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.

Case Study: The Get Connected CD

To protect the Indiana University network and student computers in the residence halls, we prevent new computers from connecting to the network before running our "Get Connected" CD-ROM. The CD installs software and changes settings that help protect computers from threats. Largely as a result of this effort, we experienced a 45% decrease in security incidents in fall 2004 compared to the previous year, and we concluded that the project was a great success. Therefore, we have recommended that the project be continued i...

Copyright SANS Institute
Author Retains Full Rights

AD

Case Study: The Get Connected CD

GIAC Security Essentials (GSEC) Practical Assignment Version 1.4c
Option 2 – Case Study in Information Security

David A. Greenberg
20 December 2004

Paper Abstract:

To protect the Indiana University network and student computers in the residence halls, we prevent new computers from connecting to the network before running our "Get Connected" CD-ROM. The CD installs software and changes settings that help protect computers from threats. Largely as a result of this effort, we experienced a 45% decrease in security incidents in fall 2004 compared to the previous year, and we concluded that the project was a great success. Therefore, we have recommended that the project be continued in the future and that certain enhancements, including additional reporting and improving script logic, be made.

© SANS Institute 2005, Author retains full rights.

Table of Contents

Table of Contents 2
Abstract 3
The Problem 3
Developing a Solution 4
  Preventing Network Access 6
  The Get Connected CD 6
    Determine Operating System Version 7
    Check Service Pack level 7
    Install Hotfixes 7
    Enable Automatic Updates 7
    Disable unnecessary services 8
    Enable the Internet Connection Firewall 8
    Set IPSec rules 8
    Perform Registry and Local Policy changes 8
    Enable Security auditing 9
    Install anti-virus software 9
    Install additional software 9
  Install ITNow Client 10
  Register the user and computer with the DHCP Server 10
Deploying the Get Connected CD 11
The Aftermath 13
The Future of the Get Connected CD 15
References 17
Appendix A – Get Connected CD Local Security Policy 19

© SANS Institute 2005, Author retains full rights.

Abstract

To protect the Indiana University network and student computers in the residence halls, we prevent new computers from connecting to the network before running our "Get Connected" CD-ROM. The CD installs software and changes settings that help protect computers from threats. Largely as a result of this effort, we experienced a 45% decrease in security incidents in fall 2004 compared to the previous year, and we concluded that the project was a great success. Therefore, we have recommended that the project be continued in the future and that certain enhancements, including additional reporting and improving script logic, be made.

The Problem

Every fall students move back into residence halls, and most bring with them a personal computer. These same students are responsible for administering and protecting their computers from attack. Unfortunately, in years past, students have not kept their computers patched and protected from other infected systems. The result was a large number of compromised computers in the Residence Halls.

Experience led us to believe that student computers are generally behind on patches, using out of date virus patterns, and often already infected when they are brought to the University. For a computer that is already compromised, bringing the computer to the University provides the computer with a fast network connection and allows the infection to spread faster. When you combine compromised computers with un-patched, out of date computers on the same network, the result is a mass infection of student-owned and operated computers.

The influx of poorly managed student-owned computers to the Indiana University network each fall presents a risk to the University. In our SANS Track 1 Security Essentials class, we discussed that the risk due to a threat is the probability of a threat occurring multiplied by the vulnerability to the threat.[1] Preventing malicious people from attacking these computers before the attack happens is unfeasible, considering the large number of internet users that we have no control over, so we need to focus on the vulnerability side of the equation and what we can do to the student computers. By focusing on eliminating the vulnerabilities on student computers, we lower the overall risk to the University.

At Indiana University, an example problem we experienced is the W32.Blaster worm[2]. When W32.Blaster hit the University, approximately 150 student-owned

---

[1] SANS Institute. Track 1 – SANS Security Essentials. Volume 1.2. SANS Press, Jan 2004.

[2] "MS Blast / Blaster Worm Propagation." Indiana University Information Technology Security Office. 2003. Office of the Vice President for Information

© SANS Institute 2005 Author retains full rights.

computers were infected in the first day. Detecting the infected machines, notifying the students, and having them clean the infections or rebuild their computers instantly became a priority for all of the computer support units at the University. Including faculty and staff computers on all eight Indiana University campuses, there were over 700 infected computers in the first day. The infection was spreading so fast that unpatched or unprotected computers were getting infected with Blaster within seconds of being attached to the network.

For fall 2004, one of the Internet worms that the Information Technology Security Office was worried about was the W32.Sasser.Worm[3] [4], and the possibility that it could have a similar impact on the University as the Blaster worm. Simply put, the Sasser worm looks for Windows 2000 and XP computers that have not applied the patch described in Microsoft Bulletin MS04-011[5], infects them, and the newly infected computers begin scanning for more vulnerable computers to infect.

Developing a Solution

A team was assembled with the goal of finding a way to secure these personal computers when they were brought to campus. This team included programmers, domain administrators, security office personnel including me, support center staff, and DHCP and DNS administrators. As we had seen with the W32.Blaster incident, once the student is able to use the computer on the network, maintaining the computer is not a priority. It became apparent to us that, unless we force the students to take basic preventative measures before connecting to the network, they may never protect their computers. Before allowing these computers on the network, the team wanted to ensure that the computers had the latest operating system patches and that antivirus software was installed and using current detection patterns. This would both fix the vulnerabilities and detect malicious software. Ideally, the team would put some mechanism in place to ensure that these protection measures continue to happen as long as these computers remain on the University network.

