MUMMY SPIDER | Threat Actor Profile

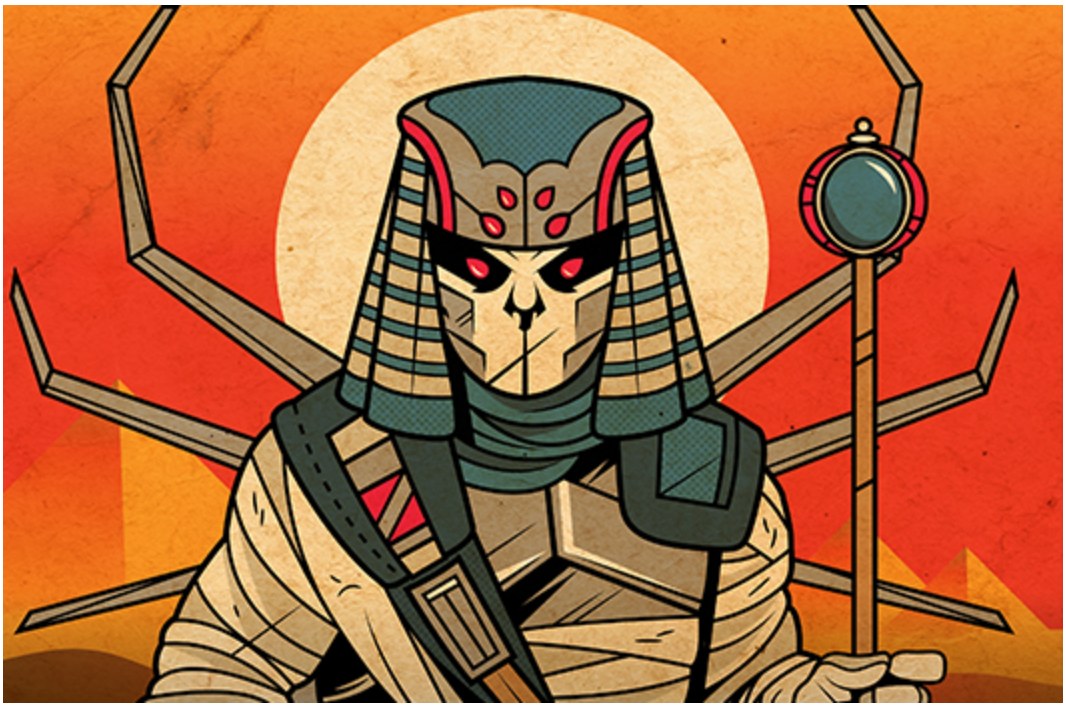
crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/

February 8, 2018

Meet CrowdStrike's Adversary of the Month for February: MUMMY SPIDER

February 8, 2018

Adam Meyers Research & Threat Intel



In continuance of our monthly blog post to introduce a new threat actor, February 2018 features a criminally motivated actor we call **MUMMY SPIDER.** This actor is **associated with the malware commonly known as Emotet or Geodo.**

MUMMY SPIDER is a criminal entity linked to the core development of the malware most commonly known as Emotet or Geodo. First observed in mid-2014, this malware shared code with the Bugat (aka Feodo) banking Trojan. However, **MUMMY SPIDER swiftly developed the malware's capabilities to include an RSA key exchange for command and control (C2) communication and a modular architecture.**

MUMMY SPIDER does not follow typical criminal behavioral patterns. In particular, **MUMMY SPIDER usually conducts attacks for a few months before ceasing operations for a period of between three and 12 months**, before returning with a new variant or version.

After a 10 month hiatus, MUMMY SPIDER returned Emotet to operation in December 2016 but the latest variant is not deploying a banking Trojan module with web injects, it is currently acting as a 'loader' delivering other malware packages. The primary modules perform reconnaissance on victim machines, drop freeware tools for credential collection from web browsers and mail clients and a spam plugin for self-propagation. The malware is also issuing commands to download and execute other malware families such as the banking Trojans Dridex and Qakbot.

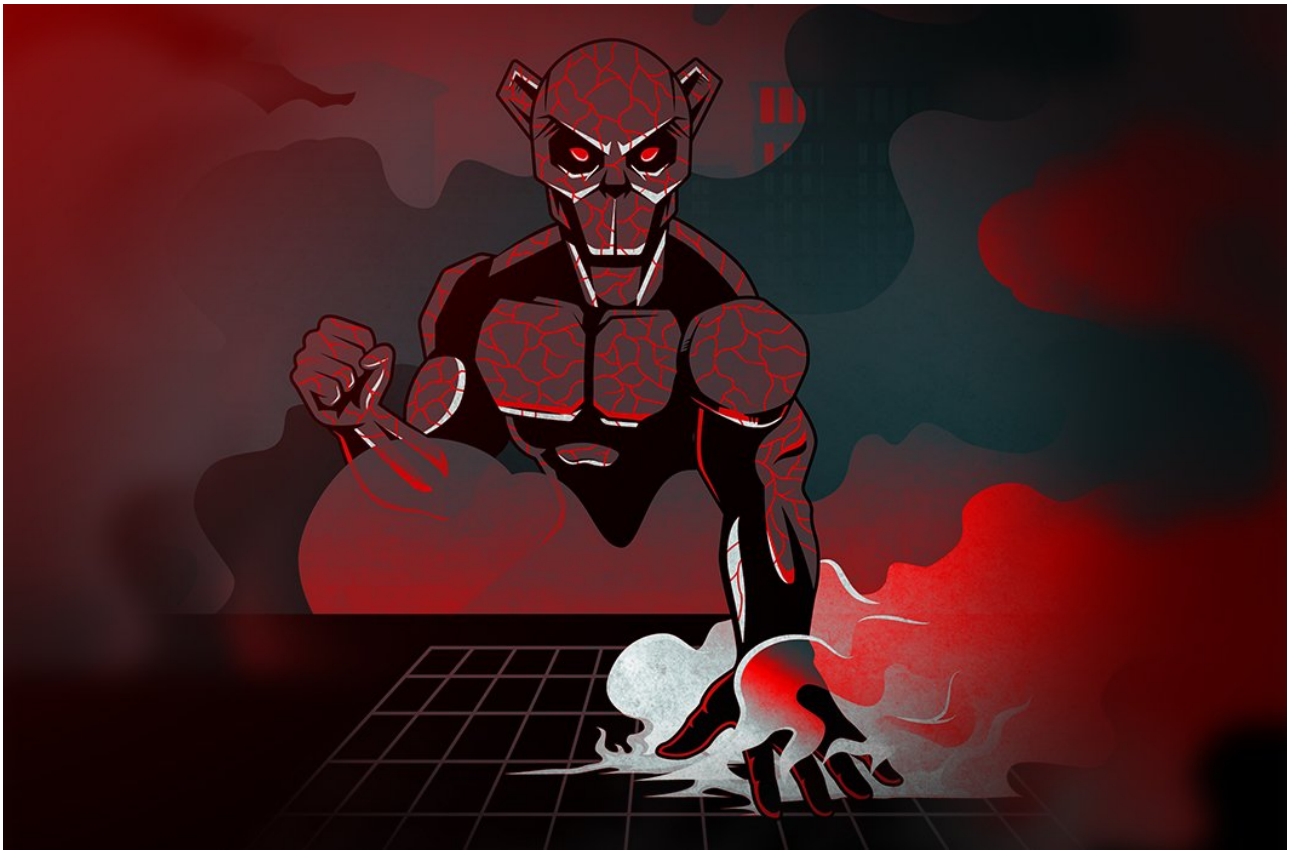
MUMMY SPIDER advertised Emotet on underground forums until 2015, at which time it became private. Therefore, it is highly likely that Emotet is operated solely for use by MUMMY SPIDER or with a small trusted group of customers.

Other Known Criminal Adversaries

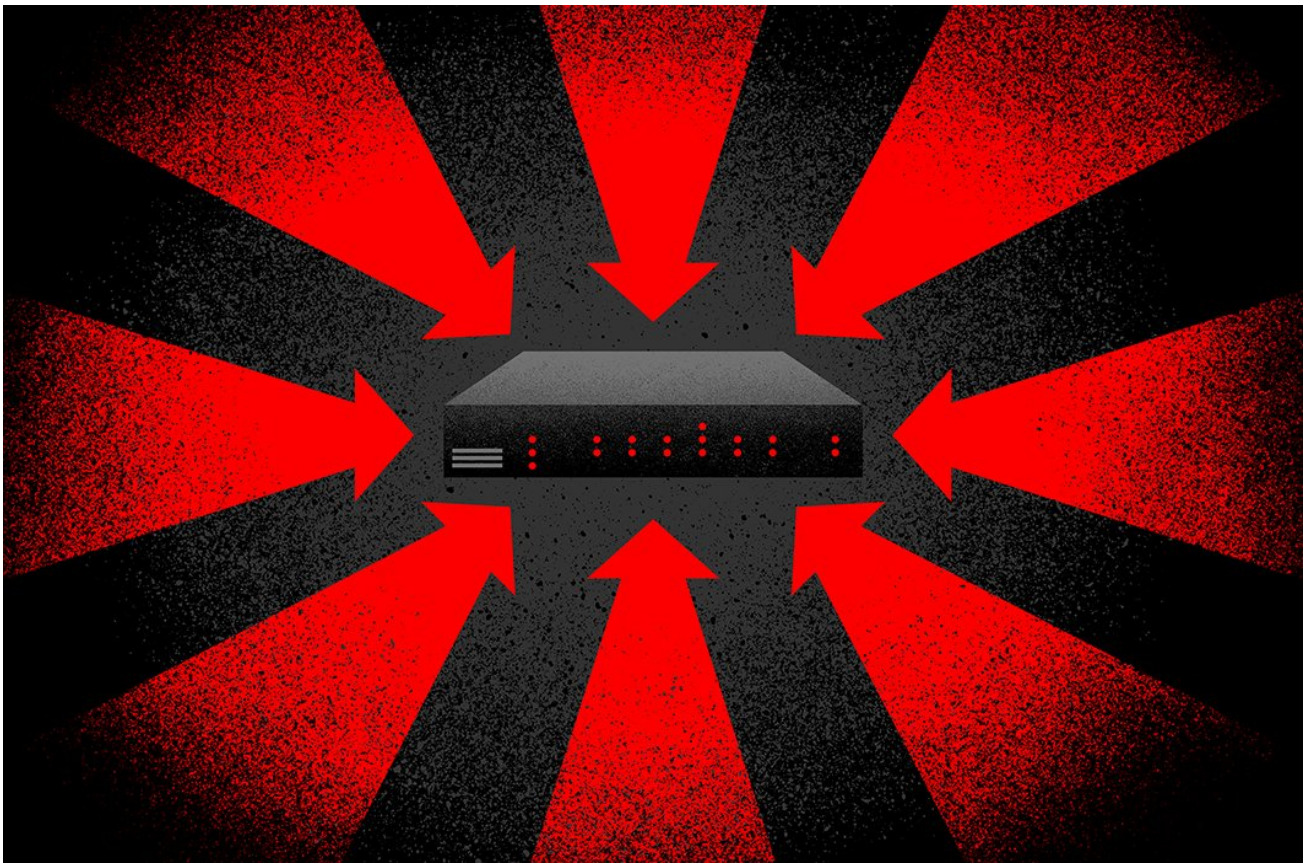
Curious about other nation-state adversaries? *Visit our threat actor center to learn about the new adversaries that the CrowdStrike team discovers.*

Learn More

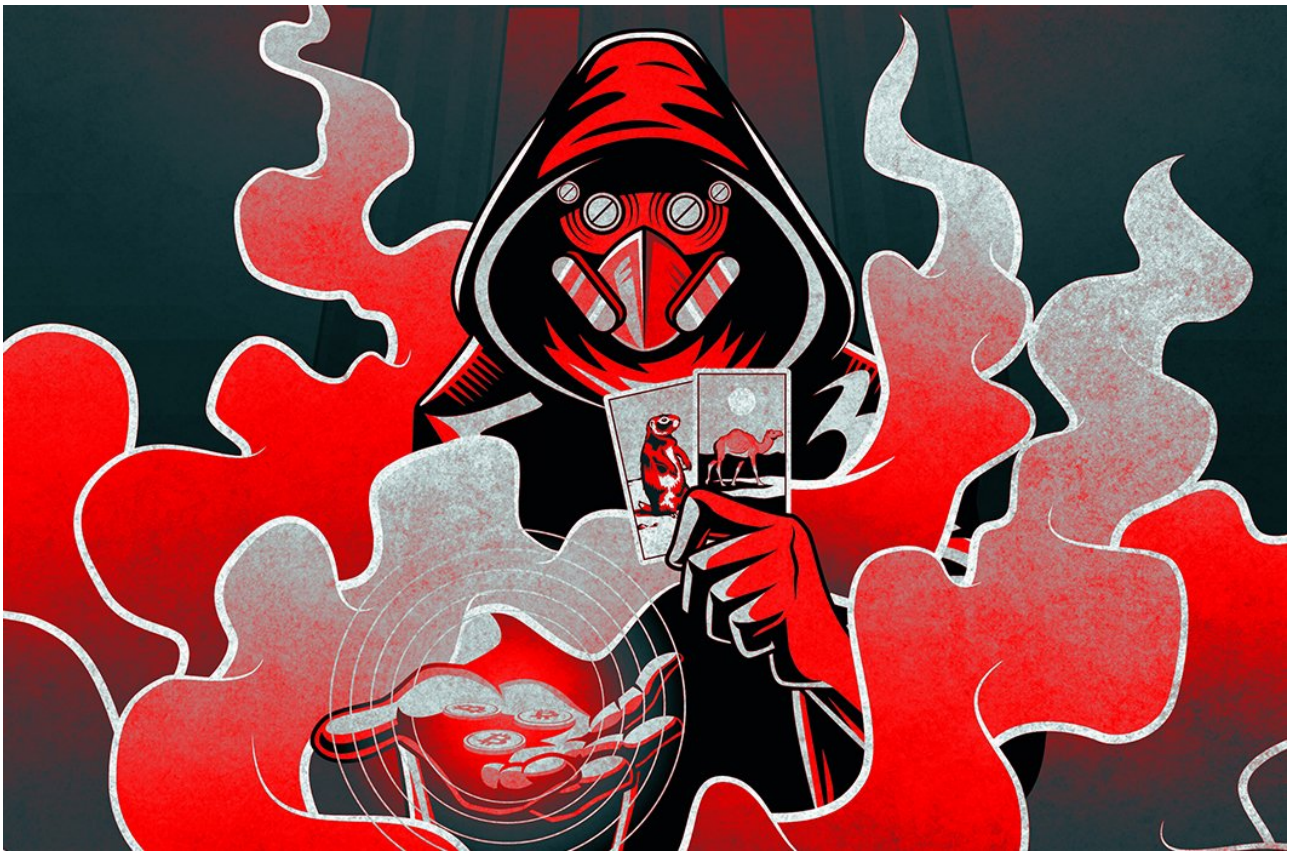
- To learn more about how to incorporate intelligence on threat actors like MUMMY SPIDER please visit the Falcon Intelligence product page.
- **Want the insights on the latest adversary tactics, techniques, and procedures (TTPs)?** Download the *CrowdStrike 2020 Global Threat Report*



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