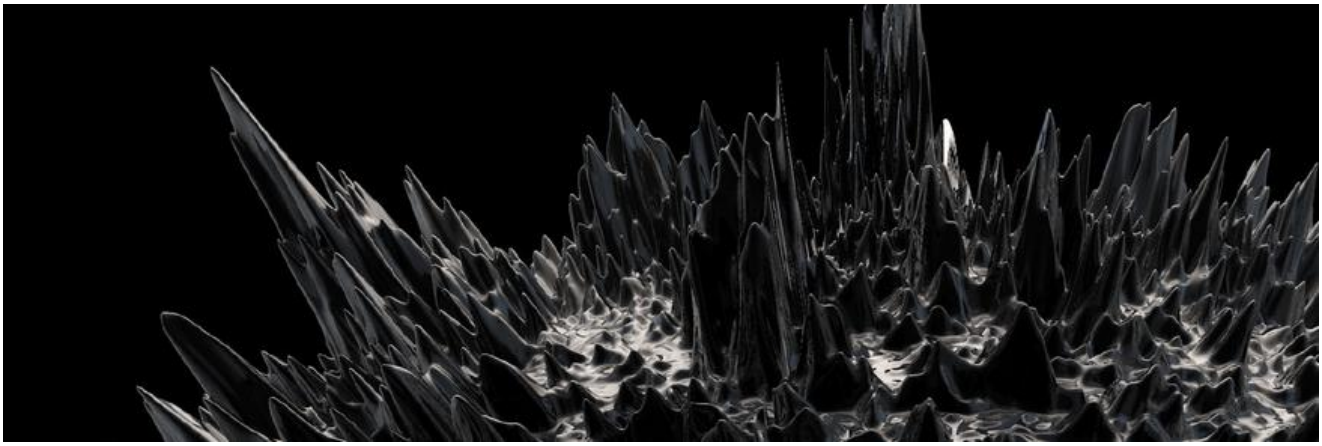
# Report: OceanLotus APT Group Leveraging Steganography

threatvector.cylance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html

The Cylance Research and Intelligence Team



RESEARCH & INTELLIGENCE / 04.02.19 / The Cylance Research and Intelligence Team
During an incident response investigation in the final quarter of 2017, BlackBerry Cylance incident responders and threat researchers uncovered several bespoke backdoors deployed by the OceanLotus APT Group (a.k.a. APT32, Cobalt Kitty), as well as evidence of the threat actor using obfuscated CobaltStrike Beacon payloads to perform command and control (C2).

While continuing to monitor activity of the OceanLotus APT Group, our researchers uncovered a novel payload loader that utilizes steganography to read an encrypted payload concealed within a .png image file.

The steganography algorithm appears to be bespoke and utilizes a least significant bit approach to minimize visual differences when compared with the original image to prevent analysis by discovery tools.

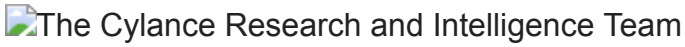
Once decoded, decrypted, and executed, an obfuscated loader will load one of the APT32 backdoors.

Thus far, BlackBerry Cylance has observed two backdoors being used in combination with the steganography loader – a version of Denes backdoor (bearing similarities to the one described by ESET), and an updated version of Remy backdoor.

However, this can be easily modified by the threat actor to deliver other malicious payloads. The complexity of the shellcode and loaders shows the group continues to invest heavily in development of bespoke tooling.

This new white paper describes the steganography algorithm used in two distinct loader variants and looks at the launcher of the backdoor that was encoded in one of the .png cover images.

## DOWNLOAD THE FULL REPORT HERE




## About The Cylance Research and Intelligence Team

Exploring the boundaries of the information security field

The Cylance Research and Intelligence team explores the boundaries of the information security field identifying emerging threats and remaining at the forefront of attacks. With insights gained from these endeavors, Cylance stays ahead of the threats.

---

Back