Spyware

US-CERT

Summary

This paper gives an overview of spyware and outlines some practices to defend against it. Spyware is becoming more widespread as online attackers and traditional criminals use it as a tool for crimes against individuals, businesses, and governments. Statutes banning spyware exist in a number of states and Congress is considering national legislation.

Spyware can lead to financial loss, as in identity theft and credit card fraud, and it can also reduce consumer's confidence in online safety and their willingness to participate in modern electronic commerce.

One approach to combating spyware is to make it less profitable for the criminals using it. Technical solutions that combat spyware focus on finding, blocking, or removing spyware.

Overview of Spyware

Spyware is one type of malicious software (malware) that collects information from a computing system without your consent. Spyware can capture keystrokes, screenshots, authentication credentials, personal email addresses, web form data, internet usage habits, and other personal information. Often, the data is delivered to online attackers who sell it to others or use it themselves to execute financial crimes, identity theft, or use it for marketing or spam.

Software installed after the user has read and agreed to a clear privacy policy or to an End-User License Agreement (EULA) that describes the data collection activities *does not* meet the definition of spyware. It is your responsibility to carefully read these polices to make sure you understand and agree with the terms of the agreement

Who Is Spying?

The people who use spyware include

- online attackers
- marketing organizations
- organized crime
- trusted insiders

Online Attackers
Online attackers primary interest in spyware is using it to steal personal information for financial crimes such as carding (illicit trafficking in stolen credit card and credit card information), for identity theft, or to sell that information to someone else who then executes more traditional financial crimes.

Marketing Organizations
Marketing organizations are interested in personal information such as email addresses, online shopping and browsing habits, keywords in search queries, and other personal and trend-related information that can be used to execute marketing campaigns like spam, spim (unsolicited messages received via instant messaging systems), browser popups, home page hijacking (changing the default web address for a user's browser), and more.

Spying by a Trusted Insider[1]
A trusted insider, for example, might be an employee who uses spyware to collect corporate information which can be sold in the underground economy, used for blackmail, or used to gain access to more valuable information at some later time.

Another example of the trusted insider group includes family members or close relations such as spouses or significant others trying to catch inappropriate behavior or infidelity.

Data Gathered by Spyware
Spyware can monitor nearly any activity or data related to your computing environment. This is not only limited to files on your hard drives, but can also include temporary data such as screen shots, keystrokes, and data packets on connected networks.

When spyware is running on a computer system, there is almost no data outside the reach of a malicious programmer. Commonly targeted data includes

- internet activity
- email and contact information
- Windows Protected Store data (defined below)
- clipboard contents
- keystrokes
- screenshots
- network traffic

How Spyware Operates

Spyware tracks online activity looking for web sites visited, financial data or identity data such as credit card numbers on screen or entered into form fields, browsing and online purchasing habits, and authentication credentials. When keywords of interest like names of banks, online payment systems or pornographic web sites are observed, the spyware starts its data collection process.

Email Addresses
Email addresses can be harvested from an infected user's computer and marketed for use in spam mailing lists. Common techniques for harvesting email addresses and other contact information includes enumerating email applications' address books, monitoring incoming and outgoing

---

[1] Trusted insiders include those who have physical access to computer systems for legitimate purposes. Some examples include employees, contractors, temporary workers, cleaning crew, etc. This group could also include family members or other close relations.

network packets related to email, and scanning files on the system's disks for strings that match the format of an email address.

Windows Protected Store
Windows contains a service called the Protected Store. Its purpose is to provide encrypted storage for sensitive data. The following are some examples of data that might be in the PStore:

- Outlook passwords
- passwords for web sites
- MSN Explorer passwords
- IE AutoComplete passwords
- IE AutoComplete fields
- digital certificates

Even though the PStore is encrypted, access to it is indirectly controlled by the data owner's login credentials. Since most spyware runs under the security profile of the user who is logged on, spyware can harvest this information.

Clipboard Content
The system clipboard often contains sensitive information. Some common examples include user credentials that are copied and pasted into login forms or product registration codes. Other information that might be found in the system clipboard buffer includes sections of potentially sensitive data from recently modified documents or personal information about you or your associates that could be used in crimes related to identity theft.

The Keys You Press
Key logging is one of the first spyware techniques used to capture sensitive data from a system. Both hardware and software key loggers exist. Hardware devices usually slip inline between the keyboard cable and computer. Modern key logging hardware is small and unobtrusive and has even been hidden inside the physical keyboard casing, making it almost impossible to detect.

One limitation of hardware-based keylogger units is the need for physical access to install and retrieve the device and its data. A more common alternative, and the type present in spyware, is the software key logger.

Software key loggers capture keyboard events and record the keystroke data before it is sent to the intended application for processing. Like most other spyware capture technologies, software based keyloggers can turn their capture on or off based on keywords or events. For example, many keyloggers target Instant Messaging clients, email applications, and web browsers but might ignore other applications that don't provide the kind of data the attacker is targeting for harvest.

Network Traffic
Network traffic is another valuable source of data. Some data commonly extracted from network captures includes user names, passwords, email messages, and web content. In some cases, entire files can be extracted and reconstructed from the captured streams.

Impact of Spyware

Spyware can cause people to lose trust in the reliability of online business transactions. Similar to the problem of counterfeit currency in the physical world, spyware undermines confidence in online economic activity. Consumers' willingness to participate in online monetary transactions decreases for fear of personal financial loss. Vendors lose confidence that the person making the purchase is who they say they are and not actually a criminal using a stolen identity or illicit funds. In efforts to manage the risk, vendors and financial institutions often implement additional verification and other loss prevention programs at increased operational cost.

Even when financial organizations cover an individual's loss from online fraud, these costs plus the overhead required to administer loss prevention programs are eventually passed back to consumers in the form of higher service fees, interest rates, or other price increases on the goods and services consumed. As a result, growth rates in commerce are slowed, costs increase, and demand shrinks.

Impact to Computers

By monitoring and reporting user activity, spyware consumes system resources as well as network bandwidth. Depending on the number of spyware components loaded on a system and their functionality, users may experience significant performance degradation.

Because spyware is not always carefully written and tested, systems infected by it are often found to have reliability problems. Affected applications may crash more frequently or the entire system may become unstable, resulting in potential productivity and data loss.

Often, spyware is difficult to remove without detailed knowledge of how it works or by taking drastic measures such as wiping the system clean and starting over.
In many cases, verifying the integrity of the system requires the operating system, patches, and applications to be reinstalled. These difficulties, combined with the efforts necessary to recover user data, can take a lot of time.

Risk of Future Security Incidents

The sensitive information collected by spyware often includes authentication credentials that may be used for future access to the infected system. People often use the same username and password for many different systems, so these stolen credentials may be used to access other systems not yet infected. Once access is gained, additional information theft or malware installation can take place.

Another way spyware puts systems at future risk is by installing backdoor access mechanisms. These backdoors give the malware operator access to control the system or to command the system to download and run arbitrary applications. Attackers can build vast collections of compromised systems without originally compromising a single system.

Common Spyware Forms

There are thousands of instances of malware. Many forms of malware act primarily as spyware while other malware programs contain spyware features. Below are examples of some frequently observed forms of spyware and their operating characteristics.

Browser session hijacking

This class of spyware attempts to modify the user's browser settings. They can be installed in various ways, but the intent is to modify the behavior of the browser so the user is directed to sites of the malware author's choice instead of sites the user might have reached normally. These redirects often lead users to advertisements that earn the hijackers commissions when they are visited.

Browser Helper Objects

Browser Helper Objects (BHOs) are a feature of Internet Explorer (IE) that can be exploited by spyware. They are not always easy to detect.

BHOs can access files, network resources, and anything else the user who launched Internet Explorer can access.

Malicious BHOs can be installed via stand-alone dropper[2] malware, but are also often installed using the "drive-by install" technique, in which code is installed or requested to be installed simply by the action of a user visiting a malicious or compromised web site.

One technology often used in this type of installation is the ActiveX functionality present in Internet Explorer. Depending on system and browser configuration, the installation may take place automatically and be carried out without prompting the user. In cases where there is prompting, information necessary to make an informed decision can be covered with popup windows or other obfuscation techniques such as naming the control "Click yes to download ringtone".

Another effective social engineering technique is inundating the user with repeated popup requests to install the software that only end when the user leaves the site or finally agrees and installs the component. Once the component is installed, it can operate independently, download and install further malware, and even modify browser settings that allow malware to be downloaded with no user notification or interaction.

Cookies and Web Bugs

Cookies are small pieces of information stored on a user's system by a web server. During subsequent visits, the web server can retrieve these cookies. Often, cookies are used for storing user authentication, preferences, and other types of user state information. They can be used to

---

[2] Droppers are a special kind of malware that deliver other malware to the client they are trying to infect. They usually operate by placing malicious files on the system and then changing the system in some way that allows the newly written malware files to be executed.

track a user across multiple web sites. Using correlation and techniques such as "web bugs", over time they can be used to build profiles of individual users.

Web bugs are HTML elements, often in the form of image tags, that retrieve information from a remote web site. While the image may not be visible to the user, the act of making the request can provide information about the user. Web bugs are often embedded in web pages or HTML-enabled email messages.

The links are used to track access using previously set cookies or with unique strings embedded in the URL. A typical use of this is to log the successful delivery of messages to a unique email address (a common technique for spammers). Once a user has accessed the image, a cookie can also be set and associated with their email address as the beginning of a profile. The cookies can then be used to track portions of the user's browsing habits.

False Anti-Spyware Tools
Applications available on some internet sites advertise themselves as spyware detection or removal tools when in fact they themselves are spyware.

Autonomous Spyware
As a class, autonomous spyware operates as a separate process or injects itself into other processes running on your system. This type of spyware often starts up when you log onto your computer and can frequently access anything on your system.

Because autonomous spyware is simply a malicious application, it can be designed to perform almost any type of spying function. Spyware in this class often includes keyloggers, bots, email and web monitoring tools, packet sniffers, and mechanisms that permit the intruder to remotely access and control an infected system.

Bots
A special class of malware known as a bot or zombie is one of the largest malware problems. Bots are remote control agents installed on your system. Bots are often controlled remotely via Internet Relay Chat (IRC). Once a system is infected with a bot, it becomes part of a bot network (*botnet*) and is used in conjunction with other botnet members to carry out the wishes of the bot owner or *bot herder*. Bots can scan networks for vulnerabilities, install various Distributed Denial of Service (DDoS) tools, capture network packets, or download and execute arbitrary programs. Often bots will contain additional spyware or install it. Computers or systems infected with bots can be used to distribute spam to make it harder to track and prosecute the spammers.

What You Can Do

To help stop the spread of spyware and other malware, it is essential to be alert to suspicious activity on your computer and to learn safe computing practices.

While some spyware is deployed by exploiting flaws in operating systems or applications, much of it still relies on social engineering to trick you into running or installing malware. You must

exercise caution when downloading anything from public web sites, newsgroups, instant messaging sessions, or when opening email attachments, even from senders they know. Identity is often difficult to verify on the internet. Frequently, attackers and their malware impersonate associates of the target user to coax them into installing the malicious code. A common example of this is when malware infects a system and then automatically emails itself to everyone in the infected persons' address book. When such an email is received, the recipient is more likely to open the contents because the sender may be a familiar, trusted source.

Don't trust unknown or known high- risk sources
When visiting unfamiliar web sites, you should exercise caution. This guideline should also apply to sites you expect to be high risk based on their content. Such sites include those with many popups, constant or required requests to install browser components and other applications, and those with content focused on illegal or questionable topics such as software cracking or hacking.

If you must visit sites of these types, never allow ActiveX controls, browser plug-ins or other types of applications to be installed on your system. If you are prompted about allowing an installation or about agreeing to terms of some kind, it is a good idea to press ALT-F4 or take other action to close the popup or browser window. Taking any other action, including answering NO to the installation request, could result in malware being installed on your computer.

Read the fine print
If you decide to install an application obtained on the internet, be sure to read all license or privacy agreements related to the software and the organization the code comes from and be sure you completely understand the details. Many times, information about monitoring functionality or the vendor's right to install additional software is included in these documents. It may be located near the end of the data or buried in long paragraphs to make it harder to detect. Although the practice of documenting things in ways that make it hard to locate can be misleading, you are ultimately responsible for your own actions. If you see agreements that seem too lengthy or hard to understand, consider this a warning sign that you may want to reconsider installing the application.

Pay attention when installing applications
Software installation packages sometimes take advantage of a user's tendency to not pay attention to the details and simply accept the default "checked" options.   If the default options are blindly accepted and prompts are ignored, clicking next, next, next may actually be agreeing to the install of spyware, adware or other applications that are not desired. Reading instructions and paying attention to what is being agreed to is important to staying safe.

Keep your operating system and software up to date
Keeping systems and applications current with security–related patches is critical. This includes patching the operating system and all installed applications, especially those related to network and internet activity like browsers, media players, email clients, news readers, and the like. These are *very* common targets of attack and second only to social engineering as a means of spreading malware.

If You Are Running Windows XP, Install Service Pack 2
Windows XP Service Pack 2 includes several features that will help avoid spyware. It includes pop-up blocking capabilities, an improved automated update process, a better host firewall, and security features to help protect you from drive-by installations of malware via ActiveX controls. There are also several other security enhancements in SP2 that are worth having.

Anti-Virus and Anti-Spyware Tools
Installing trusted anti-virus/spyware tools and keeping them and their signatures current is an important part of defensive computer security.

Browser Settings
Configuring your browser to block active content like ActiveX, Java, scripting, pop-ups, images and other potentially harmful content can increase online security. While disabling active content features can stop many threats, it also has a tendency to break many modern web sites and applications. At the very least, the richness of the browsing experience will be reduced.

One browser configuration strategy to manage the risk associated with active content while still enabling trusted sites is the use of Internet Explorer security zones. Using security zones, you can choose preset levels of security.

Email Configuration
If you use an email program, you can configure it to send and display email using plain text instead of HTML. This can eliminate most of the risks from embedded script, web bugs, and other HTML-enabled techniques used by attackers. But just as disabling active content in web browsers reduces the functionality of some features, using plaintext can reduce the usability of some features. Also, many email clients are now offering the ability to disable scripting and block images until a user takes some action to display them.

Starting your Computer Safely
Almost all spyware needs a way to start itself when you are using your computer. Spyware often starts in conjunction with system startup, user login, or when certain applications like an internet browser or other software is launched.

Not all applications that automatically start are malicious, but it is good to know which software is legitimate. One good method to find and disable spyware on your system is to examine the software installed on your computer and determine whether it starts-up automatically or not. You can find this out by looking in the system registry, startup folder, and services control panel.

With Windows XP Service Pack 2, a new feature is added to Internet Explorer that allows some management of browser add-ons. Using this tool, you can review, enable, and disable add-ons like BHOs and ActiveX controls. The tool can be found in Internet Explorer, under Internet Options on the Programs tab by clicking the Manage Add-ons… button.

Produced 2005 by US-CERT, a government organization.