TLP:WHITE

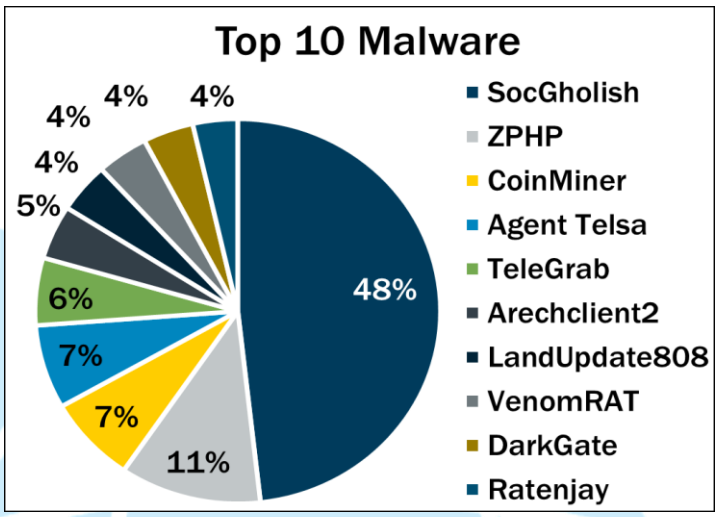
載入器 Socgholish 之分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2025 年 06 月

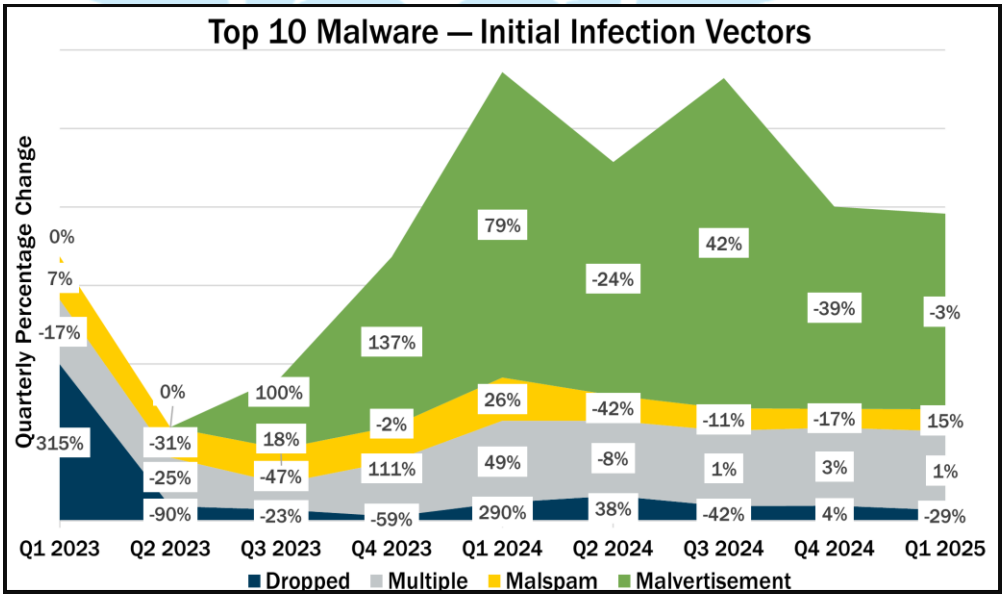
一、事件簡介

1. 根據美國網路安全中心(CIS)2025 年第一季度惡意軟體統計，下載程式 SocGholish 連續第七個季度位居十大惡意軟體榜首，緊接在它之後的是下載程式 ZPHP 與加密貨幣挖礦程式 CoinMiner。



