Steganography FAQ

Aelphaeis Mangarae [Zone-H.Org]

March 18th 2006

http://zone-h.org

Table Of Contents

Introduction

Steganography is a subject which is rarely touched upon by most IT Security Enthusiasts.
Most people don't see Steganography has a potential threat, some people don't even know what Steganography is.
With this FAQ I hope to answer any questions anyone may want to ask about Steganography, and to educate people so they can understand what exactly Steganography is.
Is Steganography a potential threat? Well your about to find out.

What Is Steganography?

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out of the usual.
Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information.
The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all.
If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.
Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing).
Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file.
What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.)
The most common use of Steganography is to hide a file inside another file.
When information or a file is hidden inside a carrier file, the data is usually encrypted with a password.

Steganography Terms

Carrier File – A file which has hidden information inside of it.

Steganalysis – The process of detecting hidden information inside of a file.

Stego-Medium – The medium in which the information is hidden.

Redundant Bits – Pieces of information inside a file which can be overwritten or altered with out damaging the file.

Payload – The information which is the be concealed.

History Of Steganography

Through out history Steganography has been used to secretly communicate information between people.

Some examples of use of Steganography in past times are:

1. During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper.
Liquids such as urine, milk, vinegar and fruit juices were used, because when each one of these substances are heated they darken and become visible to the human eye.

2. In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secret message.

3. Another method used in Greece was where someone would peel wax off a tablet that was covered in wax, write a message underneath the wax then re-apply the wax.
The recipient of the message would simply remove the wax from the tablet to view the message.

How Does It Work?

There are numerous methods used to hide information inside of Picture, Audio and Video files. The two most common methods are **LSB (Least Significant Byte)** and **Injection.** I will discuss these two methods below.

Substitution - Altering/Replacing The LSB

When files are created there are usually some bytes in the file that aren't really needed, or at least aren't that important.
These areas of the file can be replaced with the information that is to be hidden, with out significantly altering the file or damaging it.
This allows a person to hide information in the file and make sure that no human could detect the change in the file.
The LSB method works best in Picture files that have a high resolution and use many different colors, and with Audio files that have many different sounds and that are of a high bit rate.
The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside the file, the file can become noticeably distorted.

Injection

Injection is quite a simple method which simply involves directly injecting the secret information into the carrier file.
The main problem with this method is that it can significantly increase the size of the carrier file.

Steganography In Images

When hiding information inside images the LSB (Least Significant Byte) method is usually used.
To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image.
The best type of image file to hide information inside of is a 24 Bit BMP (Bitmap) image.
The reason being is this is the largest type of file and it normally is of the highest quality.
When an image is of high quality and resolution it is a lot easier to hide and mask information inside of.
Although 24 Bit images are best for hiding information inside of due to their size some people may choose to use 8 Bit BMP's or possibly another image format such as GIF, the reason being is that posting of large images on the internet may arouse suspicion.
It is important to remember that if you hide information inside of an image file and that file is converted to another image format, it is most likely the hidden information inside will be lost.

Steganography In Audio

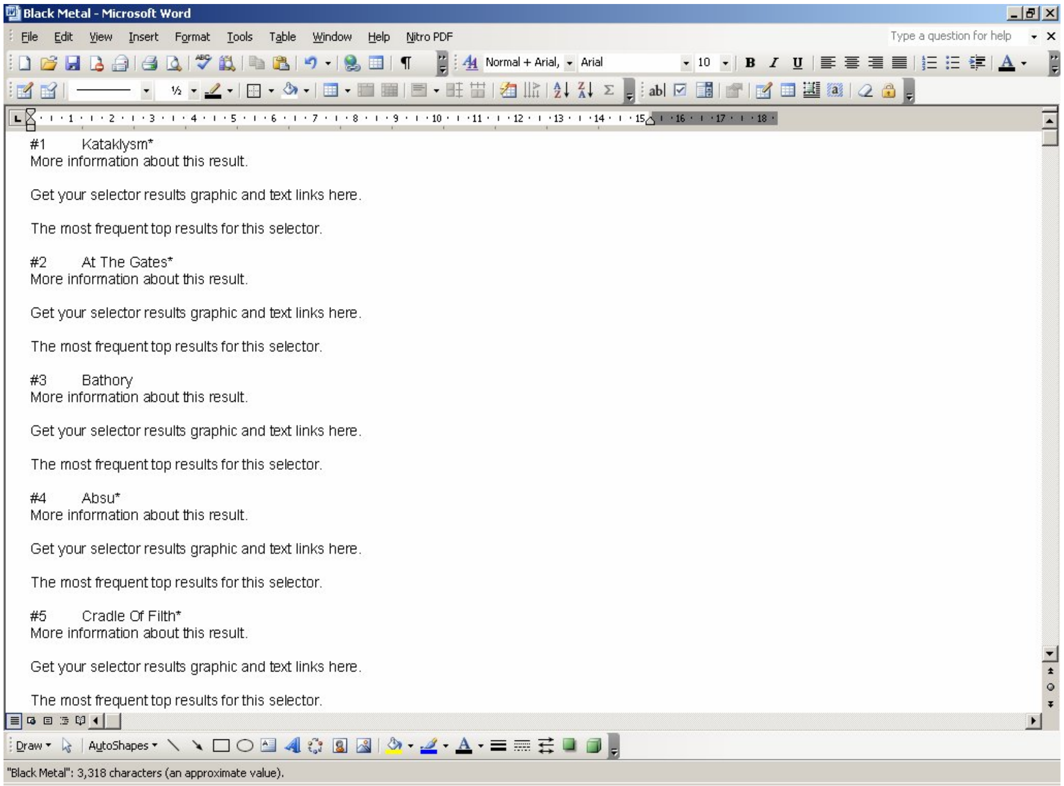
When hiding information inside Audio files the technique usually used is low bit encoding which is some what similar to LSB that is generally used in Images.
The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file.
Spread Spectrum is another method used to conceal information inside of an audio file.
This method works by adding random noises to the signal the information is conceal inside a carrier and spread across the frequency spectrum.
Echo data hiding is yet another method of hiding information inside an audio file.
This method uses the echoes in sound files in order to try and hide information.
By simply adding extra sound to an echo inside an audio file, information can be concealed.
The thing that makes this method of concealing information inside of audio files better than other methods is that it can actually improve the sound of the audio inside an audio file.

Steganography In Video

When information is hidden inside video the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method.
DCT works by slightly changing the each of the images in the video, only so much though so it's isn't noticeable by the human eye. To be more precise about how DCT works, DCT alters values of certain parts of the images, it usually rounds them up.
For example if part of an image has a value of 6.667 it will round it up to 7.
Steganography in Videos is similar to that of Steganography in Images, apart from information is hidden in each frame of video.
When only a small amount of information is hidden inside of video it generally isn't noticeable at all, however the more information that is hidden the more noticeable it will become.

Steganography In Documents

Steganography can be used in documents? Yes it’s true!
The use of Steganography in documents works by simply adding white space and tabs to the ends of the lines of a document.
This type of Steganography is extremely effective, because the use white space and tabs is not visible to the human eye at all, at least in most text/document editors.
White space and tabs occur naturally in documents, so there isn’t really any possible way using this method of Steganography would cause someone to be suspicious.
The most popular piece of software used to perform this type of Steganography is a piece of software called **SNOW.**
Below is a picture of a Word document before I have used SNOW to conceal a hidden message.


Black Metal - Microsoft Word
File Edit View Insert Format Tools Table Window Help Nitro PDF
Type a question for help
Normal + Arial, Arial 10
Draw AutoShapes

#1 Kataklysm*
More information about this result.

Get your selector results graphic and text links here.

The most frequent top results for this selector.

#2 At The Gates*
More information about this result.

Get your selector results graphic and text links here.

The most frequent top results for this selector.

#3 Bathory
More information about this result.

Get your selector results graphic and text links here.

The most frequent top results for this selector.

#4 Absu*
More information about this result.

Get your selector results graphic and text links here.

The most frequent top results for this selector.

#5 Cradle Of Filth*
More information about this result.

Get your selector results graphic and text links here.

The most frequent top results for this selector.

"Black Metal": 3,318 characters (an approximate value).

I will now use SNOW to hide a secret message inside of the document.

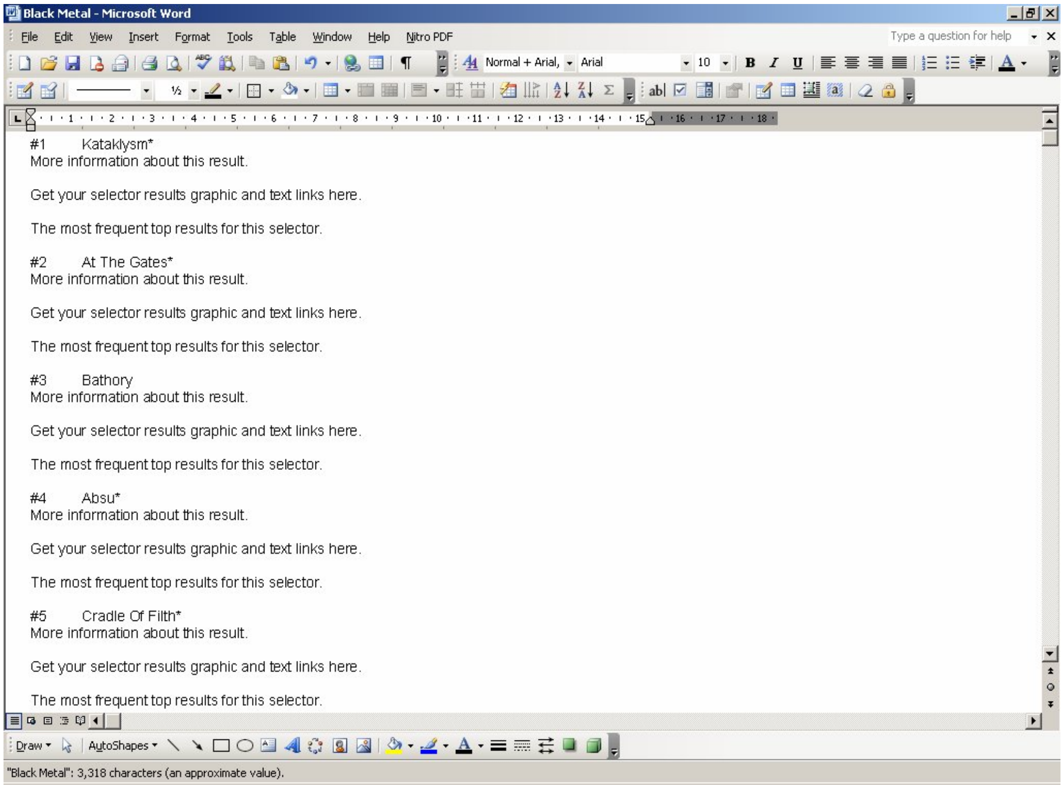
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Chris Morganti>"E:\Documents and Settings\Chris Morgan
ti\Desktop\SNOW.EXE" -C -m "Aelphaeis" -p "Zone-H" C:\Black_Metal.doc C:\Black_M
etal_Steg.doc
Compressed by 38.89%
Message exceeded available space by approximately 62.96%.
An extra 1 lines were added.

E:\Documents and Settings\Chris Morganti>
```

What I just did was hide the word “Aelphaeis” inside of the document with the password “Zone-H” (And no, our password security at Zone-H isn’t that bad, this is just an example.)

Below is a screenshot of the document after SNOW has been used to conceal the hidden message.



Black Metal - Microsoft Word
File Edit View Insert Format Tools Table Window Help Nitro PDF
Type a question for help
Normal + Arial, Arial 10
Draw AutoShapes

#1 Kataklysm*
More information about this result.

Get your selector results graphic and text links here.

The most frequent top results for this selector.

#2 At The Gates*
More information about this result.

Get your selector results graphic and text links here.

The most frequent top results for this selector.

#3 Bathory
More information about this result.

Get your selector results graphic and text links here.

The most frequent top results for this selector.

#4 Absu*
More information about this result.

Get your selector results graphic and text links here.

The most frequent top results for this selector.

#5 Cradle Of Filth*
More information about this result.

Get your selector results graphic and text links here.

The most frequent top results for this selector.

"Black Metal": 3,318 characters (an approximate value).

As you can see there is no visible difference between the two documents.
We can retrieve the message using SNOW by simply using the following command:

```
snow -C -p "Zone-H" C:\Black_Metal_Steg.doc C:\Hidden_Message.doc
```

To my knowledge there is no way of detecting Steganography in documents.

Detecting Steganography

The art of detecting Steganography is referred to as **Steganalysis.**
To put it simply Steganalysis involves detecting the use of Steganography inside of a file.
Steganalysis does not deal with trying to decrypt the hidden information inside of a file, just discovering it.
There are many methods that can be used to detect Steganography such as:

*Viewing the file and comparing it to another copy of the file found on the Internet (Picture File.)
There are usually multiple copies of images on the Internet, so you may want to look for several of them and try and compare the suspect file to them.
For example if you download a JPEG and your suspect file is also a JPEG and the two files look almost identical apart from the fact that one is larger than the other, it is most probable your suspect file has hidden information inside of it.

*Listening to the file. This is similar to the above method used for trying to manually detect Steganography in picture files.
If you are trying to detect hidden information inside of a MP3 audio file you will need to find an audio file to compare it to that uses the same compression (MP3.) The same applies to finding hidden information inside Picture files.

There are of course pieces of Software you can use to detect Steganography.

For education purposes I am going to hide a piece of information inside of a picture file (JPEG), then I am going to try and use a program called **xsteg** to try and see if the program can detect hidden information inside of the file.

I got the following image:

I used a piece of software called **JPHide.**

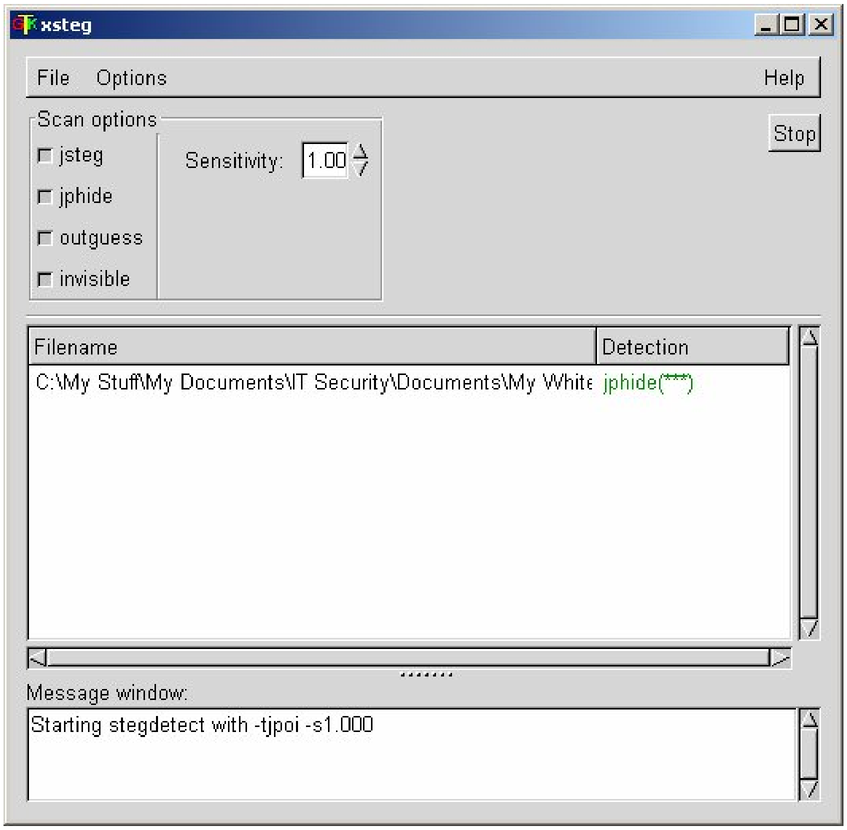
I used the software to hide the word “h4x0r” inside of the file. I encrypted the information with the password “qwerty” (a very weak password.)

This is the result:

I used the software again to hide the Introduction to this white paper, and I again used the password “qwerty”.

The difference between the images is not noticeable to the human eye what so ever.

Using xsteg I was able to detect the use of Steganography in the images.



Scan options

☐ jsteg

☐ jphide

☐ outguess

☐ invisible

Sensitivity: 1.00

Filename	Detection
C:\My Stuff\My Documents\IT Security\Documents\My White	jphide(***)

Message window:

```
Starting stegdetect with -tjpoi -s1.000
```

To sum up, the use of Steganography in the above images cannot be seen with the human eyes, only a piece of software was able to detect it.

Could Steganography Be Used By Terrorists

Could Steganography be used by Terrorists? The answer is yes it could be used by Terrorists. The question you really should be asking is, is it used by Terrorists?
It was speculated that the Terrorists that supposedly carried out the September 11th 2001 terrorist attacks used the Internet for various purposes. It was said they used the Internet in order to purchase their airlines tickets. This turned out not to be true, no authority within the US was able to back this up, because **none of the terrorists names appeared on any of the flight lists provided by American Airlines and United Airlines.**
The only people that seem to be pushing the idea that Terrorists are using the Internet and technologies such as Steganography are the people that support the idea that Al-Qaeda (saying it even exists) is a global sophisticated network of Terrorists that is constantly plotting to kill people in the western world.

USA Today:

Once the exclusive domain of the National Security Agency, the super-secret U.S. agency responsible for developing and cracking electronic codes, encryption has become the everyday tool of Muslim extremists in Afghanistan, Albania, Britain, Kashmir, Kosovo, the Philippines, Syria, the USA, the West Bank and Gaza and Yemen, U.S. officials say.

http://www.usatoday.com/tech/news/2001-02-05-binladen.htm

The USA Today articles written relating to Terrorists using Steganography were found to be fake, Jack Kelley was fired as a result for manufacturing fake news (about time someone got fired for it.)

It would be obvious that Steganography is not something that is used by Terrorists, it has just been hyped up to be a serious threat.

Steganography Tools

MP3Stego

MP3Stego will hide information in MP3 files during the compression process. The data is first compressed, encrypted and then hidden in the MP3 bit stream.

http://www.petitcolas.net/fabien/software/MP3Stego_1_1_17.zip

JPHide and JPSeek

JPHIDE and JPSEEK are programs which allow you to hide a file in a jpeg visual image. There are lots of versions of similar programs available on the internet but JPHIDE and JPSEEK are rather special.

http://www.snapfiles.com/php/download.php?id=101911

BlindSide Cryptographic Tool

BlindSide is an example of the art of Steganography - the passing of secret messages in a form such that one would not suspect the message is being passed. This is an area of cryptography that is attracting considerable interest of late. The Blindside utility can hide a file (or files) of any variety, within a Windows Bitmap image (BMP file).

http://www.mirrors.wiretapped.net/security/steganography/blindside/

GIFShuffle

The program **gifshuffle** is used to conceal messages in GIF images by shuffling the colourmap, which leaves the image visibly unchanged. **gifshuffle** works with all GIF images, including those with transparency and animation, and in addition provides compression and encryption of the concealed message.

http://www.darkside.com.au/gifshuffle/

wbStego

wbStego is a tool that hides any type of file in bitmap images, text files, HTML files or Adobe PDF files. The file in which you hide the data is not optically changed.

http://www.wbailer.com/wbstego

StegoVideo

MSU StegoVideo allows to hide any file in a video sequence. When the program was created, different popular codec's were analyzed and an algorithm was chosen which provides small data loss after video compression. You can use MSU StegoVideo as VirtualDub filter or as standalone .exe program, independent from VirtualDub.

http://compression.ru/video/stego_video/index_en.html

Steganalysis Tools

Stegdetect

http://www.outguess.org/download.php

Steganography Analyzer Artifact Scanner (StegAlyzerAS)

StegAlyzerAS gives you the capability to scan the entire file system, or individual directories, on suspect media for the presence of Steganography application artifacts. And, unlike other popular forensic tools, you can perform an automated or manual search of the Windows Registry to determine whether or not any Registry keys or values exist that can be associated with a particular Steganography application.

http://www.sarc-wv.com/stegalyzeras.aspx

Steganography Analyzer Signature Scanner (StegAlyzerSS)

StegAlyzerSS gives you the capability to scan every file on the suspect media for the presence of hexadecimal byte patterns, or signatures, of particular Steganography applications in the files. If a known signature is detected, it may be possible to extract information hidden with the Steganography application associated with the signature.

http://www.sarc-wv.com/stegalyzerss.aspx

Digital Invisible Ink Toolkit

This project provides a simple Java-based steganography tool that can hide a message inside a 24-bit color image so that knowing how it was embedded, or performing statistical analysis, does not make it any easier to find the concealed information.

http://sourceforge.net/project/showfiles.php?group_id=139031

Conclusion

Steganography is not a threat in general and **Steganography is hardly something that is used by Terrorists and I seriously doubt that it will be used by Terrorists.**
I think that Steganography is a **potential threat.** However I do not believe it will be used for purposes that are being pushed by the media. The most probable use of Steganography is probably to hide illegal material such as child pornography. I believe that Steganography may also be used to hide sensitive information and transfer it from one place to another.
For example a foreign military may have a double agent working inside the US Military, the agent steals some sensitive documents, and he wants to copy them onto CD to take home and email to his superiors.
He knows that if he burns the documents to the disk there is a disk of the disk being checked.
So what could he do? Simple, hide the documents inside picture files that look nothing out of the ordinary.
People should be focusing on the important aspects of Steganography, such as what it is really used for, instead of believing propaganda put out by the media.

About The Author

I (Aelphaeis Mangarae) am an Administrator at Digital-Underground.
– http://the-digital-underground.com
Digital Underground is a security portal where both Beginners and Professional security enthusiasts discuss IT Security.
I am also an Operator and Forum Moderator at the Zone-H.
- http://zone-h.org
Email: adm1n1strat10n AT hotmail DOT com
MSN: adm1n1strat10n AT hotmail DOT com
IRC: irc.efnet.org:6667 #d-u

Greetz To

htek, HackJoeSite, FRSilent, Read101, Syst3m Of Cha0s, The Goon Squad, Media Assassins, tomchu, nic`, BSoD, r0rkty, Nitrous, SyS64738, Trash-80, morning_wood, Astharot, Fauley, Furax, PsAuX, SecurityWireless, SysSpider, Siegfried, fritz, darkt3ch, Predator/ill skillz, Alchemist, BioHunter, Dark Sheep, Splinter, Digerati, digital-flow, butthead, spiderlance, FishNET, W--, nrs, IBMWarpst, Nixus, varu, z16bitseg, jMu, JWT, ASO, BSG, felosi, Mega~biTe, wicked, Palmeiro, Kadafiu, sNKenjoi, h4cky0u, royal & rat_hack.