Technology. Indiana University. 8 Aug 2003 <https://itso.iu.edu/bulletins/ITSO.2003.08.12.blaster>

[3] Nakayama, Takayoshi and Ladley, Fergal. "W32.Sasser.Worm." Symantec Security Response. 2004. Symantec Corporation. 27 Jul 2004 <http://www.sarc.com/avcenter/venc/data/w32.sasser.worm.html>

[4] "Several Critical Microsoft Vulnerabilities." Indiana University Information Technology Security Office. 2004. Office of the Vice President for Information Technology. Indiana University. 20 May 2004 <https://itso.iu.edu/bulletins/ITSO.2004.05.20.ms04-011>

[5] "Microsoft Security Bulletin MS04-011" Microsoft Technet. 2004. Microsoft. 10 Aug 2004 <http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx>

© SANS Institute 2005 Author retains full rights.

A large majority of student computers runs a version of the Microsoft Windows operating system, and we chose to focus on securing these computers. This is not to say that other computers do not need to be protected. But, we wanted to secure the largest number of computers possible with the least amount of effort. Indiana University strongly discourages the use of any Microsoft Windows operating system other than Microsoft Windows 2000 and Microsoft Windows XP.[6] This decision was made primarily for security reasons and because Indiana University has a license to resell Microsoft Windows XP to students at a small fraction of the retail price. For these reasons, we focused primarily on Windows 2000 and Windows XP.

Ideally, any new computer on the network would be prevented from communicating with other computers until it can be determined that it is not a threat to the network and that basic security measures have been performed. While commercial products exist that have these functions built into them, the team did not have the time to evaluate these products thoroughly nor the budget to purchase one in the necessary time frame. Therefore, we chose to solve the problem in software, which meant students would have to run a program before getting on the network.

Indiana University Residence Halls have an Ethernet wiring scheme[7] that differs from the current Ethernet standard and requires Indiana University to distribute "IU Ethernet Cables." This wiring scheme was developed in 1988. At that time, it was thought that data and voice would share the same cable. Because all the wiring at IU used USOC termination[8], which meant that pin 1 was used for grounding, an alternate cable was created that converted network communication to the Ethernet standard. These network cables became known as "IU Ethernet Cables." Since these special network cables need to be distributed to students anyway, we created a CD-ROM to distribute to the students and bundled it with their IU Ethernet Cable. This CD would contain software that would ensure the student's computer is secure enough to get on the network.

This CD would be used by a large number of students of varying computer knowledge. Our goal was to make using these CD-ROMs should be as easy as possible for the students, thereby keeping the volume of support calls low.

---

[6] "For Windows computers on the IU network, why does UITS recommend Windows 2000 or XP Professional?" Indiana University Knowledge Base. 2004. Indiana University. 9 Nov 2004 <http://kb.indiana.edu/data/aloz.html>

[7] "IU Network Cable Wiring Scheme." Indiana University Telecommunications Web Site. 1999. University Information Technology Services, Indiana University. 10 Jun 1999 <http://www.indiana.edu/~uits/telecom/data/images/wiringscheme.gif>

[8] "Registered Jack." Wikipedia. 2004. Wikipedia. 24 Nov 2004 <http://en.wikipedia.org/wiki/Registered_jack>

© SANS Institute 2005 Author retains full rights.

Additionally, students should be able to insert the CD-ROM in their computers and have the CD-ROM work with little or no interaction.

Preventing Network Access

Next, we needed a way to prevent computers from connecting to the network before we have had a chance to secure it. If we gave student computers a public IP address before they had been patched and protected, many students would not worry about securing their computers since they would be able to do everything they desire already. The method we chose was MAC address registration. When a new network device requests an IP address from the DHCP server, the DHCP server checks to see if the MAC address exists in a table associating it with an Indiana University network ID, also known as a user account. If the MAC address is not already in the table, the student must authenticate using his account and verify that he is the primary user of the computer. This process associates the computer's MAC address with the user of the computer. This also provides a means of identifying new computers and preventing them from getting on the public network.

To ensure that all computers brought into the Residence Halls go through our registration process, all previously registered MAC address registrations from subnets in the Residence Halls are removed from the database. We also configured the DHCP server to only allow registration of computers from Residence Hall subnets when registration is attempted by the process initiated by the CD. If a student attempts to register a computer without using this script, she is presented a web page instructing her to obtain and run a University provided CD before she will be allowed on the network. We configured the Indiana University DHCP Server to give each unregistered computer a private IP address (RFC 1918[9]) to prevent any infection from spreading beyond the compromised computer's own broadcast domain. This has the effect of keeping unregistered infected computers somewhat isolated. While this does not completely prevent the spread of a worm, it does limit the damage that a worm can do to the local broadcast domain instead of the entire world and buys us more time to protect other computers.

The Get Connected CD

The CD itself is a collection of scripts, shortcuts, Windows hotfixes, and Service Packs, along with some software that Indiana University is allowed to distribute to students. The CD is designed to be a self-contained unit. All the software that the CD uses is contained on the CD. This allows students to use the CD before they have connected to the network and after being blocked from the network.

The CD performs the following tasks, which I will discuss in detail:

---

[9] Rekhter, et al. "Address Allocation for Private Internets." Internet Engineering Task Force Request for Comments. 1996. Internet Engineering Task Force. Feb 1996 <http://www.ietf.org/rfc/rfc1918.txt?number=1918>

© SANS Institute 2005 Author retains full rights.

- Determine operating system version
- Check Service Pack level and install if necessary
- Install Hotfixes
- Enable Automatic Updates
- Disable unnecessary services
- Enable the Internet Connection Firewall
- Set IPSec rules
- Perform Registry and Local Policy changes
- Enable security auditing
- Install anti-virus software
- Install IU licensed software
- Install ITNow client
- Register the user and computer with the DHCP server

Determine Operating System Version

The first thing the CD does after being inserted is determine the operating system version. If the operating system is not Windows 2000 or Windows XP, the CD presents a message telling the user that the CD was only designed for these operating systems, and gives the user a telephone number for computer support.

Check Service Pack level

After the CD verifies the operating system version, it checks for the installation of the latest Windows 2000 or Windows XP Service Pack at the time of the CD printing. This was Windows 2000 Service Pack 4 and Windows XP Service Pack 1. If the appropriate Service Pack is not present, the CD installs the Service Pack and reboots the computer.

Install Hotfixes

Microsoft has released numerous updates since the most recent Service Pack for each operating system. Upon successful installation of the Service Pack, the CD installs all of the hotfixes that were available at the time of CD printing. All of the hotfix executable files are included on the CD. Installation was scripted to include the use of qchain.exe,[10] so only one reboot was required to finish the installation of multiple hotfixes.

Enable Automatic Updates

After all of the available hotfixes have been applied, the CD turns on Automatic Updates to ensure that the computer will receive any future Microsoft updates. It also configures updates to be installed between 5pm and 10pm. In Windows XP before Service Pack 2, if the computer was not on during the scheduled install

[10] "How to install multiple Windows updates or hotfixes with only one reboot." Microsoft Help and Support. 2004. Microsoft. 23 Nov 2004 <http://support.microsoft.com/kb/296861>

© SANS Institute 2005 Author retains full rights.

time, the updates are not installed. We think that students are most likely to have their computers on in the evening and that selecting these times would give us the best chance of having the updates installed.

Disable unnecessary services

Next, the CD reduces the attack surface of the computer by disabling a number of unnecessary services for the Indiana University network environment, including Universal Plug and Play, SSDP Discovery Service, Messenger, Telnet, and the Computer Browser Service. Universal Plug and Play, SSDP Discovery Service and the Messenger service have recently been exploited by Internet worms. The average student computer user has no need for these services, so we disable them by default. The Telnet service goes unused by nearly all student users of Windows XP and is disabled. The Computer Browser service is disabled because it is no longer needed in the Indiana University network for connecting to other computers. This service has been replaced by the WINS and DNS services.

Enable the Internet Connection Firewall

After reducing the attack surface of the computer, the CD enables the Internet Connection Firewall in Windows XP to protect the computer from unsolicited network communication. We did not configure any exceptions in the firewall, but students can add them manually if needed. Since the firewall allows connections initiated by the student computer, most everyday computer activities (e.g., web surfing, connecting to a file or print server, reading e-mail) are not restricted by the activation of the firewall.

Set IPSec rules

As an additional measure of protection, and because the Internet Connection Firewall is not available on Windows 2000, the CD sets IPSec rules to prevent RPC connections from computers external to the University. Anyone who has a legitimate need to connect to the RPC service on a student's computer can still create a virtual private network (VPN)[11] connection to Indiana University and connect to the RPC service through the VPN tunnel.

Perform Registry and Local Policy changes

Next, the CD sets a number of Windows registry and policy settings on the student's computer. The Windows Security section of the SANS Security Essentials course called my attention to many security settings that we later used on the Get Connected CD. For example, the Windows Security section of Track 1, suggested that only Kerberos or NTLMv2 authentication be allowed.[12] The Windows Security boot camp session demonstrated that weak passwords, which

---

[11] "The basics of VPN at IU." Indiana University Knowledge Base. 2004. Indiana University. 3 Sep 2004 <http://kb.indiana.edu/data/ajrq.html>

[12] SANS Institute. Track 1 – SANS Security Essentials. Volume 1.5. SANS Press, Jan 2004.

© SANS Institute 2005 Author retains full rights.

were encrypted using older technology, could be cracked in a matter of minutes. See Appendix A for a complete listing of these settings.

Enable Security auditing

All of the changes we have discussed so far are to prevent compromise of the computer. But when the computer *is* attacked, the student needs a record of the events. Therefore, the CD enables security auditing for the following types of events: account logon events, account management, logon events, object access, and system events. Both success and failures are logged for these events to make it easier to see when unauthorized access is being attempted and when access is successful. Only successful policy changes are logged so the user of the computer is not alerted when an attacker unsuccessfully attempts to make policy changes. In contrast, only failures are logged for privilege use. This setting logs when users attempt actions on the computer for which they do not have authorization. We felt that logging successful privilege use would generate so many events in the event log that it would cause the log to be nearly useless. When too much information is recorded, it becomes difficult to separate useful information from meaningless log information. The settings we chose for logging reflect the need to have detailed logs but keep the logs small enough to be useful and readable.

Install anti-virus software

Viruses can sometimes penetrate our defenses, or a student may be tricked into running a malicious program. In case this happens, we made installation of Symantec AntiVirus part of the CD. Indiana University has a site license for Symantec AntiVirus Corporate Edition and is able to include the software at no additional cost. During the installation process, the students are asked if they have antivirus software installed already. If they answer yes, they are informed of their responsibility to keep their anti-virus definitions up-to-date. If they indicate that they do not already have anti-virus software, they are warned that installing multiple instances of antivirus software could be detrimental to their computers. When more than one antivirus product is installed on a computer, they both scan files for infection when they are accessed. If the antivirus software considers a scan of a file by the other antivirus software as an access, the result is an endless loop of virus scanning that can slow a computer to a crawl. For students that have no anti-virus software, the IU licensed Symantec AntiVirus is installed with updated virus definition files from the time of CD printing.

Install additional software

We also used the CD to install additional software as a convenience for the students and University support units. The additional software installed includes Spybot Search & Destroy, Lavasoft Ad-Aware, a network file system logon icon, and a Residence Hall printer locator script. Spybot Search & Destroy and Lavasoft Ad-Aware are programs designed to search the computer for spyware, adware, tracking cookies, and any other software that has been identified by the

© SANS Institute 2005 Author retains full rights.

software vendor as possibly malicious[13]. Students are left to configure and run the programs on their own, but we hope that by getting the software on their computers, the students will be more likely to use it. The network file system logon and printer locator script are Indiana University specific scripts that are placed on the computer for the student's convenience. The network file storage provides a network location for the student to place important files. The printer locator script connects to the printer that is nearest the student's location based on their computer's current IP address. These are just a few examples of how the CD can be used to conveniently install software that is not directly related to security.

Install ITNow Client

In addition to securing student computers, we realized that the CD could provide us with useful statistics that could help us better support our customers. Members of the team created a reporting utility, called ITNow,[14] that records basic information about the computer and sends that information to a database. The data collected[15] includes the operating system version, service pack level, installed hotfixes, and information about the computer's hardware configuration. Anyone who uses the CD is informed that this application is installed through an end user license agreement (EULA). The ITNow client also provides information to the user of the computer about system outages and problems. For example, if a mail server is experiencing a problem, an announcement would be made through the ITNow client. Anyone running the client will see the notice from a system tray icon and the notice can be clicked for more information.

Register the user and computer with the DHCP Server

The last step performed by the CD is to open the default web browser and point the user to Indiana University's DHCP registration web page. The CD encrypts a string of text using uniquely identifiable characteristics of the computer as a key and submits that to the registration web page as an HTTP parameter. The web server receives the encrypted string of text and decrypts the string. If the string is decrypted successfully, the web server registers the MAC address with the DHCP Server and the web server displays a web page telling the user to reboot to get their public IP address. If the encoded string is not present, or if it is not decoded properly, the computer user is presented a web page with instructions on how to run the CD and register with the DHCP Server.

---

[13] "Threat Assessment Chart." Lavasoft Threat Assessment Chart (TAC). 2004. Lavasoft. Dec 2004 <http://www.lavasoftnews.com/ms/tac_main.shtml>
[14] "What is ITNow, and why should I use it?" Indiana University Knowledge Base. 2004. Indiana University. 2 Sep 2004 <http://kb.iu.edu/data/aomc.html>
[15] "In ITNow, what information is gathered about my computer?" Indiana University Knowledge Base. 2004. Indiana University. 25 Oct 2004 <http://kb.iu.edu/data/apak.html>

© SANS Institute 2005 Author retains full rights.

If the user agent string seen by the DHCP server is not of the Windows variety, the user is allowed to register without having the encrypted key. While a particularly savvy user can figure this out and bypass our registration process, we feel that this was difficult enough that average user would just use the CD instead of attempting to circumvent the process. Even if someone does circumvent the process, it would most likely be short-lived. If students do bypass our registration, there is a good chance that they did not protect their computer as well as the Get Connected CD can. If they become infected, we will notice them through our IDS, log reports, flow reports, or by external complaints. Our Information Technology Policy Office will then block the infected computer's network access until it is reformatted and the student runs the Get Connected CD. Since we have these other means of detecting compromised computers we rely on them instead of going to great lengths to force everyone through the registration mechanism.

Deploying the Get Connected CD

The steps outlined to this point would prevent infection by most worms currently circulating, including the previously mentioned Sasser worm. This is accomplished though the installation of the MS04-011 patch, enabling the Internet Connection Firewall (ICF), and preventing new computers from getting a public IP address before the CD has finished running. These changes should also prevent infected computers from spreading to a large number of Indiana University computers.

The CD was sent out to be duplicated during the last week of July. The finished product was shipped back by the CD duplicator to the software distribution unit two weeks later. The Get Connected CD was then picked up by Residence Hall staff who included it in a bundle of information and with the IU network cable that was to be distributed to students upon move in. All told, the process took about one week.

As students moved into the Residence Halls, our team met regularly to discuss the process and any problems that were encountered. The regular meetings were scheduled to ensure that any problems encountered with the CD would be fixed in a timely manner. The general feeling among the team members at these meetings was that a majority of "Get Connected" CD installations went very smoothly, however a number of issues with the CD did appear.

1. If Windows XP Service Pack 1 did not install properly, the CD went into a reboot loop. It turns out that the CD was designed to stop running if Service Pack 1 is not present, but it did not handle the failure gracefully. Since the CD was programmed to reboot after the Service Pack installation and continue running, the Service Pack installation would fail, the computer would reboot, and the CD would detect that the computer did not have Service Pack 1 installed. The CD would then attempt to install the Service Pack again, which lead to the reboot loop.

© SANS Institute 2005 Author retains full rights.

2. The DHCP Registration did not go as planned. The CD queries the computer for uniquely identifiable information through the Windows Management Instrumentation (WMI) and uses the results to encrypt the URL string. The DHCP server was not able to reliably decrypt the encrypted browser string sent by the CD through the computer's web browser. We found that the first result returned by the WMI query was not always what we expected. In some cases, certain devices attached to the computer would alter the results returned by the WMI query. This resulted in the wrong key being used for encryption and left the DHCP Server unable to decrypt the browser string. Additional coding and logic needs to be added to identify a more reliable unique identifier.
3. The CD does not attempt to detect any previously installed anti-virus software. Instead, the CD asks the computer user if anti-virus software is already installed. If the user answers no, the CD installs Symantec AntiVirus Corporate Edition. We found that some users were not aware that anti-virus software was already running on their computer and installed the Symantec AntiVirus on top of their already running anti-virus software. This resulted in a both anti-virus products scanning files in a loop and left these systems running very slowly. Removing one of the anti-virus products returned the system to normal.
4. Under certain conditions, installing anti-virus software and patches would result in a Stop Error, informally known as the Blue Screen of Death. Investigation of these machines generally showed that the computer had multiple forms of spyware installed. Some spyware is installed in such a way to make removal difficult. Installing the Microsoft hotfixes and anti-virus software prevented these installed programs from running and caused the stop error.
5. There were complaints of slower computers taking a long time to boot or log in. This was normally attributed to the ITNow client running at log in. When the client is run, it collects information about the computer for reporting. The only way to speed up this process is to try to change the way that the data is collected, and that is being looked at for the next release.
6. After the CD is run, the Automatic Updates options through the Control Panel are grayed out, preventing the user from controlling the Automatic Updates settings in this manner. The Automatic Update settings are set on the computer using the Local Security Policy. If the computer users want to change their settings, they can use the Local Security Policy (Control Panel, Administrative Tools, Local Security Policy) to change them back. Alternatively, the settings can be changed by altering the Windows registry directly. This was deemed acceptable by the team, since we prefer that only advanced users disable automatic updates.[16]

---

[16] "How to configure automatic updates by using Group Policy or registry settings." Microsoft Help and Support. 2004. Microsoft. 8 Jun 2004 <http://support.microsoft.com/default.aspx?scid=kb;en-us;328010>

© SANS Institute 2005 Author retains full rights.

7. The Get Connected CD is set to add the computer to the Indiana University Active Directory, called ADS. The tool that performs this operation did not run in a majority of cases. A possible cause of the failure is a bug in the script that performed the joining, but more investigation needs to be done on this subject. If the computers were joined to the Active Directory, we could have used group policy to apply setting changes or prevent malicious software from running through software restriction. With most computers not joined to the Active Directory, our ability is limited to make changes after the CD has been run.

The Aftermath

The Get Connected CD project places computers in a patched and protected state and helps accomplish our overall goal of increasing the overall security and minimizing the risk of compromise of student computers.

The project was able to successfully secure and register over 10,000 new computers on the Indiana University network in the first three weeks of registration. By December 2004, a total of 14,977 computers had been registered.

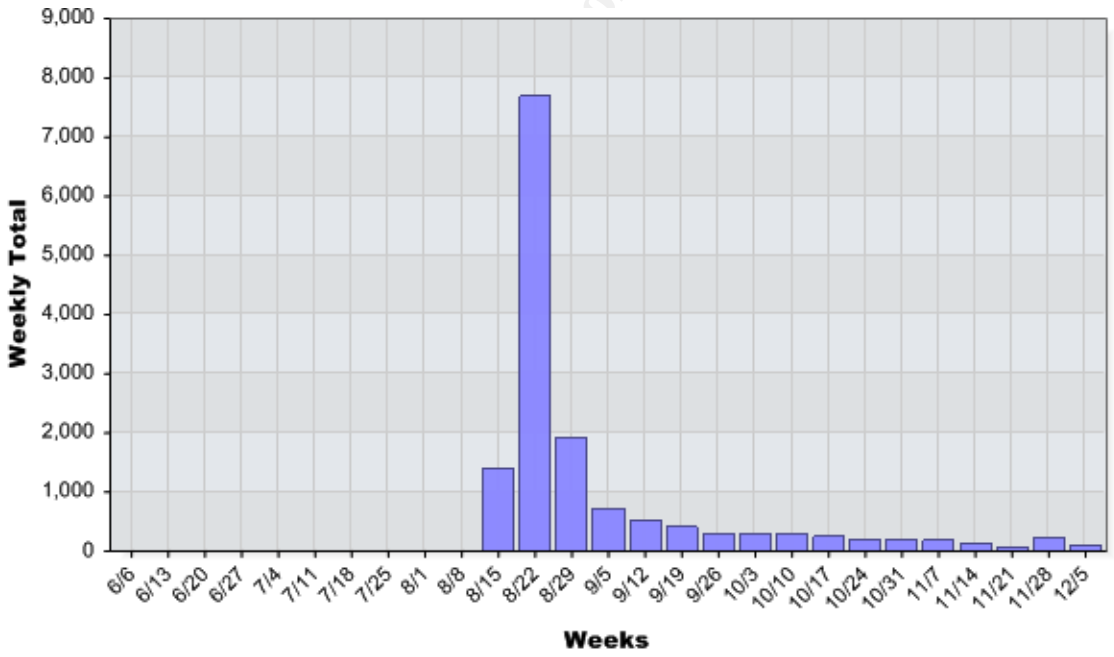

Figure 1: New systems on the network by week.

One way to evaluate the success is to talk with the Indiana University Information Technology Policy Office (ITPO), which handles incident response. The ITPO noticed a dramatic decrease in the number of security incidents concerning student computers which have run the Get Connected CD. I compared the number of incidents in the Residence Hall in the fall 2003 semester to those is fall 2004. In fall 2003, there were 369 incidents recorded by the ITPO. In fall of

© SANS Institute 2005 Author retains full rights.

2004, there have been only 201 incidents. Because of the large volume of incidents in previous years, one full time employee had been dedicated to contacting students whose computers had been compromised. This year, there have been approximately 45% fewer security incidents involving students who had run the Get Connected CD, which has freed the full time employee for other incidents. The incidents that have occurred involving student computers now tend to include Trojan horses, phishing, and bundling of software, all which trick the user into taking action and installing the malicious program. Computers that have run the Get Connected CD are rarely compromised by worms that are currently propagating on the Internet. Student computers are also rarely seen taking part in spreading a worm unless they were compromised through some other means.

The Microsoft Automatic Update service is continually downloading and installing critical security updates from Microsoft. Microsoft's self-imposed throttling of Windows XP Service Pack 2 is the only thing keeping the service pack from installing on student computers. Each week we see approximately fifteen additional computers with XP Service Pack 2 installed and the number of XP computers with Service Pack 1 decreases by the same amount.

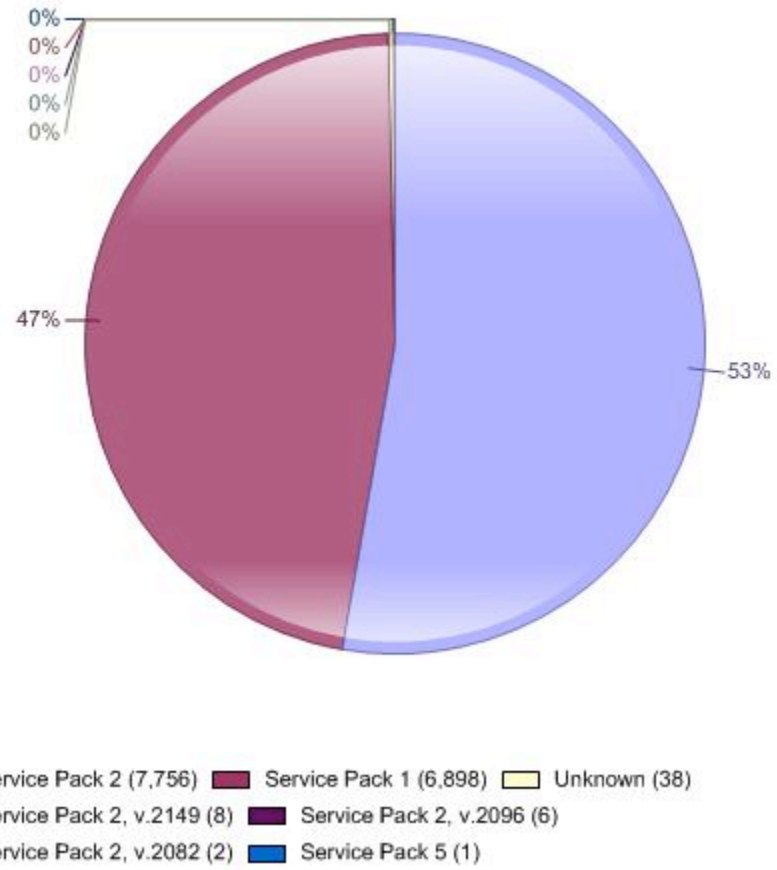

Figure 2: Snapshot of XP Service Pack level, taken 12/7/2004

© SANS Institute 2005 Author retains full rights.

Students do have the ability to turn the Automatic Update service off. If the automatic update service is turned off, we currently have no way to detect this and are unable to re-enable it remotely. To date, 14,424 students have left the service enabled and only 584 have automatic updates turned off. Having Automatic Updates turned on minimizes the chance that a student-owned machine will be left in an un-patched state, but does not guarantee it.

