惡意程式載入器來來去去，唯有 GuLoader「屹立不倒」，也唯有賽門鐵克用戶可以「臨危不亂」

2024 年 10 月 8 日發布

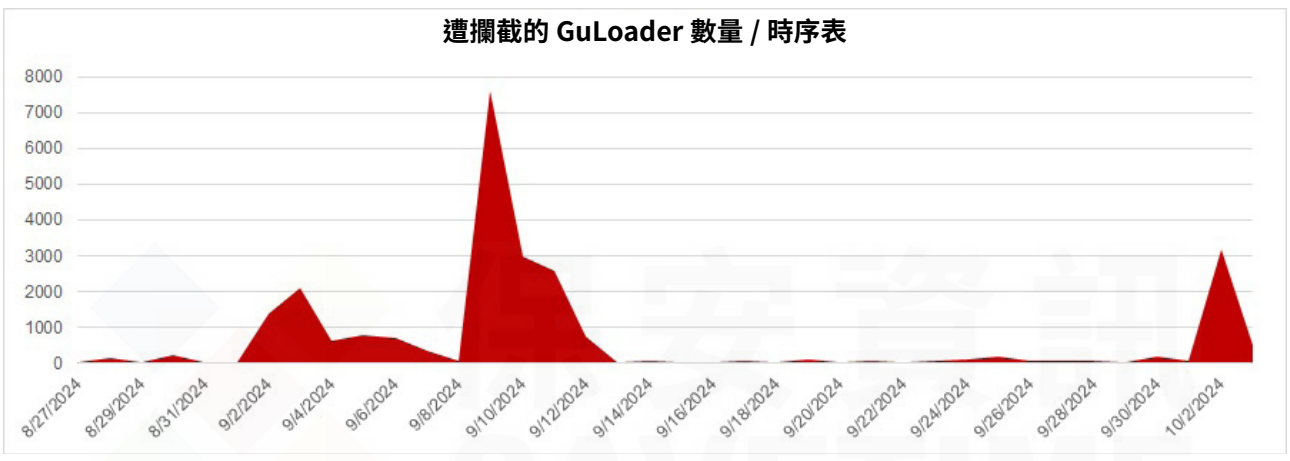
在網路犯罪的生態圈，惡意程式載入器已成為推動地下經濟的重要工具。這些惡意程式是傳送各種惡意軟體的切入點，從勒索軟體、木馬程式到惡意竊密程式，不一而足。網路罪犯利用對這些工具的需求，在暗網論壇上出售或出租這些工具，使大規模攻擊能夠同時感染數千個系統。隨著時間的推移，我們看到惡意程式載入器來來去去 (以下僅列出部分清單)，但 GuLoader 從一開始出現就具有獨特的持久性，可以說是當今威脅環境中最長壽的惡意程式載入器之一。

- GuLoader (2019年至今)
- Emotet (2014-2021 年，2022 年曾短暫重現)
- Dridex (2014 年至今)
- BazarLoader (2020 年至今)
- Zloader (2016-2022)
- TrickBot (2016-2020)
- Nemucod (2015-2016)
- Upatre (2013-2015)
- Andromeda/Gamarue (2011-2017)
- Pony (2013-2015)
- Smoke 惡意程式載入器 (2011 年至今)
- RIG 洞利用工具包 (2014-2018)
- Nymaim (2013-2017)

過去幾年來，GuLoader 的攻城掠地確實讓它躍居引領網路安全成為頭條新聞的要角。自 2019 年首次出現以來，這種精密複雜的惡意程式載入器已經成為網路罪犯最喜歡的工具，廣受駭客集團和單獨的攻擊者所採用。它有能力靈活應對各種情境和迴避技術使其成為傳送各種類型惡意軟體的多功能武器，幾乎可以滲透所有行業的組織。無論是在醫療保健、金融、政府或小型企業，GuLoader 已被部署到全球眾多領域，證明它有能力影響網路犯罪生態圈的市場的深度與廣度。

GuLoader 的主要攻擊媒介仍然是電子郵件，但隨著時間的推移，其作案手法已演變為各種傳送方式。最初它依賴惡意附件，現在已擴展到也使用惡意網址、內嵌惡意網址的 PDF、HTML 檔案，以及上架在 Google Drive 或 OneDrive 等雲端服務上的二進位檔案。

在過去幾週，賽門鐵克已經挫敗多起 GuLoader 所涉入的攻擊行動。GuLoader 活動的最高峰出現在 2024 年 9 月 9 日，超過 7,000 起封鎖數量。在這個高峰之前，9 月 5 日和 6 日出現較小幅的增加，顯示在 9 月 9 日高峰之前活動逐漸增加。高峰之後，活動水準仍然很高，但逐漸下降。在 9 月 10 日和 12 日前後出現明顯的激增。2024 年 10 月初再次復甦，再次在 10 月 2 日達到高峰，封鎖數量約為 3200 個。



這些攻擊同時被賽門鐵克多種解決方案的多層次防護技術所攔阻，包括郵件安全雲端服務 -- Email Security.cloud (ESS)、賽門鐵克端點安全完整版--Symantec Endpoint Security Complete (SESC) 以及賽門鐵克端點偵測與回應--Symantec Endpoint Detection & Response (EDR)。Cynic 是賽門鐵克的雲端沙箱解決方案，它透過分析行為而非依賴靜態簽章，在識別 GuLoader 等進階威脅方面扮演重要角色。其不斷強化的動態能力，例如：偵測不斷改變特徵的多形惡意軟體和零時差攻擊，可大幅強化賽門鐵克的電子郵件和端點安全產品。

賽門鐵克端點偵測與回應--Symantec Endpoint Detection & Response (EDR)，使用機器學習和行為分析來偵測和揭露可疑的網路活動，包括 PowerShell 執行和程序注入，同時也與 AMSI 整合以偵測混淆的腳本。EDR 會針對潛在的有害活動發出警示，排定事件的優先順序以進行快速分級事件，並允許事件回應人員執行查詢、撰寫自訂偵測規則，以及瀏覽裝置活動記錄，以便對潛在攻擊進行鑑識分析。當 SES 與 EDR 搭配使用時，結合的技術可提供多層防禦。兩者結合後，可針對已知與未知的威脅提供全面的防護，確保能在攻擊鏈的早期就能攔截，避免不斷演進的威脅，例如：GuLoader。

賽門鐵克對 GuLoader 的防護措施包括以下幾項：

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g*
- SONAR.SuspLaunch!g*

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多訊息，請參閱此 GitHub 儲存庫：https://github.com/Symantec/threathunters/tree/main/Trojan/Remcos

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：

- Scr.Guloader!gen*
- Trojan.Guloader

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 Carbon Black，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**。