CROWDSTRIKE
Investor Relations

Adversaries are Accelerating Targeted Access to Critical Networks 3x Times Faster Than Before, CrowdStrike Reveals in Annual Threat Hunting Report

September 8, 2021

OverWatch also exposes an uptick in targeting from China-Nexus adversaries; attacks targeting telecommunications and retail more than doubled in the past year

SUNNYVALE, Calif.--(BUSINESS WIRE)--Sep. 8, 2021-- CrowdStrike Inc., a leader in cloud-delivered endpoint and workload protection, today announced the release of the CrowdStrike Falcon OverWatch™ annual report: *Nowhere To Hide, 2021 Threat Hunting Report: Insights from the CrowdStrike Falcon OverWatch Team*. The report highlights an explosion in adversary activity, both in volume and velocity. CrowdStrike's threat hunters tracked a 60% increase in attempted intrusions spanning all industry verticals and geographic regions.

The report also showcases a significant drop in average breakout time – the time it takes for an intruder to begin moving laterally outside of the initial beachhead to other systems in the network – of just one hour 32 minutes, a threefold decrease from 2020. These sobering statistics show how threat actors are constantly adapting tactics, techniques, and procedures (TTPs) to accelerate their march toward their objectives.

Additional significant OverWatch observations include:

- **Adversaries have moved beyond malware.** They are using increasingly sophisticated and stealthy techniques tailor-made to evade detections — of all of the detections indexed byCrowdStrike Threat Graph® in the past three months, 68% were malware-free.
- **China, North Korea and Iran were the most active state-sponsored groups.** The report reveals the majority of targeted intrusion activity from adversary groups were based out of China, North Korea, and Iran.
- **A massive surge in interactive intrusion activity targeting the telecommunications industry**. This activity spans all major geographic regions and has been tied to a diverse range of adversaries.
- **WIZARD SPIDER was the most prolific cyber criminal**. In fact, this group was seen in nearly double the number of attempted intrusions than any other eCrime group. WIZARD SPIDER is behind targeted operations using Ryuk and, more recently, Conti ransomware.
- **A 100% increase in instances of cryptojacking** in interactive intrusions year-over-year, correlating with increases in cryptocurrency prices.
- **Access Brokers had a banner year.** eCrime actors who specialize in breaching networks to sell that access to others played a growing and important role for other eCrime actors to stage their attempted intrusions.

"Over the past year, businesses faced an unprecedented onslaught of sophisticated attacks on a daily basis. Falcon OverWatch has the unparalleled ability to see and stop the most complex threats — leaving adversaries with nowhere to hide," saidParam Singh, vice president of Falcon OverWatch, CrowdStrike. "In order to thwart modern adversaries' stealthy and unabashed tactics and techniques, it's imperative that organizations incorporate both expert threat hunting and threat intelligence into their security stacks, layer machine-learning enabled endpoint detection and response (EDR) into their networks and have comprehensive visibility into endpoints to ultimately stop adversaries in their tracks."

The report is comprised of threat data from Falcon OverWatch, CrowdStrike's industry-leading managed threat hunting team, with contributions from CrowdStrike Intelligence and Services teams, and provides an inside look at the current threat landscape, notable adversary behavior and tactics, and recommendations to increase cyber resiliency. In the 2021 report, CrowdStrike's threat hunters directly identified and helped to disrupt more than 65,000 potential intrusions – approximately one potential intrusion every eight minutes.

The mission of Falcon OverWatch is to augment the powerful, autonomous protection of the Falcon platform with smart, mission-focused expertise to deliver the outcomes necessary to stay safe. Falcon OverWatch harnesses the massive power of the CrowdStrike Threat Graph®, enriched with CrowdStrike threat intelligence, to track, investigate and advise on sophisticated threat activity. The cloud-scale telemetry of approximately 1 trillion endpoint-related events collected per day, coupled with the detailed tradecraft on over 160 adversary groups, and enriched by automation of the CrowdStrike Falcon® platform provides the OverWatch team with the unrivaled ability to quickly identify and stop the most advanced threat actors. OverWatch's insights into new and novel adversary behaviors help to continuously advance the protection provided by Falcon, resulting in the proactive prevention of malicious activity on approximately 248,000 unique endpoints.

For additional information on the report, please visit the CrowdStrike website for a blog from the OverWatch team.

You can download a complimentary copy of the report here.

About CrowdStrike

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates approximately 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

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

View source version on businesswire.com: https://www.businesswire.com/news/home/20210908005382/en/

CrowdStrike, Inc.
Kevin Benacci, 216-409-5055
press@crowdstrike.com

Source: CrowdStrike Inc.