Flax Typhoon using legitimate software to quietly access Taiwanese organizations

microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations

August 24, 2023

By Microsoft Threat Intelligence

> **Summary**
>
> Microsoft has identified a nation-state activity group tracked as Flax Typhoon, based in China, that is targeting dozens of organizations in Taiwan with the likely intention of performing espionage. Flax Typhoon gains and maintains long-term access to Taiwanese organizations' networks with minimal use of malware, relying on tools built into the operating system, along with some normally benign software to quietly remain in these networks. Microsoft has not observed Flax Typhoon using this access to conduct additional actions. This blog aims to raise awareness of the techniques used by this threat actor and inform better defenses to protect against future attacks.

Microsoft has observed a distinctive pattern of malicious activity almost exclusively affecting organizations in Taiwan using techniques that could be easily reused in other operations outside the region and would benefit from broader industry visibility. Microsoft attributes this campaign to Flax Typhoon (overlaps with ETHEREAL PANDA), a nation-state actor based out of China. Flax Typhoon's observed behavior suggests that the threat actor intends to perform espionage and maintain access to organizations across a broad range of industries for as long as possible. However, Microsoft has not observed Flax Typhoon act on final objectives in this campaign. Microsoft is choosing to highlight this Flax Typhoon activity at this time because of our significant concern around the potential for further impact to our customers. Although our visibility into these threats has given us the ability to deploy detections to our customers, the lack of visibility into other parts of the actor's activity compelled us to drive broader community awareness to further investigations and protections across the security ecosystem.

In this blog post, we share information on Flax Typhoon, the current campaign targeting Taiwan, and the actor's tactics for achieving and maintaining unauthorized access to target networks. Because this activity relies on valid accounts and living-off-the-land binaries (LOLBins), detecting and mitigating this attack could be challenging. Compromised accounts must be closed or changed. Compromised systems must be isolated and investigated. At the end of this blog post, we share more mitigation steps and best practices, as well as provide details on how Microsoft 365 Defender detects malicious and suspicious activity to protect organizations from such stealthy attacks.

Who is Flax Typhoon?

Flax Typhoon has been active since mid-2021 and has targeted government agencies and education, critical manufacturing, and information technology organizations in Taiwan. Some victims have also been observed elsewhere in Southeast Asia, as well as in North America and Africa. Flax Typhoon focuses on persistence, lateral movement, and credential access. As with any observed nation-state actor activity, Microsoft has directly notified targeted or compromised customers, providing them with important information needed to secure their environments.

Flax Typhoon is known to use the *China Chopper* web shell, Metasploit, Juicy Potato privilege escalation tool, Mimikatz, and SoftEther virtual private network (VPN) client. However, Flax Typhoon primarily relies on living-off-the-land techniques and hands-on-keyboard activity. Flax Typhoon achieves initial access by exploiting known vulnerabilities in public-facing servers and deploying web shells like *China Chopper*. Following initial access, Flax Typhoon uses command-line tools to first establish persistent access over the remote desktop protocol, then deploy a VPN connection to actor-controlled network infrastructure, and finally collect credentials from compromised systems. Flax Typhoon further uses this VPN access to scan for vulnerabilities on targeted systems and organizations from the compromised systems.

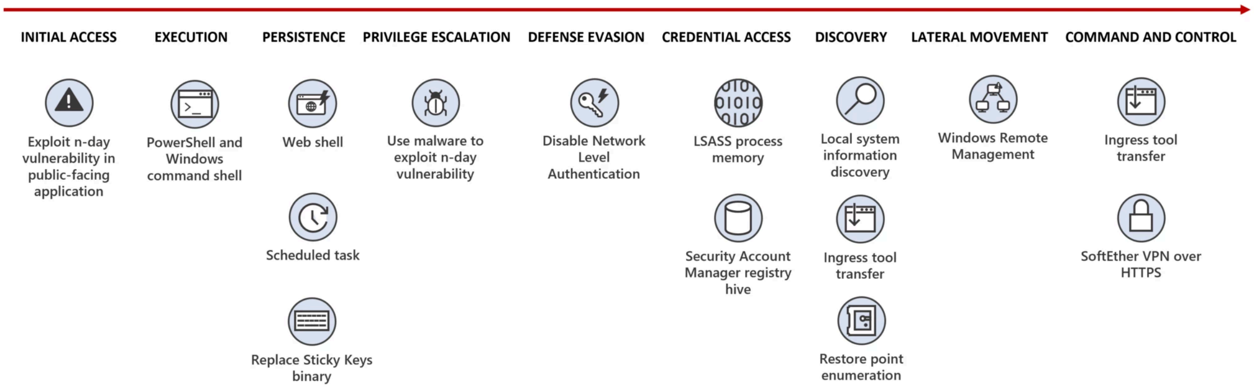
INITIAL ACCESS
EXECUTION
PERSISTENCE
PRIVILEGE ESCALATION
DEFENSE EVASION
CREDENTIAL ACCESS
DISCOVERY
LATERAL MOVEMENT
COMMAND AND CONTROL
Exploit n-day vulnerability in public-facing application
PowerShell and Windows command shell
Web shell
Scheduled task
Replace Sticky Keys binary
Use malware to exploit n-day vulnerability
Disable Network Level Authentication
LSASS process memory
Security Account Manager registry hive
Local system information discovery
Ingress tool transfer
Restore point enumeration
Windows Remote Management
Ingress tool transfer
SoftEther VPN over HTTPS

Figure 1. Flax Typhoon attack chain

Analysis of current campaign

Initial access

Flax Typhoon achieves initial access by exploiting known vulnerabilities in public-facing servers. The services targeted vary, but include VPN, web, Java, and SQL applications. The payload in these exploits is a web shell, such as *China Chopper*, which allows for remote code execution on the compromised server.

Privilege escalation

In cases where the process compromised via web shell does not have local administrator privileges, Flax Typhoon downloads and runs a piece of malware that exploits one or more known vulnerabilities to obtain local system privileges. Microsoft has observed the actor use Juicy Potato, BadPotato, and other open-source tools to exploit these vulnerabilities.

Persistence

Once Flax Typhoon can access Windows Management Instrumentation command-line (WMIC), PowerShell, or the Windows Terminal with local administrator privileges, the actor establishes a long-term method of accessing the compromised system using the remote desktop protocol (RDP). To accomplish this, the actor disables network-level authentication (NLA) for RDP, replaces the Sticky Keys binary, and establishes a VPN connection.

When using RDP, NLA requires the connecting user to authenticate to the remote system before a full remote session is established and the Windows sign-in screen is displayed. When NLA is disabled, any user attempting to access the remote system can interact with the Windows sign-in screen before authenticating, which can expose the remote system to malicious actions by the connecting user. Flax Typhoon changes a registry key to disable NLA, allowing them to access the Windows sign-in screen without authenticating, whereupon the actor will use the Sticky Keys shortcut.

Figure 2. Flax Typhoon command disabling NLA

Sticky Keys is an accessibility feature in Windows that allows users to press modifier keys (such as *Shift*, *Ctrl*, *Alt*) one at a time instead of simultaneously. It includes a shortcut where the user can press the *Shift* key five times in succession to launch *sethc.exe*, the program that manages Sticky Keys. The user can invoke this shortcut at any time, including at the sign-in screen. To take advantage of this feature, Flax Typhoon changes a registry key that specifies the location of *sethc.exe*. The actor adds arguments that cause the Windows Task Manager to be launched as a debugger for *sethc.exe*. As a result, when the actor uses the Sticky Keys shortcut on the Windows sign-in screen, Task Manager launches with local system privileges.

Figure 3. Flax Typhoon command altering Sticky Keys behavior

At this stage, Flax Typhoon can access the compromised system via RDP, use the Sticky Keys shortcut at the sign-in screen, and access Task Manager with local system privileges. From there, the actor can launch the Terminal, create memory dumps, and take nearly any other action on the compromised system. The only issue the actor faces with this persistence method is that RDP is most likely running on an internal-facing network interface. Flax Typhoon's solution is to install a legitimate VPN bridge to automatically connect to actor-controlled network infrastructure.

Command and control

To deploy the VPN connection, Flax Typhoon downloads an executable file for SoftEther VPN from their network infrastructure. The actor downloads the tool using one of several LOLBins, such as the PowerShell Invoke-WebRequest utility, certutil, or bitsadmin. Flax Typhoon then uses the Service Control Manager (SCM) to create a Windows service that launches the VPN connection automatically when the system starts. This could allow the actor to monitor the availability of the compromised system and establish an RDP connection.

