中國威脅者：Grayfly(*灰色蒼蠅)使用新發現的 Sidewalk(*人行道)惡意軟體

2021 年 9 月 9 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

最近對 Exchange 和 MySQL 伺服主機的攻擊。駭客攻擊集團重點鎖定電信產業。

賽門鐵克是博通的企業安全部門，已將最近發現的 Sidewalk 後門與與中國有關聯的 Grayfly (*灰色蒼蠅)間諜集團聯繫起來。該惡意軟體與較舊的 Crosswalk 後門 (Backdoor.Motnug) 相關，已在最近針對台灣、越南、美國和墨西哥的許多組織發動的 Grayfly 攻擊活動中部署。

近期攻擊活動的一個特點是，大量目標都在電信部門。該組織還攻擊了 IT、媒體和金融行業。ESET 最近記錄了 Sidewalk，將其歸咎於一個名為 SparklingGoblin 的新集團，該組織與 Winnti 惡意軟體家族有關。賽門鐵克的威脅獵手團隊將 Sidewalk 歸咎於中國長期從事間諜活動的 Grayfly。該組織的成員於 2020 年在美國被起訴。最近又增多的 Sidewalk 活動顯示，Grayfly 並未被沸沸揚揚的司法起訴風波影響而有所收斂。

認識 Garyfly 駭客集團

Grayfly (又名 GREF 和 Wicked Panda) 是一個針對性的駭客攻擊集團，2017 年 3 月至今，一直活躍，使用稱為 Backdoor.Motnug (又名 TOMMYGUN/CROSSWALK)的自定義後門，以及稱為 Trojan.Chattak、Cobalt Strike 的自定義載入工具 (又稱 Trojan.Agentemis) 及其攻擊中的輔助工具。

據觀察，Grayfly 的目標是亞洲、歐洲和北美的多個國家／地區，涉及多個行業，包括食品、金融、醫療保健、餐旅、製造和電信。在最近的活動中，Grayfly 繼續專注於電信，但也觀察到針對在媒體、金融和 IT 服務提供商領域運營的組織。通常，Grayfly 的目標是面向公眾的 Web 伺服主機安裝 Web shell 以進行初始入侵，然後在網路內進一步傳播。

一旦網路遭到入侵，Grayfly 可能會將其自定義後門安裝到其他系統上。這些工具允許攻擊者全面遠端存取網路和代理連線，從而允許他們存取目標網路中難以到達的部分。

儘管有時標記為 APT41，但我們認為 Grayfly 是 APT41 旗下的間諜部門。同樣，賽門鐵克單獨跟踪 APT41 的其他分支，例如：其網路犯罪部門--Blackfly。

Sidewalk(* 人行道) 攻擊活動

最近的攻擊活動的一個特點是該組織似乎對暴險程度較高的 Microsoft Exchange 或 MySQL 伺

服主機特別感興趣。這顯示初始攻擊媒介可能是針對提供面向公眾服務的伺服主機的多個漏洞的利用。

在至少一次攻擊中，可疑的 Exchange 活動被發現是在利用PowerShell 命令安裝了一個身份不明的網頁殼層 (Web Shell)。在此之後，惡意後門被執行。

安裝後門後，攻擊者部署了自定義版本的憑證傾倒 (credential dumping) 工具--Mimikatz。此版本的 Mimikatz 以前曾在 Grayfly 攻擊中使用過。

受害者案例研究

攻擊者活動的第一個跡像是在當地時間 20:39 發現的，其中 Base64 編碼的 PowerShell 命令是通過合法的 Exchange Server 相關程序執行的。該命令用於執行 certutil 以解碼和安裝網頁殼層 (Web Shell)：

```
>(^_certutil -decode -f C:\Windows\Temp\ImportContactList_-.aspx
C:\Windows\Temp\ImportContactList.aspx;if((dir C:\Windows\Temp\ImportContactList.aspx).
Length -eq 212){Remove-Item -Force C:\Windows\Temp\ImportContactList_*-*.aspx}*
```

接下來，另一個 Base64 編碼的 PowerShell 命令被執行。此命令用於將網頁殼層(Web Shell)移動到攻擊者可存取的 Exchange 安裝路徑--特別是 ClientAccess\ecp 目錄。

- mv C:\Windows\Temp\ImportContactList.aspx $envExchangeInstallPath\ClientAccess\esp\ -Force

幾分鐘後，利用 installutil.exe 執行了一個後門：

- CSIDL_WINDOWS\microsoft.net\framework64\v4.0.30319\installutil.exe /logfile= /LogToConsole=false /ParentProc=none /U CSIDL_WINDOWS\microsoft.net\framework64\v4.0.30319\microsoft.webapi.config

大約一個小時後，觀察到攻擊者執行 WMIC 命令以運行 Windows 批次檔。此批次檔用於創建計劃任務以執行後門並確保讓駭客可常駐在環境裡：

- WMIC /NODE:"172.16.140.234" process call create "cmd.exe /c c:\users\public\schtask.bat"

此後不久，執行 Mimikatz 以傾倒憑證(dump credentials)：

- sha2:b3eb783b017da32e33d19670b39eae0b11de8e983891dd4feb873d6e9333608d (Mimikatz) - csidl_system_drive\perflogs\ulsassx64.exe

此後，沒有觀察到進一步的活動。

起訴書

三名中國男子於 2020 年在美國因參與涉及 Grayfly 工具和戰術的攻擊而被起訴。起訴時，蔣

立志、錢川和傅強（均為音譯）在中國成都，在一家名為成都 404 的公司擔任高階職務的職位。該公司自稱是網路安全專家，並聲稱聘任了一個精良的白帽駭客團隊可以執行滲透測試以及其他安全營運。

起訴書指控這些人參與對美國、南國、日本、印度、台灣、香港、馬來西亞、越南、印度、巴基斯坦、澳大利亞、英國、智利、印尼、新加坡、和泰國等國共超過 100 次以上的網路攻擊。據說蔣與中國國家安全部有「合作關係」，這也將為他和他的同夥提供一定程度的國家級保護。

可能延續其強大趨勢

Grayfly 是一位有能力的參與者，可能會繼續對亞洲和歐洲各行各業的組織構成風險，包括電信、金融和媒體。該組織很可能會繼續開發和改進其自定義工具，以增強規避策略，同時使用諸如公開可用的漏洞利用和 web shell 之類的商品工具來協助他們的攻擊。

保護／緩解

有關最新的防護更新，請訪問賽門鐵克防護公告。

感染指標

SHA256	說明	偵測
1b5b37790b2029902d2d6db2da20da4d0d7846b20e32434f01b2d384eba0eded	Sidewalk loader	Trojan.Gen.MBT
b732bba813c06c1c92975b34eda400a84b5cc54a460eeca309dfecbe9b559bd4	Sidewalk loader	Trojan.Gen.MBT
04f6fc49da69838f5b511d8f996dc409a53249099bd71b3c897b98ad97fd867c	Sidewalk loader	Trojan.Gen.MBT
25a7c1f94822dc61211de253ff0a5805a0eb83921126732a0d52b1f1967cf079	Sidewalk loader	Trojan Horse
b3eb783b017da32e33d19670b39eae0b11de8e983891dd4feb873d6e9333608d	Mimikatz	Hacktool.Mimikatz

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayfly-china-sidewalk-malware
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。2021/09

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。

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)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588