Spyware

Aaron Hackworth
CERT Coordination Center[1]

1 Introduction

Spyware has existed at least since the early 1980's when keyloggers[2] were discovered on computers at university campuses. Subsequently, there has been a steady growth in the use of spyware by online attackers and traditional criminals to execute crimes against individuals, businesses, and governments.

These crimes have both direct economic impacts, as in the case of identity theft and credit card fraud, as well as more subtle, lasting impacts, caused by shaking consumer's confidence and willingness to participate in modern electronic commerce. Reducing threats from spyware is an important part of slowing the erosion of public faith in online business transactions and maintaining healthy economic growth.

Making lasting reductions in spyware activity requires recognition of the financial motives and taking steps towards architecting the value out of the activity. As a business activity, deploying spyware generates revenues from the information collected and entails basic costs such as the purchase or development of malicious software (known as malware), distribution channel costs to deploy and install spyware on the target systems, and loss expectance in the form of criminal or civil penalties levied by the courts. While this is a simplified business model, it covers the main areas and serves as a starting point to discuss how to take the value and profit out of spyware activity.

Technical solutions that combat spyware generally focus on finding, blocking, or removing spyware. The counter-response to these approaches is usually the development of improved spyware. This is because there is still enough potential profit to make the effort worthwhile. Designing systems and policies that lower the value of spyware-related activity is a better long-term solution because it helps to reduce the value of using spyware rather than simply defending against it.

The following gives an overview of spyware, provides examples of some common threats, and outlines policies and practices to defend against spyware and architect the value out of the spyware market.

---

[1] CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

2 Keylogger software captures keystrokes for the purpose of collecting passwords and other information.

2 Overview of Spyware

Spyware is a class of malware that collects information from a computing system without the data owner's consent. This data often includes keystrokes, screenshots, authentication credentials, personal email addresses, web form field 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.

For a program to qualify as spyware it must collect data without the data owner's knowledge or consent and must deliver or make it available in some way to an unauthorized party. Software installed after the user has viewed 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 described in this paper.

Examples of this kind of legitimate software are applications that track online shopping trends for delivery to a marketing company so that the user can receive targeted coupons or shopping suggestions. Some users may be receptive to this kind of service, so depending upon whether the software's activity is legally disclosed to the affected users, it may or may not qualify as spyware. If software fully and clearly states its operations, the decision to accept the terms and install the software typically constitutes an acceptance of personal responsibility for any software operations.

Reading and understanding these policies and agreements can be difficult. Agreements can be intentionally vague, difficult to understand, or so lengthy that users eventually agree from sheer frustration [Edelman 2005]. In some instances, these practices represent a form of social engineering because the intent is to persuade the user to agree to terms that they might not agree to if the agreement was clear. Users need to be educated about this point so that instead of defaulting to agreement, they would instead not agree to terms they don't understand, no matter how strong their desire to use a given software application.

Because one of the keys to classifying software as spyware is the lack of knowledge and consent from the *owner of the data collected*, multi-user systems or systems in networked environments make interesting cases for study. In these situations, software that one user agrees to may collect data on other system users. One user might agree to the terms, but if another user is logged on and the software collects data on their usage or other activities, it would meet the definition of spyware.

3 Who Is Spying?

Observation and analysis of collected malware reveals the types of data commonly extracted from systems. This gives insight into the motives and classes of people involved in the activities. In many cases, the perpetrators fall into one or more of the following categories:

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

Membership in a single group is not exclusive and often, members from various groups can be found working together to accomplish their common objectives, often at the public's expense. As previously stated, motivation varies but with few exceptions, is focused on collecting information that can be leveraged for financial gain.

Online Attackers and Organized Crime

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. Sometimes they act alone to generate, deploy, and collect the information harvested from their spyware. Under other circumstances, they may develop and launch spyware on a contractual basis for criminals or organized crime organizations that have experience in more traditional crime but lack the expertise to develop and leverage technology like malware as a tool. There are many ways to leverage and profit from spyware; there is a steady demand in the underground economy for activities related to its development, deployment, and operation, as well as for the information gathered.

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, and more.

Spying by a Trusted Insider[3]

An example of a trusted insider might be an employee who leverages 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 [McCullagh 2005].

[3] 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.

Understanding the motives of groups who seek to leverage spyware can help influence and improve the design of policies and systems that reduce the ability of spyware to satisfy these motives.

4 Data Gathered by Spyware

Based on the results of malicious code analysis performed by the CERT/CC, spyware has the capability to monitor nearly any activity or piece of data related to your computing environment. This is not only limited to persistent files on your hard drives, but can also include transient data such as screen shots, keystrokes, and data packets observed on connected networks.

Collecting all data related to a computing environment can create a volume of data that is difficult or inefficient to mine for valuable information. Because of this, spyware has evolved and now frequently includes features to limit collected data based on environment factors such as the active process name, active window title, keyword triggers in URLs, web pages and email content. Focusing the collection parameters and filtering out the noise has helped increase the value of the data collected by most modern spyware.

It is important to educate the public that when spyware is running on their systems, there is almost no data outside the reach of a malicious programmer.

Some commonly targeted data includes:

- Internet activity
- email and contact information
- Windows PStore data
- clipboard contents
- keystrokes
- screenshots
- network traffic

Internet Activity

Spyware commonly 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. One area of particular interest is data sent using HTTPS protocol. This is commonly collected data due to the tendency of web application designers to use secure sockets layer (SSL) and transport layer security (TLS) protocols only for more sensitive and therefore theoretically more valuable data. Encryption using SSL/TLS or IPSec VPN[4] tunnels makes it difficult to use data intercepted in transit, but when spyware is running on the end user's computer, it is collected trivially before encryption can occur.

Email Addresses

[4] IP Security Virtual Private Network

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 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 context of the user who is logged on, accessing this data store is programmatically trivial using the PStore API. Even though the PStore API is largely undocumented by Microsoft, publicly available explanation and source code are available on the Internet to help attackers with their development efforts.

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. Spyware that targets network traffic can capture packets that arrive on the network interface of the infected system. If the system is on a shared network segment, such as one with a hub (or switch that is not segmenting traffic properly due to attack, malfunction or errors in configuration), it can also collect packets of data that were not directed to the infected host, but just happened to pass the infected systems network segment.

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.

5 Impacts

Aside from the direct impact of financial and information theft, spyware also impacts economies and individuals in less obvious ways.

According to one article, some of the most compelling threats associated with spyware in the corporate environment include "loss of productivity and increased helpdesk costs; liability associated with privacy violations; intellectual property theft, information and premature disclosure; and loss of credibility and damage to brand" [Piscitello 2005].

Confidence in Online Business Transactions

People's trust in the reliability of online business transactions may be one of the most severe consequences of spyware since it can cause long-term economic damage. 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. The concerns from all parties involved in the transaction can slow the growth rate of commerce and therefore also slow the rate of overall economic growth. In an era where ecommerce opens global markets to established and developing economies alike, a willingness by the public to participate freely in ecommerce activities is important, if not essential.

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.

Loss in Productivity

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 the malware itself 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 generate significant overhead and take long periods 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. Typically, these applications are additional malware or other tools designed to exploit other hosts in the systems environment. These backdoor functions are also risky because they generally have weak or non-existent authentication mechanisms. Attackers scan for the backdoor ports associated with known malware and then attempt to take over the infected system, effectively stealing it from its original malicious “owner”. There are online attackers whose primary business model centers on this technique, eliminating the need for them to invest in malware development and distribution. They can build vast collections of compromised systems without originally compromising a single system.

This secondary exploitation of backdoors and other vulnerabilities exposed through spyware can often be far more damaging than the original infection [Hesseldahl 2005]. Businesses that are unable to respond to compromised systems in a timely way could fall victim to this sort of cascading effect.

6 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 common problem with Internet Explorer (IE). They are in-process[5] COM objects that are designed to make IE extensible and allow easy addition and/or modification of functionality. When Internet Explorer is started, installed BHOs are loaded into the browser's process space.

While BHOs might take the shape of an IE toolbar, there is no requirement to implement a visible interface. This allows them to carry out their function with few signs that they are running.

Running in the IE process space and with the security credentials of the currently logged on user allows BHOs easy access to data in the Internet Explorer space, as well as access to other system resources outside of IE, like files, network resources, and anything else the user who launched Internet Explorer can access.

BHOs can be installed via stand-alone dropper[6] 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. Because they can also be used to store unique identification information that allows one user to be differentiated from another, they can be used to 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 that can contain personal information.

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

[5] BHOs run in the process space of their Internet Explorer instance

[6] 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.

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 spyware often starts at user logon or system startup. Autonomous spyware applications generally have the full security rights of the user who was active when the spyware was installed or activated, so they have access to all of the resources available to that user. In many cases, this is the administrative or root user on the system, so effectively nothing on the system is off limits.

Because autonomous spyware is simply a malicious application, it can perform any spying function that is programmatically possible using its available security credentials. 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 currently observed on the Internet. Bots are remote control agents installed on multiple end user systems. These agents typically use some form of command and control channel with the most common being 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*.

To control an individual bot or an entire bot net, the attacker sends commands to the botnet via a command and control channel and then waits for the results. Common bot functionality includes network and vulnerability scanners, various Distributed Denial of Service (DDoS) tools, a capability to capture network packets, and the ability to download and execute arbitrary programs. Often bots will contain additional spyware or install it. Hosts infected with bots can be used as spam proxies making it hard to track and prosecute the spammers.

Bot herders don't necessarily need programming or exploit skills. There is an ample supply of more technical attackers willing to develop and exploit the hosts for sale in the underground economy. Additionally, the bots can be stolen from other herders by taking over their command and control channels or by exploiting backdoors in the infected hosts.

7 Defensive Measures

Education

To help stop the spread of spyware and other malware, it is essential to raise public awareness of the spyware issue. The computing public needs to know the importance of being alert to suspicious activity and of learning safe computing practices. Since much of the malicious activity on the Internet today relies on some form of social engineering to accomplish its goals, an educated public will lead to a higher cost in effort for the attackers seeking to trick them.

Be Alert

Realize that there are people on the Internet who want to exploit others for financial gain. Besides manipulating technology for their own illicit purposes, online attackers and other criminals use other forms of trickery to achieve their goals.

While some spyware is deployed by exploiting flaws in operating systems or applications, much of it still relies on social engineering to exploit users by tricking them into running or installing malware. Users need to 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 warez[7], software cracking, hacking and the like.

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

[7] warez is a term used for illegally copied commercial software

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.

The value of educating the public may also have a positive ripple effect on business in general by creating a more knowledgeable consumer base that places market pressure on organizations to engineer systems and services that help maintain their online safety.

Keep OS and Applications Patched
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.

Because of legal concerns and lack of a clear, industry-wide definition of spyware, many companies have opted not to include detection and removal capabilities for spyware in their anti-virus products. In these cases, the installation and maintenance of an independent anti-spyware program is necessary to catch these kinds of threats.

Using real-time anti-virus and anti-spyware tools and scanning applications manually prior to their execution can help locate and identify many threats before they are able to infect systems and become problems.

Alternative Internet Applications
A majority of spyware and general malware currently in use targets Microsoft applications. The foundation for this is not because Microsoft products are more or less secure than open source or other products; it is simply an economic matter of ROI (Return on Investment). Malware authors would like to maximize the total financial value from their data collection efforts. To accomplish

this they tend to target the largest market segment available. Because of the success of Microsoft and the fact that their success has led to them constituting the vast majority of client software running on the Internet, it makes sense that targeting these applications will produce a greater ROI.

Switching to alternative applications may temporarily remove systems from the preferred market segment, but this is no guarantee that when the user base for the newly select application is large enough that it too will not become a favorable target.

Browser Configuration

Even with responsible browsing habits and a fully patched system, there are risks on the Internet. Exploits such as the Download.Ject [Microsoft 2004] exploit of 2004 have demonstrated that there are circumstances where attackers exploit vulnerabilities before patches have been released and install malware with no user interaction.

Configuring your browser and other HTML rendering applications to block active content like ActiveX, Java, scripting, pop-ups, images and other potentially harmful content can increase online security. But 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 IE security zones. Using security zones, IE can be configured in a sort of "opt-in" manner with respect to browser features. For example, the "Internet" zone defaults to "Medium" security and the "Trusted Sites" zone defaults to "Low" security. A more secure configuration for IE would be to reconfigure the Internet zone to "High" security and the "Trusted Sites" to "Medium". As sites requiring active content are visited and identified as safe, they can be added to the "Trusted Sites" zone where scripting and other rich features may be enabled. This sort of change moves IE from a blacklisting configuration to a whitelisting configuration, which is an improvement, security-wise.

Email Configuration

Configuring email applications to send and display email using plain text instead of HTML 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 has the unfortunate side effect of reducing the usability of some features available though email. Because abandoning HTML-based email is not a reasonable solution in all circumstances, many email clients are now offering the ability to disable scripting and block images until a user takes some action to display them.

Monitoring Auto Started Code

Almost all Spyware needs a way to start itself when the user is active, or when the activity of interest is taking place. Often, the malware 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 knowing what should be set this way and researching entries that you cannot account for is a good method to search out and disable spyware on your system. You can find applications of this type by examining the System Registry, Startup Folder, and Services Control Panel. There are also excellent free tools available to help you find these kinds of applications in a more user friendly manner. One example is AutoRuns[8] available from SysInternals (see resources). This tool allows you to view applications that are started at boot, logon, or started with Internet Explorer and Explorer.

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, users 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. Additional tools that allow examination of installed BHOs are also available. Two examples include BHODemon[9] or BHOCop.

Network Configuration

A properly configured web proxy with filtering can help reduce spyware or render existing installed spyware unable to deliver collected information to the attacker or to update itself. Using good proxy filtering software to block access to sites known to be malicious can help. Network layer email scanning technology that filters known spam and viruses is also an excellent layer of protection for an organization.

Using a firewall to block inbound ports that are not necessary can help prevent infection through exploit or outside connection to backdoors that are installed on internal hosts. Blocking outbound connections to services that are not required for execution of an organization's business needs or goals should also be considered, with exceptions made as needed. Proper use of this ingress and egress filtering is especially important for connections to Internet-facing servers that are more likely to be attacked or exploited.

Combining network firewall and proxy solutions with an OS integrated firewall or personal firewall application can further increase protection against security threats. Protection centered on the host is important because it helps to defend the local machine against threats that are launched internally or that slip past the other security defenses. These solutions often include the ability to detect and prevent outbound connections from unknown applications such as spyware and other malware. Host-based firewall solutions should be implemented whenever possible, regardless of whether networks based solutions are in place.

Architecting the Value out of Online Data Theft

Techniques to combat spyware have emphasized system protection and technical solutions such as those described above. These forms of defense are important to raising the barriers to intrusion, but they are based on a near-term defensive strategy and do not address the long-term elimination of the problem. Failure to develop long-term strategies focused on eliminating the motives behind the crimes leaves both sides locked in an arms race with attackers still driven to

[8] Autoruns available at http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml
[9] BHODemon available at http://www.definitivesolutions.com/bhodemon.htm

develop ways around defenses and IT security professionals forced to then develop better defenses.

Affecting long term change in spyware activity will require finding ways to impact the underground economic value it provides. To do this, governments and organizations will need to *architect* the value out of the spyware. This can be done by building systems that remove or minimize the value of the data spyware targets. Advances in cryptography and low cost hardware devices such as smart cards and two factor hardware tokens make these kinds of solutions possible. With these tools and specially designed payment protocols it is possible to architect systems that allow authentication and ecommerce activities to occur without the need to expose sensitive information to theft. As new information and ecommerce systems are developed, designers must consider how spyware works and determine the places in the process where information exposure occurs. In past security designs, their concerns focused on network connections and service provider back-end systems. In the future, they need to consider expanding their focus to include end-user systems and understand how spyware works at that level to intercept data.

Increasing Attacker Risk
Countries around the world should take a close look at the issues presented by spyware and consider if their current laws, penalties and enforcement policies are sufficient to combat the problem. Global cooperation between governments and law enforcement in these areas is an important step toward increasing risk to the attackers.

In the future, efforts to remove the motivation for spyware and other malware by changing the risk/reward equation may prove to be the best way to reduce the number of incidents and promote a healthier economic environment for all legitimate participants in online commerce.

8 Resources

Definitive Solutions, Inc. tools:
BHODemon – http://www.definitivesolutions.com/bhodemon.htm

Sysinternals tools:
Autoruns – http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml

9 References

[AOL/NCSA 2004] America Online and the National Cyber Security Alliance. *AOL/NCSA Online Safety Study*. Available at <http://www.staysafeonline.info/news/safety_study_v04.pdf>. October 2004.

[DOXdesk 2005] DOXdesk website. *Definitions of parasite-related terms*. Available at <http://www.doxdesk.com/parasite/>. 2005.

[Edelman 2005] Edelman B. *Comparison of Unwanted Software Installed by P2P Programs*. Available at <http://www.benedelman.org/spyware/p2p/ >. Updated March 7, 2005.

[Esposito 1999] Esposito D. *Browser Helper Objects: The Browser the Way You Want It.* Available at <http://msdn.microsoft.com/library/default.asp?url=/library/enus/dnwebgen/html/bho.asp>. January 1999.

[Healan 2004] Healan M. *Prevent Browser Hijacking*. Available at <http://www.spywareinfo.com/articles/hijacked/prevent.php>. March 23, 2004, updated May 7th, 2004.

[Hesseldahl 2005] Hesseldahl A. *Fried by Spyware*. Available at <http://www.forbes.com/boxes/enterprisetech/2005/01/17/cx_ah_0117spyfry.html>. January 17, 2005.

[McCullagh 2005] McCullagh D. *Court: Wife broke law with spyware*. Available at <http://news.zdnet.com/2100-1009_22-5577979.html>. February 15, 2005.

[Microsoft 2004 (1)] Microsoft. *Security At Home, Fighting Spyware*. Available at <http://www.microsoft.com/athome/security/spyware/default.mspx>. 2004.

[Microsoft 2004 (2)] Microsoft. *Increase Your Browsing and E-Mail Safety*. Available at <http://www.microsoft.com/security/incident/settings.mspx>. July 16, 2004.

[Microsoft 2004 (3)] Microsoft. *What You Should Know About Download.Ject.* Available at <http://www.microsoft.com/security/incident/download_ject.mspx>. June 24, 2004, updated February 10, 2005.

[Piscitello 2005] Piscitello D. *How to Keep Spyware Off Your Enterprise Network.* Available at <http://www.securitypipeline.com/howto/57700315>. January 10th, 2005.

[Skoudis 2004] Skoudis E. *Top 10 Ways to Fight Malicious Code*. Available at <http://www.g4tv.com/screensavers/features/46958/Top_10_Ways_to_Fight_Malicious_Code.html>. February 5, 2004.

[Twist 2005] Twist J. *Solutions to net security fears*. Available at <http://news.bbc.co.uk/1/hi/technology/4273135.stm>. Updated Feb 25, 2005.

[Wagner 2004] Wagner C. *Spyware/AdWare/Malware FAQ and Removal Guide v2.1*. Available at <http://www.io.com/~cwagner/spyware/>. Updated Oct. 27th, 2004.

[Wienbar 2004] Wienbar S. *The Spyware Inferno*. Available at <http://news.com.com/2010-1032-5307831.html>. August 13, 2004.

[XBlock Systems 2005] XBlock Systems LLC website. *Intro to Spyware*. Available at <http://www.spywareguide.com/txt_intro.php>. 2005.