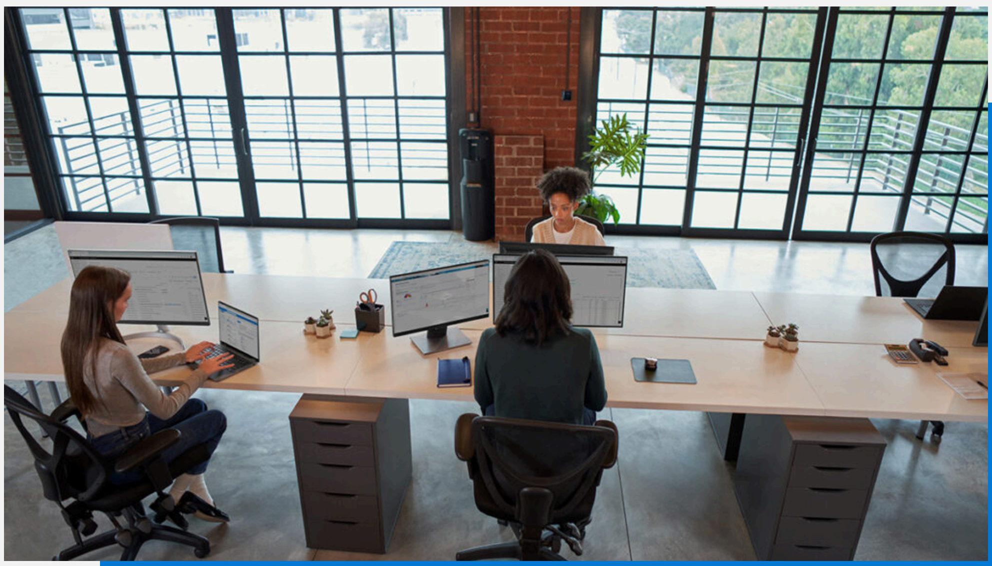


Research Incident response Microsoft Incident Response Attacker techniques, tools, and infrastructure

20 min read

Guidance for investigating attacks using CVE-2023-23397

By Microsoft Incident Response

March 24, 2023

Threat intelligence

Microsoft Defender

Microsoft Defender for Endpoint

more

February 15, 2024 update – On January 20, 2024, the US government conducted a disruption operation against infrastructure used by a threat actor we track as Forest Blizzard (STRONTIUM), a Russian state-sponsored threat actor, as detailed here: https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian

December 4, 2023 update – Microsoft has identified a nation-state activity group tracked as Forest Blizzard (STRONTIUM), based in Russia, actively exploiting CVE-2023-23397 to provide secret, unauthorized access to email accounts within Exchange servers. The Polish Cyber Command (DKWOC) partnered with Microsoft to take action against Forest Blizzard actors, and to identify and mitigate techniques used by the actor: https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/detecting-malicious-activity-against-microsoft-exchange-servers/. Users should ensure Microsoft Outlook is patched and kept up to date to mitigate this threat. Microsoft Defender XDR detects the exploitation and known post-compromise activity of CVE-2023-23397. The only updates to the original blog below are in the "Who is Forest Blizzard" section, reflecting our updated attribution, and added links to our product Threat Intelligence reports.

Who is Forest Blizzard?

The group Microsoft tracks as Forest Blizzard (STRONTIUM) is a Russian state-sponsored threat actor that primarily targets government, energy, transportation, and non-governmental organizations in the United States, Europe, and the Middle East. The United States and United Kingdom governments have linked Forest Blizzard to Unit 26165 of the Russian Federation's military intelligence agency: Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

> Forest Blizzard commonly seeks and employs publicly available exploits in addition to CVE-2023-23397. Beginning in at least the first half of September 2023, Forest Blizzard actors leveraged the WinRAR CVE 2023-38831 vulnerability to adapt spear-phishing operations against chiefly Ukrainian government targets. Other known exploits leveraged by Forest Blizzard include CVE-2021-40444, CVE-2021-42292, CVE-2021-42321, CVE-2021-34473, CVE-2020-17144, and CVE-2020-0688.
>
> Forest Blizzard continually refines its footprint by employing new custom techniques and malware, suggesting that it is a well-resourced and well-trained group posing long-term challenges to attribution and tracking its activities. Microsoft continually updates detections and protections against this threat group based on our telemetry and research. Other security researchers have used GRU Unit 26165, APT28, Sednit, Sofacy, and Fancy Bear to refer to groups with similar or related activities.

This guide provides steps organizations can take to assess whether users have been targeted or compromised by threat actors exploiting CVE-2023-23397. A successful exploit of this vulnerability can result in unauthorized access to an organization's environment by triggering a Net-NTLMv2 hash leak. Understanding the vulnerability and how it has been leveraged by threat actors can help guide the overall investigative process.

