Cloud Compromise Scenarios Part 4: Key Takeaways, Cloud Abuse, and Other Considerations

Strategic (ST)

March 22, 2021 01:07:52 PM, 21-00004109, Version: 1.1

Executive Summary

- Mandiant Threat Intelligence reviewed incidents that involved manipulation of cloud resources in a four-part series.
- We anticipate that use of the cloud compromise techniques described in this series will become increasingly common as more organizations expand their cloud presence, and as more attackers develop the necessary competencies to target cloud and hybrid systems.
- Mandiant frequently observes threat actors using cloud resources to support an element of their threat activity, such as hosting payloads, or as a destination for stolen data.
- Cloud outages are most often not malicious, but they can have a significant impact on an organization's ability to complete vital work and fulfill contracts to customers. We suggest that organizations consider creating emergency plans or modifying network architecture so that critical functions are preserved in the event of an outage.

Threat Detail

Cloud Compromise Scenarios

Mandiant Threat Intelligence reviewed dozens of incident response investigations and other evidence of threat activity that involved manipulation of cloud resources from recent years. In parts 1-3 of this series, we describe numerous ways in which threat actors manipulated users and hybrid architecture to fulfill steps in the attack lifecycle (Figure 1).

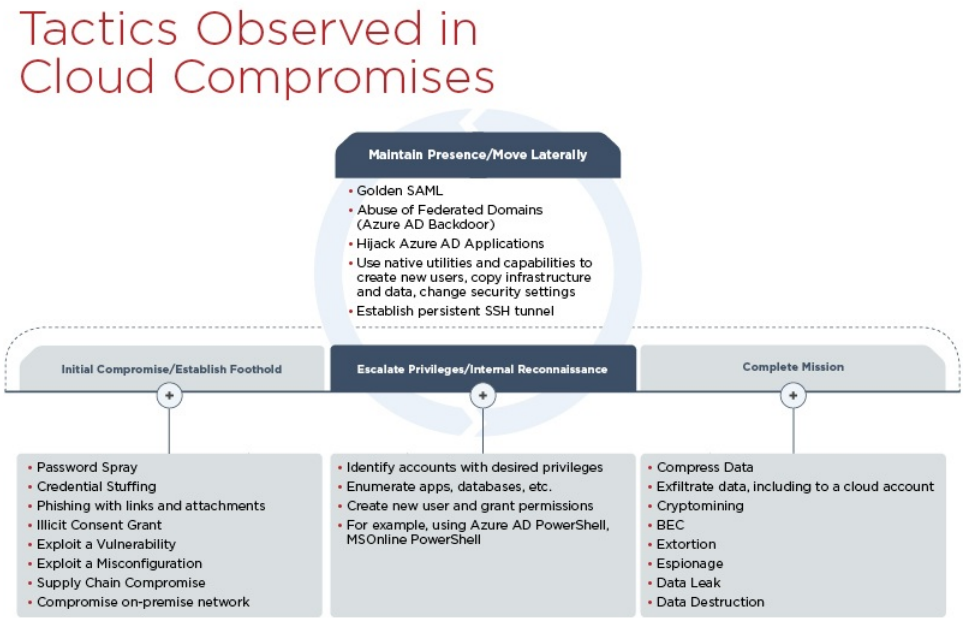

Figure 1: Cloud compromise scenarios mapped on attack lifecycle

This report is part four of a four-part series, discussing key takeaways drawn from cloud compromise scenarios, as well as ways in which threat actors abuse cloud resources (e.g., to host payloads or operate command and control channels), additional challenges inherent in cloud resources, and remediation recommendations network defenders may want to consider.

Title	Report ID
Cloud Compromise Scenarios Part 1: Initial Compromise/Establish Foothold	21-00004106
Cloud Compromise Scenarios Part 2: UNC2452 Exploits Azure AD and M365	21-00004107
Cloud Compromise Scenarios Part 3: AWS	21-00004108
Cloud Compromise Scenarios Part 4: Key Takeaways, Cloud Abuse, and Other Considerations	21-00004109

Table 1: Cloud compromise scenarios series

Key Takeaways

Cloud Security Is Cyber Security

Industry reports agree that enterprise cloud adoption is growing and that this growth has only accelerated since the onset of the coronavirus (COVID-19) pandemic. Mandiant has likewise observed greater rates of cloud adoption and use of hybrid cloud/on-premise environments among our clients as well as more frequent incidents that involve cloud resources.

Hybrid IT environments linking cloud resources to on-premises systems are complex to operate and secure. Policies and permissions governing how users, applications, programs, and databases interact with each other are often designed to facilitate ease of use and consistency of experience across platforms, sometimes at the cost of security. It is not uncommon for organizations to neglect logging and auditing of cloud environments, or to not alter default settings, which allow administrative users wide ranging access.

We suggest that organizations using cloud services apply the same standards to monitor, manage, secure, patch, log, and segment cloud systems as they do on premises systems to avoid potential security gaps. Cloud security operates under a shared responsibility model: cloud providers secure the base components of the platform, but customers are ultimately responsible for securing their data (19-00000127).

Diversity of Observed Attackers and Goals Reflect Growing Prevalence of Cloud

Mandiant Threat Intelligence observations suggest that the types of actors seeking to compromise cloud resources largely reflect overall trends, indicating that diverse attackers recognize the value of data stored in the cloud.

- The threat actors we observed attempting to gain access to or manipulate cloud resources ranged widely in terms of sophistication: from opportunistic actors using automated scanning tools or brute-force tactics to identify and exploit unsecured entry points, such as "Team TNT," to UNC2452, which we documented using several clever manipulations of different implementations of authentication between on-premises systems and cloud environments, particularly M365 and Azure.
- As for goals, Mandiant noted cloud compromise operations that were overt and disruptive (e.g., incidents in which threat actors stole, destroyed, then attempted to ransom data back to victim organizations). We also examined intrusions seeking to quietly collect sensitive government or corporate information without leaving a trace as well as relatively simple scenarios in which threat actors quietly abused computing resources to support crypto-mining.

Friend or Foe? Attackers Use Native or Publicly Available Utilities, Valid Credentials

We noted very little malware use in the internal reconnaissance, escalate privileges, move laterally, and maintain presence stages of compromises of cloud environments. Instead, attackers predominantly used utilities and capabilities that were either already present in the victim environment or open-source utilities commonly used for legitimate purposes to navigate cloud systems (see Table 2).

Example Utilities Used
Azure AD PowerShell
MSOnline PowerShell
PuTTY
Aws-cli
Mysqldump

Table 2: Examples of utilities used by threat actors in cloud compromises

The lack of known-bad forensic artifacts related to malware can complicate defenders' ability to detect, investigate, and attribute threat activity. Attackers also often use compromised, valid credentials with wide-ranging access permissions, which contributes to the challenge of distinguishing malicious actions from legitimate activity of authorized users and applications.

Cloud Compromise, Observed Techniques Likely to Increase

We anticipate that use of the techniques described in this series will become increasingly common as more organizations expand their cloud presence and more attackers develop the necessary competencies to access and successfully manipulate cloud and hybrid systems. Taking proactive steps to address potential weaknesses and harden hybrid environments ahead of broader attacker adoption could equip organizations to better defend against—and even prevent—future compromises.

Cloud Compromise Versus Cloud Abuse

In addition to incidents in which attackers sought to gain access to victim cloud environments, we documented a variety of threat actors using cloud resources to support an element of their threat activity (e.g., to host or deliver malware or as a destination for stolen data).

Threat Actor Use of Cloud for Infrastructure and Malware Distribution

Mandiant Threat Intelligence has often noted adversaries relying on cloud-based infrastructure for command and control (C&C) functions and malware delivery. Incorporating cloud-hosted communications or file sharing can provide attackers a way to bypass security controls that are not specifically configured to check traffic or documents and files sent via these systems.

