針對台灣攻擊的新後門採用隱匿的通訊方式

2024 年 8 月 20 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

前所未見的後門軟體利用 DNS 流量與命令與控制伺服器通訊

在針對台灣一所大學的攻擊中，利用一種不常見的技術，部署一個先前未見的後門 (Backdoor.Msupedge) 。

此後門最顯著的特點是透過 DNS 流量與命令與控制 (C&C) 伺服器通訊。儘管這種技術已廣為人知，並曾被多個威脅份子使用，但卻並不常見。

Msupedge 分析

Msupedge 是個動態連結程式庫 (DLL) 形式的後門軟體。已發現它安裝在下列檔案路徑中：

- csidl_drive_fixed\xampp\wuplog.dll
- csidl_system\wbem\wmiclnt.dll

wuplog.dll 由 Apache (httpd.exe) 載入，而 wmiclnt.dll 的父處理程序則未知。

Msupedge 使用 DNS 隧道 (tunneling) 與 C&C 伺服器通訊。DNS 隧道工具的程式碼基於公開的 dnscat2 工具。它透過執行名稱解析來接收指令。解析的主機名稱結構如下：

Figure 1. 用於初始名稱解析的主機名稱。

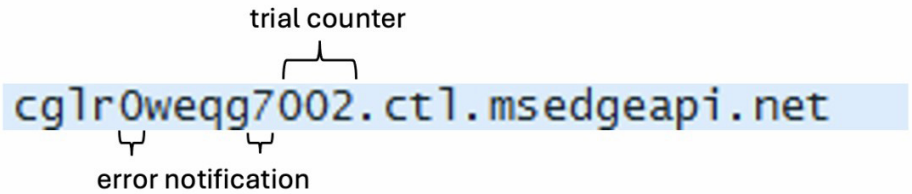

Figure 2.傳送電腦名稱後使用的主機名稱。

錯誤通知包括下列事項的成功或失敗：

- 記憶體分配
- 已接收指令的解壓縮
- 執行接收到的指令

後門似乎也會將指令執行的結果編碼為第五層網域並傳送。

Msupedge 不僅透過 DNS 流量接收指令，也使用 C&C 伺服器 (ctl.msedeapi[.]net) 解析的 IP 位元址作為指令。已解析 IP 位址第三個八位元組做為切換情況。後門的行為會根據解析 IP 位址的第三個八位字元減七的值而改變。例如：如果第三個八位字元是 145，則會轉換為 138(以十六進位表示為 0x8a)。

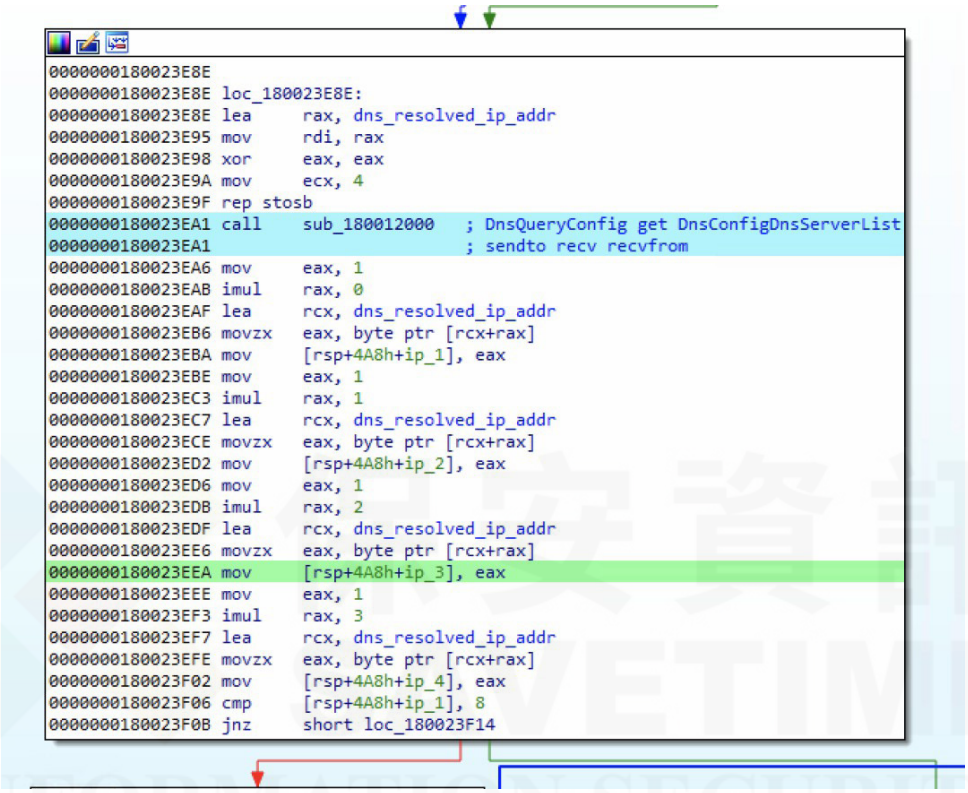

Figure 3. 擷取已解析的 IP 位址。

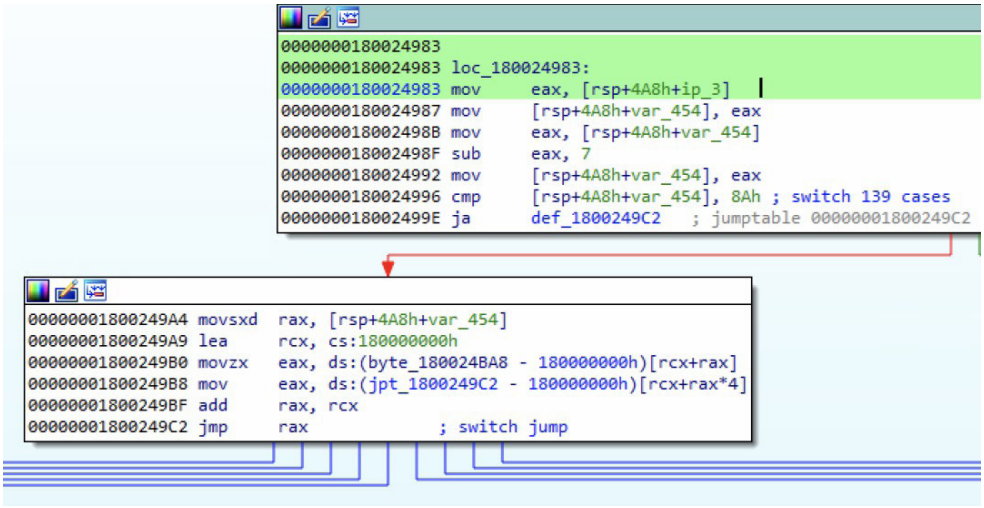

Figure 4.後門的行為會根據解析 IP 位址第三個八位元組減七的值而改變。

Msupedge 支援下列指令：

- **Case 0x8a**：建立程序。指令透過 DNS TXT 記錄接收。
- **Case 0x75**：下載檔案。透過 DNS TXT 記錄接收下載的 URL。

- **Case 0x24**：休眠 (ip_4 * 86400 * 1000 ms)。
- **Case 0x66**：休眠 (ip_4 * 3600 * 1000 ms)。
- **Case 0x38**：建立 %temp%\1e5bf625-1678-zzcv-90b1-199aa47c345.tmp 檔案，此檔案的用途不明。
- **Case 0x3c**：刪除 %temp%\1e5bf625-1678-zzcv-90b1-199aa47c345.tmp 檔案。

感染媒介

最初的入侵可能是透過利用最近修補的 PHP 漏洞 (CVE-2024-4577)。該漏洞是一個 CGI 參數注入漏洞，會影響安裝在 Windows 作業系統上的所有 PHP 版本。成功利用此漏洞可導致遠端執行程式碼。

賽門鐵克在最近幾週發現有多個威脅者正在掃描易受攻擊的系統。到目前為止，我們尚未發現任何證據可讓我們歸責於此威脅，而攻擊背後的動機仍然不明。

防護方案／緩解措施

有關 Alpha 最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

入侵指標 (Indicators of Compromise)

如果 IOC 是惡意的並且我們能夠使用該檔案，Symantec Endpoint 產品將檢測並阻止該檔案。

e08dc1c3987d17451a3e86c04ed322a9424582e2f2cb6352c892b7e0645eda43 – Backdoor.Msupedge

f5937d38353ed431dc8a5eb32c119ab575114a10c24567f0c864cb2ef47f9f36 – Backdoor.Msupedge

a89ebe7d1af3513d146a831b6fa4a465c8edeafea5d7980eb5448a94a4e34480 – Web shell

關於作者

威脅獵手團隊

賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/threat-intelligence/taiwan-malware-dns
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2024/8

更多資訊 請造訪我們的網站 **http://www.SaveTime.com.tw**
(好記：幫您節省時間.的公司.在台灣)

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的好用資源。

保安資訊連絡電話：**0800-381-500**。