CROWDSTRIKE

Protectors of the Cloud:

Combating the Rise in Threats to Cloud Environments

Introduction

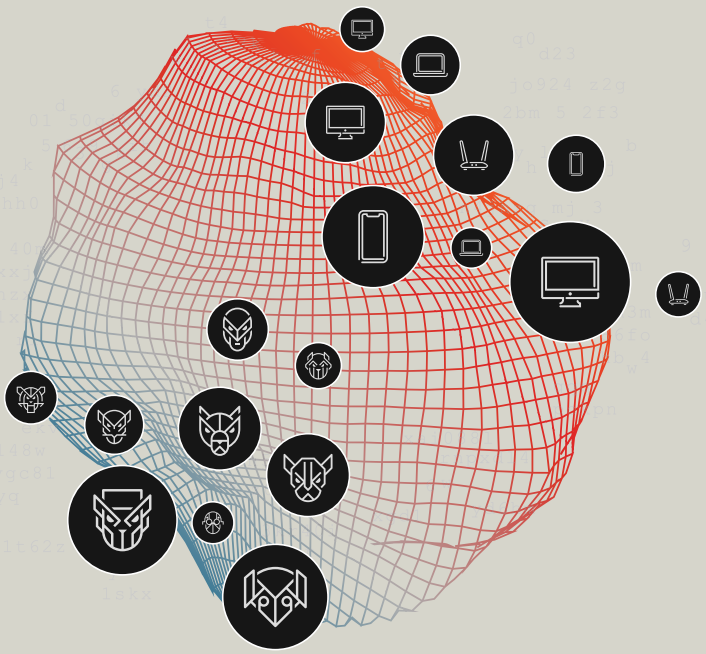
Cloud services are an essential part of the digital fabric of the modern enterprise. Yet while cloud adoption has brought increased agility, scalability and cost savings to many businesses, it has also caused a shift in focus for adversaries.

Just as organizations have realized efficiencies through the cloud, so too have attackers. Threat actors are using the same services as their prey, and for the same reason: to enhance and optimize their operations. From vulnerability exploitation to credential theft, attackers are going after any weak points that will allow them to compromise the ever-growing amount of critical business data and applications being hosted in the cloud.

In the CrowdStrike 2022 Global Threat Report, CrowdStrike experts outlined the threats facing cloud environments as part of an examination of the threat landscape facing today's businesses: ransomware-related data leaks increased 82% and interactive intrusion campaigns increased 45% from 2020 to 2021. From the data center to the cloud, the process of protecting user credentials, identifying misconfigurations and vulnerabilities, and remediating security issues is only getting more complex — and more urgent to address. Here is a look at how attackers are targeting cloud deployments.

Increasing Threats to Cloud Environments

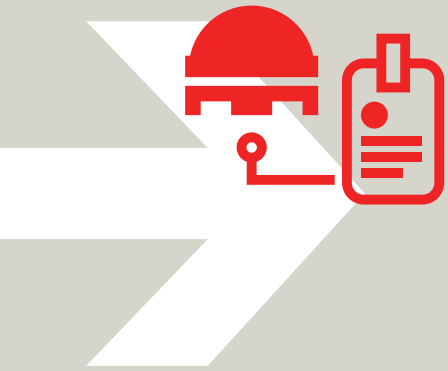
Cloud-based services now form crucial elements of many business processes, easing file sharing and collaboration. However, these same services are increasingly abused by malicious actors in the course of computer network operations (CNO), a trend that is likely to continue in the foreseeable future as more businesses seek hybrid work environments. Common cloud attack vectors used by eCrime and targeted intrusion adversaries include cloud vulnerability exploitation, credential theft, cloud service provider abuse, use of cloud services for malware hosting and C2, and the exploitation of misconfigured image containers.



Cloud Vulnerability Exploitation

Malicious actors tend to opportunistically exploit known RCE vulnerabilities in server software, typically scanning for vulnerable servers without focusing on particular sectors or regions. After initial access, actors may deploy a variety of tools. Wider criminal exploitation of cloud services for initial access includes the exploitation of Accellion FTA vulnerabilities. Since January 2021, multiple companies have self-disclosed breaches related to the exploitation of such vulnerabilities.

VMware has also been targeted by threat actors, including CVE-2021-21972 — a critical vulnerability impacting VMware ESXi, vCenter Server and Cloud foundation products. Targeting this vulnerability provides a simple and reliable method for exploitation that threat actors can use across multiple host-operating systems, attack vectors and intrusion stages. Multiple adversaries, particularly BGH actors, have likely leveraged this vulnerability.



Credential Theft

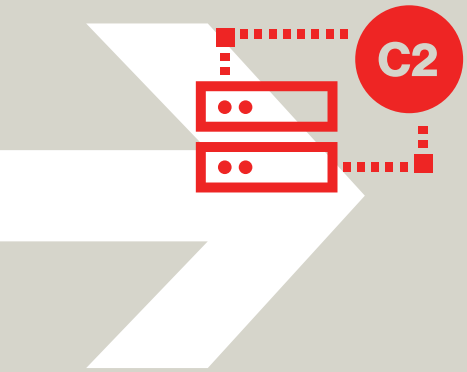
Credential-based intrusions against cloud environments are among the more prevalent exploitation vectors used by eCrime and targeted intrusion adversaries. Criminal actors routinely host fake authentication pages to harvest legitimate authentication credentials for cloud services such as Microsoft Office 365 (O365), Okta or online webmail accounts. Actors then use these credentials to attempt to access victim accounts.

Access to cloud-hosted email or file-hosting services can also facilitate espionage and theft of information. In April 2021, CrowdStrike observed COSMIC WOLF targeting victim data stored within a large CSP cloud environment. The adversary compromised the environment via a stolen credential that allowed the operator to interact with AWS using the command line. Employing this technique, the adversary altered security group settings to allow direct SSH access from malicious infrastructure.

Cloud Service Provider Abuse

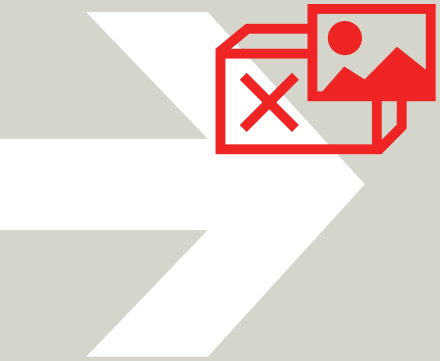
Adversaries have leveraged cloud service providers to abuse provider trust relationships and gain access to additional targets through lateral movement from enterprise authentication assets hosted on cloud infrastructure. If an adversary can elevate their privileges to global administrator levels, they may be able to pivot between related cloud tenants to further their access.

This issue is particularly significant if the initially targeted organization is a managed service provider (MSP). In this case, global administrator access can be used to take over support accounts used by the MSP to make changes to their customer networks, thereby creating multiple opportunities for vertical propagation to many more networks. This technique was used by COZY BEAR throughout 2020, with evidence of continued intrusion in MSP networks continuing into 2021.



Malware Hosting and Command and Control

Both eCrime and targeted intrusion adversaries extensively leverage legitimate cloud services to deliver malware; targeted actors also use these services for command and control. This tactic has the advantage of being able to evade signature-based detections, because top-level domains of cloud hosting services are typically trusted by many network scanning services. Using legitimate cloud services, including chat applications, can enable adversaries to evade some security controls by blending into normal network traffic. Moreover, using cloud-hosting providers for C2 allows the adversary to switch or remove payloads from an affiliated C2 URL with ease.

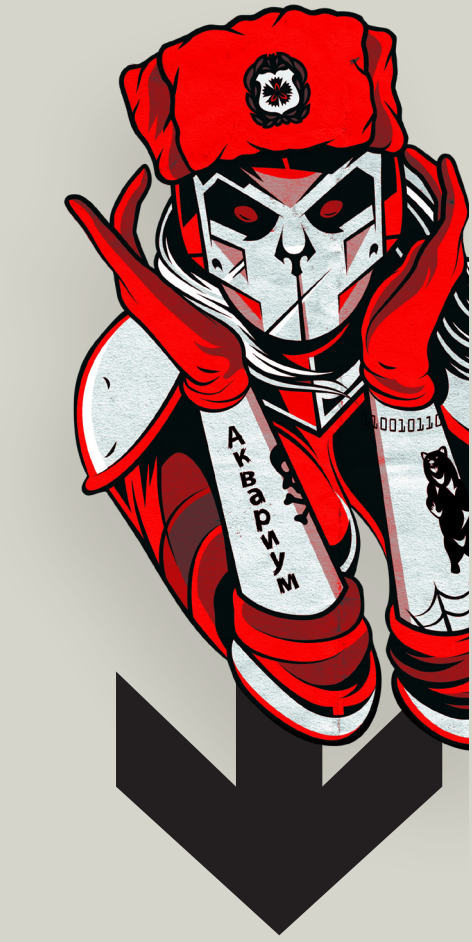


Exploitation of Misconfigured Image Containers

Criminal actors have periodically exploited improperly configured Docker containers. Docker images are templates used for creating containers. These images can be used either on a standalone basis, for users to directly interact with a tool or service, or as the parent to another application. Because of this hierarchical mode, if an image has been modified to contain malicious tooling, any container derived from it will also be infected.

In 2021, CrowdStrike Intelligence reported on the malware family *Doki*, which uses containers as both an initial infection vector and as a means for parallel track tasking. Once malicious actors gain access, they can abuse these escalated privileges to accomplish lateral movement and then proliferate throughout the network.

CrowdStrike Intelligence has also continued to track adversary operations involving the access and modification of constituent parts of Kubernetes clusters. Kubernetes is an open-source container-orchestration system that automates the deployment, scaling and management of applications and their associated shared resources. Falcon OverWatch has observed increasing adversary interest in Kubernetes clusters operating within corporate environments. The Kubernetes framework is a complex system comprising a number of constituent parts, allowing ample opportunity for misconfiguration that could provide an adversary with initial access to one component and subsequent lateral propagation opportunities that provide access to desired resources.



Threat Highlight: Russian Adversaries Look to the Cloud

FANCY BEAR

The FANCY BEAR adversary is associated with the 85th Main Center of the Special Services (aka Military Unit 26165) of Russia's Main Intelligence Directorate (GRU). Earlier in its operational lifespan, when conducting victim exploitation and credential collection, the adversary extensively used spear-phishing emails containing malicious documents or links that redirected to malicious infrastructure. However, after multiple exposures of its operations — particularly by the U.S. Department of Justice (DOJ) in 2018 — FANCY BEAR appears to have reevaluated their operational tradecraft and decreased their use of malware while shifting toward increased use of credential-harvesting tactics including both large-scale scanning techniques and victim-tailored phishing websites.

Credential harvesting plays a significant role in FANCY BEAR's acquisition of intelligence and primary access into target organizations or individuals. Adapting to the trend of public and private entities increasingly hosting parts of their internal infrastructure (e.g., email, internal chat, or identity and device-management services) via cloud services, the adversary has targeted numerous cloud-based email providers with a variety of collection methodologies throughout 2021. Examples of targeted email providers include enterprise services such as Microsoft 365 or GSuite, as well as webmail services more likely used by individuals. The adversary's credential-collection operations have technically matured over the years while maintaining a consistently high volume and tempo.

COZY BEAR

Throughout 2021, COZY BEAR also repeatedly demonstrated a high level of post-exploitation proficiency, particularly involving the enumeration of, and lateral movement within, cloud environments. During a CrowdStrike Services investigation, COZY BEAR operators were identified using authentication cookie theft to bypass multifactor authentication (MFA) restrictions implemented on target networks. This technique leverages existing local network access and has been used to access user accounts in possession of enterprise cloud service privileges. This technique highlights the adversary's ability to use a range of post-compromise activities to expand their access and maximize intelligence collection.

Future operations consistent with this cluster of COZY BEAR-associated activity are highly likely to continue mirroring this behavior, particularly through the successive identification and compromise of user accounts that are assigned administrative or special privileges on cloud services and tenants. This assessment is made with moderate confidence based on the increasing application of MFA restrictions on cloud service access and the consistency of COZY BEAR-related operations identified to date.

From the Front Lines — Adversaries Have Their Heads in the Cloud

While the pandemic accelerated the move to the cloud for many organizations, with some electing to go all-in on cloud, other organizations have continued to test the waters and gradually move certain services or capabilities into various cloud platforms. CrowdStrike is even seeing some early cloud adopters moving from legacy cloud deployments to new architectures hoping to improve scalability, maintenance and security. No matter where you are in your cloud journey, managing the security posture of cloud environments can play a critical role in preventing a breach.

CrowdStrike continues to see adversary activity in three particular areas concerning the cloud:

01 Neglected cloud infrastructure that is slated for retirement yet still contains sensitive data

02 A lack of outbound restrictions and workload protection to exfiltrate your data

03 Adversaries leveraging common cloud services to obfuscate malicious activity

Neglected or Misconfigured Cloud Infrastructure

One trend CrowdStrike has seen is adversaries targeting cloud infrastructure slated for retirement or neglected for various reasons. These attack paths stem from infrastructure that is no longer receiving security configuration updates and regular maintenance. Unfortunately, investments in security controls such as monitoring, detailed logging, security architecture and planning, and posture remediation are no longer being made in these environments.

Lack of Outbound Restrictions and Workload Protection

CrowdStrike continues to see cases where neglected cloud infrastructure still contains critical business data and systems. Attacks on such systems have led to sensitive data leaks requiring costly investigation and reporting obligations, and have resulted in impactful service outages in cases where the systems were still providing critical services that hadn't been fully transitioned to new infrastructure. Moreover, the triage, containment and recovery from such incidents have had a tremendous negative impact on some organizations.

Adversaries Leveraging Loopholes in Identity and MFA Protection Strategies

Most organizations have heard the constant drumbeat of multifactor authentication (MFA) for protecting their cloud and software-as-a-service (SaaS)-based resources by now. Yet adversaries are still able to gain access, including privileged access, to their victims' services.

CrowdStrike has identified three trends hampering the delivery of a complete authentication defense strategy:

- Failure to fully deploy MFA, especially to the most important accounts — those with administrative privileges (admins) and with access to sensitive data — sometimes as the result of excessive policy exclusion groups.
- Failure to disable legacy authentication protocols that do not support MFA.
- Failure to track and control privileges and credentials for both users and cloud service principals — including impersonation privileges and password — and certificate-based credentials for service accounts.

Synchronization of admin accounts from the cloud to the domain and vice versa also continues to play a large role in increasing the damage adversaries can do. A lack of illustrated, step-by-step guidance from cloud service providers and limited prioritization guidance from cloud security posture management (CSPM) vendors has left customers to attempt to become experts on their own, often with limited success. This has enabled adversaries to fly below the radar for months and sometimes years while they exfiltrate data, deploy ransomware code and conduct other actions toward their objectives.

An Adversary-focused Approach Is Critical to Cloud Security

The game has changed when it comes to security. When organizations only had to worry about their on-premises systems, activity was easier to monitor and analyze. Unfortunately, the traditional security and networking tools that worked in legacy environments are not as successful in the cloud. As a result, many enterprises have turned to a mix of homegrown and legacy approaches that create silos and complicate management. Poor visibility means that security risks can fly under the radar and open doors for attackers. Just as in on-premises environments, security teams with insight into the tools and tactics of attackers will have the best chance to identify and stop threats more quickly.

The CrowdStrike 2022 Global Threat Report depicted a challenging landscape for companies embracing the cloud. The most common causes of cloud breaches continue to be manual errors. Part of solving this problem involves increasing the use of templates and automation to reduce the risk of misconfigurations making their way into the production environment. A second solution is using CSPM solutions such as CrowdStrike Falcon Horizon™.

Falcon Horizon monitors cloud resources to detect misconfigurations, vulnerabilities and security threats and provides guided remediation to resolve security risks. Falcon Horizon's adversary-focused approach provides real-time threat intelligence on over 180 adversary groups and more than 70 indicator of attack (IOA) detections, and guided remediation that improves investigation speed by up to 88%.[1]

Securing cloud workloads means extending visibility, compliance and security policy enforcement from the data center to the cloud. That extension requires solutions that deliver automated detection and remediation, comprehensive observability and vulnerability management.

Falcon Cloud Workload Protection provides automated discovery into all workloads and containers, continuous cloud runtime protection, image scanning, comprehensive Kubernetes protection and managed cloud threat hunting — all in a single solution. In addition, the solution is available through Falcon Cloud Workload Protection Complete, the industry's only fully managed detection and response (MDR) service for cloud workloads and containers, enabling DevOps teams to "shift left" and build securely in the cloud by fixing issues before they reach production.

1. The Total Economic Impact of the CrowdStrike Falcon Platform

What Can I Do to Protect My Cloud Environment?

The cloud introduces new aspects to protection, and they don't all translate exactly from a traditional on-premises data center model. Security teams should keep the following firmly in mind as they strive to remain grounded in best practices.

- **Enable runtime protection and obtain real-time visibility.** You can't protect what you don't have visibility into — even if you have plans to decommission the infrastructure. Central to securing your cloud infrastructure to prevent a breach are runtime protection and visibility provided by cloud workload protection. It remains critical to protect your workloads with next-generation endpoint protection, including servers, workstations and mobile devices, regardless of whether they reside in an on-premises data center or virtual cluster, or are hosted in the cloud.
- **Eliminate configuration errors.** The most common cause of cloud intrusions continues to be human errors and omissions introduced during common administrative activities. It's important to set up new infrastructure with default patterns that make secure operations easy to adopt. One way to do this is to use a cloud account factory to easily create new sub-accounts and subscriptions. This strategy ensures that new accounts are set up in a predictable manner, eliminating common sources of human error. Also, make sure to set up roles and network security groups that keep developers and operators from needing to build their own security profiles and accidentally doing it poorly.
- **Leverage a CSPM solution.** Ensure your cloud account factory includes enabling detailed logging and a CSPM — like CrowdStrike's Falcon Horizon — with alerting to responsible parties including cloud operations and security operations center (SOC) teams. Actively seek out unmanaged cloud subscriptions, and when these are found, don't assume they are managed by someone else. Instead, ensure that responsible parties are identified and motivated to either decommission any shadow IT cloud environments or bring them under full management along with your CSPM. Then use your CSPM on all infrastructure up until the day the account or subscription is fully decommissioned to ensure that operations teams have continuous visibility.

Conclusion

Defending the cloud is likely to become more complex as adversaries evolve and increase their attempts to target cloud infrastructure as well as apps and data. However, with a comprehensive approach rooted in visibility, threat intelligence and threat detection, organizations can give themselves the best opportunity to leverage the cloud without sacrificing security.

CrowdStrike Products and Services

CrowdStrike Cloud Security

FALCON CLOUD WORKLOAD PROTECTION

Provides comprehensive breach protection across private, public, hybrid and multi-cloud environments, allowing customers to rapidly adopt and secure technology across any workload.

FALCON HORIZON™ | CLOUD SECURITY POSTURE MANAGEMENT

Streamlines cloud posture management across the application lifecycle for multi-cloud environments, enabling you to securely deploy applications in the cloud with greater speed and efficiency.

FALCON OVERWATCH™ | MANAGED CLOUD THREAT HUNTING

Partners you with a team of elite cybersecurity experts to hunt continuously within the Falcon® platform for faint signs of sophisticated intrusions, leaving attackers nowhere to hide.

FALCON COMPLETE™ | MANAGED DETECTION AND RESPONSE (MDR) FOR CLOUD WORKLOADS

Stops and eradicates cloud threats in minutes with 24/7 expert management, monitoring and surgical remediation, backed by the industry's strongest Breach Prevention Warranty.

CROWDSTRIKE SERVICES | CLOUD SECURITY ASSESSMENT

Leverages Falcon Horizon CSPM to provide actionable insights into ineffective cloud settings, cloud security misconfigurations and deviations from recommended cloud security architecture to help you prevent cloud breaches.

CROWDSTRIKE SERVICES | CLOUD COMPROMISE ASSESSMENT

Identifies any ongoing or past attacker activity in your cloud environment and removes any active threats from your network.

CROWDSTRIKE SERVICES | INCIDENT RESPONSE FOR CLOUD

Handles critical security incidents and conducts comprehensive forensic analysis to resolve immediate cyberattacks in your cloud environment.

CROWDSTRIKE SERVICES | CLOUD PENETRATION TESTING

Simulates real-world attacks on different components of your cloud infrastructure and cloud platforms to test the detection and response capabilities of your people, processes and technology, and identify vulnerabilities in your cloud environment.

CROWDSTRIKE SERVICES | RED TEAM/BLUE TEAM EXERCISE FOR CLOUD

Provides expert guidance to prepare your cybersecurity team as CrowdStrike's red team attacks and its blue team helps your team defend against a targeted attack on your cloud environment.

CrowdStrike Threat Intelligence

FALCON INTELLIGENCE | AUTOMATED THREAT INTELLIGENCE

Enriches the events and incidents detected by the CrowdStrike Falcon® platform, automating intelligence so security operations teams can make better, faster decisions.

FALCON INTELLIGENCE PREMIUM™ | CYBER THREAT INTELLIGENCE

Delivers world-class intelligence reporting, technical analysis, malware analysis and threat hunting capabilities, enabling organizations to build cyber resiliency and more effectively defend against sophisticated nation-state, eCrime and hacktivist adversaries.

FALCON INTELLIGENCE RECON™ | DIGITAL RISK MONITORING

Monitors potentially malicious activity across the open, deep and dark web, enabling you to better protect your brand, employees and sensitive data.

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
We stop breaches.

Learn more
https://www.crowdstrike.com/products/cloud-security/

Follow us:
Blog | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

Schedule a demo:
Falcon Cloud Workload Protection

Falcon Horizon CSPM

CrowdStrike Container Security