

Spyware: Causes, Effects and Prevention

Two-thirds of Internet technology professionals believe spyware will be the top threat to network security this year, according to a January 2005 poll by WatchGuard Technologies, Inc. The survey of 686 IT managers and administrators was revealing: less than a quarter of respondents cited viruses as the greatest threat; and 73 percent said more than half of their users don't know what spyware is. Spyware is usually defined as: "*A technology that assists in gathering information about a person or organization without their knowledge.*" In Internet terms, it's defined as "...programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties," and is therefore cause for public concern about privacy on the Internet.

There are also, however, many personal computer surveillance tools that allow a user to monitor all kinds of activity on a computer, ranging from keystroke capture, snapshots, email logging, chat logging and just about everything else. These tools are often designed for parents, or businesses, but can be easily abused if they are installed on your computer without your knowledge.

These tools are perfectly legal in most places, but, just like an ordinary tape recorder, if abused they can seriously violate your privacy.

What types of spyware exist?

There are a few basic types of spyware: Advertiser software (Adware), Web Bugs, Stand-Alone Commercial Computer Monitoring/Surveillance software, and Trojans.

Adware

Adware exists because businesses will pay to know your purchasing habits, preferences, household income, family composition and other demographic facts to better target advertising to entice you to buy from them and not competitors. If a marketing firm thinks you are an avid hiker, they will flood you with pop-up ads selling everything from boots to backpacks. These companies devise schemes to get you to install their software by offering a free game or other 'entertainment' type product.

Web Bugs are a form of adware that can track what you're doing online, return that information to a third party, and allow them to pop-up ads or just monitor you for demographic purposes. While these forms of spyware are intrusive, they usually do not collect any personally identifiable information, just demographics. The spyware programs certainly load executable programs and take up resources running in your computer and can, usually by accident or poor design, interfere with your own programs or operating system causing unforeseen, unexplained crashes or abnormal behavior. The most often seen effect of adware is a general slow-down of your PC as more and more resources are diverted to the spyware programs and fewer resources are available for your own use.

Other forms of spyware are not so benign. In fact, some are overtly malicious. These types of spyware are usually not introduced into your computer by a legitimate business. There is a new form of adware which is taking a lot of fire but is still technically legal due to user consent. An example of this type of adware is a company called MarketScore. They are one of the new breed of "proxy" adware companies. This type of software is again installed along with another program the user deems useful but, instead of just collecting demographic information, this software has the potential to collect absolutely all user information no matter how private.

Proxy adware works by getting the user to agree to allow all inbound and outbound traffic from their PC to be re-routed through the marketers' servers. This is done by the addition of a small software program on the user's PC. What this means is that all information sent by the user, to any other person at any time, is captured by the marketers' servers. This also applies to SSL encrypted transactions containing sensitive information such as online banking user IDs and PINs. This works because the marketer is actually a man-in-the-middle who gets the encrypted transmission from the user, is able to decrypt it because he is an authorized proxy, and then re-encrypts it and sends it on to its intended destination as the user.

This is an incredibly intrusive form of adware. Many users are actually unaware of the implications of its use either because they did not read the End User License Agreement (EULA) when installing the software or were not technically knowledgeable enough to understand the full ramifications of the Agreement. Many corporations and universities have closed their firewalls to MarketScore's servers in an attempt to protect themselves from third-party data disclosure. Third-party data disclosure is when one party is being monitored by a second party, such as MarketScore, and in the process divulges information belonging to a third party during normal daily transactions.

Commercial spyware

This software is sold for use by employers, employees, spouses, private investigators, identity thieves and others for one purpose: to record everything you do on your computer ... *silently*. These include URL recorders, keyloggers, chat monitors, screen recorders, program loggers and more. While it may have legitimate uses such as monitoring your child's Internet access or ensuring that employees do not access inappropriate websites on company time, it can be readily abused by unscrupulous people. Imagine the damage that could be done if an industrial spy got this on a PC belonging to a CEO or a Research & Development department. This form of intrusion is not just software-based. There are even certain physical devices such as a small keylogger that measures about 1 inch long by ¼ inch in diameter. It physically plugs in between the keyboard and the PC and can be put in place without the user's knowledge to log all keystrokes and then be picked up by the owner later with hope that useful information has been captured.

Trojans and other malware

The last type of spyware is broadly lumped into the category called a "trojan," which was named after the historical Trojan Horse. This type of software is most commonly used to deliver worms, viruses and other forms of 'malware' to PCs. The worst type is called a "RAT," or Remote Access Tool. This tool enables an attacker to have complete control of your PC.

How does spyware get into your PC?

Adware is often installed along with another program that the user considers useful. One example of this type of demographic software is a company called Fun Web Products. They will give you several entertainment and utility programs if you consent to allow them access to your demographic information. Trojan spyware is most often installed either by a malicious prankster or a criminal. Certain types of trojans exist solely to gather personal information, such as online banking user IDs and PINs, to enable the perpetrator to commit identity theft. As the name implies, trojan software gets installed by the user's own action or, in some instances inaction. In some cases a user clicks a link in an email and either runs an executable attachment or links to a website program that downloads and executes a program. In some cases just visiting a malicious website and viewing a page is enough to silently download and execute a spyware program. Software 'trading' with friends can also mean an Internet spyware program could be hidden in the traded software. This also applies to music files, MP3s and so forth. Even graphics are not

immune. There is an exploit that allows certain picture files to become infected with malware and be able to propagate on a vulnerable PC. As to Stand-Alone Commercial Computer Monitoring/Surveillance software, this software/hardware is most usually installed by a trusted person who has physical access to your computer.

What can happen if spyware is on your machine?

While most forms of adware are intrusive, trojans are even worse. Many trojans contain RATs. There are three main reasons why these trojans exist. The first is the prankster or 'script-kiddie'. These perpetrators aren't really hackers; they're usually much less technically astute. They manage to get a copy of an existing malware program and modify it to some extent to avoid detection by anti-virus scanners. Some do this for a joke, some to get bragging rights with their friends, some to see how many PCs they can 'own.' If their malware contains a RAT they may enter your machine, copy software and/or cause intentional or accidental damage. These people usually aren't looking for any personal information. The next use of trojans is by spammers. Spammers are slowly being squeezed by international law and are finding it harder and harder to get ISPs to host their activities. They have turned to the method of creating 'zombies.' A zombie is a PC that has been infected with, and is now controlled, by a RAT. The zombie PC is used to send bulk spam email for the spammer. By infecting thousands of home and business PCs the spammer can use them like throwaway, disposable mail generators. He can send millions of emails in a single night using someone else's bandwidth and good name.

The ISPs that get this flood of spam often block the sending machines and even get the person's account at their ISP terminated. The spammer doesn't care, it's not his machine. He just creates more zombies and moves on. Some spammers even release the malware that creates zombies and then sell software to send mail through them to other spammers. One example of this type of spamware is a company called Send-Safe.

The last, and most dangerous, use of malware is identity theft. There are a number of trojans that are created specifically to harvest online banking user IDs and PINs, credit card numbers and other financial information. Many of these also install RATs as well. Some of these RATs will make contact through your firewall to a pre-defined Internet Relay Chat (IRC) channel and then accept commands from the owner. At this point the criminal can run software on your PC, upload or download files, and actually perform almost any action that you could perform by sitting at the keyboard. The criminal can easily gather enough sensitive information to clean out your bank accounts or get credit in your name.

What are the legal implications of spyware?

The legal implications of spyware are becoming more complex for businesses as the spyware attacks become more pervasive. Recently the owner of a small business had \$90,000 stolen from his account. It was found that his personal business PC had been infected by the 'CoreFlood' trojan which has a RAT component. The criminal harvested his information and transferred the funds to an Eastern European bank account. The transaction was questioned and law enforcement engaged. The money was traced and frozen in the foreign bank but not until the criminal had successfully withdrawn \$20,000. Due to some complex international legal problems, the remaining \$70,000 remains frozen and unavailable to the rightful owner. The victim's bank claims it is blameless because the criminal had the right authorization codes to transfer the money. The victim is suing the bank because he claims the bank knew of the existence of the trojan, in general, and he wasn't warned. The bank counters with the argument that it is not responsible for protecting the victim's personal computer systems. At this time the lawsuit is unsettled and the banking industry is collectively awaiting the outcome.

At this time there are no clear, unambiguous laws governing these kinds of problems. Also, law enforcement is unable to accurately trace and prosecute criminals across all international boundaries. This has created many challenges for everyone involved in international Internet commerce. The United States is considering legislation against spyware as outlined in this article:

http://www.wired.com/news/politics/0,1283,66848,00.html?tw=wn_tophead_1

Whether such legislation will actually be passed and, if passed, will in fact be effective in combating spyware remains to be seen. This does show the seriousness of the problem and the concern which individuals, corporations and entire governments share on this issue. Getting help for spyware also can be tricky. This is because many of the websites offering help on the subject are, in fact, owned by makers of anti-spyware products and promote their own product. Some go so far as to appear to be independent, third-party websites offering a comparison of various products with the winner, of course, being the sponsoring brand. Very few are actually owned and run by spyware makers promoting their commercial surveillance products. A tiny number are 'black' or malicious websites that purport to provide anti-spyware information but actually will silently install a RAT on the PC of visitors to the website. This silent installation can only occur if the visitor PC is unpatched and vulnerable to certain, known exploits. If the user PC is fully updated there is generally little or no danger in accidentally viewing one of these malicious websites.

Other than some websites offered by a few knowledgeable, private individuals there is really no independent organization to turn to for unbiased information. Each individual or business must take the initiative to perform due diligence and deal with reputable companies in selecting an anti-virus and anti-spyware solution that meets their individual needs. While *BankFinancial* cannot promote or recommend one product or website over another, we present the following list of URLs as a starting point for your independent review and consideration and suggest you use the Internet search engine of your choice to obtain more information on this subject.

<http://www.spywareinfo.com/>

<http://enterprisecurity.symantec.com/content.cfm?ArticleID=5392>

<http://www.microsoft.com/athome/security/spyware/default.msp>

<http://www.spywareguide.com/>

<http://www.safer-networking.org/en/>

<http://www3.ca.com/securityadvisor/pest/>

Disclaimer: *"The above list is not intended to be complete or construed to be an endorsement by BankFinancial of any particular product or service. It is provided merely as informational material to help the reader to make a more informed decision concerning spyware."*

How do I prevent spyware from getting into my PC?

There are a few things that businesses and individuals can do to help prevent spyware from infesting your PC. The total solution will depend upon the perceived amount of protection needed by the individual person or business. Not all of the suggestions offered below may be appropriate in all cases.

- Firewalls. A good firewall that controls both inbound and outbound traffic can help prevent damage from some RATs by limiting access from your network/PC. A firewall solution can be either a hardware or a software solution. Hardware firewalls can range from a simple personal firewall costing less than \$100 and usable on home networks, to professional ones to protect large

networks. Likewise, software firewalls are available for both the individual and the enterprise solution.

- Anti-Virus software. A good anti-virus package is absolutely essential to help detect and remove malware. Get an anti-virus that is self-updating to obtain the latest malware definitions, and maintain it without fail.
- Anti-Spyware software. Just as anti-virus will help catch various malware attempting to infect your PC, an anti-spyware package will help to catch spyware specifically. While there is some overlap in their duties and abilities, each type of software will catch threats that the other is not designed to detect. It is vital that the anti-spyware software is either auto-updated, or manually updated regularly and frequently.
- Many spywares and malwares gain entrance to your PC because of security vulnerabilities in often-used programs, such as your web browser, or even the operating system itself. Because of this it is vital to regularly follow your software and operating system vendors' recommendations and apply security patches as soon as they become available. Unpatched, vulnerable PCs are easily and quickly exploited by spammers, identity thieves and other criminals.
- Avoid installing 'untrusted' or 'unknown' software. Trading software, MP3s or the like is an invitation to disaster. Many pirated software packages are infested with spyware and malware.
- Do not respond to links in email. Clicking links embedded in email can take you to a malicious website and put you at risk. Even if the email seems to be from a trusted site, such as your bank, do not click that link. More and more, financial institutions are making the policy to not include links in their email to help keep their customers safe. When you want to go to your bank's website, open the browser yourself, and type in their URL on the location bar yourself as well.
- Use a spamblocker of some type on your browser. These are small software applications that integrate with your browser and notify you if the site you're about to visit may be malicious or suspect. Many anti-spyware packages come with a real-time component that performs this function as well. Check with the vendor to determine the capabilities of your software.

How do I remove spyware once it's on my PC?

The first line of removal for any malware or spyware is, of course, your anti-virus and anti-spyware software. If you suspect spyware and you do not have anti-virus and anti-spyware installed, installing them will remove most of the pests. Follow the vendors' recommendations for the install of their product and, after installation run a complete system scan to ensure that your PC is clean. Remember, having an anti-virus and anti-spyware installed at the same time provides more protection than either installed alone. This may change in the future as the traditional anti-virus software vendors upgrade their package capabilities, but today running both is beneficial. If you already are running both anti-virus and anti-spyware software and still suspect a spyware infection, contact your anti-virus software vendor. Most have a customer support line staffed with individuals that can aid you in case you are unlucky enough to become infected with malware that they do not currently detect. Most vendors are quite anxious to find new malware and develop protection algorithms for them. Additionally many anti-virus and anti-spyware packages have a heuristics mode which looks for malware-like activity and may be able to find and isolate a new unknown malware

What's the outlook for spyware?

Malware, spyware, anti-virus, anti-spyware, at this point in time it's a contest, a battle of technologies between those who want to profit from your information and those who want to profit from your desire for privacy. This contest has been ongoing for almost 25 years, ever since the first viruses were discovered in-the-wild in 1981. The malware authors seek new technologies and vulnerabilities to spread their work and, unfortunately, the anti-malware companies must fight a reactive battle to each new threat. The ability to proactively detect malware is limited due to the fact that malware is just another software program and your computer is designed to run software programs.

It must have this ability or it would lack any usefulness at all. It would appear that this cat-and-mouse arrangement will continue, for at least the foreseeable future. New legislation is getting ever more draconian in its punishment and scope. However, law enforcement officials are hampered due to geo-political borders limiting their ability to successfully track and prosecute these criminals. In many cases the amount stolen from each individual may be so small as to preclude successful prosecution for any single infraction.

It is therefore imperative that each individual and business take the initiative to proactively gain the knowledge and material necessary to successfully protect their PCs from the threat of malware. Times are changing and the cyber-criminal is getting more resourceful. We must take it upon ourselves to perform due diligence and to protect our personal property as appropriate. Insurance companies have exclusions for loss if the person has contributed to the loss, such as leaving your keys in the car. These types of exclusions may also be forthcoming in the financial world for those who have not instituted common-sense methods to protect their personal data.