Helix Kitten | Threat Actor Profile

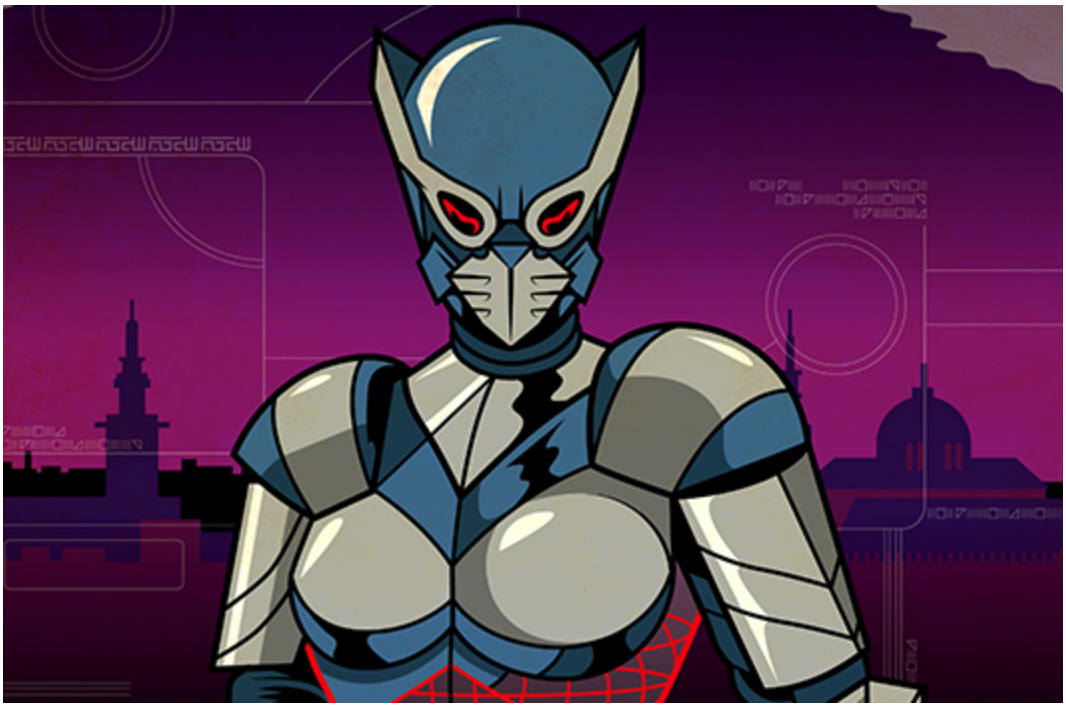
crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/

November 27, 2018

Meet CrowdStrike's Adversary of the Month for November: HELIX KITTEN

November 27, 2018

Adam Meyers Research & Threat Intel



HELIX KITTEN is likely an **Iranian-based adversary group**, **active since at least late 2015**, **targeting organizations in the aerospace, energy, financial, government, hospitality and telecommunications business verticals.**

This adversary group is **most commonly associated with a custom PowerShell implant identified as Helminth**. The Helminth implant is routinely delivered through macro-enabled Microsoft Office documents requiring user interaction to execute an obfuscated Visual Basic Script.

Additionally, **HELIX KITTEN actors have shown an affinity for creating thoroughly researched and structured spear-phishing messages** relevant to the interests of targeted personnel. In some instances, spear-phishing messages have been sent from

compromised accounts of organizations related to the target to further enhance credibility. Information technology (IT) and corporate infrastructure is a common theme of HELIX KITTEN spear-phishing messages.

In addition to Helminth, the ISMDoor implant is likely used by the Iran-based adversary to attack targets particularly those in the Middle East region. There are several infrastructure overlaps between ISMDoor and ISMAgent, a tool used exclusively by HELIX KITTEN. The implementation of the DNS transport layer protocol is very similar in both ISMDoor and ISMAgent. ISMDoor is able to exfiltrate data, take screenshots, and execute arbitrary commands on the victim's machine. Command and control (C2) is performed through a covert channel based on DNS AAAA records. The actor uses dedicated domains to host their C2 infrastructure, as the C2 protocol requires full control over the authoritative DNS server to work.

During the summer of 2018, **HELIX KITTEN actors were observed targeting entities in the Middle East** — of note, targets appeared to be located in Bahrain and Kuwait. These incidents involved spear-phishing attacks, which characteristic of HELIX KITTEN, included emails containing malicious PowerShell in their macros that connects to known C2 infrastructure.

In early November 2018, CrowdStrike® Falcon OverWatch™ observed activity from the HELIX KITTEN adversary at a customer in the telecommunications vertical. While the adversary leveraged known tooling as well as tactics, techniques, and procedures (TTPs), this activity represented a shift in targeting that could allow HELIX KITTEN to support multiple objectives.

HELIX KITTEN's operations against organizations in the telecommunications industry could allow this adversary to conduct bulk data collection of large amounts of communications data that could be later leveraged in additional intelligence activities. Targeting telecommunications can also allow the adversary to be able to reroute communications to adversary-controlled infrastructure for data collection or malware delivery. The ultimate objective of this activity remains unclear at the time of this writing, but the addition of the telecommunications sector to HELIX KITTEN's target scope is a notable development.

OilRig, Helminth, Clayslide, APT34, IRN2 are community or industry names associated with this actor.

Other Iranian-based Adversaries

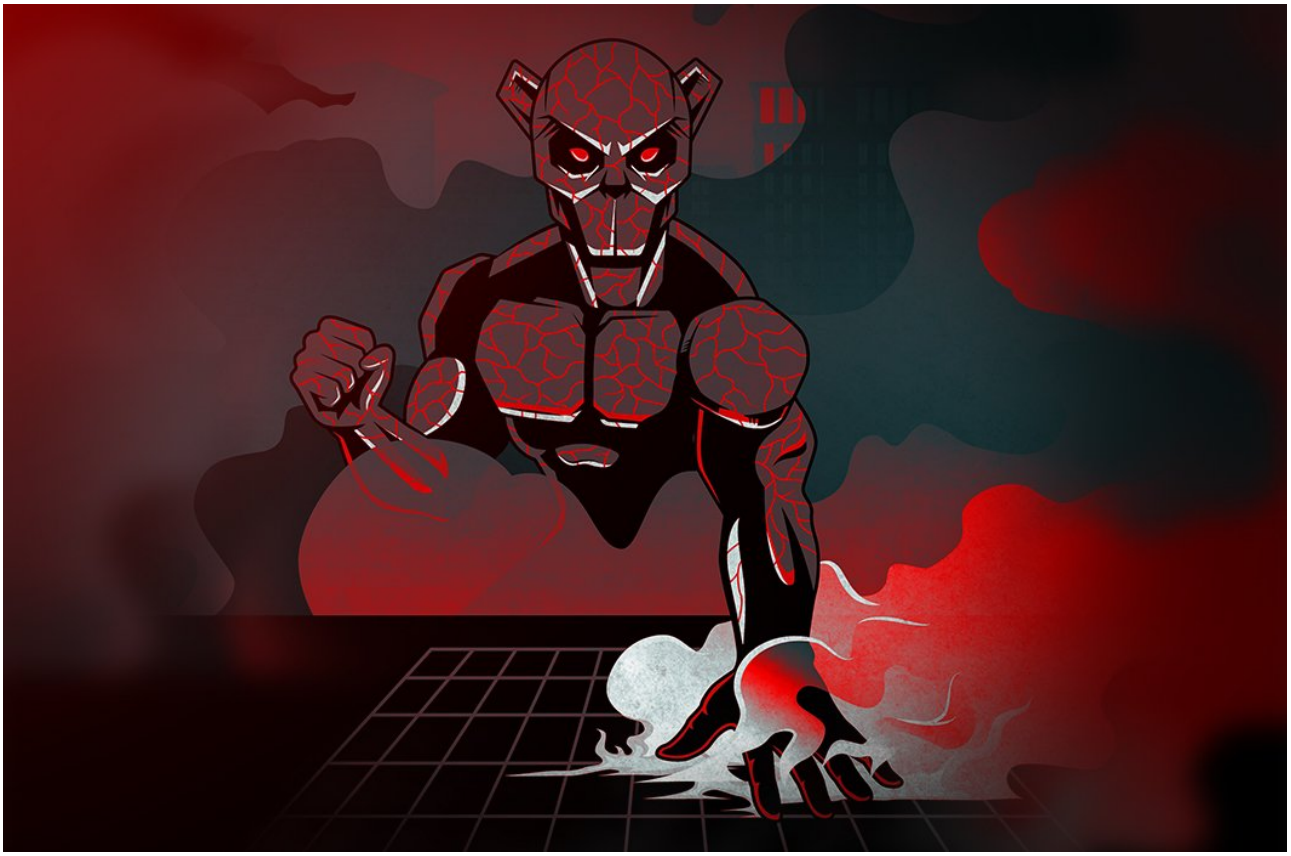
Clever Kitten

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

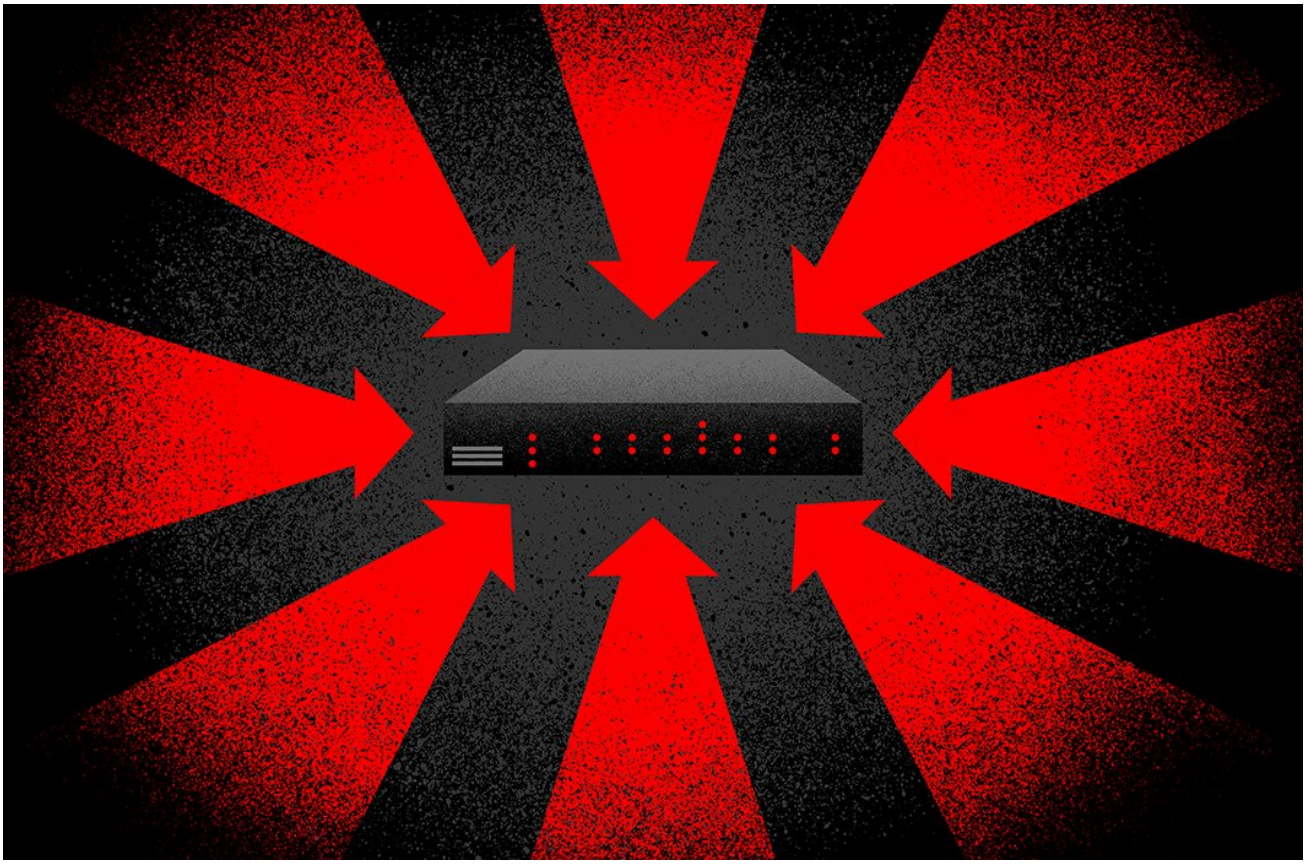
Additional Resources

- *To learn more about how to incorporate intelligence on threat actors like HELIX KITTEN into your security strategy, please visit the Falcon threat intelligence product page.*
- *Download the 2020 CrowdStrike Global Threat Report*

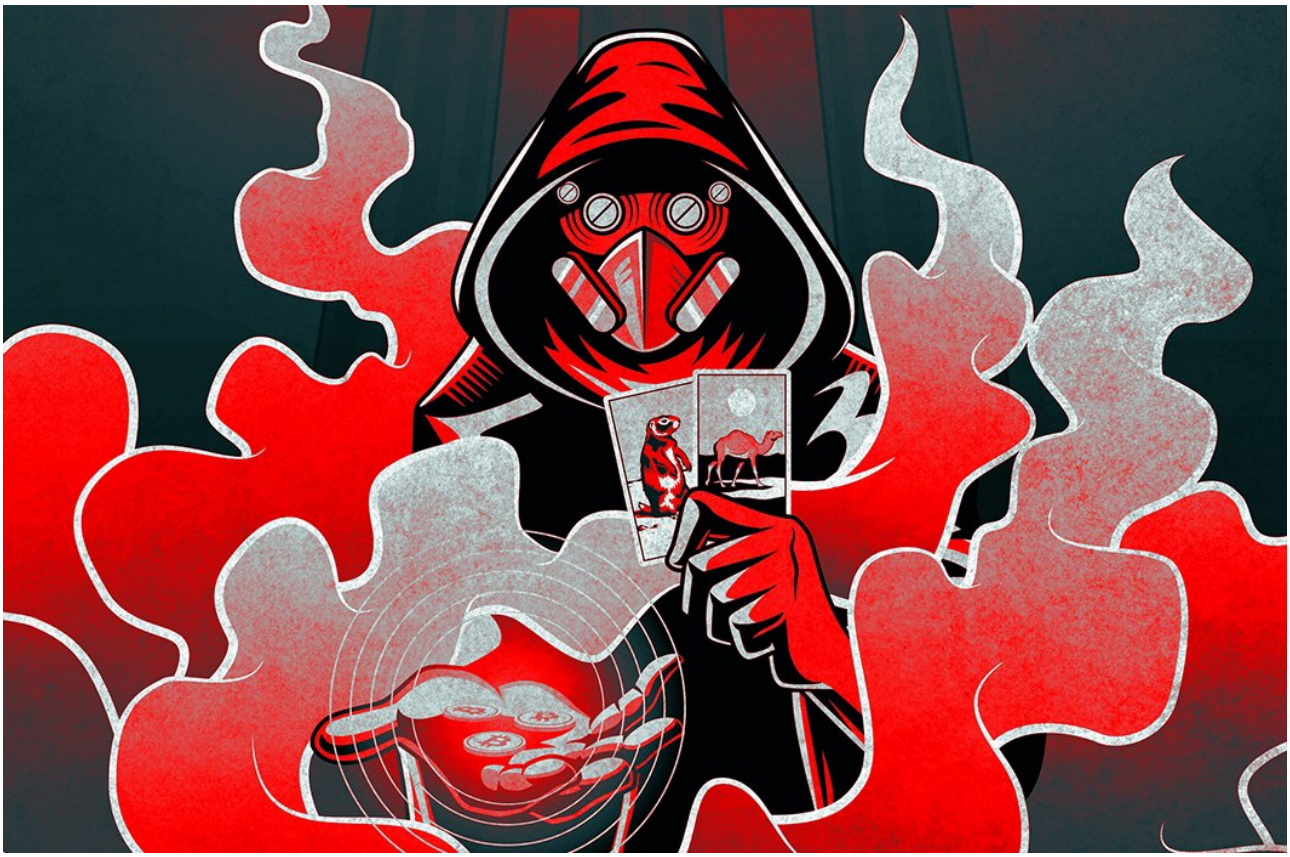
Related Content



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