

Silk Typhoon targeting IT supply chain

 microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/

March 5, 2025

[Skip to main content](#)



By

Executive summary:

Microsoft Threat Intelligence identified a shift in tactics by Silk Typhoon, a Chinese espionage group, now targeting common IT solutions like remote management tools and cloud applications to gain initial access. While they haven't been observed directly targeting Microsoft cloud services, they do exploit unpatched applications that allow them to elevate their access in targeted organizations and conduct further malicious activities. After successfully compromising a victim, Silk Typhoon uses the stolen keys and credentials to infiltrate customer networks where they can then abuse a variety of deployed applications, including Microsoft services and others, to achieve their espionage objectives. Our latest blog explains how Microsoft security solutions detect these threats and offers mitigation guidance, aiming to raise awareness and strengthen defenses against Silk Typhoon's activities.

Silk Typhoon is an espionage-focused Chinese state actor whose activities indicate that they are a well-resourced and technically efficient group with the ability to quickly operationalize exploits for discovered zero-day vulnerabilities in edge devices. This threat actor holds one of the largest targeting footprints among Chinese threat actors. Part of this is due to their opportunistic nature of acting on discoveries from vulnerability scanning operations, moving quickly to the exploitation phase once they discover a vulnerable public-facing device that they could exploit.

As a result, Silk Typhoon has been observed targeting a wide range of sectors and geographic regions, including but not limited to information technology (IT) services and infrastructure, remote monitoring and management (RMM) companies, managed service providers (MSPs) and affiliates, healthcare, legal services, higher education, defense, government, non-governmental organizations (NGOs), energy, and others located in the United States and throughout the world.

Silk Typhoon has shown proficiency in understanding how cloud environments are deployed and configured, allowing them to successfully move laterally, maintain persistence, and exfiltrate data quickly within victim environments. Since Microsoft Threat Intelligence began tracking this threat actor in 2020, Silk Typhoon has used a myriad of web shells that allow them to execute commands, maintain persistence, and exfiltrate data from victim environments.

As with any observed nation-state threat actor activity, Microsoft has directly notified targeted or compromised customers, providing them with important information needed to secure their environments. We're publishing this blog to raise awareness of Silk Typhoon's recent and long-standing malicious activities, provide mitigation and hunting guidance, and help disrupt operations by this threat actor.

Recent Silk Typhoon activity

Supply chain compromise

Since late 2024, Microsoft Threat Intelligence has conducted thorough research and tracked ongoing attacks performed by Silk Typhoon. These efforts have significantly enhanced our understanding of the actor's operations and uncovered new tradecraft used by the actor. In particular, Silk Typhoon was observed abusing stolen API keys and credentials associated with privilege access management (PAM), cloud app providers, and cloud data management companies, allowing the threat actor to access these companies' downstream customer environments. Companies within these sectors are possible targets of interest to the threat actor. The observations below were observed once Silk Typhoon successfully stole the API key:

- Silk Typhoon used stolen API keys to access downstream customers/tenants of the initially compromised company.
- Leveraging access obtained via the API key, the actor performed reconnaissance and data collection on targeted devices via an admin account. Data of interest overlaps with China-based interests, US government policy and administration, and legal process and documents related to law enforcement investigations.
- Additional tradecraft identified included resetting of default admin account via API key, web shell implants, creation of additional users, and clearing logs of actor-performed actions.
- Thus far the victims of this downstream activity were largely in the state and local government, and the IT sector.

Password spray and abuse

Silk Typhoon has also gained initial access through successful password spray attacks and other password abuse techniques, including discovering passwords through reconnaissance. In this reconnaissance activity, Silk Typhoon leveraged leaked corporate passwords on public repositories, such as GitHub, and were successfully authenticated to the corporate account. This demonstrates the level of effort that the threat actor puts into their research and reconnaissance to collect victim information and highlights the importance of password hygiene and the use of multifactor authentication (MFA) on all accounts.

Silk Typhoon TTPs

Initial access

Silk Typhoon has pursued initial access attacks against targets of interest through development of zero-day exploits or discovering and targeting vulnerable third-party services and software providers. Silk Typhoon has also been observed gaining initial access via compromised credentials. The software or services targeted for initial access focus on IT providers, identity management, privileged access management, and RMM solutions.

In January 2025, Silk Typhoon was also observed exploiting a zero-day vulnerability in the public facing Ivanti Pulse Connect VPN ([CVE-2025-0282](#)). Microsoft Threat Intelligence Center reported the activity to Ivanti, which led to a rapid resolution of the critical exploit, significantly reducing the period that highly skilled and sophisticated threat actors could leverage the exploit.

Lateral movement to cloud

Once a victim has been successfully compromised, Silk Typhoon is known to utilize common yet effective tactics to move laterally from on-premises environments to cloud environments. Once the threat actor has gained access to an on-premises environment, they look to dump

Active Directory, steal passwords within key vaults, and escalate privileges. Furthermore, Silk Typhoon has been observed targeting Microsoft AADConnect servers in these post-compromise activities. AADConnect (now Entra Connect) is a tool that synchronizes on-premises Active Directory with Entra ID (formerly Azure AD). A successful compromise of these servers could allow the actor to escalate privileges, access both on-premises and cloud environments, and move laterally.

Manipulating service principals/applications

While analyzing post-compromise tradecraft, Microsoft identified Silk Typhoon abusing service principals and OAuth applications with administrative permissions to perform email, OneDrive, and SharePoint data exfiltration via MSGraph. Throughout their use of this technique, Silk Typhoon has been observed gaining access to an application that was already consented within the tenant to harvest email data and adding their own passwords to the application. Using this access, the actors can steal email information via the MSGraph API. Silk Typhoon has also been observed compromising multi-tenant applications, potentially allowing the actors to move across tenants, access additional resources within the tenants, and exfiltrate data.

If the compromised application had privileges to interact with the Exchange Web Services (EWS) API, the threat actors were seen compromising email data via EWS.

In some instances, Silk Typhoon was seen creating Entra ID applications in an attempt to facilitate this data theft. The actors would typically name the application in a way to blend into the environment by using legitimate services or Office 365 themes.

Use of covert networks

Silk Typhoon is known to utilize covert networks to obfuscate their malicious activities. Covert networks, tracked by Microsoft as “CovertNetwork”, refer to a collection of egress IPs consisting of compromised or leased devices that may be used by one or more threat actors. Silk Typhoon was observed utilizing a covert network that is comprised of compromised Cyberoam appliances, Zyxel routers, and QNAP devices. The use of covert networks has become a common tactic among various threat actors, particularly Chinese threat actors.

Historical Silk Typhoon zero-day exploitation

Since 2021, Silk Typhoon has been observed targeting and compromising vulnerable unpatched Microsoft Exchange servers, GlobalProtect Gateway on Palo Alto Networks firewalls, Citrix NetScaler appliances, Ivanti Pulse Connect Secure appliances, and others. While not exhaustive, below are historical zero-day vulnerabilities that Silk Typhoon was observed compromising for initial access into victim environments.

GlobalProtect Gateway on Palo Alto Networks Firewalls

In March 2024, Silk Typhoon used a zero-day exploit for CVE-2024-3400 in GlobalProtect Gateway on Palo Alto Networks firewalls to compromise multiple organizations:

CVE-2024-3400 – A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

Citrix NetScaler ADC and NetScaler Gateway

In early 2024, Microsoft began to observe Silk Typhoon compromising zero-day vulnerabilities within Citrix NetScaler ADC and NetScaler Gateways:

CVE-2023-3519 – An unauthenticated remote code execution (RCE) vulnerability affecting NetScaler (formerly Citrix) Application Delivery Controller (ADC) and NetScaler Gateway

Microsoft Exchange Servers

In January 2021, Microsoft began to observe Silk Typhoon compromising zero-day vulnerabilities in Microsoft Exchange Servers. Upon discovery, Microsoft addressed those issues and issued security updates along with related guidance (related links below):

- CVE-2021-26855 – A server-side request forgery (SSRF) vulnerability in Exchange that could allow an attacker to send arbitrary HTTP requests and authenticate as the Exchange server.
- CVE-2021-26857 – An insecure deserialization vulnerability in the Unified Messaging service. Insecure deserialization is where untrusted user-controllable data is deserialized by a program. Exploiting this vulnerability gave Silk Typhoon the ability to run code as SYSTEM on the Exchange server. This requires administrator permission or another vulnerability to be exploited.
- CVE-2021-26858 – A post-authentication arbitrary file write vulnerability in Exchange. If Silk Typhoon could authenticate with the Exchange server, then it could use this vulnerability to write a file to any path on the server. It could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate administrator's credentials.
- CVE-2021-27065 – A post-authentication arbitrary file write vulnerability in Exchange. If Silk Typhoon could authenticate with the Exchange server, then it could use this vulnerability to write a file to any path on the server. It could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate administrator's credentials.

During recent activities and historical exploitation of these appliances, Silk Typhoon utilized a variety of web shells to maintain persistence and to allow the actors to remotely access victim environments.

Hunting guidance

To help mitigate and surface various aspects of recent Silk Typhoons activities, Microsoft recommends the following:

- Inspect log activity related to Entra Connect servers for anomalous activity.
- Where these targeted applications have highly privileged accounts, inspect service principals for newly created secrets (credentials).
- Identify and analyze any activity related to newly created applications.
- Identify all multi-tenant applications and scrutinize authentications to them.
- Analyze any observed activity related to use of Microsoft Graph or eDiscovery particularly for SharePoint or email data exfiltration
- Look for newly created users on devices impacted by vulnerabilities targeted by Silk Typhoon and investigate virtual private network (VPN) logs for evidence of VPN configuration modifications or sign-in activity during the possible window of compromise of unpatched devices.

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.

Microsoft Sentinel customers can use the following queries to detect behavior associated with Silk Typhoon:

- [Anomalous password reset](#)
- [Privileged logon from new ASN](#)
- [Anomalous account creation](#)
- [Web shell activity](#)
- [Potential web shell](#)
- [Sign-in password spray](#)
- [Smart lockouts](#)
- [Credential dumping tools file artifacts](#)
- [NTDS theft](#)
- [Time series keyvault access anomaly](#)
- [Keyvault mass secret retrieval](#)

- [Suspicious sign-in by AADConnect account](#)
- [New service principal running queries](#)
- [SharePoint downloads by IP](#)
- [Anomaly of MailItem access by GraphAPI](#)

Customers can use the following query to detect vulnerabilities exploited by Silk Typhoon:

```
DeviceTvmSoftwareVulnerabilities
| where CveId in ("CVE-2025-0282")
| project
DeviceId, DeviceName, OSPlatform, OSVersion, SoftwareVendor, SoftwareName, SoftwareVersion,
CveId, VulnerabilitySeverityLevel
| join kind=inner ( DeviceTvmSoftwareVulnerabilitiesKB | project CveId,
CvssScore, IsExploitAvailable, VulnerabilitySeverityLevel, PublishedDate, VulnerabilityDes
) on CveId
| project
DeviceId, DeviceName, OSPlatform, OSVersion, SoftwareVendor, SoftwareName, SoftwareVersion,
CveId, VulnerabilitySeverityLevel, CvssScore, IsExploitAvailable, PublishedDate, Vulnerabil
```

Recommendations

To help detect and mitigate Silk Typhoon's activity, Microsoft recommends the following:

- Ensure all public facing devices are patched. It's important to note that patching a vulnerable device does not remediate any post-compromise activities by a threat actor who gained privileged access to a vulnerable device.
- Validate any Ivanti Pulse Connect VPN are patched to address [CVE-2025-0282](#) and run the suggested Integrity Checker Tool as suggested in their Advisory. Consider terminating any active or persistent sessions following patch cycles.

- Defend against legitimate application and service principal abuse by establishing strong controls and monitoring for these security identities. Microsoft recommends the following mitigations to reduce the impact of this threat:
 - Audit the current privilege level of all identities, users, service principals, and Microsoft Graph Data Connect applications (use the Microsoft Graph Data Connect authorization portal) to understand which identities are highly privileged. Scrutinize privileges more closely if they belong to an unknown identity, belong to identities that are no longer in use, or are not fit for purpose. Admins may assign identities privileges over and above what is required. Defenders should pay attention to apps with app-only permissions as those apps might have over-privileged access. Read additional guidance for investigating compromised and malicious applications. Identify abused OAuth apps using anomaly detection policies. Detect abused OAuth apps that make sensitive Exchange Online administrative activities through Microsoft Defender for Cloud Apps. Investigate and remediate any risky OAuth apps. Review any applications that hold *EWS.AccessAsUser.All* and *EWS.full_access_as_app* permissions and understand whether they are still required in the tenant. This can be done using App governance in Microsoft Defender for Cloud Apps. If these permissions are no longer required, they should be removed.
 - If applications must access mailboxes, granular and scalable access can be implemented using role-based access control for applications in Exchange Online. This access model ensures applications are only granted to the specific mailboxes required.
- Monitor for service principal sign-ins from unusual locations. Two important reports can provide useful daily activity monitoring:
 - The risky sign-ins report surfaces attempted and successful user access activities where the legitimate owner might not have performed the sign-in.
 - The risky users report surfaces user accounts that might have been compromised, such as a leaked credential that was detected or the user signing in from an unexpected location in the absence of planned travel.
- Defend against credential compromise by building credential hygiene, practicing the principle of least privilege, and reducing credential exposure. Microsoft recommends the following mitigations to reduce the impact of this threat.
- Implement the Azure Security Benchmark and general best practices for securing identity infrastructure, including:
 - Prevent on-premises service accounts from having direct rights to the cloud resources to prevent lateral movement to the cloud.
 - Ensure that “break glass” account passwords are stored offline and configure honey-token activity for account usage.
 - Implement Conditional Access policies enforcing Microsoft’s Zero Trust principles.

- Enable risk-based user sign-in protection and automate threat response to block high-risk sign-ins from all locations and enable multifactor authentication (MFA) for medium-risk ones.
- Ensure that VPN access is protected using modern authentication methods.
- Identify all multi-tenant applications, assess permissions, and investigate suspicious sign-ins.

Indicators of compromise

Silk Typhoon is not known to use their own dedicated infrastructure in their operations. Typically, the threat actor uses compromised covert networks, proxies, and VPNs for infrastructure, likely to obfuscate their operations. However, they have also been observed using short-lease virtual private server (VPS) infrastructure to support their operations.

Microsoft Defender XDR detections

Microsoft Defender XDR customers can refer to the list of applicable detections below. Microsoft Defender XDR coordinates detection, prevention, investigation, and response across endpoints, identities, email, apps to provide integrated protection against attacks like the threat discussed 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.

Microsoft Defender for Endpoint

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

Silk Typhoon activity group

The following alerts might also indicate threat activity related to this threat. Note, however, that these alerts can be also triggered by unrelated threat activity.

- Possible exploitation of Exchange Server vulnerabilities
- Suspicious web shell detected
- Suspicious Active Directory snapshot dump
- Suspicious credential dump from NTDS.dit

Microsoft Defender for Identity

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

- Suspicious Interactive Logon to the Entra Connect Server
- Suspicious writeback by Entra Connect on a sensitive user

- User Password Reset by Entra Connect Account
- Suspicious Entra sync password change

Microsoft Defender XDR

The following alerts might indicate threat activity related to this threat. Note, however, that these alerts can be also triggered by unrelated threat activity.

Suspicious activities related to Azure Key Vault by a risky user

Microsoft Defender for Cloud

The following alerts might indicate threat activity related to this threat. Note, however, that these alerts can be also triggered by unrelated threat activity.

- Unusual user accessed a key vault
- Unusual application accessed a key vault
- Access from a suspicious IP to a key vault
- Denied access from a suspicious IP to a key vault

Microsoft Defender for Cloud Apps

The following Microsoft Defender for Cloud Apps alerts can indicate associated threat activity if app governance is enabled:

- Unusual addition of credentials to an OAuth app
- Suspicious credential added to dormant app
- Unused app newly accessing APIs
- App with suspicious metadata has Exchange permission
- App with an unusual user agent accessed email data through Exchange Web Services
- App with EWS application permissions accessing numerous emails
- App made anomalous Graph calls to Exchange workload post certificate update or addition of new credentials
- Suspicious user created an OAuth app that accessed mailbox items
- Suspicious OAuth app used for collection activities using Graph API
- Risky user updated an app that accessed Email and performed Email activity through Graph API
- Suspicious OAuth app email activity through Graph API
- Suspicious OAuth app email activity through EWS API

Microsoft Defender Vulnerability Management

Microsoft Defender Vulnerability Management surfaces devices that may be affected by the following vulnerabilities used in this threat:

- CVE-2021-26855
- CVE-2021-26857
- CVE-2021-26858
- CVE-2021-27065

Microsoft Defender External Attack Surface Management

Attack Surface Insights with the following title can indicate vulnerable devices on your network but is not necessarily indicative of exploitation:

- [Potential] CVE-2024-3400 – Palo Alto Networks PAN-OS Command Injection Vulnerability'
- [Potential] CVE-2023-3519 – Citrix NetScaler ADC and Gateway Unauthenticated
- ProxyLogon – Microsoft Exchange Server Vulnerabilities (Hotfix Available)

Note: An Attack Surface Insight marked as [Potential] indicates a service is running but cannot validate whether that service is running a vulnerable version. Customers should check resources to verify that they are up to date as part of their investigation.

Microsoft Security Copilot

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

- Incident investigation
- Microsoft User analysis
- Threat actor profile
- Threat Intelligence 360 report based on MDTI article (see Threat intelligence reports below)
- 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.

Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: <https://aka.ms/threatintelblog>.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn at <https://www.linkedin.com/showcase/microsoft-threat-intelligence>, and on X (formerly Twitter) at <https://x.com/MsftSecIntel>.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: <https://thecyberwire.com/podcasts/microsoft-threat-intelligence>.

Related Posts



Feb 14, 202413 min read

Staying ahead of threat actors in the age of AI

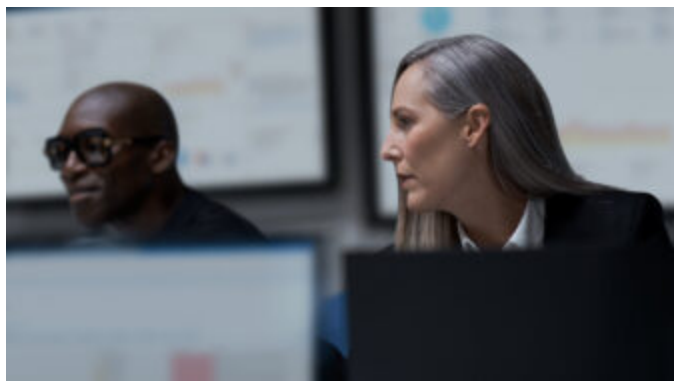
Microsoft, in collaboration with OpenAI, is publishing research on emerging threats in the age of AI, focusing on identified activity associated with known threat actors Forest Blizzard, Emerald Sleet, Crimson Sandstorm, and others. The observed activity includes prompt-injections, attempted misuse of large language models (LLM), and fraud.



Nov 9, 20236 min read

Microsoft shares threat intelligence at CYBERWARCON 2023

At the CYBERWARCON 2023 conference, Microsoft and LinkedIn analysts are presenting several sessions detailing analysis across multiple sets of threat actors and related activity, demonstrating Microsoft Threat Intelligence's ongoing efforts to track threat actors, protect customers, and share information with the wider security community.



Research

Threat intelligence

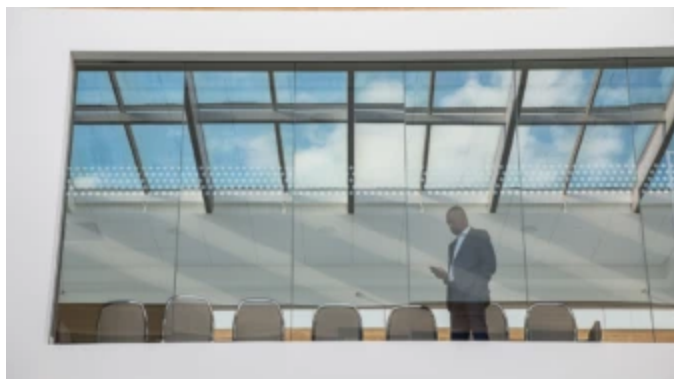
Microsoft Defender XDR

Threat actors

Aug 24, 202313 min read

Flax Typhoon using legitimate software to quietly access Taiwanese organizations

China-based actor Flax Typhoon is exploiting known vulnerabilities for public-facing servers, legitimate VPN software, and open-source malware to gain access to Taiwanese organizations, but not taking further action.



Research

Threat intelligence

Attacker techniques, tools, and infrastructure

Jul 14, 2023 10 min read


Analysis of Storm-0558 techniques for unauthorized email access

Analysis of the techniques used by the threat actor tracked as Storm-0558 (now tracked as Antique Typhoon) for obtaining unauthorized access to email data, tools, and unique infrastructure characteristics.

Get started with Microsoft Security

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

[Learn more](#)



Protect it all
with Microsoft Security