TLP:WHITE

利用 ClickFix 技術的 NetSupport RAT 分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2025 年 03 月

一、事件簡介

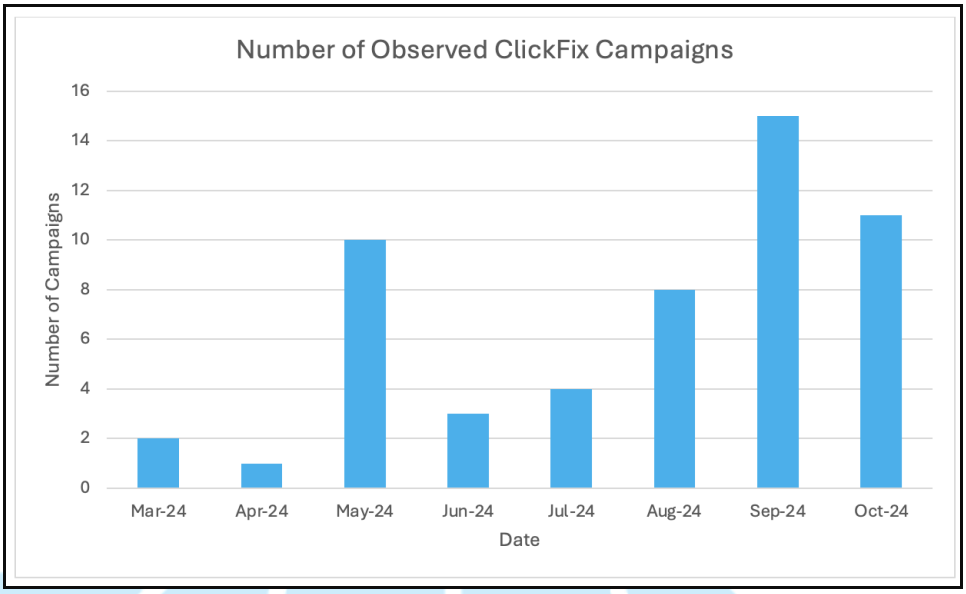
1. 2025/2 The Hacker News 報導 2025 年第一季 5 個比較活躍的惡意軟體，包含 NetSupport RAT、Lynx Ransomware、AsyncRAT、Lumma Stealer 與 InvisibleFerret。
2. 資安研究者觀察到在過去的幾個月中，出現了許多使用「ClickFix」技術的惡意軟體攻擊。它通常由偽造的 CAPTCHA 或類似的流量驗證頁面組成，指示訪客貼上並執行程式碼才能繼續。
3. 2025 年初，攻擊者開始利用 ClickFix 的技術來散播 NetSupport 遠端存取木馬 (RAT)。
4. 為了解 ClickFix 攻擊技術與 NetSupport 的攻擊行為，故進行本次分析。

二、 ClickFix 技術

1. ClickFix 攻擊鏈開始於引誘使用者瀏覽看似合法但實際上已被入侵的網站。瀏覽後，受害者會被重新導向到假的彈出視窗的網站，這些彈出視窗指示他們將腳本貼到 PowerShell 終端機中執行。
2. 以下是 McAfee 於 2024/07 所分析的受「Clickfix」技術影響的使用者分佈熱圖，可看到亞洲也在受影響範圍內。

