Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Spyware & Network Security

When dealing with network security, a security professional's first concerns are who is trying to access the network and whether or not to allow access. The primary concerns are hackers, those who attack from the Internet or from the infrastructure. Additional major concerns are viruses, Trojans, worms, and other malicious codes. There is a type of malicious code that is rarely even given a second thought: Spyware.

Copyright SANS Institute
Author Retains Full Rights

AD

Spyware & Network Security

Lester D. Cheveallier

August 05, 2001

When dealing with network security, a security professional's first concerns are who is trying to access the network and whether or not to allow access. The primary concerns are hackers, those who attack from the Internet or from the infrastructure. Additional major concerns are viruses, Trojans, worms, and other malicious codes. There is a type of malicious code that is rarely even given a second thought: Spyware.

What exactly is Spyware? Steve Gibson defines Spyware at http://grc.com/optout.htm, as:

> ANY SOFTWARE which employs a user's Internet connection in the background (the so-called "blackchannel") without their knowledge or explicit permission. Silent background use of an Internet "blackchannel" connection MUST BE PRECEDED by a complete and truthful disclosure of proposed blackchannel usage, followed by the receipt of explicit informed, consent for such use. ANY SOFTWARE communicating across the Internet absent these elements is guilty of information theft and is properly termed: Spyware.

The origin of Spyware dates back to the creation of Web browser cookies by Netscape as noted at http://users.rcn.com/rms2000/privacy/cookleak.htm. Unbeknownst to the Web surfer, big businesses like advertising agencies, media content providers, and porn sites use Spyware to collect data on a wide range of activities. The data includes Web sites visited, advertisements clicked on, music preferences, shopping habits, and what could be classified as sensitive personal information. This personal information contains name, complete mailing address, e-mail addresses, phone numbers, family members, and any other additional personal information that may be stored on an individual's hard drive.

Distribution of Spyware is a common, daily practice and can come in many forms. The most common form is via the Internet from the many Web sites that are visited every day. In this case, it is nothing more than a small text file placed in the user's Internet Temporary Files folder, commonly called a "cookie". Cookies can store personal information, such as name, address, phone number, user name and password that is entered for a particular Web site. It can personalize a Web site so that it knows whom the surfer is when they return and greet them by name. Often it is used to track surfing habits and sends this information back to the originator of the cookie. For retail Web sites, Spyware is used to track buying habits so that items can be targeted toward personal interests.

Another form of Spyware can be software that is downloaded from the Internet and installed on the computer. This form of software is commonly called freeware or shareware. One example of this is called Bearshare. Bearshare is a program similar to Napster. Unlike Napster, which is strictly music, it is geared toward all types of files.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

When Bearshare is installed, it can install three additional programs that are designed to spy on the computer. It should be noted that Bearshare is not a Spyware program.

The first of these programs is the Onflow player. Their privacy policy at http://www.onflow.com/privacy.php states the following:

> Each time the Onflow Player displays images, it transmits data to our server such as the serial number of the Player, the image displayed, the web page in which it was shown and whether you moved your mouse over the image or clicked on it. This data does not identify you.
>
> It is possible, though unlikely; that a subpoena, court order or similar cause could require us to disclose information we have concerning a particular Onflow Player or a particular registered user. Should that occur, we would have to comply with legal requirements.

From the above statements, it can be concluded that if the serial number of the player is sent, and they can provide information concerning a particular registered user or player then the individual using the player is identified.

The second is a plug-in for the browser that allows an individual to see New.net domains. The privacy policy for their plug is at http://www.new.net./policies_privacy.tp and states:

> We collect general information about you when you visit our web site. This information includes technical information related to your computer and the manner in which you are accessing our site and includes such information as the internet protocol (IP) address of your computer, what operating system your computer is using, what browser software (e.g., Explorer, Netscape or other) your computer is using, and who your Internet service provider is, the Uniform Resource Locator ("URL") of the web site from which you just came and the URL to which you go next and certain operating metrics, such as the amount of time you use our Web site.

Again, information is collected that could be traced back to a particular user, specifically the IP address.

Finally, the third application that is installed is from WhenU.com called SaveNow. As with the above programs, they claim to not gather any personal identifying information via their program. However, on the http://www.whenu.com/about_savenow.html and http://www.whenu.com/privacy.html pages of their web sites can be found the following excerpts respectively:

> WhenU.com does NOT assemble personally-identifiable profiles of SaveNow users and personally identifiable information is not required in order to use the SaveNow software.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

> Users may periodically receive an email alerting them to various offers or information (from WhenU.com or from others). WhenU.com may collect user information such as gender, age and zip code to compile anonymous trend information about Internet and WhenU.com usage patterns. WhenU.com requires individuals to be over 13 years of age in order to download and use any of its products. Therefore, no personal information is collected by WhenU.com from any person who is less that 13 years old.

As stated, WhenU.com knows a user's gender, age, what area the person resides, and his or her e-mail address which they share with others. With this information they now have a personally identifiable profile. They are nice enough to not profile young minors, however, anyone under the age of eighteen is still considered a minor. Personal information concerning minors is now in the hands of WhenU.com, and they are sharing this information with others.

Spyware can also be in commercial software that is purchased at a local retail store. One of the most well known companies accused of producing Spyware is Microsoft. When Windows 95 was first released, the security community accused Microsoft of spying on the general public. The accusation stemmed from their Windows Update Web site in which an individual's computer was scanned to determine if there were any updates available to the operating system. It was touted that this scan, in addition to its intended purpose, was sending personal information about the user and all software installed on the target computer. Although Microsoft vehemently denied this accusation, they changed their Web site, http://windowsupdate.microsoft.com/?IE, to include a message that states, "Windows Update is customizing the product updates catalog for your computer. This is done without sending any information to Microsoft."

Microsoft is not the only well known company who has been accused of dabbling in Spyware. Various parties in the security realm have analyzed Real Networks' and Netscape's software with similar results. A current list of known Spyware can be found at http://www.infoforce.qc.ca/spyware/known_e.html.

Real Networks' software; RealPlayer, RealDownload, and RealJukeBox, have the distinction of being accused of sending the user's name, MAC address, IP address, e-mail address, file downloaded, Internet address accessed, and additional identification information. Whenever any of RealNetworks' software is installed a Globally Unique Identifier, GUID, is created. GUID is a technology standard created by the Open Software Foundation, OSF, to create unique and non-repeating ID tags. Utilizing these tags is akin to assigning a unique serial number to the installed software. Doing so allows the software company to uniquely identify both software and users via the Internet. The GUIDs installed on a Windows machine can be located in the registry key: HKEY_CLASSES_ROOT\CLSID. (**DO NOT CHANGE ANYTHING IN THIS KEY**.) This GUID is sent back to RealNetworks' servers anytime a request for information is made by any of its software.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Two independent studies have been done on Real Networks' software. Richard M. Smith did the first of these in October 1999. His test was on the RealJukeBox player that was first released in the summer of 1999. He found out that player was sending information concerning what music CDs he listened to, how many songs he had recorded on his hard drive, the type of MP3 player he had, and his music preferences.

Utilizing a packet sniffer, Mr. Smith was able to discover exactly what information was being sent back to RealNetworks. The following is what a sample HTTP GET request looks like when requesting CD information:

```
GET /query.html?cmd=cddb+query+6f0fe407+7+150+74670+107840+146875+
196050215005+256182+4068&hello=realuser+real.com+
"Realnetworks+RealJukebox"+1.0&proto=4 HTTP/1.0
Accept: text/html
usr-agent:RealNetworks RealJukebox
host:cdinfo.real.com
X-Taiko-AppGUID: <GUID of system making request>
X-Taiko-AppVersion:1.0.0.438
X-Taiko-AppDistCode:FJ04
X-Taiko-AppBuildType:FREE
```

An electronic fingerprint called a TOC, Table of Contents, number that is passed in the GET request, identifies music CDs. Additionally, the GUID is sent by X-Taiko-AppGUID. With this information alone, RealNetworks can identify not only the CD being played but the user as well. If the software is registered, then any information concerning the registered user is now also available to them because it is tied to the GUID at the time of registration. The registration information includes software, e-mail address, zip code, country, Windows version, type processor, language, software version number, and GUID. It was also discovered that for most commands on the "Sites" and "Help" menu that information including GUID was sent back to RealNetworks. For complete information concerning Mr. Smith's investigation of RealJukeBox go to http://users.rcn.com/rms2000/privacy/realjb.htm.

RealDownload was not much different than RealJukeBox as discovered by Steve Gibson at Gibson Research Corporation. Mr. Gibson used the same technique, utilizing a packet sniffer, to find out what was going on in the background. As with RealJukeBox, RealDownload also used a GUID to identify itself. At the initialization of a download it passed information that could be considered even more critical to network security. This information was as follows:

MAC source address:	xx-xx-xx-xx-xx-xx
MAC dest address:	xx-xx-xx-xx-xx-xx
Frame type:	IP
Protocol:	TCP->HTTP
Source IP address:	xxx.xxx.xxx.xxx
Dest IP address:	xxx.xxx.xxx.xxx

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Source port:	xxxx
Destination port:	80
SEQ:	xxxxxxx
ACK:	xxxxxxxxx
Packet size:	xxx

Additionally it sent the following information:

```
GET /sa2.asp?
product=RealDownload
version=4.0.0.18
platform=Win98
event=downloadStart
url=<requested download file url>
refurl=<domain requested file resides on>
filesize=<file size of requested file>
mime=application/zip
percent=0
downloadid=<GUID + sequence number>
sbid=
sponsor=rdbasic
HTTP/1.0
```

The information that caught Mr. Gibson's attention after further investigation is extremely disturbing. The following information was sent to Real Networks without encryption:

```
Cookie: RNEcomm=ver2.0|xxxxxxxxxxxxxxxxx|Steve|Gibson|OFF|9X3G8
```

The x's represent Mr. Gibson's private e-mail address. Note also, that Real Networks denied that it was capable of associating any personal information made by request from RealDownload.

On July 21, 2000, RealNetworks admitted that RealDownload 'phoned home' utilizing a unique identifier by accident. They immediately released a modified version that removed the creation of a GUID and 'phone home' capabilities as noted on http://www.msnbc.com/news/436070.asp.

Netscape's Smart Download utility sends much of the same information as RealDownload. An additional key piece of information that is sent is the client computer name. If the user is also a member of NetCenter, then the logon ID and their personal e-mail address are transmitted. The full text of Steve Gibson's packet sniffing adventure with RealDownload and Smart Download can be found at http://grc.com/downloaders.htm.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

A new form of Spyware is an IMG tag for a 1-by-1 pixel GIF image file commonly known as Web Bugs. This allows Spyware to be downloaded to the system via the Web browser or an html e-mail message that is received in the mail client. They are also known as clear GIFs and invisible pixels. For a Web Bug to send information, it will be loaded from a different server from the rest of the Web page. The only sure way to stop Web bugs is to turn off the graphics in the browser and block all images from the Web sites. Unfortunately, that means that photographs and drawings on the Web will not be seen. By viewing the source of the page to spot Web Bugs, the user is warned to avoid the site in the future. To see the source code of a page choose Source in the View menu in Internet Explorer or Page Source in the View menu in Netscape Navigator. Of course, this will not stop the bugs that have already been downloaded to your system. Information on Web Bugs can be found at http://www.privacyfoundation.org/resources/webbug.asp.

How does this information affect network security and security professionals? First one must understand the potential use of Spyware in the wrong hands. By utilizing Spyware, such as a cookie, a hacker could capture a complete mapping of the network and have access to installed software, usernames, passwords, client habits, and any number of other useful tidbits. With this information in hand, the hacker would be able to gain complete control of the network, acquire any information, or just shut the whole system down. An individual may as well turn off the lights and go home.

From a security standpoint, sending personal information without prior consent is a violation of the privacy act. Or, is it? It would seem that Spyware requires its own legislative act to protect its citizens. On October 6, 2000 Senator John Edwards introduced the **Spyware Control and Privacy Protection Act of 2000**. Violation of this act, if passed, will carry a $2,500 fine per violation, not to exceed $500,000. Complete text can be found at http://www.federalcourts.com/federalcourt/Internet_Law_Library/s3180spyware.html.

Now that it is realized that Spyware is a security issue with serious implications, what can be done about it? The simplest way for the user to stop Spyware is to read the fine print when downloading and installing software. Most software companies and Web sites publish their privacy policy. If there is not a privacy policy in place, one must rethink the installation or Web site. In a network environment, the installation of software must be restricted to the domain administrators.

By using the services at http://Anonymizer.com, the Web can be surfed anonymously. That means the IP address will not be transmitted out to the Internet, and bugs cannot track the surfer back to his or her system. This is a free site that acts as a filter between an individual and the Internet by hiding the computer's IP address. For a small monthly fee, the site will manage cookies and encrypt the URLs of the sites visited.

If there is still Spyware on the computer system or network, it should be removed. Lavasoft at http://lavasoft.com provides a freeware product, Ad-aware, which will identify programs and cookies that is considered to be Spyware and allows them to be

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

deleted or will recommend uninstall through Add/Remove Programs. Even though a program that contains Spyware is removed, it may leave behind the files that are responsible and may remain active on the system. Also, if only the components responsible for report back while leaving the program is removed, it may disable the functionality.

As suggested by Kim Wimpsett at http://cnet.com/software/0-8888-8-3217791-5.html?tag=st.sw.8888-8-3217791-1.txt.8888-8-3217791-5, configuration measures that should be taken is to disable the browser's ability to view active content such as ActiveX, VBScript, JavaScript and Java graphics files which are likely to contain Web Bugs. Another consideration is to ensure one's e-mail address is not contained in any FTP settings. Running Web browser with its highest security settings will keep an individual as safe as possible. This means sacrificing the Web's interactive capability and the convenience of personalization in order to ensure privacy. Additionally, any firewall that monitors Internet traffic and allows the control of outgoing transmission is effective in the combat against Spyware.

In his article "Internet Insecurity", Chris Stein of Time Magazine made ten recommendations on how to protect oneself from identity theft. The recommendations are "Install a home firewall and virus protection.", "Be careful what you give out.", "Don't download anything unless you trust the sender --- and the file.", "Use dummy e-mail accounts.", "Don't let your browser be a blabbermouth.", "Opt out.", " Don't accept unnecessary cookies.", "Use encryption for sensitive data.", "Consider using an anonymizer.", and "Clear the memory cache after surfing the Internet.". Since there is no way to be totally secure, Stein also states, "If it has to stay secret, don't put it on a computer hooked up to the Internet."

The final solution is the decision made pertaining to the level of anonymity that is desired on the Internet. As security professionals are aware, the only way to be truly anonymous on the Internet is not to connect. Care should be taken in any case to ensure system and network integrity.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References

About SaveNow, WhenU.com, 17 Jul. 2001 <http://www.whenu.com/about_savenow.html>

Gibson, Steve, The Anatomy of File Download Spyware, 14 Jul. 2000, Gibson Research Corporation, 17 Jul. 2001 <http://grc.com/downloaders.htm>

Gibson, Steve. OptOut, Gibson Research Corporation, 17 Jul. 2001 <http://grc.com/optout.htm>

Known Spyware, 11 Jun 2001, Infoforce, 17 Jul. 2001 <http://www.infoforce.qc.ca/spyware/known_e.html>

New.Net: Privacy Policy, New.net, 17 Jul. 2001 <http://www.new.net./policies_privacy.tp

Microsoft Windows Update, Microsoft Corporation, 17 Jul. 2001 < http://windowsupdate.microsoft.com/?IE>

Onflow Privacy Policy, Onflow, 17 Jul. 2001 <http://www.onflow.com/privacy.php>

Senator Edwards, John, Spyware Control and Privacy Protection Act of 2000, 22 Sept. 2000, Federalcourts Dot Com, 17 Jul 2001, <http://www.federalcourts.com/federalcourt/Internet_Law_Library/s3180spyware.html>

Smith, Richard M. The Cookie Leak Security Hole in HTML Email messages, 30 Nov. 1999, RCN Corporation, 17 Jul. 2001 <http://users.rcn.com/rms2000/privacy/cookleak.htm>

Smith, Richard M., FAQ: Web Bugs, Privacy Foundation, 17 Jul. 2001 <http://www.privacyfoundation.org/resources/webbug.asp>

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Smith, Richard M. The RealJukeBox monitoring system, 31 Oct. 1999, RCN Corporation, 17 Jul. 2001 <http://users.rcn.com/rms2000/privacy/realjb.htm>

Stein, Chris, "Internet Insecurity." Time Magazine 2 Jul. 2001: 44-51.

Wimpsett, Kim. Stop Spyware Cold, 26 Oct 2000, CNET.com, 17 Jul 2001 <http://cnet.com/software/0-8888-8-3217791-5.html?tag=st.sw.8888-8-3217791-1.txt.8888-8-3217791-5>

Sullivan, Bob, More Privacy Concerns for Real, 21 June 2000, MSNBC, 17 Jul, 2001 <http://www.msnbc.com/news/436070.asp>

User Agreement, WhenU.com, 17 Jul. 2001 <http://www.whenu.com/privacy.html>

© SANS Institute 2001, Author retains full rights.

Last Updated: October 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS DFIR Prague 2015	**Prague, CZ**	**Oct 05, 2015 - Oct 17, 2015**	**Live Event**
SOS: SANS October Singapore 2015	**Singapore, SG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS San Francisco 2015	**San Francisco, CAUS**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
SANS Cape Town 2015	**Cape Town, ZA**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
Security Leadership Summit & Training	**Dallas, TXUS**	**Dec 03, 2015 - Dec 10, 2015**	**Live Event**
SANS Cyber Defense Initiative 2015	**Washington, DCUS**	**Dec 12, 2015 - Dec 19, 2015**	**Live Event**
SANS Seattle 2015	**OnlineWAUS**	**Oct 05, 2015 - Oct 10, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**