DUNGEON SPIDER | Threat Actor Profile

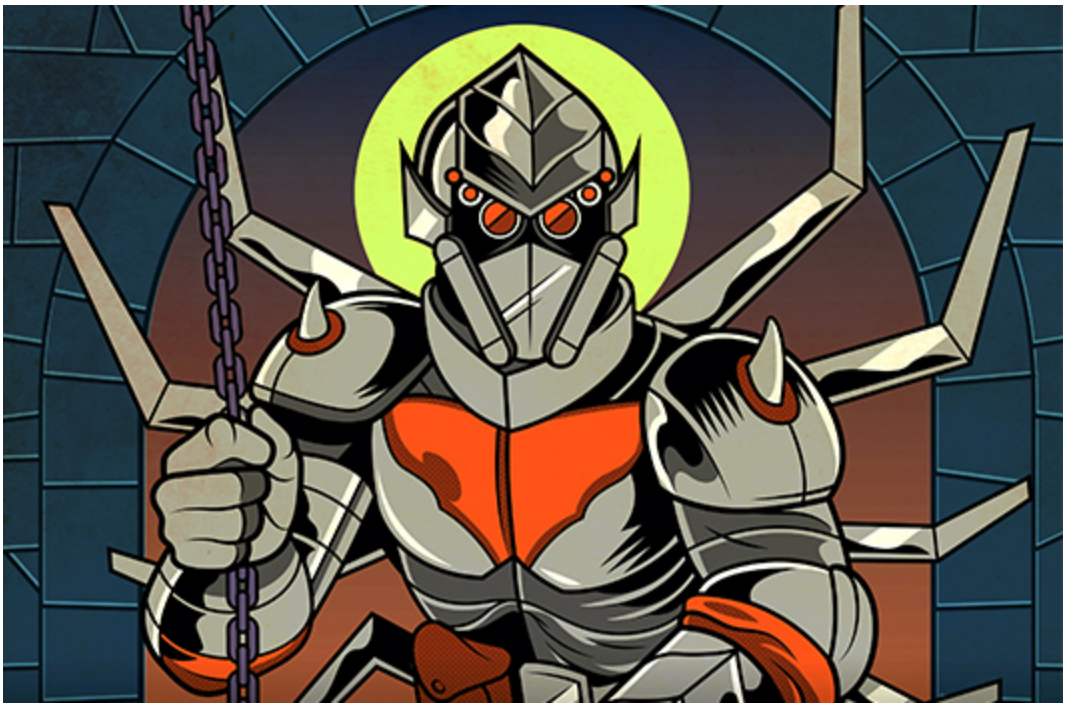
crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-october-dungeon-spider/

October 26, 2018

Meet CrowdStrike's Adversary of the Month for October: DUNGEON SPIDER

October 26, 2018

Adam Meyers Research & Threat Intel



DUNGEON SPIDER is a criminal group operating the ransomware most commonly known as *Locky*, which has been active since February 2016 and was last observed in late 2017. Locky is a ransomware tool that encrypts files using a combination of cryptographic algorithms: RSA with a key size of 2,048 bits, and AES with a key size of 128 bits. Locky targets a large number of file extensions and is able to encrypt data on shared network drives. In an attempt to further impact victims and prevent file recovery, Locky deletes all of the Shadow Volume Copies on the machine.

Locky uses a set of hard-coded IP addresses for C2 (command and control) communications, and once the victim has been infected, an initial HTTP POST is made using a file path of `/checkupdate` appended to the C2s. Locky will then continue to communicate with the hard-coded IP addresses thereafter, or it will resort to its domain

generation algorithm (DGA), if they become unreachable. Some variants of Locky also have the ability to operate offline, meaning they do not require internet connectivity or C2s to encrypt a victim's files.

Each victim is assigned a personal identification number that is generated upon infection, sent back to the C2s, and used to provide the victim-specific decryption key should the ransom be paid. Once infected with Locky, so-called "help files" are dropped onto the victim machine, providing details of how to pay the ransom for file recovery. The Locky ransom payment portal URL has remained the same for some time: `g46mbrrzpfszonuk[.]onion/{personal ID number}.`

CrowdStrike® Falcon® Intelligence™ has not observed distribution or development of Locky since late 2017, with one of the last major developments being the modification of the ransomware to use a file extension of `.diablo6`. Since Locky first came to the criminal market in early 2016, the ransomware quickly made a name for itself when it allegedly infected Hollywood Presbyterian Medical Center, resulting in a reported ransom payment of 40 Bitcoin (BTC).

A ransomware variant dubbed PyLocky was observed in September 2018 being distributed by a phishing campaign using an invoicing theme. PyLocky was found to be targeting entities in France and Germany. Of note is the fact that PyLocky claims to be a version of Locky, which as noted above, has not been active for some time.

It is Locky's notoriety that has likely led to the operators of PyLocky choosing to appropriate its name and likeness; mimicking the names of successful ransomware families is a technique often used by criminal actors to gain customers. There is no evidence, as of this writing, that PyLocky is at all related to either Locky ransomware or DUNGEON SPIDER, the developers of Locky. However, the emergence of PyLocky and its attempt to masquerade as a previously prolific and potent version of Locky indicates that adversaries continue to actively develop ransomware, and that it remains a dominant and viable threat vector.

DUNGEON SPIDER primarily relies on broad spam campaigns with malicious attachments for distribution. Locky is the community/industry name associated with this actor.

Other Known Criminal Adversaries

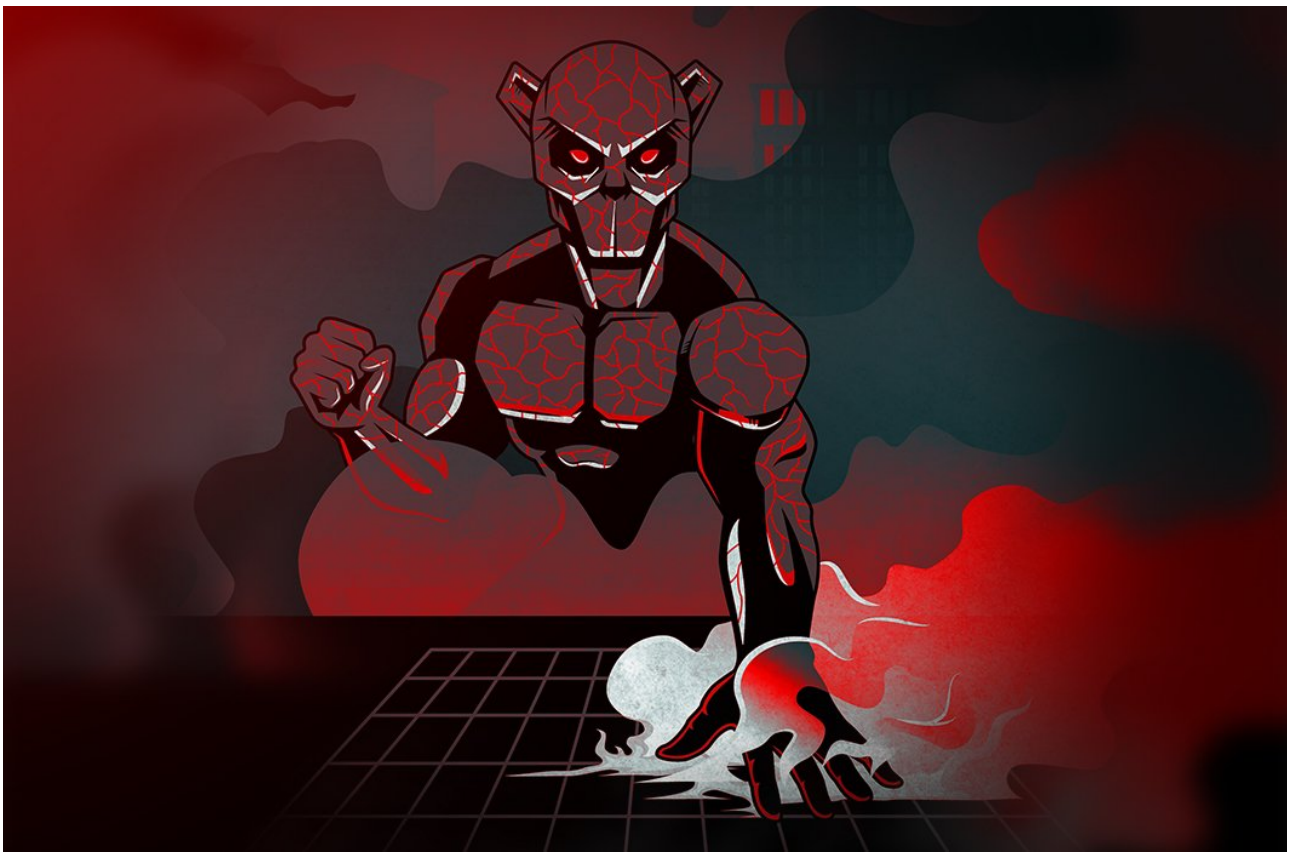
- Cobalt Spider
- Mummy Spider
- Salty Spider (Sality)
- Wicked Spider

Curious about other nation-state adversaries? *Visit our threat actor center to learn about the new adversaries that the CrowdStrike team discovers.*

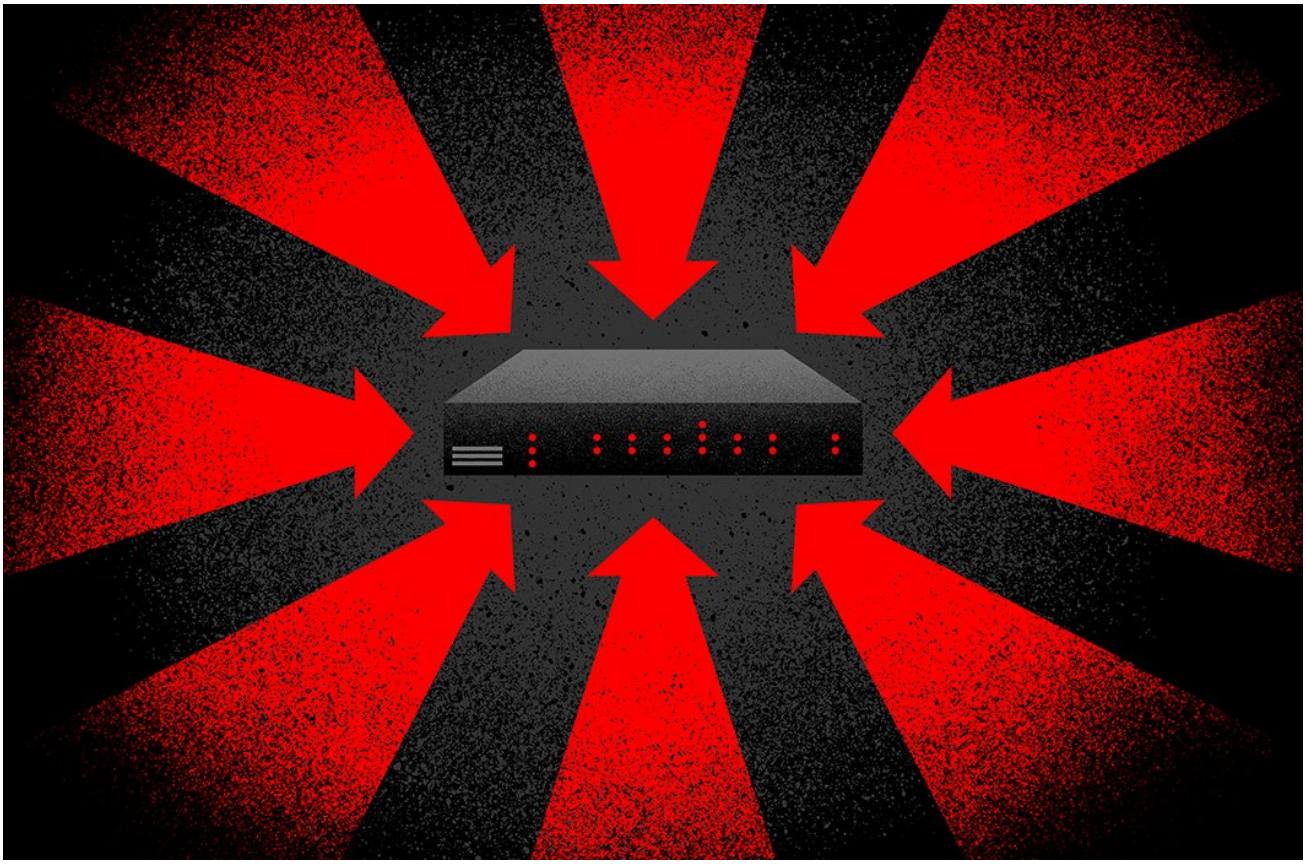
Learn More:

- *To learn more about how to incorporate intelligence on threat actors such as DUNGEON SPIDER into your security strategy, please visit the Falcon Intelligence product page*
- *Download the CrowdStrike 2020 Global Threat Report to get the latest insights on modern adversaries and their tactics, techniques, and procedures (TTPs)*

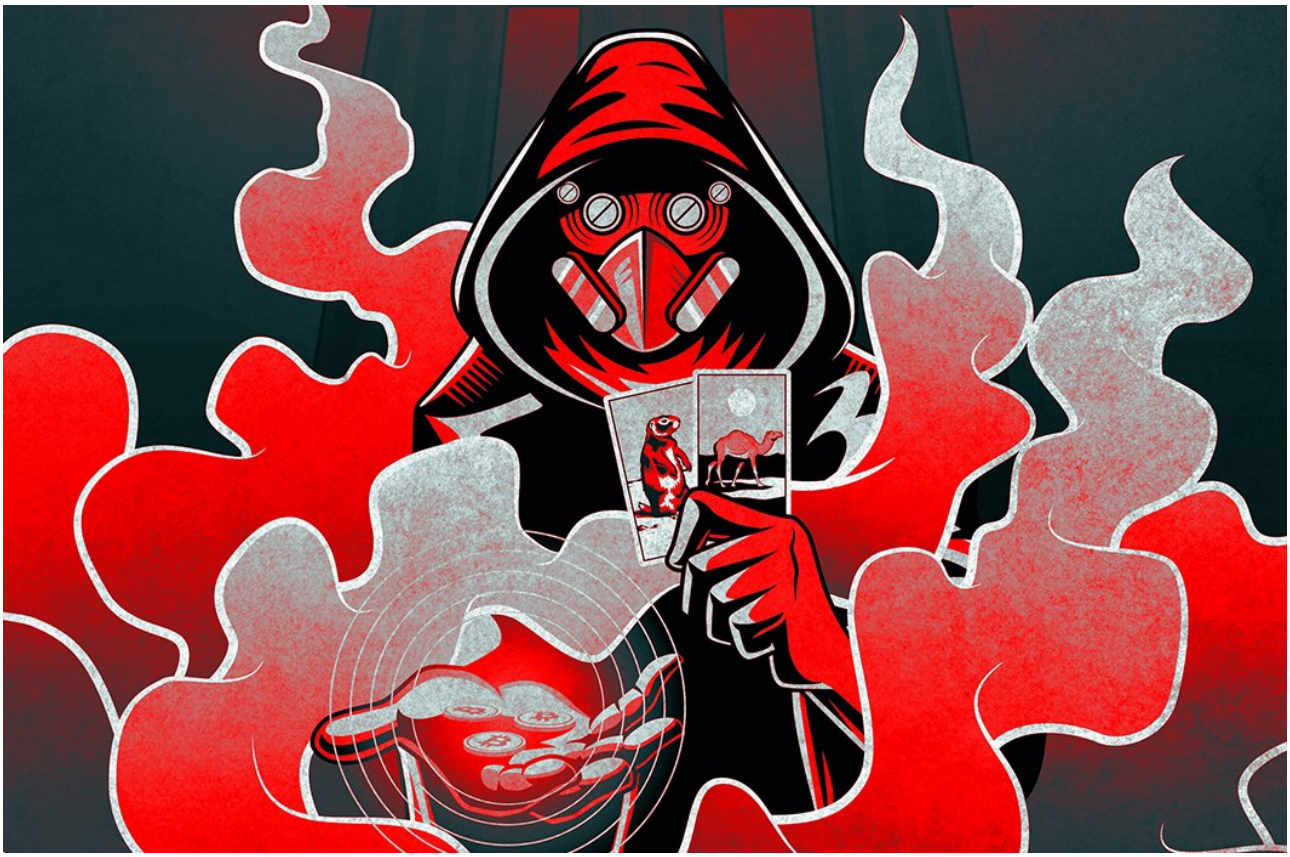
Related Content



Who is EMBER BEAR?



A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router



PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell