BACK TO NEWS RELEASES

CrowdStrike Annual Threat Report Details Attacker Insights and Reveals Industry's First Adversary Rankings

CrowdStrike reveals the adversaries with the fastest breakout time

Sunnyvale, CA – February 19, 2019 – CrowdStrike® Inc., the leader in cloud-delivered endpoint protection, today announced the release of the *2019 CrowdStrike Global Threat Report: Adversary Tradecraft and The Importance of Speed*. Key findings in the report point to the escalating activities of nation-state actors and global eCrime actors across all targeted industries, and offer lessons learned from real-life intrusions.

In today's ever-evolving cyber landscape, speed is essential for effective cyber defense. CrowdStrike's Global Threat Report reveals "breakout time" – the critical window between when an intruder compromises the first machine and when they can move laterally to other systems on the network – for top cyber adversaries. This ranking offers organizations unprecedented insight into how fast they need to be at detecting, investigating and remediating intrusions (also known as the 1-10-60 rule) to thwart adversaries they are most likely to face targeting their networks.

According to CrowdStrike's visibility, based on more than 30,000 breach attempts stopped in 2018:

- Russian nation-state actors, tracked by CrowdStrike as "Bears," are the fastest adversaries with an average breakout time of 18:49 minutes.
- North Korean nation-state actors, tracked as "Chollimas," are the second fastest with an average breakout time of 2:20:14 hours.
- Chinese nation-state actors, or "Pandas," average 4:00:26 hours.
- Iranian nation-state actors, or "Kittens," average 5:09:04 hours.
- eCrime actors, or "Spiders," have the slowest average breakout time of all adversaries: 9:42:23 hours, although some of the eCrime actors can move very rapidly and rival even the fastest nation-states.

"With the powerful combination of our massive cloud-based endpoint security dataset, threat intelligence and insights from more than 30,000 intrusions investigated by our OverWatch and Services teams in 2018, CrowdStrike has a unique understanding of adversary activity and provides the first industry ranking of adversary tradecraft," said Dmitri Alperovitch, CrowdStrike's chief technology officer and co-founder. "This year's report underscores the importance of speed of response in cybersecurity and provides valuable insights into how to defeat some of the most destructive and capable nation-state and eCrime threat actors."

Notable Highlights of the Global Threat Report:

- One of the most significant trends in eCrime for 2018 was the continued rise of "Big Game Hunting," the practice of combining targeted, intrusion-style tactics for the deployment of ransomware across large organizations.
- Another trend identified by CrowdStrike Intelligence was the increased collaboration between highly sophisticated eCrime threat actors. The use of geo-targeting to support multiple eCrime families was observed through a variety of tactics.
- The industries at the top of the target list for malware-free intrusions include media, technology and academia, highlighting the need to aggressively strengthen their defenses against more sophisticated, modern attacks.
- CrowdStrike identified several targeted intrusion campaigns by China, Iran and Russia, focused on the telecommunications sector and likely supporting state-sponsored espionage activities. Subsequent lures to drive more effective social engineering campaigns resulted in compromising telecom customers, including government entities.
- CrowdStrike observed an increasing operational tempo from China-based adversaries, which is only likely to accelerate as US-China relations continue to be strained.

The CrowdStrike Global Threat Report analyzes comprehensive threat data from CrowdStrike Falcon® Intelligence™; CrowdStrike Falcon OverWatch™, the company's industry-leading managed hunting team and CrowdStrike Services; and the CrowdStrike Threat Graph™, a massively scalable, cloud-based graph database processing 1 trillion events a week across 176 countries. Together, these teams and tools provide a holistic view of the threat environment featured in the report.

"The threat landscape is evolving at an unprecedented rate, and with every breach, a company's survival may be put on the line. Organizations can't afford a passive approach to securing their assets," said Adam Meyers, vice president of Intelligence at CrowdStrike. "As we continue to see highly sophisticated nation-state and eCrime actors elevate the level and complexity of daily threats, this report should serve as a resource for business leaders and security professionals to better understand the threat environment and make informed decisions that protect business-critical data."

"As companies continue to strengthen their security postures, adversaries are adopting more sophisticated techniques to hide their exploits and maintain their foothold," said Jennifer Ayers, vice president of OverWatch and Security Response at CrowdStrike. "Augmenting prevention, detection, and response with vigilant, real-time, 24/7 threat hunting is required to identify the clandestine actions of these actors as soon as possible in situations where time is of the essence."

CrowdStrike's co-founder and chie

Download the *2019 CrowdStrike Global Threat Report: Adversary Tradecraft and The Importance of Speed*.

About CrowdStrike®

CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence (AI), the CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver real-time protection and actionable intelligence from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

CrowdStrike Falcon protects customers against all cyber attack types, using sophisticated signatureless AI and Indicator-of-Attack (IoA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates 1 trillion security events a week from across the globe to immediately prevent and detect threats.

There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches.

Qualifying organizations can gain full access to Falcon Prevent™ by starting a free trial.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | Twitter

Contacts
CrowdStrike, Inc.
Ilina Cashiola, 202-340-0517
Ilina.cashiola@crowdstrike.com

BROWSE ALL RESOURCES

WHITE PAPERS

CROWDCASTS

VIDEOS

DEMOS & USE CASES

CASE STUDIES

COMMUNITY TOOLS

DATA SHEETS

INFOGRAPHICS

REPORTS

PRODUCTS & SERVICES

Falcon Next-Gen Antivirus
Falcon Endpoint Protection Standard
Falcon Endpoint Protection Advanced
Falcon Complete
Incident Response
Proactive Services
Experienced A Breach?

ALL PRODUCTS

TECHNOLOGY

CrowdStrike Falcon Platform

WHY CROWDSTRIKE?

Why CrowdStrike?
Industry Validation
Our Customers
Third-Party Testing
Compliance & Certification

Company

CrowdStrike's Story
Executive team
Board of Directors
Investors
News & Releases

JOIN OUR TEAM

PARTNERS

Technology Partners
Orchestration & Automation
System Integrators and Consultants
Managed Service Providers
Cloud Platforms

PARTNER LOGIN

RESOURCES

Company News & Events
Community Tools

VIEW ALL RESOURCES

BLOG

How to Install the Falcon Agent
MITRE ATT&CK Evaluation Reveals CrowdStrike Falcon as the Most Effective EDR Solution
Farewell to Kelihos and ZOMBIE SPIDER

LATEST BLOG POSTS

ENGLISH

CROWDSTRIKE

| Contact Us | Privacy