CrowdStrike Global Threat Report Highlights Key Trends in eCrime and Nation-State Activity

Company debuts brand-new eCrime Index showing intensity of cyber-criminal market over time; reveals adversaries exploit supply chains, double down on COVID-19 and ransomware

SUNNYVALE, Calif.--(BUSINESS WIRE)--Feb. 22, 2021-- CrowdStrike Inc., a leader in cloud-delivered endpoint and workload protection, today announced the release of the 2021 CrowdStrike Global Threat Report, detailing unique insights to the global threat landscape and offering best practices for organizations looking to amplify their cybersecurity maturity in 2021. The findings suggest supply chain attacks, ransomware, data extortion and nation-state threats prove to be more prolific than ever. On the heels of unprecedented growth in eCrime, CrowdStrike has introduced a new eCrime index (ECX) in this year's report. The ECX displays the strength, volume and sophistication of the cybercriminal market, and is updated weekly in real-time based on 18 unique indicators of criminal activity.

The 2021 Global Threat Report highlights that eCrime attacks made up 79% of all intrusions (via hands-on-keyboard activity) uncovered by CrowdStrike Falcon OverWatch, the organization's expert team of threat hunters. Among a popular vector for cyber criminals is the supply chain as it allows malicious actors to propagate multiple downstream targets from a single intrusion. Additionally, the report spotlights how nation-state adversaries infiltrated networks to steal valuable data seeking COVID-19 vaccine research, whereby threat actors have improved strategies to evade detection and camouflage in networks, many times deceiving their targets.

"There is a human being behind every attack, and cyber actors are getting bolder and more astute day-to-day. As such, it's critical to employ comprehensive cloud-native technology for increased visibility and prevention capabilities including threat intelligence and expert threat hunting to stay one step ahead of modern day attacks. Additionally, today's rapidly changing remote work environment highlights that identity protection is central to the defense of any enteprise's infrastructure. Organizations must take decisive action to control access and protect data in order to outmaneuver adversaries," said Adam Meyers, senior vice president of intelligence at CrowdStrike.

Other key findings from the 2021 Global Threat Report include:

- The healthcare industry will continue to face significant threats from criminal groups as CrowdStrike Intelligence confirmed 18 Big Game Hunting enterprise ransomware families infected 104 healthcare organizations in 2020.
- Adversaries from the Democratic People's Republic of Korea (DPRK) will be motivated to enhance cyber operations in 2021 due to COVID-19 and a resulting food shortage.
- Data extortion techniques will continue to accelerate through the introduction of Dedicated Leak Sites (DLS).
- China will focus on supply chain compromises and the targeting of key western verticals in support of the 14th Five Year Plan and the COVID-19 vaccine including academic, healthcare, technology, manufacturing and aerospace.

The Global Threat Report analyzes comprehensive threat data from CrowdStrike Falcon Intelligence, CrowdStrike Falcon OverWatch, the company's industry-leading managed hunting team, the CrowdStrike Threat Graph, a massively scalable, cloud-native graph database technology processing 5 trillion events per week across 176 countries and CrowdStrike Services, providing readers with deep insights on modern adversaries and their tactics, techniques and procedures (TTPs). Through innovative, crowd and cloud-enabled technology, CrowdStrike is able to leverage machine learning, mine data-at-scale and distill threat telemetry to customers, helping them to make more informed decisions. CrowdStrike's infinitely scalable and agile Security Cloud™ provides customers with the necessary threat identification, assessment and mitigation to secure both endpoints and workloads.

For additional information and to read a blog on report findings from George Kurtz, CrowdStrike's co-founder and chief executive officer please visit our website.

Download the *2021 CrowdStrike Global Threat Report*.

About CrowdStrike

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), 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 5 trillion endpoint-related events per week 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

service marks, and may use the brands of third parties to identify their products and services.

View source version on businesswire.com: https://www.businesswire.com/news/home/20210222005237/en/

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

Source: CrowdStrike Inc.