CROWDSTRIKE

2023 Cloud Risk Report:

Learn the Adversaries and Tactics Targeting the Cloud

95%
Increase in Cloud Exploitation

3X
Increase in Cases Involving Cloud-Conscious Threat Actors

Adversaries Are Sharpening Cloud TTPs

A number of adversary groups, including **COZY BEAR** (Russia-nexus), **SCATTERED SPIDER** (eCrime), **LABYRINTH CHOLLIMA** (DPRK-nexus) and **COSMIC WOLF** (Turkey-nexus) are growing more sophisticated and determined in targeting the cloud.

COZY BEAR

- **Country of origin:** Russian Federation
- **Tactics:** Uses malicious tools to modify cloud services

Learn more about this prolific adversary and how they affect the global cloud landscape.

Learn More

SCATTERED SPIDER

- **Country of origin:** Unknown
- **Tactics:** Deploys ransomware from a cloud staging environment

Get to know this eCrime adversary and how they target cloud environments.

Learn More

LABYRINTH CHOLLIMA

- **Country of origin:** North Korea
- **Tactics:** Uses cloud resources to deliver documents with malicious macros

Find out how this dangerous adversary is causing damage across the cloud landscape.

Learn More

COSMIC WOLF

- **Country of origin:** Turkey
- **Tactics:** Targets victim data stored within cloud environments

Learn how this targeted intrusion adversary operates in the cloud.

Learn More

Identity Is a Key Cloud Access Point

Threat actors are seeking new ways to leverage identities in the cloud

43%

Adversaries are becoming more reliant on valid accounts, which were used to gain initial access in **43%** of cloud intrusions observed.*

67%

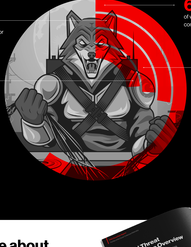
In **67%** of cloud security incidents, CrowdStrike found identity and access management roles with elevated privileges beyond what was required — indicating an adversary may have subverted the role to compromise the environment and move laterally.*

47%

Nearly half (47%) of critical misconfigurations in the cloud were related to poor identity and entitlement hygiene.*

Human Error Drives Cloud Risk

Cloud misconfigurations are gaps, errors or vulnerabilities that expose a cloud environment to risk. These can occur when security settings are poorly chosen or not implemented at all. Multi-cloud environments can be complex, and it can be difficult to tell if excessive account permissions are granted, improper public access is configured or other mistakes are made.



28% of workloads run as root or allow escalating to root*

24% of workloads have root-like capabilities*

60% of workloads lack properly configured security protections*

26% of workloads have Kubernetes Service Account Token automounted*

Learn more about threats to your cloud environment.

Download the CrowdStrike 2023 Cloud Risk Report

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/

CROWDSTRIKE
Protection that powers you

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: Protection that powers you.

*Source: Observed cloud security data over a 24-hour evaluation period