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.

Tackling Malicious Code in a University Environment: A Case Study

This paper is a case study of malicious code incidents in a large public university as seen through the eyes of the security liaison over a one-and-a-half year period. It documents Internet research of these incidents and provides some helpful resources available on the Internet for other university Information Systems Security Officers (ISSOs). This university acts as an Internet Service Provider (ISP) to the students, granting them access to the Internet in a variety of ways with multiple operating systems and platfo...

Copyright SANS Institute

Author Retains Full Rights

AD

Tackling Malicious Code in a University Environment: A Case Study

Sandy Goldston

SANS Security Essentials (GSEC) Practical Assignment: Version 1.3 (amended 12/12/2001)

"One OS to rule them all, One OS to find them,
One OS to bring them all and in the darkness bind them." [16]

Abstract and Selection Criteria

This paper is a case study of malicious code incidents in a large public university as seen through the eyes of the *security liaison* over a one-and-a-half year period. It documents Internet research of these incidents and provides some helpful resources available on the Internet for other university Information Systems Security Officers (ISSOs). This university acts as an Internet Service Provider (ISP) to the students, granting them access to the Internet in a variety of ways with multiple operating systems and platforms supported on multiple subnetworks. Although difficult to configure or control, this variety can have an advantage – diverse operating systems and e-mail applications can sometimes limit the amount of damage a specific instance of malicious code can cause given its dependencies on the operating system and/or applications it uses to spread. As long as there are users, there will be malicious code; so, as long as there are universities, there will be malicious code incidents.

Glossary of Terms

hybrid – as malicious code becomes increasingly sophisticated, a new type is emerging that combines characteristics from more than one type; e.g., malicious code that contains both worm and virus characteristics.

mobile malicious code – viruses that self-propagate. This type of virus not only spreads itself by infecting new files, but it also "transfers the newly infected files to other systems."[5] Because of this additional functionality, these viruses are only dependent on user action for initial infection and not propagation.

security liaison – a university ISSO that acts as a liaison (e.g., being "NICE") between the "suits" (e.g., administration, faculty, law enforcement) and "ponytails" (e.g., students, information technology (IT) staff) in addition to his/her regularly-defined ISSO duties.[29]

Similar Topics

For related information, see:

- College and University Information Security Professionals (CUISP) – the CUISP is an international association of computer system security practitioners in higher education.[8]

- EDUCAUSE [university] Policy Directions, Effective Practices and Solutions: *Virus Notification Program,* University of Maryland – EDUCAUSE is an excellent resource for information technology policy issues and procedures for higher education.[13]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- National Colloquium for Information Systems Security Education (NCISSE), A Society for Advancing Information Assurance & Infrastructure Protection – the NCISSE is a forum to encourage (1) information security, (2) common requirements, (3) information security skills, and (4) certification in secondary education.[17]

1. Introduction

The problems associated with malicious code are never more apparent than in the university environment. As Jerry McGovern, a former was employee at McGill University and the University of Toronto, stated:

> "University servers are hotbeds of weirdness. You never know what you are going to find on them. These are huge networks that are often pieced together piece-by-piece, and each little department has a lot of power over the security on their segment of the network. University servers offer an excellent hiding place for large files. Many of the people who are using the systems aren't technically inclined, and they just access what they need for their daily work. And these folks have huge systems – you could pop a few hundred gigs of data onto a college server, and it would never be noticed."[7]

The job description for an ISSO at a major university contains all the usual ISSO jargon; however, the most important qualification for this position may not only be professional certification and/or experience, but someone who can also be a skilled *"security liaison."* A *security liaison* is the university's ISSO who acts as the intermediary between the "suits" (e.g., administration, faculty, law enforcement) and "ponytails" (e.g., students, IT staff, system administrators). The *security liaison* must direct and coordinate the resolution of a myriad of security issues in a timely and <u>peaceful</u> manner.

This paper is a case study of malicious code incidents in a large public university as seen through the eyes of the *security liaison* over a one-and-a-half year period. It documents research of these incidents and provides some helpful resources available on the Internet for other university ISSOs. Since college campuses are notoriously known as "incubators for" or "facilitators of" malicious code, this university certainly had all the necessary ingredients: a very large numbers of users with varied technical skills (those with extremely limited skills sometimes caused as much damage as a skilled hacker!); somewhat unlimited network access; (very) limited budgets for security personnel, software, hardware, training; multiple operating systems and networks components; segmented departments; etc. And, students typically have a different mindset and motives than that of general users in the corporate world – the Internet is theirs to discover and conquer. The underlying psychological reasons behind writing and/or launching malicious code may be far more interesting than the technical impacts, but is left outside the scope of this paper. As long as there are users, there will be malicious code; so, as long as there are universities, there will be malicious code incidents.

Many universities act as an ISP to their students, granting them access to the Internet in a variety of ways with many different operating systems and platforms supported on multiple

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

subnetworks. Although difficult to configure or control, this variety can have an advantage – diverse operating systems and e-mail applications can sometimes limit the amount of damage a specific instance of malicious code can cause given its dependencies on the operating system and/or applications it uses to spread.

This large public university connects 30,000+ students and employees in dorms, libraries, computer labs, offices, dial-up connections, etc. There is no firewall, and network use / misuse is monitored through router logs and system / network *stats*. Virtual Private Networks (VPNs) are used to isolate various business functions and some departments from general user access. Malicious code is addressed through a defense in depth strategy, employing both proactive measures (e.g., policy, tools such as Tripwire, Norton AntiVirus) and reactive measures (via the security team).

2. Policy

Acceptable Use Policy (AUP) – the AUP was written to explicitly address malicious code stating: "No one shall knowingly create, install, execute, or distribute any malicious code (e.g., virus, Trojan Horse, worm) or another surreptitiously destructive program on any [University] IT resource, regardless of the result." It is also implicitly addressed under other policy bullets. Note the word "knowingly" – that's a tough thing to prove. So, most cases of malicious code were "unknowingly" spread which brings up some interesting legal issues discussed later. The AUP is posted on the university website, as are references and other general information about the "*malicious code du jour.*"

There are three very different types of "users" in the university environment – each with very different access needs and restrictions. The purpose of this paper is not to argue the importance of one group of users over the other; suffice it to say, all three had significant problems with malicious code and they are listed alphabetically.

- Administrators / Employees – from the administration's view, employee use of university-owned equipment and services falls under what is "acceptable use" in performance of job duties and is easily addressed by policies under the direction of the Human Resource office. This is typically the type of user access found in the corporate environment and specific anti-viral awareness training and applications are required and made available.

- Faculty – from the faculty's point of view, things change somewhat from those above – additional issues must be considered, e.g., intellectual property rights, "fair use," research data, publications, consulting services. Anti-viral applications are required and made available, but not necessarily monitored or enforced.

- Students – for students, as stated above, this university chose to act as an ISP and not as a "content" provider. Anti-viral applications are strongly suggested and made available with little or no cost to students; however, not all of these users take advantage of them.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

3. Proactive Measures: Tools

University budgets, being what they are (or aren't!), require mostly the use of publicly available tools.[1] The IT staff was against the use of firewalls (YIKES!). Instead, they relied solely on host-based system protections and network tools and logs.

3.1 Tripwire

The *security liaison* was successful in obtaining a university site license for Tripwire[28]. The use of Tripwire can help ensure the integrity of systems and network hosts by identifying corrupted system files. Since Tripwire must be installed on a "clean" system to be optimally effective,[10] it had not yet been implemented on all the infrastructure support servers when several university machines were found compromised. Out of the ashes rose the edict that all machines were to have Tripwire installed immediately. There's nothing like a significant incident to be the wake-up call to convince management to establish operational policy and procedures!

3.2 Norton AntiVirus

The *security liaison* was also successful in obtaining an enterprise site license for the Norton AntiVirus[19] product. This allowed the infrastructure staff to configure the product for downloading and to set defaults allowing automatic updates of definition files. Skilled users could configure the product to their own specifications, but this allowed the unskilled user to be well protected as well.

4.0 Reactive: Incident Response

The security team (consisting of the *security liaison* and several key IT personnel) handled all of the malicious code incidents – from detection and/or response, determining source, user contact, clean-up and restoration, etc. As a side note, it was quite interesting to see the dramatic decrease in the volume of incidents during spring and summer break and increase during finals week!

Victims could report malicious code incidents via phone, e-mail, in person, or from the security webpage to the HelpDesk, abuse@<universityname>.edu, the university webmaster, or directly to the *security liaison*. All reported incidents were then funneled to a central repository that allowed the *security liaison* to put out timely messages alerting support staff and general users of time-critical issues. Each reported incident was logged into a database with as much known information as possible; e.g., date, source name and/or IP, person reporting incident, type of incident, subject line of message, description, damage. Incidents were tracked for resolution and periodic incident reports were generated for university administration that would indicate problem areas by severity and frequency of occurrence.

5. Types of Malicious Code and Incident Examples

Malicious code, or "malware" as it is also affectionately known," includes viruses, worms, Trojan horses and malicious applets."[23] As malicious code becomes increasingly sophisticated,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

a new type is emerging, called a *hybrid*, that combines characteristics from more than one type; e.g., malicious code that contains both worm and virus characteristics. Malicious applets were not reported at the university during this tenure, so are not included in this paper. E-mail was the most common method of infection distribution and made up the bulk of the total of reported incidents.

Infections at the university were frequent occurrences – most required "assisted" clean-up by the installation, update, or running of anti-viral software. Some infections were by viruses, worms, or Trojans that had been around for a while. These infections tended to have a more limited distribution since some systems had the appropriate anti-viral software installed and up to date. New strands of malware caused the most profound and wide-spread damage simply because the anti-viral software tools did not yet have a definition in place to address them and in many cases, users were did not recognize the malware as such.

5.1 Virus

A virus is a self-replicating program or piece of code written to execute upon a specific action by the user. It executes on behalf of that user without the user's permission or knowledge.[23] It is parasitic in that it infects others files, called host files, and executes when the host executes by replicating and spreading itself.[22] It usually contains a malignant (damaging) or benign (e.g., display a message or banner) payload that may trigger under certain conditions (e.g, date). *Macro viruses* are written in a macro language and run automatically when an infected document is opened. *Boot viruses* are written in assembly language and infect a system during boot up or from an infected diskette. *Program viruses* infect executable programs and are usually written in assembly language or a high-level language such as C.

Now there is the newer concept of *"mobile malicious code"* – viruses that self-propagate. This type of virus not only spreads itself by infecting new files, but it also "transfers the newly infected files to other systems."[5] Because of this additional functionality, these viruses are only dependent on user action for initial infection and not propagation. Although ILOVEYOU is classified as a "worm" by most references[6], it is classified as a virus in this paper since it requires the user to perform an action (open the e-mail attachment) to become infected.[23]

ILOVEYOU Virus – No matter how often security awareness training is done, it is never enough! No matter how many times users are warned to not open e-mail attachments without checking them for viruses first, and warned to upgrade anti-virus software frequently, to run it regularly, etc.; somebody, sometime, will fall for the latest new insidious malicious code. In the case of the "ILOVEYOU" virus, the first victim that called the *security liaison* about a possible infection was an employee who said, "I know I'm not supposed to open attachments, but it came from my son with the subject, 'ILOVEYOU.' Of course I'm going to open it!" What a case of "social engineering!" Of course, several university users were infected that same way and it rapidly spread through the contacts in their Outlook address book. The damage could have been significantly worse if the use of Outlook had been more prevalent across the campus. As it was, e-mail application choices are left to the department and/or user (although some were not supported by the university), so many opted for Eudora , Lotus Notes, or GroupWise – none of

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

which were utilized by ILOVEYOU to spread itself; however, infection still occurred on those systems in which users opened the e-mail attachment.

5.2 Virus Hoaxes

No discussion of malicious code in universities can be complete without touching on virus hoaxes since a tremendous amount of resources are tied up responding to this type of bogus incident. Virus hoaxes are exactly what their name implies – false virus warnings that are mass mailed and blindly forwarded in chain letter fashion without any regard for validating the source or verifying the contents. This type of reported incident generated two e-mails from the *security liaison* in response:

(1) A warning message was sent to the sender of the message stating, "This is a virus hoax," followed by the AUP reference prohibiting chain-letter-type forwarded messages, the possible consequences of violating the AUP (e.g., loss of account access), and recommendations for validating future received e-mails before blindly forwarding them to others.

(2) Another message was sent to all the recipients the message had been forwarded to with all the above information, recommendations for reporting future virus hoaxes they received to the *security liaison* and/or sender's ISP, and warning them not to forward the message on to others.

Virus hoaxes are somewhat readily identifiable because they usually contain the following three parts[14]:

- Command: A command to forward this to message to xx people (or "everyone you know") sometimes within a specified timeframe – this is actually the most prevalent clue that the virus warning may be a hoax.

- Warning: A warning that sounds plausible even if it is disguised in "techno-geek" sounding verbiage. Even a little research on the topic usually reveals that the claim does not makes any sense. The message usually includes scare tactics; e.g., "if you don't [forward this, or delete that file, etc.], dire things will happen to you, your loved ones, your computer, your dog, etc."

- Lack of a Verifiable Source: such as a digital signature, valid e-mail address, etc. Some contain a phone number or website for verification; however, very few people ever bother checking them. Most virus hoaxes have been blindly forwarded by a well-meaning and reputable acquaintance; e.g., respected colleague, law enforcement personnel, corporate spokesperson, pastor, nun, friend, immediate family member, etc. Then it is nearly impossible to convince the recipients that it is a hoax because it came from a reputable person – as if forwarding a hoax massage through the e-mail box of a reputable person validates the original sender's authenticity or the message content!

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The university was plagued by virus hoaxes nearly as often as actual viruses; however, clean-up and restoration was considerably easier! Some of the examples that seemed to continually cycle around the campus included: *It Takes Guts to Say 'Jesus', Get More Money*, etc.

5.3 Worm

A worm is a self-contained program (or piece of code), that is able to spread functional copies of itself to other computer systems (usually via a network)[18] without user interaction.[23] So, remember, a virus requires user action to infect and spread; however, it is obvious that both the ILOVEYOU virus and ExploreZip worm are hybrids and contain characteristics of both worms and viruses so that it is difficult to classify them strictly as one type or the other. In fact, most references do not agree on their classification; however, for the purposes of this paper, ExploreZip is classified as a worm.

ExploreZip Worm – The ExploreZip worm requires user action to spread; however; it does not infect other programs or documents. It is executable code and not a macro virus. In other words, turning on the macro detection feature in Microsoft Word will not provide protection from this malicious code.[4] The ExploreZip worm did a tremendous amount of damage to .doc, .ppt, and .xls, files on university application servers. These Microsoft files were suddenly 0 bytes long and unrecoverable except from backups! Most employee machines were Intel-based Windows 9X or NT operation systems with Outlook or Exchange e-mail applications; however, the ExploreZip payload was able to damage user files even if it was unable to spread itself via e-mail. For Outlook users, the worm searched the user's inbox and sent a reply to every message and spread itself to everyone there. The damage was even more extensive than it would have been if a few users had known how to file messages into folders and not leave hundreds in their inbox! And to add insult to injury, if not cleaned from the machine, the worm restarted every time Windows restarted and the infection continued to spread.

5.4 Trojan Horses

Trojan horses appear to be normal programs; however, they perform an illicit action that the user is unaware of.[23][27]

Subseven 1.2 Gold – one particularly interesting incident had to do with a case of "e-stalking," or electronic stalking involving a Trojan horse. A female student in one of the campus apartment complexes reported that a stalker was sending her frightening messages, controlling her computer while she was sitting at it (e.g., changing the background, opening and closing the CD drive), knew personal information about her (e.g., what she was wearing, when she was there alone), etc. She insisted on having her IP address changed but was reluctant to allow the security team to scan her computer for malicious software. A honeypot was set up with her old IP and monitored for connections; however, the perpetrator was obviously aware of the action and ceased activity. Once the security team was able to convince the student that a Trojan horse must be causing the remote control and access to her machine and changing her IP did not address the problem, she allowed us to clean the system. It was easily determined that the SubSeven 1.2 Gold[26] Trojan horse was installed on her system and the stalker had physical line-of-sight access to the apartment (there was no camera on her computer). The team successfully eradicated

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

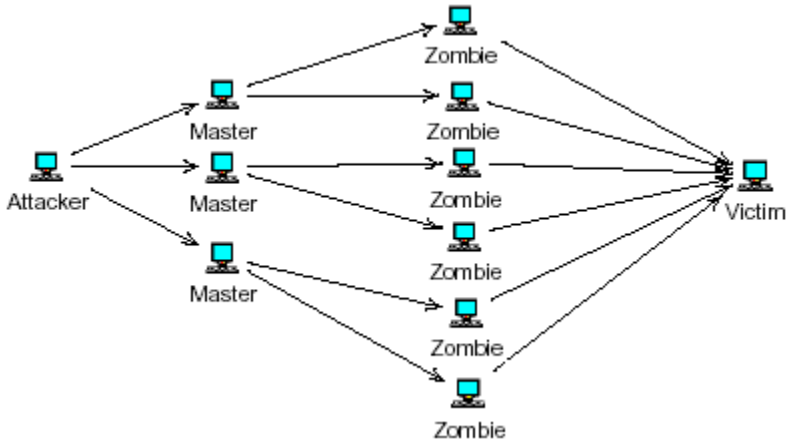
the malicious code from her computer and once the perpetrator was found living in the apartment across the hall and was counseled, the stalking subsequently ceased.

SubSeven 2.1 Gold is a remote access hacking tool in the Trojan horse family. The infecting file named, "server.exe," infects a system via an e-mail attachment. Once the user executes the attachment, the hacker remotely has complete control of the system and can execute programs, access files and address books, change the desktop, manipulate components (e.g., open/close floppy or CD drives), collect passwords, etc. It normally operates on TCP/UDP ports: 2773, 7000, 7215, 27374, or 54283.[15]

At the time, Dark Eclipse Software[9] had 107 different Trojan horses listed on their website, and in the year-and-a-half since then, more than 250 Trojans are now listed! It was also interesting to note the number of connections made to the honeypot from systems outside the United States, because anyone can troll the Internet looking for systems with the Trojan active on it – PCs in the dorms normally sit active on the network.

5.5 Distributed Denial of Service (DDoS) attacks

Since DDoS attacks are a direct result of malicious code installed on multiple (distributed) "zombie" machines, they have been included in this paper. The following figure from [20] illustrates how these zombies are used by an attacker and controlled through "masters" to launch denial of service attacks on any "victim(s)" chosen by the attacker.



trin00 – After breaking news reports of the DDoS attacks on major e-commerce sites, ISPs, federal systems, etc.(i.e., victims), the security team scrambled to determine if the attacks were coming from systems on campus. Extensive scrutiny of network traffic logs indicated the university was not participating in this particular series of attacks. However, three Red Hat Linux systems on campus had been compromised with the "trin00 tool[3]" and a victim had notified the security team that it was being attacked from those IPs.

The Linux systems were found to have been compromised through rpc.cmsd – a buffer overflow vulnerability in the Calendar Manager Service daemon.[2] A "root kit" was discovered on each system and subsequently removed from the infected machines. Root kits hide certain programs, files and network connections to make the DDoS code harder to detect; plus, there is a

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

considerable probability that multiple "back doors" were also installed on the system along with the DDoS tool.[12]

The systems were cleaned,[21] rebuilt, and had Tripwire installed on them. The *security liaison* reported the incidents to CERT and the local FBI agent. The security team heaved a great sigh of relief to not have been active participants in the highly publicized DDoS attacks and to have averted what may have potentially been a much larger and more damaging attack before it probably would have been detected!

5.6 Legal Threats

Nothing catches the attention of the university administration more than the threat of legal action. Apparently there are enough people out there that love to make threats of legal action against big, rich (NOT!) universities hoping for a high-profile courtroom battle or a significant settlement out of court to save costs and embarrassment to the university. That's one of the reasons universities have a General Counsel' office. This university had several threats made against it pertaining to malicious code; however, there was rarely justifiable cause for them and no lawsuits materialized.

A small business had become infected with the ExploreZip worm and suffered tremendous damage to their systems and network. The company had traced the initial infection back to an employee's IP on campus and threatened to sue the university and individual responsible. Apparently the university employee had received ExploreZip and was infected when he previewed the attachment. The worm was then automatically forwarded to every address in his inbox, which included a message from a listserve. Every participant on the listserve received the worm and it did considerable damage to the small business. The university employee was an innocent victim as well, a representative from the Office of the General Counsel and the *security liaison* successfully smoothed some ruffled feathers, and the threatened lawsuit never materialized; however, it did bring up some interesting issues with the concept of "due care" or "due diligence."

6. Conclusion

The sheer volume and diversity of malicious code incidents at this large public university made it a very interesting and exciting place to work. Just like finding a balance between risk and cost-effectiveness of security measures, the university ISSO (or *security liaison*) must strike a delicate balance "between information security and academic freedom"[25] – an oxymoron similar to "security vs. functionality." Because the environment is wide open, the systems diverse and distributed, system administration skills vary tremendously, and resources are stretched to their limits, "[universities are] a better weapon than a target"[25]. It takes evaluation and implementation of both proactive and reactive controls to manage it at all. The pay is low by industry standards[24], but the personal rewards are great – you never know what adventure each day will bring!

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

List of References

[1] CERT® (Computer Emergency Response Team) Coordination Center List of Security Tools: **http://www.cert.org/tech_tips/security_tools.html**

[2] CERT® Advisory CA-99-08; *Buffer Overflow Vulnerability in Calendar Manager Service Daemon, rpc.cmsd;* **http://www.cert.org/advisories/CA-99-08-cmsd.html**

[3] CERT® Incident Note IN-99-07, *Distributed Denial of Service Tools;* **http://www.cert.org/incident_notes/IN-99-07.html**

[4] CIAC (Computer Incident Advisory Capability) *Bulletin J-047: The ExploreZip Worm*, June 11, 1999; **http://www.fjuk.org/df/Security/mail/msg04966.html**

[5] CIAC Information Bulletin K-031: *Mobile Malicious Code,* **http://www.ciac.org/ciac/bulletins/k-031.shtml**

[6] CIAC *Information Bulletin K-039e*: *VBS.LoveLetter.A Worm*; May 5, 2000; **http://www.ciac.org/ciac/bulletins/k-039.shtml**

[7] *"College: A Cracker's Best Friend,"* Michelle Delio, Wired News, February 20, 2002, **http://www.wired.com/news/culture/0,1284,42063,00.html**

[8] College and University Information Security Professionals: **http://web.mit.edu/security/www/cuispnew/cuisp.htm**

[9] Dark Eclipse Software: **http://dark-e.com/archive/trojans/**

[10] *"Data and Network Integrity (DNI) / Technology to Invoke Trust in IT — The Tripwire Solution, An IDC White Paper"* C. Kolodgy, et. al., **http://-www.tripwire.com/files/literature/white_papers/Technology_to_Invoke_Trust.pdf**

[11] *"Defense Tactics for Distributed Denial of Service Attacks,"* Federal Computer Incident Response Center (FedCIRC), 2000, **http://www.fedcirc.gov/docs/DDOS-defense.PDF**

[12] *The DoS Project's "trinoo" distributed denial of service attack tool,* **http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt**

[13] EDUCAUSE [university] Policy Directions, Effective Practices and Solutions: *Virus Notification Program,* University of Maryland; **http://www.educause.edu/ep/ep_item_detail.asp?item_id=15**

[14] *Hoaxbusters,* CIAC UCRL-MI-140103: **http://hoaxbusters.ciac.org/HBHoaxInfo.html**

[15] *Intrusion Detection FAQ: What ports numbers do well-known trojan horses use?"* Joakim von Braun, **http://www.sans.org/newlook/resources/IDFAQ/oddports.htm**

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[16] *Lord of the OS,* origin unknown, collected from the Internet January 25, 2001; **http://farpg.tripod.com/f/lordos.html**

[17] National Colloquium for Information Systems Security Education, A Society for Advancing Information Assurance & Infrastructure Protection: **http://www.ncisse.org/**

[18] *NSA Glossary of Terms Used in Security and Intrusion Detection*, Greg Stocksdale, April 1998, **http://www.sans.org/newlook/resources/glossary.htm#H**

[19] Norton AntiVirus: **http://www.symantec.com**

[20] *Overview of Scans and DDoS Attacks*, NIPC Watch and Warning Unit, **http://www.nipc.gov/ddos.pdf**

[21] *Results of the Distributed-Systems Intruder Tools Workshop***;** CERT; December 7, 1999; **http://www.cert.org/reports/dsit_workshop-final.html**.

[22] SANS GIAC Information Security *KickStart Glossary of Terms*, **http://www.sans.org/audio/KS_Glossary.pdf**

[23] SANS GIAC Level One Security Essentials, *Section 1.1.6: Malicious Software*, slide 3.

[24] *Security in Numbers*, by David Foote, Information Security, August 2001, **http://www.infosecuritymag.com/articles/august01/securitymarket.shtml**

[25] *Security: It's Academic / Campus IT Admins Deal With Their Insecurities*, Neil Roiter; November 2001; **http://www.infosecuritymag.com/articles/november01/industry_academic.shtml**

[26] SubSeven 2.1 Gold: **http://dark-e.com/archive/trojans/subseven/21gold/**

[27] *Threat Assessment of Malicious Code and Human Threats, Malicious Code*; Lawrence E. Bassham & W. Timothy Polk, National Institute of Standards and Technology Computer Security Division, March 10, 1994, **http://csrc.nist.gov/publications/nistir/threats/section3_3.html#SECTION0003000000000000000**

[28] Tripwire: **http://www.tripwire.com**

[29] *University ISSO or Security Liaison? A Case Study*, Sandy Goldston, Information Security KickStart, Version 2.0 (revised August 13, 2001), December 17, 2001.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Acronyms

AUP	Acceptable Use Policy
CERT	Computer Emergency Response Team
CIAC	Computer Incident Advisory Capability
CUISP	College and University Information Security Professionals
DDoS	Distributed Denial of Service
DNI	data and network integrity
FedCIRC	Federal Computer Incident Response Center
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
IT	information technology
NCISSE	National Colloquium for Information Systems Security Education
VPN	Virtual Private Network

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: August 30th, 2015

Upcoming SANS Training

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

SANS Milan 2015	Milan, IT	Sep 07, 2015 - Sep 12, 2015	Live Event
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
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
Data Breach Investigation Summit & Training	Dallas, TXUS	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 Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 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 Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 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
FOR578 Cyber Threat Intelligence	OnlineVAUS	Aug 31, 2015 - Sep 04, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced