Disrupting active exploitation of on-premises SharePoint vulnerabilities

microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

By Microsoft Threat Intelligence July 22, 2025

July 23, 2025 update – Expanded analysis and threat intelligence from our continued monitoring of exploitation activity by Storm-2603 leading to the deployment of Warlock ransomware. Based on new information, we have updated the Attribution, Indicators of compromise, extended and clarified Mitigation and protection guidance (including raising *Step 6: Restart IIS* for emphasis), Detections, and Hunting sections.

On July 19, 2025, Microsoft Security Response Center (MSRC) published a blog addressing active attacks against on-premises SharePoint servers that exploit CVE-2025-49706, a spoofing vulnerability, and CVE-2025-49704, a remote code execution vulnerability. These vulnerabilities affect on-premises SharePoint servers only and do not affect SharePoint Online in Microsoft 365. Microsoft has released new comprehensive security updates for all supported versions of SharePoint Server (Subscription Edition, 2019, and 2016) that protect customers against these new vulnerabilities. Customers should apply these updates immediately to ensure they are protected.

These comprehensive security updates address newly disclosed security vulnerabilities in CVE-2025-53770 that are related to the previously disclosed vulnerability CVE-2025-49704. The updates also address the security bypass vulnerability CVE-2025-53771 for the previously disclosed CVE-2025-49706.

As of this writing, Microsoft has observed two named Chinese nation-state actors, Linen Typhoon and Violet Typhoon exploiting these vulnerabilities targeting internet-facing SharePoint servers. In addition, we have observed another China-based threat actor, tracked as Storm-2603, exploiting these vulnerabilities to deploy ransomware. Investigations into other actors also using these exploits are still ongoing. With the rapid adoption of these exploits, Microsoft assesses with high confidence that threat actors will continue to integrate them into their attacks against unpatched on-premises SharePoint systems. This blog shares details of observed exploitation of CVE-2025-49706 and CVE-2025-49704 and the follow-on tactics, techniques, and procedures (TTPs) by threat actors. We will update this blog with more information as our investigation continues.

Microsoft recommends customers to use supported versions of on-premises SharePoint servers with the latest security updates. To stop unauthenticated attacks from exploiting this vulnerability, customers should also integrate and enable Antimalware Scan Interface (AMSI) and Microsoft Defender Antivirus (or equivalent solutions) for all on-premises SharePoint deployments and configure AMSI to enable Full Mode as detailed in Mitigations section below. Customers should also rotate SharePoint server ASP.NET machine keys, restart Internet Information Services (IIS), and deploy Microsoft Defender for Endpoint or equivalent solutions.

Product	Security update link
Microsoft SharePoint Server Subscription Edition	Security Update for Microsoft SharePoint Server Subscription Edition (KB5002768)
Microsoft SharePoint Server 2019 *(both updates should be installed)*	Security Update for Microsoft SharePoint 2019 (KB5002754) Security Update for Microsoft SharePoint Server 2019 Language Pack (KB5002753)
Microsoft SharePoint Server 2016 *(both updates should be installed)*	Security Update for Microsoft SharePoint Enterprise Server 2016 (KB5002760) Security Update for Microsoft SharePoint Enterprise Server 2016 Language Pack (KB5002759)

Observed tactics and techniques

Microsoft observed multiple threat actors conducting reconnaissance and attempting exploitation of on-premises SharePoint servers through a POST request to the ToolPane endpoint.

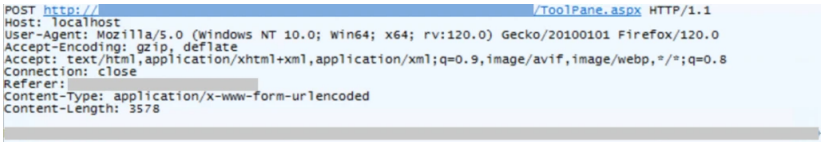

Figure 1. POST request to ToolPane endpoint

Post-exploitation activities

Threat actors who successfully executed the authentication bypass and remote code execution exploits against vulnerable on-premises SharePoint servers have been observed using a web shell in their post-exploitation payload.

Web shell deployment

In observed attacks, threat actors send a crafted POST request to the SharePoint server, uploading a malicious script named *spinstall0.aspx.* Actors have also modified the file name in a variety of ways, such as *spinstall.aspx*, *spinstall1.aspx*, *spinstall2.aspx,* etc. The *spinstall0.aspx* script contains commands to retrieve MachineKey data and return the results to the user through a GET request, enabling the theft of the key material by threat actors.

Related IOCs and hunting queries

Microsoft provides indicators of compromise (IOCs) to identify and hunt for this web shell in the Indicators of compromise section of this blog. Microsoft provides related hunting queries to find this dropped file in the Hunting queries section of this blog.

Attribution

As early as July 7, 2025, Microsoft analysis suggests threat actors were attempting to exploit CVE-2025-49706 and CVE-2025-49704 to gain initial access to target organizations. These actors include Chinese state actors Linen Typhoon and Violet Typhoon and another China-based actor Storm-2603. The TTPs employed in these exploit attacks align with previously observed activities of these threat actors.

Linen Typhoon

Since 2012, Linen Typhoon has focused on stealing intellectual property, primarily targeting organizations related to government, defense, strategic planning, and human rights. This threat actor is known for using drive-by compromises and historically has relied on existing exploits to compromise organizations.

Violet Typhoon

Since 2015, the Violet Typhoon activity group has been dedicated to espionage, primarily targeting former government and military personnel, non-governmental organizations (NGOs), think tanks, higher education, digital and print media, financial and health related sectors in the United States, Europe, and East Asia. This group persistently scans for vulnerabilities in the exposed web infrastructure of target organizations, exploiting discovered weaknesses to install web shells.

Storm-2603

The group that Microsoft tracks as Storm-2603 is assessed with moderate confidence to be a China-based threat actor. Microsoft has not identified links between Storm-2603 and other known Chinese threat actors. Microsoft tracks this threat actor in association with attempts to steal MachineKeys using the on-premises SharePoint vulnerabilities. Although Microsoft has observed this threat actor deploying Warlock and Lockbit ransomware in the past, Microsoft is currently unable to confidently assess the threat actor's objectives. Starting on July 18, 2025, Microsoft has observed Storm-2603 deploying ransomware using these vulnerabilities.

Initial access and delivery

The observed attack begins with the exploitation of an internet-facing on-premises SharePoint server, granting Storm-2603 initial access to the environment using the *spinstall0.aspx* payload described earlier in this blog. This initial access is used to conduct command execution using the w3wp.exe process that supports SharePoint. Storm-2603 then initiates a series of discovery commands, including *whoami*, to enumerate user context and validate privilege levels. The use of *cmd.exe* and batch scripts is also observed as the actor transitions into broader execution phases. Notably, *services.exe* is abused to disable Microsoft Defender protections through direct registry modifications.

Persistence

Storm-2603 established persistence through multiple mechanisms. In addition to the *spinstall0.aspx* web shell, the threat actor also creates scheduled tasks and manipulates Internet Information Services (IIS) components to load suspicious .NET assemblies. These actions ensure continued access even if initial vectors are remediated.

Action on objectives

The threat actor performs credential access using Mimikatz, specifically targeting the Local Security Authority Subsystem Service (LSASS) memory to extract plaintext credentials. The actor moves laterally using PsExec and the Impacket toolkit, executing commands using Windows Management Instrumentation (WMI).

Storm-2603 is then observed modifying Group Policy Objects (GPO) to distribute Warlock ransomware in compromised environments.

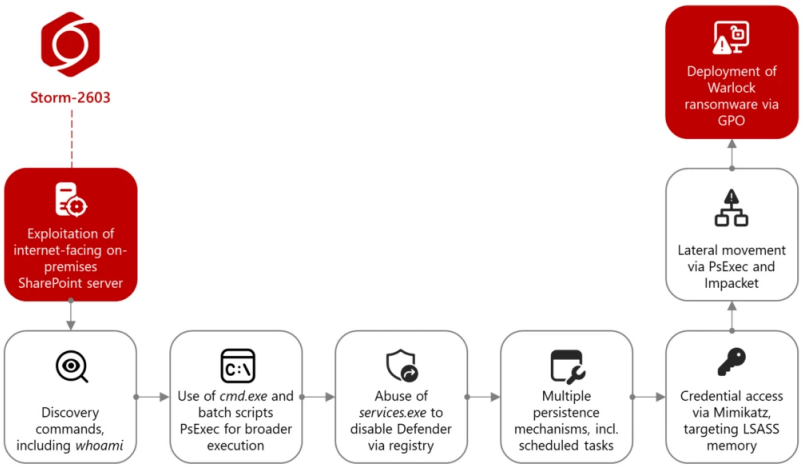

Figure 2. Storm-2603 attack chain exploiting SharePoint vulnerabilities and leading to ransomware

Additional actors will continue to use these exploits to target unpatched on-premises SharePoint systems, further emphasizing the need for organizations to implement mitigations and security updates immediately.

Mitigation and protection guidance

Microsoft has released security updates that fully protect customers using all supported versions of SharePoint affected by CVE-2025-53770 and CVE-2025-53771. Customers should apply these updates immediately.

Customers using SharePoint Server should follow the guidance below.

1. **Use or upgrade to supported versions of on-premises Microsoft SharePoint Server.**
   Supported versions: SharePoint Server 2016, 2019, and SharePoint Subscription Edition
2. **Apply the latest security updates.**
3. **Ensure the Antimalware Scan Interface is turned on and configured correctly and deploy Defender Antivirus on all SharePoint servers**
   - Configure Antimalware Scan Interface (AMSI) integration in SharePoint, enable Full Mode for optimal protection, and deploy Defender Antivirus on all SharePoint servers which will stop unauthenticated attackers from exploiting this vulnerability.
   - Note: AMSI integration was enabled by default in the September 2023 security update for SharePoint Server 2016/2019 and the Version 23H2 feature update for SharePoint Server Subscription Edition.
   - If you cannot enable AMSI, we recommend you consider disconnecting your server from the internet until you have applied the most current security update linked above. If the server cannot be disconnected from the internet, consider using a VPN or proxy requiring authentication or an authentication gateway to limit unauthenticated traffic.
4. **Deploy Microsoft Defender for Endpoint, or equivalent solutions**
   We recommend organizations to deploy Defender for Endpoint to detect and block post-exploit activity.
5. **Rotate SharePoint Server ASP.NET machine keys**
   After applying the latest security updates above or enabling AMSI, it is critical that customers rotate SharePoint server ASP.NET machine keys and restart Internet Information Services (IIS) on all SharePoint servers.
   1. Manually using PowerShell
      To update the machine keys using PowerShell, use the Set-SPMachineKey cmdlet.
   2. Manually using Central Admin: Trigger the Machine Key Rotation timer job by performing the following steps:
      - Navigate to the **Central Administration** site.
      - Go to **Monitoring** -> **Review job definition**.
      - Search for **Machine Key Rotation Job** and select **Run Now**.
6. **Restart IIS on all SharePoint servers using *iisreset.exe*.** NOTE: If you cannot enable AMSI, you will need to rotate your keys and restart IIS after you install the new security update.
7. **Implement your incident response plan.**

To protect against post-exploitation activity, including ransomware deployment, Microsoft recommends the following mitigations:

- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.
- Read our human-operated ransomware blog for advice on developing a holistic security posture to prevent ransomware, including credential hygiene and hardening recommendations.
- Run endpoint detection and response (EDR) in block mode so that Microsoft Defender for Endpoint – or equivalent EDR solution – can block malicious artifacts, even when your non-Microsoft antivirus does not detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.
- Configure automatic attack disruption in Microsoft Defender XDR. Automatic attack disruption is designed to contain attacks in progress, limit the impact on an organization's assets, and provide more time for security teams to remediate the attack fully.

- Enable LSA protection.
- Enable and configure Credential Guard.
- Ensure that tamper protection is enabled in Microsoft Defender for Endpoint.
- Enable controlled folder access.
- Microsoft Defender customers can turn on attack surface reduction rules to prevent common attack techniques. Attack surface reduction rules are sweeping settings that stop entire classes of threats. The following bullet points offer more guidance on specific mitigation advice:
    - Use advanced protection against ransomware.
    - Block credential stealing from the Windows local security authority subsystem.
    - Block process creations originating from PSExec and WMI commands.

Indicators of compromise

Indicator	Type	Description
Spinstall0.aspx	File name	Web shell used by threat actors Actors have also modified the file name in a variety of ways – such as *spinstall.aspx*, *spinstall1.aspx*, *spinstall2.aspx*
IIS_Server_dll.dll	File name	Storm-2603 IIS Backdoor
SharpHostInfo.x64.exe	File Name	Pentest tool observed during attack that is used to collect host information using NetBIOS, SMB, and WMI
xd.exe	File Name	Fast reverse proxy tool used to connect to C2 IP 65.38.121[.]198
debug_dev.js	File name	File containing web config data, including MachineKey data
\1[5-6]\TEMPLATE\LAYOUTS\debug_dev.js	File path	File path for stolen web configs
92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514	SHA-256	Hash of *spinstall0.aspx*
24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf	SHA-256	Web shell that leverages http & curl to receive and execute commands from Storm-2603 C2 "*update[.]updatemicfosoft[.]com"*
b5a78616f709859a0d9f830d28ff2f9dbbb2387df1753739407917e96dadf6b0	SHA-256	Web shell that leverages sockets & DNS to receive and execute commands from Storm-2603 C2 *"update[.]updatemicfosoft[.]com"*
c27b725ff66fdfb11dd6487a3815d1d1eba89d61b0e919e4d06ed3ac6a74fe94	SHA-256	Web shell that leverages sockets & DNS to receive and execute commands from Storm-2603 C2 *"update[.]updatemicfosoft[.]com"*
1eb914c09c873f0a7bcf81475ab0f6bdfaccc6b63bf7e5f2dbf19295106af192	SHA-256	Web shell that leverages sockets & DNS to receive and execute commands from Storm-2603 C2 *"update[.]updatemicfosoft[.]com"*
4c1750a14915bf2c0b093c2cb59063912dfa039a2adfe6d26d6914804e2ae928	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
83705c75731e1d590b08f9357bc3b0f04741e92a033618736387512b40dab060	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
f54ae00a9bae73da001c4d3d690d26ddf5e8e006b5562f936df472ec5e299441	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
b180ab0a5845ed619939154f67526d2b04d28713fcc1904fbd666275538f431d	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)

6753b840cec65dfba0d7d326ec768bff2495784c60db6a139f51c5e83349ac4d	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
7ae971e40528d364fa52f3bb5e0660ac25ef63e082e3bbd54f153e27b31eae68	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
567cb8e8c8bd0d909870c656b292b57bcb24eb55a8582b884e0a228e298e7443	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
445a37279d3a229ed18513e85f0c8d861c6f560e0f914a5869df14a74b679b86	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
ffbc9dfc284b147e07a430fe9471e66c716a84a1f18976474a54bee82605fa9a	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
6b273c2179518dacb1218201fd37ee2492a5e1713be907e69bf7ea56ceca53a5	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
c2c1fec7856e8d49f5d49267e69993837575dbbec99cd702c5be134a85b2c139	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
6f6db63ece791c6dc1054f1e1231b5bbcf6c051a49bad0784569271753e24619	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
d6da885c90a5d1fb88d0a3f0b5d9817a82d5772d5510a0773c80ca581ce2486d	SHA-256	Hash for *SharpHostInfo.x64.exe*
62881359e75c9e8899c4bc9f452ef9743e68ce467f8b3e4398bebacde9550dea	SHA-256	Hash for *xd.exe*
c34718cbb4c6.ngrok-free[.]app/file.ps1	URL	Ngrok tunnel delivering PowerShell to C2
msupdate[.]updatemicfosoft[.]com	URL	C2 domain for Storm-2603
131.226.2[.]6	IP	Post exploitation C2
134.199.202[.]205	IP	IP address exploiting SharePoint vulnerabilities
104.238.159[.]149	IP	IP address exploiting SharePoint vulnerabilities
188.130.206[.]168	IP	IP address exploiting SharePoint vulnerabilities
65.38.121[.]198	IP	Post-exploitation C2 for Storm-2603

Microsoft Defender XDR coverage

Microsoft Defender XDR customers get coordinated protection across endpoints, identities, email, and cloud apps to detect, prevent, investigate, and respond to threats like the SharePoint exploitation activity described in this blog.

Customers with provisioned access can also use Microsoft Security Copilot in Microsoft Defender to investigate and respond to incidents, hunt for threats, and protect their organization with relevant threat intelligence.

The following table outlines the tactics observed in the exploitation attacks discussed in this blog, along with Microsoft Defender protection coverage at each stage of the attack chain:

Tactic	Observed activity	Microsoft Defender coverage
Initial Access	Use of known vulnerabilities to exploit internet-facing SharePoint servers	**Microsoft Defender Antivirus** -Exploit:Script/SuspSignoutReq.A – Exploit:Script/SuspSignoutReqBody.A **Microsoft Defender for Endpoint** – 'SuspSignoutReq' malware was blocked on a SharePoint server – Possible exploitation of SharePoint server vulnerabilities
Execution	Use of a web shell to run PowerShell and exfiltrate sensitive data (e.g., MachineKey); Batch scripts and *cmd.exe* to launch PsExec for remote execution; Attempts to disable Microsoft Defender protections through registry edits using the service control manager; Escalation of privileges to SYSTEM using PsExec with the *-s* flag; Use of Impacket to execute commands remotely over WMI without writing files to disk	**Microsoft Defender Antivirus** – Trojan:Win32/HijackSharePointServer.A **Microsoft Defender for Endpoint** – Suspicious IIS worker process behavior – Suspicious scheduled task – Impacket toolkit
Persistence	Installation of web shell after exploiting SharePoint vulnerability; IIS worker process loaded suspicious .NET assembly; Scheduled task for persistence following initial access	**Microsoft Defender Antivirus** – Trojan:PowerShell/MachineKeyFinder.DA!amsi **Microsoft Defender for Endpoint** – Possible web shell installation – IIS worker process loaded suspicious .NET assembly
Credential Access	Mimikatz used to run module "sekurlsa::logonpasswords", which lists all available credentials	**Microsoft Defender for Endpoint** – Mimikatz credential theft tool
Lateral Movement	Impacket is observed leveraging Windows Management Instrumentation to remotely stage and execute payloads	**Microsoft Defender for Endpoint** – A remote resource was accessed suspiciously – Compromised account conducting hands-on-keyboard attack – Ongoing hands-on-keyboard attack via Impacket toolkit
Collection	Web shell used to extract MachineKey data	**Microsoft Defender Antivirus** – Trojan:PowerShell/MachineKeyFinder.DA!amsi **Microsoft Defender for Endpoint** – Possible web shell installation
Impact	Files encrypted in compromised environments as part of ransomware attack	**Microsoft Defender for Endpoint** – Ransomware-linked threat actor detected – Potentially compromised assets exhibiting ransomware-like behavior – Ransomware behavior detected in the file system – Possible compromised user account delivering ransomware-related file – Potential human-operated malicious activity

Note: These alerts can also be triggered by unrelated threat activity

Vulnerability management

Customers using Microsoft Defender Vulnerability Management can identify exposed devices and track remediation efforts based on the following CVEs:

- CVE-2025-53770 – SharePoint ToolShell Auth Bypass and RCE
- CVE-2025-53771 – SharePoint ToolShell Path Traversal
- CVE-2025-49704 – SharePoint RCE
- CVE-2025-49706 – SharePoint Post-auth RCE

Navigate to **Vulnerability management** > **Weaknesses** and filter by these CVE IDs to view exposed devices, remediation status, and *Evidence of Exploitation* tags.

You can also use this unified advanced hunting query:

```
DeviceTvmSoftwareVulnerabilities
| where CveId in (
  "CVE-2025-49704",
  "CVE-2025-49706",
  "CVE-2025-53770",
  "CVE-2025-53771")
```

External Attack Surface Management (Defender EASM)

Microsoft Defender External Attack Surface Management (Defender EASM) provides visibility into exposed internet-facing SharePoint instances. The following Attack Surface Insights may indicate vulnerable but not necessarily exploited services:

- CVE-2025-49704 – SharePoint RCE
- CVE-2025-53770 – SharePoint ToolShell Auth Bypass and RCE
- CVE-2025-53771 – SharePoint ToolShell Path Traversal

Note: A “Potential” insight signals that a service is detected but version validation is not possible. Customers should manually verify patching status.

Hunting queries

Microsoft Defender XDR

To locate possible exploitation activity, run the following queries in Microsoft Defender XDR security center.

Successful exploitation using file creation

Look for the creation of *spinstall0.aspx*, which indicates successful post-exploitation of CVE-2025-53770.

```
DeviceFileEvents
| where FolderPath has_any ("microsoft shared\\Web Server Extensions\\15\\TEMPLATE\\LAYOUTS", "microsoft
shared\\Web Server Extensions\\16\\TEMPLATE\\LAYOUTS")
| where FileName contains "spinstall"
| project Timestamp, DeviceName, InitiatingProcessFileName, InitiatingProcessCommandLine, FileName, FolderPath,
ReportId, ActionType, SHA256
| order by Timestamp desc
```

Post-exploitation PowerShell dropping web shell

Look for process creation where *w3wp.exe* is spawning encoded PowerShell involving the *spinstall0.aspx* file or the file paths it’s been known to be written to.

```
DeviceProcessEvents
| where InitiatingProcessFileName has "w3wp.exe"
    and InitiatingProcessCommandLine !has "DefaultAppPool"
    and FileName =~ "cmd.exe"
    and ProcessCommandLine has_all ("cmd.exe", "powershell")
    and ProcessCommandLine has_any ("EncodedCommand", "-ec")
| extend CommandArguments = split(ProcessCommandLine, " ")
| mv-expand CommandArguments to typeof(string)
| where CommandArguments matches regex "^[A-Za-z0-9+/=]{15,}$"
| extend B64Decode = replace("\\x00", "", base64_decodestring(tostring(CommandArguments)))
| where B64Decode contains "spinstall", @'C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\15\TEMPLATE\LAYOUTS',
@'C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS')
```

Post-exploitation web shell dropped

Look for the web shell dropped using the PowerShell command.

```
DeviceFileEvents
| where Timestamp >ago(7d)
| where InitiatingProcessFileName=~"powershell.exe"
| where FileName contains "spinstall"
```

Exploitation detected by Defender

Look at Microsoft Defender for Endpoint telemetry to determine if specific alerts fired in your environment.

```
AlertEvidence
| where Timestamp > ago(7d)
| where Title has "SuspSignoutReq"
| extend _DeviceKey = iff(isnotempty(DeviceId), bag_pack_columns(DeviceId, DeviceName),"")
| summarize min(Timestamp), max(Timestamp), count_distinctif(DeviceId,isnotempty(DeviceId)), make_set(Title),
make_set_if(_DeviceKey, isnotempty(_DeviceKey) )
```

Unified advanced hunting queries

Find exposed devices

Look for devices vulnerable to the CVEs listed in blog.

```
DeviceTvmSoftwareVulnerabilities
| where CveId in ("CVE-2025-49704","CVE-2025-49706","CVE-2025-53770","CVE-2025-53771")
```

Web shell C2 communication

Find devices that may have communicated with Storm-2603 web shell C2, that may indicate a compromised device beaconing to Storm-2603 controlled infrastructure.

```
let domainList = "update.updatemicfosoft.com";
union
(
    DnsEvents
    | where QueryType has_any(domainList) or Name has_any(domainList) or QueryType matches regex
@"^.*\.devtunnels\.ms$" or Name matches regex @"^.*\.devtunnels\.ms$"
    | project TimeGenerated, Domain = QueryType, SourceTable = "DnsEvents"
),
(
    IdentityQueryEvents
    | where QueryTarget has_any(domainList) or QueryType matches regex @"^.*\.devtunnels\.ms$"
    | project Timestamp, Domain = QueryTarget, SourceTable = "IdentityQueryEvents"
),
(
    DeviceNetworkEvents
    | where RemoteUrl has_any(domainList) or RemoteUrl matches regex @"^.*\.devtunnels\.ms$"
    | project Timestamp, Domain = RemoteUrl, SourceTable = "DeviceNetworkEvents"
),
(
    DeviceNetworkInfo
    | extend DnsAddresses = parse_json(DnsAddresses), ConnectedNetworks = parse_json(ConnectedNetworks)
    | mv-expand DnsAddresses, ConnectedNetworks
    | where DnsAddresses has_any(domainList) or ConnectedNetworks.Name has_any(domainList) or DnsAddresses
matches regex @"^.*\.devtunnels\.ms$" or ConnectedNetworks .Name matches regex @"^.*\.devtunnels\.ms$"
    | project Timestamp, Domain = coalesce(DnsAddresses, ConnectedNetworks.Name), SourceTable =
"DeviceNetworkInfo"
),
(
    VMConnection
    | extend RemoteDnsQuestions = parse_json(RemoteDnsQuestions), RemoteDnsCanonicalNames =
parse_json(RemoteDnsCanonicalNames)
    | mv-expand RemoteDnsQuestions, RemoteDnsCanonicalNames
    | where RemoteDnsQuestions has_any(domainList) or RemoteDnsCanonicalNames has_any(domainList) or
RemoteDnsQuestions matches regex @"^.*\.devtunnels\.ms$" or RemoteDnsCanonicalNames matches regex
@"^.*\.devtunnels\.ms$"
    | project TimeGenerated, Domain = coalesce(RemoteDnsQuestions, RemoteDnsCanonicalNames), SourceTable =
"VMConnection"
),
(
    W3CIISLog
    | where csHost has_any(domainList) or csReferer has_any(domainList) or csHost matches regex
@"^.*\.devtunnels\.ms$" or csReferer matches regex @"^.*\.devtunnels\.ms$"
    | project TimeGenerated, Domain = coalesce(csHost, csReferer), SourceTable = "W3CIISLog"
),
(
    EmailUrlInfo
    | where UrlDomain has_any(domainList) or UrlDomain matches regex @"^.*\.devtunnels\.ms$"
    | project Timestamp, Domain = UrlDomain, SourceTable = "EmailUrlInfo"
),
(
    UrlClickEvents
    | where Url has_any(domainList) or Url matches regex @"^.*\.devtunnels\.ms$"
    | project Timestamp, Domain = Url, SourceTable = "UrlClickEvents"
)
| order by TimeGenerated desc
```

Microsoft Sentinel

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

Our post on web shell threat hunting with Microsoft Sentinel also provides guidance on looking for web shells in general. Several hunting queries are also available below:

- Web shell detection
- Possible Webshell drop
- Malicious web application requests linked with Microsoft Defender for Endpoint alerts
- Web shell activity

Below are the queries using Sentinel Advanced Security Information Model (ASIM) functions to hunt threats across both Microsoft first-party and third-party data sources. ASIM also supports deploying parsers to specific workspaces from GitHub, using an ARM template or manually.

Detect network indicators of compromise and file hashes using ASIM

```
//IP list and domain list- _Im_NetworkSession
let lookback = 30d;
let ioc_ip_addr = dynamic(["131.226.2.6", "134.199.202.205", "104.238.159.149", "188.130.206.168"]);
let ioc_domains = dynamic(["c34718cbb4c6.ngrok-free.app"]);
_Im_NetworkSession(starttime=todatetime(ago(lookback)), endtime=now())
| where DstIpAddr in (ioc_ip_addr) or DstDomain has_any (ioc_domains)
| summarize imNWS_mintime=min(TimeGenerated), imNWS_maxtime=max(TimeGenerated),
  EventCount=count() by SrcIpAddr, DstIpAddr, DstDomain, Dvc, EventProduct, EventVendor

//IP list - _Im_WebSession
let lookback = 30d;
let ioc_ip_addr = dynamic(["131.226.2.6", "134.199.202.205", "104.238.159.149", "188.130.206.168"]);
let ioc_sha_hashes =dynamic(["92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514"]);
_Im_WebSession(starttime=todatetime(ago(lookback)), endtime=now())
| where DstIpAddr in (ioc_ip_addr) or FileSHA256 in (ioc_sha_hashes)
| summarize imWS_mintime=min(TimeGenerated), imWS_maxtime=max(TimeGenerated),
  EventCount=count() by SrcIpAddr, DstIpAddr, Url, Dvc, EventProduct, EventVendor

// file hash list - imFileEvent
let ioc_sha_hashes = dynamic(["92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514"]);
imFileEvent
| where SrcFileSHA256 in (ioc_sha_hashes) or TargetFileSHA256 in (ioc_sha_hashes)
| extend AccountName = tostring(split(User, @'')[1]),
  AccountNTDomain = tostring(split(User, @'')[0])
| extend AlgorithmType = "SHA256"
```

Post exploitation C2 or file hashes

Find devices that may have communicated with Storm-2603 post exploitation C2 or contain known Storm-2603 file hashes.

```
//IP list - _Im_WebSession
let lookback = 30d;
let ioc_ip_addr = dynamic(["65.38.121.198"]);
let ioc_sha_hashes =dynamic(["92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514",
"24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf",
"b5a78616f709859a0d9f830d28ff2f9dbbb2387df1753739407917e96dadf6b0",
"c27b725ff66fdfb11dd6487a3815d1d1eba89d61b0e919e4d06ed3ac6a74fe94",
"1eb914c09c873f0a7bcf81475ab0f6bdfaccc6b63bf7e5f2dbf19295106af192",
"4c1750a14915bf2c0b093c2cb59063912dfa039a2adfe6d26d6914804e2ae928",
"83705c75731e1d590b08f9357bc3b0f04741e92a033618736387512b40dab060",
"f54ae00a9bae73da001c4d3d690d26ddf5e8e006b5562f936df472ec5e299441",
"b180ab0a5845ed619939154f67526d2b04d28713fcc1904fbd666275538f431d",
"6753b840cec65dfba0d7d326ec768bff2495784c60db6a139f51c5e83349ac4d",
"7ae971e40528d364fa52f3bb5e0660ac25ef63e082e3bbd54f153e27b31eae68",
"567cb8e8c8bd0d909870c656b292b57bcb24eb55a8582b884e0a228e298e7443",
"445a37279d3a229ed18513e85f0c8d861c6f560e0f914a5869df14a74b679b86",
"ffbc9dfc284b147e07a430fe9471e66c716a84a1f18976474a54bee82605fa9a",
"6b273c2179518dacb1218201fd37ee2492a5e1713be907e69bf7ea56ceca53a5",
"c2c1fec7856e8d49f5d49267e69993837575dbbec99cd702c5be134a85b2c139"]);
_Im_WebSession(starttime=todatetime(ago(lookback)), endtime=now())
| where DstIpAddr in (ioc_ip_addr) or FileSHA256 in (ioc_sha_hashes)
| summarize imWS_mintime=min(TimeGenerated), imWS_maxtime=max(TimeGenerated),
  EventCount=count() by SrcIpAddr, DstIpAddr, Url, Dvc, EventProduct, EventVendor
```

Storm-2603 C2 communication

Look for devices that may have communicated with Storm-2603 C2 infrastructure as part of this activity.

```
//IP list and domain list- _Im_NetworkSession
let lookback = 30d;
let ioc_ip_addr = dynamic(["65.38.121.198"]);
let ioc_domains = dynamic(["update.updatemicfosoft.com"]);
_Im_NetworkSession(starttime=todatetime(ago(lookback)), endtime=now())
| where DstIpAddr in (ioc_ip_addr) or DstDomain has_any (ioc_domains)
| summarize imNWS_mintime=min(TimeGenerated), imNWS_maxtime=max(TimeGenerated),
  EventCount=count() by SrcIpAddr, DstIpAddr, DstDomain, Dvc, EventProduct, EventVendor
```

Microsoft Security Copilot

Microsoft Security Copilot customers can use the standalone experience to create their own prompts or run the following prebuilt promptbooks to automate incident response or investigation tasks related to this threat:

- Vulnerability impact assessment

Note that some promptbooks require access to plugins for Microsoft products such as Microsoft Defender XDR or Microsoft Sentinel.

Threat intelligence reports

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

Microsoft Defender Threat Intelligence

Microsoft Security Copilot customers can also use the Microsoft Security Copilot integration in Microsoft Defender Threat Intelligence, either in the Security Copilot standalone portal or in the embedded experience in the Microsoft Defender portal to get more information about this threat actor.

MITRE ATT&CK techniques observed

Threat actors have exhibited use of the following attack techniques. For standard industry documentation about these techniques, refer to the MITRE ATT&CK framework.

Initial Access

- T1190 Exploit public-facing application | Use of known vulnerabilities to exploit internet-facing on-premises SharePoint severs

Discovery

- T1033 System Owner/User Discovery | Whoami commands run after initial access and privilege escalation

Execution

Persistence

Privilege Escalation

- T1484.001 Domain or Tenant Policy Modification: Group Policy Modification | GPO modification deployed batch scripts for ransomware deployment

Defense Evasion

Credential Access

T1003.001 OS Credential Dumping: LSASS Memory | Mimikatz is used to run module *sekurlsa::logonpasswords*, which lists all available credentials

Lateral Movement

T1570 Lateral Tool Transfer | Impacket is observed leveraging Windows Management Instrumentation to remotely stage and execute payloads

Collection

Command and Control

T1090 Proxy, Technique | Fast reverse proxy tool used for C2 communications

Impact

T1486 Data Encrypted for Impact | Files are encrypted in victim environments as part of ransomware attack

References

Learn more

Meet the experts behind Microsoft Threat Intelligence, Incident Response, and the Microsoft Security Response Center at our VIP Mixer at Black Hat 2025. Discover how our end-to-end platform can help you strengthen resilience and elevate your security posture.

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn, X (formerly Twitter), and Bluesky.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast.