Sakula Malware Analysis: INOCNATION Campaign Obfuscation | Report | Fidelis Security

Published: 2022-10-04 · Archived: 2026-04-05 15:06:26 UTC

Last month, CrowdStrike published a blog on malware campaigns attributed to Sakula. We took a look at the malware specifically in the INOCNATION campaign to analyze what was new and different about the techniques used by the threat actor. It appears the entity behind this campaign took steps to make reverse engineering more difficult and chose the use of Cisco's AnyConnect Client as a lure to trick victims into installing the malware.

The RAT delivered by this campaign was not particularly interesting and had all the features you would expect in such a tool. The use of the obfuscation techniques was novel and this advisory discusses those in detail, along with how we detected them.

Key Findings:

- Two passes with different XOR keys used to obfuscate components and strings in the malware
- Trusted software used as a decoy for initial installation
- A mangled MZ header used to deceive security products
- String stacking obfuscation with Unicode strings
- Multiple layers of obfuscation for command and control traffic
- Built-in uninstall functionality.

MD5 Hashes used in this analysis:

Fidelis Security's products detect the activity documented in this paper and additional technical indicators are published in the appendices of this paper and to the Fidelis Security github at https://github.com/fideliscyber.

We want to thank our fellow security researchers at CrowdStrike for sharing hashes of the malware samples analyzed in this report.
