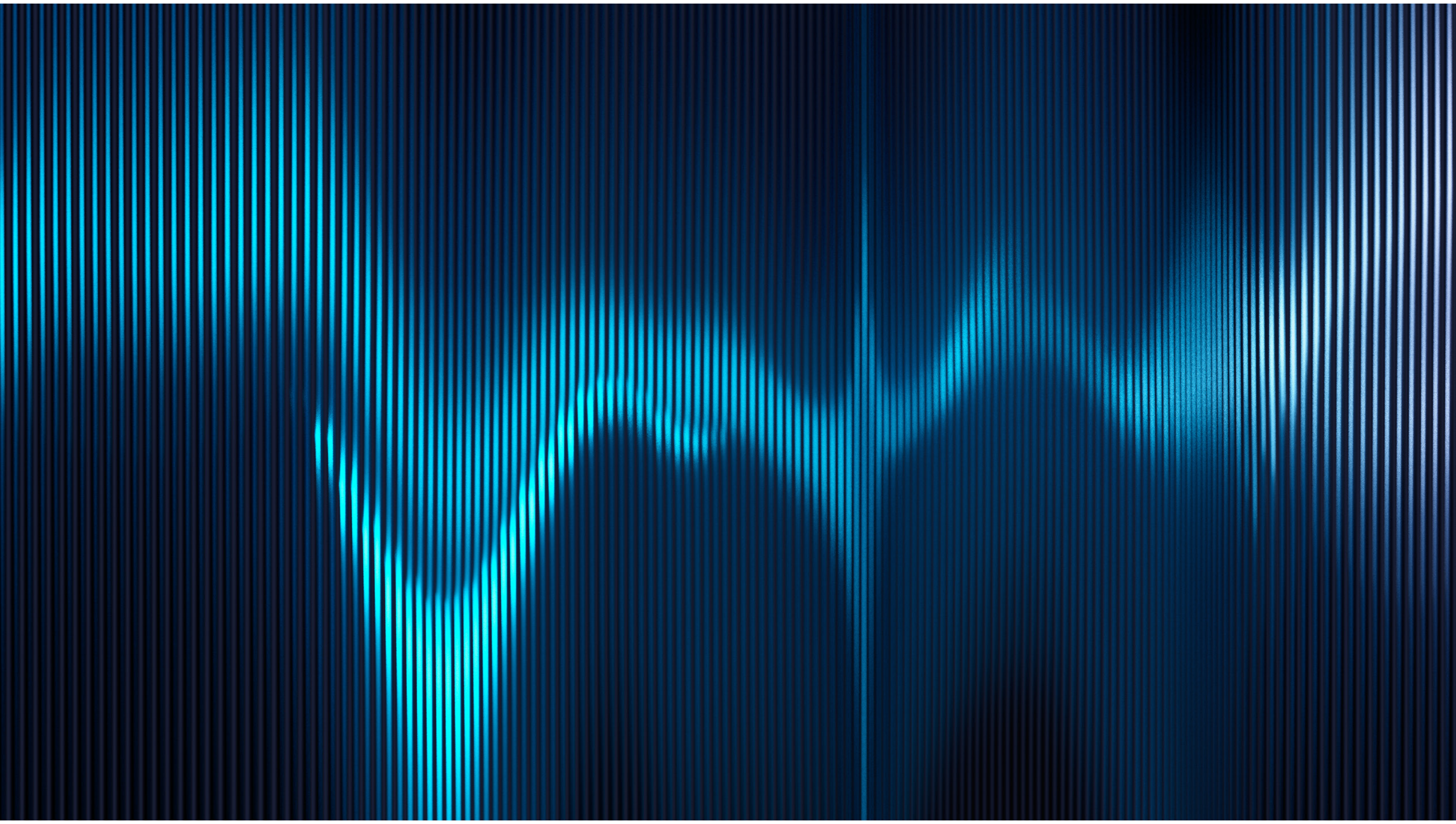
Google Cloud

Threat Horizons

H1 2024 Threat Horizons Report

Office of the CISO

Table of contents



Mission Statement

The Google Cloud Threat Horizons Report provides decision-makers with strategic intelligence about threats to cloud enterprise users, along with cloud-specific research, based on intelligence-derived threat actor trends and expertise from Google Cloud security leaders and practitioners. Most importantly, the report delivers recommendations on mitigating these risks and improving cloud security posture from Google's intelligence and security teams, including Google Cloud's Office of the CISO, Google's Threat Analysis Group, Mandiant, and various Google Cloud product teams.

Executive Summary

New year, new cloud threat insights create informed opportunities for actionable cloud security defenses

This iteration of the Google Cloud Threat Horizons Report provides a forward-thinking view of cloud security with intelligence on emerging threats and actionable recommendations from Google's security experts. This report explores top cloud threats and security concerns for 2024, including credential abuse, cryptomining, ransomware, and data theft.

In 2023, threats increased in number and sophistication targeting all IT environments—on-premise, mobile, IT/OT, and the cloud. Issues specific to cloud providers were often due to security hygiene or misconfigurations rather than underlying vulnerabilities. We saw threat actors evolve their methods for abusing and monetizing cloud infrastructure, gaining initial access to cloud networks, conducting cloud-based supply chain attacks, and running malicious operations from cloud environments.

Based on our research and analysis, the following areas should inform cloud customer security strategies in 2024:

- **Credential abuse** resulting in cryptomining remains a persistent issue, with threat actors continuing to exploit weak or nonexistent passwords to gain unauthorized access to cloud instances, while some threat actors are shifting to broader threat objectives.
- **Ransomware and data theft** remain a concern in all IT environments, including on-premise and cloud, as threat actors are continuously evolving their methods for conducting ransomware and data theft attacks—making robust data loss prevention strategies more essential than ever before.
- Increased focus on **security event logging** is necessary to address threat actors' evolving tactics of manipulation and deleting logs. Threat actors are increasingly targeting security event logging software in novel ways to disrupt and evade detection.
- **People's Republic of China (PRC)-affiliated espionage threat actors** are increasingly targeting cloud services and infrastructure given the enhanced adoption of cloud across industries globally.

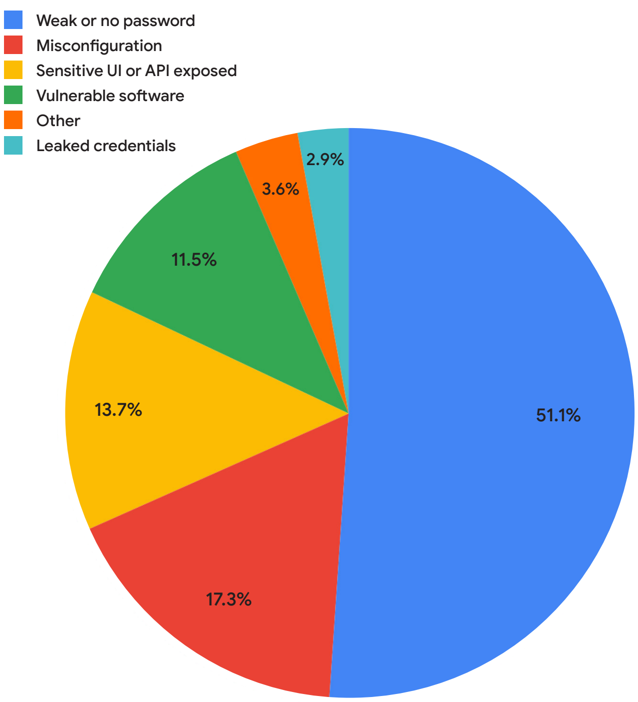
The cloud threats and security issues identified in 2023 will likely continue this year as threat actors seek new ways to bypass security measures, breach customer cloud projects, move laterally, access sensitive data, refine proven techniques, and explore new tactics using Artificial Intelligence (AI).

Looking ahead, high-profile global events in 2024 (e.g. elections worldwide, the Summer Olympics, regional conflicts in multiple regions, etc.) will continue to serve as attractive targets for threat actors seeking novel ways for conducting malicious activities like information operations, espionage, and other cyber campaigns to achieve their objectives. As such, weak points within customer cloud projects will likely be among the top methods attackers utilize to achieve their objectives. We will continue leveraging our threat intelligence and insights to identify actionable risk mitigations to help organizations enhance their cloud security.

The following sections dive deeper into the key takeaways from these cloud threat insights to better enable mitigations for the year to come.

Cryptomining Remains the Dominant Consequence of Weak Cloud Configurations

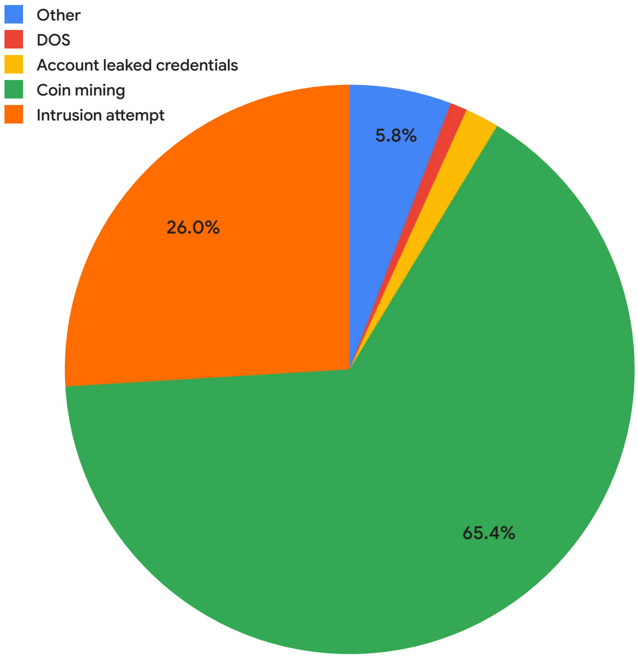
2023 Cloud Compromises: Initial Access



Credential issues remain the predominant security oversight observed among Google Cloud customers. Over half of incident data shows that threat actors are compromising Cloud instances with weak or no passwords on common remote access protocols, Secure Shell (SSH) and Remote Desktop Protocol (RDP), to gain unauthorized access to Cloud instances. This provides threat actors with easy access to compromised cloud resources, which they can monetize by selling access, often for a couple of dollars per credential pair. Given that harvesting such credentials is low-effort for a threat actor, this trend will likely continue to affect organizations that fail to meet basic standards of security.

Cryptomining remained one of the principal motivations behind threat actors who abused cloud access, accounting for nearly two-thirds of observed activity. This quick and easy money maker serves a clear profit motive for criminal actors, as it allows threat actors to use a victim's cloud processing power to mine for cryptocurrency in a shorter period of time. However, this dominance, cited in the Threat Horizons Report throughout 2023, risks overshadowing an insidious trend. Several times throughout 2023, we observed threat actors leverage illicit cloud access in an attempt to infect third parties. This less common tactic, constituting over 25% of

2023 Cloud Compromises: Impact



observed incidents, has significant security impacts for organizations on both sides of the attack. For an organization unwittingly hosting malicious activity, the risks range from reputational harm, to monetary costs and operational disruption. Even though major cloud platforms invest heavily in security and in abuse detection and mitigation, organizations should monitor their own cloud computing resources for suspicious activity to best align billing monitoring and security needs.

These complexities make using cloud resources for malicious purposes convenient for threat actors, and highlights the need for organizations to ensure they are taking steps to protect themselves. Google Cloud offers a variety of security features to support customers and protect their environments from credential abuse, including providing the following:

- **2FA:** Google Cloud currently requires 2FA for all administrative users, which adds an additional layer of security to protect accounts from unauthorized access.
- **Strong password policies:** Google Cloud enforces strong password policies, requiring passwords to be at least 12 characters long and to include a mix of letters, numbers, and symbols; additionally there are other features, including passwordless authentication which eliminates the need for passwords altogether.
- **IAM policies:** IAM policies can be used to control who has access to resources in Google Cloud, and what they can do with those resources.
- **Cloud Audit Logs:** Cloud Audit Logs track all activity in Google Cloud, which can be used to monitor for suspicious activity and to investigate security incidents.
- **Security Command Center:** Security Command Center provides a centralized view of security threats and vulnerabilities in Google Cloud. It can be used to detect and respond to security incidents quickly and efficiently.

Mitigations

- Lock down SSH, RDP, and any other known remote access software with organization-level policy controls on GCP. Google Cloud's Enterprise foundations blueprint with best practices guidance suggests creating a custom VPC network for production workloads rather than relying on the default network with pre-populated rules which expose SSH and RDP among other services. Control administrative access to virtual machines via Identity Aware Proxy.
- Use Essential Contacts to ensure every cloud service used by an organization has point of contact (POC) information updated so cloud providers can reach impacted clients promptly.
- Monitor cloud resource utilization, and establish alerts for anomalous events, such as sudden spikes in new virtual machines.
- Consider leveraging Security Command Center to detect CPU/memory spikes related to cryptomining activity and other potential malicious outbound network connections. Reimbursement for undetected cryptomining attacks is available to Premium customers.
- Reassess your cloud incident response and reconstitution plan.

Strengthen Security to Counter Ransomware Attacks and Data Theft in the Cloud

This article covers both Google Cloud and cloud service provider agnostic threats. Threat actors continued targeting unprotected public cloud storage services, misconfigured networks, and weak cloud storage naming conventions for ransomware and data exfiltration in 2023, and we anticipate that this trend will continue further into 2024. As this type of activity gains additional prominence, it is imperative that defenders strengthen cloud asset management and data protection.

While weak credentials and misconfigurations are often causes for a threat actor's initial access to cloud environments, other factors, such as weak storage defenses, application vulnerabilities, and third-party issues also led to system compromises, resulting in ransomware and data theft (Figure 1).

Common Causes of Ransomware and Data Theft in the Cloud

- Weak credentials (E.g., Default or lack of passwords in cloud applications and systems)
- Misconfigurations and errors in cloud application and system security settings (E.g., Unrestricted ports, excessive user privileges)
- Weak storage defenses (E.g., Anticipated bucket naming conventions)
- Application vulnerabilities (E.g., Zero-day exploits)
- Third-party issues (E.g., Software supply chain risk, insufficient access management)

Figure 1: Common Causes of Ransomware and Data Theft in the Cloud

Notable incidents and threat actor activity include:

- Suspected Rhysida ransomware actors allegedly breached Slovenia's largest power provider, Holding Slovenske Elektrarne, by stealing passwords for systems from an unprotected cloud storage instance in Nov. 2023.
- Threat actors conducted a ransomware attack resulting in lost customer data on cloud-hosting firms CloudNordic and AzeroCloud in Aug. 2023 when the firm's servers were misconfigured during a data center migration.
- Google Cloud Storage (GCS) team observations indicate threat actors are probing weak cloud storage bucket naming conventions to exfiltrate data (Figure 2). Uncategorized threat actors have attempted to use a bucket naming approach that would allow them to anticipate which specific bucket would most likely be used next by a user. This could allow threat actors to precreate buckets in which data is stored by users and then exfiltrate data immediately after users store it. See previous iteration of THR for insights on additional tactics used by threat actors against cloud storage.

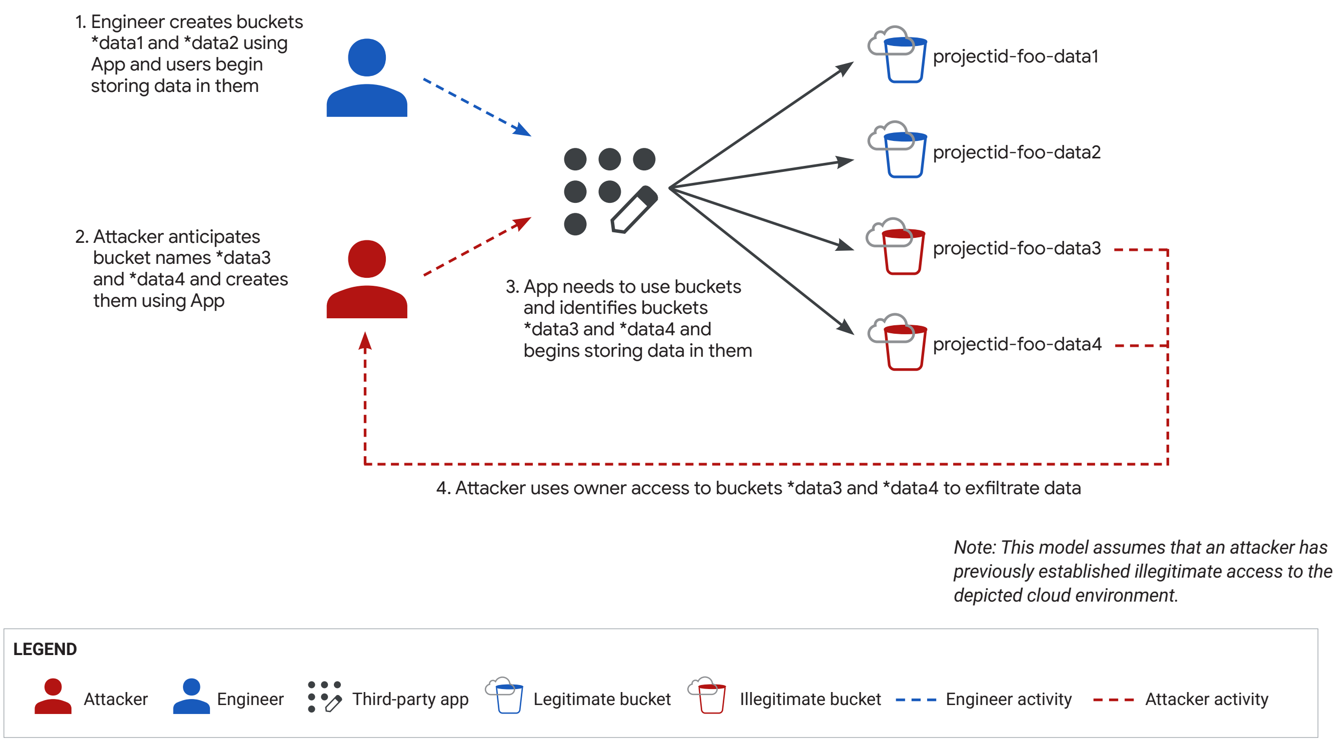


Figure 2: Model of a Cloud Storage Bucket Naming Convention Exploited by a Threat Actor

Some Extortion Groups Moving to Server-side Exploits

Rather than focusing on weak cloud credentials to gain initial access, some multifaceted extortion groups groups are shifting from using client-side to server-side exploits in incidents across multiple cloud providers. In 2023, Cl0p threat actors exploited at least three server-side zero-days and other ransomware groups exploited server-side bugs as n-days.

Notable incidents and threat actor activity include:

- In Nov. 2023, Cl0p actors exploited a now-patched zero-day in IT asset management software, SysAid, and then issued commands via SysAid to install Gracewire malware on additional hosts.
- Mandiant observed Cl0p actors engage in widespread exploitation of a now-patched zero-day in the MOVEit Transfer secure managed file transfer software in June 2023. The actors deployed the LEMURLOOT webshell for data theft, after which the CL0P^_-LEAKS data leak site claimed responsibility for attacks.
- In April 2023, Cl0p actors and associated initial access brokers exploited a now-patched zero-day in print management software PaperCut to drop TrueBot malware. After PaperCut released a patch, other groups, including the Bl00dy Ransomware Gang, exploited the bug as an n-day.
- In April 2023, ALPHV/Blackcat ransomware-as-a-service affiliates compromised victims in cases where access was obtained via an exploited n-day in GoAnywhere MFT for initial access.

Threat Actors Prioritizing Data Exfiltration Over Data Encryption

Threat actors targeting cloud environments began prioritizing data exfiltration over data encryption and stolen data advertisements grew in 2023, as threat actors demonstrated an increased focus on publicly releasing exfiltrated data from multiple cloud providers.

This could suggest that threat actors are increasingly seeking to profit by selling the data (or access to the data) rather than expecting victims to pay the ransom for decryption keys.

- Taiwan Semiconductor Manufacturing Company (TSMC) confirmed a data breach originating from a partner cloud computing company, Kinmax Technologies, conducted by the Lockbit ransomware gang, who posted TSMC data on their leak site with a $70 million USD extortion demand in July 2023. Lockbit threatened to destroy the data or make it publicly downloadable.

Threat Actors Likely to Continue Adapting Methods for Ransomware and Data Theft

In 2023 a number of threat actors adapted their tools for conducting ransomware attacks and stealing data in the cloud, which we assess will likely continue in 2024.

- Ransomware developers created Linux variants and ransomware builds specific to VMWare ESXi. As of Nov. 2023, Kinsing hackers were exploiting the Linux

Privilege Escalation Flaw (CVE-2023-4911) to gather industry-wide cloud service provider credentials and expose sensitive data in cloud environments.

- Mandiant Intelligence identified more than 100 tools—from backdoors, downloaders, and ransomware—that are either targeted or have the capability to leverage cloud-related technologies for command-and-control (C2), payload hosting, and/or data exfiltration.
- Threat actors exfiltrated stolen data from—and sent stolen data to—public cloud storage platforms when conducting ransomware attacks. In early 2023, PLAYCRYPT ransomware threat actors leveraged stolen credentials to gain access to a victim's network and use the RDP to move laterally across multiple systems. After identifying and staging data in multiple file archives in the victim's cloud environment, the threat actors exfiltrated the data and subsequently encrypted the file archives.

Mitigations

We recommend multiple approaches for Google Cloud customers to help prevent ransomware and data theft in their cloud environments, including:

- Follow Google Cloud and industry best practices for cloud asset risk management, including Cloud Asset Inventory services, Identity and Access Management, and the Cloud Controls Matrix (CCM).
- Establish a cloud-specific backup strategy with testing that includes configurations and templates of stored assets, not solely backups of data or machine state.
- Use technologies, such as WORM (Write Once Read Many), or the Bucket Lock feature on Google Cloud to provide immutable and policy compliant backup storage.
- Implement resilient architecture, such as multi-region cloud use and backup mirroring, to reduce risk of data loss or inaccessibility.
- Encrypt all backups, which Google Cloud Storage does by default. Google Cloud customers can add an additional layer of encryption by using customer-managed encryption keys (CMEK). Segregate key access roles to help prevent attackers from being able to read backups.
- Configure sensitive data protection with Cloud Data Loss Prevention and use Cloud Backup and Disaster Recovery service to backup your cloud data for recovery in the instance of an attack.
- Incorporate controls on known exploited vulnerabilities and misconfigurations linked to ransomware by leveraging Google Cloud Threat Intelligence for Chronicle and VirusTotal and following guidance from the U.S. Dept. of Homeland Security, Cybersecurity and Infrastructure Security Agency's Ransomware Vulnerability Pilot (RVWP).

Don't Get Caught in the Dark: Shining Light with Logs

In 2023, threat actors targeted security event logging software in all IT environments in a number of novel ways that evade detection, underscoring the importance of comprehensive logging practices. Robust logging practices are fundamental to an organization's security posture, and are becoming more sought out in cloud environments, as network defenders realize the potential value in collecting and gathering as much data as possible to reconstruct attacks.

Similar to network defenders, threat actors are continuously learning and adapting their Tactics, Techniques and Procedures (TTPs) in the cloud. Mandiant's M-Trends 2023 (page 43) reports that clearing logs or traces of attacker activity was among the fifth most frequent technique observed. Sophos similarly reported (page 9) that network defenders and incident responders were missing telemetry for nearly 50% of the incidents due to threat actors disabling protection and approximately 40% of the time logs were cleared, leaving no evidence for analysis and mitigation.

Implementing a security event logging solution can support establishing baseline activity in logging to subsequently detect anomalous behavior. Maintaining strong logging practices provides organizations with greater visibility into their cloud environments and activities, which can help to triage, identify, detect, and mitigate threats more quickly. Moreover, the visibility, contextual and historical background related to the activity allows defenders to observe how threat actors work to disable or tamper with logs to cover their tracks. Lack of logs can result in slowing down or preventing network defenders from mitigating threats in a timely manner. The complimentary and prominent role compliance has in cloud security logging is further supported by compliance requirements, international standards, and government and international regulations.

Threat actors are taking aim at logging systems to avoid the defender's gaze and this intent underscores the importance of exporting logs to a secure and centralized location. According to M-Trends 2023 (page 75) as well as a report from CISA (page 12), the criminal threat actor group UNC3661 (also known as Lapsus$) has been observed taking active steps to remove or disable security monitoring tools such as endpoint detection and response (EDR) tooling. The lack of logs generated from these telemetry sources should be an indicator in itself to defenders where a stream of information that was expected is no longer generating logs.

Mandiant also notes in the M-Trends 2023 report that the Lockbit ransomware has been observed clearing event logs prior to encrypting files. This results in limited visibility into how the attackers gained initial access and deployed the ransomware, what other malware may have been deployed but not found, and other attempts of lateral movement or persistence in the environment. In the Google Cloud Cybersecurity Forecast 2024 we expect that the use of wipers will be adopted by a greater number of threat actors which alongside other system files will likely remove on-device logs.

When managing logs in the cloud, some logs are enabled by default and cannot be disabled, such as Admin Activity and System Event audit logs while other logs have cost implications and require customers to enable and configure, such as Data Access audit logs and network logs. Additionally, it's important to consider the retention period of logs to assure key insights will be available and not automatically lost when required during an incident. Guidance for which types of logs to enable exists from various sources and is linked in the mitigations section below, but in general, can include telemetry from endpoints, application logs, network logs, and Cloud logs. By default, Google Cloud customers have access to all logs that are generated by their Google Cloud resources. This includes logs from applications, services, and infrastructure. Customers can also choose to export logs to other services, including Cloud Storage or BigQuery. Significantly, the security event logging capability also includes pre-built dashboards and reports intended to support organizations in identifying and responding to threats. Further, Google Cloud offers a variety of log management tools that help organizations to store, archive, and analyze security logs.

The observations from threat actor behavior, along with the requirements of regulations and compliance guidance from organizations such as NIST, CISA, and NSA communicate the urgency of enabling, properly configuring, and monitoring logs. Organizations should prioritize logging in 2024 and leverage the capabilities of the Cloud to detect threats quicker—safeguarding their data and customers. Lastly, it needs to be highlighted that in addition to logging all security events, it is equally as important to log other relevant information, such as network traffic, user activity, and system changes. This information can help organizations to better understand their environments and identify potential security risks by establishing baseline behavior to measure against future activity.

Mitigations

- **Identify relevant logs to collect and monitor** as outlined from Google Cloud's MITRE ATT&CK mapping of Google Cloud logs, NIST SP 800-92 (draft of new revision), NSA's Volt Typhoon threat hunting, or Mandiant's blog post covering Cloud logs with example attacker path scenarios.
- **Export logs to a centralized, well-governed repository** to make it easier to monitor the environment as a whole but also reduce the risk of losing visibility when threat actors delete logs or disable user-configured cloud logs.
  - Protect centralized logs by adding protections against project deletion with a Project Lien and increasing the retention on logs for longer visibility.
  - Leverage Security Command Center's Security Health Analytics to detect data access audit logs being disabled or review IAM permissions for high-sensitivity roles such to change logging settings.

   - Securely configure IAM permissions so only key individuals have access to change logging settings, which are considered a high-sensitivity role.

- **Monitor for missing logs.** Organizations should monitor for the lack of telemetry due to log deletion or endpoint protection being disabled. Leveraging a cloud-native SIEM and SOAR like Chronicle Operations Suite will help with ingesting and normalizing log data and automate alerting. Community Security Analytics also hosts pre-built queries for organizations to manually search for threats.
- **Assure sensitive information is not available** to threat actors with access to logs. Similar to defenders, threat actors can glean insights into a target's environment from logs with sensitive information.
   - Google Cloud's Cloud Data Loss Prevention (DLP) can regularly scan data and can help prevent sensitive information from falling into the hands of attackers.
   - Ensure sensitive data, such as passwords or user data, isn't written to application logs.
   - Consider tools such as TruffleHog to help find credentials stored in file systems, containers, and cloud storage.

Advanced Persistent Threat (APT) Actors In Cloud Architecture Spotlight: People's Republic of China (PRC)

Throughout 2023, the People's Republic of China (PRC) has increasingly targeted cloud infrastructure, a trend highlighted by the activities of a few nation-state backed Advanced Persistent Threat (APT) actors. The TTPs, particularly those focused on "Living-off-the-Land" (LOTL) tactics, have enabled threat actors to blend into normal network activities, evading detection. These actions align with the PRC's overarching goal of creating a Digital China. The PRC's Digital China strategy, which as of 2023 was largely new to Western audiences, has evolved over the past decade to encompass most of the world. China's Digital Strategy is supported by long standing Belt & Road Initiatives, both economic and infrastructure related projects spans the world, including the African and South American continents, laying the groundwork for greater interconnectedness worldwide.

Threat actors affiliated with the People's Liberation Army (PLA), the Ministry of State Security (MSS) and other contractors that may be affiliated with a defense entity have undergone a significant evolution over the past three decades. The cybersecurity landscape currently faces a critical challenge with the emergence of highly resilient botnet operations operated by PRC state-sponsored threat actors who relentlessly scan for vulnerabilities in computer systems vital to our daily lives so that threat actors can exploit them.

Sophisticated Evasion in Cloud Infrastructure: PRC's New Paradigm

A number of PRC-nexus threat actors have shown a high proficiency in exploiting vulnerabilities associated with cloud services, infrastructure, targeting virtual machines, and related cloud architecture, as evident in several sophisticated campaigns in 2023. In an operation described by Unit 42, PRC nexus APT infrastructure masqueraded as cloud backup services via typosquatting, primarily targeting Cambodian government organizations. In its report, Unit 42 observed a total of 24 Cambodian government organizations communicating with this infrastructure between September and October 2023. These organizations mostly focused on critical services including those in defense, government, legal, financial, telecommunications and natural resources.

The Case of UNC3236 aka *Volt Typhoon*

Google Cloud security partners track this threat as UNC3236, a PRC-nexus threat actor active since at least 2021, and characterized by cyber espionage and intelligence gathering. DHS CISA and Microsoft state that this actor is targeting US critical infrastructure, with the goal of gathering intelligence and disrupting operations, often targeting critical services in industries such as defense, government, legal, finance, telecommunications, and natural resources.

UNC3236 operations and campaigns have successfully evaded traditional EDR primarily because it is able to conduct operations without the use of malware, often using legitimate services and applications for lateral movement once in the network. They accomplish this by surreptitiously repurposing end-of-life commercial and residential routers to set up various obfuscation networks.

The challenge in detecting and tracking these covert networks is that after initial access is achieved, the corresponding C2 communications can be extremely challenging to detect. The volume of C2 traffic may be minimal if the persistent access was in and of itself the primary goal. A number of these covert networks were established by surreptitiously repurposing end of life commercial and residential routers in order to set up a Tor-like covert data transfer network to conduct malicious operations. A number of these end of life devices lack security updates, turning them into pivotal components in the actor's penetration strategy.

Specific characteristics of this adversary and its patterns of behaviors include the following observations relevant to cloud infrastructure, including:

- Proxies network traffic through compromised commercial and residential network edge devices. These covert networks make it more difficult to trace activity back to the original source.
- Uses custom versions of open-source tools to establish a command and control (C2) channel over proxy. This allows them to communicate with each other and exfiltrate data undetected.
- Attempts to create installation media from domain controllers, either remotely or locally. This gives the threat actor access to usernames and password hashes, which they can use to gain further access to the network and move laterally.
- Living-off-The-Land binary (LOLBins) commands to find information on the system, discover additional devices on the network, and exfiltrate data. This can be done without the use of malware, making it even more difficult to detect.

In January 2023, Mandiant, first reported publicly that threat actors affiliated with the PRC are responsible for a series of cyber espionage operations that have targeted internet-facing devices. Google Cloud has also observed PRC targeting of cloud environments, leveraging tactics that allow threat actors to blend in with normal network traffic, making detection challenging. Given historical campaigns and operations, and current geopolitical tensions, Google Cloud sees UNC3236 as a growing threat to cloud users in 2024.

Google Cloud has proactively implemented security measures to counter the threat posed by malicious actors that share sophisticated capabilities similar to those discussed here. Efforts in enhancing monitoring systems, leveraging advanced threat detection, and promoting industry collaboration are instrumental in strengthening infrastructure and services against sophisticated cyber threats.

The Case of Storm 0588

Most recently, in July 2023, Microsoft's Storm-0558 campaign demonstrated another sophisticated aspect of the apparatus: several agencies, and departments within the PRC and CCP focus on possible vulnerabilities and risks within cloud infrastructure and services. The campaign involved the use of forged tokens to access the email systems of about 25 entities, including government agencies and public cloud consumer accounts.

Key findings by DHS CISA, an affected U.S. government agency "identified suspicious activity by leveraging enhanced logging—specifically of MailItemsAccessed events—and an established baseline of normal Outlook activity, such as AppID." The MailItemsAccessed event logging enabled detection of otherwise difficult to detect adversarial activity. Investigations uncovered that on May 15, 2023, the threat actor began using an acquired Microsoft account (MSA) key to forge tokens to access Outlook Web Access in Exchange Online (OWA) and Outlook.com domain.

The Microsoft Exchange was impacted by a vulnerability that caused it to accept Azure AD authentication tokens as valid even though they were signed by an Acquired Microsoft Account (MSA) signing key to gain access to enterprise accounts. This vulnerability occurred as a result of an incident related to internal default settings. Microsoft clarified that this occurred as a result of a missing validation functionality in the Software Developer Kit (SDK). At some point in 2022, the development team tasked with authentication in Exchange incorrectly assumed that the Azure AD SDK performed issuer validation by default. This caused validation to be implemented incorrectly, leading to the exploited vulnerability.

While the timing of the targeting is consistent with espionage-related objectives, as well as the U.S. Secretary of State's visit to China, Google security partners concur with Microsoft's assessment that the most likely objective of this threat actor is that of a well resourced and sophisticated cyber espionage actor.

Mitigations

In addressing the complex challenges posed by sophisticated nation-state cyber threats, notably from actors associated with the People's Republic of China, cloud service providers and their customers must adopt a multifaceted and proactive approach to cybersecurity. These should consist of:

- Security by Design; Safe by Default; Security in Deployment. Security by design and secure by default are approaches to building software that are meant to be inherently secure. Security by design means that security is built into the system from the ground up, with a focus on preventing vulnerabilities and attacks. Safe by default means that the system is configured in a way that is as secure as possible by default, with the user having to take action to make it less secure. Security in deployment offers continuous assurance that controls are deployed as they should be. Google Cloud provides tooling and capabilities to integrate with customized cloud environments to support assurances that your security, risk, and compliance levels are consistently sustained. This allows cloud environment to operate with confidence that threats from ransomware, account takeovers, bots, phishing, and even more advanced attacks, are minimized,

- Leverage [Chronicle Cybershield](). As part of Chronicle CyberShield, GCP government customers can leverage cyber threat intelligence from Google and Mandiant to build a scalable and centralized threat intelligence and analysis capability. This is integrated operationally into the government SOC to identify suspicious indicators and enrich the context for known vulnerabilities. Chronicle CyberShield allows governments to build a coordinated monitoring capability with Chronicle SIEM to simplify threat detection, investigation, and hunting with the intelligence, speed, and hyperscale of Google.
- Defense in Depth Approach. Defense in depth is when you have multiple complementary controls, failsafes, and redundancies, so that if one control fails, operational integrity is maintained. Defense in Depth and zero trust approach is based on the notion that trusting any single component in a complex system can be dangerous. Therefore, it is essential to verify trust through multiple means and on an ongoing basis. This strategy provides robust defense against sophisticated cyberattacks.
- Cloud Key Management Service. Cloud Key Management Service (Cloud KMS) lets you create and manage encryption keys for use in compatible Google Cloud services and in your own applications. It can be managed via the Cloud Console in your cloud environment.For information about using your own encryption keys in Google Cloud, see Customer-managed encryption keys (CMEK).
- Engage in collaboration and information sharing within the industry through various Information Sharing and Analysis Centers (ISACs). Google's participation and membership in a number of ISAC allows us to partner and support government and industry in continuous education and training, and vital engagement with cloud providers. These ongoing and continuous engagements, discussions and partnerships further align with Google's shared fate approach. Through our shared fate approach, we recognize that it is our responsibility as the cloud provider to be active partners in cloud adoption and digital transformation. Together, we can create a forum to develop a shared understanding of emerging threats and more effective strategies to engage in comprehensive risk management. Existing ISAC membership includes:
  - Bio-ISAC
  - Health ISAC
  - Financial Services ISAC
  - Electricity ISAC
  - Multi-State ISAC
  - Elections Infrastructure ISA
  - Space-ISAC
  - Media & Entertainment ISAC

There are historical precedents for the PRC cyber-espionage activities, as demonstrated by the PLA and MSS track records of using cyber capabilities for intelligence gathering and other national security objectives. This indicates that the PRC remains a persistent and dynamic threat actor in the cyber domain. As cloud computing adoption continues to grow across the world, it is important for public and private organizations to be aware of the potential APT threats posed by the PRC and to take steps to protect their infrastructure from these attacks.

Google Cloud