



# Spyware: The Next Wave of Corporate Espionage

By **Arian Eigen Heald**  
*a.heald@easternbk.com*

**A** high-ranking vice president enters her office one morning and opens her e-mail as usual. She reviews a note from a colleague referencing a Web site with interesting financial information. She visits the Web site, reviews the information, and goes on about her daily schedule.

Unbeknownst to the vice president, her browser has downloaded an unsigned Active X program that installs itself silently in the background. Over the course of the next six months, a series of e-mails are sent from her PC with her username, password, the contents of her e-mails, and the documents in her My Documents folder on her hard drive. The mailer uses SMTP so that no "Sent" messages appear in her Outlook folders. The mail travels through several unsecured mail servers in foreign countries. Some of her company's most critical financial information has been stolen by spyware.

"Spyware" is most commonly applied to a piece of software that collects marketing information from users' PCs and forwards that information

over the Internet. Many users and organizations have strongly objected to this way of collecting personal information about purchases and Web-browsing habits to fuel the development of better marketing tools.

But users have been persuaded by marketing promotions that providing this information is harmless, that in return they can use "free" software that provides services, utilities and games. I believe, however, that there is a shift in the paradigm of what kind of information is being clandestinely sought. Spyware is moving into the corporate environment as a tool of business espionage, and there is nothing in the existing security practices of businesses today that is fully prepared to deal with it.

This article seeks to define how spyware works and what impact it will have in the corporate environment. Let's see specific definitions of the terms.

**Adware:** Free software "bundled" as part of a larger piece of software a user wants. It is usually installed with the user's permission.

The adware monitors browsing habits and sends targeted advertisements, such as pop-ups and/or e-mail. It also "phones home" to the creator of the software with the marketing data with or without personal identifying information.

**Spyware:** Software that "piggybacks" on other software and is installed invisibly. Running in the background, it records information and sends it to the software's creators.<sup>1</sup>

These definitions compare with the definitions cited in the *Computer Security Handbook*, 4th Edition.<sup>2</sup> The critical factor to note is that spyware is installed without the user's consent.

While adware can and does cross over the line to become spyware, its purpose, to provide targeted advertising, enables the user at some point to see its existence on their personal computer. Spyware does not want to be found and offers nothing back to the user.

When companies first began to track users' shopping habits and browsing patterns, it was a passive system dependent on a user visiting a site and acquiring a cookie. These cookies were frequently deleted and users would set their browsers to refuse to accept any cookies. Many sites force users (notably Microsoft) to accept cookies in order to access their sites, but the savvy user can still delete them. In an age of shrinking margins and on-time inventory, businesses have sought ever more reliable tools to control and improve their competitive edge by tracking where users go.

Marketing online has changed from "passive" recording of visits and cookies to "active" marketing based on the real-time actions of the browsing consumer. Targeted real-time popups, banner ads and browser redirections are the tools of the trade.

## Adware Enters the Mainstream

In 2000, peer-to-peer (P2P) software made its debut with Napster and sparked numerous spin-offs when Napster was sued out of existence. One of the biggest ways new P2P software such as Kazaa, Grokster and Bearshare have funded their existence is to "bundle" software, to which the user gives tacit permission by accepting the EULA (End User Licensing Agreement) during installation. The software monitors what the user is searching for, then targets banner ads at the bottom of their search window. Ironically, the rush to get "free" music fueled adware entering the PCs of millions of users, who supplied advertisers with their biggest window yet into the searches and preferences of the Internet public. Adware uses a social engineering tactic that is actually very old: "something for nothing." It was noted that only 8% of P2P software users admitted reading the EULA.<sup>3</sup>

## Browsers Bring Out the Spyware

In the late 1990s, Microsoft designed Internet Explorer to seamlessly interface the Web and the PC. Microsoft developed ActiveX, "a collection of technologies, protocols, and APIs ... that are used for automatically downloading executable machine code over the Internet."<sup>4</sup> All versions of Internet Explorer have ActiveX "Script ActiveX controls marked safe for scripting" enabled by default.

Microsoft defends ActiveX as being safe because ActiveX requires that any ActiveX control (as opposed to a Netscape "plug-in") have a digital certificate from the software publisher. This Authenticode technology allows the user to determine the key that was used to sign an ActiveX control. But once the software begins installing itself, it could delete its own key on the system. "Signed" code is not safe code.

As Simson Garfinkle points out, "The power and danger of ActiveX is that the downloaded applets basically have the run of your system."<sup>5</sup> For example, with ActiveX enabled, Microsoft will upgrade your operating system via Windows Update.

Since Internet Explorer now has 90% of the browser market, this allows unscrupulous software to access the operating systems of personal and business computers, to rename, edit and change critical system files.

JavaScript, another browser-based language originally written to run on Netscape, was developed without any intrinsic security functions, and as a result, can access various components of the browser to acquire information, such as the user's e-mail address. Since an e-mail client is usually bundled with a browser, it can provide that information by default.

The other security drawback to JavaScript lies in its ability to read the browser "history" component. Combined with the script's ability to create forms that submit themselves by e-mail, it's not hard to imagine sending a username and password by e-mail to an interested party.

## Browser-Related Software

2000 saw the entry of "free" software downloaded from the Internet that "adds to the Internet experience."

### Browser Toolbars

"DashBar is provided free by GAIN Publishing. This application is part of the GAIN Network. This software occasionally displays pop up ads on your computer screen based on your online Web surfing behavior. Click here and get DashBar with no GAIN advertising for \$30."

-GAIN Publishing promotional statement

"Having played with it for a few minutes, something became very obvious. Every single search of the 'search engine' returned a link to a sponsor's web site. All of them."<sup>6</sup>

Other examples include CoolWebSearch,<sup>7</sup> LOP, Huntbar and EZCybersearch. All of these products change stylesheets, browser trusted zones configurations, and the local hosts file.<sup>8</sup>

### Home Page Hijackers

This type of software redirects the opening browser home page to its site and cannot be uninstalled, except by adware/spyware removal software. There is no uninstallation package. Examples include: PassThisOn.com, Gohip.com, Mycpworld.com, EZCybersearch.com, and LOP.com<sup>9</sup>

### Forced Hyperlinks and Appendages

Privilation.com affixes the `privilation.com/cgi-bin/r.cgi` to the URL of Web sites visited, even when typing in the address manually.

"eZula and Surf+ insert hyperlinks into web pages you visit: These hyperlinks are not placed there by the author of the web page, but are inserted after the fact (actually, inside your browser) by the eZula and Surf+ software: These force-fed hyperlinks are often really just ads that bring you to sites that paid for the linkage—all without any involvement on the part of the web site owner or page author."<sup>10</sup>

### Browser Redirects

Whenever a browser is opened, this type of software changes default search engine, reloads the configuration upon reboot, redirects to another search page whenever Google or Yahoo are selected, and monitors all hyperlinks typed in and redirects any without www.

A variant on this is the "error-page hijacker," which redirects all error pages to a particular server. An example of this is Internet Optimizer and Httpper.<sup>11</sup>

According to Microsoft, "a 'Browser Helper Object' is a DLL that will attach itself to every new instance of Internet Explorer 4.0. You can use this feature to gain access to the object model of a particular running instance of Internet Explorer. You can also use this feature to get events from an instance of Internet Explorer 4.0."<sup>12</sup> Microsoft has listed this "feature" as a "way to customize the browser."<sup>13</sup>

Unfortunately, this "feature" has been used to "radically change browser settings, including home pages and bookmarks, and make it difficult or impossible for people to change these back without knowing how to manipulate the Windows registry. Recent examples of these BHOs, distributed by Web advertising portals Lop.com and Xupiter.com, redirect browsers to their respective sites at every available opportunity."<sup>14</sup> BHOs are also known as Data Transponders, since once installed, they will contact a server that provides a stream of constant advertising pop-ups when the user is online.<sup>15</sup>

## The Next Generation of Cookies: Web Bugs

"A Web Bug is a graphic on a Web page or in an e-mail message that is designed to monitor who is reading the Web page or e-mail message. Web Bugs are often invisible because they are typically only 1-by-1 pixels in size. They are represented as HTML IMG tags."<sup>16</sup> If the e-mail is opened via the preview feature of many e-mail clients, the Web Bug automatically sends its information out via port 80.