This document covers:

- An overview of the vulnerability
- Exploit scenarios
- Post-exploit activities observed in attacks
- Techniques for determining if an organization was targeted or compromised via this vulnerability
- Mitigations available to protect your environment

Exploitation of CVE-2023-23397 leaves very few forensic artifacts to discover in traditional endpoint forensic analysis. This blog describes how Microsoft Incident Response (previously known as Microsoft Detection and Response Team – DART) was able to detect the abuse of CVE-2023-23397 and how organizations can identify historical and present evidence of compromise through this vulnerability.

This vulnerability triggers a Net-NTLMv2 hash leak. Abuse of the leaked Net-NTLMv2 hash is post-exploitation activity. In this blog, we emphasize specific observed post-exploitation activity that targeted Microsoft Exchange Server. However, there are numerous ways that a leaked Net-NTLMv2 hash could be used by a threat actor.

Understanding the CVE-2023-23397 vulnerability

CVE-2023-23397 is a critical elevation of privilege vulnerability in Microsoft Outlook on Windows. It is exploited when a threat actor delivers a specially crafted message to a user. This message includes the *PidLidReminderFileParameter* extended Messaging Application Programming Interface (MAPI) property, which must be set to a Universal Naming Convention (UNC) path share on a threat actor-controlled server (via Server message block (SMB)/transmission control protocol (TCP) port 445).

In exploitation of CVE-2023-23397, threat actors can specify the value for the *PidLidReminderFileParameter* in specially crafted messages to trigger a Net-NTLMv2 hash leak to threat actor-controlled servers.

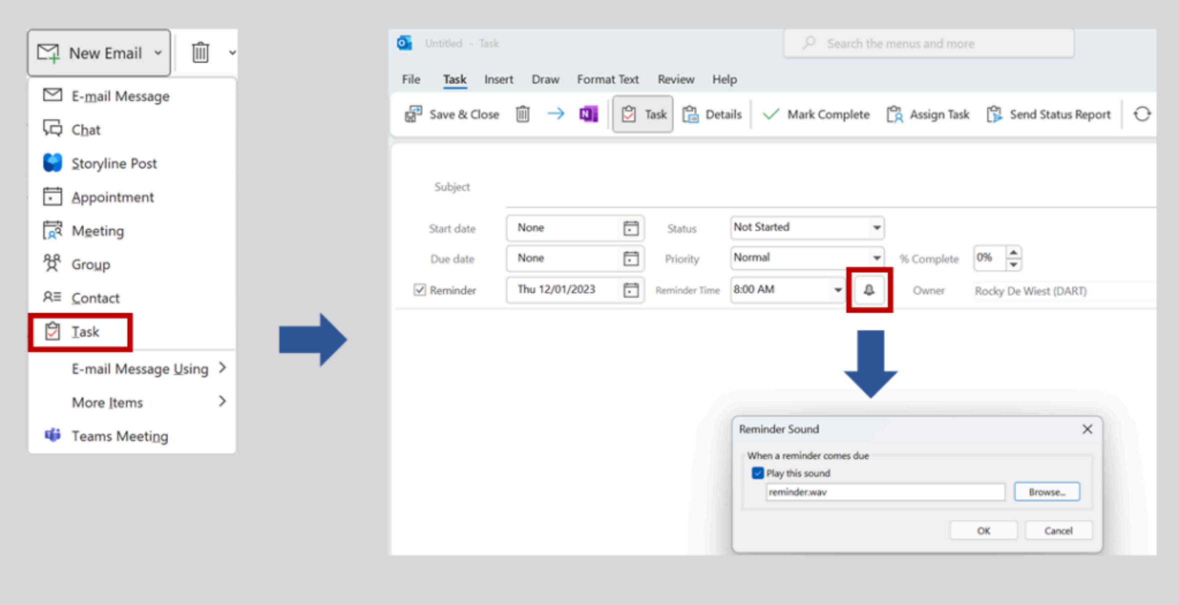
The user does not need to interact with the message: if Outlook on Windows is open when the reminder is triggered, it allows exploitation. The connection to the remote SMB server sends the user's Net-NTLMv2 hash in a negotiation message, which the threat actor can either a) relay for authentication against other systems that support NTLMv2 authentication or b) perform offline cracking to extract the password. As these are NTLMv2 hashes, they cannot be leveraged as part of a Pass-the-Hash technique. All versions of Microsoft Outlook on Windows are impacted. Outlook for Android, iOS, Mac, and users who use Outlook on the web (OWA) without using the Outlook client are not affected.

Microsoft has traced evidence of potential exploitation of this vulnerability as early as April 2022.

This technique leverages the Transport Neutral Encapsulation Format (TNEF). TNEF is a Microsoft-specific format for transmitting formatted email messages. A TNEF message contains a plaintext version of the message and an attachment that packages the original formatted version of the message. Typically, this attachment is named *Winmail.dat*. The *Winmail.dat* attachment includes formatting, attachments, and Outlook-specific features such as meeting requests including extended MAPI Properties. Details about TNEF can be found here:

- https://learn.microsoft.com/office/client-developer/outlook/mapi/transport-neutral-encapsulation-format-tnef
- https://learn.microsoft.com/exchange/mail-flow/content-conversion/content-conversion.

Outlook on Windows is designed to enable a user to specify a custom sound file associated with a reminder.



Subject

Start date: None | Status: Not Started

Due date: None | Priority: Normal | % Complete: 0%

☑ Reminder: Thu 12/01/2023 | Reminder Time: 8:00 AM | Owner: Rocky De Wiest (DART)

Reminder Sound

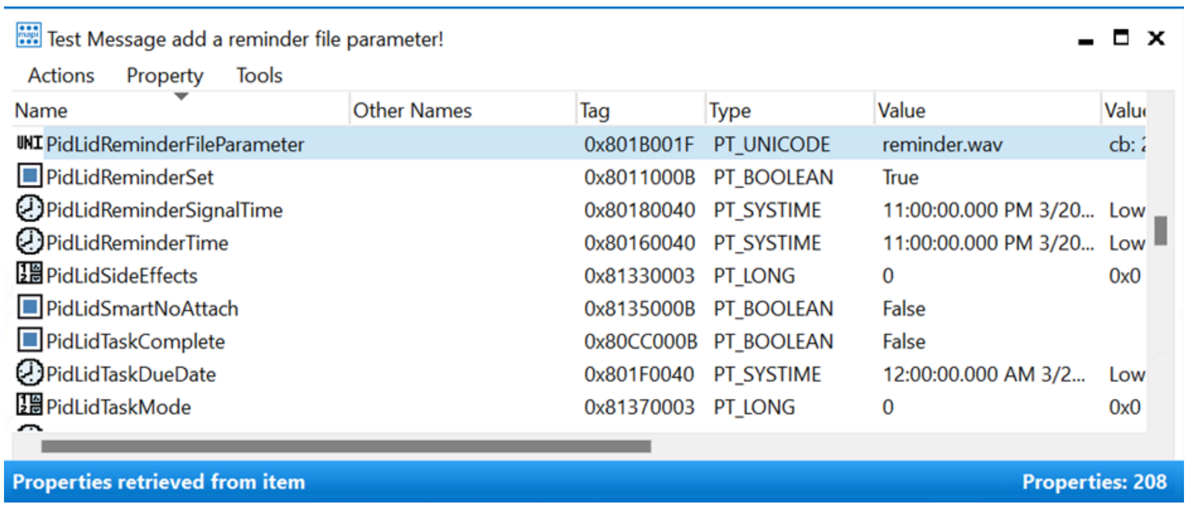
When a reminder comes due

☑ Play this sound

reminder.wav

Figure 1. Setting a custom sound to play when a reminder is triggered in Outlook on Windows client

Modifying this value sets the *PidLidReminderFileParameter* extended MAPI property, which is stored as a property associated with the specific mail object. A tool such as MFCMAPI (see https://github.com/stephenegriffin/mfcmapi) can be used to view extended MAPI properties associated with an object. In the following screenshot, the value of the *PidLidReminderFileParameter* is shown set to *reminder.wav*, the *PidLidReminderSet* is "True", and the reminder times are set to occur in the past.



Name	Other Names	Tag	Type	Value	Valu
PidLidReminderFileParameter		0x801B001F	PT_UNICODE	reminder.wav	cb:
PidLidReminderSet		0x8011000B	PT_BOOLEAN	True	
PidLidReminderSignalTime		0x80180040	PT_SYSTIME	11:00:00.000 PM 3/20...	Low
PidLidReminderTime		0x80160040	PT_SYSTIME	11:00:00.000 PM 3/20...	Low
PidLidSideEffects		0x81330003	PT_LONG	0	0x0
PidLidSmartNoAttach		0x8135000B	PT_BOOLEAN	False	
PidLidTaskComplete		0x80CC000B	PT_BOOLEAN	False	
PidLidTaskDueDate		0x801F0040	PT_SYSTIME	12:00:00.000 AM 3/2...	Low
PidLidTaskMode		0x81370003	PT_LONG	0	0x0

Properties retrieved from item   Properties: 208

Figure 2. Resulting extended MAPI Properties and their values as a result of customizing the sound to play when reminders are triggered as seen using MFCMAPI.

To further deceive users, threat actors may also set the *PidLidReminderTime* property to remain dormant in the mailbox until a future date.

The affected Net-NTLMv2 hash belongs to the user signed in to the Windows device where the Outlook client application is running, regardless of the identity that received the malicious message. If the user does not dismiss the reminder/task Outlook alert or the reminder is recurring (i.e., fires multiple times), the user's Net-NTLMv2 hash can be leaked multiple times.

Note: Interaction based on the WebDAV protocol is not at risk of leaking credentials to external IP addresses via this exploit technique. While the threat actor infrastructure might request Net-NTLMv2 authentication, Windows will honor the defined internet security zones and will not send Net-NTLMv2 hashes. In other words, an external threat actor can only exploit this vulnerability via the SMB protocol. If a target device can communicate to external threat actor infrastructure over port 445 (SMB), Net-NTLMv2 hashes might be sent; however, if this communication via SMB is not possible, Windows will fall back to leveraging WebDAV. WebDAV will set up a connection with the threat actor infrastructure, but Net-NTLMv2 hashes will not be sent.

Observed post-exploitation actions

In a recent engagement, Microsoft Incident Response has observed additional post-exploitation activities following exploitation of CVE-2023-23397. The presence of artifacts associated with these post-exploitation activities can strongly suggest compromise of user accounts. These post-exploitation activities include:

Initial access (authentication bypass):

Using a Net-NTLMv2 Relay attack against Exchange Servers (**NOTE:** Azure Active Directory, the default authentication service for Exchange Online, is not directly susceptible to a Net-NTLMv2 relay attack. However, it is possible that a federated identity provider may be susceptible).

Credential access/lateral movement:

Using the Exchange Web Services (EWS) API to send additional messages with the malicious value of the *PidLidReminderFileParameter* extended MAPI property to users inside and external to the organization.

Discovery/persistence:

Using the EWS API to enumerate folders in a compromised user's mailbox and changing the mailbox folder permissions using the *UpdateFolder* API so that any authenticated user can access all mailbox folder content with "owner" privileges. This technique established additional persistent access to contents of user's mailboxes even if a password was reset or otherwise remediated.

The following diagrams show initial access using a Net-NTLMv2 Relay attack, persistence via modifying mailbox folder permissions, and lateral movement by sending additional malicious messages.

Figure 3. Observed threat actor exploitation of CVE-2023-23397 to gain unauthorized access to Exchange Server and modify mailbox folder permissions for persistent access to the mailbox.

Figure 4. Observed threat actor activity to extend their access in a compromised environment by using a compromised e-mail account to target other members of the same organization.

Threat hunting guidance: Evidence of targeting

Organizations should use an in-depth and comprehensive threat hunting strategy to identify potential credential compromise through CVE-2023-23397. While running the Exchange scanning script provided by Microsoft is an effective first step, this script does not provide visibility into malicious messages for all scenarios.

- Outlook allows users to open multiple mailboxes at the same time. If a user has configured their Outlook to open mailboxes from multiple e-mail services, a malicious message received through one of those other services will still trigger the vulnerability but that message is not in the scanned mailboxes. (Note: Independent of what mailbox or the identity used to access the mailbox, if a malicious message is received, the credential that will leak belongs to the identity currently signed in to the Windows device.)
- Users may move messages to a local file (PST). Local e-mail stores are not scanned when scanning the Exchange environment. Archived messages may show evidence of a prior compromise. If the local files are open in Outlook, messages can still trigger the vulnerability.

If messages have been deleted from Exchange (some organizations may have a policy limiting data retention), then the messages will no longer be available in Exchange.

If no suspicious or malicious values are identified through the Exchange scanning script, organizations should also hunt for known threat actor indicators of compromise (IOCs) related to the exploitation of this vulnerability.

For example, if IP addresses and URIs are extracted from the *PidLidReminderFileParameter* values, incident responders should review all available security telemetry for presence of these newly identified indicators. Data sources can include:

- Firewall logs
- Proxy logs
- Azure Active Directory sign-in logs for users of Exchange Online
- IIS Logs for Exchange Server
- VPN logs
- RDP Gateway logs
- Endpoint telemetry from an endpoint detection and response (EDR) solution if available
- Forensic endpoint data such as windows event logs from end user systems

For example, using advanced hunting in Microsoft Defender for Endpoint, multiple tables can be queried simultaneously to uncover activities related to IP address indicators:

```
//Search for activity around IoAs
let IoCs = dynamic(["<IP Address 1>","<IP Address 2>"]);
let range = ago(30d);
union (DeviceProcessEvents | where Timestamp > range | where
ProcessCommandLine has_any (IoCs)),
     (DeviceNetworkEvents | where Timestamp > range | where RemoteIP
in (IoCs) or LocalIP in (IoCs)),
     (DeviceLogonEvents | where Timestamp > range | where RemoteIP
in (IoCs))
| extend SignatureName =
tostring(parse_json(AdditionalFields).SignatureName)
| project-reorder Timestamp, DeviceName, ActionType,
LocalIP,RemoteIP, RemotePort,SignatureName,ProcessCommandLine
| sort by Timestamp desc
```

Hunting strategically

There are several approaches to identifying whether your organization was targeted, including the following (ordered from the most high-fidelity to more anomaly-based approach):

- Review suspicious messages, calendar items, or tasks with reminders that were reported by users
- Examine network logging and endpoint logging for evidence of known atomic indicators
- Scan Exchange for delivered messages with the *PidLidReminderFileParameter* set
- Hunt for anomalous behaviors based on:
    - NTLM authentication involving untrusted or external resources. This can be observed in Exchange Server logging, Microsoft Defender for Identity, and Microsoft Defender for Endpoint telemetry.
    - WebDAV connection attempts through process execution events.
    - SMBClient event log entries.
    - Firewall logs for suspicious outbound SMB connections.

Review suspicious messages, calendar items, or tasks reported by users

Users in targeted organizations will have received messages with the malicious value of the *PidLidReminderFileParameter* value set. In some cases, users may have reported these suspicious messages, tasks, or calendar invitations to their security team. A high-level investigation of messages potentially exploiting CVE-2023-23397 may not reveal any overt malicious elements, as embedding malicious URLs or other content in the message body itself is not necessary. A deeper analysis of the message's extended MAPI properties (specifically, the *PidLidReminderFileParameter* value) is required to confirm if it is malicious.

Scan for messages with malicious properties

Organizations should search their Exchange environment for messages where the *PidLidReminderFileParameter* value is set. Microsoft has provided a script to enable organizations perform this search here, including instructions: https://microsoft.github.io/CSS-Exchange/Security/CVE-2023-23397/.

The script produces a CSV file enumerating each message that has the *PidLidReminderFileParameter* property set, and will report on targets that are local on the computer, internal to the network, or on the internet. Any messages identified where this property references a server in the "InternetZone" should be considered malicious. References to intranet servers should also be carefully analyzed. Figure 5 depicts a sample output from this script.

Figure 5. Sample output for PidLidReminderFileParameter detection script.

Customers with a large number of mailboxes in Exchange may consider customizing the script logic strategically, by:

- Initially targeting high-value users by specifying a list of mailboxes of interest.
- Timeboxing: As the first known exploitation of this vulnerability was in April 2022 performance can be improved by prioritizing a search from 2022 onwards. It is still recommended to search further historically as well, however with lower priority, as it is possible this exploit was used prior to April 2022.
- Running multiple concurrent scans across different user mailbox sets by using batching (see script documentation).

If any suspicious or malicious messages are identified via this script, organizations should further triage their environment, including:

- examination of the targeted users' logon behaviors
- hunting for further presence of any malicious domains or IP addresses in available network and endpoint logging.

Artifacts on endpoints

Organizations should review SMBClient event logging, Process Creation events, and other available network telemetry to identify potential exploitation via CVE-2023-23397. To determine whether any such exploitation led to a threat actor gaining unauthorized access to the environment, analysis of authentication events, network perimeter logging, and Exchange Server logging (if Exchange Server is used by the organization) will be instrumental.

Microsoft-Windows-SMBClient/Connectivity event logs

This event logging channel records server errors and warnings for both SMB and WebDAV connections, and provides a source to identify potential compromise through CVE-2023-23397, as it may reveal failed outbound connection attempts to threat actor-controlled infrastructure.

The ServerName field in EventIds 30800, 30803, 30806, 30804, and 31001 should be monitored for non-trusted servers, as illustrated in Figure 6.

Figure 6: Sample event where SMB traffic was blocked in the firewall.

It is critical to note that the presence of these events cannot be used to confirm whether credentials were leaked, and can only be used as evidence that an outbound connection attempt was made by the device but failed (due to a protocol or network error). Microsoft Incident Response observed during an engagement that a device affected by CVE-2023-23397 attempted to connect multiple times to threat actor infrastructure, failing occasionally and producing these event log entries, but otherwise successfully leaking credentials to the threat actor.

WebDAV Process Creation events

If SMB traffic to the internet is blocked by your organization or otherwise fails, Windows will fall back to using WebDAV to attempt to complete the connection. This behavior, paired with CVE-2023-23397 execution, results in a potentially unique Process Creation event and command line parameters that organizations can hunt in endpoint detection and response (EDR) telemetry or other endpoint logging (such as Sysmon logs, as depicted in Figure 7):

- Parent process command line: *C:\Windows\system32\svchost.exe -k LocalService -p -s WebClient*
- Child process command line: *rundll32.exe C:\Windows\system32\davclnt.dll,DavSetCookie <IP Address> hxxp://<Threat actor IP>/folder/sound.wav*

It is possible that the filesystem URL may not have a traditional .wav file extension.

Figure 7: Sample WebDAV process create event

It is critical to note that the presence of this process tree in your environment cannot be used to confirm whether credentials were leaked. It can only be used as evidence that a message exploiting CVE-2023-23397 was **delivered**, **triggered an attempted outbound SMB connection**/credential leak to threat actor infrastructure, **but failed in the given instance** as credentials cannot be leaked through WebDAV with this vulnerability. If this failure was the result of a transient network issue (rather than SMB being blocked deliberately and systemically), it is still possible that credentials may have been leaked.

Exchange Server logs

For organizations using Exchange Server, there are several log sources that can provide value in hunting for indicators of attack or compromise through CVE-2023-23397. These log sources may potentially reveal unauthorized access to Exchange Server via a Net-NTLMv2 Relay attack, as well as possible post-exploitation activities. These logs do not provide value in determining whether a NTLMv2 hash was leaked, however.

Microsoft provides this tool to enable organizations to collect relevant Exchange Server logs: https://microsoft.github.io/CSS-

Exchange/Diagnostics/ExchangeLogCollector/.

Microsoft Incident Response recommends collecting all logs with the *-AllPossibleLogs* command line flag; however, a more minimal collection can be obtained using the following flags:

- *-EWSLogs*
- *-IISLogs*
- *-PowerShellLogs*
- *-ServerInformation*
- *-ExchangeServerInformation*
- *-MessageTrackingLogs*
- *-OWALogs*

Collected logs can be reviewed by ingesting them into Azure Data Explorer, Log Analytics in Azure Monitor, or another SIEM or log parsing utility (such as Log Parser Studio).

Exchange IIS logs

Analysis of IIS logs from Exchange Server (or, if the server is behind a reverse proxy, the IIS logs from the proxy server) can provide insight into potential threat actor behavior.

NOTE: If Exchange Server is protected by a reverse proxy, client IP values (cIP) in logging will only show the IP address of the proxy server. In this case, access to logs from the proxy is critical to determine if connections originated from untrusted IP addresses.

Reverse Proxy Logs

If a reverse proxy is implemented and configured to register headers, such as those that include authentication methods and Net-NTLMv2 negotiations, it is possible to identify Net-NTLMv2 Relay behavior. Microsoft Incident Response was able to leverage these logs in a recent engagement: certain users appeared to authenticate from their appropriate and expected workstations, but the authentications originated from IP addresses associated with threat actor infrastructure.

EWSLogs

Exchange Web Services (EWS) logs include the *AuthenticationType*. If a Net-NTLMv2 Relay attack was leveraged against an EWS Endpoint, it can often be seen in these logs. Strategies to hunt for anomalies in these logs include:

- Filtering EWSLogs by *AuthenticationType* for NTLM
- Grouping by *ClientIpAddress* (NOTE: The external client IP address may need to be parsed from the field, as it can contain the results of proxying the ClientIP to the Exchange Server backend component. Fields will be in the form <*ClientIP*>*:*<*PortNumber*> <*ProxiedIPAddress*>).
- Group by the *AuthenticatedUser*

Any authentications using NTLMv2 originating from unknown or untrusted IP addresses should be further examined. If a single external IP address is associated with multiple users' authentications, and the IP address is not consistent with those users' typical patterns of behavior (based on factors such as geolocation, hosting provider, or User Agent string), events associated with such an IP should be investigated further.

If a threat actor changes mailbox permissions or mailbox folder permissions as part of their post-exploitation behaviors, *SoapActions* including "GetFolder", "UpdateFolder", and "FindFolder" may be observed for the combination of the authenticated user and IP address.

If a threat actor attempts to access email for a compromised user, *SoapActions* including "ResolveNames","GetDelegate","GetFolder","FindFolder","FindItem", and "GetItem" may be observed for the combination of the authenticated user and IP address.

The following Kusto Query Language (KQL) query can assist with parsing and summarizing EWS logging for the purposes described above, if the relevant logs have been ingested into Azure Data Explorer.

```
EWSLogging
| where AuthenticationType == 'NTLM'
| extend IpAddress = tostring(split(ClientIpAddress,":")[0])
| summarize count(), min(['DateTime']),max(['DateTime']),
    make_set(SoapAction), make_set(UserAgent) by AuthenticatedUser,
IpAddress
```

Exchange HTTP Proxy EWS Logs

HTTP Proxy EWS logs can be useful to identify the details of NTLMv2 authentications. The user name, workstation name, and domain name can be extracted from those values using the techniques described in

- https://community.pulsesecure.net/t5/Pulse-Secure-vADC/HowTo-Decode-and-log-the-username-in-an-NTLM-connection/ta-p/28869
- https://davenport.sourceforge.net/ntlm.html

Exchange Server Message Tracking Logs

Exchange Server Message Tracking Logs are useful to identify messages with certain subjects or from certain sender IP address values. Refer to the following Microsoft Learn pages for more details:

- https://learn.microsoft.com/exchange/mail-flow/transport-logs/transport-logs?view=exchserver-2019
- https://learn.microsoft.com/exchange/monitoring/trace-an-email-message/run-a-message-trace-and-view-results

Additional indicators of compromise

Potential registry key modification

Microsoft Incident Response identified a registry key that can indicate that a reminder was triggered for a Note or Task item. This registry key holds certain properties (e.g., location and size) of the UI window that is created when the reminder triggered. If a user has not used the reminder functionality within Tasks or Notes, these registry keys will not exist. Figure 8 depicts the Task key as viewed in RegEdit:

- *HKCU\Software\Microsoft\Office\<VERSION OF OUTLOOK>\Outlook\Tasks*
- *HKCU\Software\Microsoft\Office\<VERSION OF OUTLOOK>\Outlook\Notes*

Figure 8: Example registry key for a Task item.

The presence of these keys provides evidence that a user has received a reminder for a Task or Note. If the presence of this registry key is identified, and appears to be anomalistic for your organization, threat hunters should examine the user's mailbox as well as network/endpoint telemetry for further evidence of compromise using the techniques described in this blog, especially by performing temporal analysis around the *LastModified* timestamp of the registry keys.

Hunting for outbound SMB connections

Network perimeter telemetry and/or EDR data can be investigated for SMB connections involving external IP addresses as part of a larger threat hunting strategy.

The following query can be used in the advanced hunting portal of Microsoft Defender for Endpoint to further align SMB connections with Net-NTLMv2 behavior.

The query will identify connections involving port 445 (standard for SMB) involving remote public IP addresses. By filtering on both Local and Remote parameters, the query will also include records of the *NetworkSignatureInspected* ActionType. If threat actor infrastructure is attempting to harvest Net-NTLMv2 credentials, the *NetworkSignatureInspected* ActionType should include a *SignatureName* of NTLM-Challenge. This indicates a Net-NTLMv2 negotiation was attempted.

For more information about the *NetworkSignatureInspected* actions, check Hunting for network signatures in Microsoft Defender for Endpoint.

```
//Hunt for SMB to the internet
let range = ago(30d);
DeviceNetworkEvents
| where Timestamp > range
//Connections have RemotePort set to 445
//NetworkSignatureInspected have LocalPort set to 445
| where RemotePort == 445 or LocalPort == 445
| where not(ipv4_is_private(RemoteIP)) or
not(ipv4_is_private(LocalIP))
| extend SignatureName =
tostring(parse_json(AdditionalFields).SignatureName)
| project-reorder Timestamp, DeviceName, ActionType,
LocalIP,RemoteIP, LocalPort, RemotePort,SignatureName
| sort by Timestamp desc
```

NOTE: Organizations may consider filtering out their own public IP address space from the query above.

Microsoft product detections

Organizations using Microsoft Defender for Endpoint or Microsoft Defender for Office 365 can identify threats using the following detections.

- **Microsoft Defender for Endpoint** provides detections with the following titles in the security center can indicate threat activity on your network:
    - **Possible target of Net-NTLMv2 credential theft** – This detects specific attacks observed by Microsoft prior to disclosure of the vulnerability and might not detect variations on the attack after publishing.
- **Microsoft Defender for Office 365** detects messages exploiting this vulnerability and shows administrators the following alerts to indicate that the file contains a critical elevation of privilege exploit related to CVE-2023-23397:
    - Exploit_Office_CVE_2023_23397_A
    - Exploit_Office_CVE_2023_23397_B
    - Exploit_Office_CVE_2023_23397_C
    - Exploit_Office_CVE_2023_23397_D
    - Exploit_Office_CVE_2023_23397_E
    - Exploit_Office_CVE_2023_23397_F
    - Exploit_Office_CVE_2023_23397_G
    - Exploit_Office_CVE_2023_23397_H

Recommendations

Microsoft Incident Response recommends the following steps to mitigate this type of attack and the observed post-exploitation behavior:

- Ensure Microsoft Outlook is updated as soon as possible to mitigate the issue. If patching is not immediately possible, ensuring you have implemented these security best practices can help mitigate this threat:
  - Add users to the Protected Users group, which prevents the use of NTLM as an authentication mechanism. This might impact applications that require NTLM, but the settings will revert once the user is removed from the Protected Users group. This makes troubleshooting easier than other methods of disabling NTLM authentication. The Protected Users group provides credential protections beyond disabling NTLM and should be used for high-value accounts, such as domain administrators, when possible.
  - Block TCP 445/SMB outbound from your network by using a perimeter firewall, local firewall, and through your VPN settings. This helps prevent the exploitation of CVE-2023-23397 to send NTLM authentication messages to remote file shares. For remote users, it is important to check split tunnel VPN settings to ensure outbound traffic is blocked when they are not on your corporate network.
- For organizations leveraging on-premises Microsoft Exchange Server, apply the latest security updates to ensure that defense-in-depth mitigations are active.
- Where suspicious or malicious reminder values are observed, make sure to use the script to remove either the messages or just the properties, and consider initiating incident response activities.
- For any targeted or compromised user, reset the passwords of any account logged in to computers of which the user received suspicious reminders and initiate incident response activities.
- Use multifactor authentication to mitigate the impact of potential Net-NTLMv2 Relay attacks. NOTE: This will not prevent a threat actor from leaking credentials and cracking them offline.
- Disable unnecessary services on Exchange.
- Limit SMB traffic by blocking connections on ports 135 and 445 from all inbound IP addresses except those on a controlled allowlist.
- Disable NTLM in your environment.

Understanding mitigations

To address this vulnerability, you must install the Outlook security update, regardless of where your mail is hosted (e.g., Exchange Online, Exchange Server, some other platform) or your organization's support for NTLM authentication.

When using Exchange Online or Exchange server as your mail host, you can take the following additional actions:

- Determine if your organization was targeted by actors attempting to use this vulnerability
- Provide defense in depth for new messages received outside your organization

Protections in Outlook

Outlook for Windows first checks if the path specified by the *PidLidReminderFileParameter* message property is to a location that is not in the local or trusted network. If the path points outside of the local or trusted network locations, the parameter is not honored when updates are installed.

Protections in Exchange Online

Exchange Online drops the *PidLidReminderFileParameter* message property at TNEF conversion when a new message is received.

Protections for Exchange Server

Exchange Server (with March 2023 SU) drops the *PidLidReminderFileParameter* message property at TNEF conversion when a new message is received.

Conclusion

While leveraging NTLMv2 hashes to gain unauthorized access to resources is not a new technique, the exploitation of CVE-2023-23397 is novel and stealthy. Even when users reported suspicious reminders on tasks, initial security review of the messages, tasks, or calendar items involved did not result in detection of the malicious activity. Furthermore, the lack of any required user interaction contributes to the unique nature of this vulnerability. In this document, Microsoft Incident Response has highlighted threat hunting techniques and strategy for exploitation of this CVE, alongside some hunting techniques for observed post-exploitation threat actor behaviors. Furthermore, a broad threat hunting for anomalous user activity consistent with credential compromise is advised.

Observed indicators of attack

Several malicious samples have been uploaded to VirusTotal.com and a signature has been created that identifies potentially malicious messages associated with exploitation of CVE-2023-23397.

VirusTotal subscribers can review those results here: https://www.virustotal.com/gui/search/crowdsourced_yara_rule%253A000bc4a247%257CEXPL_SUSP_Outlook_CVE_2023_23397_Exfil_IP_Mar23

Known IP addresses associated with exploitation of this vulnerability in the above VirusTotal results are listed below. NOTE: These IP addresses were assessed by Microsoft Threat Intelligence to be compromised infrastructure.

- 101.255.119[.]42
- 213.32.252[.]221
- 168.205.200[.]55
- 185.132.17[.]160
- 69.162.253[.]21
- 113.160.234[.]229
- 181.209.99[.]204
- 82.196.113[.]102
- 85.195.206[.]7
- 61.14.68[.]33

Threat intelligence reports

Microsoft customers can use the following reports in Microsoft products 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.

Microsoft Defender Threat Intelligence

- Multiple threat actors continue to exploit WinRAR vulnerability CVE-2023-38831
- Forest Blizzard uses Exchange PowerShell for persistence
- CVE-2023-23397 Microsoft Outlook elevation of privilege vulnerability leads to NTLM credential theft
- Forest Blizzard

Microsoft 365 Defender Threat analytics

- Actor profile: Forest Blizzard
- CVE-2023-23397: Microsoft Outlook elevation of privilege vulnerability leads to NTLM credential theft
- Vulnerability profile: CVE-2023-38831 in WinRAR

Further reading

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

Research Threat intelligence Microsoft Defender XDR

Business email compromise

Oct 8 · 9 min read

File hosting services misused for identity phishing >

Since mid-April 2024, Microsoft has observed an increase in defense evasion tactics used in campaigns abusing file hosting services like SharePoint, OneDrive, and Dropbox. These campaigns use sophisticated techniques to perform social engineering, evade detection, and compromise identities, and include business email compromise (BEC) attacks.

Research Threat intelligence Microsoft Defender

Attacker techniques, tools, and infrastructure

Sep 26 · 20 min read

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

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, […]

Research Threat intelligence Microsoft Defender ·

Vulnerabilities and exploits

May 1 · 15 min read

"Dirty stream" attack: Discovering and mitigating a common vulnerability pattern in Android apps >

Microsoft discovered a vulnerability pattern in multiple popular Android applications that could enable a malicious application to overwrite files in the vulnerable application's internal data storage directory, which could lead to arbitrary code execution and token theft, among other impacts. We have shared our findings with Google's Android Application Security Research team, as well as the developers of apps found vulnerable to this issue. We anticipate that the vulnerability pattern could be found in other applications. We're sharing this research more broadly so developers and publishers can check their apps for similar issues, fix as appropriate, and prevent them from being introduced into new apps or releases.

Research Threat intelligence Microsoft Defender Threat actors ·

Apr 22 · 10 min read

Analyzing Forest Blizzard's custom post-compromise tool for exploiting CVE-2022-38028 to obtain credentials >

Since 2019, Forest Blizzard has used a custom post-compromise tool to exploit a vulnerability in the Windows Print Spooler service that allows elevated permissions. Microsoft has issued a security update addressing this vulnerability as CVE-2022-38028.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

- Surface Pro
- Surface Laptop
- Surface Laptop Studio 2
- Surface Laptop Go 3

Microsoft Store

- Account profile
- Download Center
- Microsoft Store support
- Returns

Education

- Microsoft in education
- Devices for education
- Microsoft Teams for Education
- Microsoft 365 Education

Microsoft Copilot

AI in Windows

Explore Microsoft products

Windows 11 apps

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft 365 Copilot

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Manage cookies Terms of use Trademarks Safety & eco Recycling About our ads