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 - Identification and Defense

You are being watched while surfing around the Internet. You may not realize it at the time but information about the websites you visit, products you purchase and even the advertising hyperlinks you follow are being collected and transmitted back to a server. This information is sold to whomever wants it. This is a general type of information that is not linked directly to you. Now, suppose you found a program you want to download, which you do. The installation completes and you reboot the system. You use the program...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Forensics
for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Spyware – Identification and Defense
Lewis Edge
GSEC Version 1.2f
December 14, 2000

Introduction

You are being watched while surfing around the Internet. You may not realize it at the time but information about the websites you visit, products you purchase and even the advertising hyperlinks you follow are being collected and transmitted back to a server. This information is sold to whomever wants it. This is a general type of information that is not linked directly to you.

Now, suppose you found a program you want to download, which you do. The installation completes and you reboot the system. You use the program until you find a software package that is more functional or you become bored with it. In any case you uninstall the program, or so you think. Without your knowledge or consent, this program has been transmitting personal data, i.e. bank account or credit card information, even personal medical history back to the developer. The software may have even left an open port, a door; to your computer allowing the perpetrator to enter your system to pick and choose the information he wants. Imagine the implications of this type of information theft. This is a prime example of a spyware infection.

What is Spyware?

Steve Gibson of Gibson Research Corporation has given the following definition of Spyware:

> **Spyware is ANY SOFTWARE**, which employs a user's Internet connection in the background (the so-called "backchannel" connection) without their knowledge or explicit permission.
>
> Silent background use of an Internet "backchannel" connection **MUST BE PRECEDED** by a complete and truthful disclosure or proposed backchannel 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.**[1]

Spyware or Adware could be delivered in the form of freeware or shareware. Software developers usually do not make enough profit from just selling their software. A way to increase the amount of money from the software would be to enter into an agreement with an agency, which gathers demographic information. This is ok but usually spyware will be involved. The information gathered could be the websites visited, banner ads clicked on, products purchased, etc.[2]

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

Spyware evolved and became even more sinister. What if the program were as robust as a commercially sold product and to use it you registered it using the general information such as name, address and telephone number? This would be great, wouldn't it? But what if you had other personal information stored on your hard drive and it was routinely transmitted across the Internet to advertisers for more advertising? This would also be done without your knowledge or consent. The program does not look so appealing now, does it?[3]

Spyware can also be delivered in a "Cookie". A cookie consists of user specific information that is stored on the users hard disk and retrieved by a web server. Basically, a web server knows you have been there before and remembers you and your preferences when revisiting the site. Unfortunately, web developers have taken this to new depths. While remembering preferences, the cookie can also gather your IP address, email address, operating system, etc.[4] Simply turning off the ability to accept cookies from websites will not help. There are many websites that will not allow you to view them unless your browser is set to accept cookies. The site can be implemented behind the scenes as a set of HTML forms, with the user's identifier passed around as a hidden data field.[5]

How Do You Identify Spyware?

Ever downloaded a 'Free' program only to find out it was Spyware? Software developers will hide the Spyware functions and not tell you. At this time there are 762 known Spyware programs. Spy Chaser lists them and allows you enter the program name to see if it is on this list. Many of those programs don't uninstall the Spyware even after uninstalling the main program leaving files on your system and entries in the registry you might never get rid of.[6] Refer to the figure 2.

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

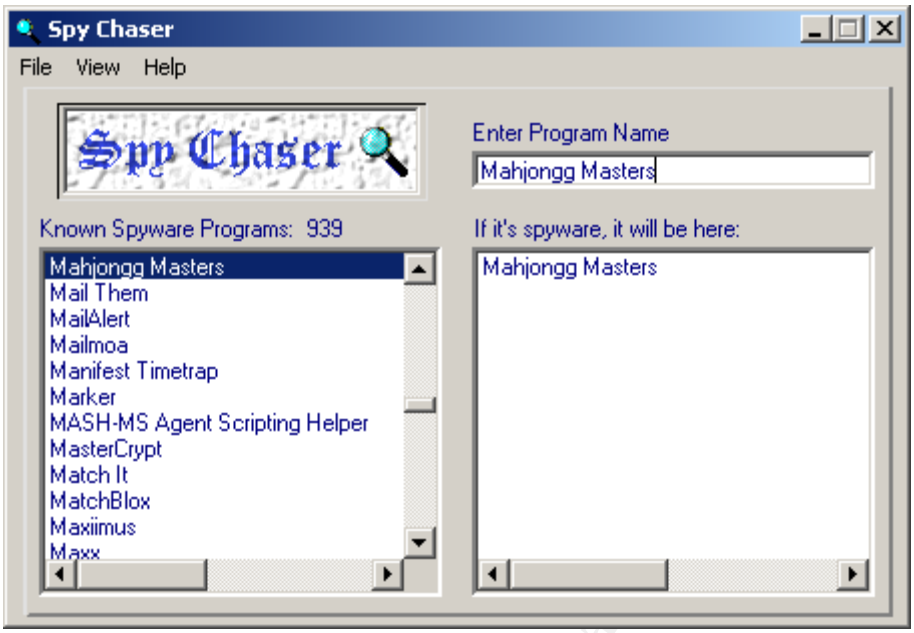

Figure 1 Spy Chaser[6]

© SANS Institute 2002, Author retains full rights.

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

Another type of spyware checking software is Spychecker. Spychecker runs in the system tray of your Microsoft Windows 95/98/Me/NT/2000 computer. Detect "Spyware" before you download! Spychecker can detect almost one thousand so called "Spyware" products by name. If you are not sure if the freeware program you are interested in is in fact, advertising supported Spyware, simply enter the name in the Spychecker box and hit "Check". Spychecker will query the constantly updated www.Spychecker.com database and display the results in your browser, complete with a link to the privacy policy of the ad-company and more.[7] Please refer to figures 2 and 3

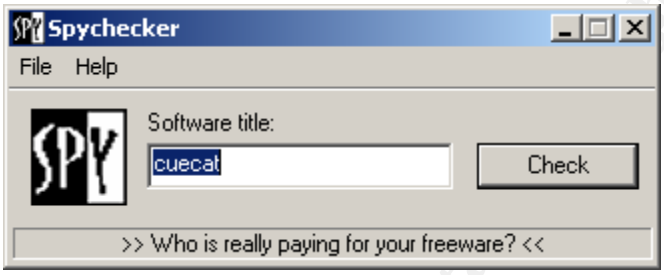

Figure 2 Spychecker[7]

You Searched For: cuecat
1 Matches Found (displaying 1 to 1)

Software	Ad Company	Privacy Policy	Last Verified	Remarks
CueCat	DigitalDemographics	statement	10/09/2000	source

Figure 3 Spychecker Search Results[7]

How Do You Defend Against Spyware?

Every day millions of computers connect to the Internet and the number increases each day. More and more users are opting for cable or DSL (Digital Subscriber Line) “always on” Internet connections. Because these connections are “always on” our computers are open to attack from a variety of sources, i.e. hackers, Trojan horses, worms, viruses and spyware. There are tools commercially available as well as available on the Internet. Some of these tools are even free for use.

Sygate Personal Firewall and Sygate Personal Firewall Pro

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

Sygate Personal Firewall is a host-based system, which delivers an enforceable rule-based security policy. Policies regarding applications trusted IP addresses, ports, protocols and scheduling can be customized to support and secure any computing configurations and requirements. SPF is equipped with bi-directional intrusion defense which prevents an external attack from the Internet an also prevents outbound communication protecting personal information from being stolen. SPF is free for personal use and SPF Pro is $39.95. Both can be acquired from the web at http://www.sygate.com.[8]

© SANS Institute 2002, Author retains full rights.

Norton Personal Firewall

Another product available for personal protection is Norton Personal Firewall from Symantec. Norton Personal Firewall can be purchased for $50 online. Norton Personal Firewall works with any type of Internet connection, i.e. dial-up, ISDN, Cable/DSL. Norton Personal Firewall is available for the following Microsoft Windows Products XP Home/XP Pro/ 2000 Pro/NT WS/Me/98.[9] You can get more information at http://www.symantec.com.

- **Norton Personal Firewall Features**

  - Controls Inbound and Outbound connections
  - Automatic configuration sets up rules for the most common Internet Applications
  - Ability to set individual firewall rules giving user full control
  - Prevents personal information from being sent to unsecured Web sites without your knowledge
  - Intrusion Protection gives an alert when a hacker tries to scan your PC for vulnerabilities
  - Ability to automatically block the system that's trying to probe your PC
  - Automatically determines which applications can safely access the Internet[9]

ZoneAlarm & ZoneAlarm Pro

ZoneAlarm is available free for personal use and $20 for business use. ZoneAlarm PRO is available for only $39 and includes a host of features designed to keep your network secure and you in control. ZoneAlarm offers immediate and complete port blocking, putting your computer in stealth mode, and effectively hiding your computer from attackers. It is easy to use because there is no need to learn ports, protocols, or programming. It immediately alerts you of activity and gives you simple yes or no control over which applications have access to the Internet. ZoneAlarm PRO includes advanced mail, safe-email attachment protection that recognizes and quarantines suspect attachments, and is customizable, also password protection, advanced logging, and more.[10]

With ZoneAlarm and ZoneAlarm Pro as with other personal firewalls, each of these programs are designed, not necessarily to keep spyware out of your system but, to keep your personal information from passing through to the Internet. You have the option of what applications and information pass through to the Internet.[10]

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

Figure 4 shows the protections afforded by ZoneAlarm and ZoneAlarm Pro. As you can see ZoneAlarm Pro and Internet Cleanup offer more features and more configuration options than ZoneAlarm standard. ZoneAlarm and ZoneAlarm Pro can be purchased from the web at http://www.zonelabs.com.

© SANS Institute 2002, Author retains full rights.

ZoneAlarm Features Matrix

Feature Availability	ZoneAlarm	ZoneAlarm Pro and Internet Cleanup
Advanced MailSafe E-mail attachment protection: shields you from malicious code.	1 file type	**37 file types**
Customizable Security Levels Tailor your PC security to the task at hand.	--	**Yes**
Mobile PC Protection Adapt your security to a new network.	Manual configuration	**Automatic**
Restricted Zone Lock out advertising sites and other Net nuisances.	--	**Yes**
"WHOIS" Hacker Tracker Find and track the source of an attack.	--	**Yes**
Password Protected Settings Set your personal security preferences, and know they're tamper-proof.	--	**Yes**
Privacy Protection Erase your Internet data trail - remove history, cache and forms.	--	**Yes**
Tracking Removal Eliminate Spyware, Active X and plugins.	--	**Yes**
Firewall Award-winning security for Internet-connected PCs.	**Yes**	**Yes**

Figure 4 ZoneAlarm Features Matrix[11]

NETGEAR RT314

The NETGEAR RT314 is a 4-port switch and router combination for cable/DSL Internet connections. The RT314 offers easily configurable firewall protection with stateful packet inspection to prevent denial of service and malicious packet attacks. It is designed with network address translation to prevent hackers from entering your network. It provides Internet filtering capability (based on time of day, web address or web address keywords), high-speed Internet sharing, VPN pass-through capabilities, logging and reporting capabilities and easy setup.[12] You can get more information at http://www.netgear.com.

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

Stateful packet inspection examines the contents of the packet to determine what the state of the communication is - i.e. it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until connection to the specific port is requested. This allows an added layer of protection from the threat of port scanning.[13]

How Do You Remove Spyware?

