JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-046A

February 15, 2024

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Threat Actor Leverages Compromised Account of Former Employee to Access State Government Organization

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing & Analysis Center (MS-ISAC) conducted an incident response assessment of a state government organization's network environment after documents containing host and user information, including metadata, were posted on a dark web brokerage site. Analysis confirmed that an unidentified threat actor compromised network administrator credentials through the account of a former employee—a technique commonly leveraged by threat actors—to successfully authenticate to an internal virtual private network (VPN) access point, further navigate the victim's on-premises environment, and execute various lightweight directory access protocol (LDAP) queries against a domain controller.[1] Analysis also focused on the victim's Azure environment, which hosts sensitive systems and data, as well as the compromised on-premises environment. Analysis determined there were no indications the threat actor further compromised the organization by moving laterally from the on-premises environment to the Azure environment.

CISA and MS-ISAC are releasing this Cybersecurity Advisory (CSA) to provide network defenders with the tactics, techniques, and procedures (TTPs) used by the threat actor and methods to protect

Actions to take today to mitigate malicious cyber activity:

- Continuously remove and disable accounts and groups from the enterprise that are no longer needed, especially privileged accounts.
- Enable and enforce multifactor authentication with strong passwords.
- Store credentials in a secure manner, such as with a credential manager, vault, or other privilege account management solution.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. SLTT organizations should report incidents to the MS-ISAC (866-787-4722 or SOC@cisecurity.org).

against similar exploitation of both unnecessary and privileged accounts.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 14. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actor's activity mapped to MITRE ATT&CK® tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Overview

A state government organization was notified that documents containing host and user information, including metadata, were posted on a dark web brokerage site. After further investigation, the victim organization determined that the documents were accessed via the compromised account of a former employee. Threat actors commonly leverage valid accounts, including accounts of former employees that have not been properly removed from the Active Directory (AD), to gain access to organizations.[1] CISA and MS-ISAC assessed that an unidentified threat actor likely accessed documents containing host and user information to post on the dark web for profit after gaining access through the account of a former employee.

The scope of this investigation included the victim organization's on-premises environment, as well as their Azure environment, which hosts sensitive systems and data. Analysis determined the threat actor did not move laterally from the compromised on-premises network to the Azure environment and did not compromise sensitive systems.

Untitled Goose Tool

Incident responders collected Azure and Microsoft Defender for Endpoint (MDE) logs using CISA's Untitled Goose Tool—a free tool to help network defenders detect potentially malicious activity in Microsoft Azure, Azure Active Directory (AAD), and Microsoft 365 (M365) environments. CISA developed the Untitled Goose Tool to export and review AAD sign-in and audit logs, M365 unified audit logs (UAL), Azure activity logs, and MDE data. By exporting cloud artifacts, Untitled Goose Tool supports incident response teams with environments that do not ingest logs into a security information and event management (SIEM) tool.

Threat Actor Activity

The logs revealed the threat actor first connected from an unknown virtual machine (VM) to the victim's on-premises environment via internet protocol (IP) addresses within their internal VPN range. CISA and MS-ISAC assessed that the threat actor connected to the VM through the victim's VPN [T1133] with the intent to blend in with legitimate traffic to evade detection.

Initial Access: Compromised Domain Accounts

USER1: The threat actor gained initial access through the compromised account of a former employee with administrative privileges (`USER1`) [T1078.002] to conduct reconnaissance and

discovery activities. The victim organization confirmed that this account was not disabled immediately following the employee's departure.

- The threat actor likely obtained the `USER1` account credentials in a separate data breach due to the credentials appearing in publicly available channels containing leaked account information [T1589.001].
- `USER1` had access to two virtualized servers including SharePoint and the workstation of the former employee. The workstation was virtualized from a physical workstation using the Veeam Physical to Virtual (P2V) function within the backup software.

USER2: The threat actor likely obtained the `USER2` account credentials from the virtualized SharePoint server managed by `USER1` [T1213.002]. The victim confirmed that the administrator credentials for `USER2` were stored locally on this server [T1552.001].

- Through connection from the VM, the threat actor authenticated to multiple services [T1021] via the `USER1` account, as well as from an additional compromised global domain administrator account (`USER2`) [T1078.002].
- The threat actor's use of the `USER2` account was impactful due to the access it granted to both the on-premises AD and Azure AD [T1021.007], thus enabling administrative privileges [T1078.004].

Following notification of the dark web posting, the victim organization immediately disabled the `USER1` account and took the two virtualized servers associated with the former employee offline. The victim also changed the password for the `USER2` account and removed administrator privileges. Neither of the administrative accounts had multifactor authentication (MFA) enabled.

LDAP Queries

Through connection from the VM, the threat actor conducted LDAP queries of the AD, likely using the open source tool `AdFind.exe`, based on the format of the output. CISA and MS-ISAC assess the threat actor executed the LDAP queries [T1087.002] to collect user, host [T1018], and trust relationship information [T1482]. It is also believed the LDAP queries generated the text files the threat actor posted for sale on the dark web brokerage site: `ad_users.txt`, `ad_computers.txt`, and `trustdmp.txt`.

Table 1 lists all queries that were conducted between 08:39:43-08:40:56 Coordinated Universal Time (UTC).

Table 1: LDAP Queries Conducted by the Threat Actor

Query	Description
LDAP Search Scope: WholeSubtree, Base Object: dc=[REDACTED],dc=local, Search Filter: (objectCategory=CN=Person,CN=Schema,CN=Configuration,DC=[REDACTED],DC=local)	Collects names and metadata of users in the domain.

Query	Description
LDAP Search Scope: WholeSubtree, Base Object: dc=[REDACTED],dc=local, Search Filter: (objectCategory=CN=Computer,CN=Schema,CN=Configuration,DC=[REDACTED],DC=local)	Collects names and metadata of hosts in the domain.
LDAP Search Scope: WholeSubtree, Base Object: dc=[REDACTED],dc=local, Search Filter: (objectCategory=CN=Trusted-Domain,CN=Schema,CN=Configuration,DC=[REDACTED],DC=local)	Collects trust information in the domain.
LDAP Search Scope: WholeSubtree, Base Object: DC=[REDACTED],DC=local, Search Filter: (& (& (sAMAccountType=805306368) (servicePrincipalName=*) (! (sAMAccountName=krbtgt)) (! (userAccountControl&2))) (adminCount=1))	Collects Domain Administrators and Service Principals in the domain.

Service Authentication

Through the VM connection, the threat actor was observed authenticating to various services on the victim organization's network from the `USER1` and `USER2` administrative accounts. In all instances, the threat actor authenticated to the Common Internet File Service (CIFS) on various endpoints [T1078.002],[T1021.002]—a protocol used for providing shared access to files and printers between machines on the network. This was likely used for file, folder, and directory discovery [T1083], and assessed to be executed in an automated manner.

- `USER1` authenticated to four services, presumably for the purpose of network and service discovery [T1046].
- `USER2` authenticated to twelve services. **Note:** This account had administrative privileges to both the on-premises network and Azure tenant.

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 2-9 for all referenced threat actor's tactics and techniques for enterprise environments in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Table 2: Reconnaissance

Technique Title	ID	Use
Gather Victim Identity Information: Credentials	T1589.001	The actor likely gathered `USER1` account credentials in a data breach where account information appeared in publicly available channels.

Table 3: Initial Access

Technique Title	ID	Use
Valid Accounts: Domain Accounts	T1078.002	The actor gained initial access through the compromised account of a former employee with administrative privileges (USER1). The employee's account was not immediately disabled after their departure.

Table 4: Persistence

Technique Title	ID	Use
External Remote Services	T1133	The actor connected a VM via the victim's VPN to blend in with legitimate traffic to evade detection.

Table 5: Privilege Escalation

Technique Title	ID	Use
Valid Accounts: Domain Accounts	T1078.002	The actor authenticated to multiple services from a compromised Global Domain Administrator account (USER2). The actor also authenticated to the Common Internet File Service (CIFS) on various endpoints.
Valid Accounts: Cloud Accounts	T1078.004	The actor used a compromised account (USER2) which was synced to both the on-premises AD and Azure AD, thus enabling administrative privileges to both the on-premises network and Azure tenant.

Table 6: Credential Access

Technique Title	ID	Use
Unsecured Credentials: Credentials in Files	T1552.001	The actor likely obtained USER2 account credentials from the virtualized SharePoint server where they were locally stored.

Table 7: Discovery

Technique Title	ID	Use
Account Discovery: Domain Account	T1087.002	Through the VM connection, the actor executed LDAP queries of the AD.

Technique Title	ID	Use
Remote System Discovery	T1018	Through the VM connection, the actor executed LDAP queries to collect user and host information.
Domain Trust Discovery	T1482	Through the VM connection, the actor executed LDAP queries to collect trust relationship information.
File and Directory Discovery	T1083	The actor authenticated to the CIFS on various endpoints likely for the purpose of file, folder, and directory discovery.
Network Service Discovery	T1046	The actor used the compromised `USER1` account to authenticate to four services, presumably for the purpose of network and service discovery.

Table 8: Lateral Movement

Technique Title	ID	Use
Remote Services	T1021	The actor connected from an unknown VM and authenticated to multiple services via the `USER1` account.
Remote Services: Cloud Services	T1021.007	The actor used the `USER2` account, which granted access to the Azure AD, as well as the on-premises AD.
Remote Services: SMB/Windows Admin Shares	T1021.002	The actor used compromised accounts to interact with a remote network share using Server Message Block.

Table 9: Collection

Technique Title	ID	Use
Data from Information Repositories: SharePoint	T1213.002	The actor likely obtained the `USER2` account credentials from the virtualized SharePoint server managed by `USER1`.

MITIGATIONS

Note: These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST), which apply to all critical infrastructure organizations and network defenders. The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector

Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

Secure and Monitor Administrator Accounts

The threat actor gained access to the network via compromised administrator accounts that did not have MFA enabled. The compromised USER2 Global Domain Administrator account could have enabled the threat actor to move laterally from the on-premises environment to the Azure tenant. In response to the incident, the victim organization removed administrator privileges for USER2. Additionally, the victim organization disabled unnecessary administrator accounts and enabled MFA for all administrator accounts. To prevent similar compromises, CISA and MS-ISAC recommend the following:

- **Review current administrator accounts** to determine their necessity and only maintain administrator accounts that are essential for network management. This will reduce the attack surface and focus efforts on the security and monitoring of necessary accounts.
- **Restrict the use of multiple administrator accounts** for one user.
- **Create separate administrator accounts** for on-premises and Azure environments to segment access.
- **Implement the principle of least privilege** to decrease threat actor's ability to access key network resources. Enable just-in-time and just enough access for administrator accounts to elevate the minimum necessary privileges for a limited time to complete tasks.
- **Use phishing-resistant multifactor authentication (MFA)** [CPG 2.H] (e.g., security tokens) for remote access and access to any sensitive data repositories. Implement phishing-resistant MFA for as many services as possible—particularly for webmail and VPNs—for accounts that access critical systems and privileged accounts that manage backups. MFA should also be used for remote logins [M1032]. For additional guidance on secure MFA configurations, visit CISA's More than a Password webpage and read CISA's Implementing Phishing-Resistant MFA fact sheet.

Reduce Attack Surface

Unnecessary accounts, software, and services in the network create additional vectors for a threat actor to compromise. CISA and MS-ISAC recommend the following:

- **Establish policy and procedure for the prompt removal of unnecessary accounts and groups** from the enterprise, especially privileged accounts. Organizations should implement a robust and continuous user management process to ensure accounts of offboarded employees are removed and can no longer access the network.
- **Maintain a robust asset management policy** through comprehensive documentation of assets, tracking current version information to maintain awareness of outdated software, and mapping assets to business and critical functions.
  - Determine the need and functionality of assets that require public internet exposure [CPG 1.A].

- **Follow a routine patching cycle** for all operating systems, applications, and software (including all third-party software) to mitigate the potential for exploitation.
- **Restrict personal devices from connecting to the network**. Personal devices are not subject to the same group policies and security measures as domain joined devices.

Evaluate Tenant Settings

By default, in Azure AD all users can register and manage all aspects of applications they create. Users can also determine and approve what organizational data and services the application can access. These default settings can enable a threat actor to access sensitive information and move laterally in the network. In addition, users who create an Azure AD automatically become the Global Administrator for that tenant. This could allow a threat actor to escalate privileges to execute malicious actions. CISA and MS-ISAC recommend the following:

- **Evaluate current user permissions** in the Azure tenant to restrict potentially harmful permissions including:
  - Restrict users' ability to register applications. By default, all users in Azure AD can register and manage the applications they create and approve the data and services the application can access. If this is exploited, a threat actor can access sensitive information and move laterally in the network.
  - Restrict non-administrators from creating tenants. Any user who creates an Azure AD automatically becomes the Global Administrator for that tenant. This creates an opportunity for a threat actor to escalate privileges to the highest privileged account.
  - Restrict access to the Azure AD portal to administrators only. Users without administrative privileges cannot change settings, however, they can view user info, group info, device details, and user privileges. This would allow a threat actor to gather valuable information for malicious activities.

Create a Forensically Ready Organization

- **Collect access- and security-focused logs** (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, and virtual private network) for use in both detection and incident response activities [CPG 2.T].
- **Enable complete coverage of tools**, including Endpoint Detection and Response (EDR), across the environment for thorough analysis of anomalous activity and remediation of potential vulnerabilities.

Assess Security Configuration of Azure Environment

CISA created the Secure Cloud and Business Applications (SCuBA) assessment tool to help Federal Civilian Executive Branch (FCEB) agencies to verify that a M365 tenant configuration conforms to a minimal viable secure configuration baseline. Although the SCuBA assessment tool was developed for FCEB, other organizations can benefit from its output. CISA and MS-ISAC recommend the following:

- **Use tools that identify attack paths**. This will enable defenders to identify common attack paths used by threat actors and shut them down before they are exploited.
- **Review the security recommendations list provided by Microsoft 365 Defender**. Focus remediation on critical vulnerabilities on endpoints that are essential to mission execution and contain sensitive data.

Evaluate Conditional Access Policies

Conditional access policies require users who want to access a resource to complete an action. Conditional access policies also account for common signals, such as user or group memberships, IP location information, device, application, and risky sign-in behavior identified through integration with Azure AD Identity Protection.

- **Review current conditional access policies** to determine if changes are necessary.

Reset All Passwords and Establish Secure Password Policies

In response to the incident, the victim organization reset passwords for all users.

- **Employ strong password management** alongside other attribute-based information, such as device information, time of access, user history, and geolocation data. Set a password policy to require complex passwords for all users (minimum of 16 characters) and enforce this new requirement as user passwords expire [CPG 2.A],[CPG 2.B],[CPG 2.C].
- **Store credentials in a secure manner,** such as with a credential manager, vault, or other privileged account management solution [CPG 2.L].
- **For products that come with default passwords,** ask vendors how they plan to eliminate default passwords, as highlighted in CISA's Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords.

Mitigations for Vendors

CISA recommends that vendors incorporate secure by design principles and tactics into their practices, limiting the impact of threat actor techniques and strengthening the secure posture for their customers.

- **Prioritize secure by default configurations,** such as eliminating default passwords and providing high-quality audit logs to customers with no additional configuration, at no extra charge. Secure by default configurations should be prioritized to eliminate the need for customer implementation of hardening guidance.
- **Immediately identify, mitigate, and update affected products** that are not patched in accordance with CISA's Known Exploited Vulnerabilities (KEV) catalog.
- **Implement multifactor authentication (MFA),** ideally phishing-resistant MFA, as a default (rather than opt-in) feature for all products.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA and MS-ISAC recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for

Enterprise framework in this advisory. CISA recommends testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see table 2-9).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA and MS-ISAC recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- MS-ISAC: Center for Internet Security (CIS) Cyber-Attack Defense: CIS Benchmarks + CDM + MITRE ATT&CK

REFERENCES

[1] CISA Analysis: Fiscal Year 2022 Risk and Vulnerability Assessments

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA and MS-ISAC do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA or MS-ISAC.

VERSION HISTORY

February 15, 2024: Initial version.