MERCURY and DEV-1084: Destructive attack on hybrid environment | Microsoft Security Blog

By Microsoft Threat Intelligence

Published: 2023-04-07 · Archived: 2026-04-05 17:21:34 UTC

April 2023 update – Microsoft Threat Intelligence has shifted to a new threat actor naming taxonomy aligned around the theme of weather. **MERCURY** is now tracked as **Mango Sandstorm** and **DEV-1084** is now tracked as **Storm-1084**.

To learn more about the new taxonomy represents the origin, unique traits, and impact of threat actors, to get complete mapping of threat actor names, read this blog: **Microsoft shifts to a new threat actor naming taxonomy**.

Microsoft Threat Intelligence has detected destructive operations enabled by MERCURY, a nation-state actor linked to the Iranian government, that attacked both on-premises and cloud environments. While the threat actors attempted to masquerade the activity as a standard ransomware campaign, the unrecoverable actions show destruction and disruption were the ultimate goals of the operation.

Previous MERCURY attacks have been observed targeting on-premises environments, however, the impact in this case notably also included destruction of cloud resources. Microsoft assesses that MERCURY likely worked in partnership with another actor that Microsoft tracks as DEV-1084, who carried out the destructive actions after MERCURY's successful operations had gained access to the target environment.

MERCURY likely exploited known vulnerabilities in unpatched applications for initial access before handing off access to DEV-1084 to perform extensive reconnaissance and discovery, establish persistence, and move laterally throughout the network, oftentimes waiting weeks and sometimes months before progressing to the next stage. DEV-1084 was then later observed leveraging highly privileged compromised credentials to perform en masse destruction of resources, including server farms, virtual machines, storage accounts, and virtual networks, and send emails to internal and external recipients.

In this blog post, we detail our analysis of the observed actor activity and related tools. We also share information to the community and industry partners on ways to detect these attacks, including detection details of MERCURY and DEV-1084's tools in Microsoft 365 Defender, Microsoft Defender for Identity, Microsoft Defender for Cloud Applications, Microsoft Defender Antivirus, and Microsoft Defender for Endpoint. As with any observed nation-state actor activity, Microsoft has directly notified targeted or compromised customers, providing them with important information needed to secure their environments.

Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or a developing cluster of threat activity, allowing Microsoft to track it as a unique set of information until we reach high confidence about the origin or identity of the actor behind the activity.

Who is DEV-1084?

Microsoft tracks the destructive actions documented in this blog post as DEV-1084. DEV-1084 likely worked in partnership with MERCURY—an Iran-based actor that the US Cyber Command has publicly linked to Iran's Ministry of

Intelligence and Security (MOIS). DEV-1084 publicly adopted the DarkBit persona and presented itself as a criminal actor interested in extortion, likely as an attempt to obfuscate Iran's link to and strategic motivation for the attack.

The link between the DEV-1084 cluster and MERCURY was established based on the following evidence:

- DEV-1084 operators were observed sending threatening emails from 146.70.106[.]89, an IP address previously linked to MERCURY.
- DEV-1084 used MULLVAD VPN, the same VPN provider historically used by MERCURY.
- DEV-1084 used Rport and a customized version of Ligolo. MERCURY has also been observed using Rport and a similar version of Ligolo in previous attacks.
- DEV-1084 used the *vatacloud[.]com* domain for command and control (C2) during this incident. Microsoft assesses with high-confidence that the *vatacloud[.]com* domain is controlled by MERCURY operators.

Microsoft assesses that MERCURY gains access to the targets through remote exploitation of an unpatched internet-facing device. MERCURY then handed off access to DEV-1084. It is not currently clear if DEV-1084 operates independently of MERCURY and works with other Iranian actors or if DEV-1084 is an 'effects based' sub-team of MERCURY that only surfaces when MERCURY operators are instructed to carry out a destructive attack.

Microsoft assesses with moderate confidence that the threat actors attempted several times and succeeded to perform initial intrusion leveraging exposed vulnerable applications, for example, continuing to exploit Log4j 2 vulnerabilities in unpatched systems in July 2022.

After gaining access, the threat actors deploy several tools and leverage techniques to maintain persistence, which provide effective and continued access to compromised devices, such as the following:

- Installing web shells
- Adding a local user account and elevating privileges to local administrator
- Installing legitimate remote access tools, such as RPort, Ligolo and eHorus
- Installing a customized PowerShell script backdoor
- Stealing credentials

Once the persistence is established, the threat actors perform extensive discovery leveraging common native Windows tools and commands such as *netstat* and *nltest*. Such reconnaissance activities were seen leveraged throughout the attack chain.

The threat actors consistently perform extensive lateral movement actions using the acquired credentials within a targeted environment. These actions mainly involved:

- Remote scheduled tasks to launch their customized PowerShell backdoor
- Windows Management Instrumentation (WMI) to launch commands on devices
- Remote services to run encoded PowerShell commands

After infecting the new devices, the threat actors often installed the same persistence mechanisms as described above. Interestingly, after each main attack step, the actors did not always immediately continue their operations but would wait weeks and sometimes months before moving to the next step.

For execution and communication, the threat actors leverage several C2 servers and sometimes deploy tunnelling tools, such as Ligolo and OpenSSH, commonly leveraged to stay under the radar of security teams and solutions.

On-premises destructive impact

In observed activity, the threat actors leveraged highly privileged credentials and access to domain controllers on on-premises destructive operations to prepare for large-scale encryption of targeted devices.

To do so, they first interfered with security tools using Group Policy Objects (GPO). With defenses impaired, the threat actors proceeded to stage the ransomware payload in the NETLOGON shares on several domain controllers.

GPO was leveraged again to register a scheduled task used to launch the ransomware payload. Finally, the ransomware payload encrypted files found on the file system of the targeted devices by changing the file name extension to *DARKBIT* and dropped ransom notes.

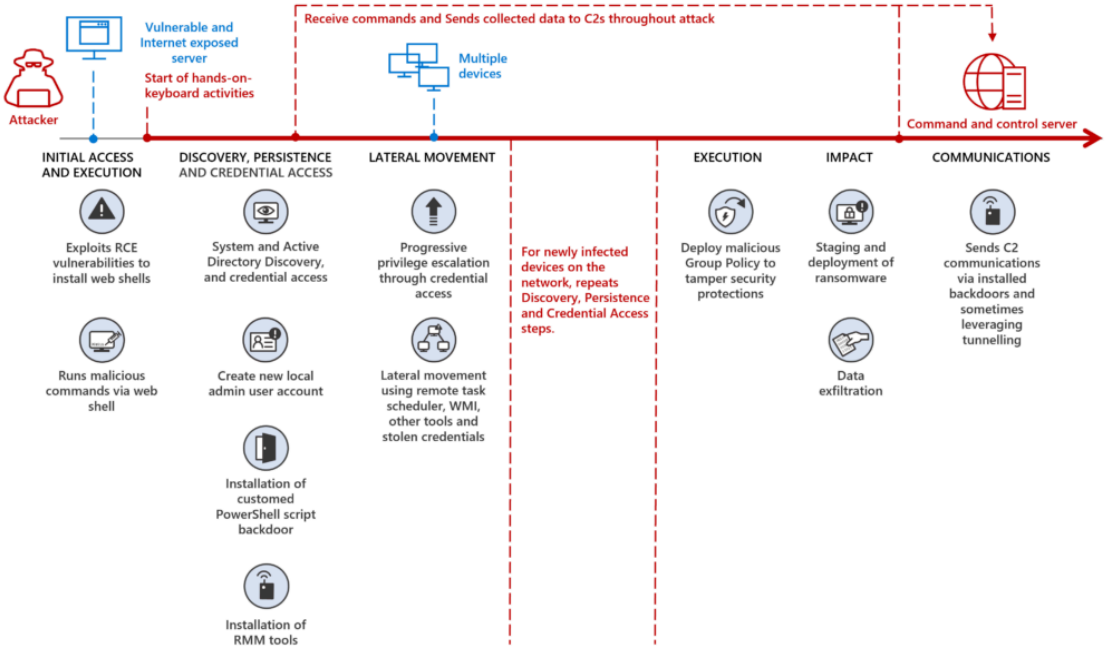

Figure 1. On-premises attack flow

Moving from on-premises to cloud

To move from on-premises to the cloud, the threat actors had to first compromise two privileged accounts and leverage them to manipulate the Azure Active Directory (Azure AD) Connect agent. Two weeks before the ransomware deployment, the threat actors first used a compromised, highly privileged account to access the device where the Azure Active Directory (Azure AD) Connect agent is installed. We assess with high confidence that the threat actors then used the AADInternals tool to extract the plaintext credentials of a privileged Azure AD account. The threat actors then used these credentials to pivot from the on-premises environment to the Azure AD environment.

Azure AD Connect is an on-premises application for managing hybrid identities through features like password hash synchronization, pass-through authentication, objects synchronization, and others. As part of the express settings installation process, multiple accounts are created both in the on-premises (Windows Server Active Directory) and cloud (Azure AD) environments. The first account is the AD DS Connector Account. The account name is prefixed with *MSOL_* and it is created with a long complex password.

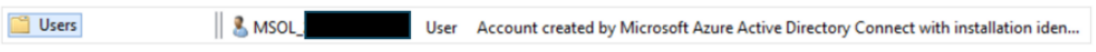

Figure 2. Example of AD DS Connector account

This account's permissions are set based on features enabled during the service's installation, but in most common scenarios, the account has permissions to replicate directory changes, modify passwords, modify users, modify groups, and so on (see all the permissions here). In addition, during installation, an Azure AD account called the Azure AD Connector Account is also created. This account is used by the synchronization service to manage Azure AD objects. The account is created with a long complex password as well, and by default (if using the express settings) prefixed with *Sync_[ServerName]*. This user is assigned with the Directory Synchronization Accounts role (see detailed permissions of this role here). In older versions, this account might be assigned with the Global Administrator role.

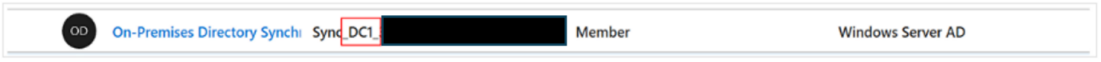

Figure 3. Example of an Azure AD Connector account

There are other entities detailed here that are created but are less relevant to this topic.

Two weeks before the ransomware deployment, the threat actors were observed using compromised credentials to access the Azure AD Connect device. Next, they set up an SSH tunnel to an attacker-controlled device. On a separate attacker-controlled compromised device, evidence indicates cloning of the AADInternals tool. One of the functions available in this tool's library is *Get-AADIntSyncCredentials*, which allows any local administrator on a device where Azure AD Connect is installed to extract the plaintext credentials of both the Azure AD Connector account and the AD DS Connector account.

Shortly before the ransomware deployment, we observed authentication from a known attacker IP address into the Azure AD Connector cloud account. Investigating this sign-in showed that the threat actors were able to access the account on the first attempt without any guessing or modification of the password, indicating that the actors possessed the password for this account. The Azure AD Connector account is configured with single-factor authentication, making it easier for the attacker to gain entry and elevate privileges.

Cloud destructive impact

On the day of the ransomware attack, the threat actors executed multiple actions in the cloud using two privileged accounts. The first account was the compromised Azure AD Connector account, which had Global Administrator permissions as it was set up for an old solution (DirSync). For the second account, which also had Global Administrator permissions, the threat actors leveraged RDP for access into the account. Even though this account had MFA in place, the threat actors accessed it through RDP, which is an open session that evades MFA blocking their activities.

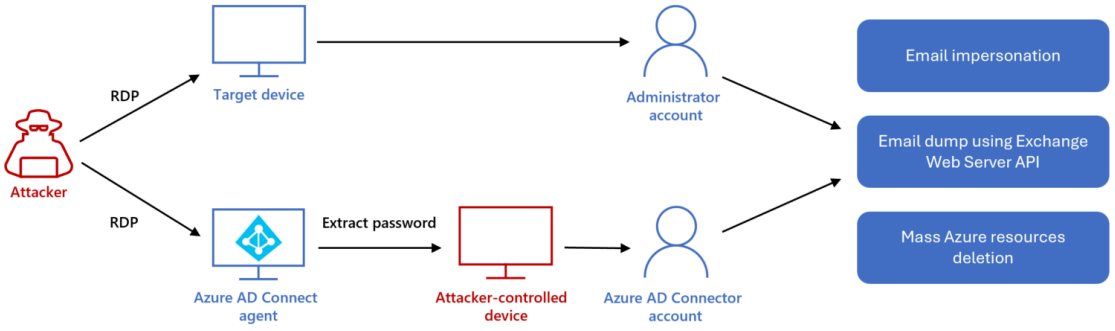

Figure 4. Pivoting to the cloud

Mass Azure resource deletion

On the same day, a successful sign-in to the Microsoft Azure environment was observed. The threat actors claimed the Global Administrator permission through Azure Privileged Identity Management (PIM) and elevated access to get permissions to the target's management groups and Azure subscriptions. The Azure AD Connector account and the compromised administrator account were then used to perform significant destruction of the Azure environment—deleting within a few hours server farms, virtual machines, storage accounts, and virtual networks. We assess that the attacker's goal was to cause data loss and a denial of service (DoS) of the target's services.

Exchange Web Server API abuse

The actors went on to provide an existing legitimate OAuth application with both the *full_access_as_app* permission and administrator consent, which granted the threat actors full access to mailboxes through Exchange Web Services.

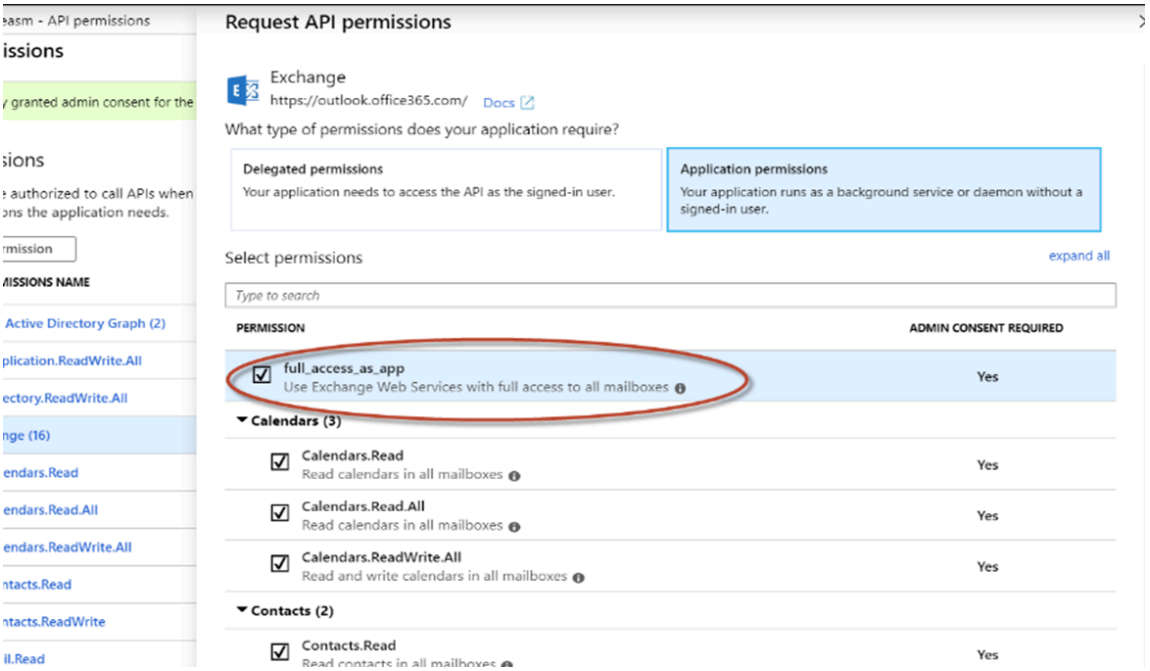

Figure 5. Adding access permission to the existing application

With the obtained cloud administrator privileges, the threat actors updated the OAuth application with certificates to conduct malicious activities. These newly added credentials could then be used to issue access tokens and authenticate on behalf of the application to access cloud resources.

We then observed the threat actors using this application's permissions to perform *GetItem* operations over many mailboxes in the target environment. They also performed thousands of search activities, which we suspect were attempts to dump mailboxes and/or search for sensitive data in them.

Email impersonation

The threat actors used the compromised administrator account to grant SMTP *Send on behalf* permissions to the Azure AD Connector account over a high-ranking employee's mailbox, using the *Set-Mailbox* PowerShell cmdlet.

Figure 6. Threat actors granting access to send emails on behalf of the target's account

Emails were then created and sent both internally and externally.

```
"MailboxOwnerUPN": [redacted]
"OrganizationName": [redacted]
"OriginatingServer": "[redacted]
"Item": {
  "Id": "RgAAAACXFTHHpr0NSrhug5nlfBhqBwCpT+1FL5q0TLAltwb6pe3PAAAAAAEQAACpT
+1FL5q0TLAltwb6pe3PAAgfLZ8YAAAJ",
  "InternetMessageId":
[redacted]
  "ParentFolder": {
    "Id": "LgAAAACXFTHHpr0NSrhug5nlfBhqAQCpT+1FL5q0TLAltwb6pe3PAAAAAAEQAAAB",
    "Path": "\\Drafts"
  },
  "SizeInBytes": 8340,
  "Subject": "[redacted]
},
"SessionId": "c9926a23-012b-4c7f-8cd6-4440fc93e0cf",
"SendAsUserMailboxGuid": [redacted]
"SendAsUserSmtp": [redacted]
}
```


Figure 7. Threat actors successfully sent email through the targeted account

The timeline below summarizes the sequence of events:

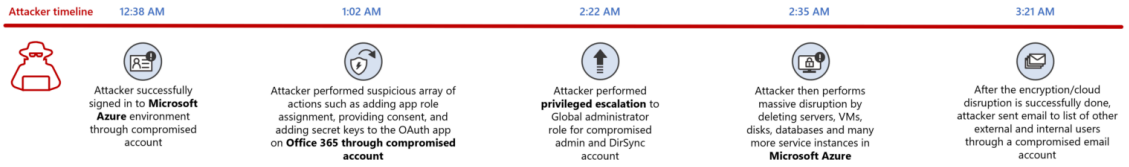

Figure 8. Cloud attack flow timeline

Mitigations for destructive attacks

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

Recommendations to secure your on-prem environment

- Refer to Microsoft's blog Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself for recommendations on building strong credential hygiene and other robust measures to defend against ransomware and human operated attacks.
- Enable tamper protection – Tamper protection is a feature in Microsoft Defender for Endpoint that prevents antivirus tampering and misconfiguration by malicious apps and actors. Customers running Intune can enable DisableLocalAdminMerge to prevent modification of antivirus exclusions via GPO.

Recommendations to secure your Azure AD environment

- 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.
- Enable continuous access evaluation – Continuous access evaluation (CAE) revokes access in real time when changes in user conditions trigger risks, such as when a user is terminated or moves to an untrusted location.
- Search unified audit logs for the *SendAs* operation to identify and track emails sent on behalf of a user mailbox.

- Further steps and recommendation to manage, design, and secure your Azure AD environment can be found by referring to Azure Identity Management and access control security best practices.

Detections

Microsoft 365 Defender

The following alerts in Microsoft 365 Defender can be used to detect suspicious operations in Azure related to the attacker activities described in this blog, including destructive activity:

- Access elevation by risky user
- Suspicious Azure resource deletions
- Suspicious Addition of an Exchange related App Role

In addition, the following alert can help detect compromised Azure AD Connect accounts:

- Unusual activities by Azure AD Connect sync account

Microsoft Defender for Cloud Apps

For Microsoft Defender for Cloud Apps with Azure Connector enabled, the following alerts can be used to detect destructive operations in Azure:

- Multiple storage deletion activities
- Multiple delete VM activities

Monitor medium and high severity alerts for highly privileged accounts as they can indicate malicious activity. For example:

- Unfamiliar sign-in properties

Find details of Azure AD Identity Protection alerts here.

Microsoft Defender for Identity

The following Microsoft Defender for Identity alerts can indicate associated threat activity:

- Suspicious additions to sensitive groups

For relevant accounts with Honeytoken configured, the following alert can indicate malicious activity:

- Honeytoken activity

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects attempted exploitation and post-exploitation activity and payloads. Turn on cloud-delivered protection to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block most new and unknown threats. Refer to the list of detection names related to exploitation of Log4j 2 vulnerabilities. Detections for the IOCs listed above are listed below:

- Backdoor:PHP/Remoteshell.V

- HackTool:Win32/LSADump
- VirTool:Win32/RemoteExec
- Trojan:PowerShell/Downloader.SB
- Trojan:Win32/Nibtse.G!tsk
- Backdoor:ASP/Shellman.SA
- Ransom:Win64/DarkBit
- VirTool:Win32/AtExecCommand

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint alerts with the following titles can indicate possible presence of the indicators of compromise listed below.

- Mercury actor activity detected
- Ransomware-linked emerging threat actor DEV-1084 detected

Reducing the attack surface

Microsoft Defender for Endpoint customers can turn on the following attack surface reduction rule to block or audit some observed activity associated with this threat:

- Block executable files from running unless they meet a prevalence, age, or trusted list criterion.
- Implement controlled folder access and add folders to the protected folders list to help prevent files from being altered or encrypted by ransomware. Set controlled folder access to Enabled.

Detecting Log4j 2 exploitation

Alerts that indicate threat activity related to the exploitation of the Log4j 2 exploitation should be immediately investigated and remediated. Refer to our Log4j related blogs to learn about this vulnerability and for a list of Microsoft Defender for Endpoint alerts that can indicate exploitation and exploitation attempts.

Detecting post-exploitation activity

Alerts with the following titles may indicate post-exploitation threat activity related to MERCURY activity described in this blog and should be immediately investigated and remediated. These alerts are supported on both Windows and Linux platforms:

Any alert title related to web shell threats, for example:

- ‘WebShell’ backdoor was prevented on an IIS Web server

Any alert title that mentions the DarkBit ransomware threat or DEV-1084, for example:

- ‘DarkBit’ ransomware was blocked
- ‘DarkBit’ ransomware was detected
- ‘DarkBit’ ransomware was prevented
- Ransomware-linked emerging threat actor DEV-1084 detected

Any alert title that mentions suspicious scheduled task creation or execution, for example:

- Suspicious scheduled task

Any alert title that mentions suspected tunneling activity, for example:

- Suspicious SSH tunneling activity

Any alert title that mentions suspected tampering activity, for example:

- Suspicious Microsoft Defender Antivirus exclusion
- Microsoft Defender Antivirus tampering

Any alert title that mentions PowerShell, for example:

- Suspicious process executed PowerShell command
- A malicious PowerShell Cmdlet was invoked on the machine
- Suspicious PowerShell command line
- Suspicious PowerShell download or encoded command execution
- Suspicious remote PowerShell execution

Any alert title related to suspicious remote activity, for example:

- Suspicious RDP session
- An active 'RemoteExec' malware was blocked
- Suspicious service registration

Any alert related to persistence:

- Anomaly detected in ASEP registry
- User account created under suspicious circumstances

Any alert title that mentions credential dumping activity or tools, for example:

- Malicious credential theft tool execution detected
- Credential dumping activity observed
- Mimikatz credential theft tool
- 'DumpLsass' malware was blocked on a Microsoft SQL server

Microsoft Defender Vulnerability Management

In addition to the mitigations above being presented and managed through Microsoft Defender Vulnerability Management, Microsoft 365 Defender customers can use threat and vulnerability management to identify and remediate devices that are vulnerable to Log4j 2 exploitation. More comprehensive guidance on this capability can be found on this blog: Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability.

Advanced hunting queries

Microsoft 365 Defender

To locate related activity, Microsoft 365 Defender customers can run the following advanced hunting queries:

// Advanced Hunting Query to surface potential Mercury PowerShell script backdoor installation

```
DeviceFileEvents
```

```
| where InitiatingProcessFileName =~ "powershell.exe"
| where FolderPath in~ (@"c:\programdata\db.ps1", @"c:\programdata\db.sqlite")
| summarize min(Timestamp), max(Timestamp) by DeviceId, SHA256, InitiatingProcessParentFileName
DeviceProcessEvents
| where InitiatingProcessFileName =~ "powershell.exe"
| where InitiatingProcessCommandLine has_cs "-EP BYPASS -NoP -W h"
| summarize makeset(ProcessCommandLine), min(Timestamp), max(Timestamp) by DeviceId
```

// Advanced Hunting Query to surface potential Mercury PowerShell script backdoor initiating commands

```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "powershell.exe"
| where InitiatingProcessCommandLine contains_cs @"c:\programdata\db.ps1"
| summarize makeset(ProcessCommandLine), min(Timestamp), max(Timestamp) by DeviceId
```

//Advanced Hunting Query for Azure resource deletion activity

```
let PrivEscalation = CloudAppEvents
| where Application == "Microsoft Azure"
| where ActionType == "ElevateAccess Microsoft.Authorization"
| where ActivityObjects has "Azure Subscription" and ActivityObjects has "Azure Resource Group"
| extend PrivEscalationTime = Timestamp
| project AccountObjectId, PrivEscalationTime ,ActionType;
CloudAppEvents
| join kind = inner PrivEscalation on AccountObjectId
| extend DeletionTime = Timestamp
| where (DeletionTime - PrivEscalationTime) <= 1h
| where Application == "Microsoft Azure"
| where ActionType has "Delete"
|summarize min(DeletionTime), TotalResourcersDeleted =count(), CountOfDistinctResources=
dcount(ActionType), DistinctResources=make_set(ActionType) by AccountObjectId
```

//AHQ used to detect attacker abusing OAuth application during the attack

```
CloudAppEvents
    | where Application == "Office 365"
    | where ActionType == "Consent to application."
    | where RawEventData.ResultStatus =~ "success"
    | extend UserId = tostring(RawEventData.UserId)
    | mv-expand AdminConsent = RawEventData.ModifiedProperties
    | where AdminConsent.Name == "ConsentContext.IsAdminConsent" and AdminConsent.NewValue == "True"
    | project ConsentTimestamp =Timestamp, UserId, AccountObjectId, ReportId, ActionType
    | join kind = leftouter (CloudAppEvents
        | where Application == "Office 365"
        | where ActionType == "Add app role assignment to service principal."
        | extend PermissionAddedTo = tostring(RawEventData.Target[3].ID)
        | extend FullAccessPermission = RawEventData.ModifiedProperties
        | extend OuthAppName = tostring(FullAccessPermission[6].NewValue) // Find app name
        | extend OAuthApplicationId = tostring(FullAccessPermission[7].NewValue) // Find appId
        | extend AppRoleValue = tostring(FullAccessPermission[1].NewValue) // Permission Level
        | where AppRoleValue == "full_access_as_app"
        | project PermissionTime=Timestamp, InitiatingUser=AccountDisplayName, OuthAppName,
OAuthApplicationId, AppRoleValue, AccountObjectId, FullAccessPermission
    ) on AccountObjectId
```

Microsoft Sentinel

Microsoft Sentinel 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 detections list above.

- full_access_as_app Granted To Application
- Potential SSH Tunnel to AAD Connect Host
- Suspicious Sign In by AAD Connect Sync Account
- Malicious web application requests linked with Microsoft Defender for Endpoint
- Web Shell Activity
- Tracking Privileged Account Rare Activity
- Mass Cloud resource deletions Time Series Anomaly
- Consent to Application discovery
- OAuth Application Required Resource Access Update

- Rare application consent
- Credential added after admin consented to ApplicationNew access credential added to Application or Service Principal

Microsoft Sentinel customers can use the TI Mapping analytic (a series of analytics all prefixed with “TI map”) to automatically match the 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. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy

Indicators of compromise (IOCs)

The below list provides IOCs observed during our investigation. We encourage our customers to investigate these indicators in their environments and implement detections and protections to identify past related activity and prevent future attacks against their systems.

