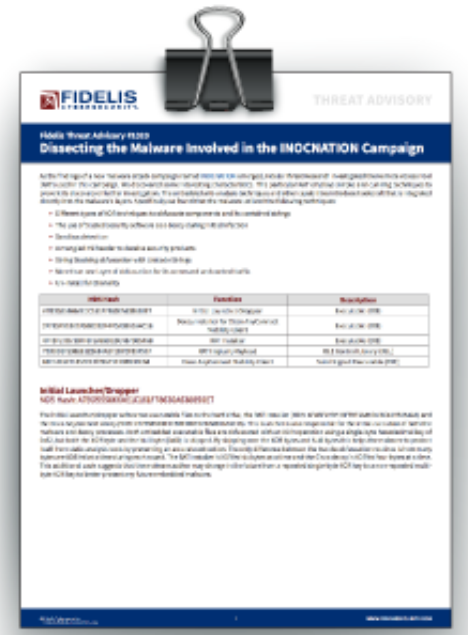
Threat Geek

Wednesday, December 16, 2015

Fidelis Threat Advisory #1020 Dissecting the Malware Involved in the INOCNATION Campaign



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:

MD5 Hash	Function	File Type
A7BD555866AE1C161F78630A638850E7	Initial Dropper/Launcher	Executable (EXE)
4F4BF27B738FF8F2A89D1BC487B054A8	RAT Installer	Executable (EXE)
75D3D1F23628122A64A2F1B7EF33F5CF	RAT Implant/Payload	OLE Control DLL
2F7E5F91BE1F5BE2B2F4FDA0910A4C16	Decoy Installer for Cisco AnyConnect Mobility Client	Executable (EXE)
68F1419721354EC1f78A71E10B54FCA8	Cisco AnyConnect Mobility Client	Valid Signed Executable (EXE)

To see the full report and findings, visit Fidelis Threat Advisory #1020 here

Fidelis Cybersecurity'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 Cybersecurity 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.

Fidelis Cybersecurity Threat Research Team

You might also like:

THREATtoons: do they make pockets that large?

THREAT GEEK WEEKLY UPDATE – JULY 14, 2011

Fidelis Threat Advisory #1016: Pushdo It To Me One More Time

Posted by ThreatGeek at 02:13 PM in Fidelis Threat Advisories, threat intelligence feed | Permalink