Spies like us

The hidden headache of spyware

Reijo Pitkanen
GSEC Practical Assignment, Option #1
Submitted: March 26 2004

Table of Contents

Abstract

Spyware and Adware parasites are technically not considered “malware" given that they don't usually fit into the standard worm, virus and trojan taxonomy. Older parasites can be classified as simple trojans; non-replicating and piggy-backing on a seemingly harmless program. Newer parasites use ActiveX “drive-by” installation, preying on insecure ActiveX scripting permissions, or user inattention to ActiveX windows. Others exploit known browser vulnerabilities to install Web sites in “Trusted” areas of IE’s security model, then downloading ActiveX content without the user’s knowledge.

Currently, there are no known spyware parasites that will self-replicate or travel to other hosts once infected. This eliminates the basic Virus and Worm classification. Complicating the matter is the issue of a “host” program. Viruses can only spread with the existence of a host and spyware parasites exhibit this viral behavior. Newer parasites lie in wait, waiting for an insecure browser to pass by. Once launched, the parasites exploit deficiencies within the IE security model and infect the host machine, similar to worms and viruses. There is even a certain factor of polymorphism apparent in rare parasites where random class ID’s will be used in an attempt to evade detection.

Anti-virus companies are not in total agreement on how to treat the spyware threat. Computer Associates, Symantec and Norton all maintain support for most of the basic trojan-like parasites. Some Anti-virus programs also detect dropped payloads like dialers and ad-rotating DLL’s. Most don’t detect all of the fingers that an average parasite installs throughout a system. This has created a whole new market for applications: Spyware removers, blockers and scanners.

Spyware appears to be evolving in the application process space, taking on many of the traits and characteristics of malware while exploiting insecurities within that space.

History

In the early days of spyware the dishonesty was only partial. Click-trackers, media viewers and ad-rotators were voluntary to install, usually to help "support" a program one had just downloaded. Some packages even started out reasonably legitimate[1] such as price-comparison search engines. Legal click-through agreements were pages long, explicit about what data was collected, who it went to, and why. It was once common to package these add-ons with other programs such as peer-to-peer file sharing clients like Audiogalaxy, Grokster and Kazaa.

Once installed, most users did not like the amount of control the new packages took, spawning popup ad windows randomly, setting homepages, and installing search-bars that would crash browsers. When deleted, the most virulent parasites would simply re-install (sometimes only partially), leaving the host in varying states of disarray.

Later, people figured out how to package software without the parasites, removing all the undesired components and making sure that new "updates" from spyware companies would not be honored. Others started developing Web sites for user education and community discussion. Still others used their time to develop various techniques and programs to slow or halt the proliferation of the parasites. Just like the malware world, the familiar arms-race started.

Spyware has been forced to look more and more legitimate, all while attempting to hide its less honest mission from the user in any fashion possible. Web browser exploits that allow remote code execution without user approval have been used to propagate spyware. ActiveX “drive-by” installations[2] are now a common method of distribution.

Congress and the lawmakers have taken notice as well. On February 26, 2004, three U.S. Senators introduced a bill[3] to combat spyware via privacy laws. The new bill proposed civil and criminal liability against creators of software that does not provide:

> “…clear notification… of the name and general nature of the computer software that will be installed if the user grants consent; and”
> “…a separate disclosure, with respect to each information collection, advertising, distributed computing and settings modification feature…”

[1] http://www.doxdesk.com/parasite/ClickTheButton.html
[2] http://www.doxdesk.com/parasite/IGetNet.html
[3] http://wyden.senate.gov/leg_issues/legislation/s2145_spyblock.pdf - Bill S2145 (SPYBLOCK Act)

Current Analysis

Infection Vectors

All biological parasites require some method in which to attach to their host. Spyware parasites differ only in the methods used. Thankfully, most of the digital variety offer simple means to inoculate against.

User misdirection or "Social Engineering" is the most used tactic. As covered earlier, packaging parasites with quasi-legal software distributions is one way. Other common tricks involve directing the user to download and install a piece of software in order to correctly view a Web site, assist in your Web searches, or provide a harmless animation that will entertain you on your desktop.

ActiveX "drive-by" installation happens when a Web site embeds ActiveX objects in Web pages. The ActiveX controls are then downloaded and installed, leaving the user with no indication of the recent activity. This allows parasites to literally "leech" on to browsers as they pass by the suspect Web site.

Truly bad parasites use known browser exploits to install themselves without user knowledge. By altering security zone settings or adding a distribution site to the "Trusted Sites" zone, suspect Web sites can avoid prompting the user to install or download components, even with appropriate security settings.

Caveat Emptor - A well-to-do user is given a large amount of input on what to buy to secure their computer and not surprisingly, some of it is false and misleading. Anti-spyware programs that are sold under the pretenses of removing spyware may do just that; installing their own list of parasites instead. The following products have been identified to install spyware, rather than remove it as advertised:

> Spy Wiper / AdWare Remover Gold / BPS Spyware Remover / Online PC-Fix / SpyFerret / SpyBan / SpyBlast / SpyGone / SpyHunter / SpyKiller / SpyKiller Pro / SpywareNuker / TZ Spyware-Adware Remover / SpyAssault / InternetAntiSpy / Virtual Bouncer / AdProtector / SpyFerret / SpyGone / SpyAssault[4]

Payloads & Methods

The most common payload is an ad-rotator or request redirector in DLL form which is generally dropped in a system folder and registered. Once registered, the suspect DLL will then take over various aspects of browsing. Simple searches will be redirected through the parasite DLL, redirecting the user to an un-requested search engine. Complex instances intercept local MIME-type handling for text/html to evade detection from anti-spyware software. Parasites will gather data on user browsing habits, forms filled out, and possibly even keystrokes. Then, this data will be relayed back to a

[4] http://cybercoyote.org/security/spyware.htm#bogus - Spyware and Adware

collection server.

Browser Helper Objects (BHO's) are DLL's that live within the Internet Explorer process space, extending the functionality of Internet Explorer.[5] Microsoft Money and Adobe Acrobat Reader both use BHO's to extend functionality. Money does it by integrating IE's features with its own environment and Acrobat by allowing the IE core to understand and handle PDF. A typical parasite BHO will be the core of the parasite's behavior.

Registry files to assist re-infection are relatively common. If upon reboot the appropriate registry keys have been set, the user will face a never ending cycle of deleting registry keys just to have them come back. These are generally simple files that can be imported easily without noise. They generally contain the installation path for the DLL(s) included with the parasite, browser settings and Run keys[6].

CSS files that exploit the ability to run Javascript code have been known to be dropped, but as this is now (hopefully) widely patched, new parasites are no longer attempting to use them.

Batch files and executables are used to re-install the parasite package when reboots or re-installs occur. Certain parasites[7] will replace system utilities with bogus applications that will launch the real application after re-installing the parasite. Other variants of executables stay resident in memory, refreshing the installation every few seconds.

Distributed code execution payloads present to the spyware distributor a virtual "zombie" net of machines, waiting for a piece of code to be compiled, distributed and then executed across every machine the package has been installed on. This allows spyware companies to resell cycles, space and traffic to third-party companies. Xupiter[8] has been known to utilize this to distribute a component to an online casino. BDE and Gator[9] do much the same thing, but only execute code signed by the creators.

New strains of spyware now have payloads specifically targeted to kill anti-spyware programs when opened, drop /etc/hosts files to block anti-spyware sites, and kill personal firewall processes.

[5] http://support.microsoft.com/default.aspx?scid=kb;EN-US;q179230

[6] HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, ..\Runonce, etc.

[7] CWS.Smartsearch.3 - http://www.spywareinfo.com/~merijn/cwschronicles.html#smartsearch

[8] http://www.doxdesk.com/parasite/Xupiter.html

[9] http://www.doxdesk.com/parasite/Gator.html

The invisible war

Identification and targeting

Identifying and targeting a spyware application is a bit like shooting in the dark. It could be a virus, it could be a worm, or it could be a Trojan. Now, it can also be spyware. Once virus scanners have been run and problems are still manifesting, it's time to move on to less known methods. First, we cover identification.

Basic signs:

- Browser homepage keeps resetting to an unwanted site
- Access is blocked to Internet Explorer -> Tools -> Internet Options, or options change back after reboot
- Random ads popup on desktop when no browser is open
- New search bars appear in IE/Explorer windows
- Favorites mysteriously added
- Browser windows randomly closing
- All searches being redirected
- Unqualified names (http://localname) redirecting to Internet sites

If three or more of the above are true and an updated virus scan has been run, the machine has probably been compromised by parasites. Now, a search engine becomes a necessity.

The community around spyware has exploded, and nothing can take the place of education. Community forums[10] provide up-to-date information on new strains and attack vectors. Whole discussions have been launched discussing the taxonomy of the spyware genus, allowing people to identify common strains and recommend one-stop solutions and signatures. Web forums are also where one-off parasite removers can be found, usually within days of the parasite being reported. Anti-virus companies are starting to take note as well, adding parasites to their malware databases and producing one-off parasite removers as well.

The regedit utility included with Microsoft Windows allows a look into the configuration core of windows. Get friendly with it. Regedit and the registry editing utilities allow a wide range of flexibility in querying, adding, deleting, and merging registry data. Almost every parasite leaves at least one registry entry, most leave five or six in different locations. There are utilities to assist in viewing the registry in the context of spyware. BHODemon and HijackThis are available for free download. Interpreting the results is still not always easy, as entries can be named like system files and mask the parasite.

The basic areas of the registry to search are the following:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

[10] "SWI Forums" URL: http://www.spywareinfo.com/forums/ (23 Mar. 2004)

HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Internet Explorer\Main

An example using the Windows XP command line:

```
C:\>reg query "HKCU\Software\Microsoft\Internet Explorer\Main" /v "Start Page"

! REG.EXE VERSION 3.0

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
    Start Page  REG_SZ  http://www.google.com/
```

Sniff network traffic going to specific Internet hosts. Use a firewall block list that addresses spyware companies. Convert this into a list of host Netblocks. Observing this traffic from known spyware companies and parasite hosts can be used to identify the parasite. Tracing back the ownership of the destination domains to a specific parasite instance is not always possible, but well documented when it is. Tcpdump or Ethereal can be used effectively for this.

A Tcpdump syntax file can be created and run by the following syntax:

```
C:\type c:\ads.txt
host 192.168.99.100 and port 80 or
host 192.168.99.101 and port 80 or
host 192.168.99.102 and port 80

C:\windump –F c:\ads.txt
```

Run an uninstaller like Ad-Aware or Spybot Search & Destroy. The decision to run a spyware scanner is much like the decision to run an anti-virus program; most people don't think about it until it's too late. No single scanner will be able to detect all known parasites, however this can be mitigated by running two or three. This is horribly inefficient, but effective. Rebooting two or three times while using utilities like this is not uncommon, as some bits can only be deleted upon restart.

Inoculation

In a modern Windows environment, you can secure your local computer or domain from most of the simple infection vectors by doing the following:

- Restricting allowed ActiveX controls

  By setting the "kill bit" on ActiveX CLID's, Internet Explorer will not load certain ActiveX controls, regardless of security setting[11]. By listing out known evil ActiveX controls, a large portion of the parasite population cannot install or function. This is

[11] MS KB:"240797 - How to Stop an ActiveX Control from Running in Internet Explorer."

how SpywareBlaster works. This is a registry entry.

- Software Installation Policy
  Inform your employees of what kind of software is allowed on the desktop. Alternately, decide what you really need to run at home. Be wary of file sharing clients and products advertised in spam. This should already be in a general security policy.

- Securing system directories
  Removing user-write permissions for core system directories should now be the de-facto standard in most updated windows installations. Parasites generally install to one of three basic paths, %SystemRoot%, %SystemRoot%\System32 or %ProgramFiles%\. This is only required on NT4/2000 domains. This can be done via Group Policy Object or directly to the file system.

- Privilege separation
  All program installation is done with a local admin account. All patches are applied under the local admin account. The user account that is used for day-to-day purposes has basic user permissions, can't install applications, and has little rights to change the inner configurations of his or her computer. If this does not sound like daily life, this is one step that can stop a majority of spyware dead. With the new Run-As service in XP Service Pack 2, there really is no excuse to log in as an administrator unless there is maintenance to be done. Windows XP Home presents a problem as all local users are assumed to be administrators. This can be done in XP Pro via the Control Panel \ User Accounts.

- Restrict Internet Explorer change rights
  Remove the ability for users to change core configuration settings in Internet Explorer[12] While this may be more draconian than some may wish, it is effective. By denying the user permission to change Internet Explorer core properties, parasites are also blocked from doing so.

- Software Execution Restriction Policy (Windows 2003 only)
  Windows 2003 allows for new ability to restrict software execution on host computers. Paths, Internet Security Zones, file hashes and digital certificates can be specifically allowed or disallowed. This approach allows for very granular policies, and a very tight element of control can be exercised on what program runs on the domain, and by whom. This is done via Group Policy Object.

Regardless of environment, the following steps can be taken to prevent and mitigate the spread of new and more virulent spyware:

- Local users should use a reputable proxy service
  An entire novel could be and probably has been written on proxy methods,

[12] Appendix 1.1 (User rights restriction in IE)

however worth mentioning are a few notables. First, almost every (Web) proxy server in the wild has some form of access control lists that can restrict traffic. Squid[13] comes with a rich ACL language built in, allowing you to identify and use a number of properties to grant or restrict access. The Microsoft ISA Proxy Server allows for a variety of methods to sanitize and block content as well. A proxy server that has been properly secured and up to date can effectively protect an entire network of users. This should not be the only method.

- An inoculated /etc/hosts file
  While not an ideal solution, the low-tech methods do work. By taking a list of sites that are distribution or connection points for known spyware parasites one can then create a hosts file containing a bogus entry for each one of these sites. Most lists like this use 127.0.0.1 (localhost) as the IP. Unfortunately, if your users must be able to see legit ads then the Internet-provided lists will likely have to be trimmed by hand.

- IDS monitoring of internal networks
  Watching your network from the inside might seem a bit redundant at first, but the benefits of an early warning system on the inside are clearly recognized. Snort provides a platform that a few enterprising users have created rule sets for[14], both to detect the presence of spyware tapping from the outside and from successfully compromised machines inside. Most of these rules are simply logical extensions of blackhole lists used in firewall configurations converted to be used with Snort. With an IDS in place on your local network, you can detect the abnormalities that spyware exhibits. When an ad-rotator finally calls home to pop-up an ad, you have a log of the compromised machine and with some accuracy, the possible strain of spyware.

- Block addresses at the border
  Rules exist for personal firewalls, netfilter and most brands of routers. A Google search for "iptables + spyware" turned up five different lists within the first 100 results. This is a very rapidly moving target, and the rule sets are updated often. Kerio personal firewall sets and IPtables are most common. By rejecting (or in some cases silently dropping) packets from or to spyware host sites, you can successfully wall off any method of traffic.

- Spyware uninstallers, eliminators
  Ad-aware, Spybot Search & Destroy, Spyware Blaster and Spyware Guard give some cost-free help. SpySweeper, Xblock and Spycop offer a commercial alternative. All overlap in different areas, but any two or three are all that should be necessary. Ad-aware and Spybot S&D are traditional scanners, opening directories and files, searching for telltale signatures of known parasites. Spyware Blaster restricts ActiveX installation by blacklisting by class ID. Spyware Guard mimics the behavior and function of real-time virus scanners, alerting users to potentially harmful parasites.

[13] http://www.squid-cache.org/
[14] Snort Rule Sets.

- Helpdesk policy

  Establish clear guidelines and instruction for the removal of parasites. Once a machine is known to be compromised by spyware, a burned CD with the freeware tools can save hours. What kind of tracking is to be done? Will your helpdesk support users with spyware? Policy questions are not answered easily but with some best practices in mind, the answers clarify. For all intents and purposes, spyware and adware should be considered as hostile agents, possibly engaging in a number of quasi-legal activities.

Conclusions

Spyware presents an entirely new laboratory in which to work for the malware world. It's a new set of infection vectors and payloads. The capabilities of parasites are limited only by how secure a given application is, rather than an underlying operating system. Trust chains are not broken by spyware, simply bent for individual purpose.

While the focus of this document has been primarily on Windows, it should be noted that UNIX-based systems could theoretically be vulnerable to exploitation by spyware. Mozilla, Firebird and Opera are all parasite-free browsers, and suggesting a switch of browser across an entire company is generally not apropos.

Spyware is traditionally sloppy. Usually very easy to identify, and as we have all been pained to learn, full of bugs. Newer strains of spyware are more virulent and harder to detect or remove. Payloads can become highly questionable when they start reporting back personal data from infected computers. Spyware is following its malware roots, except for one slight divergence. While malware creators create what they do for any number of reasons, Spyware—at least for now—is generally created to sell something. It may be the last month of browsing habits, or the ability to install unwanted Internet gambling software. Spyware is driven by the ability to sell something. Spam is also driven by the ability to sell something, and neither will go away until the money dries up.

As virus writers gear up and prepare for the next buffer overflow, spyware manufacturers are dreaming up new and invasive payloads. Spammers and Virus writers are suspected to be working together at some level, as there are viruses currently in circulation that attack Anti-spam resources[15]. It is not a stretch to see the marriage of spam, spyware and malware.

As much as policy allows, a no-tolerance approach should be taken towards spyware, eliminating it at the border, removing the ability for it to install, and following up with an occasional scan. Refine with a touch of ongoing user education though policy and feedback. Users should have an idea of what spyware is, what it does, and where it generally comes from.

Spyware will get "better"; better at doing its job without your knowledge.

[15] In fact bringing down a few Realtime Blackhole Lists (RBL) (Sobig.F / suspected)

Appendices

Appendix 1.1 (Restrict Internet Explorer change rights)

```
\Default Domain Policy (Or appropriate GPO)
    \Machine Configuration
        \Administrative Templates
            \Internet Explorer
                Security Zones: Do not allow users to change policies = Enabled
                Security Zones: Do not allow users to add/delete sites = Enabled
                Disable Automatic Install of Internet Explorer components = Enabled
    \User Configuration
        \Windows Settings
            \Internet Explorer Maintenance
                \Connection
                    <Import domain wide network and auto-proxy settings>
                \Security
                    <Import domain wide security zones and privacy settings>
        \Administrative Templates
            \Internet Explorer
                \Internet Control Panel
                    Disable the Security page = Enabled
```

Appendix 1.4 (Example /etc/hosts file)

```
127.0.0.1 localhost
127.0.0.1 UGO.eu-adcenter.net
127.0.0.1 VNU.eu-adcenter.net
127.0.0.1 ad-adex3.flycast.com
127.0.0.1 ad.ca.doubleclick.net
127.0.0.1 ad.de.doubleclick.net
127.0.0.1 ad.fr.doubleclick.net
127.0.0.1 ad.jp.doubleclick.net
127.0.0.1 ad.linksynergy.com
127.0.0.1 ad.nl.doubleclick.net
127.0.0.1 ad.no.doubleclick.net
127.0.0.1 ad.sma.punto.net
```

References

“CIACTech02-002: Microsoft Browser Helper Objects (BHO) Could Hide Malicious Code” UCRL-MI-119788. 2 Apr 2002.
URL: http://www.ciac.org/ciac/techbull/CIACTech02-002.shtml (23 Mar 2004)

Clover, Andrew. “and.doxdesk.com parasite database”
URL: http://www.doxdesk.com/parasite/ (23 Mar 2004)

Klien, Tony. “CLSID List”
URL: http://sysinfo.org/bholist.php (23 Mar 2004)

Wyden, Ron. Boxer, Barbra. Burns, Conrad. “S2145 SPY BLOCK Act” (27 Feb 2004)
URL: http://wyden.senate.gov/leg_issues/legislation/s2145_spyblock.pdf (24 Mar 2004)

“Spyware and adware” 25 Mar 2004.
URL: http://cybercoyote.org/security/spyware.htm (25 Mar 2004)

“179230 - SAMPLE: IEHelper-Attaching to Internet Explorer 4.0 by Using a Browser Helper Object” 3.0. 12 May 2003.
URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q179230 (23 Mar 2004)

Merijn “The CoolWebSearch Chronicles” 7 Mar 2004.
URL: http://www.spywareinfo.com/~merijn/cwschronicles.html (25 Mar 2004)

"240797 - How to Stop an ActiveX Control from Running in Internet Explorer.” 3.0. 06 Dec 2003.
URL: http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q240797&ID=KB;EN-US;Q240797 (23 Mar 2004).

“Spybot S&D”
http://www.safer-networking.org/ (26 Mar 2004)

“Spyware Info” 15 Mar 2004.
URL: http://www.spywareinfo.com (26 Mar 2004)

“Tom’s Computer Repair, Tips, Spyware” 2003
URL: http://www.womelsdorf.com/TIPS/adspyware.html (20 Mar 2004)