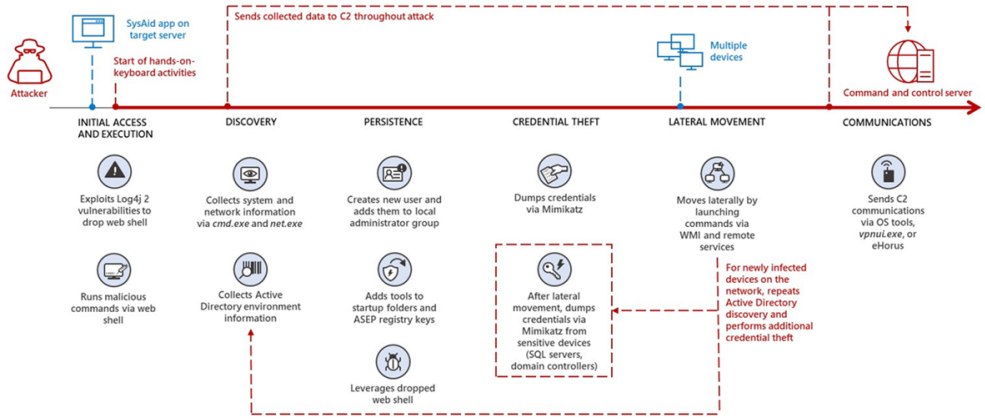
MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations

8/25/2022



In recent weeks, the Microsoft Threat Intelligence Center (MSTIC) and Microsoft 365 Defender Research Team detected Iran-based threat actor MERCURY leveraging exploitation of Log4j 2 vulnerabilities in SysAid applications against organizations all located in Israel. MSTIC assesses with high confidence that MERCURY's observed activity was affiliated with Iran's Ministry of Intelligence and Security (MOIS).

While MERCURY has used Log4j 2 exploits in the past, such as on vulnerable VMware apps, we have not seen this actor using SysAid apps as a vector for initial access until now. After gaining access, MERCURY establishes persistence, dumps credentials, and moves laterally within the targeted organization using both custom and well-known hacking tools, as well as built-in operating system tools for its hands-on-keyboard attack.

This blog details Microsoft's analysis of observed MERCURY activity and related tools used in targeted attacks. This information is shared with our customers and industry partners to improve detection of these attacks, such as implementing detections against MERCURY's tools in both Microsoft Defender Antivirus and Microsoft Defender for Endpoint. As with any observed nation-state actor activity, Microsoft directly notifies customers that have been targeted or compromised, providing them with the information needed to secure their accounts.

MERCURY TTPs align with Iran-based nation-state actor

Microsoft assesses with moderate confidence that MERCURY exploited remote code execution vulnerabilities in Apache Log4j 2 (also referred to as "Log4Shell") in vulnerable SysAid Server instances the targets were running. MERCURY has used Log4j 2 exploits in past campaigns as well.

MSTIC assesses with high confidence that MERCURY is coordinating its operations in affiliation with Iran's Ministry of Intelligence and Security (MOIS). According to the US Cyber Command, MuddyWater, a group we track as MERCURY, "is a subordinate element within the Iranian Ministry of Intelligence and Security."

The following are common MERCURY techniques and tooling:

- **Adversary-in-the-mailbox phishing:** MERCURY has a long history of spear-phishing its targets. Recently, there has been an uptick in the volume of these phishing attacks. The source of the phishing comes from compromised mailboxes and initiating previous email conversations with targets. MERCURY operators include links to or directly attach commercial remote access tools, such as ScreenConnect, in these initial phishing mails.
- **Use of cloud file-sharing services:** MERCURY utilizes commercially available file-sharing services as well as self-hosting resources for delivering payloads.
- **Use of commercial remote access applications:** The initial foothold on victims emerges via commercially available remote access applications. This allows MERCURY to gain elevated privileges and be able to transfer files, primarily PowerShell scripts, easily over to the victim's environment.
- **Tooling:** MERCURY's tools of choice tend to be Venom proxy tool, Ligolo reverse tunneling, and home-grown PowerShell programs.

- **Targeting:** MERCURY targets a variety of Middle Eastern-geolocated organizations. Mailbox victims correlate directly with organizations that do business with the Middle Eastern victims.

This latest activity sheds light on behavior MERCURY isn't widely known for: scanning and exploiting a vulnerable application on a target's device. They have been observed performing this activity in the past, but it is not very common. The exploits are derived from open source and sculpted to fit their needs.

Observed actor activity

Initial access

On July 23 and 25, 2022, MERCURY was observed using exploits against vulnerable SysAid Server instances as its initial access vector. Based on observations from past campaigns and vulnerabilities found in target environments, Microsoft assess that the exploits used were most likely related to Log4j 2. The threat actor leveraged Log4j 2 exploits against VMware applications earlier in 2022 and likely looked for similarly vulnerable internet-facing apps. SysAid, which provides IT management tools, might have presented as an attractive target for its presence in the targeted country.

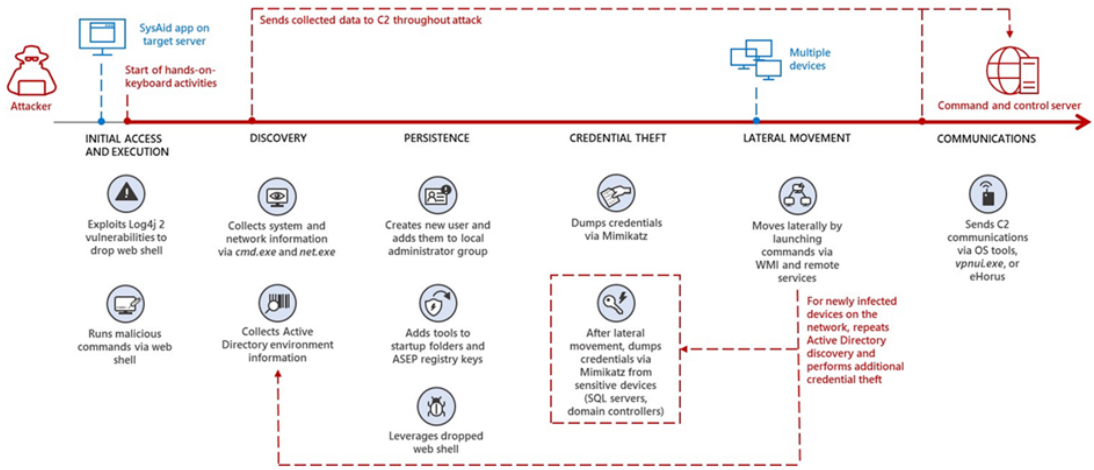


Figure 1. Observed MERCURY attack chain

Exploiting SysAid successfully enables the threat actor to drop and leverage web shells to execute several commands, as listed below. Most commands are related to reconnaissance, with one encoded PowerShell that downloads the actor's tool for lateral movement and persistence.

Executed commands:

- cmd.exe /C whoami
- cmd.exe /C powershell -exec bypass -w 1 -enc UwB….
- cmd.exe /C hostname
- cmd.exe /C ipconfig /all
- cmd.exe /C net user
- cmd.exe /C net localgroup administrators
- cmd.exe /C net user admin * /add
- cmd.exe /C net localgroup Administrators admin /add
- cmd.exe /C quser

Persistence

Once MERCURY has obtained access to the target organization, the threat actor establishes persistence using several methods, including:

- Dropping a web shell, providing effective and continued access to the compromised device.
- Adding a user and elevating their privileges to local administrator.
- Adding the leveraged tools in the startup folders and ASEP registry keys, ensuring their persistence upon device reboot.
- Stealing credentials.

The actor leverages the new local administrator user to connect through remote desktop protocol (RDP). During this session, the threat actor dumps credentials by leveraging the open-source application Mimikatz. We also observed MERCURY later performing additional credential dumping in SQL servers to steal other high privileged accounts, like service accounts.

Lateral movement

We observed MERCURY further using its foothold to compromise other devices within the target organizations by leveraging several methods, such as:

- Windows Management Instrumentation (WMI) to launch commands on devices within organizations.
- Remote services (leveraging RemCom tool) to run encoded PowerShell commands within organizations.

Most of the commands launched are meant to install tools on targets or perform reconnaissance to find domain administrator accounts.

Communication

Throughout the attack, the threat actor used different methods to communicate with their command-and-control (C2) server, including:

- Built-in operating system tools such as PowerShell
- Tunneling tool called *vpnui.exe*, a unique version of the open-source tool Ligolo
- Remote monitoring and management software called eHorus

Microsoft will continue to monitor MERCURY activity and implement protections for our customers. The current detections, advanced detections, and IOCs in place across our security products are detailed below.

Recommended customer actions

The techniques used by the actor and described in the Observed actor activity section can be mitigated by adopting the security considerations provided below:

- Check if you use SysAid in your network. If you do, apply security patches and update affected products and services as soon as possible. Refer to SysAid's Important Update Regarding Apache Log4j for technical information about the vulnerabilities and mitigation recommendations.
- Refer to the detailed Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability.
- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.
- Block in-bound traffic from IPs specified in the indicators of compromise table.
- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single factor authentication, to confirm authenticity and investigate any anomalous activity.
- Enable multi-factor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity. *Note:* Microsoft strongly encourages all customers download and use password-less solutions like Microsoft Authenticator to secure accounts.

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
hxxp://sygateway[.]com	Domain	First seen: May 16, 2022
91[.]121[.]240[.]104	IP address	First seen: May 17, 2022
164[.]132[.]237[.]64	IP address	First seen: November 26, 2021
e81a8f8ad804c4d83869d7806a303ff04f31cce376c5df8aada2e9db2c1eeb98	SHA-256	mimikatz.exe
416e937fb467b7092b9f038c1f1ea5ca831dd19ed478cca444a656b5d9440bb4	SHA-256	vpnui.exe Ligolo
25325dc4b8dcf3711e628d08854e97c49cfb904c08f6129ed1d432c6bfff576b	SHA-256	VBScript
3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	SHA-256	Remcom
3137413d086b188cd25ad5c6906fbb396554f36b41d5cff5a2176c28dd29fb0a	SHA-256	Web shell
87f317bbba0f50d033543e6ebab31665a74c206780798cef277781dfdd4c3f2f	SHA-256	Web shell
e4ca146095414dbe44d9ba2d702fd30d27214af5a0378351109d5f91bb69cdb6	SHA-256	Web shell
d2e2a0033157ff02d3668ef5cc56cb68c5540b97a359818c67bd3e37691b38c6	SHA-256	Web shell
3ca1778cd4c215f0f3bcfdd91186da116495f2d9c30ec22078eb4061ae4b5b1b	SHA-256	Web shell

bbfee9ef90814bf41e499d9608647a29d7451183e7fe25f472c56db9133f7e40	SHA-256	Web shell
b8206d45050df5f886afefa25f384bd517d5869ca37e08eba3500cda03bddfef	SHA-256	Web shell

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 portal article.

Detections

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

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint customers should monitor the alert "**Mercury Actor activity detected**" for possible presence of the indicators of compromise listed above.

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.

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 the 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:

- An active 'Remoteshell' backdoor was blocked

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, for example:

- 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

Microsoft 365 Defender customers can use threat and vulnerability management to identify and remediate devices that are vulnerable to Log4j 2 exploitation. A 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 Sentinel

Microsoft Sentinel customers can use the following queries to look for the related malicious activity in their environments.

Identify MERCURY IOCs

The query below identifies matches based on IOCs shared in this post for the MERCURY actor across a range of common Microsoft Sentinel data sets:

- https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/Mercury_Log4j_August2022.yaml

Identify SysAid Server web shell creation

The query below looks for potential web shell creation by SysAid Server:

- https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/PotentialMercury_Webshell.yaml

Identify MERCURY PowerShell commands

The query below identifies instances of PowerShell commands used by the threat actor in command line data:

- https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/powershell_mercury.yaml

In addition to the above, Microsoft Sentinel users should also look for possible Log4j 2 vulnerabilities, the details of which were shared in a previous blog post.

Microsoft 365 Defender

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

Potential WebShell creation by SysAisServer instance

```
DeviceFileEvents
| where InitiatingProcessFileName in~ ("java.exe", "javaw.exe")
| where InitiatingProcessCommandLine has "SysAidServer"
| where FileName endswith ".jsp"
```

Abnormal process out of SysAidServer instance

```
DeviceProcessEvents
| where Timestamp > ago(7d)
| where InitiatingProcessFileName in~ ("java.exe", "javaw.exe")
| where InitiatingProcessCommandLine has "SysAidServer"
| summarize makeset(ProcessCommandLine), min(Timestamp), max(Timestamp) by DeviceId
```

PowerShell commands used by MERCURY

```
DeviceProcessEvents
| where FileName =~ "powershell.exe" and ProcessCommandLine has_cs "-exec bypass -w 1
-enc"
| where ProcessCommandLine contains_cs
"UwB0AGEAcgB0AC0ASgBvAGIAIAAtAFMAYwByAGkAcAB0AEIAbABvAGMAawAgAHsAKABzAGEAcABzACAAKAAiAHAA"

| summarize makeset(ProcessCommandLine), makeset(InitiatingProcessCommandLine, 10),
makeset(DeviceId), min(Timestamp), max(Timestamp) by DeviceId
```

Vulnerable Log4j 2 devices

Use this query to identify vulnerabilities in installed software on devices, surface file-level findings from the disk, and provide the ability to correlate them with additional context in advanced hunting.

```
DeviceTvmSoftwareVulnerabilities
| where CveId in ("CVE-2021-44228", "CVE-2021-45046")

DeviceTvmSoftwareEvidenceBeta
| mv-expand DiskPaths
| where DiskPaths contains "log4j"
| project DeviceId, SoftwareName, SoftwareVendor, SoftwareVersion, DiskPaths
```