IDENTITY AND ACCESS MANAGEMENT:

THE FIRST LINE OF DEFENSE

VOL. 9

CLOUD THREAT REPORT

PRISMA® | UNIT 42™

Table of Contents

Foreword

Without effective identity and access management (IAM) policies in place, an organization can never expect to be secure in the cloud due to its very nature: dispersed, rapidly evolving, and dynamically fluctuating within an organization.

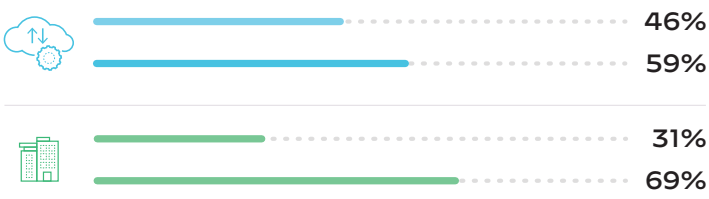


Figure 1: Percent change in cloud workload volumes since 2020

With the pandemic-induced transition to cloud platforms over the past several years, malicious actors have had an easier time than ever following their targets into the cloud. According to The 2022 State of Cloud Native Security Report, "throughout the pandemic, there were significant expansions of cloud workloads overall, jumping to an average of 59% of workloads hosted in the cloud, up from an average of 46% in 2020. In addition, 69% of organizations host more than half of their workloads in the cloud, up from just 31%...in 2020." Further, identity and access management is one of the most critical, complex, and error-prone services in the cloud. While CSP has created numerous guardrails to check and verify IAM configurations, users may still inadvertently introduce insecure configurations to IAM policies. Keenly aware of this, attackers leverage misconfigured cloud resources and quickly zero in on their targets.

If you follow Unit 42 cloud threat research closely, you may remember that it was not all that long ago that we produced a report on the importance of IAM when building a cloud security strategy. **IAM has once again taken center stage in the world of cloud security**—but this time to a heightened degree as cloud adoption has spiked with no plans to return to pre-pandemic usage.

As you will find, this report is structured around the "who, what, and how" of IAM and threat actors in the cloud. This triad of questioning is paramount to the investigation and understanding of how identity is used and targeted within cloud environments. **By asking the questions, "Who is attacking cloud infrastructure?" "How are they doing this?" and "What are they targeting?" security professionals can learn to effectively build, monitor, and protect their cloud infrastructure**.

As our cloud threat researchers explored these questions for themselves, they not only uncovered serious findings surrounding overly permissive IAM policies (for example, nearly 99% of IAM policies are overly permissive), they were also able to compile an **industry-first Cloud Threat Actor Index which is designed as a living set of dossiers on who is targeting cloud infrastructure**.

Read on to garner a deep understanding of the steps used by cloud threat actors to target your cloud infrastructure and how you can implement actionable guidance to prevent them from infiltrating your organization.

John Morello

Vice President, Prisma Cloud

Palo Alto Networks

Executive Summary

Misconfigurations continue to be at the center of almost every known cloud security incident. However, if you look closely under the hood, many times it is the result of a few poorly written policies around identity and access management (IAM). IAM is the most critical and complex component that governs the authentication and authorization of every resource in a cloud environment. Put simply: IAM is the first line of defense in most cloud environments. In this report, Unit 42 researchers analyzed 680,000+ identities across 18,000 cloud accounts and over 200 different organizations to understand their configurations and usage patterns. The research reveals that nearly all cloud identities are overly permissive, and many grant permissions that are never used. Additionally, 53% of cloud accounts allow weak password usage and 44% allow password reuse. Unfortunately, malicious adversaries appear to know this as well. Unit 42 researchers have created an industry-first Cloud Threat Actor (CTA) Index, which charts the operations performed by actor groups that target cloud infrastructure. Importantly, researchers have also found that each of the CTA groups target cloud IAM credentials. Overall, the findings indicate that when it comes to IAM in the cloud, organizations struggle to put good governance in place, opening the door for malicious actors to have wider access to cloud environments.

IAM is the first line of defense in most cloud environments.

Cloud Identities Are Too Permissive

Unit 42 researchers observed a high percentage of **overly permissive identities** in environments across all cloud service providers (CSPs). There is a big gap between reality and the principle of least privilege. A staggering 99% of the cloud users, roles, services, and resources were granted excessive permissions which were left unused. If overly permissive identities are compromised, adversaries may leverage these unused permissions to move laterally or vertically and expand the attack radius. Removing these permissions can significantly reduce the risk each cloud resource exposes and minimize the attack surface of the entire cloud environment. Best of all, right-sizing permission policies can be achieved with zero cost and performance hit.

We consider a cloud identity overly permissive if it is granted permissions that are unused in the past 60 days. An identity can be a human user or a non-human user such as a service account.

Customize Cloud Provider IAM Policies

Each cloud service provider offers a set of built-in permission policies that can be applied quickly to an identity that needs access to certain cloud resources. However, the one-size-fits-all solutions also tend to be too general and grant too many unnecessary permissions. Our research showed that there are two times more unused or excessive permissions within built-in CSP policies than in customer-created policies. The principle of least privilege discourages administrator access; however, our research shows that administrator policies are among the top three most granted managed policies.

Misconfigured IAM Opens the Door for Cloud Threat Actors

Most known cloud security incidents start with a misconfigured IAM or leaked credential (e.g., publicly exposed storage buckets and hard-coded credentials). Our research showed that 65% of the known cloud security incidents were due to misconfigurations. These are also the attack vectors that adversaries constantly seek to exploit. All the cloud threat actors (CTAs) that we identified attempted to harvest cloud credentials when compromising a server, container, or laptop. **A leaked credential with excessive permissions could give attackers a key to the kingdom**. Researchers have identified a CTA using CSP credentials in the past, showcasing that they are targeting cloud workloads beyond just compromised instances.

Cloud Threat Actors Leverage Unique Escalation Techniques

Of the five cloud threat actors listed within Unit 42's Cloud Threat Actor Index, three of the CTAs have performed container-specific operations including permission discovery (user and group levels) and container resource discovery operations. Two of the CTAs have also been documented as performing container escape operations. Additionally, all five of the CTAs have collected cloud service platform or container platform credentials as part of their standard operating procedures. With the collection of CSP credentials, CTAs would be able to move laterally to the cloud service platform itself, thus allowing the CTA to evade siloed container or cloud virtual resource security monitoring tools. Only a cloud native application protection platform (CNAPP) with proper configurations would be capable of monitoring and remediating these CTA operations.

Who's Attacking the Cloud?

What Is a Cloud Threat Actor?

Unit 42 has created an industry-first Cloud Threat Actor (CTA) Index, which has been built to assist security operation teams, threat hunters, researchers and intelligence professionals in tracking threat actors who target cloud infrastructure. The data contained within the CTA index follows the MITRE ATT&CK® cloud and container matrices, giving security professionals a common framework around which to communicate and discuss the tactics, techniques, and procedures (TTPs) employed by CTAs. The CTA index will also employ the Unit 42 ATOM service to provide security professionals with all of the known indicators of compromise (IOCs) used by the CTAs packaged within the industry standard STIX/TAXII format. This format allows for easy integration with cloud security tools and platforms.

NIST 800-150 defines a Threat Actor as "An individual or a group posing a threat."[1] Threat actors compromise systems and devices located within an organization's physical location. However, organizations now host that same infrastructure within cloud service providers (CSPs) and cloud native container platforms. Not only does this alter how organizations integrate and use this infrastructure but it also alters how threat actors will attempt to compromise this infrastructure. The move to cloud can make securing virtualized infrastructure difficult as each cloud instance has the capability of direct public access. As a result, groups that target these cloud infrastructures have developed specialized tactics, techniques, and procedures (TTPs). As such, Unit 42 observes it is vitally important to classify this new type of threat actor as a cloud threat actor.

Unit 42 researchers have defined a CTA as, "An individual or group posing a threat to organizations through directed and sustained access to their cloud platform resources, services, or its embedded metadata." Researchers have found that while cloud threat actors follow the overall same kill chain operation workflow as traditional threat actors, such as performing reconnaissance followed by initial compromise, persistence, lateral movement, privilege escalation, evasion, and exfiltration, **cloud threat actors have begun to employ a fundamentally different set of TTPs**. For instance, these different TTPs can include the ability to perform both lateral movement and privilege escalation operations simultaneously, by leveraging stolen cloud service provider access and secret keys taken from compromised container or VM accessible metadata, or local credential files.

Unit 42 researchers have defined a CTA as, "An individual or group posing a threat to organizations through directed and sustained access to their cloud platform resources, services, or its embedded metadata."

With the knowledge that 99% of IAM roles, groups, and accounts contain privileges that exceed their intended purpose, coupled with the fact that the vast majority of scraped access and secret keys will be overly permissive, CTAs with overly permissive access can directly modify, create, or delete cloud environment resources.

1. "Guide to Cyber Threat Information Sharing," *NIST Special Publication 800-150*, National Institute of Standards and Technology, October 2016, https://csrc.nist.gov/publications/detail/sp/800-150/final.

Cloud Threat Actor Capabilities

Cloud threat actors have increased in maturity and sophistication within recent years. They have elevated their technical capabilities from simply accessing exposed or misconfigured cloud storage containers or compromising exposed and vulnerable cloud-based applications like Redis, WebLogic, and ThinkPHP VMs and containers. Cloud threat actors now utilize near-zero-day exploits like Log4j to elicit sensitive cloud platform metadata, like CSP access and secret keys from compromised cloud resources. In the following examples, we will walk through two unique cloud targeting operations performed by CTAs which highlight the evolving sophistication these groups pose against cloud infrastructure.

TeamTNT Targeting Cloud Platforms and Cloud Native Applications

TeamTNT has been a highly publicized CTA since at least August 17, 2020, with the discovery of the "first crypto-mining worm to steal CSP credentials." For their most recent cloud enumeration operations, they actively targeted cloud platform services and resources. On November 30, 2021, HildeGard announced their intention to retire their offensive cloud operations; however, they were still actively posting and retweeting comments as late as January 23, 2022, with the majority of their later tweets centered around German politics. During the 28 months of known active offensive operations, TeamTNT operations grew from scraping CSP credentials from a single compromised compute instance to:

- Maintaining a Docker cryptojacking worm.
- Establishment of a robust IRC botnet infrastructure used for command and control (C2).
- The integration of memory scraping via mimipy and mimipeguins.
- The enumeration of cloud services and resources using stolen credentials from compromised cloud instances.

TeamTNT's growing operations culminated in the creation of the Chimaera repository, which contained a tracking feature that documented the total number of compromised Docker, Kubernetes, and Weave Scope instances. The highest documented number of compromised instances stood at 5,104 on September 8, 2021. Figure 2 shows how the TeamTNT actors scraped CSP and application credentials from a compromised cloud instance. These credentials could then be used to access cloud resources.

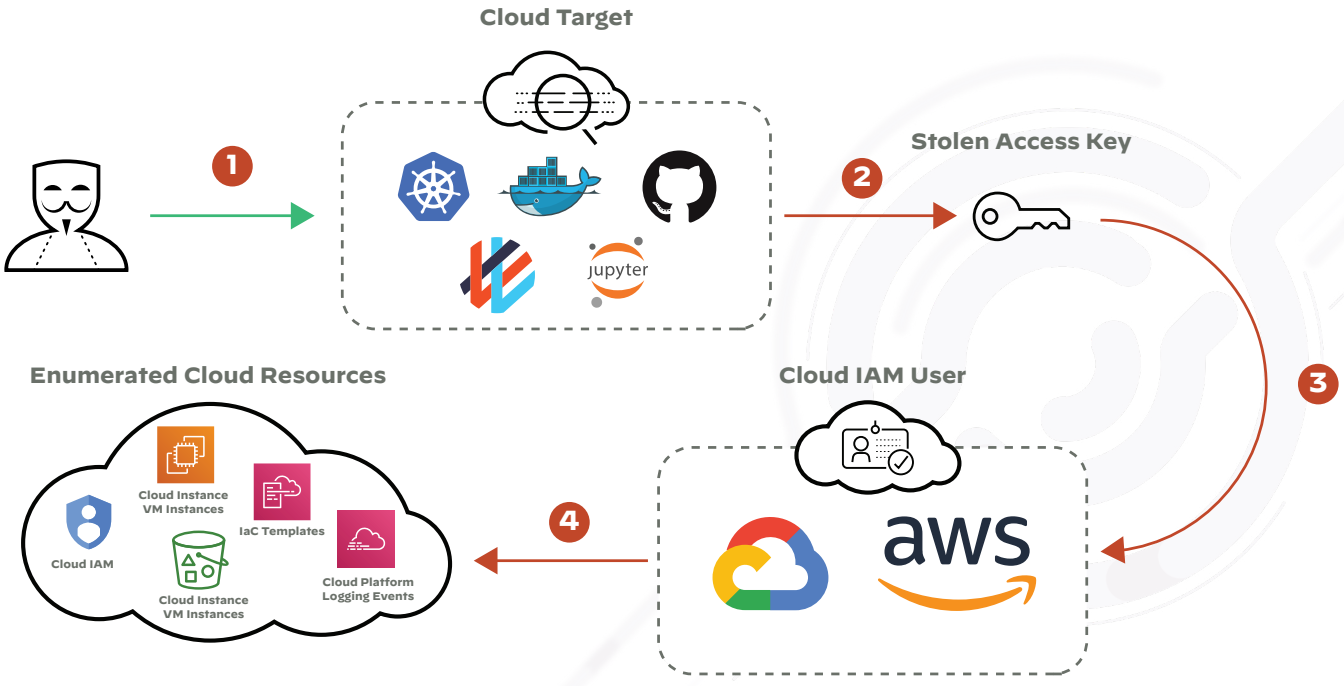


Figure 2: TeamTNT operations to scrape cloud credentials

While the HildeGard account was heavily active on Twitter, the actor continually taunted researchers and mocked nearly every report which referenced TeamTNT operations. Additionally, other CTA groups took notice of TeamTNT's success and actively copied and mimicked TeamTNT operational TTPs by modifying TeamTNT initialization scripts and even co-compromising a TeamTNT C2 host in order to better mimic their operations. The successful advancements of TeamTNT operations highlight the widening and deepening nature of the cloud threat landscape which must be addressed by both cloud security operations teams as well as cloud security products' alerting and detection methodology.

