入侵預防的稽核特徵(IPS Audit Signatures) --防範Discord和Telegram遭濫用的另一層數位監控系統

2023 年 11 月 28 日發布

Discord 和 Telegram 是近年來大受歡迎的通訊和檔案分享應用程式。Discord 主要面向遊戲社群，提供各種迎合這一人群的功能，包括語音和文字聊天頻道、檔案分享和可定制性。Telegram 則是一款泛用性更強的通訊應用程式，它為訊息提供端到端加密，讓用戶可以安全地進行通訊。

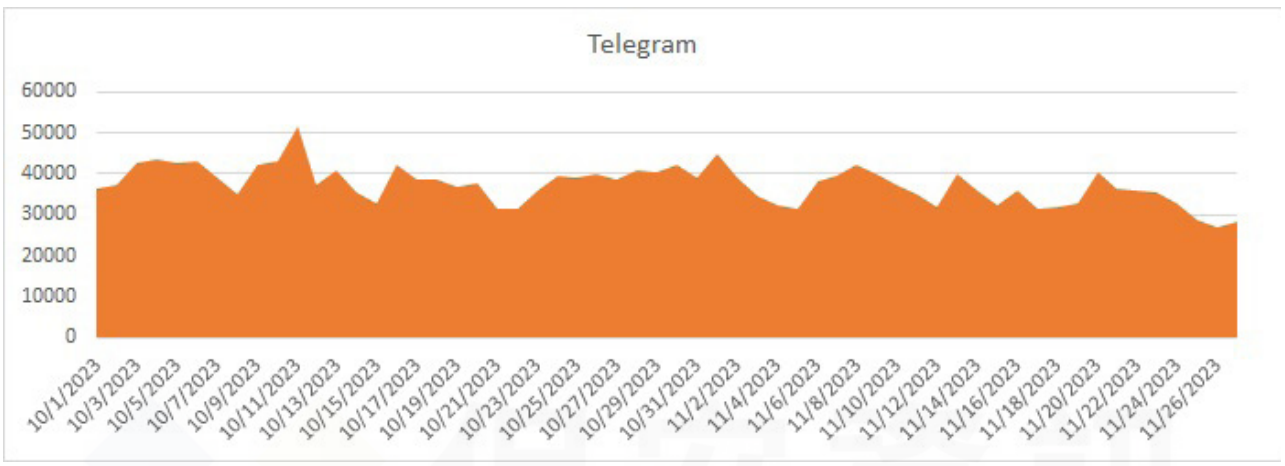
Discord 和 Telegram 的廣受歡迎，也自然成為網路犯罪分子覬覦的目標。造成這種趨勢的因素有幾個：

- **龐大的用戶群**：Discord 和 Telegram 都擁有數以百萬計的活躍用戶，這使它們成為網路犯罪分子試圖接觸廣大受眾的誘人目標。
- **檔案分享功能**：這兩個平臺都允許用戶輕鬆分享檔案，包括可執行檔，這些檔可用於傳播惡意軟體。
- **易於使用**：Discord 和 Telegram 都比較容易使用，這使得具有不同專業技術水準的用戶（包括那些懷有惡意的用戶）都能使用它們。
- **審核不易**：雖然這兩個平臺都實施一些審核措施，但由於使用者生成內容數量龐大，因此很難有效識別和刪除惡意內容。

由於這些因素，Discord 和 Telegram 已日益成為惡意檔案上架保管和竊取資訊外流的熱門途徑。網路犯罪分子濫用這些平臺分享惡意軟體、傳播被盜資料並從事其他非法活動。我們的讀者可在此處查看以前發佈的與可能利用 Discord 和／或 Telegram 威脅有關的防護公告。。

因應日益增多的惡意活動，除了更強大的防毒保護技術 (基於行為、啟發式和機器學習) 外，賽門鐵克還發佈幾款入侵預防 (IPS) 稽核特徵，以提供多一層的安全保護，讓客戶在監控未經稽核和可能被惡意行動者濫用的 Discord 和 Telegram 網路流量面向取得優勢。

賽門鐵克入侵預防的稽核特徵在過去兩個月內回報以下可疑活動：



SEP 的稽核特徵，讓您可以監控某些類型的流量，例如：Yahoo IM 登入。這些特徵預設為「不記錄」。您可以建立例外以記錄此流量，然後檢查日誌並決定如何處理流量。例如：您可能想要為該流量類型建立防火牆規則。。

賽門鐵克已經於第一時間提供多種有效保護 **(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)**。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Audit: PowerShell Process Accessing discordapp
- Audit: System Process Accessing discordapp
- Audit: Untrusted Telegram API Connection

若要進一步瞭解什麼是入侵預防 (IPS) 及其用途以及如何使用 URL 信譽攔截勒索程式？請參閱：管理入侵預防。

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 年起就全心全力於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環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。保安資訊連絡電話：**0800-381-500**。