Interested in learning more about security?

SANS Institute InfoSec Reading Room

A System Administrator's Guide to Implementing Various Anti-Virus Mechanisms: What to do When a Virus is Suspected On a Computer Network

This paper, presented in the form of sample guidelines/procedures, will express in much detail the steps, techniques and methods of defense utilized/implemented in the detection, investigation and tracing of a suspected computer virus. Proposed courses of action will be discussed. The effectiveness of these actions, as well as the use and effectiveness of established mechanisms of defense will be evaluated. It is evident that the threats and dangers associated with computer viruses will always plague the computer world...

A System Administrator's Guide to Implementing Various Anti-Virus Mechanisms:
What to do When a Virus is Suspected On a Computer Network
Robert B. Fried
June 6, 2002

Abstract

This paper, presented in the form of sample guidelines/procedures, will express in much detail the steps, techniques and methods of defense utilized/implemented in the detection, investigation and tracing of a suspected computer virus. Proposed courses of action will be discussed. The effectiveness of these actions, as well as the use and effectiveness of established mechanisms of defense will be evaluated.

Fried & Fried Securities, in reality, a fictitious privately owned corporation, will serve as a model of a real life company. It will be assumed that Fried & Fried Securities will be operating on IBM compatible, Pentium/Celeron® class systems, designed by a reputable national computer manufacturer. The LAN (Local Area Network) will be running on Microsoft Windows 2000, under the authority and supervision of a System Administrator. Each system tied to the network, will be loaded with software necessary to run a securities brokerage house. Privilege and security levels of access will be determined and configured by the System Administrator. Furthermore, each system will have access to the Internet. E-mail will be available for each computer user in the corporation. This e-mail will be filtered using e-mail scanning software installed on the network's mail server. Moreover, a regularly updated anti-virus software package supplied by the manufacturer of the computer systems, and maintained by the System Administrator will be loaded onto each computed owned by or housed on the premises of Fried & Fried Securities.

A Definition From An Expert

Dr. Fred Cohen is best known for his work and research on areas relating to computer viruses. Dr. Cohen's definition of the term 'computer virus' is widely accepted. Cohen asserts "a computer virus is a program that can 'infect' other programs by modifying them to include a, possibly evolved, version of itself" [1].

Statement of Fried and Fried Securities' Concern

As technology continues to advance, so does the threat of computer viruses and other forms of malicious code. Computer viruses are becoming more sophisticated in regards to how they are written, how they are transmitted and how they deliver their payload. New tools and strategies of defense need to be implemented to protect against computer virus infections.

In a survey conducted in October 2000 by ICSA.net, a security assurance firm, it was found that the number of companies experiencing computer disasters due to viral infections has increased by 20 percent from the previous year. It is estimated that the number of reported incidents will double by October 2001. This survey, which compiled data from over 300 companies, found that the loss of productivity due to virus infections is on the rise and that financial losses can cost a company anywhere from $100,000 to $1,000,000 a year [2].

Computer viruses should not be disregarded. They are, and will probably always be a potential threat. To prevent infection and the possibility of losses, be they financial, time or company resources, it is the position of Fried & Fried Securities to implement the precautions and procedures as we see fit and necessary to combat the threats associated with computer viruses.

Precaution Level One: Effective Training

Most computer viruses tend to spread due to human interaction/intervention [3]. Through attending a mandatory professional training course on how to prevent against computer viruses, the level of employee awareness in regards to the threats/dangers associated with computer viruses will rise. This course will focus preliminarily with the different types of viruses and simple means of prevention. Computer viruses such as file infectors, .com infectors, .exe infectors, disk infectors, and partition infectors; boot infectors, macro viruses, Trojan horses, worms and Visual Basic Scripting Viruses will be discussed in detail. The various ways in which each of these of viruses can be transmitted will also be covered. Moreover, employees will be trained on how to determine whether their computer system possesses symptoms characteristic of a computer virus. Furthermore, this course will help employees evaluate whether an e-mail qualifies as being trustworthy enough to open, read or download attachments from.

Precaution Level Two: Periodic Employee Assessment

Upon completion of the training course, employees of Fried & Fried Securities will be subjected to periodic employee assessments. These assessments will ensure that each employee is aware of the threats/dangers associated with computer

viruses and that he/she is taking the proper precautions to protect the integrity of his/her particular computer system. These assessments may be in the form of a short written exam with multiple choice or true false questions. However, assessments may also take the form of a practical exam. For example, an employee may be chosen at random to receive an e-mail that appears to be from or of an unfamiliar source. It will be up to that particular employee to decide whether that e-mail is of or from a trustworthy source. If the employee fails to successfully pass/complete exams of such a nature further training will be implemented.

Precaution Level Three: Established Mechanisms of Defense

Probably the most common and established mechanism for combating computer viruses is the use of anti-virus software. However, anti-virus software can be deemed effective only if it is frequently updated. Many anti-virus software vendors provide periodic updates, enhancements and patches to their software products. If such updates are not taken advantage of, a computer system or network of computers can be left vulnerable to virus infection.

In a survey conducted in June 2000 by Central Command, an anti-virus company, it was found that nearly 25 percent of computer users do not periodically update their anti-virus software suites. Furthermore, the survey concluded that nearly 62 percent of those surveyed had their computer become victimized by a virus infection. Moreover, 22 percent claimed that they had lost data due to their computer becoming infected by a computer virus [4].

Each computer system or network server brought to, or housed on the premises of Fried and Fried Securities must contain anti-virus software program. Anti-virus software, as provided by the computer vendor of Fried & Fried Securities will be periodically updated. The anti-virus program will be configured to perform automatic inspection of all files accessed on the computer system in which it is installed. Furthermore, any options allowing for automatic and on demand scanning will be utilized if available. Each hard drive connected to the network will be scanned daily for the presence of computer viruses. Moreover, any and all removable hard drive peripherals/devices will be scanned for the presence of computer viruses [3].

Many computer viruses spread via e-mail. Although, each employee will be trained in how to evaluate if an e-mail if from a trusted or an unsafe source, chances cannot be taken. As a result, Fried & Fried Securities will have an e-mail scanner installed on all mail servers. E-mail scanners have the ability to intercept any viruses that may be present [3].

Always Expect the Unexpected

Despite the implementation and utilization of proper precautionary measures, computer viruses may/can still slip through the cracks. This may occur because the virus may be undetectable by the anti-virus' scan engine. Problems relating to computer hardware/software such as configuration errors can also allow for a virus to infect a computer system. Furthermore, an action caused due to human interaction or intervention may have caused a virus to make its way onto a particular system. In any case, any suspicions that a virus may be present on a computer system must be reported immediately to the Fried & Fried Securities' System Administrator. The machine is to be left in its original state and should not be logged off the network or shut down.

The System Administrator Steps In

Not every irregular activity on a computer is due to a virus. Other errors, such as computer software bugs may occur. In order to truly identify/verify if a computer virus is present on a particular computer system, the individual who brought the concern to the System Administrator will be asked to fill out the following questionnaire:

Fried & Fried Securities Inc.

Suspicious Computer Activity / Incident Report

Workstation ID:	**Date:**	**Time:**
Employee:	**Department:**	**Ext:**
Last Application Utilized:	**Last file executed:**	**Last System Reboot:**

Recent Symptoms

Please Place a Check By All That Apply:

___ Computer system appears to be running/loading programs slower than usual

___ Computer system appears to hang/freeze when using a specific file/program

(specify) _____

___ Computer's hard disk drive appears to be constantly working

(hard drive light is on often)

___ Computer system time/date settings appear to have been modified

___ There are noticeable changes in file sizes and available memory

___ Strange things are appearing on the computer's monitor

___ Unusual/Unfamiliar programs running in the background

___ Something out of the ordinary occurs when using the computer

(unusual messages appear)

Other:

Recent Daily Activities

Please Place a Check By All That Apply:

___ Read/Compose electronic mail.

___ Use of database program ____ Use of spreadsheet program ____ Use of word processor program

Other:

Recent Risky Activities

Please Place a Check By All That Apply:

___ I have recently download e-mail attachments to my computer system

(When?_____ What?____)

___ I have recently taken work home with me on a floppy diskette (When?_____)

___ I have recently download files from the Internet

(When?_____)

Other:

Other information regarding this incident that may be of assistance to the System Administrator:

Signature of Employee: **Date:**

Hold Everything!

Upon notification of the suspicious computer activity/incident, and review of the above questionnaire, the System Administrator will initially proceed by promptly evaluating the performance of the system in question. During this time, the computer system will still be kept in its original state, still turned on and connected to the network. With the machine in its unhampered, original condition, it is possible for the System Administrator to accurately diagnose the system. If however, the computer system has locked/froze up, has been logged off the network, or has been shut down, there may be difficulty diagnosing the system due to any possible changes that may occur due to virus activity during the computer's boot up stages.

Let the Detection Begin

The System Administrator will begin his/her analysis by utilizing the most current version of the anti-virus software provided by Fried & Fried Securities' computer vendor. The System Administrator will configure the software so that a full scan for viruses can be performed on all the files resident on the network and on the system in question, as well as on any form of removable media utilized by the user of the computer. If in fact the anti-virus program discovers a virus, the program will hopefully proceed by safely removing it.

If no virus is detected, the System Administrator will immediately isolate/disconnect the system from the network and back up all the files resident on the computer's hard disk drive. Furthermore, the System Administrator will proceed by rebooting the machine in question with a DOS diskette that is known to be free from viruses. This essential step by the System Administrator ensures that a virus has not been run or is not in the system's memory [5]. After isolating/disconnecting, backing up all the files on the system in question and performing a reboot with a clean system boot-up diskette, the System Administrator will begin to take the courses of action necessary to determine if the computer's suspicious activity, is in fact due to a virus infection. In order to better understand how the System Administrator must proceed with his/her investigation it is important to discuss in detail some of the methods or techniques employed in the detection of computer viruses. The ways in which computer viruses are detected can be divided into three major categories: detection by appearance, detection by behavior and detection by change.

Detection By Appearance

Detection by appearance involves the investigation of executable files within the computer system in question, for the appearance of unfamiliar or suspicious code. There is no set way to go about performing such a task, however the System Administrator must use his/her own intuition. One way the System Administrator can utilize this form of detection is by asking the user of the computer in question if he/she could specify/identify the last few programs that had been executed before the suspicious activity was first noticed. If this information is available, the System Administrator can then begin to target an investigation on those particular executable files. However, this task of looking into the code of executable files is extremely tedious, requires technical knowledge of programming and is very time consuming. As a result, this method should only be utilized if one is up for the challenge and possesses the skill, patience and time to do so [5].

In many cases, anti-virus programs contain a feature that can scan files for embedded virus code. It is believed that viruses contain code that is shared with no other program. Known as a 'scan string' this code is searched for in hopes of detecting and identifying a virus. If a 'scan string' is detected' it is also possible to effectively remove the virus without any impact to the infected program. However, with the continual emergence of new viruses, utilizing this type of method is often unsuccessful. If a virus is relatively older or well known, its 'scan string' will automatically be detected. In the case of newer viruses, their codes may not be fully known or accounted for. By the time the code is identifiable and placed in an updated version of an anti-virus program, it most likely will be too late [5].

Detection By Behavior

Detection by behavior is associated with the observation of the system in question for any signs/evidence of suspicious/abnormal activity. A virus must perform certain activities in order to replicate. These activities include actions such as the reading, writing, and opening of directory files. By utilizing the detection by behavior approach it is possible to detect and stop the spread of viruses before they replicate further. Stopping the virus before it spreads can help stop the virus payload, the portion of the virus that possesses intentions other than replication [5].

This particular method can be useful to the System Administrator. Through the running of certain programs or files on the particular computer in question, certain activities running either visually or in the background can be analyzed. By doing so, the System Administrator can obtain a first hand account of what exactly is taking place on the machine in question. The System Administrator's accounts can then be compared to that of the user of the computer who initiated the report.

When performing an analysis of the computer in question, the characteristics of various types of viruses will be kept in mind:

Trojan Horses:

When infected with a Trojan Horse, a computer hacker has the potential to access your computer without the user's knowledge or consent [6]. Common symptoms of a Trojan Horse virus include [6]:

- CD-ROM drawer mysteriously opens and closes without any user interaction.
- Computer screen mysteriously flips upside down, blinks or inverts images.
- Computer system settings mysteriously change on their own.
- Internet browser installed on computer system goes to an unfamiliar web page on its own.
- Computer mouse reverses button operations / moves by itself / leaves trails / pointer disappears / freezes.
- Computer system reboots / shuts down by itself.

Worms:

Computer worms can be characterized by their ability to proactively spread themselves. Essentially, "when they enter a system, the first thing they do is transmit themselves to more systems" [7]. Worms are typically transmitted when an attachment from e-mail is downloaded and executed. Symptoms associated with an infection due to a computer worm include the following [7]:

- The virus sends itself to each contact found in the address book of an e-mail management program without the computer user's knowledge.
- The virus copies itself and sends replies to individuals who send mail to the user of the computer infected by the worm.
- The virus deletes files that are resident on the hard drive of the infected computer.
- The virus deletes files that are resident on the computer network.

Macro Viruses:

Macro viruses are viruses that are found in macros associated with a particular document. Macro viruses are not stand-alone programs in that they are found within files. Simply opening the infected file activates the virus and allows it to reside in the program's normal template file [8]. Symptoms associated with macro viruses include the following [8]:

- The only option to save a particular document is in a template format.
- A template icon is displayed for a file.
- Upon executing a file, "1" appears in a dialog box.
- Random changes to a document are discovered upon retrieving a saved document.
- New macros may be added to the list of macros utilized by a particular program.

Knowledge of some of the symptoms of various types of viruses can aid in helping the System Administrator classify the suspected computer virus. With proper classification, other characteristics known to be associated with the type of virus suspected can be sought or investigated. If however, the suspicious activity on the machine in question is unique and does not possess any of the symptoms associated with some of the other commonly found forms of computer viruses, this method of detection cannot be utilized.

Detection By Change

Detection by change involves the monitoring of changes that occur or have occurred on a computer system. Changes in a computer system can be detected in several different ways. One possible way to discover any changes in a computer system is by investigating the sizes of commonly used programs or files. If a log is kept of all programs and files resident on a computer system, it would be relatively easy to spot any noticeable or suspicious changes. Other changes that can occur on a system due to infection by a computer virus include: changes to date/time stamp as well as a decrease in the amount of memory available to a system. Such changes, however, are not always noticeable enough to spot [5].

The System Administrator will attempt to detect any changes that may have occurred to the system in question using an integrity checker. Essentially, original checksums, or special identifiers, computed for files on the network, can be compared to checksums calculated for files on the system in question. If the System Administrator compares the newly calculated checksums with the original checksums and finds a difference, it is quite possible that this file contains a virus. Although this method of detection will be very tedious, it is very comprehensive [9].

It is an extremely difficult task to keep a log/record of all known file sizes for all programs and files resident on each computer on the network. Sizes of files and programs on the computer in question can be compared to the System Administrator's test system, which runs under Windows 2000 and contains all of the software housed on Fried & Fried's network and computers. There is yet another, somewhat easier way to detect viruses by change. In fact, many anti-virus software packages, when run for the first time, following installation, record the file sizes for all files scanned. Although, this feature may look appealing, many new viruses do not modify the programs they infect [5]. As a result, this method of virus detection may not always be effective.

How to go About Tracing the Suspicious Activity to Its Source

The methods of detection may or may not be effective in regards to helping the System Administrator in his/her investigation. If the System Administrator does detect suspicious activity but the anti-virus software does not, there is now other legwork that must be done. The System Administrator's first action will be to contact the developer of the application software or file that appears to be causing the suspicious activity. The System Administrator will inquire about any reports of similar activity by other users of the particular program or file. If the suspicious activity is due to a bug in the program, the System Administrator will inquire as to what to do in regards to getting a patch from the developer. If the developer of the software program or file is unaware of any such activity, other methods for tracing the suspicious activity to it source must be utilized.

In attempting to trace the suspicious activity to its source, the System Administrator will attempt to gather information about any new viruses that have been recently announced. Internet websites such as http://www.virusbtn.com/ as well as the website operated by the developer of the anti-virus software utilized by Fried & Fried will be accessed and searched in helping the System Administrator accomplish this task. Any newly reported/discovered viruses will be researched in regards to the symptoms associated with each and possible methods of transmittance and propagation. If the System Administrator finds a virus that has symptoms and characteristics similar to newly discovered/reported viruses, methods for eliminating the virus will be sought. If however, no viruses appear to contain symptoms or characteristics consistent with that of the suspicious activity, the System Administrator will proceed to contact the developer of the anti-virus software directly. The developer of the anti-virus software will be alerted of the suspicious activity and any possible suggestions in regards to how to go about tracing the suspicious activity to its source will be sought.

If however, none of the detective methods are effective and the System Administrator does not suspect any suspicious activity, he/she cannot simply end his/her investigation. Any report of suspicious activity on a computer will be taken seriously and fully investigated. Fried & Fried believes that the time it takes to investigate the matter is worthwhile considering the risks and other unfortunate circumstances that may result due to a computer virus infection. As a result, the System Administrator will continue his/her investigation until the suspicious activity is traced to its source.

Possible Insights as to Where the Source May Be Located

There are many routes to take in attempting to trace the source of suspicious activity on a computer. The System Administrator will begin by utilizing the "find" function found within Microsoft Windows 2000 operating system environment. The "find" function will be configured to specifically find files on the computer in question's hard drive that were modified or created on the date when the user first noticed the system's suspicious activity. Furthermore, files modified or created two days prior to the first signs of suspected activity will be sought on the computer in question. Any removable media, such as floppy diskettes, zip drives and cd-roms utilized by the computer user will be analyzed in a similar fashion. The System Administrator will record those files, which match the search criteria. If any of the files found happen to be associated with the program(s) or file(s) in which the suspicious activity occurs, the System Administrator will make sure he/she pays special attention to those particular files.

Attempting to Pinpoint the Source

The "find" function of the Microsoft Windows 2000 operating system can prove useful; however, it should not be trusted with full confidence. The System Administrator cannot simply assume that those files found by the "find" command should be considered suspect. In attempting to determine whether any of the files resulting from the search performed using the "find" command should be considered suspect, a security logging application will be utilized.

Microsoft Windows 2000 allows the System Administrator to implement event logging. The event-logging feature offers the System Administrator the ability to maintain a system log, application log or a security log. Essentially, the system log allows the System Administrator to monitor any activities or changes that occur to system at startup. The security log allows for the analysis of possible changes made to administrative options/tools [10]. After properly authorizing and configuring the logging feature, the System Administrator will then utilize this feature in hopes of pinpointing the exact location of the virus. Through careful analysis of the data obtained as a result of implementing this logging feature, it may be possible to determine if any of the suspected files on the computer are involved in any of the noted changes taking place on the system. If some or one of the suspected files is/are noted to cause any unauthorized changes to the system, the System Administrator will proceed by checking the calculate the checksum of each of the suspected files. If an original checksum value for this file, in its uninfected state is available, the System Administrator will compare the two values. If there is any difference in these values, it is evident that changes in the file(s) have taken place. This change could be the result of a computer virus infection [9]. If any of the suspected files were traced using the logging software and there are deviations in the values of the newly calculated and known/original checksums of any of these files, it is quite possible to identify if any of these files are in a way associated, or in fact are the suspected virus. If this is the case, the System Administrator will take the necessary steps to carefully and safely remove the files or file from the system. The System Administrator will then perform a similar analysis of all systems on the network for the presence of those suspected files and their activity. However, this approach may be unsuccessful because the virus may have already executed and spread.

If the suspected files were not identified as causing any changes to the system in question, it is quite possible that the computer virus is eluding detection. However, it is also possible that the suspicious activity on the computer may be due to a hardware or software conflict, malfunction or error. There could be many possibilities that account for the suspicious activity. Although, assumptions can be made, the system and network will be continuously monitored. If over time, the suspicious activity is found only to occur on the system in question, that computer system will be replaced. However, the issue of the exact cause of the suspicious activity will always be on file and viewed as a potential threat.

How Did It Get There and Who Created It?

As in any crime scene there is always evidence of some sort left behind. In the case of computer hackers and virus writers, these individuals seek the attention that is driven from the attacks they perform or the viruses they create. As a result, the creator of the virus causing the suspicious activity on the computer may leave certain digital footprints behind. Most computer virus writers seeking attention tend to leave their code name behind in the source code of their programs. If this is the case, research can be done to try and pinpoint the location of the virus writer or other viruses this individual has claimed to create [11]. This research however, may often lead to a dead end because many virus writers are clever in their attempts to disguise their full identity.

If a computer virus is transmitted via an e-mail attachment research can be done in attempts to again identify and locate the writer of the computer virus. Considering the original e-mail was not yet deleted from the infected computer's e-mail inbox, the System Administrator can attempt to trace back the e-mail to the original sender. Each e-mail message contains a header containing what can be useful information. The header can possibly provide information such as the sender's e-mail address, name, and Internet Protocol address. Furthermore the header can also provide the date and time at which an e-mail was sent as well as the subject line it contained. Such information can provide law enforcement with enough clues to attempt to track down the individual responsible for the attack [12]. However, often times these clever individuals will use hacking tools to manipulate or falsify the e-mail header to prevent from being traced and apprehended.

In the case of the virus being transmitted via the computer user's floppy diskette, it is important to find out how the virus got there. The user of the computer needs to be asked several questions. Was this diskette brought from home?, Did you obtain this diskette from someone?, Do you store any particular files on this diskette? Such questions help in pinpointing how the virus was placed on the disk.

Confidence in Our Approach

Fried & Fried believes that the approach outlined above will provide the most logical and economical approach in investigating and tracing a computer virus. Unfortunately, most companies are blind to the potential dangers and threats associated with computer viruses. In fact, as stated previously, many companies fail to regularly update their anti-virus software programs. As technology advances so does the threat of computer viruses; all who utilize computers must realize this threat. Computer virus writers are getting cleverer with the passing of each day. Virus writers and hackers are devising new ways to elude detection. Although it may be true that evidence is found whenever a crime occurs; the evidence is becoming much harder to discover. New and creative approaches to virus defense such as the use of logging software

must be implemented to work in conjunction with established mechanisms of defense such as anti-virus software. By taking all the specified and outlined approaches as mentioned above, Fried & Fried feels confident that our desire to stay secure and informed will help combat this never ending battle/challenge. We must all keep in mind that together our joint efforts and actions will make a difference.

Summary, Conclusions and Further Work

It is evident that the threats and dangers associated with computer viruses will always plague the computer world. There will always be those individuals who will attempt to deceive or cause damage/discomfort to others. As technology continues to advance, computer viruses are becoming more sophisticated and complex. Virus writers are utilizing new methods to elude established methods of virus defense. In reality, no defense or method of detection is 100% effective. Computer virus writers and hackers enjoy exposing vulnerabilities that are known to exist within the computer world. With the increased popularity of the Internet, more people will find themselves vulnerable to these hackers and virus writers.

Is there hope? Cohen, asserts that there are three things one can do to "absolutely and perfectly prevent a computer virus from spreading throughout a computer system or network; limit sharing, limit transitivity or limit programming" [13]. However, in an ideal world, this advice is impossible to follow. Realistically, for now, we can only attempt to stay safe, secure, alert and informed.

References

[1]. Cohen, Fred. "How Does a Virus Spread Through a System." A Short Course On Computer Viruses. ASP Press, 1990, ISBN 1-878109-01-4, page 11.

[2]. Virus Threat Gaining Momentum: ICSA survey. http://www.securitywatch.com/newsforward/default.asp?AID=4361

[3]. Breeding, Marshall. "A Prescription for Computer Health." Information Today Feb. 2000, Vol. 18 Issue 2, p38. 2p.

[4]. Users Still Complacent About Anti-Virus Updates, Claims Survey. http://www.securitywatch.com/newsforward/default.asp?AID=4361

[5]. Skardhamar, Rune. Virus Detection and Elimination. Academic Press Inc, 1996, ISBN 0-12-647690-X..

[6]. Trojan Infection Symptoms. http://lockdown2000.com/trojansymptoms.html

[7]. Turner, James. "The Dirt on Computer Worms" http://www.csmonitor.com/durable/1999/07/01/p14s1.htm

[8]. What You Should Know About Macro Viruses. http://web6.duc.auburn.edu/desktop/training/docs/word97-2.pdf

[9]. Dixon, Eric, Charles Duncan, Rachel Jacobsen and Barbara Ward. Computer Viruses: Prevention, Preparation, Detection and Recovery. http://lal.cs.byu.edu/ketav/issue_2.12/virus/virus.html

[10]. Otey, Michael. "Windows NT Event Logs." Windows 2000 Magazine Nov. 1996. http://www.winntmag.com/Articles/Index.cfm?ArticleID=2830

[11]. Making Sense of Computer Viruses: The Virus Writers. http://www.bbc.co.uk/makingsense/viruses/writers.shtml

[12]. Reading E-Mail Headers: All About E-Mail Headers. http://www.stopspam.org/email/headers/headers.html

[13]. Cohen, Fred. "How Does a Virus Spread Through a System." A Short Course On Computer Viruses. ASP Press, 1990, ISBN 1-878109-01-4, page 61.

About the Author

Robert Fried is currently a graduate student at the University of New Haven. He is pursuing a M.S. in Forensic Science with a concentration in Advanced Investigation as well as a Certificate in Information Protection and Security. Robert holds a B.S. in Forensic Science as well as Certificates in Law Enforcement Science and Forensic Computer Investigation from the University of New Haven. His future plans are to enter into the field of computer forensics. Any correspondence with the author should be directed to Robert Fried via email: robfried@yahoo.com.

to top of page | to Reading Room Home

Last Updated: October 2nd, 2013

Upcoming SANS Training

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

SANS Seattle 2013	Seattle, WAUS	Oct 07, 2013 - Oct 14, 2013	Live Event
SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
MGT415 at (ISC)2 SecureSoCal 2013	Manhattan Beach, CAUS	Oct 31, 2013 - Oct 31, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
MGT415 at (ISC)2 SecureDallas 2013	Dallas, TXUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
SANS Forensics Prague 2013	OnlineCZ	Oct 06, 2013 - Oct 13, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced