Hidden Channels, Steganography, and the Research Professional

The use of hidden messages—i.e., messages that are available only to people who know what to look for, where, and when—has been with us for centuries. Herodotus tells how a message about Xerxes' hostile intentions was passed to the Greeks underneath the wax of a writing tablet. In ancient China, code ideograms were embedded at prearranged positions in dispatches. During the Middle Ages, monarchs used the grille system, where a wooden template was placed over a seemingly innocuous text, highlighting a secret message beneath.

Today, hidden messages are an integral part of the communications world, so the practitioner needs to be aware of this field. The practitioner also needs to be cognizant of the limits of open source searches when dealing with what are called "hidden channels" or "hidden pipelines" on the Internet.

Many people concentrate on the World Wide Web (WWW, hereafter referred to as "the Web") as the place to find hidden messages, but OSINT professionals need to understand that virtually all parts of the Internet can be used as covert communications media. The Internet is actually a combination of many services, of which the Web is but one. The Web is often and incorrectly thought of as *the* communications resource, but just as there are non-Internet open source nodes, there are a number of Internet-related but non-web channels, many of which are available for secret communication. These include:

- E-mail
- Newsgroups
- FTP
- Telnet
- Archie
- WAIS (Wide Area Information Server)
- Gopher
- Veronica
- InterNIC
- Finger.

Many of these Internet channels can be used as hidden pipelines or channels to communicate. Researchers should be aware of their potential in that role, as well as the difficulties, drawbacks, and problems associated with the more exotic, less-understood, and seldom-used channels.

These hidden channels often span the worlds of open source and cryptology. Governments develop complex codes and ciphers for their people to communicate securely. Nongovernmental individuals and entities seldom have such exotic, made-to-order means

available. They have to rely on a combination of ingenuity and the world of commercial encryption programs to provide a high level of security

A number of tools allow users to hide information "in the open." Many of these tools fall under a category called steganography, or the technique of hidden writing. Steganography—also called stego—has been defined as "security through obscurity." A carrier file contains a hidden message but is designed so that no one except the originator and the intended recipient even suspects that a covert message exists. The ingenuity of people trying to hide information in this way should never be underestimated.

Stego can be stored and transmitted within a variety of formats. Audio channels, visual channels such as pictures and videos, and even message headers can all be used as stego carrier files. These carrier files can be e-mailed, loaded into web pages, embedded in USENET files, and placed in files that can only be accessed using such relatively little-used Internet resources as FTP. The type of carrier file used to contain the stego message, and the location of that carrier file, is extremely difficult to predict.

A one-of-a-kind picture—think home snapshot or scene photographed on a vacation—often serves as a better carrier file than a picture that is widely available on the Internet because there is nothing to compare its file size against. If a music file is used as a carrier, an obscure piece of music that is otherwise unavailable on the Internet is the preferred choice because, again, there is nothing to compare its size or tonal quality against.

Stego works because it uses computer code. Computers don't actually transmit a picture, nor do they send musical notes. Sequences of 1s and 0s, called "bytes," are used to substitute for letters and numbers in text. Those 1s and 0s are a code that can also be interpreted by the computer to create dots of color or musical notes. Changing just the last number—the least important bit—of a computer bit won't be really noticeable to the human eye or ear, but to the computer that last bit alteration is a change that can be used to hold one element of a hidden message.

As difficult as locating steganographic files on the Internet can be, extracting the hidden data is even more difficult. Again, if the message is encrypted, it enters a level beyond difficult.

To see an example of how stego works, download the program Invisible Secrets (version 2.1) for free at either of these locations:
http://invisible-secrets.en.softonic.com/?kcid=786ed8f5-9d86-dcc8-2ba1-00007af52e5a&kmed=ppc&ptn=enat2&gclid=CMrTw86Wz68CFQUaQgodbV9NEw
http://www.invisiblesecrets.com/ver2/index.html

Save and open the program on your computer.

Next, go to http://stegosite.weebly.com .

On the first page, you will see two photos of the world as it looks from space at night.

Download both photos to your computer. (It is often easiest to download them to the documents file or directly to the desktop.) Note their file names.

Go to the location on your computer where you downloaded the photos. Right click (if you are using a right-handed mouse) on the icon for one of the downloads and a short menu will appear. Go the bottom of that menu and click on "Properties." On the "General" tab, note the "Size" (not "Size on Disk"). Repeat this process for the second picture file. Notice that there is a difference in the size of the files. Note which file is larger.

Now open the Invisible Secrets program from the "Start>All Programs" menu.

Right click the Invisible Secrets icon that has the "?" on it. That should bring up a welcome screen in a pop-up window. Read it and right click "Next."

You should see Step 1 on the new pop-up window. Click the radio button to "extract and/or decrypt files from a carrier file," then right click "Next."

You will see Step 2. Find the location where you downloaded the files. In the new pop-up window, enter the full computer address of the larger of the two carrier files you downloaded.

(The address will probably look something like *c:\some folder\another folder\file name*.) Make certain the carrier type says "JPEG image." Right click "Next."

On the Step 3 pop-up, enter the password "pass" (all letters lower case and no quotes around the word). Leave the decryption algorithm as "Blowfish/CBC" and right click "Next."

That will bring up a new pop-up titled "Step 4: Unhide/Decrypt Data." You should see the address of a destination folder on your computer and a checked box. Right click "Next." It may take a moment for the program to pull the message out. A new pop-up will appear saying "Unhiding/Decrypting." Right click "Explore Extracted Data." A new list will pop up showing a text icon and the name of the text file with a "txt" extension. Right click it and read the message.

Clicking "Finish" on the Invisible Secrets program file will take you back to the start of the program. Clicking "Exit" will take you out of the program.

Return to http://stegosite.weebly.com.

Go to the second page of the site, entitled "See the Difference?"

Download the picture of a white block. Note the name of the file.

If you closed the Invisible Secrets program, reopen it. If you didn't exit the program before, you should be at Step 1. If you did close the program, start with the welcome screen you saw earlier. Right click "Next." You should see Step 1 on the new pop-up window. In either case, once you are on Step 1, click the radio button to "extract and/or decrypt files from a carrier file," then right click "Next."

You will see Step 2. Select "Carrier File." Find the location where you downloaded the file. In the new pop-up window, enter the full computer address of the carrier file you downloaded. (It will probably look like *c:\some folder\another folder\file name*.) Make certain the carrier type says "JPEG image." Right click "Next."

On the Step 3 pop-up, enter the password "pass" (again, all letters lower case and no quotes). Leave the decryption algorithm as "Blowfish/CBC" and right click "Next."

That will bring up a new pop-up called "Step 4: Unhide/Decrypt Data." You should see the address of a destination folder on your computer and a checked box. Right click "Next." It may take a moment for the program to pull the message out. A new pop-up will appear saying "Unhiding/Decrypting." Right click "Explore Extracted Data." A new list will pop up showing a text icon and the name of the text file with a "txt" extension. Right click it and read the message.

"Finish" will take you back to the start of the program; "Exit" will close it. You can close the program or return to it and create your own stego file using the smaller of the two nighttime lights photo or any other jpg file you wish. Just follow the directions as you go along.

This example uses only one of many stego programs available. Remember that stego can be inserted into many different types of files. Then mentally multiply that by the number of ways the stego file can be moved and stored—e-mail, page on a web site, in a newsgroup, etc. Multiply that by the number of possible passwords to access the file. If the message within the file is encrypted, there is an additional problem. Finding stego material on the Internet and using it makes discovering a needle in a haystack an easy day!