Muddled Libra's Evolution to the Cloud

By Margaret Kelley

Published: 2024-04-09 · Archived: 2026-04-05 19:56:39 UTC

Executive Summary

Unit 42 researchers have discovered that the Muddled Libra group now actively targets software-as-a-service (SaaS) applications and cloud service provider (CSP) environments. Organizations often store a variety of data in SaaS applications and use services from CSPs. The threat actors have begun attempting to leverage some of this data to assist with their attack progression, and to use for extortion when trying to monetize their work.

Muddled Libra also uses the legitimate scalability and native functionality of CSP services to create new resources to assist with data exfiltration. All CSPs have terms of service (TOS) policies that explicitly prohibit activities like those performed by Muddled Libra.

This article covers the following:

- Various access methodologies that are used for SaaS environments and CSPs
- Common exploits
- Data reconnaissance
- Tactics to abuse CSP services for data exfiltration

All these methods follow a detectable pattern and mitigations can be implemented based on these patterns to protect an organization. With environments evolving to use more SaaS applications and a variety of CSPs, organizations need additional protections to secure their resources and those listed below can help protect them.

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- Prisma Cloud provides detection, alerting and mitigation operations across several components within multicloud and hybrid environments.
- The Unit 42 Incident Response team can also be engaged to help with a compromise or to provide a proactive assessment to lower your risk.

Amazon Web Services (AWS) and Azure customers are protected by the threats discussed through the following services:

- Amazon GuardDuty alerts organizations to abnormal activity within their environment.
- AWS Security Hub aggregates security settings and findings from a variety of AWS services and third party tools.
- AWS IAM Access Analyzer and AWS principle of least privilege security best practices provides organizations with the tools and information to secure their identity and access management (IAM)

resources.

- Azure provides recommendations for the best ways to monitor and detect threats within the Azure platform.
- Microsoft least privileged access documentation provides information about how organizations can secure their permissions.

Access Methodology

As part of Muddled Libra's tactics evolution, they start by performing reconnaissance to identify administrative users to target for their initial access when social engineering the help desk. This development was first observed late in 2023 and we have seen activity as recent as January 2024. Muddled Libra also performs extensive research to uncover information about what applications are deployed and what CSPs an organization uses.

Figure 1 illustrates the actions that fall under the MITRE ATT&CK framework for reconnaissance. We will continue to use the framework as we discuss the tactics, techniques and procedures (TTPs) of Muddled Libra.

Figure 1. Muddled Libra's reconnaissance steps.

Muddled Libra purposefully targets administrative users during their social engineering attacks since those users have elevated permissions within identity providers, SaaS applications and organizations' various CSP environments. After initial access, the group exploits identity providers to perform privilege escalation, by bypassing IAM restrictions and modifying permission sets associated with users to increase their scope of access.

The Okta cross-tenant impersonation attacks that occurred from late July to early August 2023, where Muddled Libra bypassed IAM restrictions, display how the group exploits Okta to access SaaS applications and an organization's various CSP environments. They accessed an organization's Okta Identity Portal through technology administrator accounts that the group compromised as part of their new tactic of help desk social engineering. Then they modified permissions to increase their scope of access. By modifying permission sets of compromised users, this escalated their privileges to gain further access to SaaS applications and organization's CSP environments.

Muddled Libra also added additional identity providers with impersonation privileges, which allowed them to access additional applications while impersonating other user accounts. The Conclusion section includes recommendations for Identity Portal hardening.

Accessing SaaS Applications

After gaining access to an environment, Muddled Libra uses the information obtained during reconnaissance to perform discovery internally to find the sign-in pages for SaaS applications. Organizations using single-sign-on

(SSO) portals to manage application access (such as Okta) are of particular interest. Figure 2 maps the lateral movement techniques used by Muddled Libra.

Figure 2. Muddled Libra's lateral movement steps.

The SSO portal of a technology administrator will have an organization's security information and event management (SIEM), endpoint detection and response (EDR) and password management system (PMS) listed. These administration tools are all of interest to the attackers because they can execute permission modification and identity provider configuration changes. SSO portals also allow them to quickly iterate through applications to find those that would benefit their campaign.

The SaaS Application Exploits section below expands on this activity.

Accessing an Organization's Cloud Service Provider Environments

How attackers access organizations' different CSP environments depends on their unique configurations. The Muddled Libra group takes advantage of any authentication method to gain access to an organization's cloud network, most commonly organizations' AWS and Azure environments.

Similar to the activity we described with attackers accessing SaaS applications, if SSO is integrated to an organization's CSP, attackers use this functionality to gain access to those CSP environments. If SSO is not configured, the group performs discovery across an organization's environment, to uncover CSP credentials stored in unsecured locations due to an organization's poor technology hygiene.

SaaS Application Exploits

When reviewing common SaaS application exploits, attacker activity falls under three categories:

- Finding relevant data
- Locating credentials
- Modifying SaaS application configuration

Figure 3 fits these activities under discovery in the MITRE ATT&CK framework.

Figure 3. Muddled Libra's discovery techniques using SaaS.

Depending on the type of SaaS application, the data within the application might be more beneficial for use by threat actors in traditional data exfiltration or for learning about a target's environment configuration. Historically, Muddled Libra looks for data that falls under either of these classifications within any SaaS application they compromise. They also make a large effort to search for other credentials within a SaaS application.

Sensitive credentials can be exposed in logs, as well as within PMS applications and SaaS applications that scan for sensitive information. Muddled Libra methodically searches for applications that might store this type of valuable information to then use later on in their attacks for privilege escalation and lateral movement.

Microsoft provides a wide range of services and tools that become key targets during an attack due to their high value to both organizations and threat actors. An example of how Muddled Libra takes advantage of a SaaS application is how the group exploits Microsoft SharePoint.

The SharePoint platform is used by organizations to store files that document network topology, as well as what tools an organization uses and other general information. Muddled Libra targets this platform to gain a better understanding of the network configuration within a company and which tools they can exploit, such as remote access tools.

As with any file storage tool, other sensitive information (such as passwords) can also get leaked from these documents. Also, within the Microsoft 365 (M365) suite, the group targets email boxes and other email functionality to gain access to sensitive data.

CSP Reconnaissance and Gathering Intel

A large portion of Muddled Libra's campaigns involve gathering intelligence and data. Attackers then use this to generate new vectors for lateral movement within an environment. Organizations store a variety of data within their unique CSP environments, thus making these centralized locations a prime target for Muddled Libra. Figure 4 itemizes these discovery tactics.

Figure 4. Muddled Libra's discovery techniques using AWS.

AWS Intel Gathering

Muddled Libra targets a wide range of services within an organization's AWS environment to gather more intel for use later on in the attack. These services include AWS IAM, Amazon Simple Storage Service (S3) and AWS Secrets Manager.

The IAM service provides the following information:

- Which users exist within the AWS account
- Access keys associated with users
- What identity provider connections exist

Some AWS IAM API calls that can be used for reconnaissance include:

- ListUsers
- ListGroups
- ListRoles
- ListSSHPublicKeys
- ListServiceSpecificCredentials
- ListSigningCertificates
- ListOpenIDConnectProviders
- ListSAMLProviders

The first three – listing users, groups and roles – provide the threat actors with high-level information about user groups and what unique roles an organization has created to meet their business needs. The rest of the API calls return information about the following:

- SSH public keys
- Service credentials
- Certificates
- Various identity providers

The threat actor group wants to learn about these things to broaden their understanding of the environment configuration for the next stages of their attack. None of these API calls return sensitive information associated with the various credentials.

S3 buckets, which are an AWS object level storage service, can contain any sort of data depending on an organization. Because of this, Muddled Libra spends time listing available buckets and then reviewing bucket data more closely depending on the relevance of the bucket names. Some reconnaissance AWS S3 API calls include ListBuckets and various GetBucket* operations.

Secrets Manager can store sensitive secrets, so this service is especially interesting for the group to use for lateral movement to other applications within the environment. While native cloud credentials cannot be discovered or enumerated using cloud APIs, legacy technologies such as SQL databases running within a cloud environment typically require credentials such as usernames and passwords. Secrets Manager is designed to store such secrets, and also has features for automatically rotating them periodically.

Some reconnaissance AWS Secrets Manager API calls include:

- ListSecrets
- DescribeSecret
- GetSecretValue

The GetSecretValue event specifically returns the data stored within a secret. This helps the group move laterally to other applications if the secret contains credentials.

Azure Intel Gathering

To collect sensitive data and network configuration details within Azure, Muddled Libra focuses on storage account access keys and resource groups. Storage account access keys provide access to an Azure storage account, allowing Muddled Libra to iterate through resources such as Azure Blob Storage and Azure Files to locate the most valuable data relevant to their attack.

Both Azure Blob and Azure Files provide organizations with unique storage offerings built for a variety of data types. Figure 5 highlights the group's discovery tactics using Azure.

Figure 5. Muddled Libra's discovery techniques using Azure.

Azure resource groups are logical containers used to batch resources together. By simply learning the names of the various resource groups, threat actors can figure out which resource groups contain the most valuable virtual machines (VMs) that might contain sensitive data. The Figure 6 diagram shows what these resource groups potentially encompass that might be of interest to the threat actors.

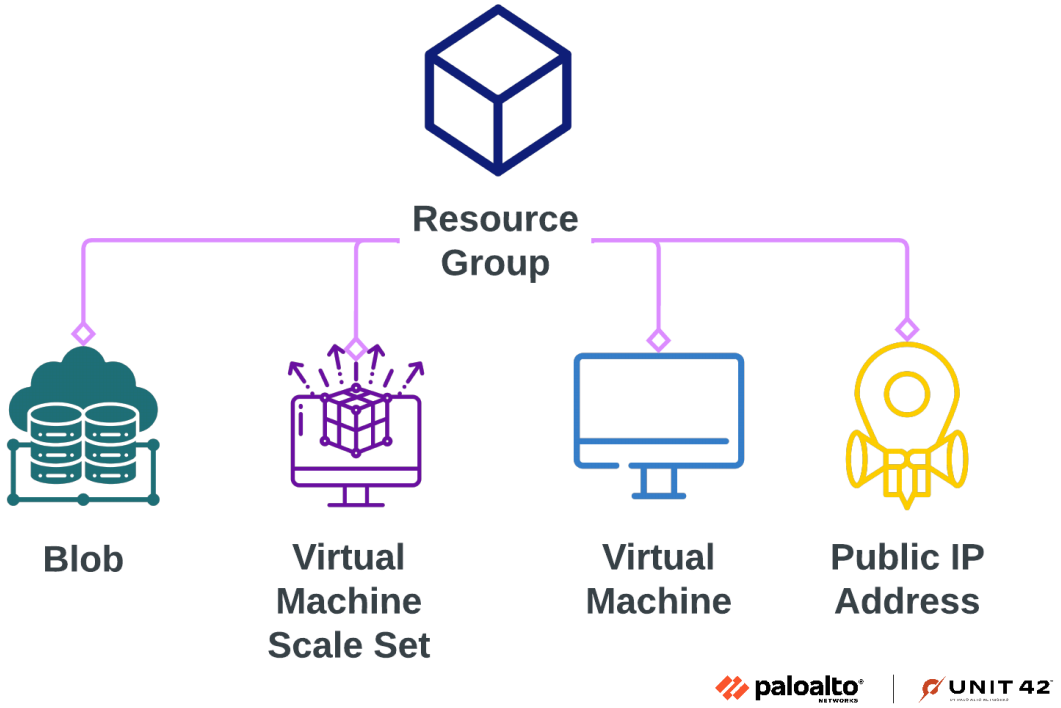

Figure 6. Resource group with various attacker targets.

CSP Data Exfiltration Techniques

Muddled Libra leverages legitimate CSP services and features to more quickly and efficiently exfiltrate data. These components exist for organizations to better manage their workloads and simplify their processes, but as with many tools, threat actors can use those same services to accomplish their malicious goals.

AWS Exfiltration Techniques

When it comes to exfiltrating data from an organization's AWS environment, Muddled Libra targets two legitimate AWS services to quickly move data. Muddled Libra uses both the AWS DataSync and AWS Transfer services, to transfer data from an on-premises environment to the cloud and then from the cloud to an external entity.

AWS DataSync enables the transfer of data from on-premises to various AWS storage services. The AWS Transfer service enables data transfer to and from various AWS storage services. Figure 7 highlights these exfiltration tactics.

Figure 7. Muddled Libra's exfiltration techniques using AWS.

By using these services in tandem, Muddled Libra can move data very quickly out of an environment. When a new AWS Transfer server gets created, the following AWS API events appear in the CloudTrail logs:

- CreateServer
- CreateUser

An AWS Transfer user is specifically created as part of the host creation, so the CreateUser event is associated with transfer.amazonaws.com as the event source. To protect against this activity, organizations can use the AWS IAM Access Analyzer to gauge the permissiveness of resources and lock down credentials to follow the principle of least privilege. In addition to limiting IAM permissions, organizations can use AWS Service Control Policies (SCP) to completely block services an organization doesn't use such as DataSync or AWS Transfer, regardless of the permissions associated with a principal.

Azure Exfiltration Techniques

One method of data exfiltration threat actors use in Azure exploits traditional VM functionality known as snapshots to take images of hosts that contain sensitive information pertinent to Muddled Libra's attack objectives. Snapshots allow users to take a point-in-time image of a virtual hard disk (VHD).

CSPs have restrictions in place regarding sharing snapshot resources with external entities. Muddled Libra avoids this by creating new VMs within the compromised environment and then saving the relevant operational data from the snapshots to the newly created hosts for staging before exfiltrating the data. Figure 8 lists these collection and exfiltration techniques.

Figure 8. Muddled Libra's collection and exfiltration techniques using Azure.

Once the data exists on the newly created VMs, threat actors can exfiltrate the data via traditional network exfiltration techniques.

Conclusion

By expanding their tactics to include SaaS applications and cloud environments, the evolution of Muddled Libra's methodology shows the multidimensionality of cyberattacks in the modern threat landscape. The use of cloud environments to gather large amounts of information and quickly exfiltrate it poses new challenges to defenders. Figure 9 displays the full attack chain used by Muddled Libra when targeting SaaS applications and organizations' CSP environments.

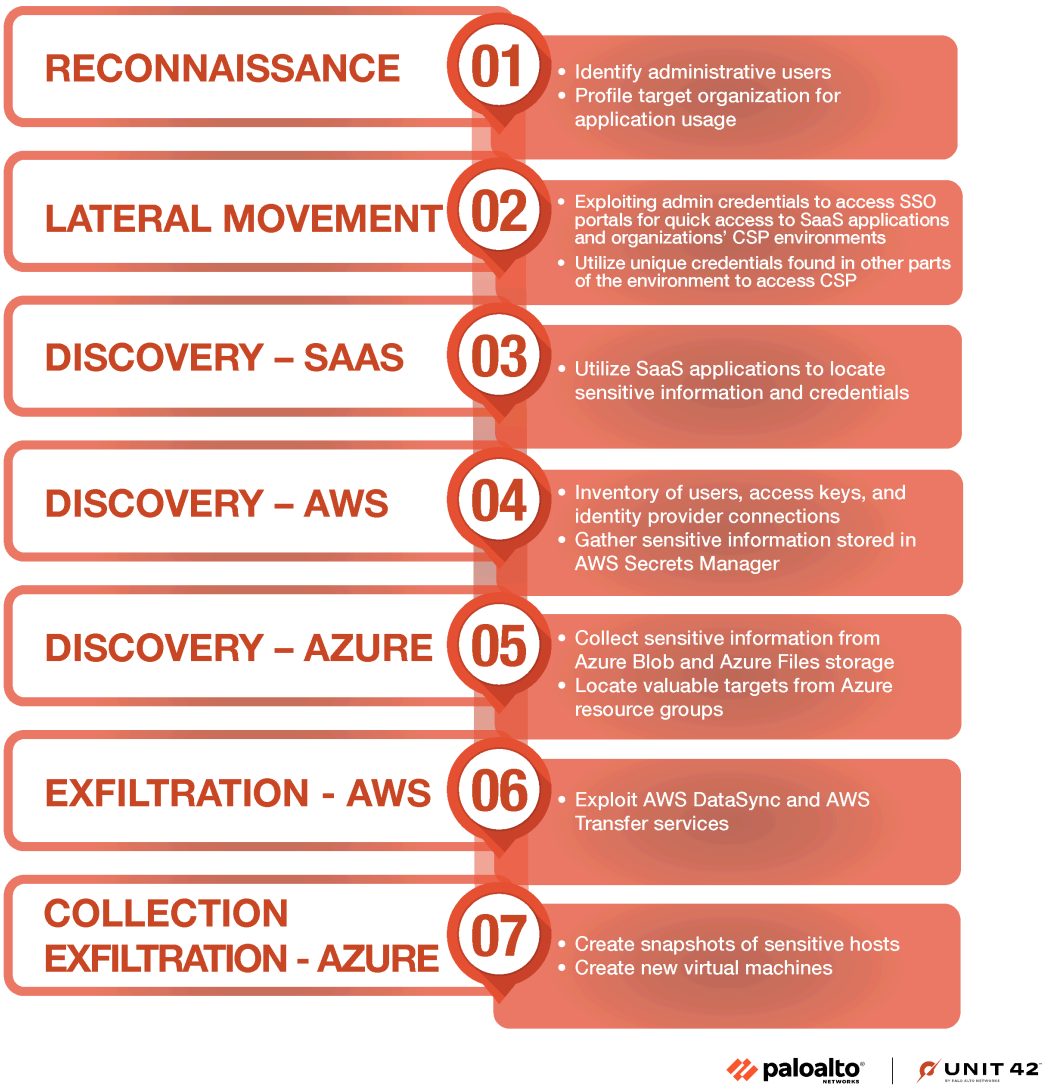

Figure 9. Muddled Libra attack chain in the cloud.

Identity Portals provide a great starting point for centralizing credential management, reducing administrative overhead and improving the end-user experience, but this also makes them prime targets for attackers. These platforms must be protected with robust and difficult-to-bypass secondary authentication factors such as hardware tokens or biometrics, and they should be closely monitored for unusual activity.

To protect CSP identities, defenders can use AWS IAM roles and Microsoft Entra Privileged Identity Management (PIM) to limit the long-term access attackers can gain, forcing attackers to reauthenticate more often. This limitation adds another layer of complexity to the threat actor's attack, and the reauthentication process creates more abnormal, detectable events for defenders.

Despite Muddled Libra's constantly changing attack tactics, defenders can build better protections by understanding the end goal of these threat actors to then implement and improve technology protections to safeguard environments.

Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from the threats discussed above through Prisma Cloud, which provides detection, alerting and mitigation operations across several components within multicloud and hybrid environments.

If you think you might have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.
