Interested in learning more about security?

SANS Institute InfoSec Reading Room

InfoWar: Cyber Terrorism in the 21st Century Can SCADA Systems Be Successfully Defended, or are They Our "Achilles Heel"?

The United States and many other countries are currently engaged in electronic and information warfare with many other foreign nations. Both the corporate world and government are vulnerable to cyber attack. Vulnerable SCADA systems which were once pushed to the side when it came to serious consideration for increased security are now potentially our "Achilles heal" when we consider the most likely target to cause major problems if exploited by our adversaries. Will this attack on SCADA systems occur? What wi...

InfoWar:
Cyber Terrorism
in the 21st Century

Can SCADA Systems Be Successfully Defended, or are They Our "Achilles Heel"?

SANS GSEC Practical (Version 1.4 - Option 1)

Michael Ratledge, CCNA, CNE, MCSE
September 26, 2002

Sun Tzu - author of "The Art of War"
The oldest known military treatise in the world
(Picture from IT Dept @ SUNY / Brooklyn)

Abstract

The United States and many other countries are currently engaged in electronic and information warfare with many other foreign nations. Both the corporate world and government are vulnerable to cyber attack. Vulnerable SCADA systems which were once pushed to the side when it came to serious consideration for increased security are now potentially our "Achilles heal" when we consider the most likely target to cause major problems if exploited by our adversaries. Will this attack on SCADA systems occur? What will be the outcome and effect on American lifestyle and our psychological well being if terrorists take advantage of this vulnerability? What recent precedence has been observed in past electronic and information warfare? When terrorists master the art of Information Warfare, the face of warfare as we know it will change forever.

These topics will be explored by looking at the history of cyber warfare, specific threats – especially to our SCADA systems, our heightened information security posture, attacks continuously on the rise, available cyber resources and conclusions for our future defense of these critical infrastructure systems.

Background

While reading Erbschloe's Information Warfare – How to Survive Cyber Attacks [1] in early 2001, with his detailed descriptions of the potential and how to protect ourselves against the same; it became painfully apparent that given the current state-of-affairs, we were both unprepared and severely incognizant of exactly where the weaknesses in our corporate, government and military infrastructure were located. At a minimum, the common person was unaware of these risks and their full potential. Here we sit more than a year after the events of September 11th, 2001 – forever burned into the American psyche as "9/11". Within ten days of "9/11", the Institute for Security Technology Studies at Dartmouth had written a "Predictive Analysis" on the "Cyber Attacks during the War on Terrorism" [2] concluding with the facts that "Cyber Attacks Immediately Accompany Physical Attacks", "Politically Motivated Cyber Attacks Are Increasing In Volume, Sophistication, and Coordination". Due to the constantly evolving news on this topic, I decided to 'freeze' the references used for this paper on September 26th, 2002. Perhaps by the time this paper is published, the reality it invokes will have passed – hopefully it will remain relevant far into the future.

In addition, due to the transient nature of the Internet I captured all web pages that are referenced in this document in case they are removed, deprecated or otherwise unavailable. There is a separate HTML-formatted version of this document that links directly to the original online text and graphics if necessary, and a complete archive of all material is available. At the time of completion of this practical (6-Oct-2002), all links were still valid and accessible.

If – in the future – these documents are required to complete the picture painted herein, download “Michael_Ratledge_GSEC_References.ZIP”.

History

The illustration on the title page is of Sun Tzu, author of the oldest known military treatise in history. Many references were made in the Security Essentials course to quotes from this text, and a there is a complete English-language translation of his work by Lionel Giles online [3]. As we learned in class, the basic military tactics from ancient times have not changed significantly, but we are on a new “electronic frontier”, where old rules of engagement no longer apply. Basic tactics remain essentially the same, but implementation and execution of them will soon take a radical departure from what the world knows as warfare. There is much precedence already extent that shows electronic warfare in the form of Internet exploitation is already being utilized – some more than five years old. Indeed prior to the public release of relevant information, it was commonplace for RF (Radio Frequency) ‘jamming’ and other electronic warfare to be utilized. In our context, we are looking at specifically Internet-based information warfare.

From Beijing Jisuanji Shijie [China Computerworld] authors discuss in Chinese [4] the potential of six concepts of future electronic warfare and how they could be utilized to change the face of the battlefield. A very hard to reach link – depending on how the government of China is feeling about the U. S. Embassy [5] discusses how as early as 1999 the Chinese government was blocking certain sites from view of their populace. The “Great Red Firewall” has recently been in the news for blocking access to “Google” and a literal “mirror” site setup to work around this blockade, but they have long been known to utilize similar tactics against Taiwan and Hong Kong, among others. They, along with Pakistan and numerous pro-Islamic militants have been shown to be both using cracking of sites to deface them and operating anti-India web-sites posting disparaging and insulting information on ineloquently named sites registered by ICANN [6]. Oddly enough, this URL mentions Osama bin Laden by name, going into the potential for him to wreak havoc with India or possibly Russia’s Internet infrastructure. China is also known to have planned military strategy to disrupt the infrastructure of Japan and South Korea. China also took advantage of the forced downing of a US Navy EP-3E spy plane at Lingshui Airfield on Hainan Island, China to further their “emerging IW capability” [7].

Now, of course the United States is far ahead in its own development and usage of Information Warfare. Previous Internet warfare usage by our allies was documented in Smederevo, Kosovo when in May 1999 a NATO attack warning had been e-mailed to the owners before it took place. This was an instance of psychological warfare, one that has become increasingly popular with U.S. and allied forces. In March of this year, electronic warfare in the form of psy-ops was utilized in the war against terrorism in Afghanistan. Air Force information warfare

specialist used broadcast AM radio to let the Taliban and al-Qaeda forces know that they were the targets of our military forces.

Unfortunately, the fact that cyber attacks on the United States were "just a matter of time" was foretold in October 1999 on the CMP Media's "TechWeb" Business Technology Network [8]. "Intrusion threats come from a spectrum of sources, ranging from thrill-seeking recreational cracker, to disgruntled employees, virus writers, criminal groups, terrorists, and foreign-intelligence services."

Specific Threats

Several specific eminent threats are already known. On December 1st, 2001 CFO Magazine published a report that "attacks on corporate networks may already be underway" – likely an understatement since many believe this type of exploit has been underway for some time [9]. Many companies are not prepared, and a recent study found that some larger companies still do not have even basic protection in place, such as virus scanning of incoming mail, real-time network storage or have failed to keep system security patches up-to-date. A new Internet virus that took advantage of a security vulnerability that had been known and had patches available for more than a year exploited this fact recently. The National Infrastructure Protection Center ("NIPC") reports that while interest is rising in protecting computer networks, too often the tools available are not powerful enough to keep hackers out.

Why don't terrorists care about your personal computer? Because power grids, dams, and other industrial facilities monitored by SCADA (Supervisory Control and Data Acquisition systems) are ripe for target and better suit their intent to damage physical infrastructure and disrupt critical industrial facilities. In fact, many recent Internet reports indicate that SCADA systems such as water supply, wastewater and similar systems are particularly vulnerable, because they have long been "outside" the realm of consideration as critical protection and major havoc in these systems could easily result in panic and even mass hysteria among the population, a terrorist's dream! These systems are the real risks, those that are widespread, likely geographically dispersed, not thought of as being critical systems and without which everyday life as we know it would be altered to the point that public confidence in their protection would be eroded, and further the confidence in those that are responsible for their protection would also be denigrated. Of course, we were aware of these risks before "9/11", but little attention was paid to mitigation of these weaknesses because other – more high profile targets were considered more important.

National infrastructure information was found on al-Qaeda computers. Investigators discovered a house in Pakistan run by al-Qaeda that was devoted to training for cyber-warfare and hacking, according to coalition intelligence officials. It is easy to predict that eventually, given the time and resources, al-

Qaeda crackers can and will learn how to break into these systems unless we persist in building new security precautions around these systems to elude their further scrutiny of SCADA systems.

The most overlooked serious risks are comprised of SCADA systems previously listed, including electrical transmission equipment, energy generation systems as well as surface transportation, financial and various other information technology systems. Unfortunately a study of SCADA systems found that approximately 40% of them were connected to the Internet, and 60% of them were accessible by modem [10]. Precedence has already been set that these systems can be compromised, and therefore it is almost a foregone conclusion that this could be a uncomplicated way to attack our infrastructure without having to invest a great deal of time, money or effort into the endeavor. The above-referenced article makes note of an attempted breach of SCADA systems in Australia that were unsuccessful 44 times – all of which were completely undetected, but the 45th attempt succeeded and allowed the disgruntled former consultant that had been denied a job to release 1 million liters of sewage into the water supply. "Marine life died, the creek water turned black and the stench was unbearable for residents". Seemingly innocuous mistakes by users have previously caused Internet routers to cascade errors into routing tables, entire electrical grids to implode upon themselves and further, crackers have been close enough to be able to shut down entire telephone systems, disrupting 911 emergency response and related systems, for example. There are a plethora of other items that could possibly be compromised given the variety of national infrastructure systems that could be exploited and limited only by the imagination of the attacker.

Hardening these systems therefore should be one of the highest priorities given the potential "pay off" and high risk as well as the psychological effect of successful exploitation.

Another item we studied in Security Essentials class was the use of steganography – a cryptographic method for placing and hiding both text and pictures inside graphics. Because these could be easily stored on the Internet and due to their nature not being obvious at all and basically indiscernible to the naked eye, they could further be straightforwardly used to communicate both instructions and diagrams or schematics, for example. Since it has been widely reported that bin Laden and his al-Qaeda operatives could be using stenography to hide maps and photographs of targets and post instructions for terrorist in chat rooms, on bulletin boards and websites, we must take this threat seriously!

This leaves a very uneasy feeling among security professionals and those law enforcement agents that are aware of the capabilities of steganography. How long would it take for us to even find these, given the weak set of detection applications that are currently available, much less the cryptographic techniques required to decipher the encrypted message, maps or photographs? This one

technique may be the most dangerous – seemingly innocuous – methodology with potential for terrorist usage that has ever been devised.

Heightened Information Security Posture

Much has been made of the United States' planned release of a national cyber security plan. Richard Clark, the head of the NIPC has long touted the release of this plan in September, planned for the 18th. A draft plan has been posted for comment, and while it is still early, the consensus among serious security professionals appears to be that there is a "whole lot missing" and numerous holes in the draft plan, further discussion is beyond the scope of this paper. Numerous other reports show everyone is more aware of info-security.

Canada recently announced a draft plan that essentially expects their ISPs to spy on their users by forcing them to allow easy access for surveillance by spy agencies and their police and would outlaw possession of computer viruses and could require ISPs to keep logs of all web browsing for six months.

A major "mistake" was recently made by a supposedly "white hat" hacker group called "ForensicTec". Thinking they had done the country a favor, they published a report that they were able to break into several government and military systems. The FBI took issue and decided to raid the firm, and they have likely ruined any potential reputation simply by ignorance of the proper procedure that is required before undertaking such exploits. Since some of the cracks they made included the U S Army's Fort Hood and NASA, these agencies also took an active interest in the investigation. This reinforces one of the basic tenants we were cautioned about in the Security Essentials class: always have the *authority* before proceeding with any type of network scan, port probing or other more active but similar technologies.

Other countries are also on edge about cyber security. It seems as though China recently made a big deal out of the issue that they believed that Microsoft was spying for the United States Government. Most security-minded people think Microsoft is likely spying for Microsoft's sales department, thus this does not seem likely, but this shows that our adversaries are paranoid as well.

Cyber-security infrastructure was faulted in GAO reports showing at least 50 government organizations are involved. This was the basis of President Bush's proposal to create a Cabinet-level Department of Homeland Security. Congress is still debating the need for this major restructuring of government.

An article in Computerworld recently reported "The National Association of State Chief Information Officers (NASCIO) today issued a report urging government leaders in all 50 states to set aside political differences and make cybersecurity and critical-infrastructure protection a top priority." [11]

Attacks on the Rise

Here we have an assortment of Internet news articles that collectively points in the direction that allow us to conclude that cyber attacks are constantly on the rise.

Over the past month, both in my major management consulting firm's e-mail system and in messages sent to a .mil account, I seem to be receiving an average of about one attempted virus delivery per day. This is triple the historic rate for the past two years. Fortunately, both sites keep their virus definitions up-to-date and all I actually ended up with was:

> *"File attachment: xxxxx.pif - The file attached to this email was removed because it was infected with the W32.Klez.H@mm virus."*

*"*Tech Pros agree the Cyberbomb is ready to go off" [12]. This is even more ominous because 47% of these network administrators of the corporations agreed and more than 45% said they were not prepared for such an attack.

The Knoxville Times reports that "Cyber Attacks are Real and Constant" because "Many groups around the world both envy and dislike the United States" which is hard to argue [13].

A recent survey of over 1000 subscribers to the soon-to-be-released CSO Magazine (Computer Security Officer), almost one half expect terrorists to launch a major strike through computer networks in the next 12 months.

Not long ago, a report issued by Riptech showed cyber attacks frequency had risen 64% over the last year [14]. "It's not just your imagination. They really are out to get you. While it's true that being a security manager these days requires a certain amount of paranoia, what you're seeing is real. Attacks on Internet-attached networks have increased substantially, and show no sign of abating."

Finally, a recent Internet report that "Cyber attacks were at an all-time high" [15] the digital risk-management company mi2g Ltd. says. This British firm which has tracked attacks since 1995 says it has spotted 9,011 overt digital attacks so far this month, a sharp increase from the 5,830 attacks spotted in August".

Certainly, having appeared on the exact date that this paper was written, it is a strong if not dubious indication that we are on the verge of a snowball effect, and we would be foolish not to expect this type of activity to continue and further increase – both frequency and sophistication – in the immediate future. All of these taken collectively show that there is a lot of attention currently being posted in the media about information security and the rapid increase of attacks.

Available Resources

Numerous companies and institutions exist that devote most – if not all – of their time to monitoring, tracking, assessing and reporting on cyber activity.

The Computer Emergency Response Team (CERT – http://www.cert.org) at Carnegie Mellon has long been a central "clearinghouse" for tracking reports of cyber attacks and malevolent Internet abuse.

The Internet Security Alliance (ISA – http://www.isalliance.org) is a superset of the CERT coordination center (CERT/CC), the Electronic Industries Association and other industry members whose "goal is to protect information systems for a safer business world".

The System Administration, Networking and Security Institute (SANS Institute –http://www.sans.org) is devoted to sharing lessons learned among these groups of computer experts, reports on network security alerts, provides education and consults with many government and private-sector corporations to provide all-encompassing and comprehensive reporting to security experts, the computer industry in general and the public at large. Also, the SANS Institute supports the http://www.incidents.org that allows everyone to share information about computer-related incidents, and protect themselves from new security threats. The "Internet Storm Center" (http://isc.incidents.org) also allows easy monitoring of currently 'popular' attacks and shows which ports are being probed on an almost real-time basis.

The Institute for Security Technology Studies at Dartmouth College (ISTS – http://ists.dartmouth.edu) is a center for counter-terrorism assessment and R&D. The ISTS is well known for their focus on cyber attacks.

The National Infrastructure Protection Center (http://www.nipc.gov) is a unit of the FBI dedicated to furthering the sharing of threats and vulnerabilities with government and private-sector companies.

Institute for the Advanced Study of Information Warfare (I A S I W - http://www.psycom.net/iwar.1.html) purpose "is to facilitate an understanding of information warfare with reference to both military and civilian life".

For government and military installations, "FedCIRC", "ASSIST" and "NavCIRT" are a few of the sites used as focal points for advance warning on all aspects of computer vulnerabilities, threats and assessments. If you work for a government or military group, consult your Information Systems Security Manager (ISSM), Network Security Manger (NSM) or other designated ISO or information security manager or officer for how to proceed and requirements for reporting incidents. The details will not be presented here, but you should

already know who these people are if you are working in the information security field for a government agency.

Obviously this is not an exhaustive catalog of cyberthreat-related sites, but collectively, these are adequate to give anyone looking for contemporary and timely information on cyber- and security-related information.

Conclusion

America and its allies are on the brink of the precipice – facing an almost certain abyss of cyberterrorism and Information Warfare that requires us to be eternally vigilant of all aspects of computer technologies, focus on information assurance and prepare us for the eventuality of a full-scale electronic attack on our infrastructure and financial assets. With no effective crystal ball it is impossible to foretell or determine precisely when the attack will come. It is a foregone conclusion among security professionals that it is simply a matter of time – almost a prophecy, rather than a prediction that this attack *will* come. Our single opportunity is to maintain the utmost collaboration and cooperation in an alliance of the public, private and government communities to frustrate and thwart every one of the attempts to launch such an attack.

Any breakdown or failure of this alliance will inevitably result in a chink in the armor that our enemies can and will exploit. Once the first shots of this new type of electronic combat are detected, we must continuously endeavor to minimize the effects and monitor all aspects of our computer-reliant society. Arguably, the first shots have already occurred.

People and the government must learn to balance liberties alongside security in the face of electronic terrorism. The general public will not willingly allow “Big Brother” any more than is absolutely required, but the government must be vigilant and observant of all aspects of daily life, especially where our vital infrastructure is vulnerable to terrorism. We have already become familiar with video monitoring – first in banks, now traffic control and accident monitoring, in high-crime areas and now even in facial profiling at major sporting events to attempt to catch criminals. Many cities already have similar systems in place.

There is a fine line between the defense and protection of our country and the privacy of its citizens, but the truth is that it grows thinner every day due to the constant evolution, progression and advancement of our technologies. This is both the new challenge and reality of life we face in the 21st century.

The goal of our enemy is to affect the psyche of our culture to the point we no longer rely on the basic everyday life to which we have become accustomed, causing panic among general public. It is obvious that a major blow in this area would have many widespread affects on our lifestyle and financial viability.

Therefore, it is our goal to diminish their capability and eliminate as many avenues of attack as possible. SCADA systems are a major weakness that could easily be exploited, and the payoff for terrorists would be very high while incurring minimum expense – due to the loose security that has traditionally been in place around these systems. Among other things, less connectivity between the Internet and the control of SCADA systems would reduce our vulnerabilities, and should be a major goal for the government in order to protect our way of life.

References – Alphabetical by Author

Arkin, William and Windrem, Robert. "The U.S.-China information war", undated.
http://www.msnbc.com/news/607031.asp

Erbschloe, Michael. Information Warfare – How to Survive Cyber Attacks. New York – McGraw-Hill Companies, 2001.

Giles, Lionel. "Sun Tzu on 'The Art of War'" translated from the Chinese, 1910.
http://all.net/books/tzu/tzu.html

Hulme, George V. "Report: Cyberattacks at an all-time high", 26-Sept-2002.
http://www.cnn.com/2002/TECH/biztech/09/26/techweb.cyberattacks/index.html

Kremmen, Julia. "Cyber attack threat is real and constant", 27-May-2002.
http://www.msnbc.com/local/knews/kns_1169305.asp

Lemos, Robert. "Tech pros: Cyberbomb's ready to go off", 25-July-2002.
http://zdnet.com.com/2100-1105-946231.html

Lemos, Robert. "What are the real risks of cyberterrorism?", 26-Aug-2002.
http://msnbc-zdnet.com.com/2100-1105-955293.html?type=pt&part=msnbc&tag=alert&form=feed&subj=cnetnews

Mosquera, Mary. "Cyberattacks Against U.S. Are A Matter Of Time", 7-Oct-1999.
http://www.techweb.com/wire/story/TWB19991007S0016

Prasad, Ravi Visvesvaraya. "Hack the Hackers", originally published in Hindustan Times, 19-Dec-2000.
http://rvp.tripod.com

Rash, Wayne. "Net attacks are on the rise… now what?", 15-July-2002.
http://zdnet.com.com/2100-1107-943792.html

Shein, Esther. "Are Companies Prepared for Cyberterrorism?", 1-Dec-2001.
http://cfomagazine.com/article/1,5309,5988||A|6|,00.html

Unattributed (Report from U.S. Embassy). "China's Internet 'Information Skirmish'", January 2000.
http://www.usembassy-china.org.cn/english/sandt/webwar.htm

Vatis, Michael A.; Bakos, George et al. "Cyber Attacks During The War On Terrorism: A Predictive Analysis", 22-Sept-2001.
http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf

Verton, Dan. "Report urges states to organize against cyberterror", 23-July-2002.
http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,72947,00.html

Wang, Xusheng; Su, Jinhai and Zhang, Hong. "China: Information Revolution, Defense Security", originally published in Beijing Jisuanji Shijie (China Computerworld), 11-Aug-1997.
http://www.infowar.com/mil_c4i/mil_c4i_121897a.html-ssi

References by Index Number

1) Erbschloe, Michael. Information Warfare – How to Survive Cyber Attacks. New York – McGraw-Hill, 2001

2) http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf

3) http://all.net/book/tzu/tzu.html

4) http://www.infowar.com/mil_c4i/mil_c4i_121897a.html-ssi

5) http://www.usembassy-china.org.cn/english/sandt/webwar.htm

6) http://rvp.tripod.com

7) http://www.msnbc.com/news/607031.asp

8) http://www.techweb.com/wire/story/TWB19991007S0016

9) http://cfomagazine.com/article/1,5309,5988||A|6|,00.html

10) http://msnbc-zdnet.com.com/2100-1105-955293.html?type=pt&part=msnbc&tag=alert&form=feed&subj=cnetnews

11) http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,72947,00.html

12) http://zdnet.com.com/2100-1105-946231.html

13) http://www.msnbc.com/local/knews/kns_1169305.asp

14) http://zdnet.com.com/2100-1107-943792.html

15) http://www.cnn.com/2002/TECH/biztech/09/26/techweb.cyberattacks/index.html

References for "Available Resources"

Computer Emergency Response Team (CERT), Carnegie Mellon, http://www.cert.org/

Incidents.org and the "Internet Storm Center", http://www.incidents.org, http://isc.incidents.org

Institute for Security Technology Studies (ISTS), Dartmouth, http://ists.dartmouth.edu/

Institute for the Advanced Study of Information Warfare (IASIW), http://www.psycom.net/iwar.1.html

Internet Security Alliance (ISA), http://www.isalliance.org

National Infrastructure Protection Center (NIPC), http://www.nipc.gov

System Administration, Networking and Security Institute (SANS), http://www.sans.org

Last Updated: October 19th, 2017

Upcoming SANS Training

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

SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Berlin 2017	OnlineDE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced