Global Information Assurance Certification Paper

SPYWARE – An Evolution in Process

Roger Sellers
May 21, 2004

GIAC Security Essentials Certification (GSEC)
Practical Assignment version 1.4b (amended 8/29/2002)
Rockford LMP
GSEC Option 1

Abstract

Malware, as described by Skoudis and Zeltser [(1)], "is a set of instructions that run on your computer and make your system do something the attacker wants it to do". These instructions can be benign or potentially destructive to the pc. Malware is classified in several categories which sometimes blur into several categories of malicious code such as virus and Trojan files, which may be detected by some antivirus software programs. Virus and Trojan files are more commonly carried or received by a user via electronic mail (email) or file sharing. Malware, in the context of this article, will be referred to as spyware, adware, and Trojans which are more commonly received via internet access using programs such as Microsoft's Internet Explorer™. Most malware is delivered to the user's computer without the user's knowledge or approval. The program code or scripts can either extract information about the user, the user's computer, or it can install other scripts or programs to be used for unknown purposes.

Most computer users do not even know what spyware is or the intended purpose of spyware. This paper hopes to give information on the types of spyware, ways to detect its presence, and how to remove or minimize spyware and its effects on pc's. In an enterprise network environment, spyware can be more costly to prevent or remove than some of the worst virus files that have been delivered to date. Spyware is different than a virus file or spam, and as such, the methods and policies used to prevent viruses are not effective against spyware, even though the destructive effects to a computer may be similar.

---

[1] Skoudis, Ed. Zeltser, Lenny. (2004). Malware Fighting Malicious Code. Prentiss Hall PTR. Upper Saddle River, NJ. P.13.

What is Malware?

Malware detections vary. The type of environment the computer is in may have different effects on malware in the way it attacks a computer or group of computers. Malware, as a classification, can include any type of destructive code that alters a computer or makes one perform some action contrary to the user's knowledge or permission. In most cases, such as with viruses and worms, computer users are their own worst enemy because they perform some action that initiates or allows the virus or worm to perform its actions against the computer. By a broad definition, malware includes:

- Virus files
- Worms
- Trojans
- Backdoors
- Key loggers
- Mobile code
- User and Kernel Root Kits
- Spyware and Adware

Each of these threats has varying delivery methods by which they can reach the user's computer. These delivery methods are commonly via electronic mail (email), Internet Messaging Services (IM), computer or peer-to-peer files sharing (P2P), Internet Relay Chat (IRC), common local file access (floppy disk), or internet access. The destruction from of any of these malicious code types can affect any single computer on an individual basis or multiple computers on a network if at least one computer is connected to the internet. Since most computers are either on the internet full-time using cable modem or DSL access, or via phone line and dial-up modem. If a computer resides on any type of network, malware can use the network to spread itself to other computers within the system (even to individual pc's that do not have any form of internet access). Network-aware malware are the most destructive forms and are the malware that network administrators and security persons are most keen to prevent. In a matter of seconds, malware could potentially spread itself to every computer connected within a network.

Communications between computers requires a hardware medium such as modem, hub, or switch, wire, and connectors. Once the hardware link is made, an operating system and application programs are used to establish connection paths or channels between computers. These connection channels or ports can be used to transfer information

between computers. Some of the 65,500+ ports available for use by a computer have specific and/or common purposes assigned to them (www.iana.org) [2] or are allocated for a specific application such as email, ftp, or HTTP (web) [3]. Some ports are used for various types of network communications such as directory proxy, port mapping, or administration [3].

Spyware, virus files, trojans, and other malware can use these common port numbers such as port 80 and other ports to transmit information between computers and networks. Sometimes, malware will use a port that is not blocked or filtered by firewalls.[4] These ports offer themselves little resistance to malware because so much traffic crosses these common ports that firewalls are occupied attempting to scan or analyze the packets on them such that a firewall would prohibitively slow down the network or information flow.

What are Spyware and Adware?

For brevity and focus, this paper will attempt to limit discussion to only what is known as spyware and adware. These forms of malware are commonly received through internet browsing. Most corporations and individual users are already aware of application software and methods to resist virus attacks initiated directly via email. Many users also employ some antivirus software solution, firewall, and/or email scanner to search out and remove viruses, worms, and trojan files. These solutions cover the most common and obvious paths malicious software can be delivered to a computer. Malware from internet browsing or "surfing" creates an entirely different set of risks.

Spyware could be considered a subsection of malware, but should not be considered any less of a threat than a virus or trojan because of its potentially destructive capabilities. Spyware is considered to be primarily related to internet web access as compared to spam or virus infections which typically use email or email attached files as the means for infection. Spyware can be more harmful to a computer because it does not have to make its presence known to the user of the computer it affects. In most cases, the user does not even know he is enabling spyware to infect his computer. Spyware commonly installs itself without user intervention via Visual Basic ™ or ActiveX™ script coding from a web page visited by the user.

---

[2] Unknown, (2003). "Port Numbers". Application Media-Types. Mar.4, 2004. URL: http://www.iana.org/assignments/port-numbers

[3] SUN Microsystems. (2003). "Appendix C Component Port Numbers". Sun Java Enterprise System 2003Q4 Installation Guide. 2003. URL: http://docs.sun.com/source/816-6874/a-port-numbers.html.

[4] Internet Security Systems, Inc. "Port Knowledgebase Exploits". 2004. URL: http://www.iss.net/security_center/advice/Exploits/Ports.

How does it get on computers?

With virus, worm, and many trojan files, the method of delivery is usually via email, Instant Messaging (IM), Peer to Peer (P2P), or Internet Relay Chat (IRC). The delivered file may require some user intervention to launch itself on the computer; once installed, it is detectable by antivirus software. After being launched, the spyware's method of infestation can vary according to the instructions in that particular program's coding. In many situations, these virus programs are written for notoriety or retribution, this is where malware, spyware, and adware begin to differ.

Internet spyware and adware are usually created as Visual Basic™ or ActiveX™ or another scripting language that is launched by a command from within a web page's HTML coding. These scripts are used to gather information about the user, web sites they visit on the internet, and/or collect information on their interests and categorize them. As a result, this type of malware has been called "spyware". On the simplest level, spyware uses text files that are designed in a specific way to collect minimal information about the user when they visit a particular internet site. These text files are called "cookie files" and are stored on the computer in a common directory that can be viewed with any text editor. Cookie files are valid and acceptable files to place on a computer, and were planned by Microsoft™ specifically for tracking purposes. An example of a cookie file which may be found on a computer would be similar to the following:

usernamer@advertising[2].txt

On a Windows 95/98 computer, cookies are stored in the c:\windows\cookies folder.

On Windows 2000 or XP, the folder path is commonly found at the following location:

C:\Documents and Settings\Username\Cookies

From cookie files, the intrusion from and destruction by spyware seems to worsen. The upsetting issue with spyware and adware is the program is designed to collect data about the user's internet habits. That data is then used by "legitimate" companies as marketing data, many times without the user's knowledge about the information being collected about them. Corporations are working hard to extract as much information about visitors' to their web sites as possible. They use this information to learn web site visitor's habits so as to encourage new users to visit their web pages and to keep visitors coming back and staying longer, in hopes of selling products or services to the visitors.

According to SearchSecurity.com's article [(5)], Internet Explorer can be exploited by trojan files that are installed from a web site by merely clicking on an HTML link within the web

---

[5] . Hurley, Edward. "Ibiza Trojan is a trip". SearchSecurity.com. News Feb. 13, 2004. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci950421,00.html.

page and going to the page. A recent exploit, called Ibiza-A, which at the time of this writing was not yet corrected by Microsoft™, would infect any pc, even pcs containing the latest service packs, hot fixes, and security updates downloaded and installed from Microsoft™. Thus, even if one did everything possible to keep his system up to date, one could still be affected by malware or spyware. The user could simply click on a window or URL link designed to entice them to look at particular web site. Once the site was viewed, it was too late; the malicious code had already been deployed on the user's computer and they were none the wiser as to its existence.

According to Edward Hurley's article (5), "a Trojan, it cannot spread by itself. The attacker would need to entice victims to a Web site that would infect the code. For example, a message containing the infectious URL can be spammed out with something enticing, such as "Today's your lucky day! You've won the lottery" or "Free porno for the next 24 hours". If the user clicked on the link for the web page or opened a window, the spyware code within the html coding of the web site would infect the user's computer.

The number of web pages containing application files using Visual Basic™, JAVA™, and/or ActiveX ™ script is increasing at a phenomenal rate. What began as an interesting tool for encouraging web site developers to track the visitors to their site has grown into an uncontrolled marketing tool. Web presence is solely concerned with drawing visitors to a particular web site. No longer content to only know when someone is visiting a site, now web site owners want to make people visit a site whether the person intends to or not. Once a person visits the website, cookie and script files are deposited on the visitor's computer to learn more about the user's internet habits. These script files often automatically report back to the owners of the initiating web site with potentially private information about the user or their internet browsing habits (the types of sites visited, how long there, and other sites visited). Some of these scripts, referred to as "back door trojans", can allow one person to monitor or take over control of another person's computer as it accesses the internet. Sophos Antivirus in their publication "Computer Viruses Demystified" (6) states,

"A Trojan can monitor the PC until it makes a connection to the internet. Once the PC is online, the person who sent the Trojan can use software on their computer to open and close programs on the infected computer, modify files, and even send items to the printer."

---

6 . Oldfield, Paul. Computer Viruses Demystified. Sophos Plc. UK. 2001. 43.

Reading the fine print

This far in the reading, one may begin to question the legality of spyware. Fortunately or unfortunately, it is legal. According to a web article "Spyware is it Ethical" by Michał Pańczak & Zane Rickard [(7)], there is a lack of legal restrictions and loop-holes on spyware and adware that allows vendors to write End User License Agreements (EULA) for their software that can be very confusing to the end user if the end user is even aware of its existence at all. Because a EULA is used to give the website the resemblance of legal licensed software, some major computer manufacturing companies are refusing to help their customers clean their computer of this spyware for fear the computer manufacturer might be sued by the spyware or adware developer, even though the computer manufacturer knows the software is spyware and potentially invasive or destructive to the end user [(8)].

Most users do not understand what EULA's are or fail to read them entirely, if at all. Many adware programs contain EULA's to give them a resemblance to being legal, but if a user fails to read the fine print, the user could give the program owner free rights to download files to their systems or access nearly anything from the user's computer [(9)]. When the user realizes this, he may become upset, but in the end, he will have no one to hold responsible but himself. Many computer users do not read EULA's. They do not realize what they are agreeing to, giving permission for, or to whom they are even giving access. Users find out too late what they have agreed to in the EULA, it is usually only when they realize something strange or different is going on with their computer. In many instances, users will download a free program (freeware or shareware) believing they are receiving a good deal on a program. Web site developers offering some freeware applications are creating interesting or useful applications such as screen savers, weather reporting, or news reporting features to entice people to download and install their software. But, as in most cases, nothing is free and users generally have to give up something to get something. In this case, it may be their privacy or some use of their computer.

Internet dive-by attack

Spyware, unlike adware, usually does not bother with a EULA. It is imbedded as a script file on a web page or bundled with other applications when a user installs programs. The situation seen often is spyware is embedded within a web page. All a person has to do is have a web specific page open on their screen. He does not need to open any special programs, or select anything to install the spyware. These embedded spyware applications can insert themselves onto a computer in such a casual manner. The user

---

[7] Panczak, Michal. Rickard, Zane. "Ethics and Spyware". Spyware is it ethical. 2004. URL: http://panczak.pl/michal/ethics.html.

[8] Unknown (alias). "It wasn't me". Open Letter to Dell. Dec. 12, 2003.

URL: http://forums.techguy.org/t184904/s6973c0dcdf044b412756f1079674945f.html

will never realize it has happened. The user is a victim and does not even know the software was installed. The user may see a misleading dialog box or nothing at all to tell the user a "drive-by" [9] software installation occurred on their computer. This occurs because spyware exploits a "feature" within Internet Explorer™ where configuration settings allow ActiveX™ scripts to run without user intervention or prompts for approval to install the script. If the security settings are set in a manner so no prompts are sent to the screen to approve or disapprove running ActiveX™ scripts, no warning is given to the user when *ANY* ActiveX™ script is run, whether it is a useful or destructive script, it will all be allowed to run.

If the security settings are increased, a warning window will open on the screen prompting the user to allow or disallow the script on each script that attempts to run within a browser window. The problem with this is the user has no idea what the purpose of the script (malicious or valid) is unless it is allowed to run, and even then, he still may never know what the script does without looking at the HTML coding in the web page itself. If a user does not allow the script to run, the web page containing the script may fail to open or open to its full extent.

The term "drive by" as used in referring to spyware has become a reference to the increasing frequency in which simply accessing a web page that contains the embedded scripts and pop-up windows can infect a computer. These scripts generally require Active-x and/or Java to be enabled and can install various types of software onto a computer that will do whatever the creator of the software intends. The computing form of the term spyware relates that the computer becomes a victim of the spyware program by doing nothing more complicated than accessing a single website on the internet, or perhaps through a pop-up window or as a result of clicking on a link to an unknown web site. Pastor Len Strozier has the earliest reference to the term "drive-by virus" [10] that can be found, in an article dated July 31, 2002, on one of his web pages. In a Microsoft Newsgroups posting, a person named Kent England whose newsgroup entry related to security and ActiveX, dated July 1, 2003, states that "Active-x controls are a common way for drive-by spyware and browser hijackers to install themselves on your computer or take control of your browser" [9] .

The problems associated with spyware and adware will continue to worsen. There are a number of web sites such as SpyWareInfo.Com that are trying to educate consumers and to help users clean their pcs after they have become infected with malware and spyware. Applications such as SpyBot Search & Destroy©, Ad-Aware©, SpywareBlaster© and others help clean a pc after it has had spyware or adware installed on it. Software is being created to help prevent spyware from being installed in the first place. Antivirus programs

---

[9] England, Kent W. "Re: Active X and Security Issues".

URL: http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-07/0247.html.

[10] Strozier, Len. "Lifelines from Len". July 31, 2002. URL: http://www.fbctoday.com/pastor/lifelines07_31_2002.htm.

are not being written to block or clean spyware and adware, but since some spyware is characteristic of or carries Trojans as part of their payload, some spyware is being detected and cleaned by antivirus programs. This is an exception as far as antivirus venders are concerned. Most vendors do not consider spyware a virus, and because of the EULA's associated with Ad-ware, many computer manufacturers and software vendors do not want to try to remove adware or spyware for fear of infringing on another company's software development rights.

As a result, users are left having their computers continually re-infected by spyware until they notice it seems much slower than it used to be, and call on a computer technician to find what is wrong and fix the problem. It is usually not until a user realizes the computer is slower and asks a computer technician that the user even learn what spyware or malware is. Some users think that their computer is slowing down because it is too old and, as a result, will replace the computer not realizing it is slower because of the effects of installed spyware, adware, and other malware.

Cleaning after spyware is not cheap

Spyware and adware, like virus and Trojan files, are analyzed by some very qualified persons and companies in order to be able to detect and create processes to remove them. When someone suspects a computer is infected with spyware or adware, like a virus, they can report it to a computer technician or contact an antivirus vendor. Unfortunately, it is hard for an average user to know who to report spyware or adware to. If the user is using a spyware removal application, they can report it to the vendor of their program. No central clearing house for information for malware is available for spyware and adware as there does within the antivirus developer industry.

An April 15, 2004, article on TechWeb's website([11]) states that in a recent survey by ISP EarthLink and WebRoot Software, "over the period from Jan. 1, 2004 to March 31, EarthLink's and WebRoot's spyware and adware detection software sniffed through over a million systems and found more than 29 million instances of spyware." The article further stated "the two firms also detected more than 360,000 system monitors and trojans among the one million machines scanned." Fortunately for computer users, some of the best software for detecting and cleaning spyware, trojans, and other malware is currently free to home users and some even free to enterprise computer networks. Many corporations are still learning about spyware and adware. These companies either don't yet understand fully how costly it can be to clean spyware for their network or how quickly spyware is infesting their computers. In NetworkWorld's May 5, 2004 segment, *TheGoodTheBadTheUgly*,[12] a short article states that in a Harris Interactive survey only

[11] Unknown. "Average PC Plagued With 28 Pieces of Spyware". TechWeb Business Technology Network. April 15, 2994. URL: http://www.techweb.com/wire/story/TWB20040415S0006.

[12] "Spyware vs. spyware". NetworkWorld, May 10, 2004. P.8.

six percent (6%) of employees at work think they have ever visited a site on the internet that contains spyware. This contrasts ninety two percent (92%) of the IT managers in the same survey estimated their organization was infected by spyware. This implies possibly that not enough is being done to educate network users as to what spyware is and how to possibly prevent it. That prevention may not be cheap though. Mark Gibbs[13] writes in "*The cost of spyware*", a scenario of what spyware and adware clean-up may cost a company. His calculations base a users annual salary of $720,000 (adjust according to your business) and a working calendar of 260 days per year. If a technician spends two hours to clean a computer of spyware, it would cost a company $138.00 to clean that computer: ($72,000/260)*((2 people * 2 hours)/ (8 hours per day)). If spyware infested only five percent (5%) of a computer network of 1000 computers, that would be approximately 600 cases of infestation per year. At a cost of $138.00 per event, it would cost a company roughly $83,000 per year to clean spyware and other malware from computers. If the percent of infections within a business in a year was higher, the cost could substantially higher. It may not take long to justify the cost of spyware prevention software being added to an IT department's annual software budget.

Reduce risk – Reduce exposure

Some developers have graciously written programs to clean certain malware after it has infected a computer and even a few program developers have written programs to prevent malware from infecting a computer by preventing it from writing to the computer's system registry. This can prevent malware from installing itself or reinstalling itself after a user has attempted to kill it. A few of these developers ask for a donation of money, or hardware as payment. Others may ask for only an email note or post card sent to them acknowledging that users like the software. At least one commercial vendor, LavaSoft™, allows the use of a version of their Ad-Aware™ program free for home users, but sells a full version to business users. There is other software for sale to all users. Regardless of which software a user selects, he needs to develop a plan and methodology to regularly detect, clean, and prevent malware, spyware, or adware from infecting his computer.

Put together a plan

People need to develop a plan of action and find software to help them keep their computers clean of spyware and other malware. So far, this paper has discussed what malware is and the basic different software that comprises what is categorized as malware. These topics presented have attempted to focus on spyware and adware and some of the processes to find, identify, and eliminate spyware and adware is very similar to virus, trojan, and worm files. In fact, many times, trojan files are used as a delivery

[13] Gibbs Mark, "The cost of spyware". NetworkWorld, April 26, 2004. P.100.

mechanism for spyware and adware just as they are for virus and worm files. In similar fashion, many of the steps or processes to defend against virus and worm files are also used to defend against spyware and adware. The best approach is to use specific software to eliminate each type of threat. Just as there are multiple threats, the best defense will utilize multiple processes in combination to defeat or prevent spyware or adware from infecting a device. There is no single program or no single trick to use to prevent spyware or adware. Each process generally requires the user to initiate an action to keep any software used up to date. It may also require some decisions to be made by a user when some potential hazard is discovered. This means the user needs to be educated to understand the threats and how he must act to defend his computer. This also means there are multiple places where the defense can become weak and holes can be created where malware can enter the computer.

Many corporations and people believe by installing only an antivirus solution on their computers and keeping it up to date that they are adequately protected from viruses and such. They assume an antivirus application covers all the vulnerabilities. Unfortunately, they are seriously mistaken, as some are beginning to understand. In the future, because of the potential for script files and other malicious code to be embedded in HTML coded web pages, we will see an increase in threats to a computer or network by merely being a part of the internet. Web pages are designed to use file types of script coding like Java™, Visual Basic™, ASP™, PHP™, and others. These scripting applications have the potential to be used maliciously just as they are proving to be useful for many daily functions of internet activities. Because they are needed for the "good" they perform, we can not generically deny their use in the security settings of internet browser applications. In most cases, the settings in browsers[14] that allow these scripts only have three options: allow for all functions, be prompted every time a function is called for, or none, deny all occurrences of the function or script. There is not much choice in between. The most secure options deny the user full access to many web pages. The least secure offers virtually no protection from malicious code. The option to prompt the user to make a decision to deny or allow the code to be run can cause extreme irritation, with the high frequency with which the user could be prompted on any given pages or collection of pages.

---

[14] Unknown. "Microsoft Making Changes to MSIE". "Spyware Weekly Newsletter: October 14, 2003.
URL: http://www.spywareinfo.com/newsletter/archives/1003/14.php.

Summary

The best defense against malware may be to have a strong defensive attitude about spyware and adware. No longer are antivirus programs the only means sufficient to protect files on a computer. Computer users need to develop a full spectrum of applications and procedures to clean their computer of spyware and other malware. Installing spyware detection programs such as SpyBot™, Adware™, Spy Sweeper™, Pest Patrol™ or others as well as antivirus software should be installed on computers as a multiple defense against malware. Also, install applications which will prevent spyware and adware from writing to the computer's registry file in the first place. If software can be used to prevent spyware from infesting a computer in the first place, there will be fewer spyware to find and delete for a computer. This could include SpywareBlaster or SpyBot which will write protect segments of the registry and prevent other software from modifying the registry without approval. IT departments and computer users need to learn how to protect against browser hijack scripts. Users should how to prevent pop-up windows. This can be done by using pop-up blocking software or internet browsers that reject or automatically close pop-up windows such as Mozilla's FireFox or an Internet Explorer shell program like CrazyBrowser. Many spyware and adware programs are initiated when pop-up windows are opened. Stopping the windows from opening stops the application from being launched. All computer users need to keep computer operating system service packs, security patches, and hot fixes up to date. IT departments need to know about intrusion detection system and application layer security on their networks. Lastly, keep all computer software up to date with the latest version, updates, and security fixes. Develop a schedule to do these updates on a regular basis and learn to automate the process as much as possible and verify that it was done. Spyware and other malware are not going to disappear. Like computer viruses, malware and spyware are here to stay and will plague computers for quite some time. So long as web sites will be capable of using scripting of some sort (Active-X, Java, asp, vbs, macros, etc.) the threat of spyware and malware will continue to exist. Accepting these facts and learning to develop the best defensive posture against spyware, adware, and other malware possible is necessary for personal computer users or network IT departments.

References

1. Skoudis, Ed. Zeltser, Lenny. (2004). Malware Fighting Malicious Code. Prentiss Hall PTR. Upper Saddle River, NJ. P.13.

2. Unknown, (2003). "Port Numbers". Application Media-Types. Mar.4, 2004. URL: http://www.iana.org/assignments/port-numbers.

3. SUN Microsystems. (2003). "Appendix C Component Port Numbers". Sun Java Enterprise System 2003Q4 Installation Guide. 2003. URL: http://docs.sun.com/source/816-6874/a-port-numbers.html.

4. Internet Security Systems, Inc. "Port Knowledgebase Exploits". 2004.

URL: http://www.iss.net/security_center/advice/Exploits/Ports.

5. Hurley, Edward. "Ibiza trojan is a trip". SearchSecurity.com. News Feb. 13, 2004. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci950421,00.html.

6. Oldfield, Paul. Computer Viruses Demystified. Sophos Plc. UK. 2001. 43.

7. Panczak, Michal. Rickard, Zane. "Ethics and Spyware". Spyware is it ethical. 2004. URL: http://panczak.pl/michal/ethics.html.

Panczak, Michal. Rickard, Zane. "Conclusion". Spyware is it ethical. 2004. URL:http://panczak.pl/michal/conclusion.html.

8. Unknown (alias). "It wasn't me". Open Letter to Dell. Dec. 12, 2003. URL:http://forums.techguy.org/t184904/s6973c0dcdf044b412756f1079674945f.html.

9. England, Kent W. "Re: Active X and Security Issues". URL:http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-07/0247.html.

10. Strozier, Len. "Lifelines from Len". July 31, 2002. URL: http://www.fbctoday.com/pastor/lifelines07_31_2002.htm

11. Unknown. "Average PC Plagued With 28 Pieces of Spyware". TechWeb Business Technology Network. April 15, 2994. URL: http://www.techweb.com/wire/story/TWB20040415S0006.

12. Unknown, "Spyware vs. spyware". NetworkWorld, May 10, 2004. P.8.

13. Gibbs Mark, "The cost of spyware". NetworkWorld, April 26, 2004. P.100. URL:http://www.nwfusion.com/columnists/2004/0426backspin.html.

14. Unknown. "Microsoft Making Changes to MSIE". "Spyware Weekly Newsletter: October 14, 2003. URL: http://www.spywareinfo.com/newsletter/archives/1003/14.php.

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event