

Table of Contents

Introduction	1
Spyware Defined	1
Methods of Distribution	2
Fake System Messages	2
Windows Message Service.....	2
Bundled with Legitimate Applications	3
Internet Explorer ActiveX Plug-ins	3
The Legal “Grey area” of license agreements.....	4
Spyware in the Enterprise.....	4
Spyware Infection Test	5
Application Installation	6
After Installation	7
Additional Infections.....	9
Conclusions	9
Reference List.....	11

Introduction

Spyware is everywhere. Everyone agrees that it is a nuisance. At the same time, it is difficult to quantify the affect spyware is having on the world, or how much revenue advertising companies are making because of it. However it falls into the same classification as spam – it is annoying, time consuming and a major source of lost productivity.

As of October 2004, 80% of desktop computers in a study of 329 homes had some form of spyware present. Of those computers that were infected, 95% of the users believed that they did not give permission for the software identified as spyware to be installed.¹ In fact, Microsoft estimates that 50% of all computer crashes are a result of spyware.² The overall idea of most spyware is simple – display advertising on a user’s computer in hopes the user will purchase the advertised product. Since the actual cost of displaying the advertisements is almost nothing, hundreds of different companies are now in the spyware market. However spyware can be much more malicious than many people would believe. Long gone are the first few years of spyware presence, which was limited to advertising pop-ups on desktop computers. Modern spyware applications are network-enabled and use different techniques such as port agility and encryption to avoid detection by existing network security controls.

Spyware Defined

Spyware and Adware are umbrella terms often used to describe any piece of software that is not “readily apparent” on a Windows-based computer system. These programs are individual software packages that almost always fall into one or more categories:

- The user did not specifically download and install the individual piece of software with his or her knowledge.
- The software does not appear in the taskbar while running or provide a simple way to shut it down.
- The software generally does not have a Start Menu folder, and often does not appear in Windows “Add/Remove Programs” control panel
- The software does not have a user interface, and the activities of the software are usually transparent to the user.
- Adware specifically is defined as Spyware which has a primary purpose of displaying advertisements on a user’s system.

In looking at these categories, Spyware draws many similarities to computer viruses. The most notable difference however, is that Spyware does not propagate itself by infecting files, or spreading through vulnerabilities in other software. This puts it in somewhat of a “grey area” in terms of its legality.

¹ AOL/NCSA Online Safety Survey (http://www.staysafeonline.info/pdf/safety_study_v04.pdf)

² Information Week, April 26, 2004

Methods of Distribution

In 90% of cases, Spyware is actually installed on a user's computer by the user themselves. Many people find this surprising, however when the techniques used are analysed, it becomes apparent that this is the case. This section analyses several of the primary methods for users to be "tricked" into installing spyware.

Fake System Messages

The typical end user has a habit of clicking "Ok" to any message box Windows pops up, usually because they believe the system knows the best course of action in any instance. Unfortunately, it is very simple to create a fake system message, by embedding a graphic into a web page.

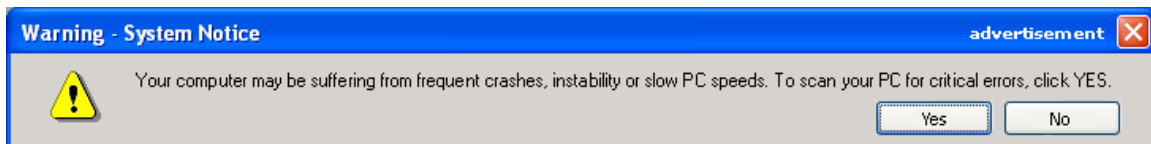


Figure 1 – Phoney System Notices

The image shown above was displayed as a pop-up that appeared while browsing a web site. It looks like a standard Windows system message, and while there is a clear piece of text that alerts the user that this is in fact an advertisement, most users would consider this a genuine message. The most dastardly technique in use with this type of message is that regardless if you click "Yes" or "No", it links to an executable file for download that will install the so called "Critical Error Check" application. While this application does have a front that supposedly scans your system registry for inconsistencies it also contains code that will also generate pop-up advertising, even while you are not actively using the Internet.

