GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Stephanie R. Betancourt GSEC Practical Version 1.2f

Steganography: A New Age of Terrorism

"Steganography is the art and science of communicating in a way which hides the existence of the communication' (Johnson). According to nameless "U.S. officials and experts" and "U.S. and foreign officials," terrorist groups are "hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites" (Schneier). Three years ago, FBI Director Louis Freeh tried to convince government authorities that terrorists were using encryption and steganography to support their organizations. Freeh urged legislators to enact stricter Internet usage laws, emphasizing that ignoring the issue would not only cause harm to the United States, but that it would make the fight against terrorism extremely difficult (McCullagh). Today, terrorist organizations such as Hamas, Hezbollah, al Qaeda, and others, are employing advanced steganography techniques to pass sensitive communications across the Internet, undetected. In the wake of several highly coordinated and deadly terrorist attacks, the United States government, and indeed, the world, is hastening to discover viable methods for the detection and prevention of this electronic subterfuge, in the hope that denying criminal networks (the use of the Internet as a communications medium) will render them incapable of mounting another attack that could cost more lives.

History of Steganography

The darker sides of governments have utilized forms of steganography for decades. In WWII, German spies used null ciphers, which "camouflaged" the real message inside an innocent "sounding" message (Johnson).

The following message was actually sent by a German Spy in WWII:

```
Apparently neutral's protest is thoroughly discounted and
ignored. Isman hard hit. Blockade issue affects pretext for
embargo on by products, ejecting suets and vegetable oils.
```

Taking the second letter in each word produces the following message:

```
Pershing sails from NY June 1 (Kahn 67).
```

As message detection improved, the clandestine world was forced to develop new technologies, which could pass more information and be even less conspicuous. In 1941, the first microdots were discovered "masquerading as a period on a typed envelope carried by a German agent" (Johnson). FBI Director, J. Edgar Hoover referred to the microdot as "the enemy's masterpiece of espionage." The message was not hidden, nor encrypted; it was just so small, that it went unnoticed. The microdot permitted the transmission of large amounts of data including maps, photographs, documents, and drawings. With swarms of letters passing through the mails, the United States government panicked. By the end of the war, censors had either prohibited or tampered with flower deliveries, radio song requests, weather reports, children's drawings sent in the mail, knitting instructions, and anything else that might possibly encode Axis intelligence

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

(Dibbell). In addition to using the microdot, another well-publicized steganography event occurred during the height of the Vietnam War. Commander Jeremiah Denton, a naval aviator, had been shot down and captured by North Vietnamese forces. Denton was paraded in front of the news media; Denton, knowing he would be unable to say anything critical of his captors, spoke to the media, while speaking, he blinked his eyes in Morse code, spelling out *T-O-R-T-U-R-E* (Carvin).

Steganography Today

Perhaps the most public accusation regarding steganography occurred several weeks ago when the Arab-language news service *al Jazeera* broadcast videotaped statements by Osama bin Laden and his associates. The Bush administration quickly responded by requesting that all media use greater discretion when it came to airing statements from Al Qaeda, fearing that the unedited statements might contain secret messages -- being communicated by certain words or phrases, combinations of clothing, or discrete nonverbal gestures (Carvin).

With the historical link between terrorists and steganography, it comes as no surprise that Middle East terrorists groups such as Hizbollah, Hamas, and bin Laden's al Qaeda, were using computerized files, email, encryption, and steganography to support their organizations (Pleming). Bin Laden's followers downloaded steganography software and other easy-to-download encryption software to carry out several plots. Wadih El Hage, one of the suspects in the 1998 bombing of two U.S. embassies in East Africa, sent encrypted e-mails under various names to associates in al Qaeda. Khalik Deek, an alleged terrorist arrested in Pakistan in 1999, used encrypted computer files to plot bombings in Jordan at the turn of the millennium. Ramzi Yousef, the convicted mastermind of the World Trade Center bombing in 1993, used encrypted files to hide details of a plot to destroy 11 U.S. airliners. Two of the files, FBI officials say, took more than a year to decrypt (Kelley).

Officials say the Internet has become the modern version of the "dead drop," a slang term "describing the location where Cold War-era spies left maps, pictures and other information" (Kelley). But unlike the "dead drop," the Internet is proving to be a much more secure way to conduct clandestine warfare (Kelley). "Who ever thought that sending encrypted streams of data across the Internet could produce a map on the other end saying 'this is where your target is' or 'here's how to kill them'?" says Paul Beaver, spokesman for *Jane's Defense Weekly* in London. "And who ever thought it could be done with near perfect security? The Internet has proven to be a boon for terrorists" (Kelley). Prior to September 11th, Mohamed Atta was seen using his Hotmail account at the public libraries in Florida to surf the Internet, downloading what appeared to be pictures of children and scenes of the Middle East (Ross). Consequently, it was from an electronic "dead drop" that the terrorists were believed to have received their final orders in coded message" (Greene).

What is Modern Steganography?

To a computer, an image is an array of numbers that represent light intensities at various points, or pixels. Digital images typically have either 24 bits or 8 bits per pixel. Each bit points to an associated color in a color index, or palette. In 8-bit color images, each pixel, which points to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

one of 256 colors on the palette, is represented as a single byte (Sellars). A byte is made up of 8 bits, and each bit is either a 0 or a 1. An example of a byte is 1111 1110. The position where the 0 is located is known as the least significant bit. The Least Significant Bit (LSB) method is the steganography technique most commonly implemented. When applying LSB techniques to each byte of a 24-bit image, three LSB bits can be encoded into each pixel (24 bits / 8 (1 byte) = 3 bytes). Any changes in the LSB will produce an image indistinguishable from the original. Unfortunately, while this technique works well for 24-bit images, one must be cautious when dealing with 8-bit images. When modifying the LSB in 8-bit images, pointers to entries in the palette are changed (Johnson). In other words, a bit change could mean the difference between a shade of blue or a shade of green.

Two files are used in this type of digital messaging. The innocent looking file, that holds the hidden information, is a "container," and the information to be hidden is the "message." A container may be a sound file, an image, spam mail, or anything large enough to hold the data. A message may be plain-text, ciphertext, other images, or anything that is small enough to be embedded in the least significant bits (LSB) of an image (Johnson). Modern steganography is the process of hiding one message file inside a container file by manipulating the least significant data to hide the message. The container image or sound file is changed in such a way, that a human eye or ear cannot detect it. While steganography may sound a bit devious, this technique was actually designed to prevent the illegal distribution of documents through modern electronic means. Without it, infringers could make identical copies of documents without paying the original author (Sellars).

Steganography Software

There are currently over 140 steganography programs available. The tools range from software that hides data in images to software that hides data in spam. Steganography programs are freely available and easy to use. Unfortunately, these two benefits have enabled terrorists to not only correspond for free, but to hide their plots without the threat of being caught.

S-Tools 4.0

Steganography Tools (S-Tools) for Windows includes several programs that process GIF images, BMP images, and audio WAV files. S-Tools will even hide information in the "unused" areas on floppy diskettes (Johnson). In addition to supporting 24-bit images, S-Tools also includes a variety of encryption routines including IDEA, MDC, DES, and Triple DES.

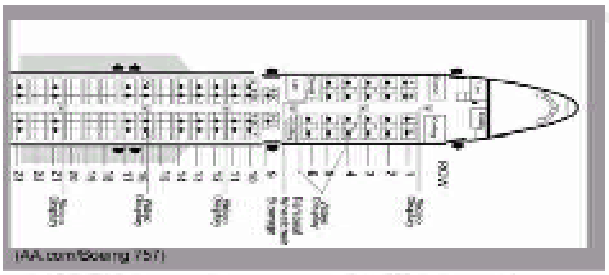
S-Tools applies the LSB methods to both images and audio files. A very useful feature is a status line that displays the largest message size that can be store in an open container file. This eliminates the possibility of attempting to store a message that is too large for a container. After hiding the message, the steganographic image will be displayed, and the original image will remain on the screen so that the new and original images can be compared.

S-Tools is not only easy to use, but appears to be quite secure, and the software does an impeccable job of concealing the data. Andy Brown, the creator of S-Tools, explains what makes this program so secure:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

S-Tools works by 'spreading' the bit-pattern of the message file to be hidden across the least-significant bits of the color levels in the image. S-Tools tries to reduce the number of image colors in a manner that preserves as much of the image detail as possible. It is difficult to tell the difference between a 256-color image and one reduced to 32…to further conceal the presence of a file, S-Tools picks its bits from the image based on the output of a random number generator. This is designed to defeat an attacker who might apply a statistical randomness test to the lower bits of the image to determine whether encrypted data is hidden there. The random number generator used by S-Tools is based on the output of the MD5 message digest algorithm, and is not easily (if at all) defeatable.

To demonstrate the ease of use, here is a general breakdown of how to hide and extract data using S-Tools. Simply use Windows Explorer or File Manager to drag and drop the container into the workspace. Similarly, drag and drop the message file into the container file. If the message has been hidden correctly, then a pop-up window will reveal the number of bytes hidden, and from this point a passphrase and an encryption algorithm may be applied to further secure the message. To apply an encryption algorithm, enter the passphrase and choose an encryption algorithm, the steganographic image is complete. In order for the message to be retrieved from the container, the recipient must know both the encryption algorithm and the passphrase to gain access to the message. Below is an S-Tools demonstration. Which Mona Lisa is hiding the Boeing 757 airplane map? The photo on the right is the one with the hidden image.



(Graphics provided by **Brian Ross**)

JSteg Shell Version 2.0

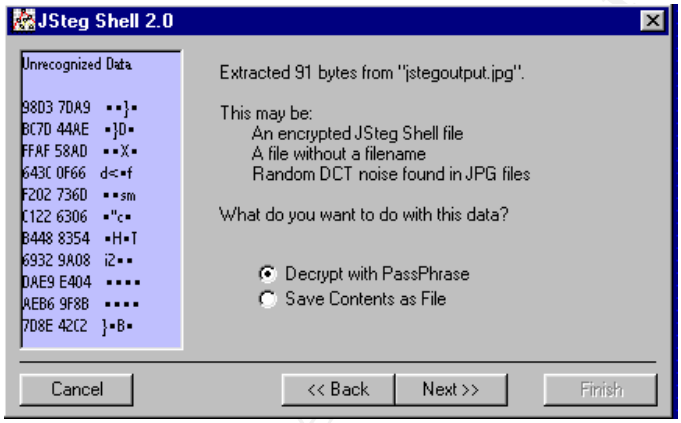
JPEG images are becoming more abundant on the Internet because large images with unlimited colors can be stored in relatively small files. For example, a 1073 x 790 pixel image with 16 million colors can be stored in a 170-kilobyte file. As a BMP, the same image would be more than 2 Megabytes (Johnson). JSteg shell is a Windows Shell. That means that it looks and runs like any other windows program, but to perform its primary task, it feeds commands to another program (jpeg-jsteg for DOS) (Korejwa). Jsteg is quite simple to use, and manipulation of the container image is near impossible to detect.

To use JSteg Shell, launch the program and choose *Hide File in JPG Image*. After the message file is selected, an RC4-40 encryption algorithm may be applied to the message by entering a passphrase. Applying an encryption algorithm to the message file is always a good idea because

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

it enforces "defense in depth." In other words, if an enemy retrieves the steganographic image, then the encryption algorithm will still have to be broken to retrieve the hidden message. Once the message file is chosen, JSteg reveals the amount of data that needs to be hidden (in bytes). A container file must be chosen. If the container is not big enough to hide the message, then an error message will be displayed. If the message is successfully hidden, then the new, steganographic image can be saved or viewed.

Retrieving a file is just as simple as hiding the file. It is basically the same process with a few minor adjustments. Choose *Extract File from JPG Image*. Select the steganographic image- using *Find,* and DJPEG.EXE will extract the data. If JSteg Shell finds hidden data that it does not recognize, then the screen below will be displayed; otherwise, this screen is skipped.



Choose *Decrypt With PassPhrase* if the ciphertext and the key are known. The data on the left of the above image is the first few bytes of the extracted data. If the file did not have JSteg Shell headers, then examining these bytes could reveal the identity of the file (Korejwa). To further examine the data, right click on the data, and a popup menu with *Bit Count Test* and *Password File Search* will appear. *Bit Count Test* will run a simple test to try to identify the data as ciphertext. *Password File Search* will try every password in a text file to try to decrypt the data. Finally, choose the filename to save the extracted data as, and read the secret message.

Spam Mimic

One of the newest spins on Steganography includes a website called Spam Mimic, where users can embed encrypted messages in spam in order to disguise the fact that confidential data has been exchanged. To use Spam Mimic, simply go to the site and choose 'encode' from the menu, type in a short message, and press enter. This generates a realistic spam message with the secret message imbedded inside it. The spam message can then be cut and pasted into an email client. Upon receiving the message, the email recipient can use the Spam Mimic website to 'decode' the spam, and retrieve the original message.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

One flaw in the software is that there is no limit on the size of the message to be encoded. Consequently, a large message will be encoded, but the spam will begin to repeat itself, which could possibly arouse suspicion. Furthermore, the site enforces government surveillance systems, similar to Echelon, to scan through Terabytes of spam on the off chance that they may contain encrypted messages of interest to the authorities (Leyden). In other words, make sure that if you are going to use Spam Mimic that it is only for legal, legitimate purposes.

Steganography Detection

Iomart, a Scottish broadband provider and corporate spyware vendor, recently leaked some information about being "called in" by "U.S. authorities" to help in the /bin/laden hunt, and about finding Al Qaeda steganographic files on "the dark side of the Web" (Greene). The company "has identified.... hundreds of files, some of them containing Arabic text and dates" (Greene).

So what's being done to protect U.S. citizens from future terrorist plots residing on the Web? In 1998, the Air Force commissioned WetStone Technologies "to develop a set of statistical tests capable of detecting secret messages in computer files and electronic transmissions, as well as attempting to identify the underlying steganographic method" (McCullagh). Thus, WetStone's "Steganography Detection and Recovery Toolkit" (S-DART) was born. Gary Gordon, vice president of cyber-forensics at WetStone Technologies, reported that while most of the steganography found has been on hacker sites, several instances have been reported on heavily traveled commercial sites such as Amazon and eBay (McCullagh). In addition to S-DART, Neil Johnson has been developing a stego-detector for the past several months. The program is designed to examine hard drives "like a virus scanner" and identify the electronic fingerprints left behind by steganographic applications. In February, Johnson helped nab a suspect who raised suspicions after repeatedly emailing photographs to addresses that appeared to be of family members, but he never received any replies (McCullagh). Unfortunately, if this technology is being implemented in the background, bin Laden and his cohorts somehow managed to slip through the cracks.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

As far as the Government is concerned, there have been a few suggestions made known to the public. One suggestion is that the NSA could keep a database of images, which would help them identify images with subtle changes in the low order bits (Schneier). U.S. officials concede that it is difficult to intercept, let alone find, hidden messages and images on the Internet's estimated 28 billion images and 2 billion Web sites (Kelley). Neil Johnson explains, finding files tainted by steganography is like "looking for a piece of straw in a haystack – forget the needle" (Dibbell). The FBI wants all encryption programs to file what amounts to a "master key" with a federal authority that would allow them, with a judge's permission, to decrypt a code in a case of national security (Kelley). Senator Judd Gregg proposed that "software developers give government security agents the 'keys' to encryption programs when they are created," this position is strongly opposed by many in the technology community who worry it could be used to invade the privacy of law-abiding computer users (Eunjung Cha, Krim).

On October 26, President Bush and Attorney General John Ashcroft convinced Congress to pass the Anti-terrorism Act. The acts gives the police expanded power to wiretap the phone of suspected terrorists, keep tabs on their email, and track their Internet activity. Still, if a steganographic image cannot be found, or if a type of encryption cannot be cracked, then America is still at risk of having terrorist plots right under her nose without anyway to intercept them.

Conclusion

While steganography may offer valuable solutions to the privacy concerns that plague the Internet, it also offers an easy way for criminals to plan their crimes and hide their intentions. Steganography is playing a big part in the world of terrorists. Although it appears that the government is indeed trying to eradicate the relationship between terrorists and steganography, one thing is for sure, the U.S. counter-terrorism effort failed September 11, costing many lives.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Works Cited

Brown, Andy. *S-Tools for Windows*. Shareware 1994.
URL: http://www.webattack.com/get/stools.shtml

Carvin, Andy. "When a Picture Is Worth a Thousand Secrets: The Debate Over Online Steganography." 31 October 2001. URL: http://www.benton.org/DigitalBeat/db103101.html (21 Nov. 2001).

Declan, McCullagh. "Bin Laden: Steganography Master?" 7 February 2001.
URL: http://www.wired.com/news/politics/0,1283,41658,00.html (1 Nov. 2001).

Dibbell, Julian. "Pirate Utopia." 20 February 2001.
URL: http://www.feedmag.com/templates/default.php3?a_id=1624

Eunjung Cha, Ariana and Eunjung Cha, Krim, Jonathan. "Terrorists' Online Methods Elusive U.S. Agencies Seek Experts' Help in Tracing Encrypted Messages." 19 September 2001.
URL: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A52687-2001Sep18

Greene, Thomas C. "iomart cashes in on WTC tragedy." 11 November 2001.
URL: http://www.theregister.co.uk/content/archive/22154.html (1 Nov. 2001).

Johnson, Neil. "Steganography." URL: http://www.jjtc.com/stegdoc/index2.html (1 Nov. 2001).

Kahn, David. The Codebreakers. New York, NY: The Macmillan Company, 1967. p. 67.

Kelley, Jack. "Terror groups hide behind Web encryption." 19 June 2001.
URL: http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm

Korejwa, John. "JSteg Shell 2.0 Screen Shots." URL: http://www.tiac.net/users/korejwa/jstegscreenshot.htm

Leyden, John. "Website combines spam with encryption." 15 December 2000
URL: http://www.theregister.co.uk/content/archive/15521.html

Kuhn, Markus. "Steganography Mailing List." 5 July 1995.
URL: http://www.jjtc.com/Steganography/steglist.htm,

Pleming, Sue. "Muslim Extremists Utilize Web Encryption." 6 February 2001.
URL: http://www.techtv.com/news/hackingandsecurity/story/0,24195,3310112,00.html (1 Nov. 2001).

Ross, Brian. "A Secret Language Hijackers May Have Used Secret Internet Messaging Technique." 4 October 2001. URL: http://abcnews.go.com/sections/primetime/dailynews/primetime_011004_steganography.html

Schneier, Bruce. "Bruce Schneier on crypto, the FBI, privacy and more." 3 October 2001.
URL: http://www.theregister.co.uk/content/archive/21993.html

Sellars, Duncan. "An Introduction to Steganography."
URL: http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html (1 Nov. 2001).

Sieberg, Daniel. "Bin Laden exploits technology to suit his needs." 21 September 2001.
URL: http://www.cnn.com/2001/US/09/20/inv.terrorist.search/

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.