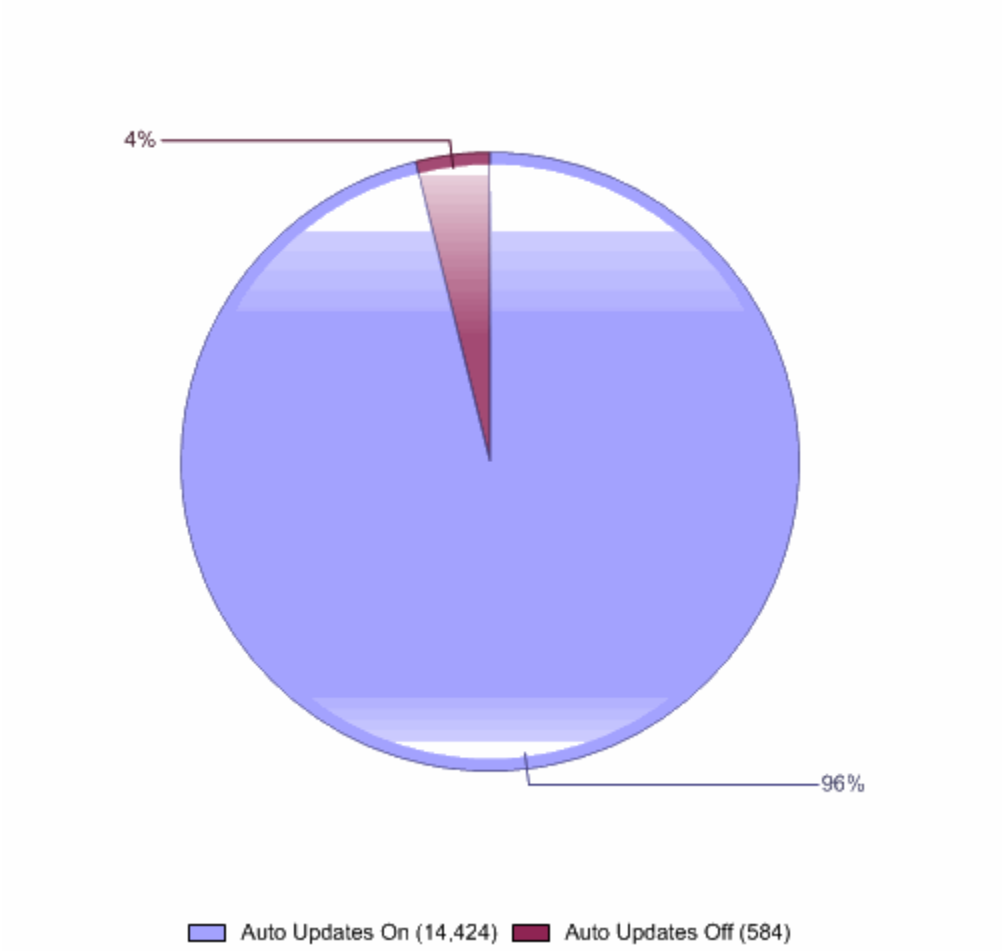

Figure 3 Automatic Update setting on student computers

The settings and changes that the Get Connected CD make on a student's computer are made in such a way that they would apply not only in the University environment, but also on other networks that the student's computer might be a part of after leaving the University. We have not had any instances where a properly installed Get Connected CD rendered a computer unusable in another environment.

The Future of the Get Connected CD

This project accomplished the established goal of increasing the security on student-owned computers in the Residence Halls. The Get Connected CD ensures that all Windows 2000 and Windows XP computers are running the

© SANS Institute 2005 Author retains full rights.

latest Service Pack, have the most recent hotfixes applied, have up-to-date anti-virus software, and leave the computer in a state that provides protection in the future.

The next semester will present new and difficult challenges that Indiana University will have to overcome to keep its network presence secure. During 2004, Microsoft made it clear to the University that redistribution of Microsoft Service Packs and updates is illegal when distributed to computers not owned by the University[17]. Until recently, Indiana University had been allowed to redistribute Microsoft Service Packs and hot fixes to computer users who were affiliated with the University through the Microsoft Higher Education Voluntary Distribution Program (HEVDP).[18] Microsoft had set a deadline in November 2004 for discontinuation of this program. Microsoft has since extended the deadline through June 30, 2005 to give schools more time to update Microsoft Windows computers. For the fall semester of 2005, we are considering ways to limit network access until the student downloads and runs a Get Connected program from our file distribution web site. A new version of Get Connected will download Microsoft software from official locations instead of repackaging the software. Once the web version of Get Connected has completed, the student computer will be given full network access.

Future enhancements to this project should provide additional assurance that student-owned computers are properly maintained. We are considering adding functionally to the ITNow client that will report the current state of a computer to a central location. We want to continually collect information about the computer's current patch status, anti-virus status, and possibly even watch for known malicious processes running on the computer. For example, if a student turns off automatic updates, the ITNow client could send e-mail to the student to verify the action. The information collected will be used to determine if a computer is allowed to remain on the public network or moved to a quarantine network. If a computer is placed on the quarantine network, the student would have to take the appropriate action on their computer and wait for the ITNow client to report the changes. Only then would they be allowed back on the public network.

With a few enhancements, Indiana University will continue to use the Get Connected CD. The 45% decrease in security incidents related to computers that have used the Get Connected CD makes this an indispensable tool to the University.

---

[17] "Description of the standard terminology that is used to describe Microsoft software updates." Microsoft Help and Support. 20004. Microsoft. 26 Jul 2004 <http://support.microsoft.com/kb/824684>

[18] "Does Your Campus Network Need Windows XP Service Pack 2?" Microsoft Education. 2004. Microsoft. 4 Nov 2004 <http://www.microsoft.com/education/HEVDP.aspx>

© SANS Institute 2005 Author retains full rights.

References

1 SANS Institute. Track 1 – SANS Security Essentials. Volume 1.2. SANS Press, Jan 2004.

2 "MS Blast / Blaster Worm Propagation." Indiana University Information Technology Security Office. 2003. Office of the Vice President for Information Technology. Indiana University. 8 Aug 2003 <https://itso.iu.edu/bulletins/ITSO.2003.08.12.blaster>

3 Nakayama, Takayoshi and Ladley, Fergal. "W32.Sasser.Worm." Symantec Security Response. 2004. Symantec Corporation. 27 Jul 2004 <http://www.sarc.com/avcenter/venc/data/w32.sasser.worm.html>

4 "Several Critical Microsoft Vulnerabilities." Indiana University Information Technology Security Office. 2004. Office of the Vice President for Information Technology. Indiana University. 20 May 2004 <https://itso.iu.edu/bulletins/ITSO.2004.05.20.ms04-011>

5 "Microsoft Security Bulletin MS04-011" Microsoft Technet. 2004. Microsoft. 10 Aug 2004 <http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx>

6 "For Windows computers on the IU network, why does UITS recommend Windows 2000 or XP Professional?" Indiana University Knowledge Base. 2004. Indiana University. 9 Nov 2004 <http://kb.indiana.edu/data/aloz.html>

7 "IU Network Cable Wiring Scheme." Indiana University Telecommunications Web Site. 1999. University Information Technology Services, Indiana University. 10 Jun 1999 <http://www.indiana.edu/~uits/telecom/data/images/wiringscheme.gif>

8 “Registered Jack.” Wikipedia. 2004. Wikipedia. 24 Nov 2004 <http://en.wikipedia.org/wiki/Registered_jack>

9 Rekhter, et al. "Address Allocation for Private Internets." Internet Engineering Task Force Request for Comments. 1996. Internet Engineering Task Force. Feb 1996 <http://www.ietf.org/rfc/rfc1918.txt?number=1918>

10 “How to install multiple Windows updates or hotfixes with only one reboot.” Microsoft Help and Support. 2004. Microsoft. 23 Nov 2004 <http://support.microsoft.com/kb/296861>

11 "The basics of VPN at IU." Indiana University Knowledge Base. 2004. Indiana University. 3 Sep 2004 <http://kb.indiana.edu/data/ajrq.html>

© SANS Institute 2005 Author retains full rights.

12 SANS Institute. Track 1 – SANS Security Essentials. Volume 1.5. SANS Press, Jan 2004.

13 "Threat Assessment Chart." Lavasoft Threat Assessment Chart (TAC). 2004. Lavasoft. Dec 2004 <http://www.lavasoftnews.com/ms/tac_main.shtml>

14 "What is ITNow, and why should I use it?" Indiana University Knowledge Base. 2004. Indiana University. 2 Sep 2004 <http://kb.iu.edu/data/aomc.html>

15 "In ITNow, what information is gathered about my computer?" Indiana University Knowledge Base. 2004. Indiana University. 25 Oct 2004 <http://kb.iu.edu/data/apak.html>

16 "How to configure automatic updates by using Group Policy or registry settings." Microsoft Help and Support. 2004. Microsoft. 8 Jun 2004 <http://support.microsoft.com/default.aspx?scid=kb;en-us;328010>

17 "Description of the standard terminology that is used to describe Microsoft software updates." Microsoft Help and Support. 20004. Microsoft. 26 Jul 2004 <http://support.microsoft.com/kb/824684>

18 "Does Your Campus Network Need Windows XP Service Pack 2?" Microsoft Education. 2004. Microsoft. 4 Nov 2004 <http://www.microsoft.com/education/HEVDP.aspx>

© SANS Institute 2005, Author retains full rights.

Appendix A – Get Connected CD Local Security Policy

[System Access]

MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 50
ResetLockoutCount = 30
LockoutDuration = 30
ForceLogoffWhenHourExpire = 1
LSAAnonymousNameLookup = 0
EnableGuestAccount = 0

[System Log]

* Audit Log Retention Period:
* 0 = Overwrite Events As Needed

MaximumLogSize = 20480
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

[Security Log]

MaximumLogSize = 81920
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

[Application Log]

MaximumLogSize = 20480
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

[Event Audit]

* 1 = Success only
* 2 = Failure only

© SANS Institute 2005, Author retains full rights.

```
    * 3 = Success and Failure

AuditSystemEvents = 3
AuditLogonEvents = 3
AuditPrivilegeUse = 2
AuditPolicyChange = 1


[Registry Values]

    * The syntax for this section is:
        o RegistryPath,RegistryType,DisplayName,DisplayType,Options
    * Registry Type
        o 1 - REG_SZ
        o 2 - REG_EXPAND_SZ
        o 3 - REG_BINARY
        o 4 - REG_DWORD
        o 7 - REG_MULTI_SZ
    * Display Type
        o 0 - Disabled
        o 1 - Enabled

MACHINE\Software\Microsoft\Driver Signing\Policy=3,1
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Disable
CAD=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous
=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1
MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\Allowe
dPaths\Machine=7,
MACHINE\System\CurrentControlSet\Control\Session
Manager\Kernel\ObCaseInsensitive=4,1
MACHINE\System\CurrentControlSet\Control\Session
Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\Auto
Disconnect=4,15
```

© SANS Institute 2005 Author retains full rights.

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes=7,
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares=7,
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1

[Privilege Rights]

* SID: S-1-5-32-545
    o Users
* SID: S-1-5-32-544
    o Administrators
* SID: S-1-5-19
    o NT Authority Local Service
* SID: S-1-5-20
    o NT Authority Network Service

SeNetworkLogonRight = *S-1-5-32-545,*S-1-5-32-544
SeTcbPrivilege =
SeIncreaseQuotaPrivilege = *S-1-5-32-544,*S-1-5-19,*S-1-5-20
SeInteractiveLogonRight = *S-1-5-32-544,*S-1-5-32-545
SeRemoteInteractiveLogonRight = *S-1-5-32-544,*S-1-5-32-555
SeBackupPrivilege = *S-1-5-32-544
SeSystemtimePrivilege = *S-1-5-32-544
SeCreatePagefilePrivilege = *S-1-5-32-544
SeCreatePermanentPrivilege =
SeCreateTokenPrivilege =
SeDebugPrivilege = *S-1-5-32-544
SeDenyNetworkLogonRight = Support_388945a0,Guest
SeDenyInteractiveLogonRight = Guest,Support_388945a0
SeDenyBatchLogonRight = Support_388945a0,Guest
SeRemoteShutdownPrivilege = *S-1-5-32-544
SeAuditPrivilege = *S-1-5-20,*S-1-5-19
SeIncreaseBasePriorityPrivilege = *S-1-5-32-544
SeLoadDriverPrivilege = *S-1-5-32-544
SeLockMemoryPrivilege =
SeSecurityPrivilege = *S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544

© SANS Institute 2005 Author retains full rights.

SeManageVolumePrivilege = *S-1-5-32-544
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-32-544
SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19
SeRestorePrivilege = *S-1-5-32-544
SeTakeOwnershipPrivilege = *S-1-5-32-544

[Service General Setting]

* 4 = Disabled, 3 = Manual, 2 = Automatic
    o Browswer = Computer Browser (replaced by WINS)
    o CiSvc = Indexing Service
    o ClipServ = Clipbook Server
    o wuauserv = Automatic Updates

Alerter,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLC
SWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CC
DCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Browser,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCL
CSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;C
CDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
CiSvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLC
SWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CC
DCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ClipSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLC
SWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CC
DCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Messenger,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA
;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
BITS,3,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
wuauserv,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDC
LCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;
CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

© SANS Institute 2005 Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

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

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**