3. 2024/10 Proofpoint 研究員觀察到 ClickFix 攻擊活動導致

AsyncRAT、Danabot、DarkGate、Lumma Stealer、NetSupport 等惡意軟體的出現。



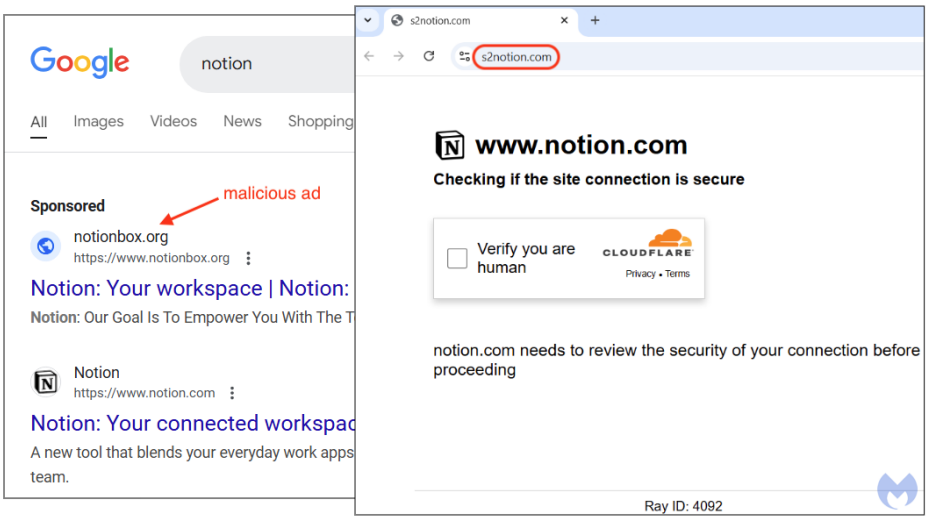
2024 年 3~10 月 ClickFix 攻擊活動量

4. ClickFix 攻擊之運作方法

(1)透過「ClickFix」取得 PowerShell 程式碼

(a)攻擊者為流行的實用應用程式 Notion 製作了 Google 廣告。

(b)第一次點擊廣告時，會被重新導向到顯示「驗證您是人類」頁面的網站，也稱為 Cloudflare Turnstile。但這不是真正的 Cloudflare，而只是一種社會工程技巧。



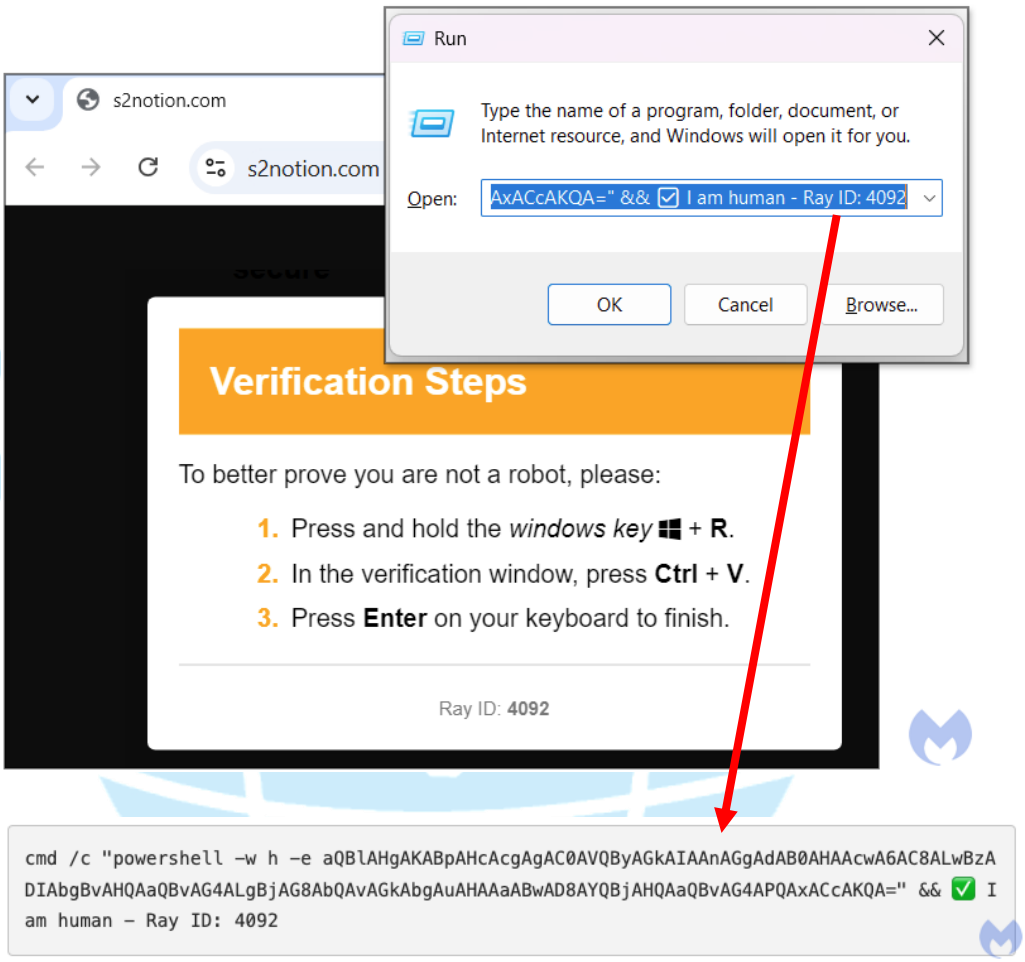
圖片來源:malwarebytes

(2) 點選勾選框以驗證我們是人類之後，會看到新的「驗證步驟」說明，告訴使用者按照視窗指示來證明不是機器人。

(a) 同時按住 Windows 鍵與 R 鍵。(啟動執行對話框。)

(b) 在驗證視窗裡按住 Ctrl 鍵與 V 鍵。(將貼上剪貼簿中的任何內容。)

(c) 按 Enter 鍵完成。(執行惡意命令。)



圖片來源:malwarebytes

三、 NetSupport RAT

1. NetSupport RAT 最初被稱為 NetSupport Manager，是作為合法的遠端 IT 支援程式被開發的，但後來被攻擊者應用於攻擊組織與擷取敏感資訊上，包括螢幕截圖、音訊、視訊和檔案。

2. 它利用 ClickFix 技術，此方法是將假的 CAPTCHA 頁面注入受感染的網站，提示使用者執行惡意 PowerShell 命令來下載並執行 NetSupport RAT。一旦安裝，該木馬就會給予攻擊者對受害者系統的完全控制權，允許進行即時螢幕監控、檔案操作和執行任意命令等活動。

3. NetSupport RAT 的特徵如下。

(1) 攻擊者可以即時查看和控制受害者的螢幕。

(2) 上傳、下載、修改和刪除受感染系統上的檔案。

(3) 遠端執行系統命令和 PowerShell 腳本。

(4) 擷取複製的文字資料，包括密碼和敏感資料。

(5) 記錄使用者敲擊鍵盤情況以竊取憑證。

(6) 啟動、停止和修改系統程序和服務。

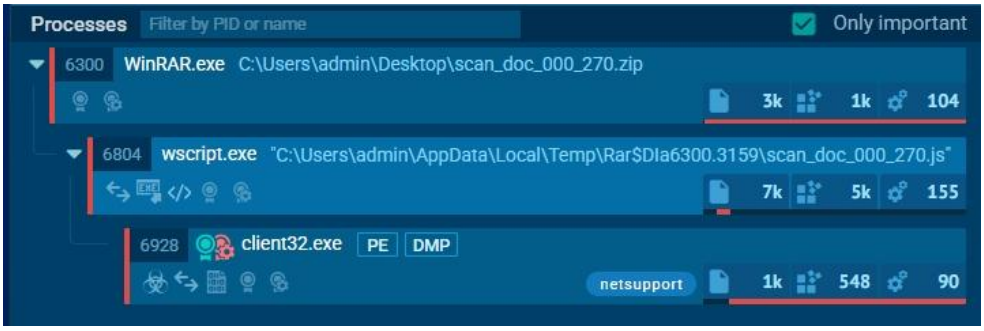
(7) 將自身安裝在啟動資料夾、登錄項目或工作排程任務中，以便在重新啟動後繼續執行。

(8) 使用程序注入和程式碼混淆來逃避偵測。

(9) 使用加密流量與攻擊者保持秘密連線。

4. NetSupport 樣本檢測

(1) 在 ANYRUN 沙箱下檢測 NetSupport RAT 樣本 scan_doc_000_270.zip，MD5:4e46301b9167ed2f4d2fcb261663fc58。系統會先呼叫 WinRAR.exe 來解壓縮 scan_doc_000_270.zip ，之後會呼叫 wscript.exe 來執行一個 JS 腳本。最後，呼叫 client32.exe 來執行 NetSupport RAT。

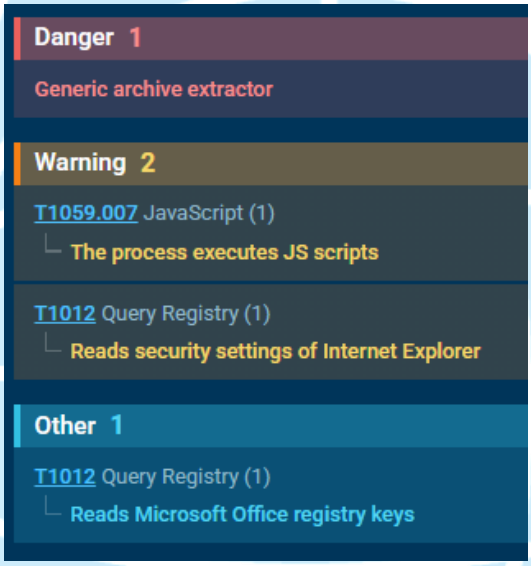


(2) WinRAR.exe 執行後的行為如下所列。

(a) 執行 JS 腳本。

(b) 讀取 Internet Explorer 的安全性設定。

(c) 讀取 Microsoft Office 註冊表項。



(3) wscript.exe 執行後的行為如下所列。

(a) 刪除檔案。

(b) 發送 HTTP 請求，連線 foxauthority.com (IP:104.21.16.1

Port:443)。

GET HTTPS[://]FOXAUTHORITY[.]COM/GB.ZIP?SN=69

(c) 建立新的登錄項目或變更現有登錄項目的值。

(d) 存取環境變數。

(e) 修改登錄啟動項目(可啟動或登入自動啟動執行)。

(f) 檢查指定資料夾是否存在。

(g) 建立新資料夾。

(h) 建立網路連線對象。

(i) 在程式目錄中建立檔案。

(j) 檢查代理伺服器資訊。

(k) 取得正在執行的腳本的完整路徑。

(l) 下載 NetSupport 執行檔。

(m)下載了 C 執行時 libraries。

(n) 刪除合法的 Windows 可執行檔案。

(o) 將可執行內容刪除或覆蓋。

(p) 建立資料夾。

(q) 將資料儲存到二進位檔案。

(r) 建立一個 Stream，可與檔案、輸入/輸出裝置、管道或 TCP/IP sockets 搭配使用。

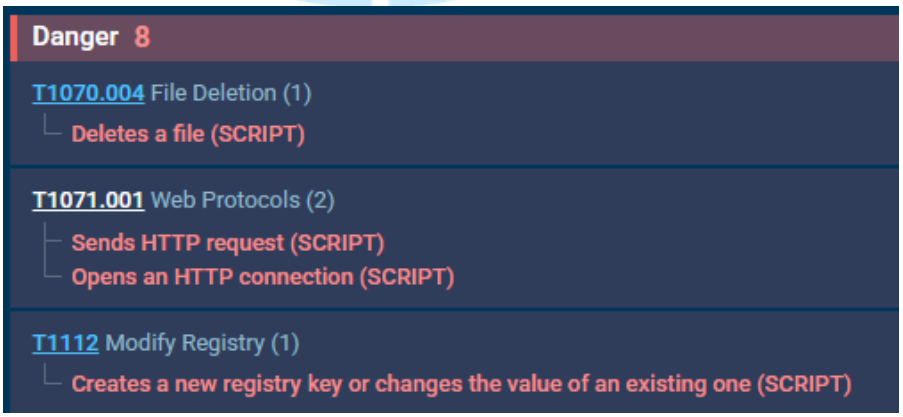
(s) 將二進位資料寫入 Stream 物件。

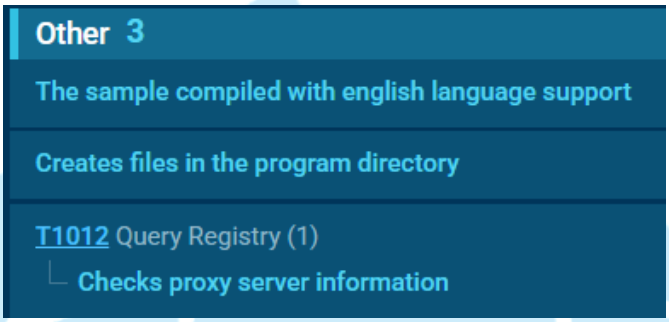
(t) 建立 FileSystem 物件來存取電腦的檔案系統。

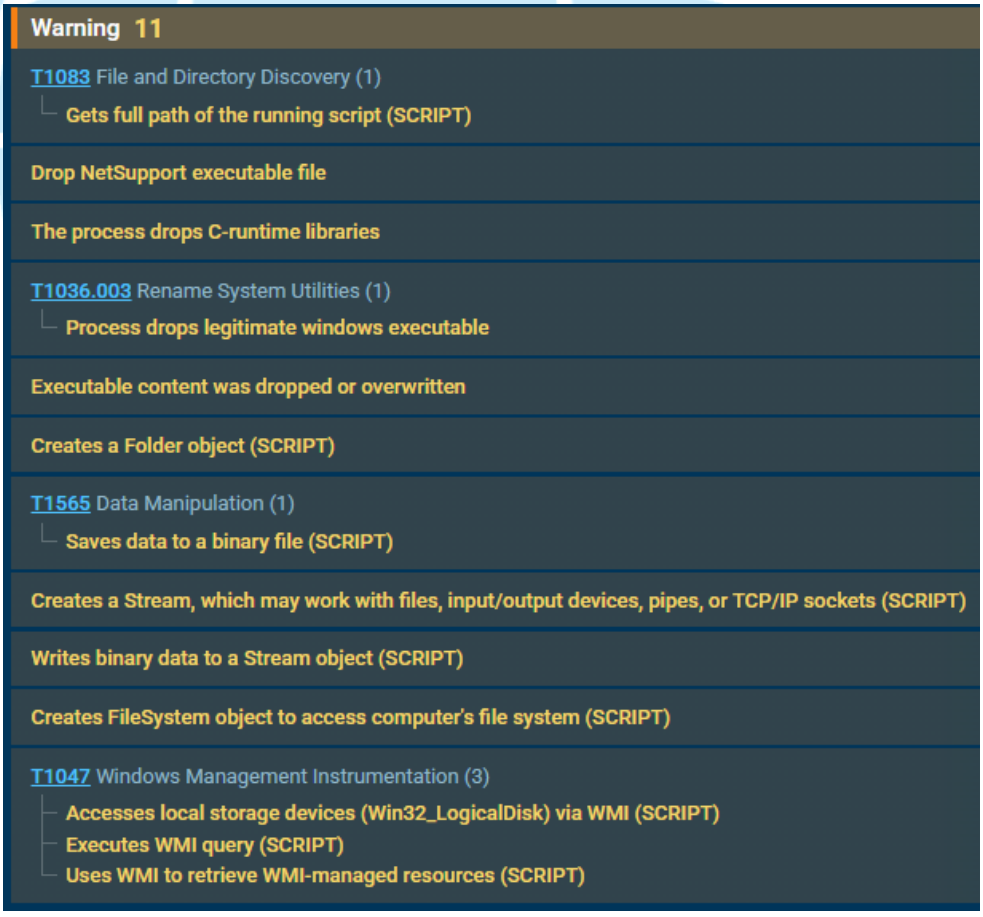
(u) 透過 WMI (Windows Management Instrumentation)存取本機儲存裝置 (Win32_LogicalDisk) 。

(v) 執行 WMI 查詢。

(w)使用 WMI 檢索 WMI 管理的資源。







(4) client32.exe 執行後的行為如下所列。

(a) 執行 NETSUPPORT。

(b) 連線到 C2 伺服器 (IP:111.90.148.193 Port:443) 。

POST HTTP://111[.]90[.]148[.]193/FAKEURL.HTM

(c) 連線 GEO.NETSUPPORTSOFTWARE.COM 侵犯潛在的企業隱私 (IP:104.26.1.231 Port:80) 。

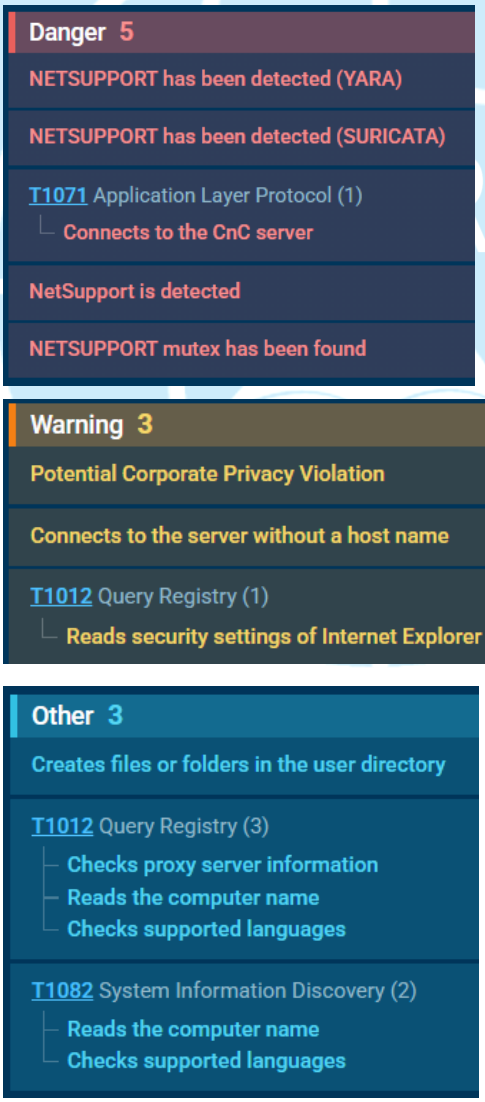
(d) 讀取 Internet Explorer 的安全性設定。

(e) 在使用者目錄中建立檔案或資料夾。

(f) 檢查代理伺服器資訊。

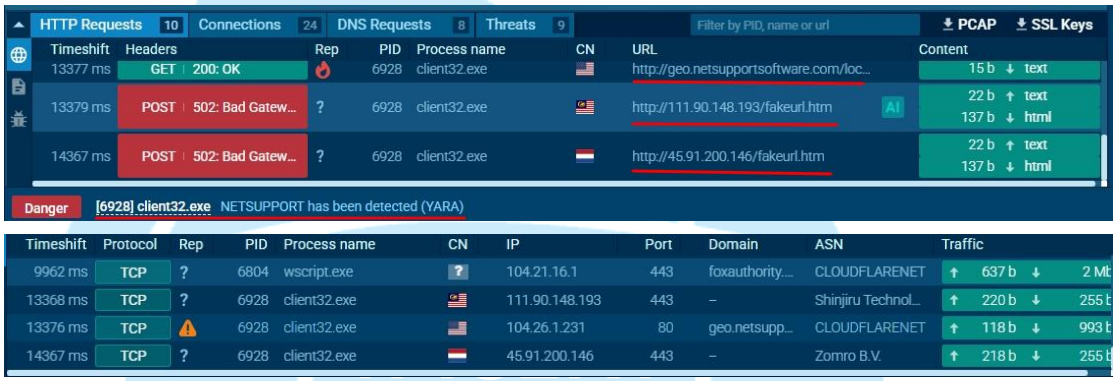
(g) 讀取電腦名稱。

(h) 檢查支援的語言。



(5) 檢視網路連線情形，發現會連線下表所列 IP。

IP	Virustotal	AbuseIPDB
104.21.16.1(美國)	1/94	此 IP 位址已被 47 個不同來源共報告 324 次被遭到濫用。最近一次報告在 2025/03/12。
111.90.148.193(馬來西亞)	1/94	_
104.26.1.231(美國)	0/94	_
45.91.200.146(荷蘭)	0/94	此 IP 位址已被 1 個不同來源報告共 1 次。最近一次報告是在 2022/12/15。



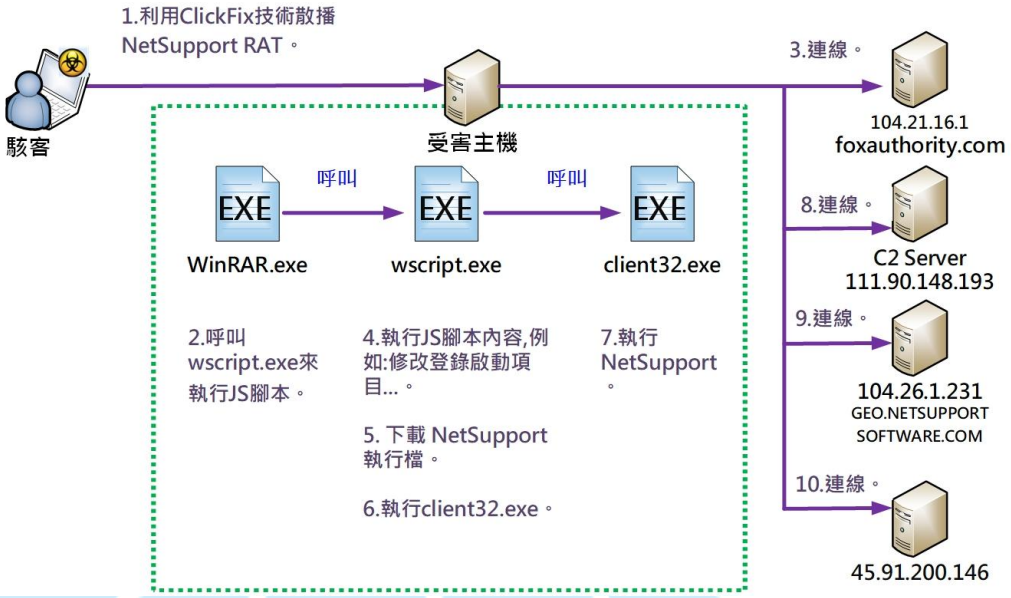
(6) 以 MITRE ATT&CK Matrix 分析 NetSupport RAT，發現該樣本所運用技術橫跨 7 個階段，其中包含:

(a) Persistence & Execution：修改登錄啟動項，透過 wscript.exe 執行腳本。

(b) Discovery：讀取電腦名稱、檢查系統語言並存取環境變數。

(c) Defense Evasion & C2 Communication：刪除合法的 Windows 可執行檔，建立網路連線以進行遠端控制。

5. 攻擊行為示意圖如下。首先，利用 ClickFix 技術散播 NetSupportRAT，在受害主機執行 NetSupport 後會連線 C2 Server。



四、 總結與建議

1. 攻擊者利用 Click Fix 攻擊技術來誘騙受害者執行惡意 PowerShell 命令來下載並執行 NetSupport RAT。假的「驗證您是人類」CAPTCHA 驗證頁面與真的頁面相似度高，當未留意網址是否正確時使用者很容易受騙。
2. 在處理本類型的攻擊事件方面，可採用下面幾個面向來偵測與防範。
   (1) 管理面
      (a) 定期開設教育訓練課程，來教育使用者 ClickFix 攻擊手法與 NetSupport RAT 特徵，以建立資安意識。
      (b) 瀏覽網站出現彈跳視窗時，須留意來源網址的正確性。
   (2) 技術面
      (a) 網路流量監控: 檢測 C2 server 的連線與異常流量的檢測。
      (b) 端點保護:採用 EDR 能偵測到記憶體內的執行、程序注入和異常腳本等行為。
      (c) 工作排程安全性：定期審核工作排程是否有未經授權的工作，尤

其是名稱模仿的工作排程。

(d) 註冊表監控：查看開機自動執行的程序是否有未經授權的修改。

參考資料

1. 5 Active Malware Campaigns in Q1 2025
https://thehackernews.com/2025/02/5-active-malware-campaigns-in-q1-2025.html

2. Security Brief: ClickFix Social Engineering Technique Floods Threat Landscape
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape

3. ClickFix vs. traditional download in new DarkGate campaign
https://www.malwarebytes.com/blog/news/2025/01/clickfix-vs-traditional-download-in-new-darkgate-campaign

4. Threat Actors Exploit ClickFix to Deploy NetSupport RAT in Latest Cyber Attacks
https://thehackernews.com/2025/02/threat-actors-exploit-clickfix-to.html

5. 社交工程攻擊 ClickFix 正在蔓延，駭客透過冒牌 Google Meet 網頁散布竊資軟體
https://www.ithome.com.tw/news/165599