Figure 4. Flax Typhoon command downloading a SoftEther VPN executable

Figure 5. Flax Typhoon command creating a service to launch the VPN connection

Flax Typhoon takes several precautions with their VPN connection to make it harder to identify. First, the actor uses a legitimate VPN application that could be found in enterprise environments. As a result, the file itself is almost certain to go undetected by antivirus products. Second, the actor almost always renames the executable file from *vpnbridge.exe* to *conhost.exe* or *dllhost.exe*. These names imitate the legitimate Windows components Console Window Host Process and Component Object Model Surrogate respectively. Third, the actor uses SoftEther's VPN-over-HTTPS operation mode, which uses protocol tunneling to encapsulate Ethernet packets into compliant HTTPS packets and transmit them to TCP port 443. This makes the VPN connection very difficult to differentiate from legitimate HTTPS traffic, which most network security appliances would not block.

In cases where Flax Typhoon needs to move laterally to access other systems on the compromised network, the actor uses LOLBins, including Windows Remote Management (WinRM) and WMIC.

Microsoft has observed Flax Typhoon routing network traffic to other targeted systems through the SoftEther VPN bridge installed on compromised systems. This network traffic includes network scanning, vulnerability scanning, and exploitation attempts.

Credential access

Once Flax Typhoon becomes established on the target system, Microsoft observes the actor conducting credential access activities using common tools and techniques. Most commonly, Flax Typhoon targets the Local Security Authority Subsystem Service (LSASS) process memory and Security Account Manager (SAM) registry hive. Both stores contain hashed passwords for users signed into the local system. Flax Typhoon frequently deploys Mimikatz, a publicly available malware that can automatically dump these stores when improperly secured. The resulting password hashes can be cracked offline or used in pass-the-hash (PtH) attacks to access other resources on the compromised network.

Flax Typhoon also enumerates restore points used by System Restore. Restore points contain data about the Windows operating system that the system owner can use to revert changes to the system if it becomes inoperable, rather than a backup of user data. Flax Typhoon could use this information to better understand the compromised system or as a template for removing indicators of malicious activity.

This pattern of activity is unusual in that minimal activity occurs after the actor establishes persistence. Flax Typhoon's discovery and credential access activities do not appear to enable further data-collection and exfiltration objectives. While the actor's observed behavior suggests Flax Typhoon intents to perform espionage and maintain their network footholds, Microsoft has not observed Flax Typhoon act on final objectives in this campaign.

Mitigation and protection guidance

Defending against techniques used by Flax Typhoon begins with vulnerability and patch management, particularly on systems and services exposed to the public internet. The credential access techniques used can also be mitigated with proper system hardening.

What to do now if you're affected

Affected organizations need to assess the scale of Flax Typhoon activity in their network, remove malicious tools and C2 infrastructure, and check logs for signs of compromised accounts that may have been used for malicious purposes.

Investigating Suspected compromised accounts or affected systems

- Find LSASS and SAM dumping to identify affected accounts.
- Examine the activity of compromised accounts for any malicious actions or exposed data.
- Close or change credentials for all compromised accounts. Depending on the level of activity, many accounts may be affected.
- Affected systems should be isolated and forensically examined for artifacts of malicious activity.
- Because Flax Typhoon alters the configuration of the operating system to produce malicious behavior, affected systems may need to be decommissioned or restored to a known-good configuration.

Defending against Flax Typhoon attacks

- Keep public-facing servers up to date to defend against malicious activity. As prime targets for threat actors, public-facing servers need additional monitoring and security. User input validation, file integrity monitoring, behavioral monitoring, and web application firewalls can all help to better secure these servers.
- Monitor the Windows registry for unauthorized changes. The Audit Registry feature allows administrators to generate events when specific registry keys are modified. Such policies can detect registry changes that undermine the security of a system, like those made by Flax Typhoon.
- Use network monitoring and intrusion detection systems to identify unusual or unauthorized network traffic. If an organization does not use RDP for a specific business purpose, any RDP traffic should be considered unauthorized and generate alerts.
- Ensure that Windows systems are kept updated with the latest security patches, including MS16-075.
- Mitigate the risk of compromised valid accounts by enforcing strong multifactor authentication (MFA) policies using hardware security keys or Microsoft Authenticator. Passwordless sign-in methods (for example, Windows Hello, FIDO2 security keys, or Microsoft Authenticator), password expiration rules, and deactivating unused accounts can also help mitigate risk from this access method.
- Randomize Local Administrator passwords with a tool like Local Administrator Password Solution (LAPS) to prevent lateral movement using local accounts with shared passwords.
- Reduce the attack surface. Microsoft customers can turn on the following attack surface reduction rules to block or audit some observed activity associated with this threat:
    - Block credential stealing from the Windows local security authority subsystem (*lsass.exe*).
    - Block process creations originating from PSExec and WMI commands. Some organizations may experience compatibility issues with this rule on certain server systems but should deploy it to other systems to prevent lateral movement originating from PsExec and WMI.
- Harden the LSASS process by enabling Protective Process Light (PPL) for LSASS on Windows 11 devices. New, enterprise-joined Windows 11 (22H2 update) installs have this feature enabled by default. In addition, enable Windows Defender Credential Guard, which is also turned on by default for organizations using the Enterprise edition of Windows 11, as well as Memory integrity (also referred to as hypervisor-protected code integrity or HVCI) for stronger protections on Windows.
- Set the WDigest UseLogonCredential registry value via Group Policy Object to reduce the risk of successful LSASS process memory dumping.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus to cover rapidly evolving attacker tools, techniques, and behaviors such as those exhibited by Flax Typhoon.

- Run endpoint detection and response (EDR) in block mode so that Microsoft Defender for Endpoint 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-compromise.

Detection details and hunting queries

Microsoft 365 Defender detections

> Microsoft 365 Defender is becoming Microsoft Defender XDR. Learn more.

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

- HackTool:Win32/Mimikatz
- Trojan:Win32/Swrort
- HackTool:Win32/Badcastle
- Behavior:Win32/CobaltStrike
- Backdoor:ASP/Chopper

Microsoft Defender for Endpoint

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

- Malicious credential theft tool execution detected
- Suspicious access to LSASS service
- Use of LOLBin to run malicious code
- System file masquerade

Hunting queries

Microsoft 365 Defender

Microsoft 365 Defender customers can run the following queries to find related activity in their networks:

Network activity with Flax Typhoon network infrastructure

```
let ipAddressTimes = datatable(ip: string, startDate: datetime, endDate: datetime)
[
"101.33.205.106", datetime("2022-11-07"), datetime("2022-11-08"),
"39.98.208.61", datetime("2023-07-28"), datetime("2023-08-12"),
"45.195.149.224", datetime("2023-01-04"), datetime("2023-03-29"),
"122.10.89.230", datetime("2023-01-12"), datetime("2023-01-13"),
"45.204.1.248", datetime("2023-02-23"), datetime("2023-05-09"),
"45.204.1.247", datetime("2023-07-24"), datetime("2023-08-10"),
"45.88.192.118", datetime("2022-11-07"), datetime("2022-11-08"),
"154.19.187.92", datetime("2022-12-01"), datetime("2022-12-02"),
"134.122.188.20", datetime("2023-06-13"), datetime("2023-06-20"),
"104.238.149.146", datetime("2023-07-13"), datetime("2023-07-14"),
"139.180.158.51", datetime("2022-08-30"), datetime("2023-07-27"),
"137.220.36.87", datetime("2023-02-23"), datetime("2023-08-04"),
"192.253.235.107", datetime("2023-06-06"), datetime("2023-06-07")
];
let RemoteIPFiltered = DeviceNetworkEvents
| join kind=inner (ipAddressTimes) on $left.RemoteIP == $right.ip
| where Timestamp between (startDate .. endDate);
let LocalIPFiltered = DeviceNetworkEvents
| join kind=inner (ipAddressTimes) on $left.LocalIP == $right.ip
| where Timestamp between (startDate .. endDate);
union RemoteIPFiltered, LocalIPFiltered
```

SoftEther VPN bridge launched by SQL Server process

```
DeviceProcessEvents

| where ProcessVersionInfoOriginalFileName == "vpnbridge.exe" or
ProcessVersionInfoFileDescription == "SoftEther VPN"

| where InitiatingProcessParentFileName == "sqlservr.exe"
```

SoftEther VPN bridge renamed to “conhost.exe” or “dllhost.exe”

```
DeviceProcessEvents

| where ProcessVersionInfoOriginalFileName == "vpnbridge.exe" or
ProcessVersionInfoFileDescription == "SoftEther VPN"

| where ProcessCommandLine has_any ("conhost.exe", "dllhost.exe") or
FolderPath has_any ("mssql", "conhost.exe", "dllhost.exe")
```

Certutil launched by SQL Server process

```
DeviceProcessEvents

| where ProcessCommandLine has_all ("certutil", "-urlcache")

| where InitiatingProcessFileName has_any ("sqlservr.exe",
"sqlagent.exe", "sqlps.exe", "launchpad.exe", "sqldumper.exe")
```

File downloaded by MSSQLSERVER account using certutil

```
DeviceFileEvents

| where InitiatingProcessAccountName == "MSSQLSERVER"

| where InitiatingProcessFileName == "certutil.exe"
```

File renamed to “conhost.exe” or “dllhost.exe”, downloaded using certutil

```
DeviceFileEvents

| where InitiatingProcessFileName == "certutil.exe"

| where FileName in ("conhost.exe", "dllhost.exe")
```

Network connection made by SoftEther VPN bridge renamed to “conhost.exe” or “dllhost.exe”

```
DeviceNetworkEvents

| where InitiatingProcessVersionInfoOriginalFileName == "vpnbridge.exe"
or InitiatingProcessVersionInfoProductName == "SoftEther VPN"

| where InitiatingProcessFileName == "conhost.exe"
```

Network connection made by MSSQLSERVER account, using SoftEther VPN bridge

```
DeviceNetworkEvents

| where InitiatingProcessVersionInfoOriginalFileName == "vpnbridge.exe"
or InitiatingProcessVersionInfoProductName == "SoftEther VPN"

| where InitiatingProcessAccountName == "MSSQLSERVER"
```

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. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy.

Microsoft Sentinel also has a range of detection and threat hunting content that customers can use to detect the post exploitation activity detailed in this blog in addition to Microsoft 365 Defender detections list above.

Indicators of compromise

In addition to compromised SOHO devices and compromised devices used for traffic proxying, Flax Typhoon maintains actor-controlled network infrastructure, including virtual private servers (VPS). Over the course of the campaign, the IP addresses listed in the table below were used during the corresponding timeframes.

IP address	First seen	Last seen	Description
101.33.205[.]106	2022-11-07	2022-11-07	Flax Typhoon network infrastructure
39.98.208[.]61	2023-07-28	2023-08-11	Flax Typhoon network infrastructure
45.195.149[.]224	2023-01-04	2023-03-28	Flax Typhoon network infrastructure
122.10.89[.]230	2023-01-12	2023-01-12	Flax Typhoon network infrastructure
45.204.1[.]248	2023-02-23	2023-05-09	Flax Typhoon network infrastructure
45.204.1[.]247	2023-07-24	2023-08-09	Flax Typhoon network infrastructure
45.88.192[.]118	2022-11-07	2022-11-07	Flax Typhoon network infrastructure
154.19.187[.]92	2022-12-01	2022-12-01	Flax Typhoon network infrastructure
134.122.188[.]20	2023-06-13	2023-06-19	Flax Typhoon network infrastructure
104.238.149[.]146	2023-07-13	2023-07-13	Flax Typhoon network infrastructure
139.180.158[.]51	2022-08-30	2023-07-26	Flax Typhoon network infrastructure
192.253.235[.]107	2023-06-06	2023-06-06	Flax Typhoon network infrastructure

Flax Typhoon hosts its SofEther VPN servers on its own network infrastructure. Because the servers use the HTTPS protocol to disguise network traffic, they must present TLS certificates. Flax Typhoon used the certificates listed in the table below on these VPN servers.

SHA-1 TLS fingerprint	Common name (CN)
7992c0a816246b287d991c4ecf68f2d32e4bca18	vpn437972693.sednc[.]cn
5437d0195c31bf7cedc9d90b8cb0074272bc55df	asljkdqhkhasdq.softether[.]net
cc1f0cdc131dfafd43f60ff0e6a6089cd03e92f1	vpn472462384.softether[.]net
2c95b971aa47dc4d94a3c52db74a3de11d9ba658	softether

References

- https://attack.mitre.org/techniques/T1190
- https://attack.mitre.org/techniques/T1505/003/
- https://attack.mitre.org/software/S0020/
- https://github.com/ohpe/juicy-potato

- https://github.com/BeichenDream/BadPotato
- https://attack.mitre.org/techniques/T1059
- https://attack.mitre.org/techniques/T1546/008/
- https://attack.mitre.org/techniques/T1105/
- https://github.com/SoftEtherVPN/SoftEtherVPN_Stable
- https://attack.mitre.org/techniques/T1543/003
- https://attack.mitre.org/techniques/T1036/005/
- https://github.com/SoftEtherVPN/SoftEtherVPN_Stable/blob/master/WARNING.TXT
- https://attack.mitre.org/techniques/T1572/
- https://attack.mitre.org/techniques/T1003/001/
- https://attack.mitre.org/techniques/T1003/002/
- https://attack.mitre.org/techniques/T1550/002/