- ▲ What information is sent to a server when a Web bug is viewed?
- ▲ The IP address of the computer that fetched the Web bug
- ▲ The URL of the page that the Web bug is located on
- ▲ The URL of the Web bug image
- ▲ The time the Web bug was viewed
- ▲ The type of browser that fetched the Web bug image
- ▲ A previously set cookie value

DoubleClick is the agency that uses Web bugs with the highest-trafficked sites. DoubleClick uses roughly 535 Web bugs on third-party sites, compared with 326 from Weather.com and 306 from Netscape.com, according to another report that tracks the pure number of bugs issued by a company.<sup>17</sup>

A recent survey by a security company listed the top 100 companies that benefited from Web bugs, and the names include Amazon, Yahoo and Google.<sup>18</sup>

These invisible .gifs represent the next generation in their ability to pull the same information as a cookie does without being visible (unless special software is installed)<sup>19</sup> or downloading anything to the user's hard drive.

## Online Software Installs

Screensavers, download managers, utilities, word processing, and games are available in the thousands, to be downloaded and installed by the browsing user to their local machine. Of concern, however, are the Web sites that do what CNET calls "drive-by downloading," where accessing a Web page initializes the install of software with only one chance to accept or deny an installation. Many users will select "yes" almost by reflex.<sup>20</sup> There are now hundreds of pieces of software offered

for free that are actually spyware.<sup>21</sup> Software packages exist that require numerous "xx-ing out" to escape installing a piece of software from a Web page.

## Deceptive Installation Packages

Utilizing the EULA common to software installation packages, many unscrupulous software developers have simply included the exact reporting functions as a portion of the license you must accept in order to install the software. To the innocent or uneducated, it may be a screen to quickly click past to get to the software benefits. One recent piece of software actually included taking all of the contacts listed in Outlook and sending them advertising e-mail.<sup>22</sup>

## Your Operating System Delivers Ads to You

Utilizing the Windows Messenger Service, marketers and other unscrupulous advertisers have perfected the art of using a little-known function of Windows (2000, XP and 2003) to send pop-ups when a user is online. If a corporation has a poorly configured firewall, these communications are allowed in.

## Surveillance Software

Preying on the fears of parents, key logger products have been offered to the consumer public ("Who is your child talking to online???" under the guise of "family protection."

Although key loggers have been extant in hacking and law enforcement circles for several years, it has been only recently that they have been offered publicly and with such scare tactics. This publicity has allowed many to purchase key loggers for reasons other than protecting their families. Recent cases of students employing key loggers at school kiosks and faculty workstations highlight their increasingly inappropriate use.

## Corporate Espionage with Spyware

Although spyware has thoroughly infested the home user's PC, numerous anti-spyware software products, both free and licensed, have arrived from outraged Internet citizens. Only late this year have corporations begun to see the risks of the following information leaving the business environment:

- ▲ **Internal E-mail Addresses:** One piece of spyware installed by an unwitting user would provide espionage agents with an entire corporate mailing list, from the CEO on down. A mass or targeted e-mail with key loggers as a product, using the return address of an internal user, would harvest further information almost immediately.
- ▲ **Logon IDs and Passwords:** This information is the "holy grail" of every self-respecting corporate espionage agent, allowing access to different servers across the business network, including files, databases and operating systems.
- ▲ **Internal Documents:** Spyware installed on one critical user's PC might well provide internal documents detailing confidential financial records, strategic business plans, product research and development, and buy-out or purchase information.

▲ **Access to Internal Databases:** Databases are the “bread-and-butter” of almost all financial corporations and are certainly critical to most large business functions. Databases, more than any other business tool, offer the espionage agents and illegal profiteers a critical attack vector. The ability to massage data (for example, money) is the gold standard, whether it is the low-level collection of credit-card numbers or the movement of funds across accounts. Agents from countries with no legislation against business espionage can use the Internet to attempt such attacks almost risk-free.

