CrowdStrike Threat Briefing

CROWDSTRIKE

PROTECTORS OF THE CLOUD

TABLE OF CONTENTS

PROTECTORS OF THE CLOUD: CLOUD VULNERABILITY EXPLOITATION

Cloud adoption has become critical to digital transformation, providing businesses with the agility and scalability they need to better serve customers. However, cloud adoption has also expanded the attack surface these businesses must monitor and protect.

Security teams struggle to keep up because of poor visibility and fragmented approaches to security management and threat detection, and because the attack surface expands with every workload deployed to the cloud. Protecting the cloud therefore requires a different security model from the one protecting your on-premises environment.

COMMON CLOUD VULNERABILITIES

To defend cloud environments, security teams must protect against common cloud vulnerabilities, including these:

- **Misconfigurations**. Misconfigurations are often caused by a lack of general knowledge or review and can include everything from users having unnecessary access to resources, to containers left exposed to the public.
- **Insecure APIs**. APIs are increasingly used in modern software development and in microservices, applications and website backends. They must handle a variety of requests. Unfortunately, some of these requests come from threat actors and target vulnerabilities and misconfigurations.
- **Lack of multifactor authentication (MFA)**. MFA requires a user to present at least two forms of identification for validation to access an account or data. User passwords are vulnerable to theft, making the lack of MFA a potentially critical vulnerability.
- **Lack of control over end-user actions**. Exercising control of who can access cloud resources and monitoring user activity are critical components of protecting the cloud. Without them, organizations risk a situation where malicious activity goes undetected.
- **Weak spots in software supply chain security**. Cloud-native applications often use open-source software. As threat actors target this software, organizations must take action to mitigate the risk of vulnerabilities and misconfigurations being introduced.

CLOUD VULNERABILITY EXPLOITATION IN ACTION

Researchers at CrowdStrike have their eyes on the ever-evolving threat landscape today's organizations are facing. As enterprises embrace new cloud architectures in search of better scalability, efficiency and security, threat actors have taken notice and are targeting cloud infrastructure.

Malicious actors tend to opportunistically exploit known remote code execution (RCE) vulnerabilities in server software, typically scanning for vulnerable servers without focusing on particular industry sectors or geographic regions. After gaining initial access, actors may deploy a variety of tools.

The wider criminal exploitation of cloud services for initial access includes the exploitation of file transfer application vulnerabilities. Since January 2021, multiple companies have self-disclosed breaches related to such exploitation.

VMware has also been targeted by threat actors, including CVE-2021-21972 — a critical vulnerability impacting VMware's ESXi, vCenter Server and Cloud Foundation products. Exploiting this vulnerability provides a simple and reliable method that threat actors can use across multiple host-operating systems, attack vectors and intrusion stages. Multiple adversaries, particularly big game hunting (BGH) actors, have likely leveraged this vulnerability.

WHAT YOU CAN DO TO PROTECT YOUR CLOUD ENVIRONMENT

- **Enable runtime protection and obtain real-time visibility.** You can't protect what you can't see — even if you plan to decommission the infrastructure. Runtime protection and continuous visibility are central to securing your cloud infrastructure to prevent a breach. It remains critical to protect your containers, servers and 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.
- **Make it your mission to eliminate configuration errors**. The most common cause of cloud intrusions continues to be human errors and omissions introduced during common administrative activities. It's essential 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 subaccounts 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 default roles and network security groups that keep developers and operators from needing to build their own security profiles and accidentally doing it poorly.
- **Be proactive when it comes to securing APIs**. The proliferation of APIs poses a challenge for developers and security teams. However, by "shifting left" and integrating security into the CI/CD process, organizations can reduce risk. In addition, code injection attacks targeting vulnerable APIs can be prevented with a web application firewall configured to filter requests by source IP address and/or HTTP header info.
- **Work smarter not harder by leveraging a cloud security posture management (CSPM) solution**. Ensure your cloud account factory includes enabling detailed logging and a CSPM — like CrowdStrike Falcon Horizon™ — with alerting to responsible parties, including cloud operations and security operations center (SOC) teams. Actively seek out unmanaged cloud subscriptions, and when 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 decommissioning of the account or subscription to ensure that operations teams have continuous visibility.

- **Gain more control over user actions.** Organizations need to employ access controls, like the ones found in CrowdStrike cloud infrastructure and entitlement management (CIEM) solutions, to manage and secure cloud resources. These controls should be supported by visibility into cloud workloads and infrastructure. To protect cloud environments, organizations must be able to enforce security policies consistently across multiple cloud platforms.
- **Secure multi-cloud resources by establishing least-privilege access**. Excessive permissions increase the risk of attack. Users should only have the level of access they need to perform their jobs effectively. With the principle of least privilege guiding decisions about access rights, organizations can reduce the amount of potential damage that could be done if an account is compromised.

PROTECTORS OF THE CLOUD: CREDENTIAL THEFT

In cloud environments, identity is the new perimeter. Threat actors are well aware of this and target credentials to compromise cloud environments and steal enterprise data. Controlling access to cloud workloads and services is fundamental to cloud security, and organizations must prioritize the prevention of credential theft to secure access to cloud assets.

Gaining credentials allows attackers to impersonate the account owner and appear as someone who has legitimate access, such as an employee, contractor, service account or third-party supplier. Because the attacker looks like a legitimate user, this type of attack is challenging for defenses to detect. Threat actors can then use their access to expand their foothold in the targeted organization.

COMMON CAUSES OF CREDENTIAL THEFT

The most common causes of credential theft include:

- **Malware**. Malicious programs can infect users' devices and steal credentials. Malware can be installed on the machines of unsuspecting users via techniques such as drive-by downloads and social engineering.
- **Phishing**. These attacks often abuse trust in popular brands to trick victims into giving up their credentials. Typically, they will use an enticing email to lure the recipient into visiting a malicious website where they enter their credentials.
- **Weak passwords or password reuse**. Attackers take advantage of poor password security practices to gain access to systems, applications and data. Weak passwords are easier for attackers to crack, and reusing passwords increases the risk that a single stolen password could lead to a broader compromise.
- **Attacks on cloud services leading to lateral movement**. Attacks against the cloud environment can lead to threat actors gaining access to on-premises systems and resources. These attacks can leverage accounts with excessive permissions to broaden their reach inside the victim's IT infrastructure.
- **Man-in-the-middle (MitM) attacks**. These attacks occur when a threat actor is able to intercept and relay communications between two parties that believe they are communicating with each other. MitM attacks allow attackers to steal credentials and eavesdrop on that communication.

CREDENTIAL THEFT IN ACTION

In an age of remote workers and cloud computing, credential theft has emerged as a common tactic for initial entry as well as a means to pivot around a compromised network after threat actors are already inside.

Threat actors routinely host fake authentication pages to harvest legitimate authentication credentials for cloud services such as Microsoft Office 365 (O365), Okta or webmail accounts. They 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 (a Turkey-affiliated threat actor) targeting victim data stored within a large cloud service provider (CSP) environment. The adversary compromised the environment via a stolen credential that allowed the operator to interact with the CSP using the command line. Employing this technique, the adversary altered security group settings to allow direct SSH access from malicious infrastructure.

WHAT YOU CAN DO TO PROTECT YOUR CLOUD ENVIRONMENT

- **Enable and require multifactor authentication (MFA)**. MFA requires a user to present two or more pieces of evidence to verify and authenticate their identity before they are granted the access they are requesting. MFA techniques raise the barrier to entry for attackers by preventing them from compromising applications and systems with a single password.
- **Conduct security awareness training against phishing.** Knowledge is power. By training users to recognize phishing attacks and social engineering schemes, organizations can turn their employees into a critical layer of defense for their IT environment.
- **Maintain good password hygiene**. Strong passwords are more difficult for attackers to crack. These passwords should be rotated regularly and should not be shared between users. Additionally, users should refrain from using the same password across multiple sites or services.
- **Use a cloud infrastructure entitlement management (CIEM) solution for identity inventory, log monitoring and least-privilege enforcement**. CIEM solutions help enterprises manage entitlements across all of their cloud infrastructure resources. The primary goal of tools like CrowdStrike Falcon Horizon™ cloud security posture management, which includes CIEM capabilities, is to mitigate the risk that comes from the unintentional and unchecked granting of excessive permissions to cloud resources. By removing unnecessary privileges, organizations can reduce the threat posed by a compromised account.
- **Properly scope permissions across users and machines**. It is critical for organizations to understand the privileged access that users and devices have. Accounts that can be used to access sensitive systems, data and applications must be tightly managed to meet the security and compliance mandates of the modern enterprise.

PROTECTORS OF THE CLOUD: ABUSE OF CLOUD SERVICE PROVIDERS

For many enterprises, cloud services have become a foundational element of IT operations as they pursue multi-cloud and hybrid cloud approaches in search of greater efficiency and agility. Threat actors continue to look to the cloud as well — but with the aim to abuse the capabilities of cloud service providers to compromise enterprise environments.

While enterprises use cloud-based services to support collaboration and business processes, these same services are increasingly abused by malicious actors for computer network operations (CNO). This trend will likely continue in the foreseeable future as more businesses seek hybrid work environments.

COMMON CLOUD ATTACK VECTORS

Common cloud attack vectors used by eCrime and targeted intrusion adversaries include:

- **Distributed denial-of-service (DDoS) attacks**. A DDoS attack is caused by an attacker overloading a web server, system or network with traffic, making it difficult or impossible for legitimate users to access IT resources. Attackers are known to abuse hijacked cloud accounts or free user trials for DDoS attacks.
- **Phishing attempts**. Cybercriminals use phishing to steal user credentials for cloud services to take over and use these accounts in their malicious schemes.
- **Email spam**. Spammers use cloud infrastructure to blast out their messages. These attackers take advantage of cloud computing services by leveraging their reliability and bandwidth to aid in their operations.
- **Cryptojacking**. In cryptojacking, attackers use a victim's computing power to mine for cryptocurrency. If an attacker can gain access to an organization's cloud resources, they can harness those assets and use them for mining operations.
- **Brute-force attack**. Brute-force attacks are a method of compromising user accounts in which a threat actor uses trial and error to guess a user's password or login credentials. Common forms include dictionary attacks and credential stuffing.
- **Hosting of malicious content**. Once cloud services have been compromised, they can be used to host malicious content including everything from phishing pages to spam bots. This tactic has the added benefit of making bad content harder to block due to threat actors using trusted brands, allowing them to hide malicious content alongside legitimate content.
- **Malicious insiders**. Internal threat actors pose a risk, as they can use their access to cloud resources to leverage those assets to launch attacks.

ABUSE OF CLOUD SERVICE PROVIDERS IN ACTION

CrowdStrike threat researchers monitor the cloud closely for malicious activity, and attackers continue to adopt tactics to improve their stealth and effectiveness. For cybercriminals, avoiding detection is made easier by abusing trusted relationships between users, providers and networks.

Adversaries leverage 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 its customer networks, thereby creating multiple opportunities for vertical propagation to many other networks. This technique was used by the threat actor COZY BEAR (a Russia-affiliated threat actor) throughout 2020, with evidence of continued intrusion in MSP networks continuing into 2021.

WHAT YOU CAN DO TO PROTECT YOUR CLOUD ENVIRONMENT

As with on-premises environments, security teams with insight into attackers' tools and tactics have the best chance to identify and stop threats more quickly. Security teams should keep the following firmly in mind to remain grounded in best practices.

