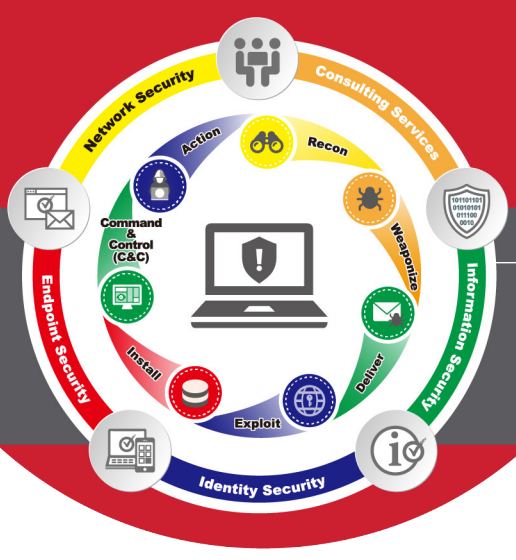


Telegram和Discord遭濫用於網路攻擊的情況越來越嚴重～安啦！賽門鐵克的用戶

2025 年 2 月 11 日發布

Telegram 和 Discord 遭濫用於網路攻擊的情況越來越嚴重

2024 年，網路罪犯越來越喜歡濫用 Telegram 和 Discord 等合法通訊平台進行資料外洩和其他非法活動。它們擁有廣大的用戶和內建豐富的功能，使其成為吸引未經授權資料傳輸的工具。迄今為止，我們已發佈 184 份與 Telegram 相關的防護公告，以及 121 份與 Discord 相關的防護公告。

在 Telegram 情境裡，威脅份子利用 Bot API 自動從受遭入侵的系統滲出資料。該平台如果遭濫用也會成為散佈惡意軟體的幫兇，目標是敏感的使用者資訊，例如：瀏覽器資料和加密貨幣錢包。此外，Telegram 成為非法市場的重要平台，有專門銷售駭客資料、惡意軟體和非法商品的頻道。聊備一格的內容審查機制和使用者的匿名性更推波助長此一趨勢。網路罪犯也使用 Telegram 進行命令與控制 (C&C) 通訊和通知。

無獨有偶，Discord 的 webhooks 也遭濫用來進行資料外洩，讓網路罪犯可以無縫傳輸所竊取的資訊。其內容傳送網路被濫用來儲存及散佈惡意軟體，將惡意軟體散佈到毫無戒心的使用者身上。和 Telegram 一樣，Discord 也是 C&C 通訊的平台。

背後有多種因素

有幾個因素助長網路威脅在這些平台上的擴散。GitHub 上有多如牛毛的惡意竊密程式--通常都是源於現有惡意軟體的後繼版本--這種方式大大降低攻擊者的技術門檻。免費存取這些工具更讓發動網路攻擊變得更容易。

易於使用和機密性進一步助長了它們遭濫用。Telegram 的加密訊息可讓網路罪犯在保持匿名的同時滲出資料，而 Discord 的 webhooks 則可簡化 C&C 作業和資料竊取。

這兩種平台還能透過 API 來整合包含 Windows、Linux、macOS 和 Android 等跨平台，輕鬆擴展成為自動化的攻擊架構，提高了攻擊的有效性。此外，這兩種平台的廣泛合法使用，讓惡意活動混入正常流量中，使偵測和緩解更具挑戰性。

以 Telegram 和 Discord 為基礎的威脅主要由網路駭客所發動，目標為消費者和企業。這些威脅可能具有高度的目標性或機會性，因此成為全球多個網路犯罪團體和個體戶的萬能工具。

消費者面臨的風險：

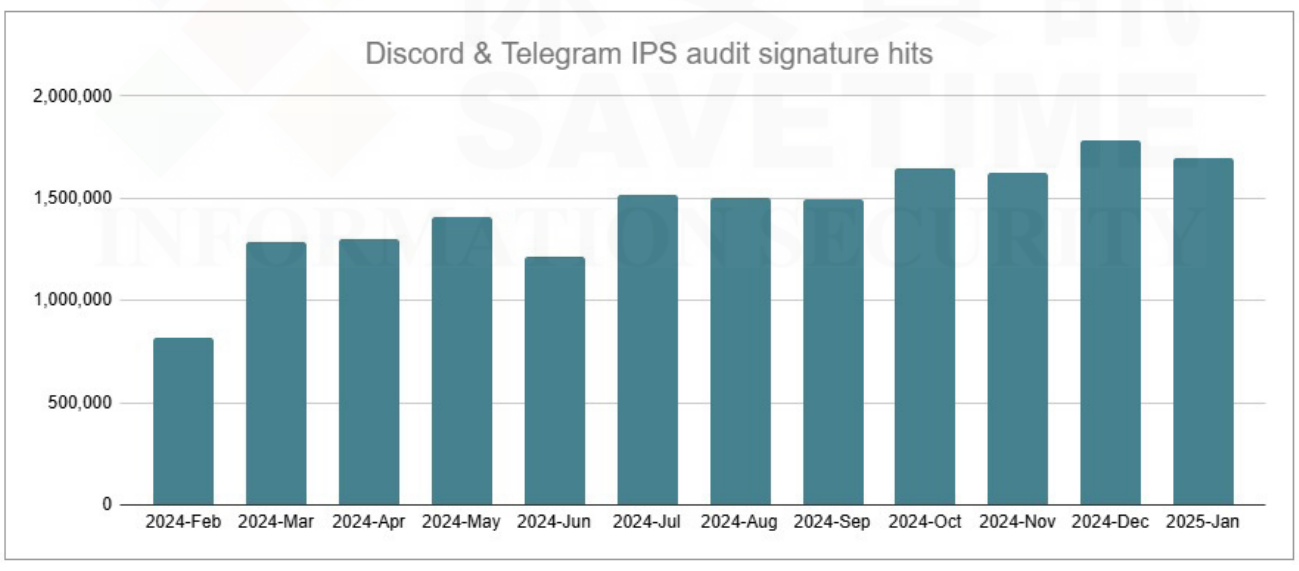
- 遊戲：在 Steam、Epic Games 等平台上的帳號和遊戲資產遭竊。
- 加密貨幣：錢包金鑰和交易所認證遭破解，讓攻擊者得以劫取資金。
- 檔案：竊取個人檔案 (本機或同步資料夾中儲存的身分證、稅務記錄和敏感檔案)。
- 瀏覽器：竊取儲存的密碼、自動填寫資料、信用卡詳細資料和 cookies。
- 鍵盤測錄：擷取按鍵以竊取密碼、私人對話及其他敏感資料。

企業面臨的風險：

- 企業資料遭竊：合約、藍圖和智慧財產外流。
- 憑證竊取：入侵企業 SaaS 帳戶、電子郵件平台和內部網路。
- 財務開採：使用企業信用卡進行採購或訂閱欺詐。
- 勒索軟體與 IAB：被盜的企業資料可用於索取贖金。或出售給始存取掮客 (Initial Access Broker-IAB) 或勒索軟體集團，為大規模的入侵提供快速取得立足點的情報。

賽門鐵克和 Carbon Black 採用多層次的防護技術能力對抗來自濫用 Telegram 和 Discord 的網路威脅：

- 檔案型防護：進階的行為、啟發式和機器學習防禦技術可在惡意檔案執行之前偵測並攔截惡意檔案。
- 以 EDR 為基礎的防護：Symantec Endpoint Security Complete 和 Carbon Black EDR 可處理與濫用這些服務相關的 MITRE ATT&CK 技術，以及這些威脅使用的許多其他一般 TTPs。
- 政策式保護：Data Center Security 預設政策可針對這些惡意軟體威脅提供零時差保護，防止它們在系統上被注入或執行。
- 網頁式防護：與惡意 Telegram Bots 或 Discord Webhooks 相關的已知網址 (URL) 會進行相對應的分類，以防止使用者存取有害網站，並防止其資料外洩。
- 網路型防護：在 2024 年，賽門鐵克建立數個端點上的網路層入侵防護系統 (IPS) 的稽核特徵，來強化安全性。以下是這些特徵一年的遙測資料：



最初，惡意竊密程式和遠端存取木馬 (RAT) 家族是濫用這些平台的主要惡意軟體。然而，到了 2024 年年中，網路釣魚的型態發生顯著變化。許多網路釣客開始濫用 TelegramBot 來滲出在網路釣魚網頁上輸入的憑證 (閱讀更多內容)。

欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲瞭解更多有關賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
沒有 SEP？試試使用賽門鐵克瀏覽器防護 (Symantec Browser Protection) 保護您的瀏覽器。
欲瞭解更多關於 Carbon Black 的資訊，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**。