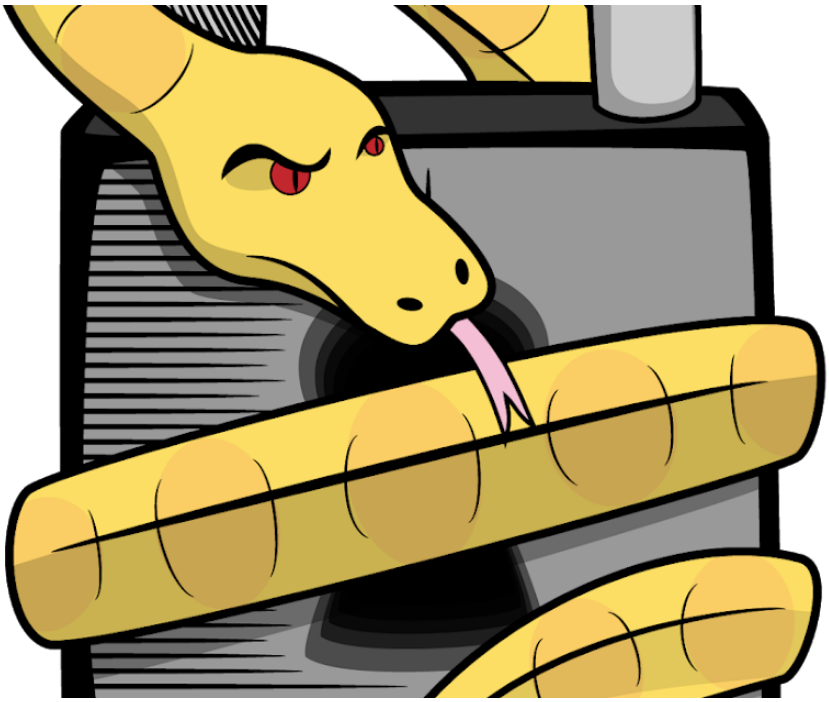
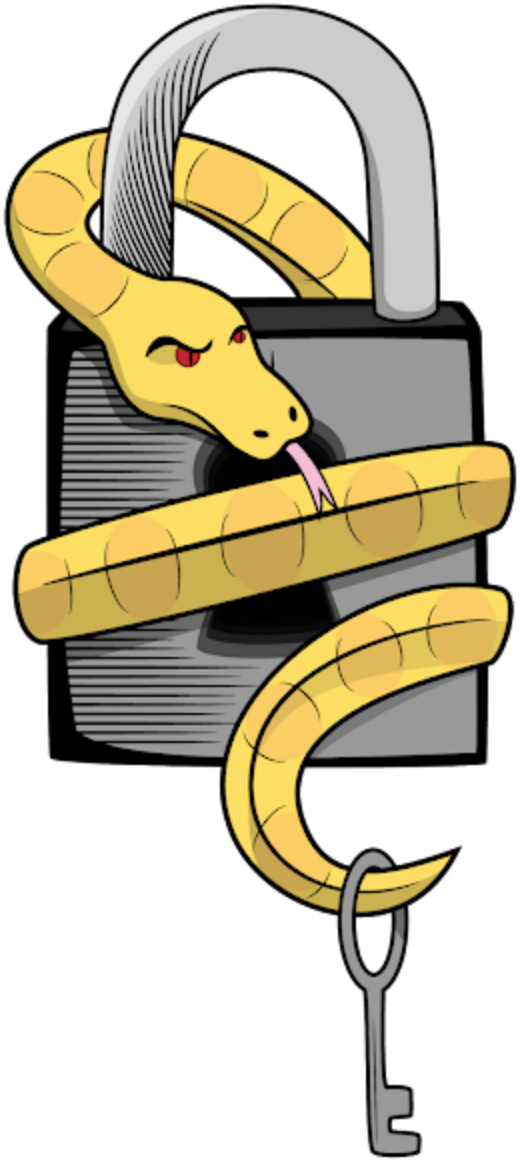
Pylocky Unlocked: Cisco Talos releases PyLocky ransomware decryptor

blog.talosintelligence.com/2019/01/pylocky-unlocked-cisco-talos-releases.html



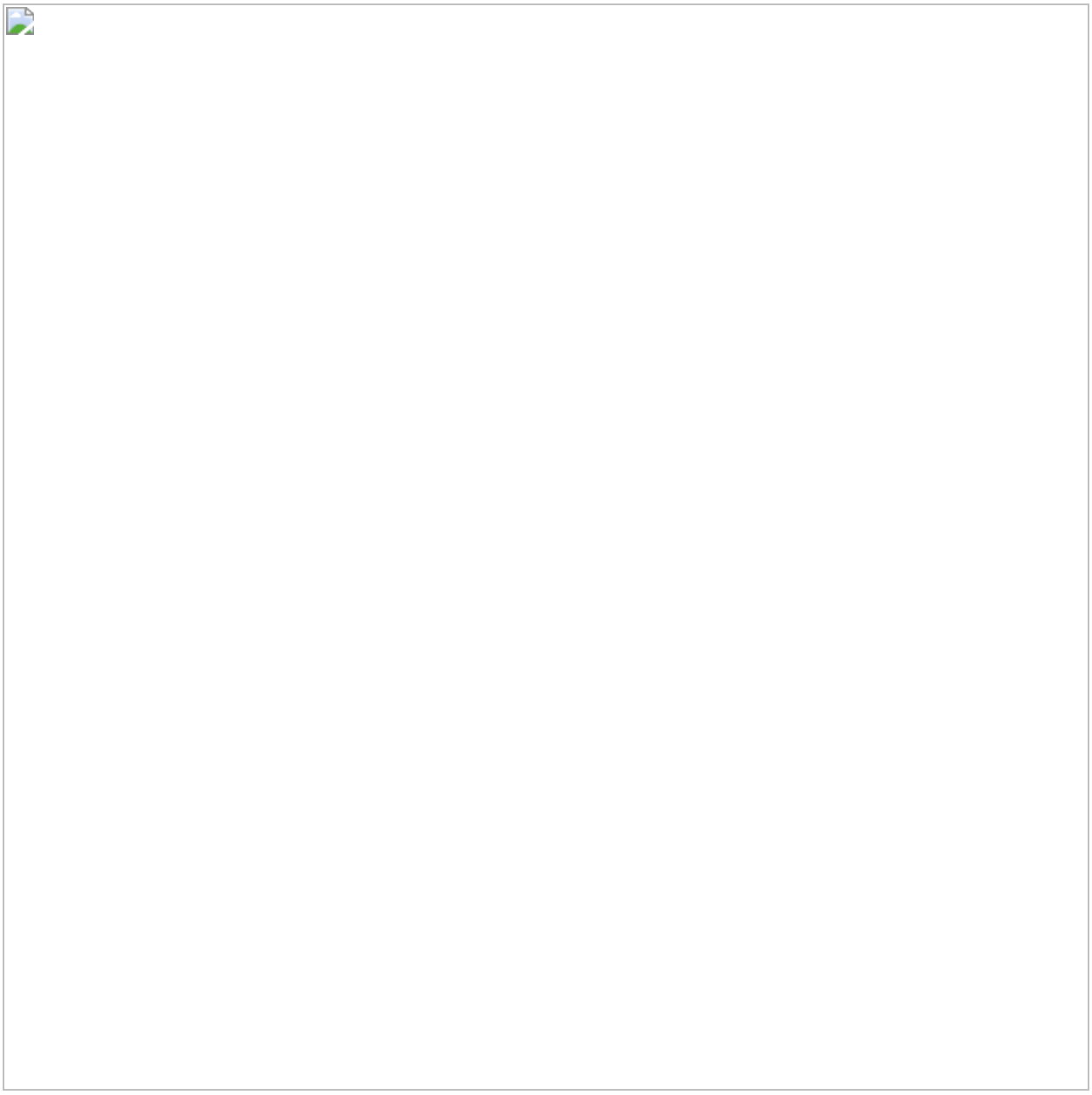


This tool was developed by Mike Bautista.

PyLocky is a family of ransomware written in Python that attempts to masquerade as a Locky variant. This ransomware will encrypt all files on a victim machine before demanding that the user pay a ransom to gain access to their decrypted files. To combat this ransomware, Cisco Talos is releasing a free decryption tool. Because our tool requires the capturing of the initial PyLocky command and control (C2) traffic of an infected machine, it will only work to recover the files on an infected machine where network traffic has been monitored. If the initial C2 traffic has not been captured, our decryption tool will not be able to recover files on an infected machine. This is because the initial callout is used by the malware to send the C2 servers information that it uses in the encryption process.

When PyLocky executes, it generates a random user ID and password and gathers

information about the infected machine using WMI wrappers. It also generates a random initialization vector, or IV, which is then base64 encoded and sent to the C2 server along with the system information the malware has gathered. After obtaining the absolute path of every file on the system, the malware then calls the encryption algorithm, passing it the IV and password. Each file is first base64-encoded before it is encrypted. The malware appends the extension ".lockedfile" to each file it encrypts - for example, the file "picture.jpg" would become "picture.jpg.lockedfile." The original file is then overwritten with the attacker's ransom note.



Example of a PyLocky ransom note.

Talos encourages users never to pay an attacker-demanded ransom, as this rarely results in the recovery of encrypted files. Rather, victims of this ransomware should restore from backups if their files cannot be decrypted. Just as in the June 2017 Nyetya attack, Talos has

observed on numerous occasions that attackers who are demanding ransoms may have no way to communicate with victims to provide a decryptor. Our free decryption tool can be downloaded here.

Indicators of Compromise

Domain Names

centredentairenantes[.]fr
panicpc[.]fr
savigneuxcom.securesitefr[.]com

Hashes

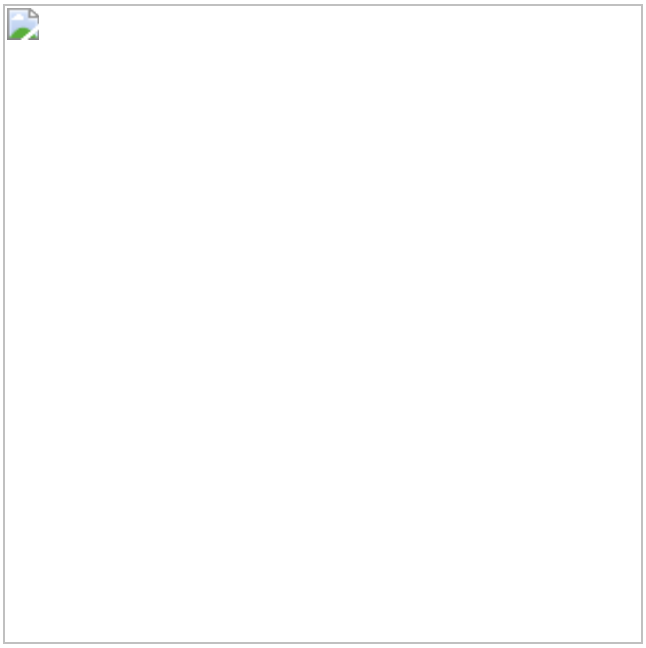
1569F6FD28C666241902A19B205EE8223D47CCCDD08C92FC35E867C487EBC999

2A244721FF221172EDB788715D11008F0AB50AD946592F355BA16CE97A23E055

87AADC95A8C9740F14B401BD6D7CC5CE2E2B9BEEC750F32D1D9C858BC101DFFA

C9C91B11059BD9AC3A0AD169DEB513CEF38B3D07213A5F916C3698BB4F407FFA

Coverage



Ways our customers can detect and block this threat are listed below.

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of this malware.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Meraki MX can detect malicious activity associated with this threat.

Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source SNORT® Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.