SPYWARE EXPLAINED

ANTI-TROJAN.ORG TECHNICAL WHITE PAPER

Author: Jonathan Read

Part 1

Spyware Explained

The Birth of Spyware

The dot com crashes of the late 90’s brought about a revolution in internet advertising. Banner advertising companies where going broke because internet users where getting sick of the annoying animated gifs. People would just ignore these adverts or worse still the emergence of firewall software like WRQ’s atguard actually blocked banner adverts rendering them useless. Hackers realised that they could make easy money with proxy clicking programs, which also led to the demise of many of the pay per click advertisers.

Advertisers realised that if they where to still make money online they would have to change tactics. Many advertisers turned to affiliate programs where publishers would get paid for actual sales made, not just for a click on a banner. The other advertisers thought of new ways to advertise, these advertisers found a way that would allow them to advertise products without even having a website or servers serving adverts. This is how spyware emerged.

At first spyware was bundled into freeware and shareware applications, but word quickly spread around the internet about this new threat and so advertisers had to resort to dirty tricks. Many spyware developers now use hacker exploits to install spyware onto computers.

If you use any of the popular operating systems, chances are you will have spyware. It is probably safe to say that most home users have LOTS of spyware on their computers. This spyware is just sitting there, quietly informing the advertisers on your music listening habits, your web browsing habits or perhaps what your favourite programs are. If you are unlucky you will be infected with a nastier spyware application like a porn dialer. Porn dialers are programs that ring up sex lines usually overseas. The phone bills from porn dialers can be huge, last month my elderly neighbors received a phone bill for over 8000 dollars, all from a porn dialer ringing up a European number from a New Zealand based address.

Browser hijacking is a common way spyware programs get you to visit their website. If your homepage keeps changing to an advertisers web page, no matter how many times you have set your favourite homepage, then you definitely have spyware. More often then not, you will also have pop up windows appearing in your browser, even if you are offline!! These can advertise mundane products but a lot of the time you will be flooded with tacky porn sites. A very good tool for dealing with browser hijacks is a program called hijackthis you can find this program at the following URL, along with instructions on using it http://tomcoyote.com/hjt/

Spyware not only invades your privacy, it also causes stability issues with most operating systems. Spyware coders don't really care how sloppy their coding is, why would they? They are only after money. Poor coding leads to spyware damaging a users system, sometimes just visiting a site that has spyware exploits embedded into the html can bring your system to a crawl. Most anti virus applications do not recognize spyware so removing spyware from an infected machine can be difficult. If a novice attempts the removal, it can even be dangerous to the system, as registry editing is always involved.

As more legitimate companies move towards bundling spyware with their software it is very important that all computer users start to use spyware scanners. Spyware scanners are a relatively new phenomenon. There are a lot of spyware cleaners around but not all are reputable. Companies that also make spyware have even made some spyware cleaners!!! I am sure if virus coders started making anti-virus products the industry would be concerned.

How Can I tell I have Spyware?

Not all symptoms are easy to diagnose, but the easy symptoms to recognize include:

- Your computer slowing down to a crawl.
- Porn sites popping up in your browser when you are surfing the net
- Your computer mysteriously dials up phone numbers during the middle of the night, normally to expensive porn chat lines leaving you with a huge bill.
- When you enter a search into your search bar, a new and unfamiliar site handles the search.
- New sites are added to your favorites list without you adding them
- Your homepage has been hijacked and even though you remove the new site it keeps coming back
- You get pop up adverts that address you by your name, even when your computer isn't connected to the internet.

How should I choose a spyware scanner?

Some of the best scanners are freeware, so if you download a scanner and it detects a heap of spyware then pops up a link to purchase the software to clean the spyware then it could be just a scam. The best freeware scanners include:

-**Spybot S&D:** http://www.safer-networking.org
-**Adaware**: http://www.lavasoftusa.com

It is important that if you make any major changes to your system that you first consult a good search engine (google.com) too see what it has to say about the problem. Removing spyware with anti spyware software should be straight forward, but it is best to be safe then sorry.

Prevention is often the best medicine, and choosing a non MS browser can significantly reduce your chances of being infected with spyware from internet exploits. Blocking active-x scripting and java scripting can also add extra security to your system. Most good firewalls will block malicious coding; investing in a good firewall would be a great idea. Always keep up to date with the latest windows updates.

Sites to avoid

Free porn sites; avoid these at all costs. There normally is a reason these are free, and more often then not its because you end up infected with a porn dialer.

Warez and cracks: This is dodgy anyway; the webmasters who run these sites don't care too much about ethics. You will find 95 percent of these sites have spyware embedded into their html code somewhere.

Mp3 sites and P2P software: These are well known to be sources of spyware, many of the big named P2P and file sharing programs come bundled with spyware so if you must use these programs then check on the internet before installing.

Part 2

The Technical Aspects of Spyware (system admin information)

Detecting spyware processes in MS windows based machines.

System admins need to pay careful attention for spyware processes that may have infected machines on their network. An infected machine cannot only pose a security risk from remote intruders; it can also mean that that particular area of the network may need auditing to strengthen security.

It is important to use a good process monitor, Windows 9x machines do not come with any process monitoring software as such, and I recommend using a third party application on all MS Windows operating systems to manage system processes (this includes XP/NT/2000 etc). Wintasks Pro is probably one of the best process monitors available today. The makers of Wintasks pro have set up a process library allowing system admins to make informed decisions when ascertaining whether a process is malicious or not. This process library can be viewed here
http://www.liutilities.com/products/wintaskspro/processlibrary/

Malware will often inject itself into legitimate processes, this is an advanced infection technique and is very difficult, but not impossible, to remove. Process injection has become very popular in the malware world. Many remote access trojans use this form of infection as it can evade rule-based firewalls. Spyware makers have begun to use this technique also. Injecting into the internet explorer process will often allow the spyware internet access; a lot of rule based firewall applications will not see the malware, only the trusted application IE and will allow communication.

System Safety Monitor is a freeware program that will help system admins protect against malware code injection. *"System Safety Monitor (SSM) is an application-firewalling tool (it is not a "firewall" in traditional understanding, so there shouldn't be any conflicts with your network firewalls). SSM controls which programs are running on* *your computer and what they are doing. For example, SSM can prevent so called "DLL Injection". Also, SSM will notify you whenever a program you want to start was modified. In addition, SSM can constantly check your registry and alert you, when an important modification was made.”* http://maxcomputing.narod.ru/ssme.html?lang=en

Detecting Spyware Auto-Start Methods in MS Windows Based Machines

Removing the auto start method is one of the most important steps in disinfection. If a system admin can remove the malware entry from auto start method used, the malware will fail to execute on reboot (even if the executable files have not been removed).

Below is a list of commonly used autostart methods for malware:

Autostart folder

All items in the autostart folder will autostart

Win.ini

```
[windows]
load=malware.exe
run=malware.exe
```

System.ini

```
[boot]
Shell=Explorer.exe malware.exe
```

Autoexec.bat

```
c:\malware.exe
```

Registry Shell open

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command]
```

A key with the value "%1 %*", will be executed each time you execute a .exe file. "malware.exe %1 %*" .

Alternate Registry Keys

```
[HKEY_CLASSES_ROOT\.exe] @="myexefile"]
[HKEY_LOCAL_MACHINE\Software\CLASSES\myexefile\shell\open\command\
@="malwaree.exe %1 %*"]
```

winstart.bat

A batch file that autostarts with windows.

Main Registry

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
```

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]

wininit.ini
This file is called upon when windows loads, it is then deleted.

When editing system.ini pay careful attention to the *Shell=Explorer.exe malware.exe* line. Only delete the malware entry, DO NOT DELETE Explorer.exe, if you do the system will not boot into windows.

An invaluable tool for system admins is Start_ups.exe http://www.pacs-portal.co.uk/startup_pages/start_ups.exe, this program features over 4000 different start up entries, and many are malware. System admins can use this tool to search for suspected spyware start up entries, avoiding damage caused by deleting legitimate entries. A non OS specific HTML version can be downloaded here http://www.pacs-portal.co.uk/startup_pages/startups_all.zip; it has all the features of the executable but can be run on all operating systems (that support html).

Configuring Internet Explorer for your Network Users
The following settings is the bare minimum that all IE users should have. If you are a system administrator, it is your job to make sure that the network users at least have these settings enabled.
Close all running instances of Internet Explorer and Outlook Express (use a process monitor if you cannot close these)
Control Panel > Internet Options > Click on the "Security" tab
Choose the "Internet" icon, and click "Custom Level"

- "Download signed ActiveX scripts" **choose**: Prompt
- "Download unsigned ActiveX scripts **choose**: Disable
- "Initialize and script ActiveX not marked as safe" **choose**: Disable
- "Installation of Desktop items" **choose**: Prompt
- "Launching programs and files in a IFRAME" **choose:** Prompt

NEXT, Click on the "Content" tab, Click the "Publishers" button choose then click "Remove" any unknowns, click Ok

Finally, Click the advanced tab, untick "Install on demand (other)", and click Apply or Ok

Using A Hosts File to Block Spyware Infected Hosts

A simple yet effective way of blocking spyware-infected servers is to add them to a host file. Creating a host file is straightforward. Open up a text editor and at the very top of the text file type:

```
127.0.0.1  Localhost
```

Now you can add the spyware-infected hosts underneath like this

```
127.0.0.1  iads.adroar.com
127.0.0.2  lists.adroar.com
127.0.0.3  advertisingvision.com
```

Once a good list of adware servers has been made, save the file as hosts (not hosts.txt just hosts). Place this file in the appropriate directory:

Windows XP

C:\WINDOWS\SYSTEM32\DRIVERS\ETC

Windows 2K

C:\WINNT\SYSTEM32\DRIVERS\ETC

Win 98\ME

C:\WINDOWS

When a computer tries to go to the malware-infected server, the hosts file will block it, instead of going to the intended server, the server address will point locally rendering the spyware useless (or blocking spyware from infecting the computer from a remote location). You can download an excellent hosts file here http://www.mvps.org/winhelp2002/hosts.txt; it has a huge database of spyware, malware and parasitic servers and will become a valuable asset in any system admins arsenal of protection.

Spyware and security resources:

http://www.spywareinfo.com
http://www.coast-info.org/glossary.htm
http://www.intranetjournal.com/spyware/
http://www.anti-trojan.org/
http://forum.gladiator-antivirus.com

About the author:

Jonathan Read is the webmaster for the worlds largest anti trojan website http://www.anti-trojan.org

Jonathan Read is a respected authority on remote access trojans and works as a security consultant in New Zealand.