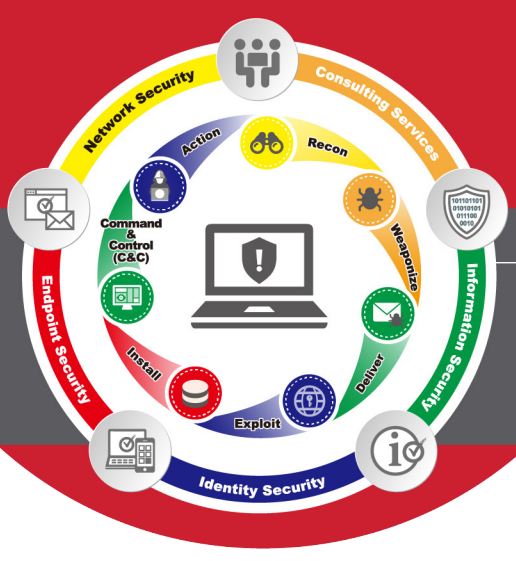


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

賽門鐵克 EDR 如何有效防護
Impacket 遭濫用且扶搖直上的危害

2024 年 8 月 13 日發布

Impacket 網路滲透測試工具

近來有多種工具可用於網路滲透測試。Impacket 是炙手可熱且功能強大的工具套件組合 (包)，已在駭客圈獲得極高知名度，它是採用 Python 撰寫，可說是專為操控網路封包所寫的開放原始碼大集合，可讓開發人員製作和解碼網路封包。它支援 IP、UDP、TCP、SMB、MSRPC 及其他數種網路通訊協定。Impacket 深受合法滲透測試者的歡迎，但也逐漸受到網路罪犯的青睞。

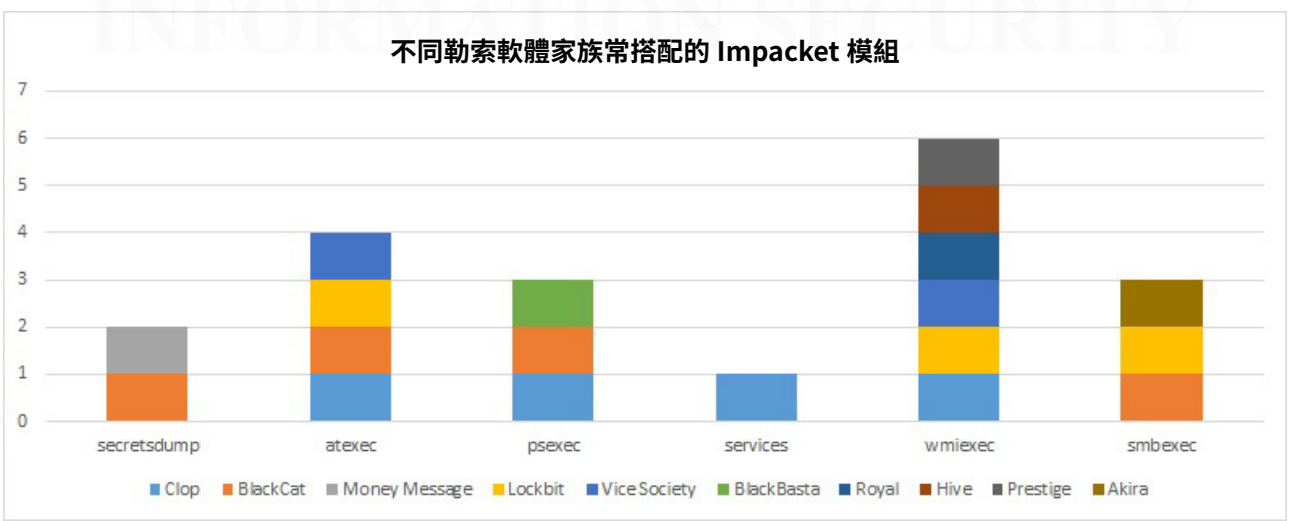
Impacket 的主要特色

- 支援最多樣的通訊協定
- 易於操控通訊協定
- 操控 SMB 檔案存取儲存協定和 NTLM 安全協議
- 操控微軟遠端程序呼叫 (MSRPC) 通訊協定
- 密碼攻擊與破解

