SANS Institute
InfoSec Reading Room

A Spyware Survival Toolkit

Living in a house with three teenagers and a wireless network will teach you a lot about spyware. Most parents have realized that there a lot of things they can't control and, if they are to keep their sanity, they learn to live with stuff like teenage fashions, music, the language of IM, driving experiences, and the spyware that ends up on the PCs of a home network. From first-hand experience, I will attempt to provide a toolkit to help avoid and/or survive the spyware that I've had to deal with. This paper will discu...

Peter McGranaghan
GIAC Security Essentials Certification (GSEC)
Option 1, Version 1.4c
March 15, 2005

A Spyware Survival Toolkit

Abstract

Living in a house with three teenagers and a wireless network will teach you a lot about spyware. Most parents have realized that there a lot of things they can't control and, if they are to keep their sanity, they learn to live with stuff like teenage fashions, music, the language of Instant Messaging (brb, gtg, pir, etc.), scary driving experiences, and the spyware that ends up on the PCs of a home network. From first-hand experience, I will attempt to provide a toolkit to help avoid and/or survive the spyware that I've had to deal with. This paper will discuss the sources of spyware, the types of spyware, and the methods of prevention, detection, and removal of spyware. In the end, however, there are still those pesky teenagers whose effortless downloading will teach you to be like Dr. Strangelove who learned to stop worrying and, if not love the spyware, at least learn to live with it. The intention of this paper is to be a lifeline to help home computer users survive the spy wars.

1 Today's Spyware Landscape

1.1 What is Spyware?

Spyware falls into the general category of malware. Malware is generally software you don't want on your PC. The SANS Institute in [1] defines malware as :

"Malware is a generic term that refers to software that was written with malicious intent and performs its actions without the user's permission"

It includes viruses, worms, Trojans, adware, spyware, browser hijackers, toolbars, searchbars, packet-capturing programs, password crackers. There are also various hybrids and combinations of these. For example, ISTBar is a combination toolbar and hijacker. For a comprehensive list of known malware see http://research.pestpatrol.com/Lists/MostPrevalentPests.asp. For a summary of types of spyware see http://www.anti-spyware-review.toptenreviews.com/types-of-spyware.html

Spyware is software which runs on your PC and collects information about you and the ways in which you use your computer. It then sends this information to a server owned by someone who will probably sell the collected information to various enterprises, legal and illegal. As the name suggests, spyware tries to keep a low profile by running in the background and avoiding detection.

1.2 Is it legal?

In the Wild, Wild West that is today's Internet it seems pointless asking what is legal. It may not always be like that and different countries are attempting to create legislation to protect us from ourselves. Until the sheriff arrives some have tried to create a safer Internet e.g. parental control of websites which can be visited (Net Nanny, AOL), 'walled garden' environments within institutions like schools. A lot of spyware is legal and what makes it legal is the infamous EULA (End User License Agreement), you know, the long rambling text which almost no-one reads but which you have to agree to in order to move on to the next step of installing software, the very same software which is about to load spyware on your computer. Some of these EULAs make interesting reading. For example, they may openly admit that they are going to disable other adware on your computer (in order to run their own) with statements like:

"You further understand and agree, by installing the software, that the software may, without any further prior notice to you, remove, disable or render

inoperative other adware programs resident on your computer."

An interesting experiment was performed by a company called PC Pitstop to measure the extent to which people ignored EULAs. They inserted a clause in their own EULA which offered a reward to anyone who sent an email to the address given in the EULA. After 3,000 downloads and four months, one person finally took advantage of the offer and received a check in the mail for $1,000, according to the company's Web site. For more details and reasons why you should read the EULA see [5].

Federal Legislation dealing with spyware in this country includes The Software Principles Yielding Better Levels of Consumer Knowledge (SPYBLOCK) Act, which is still working it's way through the Senate, and the SPY ACT (Securely Protect Yourself Against Cyber Trespass Act) http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.+29:, which is also working it's way through committees. In its current (March 2005) form, the SPY ACT would allow the FTC to fine violators up to $3,000,000 for each violation. However, some fear that the legislation may end up being so watered down and toothless that it will have no effect.

State legislation is a little more advanced. Utah has passed a Spyware Regulation Bill (House Bill 323) in 2004 (http://www.le.state.ut.us/~2004/bills/hbillenr/hb0323.htm). Violators face a fine of $10,000 per incident. California has passed State Bill 1436 Consumer Protection Against Computer Spyware Act. Similar bills are also under way in Michigan, Iowa, Pennsylvania, Virginia, and New York (see http://www.ncsl.org/programs/lis/spyware04.htm)

Given the global nature of the Internet, enforcing these laws will require a lot of international co-operation.

In an interesting twist to these attempts to legislate against spyware, Australia has turned things on their head and passed legislation to make spyware legal if used by Law Enforcement to collect information in the course of criminal investigation. The Surveillance Devices Act 2004 enables LEAs (Law Enforcement Agencies) to covertly install spyware (software and hardware) on people's computers to record, for example:

- communications being typed on the computer, such as emails and conversations in Web-based chat rooms and in Internet Relay Chat, etc,
- addresses of Web pages and other files on the Internet, e.g. addresses typed into a Web browser for the purpose of visiting the page,
- information entered into programs such as word processing and spreadsheet programs,
- PIN numbers and passwords associated with banking, email and other

accounts, and private encryption keys (notwithstanding that it is already a criminal offence involving up to 6 month's imprisonment for refusing to provide such information to Federal Police).

1.3 The Grey Area

One person's spyware is another's advertising aid. Take web beacons for example. A web beacon is a transparent image on a web site, usually 1 pixel x 1 pixel. It is also called a web bug or clear GIF. Web beacons are used in conjunction with cookies to collect information on the person who is browsing the website e.g. type of browser, time spent browsing website. This is beginning to feel suspiciously like spyware but you've probably consented to it in the EULA under some vague marketing analgesic "… to improve your shopping experience". Internet commerce needs advertising and advertising needs tools to collect information on consumers' habits. It would be a very naïve consumer who didn't know that when he buys a specialty product like, for example, a special edition commemorative coin, then he will be receiving junk mail on coins, coin collecting, coin auctions etc for a long time. Similarly, when you browse Amazon.com you must expect that your trail of web pages will be recorded and you shouldn't be surprised to be prompted next time you go to Amazon.com to buy other books or CDs similar to the ones you browsed or bought last time. This has to be taken into consideration when drafting anti-spyware legislation like the SPY ACT (Securely Protect Yourself Against Cyber Trespass Act).

The difference between spyware and advertising tools like cookies and web beacons is malicious intent. Software which is designed to cripple your computer or network is malware. Unfortunately, in the current state of Internet technology it is all too easy to take advantage of the weaknesses in the computers connected to the Internet in order to spread mayhem. However, with the tools I will describe in this paper and with a general increasing awareness of Internet security among Internet users it is possible to survive the spywars and make spyware an occasional irritation rather than a serious problem.

1.4 Who Wants to Know?

Inquiring minds may like to know where spyware sends the information it has gathered. In the case of spyware loaded by peer-to-peer filesharing software e.g.Kazaa, read the excellent GIAC/GSEC Practical paper by Armin Froemmel "Dangers and Containment Of P2P Utilities On A Corporate Network" [9]. For various Peer-To-Peer programs like Kazaa which contain adware/spyware this paper tracks the TCP ports and URLs used. Although it was written for, and the data was collected in, a corporate environment it applies equally to the home

user environment.

If you want to find out exactly who your computer is talking to then you will need a sniffer like Ethereal (http://www.ethereal.com/). This will capture packets from your network interface card and display the packet content, source, and destination is a readable format. You can experiment with Kazaa, Bearshare, Limewire, etc and still keep your PC free from the spyware they deliver by creating a virtual machine which runs on your physical machine but has it's own isolated environment (disk space, ram space, registry etc.). I used VMWARE (http://www.vmware.com/) to create a Windows XP Home Edition virtual machine and installed Ethereal on it. I had Ethereal running when I installed Bearshare, a popular peer-to-peer program. The majority of the the outgoing packets were going to TCP port http (80) which is hardly surprising and the incoming packets from TCP port 6346 which is registered in IANA to Gnutella, a peer-to-peer file-sharing project (http://www.gnutella.com/). After installation, I saw that weather.exe and save.exe had been added to my startup menu (on a real machine i.e. not virtual, these would have been blocked by a program like StartupMonitor (see section 2.1.5)). These are well-known adware programs which generate pop-ups.

Bearshare uses the Gnutella file-sharing method of getting peer IP addresses via web caches. What this means is that your computer doesn't store a list of IP addresses of other Bearshare users. Instead your computer is directed to URLs called web caches where the IP addresses are stored. Here is what was returned as web caches in the virtual machine:

```
GET /ygwc.php?client=BEAR&version=4.6.1.2&urlfile=1 HTTP/1.1
Connection: close
Host: ygwc.y-0.net
User-Agent: BearShare 4.6.1.2

HTTP/1.1 200 OK
Date: Fri, 11 Mar 2005 01:43:06 GMT
Server: Apache/2
Cache-control: no-cache
X-Remote-IP: aa.bb.cc.dd
Connection: close
Transfer-Encoding: chunked
Content-Type: text/plain
bd
http://gwebcache.linuxonly.nl/
http://loot.alumnigroup.org/
http://toadface.bishopston.net:3558/
http://g2cache.theg2.net/gwcache/lynnx.asp
http://gw.solutions.lv/~dimss/gwc/perlgcache.cgi
```

Each of the links contains IP addresses to connect to for file-sharing. Using the 'Analyze' function, Ethereal can format and summarize the packet conversations, as in the following table which shows which IP addresses and TCP ports the virtual machine was talking to during the installation of Bearshare (public IP addresses removed from the following table).

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	
192.168.109.128	1108	xx.yy.zz.aa	http	4654	4189979	1498	81357	3156	4108622	
192.168.109.128	1116	xx.yy.zz.aa	http	406	402947	140	7793	266	395154	
192.168.109.128	1117	xx.yy.zz.aa	http	91	77921	33	2147	58	75774	
192.168.109.128	1106	xx.yy.zz.aa	http	83	53588	31	6224	52	47364	
192.168.109.128	1107	xx.yy.zz.aa	http	80	61375	30	3491	50	57884	
192.168.109.128	1111	xx.yy.zz.aa	https	34	2785	26	2221	8	564	
192.168.109.128	1105	xx.yy.zz.aa	http	25	15927	10	951	15	14976	
192.168.109.128	kpop	xx.yy.zz.aa	https	21	3437	11	1411	10	2026	
192.168.109.128	1110	xx.yy.zz.aa	https	20	4135	10	1501	10	2634	
192.168.109.128	1112	xx.yy.zz.aa	https	20	4129	11	1555	9	2574	
192.168.109.128	1113	xx.yy.zz.aa	https	16	2517	8	1356	8	1161	
192.168.109.128	1123	xx.yy.zz.aa	http	16	2274	8	884	8	1390	
192.168.109.128	1104	xx.yy.zz.aa	http	12	2959	6	868	6	2091	
192.168.109.128	1138	xx.yy.zz.aa	http	12	1645	6	481	6	1164	
192.168.109.128	1121	xx.yy.zz.aa	http	11	1143	6	540	5	603	
192.168.109.128	1115	xx.yy.zz.aa	http	10	966	5	549	5	417	
192.168.109.128	1118	xx.yy.zz.aa	http	10	977	5	560	5	417	
192.168.109.128	1120	xx.yy.zz.aa	http	10	1274	5	572	5	702	
192.168.109.128	1124	xx.yy.zz.aa	http	10	976	5	559	5	417	
xx.yy.zz.aa	8000	192.168.109.128	1135	10	842	5	431	5	411	
xx.yy.zz.aa	1136	192.168.109.128	http	10	1233	5	427	5	806	
xx.yy.zz.aa	1122	192.168.109.128	http	9	1207	5	506	4	701	
xx.yy.zz.aa	6346	192.168.109.128	1125	6	366	3	180	3	186	
xx.yy.zz.aa	6346	192.168.109.128	1129	6	366	3	180	3	186	
xx.yy.zz.aa	6346	192.168.109.128	1131	6	366	3	180	3	186	
xx.yy.zz.aa	1141	192.168.109.128	http	6	366	3	186	3	180	
xx.yy.zz.aa	6346	192.168.109.128	1126	5	306	2	120	3	186	
xx.yy.zz.aa	6346	192.168.109.128	1127	5	306	2	120	3	186	
xx.yy.zz.aa	6346	192.168.109.128	1128	5	306	2	120	3	186	
xx.yy.zz.aa	6346	192.168.109.128	1130	5	306	2	120	3	186	

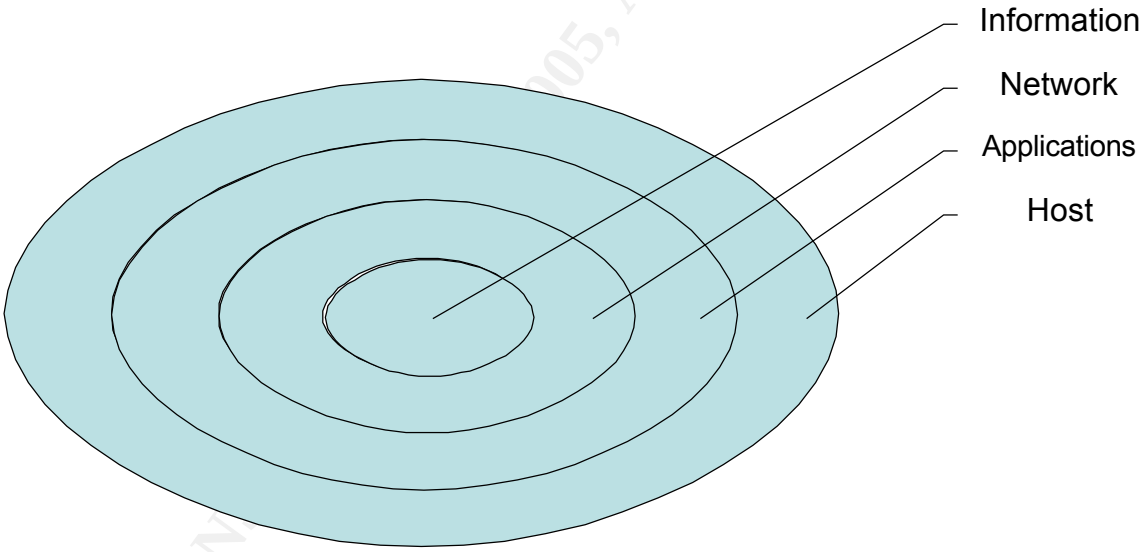
2 Prevention

When you buy a new PC and power it on for the first time how do you know what software you are getting? On a Windows machine out of the box there will be the usual icons for Internet Explorer, Windows Media Player, MSN Explorer, a lot of advertising links to the PC manufacturer's websites, trial offers for anti-virus software, music download services. On a re-cycled or rebuilt machine you get whatever the seller leaves on it, intentionally or unintentionally. Some form of certification that a computer is 'clean' would be desirable. Since that is unlikely to happen any time soon, it is still Caveat Emptor, Buyer Beware.

Can you trust the person who sold you the computer? Even if you do trust the seller, the computer may have malware on it and the seller may not be aware of it. I tried an informal survey of various retail outlets like Best Buy, Circuit City, and others by sending an email to their customer service department, asking them:

When I buy a computer from you can I be sure it does not have spyware or viruses already on it? Do you check it before you ship it?

Those that responded basically said the same thing i.e. that the computers they sell are sealed packages from the manufacturer and therefore would not have spyware or viruses on them. Sellers have no incentive to ensure that the computers they sell are clean. They can always blame the buyer. Basically, when you buy a computer you should go on the defensive right away and in the following section I will show you some ways to do just that. Of course, the same safeguards can be applied to computers you already have running in your home. They should form part of a strategy of defense-in-depth for your home computers.



As described in [2], the diagram above represents the layers of defense for computer network. To get to the information on your computer an attacker has to penetrate the network layer (router firewall, router password, wireless security e.g. WEP, WPA), host layer (user password, user privileges, OS security), application layer (personal firewall, anti-virus software, anti-spyware software), information layer (password protection, file and directory access rights e.g. write-protection).

2.1 Sanitize New PCs

When anyone in the house gets a new PC the first thing I do is to go through a process of 'sanitizing' it.

2.1.1 Internet Browser

Replace Internet Explorer with Mozilla Firefox and make this the default browser. Then remove Internet Explorer from the desktop (desktop Properties, Display Properties, Desktop Items, de-select Internet Explorer). Firefox is generally accepted to be more secure than Internet Explorer but it is probably a matter of time before weaknesses in Firefox are exploited. There will always be a better mousetrap and for the moment Firefox is it. If it isn't already installed, I also add Netscape just to have an additional browser.

2.1.2 Windows Updates

Get the latest Windows updates (unfortunately, Windows will force you to use Internet Explorer for this). Turn on the Automatic Updates.

2.1.3 Anti-virus Software

Activate virus-protection software on the PC. It may come with a 60-day trial of Norton (http://www.symantec.com/index.htm) or McAfee (http://www.mcafee.com/us/) Antivirus software, in which case it needs to be activated and the latest virus definitions downloaded. If not, contact their websites and download. There are also free downloads of virus-protection software e.g. AVG (http://www.grisoft.com/us/us_index.php). Set the anti-virus software for automatic updates if it has the option.

2.1.4 Anti-spyware Software

- Install spyware detection/removal software. Update definitions to the latest. Run the software and remove any spyware found. The most well-known free programs are Spybot S & D (search and destroy) and Ad-Aware (Note: for Ad-Aware see section 3.6 Removal Problems). There are others you have to pay for like SpySweeper, McAfee Antispyware, Spyware Eliminator, and SpySubtract. See http://www.anti-spyware-

review.toptenreviews.com/?ttreng=1&ttrkey=spy+sweeper for reviews of these and other anti-spyware software. Microsoft is finally acknowledging spyware as a problem and has released its own Antispyware program as a Beta version download. After a brief trial I uninstalled it because it was conflicting with StartupMonitor. Being a Microsoft product, it naturally allowed all Microsoft programs to be added to the startup menu, whereas StartupMonitor still prompted me to allow or not allow.

- Install SpywareBlaster. This free download adds an extra layer of protection from spyware by blocking the download of spyware/tracking cookies, preventing the installation of ActiveX-based spyware, dialers, etc., restricting the actions of spyware/ad/tracking sites in Internet Explorer. Even though you may have installed Mozilla Firefox as your default Internet browser, some (Microsoft) utilities like Windows Update will insist on using Internet Explorer. SpywareBlaster will also provide the same protection for Mozilla Firefox.

Note that programs like SpywareBlaster are pre-emptive i.e. they block spyware from running on your PC; they don't remove spyware like Spybot or Ad-aware.

2.1.5 Startup Monitor

Install StartupMonitor and StartupCPL (http://www.mlin.net/StartupMonitor.shtml). These will prevent unwanted programs from being installed in your startup menu and allow you to easily remove unwanted programs already installed in the startup menu. Microsoft's own (since it bought Giant) Antispyware attempts to do the same thing but, at least in the currently available free Beta version, it always allows Microsoft programs to be added to the startup menu. That's why I uninstalled it after trying it for a week. StartupMonitor has no such bias and blocks all software unless you accept it.

2.1.6 HijackThis

Install HijackThis (see Detection below). This free download has bailed many malware victims (including myself) out of trouble. It is usually a remedy of last resort.

2.1.7 Personal Firewall

Install a personal firewall. With Service Pack 2 Windows XP automatically has the Windows Firewall turned on. Other available firewalls include BlackICE (http://www.digitalriver.com/dr/v2/ec_dynamic.main?SP=1&PN=10&sid=26412), McAfee Personal Firewall Plus (http://www.mcafee.com/us/), Norton Personal Firewall (http://www.symantec.com/index.htm), ZoneAlarm (http://www.zonelabs.com).

2.1.8 Apply the Principle of Least Privilege

Depending on who the users are on your network you might consider reducing their privileges to lower than Administrator. Use the Principle of Least Privilege i.e. only give users the privileges they need. In a Windows XP home environment this means choosing from Administrator account, Limited account, and Guest Account. The Administrator account is intended for someone who can make systemwide changes to the computer, install software, and access all non-private files on the computer. Only a user with an Administrator account has full access to other user accounts on the computer. A user with an Administrator account:

- Can create and delete user accounts on the computer.
- Can change other users' account names, pictures, passwords, and account types.
- Cannot change his or her own account type to limited unless there is at least one other user with a computer administrator account. This ensures that there is always at least one user with a computer administrator account on the computer.
- Can manage his or her network passwords, create a reset password disk, and set up his or her account to use a .NET Passport.

A user with a Limited account:

- Generally cannot install software or hardware, but can access programs that have already been installed on the computer.
- Can change his or her account picture and can also create, change, or delete his or her password.
- Cannot change his or her account name or account type. A user with an Administrator account must make these kinds of changes.
- Can manage his or her network passwords, create a reset password disk, and set up his or her account to use a .NET Passport.

A user with Guest account has even less privileges than a limited account. Limited accounts are inherently more secure than Administrator accounts. It is up to you as network administrator for your home network to decide what restrictions you want to apply to your users.

There is also a way to run as Administrator with reduced privileges. The article in [6] discusses why it is safer not to run as Administrator and provides a way to run as Administrator with reduced privileges using a program called DropMyRights.

2.1.9 Disable Services

Disable services you don't need. This is easily done in Windows XP: Control Panel / Administrative Tools / Services. Services you should consider disabling include:

- Server (file and printer sharing)
- Universal Plug and Play
- Fax
- Remote Access services

2.1.10 File Extensions

- Remove file extensions which are not needed e.g. shell script extensions like VBE. In Windows XP Control Panel / Folder Options / File Types.
- Turn off the setting 'Hide extensions for known file types'. With this option set a file with the name harmless.doc.exe will appear as harmless.doc. This has been known to fool the most experienced users into launching malware posing as innocent documents. An example of this kind of exploitation (and many others) is described in Kevin Mitnick's book 'The Art of Deception' [3].

2.1.11 Recovery Toolkit

I'll admit my home office is a mess (and this weekend I'm going to do something about it) but under my overloaded desk there is one strong plastic box with a red cross on it which serves as my first-aid kit. In it I have:

- A zip-up CD holder with all the device installation CDs for the PCs in my home network and the Windows XP restoration CDs.
- A USB jump drive containing HijackThis, Startup.exe, Spybot S & D, Stinger (see section 2.1 above), a PasswordSafe file containing all the

passwords I need for the various users and email accounts on my home network (see http://passwordsafe.sourceforge.net/). This is safer than writing them all down on a piece of paper.
- A hardcopy of the names of useful websites (once this paper is written I can replace all my pieces of paper with a copy of the paper).
- Spare Ethernet and USB cables.

3 Detection

3.1 Symptoms of Spyware

As described in [7] the following symptoms may indicate the presence of spyware or other malware on your computer:

- you are subject to endless pop-up windows
- you are redirected to web sites other than the one you typed into your browser
- new, unexpected toolbars appear in your web browser
- new, unexpected icons appear in the task tray at the bottom of your screen
- your browser's home page suddenly changed
- the search engine your browser opens when you click "search" has been changed
- certain keys fail to work in your browser (e.g., the tab key doesn't work when you are moving to the next field within a form)
- random Windows error messages begin to appear
- Your computer suddenly seems very slow when opening programs or processing tasks (saving files, etc.)

To these I would add:

- higher than usual disk drive activity (activity light constantly flickering)
- low amount of available disk space
- unusual characters or missing characters in screen display
- computer takes longer than usual to start up

This list is not an exhaustive list. As the ingenuity of hackers and spymasters improves, then the symptoms of their handiwork will change also. In general, if your computer is behaving in an unusual or unexpected way then spyware or other malware may be to blame.

3.2 Routine Maintenance

- As mentioned above, you should have Windows Updates on automatic. Similarly for whatever anti-virus software you are running. Anti-spyware software like SpywareBlaster, Spybot, and SpywareGuard will have to be updated manually. In the case of SpywareBlaster, for an annual subscription (currently $9.95) updates can be made automatic.
- Even if the anti-virus and anti-spyware software are set to run on a fixed schedule you should check the date when they last ran in case the computer was powered off when they were scheduled to run. You may have to adjust the scheduled time for running them.
- Check for Windows updates manually. Users get so engrossed in their instant messaging, and other high-priority activities, that they may ignore requests to restart their computer for updates to take effect.
- Check the startup menu for each user. This can be done with msconfig or with Startup Control Panel from Mike Lin (http://www.mlin.net/StartupMonitor.shtml). Look for well-known pests (see http://research.pestpatrol.com/Lists/MostPrevalentPests.asp) and remove them.
- Check for expired subscriptions to anti-virus, anti-spyware software.
- Download the latest version of Stinger (http://vil.nai.com/vil/stinger/). This is a standalone virus detection and removal program free from McAfee. If you do this once a month you will have a fairly recent version available in the event that you lose Internet connection and updates were not being downloaded e.g. if a user left a computer turned off for a long period of time.
- A good checklist for security of home computers can found in [4].

3.3 User Education

Having installed various protective software, the users in your home network are going to get various pop-up reminders and prompts. For example, with StartupMonitor running they will be prompted every time an attempt is made to add a program to the startup list. Generally, the answer should be no i.e. do not add the program to the startup list. Reminders for anti-virus or anti-spyware subscription renewals will probably be ignored or lost amongst the plethora of Instant Messaging windows that are all chiming, chanting, and screaming for attention in their own customized ways. So don't count on being told about

these. Keep your own record of when the subscription renewals are due and make it part of your monthly maintenance checklist.

Users should be made aware of the symptoms of spyware (see above) and asked to report such occurrences. However, as I said before, don't expect to be told until it's too late. As long as they can send and receive instant messages kids will wade through pop-ups, ignore error messages and warnings, and put up with slow response time in their Internet browser. By the time you get to hear about it there may be a lot of bad stuff on one or more PCs in your network.

The way in which questions are worded in pop-ups can be tricky. Some adware programs come with an Uninstall but you try to use it you may be prompted with text like:

"You have chosen to Uninstall TrickyDickySoftware. This will deprive you of many opportunities to buy our exciting products. We cannot be held responsible for the negative impact this will have on your quality of life. Do you wish to reconsider your decision?"

Like the EULA discussed in section 1.2 above, users don't always read the text they are presented with and are inclined to click the box which is highlighted, usually 'Yes'.

With all the publicity in press and TV it is hard to believe that there are still people who see an attachment in an email from someone they don't know and click on it to open. Still, you should remind the users of your home computers not to open suspicious emails or attachments (not even the ones with titles like "You may never have to work again. Find out why" or "Forward this email to 10 friends or your life will never be the same again").

3.4 What Evil Lies Within?

When you suspect you may have spyware active on your computer, based on the symptoms described above, what you do next depends on how functional your computer is.

As with any malware infection of a networked computer you should disconnect it from the network to prevent the spread of any malicious code.

Assuming your computer is functioning well enough to run a spyware detection program like Spybot, this should detect whatever spyware is currently active. Make sure you check for updates before running, unless of course your browser has been hijacked or disabled in some way. If the symptoms persist you should run HijackThis and post the log on a reputable malware site like http://boards.cexx.org/. Another similar site is http://forums.net-integration.net/index.php. The question of trust arises again. How can you trust

the removal instructions you get from an 'expert'? There's no easy answer to this. I've been using the advice from the cexx website for several years without any problems. You can generally tell from the postings and discussion threads if the experts know what they're talking about.

If applications are not running or are running very slowly try re-booting in Safe Mode and running Spybot and/or HijackThis.

If you have no Internet connection with any browser e.g. Firefox, Netscape, Internet Explorer, collect a HijackThis log (in Safe Mode if necessary) and use another computer to post it.

3.5 Removal

3.5.1 Routine Removal

Most of the spyware detection programs like Spybot will also remove whatever spyware they find. You should check that the removal process has not created any new problems e.g. verify your browser and internet connection are working ok (see removal problems below).

3.5.2 Emergency Removal

In the event that your computer has been infected to the extent that applications cannot be run or are running very slowly you may have to resort to HijackThis, post the logfile to a reputable website (see section 3.4 above) and follow removal instructions. It is important to follow the removal directions carefully as you will be working directly with registry entries. Note: there are some websites which claim to provide automated analysis of HijackThis log files e.g. http://hjt.iamnotageek.com/ but they are of limited use. If you are in a situation where you need to use HijackThis I recommend you get someone experienced to look at the logfile and follow their instructions meticulously.

3.6 Removal Problems

3.6.1 Winsock problem

You've heard the expression throwing out the baby with the bath water. Well, it has been known for spyware removal software to remove more than spyware. On at least 3 occasions I have found that my Internet connection did not work after running Ad-aware. For this reason I avoid using Ad-Aware. The following is taken from [8] and explains how spyware removal can cause problems:

"When spyware breaks Windows

Typically, when spyware removal breaks Microsoft Windows, the symptoms look a lot like a DNS error. You might be able to ping a favorite Web site by IP address but not by DNS name. When you attempt to access the site, Internet Explorer typically displays a message stating that the page cannot be displayed. To understand why Windows might malfunction once spyware has been removed, you need to understand a little bit about the way that Windows attaches your computer to the Internet. Computers communicate across the Internet through the use of the TCP/IP protocol, and Windows implements TCP/IP through a mechanism called Winsock. Winsock, however, is not made up of a single file. Instead, it takes a layered approach to implementing TCP/IP in a chain-like fashion. If you were to remove a file from the chain, Winsock would cease to function properly, and Internet communications would be either handicapped or completely disabled.

Some spyware modules exploit Winsock. There are certain benefits to doing this. First of all, the spyware module appears to be part of the operating system and therefore is more difficult to detect than other types of spyware. Second, if the spyware module is hooked into the Winsock chain, it's easy for the module to monitor all Internet- and network-based communications. Finally, if a spyware module can trick Windows into thinking that it's part of the operating system, the module will not be limited to the permissions granted to the machine's current user. In most situations, the operating system and its subcomponents have full permissions over the machine.

Here's where things get tricky. Imagine that a spyware module has infiltrated the operating system and has hooked itself into the Winsock chain. Now imagine that you run a spyware removal program that detects and removes the module, but now the Winsock chain is broken and Internet access does not work. In a situation like this, it would seem as though you should simply be able to reinstall Windows over the existing copy and that, in doing so, you would replace any missing files, thus relinking the Winsock chain in the process. Unfortunately, this technique doesn't work." (Ray, P. 1)

There are various fixes for this problem. See, for example, http://www.spychecker.com/program/winsockxpfix.html

3.1.2 False Positives

A well-known false positive reported by earlier versions of Spybot is DSO exploit. This was caused by a bug in the way Spybot was trying to fix the problem. Later versions of Spybot no longer have this problem. Other false positives can be found at http://forums.net-integration.net/index.php.

4 Conclusion

Spyware is not going to go away any time soon. In a home environment where users want the freedom to roam the wide-open vistas of the Internet without seatbelts or crash helmets it is almost inevitable that bad stuff will end up on one or more home computers. In this paper I have tried to give readers a fighting chance to reduce the risk of infection and tools to deal with whatever does manage to infiltrate your defenses. These tools should form part of your defense-in-depth for your home computers.

5 References

[1] SANS Institute. Track 1 – SANS Security Essentials: Secure Communications
SANS Press, Jan 2004.

[2] SANS Institute. Track 1 – SANS Security Essentials: Defense-In-Depth
SANS Press, Jan 2004.

[3] Mitnick, Kevin D. and Simon, William L. The Art of Deception. Indianapolis: Wiley 2002.

[4] Granemann, Scott. A Home User's Security Checklist for Windows. SecurityFocus, Feb 2004
http://www.securityfocus.com/columnists/220

[5] Magid, Larry. It Pays To Read License Agreements. PC Pitstop
http://www.pcpitstop.com/spycheck/eula.asp

[6] Howard, Michael. Browsing the Web and Reading E-mail Safely as an Administrator. Microsoft Security Engineering. Nov. 2004
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure11152004.asp

[7] McDowell, Mindi and Lytle, Matt. Cyber Security Tip ST04-016 Recognizing and Avoiding Spyware US-CERT 2004
http://www.us-cert.gov/cas/tips/ST04-016.html

[8] Ray, Melissa. Fight Back Against Spyware .Lockergnome, 2004

http://channels.lockergnome.com/it/archives/20041021_fight_back_against_spyware.phtml

[9] Froemmel, Armin. Dangers and Containment Of P2P Utilities On A Corporate Network – GIAC Certified Student Practical. SANS Institute, 2003.

Last Updated: July 21st, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Pen Test Berlin 2018	OnlineDE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced