Global Information Assurance Certification Paper

W32/Goner.A Worm - Overview

James Avery

January 2, 2002

Abstract

The following paper explores and examines how the malicious Internet worm W32/Goner exploits Microsoft Windows, Microsoft Office and ICQ programs. I will discuss the characteristics and payload of the W32/Goner worm, how it exploits vulnerabilities, and propagated itself through the Internet via email, MIRC and ICQ. In addition I will also discuss and explain how to properly remove the Goner virus using guides and procedures provided by various information incident reporting agencies. Finally, I will discuss the Goner impact on worldwide computer economics, and security countermeasures that security professionals can utilize to help prevent the spread of mass email virus similar to the W32/Goner.A worm.

Introduction

With no clear-cut international laws that offer a uniform punishment of perpetrators who spread viruses, viruses have become lethal weapons for terrorist and a recreation playground for young hackers. In the case of the Goner it simply was script kiddies at it again, according to news reports from ITWORLD.COM. Four Israeli secondary-school students have admitted to creating the mass mailing Internet worm W32/Goner Worm alias (Goner, Gone.A, or Worm_Goner.A) that was discovered December 4, 2001. The four youths ages 15 and 16 admitted they created the worm as part of a competition with a rival group of hackers. According to experts the worm was written with the typical script kiddies seen in Web defacement use by many young inexperienced hackers.

Anti-virus software vendors initially classified Goner as a "high" threat because of its ability to disable a firewall and anti-virus and its fast spread throughout Europe and the United States. The Goner was originally speculated to surpass and wreak the same havoc as last year's infamous "Love Letter" worm, however that quickly dissipated mainly because of Anti-virus vendors actions and the speedy reporting of information by incident reporting agencies.[1,2,3,4,5]

Characteristic, Description and Propagation of W32/Goner

What kind of worm was W32/Goner? It is a malicious mass emailing worm that distributes itself as an email file attachment via Microsoft Outlook, Microsoft Windows, MIRC, and ICQ file transfers. The Goner arrives in a users email with the (Subject: Hi) with an attachment name "gone.scr" the worm masquerades itself as a screen saver to deliver its destructive payload. The Goner uses "Social Engineering" techniques as a way of spreading itself. The Goner utilizes "Social Engineering" as one way of spreading itself by arriving in a victim's inbox via Microsoft Outlook as an email sent from a friend or co-worker; it immediately tricks ordinary users into trusting the sender.

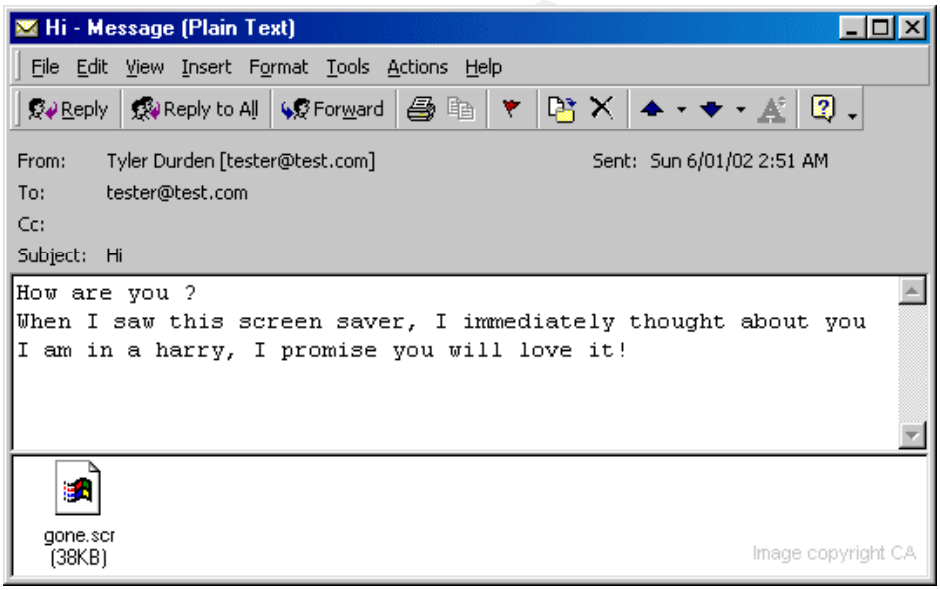
Most ordinary users are under the impression any mail received from a friend or co-worker is safe. Users believe their email is safe for two main reasons. The first, reason users believe their email is safe comes from trusting there friend or co-worker. User trust that a friend or co-worker would not send them a virus, harmful email or malicious code. Secondly the users believe that anti-virus software will catch any and every virus so they should be able to open any email without cautions or worry. With this type of user rationalization is one of the main reason why worms like the "Goner" and "I LOVEYOU" have the ability to spread so fast. If you have good "security countermeasures," sound email policy, and users education you can help prevent or slow the spread of mass email virus like the Goner. To better understand and make you more aware of the Goner virus its important that you understand some basic traits, characteristics and descriptions of how the virus works. I will provide a brief definition on some characteristic of the Goner worm because that's all needed, on other characteristic a more detail explanation is required for better understanding. [1,7,8,3]

- **Detection and date discovered:** (4 December 2001) This is the date the Goner worm was initially detected by anti-virus corporation and various information incident reporting agencies detected discovered and reported the W32 Goner worm on 4 December 2001.
- **Email:** Arrives in email with the subject "Hi" with the attachment of (gone.scr).
- **MIRC and ICQ**: Installs a backdoor through scripts contained in the dropped REMOTE32.INI file instruction are inserted to user's MIRC file to load REMOTE32.INI file.
- **Payload 1:** (Delete files) This is the condition that causes the virus to activate or drop its destructive payload. Some viruses trigger their payloads on a certain date. Others might trigger their payload based on the execution of certain programs or the availability of an Internet connection the Goner had two payloads one that deleted files and the other that displayed a message.
- **Payload 2**: (Displays a message) On the Goner virus the second payload is the hackers
  Calling card.
- **Trigger Condition:** This is to indicate the condition or date on which the virus' payload will be triggered. Please note that date-activated viruses may infect your computer 365 days a year. These viruses prior to the date specified may infect your computer.
- **Infection Length:** (38.912 bytes) this is the size, in bytes, of the viral code that is inserted into a program by the virus. If this is a worm or Trojan horse the length represents the size of the file.
- **Created in**: Visual Basic 6 compressed using Portable Executable (PE) packer total size
  Approximately 159KB. The language used by the hacker to create the Goner worm.
- **Platforms effected**: Windows 95/98, Windows NT/2000/XP, Microsoft Outlook. These are the types of computer programs effected by Goner worm.
- **Threat Assessment**: (Wild-High) - The wild component measures the extent to

which a virus is already spreading among computer users. This measurement includes the number of independent sites infected, the number of computers infected, the geographic distribution of infection, the ability of current technology to combat the threat, and the complexity of the virus. Because Goner initial spread was so fast across Europe and the United States it was given the threat assessment of high.
(Damage-Medium) - The damage component measures the amount of harm that a given threat might inflict. This measurement includes triggered events, clogging email servers, deleting or modifying files, releasing confidential information, performance degradation, errors in the virus code, compromising security settings, and ease by which the damage might be fixed. Goner was given medium damage because its ability to degrade security countermeasures such as firewalls, and anti-virus software applications.
(Distribution-High) - This component measures how quickly a threat is able to spread itself.[1,7,8,9]

Email Propagation

The mass-mailing worm arrives via email as an attachment GONE.SCR. The worm then creates and Outlook Application Object, and uses MAPI script commands to create and send bogus emails to all recipients found in the infected user's address book. Thereafter, it deletes the bogus emails. The worm arrives in an outlook email with in the following format.[8]



Payload 1

After Goner worm has been received via a users Microsoft Outlook mailbox it attempts to infect other users by sending itself to all infected users address book. After the Goner completes the task of trying to infect other users via the address book the worm

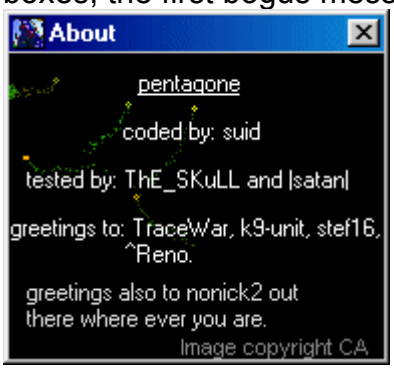
delivers its initial destructive payload of destructive code, in which the Goner, destroys all running process in memory. It terminates from memory any running process associated with the following filenames: [6,8,10]

- Aplica32.exe
- Avconsol.exe
- Avp.exe
- Avp32.exe
- Avpcc.exe
- Avpm.exe
- Cfiadmin.exe
- Cfiaudit.exe
- Cfinet32.exe
- Esafe.exe
- Frw.exe
- Icload95.exe
- Icloadnt.exe
- Icmon.exe
- Icsupp95.exe
- Icsuppnt.exe
- Lockdown2000.exe
- Navapw32.exe
- Navw32.exe
- Pcfwallicon.exe
- Safeweb.exe
- Tds2-98.exe
- Tds2-Nt.exe
- Vsecomr.exe
- Vshwin32.exe
- Vsstat.exe
- Webscanx.exe
- Zonealarm.exe
- _Avp32.exe
- _Avpcc.exe
- _Avpm.exe

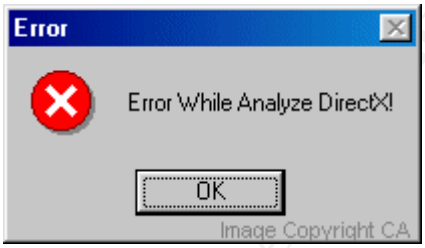
For all the running process W32/Goner fails to delete from memory, it creates a file called WININIT.INI in which deletes the remaining process files upon reboot of your computer. Furthermore if the folder called c:\\SAFEWEB is found the worm will delete all the files it contains.[7,8, 9] Once these critical system files, and security countermeasure files that control your firewall and anti-virus software applications have been deleted; the Goner worm has the ability to go without being detected in your computer it then delivers its second and final payload. [7,8, 9]

Payload 2

Upon execution Goner delivers payload 2 the (hackers calling card). At the second payload user interface is required to trigger the worm, at this point the worm uses it social engineering ability to trick infected users to execute a safe attachment sent by a friend or co-worker. The second payload is triggered immediately upon double clicking on the email attachment. Once executed the second payload is delivered by using Portable Executable (PE) packer, which is the nothing more than the screen saver (.scr) that's packed using the UPX packer program and its compiled using visual basic this is the attachment used to execute, spread and infect your systems and other networks. Once the worm executes payload two it then displays two bogus message boxes, the first bogus message box displays the following information: [8]



Once the first display message is received the Goner performs a quick worm routine and quickly displays its second bogus message box. Once this bogus message box is seen the worm drops a copy of its worm file into a registry and infects your computer by editing its auto-execute. The bogus message box and the copy of the files its drops are the following: [1,8,9]



C:\%SYSTEM%\gone.scr C:\%SYSTEM%\gone.scr

To the registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Once the registry key has been edited in your computer with the worms infected code upon every re-boot the auto-execute will be copied with the worm's infected code. The worm will basically remain active inside your network not being detective or removed until you manually remove it from your registry, which we will discuss later. The main

window of the worm bears the name "pentagone." On windows 9x, it registers itself as a service process not visible on the Task List. Despite its invisibility on the Task List, the Outlook Application Object that it opens is visible of the Task List. [8]

MIRC Propagation

Once it locates those files the Goner installs a backdoor script contained in the dropped REMOTE32.INI file. The Goner then inserts instructions into the user's MIRC.INI file to load a dropped REMOTE32.INI. The worm author can then utilize this worm extension to start Denial of Service (DoS) attacks on IRC channels, servers and users connected to the same IRC channel as the infected user. Clone users with random names, are created by the worm to achieve this. [7,8]

ICQ Propagation

Another stealthy way the Goner worm attempts to infect computer systems by finding the ICQMAPI.DLL dynamic link library, which is used to access ICQ applications. Once the Goner worm finds the ICQMAPI.DLL file from the C:\Program Files\ICQ it copies that file to the %System%. Once the file is the copied the worm has the ability to send itself out via online users contact list to other online ICQ users infecting there computer system files via ICQ. [8]
ICQ is a favorite service among hackers, there are many built in Trojans that hackers can use to cause damage once you have been infected. Some of the security risk associated with ICQ includes spoofing, sniffing, spanning, and imposturing. It's a good security practice to not allow ICQ chat because it posses such great security risk most business organizations do not allow ICQ chat service in there environment. [7,8]

Removal of the Goner Worm

Virus removal and cleanup is the most important part of handling a virus. Lets face it virus are becoming more complex and rapid than ever before because of the evil doers on the internet, therefore its essential that security professional be proficient in virus removal and clean-up. There are several ways you can remove a virus depending on the type of anti-virus software you are running some anti-virus software programs provide patches for auto removal of viruses. My personal choice however calls for manual removal of a virus rather than auto removal. Because the Goner had the ability to disable security countermeasures such as firewalls and anti-virus software, I would highly recommend re-installing both firewall and anti-virus software as an extra precaution. Below are the manual steps and procedures for removal of the Goner virus provided by McAfee anti-virus Software Company.
http://vil.mcafee.com/dispVirus.asp?virus_k=99272& [11]

WINDOWS 95/98/ME [7,8,9,10]

- Restart Windows in Safe Mode (reboot your computer, just before the large WINDOWS startup screen comes up, hit the F5 key). You can recognize that you're in Safe Mode by the text Safe Mode in the 4 corners of the desktop.
- Click START | RUN, type COMMAND and hit ENTER
- Type CD %WINDIR%\SYSTEM and hit ENTER
- Type ATTRIB -h -s -r GONE.SCR and hit ENTER
  (if File not found is returned then the virus is not active and you do not need to proceed with these instructions)
- Type DEL GONE.SCR and hit ENTER
- Click START | RUN, type REGEDIT and hit ENTER
- Click the (+) next to HKEY_LOCAL_MACHINE
- Click the (+) next to SOFTWARE
- Click the (+) next to MICROSOFT
- Click the (+) next to WINDOWS
- Click the (+) next to CURRENTVERSION
- Click RUN
- Click on C:\WINDOWS\SYSTEM\gone.scr in the DATA section on the right and hit DELETE on the keyboard
- Click START | FIND | Files or Folders
- Type REMOTE32.INI and hit ENTER
- Delete REMOTE32.INI
- Restart the computer

WINDOWS NT/2000/XP [7,8,9,10]

- Type CTRL-ALT-DEL at the same time
- Choose TASK MANAGER and then choose the PROCESS tab
- Locate the GONE.SCR process, click it, and choose END PROCESS
  (if you can't find the process, then the virus is not active and you do not need to proceed with these instructions)
- Click START | RUN, type CMD and hit ENTER
- Type CD %WINDIR%\SYSTEM32 and hit ENTER
- Type ATTRIB -h -s -r GONE.SCR and hit ENTER
- Type DEL GONE.SCR and hit ENTER
- Click START | RUN, type REGEDIT and hit ENTER
- Click the (+) next to HKEY_LOCAL_MACHINE
- Click the (+) next to SOFTWARE
- Click the (+) next to MICROSOFT
- Click the (+) next to WINDOWS
- Click the (+) next to CURRENTVERSION
- Click RUN
- Click on C:\WINNT\SYSTEM32\gone.scr in the DATA section on the right and hit

DELETE on the keyboard
- Click START | FIND | Files or Folders ...
- Type REMOTE32.INI and hit ENTER
- Delete REMOTE32.INI
- Restart the computer

Goner Worldwide Computer Economic Impact

The Goner e-mail worm was originally dubbed to supersede the 100 billion dollars in damage the "I Love You" virus caused however Goner never reached its "high" threat potential of destruction and the didn't even come close to the type damage " I Love You" caused. The Goner wasn't afforded the opportunity to inflict as much damage as the "I Love You" virus mainly because experts were quick to respond and they had dealt with similar viruses, and network security countermeasures were more secure in handling mass email type worms. Nevertheless, the Goner estimated worldwide economic impact reach about 5 million, most from cleanup costs for organizations that did not have updated anti-virus software, according to a statement on the Computer Economics Web site. Only 10 percent of the amount are for loss in productivity. About 800,000 computers worldwide received the Goner worm, but only a few systems were infected because anti-virus software vendors pushed virus-definition updates to their customers before Goner was able to spread and cause mass productivity loss. [11]

Security Countermeasures to help Prevent Goner Worm

Although there is no definite way to stop a virus there are some additional "security countermeasures" one can put in place to help prevent the worm from spreading. Below are a few suggested security countermeasures to help prevent the Goner worms from spreading.

- "User awareness" Train and educate users to be aware of the various types of mass emailing worms like the Goner. Put email policy in place to ensure user only open files attachments that they know the exact purpose of, regardless if they recognize the sender as a co-worker or friend. Teach users email countermeasures such as not opening suspicious files or attachments and to immediately alert security professional if they suspect any email that may have foul play. Make the users feel part of your security team by showing different ways they can help stop a virus from spreading via social engineering. Take the time out and show the users some various file extensions and the file they should this can really be productive especially if it's an Administrative environment. Explain to your users how anti-virus software applications work against viruses. Get your users involved, so they began to think and act security; you will be surprised how they will begin taking the proactive steps in opening only emails they know the exact purpose.

- Write and enforce security policy on the prevention of ICQ/IRC chat in a

professional environment. Most organization don't allow this usage in there environment and rightfully shouldn't, however there is always a organization that insist on having ICQ/IRC. If you happen to be the security professional, for the organization that insist on having ICQ/IRC, go over the risk analysis and threat with management in order to discourage them from usage of ICQ/IRC.

- Constantly update your anti-virus software and ensure security patches on Microsoft Outlook and Outlook Express are updated. Although most anti-virus release virus updates after a virus has already infected many Security Experts fail to do virus updates. The economic impact of the Goner itself reached 5 million mainly because organizations didn't have updated anti-virus software.

- Install worm programs that's primary design to catch worms, and prevent DoS. TruSecure by Symantec http://www.trusecure.com/, TruSecure is one of the better products in preventing mass email worms like Goner from infecting and spreading. It's a highly recommended product by various security experts, if your organization has the budget, add this product as an additional security countermeasure.

- Disable email scripting in Microsoft Outlook mail, This will avoid email scripting which can open vulnerabilities just by reading email. To disabling go to Internet Explores properties.

- Since Goner was written using Visual Basic a good security countermeasure would be to remove the Visual Basic Script file extension, this would prevent the worm from spreading. To ensure .vbs extension is registered Go to "My Computer" under the view menu click on folder options and remove the .vbs extension.

Conclusion

The Goner mass email worm was written by four teens from Israeli as part of a competition with a rival group of hackers. The Goner had the ability to disable security countermeasures by disabling anti-virus and firewall software applications the worm also could propagate via ICQ and MIRC. The goner worm code was written in Visual Basic Script (VBS) and masqueraded itself via Microsoft Outlook mail as a screensaver file. What most articles want tell you about the Goner worm is that even though this type of virus has been seen before users are still falling prey to double-clicking any attachment sent to them via email. A virus ability to spread via social engineering continues to be an extremely effective way for hackers to create viruses. As security professional we must continue to educate our users on mass email attacks and there exploits to prevent hackers from these type attacks. In the end justice prevail the four hackers attempted to conceal their identities by using the nicknames "SUID," "The Skull" and "Satan" in the pop-up window that displayed when Goner infects a system

were caught by a DALnet investigation team. The DALnet investigators found "SUID" nickname and Internet protocol (IP) address in a registry on the service. The four teens are currently confined and could face up to five years prison based on Israeli computer crimes.

References

1. Symantec Antivirus Corp.
   "Symantec Security Response W32.Goner.A"
   URL:http://www.symantec.com/avcenter/venc/data/w32.goner.a@mm.html
   (4 December 2001)

2. News Factor Network
   "Goner Worm Takes Out Firewall, Antivirus
   http://www.newsfactor.com/perl/story/15117.html.
   (5 December 2001)

3. ZDNET UK
   "HELP & HowTo: Goner"
   http://news.zdnet.co.uk/story/0,,t269-s2100431,00.html
   (5 December 2001)

4. ZDNET UK
   "Goner Proves Social Viruses Still A Threat"
   http://news.zdnet.co.uk/story/0,,t269-s2100431,00.html
   (5 December 2001)

5. ITWORLD.COM
   "Report: Isreaeli youths admit to creating 'Goner' worm
   URL: http://www.itworld.com/Sec/3832/IDG011210goner/
   (12 December 2001)

6. Computer Associates Virus Information Center
   "Win32.Goner.A"
   URL: http://www.e.ca.com/Virus/Virus.asp?ID=10599
   (17 December 2001)

7. Panda Software
   "W32/Goner.A"
   URL: http://www.ntsecurity.net/Panda/Index.cfm?FuseAction=Virus&VirusID=1124
   (4 December 2001)

8. Pc-cillin.com - Virus Info

"Worm_Gone.A"
URL: http://www.antivirus.com/pc-cillin/vinfo/virusencyclco/default5.asp?Vname=WORM_G
(4 December 2001)

9. Cert Coordination Center
"Cert Incident Note IN-2001-15"
URL: http://www.cert.org/incident_notes/IN-2001-15.html
(4 December 2001)

10. McAfee Anti-virus
"McAfee - Virus Information Library"
URL: http://vil.mcafee.com/dispVirus.asp?virus_k=99272&
(5 December 2001)

11. ITWORLD.COM
"Report: "Goner worm causes limited economic damage
URL:http://www.itworld.com/See/3832/IDG011207goner/
(7 December 2001)

12. VirusList.Com
"Goner Culprits Brought to Justice"
URL: http://www.viruslist.com/eng/default.asp?tnews=11&nview=1&id=1268
(19 December 2001)

13. Northcutt, Stephen and Novak, Judy.
Network Intrusion Detection An Analyst's Handbook, Second Edition.
Indianapolis, Indiana, New Riders, September 2000.

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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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
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 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
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
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
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 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