Global Information Assurance Certification Paper

SANS GSEC Practical

"Defending Against Spyware Invasion"

Brian J. Smith
GSEC Practical v1.4b
February 28, 2003

Abstract

Everyone who uses the Internet today is being watched. Exactly how closely someone is watching depends on the user. Spyware has become a very easy way to monitor and collect information about many users on the Internet. With the growing popularity of freeware programs, the spyware can simply be embedded with the freeware, and easily distributed and installed without the user's knowledge. Methods of detecting and eliminating spyware will be discussed, as well as ways of preventing it from being installed in the first place. Investigating the spyware that comes with Kazaa will help shed some light on different techniques software developers are using to distribute the spyware.

Introduction

Since the development and expansion of e-commerce throughout the world, companies have sought after a method by which they could track their consumers. Cookies were developed early on to accomplish this. A cookie is a text file saved on the user's local hard drive that stores preferences or other user information that a web site can use. When a user browses a company's web site, the web-server can check if a cookie already exists on the local computer. If not, the server can send a cookie along with the HTML web page. This cookie is updated every time the web site is visited giving the company an idea of how often the user has browsed their web site and in particular which parts of the web site the user visited. Unless the Internet browser is set to prompt before accepting cookies, all of this takes place without any user interaction.[1]

Many Internet users view simple cookies as a breach of privacy. Contrary to what some believe though, cookies were designed to allow web-servers to view only the cookies that they specifically created. This means that if one web site stores a username and password in a cookie, other web sites would not be able to access that information. On a home or private computer, these cookies are generally safe. On a computer shared by multiple users, privacy becomes more of an issue. Any user with local access to the computer can view cookies created by web sites that other users have visited as well as any personal information that might be stored on the cookies.

Advertising companies like Double Click, Avenue A, and Hitbox use cookies to try and determine the interests of specific customers so they can then display appropriate advertisements to them. They do this by putting up banner ads on different web sites and using cookies to track which ads have been displayed and whether any of the banner ads have been clicked on. Using this information, they can start developing a database for each user and personalizing the advertisements that pop-up at different web sites. Many companies pay to have their banner ads put on other web sites and keep track of who has clicked on the ads. Some Internet search engines use cookies to keep track of different items that have been searched for and then display advertisements that are related.

While this method of obtaining user information has proved effective, cookies do have many limitations. For advertising companies, valuable Internet browsing information about a user, such as what web sites he/she frequently visits, cannot be stored in a cookie. It is also relatively easy for users to block cookies all together, which stops these advertising companies from gathering any information at all. Some of these companies felt it would be more effective if they could create and install software that could track much more information about a user and send it back over the Internet to a central server. This software has become known as adware and spyware.

Adware vs. Spyware

Adware and spyware are programs that collect and log specific information about a user's web activity on the Internet. By way of the user's Internet connection, some or all of this information is sent back to one or more host computers. The difference between the two involves whether or not the user has granted permission for this to be done. Steve Gibson of the Gibson Research Corporation (GRC) defines spyware as:

> **Spyware is ANY SOFTWARE** which employs a user's Internet connection in the background (the so-called "backchannel") without their knowledge or explicit permission.

> Silent background use of an Internet "backchannel" connection **MUST BE PRECEDED** by a complete and truthful disclosure of 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**.[2]

Adware and spyware are typically bundled and distributed with freeware or shareware. It is a method by which software developers can make additional money.[3] The question is, why can't these software developers be legally prosecuted to stop this? Most users rarely read the entire "End User License Agreement" when they download and install software from the Internet. If additional software is being distributed, this agreement will likely have a very small section discussing the extra third-party software that will be installed along with what the user thinks he/she is getting. This is how developers can legally distribute adware or spyware.

Any adware that is embedded and distributed with freeware should also have its own "End User License Agreement" which discusses exactly what is collected and sent back over the Internet. Based on Steve Gibson's definition, the presence of this license agreement is what differentiates adware from spyware. Often, this agreement is very vague, is not complete, or is difficult to find. Throughout the rest of this document, spyware will be used broadly to include both adware and spyware programs.

Classifying the information that the spyware discloses once it has been installed is another issue that needs to be addressed. Developers of these programs will argue that no personal information is sent back over the Internet. One must ask however, what is "personal information?" If the spyware is collecting and reporting the web sites visited, banner ads clicked on, and products purchased, is this considered personal information? Many would argue that yes, this is indeed too personal to be broadcast out onto the Internet.

Programs that are used to establish peer-to-peer connections over the Internet are known to be spreading many of the spyware programs. Some of the most popular ones include Kazaa, Bearshare, iMesh, and Limewire.[4] Embedded with this freeware are spyware programs like Gator, Aureate, Comet Cursor, and Web3000 just to name a few.[5] Once installed, most of these programs are set up to run every time the computer boots up and wait to transmit data until an Internet connection has been established.

How to detect and eliminate spyware?

If the spyware has already been downloaded and installed, there are a number of programs available that can successfully detect and remove the spyware from a user's computer. Lavasoft's Ad-aware is one of the more popular spyware removal utilities. Ad-aware thoroughly scans files on the hard drive, contents in the registry and all of the cookies looking for over 4,500 spyware signature files. Once found, these files can be removed or quarantined if the user is unsure about the importance of any of them. Lavasoft provides regular updates for Ad-aware as new spyware signatures are discovered.[6] Figure 1 shows an opening screen-shot of Ad-aware 6.0.

Figure 1 - Ad-aware 6.0

Other spyware detection and removal utilities include OptOut and Spybot. For more information on these utilities, visit their web sites at:

http://www.lavasoftusa.com

http://grc.com/optout.htm
http://spybot.eon.net.au

These utilities can only detect known spyware programs and signature files. New spyware or spyware not yet discovered could potentially still be on the computer. To better investigate the presence of unknown spyware, one must establish a baseline audit for his/her computer. This requires determining exactly what programs and services are starting up every time the computer boots up. Since manually sifting through the registry and startup folder can be a tedious task, Advanced Startup Cop is a shareware program that offers a quick display of all programs that launch when Windows boots up. It gives the user the option of temporarily disabling startup programs or removing them all together. It also identifies startup programs that may be unnecessary.[7] For any startup programs that the user is not familiar with, it is a good idea to try to identify them and verify they are not important drivers. Los Angeles Free-Net offers a large list of many of these startup programs and can help someone identify whether or not they are associated with spyware. The list is located at:

http://www.lafn.org/webconnect/mentor/startup/PENINDEX.HTM.[8]

For the Windows NT, 2000, and XP machines, minimizing the services that start automatically is also important to create the baseline audit. Black Viper provides a web site that explains many of the different services available on the computer and suggests when these services should be set to automatic, manual, or disabled. The web site is at http://www.blackviper.com. Once a baseline audit list of startup programs and services has been recorded, it can be used to regularly analyze the computer and verify that no unknown additions or changes have taken place. The baseline audit should be updated regularly as new programs are installed.

Scanning through the cookies stored on the hard drive is another way of detecting unrecognized spyware. For Windows 95 and 98, all cookies are stored in the Windows\Cookies folder. For Windows 2000 and XP, they are stored in each of the users folders under Documents and Settings. Most of the cookies should be identifiable from web sites that have been visited. For those that are not recognizable, a search for some information about them through Google can reveal a lot. Simply deleting them and watching if they return is another method often employed. There may be some cookies that a user knows he/she does not want. Newer versions of Internet Explorer, Netscape and Mozilla offer ways to specify individual cookies or cookies from a specific domain that can be blocked all together.

Spyware detection with firewalls

Firewalls can also play an important role in stopping spyware. While most firewalls are not designed to stop spyware from coming onto the user's system,

they can monitor what information leaves the system and block programs from passing any of the user's personal information out to the Internet. Some personal firewalls that can accomplish this include Sygate, Norton Personal Firewall, and ZoneAlarm. Each of these firewalls monitors both incoming and outgoing information and will alert the user when an unknown program is trying to open a port and get access to the Internet. They can be customized so that certain programs can act as servers from the computer while others will send a notification before any information is passed along. The log files that are maintained by these firewalls are also important to look over since they will reveal outside sources that are trying to gain access to the user's computer either randomly or repeatedly. Figure 2 is a screen-shot from ZoneAlarm.

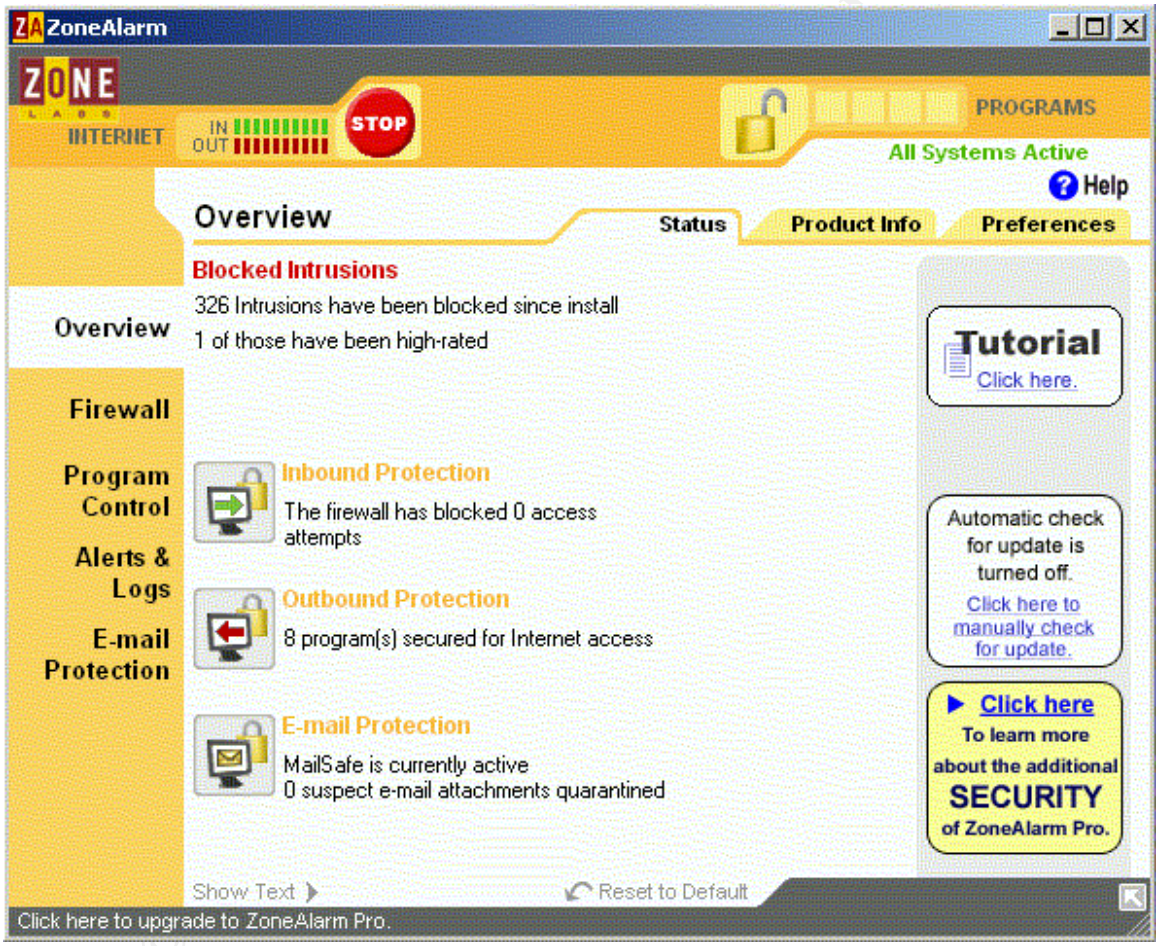

Figure 2 - ZoneAlarm

Stand-alone firewalls can also help to some degree. What is important, though, is that they be "stateful" firewalls, not merely packet filters. Stateful firewalls maintain a connection history and ensure that information coming from an outside source will not be allowed to pass through unless a connection has been previously established. All communication through the firewall therefore must have been initiated by a computer behind the firewall. This proves very effective

in stopping port scanning and closes many vulnerabilities that might exist in some common Windows applications. An example of a stateful firewall is Cisco's PIX Firewall.[9]

Spyware prevention in a corporate environment

Spyware is a difficult issue to deal with in a corporate environment. A lot of users treat their work computer like their home computer. Some will try to take advantage of the high-speed Internet connection they have at work and install a peer-to-peer program in order to download MP3s and MPEGs. These peer-to-peer programs are dangerous on a corporate network because they create holes in the firewall and could potentially give an outsider easy access to a company's intranet. If spyware gets installed along with the peer-to-peer program and is able to capture someone's username and password, unauthorized users could gain access to confidential material.

Policies can and should be created that restrict people from downloading and installing extra software without prior approval. Trying to enforce these policies may not be that easy, however. One method could involve removing administrative rights from all users. Doing this would somewhat limit them on the types of software they could install. Setting up either network-based or host-based perimeter firewalls could also be used to monitor what applications are sending data onto the Internet. Informing all of the employees about the dangers behind downloading freeware and/or spyware is another common method used but not everyone will appreciate or fully understand the inherent risks behind spyware.

Spyware embedded with Kazaa v2

Kazaa offers a good example of spyware embedded with applications. Kazaa is a very popular freeware program used to establish peer-to-peer connections with other Kazaa members in order to transfer files such as MP3s. On the Kazaa web site they have a link to the End User License Agreement. This agreement is divided into seventeen sections and each of those sections is subdivided further. Section 9.1 states:

> **9.1** During the process of installing the Software, you may be offered the possibility to download or install software from third party software vendors pursuant to licences or other arrangements between such vendors and yourself ("Third Party Software"). In the event you do not wish to download this THIRD PARTY SOFTWARE you should uncheck the appropriate boxes. Please note that the THIRD PARTY SOFTWARE is subject to different licences or other arrangements, which you should read carefully. By downloading and using this THIRD PARTY SOFTWARE you accept these THIRD PARTY SOFTWARE licences or other arrangements and acknowledge that you have read them and

> understand them. Sharman does not sell, resell, or license any of this THIRD PARTY SOFTWARE, and Sharman disclaims to the maximum extent permitted by applicable law, any responsibility for or liability related to the THIRD PARTY SOFTWARE. Any questions, complaints or claims related to the THIRD PARTY SOFTWARE should be directed to the appropriate vendor.[10]

This statement leads one to believe that if a user does not want any additional software installed with Kazaa, he/she can simply uncheck the appropriate boxes and Kazaa will be the only thing installed. Unfortunately, other third-party programs will always be installed with Kazaa.

During the first part of the installation process, a window appears asking if the user wants to install SaveNow. The license agreement for SaveNow is included in this window and explains, to some degree, what SaveNow does. It is an advertising program that tries to provide relevant pop-up ads based on URLs visited and search terms entered into search engines. The license agreement reports that it logs the user's local country and zip code as well. The SaveNow software uses this information and connects to WhenU.com servers to create a log of the type of advertisements the user should receive. The program is set to run every time the computer boots up. Kazaa promotes this software by saying "Using SaveNow Keeps Kazaa FREE."

The next window in the Kazaa installation process lists four more promotional software bundles: DelFin, MediaLoads, b3d Projector, and New.net. DelFin and MediaLoads are supposed to display "TV-like entertainment" during the dial-up process, but are known to display regular advertisements as well. New.net is supposed to allow users to visit unofficial domain names such as '.shop,' but it also helps to direct users to sponsored web pages. The b3d Projector promises a richer, more dynamic level of pop-up ads.[11] Users installing Kazaa are provided one checkbox to select whether or not they want to install all four of these promotional software packages. By default, this checkbox and the SaveNow checkbox are both selected. Hence the normal user, who may not understand what each of these applications does, will go with the default settings and install all five of these promotional packages in addition to Kazaa.

If all of the boxes are unchecked, the user expects Kazaa to be the only application installed. Upon inspection after the installation, and after comparing it with the previously recorded baseline audit, a few key items have been added. Using Advanced Startup Cop one will find that Kazaa.exe has been setup in the registry to run every time the computer boots up. In the registry key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce bulldownload.exe has been added. The next time the computer boots up, bulldownload.exe will display a prompt asking the user to download a 20-day free trial version of BullGuard Anti-virus software. The choice not to install it is provided however. The program that is always installed automatically with Kazaa

with no user notification is called Cydoor. Several new registry entries are added which can be detected using Ad-aware and at least two new DLLs are installed, cd_clint.dll and cd_htm.dll. The cd_client.dll file exports at least five new functions that can be used by "Cydoor-sponsored" applications.

- int ServiceShow - places the banner window on the program
- int ServiceClose - closes the banner window
- void ChannelWrite - used in 2-way communication
- void ChannelRead - used in 2-way communication
- void DescWrite - sends back information about the user[12]

Cydoor does not come with an uninstall program and uninstalling Kazaa does not remove it either, so in order to remove it, someone would have to manually delete the files and registry entries or use a removal utility like Ad-aware. Without the cd_client.dll file, Kazaa will no longer function and will kindly display an error message saying "You have uninstalled a part of Kazaa that is needed to run. Kazaa will quit now so you can re-install it." Modified cd_clint.dll files are available to trick Kazaa into thinking Cydoor is still installed. If Cydoor is not removed it will begin storing ads on the hard drive, recording any of the ad transactions that take place, and reporting this back to a host computer over the Internet. Kazaa does offer a version with no extra software attached but the user will have to pay to receive this version.

Kazaa is just one example of freeware embedded with spyware that can be easily downloaded and installed. With multiple freeware programs installed, the amount of spyware on the computer could multiply rapidly. Unfortunately, there does not seem to be an easy way of stopping companies from embedding spyware.

Future of spyware

As adware and spyware continues to evolve, new ways to track consumers and collect information about consumers will emerge along with ingenious ways of remaining undetected. Recently stealware has been introduced into the Internet world. Stealware (aka parasiteware) actually alters the tracking code that is stored in the cookies on the computer.[13] As an example, assume Company A is a small start-up Internet company. In order to help pay for some of their initial costs, they post banner ads on their web site for larger retail companies. If a user who is visiting Company A's web site clicks on one of the ads, Company A will receive a portion of money from the larger retail company. This information about banner ads that have been clicked on is stored in cookies on the user's computer. Now assume that Company X has discovered a way to install stealware on this user's machine. If the user visits Company A's web site, clicks on an ad, and purchases something from the retail company, a cookie is created indicating this occurred. The stealware replaces the cookie and specifies instead that the user clicked on the ad from Company X's web site, not Company A's.

Based on the information from this cookie, the retail company will give Company X the small portion of money that Company A deserves. All of this occurs in the background while the user is connected to the Internet and cannot be easily tracked.

The software developers for the multimedia program RadLight v3.03 recently tried a new way to remain undetected. When the program is installed, it searches for the default directory of Ad-aware. If the directory is found, the RadLight installation process will remove Ad-aware without warning. The software has since been changed but it offers an idea of what some software developers are willing to try.[14]

Conclusion

Spyware is a very hot topic today and will continue to be in the future. Companies that produce the software that can be referred to as spyware argue they are simply delivering personalized advertisements. The software that gets installed, however, has the potential to do a lot more. All of the Internet transmissions from these programs occur in the background, making it nearly impossible to determine exactly what is being transmitted. Utilities like Ad-aware and Spybot have been developed to help deter a lot of the well-known spyware offenders but this does not stop new spyware programs from being created.

The ultimate question is, whose responsibility is it to keep personal and confidential information from leaking out into the Internet? In a corporate environment, relying solely on the user could prove to be a big mistake. Many users will download what they want and are unaware or simply do not care what the consequences are. Making it the network administrator's responsibility is often impracticable especially in a large corporation. In a home environment, the user must take control, but how plausible is it that everyone will take the time to learn how to stop spyware? The user's ISP cannot be asked to monitor every bit of information that leaves the client's computer. At this stage the most important thing is user awareness. If users at least understand what could be occurring and who could be watching them while on the Internet, they can be the ones who judge the value of what is stored on their computers.

References

[1] "Cookie – a searchSecurity definition." 13 October 2000. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211838,00.html (February 2003).
[2] Gibson, Steve. "OptOut – Internet Spyware Detection and Removal." 20 March 2002. URL: http://grc.com/outpout.htm (February 2003).
[3] Edge, Lewis. "Spyware – Identification and Defense." 14 December 2001. URL: http://www.sans.org/rr/privacy/spyware.php (February 2003).
[4] "SpywareInfo > What is spyware?" 12 February 2003. URL: http://www.spywareinfo.com/articles/spyware/ (February 2003).
[5] Gibson, Steve. "OptOut – Index of Known Spyware." 02 December 2002. URL: http://grc.com/oo/spyware.htm (February 2003).
[6] "Ad-aware – Software – Lavasoft." 13 February 2003. URL: http://www.lavasoftusa.com/software/adaware/ (February 2003).
[7] "StartUp Cop for Windows 95/98/ME/NT/2000 and XP." 13 February 2003. URL: http://www.windows-startup-cop.com/ (February 2003).
[8] Mayer, John. "Program (Executable) Name List (DIRECT links)." 10 February 2003. URL: http://www.lafn.org/webconnect/mentor/startup/PENINDEX.HTM (February 2003).
[9] Senner, Lisa. "Anatomy of a Stateful Firewall." 09 May 2002. URL: http://www.sans.org/rr/firewall/anatomy.php (February 2003).
[10] "End User License Agreement." 13 February 2003. URL: http://www.kazaa.com/us/terms.htm (February 2003).
[11] Barrett, Robertson. "Five Major Categories of Spyware." 21 October 2002. URL: http://www.consumerwebwatch.org/news/articles/spyware_categories.htm (February 2003).
[12] "Advertising Spyware: CyDoor CD_Load.exe (Ads On Software (tm))." 14 February 2003. URL: http://www.cexx.org/cydoor.htm (February 2003).
[13] "Stealware." 28 February 2003. URL: http://www.spyware.co.uk/stealware.shtml (February 2003).
[14] McWilliams, Brian. "Anti-spyware program targeted by multimedia player." 24 April 2002. URL: http://www.computeruser.com/news/02/04/24/news9.html (February 2003).

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS