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.

Are You Being Watched?

Society today has become more sensitive to the dangers of their physical surroundings. Everyone knows not to go out alone, not to talk to strangers, not to pickup hitchhikers. However, not everyone is aware of just how dangerous a place the Internet can be. We happily open up our web browser and surf away, not even thinking for a moment that we might not be alone. In reality, it is not just you and the Internet out there. We would be very alarmed, if someone were following us around town and recording all of our activi...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Are You Being Watched?

Lorna J. Hutcheson

July 20, 2001

Introduction

Society today has become more sensitive to the dangers of their physical surroundings. Everyone knows not to go out alone, not to talk to strangers, not to pickup hitchhikers. The list could go on and on. However, not everyone is aware of just how dangerous a place the Internet can be. We happily open up our web browser and surf away, not even thinking for a moment that we might not be alone. However, in reality, it is not just you and the Internet out there. We would be very alarmed, if someone were following us around town and recording all of our activities. But, most users are unaware that the same ability exists and is currently being used on the unsuspecting Internet traveler. With every trip out on the Internet, users are being watched and profiled.

How can that be, you might wonder. You are a safe Internet user. You don't accept cookies, you turned off your Java Scripting and more importantly you are behind your company's firewall. Unfortunately we will see that it isn't enough. The Internet Backchannel provides a very real path to get to you and if you are not talking, don't be so sure your computer isn't. Three areas of concern are the Internet Backchannel, spyware and user profiling. This paper is not meant to provide a thorough analysis of the problem. Each of the three areas to be discussed is a major problem area and cannot be covered in great depth here. However, the purpose of this paper is to make you aware that while you are sitting at home and quietly surfing the Internet, you really should be worried about who is watching.

Internet Backchannel

The "Internet Backchannel" is a term just coming into existence and is rapidly gaining usage. It refers to an existing Internet connection that can be used by others for their own purposes while the connection's owner is using it or it sits idle.[1] The Internet Backchannel is a powerful connection. All users, when they are connected to the Internet are providing a path right to their computer and leaving the door open. The Internet/HTTP uses port 80 as a standard. Since this is so well known and nearly everyone is connected to the Internet, it has provided a direct connection that is being exploited. What can someone really do? I will give you a personal example as I was researching this project. I went to OptOut's web site and wanted to check out a discussion group. I am behind a firewall in our testbed area and wasn't really worried about the site. However, when I clicked on the link to go to the discussion group, a window popped up that said it was going to upgrade my Outlook Express. I wanted to say no, but my only option was OK. I tried to close it with brute force, but it proceeded to download to my system anyway. It changed my files, updated my registry and then launched Outlook Express. If that is not power, I don't know what is. This was all running in the open where I could see it, what if it was in stealth mode?

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Unknown to many users, this connection allows anyone to take advantage of them while they are on the Internet. Not every person on the Internet is bad, but it does provide those who choose to do so a way to abuse its intended purpose. Let's look at a few examples.

Firewalls were designed to **assist** network administrators in protecting their networks. However, it gives those who are less informed a false sense of security. Network administrators, who want to allow users to connect to the Internet, open up port 80. Unfortunately, by doing so, it opens a path into their network. If a company wants to collect information on you, you are not protected by the firewall. Take a cookie for example. Cookies were designed to assist web developers in knowing that a user had been there before and certain preferences that they may have. Unfortunately, some have taken advantage of this and exploited the ability. Instead of just sending preferences about the web site, they can also send your IP address, email address operating system and several other identifying pieces of information. Your firewall or proxy server is useless in these cases. It simply rides on the Internet Backchannel right out of your system to whoever is on the receiving end. To make matters worse, they are not encrypted so anyone with a sniffer can see the information. A good example and case study is located at OptOut, a website maintained by Steve Gibson.[2]

Ok, let's say you are smart enough to know not to accept cookies and disable them or be prompted first. That will not stop information about you from being gathered. At a site called Web Developers Journal, web designers are told how to bypass this small problem and don't understand why users would not want to accept cookies in the first place. In an article by Dave Cartwright he states "The only drawback, of course, is that some users turn off the cookie support on their browsers, labouring under the misconception that cookies are in some way insecure. There are ways around this, though. For example, the site can be implemented behind the scenes as a set of HTML forms, with the user identifier passed around as a hidden data field."[3]

Software is being designed to take advantage of the Internet connection. A product called HTTPtunnel does this very thing. It is free software that users can download and lets them bypass the firewall. Their website makes this statement "This can be useful for users behind restrictive firewalls. If WWW access is allowed through a HTTP proxy, it's possible to use httptunnel and, telnet or PPP to connect to a computer outside the firewall."[4] If this program is used, the Internet Backchannel is accessed undetected by the firewall. Now users can bring data in and out without being detected. There are many other sites that brag about this very capability.

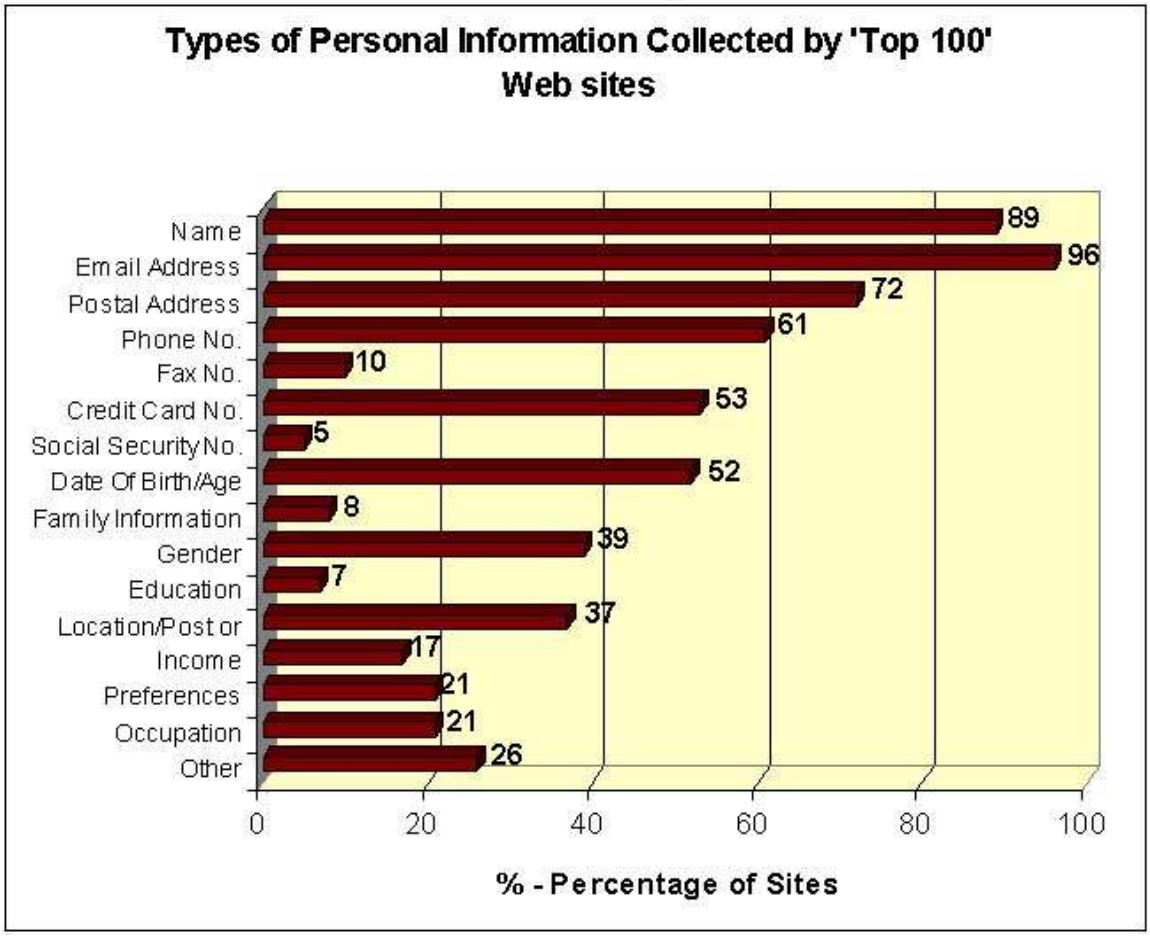
Firewalls and Proxy servers were designed to protect users. The Internet, protocols, and other standards were developed to ensure compliance and allow communication across a wide variety of platforms. However, as history shows, someone will find a way to use it in a fashion it was never intended to be used. This leaves us in a position to always have to be on guard and be aware of our surroundings, no different than walking by yourself at night or in the daytime for that matter. Now that we know a path exists to us by simply using the Internet, we need to take a look at what people are doing with this capability.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

User Profiling

Many people may think that a little information about my machine isn't bad or "who cares if they have my email address." Unfortunately, over a period of time, this type of information can add up. User profiling is taking information about someone and continually updating it and compiling it in one central location. By doing this, you will eventually get a good profile of that person. Those who get this data are also not usually shy about sharing it or careful in protecting it. If creditable companies and individuals have the capability to collect this information, so do criminals and really bad people. Below are two studies that demonstrate exactly how much they can learn about you. This information is from a report done by Dave Halstead and Helen Ashman. The results are quite startling.

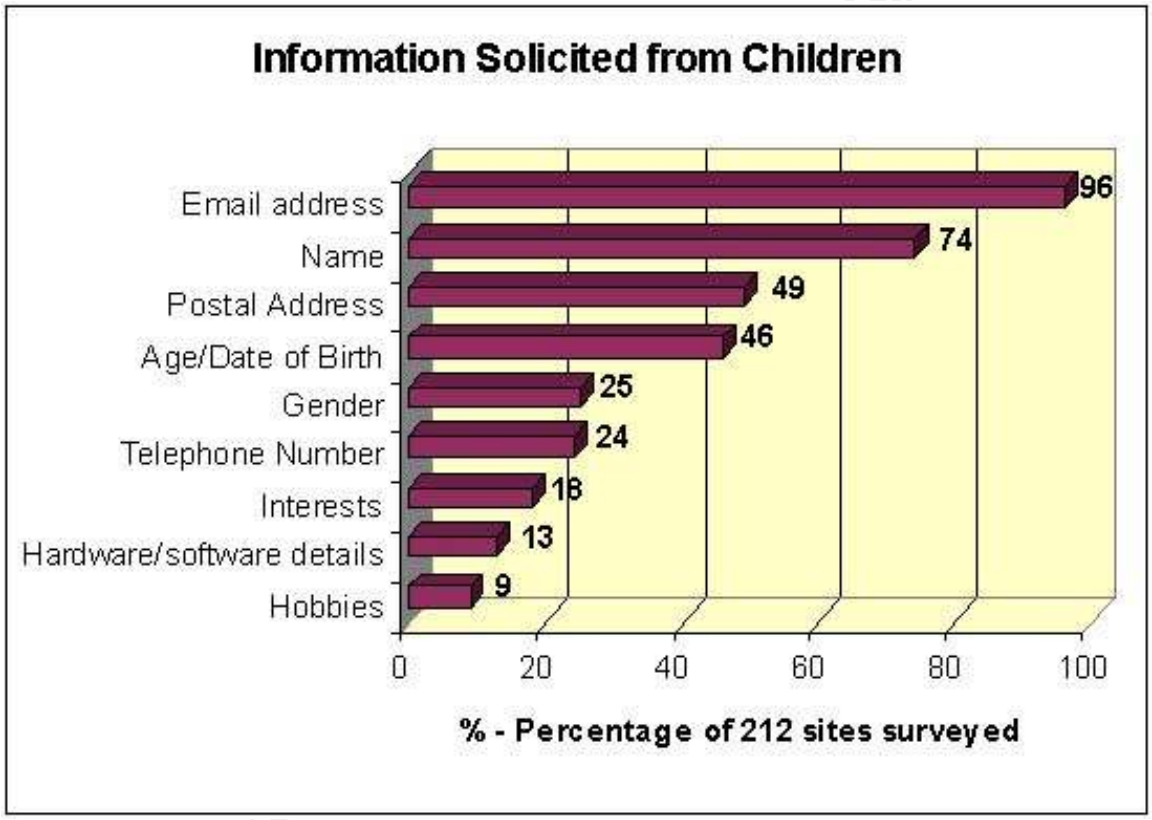
"The following graph based on figures from a report to the Federal Trade Commission which studied 100 commercial web sites and their privacy policies, shows clearly the sort of data that is collected."[5]



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

If that doesn't bother you, look at the next chart and the information that is collected.

"CME's recent survey of 75 randomly chosen kids' sites and 80 top commercial children's sites, highlight how extensive these practices are - the results found that 95% of the random sample collect personally-identifiable information from children, with only 27% displaying a privacy policy! A similar survey by the FCC (US Federal Communications Commission) found some alarming statistics. Of the 212 web sites included almost all (96%) solicited the children's email address with almost half (49%) requesting their postal address. The following chart shows a clear summary the information solicited by sites in the survey."[6]



Information of this nature has no business being collected and compiled without the user's knowledge and consent. But, there are many ways this occurs once you visit a web site. They can extract information about you from your machine and it won't be long till they can compile information about you from many different sources. If a web site can get to your machine that easy, think about a hacker. You may think or feel that you are in control about your Internet wanderings, but think again. A white paper at the Davisor web site states "User actions may be tracked in the application, which is used to connect to the Internet, somewhere on the route to the used service, or within the service. To get the most information, tracking should be done as close to the user as possible."[7]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Information about every website you visit, what you click on and even down to the amount of time you spent on a page is being compiled and sent back to who ever decides to follow you around. What are they doing with this information. Are they watching what you buy to determine likes and dislikes for marketing purposes or are they doing this to determine if you are a good place to rob because you have a lot of money and they know what you bought? How about those with people with children? If a child is on the Internet and mom and dad haven't been conscience of what they are doing, some not so nice person can be following your child around in cyberspace. Do you want them to have your home address? There is way that information about you is being collected and that is spyware.

Spyware

"Spyware is ANY SOFTWARE which employs a user's Internet connection in the background (the so-called "backchannel") without their knowledge or explicit permission."[8] You may be extremely careful while you're on the internet and take every precaution possible, only going to sites that have valid certificates, or those sites that are well known, but are you still really safe. Say you visit a site and download a shareware program. It's one everybody uses so it must be safe. Steve Gibson found out that this was not entirely the case. When you read his article entitled "The Anatomy of File Download Spyware" you find important information about him and his system was being sent out with out his permission.[9] It was a well know product from RealNetworks called RealDownload.

You may be extremely careful out on the Internet, but who is your computer talking to? With spyware, the information is being sent on the Internet Backchannel and does not tell the user that it is happening. There is even software designed to run in stealth mode on your computer and transmit out everything you do. There are many sites that post lists of known spyware or suspected spyware. It is amazing to see the number of software programs that report back to their home server.

Some companies have end-user license agreements they try to hide behind. Most users do not read all of those pages of fine print. Companies claim they told you what they were going to do, but then make it so long and vague even a technical person can't understand it. A prime example of this is found in the end-user license agreement provided with Transcom software. Look at this statement buried in the middle of three pages of legal and technical jargon. I have bolded the key points "By becoming an End-user, you hereby agree that TransCom may share with other parties both aggregate information and limited individual information gathered during your use of TransCom's BeeLine and/or the Internet. 'Aggregate Information' is information that describes the habits, usage patterns and/or demographics of its End-Users as a group but **does not indicate the identity of the particular End-User**…You also agree that locator information about you may be gathered, processed or used as provided in the following paragraph. 'Locator information' consists of an End-Users name, e-mail address, physical address and/or other data that enables the recipient to **personally identify the End-**

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

User."[10] Exactly what are they saying? Are they or are they not going to associate information with your identity. More importantly what are they doing with the information being transmitted to them and who are the recipients of this information? Information that will be sent unknown to you. Not only are they collecting information dealing with your use of the product, but will monitor you on the Internet.

Conclusion

The Internet is a valuable tool. However, it is extremely important to realize that you are not alone out there. What you do, where you go, who you chat with, what you buy, personal information, system information etc. is all being collected and analyzed. When all of the little pieces of information about you are collected into one database, the profile it reveals should scare you. Users behind a firewall or proxy server are not safe. Even if you don't go out on the net much, when you do venture out who is your computer talking to?

Here is the really tough question. How do we fix the problem? The information in this paper begs an answer to that very question. However, an end is not in sight. The Internet gained speed and exploded so fast it has left many areas trying to catch up. Standards have been written to support multiple platforms that were designed before there was ever an Internet. It's like putting the cart before the horse. The Internet changed the way the world conducts business and works. Almost every business, company, school etc out there today, uses the Internet. Pulling the plug is not a solution due to the amount of money invested in the Internet world. It is almost a form of artificial intelligence more than it is anything. Every time one problem gets addressed and fixed, someone finds a way to get around it. To complicate matters further, the Internet changes on a daily basis. It is changing so fast that standards can not keep up with it, much less drive it in the direction it should go. Legal laws and regulations are another area that is trying to keep up. No one knows how to handle the Internet and its infringements on many areas of our postal service, phone companies etc.

Laws are being introduced in many areas to help control those who do this type of profiling. Senator John Edwards has introduced a Spyware Control Act to try and regulate companies. He states "I have been closely following the privacy debate for sometime now, and I am struck by how often I discover new ways in which our privacy is being eroded…Spyware is among the more startling examples of how this erosion is occurring."[12] If laws get passed to help control this area of profiling users, how is it going to be enforced in a world where the culprit can be hundreds of thousands of miles away and in another country which crosses jurisdiction. What about those companies, who say what they are going to do, but do it in such a complicated way that the average user has no idea what they are agreeing to.

In essence, at this point and time, there is no answer or solution to the problem. The only thing we can do is damage control. I am not saying to go unplug your computer from the Internet or never go out on it again. But, I am saying that just as you are aware of your physical surroundings and the dangers lurking in the shadows or in plain view, you have

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

to be aware of the dangers that exists on the Internet. We cannot stop the problem or make it go away, but we can help minimize the effects of it. I will leave you with one final thought. "The Freedom system has had some excellent reviews, which are summed up with comments like the following, from Patrick Norton of PC Magazine:

> 'If online privacy is an issue for you, we can't think of a better option, except for not going online at all.'"[11]

Works Cited

[1]Gibson, Steve. "The Code of Backchannel Conduct"
URL: http://grc.com/oo/cbc.htm

[2]Gibson, Steve. "The Anatomy of File Download Spyware"
URL: http://grc.com/downloaders.htm

[3]Cartwright, Dave. "Customize Your Content With User Profiling"
URL: http://www.webdevelopersjournal.com/articles/user_profiling.html

[4]NOCREW. "HTTPtunnel"
URL: http://www.nocrew.org/software/httptunnel.html

[5]Halstead, Dave and Ashman, Helen. "Electronic Profiling"
URL: http://ausweb.scu.edu.au/aw2k/papers/halstead/paper.html

[6]Halstead, Dave and Ashman, Helen. "Electronic Profiling"
URL: http://ausweb.scu.edu.au/aw2k/papers/halstead/paper.html

[7]Davisor. "Universal Profiling"
URL: http://www.neuslab.com/main/whitepapers/up.html

[8]PcMedix Web Designs."What is Spyware?"
URL: http://www.pcmedixwebs.com/spyware.htm

[9]Gibson, Steve. "The Anatomy of File Download Spyware"
URL: http://grc.com/downloaders.htm

[10]Gibson, Steve. "Fine Print Funny Business"
URL: http://grc.com/oo/fineprint.htm

[11]Halstead, Dave and Ashman, Helen. "Electronic Profiling"
URL: http://ausweb.scu.edu.au/aw2k/papers/halstead/paper.html

[12]Krebs, Brian. "Senator John Edwards Introduces 'Spyware Control Act'"
URL: http://grc.com/spywarelegislation.htm

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Internet References

AntiOnline. "FightBack! Help AntiOnline In Its Fight Against Malicious Hackers." 23 Jul 2001. URL: http://www.antionline.com/cgi-bin/Fight-Back?question=What_Information_Can_The_Websites_I_Visit_Find_Out_About_Me (16 Jul 2001).

Cartwright, Dave. "Customize Your Content With User Profiling." 4 Apr 2000. URL: http://www.webdevelopersjournal.com/articles/user_profiling.html (19 Jul 2001).

CEXX. "Trouble With Spyware & Advertising-Supported Software." URL: http://cexx.org/problem.htm (6 Jul 2001).

Cosley, Casey. "What is Spyware?" URL: http://www.acecmt.com/spyware.html (11 Jul 2001).

Davisor. "Profiling Basics" 3 Apr 2001 URL: http://www.neuslab.com/main/whitepapers/profbasics.html (19 Jul 2001).

Davisor. "Universal Profiling" 9 Mar 2001 URL: http://www.neuslab.com/main/whitepapers/up.html (19 Jul 2001).

Digital Image Design Incorporated. "Selected Client List" URL: http://www.didi.com/www/areas/services/clients/index.html (19 Jul 2001).

Digital Image Design Incorporated. "User Profiling" URL: http://www.didi.com/www/areas/services/technology/2/ (19 Jul 2001).

Fitzsimons, John. "Am I infected?" URL: http://www.alphalink.com.au/~johnf/spyware.html (21 Jun 2001).

Engage. "Engage ProfileServer" URL: http://www.engage.com/solutions/software/ProfileServer (19 Jul 2001).

Gibson, Steve. "Fine Print Funny Business" URL: http://grc.com/oo/fineprint.htm (20 Jun 2001).

Gibson, Steve. "Internet Connection Misuse & Abuse" URL: http://grc.com/optout.htm (20 Jun 2001).

Gibson, Steve. "The Anatomy of File Download Spyware" 14 Jul 2001. URL: http://grc.com/downloaders.htm (20 Jun 2001).

Gibson, Steve. "The Code of Backchannel Conduct" URL: http://grc.com/oo/cbc.htm (20 Jun 2001).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Halstead, Dave and Ashman, Helen. "Electronic Profiling"
URL: http://ausweb.scu.edu.au/aw2k/papers/halstead/paper.html (15 Jul 2001).

Hazeleger, Dick. "Spyware List" 3 Jun 2001.
URL: http://www.alphalink.com.au/~johnf/dspypdf.html#7 (3 Jul 2001).

Krebs, Brian. "Senator John Edwards Introduces 'Spyware Control Act'" 10 Oct 2001.
URL: http://grc.com/spywarelegislation.htm (20 Jun 2001).

Lalonde, Gilles. "The Spyware Infected Software List" 11 Jun 2001.
URL: http://www.infoforce.qc.ca/spyware/ (3 Jul 2001).

Naviant make contact. "High Tech Household File"
URL: http://www.naviant.com/Products/elist/hthh.asp (20 Jun 2001).

Naviant make contact. "Identify Online Households and Turn Them into Buyers"
URL: http://www.naviant.com/Products/eTargeting/eTargeting.asp (20 Jun 2001).

Naviant make contact. "Registration Reports-Data Reporting Tool"
URL: http://www.naviant.com/Products/eRegistration/reporting.asp (20 Jun 2001)

NOCREW. "HTTPtunnel"
URL: http://www.nocrew.org/software/httptunnel.html (9 Jul 2001).

PcMedix Web Designs."What is Spyware?" 31 May 2001.
URL: http://www.pcmedixwebs.com/spyware.htm (20 Jun 2001).

Salkever, Alex. "A Prime Port of Call for Hackers?" 11 Jul 2000.
URL: http://www.businessweek.com/bwdaily/dnflash/july2000/nf00711e.htm (11 Jul 2001).

SpyCop. "Is Your Boss, Spouse or Competition Spying On You?"
URL: http://spycop.com (20 Jun 2001).

Vazquez, Johann. "Java Tip 103: Send HTTP requests for serialized objects "
URL: http://www.javaworld.com/javaworld/javatips/jw-javatip103.html (6 Jul 2001).

Wimpsett, Kim. "All About Spyware" Find and Eliminate Snooping Software and Web Bugs. 26 Oct 2000. URL: http://www.cnet.com/internet/0-3761-8-3217791-2.html?tag=st.int.3761-8-3217791-3.SUBDIR.3761-8-3217791-2 (11 Jul 2001).

Wimpsett, Kim. "The Spyware Threat" Find and Eliminate Snooping Software and Web Bugs. 26 Oct 2000. URL: http://www.cnet.com/internet/0-3761-8-3217791-3.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: October 10th, 2015

Upcoming SANS Training

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

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 Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 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 Cape Town 2015	**Cape Town, ZA**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
SANS San Francisco 2015	**San Francisco, CAUS**	**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 Las Vegas 2016	**Las Vegas, NVUS**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Dubai 2016	**Dubai, AE**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SOS: SANS October Singapore 2015	**OnlineSG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**