BRANDEFENSE
CYBER THREAT INTELLIGENCE

Detection of Steganography Attacks

Author: Threat Intelligence Team

Release Date: 14.06.2022

Report ID: BD02112102

Steganography Definition

Steganography is a camouflage method of a message or an activity. It hides the malicious code which harms the victim's computer. It is not just used for cyber attacks, it was also used for messaging anonymously on the battle in the past. Commanders and soldiers communicated with this method during some wars.

Today, it is used for hiding the malicious code in a legitimate file so that the target will execute/open the file and get the message written on the foreground of the file. However, in the background, malicious code runs and does the malicious activity (connect the victim's computer to the C2 server, download another malware, encrypt the files for ransom, or other cyber attack vectors).

Why is It Important?

Malware activity can be detected by looking at their hash value, monitoring network traffic and other methods. However, an image file contains malicious code embedded into the file with steganography methods looks legitimate while downloading it. This makes detecting malware harder. Moreover, the image file can be downloaded from a legitimate image hosting services (imgur, flickr, ...). This makes getting the C2 server information harder (or even impossible). Unfortunately, steganography attacks do not infiltrate the system only by manipulating image bytes; audio files, video files and text files are also used for steganography attacks.

Threat Actors

According to Mitre ATT&CK;

ID	Name	Description
G0016	APT29	APT29 has used steganography to hide C2 communications in images.
G0001	Axiom	Axiom has used steganography to hide its C2 communications.
S0187	Daserf	Daserf can use steganography to hide malicious code downloaded to the victim.
S0038	Duqu	When the Duqu command and control is operating over HTTP or HTTPS, Duqu uploads data to its controller by appending it to a blank JPG file.
S0037	HAMMERTOSS	HAMMERTOSS is controlled via commands that are appended to image files.
S0395	LightNeuron	LightNeuron is controlled via commands that are embedded into PDFs and JPGs using steganographic methods.
S0495	RDAT	RDAT can process steganographic images attached to email messages to send and receive C2 commands. RDAT can also embed additional messages within BMP images to communicate with the RDAT operator.
S0633	Sliver	Sliver can encode binary data into a .PNG file for C2 communication.
S0559	SUNBURST	SUNBURST C2 data attempted to appear as benign XML related to .NET assemblies or as a faux JSON blob.
S0230	ZeroT	ZeroT has retrieved stage 2 payloads as Bitmap images that use Least Significant Bit (LSB) steganography.
S0672	Zox	Zox has used the .PNG file format for C2 communications.

Is It Easy to Detect Steganography Attacks?

- Attackers change the file's bits to embed the malicious code inside the file. Since the file is changed now, you might think that it can be detected so easily by just looking at the image/video file or listening to the audio file. Unfortunately, it is not that easy.

- Attackers change the as least number of bits as they can so that the file cannot be differentiated by a person. The attackers generally tend to change the LSBs (Least Significant Bits) of the file so that the change cannot be understood easily. Yes, the file is different now (you can prove that by comparing the hash values of the original file and the malicious file), but it can be detected by detection systems.

Detection Methods

- Since the legitimate files containing malicious code are injected into the victim's computer generally from a phishing email, people should be aware of the detection methods of the phishing emails. You can find more information about detection of phishing emails here:

- Increase the security awareness of the employees. They should detect phishing attacks (emails, messages, etc.), they should know that even some image files can be harmful.

- If a document asks for permission to enable active content, you should be careful since you will enable macro of the document.

- Be more careful against PowerShell events. You can set some extra rules for PowerShell logs to increase detection possibility.

- File size of the files that contain malicious code may be bigger than usual.

- You can set modern endpoint protection systems like behavioral detection mechanisms to your company. It can detect malicious activity after the malware enters the computer.

- Set the endpoint detection systems to detect the encryption and obfuscation.

- Keep firewalls and antivirus software up-to-date because new updates may contain newly discovered malware, methods or C2 servers.

Conclusion

As the detection methods are improved by the security professionals, attackers look for new methods to bypass security measures. Steganography attacks are very powerful for infecting computer without being detected. Companies and individuals should always be suspicious, when they download a file from the internet. This does not have to be restricted to computers. IoT, automated cars and VR might be target for future attacks. That is why, an awareness should be constructed today to be more ready for the future threats.