- **Monitor identities and how they are being used.** Protecting cloud environments requires focusing on identity, including securing user accounts with strong passwords and multifactor authentication (MFA) and monitoring them for suspicious activity.
- **Identify the most critical assets and monitor them looking for outbound communications and exfiltration.** Organizations need visibility into cloud environments to stay on the lookout for signs of compromise. Outbound connections should be scrutinized to pinpoint unusual communications.
- **Educate the security operations center (SOC) on cloud security.** Many SOC analysts and incident responders do not have expertise in cloud technologies. Invest in training as it is crucial that the SOC team understands cloud tools and infrastructure.
- **Develop incident response plans aligned with the shared responsibility model**. Organizations should have detailed playbooks outlining both how and who should respond to and remediate threats. Security orchestration, automation and response (SOAR) technologies are critical, enabling enterprises to collect threat-related data and automate response.
- **Focus cloud threat hunting on indicators of attack (IOAs).** As always, knowledge is power. Enterprises must leverage the latest threat intelligence to keep pace with attackers and improve their ability to detect and respond to the risks they face. **CrowdStrike Cloud Security** provides advanced cloud-native security for any cloud, powered by holistic intelligence and end-to-end protection from the host to the cloud, delivering greater visibility, compliance and the industry's fastest threat detection and response to outsmart the adversary.

PROTECTORS OF THE CLOUD: MALWARE HOSTING

Enterprise IT leaders are not the only ones who understand the potential of cloud hosting. It not only offers the potential benefits of increased uptime and scalability to legitimate businesses, it also offers the same capabilities to cybercriminals and represents another aspect of the growing threat landscape enterprises must contend with.

Attackers often use underground hosting services to avoid detection, but it is not uncommon for them to turn to legitimate cloud hosting services to serve their needs. Cybercriminals can use a free or compromised hosting account to host malware while using the hosting provider's reputation as a cover to make blocking malicious activity more difficult.

COMMON CLOUD ATTACK VECTORS

Some examples of the attacks that threat actors use to target cloud systems are:

- **Distributed denial of service (DDoS)**. DDoS attacks overwhelm a target with traffic to disrupt its operations.
- **Hypervisor denial of service (DoS)**. This type of DoS attack targets the hypervisor. If successful, it can affect all of the virtual machines (VMs) a host is running.
- **Hypercall attack**. A hypercall attack enables a threat actor to target virtual machines via the hypercall handler and could lead to the execution of malicious code with the privileges of the virtual machine manager.
- **Exploiting live migrations**. Live migrations can be compromised in a number of ways, such as making alterations that leave the systems being migrated vulnerable to attack and creating multiple fake migrations to launch a DoS attack.
- **Hyperjacking**. These attacks are aimed at taking control of the hypervisor. This attack will allow a threat actor to modify VMs and take other malicious actions if successful. These security threats help to create a challenging threat landscape that organizations must defend against. For attackers, staying under the radar is a critical priority.

In addition to these attacks, threat actors have also increased their use of Linux malware to target cloud environments, particularly ransomware.

MALWARE HOSTING IN ACTION

These security threats help create a challenging threat landscape that organizations must defend against. For attackers, staying under the radar is a top priority.

Both eCrime and targeted intrusion adversaries extensively leverage legitimate cloud services to deliver malware; targeted actors also use these services for command and control (C2). 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.

WHAT YOU CAN DO TO PROTECT YOUR CLOUD ENVIRONMENT

- **Educate and train employees**. Security awareness training allows employees to identify social engineering tactics. Additionally, security teams must understand cloud technologies and the vulnerabilities, risks and threats that can lead to compromises.
- **Strengthen access control**. Protecting access to cloud resources requires visibility into the entire cloud environment. Organizations should use identity and access management (IAM) services native to their cloud platform to implement role-based, fine-grained access control to cloud resources.
- **Practice user or network segmentation to control the spread of viruses**. Start with basic segmentation of cloud workloads between different virtual networks and only allow required communication between them. Additionally, incoming traffic to your applications should be restricted using network or application layer firewalls.
- **Implement cloud-native application protection platform (CNAPP) capabilities to detect and respond**. A CNAPP is an all-in-one cloud-native software platform that simplifies monitoring, detecting and acting on potential cloud security threats and vulnerabilities. A CNAPP combines multiple tools and capabilities into a single software solution to minimize complexity and facilitate **DevOps** and DevSecOps team operations while offering end-to-end cloud and application security through the entirety of the continuous integration and continuous delivery/deployment (CI/CD) application lifecycle. The CrowdStrike Falcon® platform offers **powerful CNAPP capabilities** to secure containers and help developers rapidly identify and remediate cloud vulnerabilities.
- **Leverage cloud threat hunting**. Threat hunting is the practice of proactively searching for cyber threats lurking undetected in your network. Cloud threat hunting digs deep to find malicious actors in your environment that have slipped past your initial cloud security defenses.

PROTECTORS OF THE CLOUD: EXPLOITATION OF MISCONFIGURED IMAGE CONTAINERS

Organizations are using containers to achieve new levels of efficiency and scalability in the cloud. However, this has increased the complexity of the attack surface they need to protect and has placed containers in the crosshairs of adversaries.

Container security starts with the container image. Developers sometimes use base images from an external registry to build their images. Unfortunately, these images can contain malware or vulnerable libraries. This reality makes it critical for organizations to prioritize image assessment as part of their cloud security strategy.

COMMON TYPES OF CONTAINER IMAGE MISCONFIGURATIONS

Here are some typical security issues involving container images:

- **Using a root user account in containers**. Running a container with root privileges increases the danger from attackers looking to compromise the host machine.
- **Using outdated, vulnerable, backdoored images**. Attackers will take advantage of vulnerable or compromised images, so image scanning is a vital defense.
- **Unwanted users being part of a Docker group**. If a user is part of a Docker group, it is possible to escalate their privileges to root access. This is a prime position for a threat actor.
- **Use of a privileged flag**. Running a container with a privileged flag gives users access to the host's resources, which an attacker can abuse if the container is compromised.
- **Mounting sensitive host files or directories onto the container**. Docker enables users to mount the host machine's files and directories onto containers, which can increase the attack surface if the files are sensitive.

These and other misconfigurations involving Docker or Kubernetes represent a significant risk to organizations, and identifying them is a critical component of your cloud security strategy.

MISCONFIGURED IMAGE CONTAINERS IN ACTION

Reducing risk requires knowing the threats your organization faces. In cloud environments, that includes understanding how containers are being targeted.

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. The CrowdStrike Falcon OverWatch™ threat hunting team has observed increasing adversary interest in Kubernetes clusters operating within corporate environments. The Kubernetes framework is a complex system comprising several 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.

WHAT YOU CAN DO TO PROTECT YOUR CLOUD ENVIRONMENT

- **Reduce attack surfaces in container images (like removing debugging tools)**. To reduce the attack surface, enterprises need to focus on detecting vulnerabilities, malware, compliance violations and more, from build to runtime.
- **Perform vulnerability scanning as a part of container creation and staging processes to the container registry**. Vulnerability scanning enables enterprises to catch security issues before they can be exploited by attackers.
- **Avoid using publicly shared container images**. These images may be outdated or vulnerable, potentially introducing additional risk into your cloud environment.
- **Limit container privileges**. Follow the principle of least privilege to ensure containers do not have excessive permissions.

Keeping cloud infrastructure safe requires security coverage throughout the CI/CD pipeline. By shifting security left and proactively assessing containers, **CrowdStrike cloud security** can help your organization reduce risk by identifying any vulnerabilities, embedded malware, stored secrets or other security issues before deployment.

Learn more about the cloud security threat landscape and how to protect your cloud environments in this CrowdStrike eBook.

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: **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/**