2024 CrowdStrike Threat Hunting Report: Nation-States Exploit Legitimate Credentials to Pose as Insiders

North Korean insider threat targets U.S. technology companies; cloud and cross-domain attacks, credential and RMM tool abuse persists

AUSTIN, Texas--(BUSINESS WIRE)--Aug. 20, 2024-- CrowdStrike (NASDAQ: CRWD) released the 2024 Threat Hunting Report, highlighting the latest adversary trends, campaigns and tactics based on the frontline intelligence from CrowdStrike's elite threat hunters and intelligence analysts. The report reveals a rise in nation-state and eCrime adversaries exploiting legitimate credentials and identities to evade detection and bypass legacy security controls, as well as a rise in hands-on-keyboard intrusions, cross-domain attacks, and cloud control plane exploits.

Key findings include:

- **North Korea-Nexus Adversaries Pose as Legitimate U.S. Employees:** FAMOUS CHOLLIMA infiltrated over 100 primarily U.S. technology companies. Leveraging falsified or stolen identity documents, malicious insiders gained employment as remote IT personnel to exfiltrate data and carry out malicious activity.
- **Hands-on-Keyboard Intrusions Increase by 55%:** More threat actors are engaging in hands-on-keyboard activities to blend in as legitimate users and bypass legacy security controls. 86% of all hands-on intrusions are executed by eCrime adversaries seeking financial gains. These attacks increased by 75% in healthcare and 60% in technology, which remains the most targeted sector for seven years in a row.
- **RMM Tool Abuse Grows by 70%:** Adversaries including CHEF SPIDER (eCrime) and STATIC KITTEN (Iran-nexus) are using legitimate Remote Monitoring and Management (RMM) tools like ConnectWise ScreenConnect for endpoint exploitation. RMM tool exploitation accounted for 27% of all hands-on-keyboard intrusions.
- **Cross-Domain Attacks Persist:** Threat actors are increasingly exploiting valid credentials in order to breach cloud environments and eventually using that access to access endpoints. These attacks leave minimal footprints in each of those domains, like separate puzzle pieces, making them harder to detect.
- **Cloud Adversaries Target the Control Plane:** Cloud-conscious adversaries like SCATTERED SPIDER (eCrime) are leveraging social engineering, policy changes and password manager access to infiltrate cloud environments. They exploit connections between the cloud control plane and endpoints to move laterally, maintain persistence and exfiltrate data.

"For over a decade, we've vigilantly tracked the most prolific hacktivist, eCrime, and nation-state adversaries," said Adam Meyers, Head of Counter Adversary Operations at CrowdStrike. "In tracking nearly 250 adversaries this past year, a central theme emerged—threat actors are increasingly engaging in interactive intrusions and employing cross-domain techniques to evade detection and achieve their objectives. Our comprehensive, human-led threat hunting directly informs the algorithms that power the AI-native Falcon platform, ensuring that we stay ahead of these evolving threats and continue to deliver the industry's most effective cybersecurity solutions."

Additional Resources

- Download the 2024 CrowdStrike Threat Hunting Report.
- 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 to amplify security practices.

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/20240820982024/en/

Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike