

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



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

Featured

Recent

Video

Category

Start Free Trial

Harnessing the Power of the Threat Graph



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 detailed tradecraft information on more than 120 adversary groups tracked by the CrowdStrike Intelligence team, OverWatch has the unparalleled ability to see and stop the most sophisticated breaches. This report is a summary and analysis of the work they perform continuously to protect CrowdStrike customers across the globe.

Escalation of eCrime Activities Across All Industries

This year, the OverWatch team saw a significant increase in the relative frequency of eCrime campaigns targeting customers, compared with attacks 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.

Featured

Recent

Video

Category

Start Free Trial

targeted the widest range of industry verticals so far in 2019, as compared to their state

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™](#) 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.

Featured

Recent

Video

Category

Start Free Trial

Download the report for more details on each of these events.

A Wide Range of Adversary Techniques Used Against a Telco



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

Featured

Recent

Video

Category

Start Free Trial

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.

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 impacting organizations in virtually every industry. In addition, targeted adversaries are employing increasingly creative techniques to avoid detection and perform actions on objectives. However, the report also shows that many of the techniques used by eCrime actors are easily defensible through strong security measures and a proactive security posture. Toward that end, there is a list of recommendations provided to help your organization maximize its protection against the intrusions observed by the OverWatch team. This includes leveraging security solutions that look beyond malware to defend 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.

Featured

Recent

Video

Category

Start Free Trial

- [Read the press release.](#)
- [Download the 2019 Mid-Year OverWatch Report.](#)

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

X Tweet

in Share

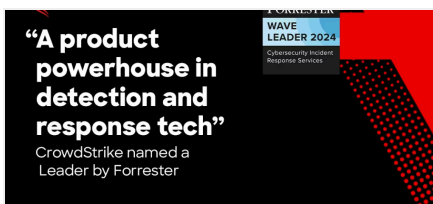


BREACHES **STOP** HERE

START FREE TRIAL

PROTECT AGAINST MALWARE, RANSOMWARE AND FILELESS ATTACKS

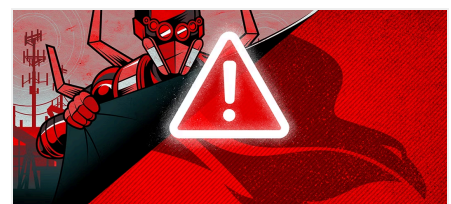
Related Content



CrowdStrike



How to Defend



The Anatomy of

Featured

Recent

Video

Category


Start Free Trial

Response
Services



CROWDSTRIKE | BLOG



	Cloud & Application Security	104
	Counter Adversary Operations	184
	Endpoint Security & XDR	306
	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



Featured

Recent

Video

Category

Start Free Trial



Get started with CrowdStrike for free.

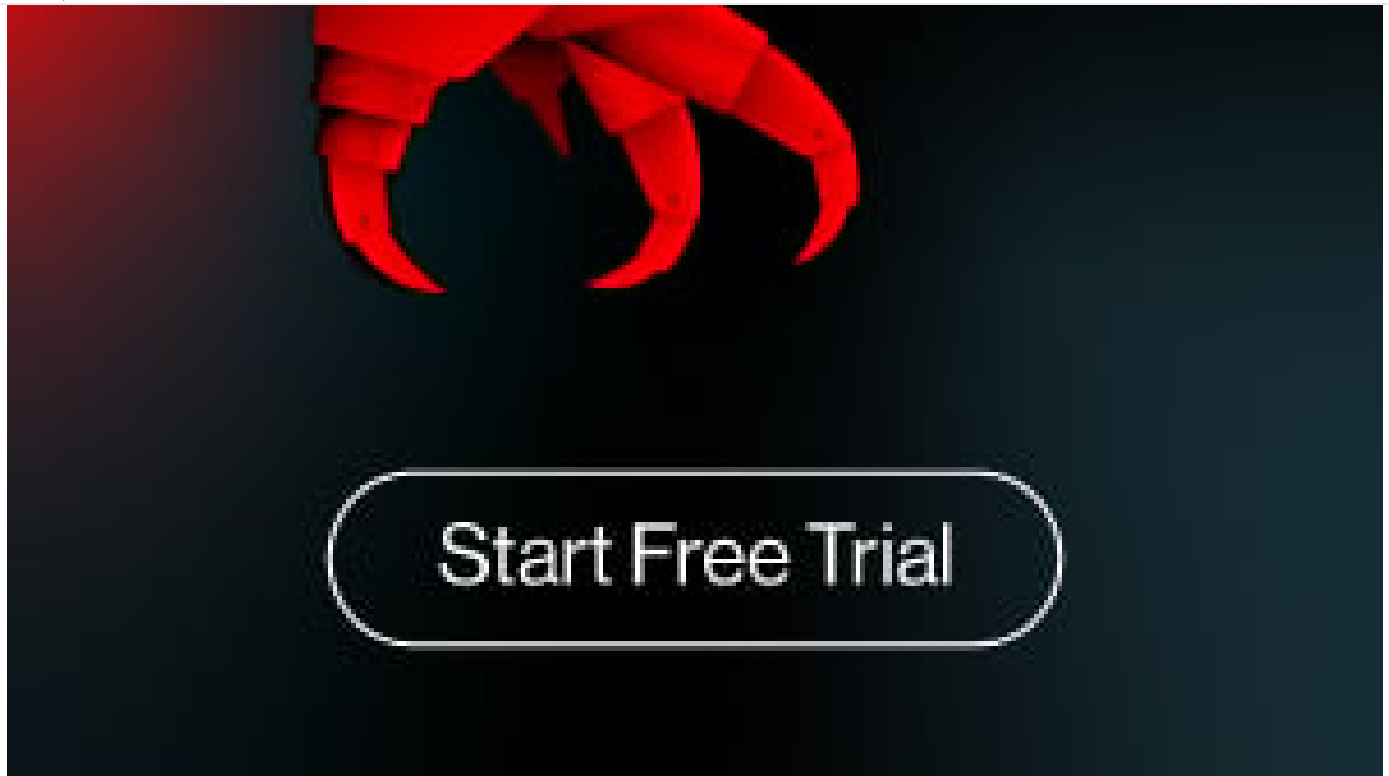
Featured

Recent

Video

Category

Start Free Trial



Featured

Recent

Video

Category

Start Free Trial



October 01, 2024

CrowdStrike Named a Leader in 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

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

SUBSCRIBE

Sign up now to receive the latest notifications and updates from CrowdStrike.

Sign Up

Featured

Recent

Video

Category

Start Free Trial

See Demo



« 5 Tips for a Happy Marriage Between IT Cybersecurity and Operational Technology Teams

Saved by the Shell: Reconstructing Command-Line Activity on MacOS »

