
Now that we are all so
well-educated about
spyware...

...can we put the bad guys
out of business?

Karen McDowell, Ph.D.
University of Virginia
Spring 2006

Three Characteristics of Spyware

- Spyware is defined by three characteristics, the first being installation on a user's computer without user's knowledge or consent.
- Second: it provides computer users with no easy way to uninstall the software
- Third: the nature of the beast is to track what you do and where you go on your computer. No one knows what happens to that information.

Front Door vs Back Door

- The front door to computers and networks, email systems and Websites are often locked down by antivirus software, firewalls, and email filtering systems.
- Companies and individuals spent \$18 billion on computer-security hardware and software in 2005, up 19.2% from 2004, according to research firm IDC.
- A December report by the National Cyber Security Alliance shows more than 81% of home-computer users have antivirus software installed on their PCs.

Back Door

- Add to these the continuing maturation of malware attacks on enterprise systems and the tendency toward collaboration among hackers
 - Bots, botkits, botmasters, botnets, botherds, botarmies
 - Keyloggers
 - Rootkits
 - Typo-Squatters
 - Spear-phishing
 - Targeted Trojans
 - Drive-by Downloads
 - Cross-site Scripting
 - Ransomware
 - Attacks on popular applications, like Adobe Macromedia Flash, RealNetworks-Real Player, Apple's Safari Browser, and others.

How Does This Ugly Stuff Get In?

- Spyware frequently gets into the computer through banner ad-based software, much posted by botmasters, where the user is enticed to install the software for free.
- Other sources of spyware include instant messaging, various peer-to-peer applications, popular download managers, online gaming, most porn sites, email and other.
- In the past, a lot of spyware targeted Internet Explorer. Now, however, Firefox has been reporting multiple vulnerabilities.

Bots Conscript Your Computer!

- “Bots are the No. 1 emerging threat to the health of the Internet.”
- Computers that have been infected by worms, viruses, or spyware, so that a hacker can control them remotely.
- Botnets now number 79 to 100 million machines world-wide.
- Botmasters manage their bots for all sorts of “criminal activities, including stealing financial information and proprietary data stored on a computer.”
- They also cause DDOS attacks, spam, spyware, and Google AdSense abuse. They manipulate online polls and games, create mass identity theft, and even raise their trust ratings on Ebay.

Bots are *Serious Trouble*

- Botmasters defeat the traditional, signature or behavior-based methods we use to protect our computers
- With more machines and new software so signature-based protection doesn't work, they can divide their resources and keep their messages under the threshold that behavior-based networks flag.
- These bots can be direct threats against infrastructure. They can be used to take out cellular networks through distributed SMS attacks and to direct anonymous threats.

Keyloggers

- A small, fairly simple program, which a programmer can write in a couple of days, captures everything a user is doing, including keystrokes, mouse clicks, files opened and closed and sites visited.
- Slightly more sophisticated programs of this kind also capture text from windows and make screenshots, so the information is captured, even if the user doesn't type anything.
- No current anti-virus technology will identify 100% of current keylogger threats, but StrikeForce Technologies, based in Edison, N.J., is developing an anti-keylogging toolbar for IE, that promises to encrypt text from the moment it leaves the computer keyboard and send it directly to the browser. It is scheduled for release in June.

Keylogger Use on the Rise!

- According to data compiled by computer security companies in 2005, the use of keyloggers and other malware has soared.
- New York Times reports that Brazilian police recently broke up a fraud ring – stole \$4.7 million USD from 200 different accounts using keyloggers.
- Russian authorities broke up a similar ring which had stolen over \$1.1 million from personal bank accounts in France.
- Can be surreptitiously installed in a myriad of ways, from spyware drive-by Web downloads, hidden within peer-to-peer applications or downloads, inside Trojan horses and other viruses, files shared through IM, email, and more.

Rootkit - Classic Trojan Horse

- Rootkits hide spyware from your antispymware programs—they fly below the radar of your antivirus to maintain a persistent and undetectable presence.
- They monitor traffic and keystrokes, create a backdoor into the system for the hacker's use, alter log files, attack other machines on the network, and alter existing system tools to circumvent detection.
- McAfee research indicates that the use of so-called "stealth technologies" has jumped by over 600 percent during the last three years – increasingly complex and harder to detect.
- Number of rootkit attacks was up by 700 percent during the first quarter of 2006, compared with the same period in 2005.

Rootkits: Possible to Remove?

- Microsoft security officials suggested businesses should consider investing in an automated process to wipe hard drives and reinstall operating systems as a practical way to recover from this kind of malware infestation.
- "When you are dealing with rootkits and some advanced spyware programs, the only solution is to rebuild from scratch."
- One possible way to detect them is to run tcpview, available from www.sysinternals.com, and see who's listening.
- F-Secure Beta program purports to detect them in less than a minute.

Typo-Squatters

- When a user visits a Web site, his browser may be instructed to visit other third-party domains without his knowledge. Some of these third-party domains raise security, privacy, and safety concerns.
- The Strider URL Tracer, which Microsoft makes available for download, is a tool that reveals these third-party domains. It also includes a Typo-Patrol feature that generates and scans sites that capitalize on inadvertent URL misspellings, a process known as typo-squatting. The tool also enables parents to block typo-squatting domains that serve adult ads on typos of children's Web sites.
- <http://research.microsoft.com/URLTracer/>

From Phishing to Spear-Phishing

- Hybrid form of phishing which targets specific victims
- Much harder to detect because bogus email websites and websites not only look like near perfect replicas of communiques from ecommerce companies like banks or a person's employer, but also are targeted at persons known to have an established relationship with the sender.
- Spear-phishers are now piggybacking on spyware.

Why does Phishing work so well?

- Recent study conducted by Harvard and U.C. Berkeley to determine what users do to verify the trustworthiness of a website
- 90% of participants were fooled by phishing sites – did not notice browser cues
- Not a function of age, gender, number of hours on computer or other factors—across the board

Five Ways to Avoid Spear Phishing

- Never reveal personal or financial information in a response to an email request, no matter who appears to have sent it, even if from your *Mother*.
- If you receive an e-mail message that appears suspicious, call the person or organization listed in the From line before you respond or open any attached files.
- Never click links in an email message requesting personal or financial information. Enter the Web address into your browser window instead.
- Report any email that you suspect might be a spear phishing campaign within your office.

Targeted Trojans

- New wave of Trojan attacks aim at specific targets to keep the malware writers under the radar and avoid the FBI – much like spear-phishing.
- Not self-replicating – sent to a few hundred email addresses.
- “Trojans are financially motivated...and they're often configured to turn off your security to steal your financial information and turn your computer into a zombie—part of a botnet—that can be used to launch spam or further virus attacks.”*
- The intent is to write malware that bypasses basic defenses, then appeals to the personal interests of users to induce them to open documents or click on links that load malicious code.
- One targeted trojan aimed at a transportation company – and caught by a security firm late last year – was even designed to look like a request for proposal, or RFP, from a potential client.

Drive-By Downloads

- Drive-by downloads are programs that automatically download and are installed on your computer without your knowledge—much less your permission. The action is cloaked, i.e., invisible to you, the user. It occurs simply by visiting an "unfriendly" web site or by opening an *HTML email*.
- Often more than one program is downloaded, e.g. file sharing with tracking spyware.
- To protect your computer, you can keep your spyware definitions up-to-date, and read your email in plain text and *not HTML*.

Cross-Site Scripting

Active Exploitation of Cross-site Scripting Vulnerability in eBay.com

added April 3, 2006 | updated April 13, 2006

US-CERT is aware of an active exploitation of a cross-site scripting vulnerability in the [eBay](#) website. Successful exploitation may allow an attacker to take various actions, including the following:

Obtain sensitive data from stored cookies

Redirect auction viewers to [phishing](#) sites where further disclosure of login credentials or personal information can occur

Create auctions that use script to place login areas on the eBay website, where credentials may be sent to a remote server with malicious intent

Until a practical solution or more information becomes available, US-CERT recommends the following:

Disable Scripting as specified in the [Securing Your Web Browser](#) document and the [Malicious Web Scripts FAQ](#).

Add "ebay.com" to the Restricted Sites zone in Internet Explorer.

Validate web site addresses as described in the eBay [Spooof Email Tutorial](#) and US-CERT Cyber Security Tip [ST04-014](#).

Validate web site certificates as described in US-CERT Cyber Security Tip [ST05-010](#)

Ransomware – an Old Scam

- Trojan horse will infect your machine and without warning encrypt your files. Then the attacking party will demand some cash for the files to be restored/ opened.
- Say you pay up: Bad Guys cannot protect you from other Bad Guys. There are so many Bad Guys out there, who is to say others won't attack you? If you give them money, they will come back, and they will also bring friends.
- Ransomware criminals usually attack corporate entities...
- Embarrassing and frightening and also on the rise

Attacks on Popular Applications

- “The bottom line is that security has been set back nearly six years in the past 18 months. Six years ago attackers targeted operating systems, and the operating system vendors didn't do automated patching. In the intervening years, automated patching protected everyone from government to grandma. Now the attackers are targeting popular applications, and the vendors of those applications do not do automated patching.”
- Check Add/Remove Programs frequently and Update all programs.

Usual Suspects in the Top Ten Threats

- DesktopScam
- Looking-For.Home Search Assist...
- Virtumonde.A
- Hotbar
- Starware.Toolbar
- WhenU.Save*
- 180 Search Assistant*
- EliteBar
- ISTBar*
- DirectRevenue-ABetterInternet aka Aurora

Two Key Players...

- Eric Howes, independent researcher, MVP and former graduate student (University of Illinois at Urbana-Champaign), provides resources to protect user privacy and security on Internet and conducts testing of antispyware apps.
<http://spywarewarrior.com>
- Benjamin Edelman, a PhD candidate in Economics at Harvard, also an independent researcher, who studies the methods and effects of spyware.
<http://www.benedelman.org>

Beware! Yap Browser and Yapsearch

- Dangerous software, including the actual YapBrowser program itself, which are downloaded from the 180 Search Assistant Zango servers.
- Redirects the user to a child porn site. As of today, April 24, 2006, this site has been removed, but it may possibly reappear on another website.
- Zango is related to 180SearchAssistant and is very attractive to children and teens.
- 180Solutions claims to have cleaned up their act, so why did this happen?

Remember!

- Spyware is ever smarter, often installing two executables that monitor each other. If one is deleted, the other one goes and reinstalls itself again. These are called resuscitators or helpers.
- Spyware is also polymorphic, which means spyware chooses random file names automatically.
- Spyware seeks to hide itself. Popups either want to lure you into clicking on them, or your computer is so infested they overwhelm it.

About Wild Tangent & Viewpoint

- Both *claim* not to be spyware, but have built in components to update themselves and gather info about the user and the computer system
- They also affiliate with *unknown third parties* who have access to your computer through the open back door used for their services
- WildTangent, a plug-in for games, contains a Web driver and sends banner advertising to the computer it is installed on. It also sends a user's sensitive information, including the user's name, address, phone number, and email address, to its server, and collects the user's system configuration information.
- Viewpoint Media Player, Toolbar and Manager also load with AOL and Netscape and purport to supply a media player for the user's online experience. According to their EULA, which is tricky to access, their software collects "data in the aggregate"

Is “Related Software” Safe?

- If details in a EULA for a product that interests you indicate the company reserves the right to install related software on your computer or conduct other activities, or the app does not have a EULA, do not use this software.
- Deceptive website and/or downloads will often obscure a EULA, if they present one at all.
- EULAs often are not clear. “These agreements give a patina of legitimacy by having some form of disclosure.”

The Claria Story

- Largest online behavioral marketing company in the whole world. Began 1998 as The Gator Corporation to deliver one-to-one marketing on the Internet.
- Developed massive consumer audience by offering valuable web/software content for free in exchange for the right to show highly targeted advertising based on consumers' "anonymous" surfing behavior.
- The Gator eWallet—software that stores user passwords—Claria's first free ad-supported software product. Developed also Gain, Precision Time and Date Manager
- Claria finds its spyware extraordinarily profitable to the tune of \$90 million in revenue and \$35 million in profit last year.

What's It Called?

- Whatever you do, don't call it spyware!
- In 2002, Claria, then known as Gator, was one of the most reviled names on the Internet.
- In late 2003, Claria filed a libel suit against PCPitstop.com, a mom-and-pop site that distributed spyware-removal tools. The suit claimed that PCPitstop was infringing on Claria's business by including the company on a list of firms that distributed spyware.
- What effect do you think this created?
- Now Claria is a "rising star," in what some would call a sleight of hand.

Free Removal Tools...

- Spybot 1.4 (www.safernetworking.org)
- Ad-Aware SE Personal (www.lavasoftusa.com) –
Lavasoft does not allow its use on machines owned by businesses or colleges
 - These recommended by PC World, PC Magazine, and other publications, including the Wall Street Journal
 - Spyware growth has exploded because of economic incentives, faster than these two products, even with regular updates, can handle it. According to reliable data, Spybot and Ad-Aware together barely removed half the spyware components on an infected PC.

More Spyware Removal Tools

- Spy Sweeper – www.webroot.com/
- CounterSpy – www.sunbelt-software.com/
- Microsoft Windows Defender Beta – www.microsoft.com
- Excellent feature comparison of many of these products at <http://spywarewarrior.com/asw-features.htm#overview>

Beware of Bogus Antispyware

- Beware of antispyware programs offered via pop-up ads or email spam. Some of these are malicious, and will install rather than expunge spyware and adware.
- More than 100 examples of disreputable antispyware applications on the web, according to Eric Howes, who created a very comprehensive and thoroughly researched website about spyware at http://www.spywarewarrior.com/rogue_anti-spyware.htm
- Rogue programs can install browser home page hijackers and open your computer's back door for others.

Strategies to Prevent Spyware

- Download and update effective antivirus protection
- Backup your data frequently to external media & store in a safe place.
- Exercise extreme caution when downloading files to your system – know what you want
- Do not accept free Internet offers
- Limit online travel to reputable sites
- Secure your web browser
http://www.cert.org/tech_tips/securing_browser/
- Download and update at least two spyware removal programs. Configure them to auto-update
- Do Windows Updates faithfully!
- Run Microsoft's Security Baseline Analyzer
<http://www.microsoft.com/technet/security/tools/mbsahome.msp>
- Good information at
<https://www.trustedcomputinggroup.org/home>