If you suspect you have installed spyware on your personal computer there is a free software download available that will scan your system including memory, registry and hard drives. The software runs in a scan wizard type of interface that will guide you through the scanning and removal process of spyware. Lavasoft has created a program called **Ad-aware**. Some of the features of **Ad-aware** are listed below.[14] You can get more information at http://www.lavasoftusa.com.

Ad-aware [14]

- Backup and restore functionality
- Multi Language Support
- Shell Integration
- Ability to Ignore selected components
- Scanning of removable drives

© SANS Institute 2002, Author retains full rights.

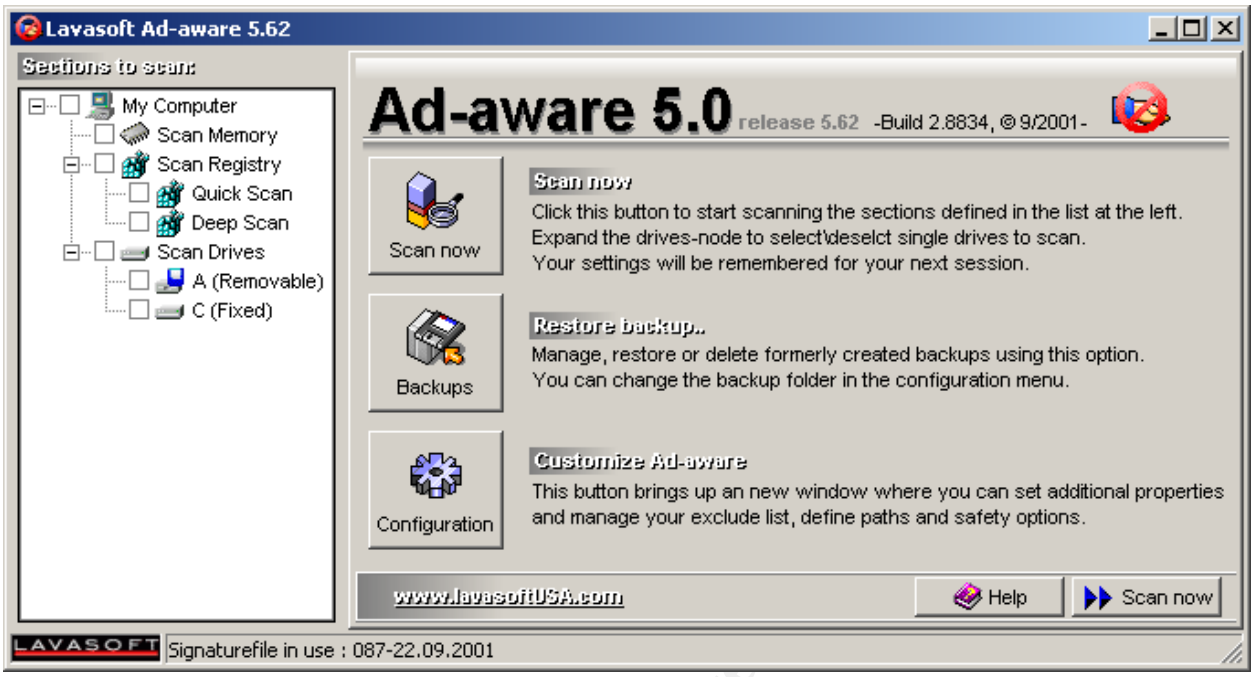

Figure 5 Ad-aware User Interface[14]

© SANS Institute 2002, Author retains full rights.

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

Ad-aware allows you to select not only the drives you wish to scan but also the type of scan you want to run. You can choose to run a registry scan as well as a scan of the hard drives including removable storage.[14] Please refer to figure 5.

When your selections have been made click on 'Scan now' and your scan will proceed. If any components are found, you will have the option to remove them from your system.[14] Refer to figure 6.

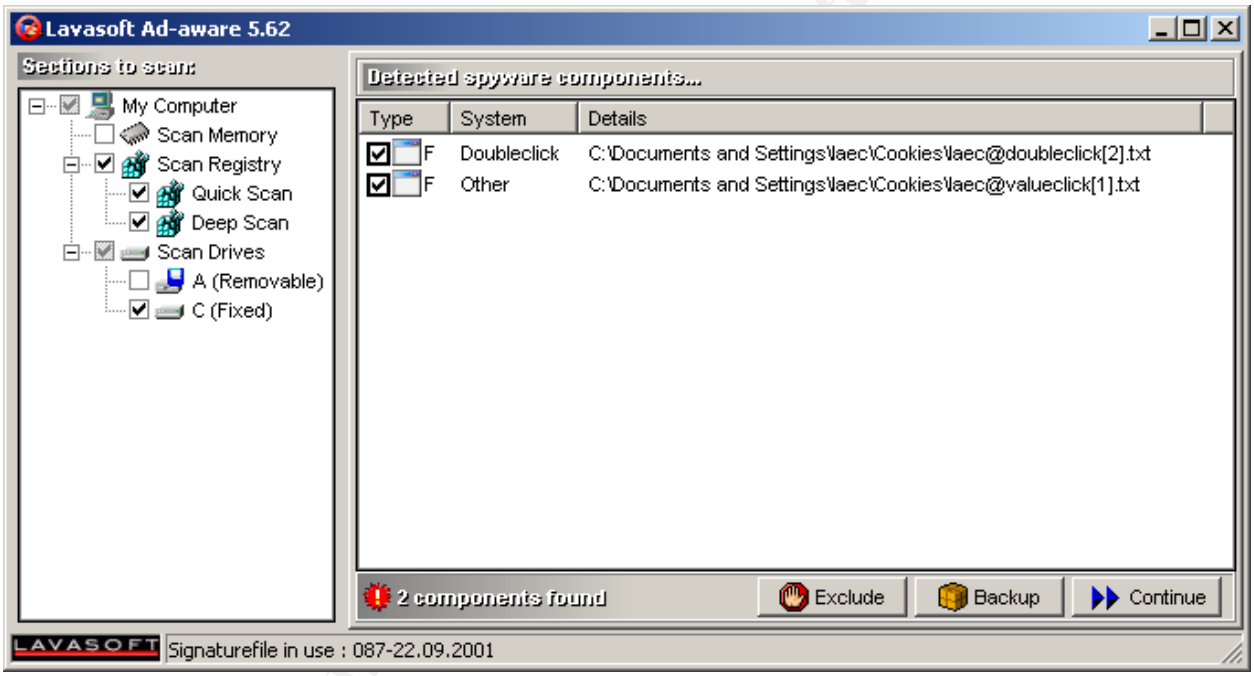

Figure 6 Detected Components[14]

Conclusion

We have discussed what spyware is, the ways we can identify spyware, defending against spyware, and a way to remove spyware. Ultimately, it all comes down to the users. It is the responsibility of the users to practice safe surfing. Don't give out personal information when that information is not needed. You must remember you are not out there alone. If an individual can get personal information from you using an attack of

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

some kind or some form of spyware, they will. Your information privacy is no longer guaranteed, however, it is your choice as to the level of privacy you wish to have while doing your surfing. It is the individual user's job to implement solutions to enjoy that level of privacy and protect their personal information.

© SANS Institute 2002, Author retains full rights.

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

Is there anything that can be or is being done to protect the privacy of web surfers? At this time Senator John Edwards, D-NC has introduced legislation that would force software manufacturers to notify consumers when their products include "spyware". It is called the "Spyware Control and Privacy Protection Act".[15]
It states "manufacturers that build spyware into their products must give consumers clear and conspicuous notice – at the time of installation - that the software contains spyware. Such a notice would describe what information would be collected and to whom it would be sent. The spyware would then be forced to lie dormant unless the consumer chooses to enable it."[15]

We must also note that in addition to notice an choice, consumers would have the benefit of the remaining two "Fair Information Practices" endorsed by the Federal Trade Commission: Access and Security. Software users would have the ability to find out what information has been collected about them and to correct any errors.[15]

The Edwards' Bill comes at a time when freeware producers are getting their share of bad press because of embedding spyware into their programs. The producers argue that the programs are geared only at improving advertising returns. Producers such as RealDownload, Intuit's Quicken and NetZip's Download Demon now have advertisements in their programs window.[15]

However, the bill also includes what Senator Edwards has categorized as "common sense exemptions". He feels a user's consent should not have to be obtained if a spyware program provides information for technical support or verifies that the program's user is the same as the licensed user. If legislation is going to be enacted which requires full disclosure, of information to be gathered, to the user then full disclosure should be made. Senator Edwards' exemptions allow for so-called approved spyware to exist without the same requirements for disclosure.[16]

Gilles Lalonde put it best "… what I do in the privacy of MY own HOME is MY business and My business alone, like what you personally do in the privacy of YOUR own HOME, is YOUR business and Your business alone. Software authors that use spyware do not care about anyone's privacy. The breach our personal privacy and spoil our Internet experience".[17]

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

References

1. Gibson, Steve. "Optout, Tell Unwelcome Spyware to Pack its Bags!" 25 November 2001. URL: http://grc.com/optout.htm

2. ATExcellence Perl Resources for Windows NT/2000 "Spyware and Adware, What is it, how do you get infected." 17 November 2001. URL: http://www.atexcellence.com/internet-security.htm

3. "What is Spyware?" ZDNet Reviews, 28 June 2001. URL: http://www.zdnet.com/products/stories/reviews/0,4161,2612053,00.html

4. Hutcheson, Lorna J. "Are You Being Watched?" 20 July 2001. URL: http://www.sans.org/infosecFAQ/privacy/watched

5. Cartwright, Dave. "Customize Your Content with User Profiling." 2 December 2001. URL: http://www.webdevelopersjournal.com/articles/user_profiling.html

6. "Spy Chaser."10 December 2001. URL: http://camtech2000.net/Pages/SpyChaser.html

7. "Spychecker." 17 November 2001. URL: http://spychecker.com/spychecker.html

8. "Sygate Personal Firewall." 3 December 2001. URL: http://www.sygate.com/products/sheild_ov.htm

9. "Some key features of Norton Personal Firewall 2002." 15 November 2001. URL: http://www.symantec.com/sabu/nis/npf/features.html

10. Krein, Derek. "Layers of Defense for the Small Office and Home Network" 24 July 2001. URL: http://www.sans.org/infosecFAQ/homeoffice/layers.htm

11. "What Are Your Security Needs?" 15 November 2001. URL: http://www.zonelabs.com/zap26_za_grid.html

12. "NETGEAR RT314 Cable/DSL Switch/Router." 4 December 2001. URL:http://www.netgear.com/product_view.asp?xrp=4&yrp=12&zrp=55

13. Gomes, William Victor. "Great walls of fire" 11 April 2001 URL: http://www.ciol.com/content/flavour/netsec/101041101.asp

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

14. "Ad-aware." 19 November 2001
URL: http://www.lavasoftusa.com/aaw.html

References cont.

15. Krebs, Brian. "Senator John Edwards Introduces 'Spyware Control Act'"
9 October 2000. URL: http://grc.com/spywarelegislation.htm

16. Underhill, Sandra. "Spyware Bill Introduced in Congress",
11 November 2000.
URL: http://www.infinisource.com/features/spyware-pf.html

17. "Do you realize your computer could be sending information about you without your permission!!!" 11 November 2001.
URL: http://www.spyware.co.uk

© SANS Institute 2002, Author retains full rights.

Last Updated: September 3rd, 2015

Upcoming SANS Training

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

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 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 South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 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
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced