies:

- Selectively disabling cookies from particular sites
- Setting browser security options to disable cookies in certain circumstances
- Using browser audit tools to review information collected and maintained by browsers

For example, Mozilla Firefox provides the ability to remove specific cookies and disallow future cookies from being set from the sites that have had their cookies removed (see Figure 4.4).

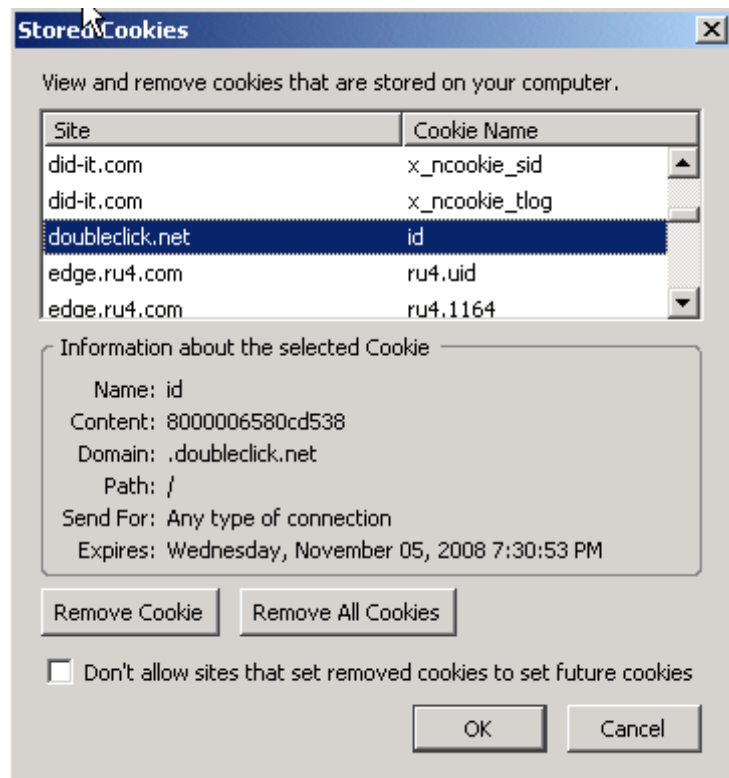


Figure 4.4: Mozilla Firefox allows users to view details of cookies as well as to remove and control the resetting of cookies.

IE provides general levels of cookie control and allows users to define custom configurations for handling cookies from first party as well as third-party sites (see Figure 4.5). A first-party site is one intentionally visited by a user; third-party sites are sites that the user did not directly navigate to but were contacted on behalf of the user by the first-party site. Third-party sites include Web-tracking sites and behavioral-monitoring sites.

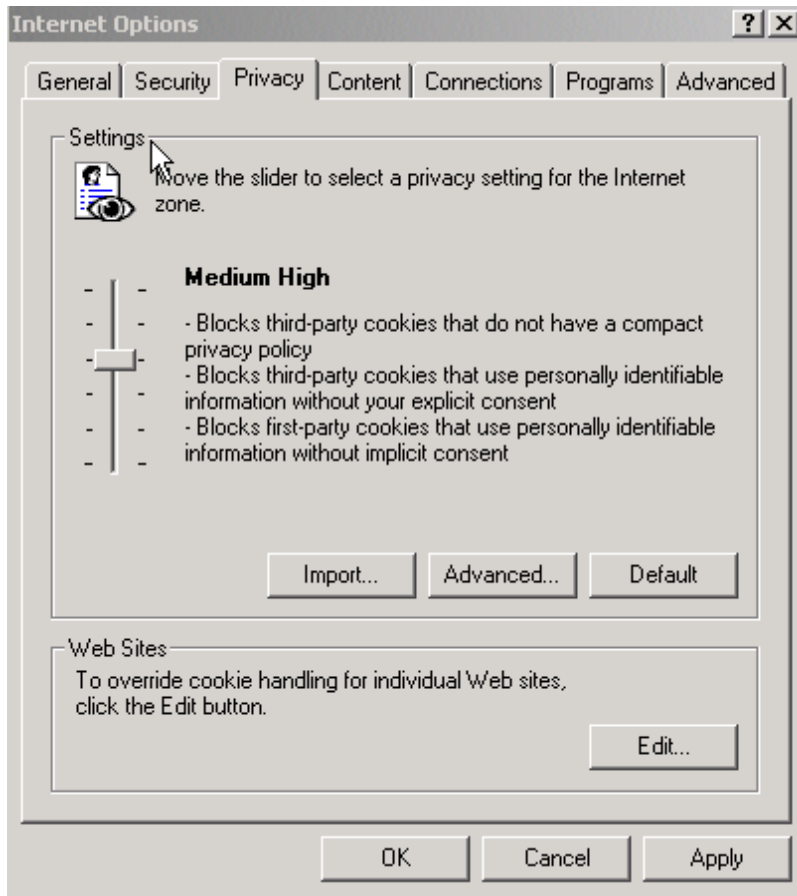



Figure 4.5: IE allows users to choose from predefined sets of cookie controls or to configure their own set through the Advanced option.

In addition to browser settings, third-party tools are widely available for examining cookies, browser history, caches, and related information stored in browsers.

It should be assumed, for security purposes, that any information stored in a browser is accessible to spyware, particularly tracking software. Cache and cookie audit tools (such as the one that Figure 4.6 shows) can be used to monitor information maintained by browsers. Other types of cookie-management utilities include cookie-removal tools, and real-time cookie blocking.

 Cookie management features vary by browser, so features in Mozilla Firefox may not be available in IE and vice versa.

| URL | Filename | Hits | Size (Bytes) | Last Modified | Last Access |
|---|--|------|--------------|------------------------|------------------------|
| Cookie.dsullivan@burstnet.com/ | \\dsullivan@burstnet[2].txt | 2 | 148 | 7/28/2005 10:23:48 ... | 7/28/2005 10:23:48 ... |
| Cookie.dsullivan@ca.com/ | \\dsullivan@ca[1].txt | 6 | 134 | 5/4/2005 7:19:29 PM | 10/6/2005 5:47:12 P... |
| Cookie.dsullivan@centrport.net/ | \\dsullivan@centrport[1].txt | 10 | 88 | 6/13/2005 7:09:56 P... | 11/3/2005 6:57:21 A... |
| Cookie.dsullivan@chatboards.ebay.com/ | \\dsullivan@chatboards.ebay[1].txt | 2 | 104 | 5/11/2005 4:00:21 P... | 5/11/2005 4:00:29 P... |
| Cookie.dsullivan@cheats.gamespot.com/ | \\dsullivan@cheats.gamespot[2].txt | 9 | 226 | 8/27/2005 10:42:32 ... | 8/27/2005 10:42:32 ... |
| Cookie.dsullivan@choicehotels.com/ires | \\dsullivan@ires[2].txt | 4 | 258 | 7/31/2005 11:06:09 ... | 8/9/2005 7:07:34 AM |
| Cookie.dsullivan@cisco.com/ | \\dsullivan@cisco[1].txt | 1 | 97 | 9/5/2005 11:02:39 A... | 9/5/2005 11:02:39 A... |
| Cookie.dsullivan@citi.bridgetrack.com/ | \\dsullivan@citi.bridgetrack[1].txt | 34 | 1280 | 8/5/2005 5:01:17 PM | 8/5/2005 5:01:17 PM |
| Cookie.dsullivan@click.theonion.com/ | \\dsullivan@click.theonion[1].txt | 11 | 178 | 10/12/2005 3:52:46 ... | 10/12/2005 3:52:46 ... |
| Cookie.dsullivan@cnn.122.2o7.net/ | \\dsullivan@cnn.122.2o7[1].txt | 7 | 131 | 10/22/2005 7:47:06 ... | 10/22/2005 7:47:06 ... |
| Cookie.dsullivan@cnn.com/ | \\dsullivan@cnn[2].txt | 7 | 177 | 10/22/2005 7:47:05 ... | 10/22/2005 7:47:05 ... |
| Cookie.dsullivan@cnaudience.com/ | \\dsullivan@cnaudience[1].txt | 2 | 102 | 7/22/2005 2:17:40 P... | 8/5/2005 4:50:48 PM |
| Cookie.dsullivan@com.com/ | \\dsullivan@com[1].txt | 13 | 311 | 10/28/2005 1:33:55 ... | 11/3/2005 6:56:16 A... |
| Cookie.dsullivan@commons-services.novartis.com/ | \\dsullivan@commons-services.novartis[1].txt | 1 | 95 | 6/18/2005 12:20:55 ... | 6/18/2005 12:20:55 ... |
| Cookie.dsullivan@creativeby.viewpoint.com/ | \\dsullivan@creativeby.viewpoint[1].txt | 7 | 152 | 7/22/2005 9:28:04 P... | 7/22/2005 9:28:04 P... |
| Cookie.dsullivan@data.coremetrics.com/ | \\dsullivan@data.coremetrics[1].txt | 2 | 101 | 8/12/2005 11:06:23 ... | 8/12/2005 11:31:55 ... |
| Cookie.dsullivan@dealtime.com/ | \\dsullivan@dealtime[1].txt | 1 | 100 | 4/28/2005 10:52:49 ... | 4/28/2005 10:52:49 ... |
| Cookie.dsullivan@dell.com/ | \\dsullivan@dell[1].txt | 2 | 81 | 4/2/2005 7:32:56 AM | 4/13/2005 4:20:02 P... |
| Cookie.dsullivan@delta.com/ | \\dsullivan@delta[1].txt | 5 | 80 | 4/12/2005 9:21:35 P... | 8/25/2005 10:40:47 ... |
| Cookie.dsullivan@did-it.com/ | \\dsullivan@did-it[2].txt | 2 | 285 | 8/6/2005 10:03:10 A... | 8/6/2005 10:03:10 A... |
| Cookie.dsullivan@dist.belnk.com/ | \\dsullivan@dist.belnk[2].txt | 2 | 186 | 7/17/2005 8:06:42 A... | 7/17/2005 8:06:42 A... |
| Cookie.dsullivan@dogpile.com/ | \\dsullivan@dogpile[1].txt | 1 | 100 | 6/26/2005 2:52:05 P... | 6/26/2005 2:52:05 P... |
| Cookie.dsullivan@doubleclick.net/ | \\dsullivan@doubleclick[1].txt | 17 | 83 | 8/3/2005 9:47:58 PM | 10/22/2005 7:46:59 ... |
| Cookie.dsullivan@ebay.com/ | \\dsullivan@ebay[2].txt | 195 | 1065 | 5/11/2005 4:01:13 P... | 8/27/2005 8:12:48 A... |
| Cookie.dsullivan@edge.ru4.com/ | \\dsullivan@edge.ru4[1].txt | 33 | 1286 | 6/27/2005 2:04:10 P... | 7/10/2005 9:08:02 A... |
| Cookie.dsullivan@ehg-airtran.hitbox.com/ | \\dsullivan@ehg-airtran.hitbox[1].txt | 16 | 1068 | 8/4/2005 1:27:58 PM | 8/4/2005 1:27:58 PM |
| Cookie.dsullivan@epinions.com/ | \\dsullivan@epinions[1].txt | 1 | 99 | 5/6/2005 3:50:48 PM | 5/6/2005 3:50:48 PM |

Figure 4.6: Cookies are not easily segregated by function. Personalizing cookies as well as tracking cookies are not distinguished by browsers. (Screenshot of STG Cache Audit, a shareware utility available at <http://www.stgsys.com/audit.asp>.)

Defining Spyware

Perhaps the most well known form of PUP is spyware. This guide follows the criteria used by McAfee's anti-spyware researchers Prabhat K. Singh, Fraser Howard, and Joe Telfatici in their article "How Dare You Call it Spyware" published in the *Virus Bulletin*, December 2004 to define spyware.

📖 "How Dare You Call it Spyware" and related research, is available online at <http://www.virusbtn.com>.

Singh, Fraser, and Telfatici categorize spyware, and malware in general, according to six criteria:

- Installation methods and effects
- Concealment
- Injection
- Payload

The combination of structural and functional attributes provides a reasonable approach that should minimize otherwise unhelpful debates about what constitutes spyware and other PUPs.

Installation Methods and Effects


Installation programs change a device by installing code in such a way that it executes each time the system is restarted or when some predefined system event occurs. The program may be run by several methods, including:

- Adding a system service that starts when the computer is rebooted
- Employing COM objects that store startup information in the system registry
- Using Browser Helper Objects in IE
- Adding an entry to one of the two registry settings that control the automatic execution of programs during system startup
- Using network-level intercepts that redirect traffic to spyware-related sites

Each of these techniques changes either a system configuration or the functioning of a core component of the OS, usually without the user's knowledge.

Concealment

PUPs use many methods to hide their existence. The goal, of course, is to prevent detection and removal from a machine. Virus writers have created a number of techniques for changing the structure of a program without changing its behavior, which can be adopted for spyware.

 For more information about concealment techniques, see Chapter 3.


In addition to masking code, spyware writers may change registry entries to avoid detection. COM objects, for example, use globally unique identifiers (GUIDs), which are long strings of characters. These can be randomly changed on each installation to prevent anti-spyware programs from matching registry entries based on those character strings.

Injection

Injection is the process of inserting code into an executable object, such as another program. Some ways to accomplish this are:

- Inserting registry entries in such a way as to force a dynamic link library (DLL) to load in memory when the system starts
- Using the Windows system function SetWindowsHookEx function, which allows applications to monitor system events, such as keyboard events
- Injecting an execution thread in another process, such as IE

Spyware can use any of these techniques but the last is usually used.

 OS hooks are powerful tools for programmers but are dangerous on vulnerable systems. Hooks are designed to intercept messages between components, such as the keyboard and an application, and carry out additional activities. Hooks in the Windows OSs allow programmers to carry out tasks on keyboard and mouse events when the foreground task is not utilizing system resources and at other times as well. For technical details on Windows OS hooks, see the Microsoft Developers Network at <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winui/winui/windowsuserinterface/windowing/hooks.asp>.

Payload Types

Payload is the part of a PUPs that carries out the program's core function, such as doing something to the host computer, communicating data to third parties, or receiving commands from third parties. Although much of the code of a virus, worm, or spyware program may be designed to control installation and concealment, the payload is the portion that delivers the core functions intended by the spyware writer.

Host payloads are program components that change the behavior of the host. This change can include:

- Displaying banner ads
- Intercepting and redirecting URLs
- Consuming computer and storage resources
- Monitoring Web browsing activities

Network payloads transmit information to and from the host computer. Viruses, worms, Trojan horses, and blended threats may establish connections to servers controlled by their program's developers to download updated payloads, receive instructions to carry out particular tasks—such as distributing spam, or initiate a Denial of Service (DoS) attack on a third-party site. Spyware typically sends information about user behaviors and activities back to a central server. Table 4.1 provides a summary of malware characteristics displayed by spyware.

| Malware Characteristic | Use in Spyware |
|----------------------------------|---|
| Installation methods and effects | COM objects, Browser Help Objects, and network intercepts |
| Survey techniques | Not used in spyware |
| Replication methods | Not used in spyware |
| Concealment | Use techniques developed for viruses; randomly generate GUIDs |
| Injection | Often inject code into IE process |
| Payload type | Both host- and network-based payloads |

Table 4.1: Spyware can be identified using the criteria defined by McAfee's malware researchers.

With an understanding of criteria used for classifying spyware according to its structure and function, you can turn your attention to more specific spyware behaviors.

Spyware and other PUP Behaviors

PUPs can conceal themselves and carry an undesirable payload. Beyond the fact that their presence constitutes a risk, there are specific behaviors that are common to PUPs:

- Monitoring keystrokes
- Scanning files
- Reading cookies
- Changing browser and registry settings
- Installing Browser Helper Objects
- Capturing screenshots

Keystroke monitoring has already been discussed; the remaining behaviors are addressed in the following sections.

File Scanning

Once in place on a computer, spyware can set about its work of collecting information. This task is often done by monitoring activities but can also be accomplished by scanning existing data for sensitive information including:

- Usernames and passwords
- Account numbers
- Personally identifying information, such as Social Security numbers
- Potentially proprietary files, such as computer aided design files

File scanning is the general process of searching for information but can also be more targeted as with cookie reading.

Reading Cookies

Cookies are tied to a single Web site. Only the Web site that places the cookie is able to read it from within an HTML page. This setup allows Web site designers to maintain the privacy and integrity of their cookies. The obvious irony notwithstanding, it also serves to protect the interest of users who cannot have their browsing habits analyzed simply by reading all cookies on a computer (advertisers have found other ways; see the sidebar “Large-Scale Web Activity Monitoring”).

For spyware/adware writers, cookies are an obvious wealth of information. Users’ interests are documented in cookies. Spyware authors do not even have to know the structure of a cookie, just knowing the names of Web sites allows for profiling. Web directories such as Google Directory, Yahoo Directory, and the Open Directory Project hierarchically organize myriad Web sites so that spyware writers do not even need to maintain their own database of Web site categories for profiling.

Large-Scale Web Activity Monitoring

Spyware is not the only way to monitor users' online activity; in fact, advertising companies such as DoubleClick have been quite successful in tracking users without the use of spyware. Rather than place an unwanted program on a user's computer, Web advertisers work with Web sites to deploy links to small, transparent image files (1 × 1 pixel) hosted by the advertiser. These links are embedded in target pages on a Web site. When a browser downloads one of those pages from the target Web site, the transparent image is downloaded from the advertiser's server. When that happens, the advertiser is able to capture information about the browser downloading the image.

Changing Browser Settings

Another common activity for spyware is to change browser settings. Security settings and configurations are often targeted. Security settings in browsers control several aspects of browsing behavior, including:

- History tracking
- Saved form information
- Saved passwords
- Cookie controls (see Figure 4.7)
- Enabling and disabling Java, JavaScript, and ActiveX controls
- Allowing Web applications to install software on the local computer

Spyware may change feature settings that would not allow it to function, such as running ActiveX controls or other plug-ins. A common problem with spyware is that it changes browser settings, such as when homepage hijacking occurs (described earlier).

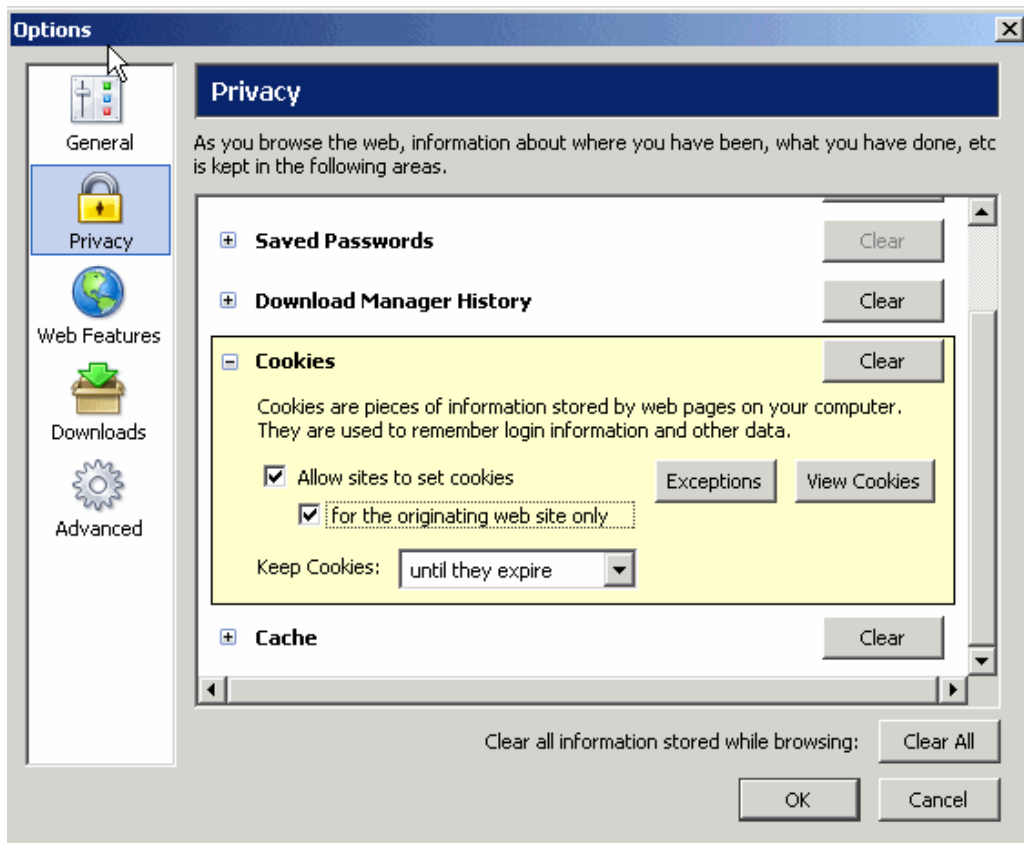



Figure 4.7: Firefox provides a mechanism to control the use of third-party cookies by allowing users to specify that cookies are allowed only for the originating Web site.

Installing Browser Help Objects

Browser Help Objects are plug-ins designed to extend the functionality of browsers. Like so many security vulnerabilities, this one started as a good idea, which has been exploited. Typical behaviors of Browser Help Objects include:

- Installing unwanted search assistant toolbars
- Displaying banner ads
- Redirecting homepages
- Displaying pop-up and pop-behind ads

In addition to exhibiting these unwanted behaviors, Browser Help Objects can be difficult to remove and sometime requires editing the Windows registry.

 It should be emphasized that not all Browser Help Objects are currently considered spyware. Google Toolbar and the Adobe Acrobat reader plug-in for IE are implemented as Browser Help Objects.

Malware vs. Malware

In addition to the other behaviors typical of PUPs, recent trends in malware behavior include commandeering other malware. Some examples noted by malware researchers at McAfee include:

- Adware that removes other adware
- Viruses that remove other viruses
- Blended threats that distribute spyware
- Bot armies commandeered by other malware
- Malware shutting down firewalls and antivirus software
- Malware changing browser security settings

Corporate and home computers are becoming something of prizes in what amounts to a cyber turf battle. Compromised computers are valuable resources and attackers are becoming more creative in their methods for capturing and maintaining at least some control over them.

Impact of Spyware

The impact of spyware on business operations falls into three general categories:

- Reduced computing performance
- Loss of proprietary and confidential information
- Help desk and recovery costs

Reduced Computing Performance

Hardware vendors promote the speed of their processors, data buses, disk drives, and just about every other component within a PC. This promotion is not surprising, when so many users are putting more demands on their systems. Applications are more complex and users are running more of them. It is not unusual for a user to have multiple programs open at once, including:

- Email
- Instant messaging
- Office applications, such as word processing and spreadsheets
- Online meeting/conferencing software
- Web browsers
- Database applications
- Image editing programs

Memory-intensive programs can fill RAM to capacity, which forces paging of data to disk, slowing response times. Computing-intensive programs, such as computer aided design, can consume available CPU cycles. Large downloads can consume bandwidth. The result is a sluggish system and an unhappy user.

Spyware, like other programs, will consume resources as well. Although writing data to files and copying files back to a central server can use some disk and bandwidth resources, one especially problematic practice of spyware is the way in which it monitors activities.

Performance Effects of Monitoring

Windows OSs provide the ability to trigger specialized processing when a particular event occurs, such as a key being typed or a window moved. (This action was discussed earlier with regard to keylogging.) These specialized triggers are known as hooks.

Hooks have legitimate uses but they slow processing even when designed carefully. For example, when a window is opened on the desktop, messages are sent among various components of the OS to create a window data structure and display it on the screen. Imagine if a spyware program inserted a hook to intercept window open messages so that every time a window was opened, the following tasks were executed:

- Determine the application opening the window.
- If the application is Outlook Excel or Word then
 - Record the time of the window open event in a log file
 - Capture a screenshot of the window
 - Save the screenshot to a file

This one program alone could slow a system by consuming memory and writing large amounts of data to the disk. This type of video frame grabbing is one way to steal proprietary information and conduct industrial espionage. In addition to the overhead of monitoring, the number of spyware applications on a computer will influence the overall impact.

Number of PUPs

The second factor in the performance impacts of spyware and other PUPs is the number of these programs running on a system. A single program may have negligible impact on performance, but when the number climbs to half a dozen or more, the drain on system resources can become noticeable.

Loss of Proprietary and Confidential Information

Another impact of spyware is the loss of proprietary or confidential information. Proprietary business information—such as sales plans, customer lists, and design documents—can be easily copied to a remote FTP server by spyware or other malware without the knowledge of the owner. Even when malware is detected, it may not be clear what information is compromised.

Another concern is the loss of personal information, especially Social Security numbers, account numbers, and other information that can be used for identity theft or online fraud. Online transactions are not always insured against fraud, so recovering lost funds can be challenging in the best of cases.

Know Your Online Agreements

Many people believe that if someone steals their credit card information and makes fraudulent charges or forges checks in their name, their liability is limited. Such is not always the case and it certainly is not necessarily the case with online transactions. *USA Today* reported two enlightening examples of online fraud: one involved a commercial bank account and the other a personal retirement account.

The first case involved a business owner who lost \$20,000 after a cyber criminal managed to transfer more than \$90,000 from the businessman's account into a third-party account. A cash withdrawal of \$20,000 was made the next day before the funds could be restored. It was later learned that a Trojan horse program called Coreflood had captured and transmitted the businessman's account name and password to the thief or an accomplice. The bank refuses to compensate for the loss claiming its safeguards were in place and since this was a business account, it is governed by the Uniform Commercial Code, which limits online service provider liability.

In the second case, a man discovered a thief was in the process of selling \$60,000 worth of stock from his online brokerage account. The man alerted the brokerage firm, which stopped the trade. The victim was later informed that the brokerage's actions were a "one-time courtesy" and that in the future he would be responsible for trades made from his account.

The moral of both stories is to know the details of your agreements with online service providers. And beware, consumer protections are not always available to businesses. For more information, see "Cyber Crooks Break into Online Accounts with Ease" at


http://www.usatoday.com/money/industries/technology/2005-11-02-cybercrime-online-accounts_x.htm.

Help Desk Costs

Help desks often bear the brunt of spyware's impact. According to a recent Computerworld survey:

- 83 percent of respondents reported desktop support and performance issues
- 50 percent of respondents reported increased Help desk activity due to spyware
- 79 percent of respondents reported spyware incidents significant enough to involve an IT department response
- When enterprise anti-spyware solutions were implemented in one company, the number of Help desk calls dropped by 30 percent
- In another company, the installation of anti-spyware software and Windows upgrades virtually eliminated spyware-related Help desk calls

As noted earlier, the computer manufacturer Dell reported that spyware accounted for as much as 20 percent of its Help desk calls in late 2004.

 For more information about the Computerworld spyware survey, see “Spy Stoppers Fight Back” at <http://www.computerworld.com/securitytopics/security/story/0,10801,105764,00.html>.

The proliferation of spyware has reached the point at which organizations are observing quantifiable impacts on their system performance as well as their Help desk costs.

Summary

PUPs such as adware and spyware clearly demonstrate the contrasting interests of Web users. On one side, you have PUP developers who realize the potential economic gain from targeted advertising, commandeering computing resources and network bandwidth, and artificially inflating page hits. On the other side, you have large numbers of corporate and home users whose computers are running multiple spyware applications that reduce their system performance, tamper with system configurations, hijack applications, and create vectors for potential information theft.

Like other malware, PUPs are best dealt with using a layered defense. Network devices, such as content-filtering appliances, in conjunction with desktop anti-spyware programs can minimize the impact of spyware. This topic will be addressed in further detail later in this guide; the next chapter will focus on another threat to Web users—phishing scams.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.