圖片來源:美國網路安全中心 CIS

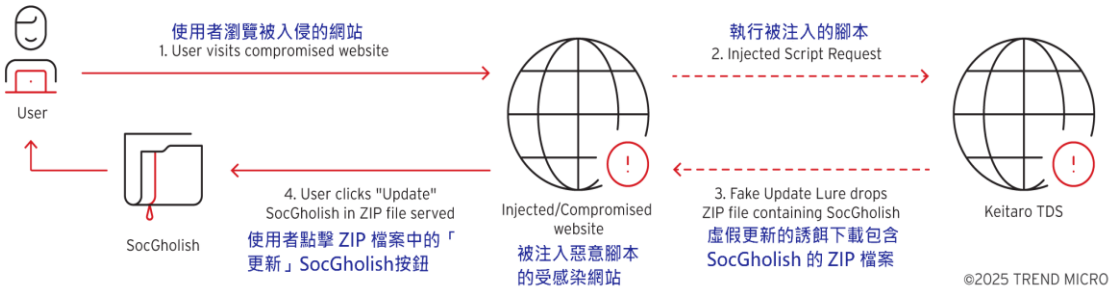
2. LandUpdate808、SocGholish 和 ZPHP 是透過惡意廣告引進的惡意軟體，在 2025 年第一季因 SocGholish、ZPHP 和 LandUpdate808 的感染活動，惡意廣告成為第一大感染媒介。



圖片來源:美國網路安全中心 CIS

二、 Socgholish 的介紹與 MITRE ATT&CK 技術分析

1. 資安公司 redcanary 在「2025 威脅偵測報告」指出，SocGholish(又名 FakeUpdates） 是 2024 年的頭號威脅，它是一款用 JavaScript 編寫的下載程式，利用偽裝成軟體更新的下載程式 (例如:瀏覽器程式的更新)，來誘騙至受感染網站的使用者執行惡意軟體。
2. SocGholish 至少自 2017 年起活躍，而它的散播主要與使用該軟體的駭客組織 Mustard Tempest ，以及來自俄羅斯的駭客組織 Evil Corp 有關。
   (1) Mustard Tempest(又稱 DEV-0206、TA569、GOLD PRELUDE、UNC1543) 是一家代理商，至少自 2017 年以來一直經營散播 SocGholish 的通路。
   (2) Mustard Tempest 與 Evil Corp 合作，提供下載其他惡意軟體的存取權限，包括 LockBit、WastedLocker 和遠端存取工具。
3. 自 2025 年年初以來，SocGholish 的檢測數量在美國最高，其次是日本，然後是台灣。政府機構是受影響最嚴重的組織，銀行業和顧問業分別位居第二和第三。
4. 2025/3 趨勢科技研究發現 SocGholish 的入侵技術協助勒索軟體 RansomHub 散播。分析了 SocGholish 的惡意軟體即服務 (MaaS) 框架及其在透過受感染網站部署 RansomHub 中的作用，發現使用高度混淆的 JavaScript 載入器 SocGholish 來逃避偵測並執行各種惡意任務。



SocGholish 從被入侵的網站到 payload 傳送的傳送流程

圖片來源:趨勢科技

5. 根據 MITRE ATT&CK 分析可得知 SocGholish 使用的技術如下表所示，例如:將 payload 以 JavaScript 方式執行，偽裝成瀏覽器更新的惡意內容來進行散播，搜集系統資訊與系統位置，以及確認是否是 AD 網域的成員…等。

ID	Name	Use
T1059.007	命令和腳本解譯器：JavaScript	payload以 JavaScript 形式執行。
T1074.001	資料暫存：本地資料暫存	可以使用命名約定 rad<5-hex-chars>.tmp 將 whoami 的輸出傳送到本地臨時檔案。
T1482	發現信任的網域	可以分析受損系統以識別網域信任關係。
T1189	驅動式入侵	SocGholish 已透過受感染的網站散播，其惡意內容通常**偽裝成瀏覽器更新**。
T1048.003	透過替代協定進行滲透：透過未加密的非 C2 協定進行滲透	可以**透過 HTTP 將資料直接洩漏到其 C2 網域**。
T1105	Ingress 工具轉移	可以**將其他惡意軟體下載到受感染的主機**。
T1036.005	偽裝：匹配合法資源名稱或位置	SocGholish 命名為 AutoUpdater.js，以**模仿合法的更新檔案**。
T1027.013	混淆的檔案或資訊：加密/編碼檔案	對其第二階段伺服器 URL 具有單一或雙重 Base-64 編碼引用。
T1027.015	混淆檔案或資訊：壓縮	JavaScript payload**已在壓縮的 ZIP 檔案中傳送**。

ID	Name	Use
T1566.002	網路釣魚：魚叉式網路釣魚連結	SocGholish 已透過包含惡意連結的電子郵件散播。
T1057	發現程序	可以列出目標主機上的程序。
T1518	發現軟體	可以**識別受害者的瀏覽器**，以便**提供正確的虛假更新頁面**。
T1082	發現系統資訊	能夠**列舉系統訊息，包括受害者電腦名稱**。
T1614	發現系統位置	可以使用基於 IP 的地理定位將感染限制在北美、歐洲和少數亞太國家的受害者。
T1016	發現系統網路配置	能夠列舉受害者的網域名稱，以及**主機是否是 Active Directory 網域的成員**。
T1033	發現系統所有者/使用者	可以**使用 whoami** 從受感染的主機取得使用者名稱。
T1204.001	使用者執行：惡意連結	引誘受害者與受感染網站上的惡意連結互動，然後執行該操作。
T1102	Web 服務	已使用 Amazon Web Services 來託管第二階段伺服器。
T1047	Windows 管理規範	**使用 WMI 呼叫來執行腳本和進行系統分析**。

三、 SocGholish 感染的四個階段

SocGholish 的感染過程大致可以分為四個階段，每階段的內容分述如下。

第一階段：惡意注入。

惡意攻擊者入侵合法網站並注入惡意程式碼。惡意程式碼會分析使用者訊息，篩選出進一步攻擊的理想目標，第二階段由此開啟。

第二階段：SocGholish。

如果受害者滿足某些條件，第一階段注入的 JavaScript 就會偷偷植入 SocGholish。 SocGholish 通常以虛假瀏覽器更新的形式出現。如果受害者點擊該更新，SocGholish 就會下載到受害者的裝置上。 SocGholish 開啟了第三階段。

第三階段：與 C2 建立連線。

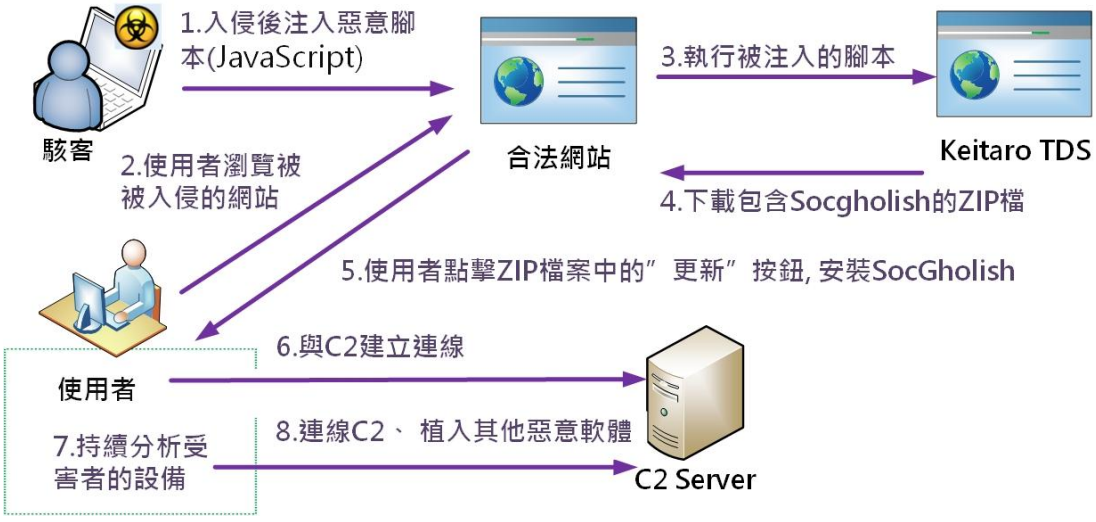
在使用者裝置上安裝 SocGholish 後，惡意軟體會與 C2 進行連線，並從中接收進一步的指令。在此過程中，攻擊者可能會選擇啟動第四階段。

第四階段：後續惡意軟體和感染。

安裝後，SocGholish 會持續分析受害者的設備，並隨後連線 C2 伺服器來植入其他惡意軟體，通常包括遠端存取木馬或勒索軟體。

四、 SocGholish 的攻擊行為

駭客入侵後會注入惡意腳本於合法網站上，當使用者瀏覽網站時，則被注入的腳本執行後會下載包含 SocGholish 的壓縮檔。當使用者解壓縮檔案並點擊更新軟體的按鈕後，則會安裝 SocGholish 於使用者的主機上。之後，該主機會與 C2 Server 建立連線，持續分析主機，以及連線 C2 Server 並植入其他惡意軟體於主機上。



五、 總結與建議

1. SocGholish 利用社交工程與 JavaScript 惡意腳本的攻擊，主要透過偽造瀏覽器更新提示來引誘受害者下載惡意軟體，進而進一步部署如 Cobalt Strike、RAT 或 勒索病毒（如 LockBit）。
2. SocGholish 的特點是其混淆的 JavaScript 載入器，它使用各種規避技術來繞過傳統的檢測方法，故不容易檢測出它。因此，如何防範 SocGholish 是一個重要議題。
3. 防範 SocGholish 載入器的方法如下，提供參考。

(1) 教育使用者提升警覺

教育使用者「瀏覽器不會透過網站提示你更新！」的觀念，強調不要點擊任何「這個瀏覽器版本過期」或「點此更新 Chrome」這類彈跳視窗，並且鼓勵從官方渠道（如 Google、Mozilla）來源進行軟體更新。

(2) 使用可靠防毒/EDR 解決方案

使用支援行為偵測與腳本分析的防毒軟體，也可用 EDR 攔截由 Socgholish 掛載的可疑 JS 腳本或 PowerShell 的執行。

(3) 限制 PowerShell 與 Script 執行

限制使用者執行 PowerShell 或 Windows Script Host（例如 .vbs/.js），而且可對 Script Execution Policies 做策略控管，以及使用 Applocker、Windows Defender Application Control（WDAC）限制未簽名腳本執行。

(4) DNS 與網域過濾

使用 DNS 防護服務來封鎖已知 Socgholish 相關的惡意網域或 TDS（流量導向系統），並且設定防火牆禁止非必要的地理區域或可疑網段流量。

(5) Web Proxy 與 URL 過濾

對 HTTP/HTTPS 流量進行監控與過濾，並且建立自訂 URL 類別封鎖，例如「Software Updates」「Browser Warning Pages」。

(6) 威脅情資整合

訂閱並匯入 Socgholish 的 IOCs（Indicators of Compromise）：(a)惡意網域（例如 update-browser[.]com, chrome-upgrade[.]org 等）、(b)C2 主機 IP、User-Agent、腳本指紋等，多數情資供應商（如 Proofpoint、Recorded Future、Mandiant）都追蹤這類攻擊活動。

(7) 端點監控（EDR/XDR）

可監控如以下的行為模式：(a)使用者透過瀏覽器下載 .js、.zip、.iso 等檔案、(b)解壓縮後出現 PowerShell 或 WScript 執行異常行為、(C)突然連外連線至陌生 IP/C2。

(8) SIEM 檢查（如 Splunk、Elastic）

可監控以下 log 模式：(a)多個使用者同時嘗試下載更新程式（JS/EXE）、(b)使用者端出現 powershell -EncodedCommand 的行為、(C)不明檔案在 AppData\Local\Temp、Downloads 中出現並執行。

4. 有關 SocGholish 的預防策略總覽整理如下表，提供學校參考。

層級	預防策略
使用者教育	不點擊網站中的瀏覽器更新提示
系統端安全	限制 PowerShell、腳本執行； 使用 EDR/XDR
DNS/網路層	阻擋已知惡意域名與可疑流量
威脅情報整合	定期更新 IOCs，整合 SIEM 偵測
行為分析	偵測異常下載、執行、連線行為

參考資料

1. **Top 10 Malware Q1 2025 (2025/04/23)**
   https://www.cisecurity.org/insights/blog/top-10-malware-q1-2025
2. **SocGholish**
   https://redcanary.com/threat-detection-report/threats/socgholish/
3. **Threat hunting case study: SocGholish (2025/02/13)**
   https://intel471.com/blog/threat-hunting-case-study-socgholish
4. **SocGholish: From loader and C2 activity to RansomHub deployment(2025/05/01)**
   https://www.darktrace.com/blog/socgholish-from-loader-and-c2-activity-to-ransomhub-deployment
5. **SocGholish’ s Intrusion Techniques Facilitate Distribution of RansomHub Ransomware (2025/03/14)**
   https://www.trendmicro.com/en_us/research/25/c/socgholishs-intrusion-techniques-facilitate-distribution-of-rans.html
6. **Cybersecurity Stop of the Month: Detecting and Analyzing a SocGholish Attack**
   https://www.proofpoint.com/us/blog/email-and-cloud-threats/detecting-analyzing-socgholish-attack