CrowdStrike 2023 Threat Hunting Report Reveals Identity-Based Attacks and Hands-on-Keyboard Activity on the Rise as Adversaries Look to Bypass Defenses

A 583 percent increase in Kerberoasting identity attacks and 3x spike in malicious use of legitimate RMM tools take center stage, while adversary breakout time hits a record low

AUSTIN, Texas and BLACK HAT, Las Vegas, NV – August 8, 2023 – CrowdStrike (Nasdaq: CRWD), today announced the release of the *CrowdStrike 2023 Threat Hunting Report*. The company's sixth annual edition of the report, which covers attack trends and adversary tradecraft observed by CrowdStrike's elite threat hunters and intelligence analysts, revealed a massive increase in identity-based intrusions, growing expertise by adversaries targeting the cloud, a 3x spike in adversary use of legitimate remote monitoring and management (RMM) tools, and a record low in adversary breakout time.

Covering adversary activity between July 2022 and June 2023, the report is the first to be published by CrowdStrike's newly unveiled Counter Adversary Operations team, which was officially announced this week at Black Hat USA 2023.

Key findings from the report include:

- **583% increase in Kerberoasting identity attacks highlight massive escalation in identity-based intrusions:** CrowdStrike found an alarming nearly 6x year-over-year (YoY) spike in Kerberoasting attacks, a technique adversaries can abuse to obtain valid credentials for Microsoft Active Directory service accounts, often providing actors with higher privileges and allowing them to remain undetected in victim environments for longer periods of time. Overall, **62% of all interactive intrusions involved the abuse of valid accounts**, while there was a **160% increase** in attempts to gather secret keys and other credentials via cloud instance metadata APIs.
- **312% YoY increase in adversaries leveraging legitimate RMM tools:** Giving further credence to reports from CISA, adversaries are increasingly using legitimate and wellknown remote IT management applications to avoid detection and blend into the noise of the enterprise in order to access sensitive data, deploy ransomware or install more tailored follow-on tactics.
- **Adversary breakout time hits an all time low of 79 minutes**: The average time it takes an adversary to move laterally from initial compromise to other hosts in the victim environment fell from the previous all time low of 84 minutes in 2022 to a record 79 minutes in 2023**. Additionally, the fastest breakout time of the year was recorded at just seven minutes.**
- **The financial industry saw a stunning 80% YoY increase in interactive intrusions:** Defined as intrusions that use hands-on keyboard activity, interactive intrusions were up 40% overall.

- **Access Broker advertisements increase by 147% on criminal or underground communities:** Ready access to valid accounts for sale lowers the barrier to entry for eCrime actors looking to conduct criminal operations, and allow established adversaries to hone their post-exploitation tradecraft to achieve their objectives with more efficiency.
- **3x increase in adversary use of Linux privilege-escalation tool to exploit cloud environments:** CrowdStrike witnessed a **threefold increase in Linux tool linPEAS**, which adversaries use to gain access to cloud environment metadata, network attributes, and various credentials that they can then exploit.

"In our tracking of over 215 adversaries in the past year, we have seen a threat landscape that has grown in complexity and depth as threat actors pivot to new tactics and platforms, such as abusing valid credentials to target vulnerabilities in the cloud and in software," said Adam Meyers, head of Counter Adversary Operations at CrowdStrike. "When we talk about stopping breaches, we cannot ignore the undeniable fact that adversaries are getting faster and they are employing tactics intentionally designed to evade traditional detection methods. Security leaders need to ask their teams if they have the solutions required to stop lateral movement from an adversary in just seven minutes."

Additional Resources

- Download your copy of the full *2023 CrowdStrike Threat Hunting Report* on the CrowdStrike website.
- Listen to the CrowdStrike Adversary Universe podcast to Know and Stop the Adversary.
- Read the blog summarizing the report findings here.
- Register here to join the CrowdStrike Counter Adversary Operations team for a live CrowdCast on August 23 in North America or August 24 in EMEA and APJ.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms 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/

Contact

Kevin Benacci
CrowdStrike Corporate Communications
press@crowdstrike.com