

Microsoft Copilot for Security

GA highlights and Full
capability View





Primary use cases



Incident summarization



Impact analysis



Reverse engineering of scripts



Guided response



New product highlights for General Availability

Customize and manage Copilot for Security for your security and IT team's daily operations



Custom promptbooks

Create custom promptbooks based on your data sources and procedures, each promptbook running the series of prompts your team follows to accomplish workstreams.



Knowledgebase integration

Your business logic can be integrated to empower Copilot for Security to perform activities based on your step-by-step guides.



Admin usage reporting

Review your team's product usage to forecast spending and inform provisioning.



Language availability

Model available in 8 languages and user experience available in 25.*



Custom Promptbook

Microsoft Copilot for Security / My sessions / Untitled

Share Export

Microsoft Defender XDR incident investigation

Get a report about a specific incident, with related alerts, reputation scores, users, and devices.

Inputs

Incident Id

Prompts

- 1 Summarize Defender incident <IncidentId>. ✓ X
- 2 Tell me about the entities associated with that incident.
- 3 What are the reputation scores for the IPv4 addresses on that incident?
- 4 Show the authentication methods setup for each user involved in that incident. Especially indicate whether they have MFA enabled.
- 5 If a user is listed in the incident details, show which devices they have used recently and indicate whether they are compliant with policies.
- 6 If any devices are listed in the previous output, show details from Intune on the one that checked in most recently. Especially indicate if it is current on all operating system updates.
- 7 Write an executive report summarizing this investigation. It should be suited for a non-technical audience. Include a verdict, confidence, evidence, key takeaways, and an executive summary.

+ Add prompt

How can Copilot for Security help? ?

AI-generated content may be incorrect. Check it for accuracy.



Knowledgebase integration

The screenshot shows the Microsoft Copilot for Security interface with a dark theme. A central modal window titled "Manage sources" is open, showing a "Files" tab with a file upload area and a list of uploaded files:

- Woodgrove Data Handling Policy.docx (Uploading...)
- Phishing playbook.docx (1/20/2024 | 2.5MB)
- Security 101.pdf (1/13/2024 | 3.7MB)

Background cards include:

- ServiceNow incident investigation**: A report about a Windows Server 2019 machine that occurred on a Windows Server 2019 machine, involving suspicious activities related to multiple users.
- Microsoft Sentinel**: A card for suspicious script analysis, mentioning a PowerShell script found in a potential security incident.
- Suspicious script analysis**: A detailed report on a PowerShell script.
- Threat actor profile**: A card for "Mist Sandstorm", also known as "PHOSPHORUS", an Iran-affiliated cyber activity group.
- Non-Compliant Managed Device Triage**: A card for a non-compliant device with instructions to resolve the issue.

At the bottom, there's a footer bar with a "How can Copilot for Security help?" button and navigation icons.



Usage Reporting

Microsoft Security Copilot

Home
My sessions
Promptbook library

Owner

Owner settings
Role assignment

Usage monitoring

Usage monitoring

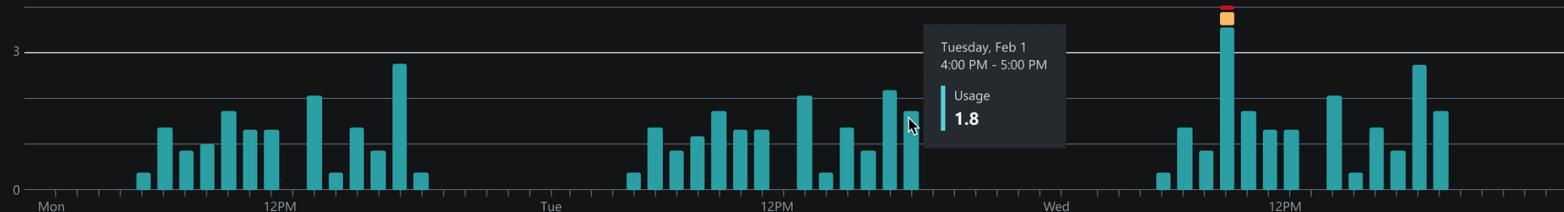
Last updated Feb 2, 2024

The number of security compute units available to your organization is determined by the units you have purchased per hour and unused units that have rolled over. Unused full or partial units will expire 24 hours after they become available. [Learn more](#)

Units per hour
3 units

Change

Date: Last 3 days ▾



| Date ↓ | Unit usage | Unit status |
|----------------|------------|-------------------------------|
| Feb 2, 4:10 PM | .02 | |
| Feb 2, 4:02 PM | .12 | |
| Feb 2, 3:28 PM | .04 | |
| Feb 2, 3:12 PM | .6 | |
| Feb 2, 2:10 PM | .43 | |
| Feb 2, 2:08 PM | .01 | |
| Feb 2, 2:07 PM | .89 | ▲ All available units used |
| Feb 2, 2:02 PM | .16 | △ 90% of available units used |
| Feb 2, 2:00 PM | .25 | |

Settings

Mona Kane
Mona.kane@contoso.com

Sign out

Contoso

?



Language Settings

Microsoft Edge for Security

Continue your test session.

ServiceNow incident

Suspicious incident - Medium Severity

This report summarizes the investigation of a medium severity suspicious incident that occurred on a Windows Server 2019 machine running ServiceNow. The investigation found multiple suspicious activities related to multiple accounts.

Updated 4 min ago

Get started using these examples

Home Suspicious script analysis

Suspicious script analysis

Get a report analyzing the intent, intelligence, threat level, and impacts of a suspicious script.

Microsoft Security 11:30

Microsoft Edge for Security help!

Settings

Preferences

Data and privacy

About

Theme

Light

Dark

High contrast

Follow operating system theme

Language

App language

English (United States)

English

French

German

Japanese

Spanish

is displayed with incidents. To immediately refresh the browser.

Suspicious script analysis

The conversation involves an analysis of a PowerShell script that was found as part of a potential security incident. The script is...

PowerShell 11:30

Threat actor profile

Min Sanderson, also known as PEGASUS, is an Iran affiliated cyber activity group that has been active since...

Min Sanderson 11:30

View of incident 11:30

Non-Compliant Managed Device Triage

Get compliance status for a device with explanations and instructions to resolve the issue.

Microsoft Security 11:30



Microsoft Copilot for Security



Copilot for Security Use Cases

End-to-end scenarios: incident response, threat hunting, intelligence gathering, & posture management

| Item | Use Case | Description |
|--------------|---|--|
| Key Features | Incident response | Copilot for Security can swiftly summarize information about an incident by enhancing incident details with context from data sources, assess its impact, and provide guidance to analysts on how to take remediation steps with guided suggestions. |
| | Security posture management | Copilot for Security provides information on events that might expose organizations to a known threat. Analysts are provided prescriptive guidance on how to protect against those potential vulnerabilities. |
| | Security reporting | Copilot for Security can generate ready-to-share executive summaries or reports on security investigations, publicly disclosed vulnerabilities, or threat actors and their campaigns. |
| Integrations | Microsoft Copilot for Security in Microsoft Defender XDR | Bringing Copilot for Security to Microsoft Defender XDR allows teams to understand attacks immediately, promptly assess and apply appropriate mitigation to stop and contain attacks, quickly analyze complex files, and hunt for threats with ease. |
| | Microsoft Copilot for Security (preview) and Intune | Use Copilot for Security to view managed device attributes and configuration data. You can get information about your devices, apps, compliance & configuration policies, and policy assignments managed in Intune. |
| | Microsoft Copilot for Security (preview) and Entra | Copilot for Security can assist in investigating identity risks and helping with troubleshooting daily identity tasks, such as why a sign-in required multi-factor authentication. IT admins can ask about users, groups, sign-ins and permissions and instantly get a risk summary, steps to remediate and recommended guidance for each identity at risk, in natural language. |
| | Microsoft Copilot for Security (preview) and Purview | Copilot for Security will be able to quickly generate a comprehensive summary of alerts and information to accelerate investigation and response, upskill talent via guided responses to navigate through information efficiently. Embedded scenarios will be surfaced in Data Loss Prevention, Insider Risk Management and eDiscovery and Communication Compliance. |
| | Microsoft Copilot for Security (preview) and Microsoft Defender Threat Intelligence | Copilot for Security delivers from Microsoft Defender Threat Intelligence (Defender TI) information about threat actors, indicators of compromise (IOCs), and tools, as well as contextual threat intelligence. You can use the prompts and promptbooks to investigate incidents, enrich your hunting flows with threat intelligence information, or gain more knowledge about your organization's or the global threat landscape. |

Copilot for Security – Using Prompts

Prompts are the primary input Copilot for Security needs to generate answers that can help you in your security-related tasks

Use promptbooks

The screenshot shows a dark-themed interface with a sidebar on the left containing a list of promptbook entries:

- PROMPTBOOKS**
- Microsoft Sentinel incident investigation**
Get a summary of an important security incident, along with related alerts, entities, and intelligence.
- Microsoft 365 Defender incident investigation**
Get a summary of an important security incident, along with related alerts and intelligence.
- Threat actor profile**
Get a report profiling a known actor with suggestions for protecting against common tools and tactics.
- Suspicious script analysis**
Get a suspicious script analysis and related intelligence report.
- Vulnerability impact assessment**
Get a report summarizing the intelligence for a known vulnerability and how to address it.

Select from prompt suggestions

The screenshot shows a dark-themed interface with a sidebar on the left containing a list of prompt suggestion entries:

- PROMPT SUGGESTIONS**
- Analyze a script or command**
Analyzes and interprets a command or script to natural language
- Append Comment To ServiceNow Incident**
Appends / adds comment to a specific ServiceNow Incident
- Generate and run Defender Hunting Queries**
Retrieves data from Microsoft 365 Defender (M365 Defender) related to emails, alerts, processes, ident...
- Generate and Run Sentinel Hunting Queries**
Retrieves data from Microsoft Sentinel related to emails, alerts, processes, identities and roles, logins, ...
- Get ServiceNow Incident Comments**
Gets detailed comments for a ServiceNow incident
- See all system capabilities**

Create your own prompts

Sample prompts:

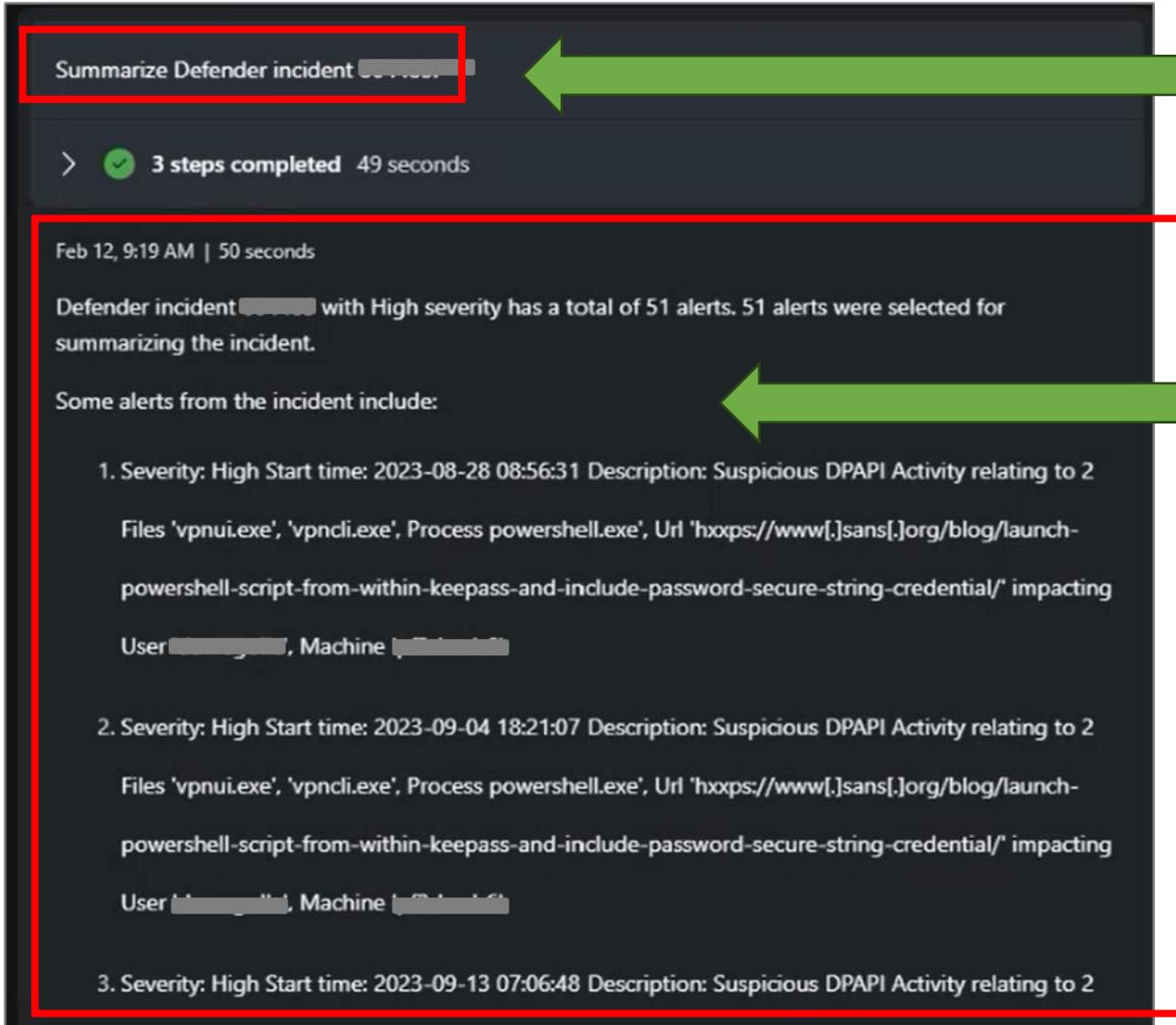
What is the latest active Defender incident assigned to me, angus.macgregor@contoso.com? Summarize it, including the alerts associated with it.

Elaborate on the details of this alert including the entities involved.

Tell me more about the user entity.

Scenario 1 – Incident Summarization

Using promptbooks



Use natural language query to ask Copilot for Security e.g. summarize specific incident

Results will show in matter of seconds / minutes!

Scenario 1 – Incident Summarization

Using promptbooks

The entities associated with Defender incident 804485 include:

1. Device: [REDACTED]

- Azure AD Device ID: [REDACTED]
- Defender AV Status: 'updated'
- First Seen: '2022-02-10T14:18:44.793Z'
- Health Status: 'active'
- Logged On Users: [REDACTED]
- MDE Device ID: [REDACTED]
- Onboarding Status: 'onboarded'
- OS Build: 19045
- OS Platform: 'Windows10'
- RBAC Group ID: [REDACTED]
- RBAC Group Name: 'Windows 10 & 11'
- Risk Score: 'high'
- Version: '22H2'
- Tags: '[REDACTED]'

2. User: [REDACTED]

- Azure AD User: [REDACTED]
- Domain Name: 'I [REDACTED]
- User Principal Name: 'D [REDACTED].com'
- User SID: [REDACTED]

3. Files:

- 'vpnccli.exe' located at 'C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client' published by 'Cisco Systems, Inc.' with a size of 145048 bytes. The SHA1 hash is [REDACTED] and the SHA256 hash is [REDACTED]
- 'vpnui.exe' located at 'C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client' published by 'Cisco Systems, Inc.' with a size of 2044568 bytes. The SHA1 hash is [REDACTED] and the SHA256 hash is [REDACTED]

4. Processes:

- The processes involved in the incident include 'powershell.exe' and 'cmd.exe'.

5. URL:

- The URL associated with the incident is '[hxps://www.sans.org/blog/launch-powershell-script-from-within-keepass-and-include-password-secure-string-credential/](https://www.sans.org/blog/launch-powershell-script-from-within-keepass-and-include-password-secure-string-credential/)'.

These entities were involved in a series of suspicious activities, including DPAPI activity and process discovery, which were detected and flagged by Microsoft Defender for Endpoint.

References

[Incident Page](#)

Highlight which entities were involved in the incident so your team can immediately take action e.g. which device was involved, user, files, processes, URLs, etc.

Scenario 2 – Executive Summary Report

Using promptbooks

The screenshot shows a dark-themed user interface for Copilot for Security. At the top, a red-bordered box contains the instruction: "Write an executive report summarizing this investigation. It should be suited for a non-technical audience." A green arrow points from this box to the explanatory text on the right. Below the instruction, a progress bar indicates "3 steps completed 50 seconds". The main content area contains several paragraphs of text describing a recent security incident, mentioning unusual activity, specific processes like 'powershell.exe' and 'cmd.exe', and the user account involved. It also discusses security measures like Multi-Factor Authentication (MFA) and device compliance.

Write an executive report summarizing this investigation. It should be suited for a non-technical audience.

> 3 steps completed 50 seconds

In a recent security incident, our systems detected unusual activity involving one of our devices and a user account. The incident, classified as high severity, spanned several months from August 2023 to February 2024 and triggered a total of 51 alerts.

The incident began with suspicious activity on a device running Windows 10, identified as [REDACTED]. The activity involved a user account under the name '[REDACTED]'. The suspicious activity was linked to two files, 'vpnui.exe' and 'vpncli.exe', and a process known as 'powershell.exe'. This activity was associated with a specific web address and was detected intermittently over several months, always involving the same user and device.

In addition to these alerts, our systems also detected an unusual process discovery on the same device in September 2023. This alert involved the processes 'powershell.exe' and 'cmd.exe', and again, it impacted the same user.

The user account involved in this incident, '[REDACTED]', has robust security measures in place. It uses Multi-Factor Authentication (MFA), a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity. This user account has five different authentication methods set up, including the Microsoft Authenticator and Phone Authentication methods.

The device '[REDACTED] 5' associated with this incident is in compliance with our security policies and is up-to-date with all operating system updates. This means that the device has the latest security patches and updates installed, which are crucial for protecting the device against known vulnerabilities.

In summary, while this incident is concerning due to its high severity and the number of alerts triggered, our security measures, including Multi-Factor Authentication and compliance with security policies, have been effective in managing the situation. We will continue to monitor the situation closely and take any necessary actions to ensure the security of our systems.

Copilot for Security can help you write an executive report summarizing the steps that you took in this investigation and written for a non-technical audience.

TIP: What is great about this skill is that it is not adding more work on the analyst. It is just enhancing their capabilities, allowing them to know more, work faster, and understand the threats and risks the organization is facing.

Scenario 3 – Analyze “Suspicious” Script

Using promptbooks

Run

Suspicious script analysis

Get a report analyzing the intent, intelligence, threat actors, and impacts of a suspicious script.

```
① <code>$password = [REDACTED] Remove-Variable -Name p<REDACTED>
#<REDACTED>
#&"C:\Program Files\KeePass Password Safe<REDACTED>.exe" -entry-url-
open -ul</code>
```

Prompts (7)

The following script was found as part of a potential security incident. Explain what this script does step by step and infer the intent. Also note any actions expressed that could be malicious in nature, including destructive activities, stealing of information, or changing of sensitive settings: <SNIPPET>

Is this script malicious?

Provide the reputation of any IPs or hostnames found.

Are there any threat intelligence articles that reference the IOCs that were found?

Show me the profiles of any threat actors referenced.

If this script was malicious, what are the recommended policy changes to protect against it?

1 Copy the suspicious script in the promptbook

Feb 12, 10:00 AM | 2 minutes 49 seconds

analysis of the script

2 The provided PowerShell script is used to automate the process of connecting to a Cisco AnyConnect VPN. Here's a step-by-step breakdown of what the script does:

1. The script retrieves a username and a password from a Base64 string. The password is decrypted using the `System.Security.Cryptography.ProtectedData` class. This is a standard method for storing sensitive information like passwords in a secure manner.

```
1 $username = [REDACTED];
2 $cipherbytes = [System.Convert]::FromBase64String(
[REDACTED]
3 [System.Reflection.Assembly]::LoadWithPartialName('System.Security') | Out-Null;
4 [byte[]] $m_pbOptEnt = @([0xA5,0x74,0x2E,0xEC]);
5 $plainbytes =
[System.Security.Cryptography.ProtectedData]::Unprotect($cipherbytes, $m_pbOptEnt, 0);
6 $password = [REDACTED] $plainbytes );
7
```

2. The script checks the status of the Cisco AnyConnect VPN connection. If the VPN is disconnected, it stops the `vpnctl` process, connects to the VPN using the `vpnctl` command-line interface, and

The intent of this script appears to be automating the process of connecting to a VPN and launching a KeePass entry. While the script itself does not contain any inherently malicious actions, it's worth noting that the misuse of such scripts by unauthorized individuals could potentially lead to unauthorized access to the VPN and the KeePass entry. Therefore, it's crucial to ensure that this script is used by authorized individuals only and that the system where this script is run is secure.

3 Results will also provide assessment if the script is malicious or not

Results will show blow by blow

4 Write me a report that summarizes the findings from the investigation. It should be suitable for a non-technical audience.

3 steps completed 1 minute 2 seconds

Feb 12, 10:12 AM | 1 minute 5 seconds

Provide Executive Summary

Our investigation focused on a PowerShell script that was found as part of a potential security incident. The script is designed to automate the process of connecting to a Cisco AnyConnect VPN. Here's a simplified explanation of what the script does:

- It retrieves a username and a password.
- It checks if the VPN is connected.
- If the VPN is disconnected, it stops a process, connects to the VPN, and then restarts the process.
- If the VPN is already connected, it simply outputs a message saying "VPN Already Connected".
- Finally, the script removes the password from memory and launches a KeePass entry.

The script itself does not contain any inherently malicious actions. However, if misused by unauthorized

Scenario 4 – Assess Vulnerabilities

Using prompt suggestions

The screenshot shows a dark-themed web application interface. At the top left, there's a navigation bar with a back arrow and the text "AssessVulnerabilityImpact". Below it, a red box highlights the URL "VulnerabilityId: CVE-2024-21350". A large green arrow points from the text "You can use the out-of-the box prompt suggestions such as AssessVulnerabilityImpact to simplify your investigation." to this highlighted URL.

The main content area displays a list of log entries:

- > ✓ Chose Incident Analysis
- > ✓ Processed your request 4 seconds
- > ○ Preparing your response ... 3 seconds

Below the logs, the date "Feb 15, 9:18 AM | 31 seconds" is shown. The main text block describes the vulnerability with ID CVE-2024-21350, titled "Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability", which has a high severity level and affects various Microsoft software versions.

Following this, a section titled "Here are the details of the devices impacted by this vulnerability:" lists five devices:

1. Device ID: [REDACTED], Device Name: [REDACTED], Software: windows_10, Version: 10.0.19044.3930
2. Device ID: [REDACTED], Device Name: [REDACTED], Software: windows_11, Version: 10.0.22621.3007
3. Device ID: [REDACTED], Device Name: [REDACTED], Software: windows_11, Version: 10.0.22631.3007
4. Device ID: [REDACTED], Device Name: [REDACTED], Software: windows_10, Version: 10.0.19044.3930
5. Device ID: [REDACTED], Device Name: [REDACTED], Software: windows_10, Version: 10.0.19044.3930

A note at the bottom states: "Please note that this is not the complete list. There are more devices affected by this vulnerability. It is recommended to patch these devices as soon as possible to mitigate the risk of a potential exploit."

You can use the out-of-the box prompt suggestions such as AssessVulnerabilityImpact to simplify your investigation.

Here you can see details of all the devices impacted by this specific vulnerability...

Scenario 5 – Enrich Incidents with Threat Intelligence

Using prompt suggestions

EnrichIncidentWithThreatIntelligence

IpAddresses: [REDACTED]

> 3 steps completed 16 seconds

Feb 15, 9:27 AM | 17 seconds

The IP address "[REDACTED]" has been enriched with threat intelligence context. Here are the details:

- The IP was first seen on 2023-07-05 and last seen on 2024-02-08.
- The netblock associated with this IP is "[REDACTED]0/20".
- The organization associated with this IP is "Akamai Technologies, Inc." and the Autonomous System Number (ASN) is "[REDACTED]."
- The country associated with this IP is Great Britain (GB).
- The hosting provider for this IP is "Akamai".
- The reputation score of the IP is 0, which classifies it as "UNKNOWN". There are no specific rules or MITRE TTPs associated with this IP, and the last seen date is also not available.
- There is no resolution information available for this IP.

Please note that a reputation score of 0 and a classification of "UNKNOWN" means that there is no known threat associated with this IP based on the current threat intelligence data. However, it's always a good practice to keep monitoring and updating the threat intelligence context for the most accurate information.

You can Enrich the Incidents with Threat Intelligence feeds.

Here you can see details of each entities such as IP address with Microsoft Defender Threat Intelligence.

Scenario 6 – Searching for any TOR Activities

Custom Prompts / Scenarios specific to <Customer Name> day to day SecOps

The screenshot shows the Microsoft Security Copilot interface. At the top, there's a red box highlighting the search bar with the query "tell me if any user is communicating to TOR network". A green arrow points from this bar to the text "Use natural language query to ask Copilot for Security e.g. specific users communicating to TOR network". Below the search bar is a table with three rows of data:

| Timestamp | DeviceId | DeviceName |
|------------------------------|------------|------------|
| 2024-01-28T11:48:20.8785979Z | [REDACTED] | [REDACTED] |
| 2024-01-28T11:45:31.5317508Z | [REDACTED] | [REDACTED] |
| 2024-01-28T11:48:20.8785979Z | [REDACTED] | [REDACTED] |

An "Export to Excel" button is visible above the table. A green arrow points from the table area to the text "Results will show in matter of seconds / minutes!". Below the table, a code block shows the Kusto Query Language (KQL) query used to generate the results:

```
1 DeviceNetworkEvents
2 | where Timestamp > ago(30d)
3 | where RemoteIP in (
4     externaldata (IP_Address:string)
5     [https://check.torproject.org/torbulkexitlist"]
6     | project RemoteIP=IP_Address
7 )
8 | project Timestamp, DeviceId, DeviceName, ActionType, RemoteIP, RemotePort,
InitiatingProcessSHA1, InitiatingProcessSHA256, InitiatingProcessMD5,
InitiatingProcessFileName, InitiatingProcessId, InitiatingProcessCommandLine,
InitiatingProcessAccountDomain, InitiatingProcessAccountName
9
```

A green arrow points from the KQL code to the explanatory text below it: "This query checks for any communication from your network to the TOR network by comparing the remote IP addresses in your network events with the list of TOR exit nodes. The results include details such as the timestamp of the event, device ID and name, action type, remote IP and port, and information about the initiating process."

At the bottom of the interface, there's a prompt: "Ask anything about security, or type / for suggestions or * for promptbooks".

Use natural language query to ask Copilot for Security e.g. specific users communicating to TOR network

Results will show in matter of seconds / minutes!

It can also provide a ready-made KQL query to further help your team with the investigation

Scenario 6 – Searching for any TOR Activities

Custom Prompts / Scenarios specific to <Customer Name> day to day SecOps

who is the primary user of [REDACTED]

> 3 steps completed 36 seconds

Feb 15, 10:37 AM | 36 seconds

The primary user of the device with the name [REDACTED]D is [REDACTED]. The user's principal name is [REDACTED].com. The device is registered under the company ownership type and is managed by Microsoft Intune.

The device is part of 9 groups, including [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED].

Please note that this information is based on the latest data available and may vary if the device settings or user information have been updated recently.

References

[Microsoft Intune](#)

Looks right Needs improvement Inappropriate

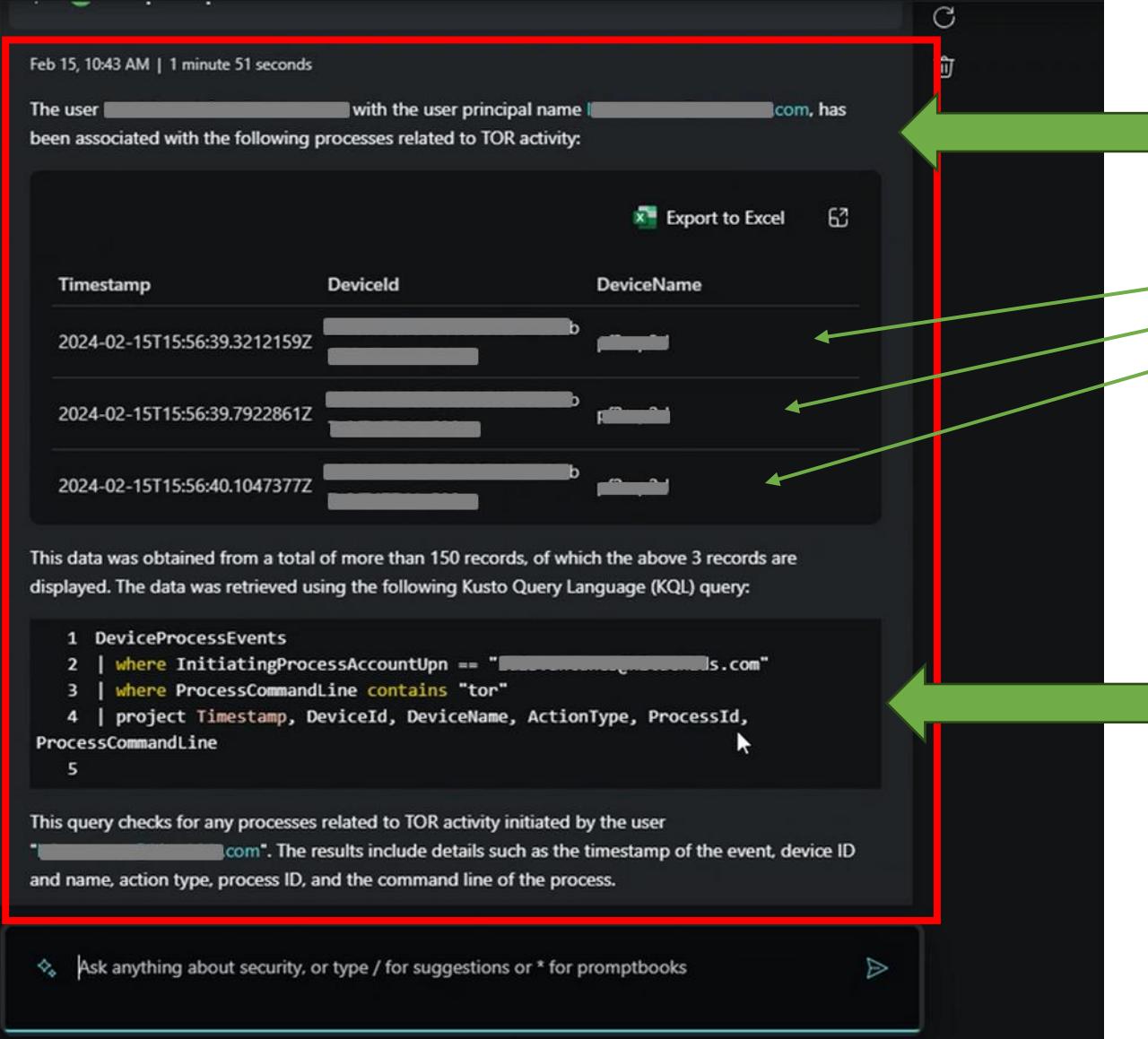
You can further ask more questions relating to the previous prompt (contextual)...enhancing the investigation experience of your SecOps team...

Detailed insights relating to the user of the affected device

Provides citation to where's the source of this information.

Scenario 6 – Searching for any TOR Activities

Custom Prompts / Scenarios specific to <Customer Name> day to day SecOps



Feb 15, 10:43 AM | 1 minute 51 seconds

The user [REDACTED] with the user principal name [REDACTED].com, has been associated with the following processes related to TOR activity:

| Timestamp | DeviceId | DeviceName |
|------------------------------|------------|------------|
| 2024-02-15T15:56:39.3212159Z | [REDACTED] | [REDACTED] |
| 2024-02-15T15:56:39.7922861Z | [REDACTED] | [REDACTED] |
| 2024-02-15T15:56:40.1047377Z | [REDACTED] | [REDACTED] |

Export to Excel

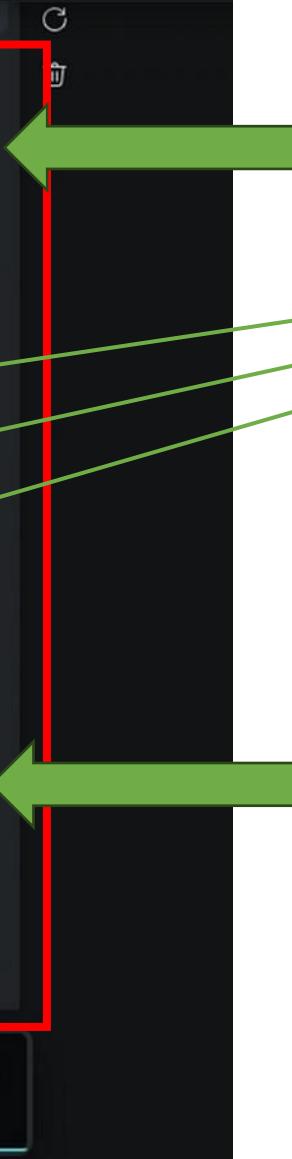
This data was obtained from a total of more than 150 records, of which the above 3 records are displayed. The data was retrieved using the following Kusto Query Language (KQL) query:

```
1 DeviceProcessEvents
2 | where InitiatingProcessAccountUpn == "[REDACTED].com"
3 | where ProcessCommandLine contains "tor"
4 | project Timestamp, DeviceId, DeviceName, ActionType, ProcessId,
ProcessCommandLine
5
```

This query checks for any processes related to TOR activity initiated by the user "[REDACTED].com". The results include details such as the timestamp of the event, device ID and name, action type, process ID, and the command line of the process.

| Ask anything about security, or type / for suggestions or * for promptbooks

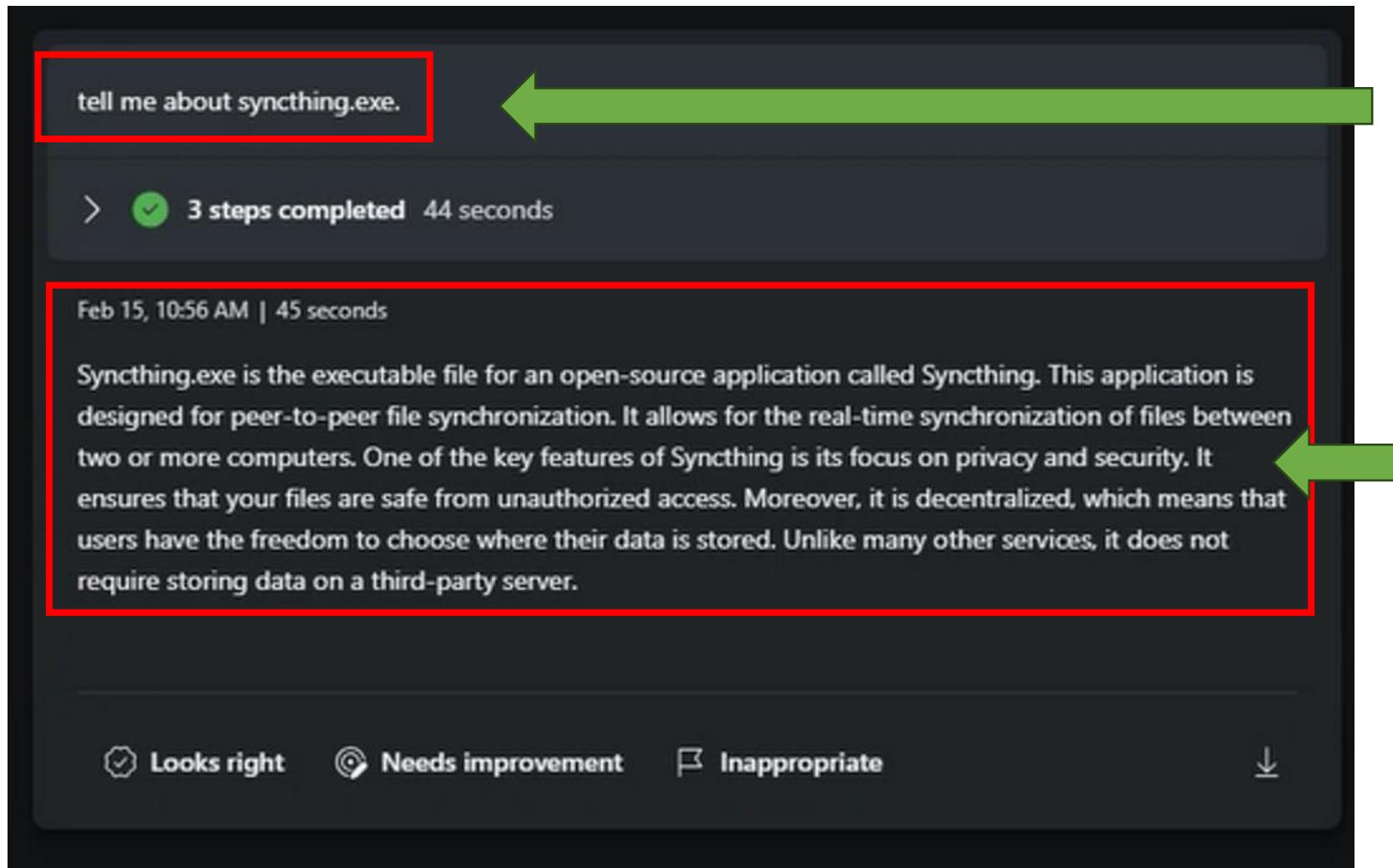
More details about the user involved e.g. x number of times TOR activity was detected!



Another ready-made KQL query (different perspective) to further help your team with the investigation

Scenario 7 – Investigate “unknown” file

Custom Prompts / Scenarios specific to <Customer Name> day to day SecOps



You can ask Copilot for Security to tell us more about process / PE file that may be prevalent in your environment

Leverage Copilot for Security integration with Microsoft Defender Threat Intelligence to investigate unknown “indicators” such as unknown files...see if they are affiliated with a known threat actor.

Scenario 8 – Provide DLP recommendations

Custom Prompts / Scenarios specific to <Customer Name> day to day SecOps

provide me a recommendation to minimize this incident

> Chose Generic 31 seconds

> Processed your request 10 seconds

> Preparing your response ... 8 seconds

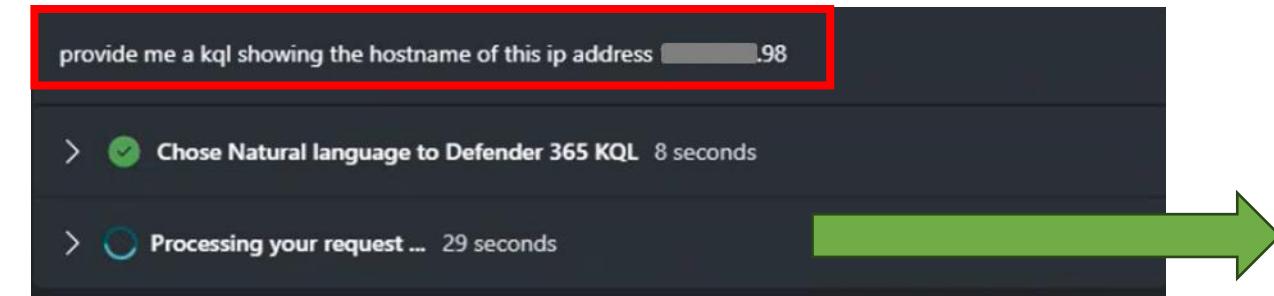
To minimize the impact of the incident involving multiple users and cloud applications with potential data exfiltration detected through DLP rules for Microsoft Teams, the following actions can be taken:

1. **Investigate the incident:** Identify the users involved, the data that was potentially exfiltrated, and the cloud applications that were used. This will help in understanding the scope of the incident.
2. **Notify the affected users:** Inform the users involved about the incident and advise them to change their passwords and to be vigilant for any suspicious activity in their accounts.
3. **Update DLP rules:** Review and update the Data Loss Prevention (DLP) rules to ensure they are effective in detecting and preventing data exfiltration. This could involve tightening the rules or adding new ones based on the nature of the incident.
4. **Monitor the situation:** Keep a close watch on the affected users' accounts and the cloud applications involved for any further suspicious activity.
5. **Conduct a security audit:** Perform a comprehensive security audit to identify any vulnerabilities or weaknesses that could have led to the incident. This could involve reviewing access controls, user privileges, and security configurations.

Leverage Copilot for Security to provide recommendations for specific incidents

Scenario 9 – KQL assistance

Upskill your security talent with cyber-trained generative AI



The system has completed 3 steps in 44 seconds. It shows the timestamp "Feb 20, 9:14 AM | 45 seconds" and the generated KQL query:

```
1 IdentityLogonEvents  
2 | where IPAddress == "1.2.3.4.98"  
3 | project DeviceName  
4
```

You can run this query in your Azure Sentinel workspace to get the hostname associated with the IP address. Please note that this query will return results based on the data available in your Azure Sentinel workspace. If the IP address has not been logged in any IdentityLogonEvents, the query may not return any results.

References

[Go hunt in Microsoft 365 Defender](#)

Feedback buttons: Looks right (checked), Needs improvement, Inappropriate. A downward arrow icon is also present.

Try the following prompts:

- *Looks for accounts that uploaded multiple code repositories to external web domain*
- *Find devices using torrenting software or browsing related to torrents*
- *Detect inactive users accounts those that have not logged for the past 60 days*
- *Identify strings in process command lines which match Base64 encoding format*

TIP: Generate Powershell Script

Showing here what else is possible with Copilot for Security

Write a powershell script to test the SMB versions and state across all the affected machines



This PowerShell script tests the SMB versions and state across all the affected machines: parkcity-win10s, parkcity-win10v, parkcity-win10r, parkcity-win11u, and parkcity-dc. The script defines a function `Test-SMBVersionAndState` that retrieves the SMB server configuration and state for a given machine. It then iterates through the list of machines, calls the function for each machine, and displays the results in a table format.



Data provided from Demo Environment

```
1 # Define the list of affected machines
2 $machineList = @("parkcity-win10s", "parkcity-win10v", "parkcity-win10r",
"parkcity-win11u", "parkcity-dc")
3
4 # Function to test SMB version and state
5 function Test-SMBVersionAndState {
6     param (
7         [string]$MachineName
8     )
9
10    try {
11        # Get SMB server configuration
12        $smbServerConfig = Get-SmbServerConfiguration -CimSession
$MachineName
13
14        # Check if SMB1 is enabled
15        $smb1Enabled = $smbServerConfig.EnableSMB1Protocol
16
17        # Check if SMB2 is enabled
18        $smb2Enabled = $smbServerConfig.EnableSMB2Protocol
19
20        # Check if SMB3 is enabled
21        $smb3Enabled = $smbServerConfig.EnableSMB3Protocol
22
23        # Get SMB server state
24        $smbServerState = Get-SmbServerState -CimSession $MachineName
25
26        # Create a custom object to store the results
27        $result = [PSCustomObject]@{
28            MachineName = $MachineName
29            SMB1Enabled = $smb1Enabled
30            SMB2Enabled = $smb2Enabled
31            SMB3Enabled = $smb3Enabled
32            SMBServerState = $smbServerState.ServerState
33        }
34
35        # Return the result
36        return $result
37    }
38    catch {
39        Write-Error "Error testing SMB version and state on $MachineName:
$_"
40    }
41 }
42
43 # Iterate through the list of machines and test SMB version and state
44 $results = @()
45 foreach ($machine in $machineList) {
46     $result = Test-SMBVersionAndState -MachineName $machine
47     $results += $result
48 }
49
50 # Display the results
51 $results | Format-Table -AutoSize
52
```

TIP: Summarize IOCs related to Intel Profile

Showing here what else is possible with Copilot for Security

Can you summarize the IOC's that is related to this intel profile? prepare it as list and give   me direct link for MDTI portal?

>  3 steps completed 33s

Data provided from Demo Environment

Mar 27, 5:27 AM | 35.34s

Here is a summary of the Indicators of Compromise (IOCs) related to the Mint Sandstorm threat actor:

- Total number of indicators: 72

A few examples of the IOCs are:

 Export to Excel 

| Indicator Type | Indicator Value | Last seen |
|----------------|--|----------------------------|
| hash_sha256 | 0696725EC2AACF47AB3746D 3A785FAD0D2DC48B71BCF37 AA8F0ED93F5BFC85 | 10/25/2023 13:06:27 +00:00 |
| hash_sha256 | 1CA65E5642EF40D933B50C16F C72C5546134338939D921BE0E C2A512AF4D5D18 | 10/20/2023 08:05:20 +00:00 |
| hash_sha256 | 1DBAF005861E716C641F9A8BF FD07A6FE46EEA75E90C9C8456 5FA12CE4CED287 | 10/23/2023 14:07:09 +00:00 |
| hash_sha1 | 22F3F57850EDE3019B4825AA6 C8808CC711223B9 | 08/23/2023 11:46:49 +00:00 |

For the complete list of IOCs and more information, you can visit the [MDTI Portal](#).



Under Threat Intelligence

Intel Profiles > Mint Sandstorm

Threat actor January 12, 2020

Mint Sandstorm

Aliases: PHOSPHORUS, Charming Kitten, Newcastle, APT35, Parastoo

Description TTPs Indicators (65)

Snapshot

The actor Microsoft tracks as Mint Sandstorm (PHOSPHORUS) is an Iran-affiliated activity group, active since at least 2013. Mint Sandstorm (PHOSPHORUS) is known to primarily target dissidents protesting the Iranian government, as well as activist leaders, the defense industrial base, journalists, think tanks, universities, and multiple government agencies and services, including targets in Israel and the United States. Mint Sandstorm (PHOSPHORUS) focuses on espionage. The actor is known to obtain initial access from broad scale exploitation of remote access devices to spear-phishing campaigns. Mint Sandstorm (PHOSPHORUS) also uses credential harvesting to obtain access to official work accounts as well as personal accounts. Previous tooling observed includes commodity malware, such as information stealers. The actor has also been observed developing custom malware, including their phishing documents that use template injection to load malicious content. Mint Sandstorm (PHOSPHORUS) has also conducted ransomware attacks against multiple organizations. Microsoft has tied such ransomware campaigns to Storm-0270 (DEV-0270), a sub-group of Mint Sandstorm (PHOSPHORUS). Mint Sandstorm (PHOSPHORUS) is tracked by other security companies as Charming Kitten and APT35. Mandiant refers to modern day Mint Sandstorm (PHOSPHORUS) as APT42.

Targeting Details

Mint Sandstorm (PHOSPHORUS) targets include Iranian citizens, especially those who are branded as dissidents by the Iranian government, along with political figures, journalists, and human rights activists.

External to Iran, there is a persistent effort against Western defense agencies, members of the U.S. defense industrial base, Middle Eastern experts/think tank analysts, and organizations that work on sanctions issues involving Iran.

Occasionally, Microsoft security researchers have observed one-off targeting involving world events. For example, with the coronavirus (COVID-19) pandemic, Microsoft observed targeting of large world health organizations by Mint Sandstorm (PHOSPHORUS). By contrast, the Mint Sandstorm (PHOSPHORUS) ransomware cluster uses opportunistic scanning to compromise organizations of all sizes, and then ransoms those organizations indiscriminately.

Microsoft Threat Intelligence speculates that the intent of the Mint Sandstorm (PHOSPHORUS) activity group is driven by political, economic, and intelligence requirements, as well as furthering cyber retaliation efforts against campaigns which influence Iranian interests in a global context. The patriotic hacking activities and defacements that founded the group appear to have ceased, demonstrated by the observed shift to espionage-focused targeting.

Country/region of origin

Iran

Targets

Digital, Print and Broadcast M...
Government Agencies & Servi...
Non-Government Organizatio...

TIP: Summarize Vulnerabilities related to software

Showing here what else is possible with Copilot for Security

The screenshot shows a Copilot for Security interface. At the top, there is a red box highlighting a text input field containing the query: "Keep using threat intelligence and tell me all the CVE's that is relevant to ManageEngine?". Below this, a progress bar indicates "3 steps completed 30s". A yellow banner reads "Data provided from Demo Environment". The main content area displays a list of six CVEs related to ManageEngine, each with a source link. At the bottom, a note says "For more information on these CVEs and related threat intelligence, you can visit the MDTI Portal."

Keep using threat intelligence and tell me all the CVE's that is relevant to ManageEngine?

> 3 steps completed 30s

Data provided from Demo Environment

Mar 27, 5:31 AM | 30.67s

Here are the CVEs related to ManageEngine that I found in the threat intelligence articles:

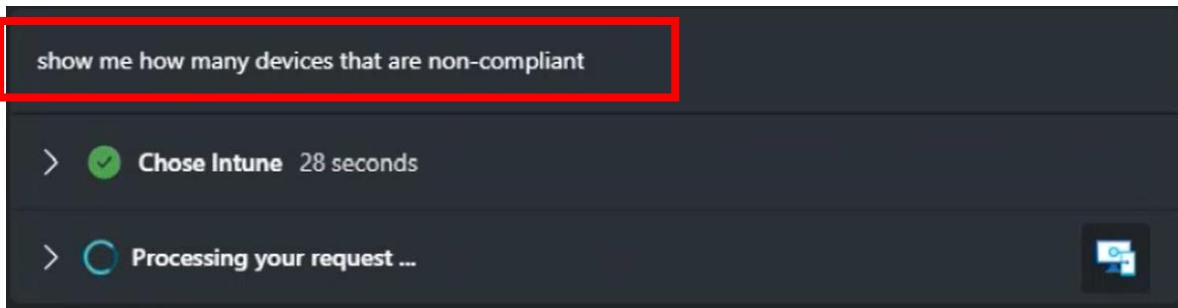
1. CVE-2022-47966: Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475 ([source](#))
2. CVE-2022-42475: Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475 ([source](#))
3. CVE-2023-27350: Multiple Iranian actors exploiting newly disclosed vulnerability in PaperCut for initial access ([source](#))
4. CVE-2021-40539: Mint Sandstorm exploits ManageEngine vulnerability in wave of seemingly opportunistic activity ([source](#))
5. CVE-2021-44515: FBI Flash: APT Actors Exploiting Newly-Identified Zero Day in ManageEngine Desktop Central ([source](#))
6. CVE-2021-44077: AA21-336A: APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus ([source](#))

For more information on these CVEs and related threat intelligence, you can visit the [MDTI Portal](#).

Leverage Copilot for Security integration with Microsoft Defender Threat Intelligence to summarize all CVE's related to a specific software e.g. ManageEngine in this example.

Scenario 10 – Show non-compliant device from Intune

Intune Integration with Copilot for Security



Gets insights from your Intune data (device attributes, configuration data, apps, policies). This information can help you understand your security posture and possibly troubleshoot device issues like misconfigured devices.

The results here shows all the non-compliant devices in Demo environment

The screenshot shows a report titled "Feb 20, 10:41 AM | 35 seconds" with a red box around the text: "There are a total of 500 devices that are non-compliant. However, it's not feasible to list all of them here due to the large number. I recommend using supported filters like the OS platform, compliance state, or a specific enrolled or active date range to narrow down a group of devices for investigation. For instance, you could ask for all the Windows non-compliant devices enrolled within a specific timeframe." Below this, another red box highlights the text: "Here are some examples of non-compliant devices:" followed by a table. A green arrow points from the text "The results here shows all the non-compliant devices in Demo environment" to the table.

| Device ID | User | Operating System |
|-----------|------------|------------------|
| ... | j...@a.com | iOS |
| ... | com | iOS |
| ... | n... | iOS |
| d... | 1... | iOS |
| ... | m... | iOS |
| ... | ... | iOS |

Scenario 11 – Embedded experience w/ Defender XDR

Defender XDR Integration with Copilot for Security

The screenshot shows the Microsoft Defender XDR interface. On the left is a navigation sidebar with various security-related options like Home, Incidents & alerts, Hunting, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices, Identities, Endpoints, Vulnerability management, Dashboard, Recommendations, Remediation, and Inventories. The main area is titled "Advanced hunting" and contains a search bar, a "Run query" button, and a "Security Copilot" button (which is highlighted with a red box). Below these are sections for Shared queries, My queries, and Community queries. A "Query" section displays KQL code for finding TOR activity. To the right, a "Security Copilot" panel is open, showing a conversation where it asks for TOR activity and provides a generated KQL query. A green arrow points from the text below to this panel.

Ask Copilot for Security to generate KQL for you for specific query

Security Copilot is embedded in Microsoft Defender XDR for security teams to efficiently summarize incidents, analyze scripts and codes, use guided responses to resolve incidents, generate KQL queries, and create incident reports.

Scenario 12: List Departing users doing data exfiltration

Not able to test this due to Insider Risk Management not enabled / setup

The image shows two screenshots side-by-side. On the left is the Microsoft Purview Insider risk management interface, which displays a message about needing permissions to get started. It includes sections for assigned permissions, benefits (detecting sensitive data leaks), and a preview of the Microsoft 365 Activity Explorer. A red arrow points from the bottom right of the Purview screenshot to the top right of the Copilot screenshot. On the right is the Microsoft Security Copilot interface, showing a summary of a Defender incident (ID 20259) and other security-related cards.

Steps needed to enable this scenario:

1. Enable Insider Risk Management (included as part of your M365 E5). See the steps [here](#).
2. Create Insider Risk Management Policy -> Data theft by departing users. This will monitor those users who have tendered their resignation.
3. Ensure Microsoft Purview is enabled in the Manage Plugins settings of Copilot for Security.

TIP: Departing users doing data exfiltration

Sample screenshot Copilot for Security integration with Insider Risk Management

Microsoft Purview PREVIEW

Search

New Microsoft Purview portal

Copilot

Potential data theft – Employee Departure

(86e52569) Potential data theft – Employee Departure

High Risk score: 100/100 Alert created on Apr 21, 2023 (UTC)

Activity that generated this alert Reduce alerts for this activity

Cumulative exfiltration activities

100/100 High severity | Dec 3, 2023 - Dec 18, 2023 (UTC)

348 events: All exfiltration activities with prioritized content:

More events than 100% compared to all users in org.

Priority content includes: 1 sensitive info types.

449 events: All exfiltration activities:

More events than 100% compared to all users in org.

449 events: Emails sent with attachments outside the organization:

More events than 100% compared to all users in org.

Note: 140 other activities have the same risk score of 100/100

View all activity

All risk factors Activity explorer User activity Forensic evidence

Filter: Show: All scored activity for this user Risk category: Any Activity Type: Any Reset all

Sort by: Date occurred

User activity scatter plot 6 Months 3 Months 1 Month

Triggering event: Exfiltration activity detected Mar 5, 2024 (UTC)

Exfiltration: Emails with attachments sent outside the organization Mar 5, 2024 (UTC) | Risk score: 75/100 30 emails: sent to 1 recipient outside the organization 21 emails: containing sensitive info, including: Project Obsidian

Access: Sensitive SharePoint files accessed Mar 5, 2024 (UTC) | Risk score: 5/100 14 events: Sensitive files accessed from 1 SharePoint site 13 events: Files containing sensitive info, including: Project Obsidian, U.S. Social Security Number (SSN), All Full Names, UAE Identity Card Number, Credit Card Number 6 events: Files that have labels applied, including: Project Obsidian

Triggering event: Exfiltration activity detected 35 annotations 37 annotations

Risk score

Alert summary Mar 8, 2024 3:04 PM

Here's the summary for Purview IRM alert:

The alert with Id: 86e52569-5953-4272-82b4-c8dae7e8cc0d is a High severity Insider Risk Management alert involving isaiah@woodgrove.ms detected on April 21, 2023 21:39:29 (UTC). The policy "Potential data theft – Employee Departure" was triggered when an HR Offboarding event was detected. The user's activity that led to this alert getting generated was identified as Cumulative Exfiltration. The alert is in Confirmed state and is being investigated. The alert also has a case "Case 034: Potential data leak" associated with it.

The user is considered High risk based on the following risk factors:

- Emails with attachments sent outside the organization (March 6, 2024 23:59:59 UTC) - User is found to be sending 30 emails with attachments outside the organization. The emails contained priority content and were sent to 1 recipient. A total of 30 emails were sent and 1 of them contained sensitivity info.
- Sensitive SharePoint files accessed (March 6, 2024 23:59:59 UTC) - User is found to be accessing 14 sensitive SharePoint files. The files contained priority content and were accessed from 1 SharePoint site with sensitivity label applied. A total of 5 instances of sensitivity info were found in the files.

Additionally, an HR event was detected on March 8, 2024 (UTC) indicating that the user's resignation date has been set.

AI generated. Verify for accuracy.

Data provided from Demo Environment

Copilot for Security User Context

We were not able to test some scenarios due to limited access rights to certain resources

show me the latest sentinel incidents

> ✓ Chose Sentinel 30 seconds

> ! Your role doesn't have access to that information. 1 second

> ✓ Prepared your response 4 seconds

Feb 20, 10:36 AM | 36 seconds

I'm sorry, but it appears that your account is not authorized to access the requested Microsoft Sentinel incidents data. Please ensure that you can access the source system directly with the credentials you are currently logged in as, and that any necessary privilege escalation has been performed in advance of your query.

✓ Looks right ! Needs improvement ✗ Inappropriate

does device ! Se has any security incident?

> ✓ Chose Incident Analysis 16 seconds

> ! Your role doesn't have access to that information. 2 seconds

> ✓ Prepared your response 5 seconds

Feb 20, 10:42 AM | 25 seconds

I'm sorry, but I'm unable to retrieve the security incident details for the device with ID 1 [REDACTED]-[REDACTED]. The account used to perform this operation does not have the necessary permissions to access this data. Please ensure that you have the appropriate access rights in the source system and that any necessary privilege escalation has been performed in advance of your query.

Security Copilot uses **on-behalf of authentication** to access security related data through active Microsoft plugins.

Specific Microsoft Entra roles must be assigned in order for a group or individual to access the Security Copilot platform. Once you're logged into the portal, your access determines what plugins are available to utilize.

Defender XDR Embedded Experience Capabilities



Incident Summary in Microsoft Defender XDR

Incidents > Email messages containing malicious URL removed after delivery involving multiple users

Email messages containing malicious URL removed after delivery involvi...

Informational | Resolved | ajourn@woodgrove.ms | Credential Phish

Attack story Alerts (7) Assets (8) Investigations (0) Evidence and Response (14) Recommended actions (20) Summary Similar incidents (5)

Alerts Incident graph Layout Group similar nodes

Play attack story Unpin all Show all

Dec 6, 2023 2:33 PM Resolved Email messages containing malicious URL removed after delivery 2 Users 2 Mailboxes

Dec 6, 2023 2:34 PM Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger

Dec 6, 2023 2:34 PM Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger

Dec 6, 2023 2:34 PM Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger

Dec 6, 2023 2:34 PM Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger

Dec 6, 2023 2:35 PM Resolved Email messages containing malicious URL removed after delivery 2 Users 2 Mailboxes

Dec 6, 2023 2:35 PM Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger

Dec 6, 2023 2:35 PM Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger

Incident graph showing communication and associations between users (pattif, debrab, pradeepg, meganb) and external entities (www.aconsciousrethink.com). Nodes represent users and emails, with edges indicating communication or association.

Communication Association

Security Copilot

Incident summary
Mar 5, 2024 5:59 PM

The informational severity incident 'Email messages containing malicious URL removed after delivery involving multiple users' occurred between 2023-12-06 06:33:02 UTC and 2023-12-06 06:37:29 UTC. It was tagged as Credential Phish.

- InitialAccess: At 2023-12-06 06:33:02 UTC, email messages containing a malicious URL 'hxwp://www.aconsciousrethink.com/8051/intresting-topics-to-talk-about/' were removed after delivery. The email, titled 'EXTERNAL Follow up -|Here is your next Security 101 content', impacted users 'pattif' and 'pradeepg'.
- InitialAccess: At 2023-12-06 06:34:05 UTC, another email with the same title and a similar malicious URL 'hxps://www.aconsciousrethink.com/8051/intresting-topics-to-talk-about/' was removed after being delivered to user 'debrab'.
- InitialAccess: At 2023-12-06 06:35:26 UTC, more email messages containing a malicious URL were removed after delivery, impacting users 'meganb' and 'pradeepg'.

AI generated. Verify for accuracy.



Guided response in Microsoft Defender XDR

Incidents > Email messages containing malicious URL removed after delivery involving multiple users

Email messages containing malicious URL removed after delivery involving multiple users

Informational | Resolved | ajourn@woodgrove.ms | Credential Phish

Attack story | Alerts (7) | Assets (8) | Investigations (0) | Evidence and Response (14) | Recommended actions (20) | Summary | Similar incidents (5)

Alerts

- Dec 6, 2023 2:33 PM • Resolved Email messages containing malicious URL removed after delivery 2 Users 2 Mailboxes
- Dec 6, 2023 2:34 PM • Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger
- Dec 6, 2023 2:34 PM • Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger
- Dec 6, 2023 2:34 PM • Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger
- Dec 6, 2023 2:35 PM • Resolved Email messages containing malicious URL removed after delivery 2 Users 2 Mailboxes
- Dec 6, 2023 2:35 PM • Resolved Email messages containing malicious URL removed after delivery 2 Users 2 Mailboxes
- Dec 6, 2023 2:35 PM • Resolved Email messages containing malicious URL removed after delivery 2 Users 2 Mailboxes

Incident graph

The incident graph displays the following connections:

- pattif (User) connects to www.aconsciousrethink.com (External URL).
- pattif (User) connects to debrab (User).
- pattif (User) connects to [EXTERNAL] Follow up - Here is your next Security 101 content (Email).
- pattif (User) connects to [EXTERNAL] Patti Don't miss 4341-Con Event next month (Email).
- debrab (User) connects to www.aconsciousrethink.com (External URL).
- debrab (User) connects to debrab (User).
- debrab (User) connects to [EXTERNAL] Follow up - Here is your next Security 101 content (Email).
- pradeepg (User) connects to www.aconsciousrethink.com (External URL).
- pradeepg (User) connects to [EXTERNAL] Follow up - Here is your next Security 101 content (Email).
- pradeepg (User) connects to [EXTERNAL] New design spec Process | SpecDis-1 (Email).
- meganb (User) connects to [EXTERNAL] Follow up - Here is your next Security 101 content (Email).

Communication | Association

Incident details

Assigned to: ajourn@woodgrove.ms | Incident ID: 20847

Classification: True alert | Categories: Initial access

First activity: Dec 6, 2023 2:33:02 PM | Last activity: Dec 6, 2023 2:37:29 PM

Impacted assets

Users (4): Debra Berger, Patti Fernandez, Megan Bowen, Pradeep Gupta

Mailboxes (4): User display name

Patti Fernandez, Pradeep Gupta, Debra Berger, Megan Bowen

Active alerts in this incident (0/7)

High (0) | Medium (0) | 2 more

View all alerts

Security Copilot

Guided response

Mar 5, 2024 5:59 PM | Completed recommendations 1/6

Status: All

Triage

Containment

New | Isolate device Test-User

This action will isolate the device from the network. It will remain connected to the Microsoft Defender for Endpoint service.

Isolate device | View device

AI generated. Verify for accuracy.

Remediation

New | Delete similar emails

We found emails that are very similar to emails involved in this incident. Delete these emails to contain the attack.

Soft delete emails | View similar emails

AI generated. Verify for accuracy.

New | Suspend the account Test User in AAD

Risky sign-ins were detected after the user Test User clicked a known phishing link. Stop possible compromise by deactivating the user account.

Suspend user in Azure AD | View user

AI generated. Verify for accuracy.

Analyze the suspicious script in Microsoft Defender XDR



Incidents > Multi-stage incident involving Initial access & Command and control including Ransomware on multiple endpoints reported by multiple sources > PsExec launched a command or script

Part of incident: Multi-stage incident involving Initial access & Command and control including Ransomware on multiple endpoints reported by multiple sources [View incident page](#)

parkcity-win10v Risk level High ...
Windows10 ParkCity Alpineskihouse

PARKCITY\jonaw
Account Executive

Alert story

2:44:44 PM powershell.exe executed a script Remote execution
2:44:45 PM powershell.exe executed a script Remote execution
2:44:49 PM powershell.exe executed a script Remote execution
2:44:49 PM [7720] powershell.exe -EncodedCommand YwB1AHIAbAAgAHYAZQBjAHQAbwB... Remote execution

Command line
[Analyze](#)
powershell.exe -EncodedCommand YwB1AHIAbAAgAHYAZQBjAHQAbwByAHMAYQBuAGQAYQByAHIAbwB3AHMALgBjAG8AbQANAAoADQAKAGYAdQBuAGMAdABpAG8AbgAgAEcAZQB0AC0AVQBzAGU

Command line (decoded)
[Analyze](#)
curl vectorsandarrows.com
function Get-UserPRTToken

Process id 7720
Execution details Token elevation: Full, Integrity level: High
Image file path C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Image file SHA1 d3ea331bdcc214ec7ea134492d2af8cf5195cc63
Image file creation time Oct 15, 2023 11:37:19 PM
Image file last modification time Oct 15, 2023 11:37:19 PM

Script analysis

Script analysis Mar 5, 2024 6:13 PM

The provided script performs several actions that are indicative of malicious activity. It starts by making a curl request to the URL "vectorsandarrows.com". Then, it defines and calls a function `Get-UserPRTToken` to interact with the `browsercore.exe` process and retrieve the user's Primary Refresh Token (PRT) from Microsoft's OAuth2 authorization endpoint. The retrieved PRT is written to a file named `phtt.bin` in the system's temp directory. The script also downloads the `psexec.exe` tool from the Sysinternals live site and saves it as `notepad.exe` in the system's temp directory. Finally, it downloads the `mimikatz_trunk.zip` file from the GitHub repository of Mimikatz and saves it as `mechanizeprune.zip` in the system's temp directory. These actions suggest that the script is likely part of a larger attack that involves credential theft and remote command execution.

1. The script starts by making a curl request to the URL "vectorsandarrows.com".
2. The script defines a function `Get-UserPRTToken` which is used to interact with the `browsercore.exe` process to retrieve the user's Primary Refresh Token (PRT) from Microsoft's OAuth2 authorization endpoint.
3. The script calls the `Get-UserPRTToken` function and writes the output to a file named `phtt.bin` in the system's temp directory.

Details

INSIGHT
Quickly classify alerts about threats
Classify alert

Alert state Not Set
[Set Classification](#)

Classification Not Set
[Set Classification](#)

Alert details

Category Lateral movement

Detection source EDR

curl vectorsandarrows.com

function Get-UserPRTToken

Get-UserPRTToken > \$Env:temp\phtt.bin

Advance Hunting query in Microsoft Defender XDR

Home

Exposure management

Investigation & response

Incidents & alerts

Incidents

Alerts

Hunting

- Advanced hunting
- Custom detection rules

Actions & submissions

Secure score

Partner catalog

Threat intelligence

Assets

Microsoft Sentinel

Identities

Endpoints

Email & collaboration

Cloud apps

Advanced hunting

Explore your content from Sentinel

All data from Sentinel, including tables, queries and functions is now available for you to explore.

New query*

Schema Functions Queries ...

Search

Run query Set in query Save Share link Security Copilot

Query

```
1 AADNonInteractiveUserSignInLogs
2 | where TimeGenerated > ago(14d)
3 | where isempty(MfaDetail) or MfaDetail == "disabled"
4 | project TimeGenerated, UserDisplayName, UserPrincipalName, MfaDetail
5
```

Getting started Results Query history

Export 500000 items Search 00:01.391 Low

| TimeGenerated | UserDisplayName ↑ | UserPrincipalName | MfaDetail |
|------------------------|-------------------|----------------------|-----------|
| Mar 5, 2024 9:15:06 AM | A-Shawni Mitchell | asmitch@woodgrove.ms | |

Help resources

Security Copilot

Mar 5, 2024 6:16 PM

Write a query to find top 10 vulnerabilities based on M365 Defender

Mar 5, 2024 6:17 PM

Here is the Kusto Query Language (KQL) query that you can use to find the top 10 vulnerabilities based on Microsoft 365 Defender:

```
AlertInfo
| where ServiceSource == "Microsoft 365 Defender"
| summarize count() by AlertId
| top 10 by count_desc
```

Add and run

AI generated. Verify for accuracy.

Mar 5, 2024 6:21 PM

Write a hunting query to identify users that have logged on without MFA in last 14 days.

Mar 5, 2024 6:22 PM

Here is the Kusto Query Language (KQL) query that you can use to identify users who have logged on without Multi-Factor Authentication (MFA) in the last 14 days:

```
AADNonInteractiveUserSignInLogs
| where TimeGenerated > ago(14d)
| where isempty(MfaDetail) or MfaDetail == "disabled"
| project TimeGenerated, UserDisplayName, UserPrincipalName,
```

Add and run

AI generated. Verify for accuracy.

Ask a question to generate a query

Device Summary in Microsoft Defender XDR



Device Inventory > cpc-khotz-oakj9

cpc-khotz-oakj9

No known risks | Criticality: None | Active | Full Remediation - Cloud PCs

Overview Incidents and alerts Timeline Security recommendations Inventories Discovered vulnerabilities Missing KBs Security policies

Device details

| | |
|--------------|---|
| Category | Type |
| Endpoint | - |
| Subtype | Discovery source |
| Workstation | Endpoint |
| Domain | OS |
| AAD joined | Windows 11 64-bit (Release 22H2 Build 22621.1555) |
| SAM name | Asset group Full Remediation - Cloud PCs |
| Health state | Data sensitivity |
| Active | None |
| IP addresses | MAC address |
| 10.1.0.6 | - |

Active alerts (Last 180 days)

No active alerts or incidents

Security assessments

Exposure level: High

65 active security recommendations

Discovered vulnerabilities (392)

Critical (15) High (270) Medium (107)

Logged on users (Last 30 days)

0 logged on users

There were no logged on users during the given time range

View all recommendations

Security Copilot

Device summary
Mar 5, 2024 6:35 PM

The device named 'cpc-khotz-oakj9', owned by Kristina Hotz (khotz@woodgrove.ms), is a Cloud PC with a high exposure level. It has several risky settings and vulnerable software installed, which significantly impacts its security posture.

- Antivirus - Tamper Protection: Status is off, leaving the device vulnerable to malicious apps that can change important Microsoft Defender for Endpoint settings.
- Antivirus - PUA Protection: Status is non-blocking, making the device susceptible to unwanted applications with potentially malicious behavior.
- Antivirus - Signature: The antivirus signature was last updated a year ago, potentially exposing the device to recently discovered viruses.
- Exploit Guard: Controlled folder access is off, making key system files vulnerable to changes made by malicious and suspicious apps.
- Firewall: Several firewall notifications are off, which could potentially allow an attacker to remotely exploit a weakness in a network service.
- Attack Surface Reduction: Status is off, leaving the device vulnerable to common attack techniques used in cyber attacks and malicious software.
- Credential Guard: Status is off, potentially allowing malicious attackers to gain access to user credentials stored in memory.

Vulnerable software

- .net_framework_4.8.1.0: This software has a critical severity level, indicating a high risk.
- windows_11_10.0.22621.1555: This software has a critical severity level, indicating a high risk.
- windows_defender_1.1.19500.2: This software has a high severity level, indicating a significant risk.
- defender_security_intelligence_updates

File Analysis in Microsoft Defender XDR



Incidents > Multi-stage incident involving Privilege escalation on multiple endpoints reported by multiple sources > Rubeus.exe

Rubeus.exe

Signer: ⚠ Unsigned • Size: 429.06 KB

File was submitted for Deep analysis. Status: Success. See report

Overview Incidents & Alerts Observed in organization File names File content Deep Analysis

File Details

Object details

SHA1
fc870d086c53ded2e9430 🔗
0f7569aa9478186f2c7

SHA256
a1fddd460edd35ed449d 🔗
32cc43bc15675c48a314a
6fa5fb158e3bc4fea460be
1

MD5
7a7c8fa61d748cbe00348 🔗
46015e5bd8a

File size
429.06 KB

Is PE
true

Signer
✗ Unsigned file
⚠ This file's signer is unknown

View in VirusTotal

Incidents & Alerts

9 active alerts, 2 incidents

High (3) Medium (3) Low (2) 1 more

View Incidents & Alerts

VirusTotal

54/69 (High risk)

VirusTotal Ratio

View all devices

Security Copilot Manage indicator ...

Observed devices (last 30 Days)

2 devices

| Date (First / Last) | Devices |
|----------------------|--|
| Feb 15, 2024 (First) | 🔗 parkcity-win10v... |

File analysis Mar 5, 2024 7:06 PM

Overview

The file has been detected as malicious by 54 out of 69 engines in the VirusTotal Static Scan, with labels such as "Hacktool", "Trojan", and "Malware". The absence of a digital certificate further raises suspicion. The PE Metadata reveals an image size of 458752, but lacks company information. The file has not been quarantined by an analyst yet. These factors suggest a potential security risk associated with the file.

Hide details

PE header

The PE header information reveals that the entry point address is 430518, the image size is 458752, and the machine type is 332. The image size is relatively large, which could indicate the presence of additional, potentially malicious, code. The machine type 332 corresponds to Intel 386 or later processors and compatible processors, which is a common target for many types of malware due to its widespread use.

Strings

The strings present in the file provide some insight into its potential behavior. Several strings suggest interactions with Kerberos, a network authentication protocol, such as "KERB_TICKET_CACHE_INFO_EX2", "KERB_PA_PAC_REQUEST", and "KerbSetPasswordMessage". This could indicate that the file is attempting to manipulate or exploit Kerberos authentication, which is a common tactic used in privilege escalation attacks.

Other strings like "TestUsernamePassword", "get_Domain", and "get_PdcRoleOwner" suggest that the file may be attempting to gather sensitive information, such as usernames, passwords, and domain details. This could be indicative of information gathering or credential theft behavior.

The string "ComVisibleAttribute" suggests that the file may be interacting with COM objects, which

Incident Report in Microsoft Defender XDR



Incidents > Email messages containing malicious URL removed after delivery involving multiple users

Email messages containing malicious URL removed after delivery involving multiple users

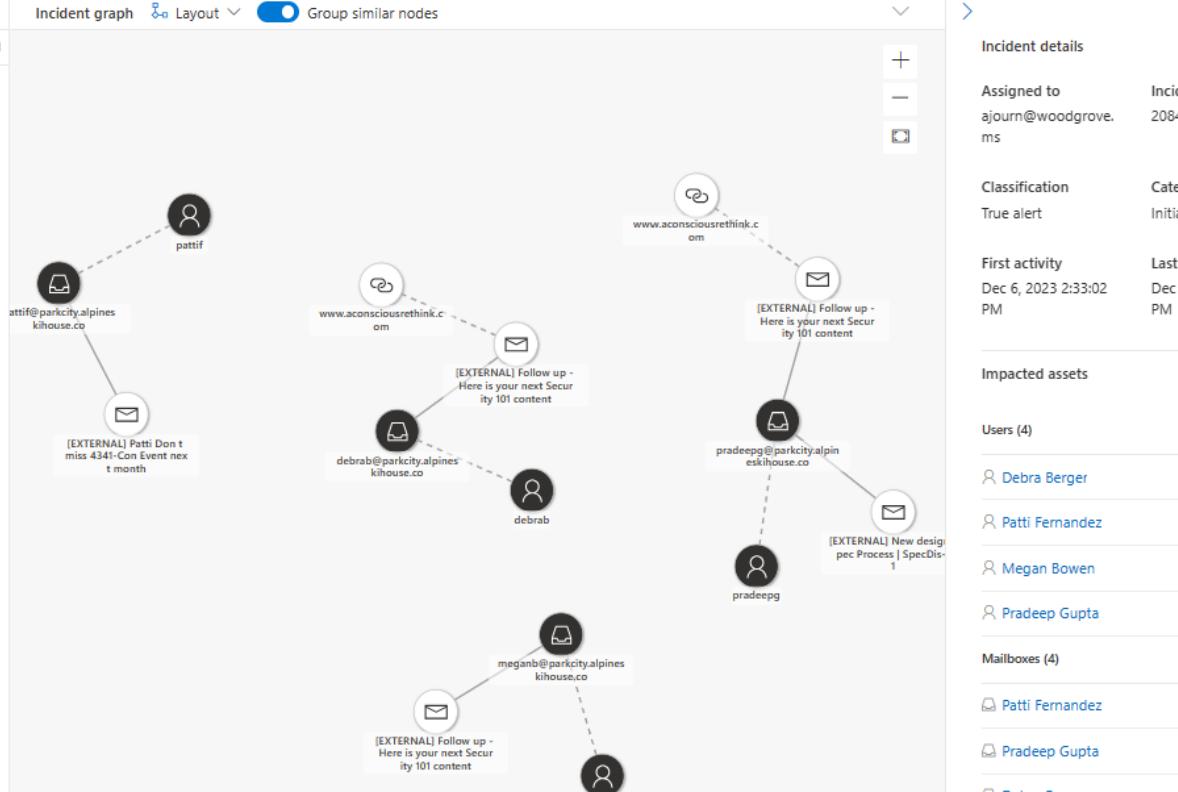
Informational | Resolved | ajourn@woodgrove.ms | Credential Phish

Attack story Alerts (7) Assets (8) Investigations (0) Evidence and Response (14) Recommended actions (20) Summary Similar incidents (5)

Alerts

- Dec 6, 2023 2:33 PM • Resolved Email messages containing malicious URL removed after delivery 2 Users 2 Mailboxes
- Dec 6, 2023 2:34 PM • Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger
- Dec 6, 2023 2:34 PM • Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger
- Dec 6, 2023 2:34 PM • Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger
- Dec 6, 2023 2:34 PM • Resolved Email messages containing malicious URL removed after delivery Debra Berger Debra Berger
- Dec 6, 2023 2:35 PM • Resolved Email messages containing malicious URL removed after delivery 2 Users 2 Mailboxes
- Dec 6, 2023 2:35 PM • Resolved Email messages containing malicious URL removed after delivery 2 Users 2 Mailboxes
- Dec 6, 2023 2:35 PM • Resolved Email messages containing malicious URL removed after delivery 2 Users 2 Mailboxes
- Dec 6, 2023 2:35 PM • Resolved Email messages containing malicious URL removed after delivery 2 Users 2 Mailboxes

Incident graph Layout Group similar nodes



Communication --- Association

Incident details

| | |
|------------------------|------------------------|
| Assigned to | Incident ID |
| ajourn@woodgrove.ms | 20847 |
| Classification | Categories |
| True alert | Initial access |
| First activity | Last activity |
| Dec 6, 2023 2:33:02 PM | Dec 6, 2023 2:37:29 PM |

Impacted assets

Users (4)

- Debra Berger
- Patti Fernandez
- Megan Bowen
- Pradeep Gupta

Mailboxes (4) User display name

- Patti Fernandez Patti Fernandez
- Pradeep Gupta Pradeep Gupta
- Debra Berger Debra Berger
- Megan Bowen Megan Bowen

Active alerts in this incident (0/7)

Classification

True positive - Phishing

The incident was classified as a "TruePositive" due to the detection of a coordinated phishing campaign involving multiple users. The emails contained URLs

Incident report

Incident report Mar 5, 2024 7:15 PM

Incident title Email messages containing malicious URL removed after delivery involving multiple users

Incident details

| | |
|--------------|---|
| Analysts | ajourn@woodgrove.ms shobhitg@woodgrove.ms sewasong@woodgrove.ms |
| Time created | 12/06/2023 06:33:02 |
| First log | 12/06/2023 09:25:04 |
| Last log | 03/04/2024 06:27:02 |
| Time closed | 02/17/2024 21:46:02 |

Incident summary

The informational severity incident 'Email messages containing malicious URL removed after delivery involving multiple users' occurred between 2023-12-06 06:33:02 UTC and 2023-12-06 06:37:29 UTC. It was tagged as Credential Phish.

- InitialAccess: At 2023-12-06 06:33:02 UTC, email messages containing a malicious URL 'hxps://www.aconsciousrethink.com/8051/interesting-topics-to-talk-about/' were removed after delivery. The email subject was '[EXTERNAL] Follow up - Here is your next Security 101 content' and it impacted users 'pattif' and 'pradeepg'.
- InitialAccess: At 2023-12-06 06:34:05 UTC, another email with the same subject and a similar malicious URL 'hxps://www.aconsciousrethink.com/8051/interesting-topics-to-talk-about/' was removed after being delivered to user 'debrab'.
- InitialAccess: At 2023-12-06 06:35:26 UTC, more email messages containing a malicious URL were removed after delivery, impacting users 'meganb' and 'pradeepg'.

Export Incident as PDF in Microsoft Defender XDR



Incidents > Email messages containing malicious URL removed after delivery involving multiple users

Email messages containing malicious URL removed after delivery involving multiple users

Informational | Resolved | ajourn@woodgrove.ms | Credential Phish

Attack story Alerts (7) Assets (8) Investigations (0) Evidence and Response (14) Recommended actions (20) Summary Similar incidents (5)

Security Copilot Manage incident Activity log Ask Defender Experts ...

Generate incident report Export incident as PDF

Security Copilot

Manage incident ...

Activity log

Ask Defender Experts

Generate incident report

Export incident as PDF

Your exported PDF is ready

We'll keep the PDF available for download for a few minutes.

Download Cancel

Executive summary

Incident details

Copilot

Incident summary
The informational severity incident 'Email messages containing malicious URL removed after delivery involving multiple users' occurred between 2023-12-06 06:33:02 UTC and 2023-12-06 06:37:29 UTC. It was tagged as Credential Phish.

- InitialAccess:** At 2023-12-06 06:33:02 UTC, email messages containing a malicious URL '<http://www.aconsciousrethink.com/8051/interesting-topics-to-talk-about/>' were removed after delivery. The email, titled '[EXTERNAL](#) Follow up - Here is your next Security 101 content', impacted users 'pattif' and 'pradeepg'.
- InitialAccess:** At 2023-12-06 06:34:05 UTC, another email with the same title and a similar malicious URL '<http://www.aconsciousrethink.com/8051/interesting-topics-to-talk-about/>' was removed after being delivered to user 'debrab'.
- InitialAccess:** At 2023-12-06 06:35:26 UTC, more email messages containing a malicious URL were removed after delivery, impacting users 'meganb' and 'pradeepg'.

AI generated. Verify for accuracy.

Analysts involved in the incident:
ajourn@woodgrove.ms, shobhitg@woodgrove.ms, sewasong@woodgrove.ms

Classification

True alert - Phishing

Copilot

Classification reason
The incident was classified as a "TruePositive" due to the detection of a coordinated phishing campaign involving multiple users. The

Threat Intelligence copilot in Microsoft Defender XDR



Intel Profiles

Intel Profiles are a definitive source of Microsoft's shareable knowledge on tracked threat actors, malicious tools, and vulnerabilities, curated and continuously updated by Microsoft Threat Intelligence experts to provide relevant and actionable threat context.

Threat actors (205) Tools (70) Vulnerabilities (76)

Country/region of Origin Targets Search by keyword

Profile ↑ Country/region of ori... Targets Defender TI indicators

Aqua Blizzard Russia Government Agencies & 2530
Government Agencies &
Non-Government Organ
Aliases: ACTINIUM, Armageddon, Gamaredon, Primitive Bear, SectorC08, shuckworm, UNC530
The actor that Microsoft tracks as Aqua Blizzard (ACTINIUM) is a nation-state activity group based out of Russia. The Ukrainian government has publicly attributed this group to the Russian Federal Security Service (FSB). Aqua Blizzard (ACTINIUM) is known to primarily target organizations in Ukraine including government entities, military, non-governmental organization...

Blue Tsunami Israel Financial Services 0
Non-Government Organ
Other business entities
The actor Microsoft tracks as Blue Tsunami is a private sector offensive actor (PSOA) group based out of Israel. Microsoft assesses with high confidence that Blue Tsunami activity is strongly associated with Black Cube, an Israeli private

Security Copilot

Mar 5, 2024 10:29 PM

Give me an overview of the most active threats in my environment.

Mar 5, 2024 10:29 PM

Here are the most active threats in your environment:

Intel Profiles

- Storm-0861: The actor that Microsoft tracks as Storm-0861 (DEV-0861) is an Iran-based activity group. Storm-0861 (DEV-0861) is known to target organizations in the Middle East. Storm-0861 (DEV-0861) focuses on scanning and remote exploitation of target systems. [Intel Profile Link](#)
- Storm-0784: Storm-0784 is an Iran-based activity group with ties to the Islamic Revolutionary Guard Corps (IRGC). Storm-0784 primarily pursues Israeli organizations and specializes in targeting industrial control systems and 'Internet of Things' (IoT) devices. [Intel Profile Link](#)
- Magenta Dust: Note: Microsoft has updated reporting on Magenta Dust, the group formerly tracked as PROMETHEUM and Magenta Sandstorm, to reflect the group's ties to Turkey. Magenta Dust (PROMETHEUM) is an activity group who has carried out operations at least as far back as 2012. Magenta Dust has primarily sought information from individuals of interest and carried out operations targeting individuals in nearly 50 countries. Magenta Dust operators have used relatively sophisticated tradecraft, notably, high-end adversary-in-the-middle (A2M) and inline traffic inception attacks. Additionally, in May

Tell me about Aqua

Threat analytics

Threat intel reports are being updated in stages to align with the Microsoft 365 Defender rebrand into Microsoft Defender XDR.

| Ransomware | Extortion | Phishing | Hands on keyboard | Activity group | Vulnerability | Attack campaign | Tool or technique |
|------------|-----------|----------|-------------------|----------------|---------------|-----------------|-------------------|
| 94 | 0 | 57 | 0 | 177 | 106 | 0 | 0 |

Latest threats

| Vulnerability profile: Mirth Connect CVE-2023-37... | Threat overview: Cloud identity abuse | Tool profile: KdcSponge |
|---|---|---|
| 0 / 0 | 275 / 962 | 23 |
| Vulnerability profile: CVE-2024-1709 and CVE-20... | Technique profile: Password spray attacks | Threat overview: On-premises credential theft |
| 0 / 0 | 216 / 750 | 23 |
| Vulnerability profile: Multiple vulnerabilities in Iva... | Threat overview: Human-operated ransomwa... | Technique profile: Kerberos attacks |
| 0 / 0 | 179 / 888 | 23 |
| Vulnerability profile: CVE-2024-21412 Internet Sh... | Threat overview: On-premises credential theft | Actor profile: Jade Sleet |
| 0 / 0 | 156 / 777 | 23 |

Active Alerts Resolved Alerts 1 more

High-impact threats

| Threat overview: Cloud identity abuse | Tool profile: KdcSponge |
|---------------------------------------|-------------------------|
| 275 / 962 | 23 |

Active Alerts Resolved Alerts 1 more

Highest exposure threats

| Threat overview: On-premises credential theft | Technique profile: Kerberos attacks |
|---|-------------------------------------|
| 23 | 23 |

Actor profile: Jade Sleet

High 70-100 Medium 30-69 Low 0-29

Search 382 items Customize columns Filter

| Threat | Alerts | Impacted assets | Threat exposure level | Misconfigured devices | Vulnerable |
|--------------------------------------|--------------|-----------------|-----------------------|-----------------------|---------------|
| Vulnerability profile: Mirth Con... | 0 active / 0 | | 0 - Low | 79 | 0 |
| Vulnerability profile: CVE-2024-... | 0 active / 0 | | 0 - Low | 79 | 0 |
| Vulnerability profile: Multiple v... | 0 active / 0 | | 0 - Low | 79 | 0 |
| Vulnerability profile: CVE-2024-... | 0 active / 0 | | 6 - Low | 79 | 12 |
| Tool profile: KdcSponge | 0 active / 0 | | 23 - Low | 79 | Not available |

Ask anything about threat intelligence...

Purview Embedded Experience Capabilities

DLP Alert Summary



Microsoft Purview

https://purview.microsoft.com

Contoso | Microsoft Purview

Search

Try the new Microsoft Purview

Alerts

Export Refresh

Filter Reset Filters

Time range: 1/23/2023-2/15/2023 User: Any Alert status: Any Alert severity: Any

- Alert name
- DLP policy match for document 'sales-strategy2023.doc' in SharePoint
- DLP policy match for document 'resume_345.doc' in SharePoint
- DLP policy match for document 'resume_345.doc' in SharePoint
- DLP policy match for document 'resume_345.doc' in SharePoint
- DLP policy match for document 'resume_345.doc' in SharePoint
- DLP policy match for document 'Q2-Customer Data.xlsx'
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint

Alert: DLP policy match for document 'Q2-Customer Data.xlsx'

Details Events User activity summary

Alert summary by Security Copilot

The low severity DLP (Data Loss Prevention) alert with ID d1583893090588d-2349d-423085-0909328fbk2948 was generated on 1 Feb 2023 9:03 AM. The alert is currently in "Active" status and is associated with the user jordan.minke@contoso.com. The file involved in this alert is Q2-CustomerData.xlsx, located at <https://contoso.sharepoint.com/sites/Project1>.

The policy responsible for this alert is named "U.S. Financial Data Default Policy" with Policy ID efb767b0-4b45-4948-94b9-b63fb3a773ae. The rule that triggered the alert is "Check Financial Leak" with Rule ID 4bebff68-ab11-4f05-a11a-9cd77323a97.

The file was found to contain Credit Card information which is blocked from sharing under the purview of above policy. Additionally, Jordan Minke is marked as Medium risk level in Insider Risk Management.

AI generated. Verify for accuracy.

Alert ID
583893090588d-2349d--423085-0909328fbk2948

Alert status
Active

Alert severity
Low

Time detected
1 Feb 2023 9:03 AM

View details ...

Insider Risk Alert Summary



Microsoft Purview

https://purview.microsoft.com

Contoso | Microsoft Purview

Search

Try the new Microsoft Purview

Home

Insider Risk Management

Overview

Alerts

Cases

Policies

Users

Notice templates

Adaptive protection (preview)

Solutions

Related

Communication compliance

Data Loss Prevention

Information barriers

(7bbc3040) Data theft by departing users

High severity Risk score: 90/100 Alert created on Sept 30, 2023

Activity that generated this alert

Data infiltration: Files downloaded from unallowed site
87/100 High severity | Sept 28, 2023 (UTC)
12 events: Files downloaded from 1 unallowed site
8 events: Files that have labels applied, including: Project Alpha
Factors that impacted risk score
Includes unallowed domains (1 event)

Reduce alerts for this activity

Triggering event

Sept 25, 2023 (UTC)
An HR connector imported a resignation date for this user.

User details

jdoe@ediscodf.onmicrosoft.com
View all details

User alert history

Last 30 days

| Event Type | Count |
|------------------------------------|----------|
| Data theft for departing employees | 3 alerts |
| Sensitive data leaks | 1 alert |
| Security violations | 2 alerts |

Summary Activity explorer User activity Forensic evidence

Risk factors

| Category | Value |
|-------------------------------|------------------------------|
| Top exfiltration activities | 1.9K exfiltration activities |
| File uploads to cloud storage | 1,181 |
| Files copied to USB | 342 |
| Files shared externally | 181 |

[View all exfiltration activities](#)

| Category | Value |
|---------------------------------------|--|
| Cumulative exfiltration activities | High severity cumulative exfiltration activities detected from 9/24-9/28 |
| File downloads from SharePoint Online | More events than 99% other users |
| User | 5,240 |
| Org average | 838 |
| Files copied to USB | More events than 95% of other users |
| User | 1,272 |
| Org average | 324 |
| Documents printed | More than 92% of other users |
| User | 342 |
| Org average | 120 |

[View all cumulative exfiltration activities](#)

| Category | Value |
|-----------------------|-----------------------|
| Sequences of activity | No sequences detected |

| Category | Value |
|--------------------------------|----------------------------------|
| Unusual activity for this user | 3 patterns of unusual activities |
| Priority content | No priority content detected |
| Unallowed domains | 4 unallowed domains |

Security Copilot

Alert summary

The alert with alert id: 7bbc3040 is a high severity Insider Risk Management alert involving Jane Doe that was detected on September 30, 2023. The policy "Data theft by departing users" was triggered when the user submitted their resignation on September 28, 2023. The user was involved in 2 events where files containing sensitivity labels were downloaded from an unallowed site that led to this alert being generated. The alert is currently in "Needs review" state.

AI generated. Verify for accuracy.

Communication Compliance Investigation



Microsoft Purview

https://purview.microsoft.com

Contoso | Microsoft Purview

Communication Compliance > Policies > Inappropriate text policy

Pending 34 Resolved 12 Exports

Filter set: Default Save

Body/Subject: All values Date: All values Sender: All values Tags: All values Add filter

Resolve Summarize Notify ... 1 of 34 selected

| Subject | Tags | Sender |
|----------------------------------|------|-------------------------|
| Project Sync | ... | nestorwilke@contoso.com |
| Project Sync-202310... | ... | nestorwilke@contoso.com |
| I have tried to rectify this ... | ... | lwhite@contoso.com |
| Unauthorized disclosure | ... | uharris@contoso.com |
| Credit bureaus keep addin... | ... | adelevance@contoso.com |
| Money laundering | ... | nestorwilke@contoso.com |
| Gifts | ... | wsmith@contoso.com |
| Stock activity | ... | aadams@contoso.com |
| Stock action today | ... | kmartin@contoso.com |
| Customer complaints | ... | lhernandez@contoso.com |
| The merger is not yet fin... | ... | vadavis@outlook.com |
| I have disputed this acco... | ... | wgonzalez@gmail.com |
| RE: Stock action today | ... | kmartin@contoso.com |

Project Sync-20231016_163105-Meeting Recording

Summary User history

Conditions detected: Gifts & entertainment (provide our service at no View all)

Transcript

| | | |
|----|-----------------------|--|
| NW | Nestor Wilke 00:00:11 | I am doing it one minute. |
| GA | Grady Archie 00:00:45 | How about that Contoso stock price, right |
| NW | Nestor Wilke 00:00:47 | With this P.E. ratio, it's crazy |
| GA | Grady Archie 00:00:50 | And we know the forecast for next quarter so |
| NW | Nestor Wilke 00:00:54 | No more weak stocks Contoso to the moon |
| GA | Grady Archie 00:01:01 | I'm putting in a buy order right now |
| NW | Nestor Wilke 00:01:07 | Me too |
| GA | Grady Archie 00:01:01 | Early retirement here I come |
| GA | Grady Archie | See you on the beach |

Resolve Summarize Notify Tag as ...

Security Copilot

What content in the message was flagged as Gifts and Entertainment?

This Teams meeting transcript occurred between Nestor Wilke and Grady Archie with subject about T1. The Teams meeting was flagged by the Gifts & Entertainment and Stock Manipulation classifiers.

In the context of the Gifts & Entertainment classifier, a summary of this message is:

- Nestor offers Grady "free complimentary vacation on the company" which can constitute gifting in the workplace

In the context of the Stock Manipulation classifier, a summary of the message is:

- The phrase "weak stocks" refers to Contoso's stock and may suggest Microsoft stocks will increase in the near future
- Mentions of weak stocks can be tied to a corresponding action done by an individual in the meeting and possible stock manipulation

AI generated. Verify for accuracy.

What content in the message was flagged as Threat, Harassment, Regulatory Collusion categories detected?

Generate a simple summary

Ask a question about this message...

eDiscovery Natural Language to KQL



Screenshot of the Microsoft Purview eDiscovery interface showing the conversion of a natural language query into Keyword Query Language (KQL).

The interface includes a sidebar with navigation links: Home, eDiscovery (selected), Overview, Cases, Solutions, Data Lifecycle Management, and Data Map.

The main area shows a case titled "Contoso vs. Robinson" with a draft query named "Fabrikam production". The version is Draft 1 (Current) (Today, 3:14 PM).

The "Query" section displays a "Draft KQL with Security Copilot" preview. It shows a "Natural language prompt" and its corresponding "Keyword Query Language (KQL) response".

Natural language prompt:

1. Find all documents containing the work 'secret' or similar words like 'confidential', 'classified', 'restricted', 'sensitive', or 'privileged'.
2. The documents should be created in 2021.
3. The documents should be updated between 01-01-2023 and 30-06-2023.
4. The file size should be less than or equal to 1,000,000 bytes.
5. The document should be shared with Anne Keeting.

Keyword Query Language (KQL) response:

```
(“secret” OR “confidential” OR “classified” OR “restricted” OR “sensitive” OR “privileged”) AND (Created<=“2021-12-31”) AND (LastModifiedTime>=“2023-01-01” AND LastModifiedTime<=“2023-06-30”) AND (Size<=1000000) AND (SharedWithUsersOWSUSER:“Anne Keeting”)
```

Buttons include "Generate KQL", "Refine", "Suggested prompts", "Copy KQL", "Save as draft", and "Run query".

The bottom section shows "Data sources" and "Condition builder" tabs, with "Keyword Query Language (KQL)" selected. A note says "Start by adding data sources." with a "Add data sources" button. A "What's new" section on the right says "What're you looking for today?" and provides a search bar.

Intune Embedded Experience Capabilities

Learn more about a setting in Microsoft Intune portal

The screenshot shows the Microsoft Intune admin center interface. On the left, the navigation bar includes Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area shows the 'Windows 10/11 compliance policy' for Windows 10 and later. Under 'Compliance settings', several settings are listed with their status: BitLocker (Not configured), Secure Boot (Not configured), Code integrity (Not configured), Require a password to unlock mobile devices (Not configured), and Simple passwords (Not configured). A 'Copilot (preview)' window is open, providing AI-generated insights about the 'BitLocker' setting. The insights explain that the 'BitLocker' setting under the 'DeviceHealth' category in a Windows 10/11 compliance policy in Intune is used to require BitLocker Drive Encryption on Windows devices. It encrypts all data stored on the Windows operating system volume, uses the Trusted Platform Module (TPM) to help protect the Windows operating system and user data, and helps confirm that a computer isn't tampered with, even if it's left unattended, lost, or stolen. The Copilot also notes that the 'BitLocker' setting is part of the 'FileVault' category in the 'Endpoint protection' section.

Device Compliance Policy setting assistance

Device Configuration Policy setting assistance

Summarize a policy in Microsoft Intune portal

Microsoft Intune admin center

Home > Devices | Configuration >

Windows Autopatch - Data Collection

Device configuration profile

[Summarize with Copilot](#) [Delete](#)

Device and user check-in status

| Succeeded | Error | Conflict | Not applicable | In Progress |
|-----------|-------|----------|----------------|-------------|
| 0 | 0 | 0 | 0 | 0 |

[View report](#)

Device assignment status
This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state.

Per setting status
View the configuration status of each setting for this policy across all devices and users.

Properties

Basics [Edit](#)

Name: Windows Autopatch - Data Collection
Description: Allows diagnostic data from this device to be processed by Windows Autopatch. This policy is required by the Windows Autopatch service. Any changes you make to this policy will not be saved. Windows Autopatch will

Copilot (preview)
AI generated insights about policy

3/13/2024, 1:51:37 AM
Summarize this policy

3/13/2024, 1:52:03 AM
The policy you're asking about is named "Windows Autopatch - Data Collection". It has several settings configured:

- Allow Microsoft Managed Desktop Processing:** This setting is currently allowed. It permits diagnostic data from the device to be processed by Microsoft Managed Desktop. If this policy is disabled or not configured, diagnostic data from this device will not be processed by Microsoft Managed Desktop.
- Allow Telemetry:** This setting is currently set to "Full". It allows the device to send diagnostic and usage telemetry data. The most restricted value is 0.
- Limit Enhanced Diagnostic Data Windows Analytics:** This setting is currently enabled. It enables organizations to send Microsoft a specific set of diagnostic data for IT insights via Windows Analytics services.
- Limit Diagnostic Log Collection:** This setting is currently enabled. It specifies whether diagnostic log data can be collected when more information is needed to troubleshoot a problem.
- Limit Dump Collection:** This setting is currently enabled. It limits

Explore a device in Microsoft Intune portal

Microsoft Intune admin center

Home > Devices | Overview > Windows | Windows devices >

Analyst-AADJ-Wo

Search Explore with Copilot

Retire Wipe Delete Remote lock

Overview

Manage Properties

Monitor Hardware Discovered apps Device compliance Device configuration App configuration Local admin password Recovery keys User experience Device diagnostics Group membership Managed Apps Filter evaluation Enrollment Remediations (preview)

Essentials

| | |
|---------------------|--|
| Device name | : Analyst-AADJ-Wo |
| Management name | : Avery.Athawes_1237_Windows_12/5/2023_1:32 PM |
| Ownership | : Corporate |
| Serial number | : 0000-0010-0386-5753-2255-6863-82 |
| Phone number | : --- |
| Device manufacturer | : Microsoft Corporation |

Device actions status

| Action | Status | Date/Tim |
|---------|--------|----------|
| No data | | |

Copilot (preview)

AI generated insights about this device

3/13/2024, 1:59:19 AM

Hi Shobhit,

Ready to explore? Select one of the suggestions below to get started...

- Summarize this device
- Analyze an error code
- Compare this device with another device
- Show apps on this device
- Show policies assigned to this device
- Show group memberships
- Show the primary user of this device

Copilot can make mistakes so remember to verify the results. To help improve the experience, please share your feedback with us.

You can always use the prompt guide for suggestions by selecting this button

Compare two devices in Microsoft Intune portal

Microsoft Intune admin center

Home > Devices | Overview > Windows | Windows devices >

Analyst-AADJ-Wo

Search Explore with Copilot Retire Wipe Delete Remote lock

Overview

Essentials

Device name : Analyst-AADJ-Wo
Management name : Avery.Athawes_1237_Windows_12/5/2023_1:32 PM
Ownership : Corporate
Serial number : 0000-0010-0386-5753-2255-6863-82
Phone number : ---
Device manufacturer : Microsoft Corporation

Device actions status

| Action | Status | Date/Tin |
|---------|--------|----------|
| No data | | |

Copilot (preview)
AI generated insights about this device

Show apps on this device
Show policies assigned to this device
Show group memberships
Show the primary user of this device

Copilot can make mistakes so remember to verify the results. To help improve the experience, please share your feedback with us.
You can always use the prompt guide for suggestions by selecting this button ⓘ

3/13/2024, 2:02:08 AM
Compare this device with another device

Hardware
Configuration profiles
Compliance policy
App policies
Discovered apps
Managed apps

The screenshot shows the Microsoft Intune admin center interface. On the left, there's a navigation sidebar with various options like Home, Dashboard, All services (which is selected and highlighted with a red box), Devices (also highlighted with a red box), Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area shows a device named 'Analyst-AADJ-Wo' with its management name, ownership, serial number, phone number, and manufacturer details. Below this is a 'Device actions status' section with a table showing 'No data'. To the right, there's a 'Copilot (preview)' window with a heading 'AI generated insights about this device'. It has four buttons: 'Show apps on this device', 'Show policies assigned to this device', 'Show group memberships', and 'Show the primary user of this device'. A note below says 'Copilot can make mistakes so remember to verify the results. To help improve the experience, please share your feedback with us.' and 'You can always use the prompt guide for suggestions by selecting this button ⓘ'. At the bottom of the Copilot window, there's a timestamp '3/13/2024, 2:02:08 AM' and a button 'Compare this device with another device'. A red box highlights the 'Devices' option in the sidebar and the 'Explore with Copilot' button in the main area. Another red box highlights the 'Copilot (preview)' window.

Copilot (preview)
AI generated insights about this device

The comparison between the two devices managed by Intune, based on the available hardware data, is as follows:

| Property | Device 1 (13bddc15-4053-4b8d-a5f0-2a410917edc2) | Device 2 (CPC-User0-1ZWVS) |
|------------------|---|----------------------------|
| Manufacturer | Microsoft Corporation | Microsoft Corporation |
| Model | Virtual Machine | Cloud PC Enterprise |
| Operating System | Windows | Windows |
| OS Version | 10.0.22621.2715 | 10.0.22621.3155 |
| Management Agent | Mdm | Mdm |
| Device | Not specified | Not specified |

The similarities between the two devices include the manufacturer (Microsoft Corporation), the operating system (Windows), the management agent (Mdm), the encryption status (not encrypted), and the registration and enrollment method (WindowsAzureADJoin).

The differences between the two devices are in the model, OS version, physical memory, total storage space, free storage space, and compliance state. Specifically, Device 1 is a Virtual Machine with more physical memory and free storage space but is noncompliant. On the other hand, Device 2 is a Cloud PC Enterprise model with 2vCPU/8GB/128GB, has slightly more total storage space, and is compliant.

In terms of unique properties, Device 1 (13bddc15-4053-4b8d-a5f0-2a410917edc2) stands out for its noncompliance status and higher physical memory. Device 2 (CPC-User0-1ZWVS) is unique for its compliance status and slightly higher total storage space.

The screenshot shows the 'Copilot (preview)' feature comparing two devices. It lists the properties of both devices in a table. Below the table, it says 'The similarities between the two devices include the manufacturer (Microsoft Corporation), the operating system (Windows), the management agent (Mdm), the encryption status (not encrypted), and the registration and enrollment method (WindowsAzureADJoin).'. Then it lists 'The differences between the two devices are in the model, OS version, physical memory, total storage space, free storage space, and compliance state. Specifically, Device 1 is a Virtual Machine with more physical memory and free storage space but is noncompliant. On the other hand, Device 2 is a Cloud PC Enterprise model with 2vCPU/8GB/128GB, has slightly more total storage space, and is compliant.'. At the bottom, it says 'In terms of unique properties, Device 1 (13bddc15-4053-4b8d-a5f0-2a410917edc2) stands out for its noncompliance status and higher physical memory. Device 2 (CPC-User0-1ZWVS) is unique for its compliance status and slightly higher total storage space.' A red box highlights the 'Property' column in the table.

Analyze an error code in Microsoft Intune portal

Microsoft Intune admin center

Home > Devices | Overview > Windows | Windows devices >

Analyst-AADJ-Wo

Explore with Copilot

Overview

Manage

- Properties
- Monitor
- Hardware
- Discovered apps
- Device compliance
- Device configuration
- App configuration
- Local admin password
- Recovery keys
- User experience
- Device diagnostics
- Group membership
- Managed Apps
- Filter evaluation
- Enrollment
- Remediations (preview)

Essentials

| | | |
|---------------------|---|--|
| Device name | : | Analyst-AADJ-Wo |
| Management name | : | Avery.Athawes_1237_Windows_12/5/2023_1:32 PM |
| Ownership | : | Corporate |
| Serial number | : | 0000-0010-0386-5753-2255-6863-82 |
| Phone number | : | --- |
| Device manufacturer | : | Microsoft Corporation |

Device actions status

| Action | Status | Date/Tin |
|---------|--------|----------|
| No data | | |

Copilot (preview)

AI generated insights about this device

3/13/2024, 2:09:24 AM

Analyze an error code

3/13/2024, 2:09:24 AM

Enter an error code to analyze.

Error code * ⓘ

0x801c0003

Submit

3/13/2024, 2:10:06 AM

The error code 0x801c0003 is associated with the enrollment of Windows devices in Microsoft Intune. This error can occur under several scenarios:

1. The user has more devices enrolled than the device limit. In this case, you can review documents to remove a device or change the device limit.
2. The setting "Users may join devices to Microsoft Entra ID" is set to "none." It should be set to all or select users.
3. The device is already enrolled by another user. If that's the case, you should remove the device from the Azure Intune console or manually unenroll the device before trying again.

Copilot for Security Standalone Experience Capabilities

Featured Prompts and Prompt Suggestions



PROMPT SUGGESTIONS

Analyze a file
Get detailed file information, including heade...

Analyze a script or command
Analyzes and interprets a command or script ...

Analyze ServiceNow Incidents
Analyze or summarize one or many ServiceN...

Append Comment To ServiceNow Incident
Appends / adds comment to a specific Servic...

Defang URLs
Defangs URLs in the given text

See all system capabilities

/

Type / in a prompt bar to see all Prompt Suggestions

Explore with Copilot

Featured Prompts | Promptbooks

Suspicious script analysis v3 (Copy)
Get a report analyzing the intent, intelligence, threat actors, and impacts of a suspicious script.

Microsoft Security - 7 prompts ▶

Vulnerability impact assessment
Get a report summarizing the intelligence for a known vulnerability and how to address it.

Microsoft Security - 6 prompts ▶

High to medium severity incidents to prio...
Asks for the top 5 high to medium severity incidents, details, and recommendations.

Microsoft Security - 5 prompts ▶

Select Featured Prompts on a homepage of Standalone experience

Promptbooks and Promptbooks Library

Microsoft Copilot for Security Preview / Promptbook library

Promptbook library

All My promptbooks Woodgrove Microsoft

| Name | Inputs | Plugins | Tags | Prompts | Owner |
|---|----------------------|---------|------|---------|-----------|
| Vulnerability impact assessment | CVEID | | | 6 | Microsoft |
| Get a report summarizing the intelligence for a known vulnerability and how to address it. | | | | | |
| Microsoft Sentinel incident investigation | SENTINEL INCIDENT ID | | | 7 | Microsoft |
| Get a report about a specific incident, along with related alerts, reputation scores, users, and devices. | | | | | |
| Microsoft 365 Defender incident investigation | DEFENDER INCIDENT ID | | | 7 | Microsoft |
| Get a report about a specific incident, with related alerts, reputation scores, users, and devices. | | | | | |
| Suspicious script analysis | SNIPPET | | | 7 | Microsoft |
| Get a report analyzing the intent, intelligence, threat actors, and impacts of a suspicious script. | | | | | |
| Threat actor profile | THREATACTORNAME | | | 5 | Microsoft |
| Get a report profiling a known actor with suggestions for protecting against common tools and tactics. | | | | | |

PROMPTBOOKS

Vulnerability impact assessment

Get a report summarizing the intelligence for a known vulnerability and how to address it.

Microsoft Sentinel incident investigation

Get a report about a specific incident, along with related alerts, reputation scores, users, and devices.

Microsoft 365 Defender incident investigation

Get a report about a specific incident, with related alerts, reputation scores, users, and devices.

View Prompt Books from Promptbook Library

Type * in prompt bar to display Promptbooks



Create Custom Promptbook

Create a promptbook

Name *

Tags

Description

Prompts

Add any inputs needed to each prompt. For example, if a prompt includes an incident ID, it should be entered in the prompt as <IncidentID>. Use angle brackets with no spaces.

whoami

Add prompt text

+ ↗ ✎

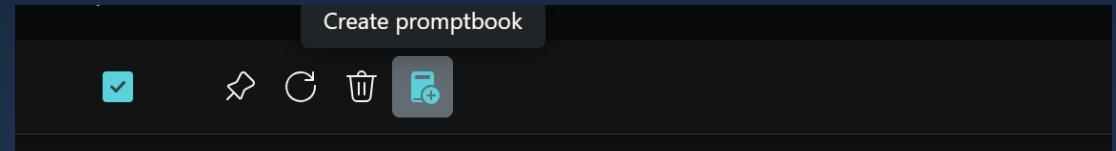
Inputs you'll need

Inputs added to the prompts will be automatically displayed here. If you don't see the inputs, make sure the format is correct.

Who can use this promptbook?

Just me

Create **Cancel**





Custom Plugins

Add a plugin X

Complete the info to add a new plugin. [Learn more](#)

Who can use this plugin? *

Just me ▼

Select an upload format *

Security Copilot plugin
Custom .yaml or .json

OpenAI plugin
manifest.json

[Plugins overview Microsoft Security Copilot \(Preview\) | Microsoft Learn](#)

Custom ⓘ

| |
|--|
| Alien Vault TI Reports Skills for looking up reports using the Alien Vault Threat Intelligence API |
| Check IP against Alienvault TI Private Skills that look up IP against my Alienvault TI that store in Sentinel |
| DefangUrls Private Skills for Defanging URLs in the given text |
| Defender Daily Operations Private XDR Scenarios we use repeatedly for our daily operations. |
| Defender KQL: Who Click on an Url Private Skills that look up URL click logs in Defender Advanced Hunting |
| EVIL PLUGIN BETA Stealing a victim's chat history 2 |

A large, abstract graphic element on the right side of the slide. It consists of several overlapping, rounded, blue shapes in varying shades of blue. The shapes are organic in form, suggesting a hand or a cluster of interconnected elements, and they overlap each other to create depth and texture.

Entra
Embedded Experience

Microsoft Copilot for Security Partners and plugins



Managed Security Service Providers



Independent Software Vendors



*With existing plugins for Splunk and ServiceNow already available in early access.