- In October 2020, FireEye devices detected and blocked spear-phishing emails that delivered a self-extracting RAR archive (SFX) that contained decoy content and a .NET backdoor, OCEANMAP. OCEANMAP communicates over IMAP protocol using an email account's Drafts folder for command and control (C&C). Pivoting from the OCEANMAP campaign, we identified the OCEANDRIVE backdoor that functions similarly to OCEANMAP, but uses Google Drive for C&C. We currently track this activity as an uncategorized cluster of activity with low-confidence ties to APT28 based on indications from a trusted third party (20-00022740).
- Mandiant observed several campaigns in early 2020 that distributed SQUIDSLEEP and SQUIDGATE. In these campaigns, actors leveraged payloads hosted on Amazon Web Services (AWS) infrastructure (20-00015109).
- We identified a suspicious archive named "Australian Ambassador requested meetings in September.zip" that was likely used in late August 2020 by APT32. The archive is likely a spear-phishing email attachment masquerading as a document of high importance. The sample uses DLL side-loading to deliver "LOTUSGHOST," which attempts to download and execute a next-stage payload hosted on Google Drive. Mandiant suspects the target is Southeast Asian countries according to additional information from a known public file-scanning service (20-00018821).
- TEMP.Zagros spear-phishing emails used Microsoft OneDrive and Onehub links with COVID-19 response or IT security lures to target government entities in the United Arab Emirates (UAE) and Saudi Arabia between April and October 2020 (20-00021611). Similar activity likely targeted government entities in Azerbaijan, Turkey, and the UAE, and an Iraqi telecommunications firm from December 2020 to February 2021 (21-00004357). The OneDrive and Onehub links lead to an archive file containing Remote Utilities or ScreenConnect, publicly available RDP tools.
- Mandiant identified four droppers hosted on GitHub that load DROPDOOR malware. The files contain COVID-19 vaccination-related lures and masquerade as PDFs but are actually Microsoft Installer (MSI) files. It is unclear if the samples have been deployed or are being staged for use in future operations (20-00017248).
- APT40 malware such as AIRBREAK and BADFLICK may use legitimate web services such as GitHub, Microsoft TechNet, and Pastebin for C&C communications in a technique known as Dead Drop Resolving (DDR). This technique is typically performed by storing encoded or encrypted strings in locations such as git commits, user profiles, and raw pastes to be retrieved later. This tactic excels at subverting network defenders since there is typically a high volume of legitimate traffic to and from these types of services (18-00020929).

Ransomware Operators Send Stolen Data to Public Cloud Services

In ransomware data theft incidents, Mandiant identified trends in data exfiltration tactics, techniques, and procedures (TTPs), including attackers leveraging legitimate utilities for file compression and using file transfer protocol (FTP), SSH file transfer protocol (SFTP), and legitimate cloud hosting and file-sharing services to host stolen data (20-00022102).

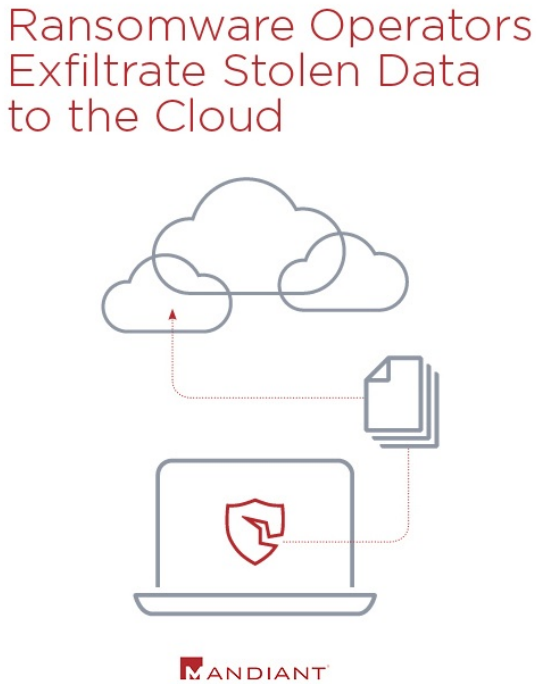

Figure 2: Ransomware operators often export stolen data to cloud resources

Uploads to cloud file storage or hosting services is one of the most common methods that threat actors use to remove data from victim environments, based on Mandiant Threat Intelligence observations. MEGA is among the services most commonly used for this purpose, though other sites, such as pCloud, Microsoft OneDrive, Send-file, DropBox, and various other services, have also been observed. Actors may use a tool such as rclone to synchronize data to a cloud file storage service or interact with the services using a web browser. Notably, actors often attempt to upload stolen data to multiple file storage services prior to finding one that is accessible and sufficiently performant in a given environment.

- We have seen actors deploying MAZE and PROLOCK use the utility rclone alongside a configuration file (rclone.conf) to copy stolen data to the cloud file hosting/sharing services such as Dropbox and MEGA (20-00007034).
- In SODINOKIBI incidents involving data theft, actors installed legitimate synchronization software offered by cloud storage providers to automatically exfiltrate a large number of files. In at least one case, the actors staged files compressed using 7-Zip before synchronizing them to the cloud service (20-00009200). Actors deploying SODINOKIBI have also used the cloud storage provider pCloud.
- Actors deploying NETWALKER have used 7-Zip to compress files and later accessed the cloud-based file hosting service MEGA. We have also observed actors using the MEGA client synchronization software to exfiltrate data.
- In observed FIN11 cases involving data theft FIN11 staged the data in RAR archives, uploaded the files to the MEGAsync servers, and then deployed the CLOP ransomware (20-00011864). In at least one case, the actors also used the publicly available WinRAR utility to compress the targeted data into a series of archives.
- In a RAGNARLOCKER incident, we observed actors using the WinRAR utility to create dozens of archives containing sensitive corporate data, which were later uploaded to MEGA using the MEGAsync utility.

Malicious Insiders Likewise Exfil to the Cloud

Malicious insiders also use cloud resources to remove corporate data from enterprise control or to establish a foothold for remote access (20-00008739). For example, in 2018, Chinese national Guangzhi Cao allegedly downloaded complete copies of Tesla's Autopilot-related source code to his personal iCloud account.

Outages

Cloud outages are most often not malicious but can have a significant impact on an organization's ability to complete vital work, provide resources to internal stakeholders, and fulfill contracts to customers.

- In 2020, outages affected numerous major cloud companies, including Microsoft Azure and 365, Google Cloud, IBM Cloud, AWS, Cloudflare, and GitHub. A November 2020 AWS outage affected almost all applications using the provider, streaming services, IoT devices, and interrupted transaction processing for cryptocurrency exchanges.
- Cloud companies are also susceptible to internet, power, or other disruptions from their providers. In January 2021, a severed fiber resulted in a widespread Verizon outage that affected AWS, Google, Slack, YouTube, and other services. An August 2020 BGP routing error by an ISP affected gaming services PlayStation Network and Xbox Live, as well as Cloudflare, Hulu, and other services (20-00017489).

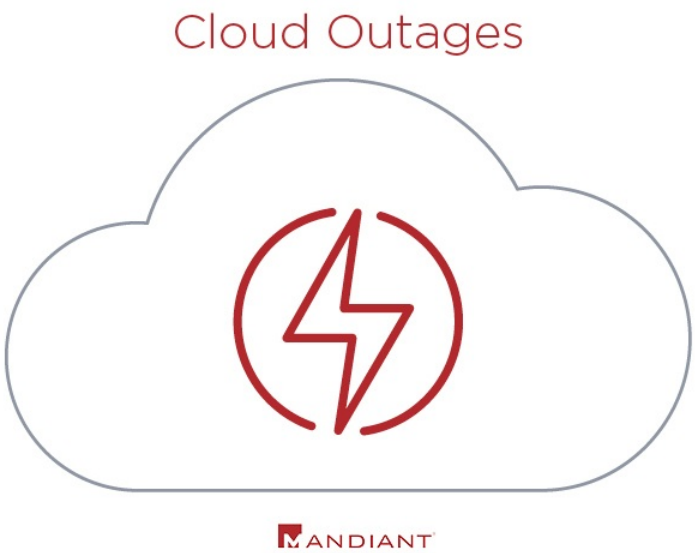

Figure 3: Cloud outage

It is possible for malicious activity to cause cloud outages, though we have not observed evidence of a successful distributed denial-of-service (DDoS) attack against large cloud providers since 2016.

- On Oct. 21, 2016, DNS provider Dyn Managed DNS was targeted by three distributed denial-of-service (DDoS) attacks that successfully impacted more than 40 Managed DNS customers in the U.S. Dyn confirmed that the attack was primarily conducted by a Mirai-based botnet; however, other botnets and booter services were also possibly part of the attack (16-00016558).
- In late 2020, Google revealed that it experienced and successfully weathered a record breaking 2.5 Terabit per second (Tbps) DDoS attack in September 2017. Google also noted that while DDoS attacks have been growing exponentially in size from 2011–2020, so has the internet.

As organizations—and third parties they rely on—increasingly migrate resources to cloud hosting, they become vulnerable to temporary loss of availability.

Mitigation Recommendations

Use of Legitimate Utilities

To mitigate against malicious use of native or otherwise legitimate utilities, organizations might consider creating detections for benign utilities that are not regularly used by their users and alerting or disallowing certain users from using PowerShell or accessing resources from the command line if these are not typical or expected behaviors.

Abuse of Valid Accounts

To mitigate risk from valid account abuse, we suggest adhering to the principle of least privilege (e.g., limiting the number of accounts with administrative privileges, limiting the scope of systems in which each administrative account can use elevated permissions, and enforcing use of MFA for console, command line, and key based authentication).

Attacker Use of Cloud Services for C&C, Malware Delivery, Exfil

- Consider using blacklists, whitelists, or group policies to restrict access to unauthorized websites, such as cloud storage, from corporate devices (20-00015041).
- Use enterprise network, email, and host-based security products with up-to-date detections to prevent and detect many common malware strains.
- Enforce data loss prevention policies where available. These policies can be customized or use templates, and can apply to Exchange, OneDrive, and SharePoint; however, the policies are only available for specific Office 365 service levels (20-00005543).
- Establish and clearly communicate corporate policies regarding how to access, use, and store proprietary data to employees. If possible, these policies should be reiterated in regular trainings.

Cloud outages

We suggest that it may be beneficial for organizations to conduct tabletop exercises to simulate a major outage from a cloud provider, explore the potential fallout, and consider creating emergency plans or modifying network architecture so that the organization can maintain critical functions in the event of an outage.

Appendix: Observed Cloud Compromise TTPs with MITRE ATT&CK Labels

Technique	ID
Initial Compromise/Establish Foothold	Phishing (T1556) Phishing with Attachment (T1556.001) Phishing with Malicious Link (T1556.002) Password Spray (T1110.003) Credential Stuffing (T1110.004) Exploit a Vulnerability (T1190) Exploit a Misconfiguration (T1190) Illicit Consent Grant Supply Chain Compromise (T1195.002) Compromise on-premise network
Internal Reconnaissance/Escalate Privileges	Identify accounts with desired privileges (T1087.004) Enumerate apps, databases, etc. (T1580) Create new user and grant permissions (TA0006, T1552, T1136.003) For example, using Azure AD PowerShell, MSOnline PowerShell
Move Laterally/Maintain Presence	Golden SAML (T1552, T1199) Abuse of Federated Domains (Azure AD Backdoor) (T1550) Hijack Azure AD Applications (T1114, T1114.002, T1098.001) Use native utilities and capabilities to create new users, copy infrastructure and data, change security settings Establish persistent SSH tunnel (T1021.004)
Complete Mission	Compress Data (T1002) Exfiltrate Data to Cloud Account (T1105, T1537) Cryptomining (T1496) BEC Data Theft and Extortion Espionage Third Party Compromise Data Exposure/Doxing Data Destruction (T1485)

Table 3: Observed cloud compromise TTPs with MITRE ATT&CK labels

Please rate this product by taking a short four question survey

Threat Intelligence Tags

Actors

- APT32
  Aliases
  - APT 32
  - APT-32
  - APT32
- TEMP.Zagros
  Aliases
  - TEMP.Zagros
- APT40
  Aliases
  - APT 40
  - APT-40
  - APT40
- FIN11
  Aliases
  - FIN 11
  - FIN-11
  - FIN11

Affected Industries

- High Tech/Software/Hardware/Services
- Technology

Affected Systems

- Enterprise/Database Layer
- Third Party Services

Intended Effects

- Political Advantage
- IP or Confidential Business Information Theft
- Credential Theft/Account Takeover
- Disruption

Motivations

- Financial or Economic
- Military/Security/Diplomatic

Malware Families

- OCEANMAP
  Aliases
  - OCEANMAP
- SQUIDSLEEP
  Aliases
  - SQUIDSLEEP
- DROPDOOR
  Aliases
  - DROPDOOR
- SQUIDGATE
  Aliases
  - SQUIDGATE
- RAGNARLOCKER
  Aliases
  - RAGNARLOCKER
- AIRBREAK
  Aliases
  - AIRBREAK
- CLOP
  Aliases
  - CLOP

- NETWALKER
  Aliases
    - NETWALKER
- SODINOKIBI
  Aliases
    - SODINOKIBI
- BADFLICK
  Aliases
    - BADFLICK
- LOTUSGHOST
  Aliases
    - LOTUSGHOST
- MAZE
  Aliases
    - MAZE
- PROLOCK
  Aliases
    - PROLOCK

Source Geographies

- China
- Iran
- Russia
- Vietnam

Tactics, Techniques And Procedures (TTPs)

- Malware Propagation and Deployment
- Hosting
- Distributed Denial-of-Service (DDoS) Attack
- Ransomware
- Insider Threat
- Monetization and Laundering

Target Geographies

- Global

Targeted Information

- Credentials
- Customer Data