一個令人不安的趨勢是，威脅份子似乎越來越依賴 Impacket 來進行橫向移動和遠端執行，特別是觀察到勒索軟體威脅分子濫用 Impacket。

以下是勒索軟體最常使用的模組及其使用方法。

不同勒索軟體家族常搭配的 Impacket 模組



Impacket 用於遠端執行的常見模組

- **atexec**：此模組被用於工作排程服務在遠端機器上執行指令
  - 命令列：
    - cmd.exe /C systeminfo > CSIDL_WINDOWS\temp\<random>.tmp 2>&1
    - cmd.exe /C powershell -ep bypass -f CSIDL_WINDOWS\temp\<random>.ps1 > CSIDL_WINDOWS\temp\<random>.tmp 2>&1
- **psexec**：這個模組提供 psexec 功能在遠端機器上執行有效酬載
  - 方法：
    - 在遠端機器上寫 beakon 到 ADMIN$ 路徑
    - 建立隨機服務："HKLM\SYSTEM\CurrentControlSet\Services\<random_name>"
- **services**：此模組在遠端機器上建立服務
  - 方法：
    - services.exe 建立服務機碼 "HKLM/SYSTEM/CurrentControlSet/Services/<random_name>"
- **wmiexec**：這個模組提供 WMI 功能來提供反向 shell
  - 命令列：
    - CSIDL_SYSTEM\wbem\wmic.exe /node:%cn% process call create CSIDL_SYSTEM_DRIVE\temp\<random>.bat
- **smbexec**：這個模組提供反向 shell
  - 命令列
    - CSIDL_SYSTEM\cmd.exe /Q /c echo cd ^> \<6,47856BB5>\C$__output 2^>^&1 > CSIDL_WINDOWS\<random>.bat & del CSIDL_WINDOWS\<random>.bat

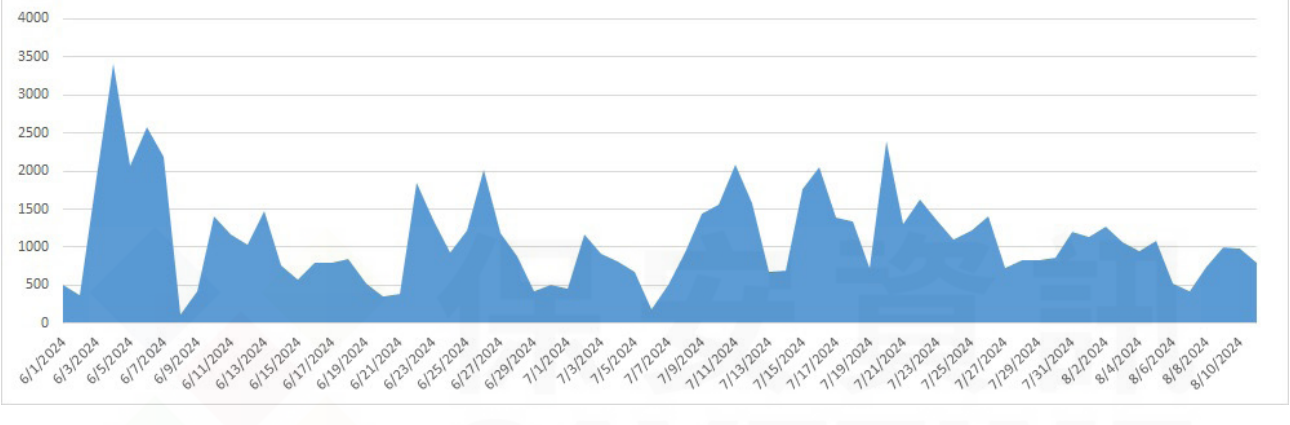
Impacket 用於憑證盜用的常見模組

- **secretsdump**：此模組用於轉存遠端機器的憑證
  - 命令列：
    - CSIDL_SYSTEM\svchost.exe -k localService -p -s RemoteRegistry
    - esentutl.exe /y "CSIDL_PROFILE\dragos\appdata\local\google\chrome\user data\default\login data" /d "CSIDL_PROFILE\dragos\appdata\local\google\chrome\user data\default\login data.tmp"。

EDR(端點偵測與回應)事件建立

賽門鐵克端點偵測與回應 (EDR：Symantec Endpoint Detection and Response) 使用機器學習和行為分析來偵測和揭露可疑的網路活動。EDR 會針對潛在的有害活動發出警示，排定事件的優先順序以進行快速分流 (類似災難現場的檢傷分類)，並允許事件回應人員瀏覽裝置活動記錄，以便對潛在攻擊進行鑑識分析。

賽門鐵克端點偵測與回應 (EDR) 有效應對不同類型的 Impacket 攻擊



威脅獵捕查詢

賽門鐵克 EDR 客戶可在以下連結找到威脅獵捕查詢。

- https://github.com/Symantec/threathunters/tree/main/ImPacket

欲瞭解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

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**。