**WHAT IS STEGANOGRAPHY AND WHAT ARE ITS POPULAR TECHNIQUES?**

Imagine if you had the power to conceal information in plain sight. Well, this is indeed possible with the use of Steganography. Steganography is the process of hiding information, images, or audio messages inside another piece of information, image, or audio. Steganography is not a new term. It has been around since about 1500 and was first used by Johannes Trithemius in his book Steganographia.

**What is Steganography in cybersecurity?**

“Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.”

**What is the use of Steganography?**

There are many ways to conceal information using Steganography. The most common method is by embedding information into digital images. We all know that digital images say, a JPEG image, contains several megabytes of data in the form of pixels. This allows some room for someone to embed steganographic information within the digital file. With the use of steganographic applications, a hacker alters the [least significant bits](https://searchsecurity.techtarget.com/answer/How-does-Steganography-work-and-does-it-threaten-enterprise-data) of the data file and embeds a malicious code into the image. Once the targeted user downloads and opens the image file in their computer, the malware is activated. Depending on its programming, the malware can now open a leeway for the attacker to gain control over the user’s device or network. The danger of Steganography is that the difference between the original image and the steganographic image is subtle and the two cannot be distinguished by the naked eye.

**Is Steganography still used?**

Yes, Steganography is still popular among cyber criminals. Recent attacks show that security researchers found a [new malware campaign](https://www.cisomag.com/hackers-using-Steganography-in-wav-audio-files-to-hide-malware/https:/www.cisomag.com/hackers-using-Steganography-in-wav-audio-files-to-hide-malware/) that used WAV audio files to hide their malware. It is believed that the attackers used Steganography to embed the malicious code inside the WAV audio file.

**3 Techniques used in Steganography**

**1. Least Significant Bit**

In this Steganography method, the attacker identifies the least significant bits of information in the carrier image and substitutes it with their secret message, in this case, malicious code. When the target downloads the carrier file, they introduce the malware into their computer which allows the attacker access to this device and the hack begins. Cybersecurity professionals commonly use sandboxes to detect these corrupt files. However, black hat hackers have invented various methods of bypassing sandboxes like sleep patching. Sleep patched malware is not easily detected by the sandbox since it poses as benign and buys time while studying the timing artifacts of the sandbox and executes when the sandbox is vulnerable.

**2. Palette Based Technique**

This technique also uses digital images as malware carriers. Here, the attackers first encrypt the message and then hide it in a stretched palette of the cover image. Even though this technique can carry a limited amount of data, it frustrates threat hunters since the malware is encrypted and takes a lot of time to decrypt.

**3. Secure Cover Selection**

This is a very complex technique where the cyber criminals compare the blocks of the carrier image to the blocks of their specific malware. If an image with the same blocks as the malware is found, it is chosen as the candidate to carry the malware. The identical malware blocks are then carefully fitted into the carrier image. The resulting image is identical to the original and the worst part is that this image is not flagged as a threat by detection software and applications.

These are just but a few methods by which black hat hackers frustrate [ethical hackers](https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/) using Steganography. Steganography allows attackers to operate in stealth mode while conducting a serious attack. Most of these attacks are zero-day exploits which give threat hunters sleepless nights. Some preventive measures against Steganography include the deployment of security patches, updating software, and educating end-users.

Receiving ethical hacking training from EC-Council will equip you with the knowledge and skill to learn how the adversaries are breaking into networks and wreaking havoc. Once professionally trained, you will receive the [Certified Ethical Hacker (CEH)](https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/) certification. This will show organizations that you are well-versed in over 340 attack technologies that are commonly used by black hat hackers and [white hat hackers](https://blog.eccouncil.org/what-is-a-white-hat-hacker/), alike.

REFERENCES

<http://www.brainkart.com/article/Classical-Encryption-Techniques_8339/>

<https://www.tutorialspoint.com/cryptography/index.htm>

<https://www.geeksforgeeks.org/cryptography-introduction/>

[https://www.techopedia.com/definition/1770/cryptography#:~:text=Cryptography%20involves%20creating%20written%20or,information%20to%20be%20kept%20secret.&text=Information%20security%20uses%20cryptography%20on,transit%20and%20while%20being%20stored](https://www.techopedia.com/definition/1770/cryptography).

<https://www2.slideshare.net/lineking/classical-encryption-techniques-in-network-security?qid=e388c29f-793d-4f2b-bcaf-9d22e9ca07b5&v=&b=&from_search=1>

<https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography>

<https://www.academia.edu/Documents/in/Cryptography>