CROWDSTRIKE
Investor Relations

2023 CrowdStrike Global Threat Report Reveals Sophisticated Adversaries Re-exploiting and Re-weaponizing Patched Vulnerabilities and Moving Beyond Ransomware

February 28, 2023

Emerging threat actors and increasing China-nexus activity drive a surge in identity and cloud threats, an uptick in social engineering, and faster breakout times

AUSTIN, Texas--(BUSINESS WIRE)--Feb. 28, 2023-- CrowdStrike (Nasdaq: CRWD), today announced the release of 2023 CrowdStrike Global Threat Report – the ninth annual edition of the cybersecurity leader's seminal report on the evolving behaviors, trends and tactics of today's most feared nation-state, eCrime and hacktivist threat actors around the world. Now tracking the activities of 200+ adversaries – including 33 new adversaries identified in the past year alone – the report found a surge in identity-based threats, cloud exploitations, China-nexus espionage and attacks that re-weaponized previously patched vulnerabilities.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20230228005546/en/

CrowdStrike Adversary Naming Conventions (Graphic: Business Wire)

The annual report is created by the world-renowned CrowdStrike Intelligence team, leveraging data from trillions of daily events from the CrowdStrike Falcon platform and insights from CrowdStrike Falcon OverWatch. Key highlights from this year's report include:

- **71% of attacks detected were malware-free** (up from 62% in 2021) and **interactive intrusions (hands on keyboard activity) increased 50% in 2022** – Outlining how sophisticated human adversaries increasingly look to evade antivirus protection and outsmart machine-only defenses.
- **112% year-over-year increase in access broker advertisements on the dark web** – Illustrating the value of and demand for identity and access credentials in the underground economy.
- **Cloud exploitation grew by 95%** and the number of cases involving **'cloud-conscious' threat actors nearly tripled year-over-year –** More evidence adversaries are increasingly targeting cloud environments.
- **33 new adversaries introduced** – The biggest increase CrowdStrike has ever observed in one year – including the highly prolific SCATTERED SPIDER and SLIPPY SPIDER behind many recent high-profile attacks on telecommunication, BPO, and technology companies.
- **Adversaries are re-weaponizing and re-exploiting vulnerabilities** – Spilling over from the end of 2021, Log4Shell continued to ravage the internet, while both known and new vulnerabilities like ProxyNotShell and Follina – just two of the more than 900 vulnerabilities and 30 zero-days Microsoft issued patches for in 2022 – were broadly exploited as nation-nexus and eCrime adversaries circumvented patches and side stepped mitigations.
- **eCrime actors moving beyond ransom payments for monetization** – 2022 saw **a 20% increase in the number of adversaries conducting data theft and extortion campaigns.**
- **China-nexus espionage surged across all 39 global industry sectors and 20 geographic regions tracked by CrowdStrike Intelligence** – Rise in China-nexus adversary activity shows that organizations across the world and in every vertical must be vigilant against the threat from Beijing.
- **Average eCrime breakout time is now 84 minutes** – This is down from 98 minutes in 2021, demonstrating the extensive speed of today's threat actors.
- **The cyber impact of Russia-Ukraine war was overhyped but not insignificant** – CrowdStrike saw a jump in Russia-nexus adversaries employing intelligence gathering tactics and even fake ransomware, suggesting the Kremlin's intent to widen targeting sectors and regions where destructive operations are considered politically risky.
- **An uptick in social engineering tactics targeting human interactions** – Tactics such as vishing direct victims to download malware and SIM swapping to **circumvent multifactor authentication (MFA).**

"The past 12 months brought a unique combination of threats to the forefront of security. Splintered eCrime groups re-emerged with greater sophistication, relentless threat actors sidestepped patched or mitigated vulnerabilities, and the feared threats of the Russia-Ukraine conflict masked more sinister and successful traction by a growing number of China-nexus adversaries," said Adam Meyers, head of intelligence at CrowdStrike. "Today's threat actors are smarter, more sophisticated, and more well resourced than they have ever been in the history of cybersecurity. Only by understanding their rapidly evolving tradecraft, techniques and objectives – and by embracing technology fueled by the latest threat intelligence – can companies remain one step ahead of today's increasingly relentless adversaries."

A closer look at some of the new adversaries:

CrowdStrike Intelligence added 33 newly tracked adversaries bringing the total number of known adversaries tracked to more than

200. More than 20 of the new additions were SPIDERS, the CrowdStrike naming convention for eCrime adversaries. Among the newly tracked BEARs (Russia-nexus adversaries), GOSSAMER BEAR's credential-phishing operations were highly active throughout the first year of the Russia-Ukraine conflict, targeting government research labs, military suppliers, logistics companies and non-governmental organizations (NGO). CrowdStrike also introduced its first Syria-nexus adversary, DEADEYE HAWK, which was formerly tracked as the hacktivist DEADEYE JACKAL.

The CrowdStrike Intelligence team benefits from an unparalleled raw collection of intelligence data, leveraging trillions of security events per day to help stop the most ubiquitous of threats and power the CrowdStrike Falcon® platform. As the platform of consolidation in security, Falcon enables organizations to proactively stop the most sophisticated of threats via its unique combination of endpoint and identity threat protection technology, adversary-driven intelligence and human-led analysis.

Additional Resources

- Download the 2023 CrowdStrike Global Threat Report.
- Visit CrowdStrike's Adversary Universe for the internet's definitive source on adversaries.
- To learn more about integrating threat intelligence into your security stack with CrowdStrike's industry-leading, adversary-focused technology, please visit our website.

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/

View source version on businesswire.com: https://www.businesswire.com/news/home/20230228005546/en/

Kevin Benacci
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike