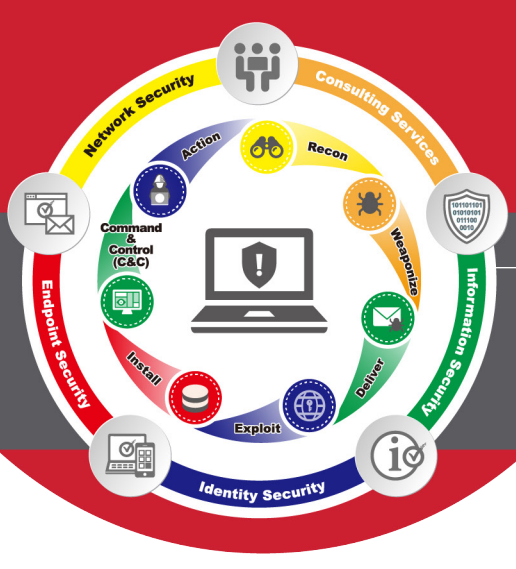


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

憑證轉存(Credential Dumping)的危害--有效滲入企業網路和促進橫向移動的入口

2025 年 4 月 22 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

取得目標組織的憑證是攻擊者為了達成各種目的的首要目標。這是攻擊初始階段之一，作為滲入企業網路和促進橫向移動的入口。憑證可從各種來源取得，包括作業系統和第三方工具。多個地下論壇會向駭客組織提供／兜售憑證，有些行動者會使用新穎的方法來取得這些憑證。遭竊取的憑證通常以雜湊 (hash) 或明文傳輸密碼的形式存在。

攻擊者使用作業系統憑證轉存手法

取得帳戶登入資訊和憑證，對於攻擊者的攻擊活動至關重要，因為這可讓他們

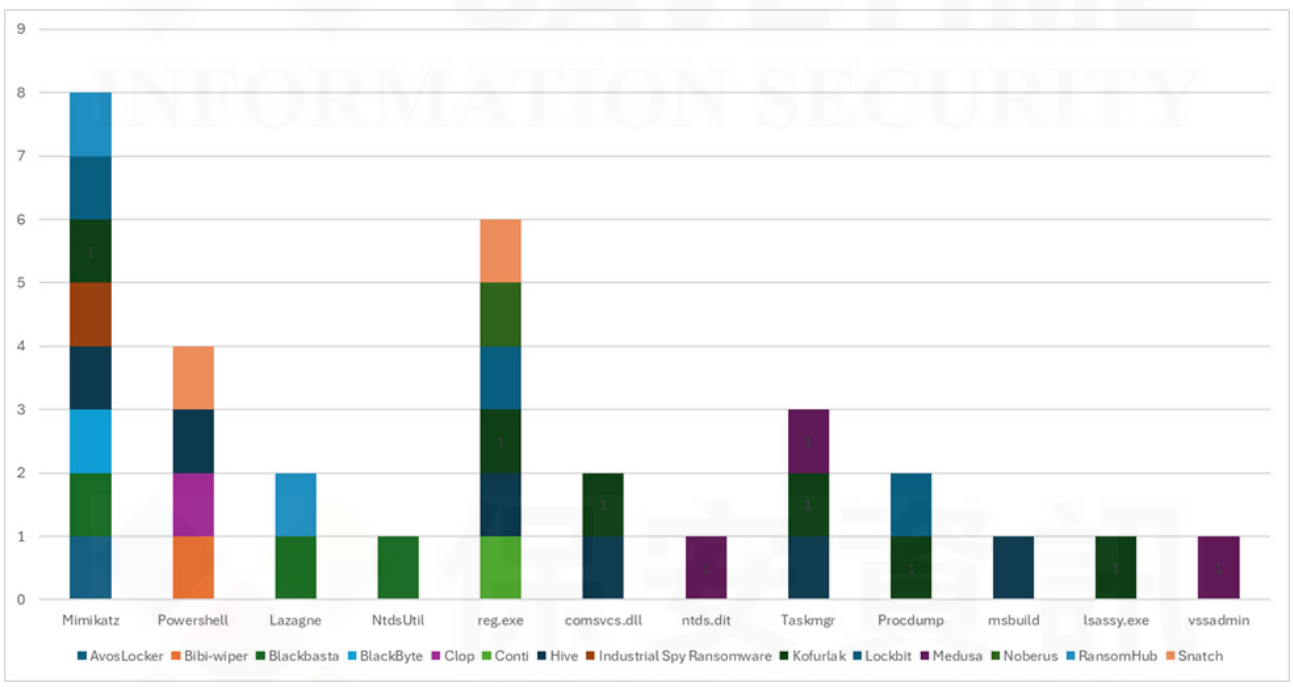
- 存取受限制的資訊、網路資源和重要資產
- 以新的權限存取網路內的其他系統和服務
- 建立新帳號並將其刪除，滅跡以阻礙鑑識分析
- 透過密碼模式和政策收集其他憑證

在 Windows 作業系統中，憑證會儲存在數個地方：

- 安全帳戶管理員(SAM)資料庫
  - Windows Security Accounts Manager(SAM)：是 Windows 用來管理本地用戶帳戶的組件之一。SAM 是一個資料庫檔案，包含以分散式格式儲存的使用者名稱和密碼。
- Windows 本地安全認證子系統服務 (LSASS) 記憶體
  - Local Security Authority Subsystem Service：LSASS 是一個 Windows 程序，負責驗證使用者登入並執行安全政策。當使用者登入時，LSASS 程序會從 SAM 資料庫擷取使用者的憑證，並在會話期間將其儲存在記憶體中。
- NTDS.dit
  - 這是 Microsoft's Active Directory Domain Services 網域服務 (AD DS) 中的主要資料庫檔案。此檔案包含重要的網域資訊，包括使用者的密碼雜湊值。
- Local Security Authority (LSA)本地安全授權隱私
  - LSA 隱私儲存在 HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets 的註冊表中，其中可能包含各種不同的憑證資料。
- 暫存的網域憑證
  - 在網域控制器不可用的情況下，通常儲存在 LSASS 記憶體中的快取網域憑證可用來驗證使用者。
- 憑證管理員
  - Windows Credentials Manager 是一個 Windows 程式，用來儲存認證憑證--主要是網頁和裝置憑證。
- 群組政策(Group Policy)
  - 群組政策允許集中管理 Active Directory (AD) 中的使用者和電腦設定。

常用的憑證轉存工具的使用情境

駭客集團常用的憑證轉存的技術



熱門趨勢

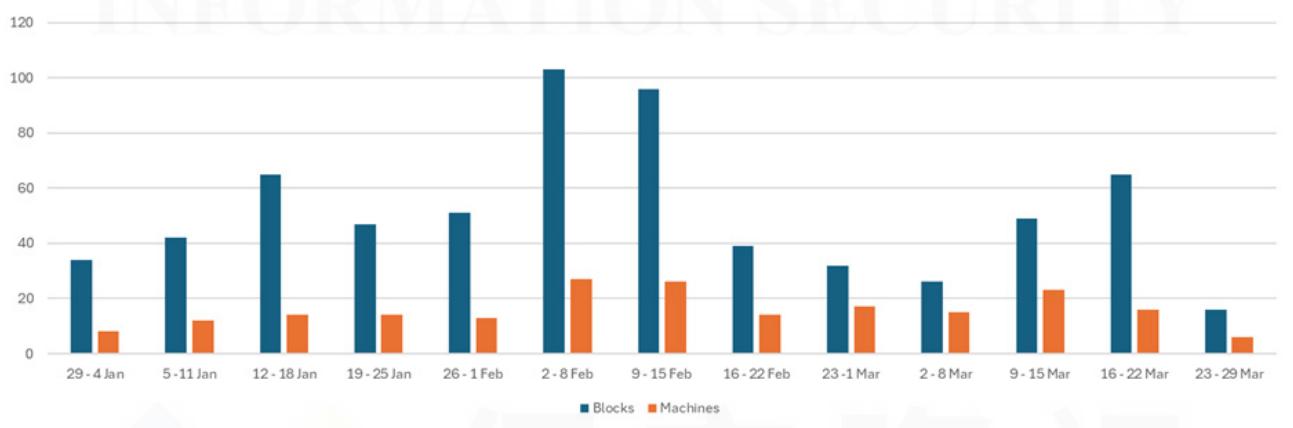
- Mimikatz 是一種開放原始碼的憑證轉存工具，常被駭客利用。最常見 Mimikatz 執行方法包括
  - mimikatz.exe "privilege::debug" "sekurlsa::pth /user: /domain:MEB /ntlm:"
  - mimikatz64.exe "privilege::debug" "log.txt" "sekurlsa::minidump lsass.dmp" "sekurlsa::logonPasswords full"
  - imfa.exe kerberoast /domain:corpmty.ccontrol /outfile:CSIDL_SYSTEM_DRIVE\temp\temp.txt /format:hashcat
- 使用 reg.exe 從 Windows 註冊表轉儲 hive 檔案。這些檔案包含敏感資訊，例如：散列憑證，攻擊者可能會利用這些資訊進行橫向移動。
  - reg save HKLM\SAM sam.hiv
  - reg save HKLM\SYSTEM SYSTEM.hiv
  - reg save HKLM\SECURITY security.hiv
- LaZagne 是一個用於攻擊鏈的入階後階段的開放原始碼工具，用來擷取大量儲存在系統中的密碼。
  - lazagne.exe all > lazagne.txt
- Comsvcs.dll 是合法的 Windows dll，據觀察，駭客會濫用它來轉存程序記憶體，尤其是 LSASS，試圖擷取憑證。
  - rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump <process id> lsass.dmp full
- 使用 Ntdsutil.exe 擷取 Active Directory 資料庫 - NTDS.dit，通常用於離線密碼破解。
  - ntdsutil.exe "ac i ntds" ifm "create full c:\zemp" q q
- Procdump 是一個合法的 Sysinternals 工具，用來產生程序轉存以進行故障排除，但它可能會被駭客用於惡意目的，例如：擷取憑證資料。
  - procdump64.exe" -accepteula -ma <pid> out.dmp
- 使用磁碟區陰影複製 (vssadmin) 從 NTDS 存取憑證資訊。
  - vssadmin create shadow /for=c：

端點偵測與回應(EDR)自動偵測網路中的可疑活動

賽門鐵克端點偵測與回應 (Symantec Endpoint Detection and Response：EDR) 使用機器學習和行為分析來偵測及暴露可疑的活動。EDR 提醒您有關可能有害的活動、排定資安事端的優先順序以便快速分類，並讓您在您的潛在攻擊蒐證分析期間導覽裝置活動記錄。以便對潛在攻擊進行鑑識分析。

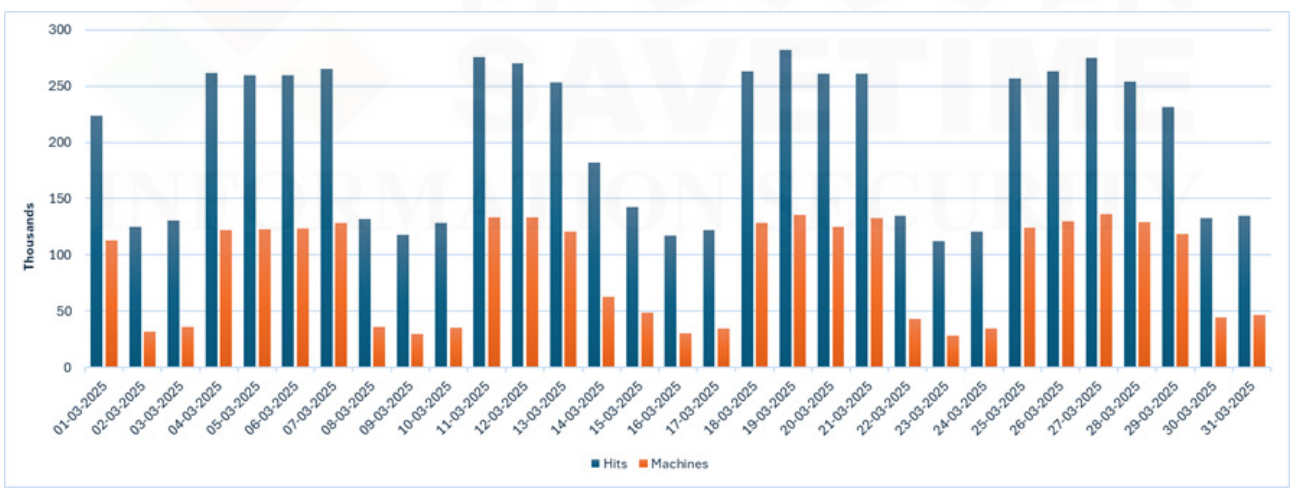
提供憑證轉存的保護

賽門鐵克 EDR 攔截憑證轉存嘗試的成效



EDR 提供憑證轉存嘗試的可視性

EDR 結合 MITRE 事件充實更新 (MITRE event enrichment updates) 提供憑證轉存嘗試的可視性



要了解更高階等級的安全防護以及端點資安持續監控與異常反應系統(EDR):Symantec Endpoint Detection & Response，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求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。