CROWDSTRIKE
Investor Relations

2024 CrowdStrike Global Threat Report: From Breakout to Breach in Under Three Minutes; Cloud Infrastructure Under Attack

February 21, 2024

Report indicates adversaries seek to disrupt global elections and exploit generative AI technology

AUSTIN, Texas--(BUSINESS WIRE)--Feb. 21, 2024-- CrowdStrike (Nasdaq: CRWD) today announced the findings of the 2024 CrowdStrike Global Threat Report, highlighting a surge in adversaries leveraging stolen identity credentials to exploit gaps in cloud environments and maximize the stealth, speed and impact of cyberattacks. The report also details the biggest threats on the horizon for 2024, including the disruption of global elections and the exploitation of generative AI to lower the barrier of entry and launch more sophisticated attacks.

In the 10th annual edition of the cybersecurity leader's seminal report, CrowdStrike highlights activity from some of the 230+ prolific threat groups that it tracks today. Key findings in the 2024 report include:

- **Dramatic Increase in Attack Velocity:** The speed of cyberattacks continues to accelerate at an alarming rate. The report indicates that the average breakout time is down to only 62 minutes from 84 in the previous year (with the fastest recorded attack coming in at 2 minutes and 7 seconds). Once initial access was obtained, it took only 31 seconds for an adversary to drop initial discovery tools in an attempt to compromise victims.
- **Stealthy Attacks Spike as Adversaries Compromise Credentials:** The report notes a sharp increase in interactive intrusions and hands-on-keyboard activity (60%) as adversaries increasingly exploit stolen credentials to gain initial access at targeted organizations.
- **Adversaries Follow as Business Moves to the Cloud:** Adversaries turned their sights to the cloud through valid credentials – creating a challenge for defenders looking to differentiate between normal and malicious user behavior. The report shows cloud intrusions increased by 75% overall with cloud-conscious cases amplifying by 110% Year-over-Year.
- **The Exploitation of Generative AI on the Horizon:** In 2023, CrowdStrike observed nation-state actors and hacktivists experimenting with and seeking to abuse generative AI to democratize attacks and lower the barrier of entry for more sophisticated operations. The report highlights how generative AI will likely be used for cyber activities in 2024 as the technology continues to gain popularity.
- **Disrupting Democracy by Targeting Global Elections**: With more than 40 democratic elections scheduled in 2024, nation-state and eCrime adversaries will have numerous opportunities to disrupt the electoral process or sway voter opinion. Nation-state actors from China, Russia and Iran are highly likely to conduct mis- or disinformation operations to sow disruption against the backdrop of geoconflicts and global elections.

"Over the course of 2023, CrowdStrike observed unprecedented stealthy operations from brazen eCrime groups, sophisticated nation-state actors and hacktivists targeting businesses in every sector spanning the globe. Rapidly evolving adversary tradecraft honed in on both cloud and identity with unheard of speed, while threat groups continued to experiment with new technologies, like GenAI, to increase the success and tempo of their malicious operations," said Adam Meyers, head of Counter Adversary Operations, CrowdStrike. "To defeat relentless adversaries, organizations must embrace a platform-approach, fueled by threat intelligence and hunting, to protect identity, prioritize cloud protection, and give comprehensive visibility into areas of enterprise risk."

As the cybersecurity consolidator in the AI-era, CrowdStrike pioneered the adversary-focused approach to cybersecurity and provides customers with adversary-driven intelligence, human-led analysis and the groundbreaking technology required to stay ahead of threats. This unique approach combines the unparalleled power of CrowdStrike Falcon® Intelligence with CrowdStrike Falcon® OverWatch's elite team of threat hunters to fuel the AI-native CrowdStrike XDR Falcon® platform to accelerate investigations, remediate threats and ultimately stop breaches.

Additional Resources

- Download the 2024 CrowdStrike Global Threat Report.
- To learn more about CAO's new modules, please visit our website.
- Visit CrowdStrike's Adversary Universe for the internet's definitive source on adversaries.
- Listen to the Adversary Universe podcast to glean insights into threat actors and recommendations for bolstering security.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

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

Follow us: Blog | Twitter | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

View source version on businesswire.com: https://www.businesswire.com/news/home/20240221587143/en/

Kirsten Speas
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike