網路釣客加大對Telegram聊天機器「應用程式介面」(API)的惡意濫用

2024 年 6 月 11 日發布

Telegram 服務

Telegram 是一種安全的雲端訊息服務平台，以其「高度隱私性」、「豐富的跨平台支援」、「免費且極大的開發彈性」三大特色和自毀訊息而聞名。它支援大規模群組、廣播頻道和廣泛的媒體／檔案共用。該服務在全球擁有數億活躍用戶。

濫用行為呈上升趨勢

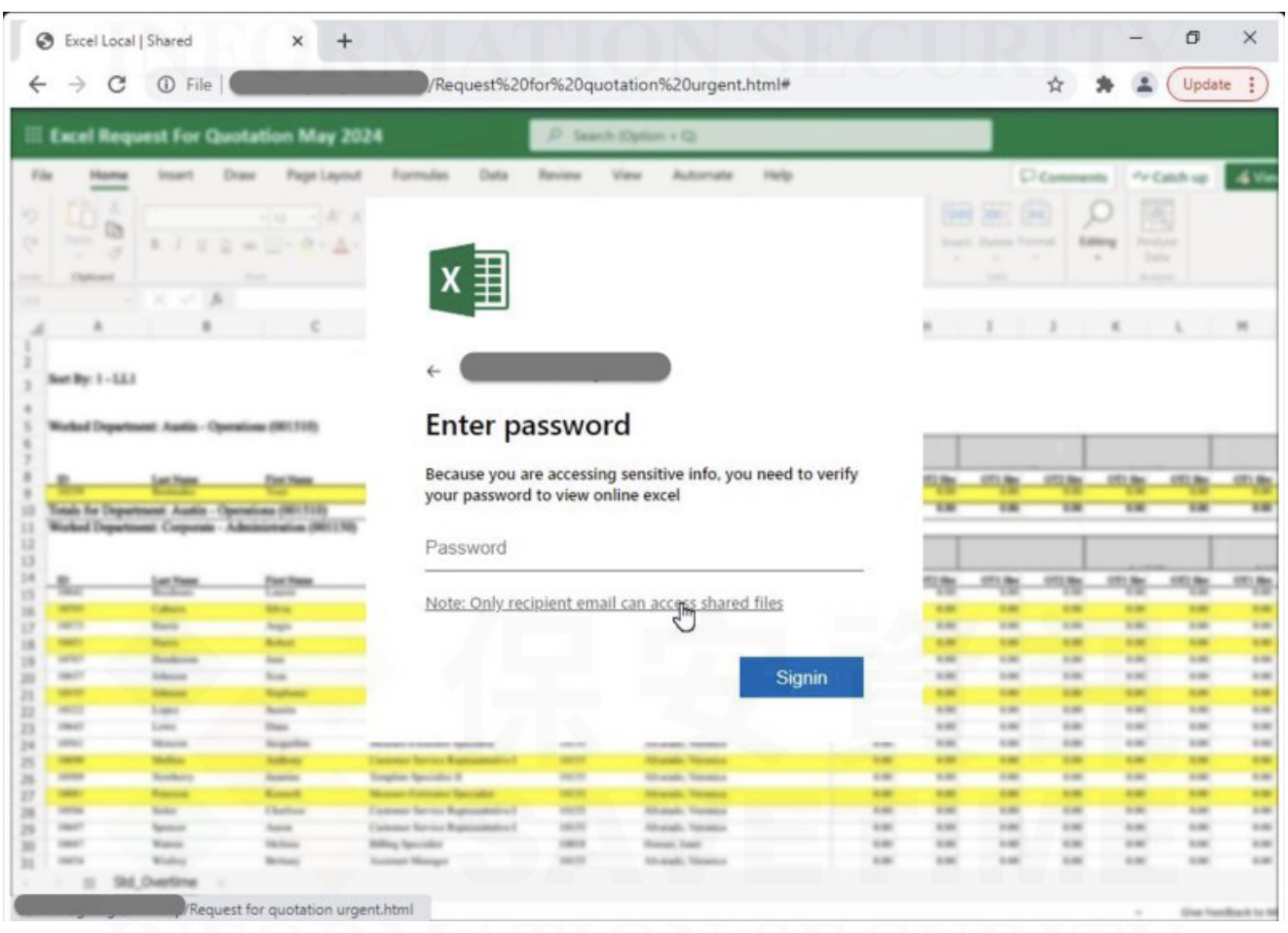
在過去幾個月裡，越來越多的網路釣客透過惡意 HTML 檔案，效仿惡意竊密程式和遠端存取木馬 (RAT)，現在還濫用 Telegram Bot API 來竊取用戶的憑證和其他敏感資訊，例如：信用卡詳細資訊。這些活動遍佈全球，它們可能給企業帶來重大的財務損失、運營中斷和信譽受損。攻擊者使用竊得的憑證進行帳戶劫持、身份／財務盜竊和其他攻擊，並經常在暗網上出售竊取的資料。

此一增長的原因有幾個關鍵因素。從威脅行為者的角度來看，Telegram 提供的易用性和匿名性使其成為一個極具吸引力的選擇。Telegram Bot API 直接明瞭，只需最低限度的程式設計技能，並提供一種高效率、可擴展的方式來處理大量被盜資料。Telegram 的即時性使攻擊者能夠立即接收憑據和其他敏感資訊，使其能夠在受害者做出反應之前迅速採取行動 (例如：更改密碼、通知他們的 IT 部門等)。此外，從傳統的網路釣魚滲透方法轉向新技術可以暫時規避現有類型的監控和保護。

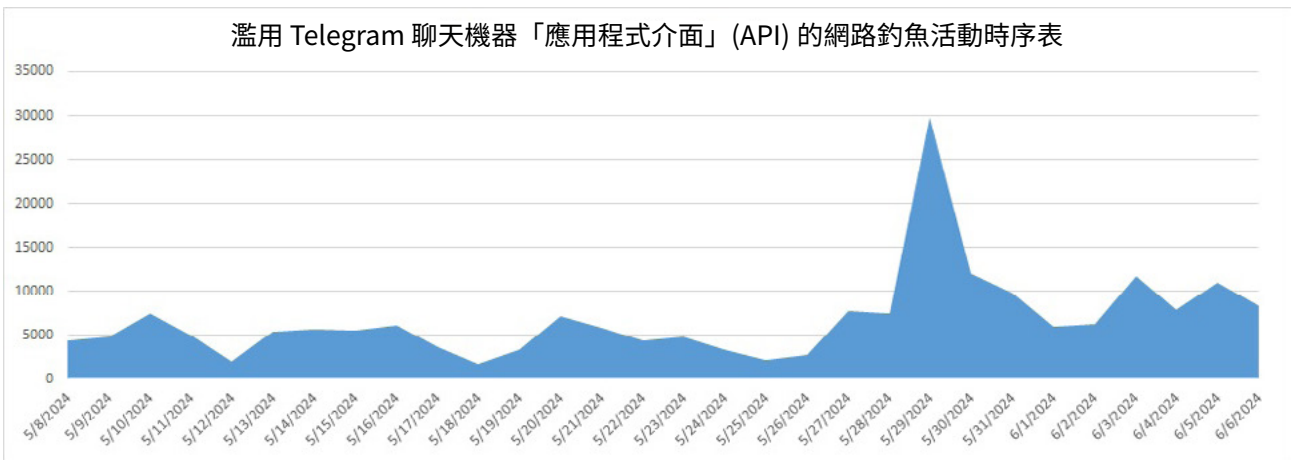
攻擊工作流程

1. 攻擊者通常會先建立一個 Telegram 機器人，獲取允許機器人與 Telegram 伺服器通訊的 API 權杖。接著，攻擊者建立一個 Telegram 公開或私人頻道，機器人將在該頻道中發送竊取的憑證。
2. 發送給受害者的釣魚郵件包含 HTML 檔，其中大部分都偽裝成合法的辦公室文件 (PDF、Excel、Word 等)。被開啟後，這些檔會顯示一個偽造的登錄頁面，仿造安全文件登錄畫面的外觀。用戶被提示輸入憑證以『檢視』文件，但輸入的憑證不會瀏覽任何真實檔案，而是直接發送給攻擊者。
3. 被截取的憑證會透過 Telegram Bot API 發送給 Telegram 機器人。HTML 檔案中的 JavaScript 代碼會使用竊取來的憑證向 Telegram Bot API 發送 HTTP GET 或 POST 請求。腳本會防止表單以傳統方式提交，收集用戶名和密碼，並透過機器人將這些資訊發送到指定的 Telegram 頻道。
4. 最後，一旦憑證被發送給機器人，它們就會被發佈到 Telegram 頻道中。攻擊者可以即時監控該頻道，收集竊取的資訊。這種方法可以讓網路釣魚者以最小的代價有效率且匿名地收集憑證。

一份典型的偽造檔案，要求輸入使用者密碼



觀察到的惡意 HTML 表現出不同程度之混淆，並採用不同的腳本技術。下圖反映近期的攻擊趨勢。



要在不斷變化的威脅環境中保持領先地位，就需要全天候監控、持續創新、自適應的安全政策以及跨技術的威脅情報共享。賽門鐵克整合所有功能且更強大威脅情資，以促進對本公告所述威脅的強大防禦，確保提供全面保護，最終讓用戶高枕無憂。

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：

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Phish.Html*
- Phish.TGhtml
- Scr.Phish!gen7

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。

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**。