CTA Using Log4j to Target CSP Credentials

The exploitation of novel attack vectors has long been a reliable source for new threats. However, potential CTA usage of the recent Log4j vulnerability is particularly noteworthy. On December 9, 2021, a remote code execution (RCE) vulnerability in Apache Log4j 2 was identified being exploited in the wild. Public proof of concept (PoC) code was released and subsequent investigation revealed that the exploitation was effortless to perform. Reports surfaced pointing to the open source Go Language tool interactsh, a tool designed to detect vulnerabilities that cause external interactions, having experienced a high volume of requests to build detection tools for the Log4j vulnerability. Many of these requests were the direct result of malicious actors attempting to locate vulnerable computer systems.

As early as December 10, 2021, an unknown CTA group was reported to have integrated the Log4j vulnerability into their arsenal. The usage of the Log4j vulnerability also allowed the operators to harness the detection evasion capabilities of the vulnerability, which make the detection of these attacks much more difficult. This usage of defense evasion and discovery techniques also indicates CTAs are incorporating 1-day exploitation TTPs with those of lateral movement and privilege escalation techniques, allowing the CTA group to leverage cloud instances to a much greater extent, and signals the direct targeting of cloud IAM credentials being incorporated within the CTA's operations.

Figure 3 highlights the exploitation of Log4j—step one. The collection of the identified access keys (step two) is then followed by enumerating the cloud services allowed to the IAM policy assigned to the exposed access key (step three).

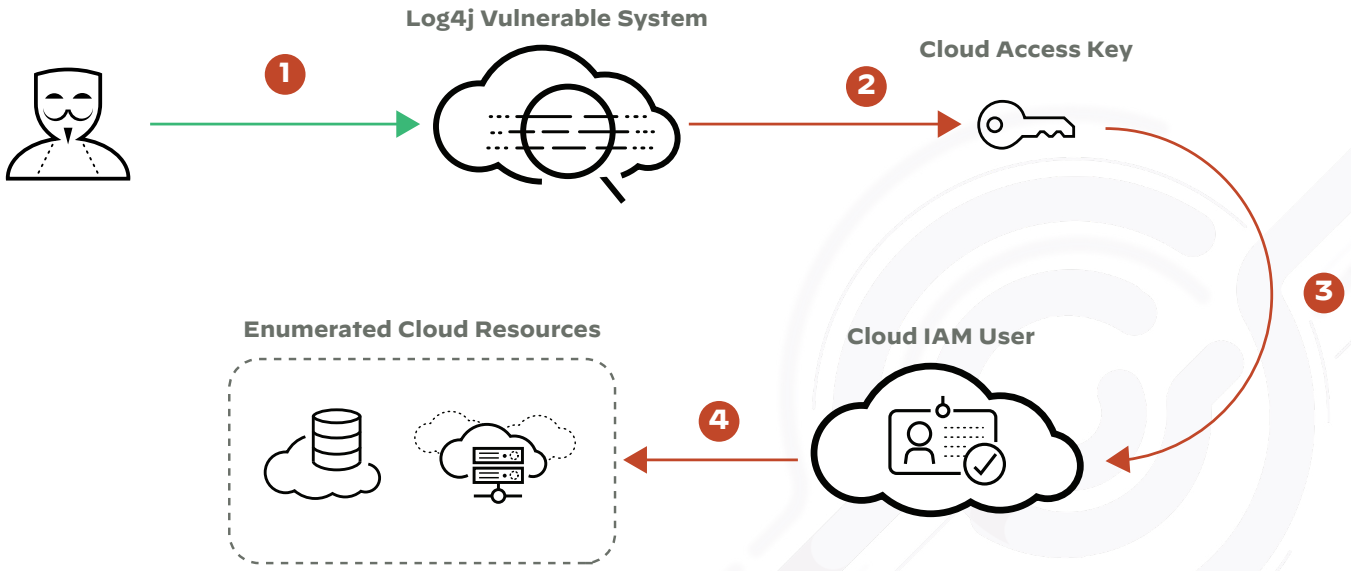


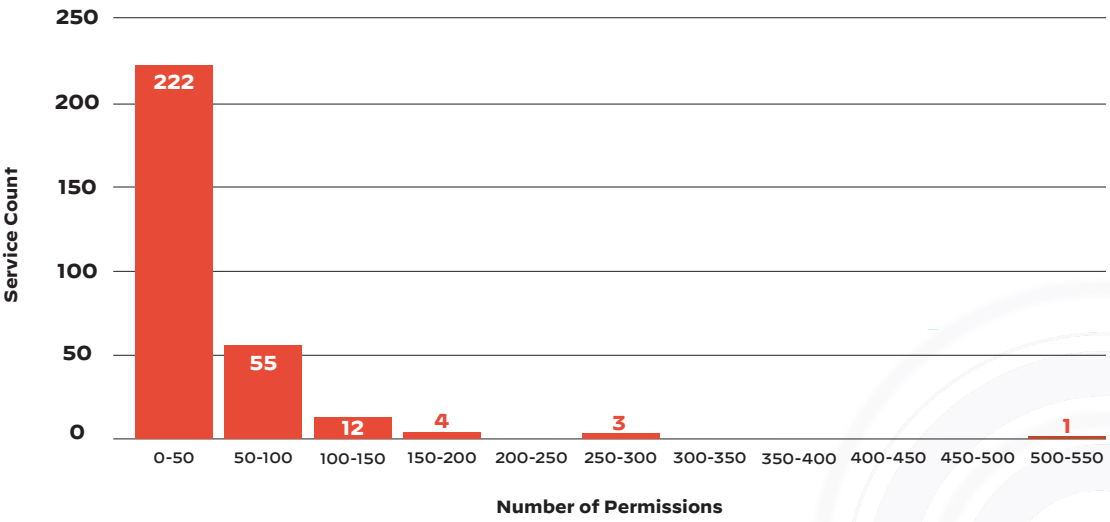
Figure 3: TeamTNT operations to scrape cloud credentials

The Role of IAM in CTA Operations

The active collection and enumeration of cloud resources using stolen CSP access and secret keys presents a risk to the identity-based resources of cloud platforms. Misconfigurations within the identity user, role, or group policies within a cloud platform can significantly increase the threat landscape of an organization's cloud architecture. Due to the active collection and direct targeting of a cloud service platform's access and secret keys as performed by both TeamTNT and Kinsing, as well as other groups yet unknown, the question has to be why. **The following three use cases present avenues as to how the targeting of CSP access and secret keys by CTAs could have a devastating effect upon an organization**.

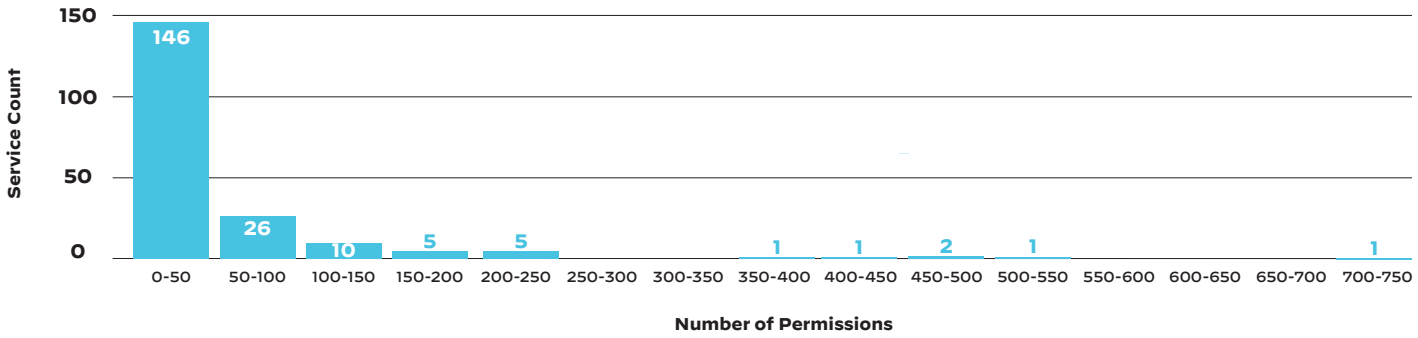
Identity: The Gateway to Your Cloud Infrastructure

Cloud service providers offer granular control of how each cloud service or resource can be accessed. The number of actions available for each service ranges from below 10 to above 500. On average, each cloud service has 50 actions that can be granted selectively to an identity. As granular as the cloud access control can be, no one can fully grasp all the actions in every cloud service. In a modern cloud native environment with hundreds or thousands of workloads, every machine (non-human) identity associated with the workloads poses a risk to the cloud infrastructure. With the adoption of hybrid and multicloud infrastructure, the number of credentials needed for different services grows significantly. The expanded security boundary makes identity access control more difficult, and also more critical.



Note: The majority of AWS services have 0-50 permissions that can be granted selectively

Figure 4: AWS services categorized by the number of their available permissions



Note: The majority of Azure services have 0-50 permissions that can be granted selectively

Figure 5: Azure services categorized by the number of their available permissions

Evidence-Based Findings

99% of cloud identities are overly permissive

We consider a cloud identity overly permissive if it is granted permissions that are unused in the past 60 days. Out of the 680,000 cloud users, roles, and service accounts we studied, only 1% of the identities are granted least-privileged permissions (not overly permissive).

62% of the organizations have cloud resources publicly exposed

A publicly exposed cloud resource allows anyone on the internet to access it without authentication. IAM policies attached to cloud resources such as buckets and functions determine who can access the resources and what actions can be performed on the resources. The stories of leaked data from cloud storage are often due to misconfigured IAM policies that allow everyone to access the data. There are legitimate use cases such as web content hosting that needs to be made public, but many resources are also unintentionally made public. Anyone who knows the endpoint, usually an URL, can access these exposed resources. Confidential data may be read from exposed buckets or databases, and malicious payloads may be inserted into exposed functions or queues.

CSP-managed policies are granted 2.5 times more permissions than customer-managed policies

Each cloud service provider offers a set of built-in permission policies that can be applied quickly to an identity that needs access to certain cloud resources. These managed policies help users quickly bootstrap a cloud native application without dealing with hundreds of the permissions required to run the workloads. Research done using Prisma Cloud's internal data shows that users across different CSPs use more CSP-managed policies than customer-managed policies. However, to accommodate the needs of different applications and users, the permissions in these policies need to be broad. A managed policy may grant one hundred permissions to a user even if the user only needs ten permissions. These excessive permissions pose unnecessary risks to the cloud environments. As Figure 6 shows, 43% of the IAM policies within AWS environments were built-in policies managed by AWS and 87% of the policies in Azure environments were built-in IAM roles managed by Azure. These results show that CSP-managed policies are the preferred choices for most cloud users.

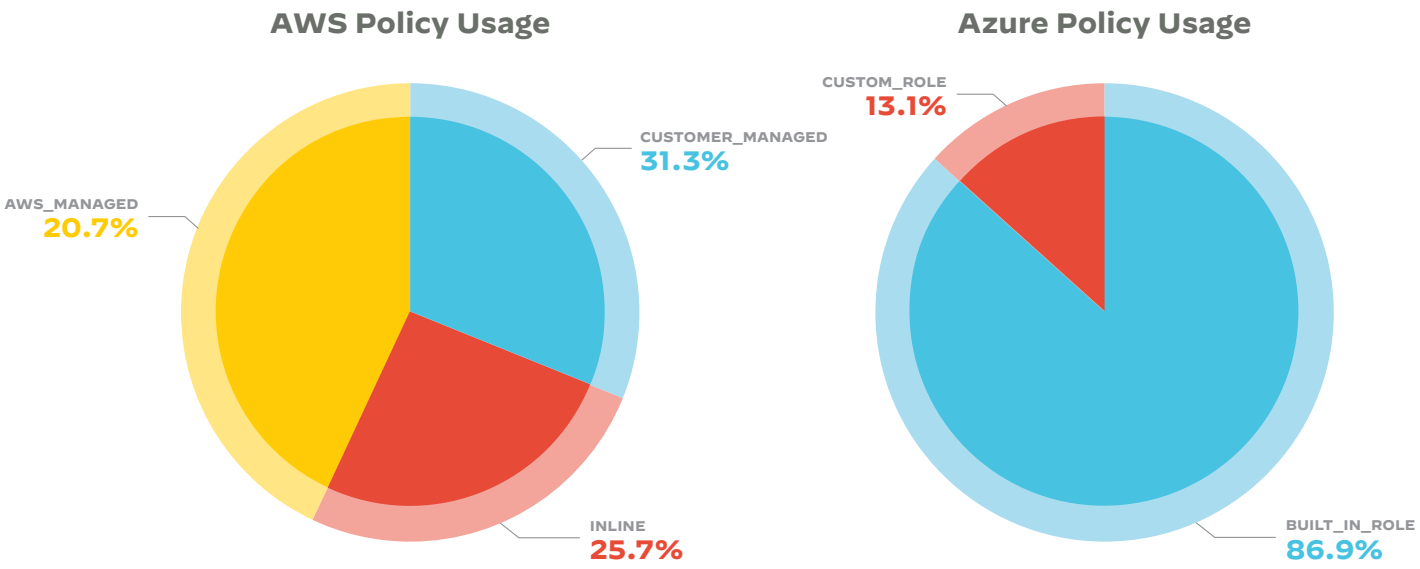
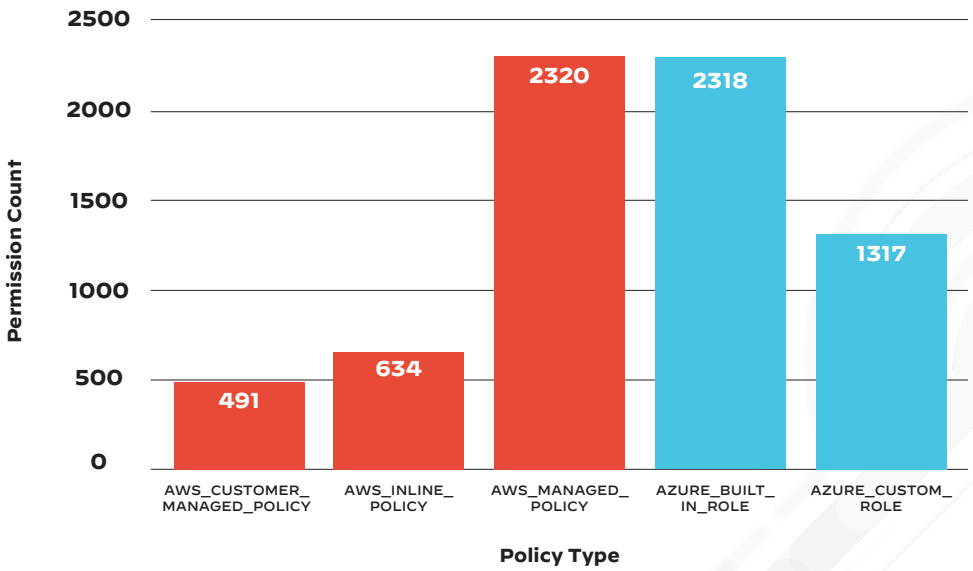


Figure 6: Breakdown of the granted policy types

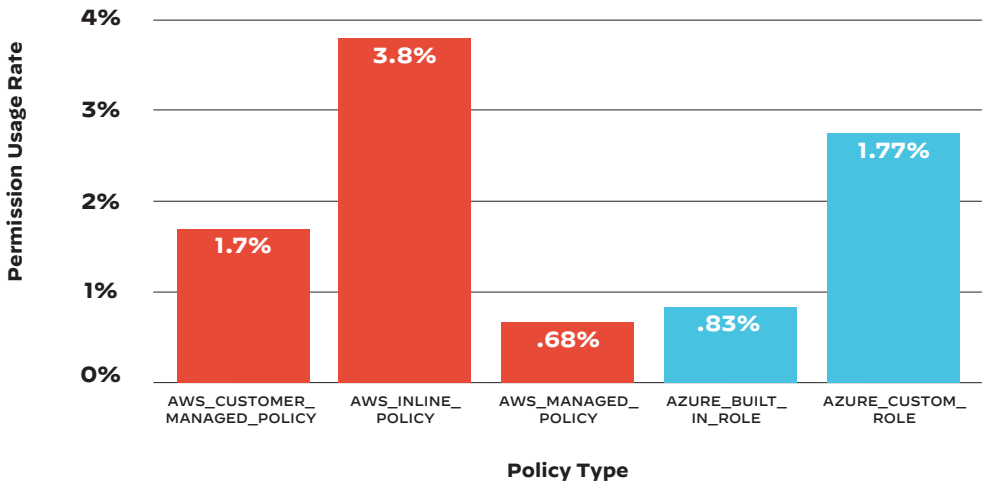
Figure 7 shows the average number of permissions granted by different types of permission policies. AWS_CUSTOMER_MANAGED_POLICY and AZURE_BUILT_IN_ROLE are CSP-managed policies by AWS and AZURE. AWS_CUSTOMER_MANAGED_POLICY, AWS_INLINE_POLICY, and AZURE_CUSTOM_ROLE are all policies created and managed by the users. Our data shows that on average, CSP-managed policies grant 2.5 times more permissions than customer-managed policies. Note that CSPs provide users options to reduce permissions on CSP-managed policies, but many users don't take full advantage of this opportunity to improve their security posture.



CSP managed policies (AWS_CUSTOMER_MANAGED_POLICY and AZURE_BUILT_IN_ROLE) grant 2.5 times more permissions than customer-managed policies

Figure 7: Average number of permissions granted by each policy type

Figure 8 shows the percentage of the granted permissions that were actually used in the past 60 days. We compare this percentage, or usage rate, between different policy types. Our data shows that the usage rate of the CSP-managed policies is 2.3 times lower than the usage rate of the customer-managed policies.



The percentage of the used permissions in CSP-managed policies are 2.3 times lower than customer-managed policies

Figure 8: Permission usage rate of each policy type

Table 1: Top 5 Most Frequently Used CSP-Managed Policies	
AWS	**Azure**
ReadOnlyAccess	Contributor
AWSLambdaVPCAccessExecutionRole	**Owner**
AdministratorAccess	Storage Blob Data Contributor
AWSSupportAccess	Billing Reader
AWSConfigRulesExecutionRole	Virtual Machine Contributor

As can be seen within table 1, AWS's AdministratorAccess policy and Azure's Owner role are two of the most used policies within each CSP. Unfortunately, both of these policies also grant full access to attached identities. Identities with AdministratorAccess or Owner's role are granted with all the permissions to every cloud service and resource. These policies should be granted with caution by the customer and only a minimal number of identities should have such privilege.

```
{
    "Statement": [
        {
            "Action": [
                "*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

AWS AdministratorAccess Policy

```
[
    {
        "actions": [
            "*"
        ],
        "dataActions": [],
        "notActions": [],
        "notDataActions": []
    }
]
```

Azure Owner Role

The majority (53%) of cloud accounts allow weak IAM passwords (<14 characters), and 44% of the accounts allow IAM password reuse

Weak passwords are vulnerable to brute-force or credential-stuffing attacks. Cloud administrators should enforce policies to prevent users from creating weak passwords or reusing old passwords. It is also best not to have permanent credentials such as passwords and access keys in cloud environments. If these credentials are accidentally leaked, adversaries can directly access the sensitive resources. It is more secure to use federated identities or single sign-on to reduce the number of usernames/passwords.

The Cloud Threat Actor Matrices

Researchers have curated a list of five cloud threat actors whose TTPs align with the direct targeting of cloud service platforms, allowing these cloud threat actors to bypass traditional security defenses. Defining the TTPs used by cloud threat actors will allow organizations to evaluate their strategic defenses against cloud-targeting threat actors and will provide the indicators necessary to build monitoring, detection, alerting and prevention mechanisms to protect their cloud native infrastructure.

Within the following tables you will find specific Cloud and Container TTPs employed by each CTA group.

Cloud specific TTPs	Cloud credential Usage/Discovery TTP	Container specific TTPs	Container Escape/Resource specific TTPs

TeamTNT

TeamTnT was the first cloud threat actor known to have actively targeted cloud credential files on compromised cloud workloads. Their operations include the enumeration of cloud platform services, lateral movement within Kubernetes clusters, establishment of IRC botnets, and the hijacking of compromised cloud workload resources in order to mine the Monero (XMR) cryptocurrency.

Key Takeaway: TeamTNT is considered to be the most sophisticated cloud threat actor in terms of cloud identity enumeration techniques.

Table 2: TeamTNT Cloud Threat Actor TTPs

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
T1078 - Valid Accounts	T1610 - Deploy Container	T1078 - Valid Accounts	T1078 - Valid Accounts	T1078 - Valid Accounts	T1110 - Brute Force	T1046 - Network Service Scanning	T1550 - Use Alternate Authentication Material
T1078.001 - Valid Accounts: Default Accounts		T1078.001 - Valid Accounts: Default Accounts	T1078.001 - Valid Accounts: Default Accounts	T1078.001 - Valid Accounts: Default Accounts	T1528 - Steal Application Access Token	T1049 - System Network Connections Discovery	T1550.001 - Use Alternate Authentication Material: Application Access Token
T1078.003 - Valid Accounts: Local Accounts		T1078.003 - Valid Accounts: Local Accounts	T1078.003 - Valid Accounts: Local Accounts	T1078.003 - Valid Accounts: Local Accounts	T1552 - Unsecured Credentials	T1069.003 - Permission Groups Discovery: Cloud Groups	
T1078.004 - Valid Accounts: Cloud Accounts		T1078.004 - Valid Accounts: Cloud Accounts	T1078.004 - Valid Accounts: Cloud Accounts	T1078.004 - Valid Accounts: Cloud Accounts	T1552.001 - Unsecured Credentials: Credentials In Files	T1082 - System Information Discovery	
		T1136 - Create Account	T1611 - Escape to Host	T1550 - Use Alternate Authentication Material	T1552.003 - Unsecured Credentials: Bash History	T1087 - Account Discovery	
				T1550.001 - Use Alternate Authentication Material: Application Access Token	T1552.004 - Unsecured Credentials: Private Keys	T1087.001 - Account Discovery: Local Account	

Table 2: TeamTNT Cloud Threat Actor TTPs (continued)							
Initial Access	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**
				T1562 - Impair Defenses	T1552.005 - Unsecured Credentials: Cloud Instance Metadata API	T1087.004 - Account Discovery: Cloud Account	
				T1562.001 - Impair Defenses: Disable or Modify Tools	T1552.007 - Unsecured Credentials: Container API	T1518 - Software Discovery	
				T1562.003 - Impair Defenses: Impair Command History Logging	T1562.003 - Impair Defenses: Impair Command History Logging	T1518.001 - Software Discovery: Security Software Discovery	
				T1562.004 - Impair Defenses: Disable or Modify System Firewall		T1526 - Cloud Service Discovery	
				T1562.007 - Impair Defenses: Disable or Modify Cloud Firewall		T1580 - Cloud Infrastructure Discovery	
				T1562.008 - Impair Defenses: Disable Cloud Logs		T1526 - Cloud Service Discovery	
				T1610 - Deploy Container		T1619 - Cloud Storage Object Discovery	

WatchDog

WatchDog is a cloud-focused threat group that has a history of cryptojacking operations as well as cloud service platform credential scraping. They were first known to operate on January 27, 2019. They use a variety of custom-build Go Scripts as well as repurposed cryptojacking scripts from other groups including TeamTNT. They are currently considered to be an opportunistic threat group that targets exposed cloud instances and applications.

Key Takeaway: The Stealer. Technically adept coders; however, they are willing to sacrifice skill for easy access.

Table 3: WatchDog Cloud Threat Actor TTPs				
Execution	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**
T1610 - Deploy Container	T1611 - Escape to Host	T1562 - Impair Defenses	T1528 - Steal Application Access Token	T1046 - Network Service Scanning
		T1562.001 - Impair Defenses: Disable or Modify Tools	T1552 - Unsecured Credentials	T1518 - Software Discovery
		T1562.003 - Impair Defenses: Impair Command History Logging	T1552.001 - Unsecured Credentials: Credentials In Files	T1518.001 - Software Discovery: Security Software Discovery
		T1562.004 - Impair Defenses: Disable or Modify System Firewall	T1552.003 - Unsecured Credentials: Bash History	T1613 - Container and Resource Discovery
		T1562.007 - Impair Defenses: Disable or Modify Cloud Firewal	T1552.004 - Unsecured Credentials: Private Keys	
		T1562.008 - Impair Defenses: Disable Cloud Logs	T1552.005 - Unsecured Credentials: Cloud Instance Metadata API	
		T1610 - Deploy Container	T1552.007 - Unsecured Credentials: Container API	

Kinsing

A cloud threat actor that uses the name Kinsing as the directory location for a family of cryptocurrency mining malware and supporting initialization files. The group targets exposed Docker Daemon APIs using GoLang based malicious processes running on Ubuntu containers and has begun to expand their operations outside of Docker containers specifically targeting container and cloud credential files contained on compromised cloud workloads.

Key Takeaway: Opportunistic CTA with heavy potential for cloud credential collection, but just in it for the money.

Table 4: Kinsing Cloud Threat Actor TTPs

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
T1078 - Valid Accounts	T1610 - Deploy Container	T1078 - Valid Accounts	T1078 - Valid Accounts	T1078 - Valid Accounts	T1528 - Steal Application Access Token	T1613 - Container and Resource Discovery
T1078.003 - Valid Accounts: Local Accounts		T1078.003 - Valid Accounts: Local Accounts	T1078.003 - Valid Accounts: Local Accounts	T1078.003 - Valid Accounts: Local Accounts	T1552 - Unsecured Credentials	
T1078.004 - Valid Accounts: Cloud Accounts		T1078.004 - Valid Accounts: Cloud Accounts	T1078.004 - Valid Accounts: Cloud Accounts	T1078.004 - Valid Accounts: Cloud Accounts	T1552.001 - Unsecured Credentials: Credentials In Files	
				T1610 - Deploy Container	T1552.004 - Unsecured Credentials: Private Keys	

Rocke

Rocke group is a cloud threat actor that specializes in ransomware and cryptojacking operations within cloud environments. This group is known for using the computing power of compromised Linux-based systems, typically hosted within cloud infrastructure. Rocke was originally identified in 2016 and was called Iron Group, and they primarily focused on ransomware operations with the use of their Iron Ransomware toolset and the backdoor malware IronStealer. In May 2018 they developed BotNet capabilities through the use of their XBash toolset. In August 2018, they evolved their operations again by adding the capability to disable and remove cloud security tools from compromised cloud systems. In February 2019, they added a new tool to their playbook which allows for Proxy, Shell, and Lua script capabilities. In August 2019, they were reported to have compromised 28.1% of organizations with cloud infrastructure.

Key Takeaway: The old-timer, slowly ramping up cloud endpoint enumeration techniques, have not gotten to containers yet.

Table 5: Rocke Cloud Threat Actor TTPs

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
T1078 - Valid Accounts	T1078 - Valid Accounts	T1078 - Valid Accounts	T1078 - Valid Accounts	T1110 - Brute Force	T1046 - Network Service Scanning	T1550 - Use Alternate Authentication Material
T1078.001 - Valid Accounts: Default Accounts	T1078.001 - Valid Accounts: Default Accounts	T1078.001 - Valid Accounts: Default Accounts	T1078.003 - Valid Accounts: Local Accounts	T1552 - Unsecured Credentials	T1087 - Account Discovery	T1550.001 - Use Alternate Authentication Material: Application Access Token
T1078.003 - Valid Accounts: Local Accounts	T1078.003 - Valid Accounts: Local Accounts	T1078.003 - Valid Accounts: Local Accounts	T1078.003 - Valid Accounts: Local Accounts	T1552.001 - Unsecured Credentials: Credentials In Files	T1087.001 - Account Discovery: Local Account	
T1078.004 - Valid Accounts: Cloud Accounts	T1078.004 - Valid Accounts: Cloud Accounts	T1078.004 - Valid Accounts: Cloud Accounts	T1078.004 - Valid Accounts: Cloud Accounts	T1552.003 - Unsecured Credentials: Bash History	T1087.004 - Account Discovery: Cloud Account	

Table 5: Rocke Cloud Threat Actor TTPs (continued)						
Initial Access	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**
	T1136 - Create Account		T1550 - Use Alternate Authentication Material	T1552.004 - Unsecured Credentials: Private Keys	T1518 - Software Discovery	
			T1550.001 - Use Alternate Authentication Material: Application Access Token	T1552.005 - Unsecured Credentials: Cloud Instance Metadata API	T1518.001 - Software Discovery: Security Software Discovery	
			T1562 - Impair Defenses	T1552.007 - Unsecured Credentials: Container API		
			T1562.001 - Impair Defenses: Disable or Modify Tools			
			T1562.003 - Impair Defenses: Impair Command History Logging			
			T1562.004 - Impair Defenses: Disable or Modify System Firewall			
			T1562.007 - Impair Defenses: Disable or Modify Cloud Firewall			
			T1562.008 - Impair Defenses: Disable Cloud Logs			

8220

8220 is a cloud-focused threat group which has been active since at least 2017. Tools commonly employed during their operations are PwnRig or DBUsed which are customized variants of the XMRig Monero mining software. The 8220 mining group is believed to have originated from a GitHub fork of the Rocke group's software. 8220 has elevated their mining operations with the use of cloud service platform credential scrapping through the usage of the Log4j exploitation starting in December 2021.

Key Takeaway: Cousin to the old-timer (Rocke), adopting containers into their target set; coming back out of retirement harder and faster.

Table 6: 8220 Cloud Threat Actor TTPs						
Initial Access	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**
T1078.003 - Valid Accounts: Local Accounts	T1610 - Deploy Container	T1078.003 - Valid Accounts: Local Accounts	T1078.003 - Valid Accounts: Local Accounts	T1518 - Software Discovery	T1110 - Brute Force	T1087.001 - Account Discovery: Local Account
		T1136 - Create Account		T1562.001 - Impair Defenses: Disable or Modify Tools	T1552 - Unsecured Credentials	T1087.004 - Account Discovery: Cloud Account
				T1610 - Deploy Container	T1552.001 - Unsecured Credentials: Credentials In Files	T1518.001 - Software Discovery: Security Software Discovery
					T1552.003 - Unsecured Credentials: Bash History	

Table 6: 8220 Cloud Threat Actor TTPs (continued)						
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
					T1552.004 - Unsecured Credentials: Private Keys	
					T1552.005 - Unsecured Credentials: Cloud Instance Metadata API	
					T1552.007 - Unsecured Credentials: Container API	

CTA groups use cloud-specific TTPs in order to achieve their offensive objectives. Each of the tables listed above highlight specific TTPs which are cloud or container platform specific. The TTPs highlighted in orange denote TTPs that are specific to cloud platforms, whereas the TTPs highlighted in green denote TTPs which are container platform specific. Additionally, the TTPs which have red font color denote TTPs which equate to operations that can lead to the wider compromise of cloud operations, including access key discovery, container escape operations, and increased permissions. As can be seen within each of the CTA tables above, these key indicators mark a defining factor for CTA operations. **The direct targeting of cloud-based credentials and container host manipulation tactics allows these groups the likely result of an initial foothold within the compromised organization's cloud infrastructure**.

Potential CTA Future Developments

Given the recent Russia-Ukrainian-related cyber activity, it is important to note that Russian nation-state operators have historically used cloud infrastructure to host malicious content for their offensive operations. There is also evidence these groups have targeted cloud infrastructure specifically. The following three examples highlight how cloud infrastructure has been used or targeted within nation-state operations. Advanced persistent threats (APTs) have always employed the usage of stealing legitimate credentials from compromised systems, and cloud environments are no exception.

APT 28 (Fancy Bear)

- Used Kubernetes infrastructure to perform brute-force attacks.

APT 29 (Cozy Bear)

- The SolarWinds Attack in December 2020, initially started using the SolarStorm exploitation operation, has been linked to APT 29 also known as Cozy Bear or Nobelium. APT 29 actors were able to compromise at least 140 organizations by injecting backdoor code into a signed SolarWinds Orion Hotfix. This hotfix was then downloaded and installed by organizations unaware of the backdoor code. While the Solarwinds Orion platform is not considered to be a cloud application, there are legitimate cloud container images available that do allow organizations to build the application within a dynamic cloud environment. The targeting of this application presents a novel approach to cloud targeting operations by APT groups.

APT 41 (Gadolinium)

- Used Microsoft's Azure cloud platform to host Command and Control resources during their operations. Using a legitimate platform like Azure to host malicious resources can allow APT groups to have their malicious infrastructure appear more legitimate. If a compromised organization sees that their Azure Virtual Machines communicate with another Azure resource, they could accept these communication patterns as legitimate, even if the malicious actions are detected and alerts are generated.

Additionally, it will be critical for security professionals and researchers to continue to monitor cloud environments for the scraping of CSP access and abnormal access activities in the compromised container or cloud workloads; researchers have found that after stealing access keys, CTAs will attempt to use these keys to perform malicious activities in the cloud platforms.

Conclusion and Recommendations

As we have outlined in this report, identity and access management governs the security of cloud infrastructure and helps protect organizations from attacks performed by Cloud Threat Actors. Properly configured IAM can block unintended access, provide visibility into cloud activities, and reduce blast radius when security incidents happen. However, maintaining IAM in the most secure state is challenging due to its dynamic nature and complexity. Historically, IAM misconfigurations have been the entry point and pivot cybercriminals most commonly exploit. To assist in the defense of cloud environments against CTAs, organizations should look to activate the following tactics:

1. **CNAPP Suite Integration**: Monitoring and alerting on security events within a unified platform that includes support for applications at runtime while also integrating security into development workflows is essential to ensuring comprehensive security. According to Gartner:

   > Cloud-native application protection platforms (CNAPPs) are an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production. CNAPPs consolidate many previously siloed capabilities, including:
   >
   > a. Development artifact scanning, including containers
   >
   > b. Cloud security posture management
   >
   > c. IaC scanning
   >
   > d. Cloud infrastructure entitlements management
   >
   > e. Runtime cloud workload protection platform[2]

   Given the level of access CTAs can acquire by compromising a cloud workload, a **CTA could successfully evade a siloed set of cloud security capabilities** like Cloud Workload Protection (CWP) monitoring and detection mechanisms by accessing the cloud platform itself. An organization only using CWP would fail to detect auditable events at the cloud platform level that would be detected with cloud security posture management (CSPM). Likewise, if an organization is only using CSPM, they would fail to detect events taking place on individual workloads. Only by using a suite of tools within a CNAPP would a CTA moving their access directly from the compromised cloud instance to the CSP platform itself be detected. Researchers recommend using a CNAPP suite of tools which includes both a CSPM tool as well as a CWP tool in order to maintain both container and CSP console operations.

2. **Focus on Hardening IAM Permissions**: By allowing overly permissive IAM identities within a cloud environment, it unnecessarily exposes the organization to substantial risk. Read eight best practices below for securing IAM in your cloud infrastructure:

   a. Minimize the use of admin credentials. The less frequently admin credentials are granted or used, the less likely they are compromised.

   b. Minimize the usage of long-term credentials such as user password, access key, and service-account key.

   c. Enforce multi-factor authentication (MFA) for permissions that modify business-critical resources such as database deletion, snapshot deletion, and encryption key update.

   d. Configure a strong password policy. The National Institute of Standards and Technology (NIST) recommends an eight-character minimum length and skipping character composition rules as they are painful for users.

   e. Use federated identity management (FIM) to centrally manage access control.

   f. Grant each identity only the necessary permissions for their jobs. (Principle of least-privilege). Continuously audit all the identities in your cloud environments using tools such as AirIAM and Cloud Infrastructure Entitlement Management (CIEM).

2. Neil MacDonald, Charlie Winckless, Gartner Innovation Insight for Cloud-Native Application Protection Platforms, August 25, 2021, https://www.gartner.com/doc/reprints?id=1-27AL6QP3&ct=210826&st=sb.

g. Monitor IAM activities. All major CSPs have services that monitor IAM usage. These services help identify abnormal activities such as brute-force attacks and logging from unrecognized divides or locations.

h. Auto-remediate excessive privileges. Entitlement audits should not be done manually, as the workloads in cloud environments change rapidly and frequently.

3. **Increase Security Automation:** In The State of Cloud Native Security Report 2022 by Palo Alto Networks, research shows that organizations with a high level of security automation are two times more likely to have a strong security posture. As cloud adoption continues to rise, security teams must be able to keep up with cloud vulnerabilities at scale. By incorporating automation wherever possible, the manual steps typically involved in resolving a security issue can be dramatically reduced. Furthermore, security teams can resolve more security risks faster, both during the development and runtime phases and everywhere in between.

Ready to Identify the Threats in Your Cloud?

Prisma® Cloud analyzes more than 10 billion events every month. By proactively detecting security and compliance misconfigurations as well as triggering automated workflow responses, Prisma Cloud helps ensure you continuously and securely meet the demands of your dynamic cloud architectures. To get started with Prisma Cloud, request your free trial today.

Methodology

Between January 2022 and March 2022, Unit 42 researchers monitored and analyzed the IAM configurations and usage activities across all Prisma Cloud customers. The data contain 680,000 identities in 18,000 cloud accounts over 200 different organizations to evaluate the current state of IAM security. Using the unique capabilities in the Cloud Infrastructure Entitlement Management platform, researchers could calculate the effective permissions of every cloud identity, look into the usage history of each permission, and identify the misconfigurations in the permissions policies. With visibility into the usage history of every effective permission, we can learn how every permission was used in each identity. All the metrics in this report were derived by aggregating the IAM configurations and logs of identities across hundreds of different organizations.

Researchers also researched hundreds of cloud malware samples detailing the operations of Cloud Threat Actors across multiple offensive operations and several toolsets. Researchers used Palo Alto Network products to assist in the collection, analysis and collected metadata for each of the CTA malicious samples.

Palo Alto Networks Prisma Cloud

Prisma® Cloud trend data utilizes multiple threat intelligence sources. Unit 42 researchers used proprietary data sources to gather organizational alert and event data. This data was anonymized, and then analyzed and compared to the results of previous cloud threat report analytics to produce trend information.

Palo Alto Networks WildFire

The cloud-based WildFire® malware prevention service employs a unique multi-technique approach, combining dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive threats.

Palo Alto Networks AutoFocus

The AutoFocus™ contextual threat intelligence service provides the intelligence, analytics, and context required to understand which attacks require immediate response, as well as the ability to make indicators actionable and prevent future attacks.

About

Prisma Cloud

Prisma® Cloud is a comprehensive cloud native security platform with the industry's broadest security and compliance coverage—for applications, data, and the entire cloud native technology stack—throughout the development lifecycle and across hybrid and multicloud deployments. Prisma Cloud's integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively, and accelerate cloud native application development and deployment securely.

Prisma Cloud's Cloud Infrastructure Entitlement Management (CIEM) module provides users with broad visibility into effective permissions, continuously monitors multicloud environments for risky and unused entitlements, and automatically makes least privilege recommendations. Users gain simple yet powerful insight into the net-effective permissions for every role—including those associated with an IdP provider—all seamlessly integrated into Prisma Cloud.

Unit 42

Unit 42 brings together our world-renowned threat researchers with an elite team of security consultants to create an intelligence-driven, response-ready organization. The Unit 42 Threat Intelligence team provides threat research that enables security teams to understand adversary intent and attribution while enhancing protections offered by our products and services to stop advanced attacks. As threats escalate, Unit 42 is available to advise customers on the latest risks, assess their readiness, and help them recover when the worst occurs. The Unit 42 Security Consulting team serves as a trusted partner with state-of-the-art cyber risk expertise and incident response capabilities, helping customers focus on their business before, during, and after a breach.

Authors

Jay Chen, Principal Researcher, Public Cloud Security, Palo Alto Networks
Nathaniel "Q" Quist, Principal Researcher, Public Cloud Security, Palo Alto Networks

Contributors

This report would not be possible without the tremendous work and efforts taken by the larger Palo Alto Networks team. The following people assisted significantly in its creation.

Editing

Aimee Savran
Erica Naone
Grace Cheung
Kelly Kane

Data Validation

Bar Schwartz
The larger Prisma Cloud IAM Team

Threat Intelligence Validation

Unit 42 ARES Team

Initial Cloud Threat Report Vision

Matthew Chiodi

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com