Global Information Assurance Certification Paper

Steganography in the Corporate Environment

Joann Kennedy

April 9, 2004

SANS\GIAC Practical – GSEC Certification
Version 1.4c

Table of Contents

Abstract

The purpose of this paper is to explain how proper policies and procedures can minimize the impact of steganography in a network environment. This paper will outline how steganography is used for the purposes of corporate espionage and creating downstream liability. Additionally, it will lay the foundation for what steganography is, how it is accomplished and the common methods for detecting and/or defeating steganography. Finally, this paper will provide detailed information about corporate policies and network procedures that should be implemented to minimize the negative impact of steganography in a network environment.

Introduction

Hacked? Infected with a virus? For many years, network intrusions and virus infections seemed to be the most significant network related issues facing a corporation. But in reality, these can become fairly insignificant when compared to the introduction of steganography into the corporate environment for the commission of corporate espionage or the creation of other liabilities. Steganography, Greek for "hidden writing", is the art and science of writing hidden messages in such a way that no one apart from the intended recipient even knows that a message has been sent (Wikipedia 1).

This paper will explain how the use of steganography in a network environment can be used to damage or destroy a company by facilitating the theft of intellectual property and creating downstream liability issues for the organization. This paper will provide a detailed description of steganography and how it is used. Additionally, this paper will discuss methods of steganography detection and the policies and procedures that should be implemented to prevent or minimize the damage caused by steganography.

Theft of Intellectual Property and Corporate Espionage

Intellectual property, defined as the formulas, prototypes, copyrights and customer lists maintained by a company, can be far more valuable than the actual items they sell. In fact, "…intellectual property is widely recognized as the driving force behind America's success." (Sticky 1). It would make sense, then, that this information would be well-guarded and protected within the corporate environment. That is often not the case, however. "According to the 2002 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, the cost to American companies of foreign and domestic economic espionage and theft of intellectual property is $300 billion dollars a year and rising" (LUBRINCO 1). And in all reality, that is just the reported losses. Many businesses opt not to report corporate espionage for fear that their stock prices and reputation will be negatively impacted.

The term espionage has long referred to the use of spies to collect information about what another entity is doing or planning (Espionage 1). Throughout history, spies have

been used to infiltrate the enemy and report back with information regarding their capabilities and strategies. In the corporate environment, this is referred to as corporate or economic espionage. And the "spies" are not the usual suspects. "According to recent statistics, more than 80 percent of information theft facing businesses in the United States occurs internally. This means that a company's greatest threat to loss of sensitive information comes from within – its own employees" (Wiseman 1).

Consider the following scenario:

> Sean comes into the office wearing his typical headset tied back to his MP3 player. But this is not a typical day for Sean. Once everyone in his office leaves for lunch, he gets to work. Over the last few weeks, Sean has collected a variety of the newest designs and production notes for new ad projects at his company. He has been offered a substantial amount of money if he can pass these files off to a competitor.
>
> He plugs his MP3 player into his computer and brings it online to receive files. Sean also takes out his USB memory key ring and inserts it into the USB port of the PC. He then starts up a program from the key ring called ***Steganography***, which is from SecureKit and works with images or sound files. His goal is to embed the production files into a series of MP3 songs. He knows that MP3s do not use the entire audio range, so there is some space on the high side of the frequency to stash data of his own. Once the files have been embedded, Sean copies them up the MP3 player into a custom play list. He then removes the USB memory and sticks it back onto his key ring. The headset goes back on and when his coworkers return, they find Sean listening away to his tunes. That night when everyone leaves the office, they go by the security desk and Sean, wearing his headset with music playing, is waved on through. The company's most recent plans and designs for a new advertising job have just walked out the door. (Sweeney 1).

Quickly and easily, sensitive information can just "walk right out the door", taking with it, a company's future income and competitive edge.

Steganography and Downstream Liability

In addition to corporate espionage, downstream liability is yet another concept that network administrators have begun to consider. Simply stated, it means that one company would be liable to another company for damage caused by a criminal hacker (Wright 1). To date, references to downstream liability center around dedicated denial of service attacks launched from hacked networks for the purpose of overwhelming and collapsing the network of another company. After many such attacks, lawmakers decided that those tasked with developing and administering corporate networks have a legal obligation to operate their networks in a safe and reasonable manner. Failure to conduct routine network maintenance and eliminate potential hazards could allow a hacker to access a company's network and use that network for criminal means. And therefore, the hacked company could be held financially responsible for damages caused by the attack.

Steganography may add a new twist to this concept. Consider for a moment what would happen if a corporation's web site was used to house sensitive customer information concealed through steganography. Those who knew that the images

existed on the web site could use specialized software and passwords to access the data for purposes such as identity theft, while the network security administrator remained oblivious to the data's existence. At some point in the near future, lawmakers may decide that prevention and detection of this type of activity is also the responsibility of the network administrator. In addition to civil penalties, the company may also be criminally charged for possessing and distributing illegal material. This type of situation would create negative publicity and financial repercussions as great as any other type of network intrusions.

Definition of Steganography

As previously discussed, steganography involves concealing information within another medium, therefore allowing information to be passed to the receiver without anyone else knowing that the message even existed. The process generally involves placing a hidden message within some transport medium, called the carrier (Kessler 2). This is different from cryptography which transforms a message into an unreadable string of characters that can only be deciphered by the intended recipient using an agreed upon "decoder ring". With cryptography, it is obvious that a message has been sent, but the contents of the message are scrambled. With steganography, the casual observer would not even know that a message had been sent.

Throughout history, various forms of steganography have been used to communicate with allies during times of war. From tattooing information onto the shaved heads of messengers to the use of invisible ink, steganography has been used repeatedly and successfully to transmit information covertly.

In today's context, computers are the primary tools used for generating steganography messages – using either very simple or very complex methods. In the most simplistic form, information can be created on a hard disk drive partition and the partition can be hidden using system utilities. Similarly, information can be written to a file and the file's properties can be changed so that the file is hidden. To other casual users of the computer, the information would be non-existent. For the intended receiver, however, using similar system utilities would "unhide" the partition or file and reveal the information. More sophisticated methods of steganography involve the use of specialized software to manipulate a carrier message to hide the encrypted content of the hidden message. In this scenario, the intended recipient must know what software, encryption method and password were used before the hidden message can be uncovered.

Uses for Steganography

Steganography can be employed for both legitimate and illegal purposes. In today's digital world, published works, such as written material, artwork or musical productions can be easily duplicated. "Information (or data) hiding, a form of steganography, can be used to embed data into digital media for the purpose of identification, annotation, and copyright" (Bender 1). For example, "…an author can embed a hidden message in a

file so that he/she can later assert their ownership of intellectual property and/or copyright" (Kessler 3).

Additionally, the technology used for printers and scanners has developed to such a level that it is now possible to create high quality reproductions of original material. This advance has opened the door for counterfeiters to easily manufacture currency and other important documents. Steganography can be used to deter this type of activity. "Embedding a digital signature into a secure document that can be recognized by a printer as it prints allows the printer to refuse the printing of any documents that it detects as secure or protected" (Bender 550).

Another legitimate use of steganography involves image authentication. With today's technology, image manipulation only requires a little knowledge and free or inexpensive software applications to alter an original image. Image authentication can be used to verify that the picture being seen is identical to the picture that was originally created and disseminated. "By using data hiding techniques, a checksum of the original work can be calculated and embedded directly into an image for verification purposes" (Bender 555). Later checksums of the image can be compared to the original value to determine if the image has been altered.

Steganography, by nature, is used to conceal information. And although there are legitimate purposes for its use, steganography is often used to conceal illegal or unethical material. It was originally reported after the September 11th attacks that terrorist organizations were using steganography for covert communication to plan the attacks on the United States. Although no concrete evidence was located to substantiate these claims, it is extremely evident how this technology could be used for future terrorist activity.

Aside from terrorist activity, many other illegal operations can benefit substantially by concealing their communication or the fruit of their labor. Consider child pornography. Steganography can be used to hide digital images of children in other legitimate files and images. In this manner, the illegal images can be stored, transmitted and displayed with little or no risk of detection. Also consider those involved in corporate espionage. Using steganography, corporate spies can easily conceal the intellectual property and trade secrets that they are stealing within innocent-looking files that can be easily transported without detection.

Methods of Steganography

Methods of steganography are potentially unlimited, but a few common techniques dominate the steganography software market today. Messages are typically hidden in large files such as images and sound files, or transmitted using covert TCP/IP channels.

"To hide a message inside an image without changing its visible properties, the cover source can be altered in 'noisy' areas with many color variations, so less attention will be drawn to the modifications" (Krenn 3). Although steganography can employ text

documents as a carrier file, typically digital images, audio and video files are used because they contain more "noisy" areas that can be used for manipulation. Although there are many variations, most steganography software follows the same basic practice. Typically, a carrier file is selected, or in some applications generated and the file containing the information to be concealed is identified. In some cases, the hidden data is embedded in its original format. In more advanced applications, the information to be hidden is first encrypted using a password or passphrase and then the encrypted data is embedded in the carrier file. Once the carrier file is received by the intended recipient, the same software used to embed the hidden data must be used to extract the information. If the data was encrypted prior to its insertion into the carrier file, the intended recipient must also know the encryption type and password or passphrase used for the encryption.

Within digital images, audio files and video files, information hiding can be accomplished using many different steganography techniques. The following sections will highlight the most common methods currently in use.

Least Significant Bit

One of the most common and widely used methods of steganography utilizes modifications to the least significant bits (LSB) of each color pixel within a digital image. A digital image, such as a bitmap (BMP) or a graphic interchange format (GIF) contains thousands, even millions, of pixels, or colored dots, to create the picture. "Each pixel on a computer monitor selects from three (3) primary color variations: red, blue and green, also referred to as RBG" (Caldwell 2). In a 24-bit image, each of these three (3) colors is represented by one (1) byte, or eight (8) bits, with a bit being the smallest unit of data that can be stored on a computer. Each bit within the byte is assigned a value so that the sum of the bits totals anywhere between zero (0) and 255. The bits are valued from left to right – 128, 64, 32, 16, 8, 4, 2 and 1. For example, the color white would be represented as 11111111, 11111111, 11111111. The color black would be represented as 00000000, 00000000, 00000000. Changes to these bits are reflected as a change in color and light intensity within the image.

In its most basic form, the LSB method of steganography involves changing the lowest valued bit in each byte. This is the far right-hand bit of the byte, which is represented with a value of one. Changes to this value will alter the color displayed in the image, but the change is so miniscule that it is indiscernible by the human eye. Since text characters are represented as one byte, or eight (8) bits, for each letter, steganography software, such as S-Tools, can substitute one bit from a byte of text for the LSB of each color byte. This process is continued until the entire file to be hidden has been embedded into the carrier file.

Simplistic steganography applications using the LSB method of substitution randomly select which bits will be used for the process. More advanced applications first evaluate the carrier image and determine which bits should be altered to minimize detection and maintain the original appearance of the image.

Discrete Cosine Transformations

Unlike the above mentioned BMP and GIF images, images stored in JPEG format (joint photographic experts group) do not store the individual values of each pixel. Instead "discrete cosine transformations (DCT) are used by the JPEG compression algorithm to transform successive 8 x 8 pixel blocks of the image into 64 DCT coefficients each." (Krenn 5). In essence, the values of groups of pixels are averaged to represent one color for a larger area of pixels. This process requires less storage space since less information is required to generate the image. Although some information is lost during JPEG compression process, the overall difference in appearance is not overwhelmingly apparent to the untrained human eye. "Although a modification of a single DCT will affect all 64 image pixels, the LSB of the quantized DCT coefficient can be used to hide information." (Krenn 6). Similar to the LSB method of steganography used for BMP and GIF images, substitution of the LSB in DCT's will result in changes to the image file that are not apparent to the human eye. Tools such as JP Hide and Seek and JPegX can be used to accomplish this quite efficiently.

Audio and Video Steganography

The above-mentioned techniques focus on embedding information into digital image files. Steganography applications, such as Steganos Security Suite and MP3stego, can also utilize digital audio and video files as carriers.

Just as digital image steganography relies on the limitations of the human eye to perceive minute changes in color and light intensity, steganography of digital audio carriers relies on changes to ranges of frequencies inaudible to the human ear. "Using any frequencies above 20.000 Hz, messages can be hidden inside sound files and will not be detected by human checks" (Krenn 6).

Since digital video files are combinations of images and sound, the steganography methods discussed above can be used transform digital video files into carriers. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. Therefore, any small but noticeable distortions might go unnoticed by humans because of the continuous flow of information (Krenn 6).

Covert Channels in the TCP/IP Protocol

"A covert channel is described as 'any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy'" (Rowland 1). Through manipulation of the TCP/IP packet headers used to transmit information between computers, raw or encrypted information can be hidden and transmitted essentially undetected.

By design, the TCP/IP protocol requires a "three-way" handshake between computers attempting to communicate with each other. This process requires the initiating computer to send a packet of information to a remote computer, announcing the new connection and other identifying information that will be necessary for continued transmission. The remote computer is then required to send a response packet stating that the initial packet was received and that the remote computer is awaiting further information. The initiating computer then sends a third packet to the remote computer indicating that the response was received and data transmission can begin.

Within each subsequent packet that is that is transmitted using the TCP/IP protocol, there is a "header" area which provides information about the packet, such as its size, identification and IP address. "Within each header, there are a multitude of areas that are not used for normal transmission or are "optional" fields to be set as needed by the sender of the data" (Rowland 4). Using a steganography application, such as "covert_tcp", these areas can be exploited and used for concealing information in the packet headers. The actual message being transmitted would be considered the carrier file since the information to be hidden is embedded within the packet header. The intended recipient would simply need to capture these packet headers and use covert_tcp to reveal the hidden information.

Other Methods of Steganography

In addition to the steganography methods detailed above, it is important to remember the less technical, often overlooked, methods of concealing data. A perfect example of this is the alteration of file properties and partition tables to hide files and partitions containing secret information.

Information can also be concealed within file headers and file slack. File headers designate the type of file as well as the configuration information for the file. Just as TCP/IP packet headers contain unused or optional fields for information, so do file headers. File slack is a byproduct of FAT 12, FAT 16 and FAT 32 file systems, which store files in one (1) cluster segments that may or may not be filled completely by the file. The area remaining from the end of the file to the end of the cluster is referred to as file slack. Information can be hidden in this area that is not viewable within the carrier file, but can be carved out using an application as basic as a hex editor.

In the NTFS environment, the Master File Table (MFT) is responsible for maintaining information about all of the files stored on a computer. The MFT is comprised of records for each file stored. These records contain attributes which store specific information about the file, such as the file name, size, storage location, etc. Within each record, there is a data attribute that may contain the actual data from the file or the location where the data is stored. Using basic system utilities, it is possible to create hidden files and append them to the original file in Alternate Data Streams (ADS). These ADS's are essentially hidden from the file system and will not appear in any directory listings. For those who know that these ADS's exist, they are relatively easy to

recover; therefore, they create a prime opportunity to safely conceal data while still being able to access the information.

Steganalysis – Detecting Steganography

"The process of detecting steganographic messages is known as steganalysis" (Berg 1). It is a relatively new discipline that is constantly developing and improving methods to detect steganography. Currently, there are two (2) established methods of manual detection: visual inspection and statistical analysis.

Visual inspection is exactly what it appears to be. A steganalyst, the person responsible for performing steganalysis, must visually inspect and review each suspected file to determine if that file is a carrier for a hidden message. This process can be relatively simple if the steganalyst can review the original cover file before it was converted into a carrier file. For example, if two seemingly identical images are located on a computer, they can be compared, side by side, to determine if any visual differences can be detected. Due to the advancing technology of steganography software, this can be extremely difficult if not impossible to detect. But it can be useful and worth the attempt if less robust steganography tools are employed or if the carrier file was not particularly suitable for the information that was embedded within it. Another challenge to visual inspection is that often times the original cover file is destroyed after it has been transformed into a carrier file. Therefore, no original file remains for comparison. Unless the steganography method used was extremely ineffective at concealing the data, visual inspection of the carrier file will likely produce no definitive answers.

Statistical analysis can also be employed to reveal the existence of carrier files and hidden messages. "Steganographic techniques generally alter the statistics of the carrier and longer hidden messages will alter the carrier more than the shorter ones" (Kessler 16). Using a histogram, or graphic representation of a frequency distribution, a steganalyst can compare the frequency distribution of the colors of a potential carrier file with the theoretically expected frequency distribution of a "normal" file.

In addition to these manual methods of detection, a few automated tools have also been developed to assist with the detection of steganography within carrier files. Once such tool, Stego Suite from WetStone Technologies, "…provides the ability to quickly examine and evaluate digital image and/or audio data for the presence of hidden information or communication" (Wetstone 1). Additionally, this tool can be used to recover encrypted messages hidden in carrier files.

Another tool, Stego Detector, is currently under development by George Mason University graduate student Neil Johnson. "This program is designed to search hard drives for electronic "fingerprints" that typically result from steganography applications. Similar to a virus scanner, Stego Detector identifies these file signatures within carrier files" (Caldwell 3).

Methods for Defeating Steganography

While tools and techniques have been and are continuing to be developed for steganography detection, they are still in their infancy and should not be relied upon one hundred percent to protect against and prevent the use of steganography in the corporate environment. In addition to the use of these tools, organizations can use a two-pronged approach - corporate security policies and network protocols - to prevent or minimize the usefulness of steganography attacks against a corporate network. The following sections outline basic concepts and suggestions that should be included in a company's policies and procedures.

Corporate Security and Acceptable Use Policies

Corporate security and acceptable use policies outline what an employee or network user is and is not allowed or authorized to do within the corporate environment. These policies establish "rules of conduct" to be followed by all employees. They should clearly explain what is and is not acceptable and what the penalties for violation will be. These policies provide an organization with the legal footing needed to enforce and prosecute violators and prevent continuing abuses.

The following are basic issues relating to steganography that should be addressed within a company's policies:

- Designate who, if anyone other than the network administrator is allowed to install software on the network computers.
- If employees and other network users are allowed to install software applications, identify which types of software require prior authorization for installation. Also identify which applications, such as wiping and steganography utilities are prohibited from installation.
- Define which types of removable media, if any, are allowed to be used in conjunction with network computers.
- Identify intellectual property and other sensitive data that is used in the course of business and restrict users' access to sensitive information.
- Clearly state what types of information are considered sensitive. Also include in this section any non-compete clauses that are conditions of employment.
- Clearly outline the punishments and civil liabilities associated with each policy violation.

Network Protocols and Procedures

While strong security and acceptable use policies provide corporations with the legal ammunition needed to prosecute and punish violators, they do little to actually protect the company from a steganography attack. For this reason, these policies need to be supported with strong network protocols and procedures that can lessen, if not eliminate, the ramifications of such an event.

For example, an acceptable use policy that states users are not allowed to install any software without prior authorization looks good on paper. But it does little to prevent a rogue employee from downloading and installing any software application he/she chooses. Backing up that policy with a network protocol that technologically restricts an employee's ability to install any applications on a network computer is much stronger. The network protocols and procedures implemented can prevent the event from occurring.

Consider the following suggestions when developing network protocols and policies:

- Wherever possible within the network environment, disable users' ability to install software application without prior authorization.
- Wherever possible, disable the users' ability to connect external devices such as thumb drives, personal data assistants and MP3 players, to a network machine.
- Restrict users from saving information directly to one computer or hard disk drive. Require that all data be stored on user specific directories housed within the network or file server.
- Monitor network traffic for high volumes of graphics, audio and image files that may be used as carriers.
- Monitor network traffic for large segments of unintelligible datastreams, such as what may be seen if encrypted data were being transmitted.
- Create a baseline hash of all of the images stored on the corporate web site. Periodically rehash the images to ensure that they have not been altered or used as carriers for hidden messages.
- Establish a means to recompile all graphic, audio and video files using a lossy compression scheme, such as JPEG or MPEG compression.
- Develop methods for randomly sampling and testing information transmitted and stored throughout the network.

In addition to implementing these types of policies, it is also crucial that IT managers and network administrators remain vigilant in monitoring the latest developments in steganography and steganalysis. The technology in this area is continuously changing and it requires constant policy and protocol updates to detect and prevent steganography attacks.

Conclusion

Throughout the centuries, various methods of steganography have been used to conceal information and to communicate covertly. With today's technology and the ever increasing number of steganography software applications being developed, hiding data is easier now than it has ever been in the past. Due to the software's relative ease of use and the increasing technical knowledge of the average user, steganography and

the damage that it can cause should be a key concern of any corporation interested in maintaining profits and remaining competitive in their market.

It is common knowledge that the development and implementation of a strong corporate diversity awareness program can lessen the impact of a lawsuit over a diversity-related issue should one arise. It stands to reason that should a company's network system be used to surreptitiously house or transmit illegal material, having policies and procedures in place to address and deter the activity should also lessen the company's downstream liability threat. These same policies and procedures should also help in protecting a corporation's intellectual property and assist in the civil and criminal prosecution of violators.

By taking a proactive stance and developing the appropriate policies and procedures, a company can prevent or at the very least minimize the impact of a steganography attack on their corporate network – and their bottom line.

NOTE: For additional information relating to steganography software currently available, refer to the following location:

http://www.jjtc.com/stegoarchive/stego/software.html

List of References

Bender, W. et al. "Applications for Data Hiding." *IBM Systmes Journal*. Vol 39, Nos. 3 & 4, c. 2000, pgs. 547 – 566. http://www.almaden.ibm.com/cs/people/dgruhl/afdh.pdf

Berg, George et al. "Searching for Hidden Messages: Automatic Detection of Steganography." Aug. 30, 2004, pgs. 1 – 5. http://www.cs.albany.edu/~davidson/Publications/IAAI103.pdf

Borders, Toni. "Steganography Policies for Protecting Your Web Site." SANS Institute 2003. Pgs. 1 – 13. http://www.giac.org/practical/GSEC/Toni_Borders_GSEC.pdf

Caldwell, James. "Steganography." *CrossTalk The Journal of Defense Software Engineering*, June 2003 Issue, pgs. 1 – 5. http://www.stsc.hill.af.mil/crosstalk/2003/06/caldwell.html

"Espionage Definition". Sep. 7, 2004, pg 1. http://www.legal-definitions.com/Misc/espionage.htm

Kessler, Gary C. "An Overview of Steganography for the Computer Forensic Examiner." Aug. 15, 2004, pgs. 1 – 22. http://www.wetstonetech.com/f/stego-kessler.pdf

Krenn, Robert. "Steganography and steganalysis." Aug. 15, 2004, page 1 – 9. http://www.krenn.nl/univ/cry/steg/article.pdf

LUBRINCO Group. "Protection of trade secrets and intellectual assets". The LUBRINCO Group, Inc., c. 1997-2004. July 10, 2004, pg. 1. http://www.lubrinco.com/lgecoesp.html

Luong, Mihn. "Corporate Espionage: A Real Threat." *Optimize Magazine, Internet Week*. Sep. 3, 2004, pgs 1 – 6. http://www.internetweek.com/shared/printableArticle.jhtml?articleID=15202264

Rowland, Craig H. "Covert Channels in the TCP/IP Protocol Suite." Aug. 30, 2004, pgs. 1 – 11. http://www.firstmonday.dk/issues/issue2_5/rowland/

"Sticky Fingers". Aug. 3, 2004, pg. 1. http://www.crisismanagement.com/StickyFingers.htm

Sweeney, Michael. "Tools to combat your client's steganography risks." CNET Networks, Inc, c. 1995 – 2003. Aug. 15, 2004, pg. 1. http://techrepublic.com.com/5100-6329_11-5146631.html

WetStone Technologies. "Digital Forensic Solutions." 2002 WetStone Technologies, Inc. Aug. 30, 2004. http://www.wetstonetech.com/f/pr_StegoSuite4.0.pdf\

Wikipedia. "Steganography". Aug. 15, 2004, pg 1. http://en.wikipedia.org/wiki/Steganography

Wiseman, Dylan W. "An Introduction to California Trade Secrets Law." Sep. 3, 2004, pg. 1. http://library.lp.findlaw.com/articles/file/00073/009531/title/Subject/topic/Intellectual%20Property_Trade%20Secrets/filename/intellectualproperty_1_764

Wright, Ben. "What is the real threat of downstream liability?" Sep. 3, 2004, pg 1. http://expertanswercenter.techtarget.com/eac/knowledgebaseAnswer/0,295199,sid63_gci980206,00.html

Last Updated: July 24th, 2017

Upcoming Training

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
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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
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
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
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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor