得力於威脅檢測平臺：STARGate提供的網頁威脅洞察力(URL Insight)，賽門鐵克解決方案能夠有效抵禦複雜攻擊鏈的威脅

2025 年 5 月 27 日發布

專業術語解說：

STARGate(*星際之門) 是賽門鐵克安全技術與回應 (STAR：Security Technology and Response) 團隊所維運的基於機器學習、雲知識和深度內容檢查的威脅檢測平臺。其管理框架具備自動更新所有支援防護軟體的功能，無須由使用者自行更新。

在現今瞬息萬變的威脅環境中，攻擊者持續精進他們的方法，利用各種不同且通常是合法的工具，試圖規避安全措施以散佈惡意的有效酬載。這一點在我們過去幾個月來持續監測到的網路釣魚和垃圾攻擊行動上尤其明顯。

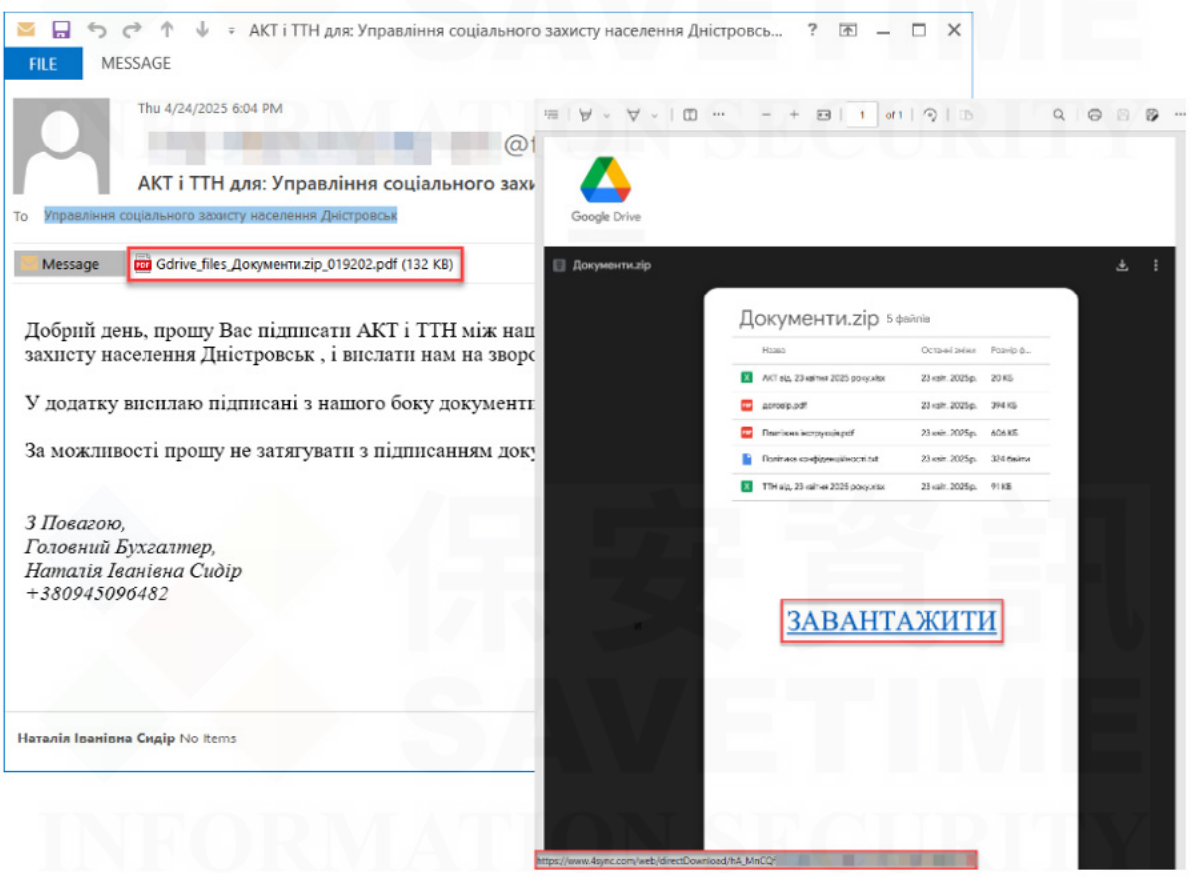
俄羅斯文的 PDF 偽造付款文件詐騙行動

自 2024 年 12 月以來，我們觀察到一波鎖定烏克蘭電子郵件地址的目標式郵件攻擊，這類攻擊使用一般的雲端儲存服務來傳送遠端存取木馬程式 (RAT)。

此類攻擊行動通常以一封包含 PDF 附件的釣魚電子郵件引爆，在某些情境中，直接在電子郵件本文中嵌入惡意網址。內嵌的惡意網址通常指向雲端硬碟平台，例如：4Sync 或 Dropbox。如果點擊這些連結，就會下載包含惡意 JavaScript 檔案的 ZIP 壓縮檔。

該 JavaScript 檔案一旦被執行，會嘗試下載和執行遠端存取工具。較早期的攻擊行動依賴 NetSupport RAT，這是一種合法的遠端管理工具，常被威脅份子濫用於隱匿存取和控制。最近的攻擊行動則轉為使用 Remote Manipulator System (RMS) Remote Utilities，顯示攻擊者的攻擊工具可能已經進化或更多樣化。

具體來說，在最新的四月攻擊中，一封附有 PDF 樣板的電子郵件會被寄出，該樣板會顯示內嵌有 4sync 網址的偽造 GDrive 內容。



如上文所述，點選 4sync 連結會下載包含 JavaScript 檔案的 ZIP 壓縮檔。惡意 JavaScript 程式碼隨後會嘗試下載 RMS/RemoteUtilities 的 MSI 安裝程式到受害者電腦，提供遠端存取給攻擊者。

STARGate 提供的網頁威脅洞察力(URL Insight)

當 STARGate 的 URL Insight 識別出嵌入在 PDF 中的 4sync 惡意網頁，或像先前的攻擊一樣，直接嵌入在電子郵件本文中時，它會主動在攻擊鏈的初始引爆點阻止此攻擊。此攻擊會在電子郵件閘道層以 Web.Reputation.2 命名的威脅分類來封鎖，保護終端使用者不會下載攻擊者的遠端存取安裝程式。

STARGate URL Insight 負責從賽門鐵克的雲端網頁安全引擎 (WebPulse) 產出防護效益，截取具有惡意內嵌 URL 的可疑檔案或電子郵件，以及下載檔案的來源 URL。WebPulse 會對來自數千家不同企業、數百萬賽門鐵克端點防護 (Symantec Endpoint Protection) 的使用者，以及賽門鐵克電子郵件安全 (Symantec Email Security) 產品所掃描的數十億封電子郵件的 URL 進行分類與評比。這些情報是賽門鐵克豐富的威脅情報資料庫中一部分。

目前，STARGate 的 URL Insight 每日評估 Symantec Enterprise 產品中超過 30 億個網頁，且每日偵測出 20 萬個以上的**惡意內嵌網址，在攻擊行動期間 (例如：我們在 3 月和 4 月看到的攻擊行動) 更會激增超過 100 萬個**：

此外 URL Insight 可為 STARGate 其他先進技術提供更豐富寶貴的脈絡，進而實現多樣化的多層次安全方法。STARGate 的 URL Insight 價值實現也廣泛應用於賽門鐵克企業安全產品，例如：

- 賽門鐵克郵件安全雲端服務 (ESS：Email Security Service)
- 賽門鐵克地端自建郵件安全閘道 (SMG：Symantec Messaging Gateway)
- 雲端安全服務：CloudSOC
- 賽門鐵克防護引擎專為：NAS／雲端儲存
- 賽門鐵克 Sharepoint 服務防護
- 賽門鐵克雲端沙箱：Cynic

欲了解有關有效抵禦複雜攻擊鏈的威脅情資：STARGate(*星際之門) 及其支援產品的詳細資訊，請點擊此處。

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。

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**。