Windows Message Service

With the release of Windows XP, the Windows Message service was set to start by default. This service is one that allows a network administrator to send network alert messages, which will be received by every Windows client running the Message service, and pop-up the received message to the user's terminal. Unfortunately, programmers quickly developed software applications to continually send out these same

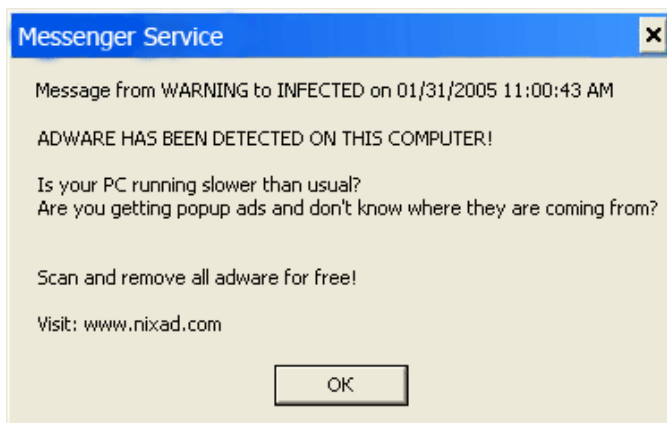


Figure 2 – Windows Messenger Spam

messages to random IP addresses across the Internet, and now there are so many continually running, that it is almost guaranteed that an un-patched Windows XP computer will receive one of these messages within 30 minutes of being connected to the Internet.

While these messages on the surface are harmless as they are just text displayed in a message box, they usually contain messages like the one above. They almost always instruct users to proceed to a web site and download a piece of software, which no doubt contains spyware, adware or worse.

Bundled with Legitimate Applications

The most common form of infection is by bundling spyware with a legitimate application. This is done for a number of reasons, usually the company that provides their software to the user for free will receive royalties each time a user installs the spyware along with it. Many peer to peer file sharing applications bundle spyware so they can generate revenue offset the costs associated with running their P2P networks.

Many times the fact that spyware will be installed is stated in the end-user license agreement, unfortunately while this provides a legal backing for the company, the plain and simple fact is that users do not read license agreements, due to their legal and lengthy wording.

Internet Explorer ActiveX Plug-ins

ActiveX was heralded by Microsoft as a plug-in system for Internet Explorer that would allow developers to customize their web sites, create dynamic and fluid content as well as integrate the user more into the web browsing experience. Today, aside from Microsoft, ActiveX is for the most part used by very few web sites. This is because it is only compatible with Internet Explorer, and it requires the user to install a plug-in. Spyware companies however, have found a huge advantage to deploying ActiveX plug-ins. Since an ActiveX plug-in, once installed allows the application to interact directly with the operating system, this is a perfect way to deploy spyware applications.

Microsoft designed ActiveX applications to be easy to install. The process is automatically initiated by the remote web site. The only notification a user has regarding the plug-in, is a message box alerting the user that the web site is attempting to install a plug-in. The box also gives the name of the plug-in and the company that wrote it. Unfortunately this information is provided by the application itself, so instead of a message box that would say "Web Browser Tracking Plug-in" programmers often substitute other names in their programs, such as "Internet Speed Optimizer". All a user has to do, is click "Ok" to this dialog box and the ActiveX code whatever it may be is downloaded and installed on the computer.

The Legal “Grey area” of license agreements

Many companies that develop Spyware applications argue that their software is legal, since the fact that the software will be installed, and what the software does is outlined in the EULA that the user agreed to during the installation. Unfortunately license agreements have become so convoluted, lengthy and difficult to read that they have effectively become impossible to read. To further analyse this, I downloaded the P2P file sharing application Kazaa. On the Kazaa web site, they have statement that says “Our application contains no spyware of any kind”. Upon installation, I was greeted with an EULA of 7,198 words which totalled 19 printed pages.³

To my surprise, section 9.4 of the EULA is titled “Embedded Third Party Software”, which states that six separate pieces of software will be installed along with Kazaa. At two of these specifically state that they will track download and browsing habits, and one will display advertising. As if this were not enough reading, each subsection of 9.4 states that if you accept this agreement, you also implicitly accept the license agreements of each of these individual pieces of software, which can be found on the respective third party web sites. After finding and downloading all of these agreements, they totalled 8,794 words or 21 printed pages.

Combining all these agreements together, for a user to install the Kazaa Media Desktop application one would have to read and agree to 15,992 words, or 40 pages of license agreements. I think it is safe to assume, that there are very few Kazaa users who have read the collective EULAs. It is this method by which Kazaa can proudly state on their web site that their application contains no spyware, because to them the definition of spyware is software which is installed without alerting the user to their presence.

Spyware in the Enterprise

Potential affects of spyware in the home are limited to annoyance, with the low possibility of compromised personal finance information. However in the business world the losses are potentially much higher. The risks of running network-enabled applications in an enterprise environment can be determined by grouping them according to their network evasiveness and their controlling entity; the user or the enterprise.⁴

Figure 3 shows four quadrants with applications grouped according to the above factors. The applications most dangerous for IT administrators are the ones that are not directly administered by the enterprise, and use evasive techniques to access Internet servers.

³ Kazaa End User License Agreement - <http://www.kazaa.com/us/eula.htm>

⁴ FaceTime White Paper – Spyware Prevention: Effective Network Protection (<http://www.facetime.com>)

Applications such as P2P file sharing and instant messaging fall into this category. They are not easily stopped by standard firewall rules. Obviously Spyware and Malware/Viruses are of top concern to administrators, and rightly so. The presence of spyware usually goes unknown, and by using standard HTTP calls to servers, it passes through the firewall with regular web traffic.

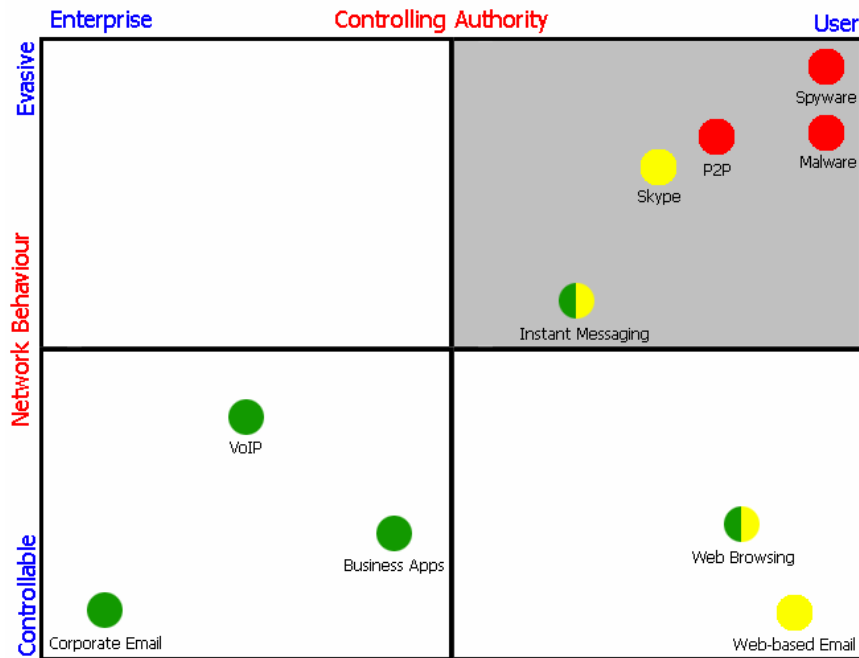


Figure 3 – Application Security Groups

Aside from the potential losses from a security breach, spyware causes large amounts of lost productivity. For example, if a user gets three pop-up advertisements a day and requires an average of 5 seconds to close each advertisement, that’s about 90 minutes wasted over the course of a year. If you value the average user’s time at a conservative \$10 an hour and take 100 million infected PCs in North America, that’s about \$1.5 billion of wasted time every year.

Spyware Infection Test

To get an idea of how quickly and how much spyware a typical user will get on their machine, a controlled test was performed on a computer with a freshly installed copy of Windows XP with service pack 1 pre-installed. For this test, the computer was connected to Sheridan’s network which in actuality likely provides some safeguards from certain remote exploits for Windows, as opposed to a home Internet connection where the ISP may not block certain network ports that worms and viruses use.

Application Installation

Flying Icons 3D Screensaver is an application that users can download free of charge.⁵ The program's web site advertises it as "*A unique 3D based screensaver which uses actual user's desktop with all icons which are turned into 3D objects flying in the 3D world.*" Note the spelling mistake and bad grammar - this is the first clue to the quality of the software.

The download consisted of a single executable file, which launched a standard setup program. For detailed information regarding the install procedure, please visit <http://www.benedelman.org/spyware/installations/3d-screensaver/>. As soon as the installation supposedly completed, the host began making TCP connections to various servers on the Internet.

The first sign that this 3D Screensaver application was more than it appeared to be was immediately after the install process completed. The host machine first queried its DNS server for the IP address of public.zangocash.com. An interesting fact came to light when the DNS response was examined.

```

Domain Name System (response)
  Queries
    public.zangocash.com: type A, class IN
  Answers
    public.zangocash.com: type A, class IN, addr 205.205.86.50
  Authoritative nameservers
    zangocash.com: type NS, class IN, ns ns1.180solutions.com
    zangocash.com: type NS, class IN, ns ns2.180solutions.com
  
```

Figure 4 - DNS Response for public.zangocash.com

The authoritative name servers for zangocash.com are run by 180solutions, a well known spyware marketing company. Upon completion of the DNS lookup, the host machine then opened an HTTP connection to public.zangocash.com

```

POST /php/rpc_uci.php HTTP/1.1
Accept-Encoding: gzip
Connection: keep-alive
Content-Length: 352
Content-Type: text/xml
Host: public.zangocash.com
User-Agent: ZC XML-RPC C++ Client
<?xml version="1.0"?>
<methodCall>
<methodName>uci.get</methodName>
<params><param><value><string>
6efa630d9d3893a7e1abb635b866368294997997094705d3ca61
e582522d734a6ef0e3b91f0b456d01d87f376135613037353730
3463316666376236383534313433373062323462383263:other:
0:0:win:winxp:other:exe
</string></value></param></params></methodCall>
  
```

Figure 5 – HTTP Post Information

Once the connection was made the host sent an HTTP POST command with a large string of data to the server. The HTTP POST method is generally used to send a block of data to a running process on a web server, typically for posting in forums, or uploading files.⁶ Figure 5 to the left shows the data contained in the transmitted segment, including the string sent to the server. By looking at the "Accept-

⁵ Flying Icons 3D Screensavers - <http://www.3d-icons.com/>

⁶ RFC 2616 – The HyperText Transfer Protocol HTTP/1.1

Encoding” field it is apparent that the data is in gzip format. It is now clear that the application running on the host machine has transmitted some sort of machine identification, or system information to the public.zangocash.com server.

The next thing that happened immediately following on the host machine was an HTTP connection to static.zangocash.com, where it downloaded a file named zangoinstaller.exe. This file was automatically downloaded and run on the system without any user intervention or notice. As soon as the file was run, five additional DNS queries were made.

As each one of these queries was responded to, an HTTP connection was then made to the resolved server. Figure 6 below summarizes the files downloaded by the host machine. The circled files are ones that were downloaded by the client. The files accessed from cts.180solutions.com were accessed with an HTTP POST method, which indicates that the client was sending data to the server. In this case the data was passed directly in the URL string. The “trackedevent.aspx” and the values passed to it seem to track installation information, unique user identifiers as well as time and status of the installation.



Figure 6 – Servers and files accessed after installation

After Installation

After the installation was complete a new icon was visible in the task bar beside the clock, volume control etc. By holding the mouse over the icon, the title “Zango” appeared. The application did not appear to have any function, as the only menu options by right-clicking the icon was two links to zango.com, a link to display the license agreement, and an “About Zango” option.

After rebooting and being left idle for 15 minutes, Ethereal was opened and packet capturing was initiated. During the capture, Internet Explorer was launched which had google.com set as the home page. The list of HTTP

requests is shown in figure 7. For users located in Canada, Google automatically redirects the web browser to google.ca. So the first two HTTP connections are to be expected. However, the five others are obviously not related to Google.

Topic / Item	Count	Percent
[-] HTTP Requests by HTTP Host	31	
[-] www.google.com	1	3.23%
[-] www.google.ca	2	6.45%
[-] tv.180solutions.com	1	3.23%
[-] view.atdmt.com	1	3.23%
[-] postajob.monster.ca	1	3.23%
[-] servedby.advertising.com	2	6.45%
[-] media.monster.com	22	70.97%

Figure 7 – HTTP Requests

Not shown in figure 7 is the fact that an SSL connection was established to *cookie.monster.ca*, and several packets of encrypted data were exchanged between the host and server. It is assumed based on the name of the server, that this is a web tracking cookie that was loaded on the host machine. However the purpose of encrypting a simple web tracking cookie is not clear, and it is the author’s opinion that

there may have been more than a simple cookie contained in the encrypted data.

About five seconds after loading the Google home page, a pop-under window was opened displaying an advertisement for “monster.ca”. It was also noticed that a new toolbar was present in Internet Explorer that was labelled “Zango Search”.

To test if these newly installed applications would affect searching, I typed in Google’s search box the phrase “Voice over IP”, and pressed Search. The web browser established a new HTTP connection to google.ca, and submitted the search request. It then established an HTTP connection to tv.180solutions.com and submitted the following string to the server:

```

HTTP Method: POST
showme.aspx?keyword=%2egoog%2eca+voice%2bover%2bip&&id=7289&ver=6.11&duid=76EB7C31C9DBBB95326406992839EA636196D5DDBFC45EF48B7EF281643AA282&partner_id=451026109&product_id=7289&browser_ok=y&md=35&basename=zango&KWV=675&tzbias=5&MT=0176EB7C31C9DBBB95326406992839EA636196D5DDBFC45EF48B7EF281643AA282&DMT=0176EB7C31C9DBBB95326406992839EA636196D5DDBFC45EF48B7EF281643AA282&WID=01C5DE4988DB9D00&GMA=1&GVI=1&GPI=1&HMP=79727BE690D97BCE0102A0025BFB9AD2CC7BF9C0D401870458F8310ED6532C14&bid=0&SID=MVYXGXS&OS=5.1.2600.2&SLID=1033&ULID=1033&TLOC=1033&ACP=1252&OCP=437&DB=iexplore.exe&IEV=6.0.2800.1&TPM=401137664&APM=200204288&TVM=2147352576&AVM=2075295744&FDS=4278071296&LAD=1601:1:1:0:0&WE=5&SRW=1024&SRH=768&CD=www.google.ca&SC=0190DD39F9A9427BF110138C5702F5A703C800C04421B5ACD96B243CA916D594F0
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
    
```

Figure 8 – Data sent to tv.180solutions.com

In the string, 39 different variables are passed to the 180solutions web server. The most prominent of these values is the search string that was submitted and the address of the site where the form was submitted. Other recognizable

variables include the name and version of the web browser being used, a UID value, and the operating system running on the host machine.

This is of particular concern, because although this particular application seems to limit itself to recording and submitting Google search queries, there is nothing stopping a more malicious spyware logger from recording online banking card numbers and passwords, or any data submitted from a web form. Even sites that use a secure SSL connection for submitting the username and password would not be safe because the information is recorded when the user enters the information into their machine. Needless to say, this would be a huge breach of security which could easily be taken advantage of.

Additional Infections

The next day upon examining the infected system, another application was found to be running in the process list: `wnad.exe`. After some researching it was found that this application is a parasite that constantly scans every web page you visit, and harvests email addresses found on those sites for use in spamming activities.⁷ During web browsing, the application did not appear to send any data to Internet servers; however it seems that this type of application would most likely just “call home” from time to time, to deliver the list of email addresses it has compiled up to this point. Not wanting to assist spammers with collecting even more email addresses, the process was ended as soon as it was discovered.

After removing this application and rebooting, the Windows Local Security Authority application (`lsass.exe`) began experiencing random crashes while using the desktop system. Upon further examination it turned out that the computer system had been infected with the Sasser worm⁸. The system was then shut down and taken off the network.

Conclusions

The infection test has proven that spyware is covert, and there is much more going on behind the scenes than simple advertising. Spyware applications are data miners, who want to know everything they can about a user. They are also cumulative, one spyware application often installs another, which can lead to security vulnerabilities and the “uninvited friend who invites more friends to the party” syndrome. Increasingly, spyware is becoming more invasive, harvesting everything it can. At the same time, marketing companies are touting applications as “spyware free” because they disclose the fact that additional applications will

⁷ WinAd Client Information – <http://www.cexx.org/osama.htm>

⁸ Sasser Worm Indications & Cleaning Instructions -
<http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>

be installed. Unfortunately these disclosures are buried in gargantuan end user license agreements.

There is no clear cut solution to stopping spyware. While there are many applications designed to identify and remove unwanted software, these are usually not run until there is a definite problem – usually long after the infection has occurred. End users are being told that software does not contain spyware and is safe to download, even though it does. Many enterprise environments have no specific policy in place regarding monitoring or cleaning spyware.

Legal guidelines must be established regarding the requirements of installation programs to disclose in clearer terms what is being put on a user's machine. Without these any more initiatives, spyware will become as ubiquitous as email spam is today, costing I.T. departments more money yearly.

Finally, reputable legitimate companies should be discouraged from developing spyware-like applications, no matter what the end motive is. The software industry tends to follow trends, and I fear that if this trend of semi-legitimate spyware applications continues, home computer users and enterprise businesses will all suffer for it.

Reference List

1. AOL/NCSA Online Safety Survey
(http://www.staysafeonline.info/pdf/safety_study_v04.pdf)
2. FaceTime Spyware White Papers
(<http://www.facetime.com>)
3. Flying Icons 3D Screensavers
(<http://www.3d-icons.com/>)
4. RFC 2616 – The HyperText Transfer Protocol HTTP/1.1
(<http://www.ietf.org/rfc/rfc2616.txt>)
5. Sasser Worm Indications & Cleaning Instructions –
(<http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>)
6. Microsoft Spyware Analysis
(<http://www.microsoft.com/athome/security/spyware/software/isv/analysis.msp>)
7. The Effect of 180Solutions on Affiliate Commissions and Merchants
(<http://www.benedelman.org/spyware/180-affiliates/>)
8. Sharman Networks Kazaa EULA
(<http://guide.kazaa.com/us/eula.htm>)