



National Webcast Initiative Adware/Spyware How to Protect Yourself from Today's Most Dangerous Spyware Threats

February 9, 2005 -- 3:00pm-4:00pm Eastern

Question and Answer Transcript

The following is a compilation of questions submitted to the presenters through the written Q and A tool during the webcast. The transcript has been edited for relevance.

Question: Is Spyware the same as building a "firewall?"

Answer: A firewall and spyware protection are two different security mechanisms. A firewall alone will not block all types of spyware/adware so spyware/adware software is recommended in addition to a firewall. Please note that some personal firewall products may be bundled with anti-virus software and spyware software.

Question: What is the best way to stop pop-ups from showing up on my computer?

Answer: First, make sure you have the latest security patches installed on your system. Second, the most recent browsers (IE 6 on XP SP2 and Firefox) include pop-up blockers that are enabled by default. If your browser does not have a pop-up blocker, and you can't upgrade to a new one, some Internet Service Provider's provide pop-up blocking software so you may want to check into that. Finally, there are a number of commercial products you can buy from your local computer vendor that block pop-ups.

Question: What would be the perceived impact of technologies that are behavioral based, i.e. Cisco CSA on the impact of Spyware. And, what might be the next generation attack vector once spyware problem is "under control?"

Answer: Although behavioral based products may eventually help stay ahead of the curve, as with was the case with viruses, spyware is expected to continue to evolve to try to circumvent improved protection.

Question: Assuming that my computer is patched with the latest patches and has anti-spyware software on it (Spybot, Adaware, Microsoft Anti-spyware, Spysweeper), what are the odds of it being infected if the computer is left connected to its broadband connection 24hrs a day?

Answer: If you are not also running current anti-virus software and a firewall, the chances are still very good that your computer can be compromised.

Question: Are there any, or do you know of any, "canned" presentations that one could use for user awareness?

Answer:
<http://www.microsoft.com/athome/security/spyware/software/default.msp> has a spyware video and other awareness information. The National Cyber Security Alliance sponsors a website with a variety of information regarding cyber security awareness at <http://www.staysafeonline.info/>

Question: Is one browser - I.E. or Netscape, etc. safer than another?

Answer: Although IE tends to be targeted more often, all browsers have security vulnerabilities. We recommend keeping your patches updated and running current anti-virus, anti-spyware and firewall software rather than relying solely on using a different browser.

Question: What are examples of the top enterprise level anti-spyware scanners?

Answer: <http://en.wikipedia.org/wiki/Spyware> maintains a list of products that may be of interest.

Question: Are there anti-spyware applications network administrators can use to identify client systems that have adware on it? And, can we remove them remotely?

Answer: Network Intrusion Detection Systems and Intrusion Prevention Systems can, in some cases, detect spyware/adware if it generates network traffic. However it should supplement, not replace an enterprise anti-spyware product.

Question: Can we as end users effect any change (in volume and viciousness of adware/spyware) by "voting with our wallets" and not patronizing certain commercial entities?

Answer: Most of the income is derived when the victim follows the links or ads. Certainly, not purchasing the advertised products is another way of addressing the problem.

Question: We are having problems removing a spyware named comment cursor?

Answer: Not knowing the details of your environment, this could be due to a number of reasons. You may want to contact your anti-spyware software vendor's support for assistance.

Question: What percentages have you seen recently where phishing has or is becoming more dangerous than spyware?

Answer: Both phishing and spyware are problems. Some recent statistics related to these issues: According to the National Cyber Security Alliance, 9 out of 10 PCs are infected with spyware. The Anti-Phishing Workgroup estimates that the volume of phishing email is growing at a rate of over 30%, month after month. Please go to the following links for more information: <http://www.staysafeonline.info/index.html> and <http://www.antiphishing.org/>.

Question: My spyware scanner often finds a DSO exploit. What is this?

Answer: DSO exploit is a spyware program that changes windows registry settings to lower your internet explorer security. The following site contains information on it and its removal - <http://www.nsclean.com/dsostop.html>.

Question: Are there going to be any laws that will be enforced to prevent spyware similar to the ones in place for virus makers?

Answer: There is currently a law making its way through congress. Please write to your congressman for more details.

Question: Is there any recourse to a company that sells your e-mail address without your permission?

Answer: The best way to protect yourself is to carefully read all policies and use agreements before giving any company your email address. Many times the right to resell your email address is contained in the fine print as "sharing with our associates."

Question: What is your feeling of "spyware" and "adware" removal programs such as adaware and spybot search and destroy?

Answer: Generally, spyware/adware products are fairly new and the spyware authors are very prolific so the products are always playing catch-up. As a rule of thumb, anti-spyware products are not 100% effective so they should be used in combination with anti-virus software, firewalls, and keeping security patches applied.

Question: Does MarketScore fall within your definition of spyware?

Answer: MarketScore functions as an intermediary for all of your connections. You need to assess the risk of an intermediary being able to see your information and passwords and determine if you trust that intermediary to keep this information confidential. It is not spyware but it should be evaluated for security risks before choosing to use it.

Question: Is it possible to be exposed to a virus, or Trojan, by merely viewing an email message in Microsoft Outlook 2002?

Answer: Yes, it is possible but it depends on how Outlook is configured, whether your system is up-to-date with the latest security patches and running current anti-virus software, etc.

Question: What is the best way to train our users NOT to download third party software that may have spyware/adware included?

Answer: Regular security awareness training, newsletters, periodic email tips, posters, etc. all help keep it in the front of people's minds. You can help prevent "accidents" by locking down your user's workstations so they don't normally run with administrator privileges so some (but not all) spyware can't install completely.

National Webcast Initiative

Adware/Spyware

How to Protect Yourself from Today's Most Dangerous Spyware Threats

February 9, 2005

Questions and Answers Transcript

Question: What does Bot mean or stand for?

Answer: It is a short name for Robot.

Question: We are Mac-based and are running the firewall that comes with OS 10.3 for all networked/Internet-connected computers. Is this effective against adware, spyware, etc.?

Answer: Adware/spyware also includes tracking cookies left on your system when visiting some websites. Although not malicious per se, tracking cookies are a privacy issue and an example that is neither unique to Windows nor blocked by firewalls. So anti-spyware software in addition to your firewall is recommended.

Question: Does spyware typically "run over" standard windows files and do they just erase them or rename them in general?

Answer: This sounds like a virus or worm. Spyware is an additional program downloaded to your machine to make changes to configurations to track your actions, but does not "overwrite" or replace pieces of your operating system.

Question: If you purchase and renew a product such as Spyware Stormer, and it is finding infections, should we keep using these products?

Answer: As with anti-virus software, it is critical to keep your anti-spyware product updated regularly because new spyware/adware comes out frequently.

Question: Does the web browser (Internet Explorer, Netscape, Opera or Mozilla) have an impact on receiving spyware or adware?

Answer: The web browser is typically a method of infection for spyware. Spyware can also be packed in legitimate applications for customer tracking and support. Many times spyware is misrepresented as legitimate software and users install it.

Question: My anti-spyware client identifies spyware in the registry, but the software doesn't (or I can't) remove them. How do I go about removing these? Do some anti-spyware clients remove spyware in the registry?

Answer: Yes, some anti-spyware products will clean up your registry if it has permission to do so. You may want to contact your current anti-spyware vendor for help before considering replacing it.

Question: If you're using IE and the Internet Security settings is Medium or Higher, how is the spyware installed by just visiting a page? Is it the scripting security settings?

Answer: Sometimes spyware can be installed automatically through vulnerabilities in your web browser. Spyware may also misrepresent itself as legitimate software and users intentionally install it. If your security setting is set to HIGH, you may be prompted to install the spyware. Because most users do not understand what that means, they click OK anyway.

Question: It was mentioned in the Webcast that there are websites that appear innocent but can actually load spyware - adware. Is there a list of these websites somewhere?

Answer: You can visit <http://en.wikipedia.org/wiki/Spyware> for a listing of sites.

Question: How does spyware defend itself?

Answer: It makes changes to your system that makes it harder to detect, such as editing your registry or putting entries in your host file.

Question: How effective is a program like the Cisco Secure Agent at stopping spyware?

Answer: Host based security is only as effective as the rules in place and the signatures that are installed and configured. As long as it can identify the spyware it can block it, but spyware evolves rapidly.

Question: Do you recommend Hijack This logs?

Answer: Hijack This captures information about your system so that someone can analyze the information and assists you in the diagnosis of the problem. It doesn't detect or remove spyware or adware.

Question: Will a personal firewall, e.g. ZoneAlarm, allow you to prevent spyware from unknowingly sending out information from your PC?

Answer: No. Most spyware will appear as legitimate traffic.

Question: Your thoughts on Firefox Vs IE?

Answer: Although a lot of people recommend moving away from IE, you can't un-install IE, therefore, a lot of the vulnerabilities still exist and can be exploited. In addition, Firefox has security vulnerabilities. Which browser you use is less important as keeping it configured properly and keeping patches applied.

Question: Can a single spyware removal application remove all spyware?

Answer: Generally spyware products are not 100% effective and should be used in combination with firewalls and anti-virus software.

Question: My family uses AIM. Would you recommend removing this completely?

Answer: AIM itself is a legitimate service however it can also be used for nefarious purposes. Most new anti-virus software products also work with AIM but you should monitor usage. Configure it to not allow file transfers and only allow people you know (i.e. your buddies) to connect to you.

Question: Can you see spyware programs via Task Manager?

Answer: In some cases, however, they tend to mask their names to look like legitimate software.

Question: Is there a list of safe active x or browser helper objects/components?

Answer: Not that we are aware of. Most objects, if used as intended, are safe. The problem is adversaries continually find ways to misuse "safe" items for their own purposes.

Question: Do you recommend installing two or more competing anti-spyware, anti-virus, etc., software applications, or do they conflict with each other?

Answer: There is a good chance multiple competing products will cause conflicts and too many products may end up slowing down your system! A single good quality anti-virus software plus a single anti-spyware product plus a single firewall should provide an adequate level of security.

Question: Are all platforms (operating systems) affected by spyware? Are some more vulnerable than others? If so, which?

Answer: Since spyware also includes tracking cookies which are platform independent, all platforms can be affected by spyware to varying degrees. Some platforms are less of a target than Windows.

Question: Are gaming chat rooms that teen's access risky?

Answer: It depends on who is running the gaming chat room and how well they monitor it.