## The New Paradigm

Ironically, the corporate network, focus of intensive efforts from Information Security professionals, provides little or no protection from the spyware listed in this article.

Information can be sent across port 80, a common outbound protocol, with an encrypted payload using Get and Post commands. The same information could be sent in an outbound e-mail. Information could be posted via an image file with a bitmap packer.<sup>23</sup> With ActiveX and JavaScript enabled in the browser, any corporate user who surfs the Internet is vulnerable.

Spyware is well on its way to becoming the new moneymaker for corporate espionage agents and data collection companies. Corporations have begun reporting attacks,<sup>24</sup> and purchasing software from companies that will scan the desktop for such agents. However, given that spyware can, via ActiveX, replace critical systems files with files of the same name in the background of the installation, it is going to be extremely difficult to stay ahead of attacks.

Since the public market has become saturated by adware and spyware, unscrupulous businesses and individuals will seek out new sources of revenue that spyware can generate. Supplying competing companies and governments with internal business information, research and financial statements is a compelling motivator to invade the corporate network as invisibly as possible.

## Defenses

Since deployment of enterprise-wide anti-spyware tools is still a distant goal due to lack of product, other options will need to be considered:

### Thin Clients

Corporations may find that moving to a totally configured desktop loaded from a remote server to be the safest way to ensure little or no spyware becomes resident. Terminal services have become very popular for the ease of deployment and creating a standard software build that can be upgraded and patched one time only.

### Browser Configurations

The business environment will require a customized browser in order to protect the internal environment from ActiveX and JavaScript attacks.

1. Lock and limit ActiveX
2. Disable JavaScript
3. Manage and monitor cookies
4. Disable file downloads

## Internet Software Installs

Software installations from unknown sources have the highest dangers. Even reputable vendors have had web sites with downloadable software hacked and their executables replaced with product that included back-door code.<sup>25</sup> Group policy deployed across the domain can ensure users without administrative rights will not be able to install software. The risk vector is in the Information Systems departments where users with administrative rights locally and on the domain can be lured into installing intriguing software.

### Monitor EULAs

Corporate purchasers and individual users need to be vigilant about reviewing licensing statements and privacy policies of software installs.

### Disable the Messenger Service on Windows OS

In addition to the ever-urgent need to patch and secure operating systems, disabling legacy services that invite rogue code into the network should be a priority. A simple script will enable this to be removed or disabled on servers and desktops.

### Disable HTML-Based E-mail

Although many businesses enjoy the extra communication options that HTML mail offers, the risk from attack e-mail will continue to grow. At the very least, disabling it will eliminate spammers from harvesting active e-mail addresses via Web bugs.

### Anti-Spyware Software

There are now at least six commercial products that offer to remove various adware/spyware infestations on the desktop. Outraged Internet citizens offer two freeware products. Also of use are the forums and discussions related to adware and spyware on various sites.

### Firewalls: Personal and Corporate

Finally, consider use of an application firewall on each PC. Windows XP Service Pack 2 provides one by default. Users will need to be educated to stop inappropriate outbound connections.

Application-level corporate firewalls may have sufficient power to examine the outgoing packets in the near future. It remains to be seen if firewalls will be able to handle both inbound and outbound threat vectors.

### Policy Decisions

Corporations will need to re-evaluate who really needs Internet access or may require that the Internet be accessed via a terminal server.

## Conclusion

The vice president who opened her e-mail from an address of someone she thought was a peer was actually sent an e-mail by a corporate investigator who spoofed the return address and embedded a Web bug to confirm the address was live. The phony Web page she visited installed an ActiveX script onto her PC. After that, the investigator sat back and collected confidential financial data through several open relays from a server out of the country.

“Relatively benign attacks intended to win attention by disrupting networks are being eclipsed by sophisticated attempts to steal passwords and other confidential information that can be used to deliver cash.”<sup>26</sup> We are now seeing the evolution of hacking, adware data collection and insecure software into industrial spyware focused on the

business sector. It no longer matters if the user travels outside the protection of the LAN with a laptop since attacks come in through already-opened ports on the firewall.


The increased sophistication of spyware has not gone unnoticed by government regulators.

Financial institutions especially will need to address this risk and document controls for the FDIC. The Gramm-Leach-Bliley Act will require banks to track their information flow much more strictly.

Publicly held corporations will be required by the Sarbanes-Oxley Act to demonstrate the security of their data from this threat.

Existing tools to secure a corporate network are of little use in addressing spyware, since all of the current product must be loaded and maintained on the desktop PC. There is no server-level product, which is just as vulnerable due to browsers being loaded as part of every server OS.

Hopefully anti-virus vendors will begin picking up this issue as a selling point and incorporate it into their product line. Or it may be the turning point for the desktop landscape in businesses, as the cost of keeping spyware out may be higher than deploying a thin client.

In any case, insecure software and the Internet have allowed the corporate environment to become vulnerable to the pillaging of its assets in a way not known before. Information security professionals will need to research the best possible desktop configuration, which may include a third-party browser with less vulnerable add-ons. The arena for managing the risk of corporate information loss has moved to the desktop, and we must implement solutions quickly. 

---

*Arian Eigen Heald, M.Div., CNE, MCP, is the data security officer for Eastern Bank. She completed her Master of Science in Information Assurance from Norwich University in June 2004.*

<sup>1</sup> <http://news.com.com/2009-1023-985524.html?tag=nl>

<sup>2</sup> p. 33-34, *Computer Security Handbook*, 4th Edition, Bosworth, Seymour; Kabay, M. E., editors, Wiley and Sons, Inc., 2002

<sup>3</sup> <http://news.com.com/2009-1023-885144.html?tag=nl>

<sup>4</sup> p. 308, *Web Security, Privacy and Commerce*, 2nd Edition, Garfinkel, Simson, O'Reilly Publishers, 2002.

<sup>5</sup> p. 311, *ibid.*

<sup>6</sup> Spyware Weekly Newsletter, December 24, 2003

<sup>7</sup> <http://www.merijn.org/cvschronicles.html>

<sup>8</sup> [www.cexx.com](http://www.cexx.com) (CounterExploitation.com)

<sup>9</sup> <http://www.langa.com/newsletters/2002/2002-01-31.htm#2>

<sup>10</sup> <http://217.115.153.73/parasite/InternetOptimizer.html>

<sup>11</sup> <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q179230>

<sup>12</sup> <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp>

<sup>13</sup> <http://news.com.com/2009-1023-985524.html?tag=nl>

<sup>14</sup> <http://cexx.org/vx2.htm>

<sup>15</sup> [http://www.eff.org/Privacy/Marketing/web\\_bug.html](http://www.eff.org/Privacy/Marketing/web_bug.html)

<sup>16</sup> <http://zdnet.com.com/2100-11-528627.html>

<sup>17</sup> [http://www.securityspace.com/s\\_survey/data/man.200311/webbug\\_site.html](http://www.securityspace.com/s_survey/data/man.200311/webbug_site.html)

<sup>18</sup> <http://www.bugnosis.org/>

<sup>19</sup> <http://news.com.com/2100-1023-877568.html?tag=nl>

<sup>20</sup> <http://www.cexx.org/adware.htm> and <http://217.115.153.73/parasite/> and <http://www.grc.org> as well as a searchable database at [http://www.spywareguide.com/product\\_search.php](http://www.spywareguide.com/product_search.php)

<sup>21</sup> [http://www.winnetmag.com/WindowsSecurity/Article/ArticleID/27122/WindowsSecurity\\_27122.html](http://www.winnetmag.com/WindowsSecurity/Article/ArticleID/27122/WindowsSecurity_27122.html)

<sup>22</sup> <http://www.eweek.com/article2/0,4149,1396750,00.asp>

<sup>23</sup> <http://www.spychecker.com/software/encrypt.html> see, for instance, bmpPacker, a freeware utility

<sup>24</sup> <http://news.com.com/2100-1032-5108965.html>

<sup>25</sup> <http://news.com.com/2100-1001-965916.html?tag=nl>

<sup>26</sup> <http://news.com.com/2100-1032-5108965.html>