Falcon OverWatch Threat Hunting Report Finds an Increase in eCrime as Adversaries Mature Their Skills

October 01, 2019 | falcon.overwatch.team | From The Front Lines

CROWDSTRIKE
2019 FALCON OVERWATCH REPORT
OBSERVATIONS FROM THE FRONT LINES OF THREAT HUNTING

The CrowdStrike® Falcon OverWatch™ elite threat hunting team has released a new report, **The 2019 OverWatch Mid-Year Report: Observations from the Front Lines of Threat Hunting.** This is the second year for this report, which is once again filled with compelling stories that provide insight into today's threat landscape, the trends you should be aware of, and the tactics, techniques and procedures (TTPs) that were most prevalent during the first half of 2019. Based on real-world analysis by the OverWatch team, which comprises cross-disciplinary specialists, the report is designed to provide critical information to inform your security strategy, helping you optimize your organization's protection today and for the future.

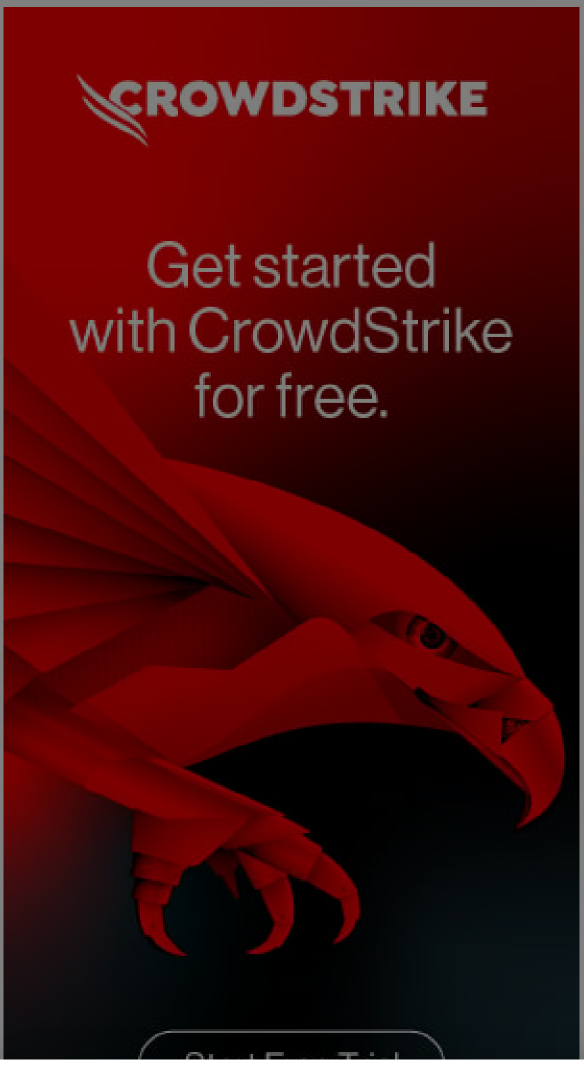
Harnessing the Power of the Threat Graph

As an integral part of the CrowdStrike Falcon®® platform, OverWatch harnesses the power of the massive CrowdStrike Threat Graph®, enriched with threat intelligence, to continuously hunt for threats while investigating and advising on sophisticated threat activity in customer environments. Armed with cloud-scale telemetry from over two trillion endpoint events collected per week, and

CATEGORIES

Cloud & Application Security	104
Counter Adversary Operations	184
Endpoint Security & XDR	307
Engineering & Tech	78
Executive Viewpoint	162
Exposure Management	84
From The Front Lines	190
Identity Protection	37
Next-Gen SIEM & Log Management	91
Public Sector	37
Small Business	8

CONNECT WITH US



that were state-sponsored or of unidentified origin. The team attributes this increase to a continuously evolving eCrime ecosystem, buttressed by greater access to "TTPs-for-hire" services, and an ongoing pursuit of larger payoffs via "Big Game Hunting" attacks. This illustrates how the free exchange of TTPs among nation-state and eCrime adversaries has resulted in an escalation of eCrime activity, emphasizing that organizations in any industry and of any size can become victims of sophisticated and strategic attacks.

Targeted Verticals per Adversary Group

The report looks at the top 10 industries targeted in the first half of 2019 and compares them to 2018. It also includes data indicating the targeting of vertical industries by specific nation-state adversaries such as BEARS (Russia), PANDAS (China), CHOLLIMAS (N. Korea), and others, including SPIDERS (eCrime). It is noteworthy that SPIDERS have targeted the widest range of industry verticals so far in 2019, as compared to their state-sponsored counterparts.

Targeted Adversary Tactics and Techniques

The report provides a heat map of adversary tactics and techniques identified by the OverWatch team, which covers the sophisticated and/or persistent intrusion campaigns the team observed in the first half of 2019, as well as a comparison mapping to 2018. These tactics and techniques are mapped along the MITRE ATT&CK^{TM} framework to ensure their accurate and consistent identification. The OverWatch team found that the results observed in this report closely mirror the results from 2018, with popular techniques such as "Valid Accounts," "Command-Line Interface," "Scripting" and "PowerShell" continuing to be highly prevalent attack methods. Some of insights the team gained regarding adversary tactics and techniques include the following:

- The predominant initial access techniques remain consistent, and include the use of valid accounts, spear-phishing, and exploitation of public-facing applications.
- There appears to be a heightened priority to evade detection, often using openly available tools such as PC Hunter and Process Hacker. As a result, network defenders must be sure to take steps to harden their security controls.
- Once they have gained access, attackers use various means to maintain a foothold. That's why threat hunting should proceed even after remediation to ensure the adversary can't reappear via a backdoor access not yet discovered.

Other Important Observations From the Report

The report includes a number of deep dives into specific adversary tools being

September 25, 2024

Recognizing the Resilience of the CrowdStrike Community
September 25, 2024

CrowdStrike Drives Cybersecurity Forward with New Innovations Spanning AI, Cloud, Next-Gen SIEM and Identity Protection
September 18, 2024

degree of access. The OverWatch team also observed an extensive use of web shells and custom tools, as well as attempts at credential dumping, "search order hijacking," and webmail services for command and control (C2) communications.

An Extensive Intrusion Targeting a Healthcare Organization

The report offers details on a protracted intrusion against a healthcare organization that predated the customer's installation of the Falcon platform. The visibility provided by Falcon allowed the OverWatch team to extend its hunt, eventually discovering the full extent of a significant intrusion. The team observed evidence of a strong adversary foothold, credential dumping, lateral movement and data exfiltration across the victim's network.

Custom Tooling and Rapidly Changing TTPs Used Against an Aviation Company

An intrusion against an aviation company revealed an adversary with a high level of administrative access using broad and consistent lateral movement, credential dumping and reconnaissance. The OverWatch team reports on the actor's extensive use of custom tooling and techniques such as SMB (Server Message Block) protocol brute force, as well as the ability to rapidly change TTPs. The team surmised that the adversary's key objective was the maintenance and expansion of their foothold in the victim's network.

eCrime Activity Against a Telecom Vertical

The OverWatch team observed an eCrime adversary engaging with a Linux-based Confluence server in a telecom organization. The actor initially engaged in light reconnaissance activity viewing multiple files relating to Confluence configuration and environment variables. The adversary then moved to retrieving and installing the ngrok tunneling tool from a remote resource, before leveraging a Python reverse shell and a netcat to establish a connection to actor-controlled infrastructure and data exfiltration. The team believes that this intrusion is the result of the opportunistic compromise of a critical vulnerability previously reported as part of a Confluence Security Advisory that was issued early in 2019.

Recommendations for Safeguarding Organizations

The report illustrates that 2019 is proving to be an active year for adversaries with a significant increase in eCrime as well as the inter-relationships across different eCrime groups. These groups continue to strengthen their organizations, forge alliances and expand their footprints in ways that are against modern attacks with real-time protection via machine learning, AI and behavioral analysis. It's also crucial that organizations optimize their security by deploying threat hunting teams, whether internal or via managed detection and response (MDR) services such as Falcon OverWatch. As part of the Falcon platform, the OverWatch team works to rapidly detect, investigate and remediate intrusions before adversaries can accomplish their objectives and cause a data breach. **Download the CrowdStrikeFalcon OverWatch 2019 Mid-Year report** for detailed accounts of the sophisticated intrusions observed in the first half of 2019, observations on the trends, tools and tactics adversaries are using and recommendations you can implement in your organization.

Additional Resources

- *Read the press release.*
- *Download the 2019 Mid-Year OverWatch Report.*
- *Visit the CrowdStrike Falcon® OverWatch webpage.*

- *Download the CrowdStrike 20120 Global Threat Report*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*

Tweet Share

Related Content

CROWDSTRIKE
FORRESTER WAVE LEADER 2024
“A product powerhouse in detection and response tech”
CrowdStrike named a Leader by Forrester

CrowdStrike Named a Leader with “Bold Vision” in 2024 Forrester Wave for Cybersecurity Incident

How to Defend Employees and Data as Social Engineering Evolves

The Anatomy of an ALPHA SPIDER Ransomware Attack