Global Information Assurance Certification Paper

Spyware – Ignorance is the Biggest Hurdle

David Miller

GSEC Version 1.4b
July 19, 2003

Introduction

Imagine for a moment that you have stopped by the local Kinko's store to have some copies made. The order is small and will only take 15 minutes. So, you decide to wait. Off to the side you notice a number of vacant computers. You think to your self that there is no better way to pass the time than by spending it browsing the web. So, you logon to one of them and start surfing. During your web explorations you see something you want to buy. But, do you have enough money for it? Most people instinctively know that physical security is import. Being no different you quickly scan the store to see if anyone is watching. Feeling confident that the coast is clear you pop into your online bank to take a peak at your balance. 'Yep, plenty of money', you say to yourself. You quickly logoff, pay for your copies and head out to make your purchase. Seems like a fairly benign situation, right? Wrong! Like many of the Kinko's customers in the New York area you may find that you are now the victim of identify theft.

According to an article in The Mercury News Juju Jiang had secretly installed software that logged individual keystrokes in at least 14 different Kinko's stores. Over the last year he had used these 'spies' to capture more than 450 user names and passwords. He then used this information to access their bank accounts and even open up new ones.

In an effort to mitigate personal and corporate risk; this paper will attempt to educate the reader on the topic of spyware, give some insight on the proper assessment of the threats it poses, introduce useful tools and suggest additional layers to be included in security systems.

Identity theft and the use of spyware are on the rise

The article quoted above also documents that a former Boston College student had done the same thing to a number of computers on their campus. Still another article on AllAfrica.com indicated that nine South Africans also fell prey to the same thing. The article then went on to say that, "Identity theft, where fraudsters steal personal data by using such software, has risen 80% in the past 12 months. Last year 7million US adults fell victim, throwing SA's total of nine known victims into paltry perspective."[2]

Go to any good search engine, enter the word spyware and you will be given many more examples like the ones just described. Given recent headlines it is easy to see that spyware is rapidly becoming a threat equivalent to that of viruses and worms. One of the key issues facilitating this trend is the ignorance of what spyware is in the general populace. Those that have heard of spyware are only familiar with some of its

capabilities. In fact, the term spyware has become somewhat synonymous with adware. This is a problem because most people educate themselves on adware, form an opinion and make decision without knowing the full breadth of the spyware problem. To add insult to injury adware is trivialized as nothing more than a marketing tool with nothing more at stake than our browsing habits. By studying spyware, its uses and impacts, we can better understand how to assess the true risks and what actions are appropriate and necessary.

How did we get here?

Perhaps a brief history lesson is in order. I have attempted to piece together my best guess as to how it all happened. Like any software the motives started out somewhat noble. In an attempt to protect their own assets, employers built software to monitor the activities of their employees. Parents also utilize this technology to monitor the activities of their children. Some technology organizations utilized it in an attempt to heighten their ability to help diagnose problems for their users and enhance their help desk activities. From there, however, it goes down hill.

At the same time, or possibly earlier, in the mid 90's the internet was hitting a peak. Advertising had just been introduced and people were starting to recognize the money side of the internet. The pornographic industry seemed to emerge as one of the more "charismatic" sides of the internet. In an attempt to capture would be buyers/viewers they began to delve into some of the more cutting edge technology. Some of the more seedy uses of this technology included popup advertisements and websites with endless mazes of pages from which one could never escape.

It wasn't long before the legitimate companies saw the potential. Assuming positive intent the ad agencies could arguably be viewed as serving a legitimate purpose. The thought being that they could help individuals find what they were shopping for by catering the ads to the individuals unique tastes. To do this they had to first find a way to obtain a lead into those unique tastes. From there we started back down the path of the ethically questionable uses. For example, File Sharing, obtaining information without consent, software that utilizes others' CPU, disk space and bandwidth resources for their own purposes. Until, finally, we have out right identity theft and compromised corporate confidentiality.

Terms and definitions

Now that we know where we have been. Let's put a label and formal definition to it. Spyware is defined as technology that gathers information about a person or organization which it then transmits to someone else without first obtaining permission to do so. This action can be legal or illegal depending on the circumstances. Like traditional spies the spyware will employ any tactic in reaching its goals and it will attempt to remain unnoticed during all of its activities. After all, what use is a spy if you know who he is? What the 'spy' collects is unique to the individual pieces of spyware and this is what creates spyware subcategories. Some collect keystrokes while others collect personal information (i.e. name, address, social security number, bank account

numbers, etc.). Still others are content with just your browsing habits or computer specifications.

Adware is a subcategory of spyware which specifically targets your browsing habits, preferred advertisement types, and your online shopping habits. Some adware may even hijack the ads of other companies, replacing them with its own. Unlike other forms of spyware, adware in most cases does disclose its intent in an End User License Agreement (EULA). However, there is much controversy about whether or not that agreement is clearly and conspicuously informing the computer user of the presence of spyware and its intended function.

Another subcategory of spyware is hijackware. Hijackware is unique in that it is not necessarily interested in where you have gone or where you want to go. Its primary goal is to force you to go where it wants you to go. The sudden change of your Home Page or search settings is usually indicative of a Hijacker. A different form of hijacker is the Dialer. A dialer is a type of software mostly used by pornographic vendors. It basically disconnects the user from their modem's usual Internet service provider and reconnects to another for which the user is then billed exorbitant fees.

Browser Help Object (BHO) is a component that Internet Explorer will load whenever it starts. It can create windows, perform any desired action, monitor messages, detect events and in general do anything that a normal windows application can do. The BHO is exploited to replace browser ads with other ads, change Internet Explorer settings and monitor your browser habits as well.

Parasiteware is the term for a piece of adware that is a little more aggressive. Rather than just reporting your browsing habits it attempts to exploit them on the spot. It does this in a number of ways. One is by insuring that if an ad is clicked it is taking credit for leading you there. Businesses usually pay a commission to affiliate web sites that send shoppers their way. Parasites can steal these commissions by inserting their own code in place of the real referral site. However, parasiteware posses little threat to the end user.

Malware is another generic term which has subcategories and deserves some defining as spyware is often labeled as a malware subcategory. Malware is malicious in nature and the subcategories are much better known than the above spyware categories. A virus is one such subcategory and is defined as a program which executes on behalf of a user without that users permission. Viruses normally have a mechanism for replicating themselves and are usually parasitic in nature. They are parasitic in that they rely on some form of host to assist in the infection of a target system. This host can be anything from another program to a simple email. A worm is also a form of malware that is capable of spreading copies of its self to other computer systems. Worms, unlike viruses, do not require a specific user action to enable infection or propagation.

Another subcategory is the Trojan horse which is defined as “a program that purports to perform a certain task but that actually carries out other activities behind the scenes”[4]. The other activities may include anything from looking at files and directories to deleting

file and directories. If installed by a user with admin privileges it will give a hacker access to perform administrative function on the computer. Normally, they do not exercise these rights in your best interest.

In the book Hacking Exposed: Network Security Secrets & Solutions, Third Edition, the authors use the paradigm that the best way to fight the enemy is to know the enemy. An attempt will be made here to do the same using spyware as the topic of discussion.

Know the terrain

While the problem started in the mid to late 90's we find ourselves in the year 2003. The modern hacker has many more obstacles in front of him than he did in earlier times. For one, many people are more security conscious and are using what is called a Defense in Depth strategy toward security. Defense in Depth is a security paradigm invented by the United States Department of Defense. The core belief of a Defense in Depth practitioner is that any one security mechanism, by itself, can be overcome and it is therefore necessary to use several layers of security to realize true protection. Such security layers would include a fire wall, virus scanner, data encryption, etc.

As a global community we are more communicative; a minor happening in southern Asia is almost instantly reported on the other side of the globe. Hackers are being forced to be as quiet as possible in their endeavors. To do otherwise would have a major impact on their effectiveness. If word of a new virus being testing gets leaked out prematurely the market would react with global immunization before it could truly be deployed. That being said these negatives can still be used to their advantage. Viruses spread at lightening quick speeds and many, with meager security systems, have a false sense of security.

To know the terrain means that we must know our systems; both their strengths and weaknesses. To know the terrain one must also do more than understand what others are doing. It is imperative that you understand your own system, how it works and what security is in place. Once you know the terrain of you own systems it will be easier to assess your own specific vulnerabilities to Spyware. Assuming homogeneous security systems, all consisting of a Fire Wall and Virus scanner, what methods can a hacker employ to infiltrate our systems?

Know your enemy

"Observe your enemies, for they first find out your faults."
Antisthenes, Athenian Philosopher 440 B.C.E.

The modern hacker is very aware of the terrain. In fact, they employ the same methods in protecting themselves from attack. However, unlike us they also have a desire to find the faults in the system, faults which they can then exploit. If we were to observe a hacker we would find that he has two key items in his toolbox which, when combined, give him the advantage against most common defenses. The hacker can combine the deception of social engineering with the strength and stealth of a Trojan horse. He just

has to get you to install the software. From there on the only limitation would be the programming language used to build the malware and the imagination of the builder.

Spyware's Social Engineering side

Social Engineering is a term used for techniques that rely on human weaknesses rather than those in software; the goal is to trick people into revealing confidential information that compromises security. One such example of social engineering is a Drive by Download. The idea being that if you blind side a potential victim with a request to download and install software, they will instinctively agree. Most people do not understand the internet or their computers and naturally assume that the request for installation originated from their own computer and is therefore legitimate. Some software, such as Hotbar, will even install regardless of your answer.

Misrepresentation of intent and/or source is another example. As you might surmise from the name, this is when you download software thinking it is from a legitimate source or with a legitimate purpose. If the software says it stops ads then that must be what it does. We never think that the software might do just the opposite. Normally, this misrepresentation comes in the form of an End User License Agreement (EULA). The EULA may state the purpose; however, you just can't seem to find it. Gator's EULA, when copied into a word document with a size 12 font yields a 15 page document. Shrink that down to a size 6 font, slap it in a 2 inch by 3 inch box with a scrollbar, and the End User is going to be begging for a button to click. Even if they are clicking a button that says "Yes" or "I accept". The problem is that if you say yes there is not a court in the world that will listen to your problems.

Our representatives in Washington do deserve some credit; they are attempting to wrap some legislation around the EULA issue. Unfortunately, the positive uses of spyware have effectively muddied the water and forced the topic into debate. Where Malware can always be effectively labeled as malicious and unwanted, the uses and motives of spyware are not always so easily defined. In October of 2000, Senator John Edwards introduced the "Spyware Control and Privacy Protection Act".

The summary of that Act is as follows:

> Requires any online tracking software, or "Spyware," that is made available to the public, to include: (1) a clear notice that software contains such capability; (2) a description of the information subject to collection; and (3) clear electronic instructions on how to disable such capability without affecting software performance or operation. Prohibits such capability from being enabled unless the user consents in advance.[7]

On July 30, 2003 Representative Mary Bono (R-Calif.) introduced a new bill, cosponsored by Representative Edolphus Towns (D-NY), which mirrors the sentiment of the Act put forth by Senator John Edwards. The "Safeguard against Privacy Invasions Act--H.R. 2929" would require that:

> Any organization that offers spyware to post an agreement clearly and conspicuously informing the computer user of the presence of spyware and its intended function. The spyware provider would be required to post the mechanism for accepting such an agreement on the same page as the web agreement, and could not load such spyware without obtaining proper consent.[8]

One would hope that this would be enough. Hope maybe the only thing we have. Take a look at this EULA belonging to a company called Aureate:
"By using this software, you agree that you understand that this software will connect to the Internet UBIQUITOUSLY to download advertisement and/or to provide software updates."[19]

According to the Merriam-Webster Dictionary Ubiquitously means:
Existing or being everywhere at the same time: constantly encountered: WIDESPREAD.
So, you are agreeing to allow the software to incessantly connect to the internet and Aureate reserves the right to download advertisements and provide software updates. Software updates can be interpreted to mean anything from legitimate updates to Trojan horse installation. This EULA is not the most recent example. In fact, I attempted numerous times to find an Aureate or Radiant sponsored copy and failed. However, it does provide an excellent example of how they are used. For a more detailed discussion of how these EULA are used please look at Steve Gibson's OptOut page at http://grc.com/oo/fineprint.htm. For an up-to-date example one need only look at current applications such as Gator (http://www.gator.com/help/privacy_license-5.html).

Even though most spyware applications are simply irritating it is not the legitimate ones we need to worry about. It's the motives of the other ones we must determine. When it comes to security you have to assume the worst. In the case of the EULA that means we should assume there is something they aren't telling us. In agreeing with an EULA you should never have to give up the right to dictate what gets installed and when. Nor should you give up the right to impart your confidential data to whom you want and when you want. Most EULAs are attempting to convince you that the relinquishment of these rights is a legitimate price to pay for the use of their software.

In the case of the Kinko incident the user was not guilty of succumbing to social engineering and installing the software. However, there is still an element of it present. The hacker was preying on the fact that most people assume good security when using a public computer. It probably never crossed the mind of Kinko's customers that they were using an insecure system. This is not to say that Kinko's was negligent. However, use of a public system does not absolve us of our responsibility for the security of our own personal and corporate data.

Spyware's Trojan horse side

The other tool the hacker has at his disposal is the Trojan horse. If he can get you to install the software, under the pretext of legitimacy, then what he does after is up to his own discretion. To obtain this pretence of legitimacy the spyware software is often bundled with other software. The majority of this legitimate software is freeware or

shareware. This combination of software is appealing because it offers what you want at little or no out of pocket cost. If the developer of the software can make a buck off of an adware agency why not bundle them together. Seems like a win/win situation. We get free software, the developer gets paid, and the ad agency has someone to look at their ads.

No different from other Trojan horses, spyware wants to do its job with out detection. Spyware assumes detection is inevitable and usually come equipped with a number of detection avoidance mechanisms and backdoors. A backdoor is a mechanism by which the Trojan horse can quickly regain access and continue the hunt. Examples of these would be:

- Missing or disappearing uninstallers.
- Uninstallers that leave working code behind.
- Silent downloads and 'updates' better termed arbitrary code execution.
- Uninstallers that require a pass code (thwarting your anti-virus' ability to uninstall).
- Removal refusal.
- Disabling security software (The best way to avoid detection is to remove the detector).
- Reverting settings back to its desired state (hijacking)
- KitchenSinkWare – downloads all of its buddies. So, what if you uninstall it. You don't know who else he invited to continue the work.
- Startup files – allowing the software to restart at boot up.
- Masquerading – modifying the name of the executable so that it is less visible. Some forms of spyware simply perform a rename function during uninstall.

The spyware architecture

At the end of the day we are left with a simple yet dangerous design. The spyware goes through the following steps:

1. The spyware, in a parasitic manner and a way reminiscent of a Trojan horse, is bundled as part of a piece of average software. Normally, this software is freeware or shareware which has some legitimate use for the user.
2. Next the user either willingly downloads the software, is asked to download the software as he surfs the net or the software is installed in some other manner without the user's knowledge. No matter which method is used the spyware designer is relying on the fact that the user is involved that he will mindlessly answer yes to any dialog boxes rather than delve into what is being installed. Part of the installation usually includes adding the program to the list of executables launched at computer startup.
3. At this point the spyware is installed and is launched each time the computer is rebooted. Unlike the install process, the user is not made aware of the program and it is left alone to locate the desired information. Theoretically, the spyware can now access anything and everything it wants. The only limitation on the spyware is the programming language used to build it and the programmer's

imagination. This could include downloading and auto installing another program with real teeth.

4. Once the target information is obtained the spyware prepares a communication and relays it back to a centralized server.
5. The data within the communication is now categorized, stored and utilized at the sole discretion of the builder/owner of the spyware.
6. Subsequent, information is gathered and sent to the centralized server at predefined intervals. Normally, these communications include a unique identifier that allows the spyware creator to link the data now being received with that of previous communications.

What risks does this pose?

What has just been described is a very real threat. However, depending on our vulnerabilities the risk may be low. Should we assume that, like other Trojan horses, these are few and far between? Should we assume that it only happens to the other guy?

First we must understand that spyware is not a small issue, nor is it going away. A summary, by category, of a total of 543,409 pests reported by PestPatrol users within the last 28 days reveals the following:

Pest	Count
Adware	339,138
Browser Helper Object	101,753
Spyware	38,434
Spyware Cookie	24,296
P2P	18,056
Hijacker	8,579
Key Logger	3,275
Dialer	1,230
RAT	1,157
Commercial RAT	882

For the sake of brevity the remainder of the list is not shown.[11] However, from the results displayed it is clear that spyware is a growing threat and it and its subcategories form the top seven pests identified. The other things you see on this list are Remote Administration Tools (RAT). A RAT is just another name for a Trojan horse. So no matter how you slice it you are dealing with a Trojan horse or spyware in one shape or another. Because the software is installed by the user and does not have the same 'signature' as a normal virus or worm most virus scanners and firewalls are going to be impotent to stop them. Another report indicates that spyware hit a growth spurt in 2002. Climbing from 6 to 370 forms of adware and from 4 to 279 forms of spyware.[12] According to Websense 1 in 3 European businesses have been infected with some form of spyware.[10] Granted these are results as indicated by vendors of anti-spyware software. Whether or not they are a little high or low, they are just putting numbers around something the rest of the industry instinctively already knows.

Obviously, we don't want to willingly place software on our computer that

- Gathers personal or corporate data and negatively impacts our confidentiality.
- Secretly installs unknown software possibly even Trojan horses.
- Opens backdoors or otherwise compromises the integrity of our system.
- Takes up system resources, bandwidth and otherwise compromises our system availability.
- Poses a security risk.

If you do not have a mechanism for finding Trojan horses and/or Spyware chances are you are vulnerable to this threat. If you are just guarding grandma's cookie recipe do not worry about it. But, chances are that you are guarding something more and the risk is high. One of the key things to keep in mind is that you do not know what the spyware has done. Normally, the best practice after being infected with a Trojan horse is to perform a low level format on the computer and reinstall the operating system. The reason for this drastic measure is because you just do not know what backdoors or other software the Trojan horse has put in place. Unless the system is put back to a known state of security (i.e. restoration or reinstallation), you will always have a potentially compromised system. Spyware must be treated with the same respect. While you may be fine with what the EULA said, the fact is you just do not know what the spyware is doing.

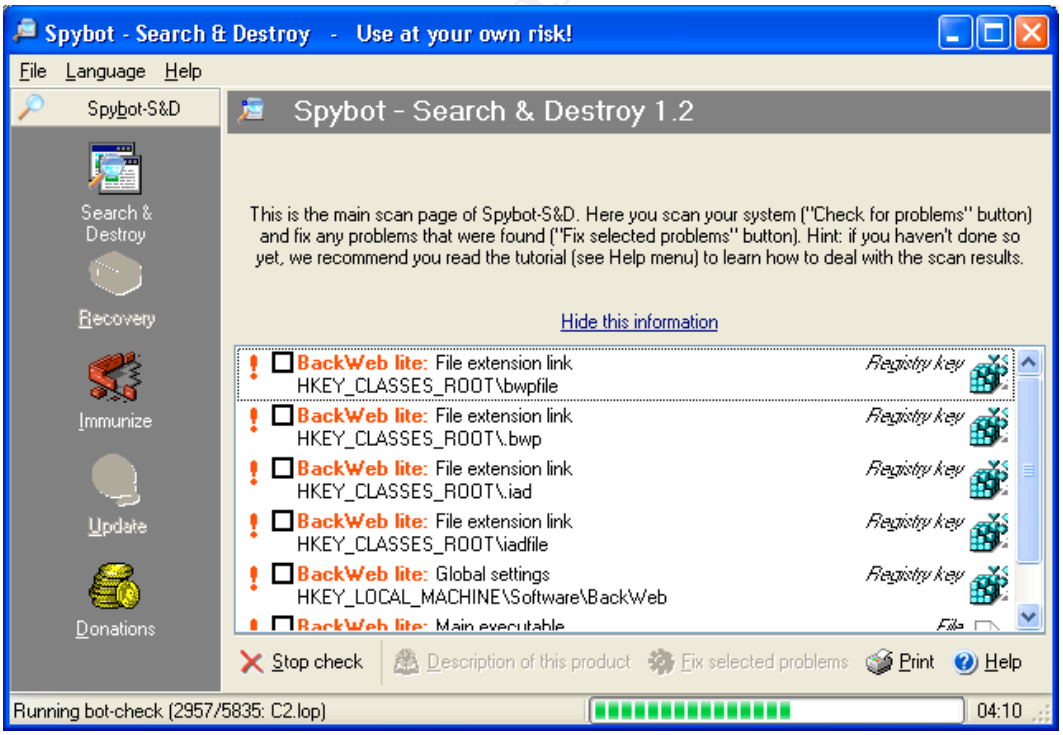
How can we meet the threat?

To meet this threat we must practice Defense in Depth! Avoid relying on one or two items for your systems security. Chances are that the hacker knows what the average security measures are and has thought of ways to by pass them. You have to put a few extra layers in between you and them that are not easily anticipated nor overcome. After all, an ounce of prevention is worth a pound of cure. The following paragraphs represent layers you may consider when next updating your security.

Just be cognizant of the threat. Avoid the Social Engineering traps. Don't just launch an executable on the net. Download it and check it with your virus scanner. Attempt to open the bundle of files to see what will be installed. Install the software on a system of little consequence to see what is installed and how it works. Read the EULA and say no once in a while. If the system really needs it, it will ask again. Computers are flexible. They're rarely guilty of giving you an ultimatum with only one shot to say yes. If you are using a public PC don't just assume high security standards. Ask the manager of the establishment about the security measures employed there. Be cognizant of physical security issues. Somebody is always watching and it only takes an instant to lose a disk in a sea of fellow consumers.

Add a piece of Anti-Spyware to your defensive layering. There are a number on the market. "Spybot - Search & Destroy 1.2" is one such application. It can be downloaded from http://www.safer-networking.org/ . Once you have installed it, you can run the application and you will receive the following window:

From here you can do a number of things. One of the first things to do is check for existing problems. Click the “Check for problems” button and Spybot will search the computer system for all spyware and other threats.



If you click on an item it will display any available information such as the URL of the host site and what the spyware is guilty of doing. Spybot then gives you the chance to select the ones you want to remove which you can then fix. Spybot is just one of many anti-spyware applications accessible to you. Other tools include PestPatrol and Ad-aware. These are similar in functionality and have been document by their respective vendors much better than this paper can do here. The key to remember here is that most spyware is capable of slipping past the detection of today's virus scanners. Anti-Spyware software is an excellent way of mopping up what the virus scanner is missing.

Another way of safe guarding against spyware is to place the URLs of know spyware companies in your hosts file with incorrect IP Addresses. Sounds funny but it works. When you put the URL of a website in your browser, the computer will first consult the hosts file before starting to search the web for the site. The idea is that the computer should not waste time searching the net for something that it already knows or uses often. The hosts file can allow people to store links to the other computers on the network. The computer 192.168.0.1 can now be accessed by a common name like 'OFFICE_COMPUTER' or 'HAL'. The benefit, in the war against spyware, is that Windows will not validate the IP address given in the hosts file. So, by associating a URL for a known spyware website with an incorrect IP Address you can render the URL unreachable. This in turn mitigates the spyware's ability to communicate out. For a much more detailed description of this go to the following URL http://accs-net.com/hosts/how_to_use_hosts.html. The site has a downloadable list of URLs and detailed instructions on how to use it. A brief summary of the instructions follows. There are some restrictions on what you can do with a hosts file.

- You cannot use wild cards (i.e. www.*.com meaning any URL starting with "www" or ending with "com").
- You can block URLs, but, you cannot block IP Addresses.
- This will block the entire site and not just a subdirectory.
- The site will be inaccessible. Even if you want to surf to the website. If you are using the hosts file to block it, it is block period.

To use the hosts file one must do the following:

1. Find the URL you wish to block.
2. Locate your hosts file.
    a) *Windows 95/98/Me* **c:\windows\hosts**
    b) *Windows NT/2000/XP Pro* **c:\winnt\system32\drivers\etc\hosts**
    c) *Windows XP Home* **c:\windows\system32\drivers\etc\hosts**
    d) *For most Unix and Linux boxes just look in your /etc directory*
3. Take a backup of the hosts file before making any changes. In windows you can just copy and paste the file under a different name.
4. Open the hosts file in any text editor (notepad or vi) and append the URLs you want to block. Entries should be in the following format
    127.0.0.1 CookieCop

127.0.0.1 www.yahoo.com

Unless you really know what you are doing it is recommended that you not delete anything from the file. Remember, while we are using the file to block URLs, the real purpose of the hosts file is to speedup the process. Deleting something may impact you negatively.

5. Make sure the hosts file is saved as hosts with no extensions (i.e. hosts.txt).
6. You can now test the system by attempting to go to blocked URL in your internet browser. If you are unable to connect to the website (i.e. www.yahoo.com from above) then you know it is working.
7. Keep the hosts file updated with the latest spyware URLs. The URL listed above keeps a master host file that you can download or otherwise use for updates.

Another good practice is to install multiple firewalls. For instance, you could have a hardware firewall acting as the primary and a software firewall installed on each system in the network as a secondary level. The benefits here is that the software firewall installed on the PC can alert you to the fact that something is attempting to communicate out and will ask if you want to block or permit the communication before it goes to the network or the internet. The other benefit is that it protects each individual PC from the other computers on the network. If a hacker is lucky enough to get through the primary firewall he will still have a hard time getting into each PC on the network. That is assuming you have been diligent in setting up the firewalls. Another recommendation is to be as diligent in designing the filters for outgoing traffic as that of incoming. Most people create elaborate filters for incoming traffic and fail to recognize the simple threat posed by an internal application communicating out. Do not forget to make sure your last rule is to deny all traffic that does not meet the criteria of the previous rules.

Keep all anti-virus, anti-spyware, firewall software, operating systems and software in general patched and up-to-date. Vulnerabilities are discovered almost daily. You can not afford not to be current.

Perform audits and develop an intrusion detection mechanism. Intrusion detection does not mean you have to spend a lot of money on the latest software. It can be as simple as making sure you are logging events and then checking those logs on a normal basis. Check for active ports with the netstat command. Another audit tool is to review your computer's startup files and running services. Spyware will often modify your startup files which allow it to run without your knowledge every time you boot. It pays to be familiar with your systems startup files so that you can recognize intrusions and problems. In Windows XP Start → Run→ regedit will launch the Registry editor. Warning!!! If you are not familiar with the registry refrain from deleting or updating anything. Messing with the registry can cause serious problems. From within the editor you can look in the HKEY_LOCAL_MACHINE\software\microsoft\windows\current version\ directory for startup files. You will want to look in the Run, RunOnce, RunOnceEx, WinLogon and RunServices subdirectories.

Aside from the registry you can also look in the %systemroot%\profiles\%username%\startmenu\programs\startup directory for startup files.

In the same way it is important to know what programs/services your system needs and which are not necessary. Spyware often preys on a user's ignorance in this area. On Windows XP you can perform a control-Alt-delete and select Task Manager. Once on the Task Manager screen select the Processes tab. This tab shows you all of the services running on your system. If you see anything running that you are unfamiliar with you need only run to your favorite internet search engine and ask. Type in the name of the dll or exe file that is running and you will know within a few clicks whether it something you need or not.

An addition layer would be to encrypt your sensitive data. This would insure that at least if the Spyware made it past all your defenses there would be no key data in plan view to steal. It is unlikely that most Spyware is equipped to decrypt your data on the fly. This can be very tedious. However, it will force you to become familiar with what you are attempting to protect and where it is stored. Most people just place files where ever they fall. Another good piece of advice is to install the operating system on the C:\ drive and all other programs on a D:\ drive. Taking that one step further is to place all user directories and personal files on an E:\ drive. Most hackers do not know the structure of your computer. So, they have to make assumptions. Doing the above insures that when the spyware is installed and ready to do its work it does not have access to the drives with critical stuff on them.

Finally, keep an inventory of your systems and backups of key data. Make sure that if you are impacted you can easily recover or at least restore to a stable state. Windows XP has an excellent backup and recovery system. I urge you to take advantage of it if you have it.

Summary

A man's computer is his castle. Like castles of old we should build in layers of security. Castles of old had moots, high walls, gates, and an army inside. Similarly our servers and computers should have multiple layers of security. Reliance on one form of security is dangerous. Most importantly, the idea behind the castle is not that you never let anybody in. Rather, it is that you are selective and assume negative intent allowing only allies to enter. It is much easer to selectively let the good in than to ask the bad to leave. Spyware is still a rather unknown technology. This newness coupled with its use of social engineering and Trojan horse components make it a formidable foe. Knowing that the enemy exists and using the tips documented above should give you the tools necessary to start cleaning house and combating the spyware before it enters your castle walls.

References:

1. "Kinko's spyware case highlights risks of public Internet terminals." The Mercury News. 22 Jul 2003. URL: http://www.siliconvalley.com/mld/siliconvalley/business/special_packages/6359407.htm

2. Stones, Lesley. "Helpful Software Threatens Security" allAfrica.com. 28 Jul 2003. URL: http://allafrica.com/stories/200307280454.html

3. GSEC course material

4. McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed: Network Security Secrets & Solutions, Third Edition. Burkeley:Osborne/McGraw-Hill, 2001. XXV, 554 – 560

5. "Internet Intruders: Spyware, Adware, Hijackers and Other Pests." PestPatrol. 23 Jun 2003. URL: http://www.safersite.com/Support/About/About_Spyware.asp

6. "Social Engineering" hyperdictionary. URL: http://www.hyperdictionary.com/computing/social+engineering

7. "Spyware Control and Privacy Protection Act of 2001" Technology Legislation Survey. 29 Jan 2001. URL: http://www.empower.org/tech_book/S197.HTM

8. "Bono Introduces 'SPI' Act to Protect Internet Users from Downloading Unwanted 'Spyware'" 28 Jul 2003. URL: http://www.house.gov/apps/list/press/ca45_bono/072803_spyware.html

9. "Intro to Spyware" Spyware-Guide.com URL: http://www.spywareguide.com/txt_intro.php

10. "Spyware found in 30% of European businesses" Out-law.com. 02 Oct 2002. URL: http://www.out-law.com

11. "Pest Prevalence" Pest Research Center Statistical Reports. 17 Aug 2003. URL: http://www.safersite.com/Support/Stats/MostPrevalentKindsOfPests.asp

12. Borland, John. "Spyware epidemic rallies call for action" ZDNet. 24 Feb 2003. URL: http://zdnet.com.com/2100-1104-985644.html

13. "Morpheus: A New Low" Speedy3D. URL: http://www.speedy3d.com/doc/article.php?fldAuto=3&faq=5

14. "How to use the Hosts Files" URL:http://accs-net.com/hosts/how_to_use_hosts.html

15. “Spyware” Wikipedia: The free encyclopedia. URL: http://www.wikipedia.org/wiki/Spyware

16. “Ubiquitous” Merriam-Webster Dictionary. URL: http://www.m-w.com/cgi-bin/dictionary

17. Gibson, Steve. “OptOut No One Agrees to an Unread Agreement!” Gibson Research Corporation. 10 May 2000. URL: http://grc.com/oo/fineprint.htm

18. “What’s Bad” PestPatrol. URL: http://www.pestpatrol.com/PestResearchCenter/Whats_Bad.asp

19. “Top 5 Spyware Offenders” Computer Support Services for faculty and staff. 01 Apr 2002. URL: http://css.ucr.edu/spyware/

20. “Privacy Statement and End User License Agreement” Aug 2003 URL: http://www.gator.com/help/privacy_license-5.html