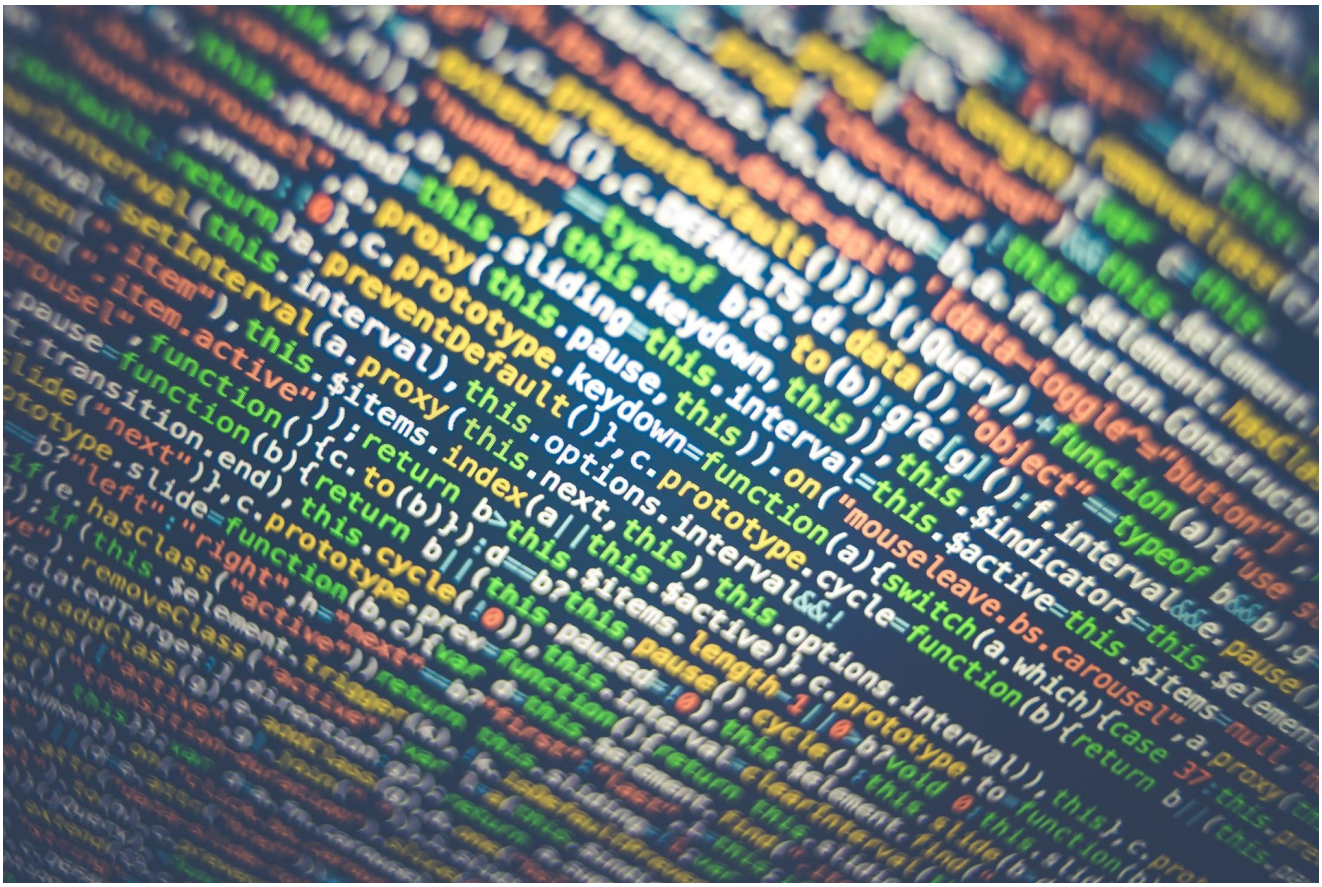
調查局 08/19 公布中國對台灣政府機關駭侵事件說明

teamt5.org/tw/posts/mjib-holds-briefing-on-chinese-hackers-attacks-on-taiwanese-government-agencies/

Global Support & Service



8.22.2020Global Support & Service

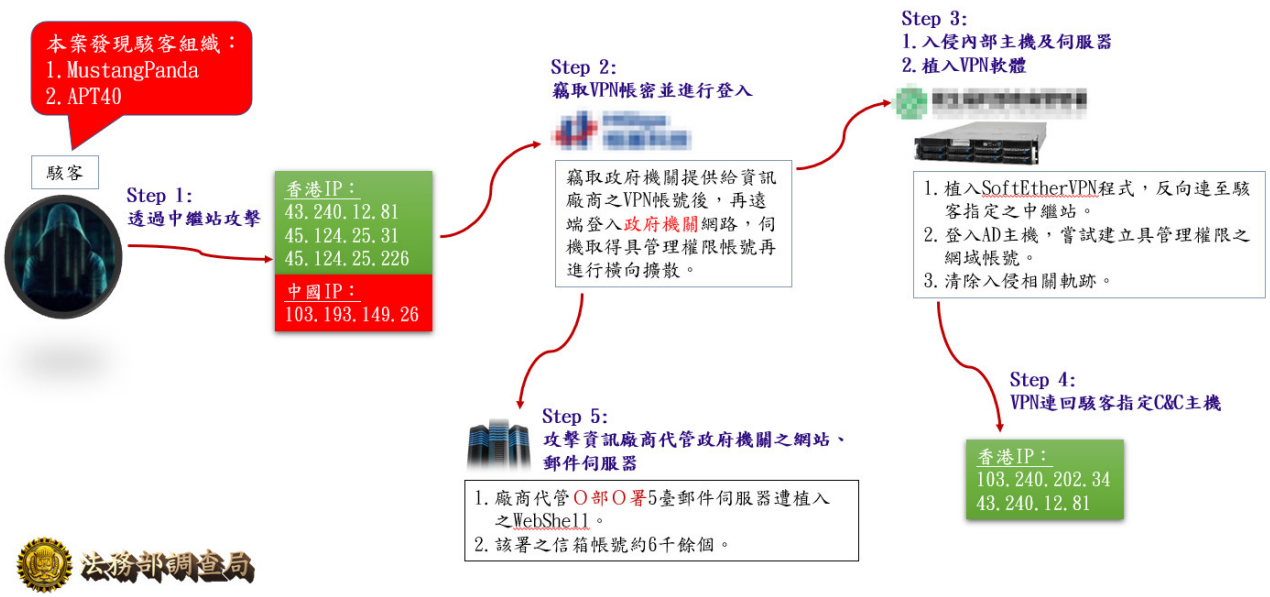
Share:

前言

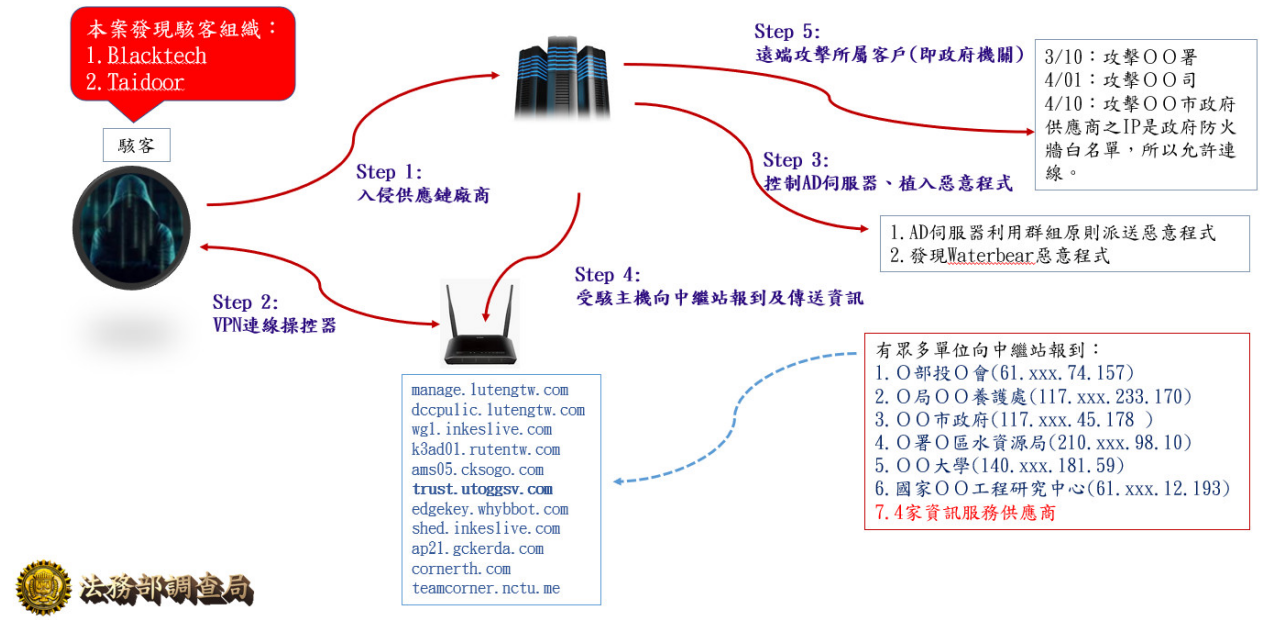
法務部調查局綜整近期所偵辦的數起台灣政府機關遭駭案件，於 19 日發表記者會，提到政府部門的委外資訊服務供應商遭中國駭客組織攻擊現況，目前已知有市政府、水資源局等至少 10 個單位，以及 4 家資訊服務供應商遇害。

調查局資安工作站也發現，駭客在入侵政府機關內部的主機與伺服器後，為了要長期潛伏以及將獲取資料傳出，還會安裝 SoftEther VPN 程式，以連線到駭客指定的中繼站。

本次調查局公布的攻擊族群：MustangPanda、APT40、Blacktech 與 Taidoor，皆是 TeamT5 長期追蹤的標的，我們有信心能夠偵測這些族群使用的後門程式、駭客工具以及攻擊手法。



圖一、駭客透過供應鏈攻擊我政府機關 -1（圖片來源：法務部調查局）



圖二、駭客透過供應鏈攻擊我政府機關 -2（圖片來源：法務部調查局）

IOC 情資

TeamT5 長期進行駭客追蹤研究，根據法務部調查局所提供的情資內容，關聯出駭客族群慣用的惡意程式與相關 IOC 情資供使用者匯入至閘道端或端點防護設備比對使用，詳細惡意程式說明與 IOC 清單如下所示。

惡意程式家族	類型	描述	攻擊族群	首次出現
dbgPrint	RAT	dbgPrint 為中國駭客族群 HUAPI 慣用的後門程式，其名稱來自於該後門程式早期版本的字串(strings)內容。dbgPrint 後門程式通常由 PE 型態的 Loader、插入 shellcode 的 DLL 檔及惡意 Payload 所組成。同時也具備防毒免殺(anti-antivirus)的功能模組。	HUAPI (又稱為 Plead 或 Blacktech)	2009 年
CobaltStrike Beacon	RAT	Cobalt Strike 是一款滲透測試或紅隊演練常使用的攻擊框架，而 CobaltStrike Beacon 則是從 Cobalt Strike 攻擊框架所產生的惡意 Payload。雖然 Cobalt Strike 為商業付費工具，但是經過破解並流傳於許多論壇或網站中，因此有許多駭客皆透過他進行惡意攻擊。	商業付費工具，無法明確定義出背後的攻擊族群	2016 年

表一、惡意程式分析說明

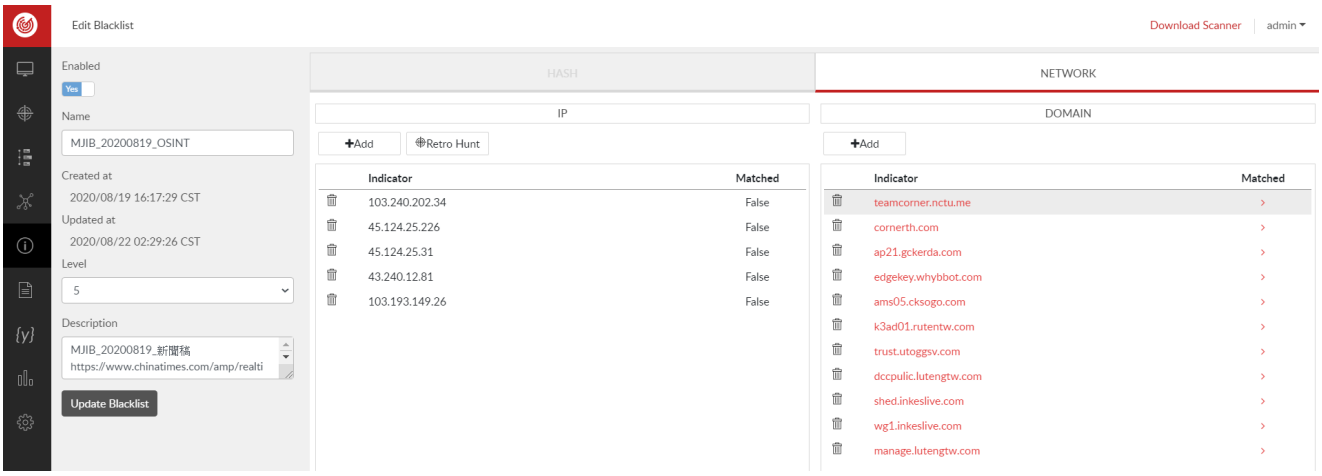
IOC	類型	提供來源
manage.lutengtw.com	Domain	法務部調查局
dccpulic.lutengtw.com	Domain	法務部調查局
trust.utoggsv.com	Domain	法務部調查局
wg1.inkeslive.com	Domain	法務部調查局
k3ad01.rutentw.com	Domain	法務部調查局
ams05.csksogo.com	Domain	法務部調查局
edgekey.whybbot.com	Domain	法務部調查局
shed.inkeslive.com	Domain	法務部調查局
ap21.gckerda.com	Domain	法務部調查局
cornerth.com	Domain	法務部調查局
teamcorner.nctu.me	Domain	法務部調查局
43.240.12.81	IP Address	法務部調查局

IOC	類型	提供來源
45.124.25.31	IP Address	法務部調查局
45.124.25.226	IP Address	法務部調查局
103.193.149.26	IP Address	法務部調查局
103.240.202.34	IP Address	法務部調查局
a8373a143a915518a33c4af19fff01e7	MD5 Hash	TeamT5
20714b487b5b63ff8e52b911d19d6da1	MD5 Hash	TeamT5
6c490c833bfff677c89d9bb81bef0cf5	MD5 Hash	TeamT5
d395580fea6fb840798dc1ee65756484	MD5 Hash	TeamT5
4a1941df8b251716f66e2777425ac0e5	MD5 Hash	TeamT5
c11f40af68c07b309bd103d69b7bb14a	MD5 Hash	TeamT5
387fe30ffc270939c299d1eaebcdcd4d	MD5 Hash	TeamT5
93bfdce35e3ab86508e09deedca6552f	MD5 Hash	TeamT5
1857fbce5c5269a1d4e40204ccccd7d1	MD5 Hash	TeamT5
www.kaspersky-security.net	Domain	TeamT5
www.symantec-endpoint.net	Domain	TeamT5
www.symantec-product.com	Domain	TeamT5
update.symantec-product.com	Domain	TeamT5
update.trendmicro-service.com	Domain	TeamT5
googleupdatesrv.com	Domain	TeamT5
103.234.96.213	IP Address	TeamT5
103.242.0.152	IP Address	TeamT5
43.240.12.80	IP Address	TeamT5
43.240.12.82	IP Address	TeamT5
43.240.12.83	IP Address	TeamT5
45.32.43.59	IP Address	TeamT5

IOC	類型	提供來源
45.76.189.109	IP Address	TeamT5

表二、IOC 清單

ThreatSonar 惡意威脅鑑識分析平臺的用戶，可將上方表二之 IOC 匯入以強化威脅偵測與識別，亦可追溯比對過去資料是否命中 IOC。示意圖如下。

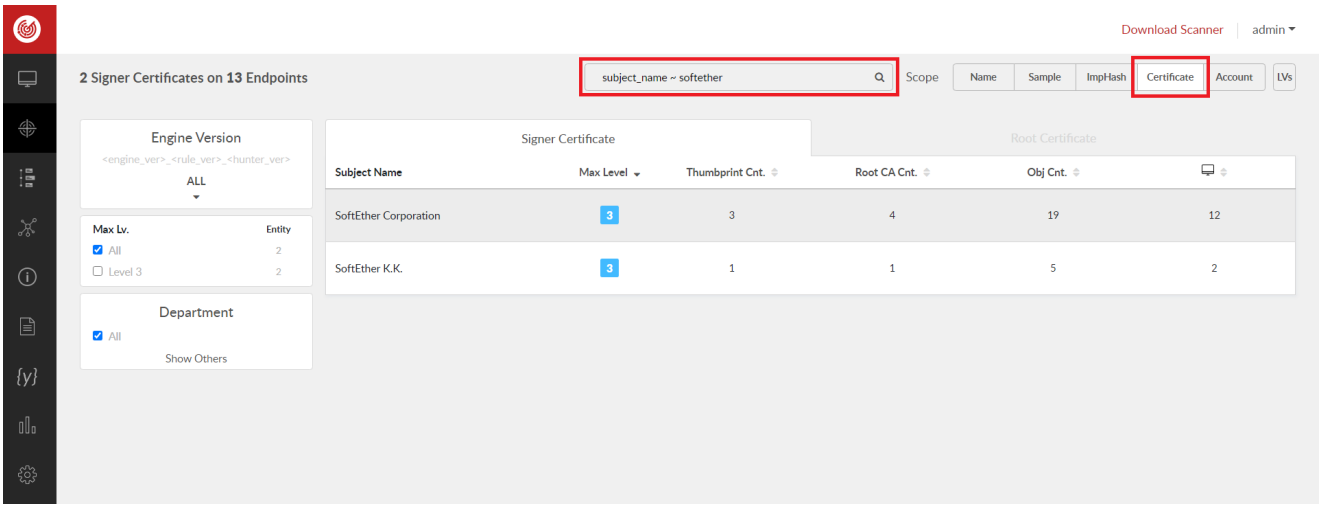


圖三、ThreatSonar 支援 Hash、IP 及 Domain IOC 情資匯入

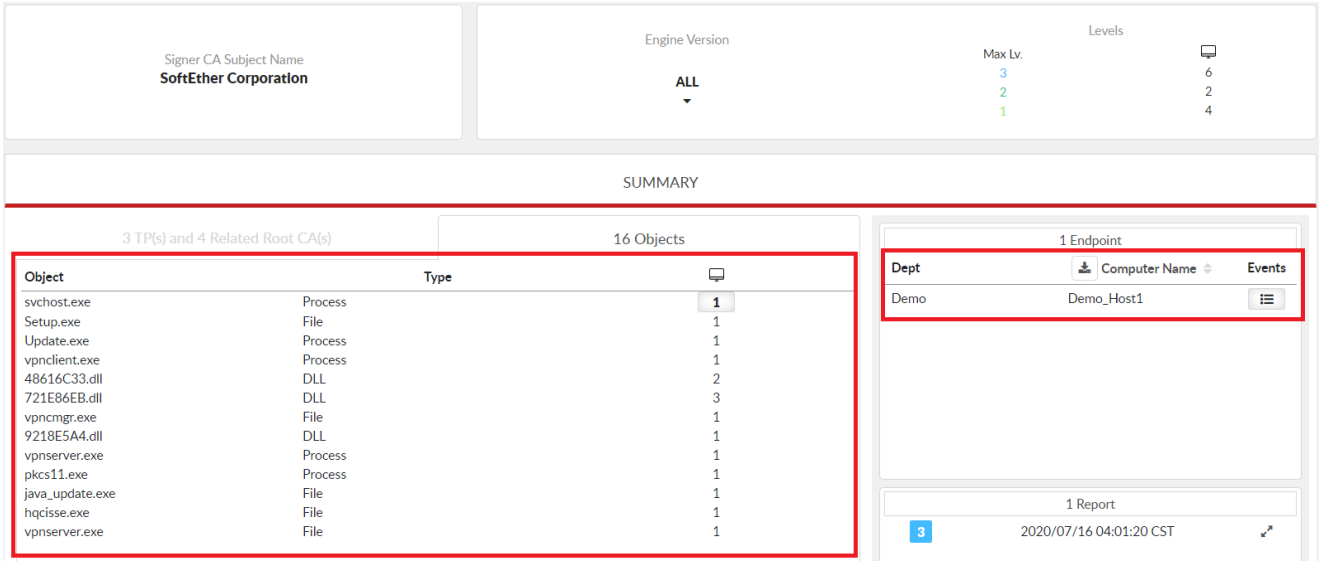
如何透過威脅狩獵找出 SoftEther VPN 程式

根據法務部調查局的偵辦結果，駭客為了長期潛伏於受害環境，因此會透過 SoftEther 這類的合法 VPN 程式進行遠端控制。ThreatSonar 具備主動威脅狩獵（Threat Hunting）功能，故可以快速地在環境中找出 SoftEther VPN 程式。

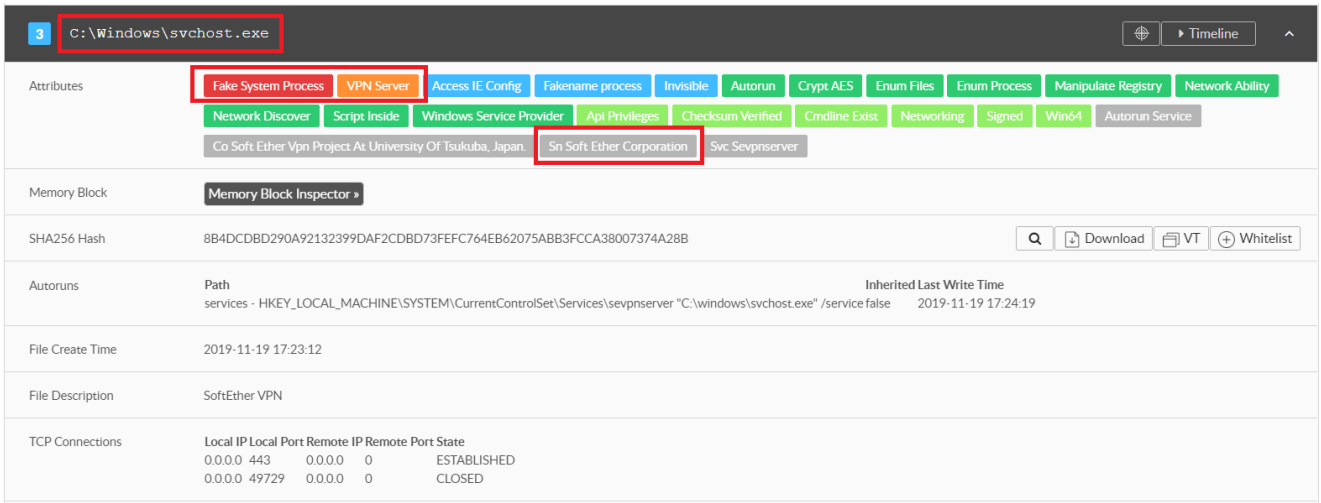
其步驟為在威脅狩獵（Hunter）功能中，切換 Scope 至憑證（Certificate），搜尋 "filename ~ softether"（請選擇 Engine Version 為全選），可依憑證內容搜尋環境內符合條件的 SoftEther 憑證及其對應的端點與程式清單。其流程步驟示意圖如下。



圖四、以 filename 查詢符合條件的 SoftEther 憑證



圖五、具備 SoftEther 憑證的端點與程式清單



圖六、駭客將 SoftEther VPN 程式偽裝成 svchost.exe

*圖片來源：Unsplash

Share: