CROWDSTRIKE

# 2023 Cloud Risk Report

## The Rise of the Cloud-Conscious Adversary

# Contents

# Executive Summary

Cloud-conscious cyberattacks skyrocketed from 2021 to 2022: Observed cloud exploitation cases grew by 95% and cases involving adversaries targeting cloud environments have nearly tripled, increasing 288% year-over-year.[1]

Defending cloud environments from this activity requires knowledge of what threat actors are doing — how they're breaking in and moving laterally, which resources they target and the steps they take to evade detection.

The CrowdStrike 2023 Cloud Risk Report puts a spotlight on adversaries targeting enterprise cloud environments and the tactics, techniques and procedures (TTPs) they employ. It uncovers key trends in adversary activity, shares real-world stories of recent attacks on cloud environments, reveals critical oversights that are leaving organizations vulnerable, and offers guidance for defending against increasingly cloud-conscious adversaries.

1 CrowdStrike 2023 Global Threat Report

# Among the key findings:

## Adversaries are sharpening their use of cloud TTPs.

- A number of adversary groups, including SCATTERED SPIDER (eCrime), COZY BEAR (Russia-nexus), COSMIC WOLF (Turkey-nexus) and LABYRINTH CHOLLIMA (North Korea-nexus), are growing more sophisticated and determined in targeting the cloud.
- Nation-state and criminal adversaries are using cloud infrastructure to host phishing lure documents and malware. Adept threat actors implement command-and-control (C2) channels on top of existing cloud services.
- In 28% of incidents CrowdStrike found during the observation window, adversaries manually deleted a cloud instance to remove evidence and evade detection.*

## Identity is the key cloud access point.

- Adversaries are ramping up their use of valid accounts, which were used to gain initial access in 43% of cloud intrusions CrowdStrike observed over the last year.
- Nearly half (47%) of critical misconfigurations in the cloud are related to poor identity and entitlement practices.*
- In 67% of cloud security incidents, CrowdStrike found identity and access management (IAM) roles with elevated privileges beyond what was required — indicating an adversary may have subverted the role to compromise the environment and move laterally.*

## Human error drives cloud risk.

- 60% of containers CrowdStrike observed lacked properly configured security protections.*
- 36% of cloud environments had insecure cloud service provider default settings.*

---

**The findings in this report are drawn from data and observations from real-world cyberattacks. These incidents were uncovered, analyzed and neutralized by CrowdStrike Falcon® Cloud Security, CrowdStrike Falcon® Intelligence, CrowdStrike® Falcon OverWatch™ managed threat hunting, and incident response engagements.**

**CrowdStrike expects cloud targeting to continue to accelerate. As threats evolve, it is imperative organizations learn what they are up against in order to effectively protect cloud environments.**

# Cloud Threat Landscape Overview

## Top Cloud-Conscious Adversaries

Cloud-conscious adversaries, which abuse cloud-specific features to achieve their goals, pose significant risk to cloud environments. They have a deep understanding of cloud infrastructure and continue to refine their tactics to abuse cloud services and exploit cloud vulnerabilities and misconfigurations. Defending against these threat actors requires an understanding of the motivations, strategies and techniques they use to infiltrate the cloud.

Below are four prolific adversaries and their unique tactics.