

Spyware: Risks and Prevention

*Martin Overton
IBM, UK*

About Author

Martin Overton, IBM

Martin currently works for IBM [EMEA Managed Security Services Delivery (MSSD) core team] as a malware/anti-malware specialist, and is part of the Global Virus Emergency Team as well as the World-Wide Threat Team.

He is a regular speaker at the Virus Bulletin International Conferences, and has lost count of the many other presentations he has done and is a regular contributor to the Virus Bulletin periodical.

Martin is a charter member of AVIEN, a WildList reporter, a member of the Anti-Phishing Working Group and a founder member of the UK ISS User Group (UKISSUG).

To date he has accumulated over sixteen years of experience in investigating and combating viruses, Trojans and related malicious software (malware).

His hobbies, when time allows, include reading (mainly science fiction and science/technology/history books), astronomy, keeping a number of bugs (tarantulas and scorpions); and is a member of the British Tarantula Society. If this doesn't mark him as being weird enough, he also likes snakes (owning a Californian Kingsnake). Oh yes, and he does some computer programming. Occasionally his wife and son get to see him!

Contact Details: 51Cook Road, Horsham, West Sussex, RH12 5GJ, England, phone: +44 2392 563442, email: overtonm@uk.ibm.com.

Keywords

Spyware, Malware, IDS, IPS, Firewall, Policy, Education, Bots, Dialler, Trojan

Abstract

Spyware has grown over the last two years from a minor annoyance to what it is today; a major headache for companies and academia (most of them just don't know it yet) and home users alike.

This paper will investigate the growth of this threat and the 'cart-load' of risks and issues that Spyware and related risks bring to the corporate table. Furthermore it will investigate what the security staff in corporations can implement to address the risks and their company's liability, including.

- *Policy*
- *Education*
- *Firewalls*
- *Proxies*
- *Intrusion Detection Systems*
- *Anti-Virus tools*
- *And last but not least, Anti-Spyware tools.*

The processes, procedures and other solutions and guidance offered in this paper will come mainly from real-world experience of tackling spyware and related issues/risks.

Disclaimer:

Products or services mentioned in this paper are included for information only. Products and/or services listed, mentioned or referenced in any way do not constitute any form of recommendation or endorsement by IBM or the papers author.

*This paper was written for, and presented at, the 2006 EICAR conference held at Hotel Hafen,
Hamburg, Germany between April 29th – 3rd May 2006.*

I would welcome any constructive feedback on this paper and its content.

Introduction

This paper will discuss spyware, what it is, some of the ways it gets on to your systems and finally what tools and methodologies you can use to combat it. Before we start let us cover a few definitions so that we all know what I mean by the relevant terms used in this paper.

I would strongly suggest that unless you have in-depth knowledge of Spyware and related malware that you try and obtain copies of the books/papers/articles listed in Appendix A.

What is Spyware

I will use the following definition:

"Spyware is the generic name for any application that may track your online and/or offline PC activity and is capable of locally saving or transmitting those findings for third parties sometimes with, but more often without your knowledge or consent".

If you want the full definition of what makes something spyware, then feel free to look here: <http://www.antispywarecoalition.org/documents/definitions.htm> However, don't expect it to be very concise!

Just like virus and other malware nomenclature, if you ask several experts, you'll probably get multiple and sometimes opposing definitions, you have been warned.

Spyware comes in many forms including adware, key loggers, trojans, browser hijackers, and diallers.

In fact most malicious spyware such as Trojans, key loggers, password and information stealers, bots and remote access Trojans have been detected by anti-virus products for a number of years. Spyware is now used to group these threats into a 'genus', although personally I would group them all in the genus 'malware' and be done with it. All the categories and sub-categories being banded about only confuse those that are outside the industry, including potential customers.

According to Wikipedia¹ *"The first recorded use of the term spyware occurred on October 17, 1994 in a Usenet post that poked fun at Microsoft's business model."*

They go on to state: *"However, in early 2000 the founder of Zone Labs, Gregor Freund, used the term in a press release for the ZoneAlarm Personal Firewall. Since then, computer-users have used the term in its current sense."*

Wikipedia also state the following about the creation of the first so-called 'Anti-Spyware' tool:

"In early 2000, Steve Gibson of Gibson Research realized that advertising software had been installed on his system, and he suspected that the software was stealing his personal information... As a result of his analysis in 2000, Gibson released the first anti-spyware program, OptOut"

This paper will focus on malicious spyware, including: Trojans, key loggers and diallers as well as other classes of malware which include or can install spyware functionality such as many bots, remote access Trojans and worms, either as core functions, add-on modules, helpers or other downloaded files or components.

¹ Source: <http://en.wikipedia.org/wiki/Spyware>

Discussion

This section of the paper will discuss, whether spyware is a problem, and if so why. The common ways systems get infected by spyware. What the risks and consequences are of your system being infected by spyware. Then I will cover some of the tricks used by spyware to allow it to hide from anti-malware tools and regenerate itself when removed. Finally I will cover how big a problem it already is and suggest how much bigger a problem it may become.

Then we will move on to how to tackle this scourge. The solutions suggested will range from simple policies and procedures through to education and onto tools; both software and hardware based ones. This will include some generic solutions to help minimise the threat from malware and hackers as well as spyware.

Is Spyware a Problem?

Well, according to a number of surveys it is a problem, a BIG problem. The trouble is that many of those infected may not even be aware of spyware and/or that their system is infected. Furthermore they may be blissfully unaware that their browsing habits, at the very least, or their financial data or every key press they make is actually being recorded, and being sent to the malware/spyware authors to misuse, as they see fit.

- More than 33 percent of system crashes reported to Microsoft were found to be due to spyware.²
- Nine out of Ten PCs connected to the Internet are infected with spyware.³
- A spy audit report published by Earthlink and Webroot in 2004 found an average of 26.5 spyware traces are present on a given PC. In a six-month period, two million scans found 55 million pieces of spyware.⁴
- 92% of corporate IT managers at companies with more than 100 employees claim they have a "major" spyware problem.⁵
- A very recent study by Webroot claimed that Spyware cost firms \$62B in 2005⁶

How do I get infected?

The main target for spyware authors is the same one as for the authors of other classes of malware, this being Microsoft Windows. There have been some cases of spyware being created for other operating systems such as Linux and Mac, but these are a mere drop in the ocean.

There are many ways to get infected with spyware; however the most common ways are via web sites that use scripting, known vulnerabilities or by the author relying on social engineering to get you to install their spyware. Spyware can also get installed as part of a free tool or utility that you downloaded or have installed from some media⁷. Let us look at each of these in turn:

The most common way that spyware gets installed on a computer is by the computer user installing it.

² Source: Microsoft

³ Source: National Cyber Security Alliance, June 2003

⁴ Source: <http://www.webroot.com/company/pressmedia/pressreleases/20040804-spywarereport/>

⁵ Source: Web@Work Study, March 2004

⁶ Source: <http://www.scmagazine.com/uk/news/article/540680/?n=uk>

⁷ Such as CD, DVD, USB Media drives, PDAs, Smart Phones and last but not least floppy disks.

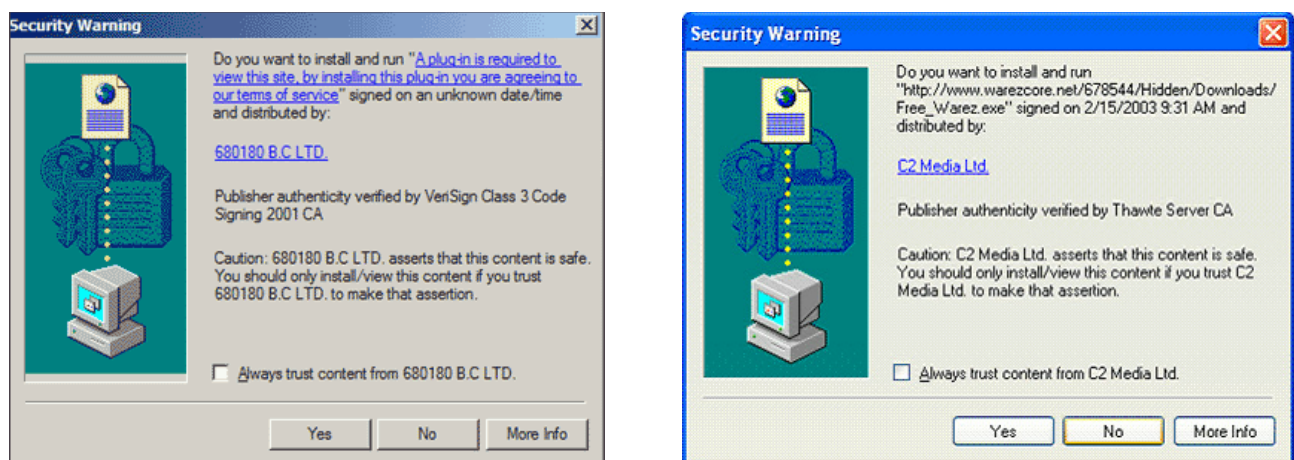
Web browsing:

Spyware authors can also infect a system browsing a malicious website by exploiting vulnerabilities in the Web browser itself or the so-called helpers; plugins [usually ActiveX] such as viewers, java virtual machines, scripting languages such as VBscript or JavaScript [aka Jscript]. They may even take advantage of server side scripting languages such as Miva, PHP or CGI [such as PERL, Python, C/C++/C#, Unix Shell, Fortran, TCL and so on]. When the user navigates to a Web page controlled by the spyware author and/or cyber-criminals, the code on the malicious web page will attempt to attack the browser, or one of the helpers, and download and install spyware on to the visiting computer.

Why is this form of attack so common? Well, over the last few years we have seen the window between a vulnerability being announced and malware exploiting it shrink from years to months, weeks and more often now just a few days. So, this area needs to be addressed in the fight against malware and spyware as many use known vulnerabilities [which have patches available, and occasionally some that don't] to gain access to vulnerable systems.

Some of these vulnerabilities may be used when you visit a website which uses exploit code that your system is not yet patched against. These are commonly called 'drive-by-downloads' or 'drive-by-infections'. In some cases of these types of attacks, such as with the WMF vulnerability you may not even be aware that your computer has become infected. There is no warning, no download prompt, nothing to warn you or tip you off that something nasty and underhand has taken place during your visit to the site.

The next trick used by spyware authors is to use pop-ups to get you to install their wares, usually under the guise of some required plug-in or viewer, see *figure 1 and 2* for examples of what such a plug-in prompt may look like.



Figures 1 and 2: Plug-in Dialogue Box

As you can see this looks like just another dialogue box as you may be offered when visiting a web site that requires a plug-in installed for some of the content offered to be shown or for the page to work correctly. In reality these types of bogus plug-in download prompts when actioned, commonly install either diallers, key loggers or other Trojans.

Wikipedia have this definition of a dialler:

“A dialer (or dialler) is a computer program which creates a connection to the Internet or another computer network over the analog telephone or ISDN network. Many operating systems already contain such a program for connections through the Point-to-Point-Protocol (PPP).

Nowadays, the term "dialer" often refers specifically to dialers which connect without the user's full knowledge as to cost, with the creator of the dialer intending to commit fraud.”

In the case of diallers they replace the original ISP dialler with their own, this then connects to the internet via a premium rate number using the telephone system via a narrowband modem, and this can easily run up large bills. The first the user normally knows about it is several months later when their phone bill turns up.

The good news about diallers is that they can only work if you have a narrowband modem installed and you have the modem cable connected to a phone socket. This is even the case if you use broadband [DSL/aDSL/sDSL] normally. As long as the modem is plugged in it will force the computer to use the narrowband modem rather than the broadband connection.

This type of trick is not limited to those types of installations; they could just as easily be used to install a bot, downloader or mass-mailing worm.

The next two screenshots *figure 3 and 4* shows another common trick, the browser pop-up.

A pop-up is a type of window that appears on top of, and often over the current browser window of the web site that is being browsed. The other common type is the pop-under, which as the name suggests will appear behind the current browser window and is not often seen until the browser is minimised.

Clicking anywhere apart from the windows [X] control will usually either take you to the advertisers site, start a download or try and install a Browser Helper Object or ActiveX component which may be spyware or other malware. This is also commonly used to install bogus anti-spyware tools that are either spyware in their own right or will install spyware on to the system and detect it. The bogus anti-spyware will then inform the user that they have spyware on their computer and inform them that it can only be removed once they have paid for the anti-spyware program.

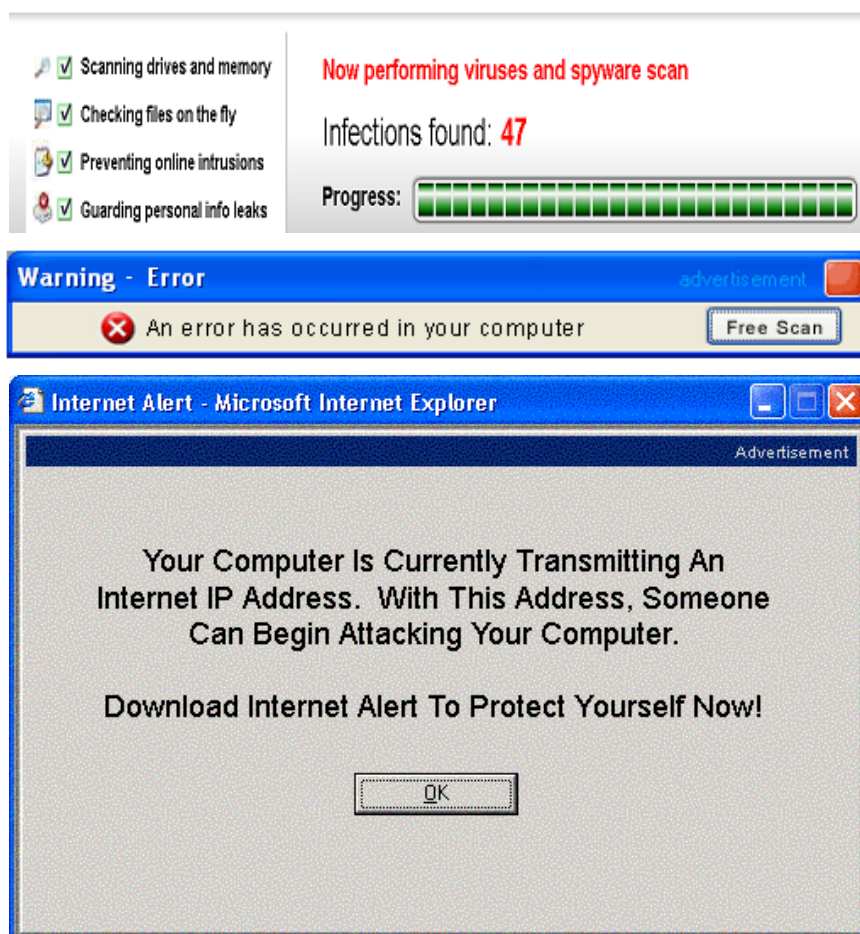


Figure 3, 4 and 5: Typical banner adverts and pop-up

Social Engineering:

Here's a short, but very apt, definition from the Jargon File: '*Social engineering n. Term used among crackers and samurai (hackers for hire) for techniques that rely on weaknesses in wetware (people) rather than hardware or software*⁸.'

It is the human element that is the biggest risk, as no matter how strong your security, it is only as strong as its weakest link; the human behind the keyboard. "You [they] are the weakest link.....in security" it is a shame we can't say "Good-bye!" to those that refuse to learn.

Furthermore, just to underline just how big a threat social engineering is, Bruce Schneier in his book "*Secrets and Lies*" lists social engineering as one of six 'aspects of the human problem' when focusing on information systems security. He states that social engineering is 'very effective', and that it goes straight to the 'weakest link in any security system: the poor human being trying to get his job done, and wanting to help out if he [or she] can.

In reality, however, social engineering is lots of things and it is even harder to pin-down when it is used in relation to malware, but the key to it all is the following: 'Someone wants something you have (or have access to) or wants you to perform an action (such as disclose information, run a program). To achieve this, the would-be Social Engineer will lie (claim to be someone or something they are not, or that they have access to something they are not entitled to), cheat (forge credentials or get you to run code that does something to escalate rights or install a backdoor by convincing you that it is something else) and steal (data, passwords, identities and/or availability of system resources)'.

In summary, the would-be Social Engineer plays on the natural human tendency to trust, and to want to help others, as a way to get you to do their dirty work for them.

Software:

Another common way for Spyware to get onto a computer is as part of an application which the user has chosen to download and install. This is a problem not just for freeware and shareware as is usually suggested; it can even come on some music CDs, just ask Sony⁹. To say that the Sony incident caused a media storm and a customer backlash would be an understatement¹⁰.

Another area of concern is the growth of bogus anti-spyware software which is either spyware itself or downloads and installs spyware once it has been installed.

Those that use Peer to Peer [P2P] software are also at risk from spyware; just like with other classes of malware, bogus files are often found on these networks claiming to be useful tools, utilities, full applications or movies, music or pictures, which when run will infect the computer instead.

Vulnerabilities:

I have already covered vulnerabilities to a certain extent in the section on web browsing, however vulnerabilities are not limited to just web browser or associated helper application such as plug-ins, toolbars and so on.

Many bots rely on operating system vulnerabilities to force their way onto a new 'victim' computer. Some of these carry key logging or other spyware capabilities or can, once installed download them as requested by the botnet owner.

⁸ Source: <http://www.tuxedo.org/~esr/jargon/html/entry/social-engineering.html>

⁹ See here for one of the original reports disclosing that Sony was using 'rootkit-like' technology on a number of music CDs:- <http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html>

¹⁰ See here for a good overall roundup of the issues, resulting media storm and finally the legal ramifications for Sony:- http://en.wikipedia.org/wiki/2005_Sony_CD_copy_protection_controversy

If you want more details on bots and botnets then I would suggest that you download and read a copy of my Virus Bulletin 2005 paper¹¹ on the subject.

E-mail:

It is becoming increasingly common for spyware to be installed by a downloader which is either spammed out or seeded by a botnet. This allows the spyware author to get a [usually] small executable out, which may be undetected by the anti-malware tools on many systems at that time.

Once the downloader Trojan has been launched it then often proceeds to disable or lower security settings in Internet Explorer, any anti-virus, personal firewall or other security software it can identify. Once the defences are reduced or neutralised the downloader Trojan will then invite in its friends. These could be bots, key loggers, browser hijackers and so on.

Below is an example of why and how this works using a castle as an analogy:

A soldier pretends to be a serf and gains employment in the kitchens of an enemy castle. Once in he is effectively invisible to the guards and immediately takes action. First he drugs the drink for all the soldiers and once they are all unconscious he acts.

He disables or sabotages all the defences he can, and then lets down the draw-bridge, signals to his comrades and their allies. They storm the castle and kill all the sleeping guards and their enemies who own the castle then proceed to rape and pillage at their leisure. The castle is now theirs.

Windows Messenger:

If your system has the Windows Messenger service running and it is not being protected by a personal firewall you may see strange messages. An example of such as message appears in *figure 6*, below.



Figure 6: Typical Windows Messenger service pop-up

The Messenger Service was originally designed by Microsoft for use by system administrators to notify Windows users about their networks. However, some advertisers have started using this service to send information via the Internet.

All Microsoft Windows operating systems (98, ME, XP, 2000, NT) allow anyone on the internet to pop up Windows Messenger Service messages on your screen. The person sending the message may know nothing about your computer, where it is or what it is used for. It is just another target for their messenger service spam, or a way to get the recipient to panic and install their wares. Of course in many cases the wares offered contain spyware or other malware

Now let me make this perfectly clear, this is not, and has absolutely nothing whatsoever to do with the Microsoft instant messaging client, which used to be originally known as Windows Messenger and it now more commonly known as MSN Messenger.

¹¹ http://arachnid.homeip.net/papers/VB2005-Bots_and_Botnets-1.0.2.pdf

Other Malware:

Finally, as I’ve hinted at in the relevant sections above, once any malware has become installed on your computer it can easily invite in [download] and install, other malware including Spyware

So, to sum up, once spyware gets onto your system it won’t be alone for long once one is installed it tends to invite [install] other spyware to keep it company, and to make some money on the side too for its trouble. In other words your computer becomes an open house to malware

Risks

Risk is a difficult area to cover. Most of us understand what constitutes a risk, however everyone’s perspective on risk is different; one person’s acceptable risk [such as mountaineering, motorcycle racing, bungee jumping, or keeping venomous animals (snakes, tarantulas and/or scorpions)] is another person’s unacceptable risk. So, I will cover the areas of risk assuming that we are dealing with a company/institution/person that is inherently risk sensitive or averse.

What are the risks? Many are the same as other classes of malware and as such they fall neatly into the CIA triad:

CIA Triad Principle	Examples of how spyware affects the principle
<p>Loss of integrity</p>	<p>System files modified, deleted or replaced Malicious code injected into system processes or files Security settings altered or removed Security tools modified, disabled or bypassed System used as a mule to store illegal and/or stolen material Data modified, stolen or deleted</p>
<p>Loss of availability</p>	<p>System running slower than before spyware was installed Unable to get to certain sites or re-directed to other sites Windows popup storms Reduced memory and/or disk space Reduced network bandwidth</p>
<p>Loss of confidentiality</p>	<p>Theft of credentials, such as passwords and other account details Intellectual property theft Financial data theft</p>

What personal, financial and other data are the malware authors, and the cyber criminals that are often paying them to create the tools, currently interested in? The following for starters:

- Your name and address.
- Your telephone number(s)
- Your Social Security Number (or the equivalent used outside the US)
- Web site login data, such as Banks, Building Society, eBay, PayPal, ISP, etc.
- Credit-card numbers and .CVV or CVV2¹²
- Bank account details; account number and sort code
- CD Keys [Software Registration Keys/Numbers]
- Software registration keys
- Passport details

¹²More details on CVV and CVV2 can be found here:
http://support.worldpay.com/kb/product_guides/worldaccess/help/security_code_verification.html

- Driving license details
- Identity card details

So, really it is not so much Privacy at stake here, although that is a concern, what the malware authors and those creating and using spyware are really up to in this area is identity theft and fraud. In many ways this area is very similar to what the 419 [Advance Fee Fraud] and Phishing scams are trying to do. However, many bots and other spyware are using key logging techniques and/or are searching your hard drive for the data and handing it over without your knowledge, consent and without any assistance from you.

Identity Theft definition:

Identity theft results from the theft of key personal information. The perpetrator uses the information to create identification and credit cards. Identity theft often results in months of turmoil for the victim. Many people find that they need to restore credit ratings and to be freed from liability for illegal purchases.¹³

The following statistics about identity theft show a worrying trend¹⁴:

- According to 2 studies done in July 2003 (Gartner Research and Harris Interactive), approximately 7 million people became victims of identity theft in the prior 12 months. That equals 19,178 per day, 799 per hour, 13.3 per minute.
- The incidence of victimization increased 11-20% between 2001-2002 and 80% between 2002 -2003 (Harris Interactive). This same study found that 91% of respondents do not see an "end to the tunnel" and expect a heavy increase in victimization. 49% also stated that they do not feel they know how to adequately protect themselves from this crime.
- The Federal Trade Commission (FTC) reports that 27.3 million Americans were victimized by identity theft in the past five years, costing consumers \$5 billion and businesses nearly \$48 billion in 2002 alone.

So, as you can clearly see, the malware authors and those using spyware with key logging and data searching/stealing capabilities are in this for the money, not the fame or the intellectual challenge as has been used as justification for writing malicious code in the past. They have grown up from being the electronic equivalent of vandals and graffiti artists, and have become thieves, nothing more, nothing less. The really worrying part is that many malware authors are in the pay of organised crime syndicates and it can only be a matter of time before we see our first millionaire malware author.

Intellectual Capital

In many ways this is very similar to the issues with privacy and identity theft; except the data is not of a personal nature, it is sensitive or valuable information that can be sold to information brokers or may even be used to blackmail the company by threatening to send the information to a competitor unless they, the cyber-extortionists, are paid. They may even threaten to implicate a particular employee as being in league with them, either to get money or more data [intellectual property] from them or the company they work for.

Let us say that you work for a military, financial, medical or indeed any organisation or institution that has intellectual property that would be worth something to another party, let us say a competitor in your area of business or expertise. How much damage would it cause you personally or your company/institution if that data was copied, millions, billions?

Many bots and other spyware classes have the ability to search for data. Some also open backdoors to allow full access to the file system of the infected system as well as any system that it is

¹³ Source: http://www.cscic.state.ny.us/msisac/webcasts/05_05/info/glossary.htm

¹⁴ Source: http://www.wholesecurity.com/threat/identity_theft.html

connected to, such as file and print servers. Imagine a firewall administrator whose system is infected; imagine if the firewall rule base was remotely modified by a malicious third party.

Spyware can be used to turn on microphones and web cams and record you or your meetings, scary huh?

So, what can I do to protect myself?

One thing you should be aware of is that there is no 100% solution to the spyware problem. Any company that informs you that their product offers 100% protection from spyware are either naïve or just don't fully understand the real problem.

However if you approach the problem in the right way, then you can minimise the percentage gap from that perfect 100%. A well-designed approach can be expected to give a 98-99.5% protection from spyware and their effects.

The key thing to take onboard is that you or your company policy should advocate so-called 'Safe-Hex'¹⁵.

Policy and Procedures

Policies and procedures are the foundation of your company's security stance, it will also show how seriously you take security, or not as the case may be.

Just like foundations for a building, unless they are of a good quality and built on firm principles [or ground] then they will fail, crumble or sink without trace, leaving you or your company exposed to the elements; be they physical or technological.

The human element of security is the hardest to address, due to the general lack of interest in security which most end-users display, even to the extremes of openly flouting the rules and ignoring the security policies and procedures in place, much to the chagrin and disgust of the security staff that created them to protect their companies systems and networks¹⁶.

Policies should not contain product names or detailed solutions, these should only be placed in procedure and technical solutions documents. All security policies and procedures [and related documents] should be reviewed at least once a year. This will enable new threats to be discussed and addressed and the relevant documentation updated to reflect this.

Your policy should include a statement informing staff that downloading and installing unauthorised software is not permitted. Any overrides of this policy should be signed off by the security department.

Use the K.I.S.S¹⁷ approach for your anti-malware policy. The reason for keeping it simple is so that your staff can remember it.

Passwords

As many bots now have the ability to perform dictionary attacks to try and gain access to your system the need for good quality passwords, or even better pass-phrases is an absolute must. A dictionary attack is where a 'list' of passwords is tried, one after another until the list is completed, or access is gained to the system being attacked.

I'm currently not aware of any bots or other malicious spyware which carry out brute forcing of passwords and/or pass-phrases; however I do expect this to happen before too much longer. A brute-force password attack would try every combination of numbers and letters [and maybe other non-standard ASCII characters too] until it gets access or runs out of combinations.

¹⁵ You will find a good safe-hex description here: - <http://www.claymania.com/safe-hex.html>

¹⁶ Source: You are the Weakest Link, Goodbye! – Malware Social Engineering Comes of Age – Martin Overton - Virus Bulletin March 2002 pp 14-17

¹⁷ **Keep It Simple Stupid**

There are stand-alone tools out there that will perform these attacks, such as John the Ripper and Lophtrcrack on both Windows and *NIX systems.

We may also see bots and other malicious spyware trying to steal password hashes instead of the plain-text password, as a number of tools exist that have pre-hashed [computed] thousand or millions of passwords/phrases and then it is just a matter of comparing the stolen hash against them until a match is found. These types of attacks are generally referred to as Rainbow tables¹⁸. As an example of the power and speed of this approach using a set of Rainbow Tables of 64GB which covers the following characters [ABCDEFGHIJKLMN0PQRSTUVWXYZ0123456789!@#\$%^&*()_+~`[]{}|\:;'"<>.,?/] and key space [7555858447479 possibilities which equates to 2^{42.8}] will break any 14 character password in a few minutes! [Based on at least a fast Pentium 4 based PC]

Now, imagine spyware which steals the LMHashes from Windows systems or Unix MD5 or SHA1 hashes and passes them off to such a system.

Education

I commented about the 'human problem' [aka Wetware] in a Virus Bulletin article back in 2002 which stated that *"the overall view of most end-users that security is an IT issue, and therefore not their problem. They seem to think that the technology will save them, what they really need to understand is that they are part of the problem, and are currently exacerbating it."*

Education is important, but for most staff a simple security policy and acceptable use policy will be more effective than trying to educate them about all the types of risks out there on the internet. Instead focus on your support and technical staff, as they will probably be more interested and likely to retain the knowledge for a longer period. They may even end up by educating the end-users they visit and rub off some of their knowledge onto them; a bit like 'pollination' but without the mess.

Browsers

The first bit of advice I will offer is to use a browser that doesn't use/support ActiveX, as this is one of the main ways for spyware to get onto your system. I would suggest that you consider using Opera or Mozilla/Firefox instead. A recent study from the University of Washington found that *"Internet Explorer users can be as much as 21 times more likely to end up with a spyware-infected PC than people who go online with Mozilla's Firefox browser"*.¹⁹

Don't get me wrong this won't stop all spyware getting onto your system via a web browser, but it should significantly reduce the risk of spyware getting on to your computer via a browser. Likewise, not visiting the internet's 'grey' areas or its seedy 'under-belly' will help, as many sites in these areas have bogus plug-ins and add-ons which are really spyware.

If you must use Internet Explorer then please make sure that you have it fully patched and set the security up correctly. At the very least set the Microsoft ActiveX support in IE to prompt you. To do this in Internet Explorer, click on Tools > Internet Options > Security > Custom Level, then click the check boxes that force ActiveX controls to ask permission before running.

Kill the Messenger

As mentioned earlier in the paper you should seriously consider disabling the Windows messenger service, as this will help to close one common avenue used to get your staff to install spyware and other malware onto their computers.

Instructions for disabling the Windows messenger service can be found here:

- Windows XP - <http://www.microsoft.com/windowsxp/using/security/learnmore/stopspam.mspx>

¹⁸ More details on Rainbow Tables can be found here: <http://www.antsight.com/zsl/rainbowcrack/>

¹⁹ Source: http://news.yahoo.com/s/cmp/20060210/tc_cmp/179102616

- Windows 2000 - <http://www.microsoft.com/windows2000/techinfo/administration/communications/msgrspam.asp>

Patch and Patch again

According to a new survey 'Two-thirds of U.K. businesses fail to patch²⁰ their Windows desktops and servers. An older survey found 'Patch Management An Ongoing Challenge For Many Companies²¹' with 'only about one in five completely ready for the next virus attack'. Why is this a problem?

For home systems and those not already managed via third party or in-house patch management tools, you should at the very least ensure that all Windows systems are set to automatically check the Windows Update website at least once a week. If your systems run Windows 2000, 2003 or XP make sure you enable the Windows update service via Automatic Updates. This will ensure that updates are automatically downloaded and installed on those systems.

There have been a number of malware using so-called 'Zero-day' exploits. In this case there is no patch from the vendor to actually fix the hole in the operating system or application, and other mitigation techniques are required to partially or ideally completely manage the situation until a patch becomes available. An example of this would be the WMF exploit that surfaced in December 2005, but was not patched by Microsoft until January 2006.

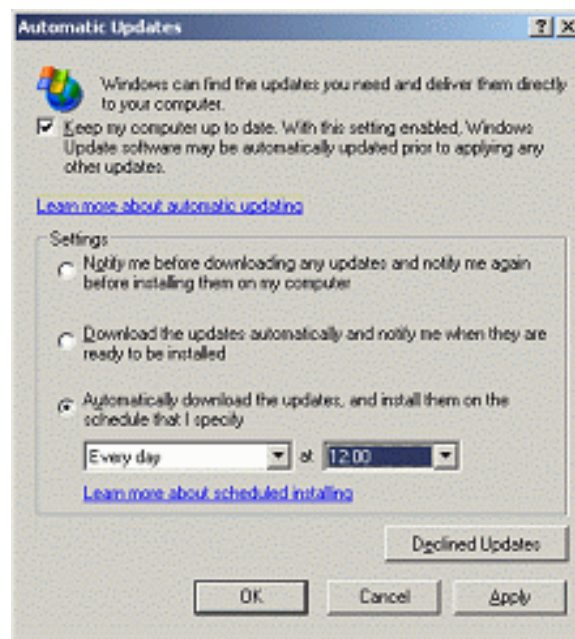


Figure 7: Windows Automatic Update Feature

If you or your customers prefer to control when Windows updates are deployed across their networks then you could use the Microsoft Software Update Server [SUS] or its replacement WSUS²².

Here is some data on WSUS from the Microsoft site:

Windows Server Update Services is a patch and update component of Windows Server and offers an effective and quick way to help keep systems up to date. Windows Server Update Services provides a management infrastructure consisting of the following:

²⁰ Source: <http://www.scmagazine.com/uk/news/article/541973/?n=uk>

²¹ Source: <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=60405225>

²² <http://www.microsoft.com/windowsserversystem/updateservices/downloads/WSUS.msp>

- Microsoft Update: The Microsoft Web site that Windows Server Update Services components connect to for updates to Microsoft products.
- Windows Server Update Services server: The server component that is installed on a computer running a Windows 2000 Server with Service Pack 4 (SP4) or Windows Server 2003 operating system inside the corporate firewall. Windows Server Update Services server provides the features that administrators need to manage and distribute updates through a Web-based tool, which can be accessed from Internet Explorer on any Windows computer in the corporate network. In addition, a Windows Server Update Services server can be the update source for other Windows Server Update Services servers.
- Automatic Updates: The client computer component built into Windows 2000 with SP3, Windows XP, and Windows Server 2003 operating systems. Automatic Updates enables both server and client computers to receive updates from Microsoft Update or from a server running Windows Server Update Services.

There are lots of other third party patch management systems available, and some companies create their own instead of using off-the-shelf patch management tools.

Below are links to articles covering other solutions:

- <http://www.networkworld.com/reviews/2003/0303patchrev.html>
- <http://www.serverwatch.com/tutorials/article.php/3414841>
- <http://www.serverwatch.com/tutorials/article.php/3381211>
- <http://www.serverwatch.com/tutorials/article.php/3424551>

Perimeter and Network Firewalls

To help minimise the chances of infected systems ‘phoning-home’ once successfully infected by a malicious spyware you should ensure that you operate a ‘deny-all’ policy on your firewalls; both at the perimeter and also on other firewalls used to partition your network. If your company/institution does not allow IRC, which is widely used by bots, then ensure that this traffic cannot traverse your firewalls and network by using suitable filtering. For IRC start by ensuring that the default range of ports is not open, these being: 6600 – 7000/TCP.

The same goes for all other network aware applications that need [or want] to connect to the internet or across your own network, use a deny all firewall set-up. Only open up ports that need to be open for internet access. This will help not just in tackling spyware but malicious software in general which wants to connect to the internet to get new instructions, drop its key logs or download new versions of itself or other malware to replace it or supplement it.

Application Firewalls (Proxies)

Where possible proxy all traffic destined for the Internet, this includes IRC, HTTP, FTP and any other protocol or application that can be set-up to use a proxy server. All traffic for these protocols that do not use the proxies should be blocked.

Be aware that there are ways to make any application [even spyware] able to use a proxy, these include using Netcat, SocksCap, and HTTP-Tunnel.

If you do use a proxy, ensure that it is secured and you enable logging so that you can review the logs to look for any suspicious traffic which has passed through the proxy server.

Intrusion Detection Systems [IDS]

IDS Definition: “A system that tries to identify attempts to hack or break into a computer system or to misuse it. IDSs may monitor packets passing over the network, monitor system files, monitor log files, or set up deception systems that attempt to trap hackers²³”.

IDS comes in two main flavours; NIDS [Network based Intrusion Detection Systems] and HIDS [Host based Intrusion Detection Systems] and they both have a place in the fight against spyware especially bots and botnets. Then there is the offspring of IDS, known as IPS.

Back in 2003 the Gartner Group, caused something of a stir by pronouncing that Intrusion Detection Systems (IDS) and their Intrusion Prevention Systems (IPS) offspring were a market failure -- and in fact will be obsolete by the middle of the decade. I believe that the Gartner pronouncement was somewhat hasty in writing off IDS technologies.

The problem is not with IDS and IPS technologies; the problem is managing these tools and technologies and the massive amount of data they produce. Too many companies treated IDS and IPS as they did Anti-Virus; they installed them and left them to update themselves. Very few took the time to look at what the IDS/IPS was finding and fine-tuning them to get the best out of them or [even more worryingly] doing anything about the alerts that were being generated.

Host based Intrusion Detection Systems:

Most HIDS do one or more of the following to detect that a system may have been compromised:

1. Integrity checking
2. System Log monitoring
3. Policy driven behaviour blocking
4. Kernel wrapping
5. Buffer overflow detection

Network based Intrusion Detection Systems:

NIDS Definition²⁴: Monitors all network traffic passing on the segment where the agent is installed, reacting to any anomaly or signature based activity. Basically this is a packet sniffer with attitude. They analyse every packet for suspected nefarious activity, most will also look for anomalies within the protocol.

There are many NIDS products on the market, probably the best known are:

- Snort
- RealSecure

SNORT can easily be augmented by either downloading extra signatures/rules or by creating your own. These signatures may also be able to be used [sparingly] with RealSecure's own SNORT signature support feature, known as TRONS.

A group known as 'Bleedingsnort' maintain numerous bleeding-edge signature/rule sets, not only for malware but new exploits and spyware. However the signatures/rules they produce are indeed 'bleeding-edge' and therefore may be more likely to cause false positives or even worse false-negatives. Of course it all depends on the quality of the signatures/rules produced and the level of testing they go through to minimise both false-positives and false-negatives alike.

Bleedingsnort can be found here: <http://www.bleedingsnort.com>

My own Snort signatures can be found on my own personal website here:

<http://arachnid.homeip.net>. However access is not available without requesting access to the relevant protected section of the site.

²³ http://myphliputil.pearsoncmg.com/student/bp_hoffer_moderndbmgmt_6/glossary.html

²⁴ Source: <http://www.networkintrusion.co.uk/ids.htm> Also has other useful definitions, such as IPS, HIDS, etc.

If you want to know more about creating your own signatures or installing running SNORT then I'd suggest you download a copy of my paper 'Anti-Malware Tools: Intrusion Detection Systems'²⁵ which was written for the EICAR 2005 conference.

Intrusion Prevention Systems [IPS]:

IPS Definition: An intrusion prevention system (a computer security term) is any device which exercises access control to protect computers from exploitation. "Intrusion prevention" technology is considered by some to be an extension of intrusion detection (IDS) technology, but it is actually another form of access control, like an application layer firewall.

Intrusion prevention systems were invented by vendors who decided to make access control decisions based on application content, rather than IP address or ports as traditional firewalls had done. This ability to inspect network traffic at a deeper level confused them with intrusion detection systems, which also inspect network traffic for signs of intrusions.²⁶

Intrusion prevention systems may also act at the host level to deny potentially malicious activity.

According to some researchers, IDS is dead²⁷ and has been replaced by IPS. Examples of IPS products include: IntruShield from McAfee, Proventia from Internet Security Systems and Attack Mitigator from Top Layer. Just like with IDS there are both Network and Host based solutions available.

The beauty of IPS is that it can stop malicious traffic it recognises in its tracks, thereby stopping an infected system infecting others on the network. This includes spyware.

Enterprise Anti-Virus / Anti-Spyware

The use of anti-virus technologies as a detection method for systems infected by malicious spyware is self-evident, as many bots, key loggers, diallers are now reliably detected by anti-virus products.

Because of this we are seeing the inclusion of techniques in many of the modern bots and some other malicious spyware to allow them to disable as many security and anti-virus products as possible. In some cases this functionality may well be the first to be deployed, as a dropper being spammed out. Once run the dropper lowers or neutralises any local defences and then opens up the backdoor, or just downloads more components as required to complete the infiltration.

The thing to remember with anti-virus tools is that they can only [normally] detect malware they know about. New malware variants may well be detected by heuristics; however they are still far from perfect.

Many anti-virus vendors have bought in spyware detection technology, such as via an acquisition or licensing deals. Others have created their own and seamlessly integrated spyware detection into their existing anti-virus products. Either way it is good news for their customers.

A number of the major vendors in both the anti-virus and anti-spyware markets have had their products tested by independent third party testing bodies. One of these bodies is operated by Westcoast labs and is known as Checkmark.

Below you will find a table of products certified under the Anti-Spyware Checkmark.

Anti-Spyware Desktop ²⁸	Anti-Spyware Gateway ²⁹	Anti-Spyware Installed ³⁰
---	---	---

²⁵ <http://arachnid.homeip.net/papers/EICAR2005-IDS-Malware-v.1.0.2.pdf>

²⁶ Source: http://en.wikipedia.org/wiki/Intrusion_prevention_system

²⁷Source: <http://www.esecurityplanet.com/views/article.php/2228631>

²⁸ Source: http://www.westcoastlabs.org/cm-av-list.asp?Cat_ID=8

²⁹ Source: http://www.westcoastlabs.org/cm-av-list.asp?Cat_ID=11

AhnLab Computer Associates Equinet ESET Internet Security Systems Kaspersky Labs McAfee McAfee Consumer Panda Software International SOFTWIN SOPHOS Trend Micro Inc.	Aladdin Knowledge Systems Equinet Finjan Trend Micro Inc.	Webroot Software Inc.
---	--	-----------------------

As you can see this includes not only desktop products but also gateway solutions. There are also hardware [appliance] solutions that can be used to combat malware at the perimeter of the network, these use a variety of techniques such as URL filtering, active content blocking or filtering many of these appliances are policy driven, so that you can decide what should and shouldn't be allowed in to your network. Examples of these devices include:

- Bluecoat WebFilter
- Finjan Vital Security™ Web Appliance
- McAfee Secure Web Gateway

A number of the largest anti-virus vendors offer products that can be centrally managed and will also offer compliance statistics for coverage and how up-to-date the signatures and products are within your network. Some of the management tools have been updated to manage spyware detection and personal firewall components alongside the traditional anti-virus functionality. This allows complete coverage of not only desktops but also servers and in some cases security appliances and other perimeter/network solutions.

The next section will look at some of the many anti-spyware tools that are available, and will really focus on home users solutions and tools that may be useful to support staff in organisations or academia.

³⁰ Source: http://www.westcoastlabs.org/cm-av-list.asp?Cat_ID=12

End User Anti-Spyware tools

If you want spyware protection for your home computer, bearing in mind that home users' computers are more likely to be infected than those in large businesses, then this is the section of the paper for you.

However, if you are looking for anti-spyware tools that might be suitable for use in a small to medium business or tools that may be useful for support staff; be they in small, medium or large businesses or even academia then this section should still be useful to you.

Microsoft may have come late to the anti-spyware party and by acquiring an anti-spyware company [Giant Anti-Spyware] and gate-crashed it, but they have arrived and everyone has noticed them, so lets get the introductions over with.



Figure 8: Microsoft Windows Defender (Beta 2) screenshot.

I have only tested it briefly and my results have been mixed, but it does seem to have reasonable levels of detection, however they do not, in my limited testing seem to be as good as either Adaware or Spybot Search & Destroy.

It does seem that Microsoft are taking spyware seriously, so given that this is a beta the finished product may well end up as a force to be reckoned with.

Microsoft has recently published a fact sheet³¹ on Windows Defender.

Either way I would only suggest that Windows Defender is used alongside either Ad-Aware or Spybot Search & Destroy or an anti-virus product that has good spyware detection built in.

One of the anti-spyware tools I suggest that home users should consider is Ad-Aware. The product is easy to use, accurate and signature updates are regular. The free version will do on-demand scans and clean, however if you want on-access protection you will have to buy the Plus edition. This will get you the Ad-Watch on-access component that will block spyware as it tries to download or install.

³¹ Which can be found here: <http://download.microsoft.com/download/e/2/8/e28d34ec-4775-4626-ac19-a1b0e95e458c/DefenderBeta2FS.doc>



Figure 9: Ad-Aware SE screenshot.

Likewise, I also suggest Spybot Search & Destroy to home users, and technical support staff too for cleaning up spyware infected/infested computers on their networks. Like Ad-Aware it works in two modes, on-demand and it also has an on-access component, known as Tea-Timer which not only will block spyware in real-time it also monitors the registry.

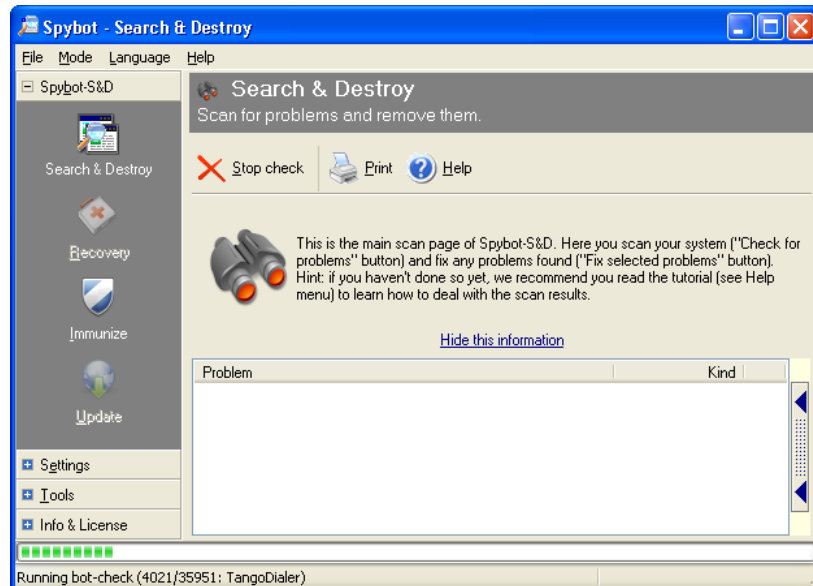


Figure 10: Spybot Search & Destroy screenshot.

Both of these anti-spyware tools well respected and updated regularly to detect new threats and are available in many different languages.

Before I finish this section of the paper, I would like to bring your attention to the fact that you need to be very careful when selecting an anti-spyware solution/tool, as there are a number of them that are spyware in their own right. You can find a list of the known 'bogus' anti-spyware and anti-malware tools here: http://www.spywarewarrior.com/rogue_anti-spyware.htm

Other useful tools:

This section is very much for the technical support staff that need to be able to diagnose and clean up the computers which get infected/infested with spyware in their organization.

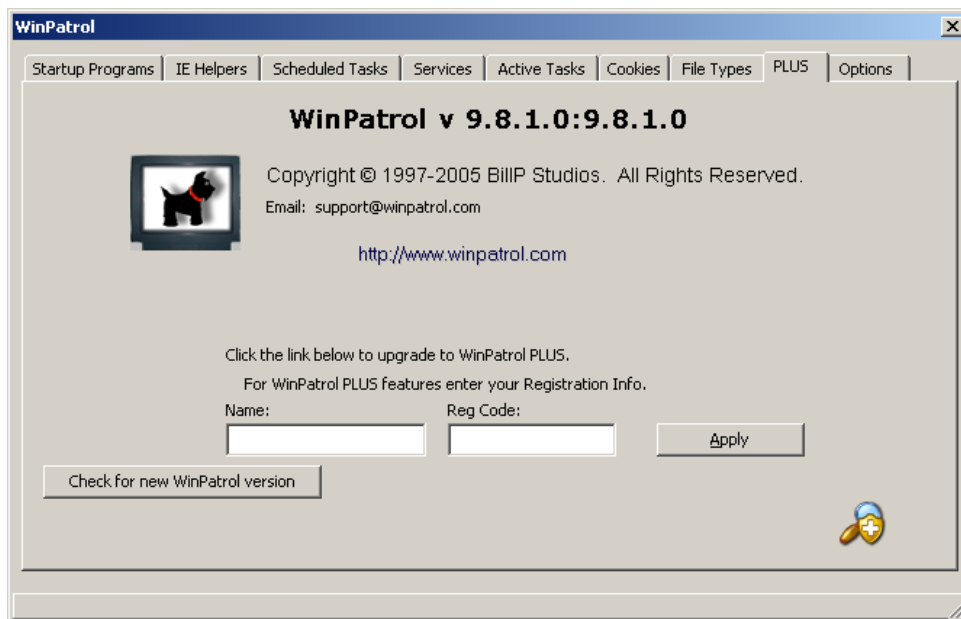


Figure 11: WinPatrol screenshot.

WinPatrol is an interesting tool described by its author as a “*robust SECURITY MONITOR, WinPatrol will alert you to hijackings, malware attacks and critical changes made to your computer without your permission.*”

It is a rather useful watchdog tool, as it monitors numerous parts of the operating system and key applications, such as Internet Explorer. It is also a useful diagnostic tool, not unlike HijackThis, which I will cover a little later on. However, unlike HijackThis, WinPatrol regularly checks the system areas monitored and warns you about any changes. You get to decide whether the change is allowed or not.

It has functionality that is found in a number of individual diagnostic tools, such as Sysinternals autoruns³² and a number of Windows tasks, such as displaying the current active tasks and services.

Another excellent diagnostic tool is HijackThis³³.

This is how the author describes it:

“A general homepage hijackers detector and remover. Initially based on the article Hijacked!, but expanded with almost a dozen other checks against hijacker tricks. It is continually updated to detect and remove new hijacks. It does not target specific programs/URLs, just the methods used by hijackers to force you onto their sites. As a result, false positives are imminent and unless you are sure what you're doing, you should always consult with knowledgeable folks (e.g. the forums) before deleting anything.”

³² Which can be downloaded from here: <http://www.sysinternals.com/Utilities/Autoruns.html>

³³ Which can be downloaded from here: <http://www.spywareinfo.com/~merijn/downloads.html>

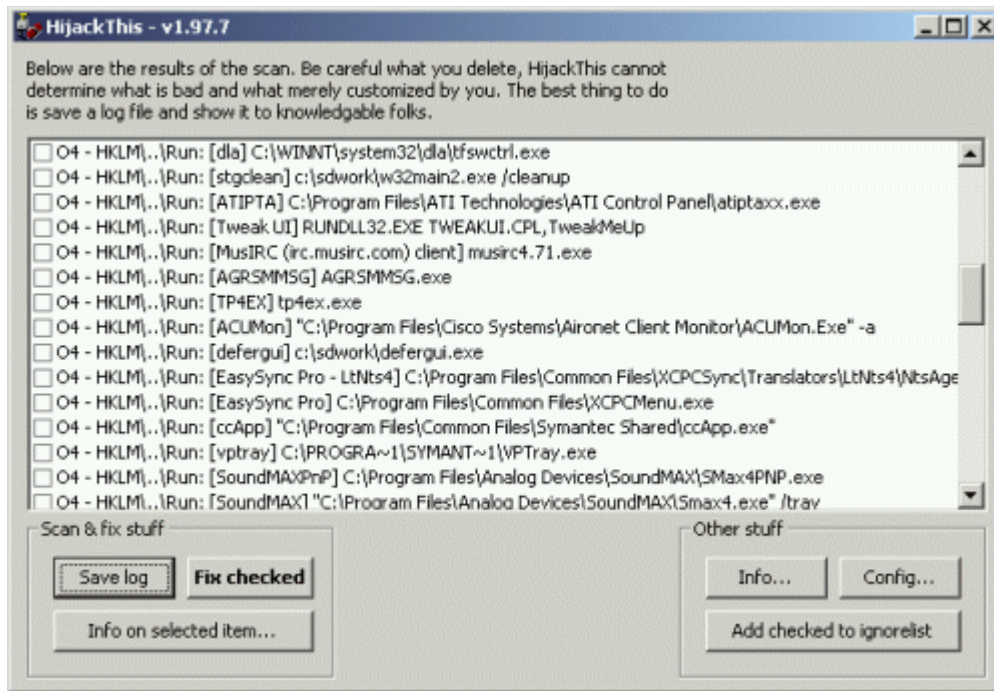


Figure 12: HijackThis screenshot

This tool is not for non-techies, luckily some kind soul has come to the rescue to assist in understanding the raw log files produced by HijackThis. This online tool is known as the ‘HijackThis Log Analyser³⁴’. This is a useful site for turning the output of HijackThis into something that means something to most end-users, not just techies or propeller-heads.

