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.

An Analysis of Terrorist Groups Potential Use of Electronic Steganography

The events of September 11th, 2001 have irrevocably altered the landscape of computer security. In the aftermath of these events, various urban legends and rumors have developed surrounding terrorists' online activities. One such topic has been in the alleged use of electronic steganography, a method to covertly hide messages within another, by terrorist groups. This paper provides an overview of steganography, its historical use during times of war, and how modern day electronic steganography can be accomplished. An o...

Copyright SANS Institute

Author Retains Full Rights

AD

An Analysis of Terrorist Groups' Potential
Use of Electronic Steganography

SANS Security Essentials GSEC Practical Assignment Version 1.3

Stephen Lau

February 18, 2003

Abstract

The events of September 11th, 2001 have irrevocably altered the landscape of computer security. In the aftermath of these events, various urban legends and rumors have developed surrounding terrorists' online activities. One such topic has been in the alleged use of electronic steganography, a method to covertly hide messages within another, by terrorist groups. This paper provides an overview of steganography, its historical use during times of war, and how modern day electronic steganography can be accomplished. An overview is provided of current techniques to detect steganography on the Internet, which have so far failed to uncover any evidence of steganography on the Internet, and possible future avenues of research in detecting online steganography using techniques similar to the Federal Bureau of Investigation's Carnivore system. The paper concludes with examples of the dangers of unsubstantiated steganography claims and privacy considerations in detecting online electronic steganography.

Introduction

The tragic events of September 11th, 2001 have caused a major reevaluation of security procedures within the United States. Overnight, seemingly normal events have become suspect. Potential terrorists and terrorist activity lurk in every aspect of United States life and culture. Although much of this increased awareness for security and of potentially suspicious activity is most likely an adverse short-term reaction to the September 11th events, it is obvious that many changes that have been set in motion since that date will be permanent. Fundamental changes in the approach to security both online and in real life are underway and will forever change our perceptions of both real life security and computer security.

Online criminal activity such as distributed denial of service attacks, web page defacements, cracker intrusions, are now perceived in a different light, especially by the mainstream American public. Long dismissed as being the online equivalent of teenage delinquency, they are now viewed as potential terrorist activity. An anti-terrorism bill, "USA Patriot Act"[24] recently enacted within the United States lists computer crimes such as web defacement and denial of service attacks as potential terrorist activity and subject to far more punitive damages than in the past. Government organizations, educational institutions and corporations are reviewing and removing or limiting access to information available on the Internet that can potentially be used for terrorist activity.

The capability of the Internet as a means of mass instant communication has helped to spread news and, unfortunately, rumors far and wide quite quickly. Instant urban legends appear almost daily. Not wanting to miss out on potential news stories, some of these

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

rumors have been picked up by the United States mainstream media, giving it more "credibility" in the eyes of a large majority of the American public. This has lead to a confusing mix of both information and disinformation. Have you heard the story of the man who "surfed" the debris down from the 86th floor of the World Trade Center? A false story reported on many mainstream media sources.[25] How about the school kid in New York City who looked out the window in his classroom a week before September 11th and told his teachers that they wouldn't be there next week? Strangely enough, this "urban legend" was actually true. [26][1][1]

For computer security professionals and law enforcement dedicated toward online activities, how does this affect our professions and how can we determine what is "true" and what is not? With limited resources available to combat potential terrorist threats, it is essential now more than ever that these limited resources be applied efficiently and effectively.

News stories began appearing in mainstream United States media in the days following September 11th reporting that Osama bin Laden and the al-Qaeda were using the Internet to covertly communicate between various terrorist cells to plan and relay information. Although news of the potential for the Internet to be used for terrorist activity has been percolating in the ocean of online criminal activity even before September 11th, [11][9] recent events have brought this potential to the forefront of attention. [8][3][22] One interesting aspect of the media reports was that the al-Qaeda were supposedly using a technique known as steganography to covertly communicate.[22]

Assuming that terrorists are using the Internet to covertly communicate, several questions arise. Is it possible to determine if there is actually covert communications occurring? What type of techniques could they be using? Are the rumors that covert communications actually true?

Background

Steganography is, in broad terms, embedding covert communications within seemingly innocuous communications. Only persons who have knowledge of the embedded information and possess a "key" will be able to decode and view the information. This key can take many forms. It can range from a passphrase for electronic steganography to an understanding of a method to decode the information. Unlike other forms of information hiding such as encryption, where both parties encrypt the information and transfer a cipher, steganography aims to prevent a third party from realizing that any covert communication has taken place. Steganography exploits communications that appear innocuous to a casual observer, using it as a cover medium to hide the underlying message. Clearly it is obvious that such a form of communication can be of interest to terrorist groups where the identities of the sender and receiver and the fact that the communication actually occurred are obscured.

Steganography requires various components to successfully encode, transmit and decode a hidden message. Foremost, steganography requires a cover medium to hide the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

underlying message. This cover medium can take many different forms. Selection of the cover medium is usually such that it would not attract attention to itself. The cover medium itself also must contain enough information such that any hidden message will not be noticeable.

Steganography as a form of information hiding is not a recent development.[10] An oft-mentioned example is a steganographic technique that was used in Roman times. A Roman General shaved the head of a slave and tattooed a message to the shaved head. After the hair grew back, the slave delivered the message by walking to the message's intended recipient who subsequently shaved the slave's head to reveal the hidden message. In this example, the cover medium was the slave, which, in Roman times, was not an unusual sight.

Along with the cover medium, some sort of information hiding method is required. This can also take many forms. In the previous example, the information hiding method was allowing the slave's hair to grow back. One would hope that the information that was being transmitted was not of a time critical nature. The subsequent method of unlocking this information was shaving the slave's head, revealing the tattooed information.

Additionally, the initial information that a message is to be steganographically transmitted and the method to unlock the message needs to be conveyed to the receiving party. This is usually done via an alternative method of communication, commonly called "out of band" communication. Once the first message has been steganographically transmitted, information pertaining to any subsequent steganographic transmissions can be transmitted within the first communication. Although in the example of the slave it is not given how the original transmission occurred, one can surmise that knowledge of this method of information transmission was exchanged at some prior point.

Finally, after the hidden information has been recovered, it is wise to destroy the cover medium containing the information. This will prevent subsequent analysis of the cover medium to reveal the hidden information. In our historical example, the final fate of the slave is left as an exercise for the reader. In instances where a cover medium is altered to produce a second copy containing information, the original cover medium should be immediately destroyed so that comparisons to the original can never occur.

In the 20th century, the use of steganography was common during wartime. During World War II, Great Britain's BBC routinely used steganography in their radio transmissions. Key, yet innocuous, phrases such as "The chair is against the wall" were interspersed within radio broadcasts. Only groups or individuals who knew that the phrase "The chair is against the wall" meant that Allies were expecting to bomb a particular city tomorrow were able to decode the information. The cover medium in this example was the radio transmissions, something that anyone with a radio receiver could intercept. French resistance operatives could receive this information while in the presence of Axis troops without their knowledge. Without both the knowledge that a message was being transmitted and the key to decode the message, it was close to impossible to determine that a transmission had actually occurred.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The perceived threat of steganography as a means for encoded information exchange during World War II caused the United States to prohibit international mailing of items that could be used to hide encoded messages. These included seemingly innocuous items such as children's report cards, newspaper clippings, crossword puzzles, chess game moves and knitting instructions. [23]

Modern Steganography

Modern steganographic methods include embedding electronic communications, such as a text message or an image, within another text message or image. Additionally, the message can also be encrypted to further conceal its content. For a successful encoding, a good cover medium must be utilized. For electronic steganography over the Internet, images are good candidates for cover medium. This is because a cover medium must contain enough information to hide the underlying message while subsequently not appearing to have been modified. It is also desirable for the cover medium to be common enough so as to not attract attention. Images on the Internet are both ubiquitous and can be created to contain enough cover information to hide the underlying message. [10]

A simple example of using images to steganographically hide a message is to modify the least significant bits of an image to encode the message. By modifying the least significant bit, the original image and the modified image appear identical to the human visual systems. The altered image can be sent via email to the intended recipient or posted on websites for recipients to download. Only persons who have knowledge of the hidden message will be able to decode and recover it. Although this method appears to work well, a simple statistical analysis of the image will usually reveal that additional information is hidden within it.

In recent years, more sophisticated techniques of steganography have evolved, specifically to defeat most standard methods of detecting steganography.[18] These involve analyzing the image prior to embedding the message to determine its statistical properties. By locating redundant bits of an image and probabilistically replacing the redundant bits with new information, one can defeat most basic statistical analyses. In addition, by subsequently modifying other portions of the image, one can recreate the "statistical" footprint of the original unmodified image that can thwart most attempts at statistical analysis.

One does not need to understand the complexities of message encoding to create a steganographic image. Freeware steganographic tools are readily available on the Internet. Most of these have easy to use point and click interfaces that enable a user to quickly encode information. Steganographic tools available on the Internet range from "StegFS"[14] a free steganographic file system to Windows based tools such as "S-Tools"[2], OutGuess[16], JSteg[12] and JPHide[13] to embed information within images.

The majority of current publicly available tools to embed information using JPEG images incorporate a passphrase to encrypt the message, thus further protecting it. Although this

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

further protects the underlying information, it is somewhat counter to the fundamental basis of steganography that relies on the encoding mechanism and the innocuous nature of the cover medium for its protection.

Accordingly, with the development and release of tools to steganographically hide information within images, various tools have also been developed and released to detect steganographic content.[20][19] Most of these tools use statistical analysis to detect steganographic content. Once an image is suspected to have information hidden within it, the majority of tools launch a dictionary attack to determine the passphrase that was used to encrypt the hidden information.

Although most of the initially available tools generated output that could be easily defeated by simple statistical analysis, various tools have appeared recently with more sophisticated information hiding and encryption algorithms that can escape simple forms of statistical analysis. For example, content encoded using the latest version of Outguess[16], a freely available tool on the Internet, is not detectable using most available tools to detect steganographic content. Similar to encryption technologies, new encoding techniques are being developed at the same rate as techniques to detect them.

Figure 1: One of these images contains embedded information.

Figure 1 shows two seemingly identical images. The left one contains steganographic information, in this case the first page of this document in ASCII format. The information was encoded into the left image using JPHide[13], a freeware steganography tool available for Windows. Approximately 4KB of information is hidden within the image on the left. It took approximately 1 minute to hide the information and write out the new JPEG file using the tool's point and click user interface. Subsequent extraction of the information from the image is also a simple point and click operation.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Locating Steganographic Content on the Internet

Although it is difficult to visually detect images that have been modified by steganography, it is possible to detect most steganographic images using statistical analysis. This is because most of the available tools available on the Internet generate output that can be statistically analyzed. Tools that have been developed to analyze images have so far been designed to analyze locally accessible images one at a time. In order to detect steganographic images on the Internet, one would have to be able to retrieve potential images off the Internet and analyze them.

One such analysis was done on images on Ebay, (http://www.ebay.com) an online auction site.[19] As part of Ebay's online auction service, Ebay allows sellers to post images or links to images of items that are available for sale. The analysis, done by Provos and Honeyman, developed a method to automatically extract images off Ebay searching for steganographic content and subsequently attempting to decode any content that they believed was hidden within the image.

Their technique involved three separate components. The first part consisted of the development of a web crawler specifically designed to extract URLs of JPEG images stored on a website. The web crawler, called "Crawl", automatically crawled through a website indexing images that met a certain criteria. The various criteria used to select images were user definable.

The second component of their system was called "Stegdetect". It was developed to detect steganographic images that were developed using three well-known steganographic systems available on the Internet. These were JSteg, JPHide and Outguess. By analyzing the method with which each of these systems encoded messages within images, they were able to develop potential signatures that could be used for detection. After analyzing all three system's encoding schemes, they discovered that none of the systems produced a clear signature, Subsequently, the false negative report rates ranged from 2% for JSteg to as high as 60% for Outguess. The false negative rate varied based on the size of the image and the size of the message being encoded. Running Stegdetect on a 333 MHz Celeron processor, they were able to achieve an analysis rate of 127KBps analyzing against all three steganographic systems.

The final component launched a dictionary attack against suspected images. The purpose of the dictionary attack was to attempt to determine the passphrase used to originally encode the message. This dictionary attack was distributed across several workstations. Of course the dictionary attack relied on the fact that the original creator of the image selected a weak password for the encoding.

After running this system against 2 million images located on Ebay, they were not able to locate any images that contained embedded information. Out of 2 million images, approximately 17,000 were flagged as potentially containing steganographic content. They processed all of these images with Stegbreak but were unable to locate any hidden

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

content. The group is now currently launching their system against images posted on USENET.

Their conclusions from the first round of images were the following: [19]

- There is no significant use of steganography on the Internet
- Nobody uses steganographic systems that we can find
- All users of steganographic systems carefully choose passwords that are not susceptible to dictionary attacks.

Future Directions

If terrorist groups are using the Internet for transferring steganographic images, the question becomes in detecting this usage. Current attempts at locating steganographic imagery on the Internet have focused on searching the Internet for imagery and then subsequently analyzing this imagery for steganographic content. So far these methods have failed to locate any steganographic imagery.

Although this "data mining" approach might eventually locate some sort of steganographic imagery, it is completely blind to images that are not posted on public websites or newsgroups. Many images are routinely transferred via email, chat programs such as Internet Relay Chat (IRC) and posted to numerous "members only" clubs, communities and groups, such as clubs.yahoo.com or communities.msn.com. Any data mining approach will ultimately miss transitory or restricted access caches of imagery that exist on the Internet. Additionally, it is quite conceivable that a data mining approach will spend most of its time on imagery that is rarely or never accessed by any user.

Since one can assume that the purpose of creating a steganographic image is for electronic distribution to the intended recipients, it is obvious that at some point this image will be electronically transferred from one location to another. With the purpose of electronic distribution in mind, it makes logical sense to narrow any type of search for steganographic imagery to images that are actually electronically transferred, ignoring images that are never electronically transmitted.

The majority of imagery transferred across the Internet utilizes well-known standards, such as JPEG or GIF. Both of these formats are documented and have well-established patterns that can be easily detectable.

For example, JPEG images utilize the "JPEG File Interchange Format" (JFIF).[30] According to the JFIF standard, any JPEG image has the following attribute:

1. A JFIF-standard file will start with the four bytes (hex) FF D8 FF E0, followed by two variable bytes (often hex 00 10), and followed by the ASCII string 'JFIF'.

Similarly, a GIF file will contain the string "GIF" within the file as one of its defining attributes.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Since most Internet protocols used to transfer images are of the stateful variety, i.e. IRC DCC, http, ftp, it is possible to determine when a block of data is being transferred, in our case an image. Using the stateful information of a connection in conjunction with the identifying headers of any JPEG or GIF image, it is conceivable to determine, by looking at network traffic, that an image is being transferred.

Recently, there have been many articles written about the United States's Federal Bureau of Investigation developing a system known as "Carnivore".[6] Although most of the details of the system are classified, it is known that the Carnivore system was meant to be placed at various Internet Service Provider's locations with the sole purpose of detecting and archiving unencrypted email transmissions. Although this appears technologically advanced, the concept behind Carnivore is not beyond the reach of currently available free tools or hardware. By splitting a site's border connection and running the resultant traffic through another system for analysis, it has already been shown that one can analyze and capture traffic at OC-12 rates and greater without significant loss. [4][15]

One can imagine a system, not unlike Carnivore that instead of looking for email looks for transmitted imagery. I will call this prototype system "Pixelvore" as homage to the original "Carnivore" system. Since the majority of websites are not SSL enabled, URL information is sent across clear text with the subsequent data being sent back unencrypted. One can envision the development of a system tapped directly into an Internet backbone with the sole purpose of looking for web based image requests, detecting it and subsequently capturing the imagery and saving it for offline analysis.

In a basic http transmission of a JPEG image, the requesting site opens a TCP connection (usually, but not necessarily on port 80) to a server. An ASCII string is sent across the connection, usually of the form GET <some ASCII string>. In response, the server will transmit back the JPEG image over the connection to the requestor. In a basic http connection, the connection is then torn down.

In concept, Pixelvore could sit somewhere between the two locations, capturing all TCP port 80 traffic, not unlike tcpdump. Background analysis of this captured traffic could analyze the initial traffic between the src/dst pairs looking for ASCII URL strings ending with the ".jpg" extension. This would potentially narrow the search down to src/dst pairs with JPG image transmissions. Isolating the subsequent reply traffic would potentially yield the JPEG image. Alternatively, using the JPEG standard, one could look for traffic that contained a JPEG header, however in either case it would be desirable to retrieve the original URL location of the image in case it is determined to contain steganographic content. Once the original images are captured, one could employ Stegdetect or something similar against these images.

Although such a system does not yet exist, at least not publicly announced, a compelling rationale for it would be in its non-invasive nature of searching for steganographic imagery. Neither the sending or receiving parties would be aware that their traffic was being monitored and analyzed for steganographic content. Such a system could be easily

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

tailored to monitor connections between two hosts, or group of hosts that are of interest, ignoring other traffic.

Like Carnivore, a system such as Pixelvore would attract privacy and ethical questions that are beyond the scope of this discussion. Although such a system would most definitely be challenged legally, history has shown that during times of crises, it is not beyond governments to censor or monitor its civilian population. As stated earlier, innocuous items such as children's report cards were banned from being mailed overseas during World War II by the United States government for fear of steganography.

Steganography Goes Mainstream

Even with easily accessible means to steganographically hide information within an image, one does not necessarily need sophisticated methods to encode information. Historic use of steganography has shown that low technology solutions have been highly effective.

In late September 2001, several posters appeared in Bangladesh and in Pakistan that raised the eyebrows of people familiar with the television show, "Sesame Street."[7] Bert, one of the characters on "Sesame Street" could be seen in one small corner of the poster. At first, various "experts" on terrorism claimed that the image of Bert was deliberately planted as a hidden message to sleeper terrorist cells in the United States. A Bangladesh entrepreneur subsequently claimed that he had created the poster by piecing together random images of Osama bin Laden he had found off the Internet. Strangely, the appearance of this poster in photos taken at Pakistan protests occurring on the same day as the protests in Bangladesh were never explained. One of the fallouts of this incident, along with other similar perceived threats of encoded messages from unreviewed video transmissions from Osama bin Laden, caused the United States government to request that United States media refrain from showing unreviewed video originating from the Middle East.

Figure 2 Bert and Osama bin Laden images[7]

The appearance of the character Bert on posters in Bangladesh coupled with the theories that this was a secret message caused mainstream media to scramble to explain steganography to the general public. Articles appeared in mainstream United States media outlets, such as Time Magazine and ABC News. In October, the ABC television show, "Primetime Live", addressed the issue of steganography on the Internet with live televised examples of decoding steganographic images. Unfortunately, the broadcast did

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

not clearly state that these images were fabricated for demonstrations purposes and were not, as implied, images found "in the wild" on the Internet.[21][17]

Conclusions

Although there have not been any steganographic imagery located on the Internet, it is quite conceivable that steganography is being used to covertly transmit information between different parties given the historic use of steganography. Tools are readily available to create steganographic images and they are becoming sophisticated enough so that normal methods of detecting steganographic content are ineffective.

As expected, the concept of using steganography on the Internet has attracted entrepreneurs to capitalize on the perceived threat. Several companies have announced products that will purportedly scan internal corporate networks for images containing steganographic images. One could assume this would be to locate employees who are covert terrorists lurking under the guise of productive employees. [29]

The United States legislature has also reacted to this perceived threat by enacting legislation that will allow the government to detect encoded images based on perceived threat. The "USA Patriot Act," signed on October 26, 2001 grants sweeping powers for the United States federal government to monitor electronic communication for terrorist activities. [24][5] The electronic communication portion of the act was passed even given the fact that there has yet to be any substantial proof that terrorist cells are using covert electronic communications.

The threat and fear of electronic steganography has the potential to be devastating for privacy concerns. One chilling example that recently occurred was the fate of Muzaffar Wandawi, a self taught artist living in the Netherlands. [28][27][26] In October 2001, various news services picked up a story that a "former National Security Agency instructor" had uncovered evidence on the Internet that al-Qaeda terrorists were hiding messages of the September 11th attack within images of paintings and posters on the Internet. The paintings were the work of Mr. Wandawi. Additionally, the "expert" stated that the images proved that they were planning a widespread biological attack against the United States and that Mr. Wandawi had intimate knowledge of these attacks since he had created these paintings with hidden messages. The reports and coverage in various United States newspapers and media outlets caused the United States government to issue a warning of heightened awareness for a potential terrorist attack. Upon further investigation, however, it was shown that Mr. Wandawi had no connections to terrorist groups and that there were no hidden messages within his paintings.

The concepts of computer security are currently in uncharted territories that are being mapped as we go. For computer security professionals faced with dealing with potential terrorist threats, the challenge is in understanding the threats, determining which ones are substantiated with evidence and which ones are urban legends or just plain wrong. Unfortunately, with the ever-shifting landscape these threats are changing on an almost daily basis. Urban legends that have been circulating the Internet for years, i.e. envelopes

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

sent through the mail contain deadly biological agents, can suddenly and tragically turn into reality. Although there have yet to be a single steganographic image found on the Internet, one can easily imagine how quickly the landscape will change again if an image is found containing credible evidence of a future terrorist attack. Are terrorists using the Internet for covert communications? Unfortunately, until credible evidence is found that they are, the only answer these days is "maybe".

References

[1] Alter, Jonathan, "Trade Center Warning Baffles Police", MSNBC, 10/12/01, http://www.msnbc.com/news/642074.asp?0si=-

[2] Brown, Andrew, S-Tools, http://members.tripod.com/steganography/stego/s-tools4.html

[3] Campbell, Duncan, "How the Terror Trail Went Unseen", Telepolis, 10/08/2001, http://www.heise.de/tp/english/inhalt/te/9751/1.html

[4] CoralReef, http://www.caida.org/tools/measurement/coralreef/

[5] Electronic Frontier Foundation, "EFF Analysis of the Provisions of the USA PATRIOT Act That Relate to Online Activities", 10/31/2001, http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html

[6] Federal Bureau of Investigations, "Carnivore Diagnostic Tool", http://www.fbi.gov/hq/lab/carnivore/carnivore.htm

[7] Harvey, Doug, "Sesame Osama", LA Weekly, 09/19/01, http://www.laweekly.com/ink/01/48/new-harvey.shtml

[8] Hoffman, Lisa, "How Terrorists Hide Messages Online", Scripps Howard News Service, 10/05/01, http://www.capitolhillblue.com/Article.asp?ID=22293

[9] Horvath, John, "The Internet: A Terrorist Network?", Telepolis, 08/22/01, http://www.heise.de/tp/english/inhalt/te/9350/1.html

[10] Johnson, Neil F., Jajodia, Sushil, "Steganography: Seeing the Unseen", IEEE Computer, February 1998

[11] Kelley, Jack, "Terror groups hide behind Web encryption", USA Today, 02/05/2001, http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm

[12] Korejwa, John, JSteg, http://www.tiac.net/users/korejwa/jsteg.htm

[13] Latham, Allan, JPHide, http://linux01.gwdg.de/~alatham/stego.html

[14] McDonald, Andrew, StegFS – A steganographic file system, http://www.mcdonald.org.uk/StegFS/

[15] Paxson, Vern, "Bro: A System for Detecting Network Intruders in Real Time", 1999, Proceedings of 1999 Computer Networks

[16] Provos, Niels, OutGuess – Universal Steganography, http://www.outguess.org

[17] Provos, Neils, "First Steganographic Image in the Wild", 10/12/01, http://www.citi.umich.edu/u/provos/stego/abc.html

[18] Provos, Niels, "Defending Against Statistical Steganalysis", 10th USENIX Security Symposium, August 2001

[19] Provos, Niels, Honeyman, Paul, "Detecting Steganographic Content on the Internet", ISOC NDSS'02, San Diego, CA

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[20] Provos, Niels, Stegbreak, http://www.outguess.org/detection.php
[21] Ross, Brian, "A Secret Language", ABC News, 10/04/01, http://abcnews.go.com/sections/primetime/DailyNews/PRIMETIME_011004_steganography.html
[22] Schneier, Bruce, "Terrorists and steganography", ZDNet, 09/24/01, http://www.zdnet.com/zdnn/stories/comment/0,5859,2814256,00.html
[23] "Tools for Privacy: The Ancient Art of Steganography", http://141.59.43.36/rz/www/stego.htm
[24] United States Patriot Act - http://www.house.gov/judiciary/hr2975terrorismbill.pdf
[25] Urban Legends Reference Pages, "Rumors of War (The Fall Guy)", http://www.snopes2.com/rumors/survivor.htm
[26] Urban Legends Reference Pages, "Rumors of War (Paint Your Dragon)", http://www.snopes2.com/rumors/wandawi.htm
[27] Wandawi, Muzaffar, http://www.wandawi.com/
[28] Wendland, Mike, "Online, conspiracy searchers find plots virtually everywhere", Detroit Free Press, 10/20/01, http://www.freep.com/money/tech/mwend20_20011020.htm
[29] WetStone, "WetStone Announces Stego Watch Service", 10/04/01, http://www.wetstonetech.com/pr0184.htm
[30] "JPEG File Interchange Format", 09/01/92, http://www.w3.org/Graphics/JPEG/jfif3.pdf

© SANS Institute 2001, Author retains full rights.

Last Updated: October 23rd, 2014

Upcoming SANS Training

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

SANS Cyber Defense San Diego 2014	**San Diego, CAUS**	**Nov 03, 2014 - Nov 08, 2014**	**Live Event**
SANS DFIRCON East 2014	**Fort Lauderdale, FLUS**	**Nov 03, 2014 - Nov 08, 2014**	**Live Event**
SANS Sydney 2014	**Sydney, AU**	**Nov 10, 2014 - Nov 22, 2014**	**Live Event**
SANS Korea 2014	**Seoul, KR**	**Nov 10, 2014 - Nov 15, 2014**	**Live Event**
SANS Tokyo Autumn 2014	**Tokyo, JP**	**Nov 10, 2014 - Nov 15, 2014**	**Live Event**
Pen Test Hackfest	**Washington, DCUS**	**Nov 13, 2014 - Nov 20, 2014**	**Live Event**
SANS London 2014	**London, GB**	**Nov 15, 2014 - Nov 24, 2014**	**Live Event**
SANS Hyderabad 2014	**Hyderabad, IN**	**Nov 24, 2014 - Nov 29, 2014**	**Live Event**
Healthcare Cyber Security Summit	**San Francisco, CAUS**	**Dec 03, 2014 - Dec 10, 2014**	**Live Event**
SANS Cyber Defense Initiative 2014	**Washington, DCUS**	**Dec 10, 2014 - Dec 19, 2014**	**Live Event**
SANS Oman 2015	**Muscat, OM**	**Jan 03, 2015 - Jan 08, 2015**	**Live Event**
SANS Security East 2015	**New Orleans, LAUS**	**Jan 16, 2015 - Jan 21, 2015**	**Live Event**
SANS Gulf Region 2014	**OnlineAE**	**Nov 01, 2014 - Nov 13, 2014**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**