OceanLotus APT Uses Steganography to Shroud Payloads

By Lindsey O'Donnell

Published: 2019-04-03 · Archived: 2026-04-05 18:06:44 UTC

The OceanLotus APT is using two new loaders which use steganography to read their encrypted payloads.

The advanced persistent threat (APT) group OceanLotus has switched up its tactics to use steganography to cloak encrypted payloads within .png image files.

Researchers said that they discovered the OceanLotus APT group – a Vietnam-linked cyber-espionage group also known as APT32 – using the tactic to hide their payloads since September 2018. After victims click on malicious files sent via phishing emails, a loader will execute a next-stage encrypted payload that is obfuscated using steganography – a method of hiding code within an image. Once decoded, decrypted, and executed, the payload will deploy the APT's backdoor.

"The threat actor will first encode an image with their payload of choice, before distributing it with a simple decoder to a target," Tom Bonner, BlackBerry Cylance director of threat research, told Threatpost. "There are many tools that can be used to encode/decode data in images, but the OceanLotus implementation appears to be bespoke, and therefore not easily prone to detection by standard analysis tools."

OceanLotus, active since at least 2014, has targeted private sector industries and foreign governments, primarily in Southeast Asian countries including Vietnam or the Philippines, according to Bonner. OceanLotus actors are known to deliver their malicious attachments via spear phishing emails.

In the latest campaigns launched by the APT, researchers said that they observed two new obfuscated loaders deploying two types of APT32-specific backdoors. These loaders have been observed active since September 2018 – but this is the first time that their existence has been reported, researchers said.

The first steganography-based loader deploys a version of a backdoor dubbed "Denes." The malware loader first attempts to imitate McAfee's McVsoCfg dynamic link library (DLL) file, researchers said. That tricks the legitimate "On Demand Scanner" executable on the system to side-load the malicious file, which then loads a next-stage encrypted payload. That payload is stored in a separate .png image file and uses steganography to avoid detection.

Figure 3. "Kaito Kid"

"The user does not interact with the image (nor is the image sent via email), rather the image is used to hide the payload from analysts/tools/monitoring software," Bonner told Threatpost. "In a way, the payload is hiding in plain sight, as an image carrying a payload will be virtually indistinguishable from an original image."

Researchers said that one of the payloads they encountered for instance was encoded inside an image of a popular Japanese mange series character (Kaito Kuroba).

The encoded payload is also encrypted with AES128 and further obfuscated with XOR in an attempt to fool steganography detection tools, researchers said. Once uploaded, the payload is then decrypted.

The second loader uses the same extraction technique as the first (an executable tricked into side-loading a malicious DLL), although the loader itself differs a bit in implementation and loads an updated version of a different backdoor called 'Remy.' And while, the DLL loader in this instance also loads the next-stage payload using a custom .png steganography method, it also uses a separate .png image.

Figure 25. Image containing encoded payload

Here, the payload is extracted from the .png image after the victim clicks on the phishing email. The .png image for this second loader (left) appears to have been taken from an inspirational quotes website, researchers said.

While steganography is an old-school tactic, bad actors are continuing to push the boundaries when using steganography to conceal their malware. Steganography has been used in several campaigns over the past year, including in uploaded images on trusted Google sites and even in memes on Twitter.

Source: https://threatpost.com/oceanlotus-apt-uses-steganography-to-shroud-payloads/143373/