Indicator	Type	Description
9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff	DEV-1084 ransom payload	8thCurse.exe
80bd00c0f6d5e39b542ee6e9b67b1eef97b2dbc6ec6cae87bf5148f1cf18c260	DEV-1084 batch script	
8dd9773c24703e803903e7a5faa088c2df9a4b509549e768f29276ef86ef96ae	DEV-1084 batch script	
486eb80171c086f4d184423ed7e79303ad7276834e5e5529b199f8ae5fc661f2	DEV-1084 batch script	
f1edff0fb16a64ac5a2ce64579d0d76920c37a0fd183d4c19219ca990f50effc	DEV-1084 batch script	
887ae654d69ac5ccb8835e565a449d7716d6c4747dc2fbff1f59f11723244202	DEV-1084 batch script	
3fba459d589cd513d2478fb4ae7c4efd6aa09e62bc3ff249a19f9a233e922061	DEV-1084 batch script	
0dde13e3cd2dcda522eeb565b6374c97b3ed4aa6b8ed9ff9b6224ea97bf2a584	DEV-1084 batch script	
afd16b9ad57eb9c26c8ae347c379c8e2b82361c7bdff5b189659674d5614854c	DEV-1084 batch script	
3e59d36faf2d5e6edf1d881e2043a46055c63b7c68cc08d44cc7fc1b364157eb	DEV-1084 batch script	
786bd97172ec0cef88f6ea08e3cb482fd15cf28ab22d37792e3a86fa3c27c975	DEV-1084 batch script	

36c71ce7cd38733eb66f32a8c56acd635680197f01585c5a2a846cc3cb0a8fe2	DEV-1084 batch script	
016967de76382c674b3a1cb912eb85ff642b2ebfe4e107fc576065f172c6ef80	DEV-1084 batch script	
3059844c102595172bb7f644c9a70d77a198a11f1e84539792408b1f19954e18	DEV-1084 batch script	
194.61.121[.]86	Command and control	
hxxps://pairing[.]rport[.]io/qMLc2Wx	Download Rport software from it	
141.95.22[.]153	Command and control	
193.200[.]16.3	Command and control	
192.52.166[.]191	Command and control	
45.56.162[.]111	Command and control	
104.194.222[.]219	Command and control	
192.169.6[.]88	Command and control	
192.52.167[.]209	Command and control	
webstore4tech[.]uaenorth.cloudapp.azure[.]com	Command and control	
vatacloud[.]com	Actor-owned Rport domain	
146.70.106[.]89	DEV-1084 operators were observed sending threatening emails to the victim after the attack from	

	146.70.106[.]89, an IP address previously linked to MERCURY	
b9cf785b81778e2b805752c7b839737416e3af54f64f1e40e008142e382df0c4	Rport Legit remote access tool	rport.exe
ab179112caadaf138241c43c4a4dccc2e3c67aeb96a151e432cfbafa18a4b436	Customized Ligolo tunneling tool	
46.249.35[.]243	Command and control	
45.86.230[.]20	Command and control	
6485a68ba1d335d16a1d158976e0cbfad7ab15b51de00c381d240e8b0c479f77	db.ps1 Customized Script Backdoor	
b155c5b3a8f4c89ba74c5c5c03d029e4202510d0cbb5e152995ab91e6809bcd7	db.sqlite Customized Obfuscated Script Backdoor	

NOTE: These indicators should not be considered exhaustive for this observed activity.

Microsoft Defender Threat Intelligence

Community members and customers can find summary information and all IOCs from this blog post in the linked Microsoft Defender Threat Intelligence article.

References

- https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/
- https://ehorus.com/
- https://github.com/nicocha30/ligolo-ng
- https://www.openssh.com/
- https://github.com/Gerenios/AADInternals/blob/master/AADSyncSettings.ps1#L97
