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

又見WikiLoader惡意程式載入器強勢回歸

2024 年 1 月 23 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

WikiLoader 是早在 2022 年就被發現的惡意程式載入器，可以下載並植入惡意軟體在目標電腦上。它採用多種規避安全軟體偵測的伎倆和客製化的程式碼，與兩個主要的駭客組織 TA544 和 TA551 有所關連。

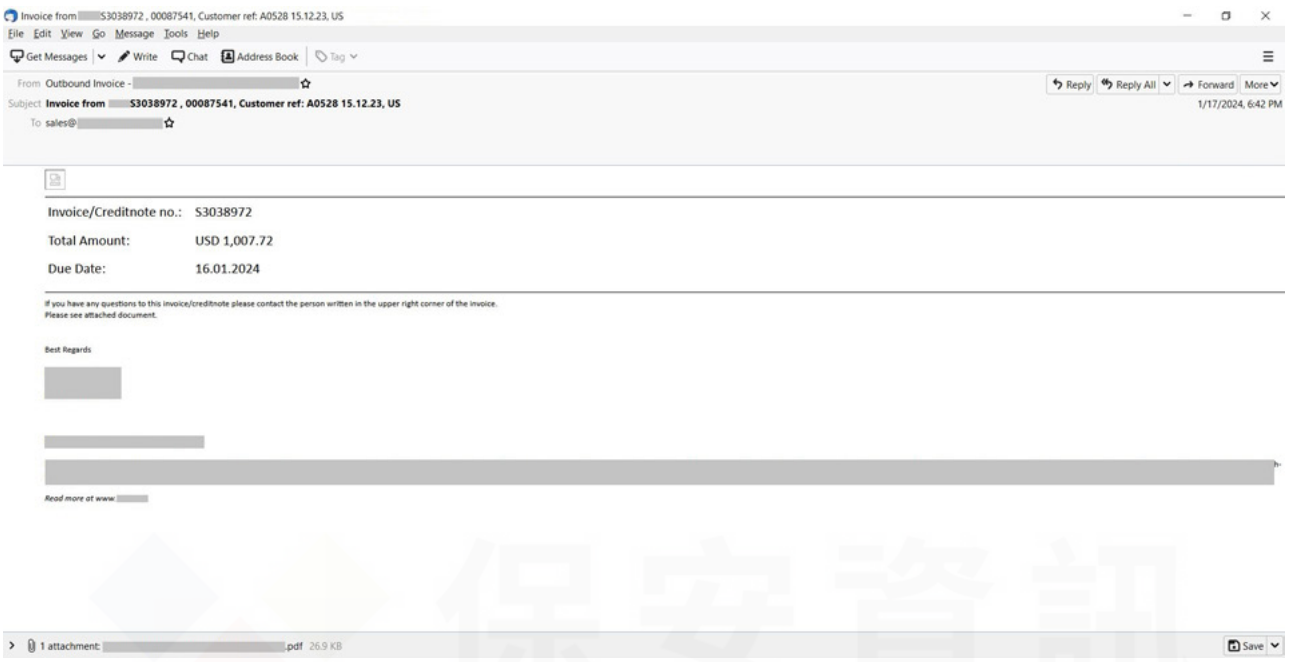
它之所以被命名為 WikiLoader，是因為最初的版本會向維基百科網站發出 Https 的連線請求，這很可能是為了檢查它是否有網際網路連接的能力，並且沒有在虛擬機器或隔離環境中運行，這可能顯示它正在被安全研究人員或某種類型的自動分析系統分析以規避安全軟體的偵測。

WikiLoader 的典型初始感染鏈始於一封包含 PDF 附件的電子郵件。在 PDF 檔中，會有一個連結，如果點擊該連結，就會下載一個壓縮的 JavaScript 檔，進而下載最終有效籌載。值得注意的是，開發者在腳本混淆方面下了很大的功夫。在超過 7 MB 的原始檔和 4383 行的程式碼中，大約 99.8% 是混淆的程式碼 (即垃圾程式碼)，目的是試圖隱藏其餘的一小部分核心惡意程式載入器的脈絡。鑒於 WikiLoader 的主要目的--提供惡意軟體散播服務--最終有效籌載可能是包羅萬象，但迄今為止較常見的是銀行金融惡意軟體，例如：Ursnif 或其他類型的惡意竊密程式。

觀察到的電子郵件主旨：

- Invoice from [company name]S7354534 , 01070875, Customer ref: A0627 15.12.23, US
- Invoice from [company name] S8786164 , 04725130, Customer ref: A0703 15.12.23, US

電子郵件範例：



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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.DLHeur!gen8
- Scr.Malcode!gen
- Web.Reputation.1
- WS.SecurityRisk.4

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：

- [33403] Audit: System Process Accessing discordapp.com

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

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。

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**。