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.

How Spyware fits into Defense in Depth

The layered approach to defending network systems, Defense in Depth, is the best approach to protecting the assets of a company or individual, but remember that this is not 100% secure. No network is completely secured against electronic, or physical attacks regardless of what solutions are used to protect it. New spyware programs crop up everyday, and the attackers are ever evolving in the ways that they try to attack system vulnerabilities, which is why our network defenses and corporate policies have to be ever evol...

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

How Spyware fits into Defense in Depth

Michael McCardle
GSEC
Version 1.4b
January 17, 2003

Purpose:

Defense in Depth describes a layered approach to securing information and resources, as well as maintaining confidentiality, integrity, and availability of these resources. A common threat to such resources that is often overlooked in this process is Spyware, or Ad ware. Most IT staff only defends against malicious code in the guise of viruses, or hackers and disgruntled employees who plan on compromising or damaging information. So what is the real risk of these Spyware programs to individuals and corporations? What are their potential for damage or information leakage and how realistic is it to maintain or create a policy and procedure for coping with these programs? These are the questions I will provide some insight to in this paper.

Overview:

A definition of Spyware provided by Steve Gibson states "Spyware is ANY SOFTWARE which employs a user's Internet connection in the background (the so-called "back channel") without their knowledge or explicit permission. Silent background use of an Internet "back channel" connection MUST BE PRECEDED by a complete and truthful disclosure of proposed back channel 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 and rightfully termed: Spyware". By the definition here, the minimum risk you have to consider is bandwidth utilization and what type of information is being gathered and sent to the distributors of the Spyware. Keep in mind that Spyware can be acquired through almost any medium including emails, "freeware"," shareware" and Internet surfing. Spyware programs are executable programs that run in the background and are capable of doing anything that programs can do without user intervention. This may include monitoring user activity on the local machine, reporting browser history files, parsing your cookies, or reading places on your hard drive such as C:\Winnt\System32\Repair to acquire data about you or your machine and send it out across the internet to some unknown location.

The term Spyware, in most cases, is synonymous with Ad ware, and is potentially a Trojan horse program. To protect against Trojans we install anti-virus software and sometimes utilities that specialize in Trojan detection and removal such as "Patchwork" from http://grc.com/pw/patchwork.htm. This is fairly common practice. I have yet to see a company that regularly uses anti-Spyware utilities to prevent against Spyware programs. Why? Spyware programs may not open a hole in the firewall for a hacker; but once the code is on a client machine, does a hacker need to breach the firewall or any other perimeter or host defense to get information? Not at all. He lets the Spyware running on the client machine do all the work for him by establishing connections to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

remote servers, through the corporate defenses, that wait for the incoming connections so they can gather information about the users. Many Spyware programs simply collect marketing information such as where the user has been on the Internet and what interests that specific user. Banner adds and other marketing ploys can then adjust the material displayed to accommodate that user to make an easy sale, or download banner ads to the local machine. In order for these marketing companies to know what to show you, they must also know how your system is configured and what software is running on it.

Some of the information that can be gathered and sent across the Internet is:

-The version of Operating System you are running
- Browser type
- Is scripting enabled
- What version of java you are running
- Screen size
- Available plug-ins
- DNS information from your current domain
- Run a trace route back to you to find out where you live on the net.

For an example of the output from such a query check out http://www.privacy.net/analyze/. It will certainly open your eyes to some of the capabilities of simple server-side Spyware.

Now you're asking, how can these Spyware programs do this? One way Spyware programs can acquire data about you and track your movements across the Internet are through files called cookies. Cookies are small files that are placed in your system by web servers when you visit, and can track and record your Internet usage. Each time you visit a site, the site checks to see if you have a cookie for that site, if you do then they retrieve your personal settings for the site, if not they deliver a cookie to your machine. Cookies come in a couple different flavors. Persistent cookies, which are configured to stay on your system for many years using an expiration date, typically many years in the future, or "session cookies" that are removed when the session is closed, usually used by shopping carts at online stores. By themselves they are harmless and some people even say helpful. They track where you're going and what your doing online, they can help customize and personalize your surfing experience by storing passwords, registration information, and remembering personalized settings to the web page you are opening if you've been there before. Most cookies will randomly generate a Serial number and assign it to you.

Spyware can use these cookies to follow you where you've been and send demographical information back to the servers waiting for your information. Typically a cookie will contain a serial number that represents you, or your machine. This serial number will remain with you for the duration of the cookie and the marketing company will identify you by looking at your serial number. Given this information, they will most likely not know your name, but they will know what web sites you have visited and which

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

product advertisements you have shown an interest in. This information will be recorded and tied to the serial number you received originally. Now the marketing company can adjust the banner ads on all web pages that you go to that participate in their program to display an add about "video cards" since you followed a link to see a video card once.

Is there a way for a Spyware or Ad-ware program to look through all of the cookies on a given machine? A bug was detected, back in 1998, which allows any web site to parse cookies on the user's system placed there by other web sites. It can occur in one out of every few thousand visitors. Some of the examples listed on www.privacy.net/cookiebug appear to include several, or possibly ALL, the cookies on the user's system. Some cookies included the user's home address, e-mail address, and numerous user ID's from various web sites. Some examples are listed on www.privacy.net/cookiebug : Here is only one example of what is on that page :

"XXX" is substituted for the personal information in the following examples.

Example:

Mozilla/4.03+[en]+(Win95;+I)

AnonTrack=E0F069xxxxxF396;+**EGSOFT_ID**=20xxxxxxx5-3343517328.29171482;+ **RMID**=cf571xxxxx99ee0;+**NGUserID**=d10xxxxxx957-884581861-3;+**KRNM**= d083adfd-xxxx85415-1;+**hanna_cust_id**=8xxxxx35;+**RoxenUserID**=0xxxxx6f;+**Admin=** 20xxxx56-2405491264.29172016;+**EW3_ID**=20xxxxx2910.885068468;+ **CFTOKEN**=1xxx;+CFID=7xxxx02;+**UID**=4xxxx16

Another way for the Spyware programs to gain information about you or your machine is to simply install itself and then execute. Spyware typically is an independent program that runs in the background. Programmers working for a Spyware distributing company can write a routine that can run with system privileges and retrieve information from your computer. If they want to retrieve word documents from their targets, then they write code that looks for word documents and sends them back to the proper place on the Internet. If they want passwords, then they can write a routine that copies the SAM from any machine running Windows NT, or Password files from a Win9x box. The thing to keep in mind is that these programs are limited only by the imagination of the author, or the limitations of the programming language being used.

In October of the year 2000, Senator John Edwards introduced the 'Spyware Control and Privacy Protection Act" which states that this Spyware must make the user aware of it's presence and give them a choice to back out of using or enabling the Spyware, as well as what information and to whom the information is being sent to; and for users to see what information has been gathered about them to date. In addition, the manufacturers would have to properly encrypt and protect this user data from other sources, such as hackers. One final note on this bill is that the end users will have the right to sue the manufacturer for up to $500,000.00 dollars per violation if they violate

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

their own policy in any way. This has not deterred the distribution of Spyware by some of the Spyware companies.

A recent virus currently being passed around the Internet called "Friend Greetings", by *Permissioned Media*, is a great example of why you need to read the EULA's. This is an application that you have to install, and once it's installed to your system it runs in the background. The user receives an email stating that they have a Greeting card. In the body of the email it says you can pick up the greeting card by going to the link provided in the email. When you click on the link, it takes you to the web site and begins an installation process on your computer. It pops up the End User License Agreement, which is where most people click I agree or next instead of reading the EULA. However, if they were to read this EULA they could see what the program is going to do. Some excerpts of their EULA are as follows:

"2. Consent to Receive Ads and Use of Information. By downloading, installing or using PerMedia, you agree to receive advertisements from Permissioned Media's business partners and associates."

8. Disclaimer of Warranty. USE OF PERMEDIA, PERMISSIONED MEDIA'S WEB SITE, OR ANY CONTENT IS ***AT YOUR OWN RISK.***

3. Updates/New Information. Permissioned Media reserves the right to add additional features or functions to the version of PerMedia you install, or to add new applications to PerMedia, at any time.

*9. Limitation of Liability. IN NO EVENT WILL PERMISSI*ONED MEDIA NOR ITS EMPLOYEES, *DISTRIBUTORS, DISTRIBUTEES, SUPPLIERS, BUSINESS ASSOCIATES, ADV*ERTISERS, DIRECTORS OR AGENTS *(COLLECTIVELY "AFFILIATES") BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENT*AL OR CONSEQUENTIAL *DAMAGES ARISING….. LOST PROFITS, B*USINESS INTERRUPTION, LOSS OF *INFORMATION, LOST OPPORTUNITY OR OTHER PECUNIARY LOSS, EVEN* IF PERMISSIONED MEDIA OR ITS *AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.*"

This EULA seems to follow the "Spyware Control and Privacy Protection Act" which is a great step in the right direction. Unfortunately no one reads the EULA's. This program maintains the right to email itself to every email address in your address book, send information back to Pemissioned Media, and download new software to your machine. This application functions like classic a Spyware application. However, according to the definition of Spyware provided by Steve Gibson, it is not Spyware because it states exactly what it does in the EULA. Where do you draw the line? I Think Permissioned Media has covered themselves by providing the information necessary in the EULA so they can't be considered a textbook example of Spyware. The biggest problem with this one is the fact that Permissioned Media retains the right to install new software to your machine, more than likely without any further consent. What is the newer software going to send? If someone where to compromise their servers and acquire the ability to push

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

their own software through Permissioned Media's updater, they could easily push Trojans, or other malware to the people who have this installed on their systems. Users must read the EULA. IT staff must educate the end users about this threat.

If the public knew what was going on in the background could they defend against it? Sure they could. There are numerous programs out there both free and with purchase programs that can help defend against Spyware, Ad-ware, and Cookies that can assist these programs in collecting information about you. Ad-Aware is one such program designed to defend against the use of Spyware, or Ad-Ware. This is available from http://www.lavasoftusa.com/. Ad-aware 5.83 is a free multi Spyware removal utility that scans your memory, registry and hard drives for known Spyware components and lets you remove them safely.

What does all this mean to big business? What about to home users? The home user is more vulnerable to Spyware simply due to budget, and a lack of necessary knowledge and resources to defend a machine against electronic attacks. Personal firewalls, anti-Virus, and Anti-Spyware utilities should be on every home machine. These utilities should be configured correctly and kept up to date with service packs, hot fixes and signature files. A poorly configured piece of software can be more dangerous in some situations than no software at all. Another thing to watch for, or take into careful consideration is the freeware and shareware out there that you can download which contains spyware. Once these programs are installed and running on a system, the spyware kicks in and starts collecting information and reporting back to the originator of the program. In many cases, if you clean the spyware off of your system, the application you downloaded and installed will not work. Just because it is tagged as "freeware", doesn't mean you don't pay in some form or another. Take for example Cute FTP version 4.2 Beta 6. I downloaded and installed this Shareware program to a clean Windows 2000 Professional Service Pack 2 machine. During installation I noticed part of the End User License Agreement stated :

"3. INFORMATION COLLECTION. Evaluation copies of the Software display advertising banners. In order to deliver advertisement banners effectively, GlobalSCAPE or its advertising agencies collect information concerning your computer and your use of the Software in the following ways:

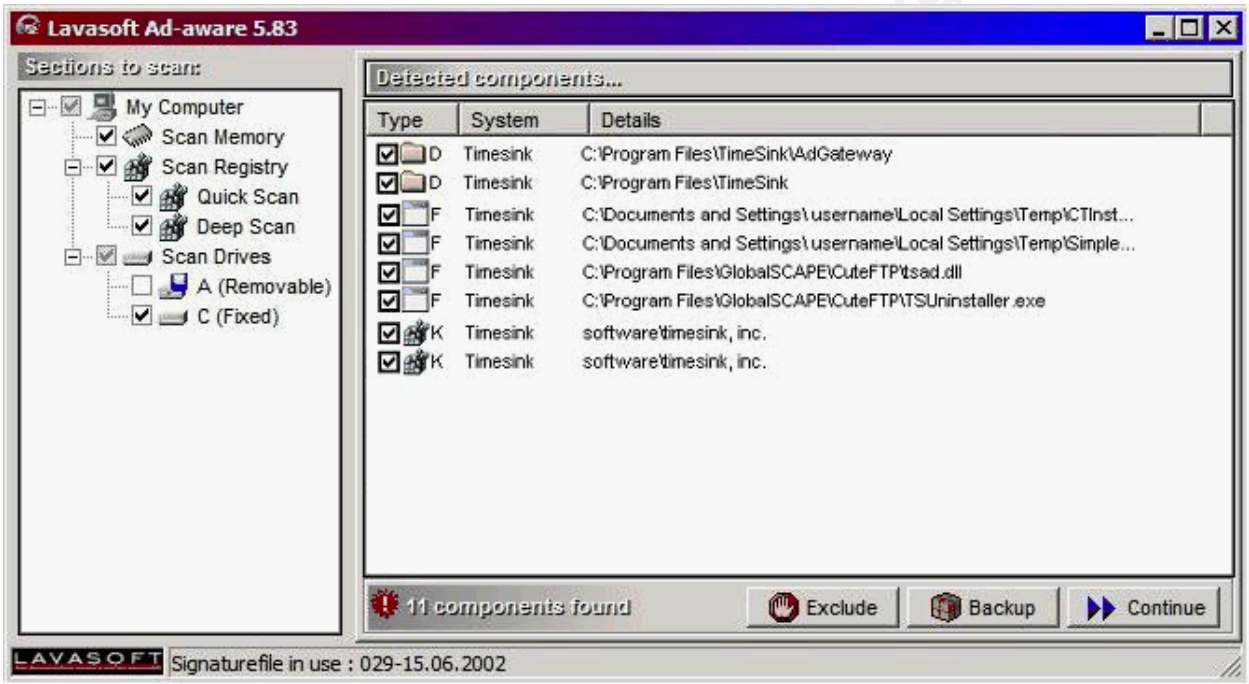
(i) During installation. You will be asked to complete a voluntary demographic survey. This information is not associated with your name or any characteristic that would personally identify you.

(ii) During Software use. The Software will report usage statistics including session duration, number of advertisement banners viewed and number of advertisement banners clicked on. The Software will not monitor the content of your use of the Software, i.e., sites selected, files transferred or content of files.

(iii) System Information. The Software will collect certain system information including Internet Protocol address, operating system type/version, domain name and telephone area code."

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Make sure you read the EULA's! Most people I know, including myself, usually click "I Agree" and do not read the EULA. It seems to be stated fairly clear to me that this application will send information to the Internet, however it does not state specifically what it will be sending. From Section 3 (i) – the information entered here includes Marital Status, Household Income, Gender, Job Function, Education, Year of Birth, State/Province, Country, Postal or Zip Code, and Interests. In section 3(iii) it states it will collect certain system information including domain name and telephone area code and IP address, operating system type/version. Continuing on, I completed the installation of Cute FTP, and ran "Ad-Aware" 5.83 from Lavasoft Software, with signature file version 029-15.06.2002 and it found 8 components related to the installation of Cute FTP.



As you can see from the report generated by Ad-aware there were numerous files, folders and registry entries that enable the Spyware at system startup. The Time Sink program as far as I can tell does just what the EULA says it does, it uses your system resources, and internet pipe to send and receive information to Time Sink servers on the Internet. Not only is this bad enough, but you must also think about once they are in possession of your information, how secure is it on their servers? That's a whole other issue though. To my surprise, when I uninstalled Cute FTP, these Spyware components were removed from the system. The only thing left on the system was an empty directory structure for C:\Program Files\GlobalSCAPE\CuteFTP.

If there is a personal firewall in place, using egress filtering at the application level may help in stopping the transmissions of personal information to the spyware servers awaiting the session. Egress filtering with an application level firewall, such as Zone Labs' "Zone Alarm" has the ability to detect an application trying to access the Internet, and can ask the user if they want to give this application or program the ability to go to the Internet. If you did not initiate the application launch, and are not sure what it is or

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

where it is trying to go, you can deny access and save the rule. If it was a spyware program, that should effectively block that specific program from sending information back to the Internet. The only problem is that your typical home users are not going to know the name of the operating system components that NEED to access the Internet once a dial-up connection has been established, or is being established. That being the case, one needs to be careful not to keep themselves from connecting to the Internet by denying a core operating system component access to the Internet. The firewall software in conjunction with a hosts file that contains entries of known spyware servers with all addresses being localhost (127.0.0.1), or simply the wrong IP addresses entered, works well. Here is an excerpt of a hosts file, that could be used:

```
127.0.0.1      Servername.doubleclick.com
127.0.0.1      Servername.flycast.com
192.168.0.0    Servername.valueclick.com
```

Several web sites such as http://www.accs-net.com/hosts/ maintain lists of known spyware servers and have created hosts files from the databases that you can download and install on your system. With a mis-configured hosts file, name resolution will fail and your computer will not be able to find the spyware servers to send the information to. In addition, anti-spyware software provides another layer to the defense of the system. Keeping the Anti-Spyware software up to date and scanning your system on a regular basis as well as keeping any real time monitoring up and running is a must. The same goes for the Anti-Virus software, which can detect viruses, Trojans, and worms on the system. Anti-virus software that is configured correctly to clean the malware, maintain real-time monitoring of the system, and continue virus signature updates and scanning engine updates adds yet another layer of defense to the system.

Your home machine may not contain multi-million dollar secrets on it, but a malicious user can get personal information about you, or use your system in part of a Distributed Denial of Service attack causing mutli-million dollar damage to E-Commerce sites. It's a simple task to take a couple minutes out of your Internet surfing to download programs that can help protect your machine, thereby protecting the web servers you like to visit. With the available bandwidth today for the home user, these small applications take no time at all to acquire. Protecting your personal information such as credit card ID's, home address, phone numbers, user ID's, bank account numbers, etc. is the "real" threat to the home user. You have to find out what resources, or assets, you want to protect. Do you want to protect your user ID's for Hotmail; do you have personal finance information on your system that, if it fell into the wrong hands, could cause havoc, or Aunt Sara's apple pie recipe? In order to set up the proper defense on a system, you have to know what has to be protected, then you can deploy a plan to protect it. It all boils down to privacy. In any case, a layered approach should be taken. Multiple levels of defensive software or hardware should be present and should fail to a known state – closed. You simply cannot rely on a single piece of software or hardware to protect you assets against attacks. And you have to ask yourself, if my "assets" were compromised in any way, what would it cost me to repair the damage? Take that into

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

consideration when considering a solution to protect those asset or group of assets. Is the cost of the investment in time and money worth it to you and does it make sense?

Business machines should be a bit easier to protect, after all, we all know that every business should have a well written policy in place to deal with all aspects of network security approved by upper management, and a qualified IT staff on hand at all hours of the day, every day to serve the end users and keep them and the network servers up and running. The real risk to business machines depends on the resources that need to be protected, and how the network is configured to secure those resources. One common practice among end users is to use one password for everything. This is a bad practice that usually goes un-enforced, and can be difficult to enforce. A user that uses the same password for network logon as he/she does for their hotmail account is a security risk to the network as a whole. You may have an Intranet Site within your environment that requires a logon to access a page and offers to remember the passwords for you. Again, most users are going to use that option so they don't have to re-key their password every time they want to look at the site. The cookies on the local machine that contain that information could then be parsed by Spyware and sent back to whomever wrote the program and now they have your user ID's and passwords. They have become one step closer to gaining access to a network or node.

All machines should have current Anti-Virus and Anti-Spyware software at a minimum. Personal firewalls are a good security measure also, however in some environments this is not realistic due to applications that simply will not function through a personal firewall. Host protection, in conjunction with your perimeter defenses including firewalls, URL filtering and monitoring devices, and Intrusion Detection Software would be a start to network security. Using operating system software that provides a central point to distribute and enforce security policies such as Windows 2000 or Linux is a good choice. This helps network professionals manage and track machine usage, and keep everything standardized for easier management and troubleshooting; thereby lowering a company's total cost of ownership. Another great defensive mechanism is end user education. If the end users have the necessary knowledge, or at least an awareness of new viruses, virus hoaxes, how to update Anti-Virus and Anti-Spyware software, how to keep software current, and general good practices concerning computer / network security, it will make the network administrators job easier and the network will be more secure. And of course all employees in an organization should be issued a policy outlining the proper use of company equipment and what corrective action will take place if these guidelines are not followed, and be required to read and sign the documentation upon hiring. This will help the employees, and IT staff be more productive.

An important step in securing your networks against any electronic attack be it hackers, or some form of malware is a well written policy that addresses the aspects of your network environment and business model and provides a clear picture to everyone as to your prevention, maintenance, and recovery plan in the event that an attack should get through your defenses and cause damage to, or destroy resources. How does Anti-Spyware software fit into the policies and procedures that governs your network and is

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ever evolving to match your business plan and technological changes? It would be included in the section that covers protecting the company's assets by using current technology and training to provide security to those assets. Anti-spyware software is no less important to network security than a firewall and is necessary to provide another layer of defense for your assets. Network security should include all aspects of security using perimeter defense mechanisms such as firewalls, Anti-Virus Gateways, Proxy Servers, Intrusion Detection Systems, and URL filtering and monitoring; host security such as personal firewalls, anti-Virus software, anti-Spyware software; and physical security, which includes building security to ensure that unauthorized personnel do not use or tamper with Company equipment when no one is around; and monitoring and filtering traffic flow though the network.

The layered approach to defending network systems, Defense in Depth, is the best approach to protecting the assets of a company or individual, but remember that this is not 100% secure. No network is completely secured against electronic, or physical attacks regardless of what solutions are used to protect it. New spyware programs crop up everyday, and the attackers are ever evolving in the ways that they try to attack system vulnerabilities, which is why our network defenses and corporate policies have to be ever evolving to be effective.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References:

1. Gibson, Steve, "Opt Out", March 20, 2002, http://grc.com/optout.htm

2. Gowan, Michael, "How It Works: Cookies," February 22, 2000, http://www.pcworld.com/hereshow/article/0,aid,15352,00.asp

3. "Analyze Your Connection", http://www.privacy.net/analyze/.

4. Gibson, Steve, "Patch Work", March 15, 2001, http://grc.com/pw/patchwork.htm.

5. Team Lavasoft, September 23, 2002, http://www.lavasoftusa.com

6. http://www.privacy.net

7. Hanzlik, Stuart, "What is the Hosts File", June 12, 2002, http://www.accs-net.com/hosts/what_is_hosts.html

8. Krebs, Brian, "Sen. Edwards Intro's "Spyware Control Act"", October 11, 2000 http://www.computeruser.com/news/00/10/11/news4.html

9."Adware/Spyware@," http://www.cexx.org

10. GSEC course material

11. http://www.sans.org/giactc/GSEC.htm
"Spyware and Network Security", Lester Cheveallier, 29 Aug. 2001
"Spyware-Recent Evolving Issues", Dan Replogle, 5 Dec, 2000
"Spyware - Identification and Defense", Lewis Edge, 14 Dec., 2001

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**