Occasionally no matter how good your anti-virus or anti-spyware tools are, you may come across some spyware that you just can’t remove, or if you do, it just comes back again. The most pernicious of these is one known as CoolWebSearch. This spyware is constantly evolving and there seems to be an arms race in progress between the creators of the spyware and the creators of the anti-dote for it. This anti-dote is known as CWS shredder³⁵.

CWS shredder was acquired by Intermute which has now been acquired by TREND MICRO. It detects the new Cool Web Search variants, and CWS shredder has been incorporated into the new Trend Micro Anti-Spyware 3.0

CoolWebSearch is the name given to a wide range of different browser hijackers. Though the code can be very different between variants, they are all used to redirect users to coolwebsearch.com and other sites affiliated with its operators.

If you want even more suggestions of how to make your system spyware proof or for more advice on how to tackle spyware, then I would suggest that you read this page:
<http://spywarewarrior.com/sww-help.htm>

If you want to read just how sneaky some of the spyware can get, then I’d suggest you read Eric Chien’s excellent Virus Bulletin 2005 paper entitled ‘Techniques of Adware and Spyware³⁶’.

³⁴ The HijackThis Log Analyser can be found here: <http://www.hijackthis.de/en>

³⁵ Which can be downloaded from here: http://www.intermute.com/spysubtract/cwshredder_download.html

³⁶ Which can be downloaded from here:
<http://www.symantec.com/avcenter/reference/techniques.of.adware.and.spyware.pdf>

Anti-Rootkit Tools

Rootkits have been around for *NIX systems for many years; however they are now a growing problem for Windows systems. This is not only true in regard to bots and worms; we are now seeing Spyware authors actively using so-called 'rootkit' technology. This really should be called 'cloaking' or 'stealth' techniques rather than 'rootkit technology' as what they are doing is hiding the malware files and processes from the operating system. Malware using stealth techniques is not a new phenomenon; many years ago DOS malware authors used similar techniques.

What is a rootkit?

A rootkit is a collection of tools an intruder brings along to a victim computer after gaining initial access, usually via hacking into the box manually or by getting the a user to execute a Trojan or Worm which will install a backdoor for them to slither onto the system in the first place. A rootkit generally contains network sniffers, log-cleaning scripts, and trojaned replacements of core system utilities. There is however another type which does not tend to replace system files, these are: Kernel [LKM] rootkits which subvert the system by attaching themselves to, or by otherwise modifying the kernel of the targeted operating system.

Some examples of such kernel rootkits on Linux include: Knark, Adore, and Rtkit.

Although *NIX rootkits have been around for many years and are generally considered the major threat to *NIX security, there are also a growing number of Windows rootkits. This 'rootkit' scenario is a complete about-face when compared to other classes of malware, where DOS/Windows is the most targeted and *NIX is little more than a drop in the malware ocean.

Some examples of Wintel rootkits include: Hacker Defender, FU and Vanquish.

Why do you need to consider rootkit detection tools? Well, a number of bots already include rootkit techniques³⁷ to allow them to hide from the OS and many security tools as they bind in directly to the kernel. A number of bots have used a recompiled version of the FU rootkit driver to remove their process entry from Windows Task Manager, others have used the JiurlPortHide driver for hiding network connections. It does look like we will be seeing increasingly sophisticated and 'invisible' bots and other spyware as rootkit technologies and techniques get added to the malware and spyware author's arsenal. A good example of this evolution is RIVARTS.A which is capable of running on Windows 98, ME, NT, XP and Server 2003 and uses rootkit [aka stealthing/cloaking] techniques to hide itself from the operating system.³⁸

There are a number of tools available that claim to be able to detect and remove rootkits, these are listed below, along with the OS that they are suitable for:

- ChkRootkit [*NIX - <http://chkrootkit.org/>]
- Rootkit Hunter [*NIX - http://www.rootkit.nl/projects/rootkit_hunter.html]
- RootkitRevealer [Wintel - <http://www.sysinternals.com/ntw2k/freeware/rootkitreveal.shtml>]
- UnHackme [Wintel - <http://greatis.com/unhackme/>]
- Blacklight [Wintel - <http://www.f-secure.com/blacklight/>]

A number of anti-virus products now include so-called 'rootkit' detection functionality which is required to detect many of the more advanced ones that bind in at kernel level.

Personal Firewalls

These can be used to block unwanted applications from being able to connect to the network, effectively, in the case of a bot, stopping it from connecting to the command and control network.

³⁷ More details can be found here: <http://www.f-secure.com/weblog/archives/archive-052005.html#00000559>

³⁸ Details can be found here :
http://www.trendmicro.com/vinfo/grayware/ve_graywareDetails.asp?GNAME=TSPY_RIVARTS.A

In the case of spyware a personal firewall can be useful in stopping the spyware from connecting to the Internet and depositing its haul of stolen data.

For home users I would suggest either ZoneAlarm³⁹ or Kerio⁴⁰ as both are available as free versions, but if you want the extra protection or features then you can purchase a more advanced version of them.

Conclusions

Hopefully I have shown you if you have not already taken steps to counter spyware, then I strongly suggest you do before your computer [if you are a home user] or your network of computers [if you are a company or from academia] requires a complete rebuild to remove all the spyware and related cyber-threats that have infiltrated it and may well have stolen valuable personal, financial or intellectual property.

Spyware has been a problem for many years, and only the anti-spyware community, in the vast majority of cases were prepared to stand up and fight them on the battleground; this being your computer.

The bad news is that spyware is now commonly used by professional cyber-criminals to steal data, be it corporate secrets or your credit card or bank details. Even worse is that the quality of the spyware is getting better; this means that we are talking about these programs being written by professional programmers rather than the more usual stereo-typical malware author. Increasingly we are seeing new techniques to make the detection and removal of some spyware very, very, difficult.

The current trend in spyware to remain hidden and avoid detection means that up-to-date and multiple layers of protection have become almost mandatory for any self-respecting organization.

The good news is that not only do the dedicated Anti-Spyware tools and utilities do a good job in detecting and removing most spyware, with a few nasty exceptions, but the move from nearly all anti-virus vendors in including either better detection of spyware or offering anti-spyware add-ons is a very positive move.

As with other security threat, especially malware related ones, you need to deploy a multi-layered approach to minimise the chance of spyware getting onto you computers. This means not only do you need good technological solutions, and overlapping technologies at that, but these need to be backed up with good security policies, procedures, education and constant vigilance.

Please do not see this paper as an exhaustive or complete look at spyware, to do it real justice would require enough material to fill a large book.

³⁹ <http://zonelabs.com>

⁴⁰ <http://www.sunbelt-software.com/Kerio.cfm>

Appendix A – Suggested Reading

Implementing Anti-Virus [Malware] Controls in the Corporate Arena. Proceedings of the 16th Compsec International Conference, 1999 pp 575-586

You are the Weakest Link, Goodbye! – Malware Social Engineering Comes of Age, Virus Bulletin, March 2002 pp 14-17

Canning More Than SPAM with Bayesian Filtering, (Overton, Martin) - Virus Bulletin International Conference 2004

Anti-Malware Tools: Intrusion Detection Systems, (Overton, Martin) - EICAR International Conference 2005

Bots and botnets - risks, issues and prevention, (Overton, Martin) - Virus Bulletin International Conference 2005

Techniques of Adware and Spyware, (Chien, Eric) - Virus Bulletin International Conference 2005