
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

# 賽門鐵克入侵預防技術 ～以防護 GuLoader的實例來驗證IPS的實績

**2024 年 5 月 7 日發布**

**點擊此處可獲取--最完整的賽門鐵克解決方案資訊**

賽門鐵克的入侵預防技術讓威脅不能越雷池一步，並在初始階段就阻斷以防患未然。賽門鐵克的 IPS 是行業中最佳深度資料封包檢查引擎，可保護數以億計的端點 (桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。對於大型企業，SEP 端點防護擁有多層次防護技術，僅單一項 IPS 技術就能涵蓋 90% 以上威脅防護和事的可視性。

多年來一直支援 Windows 和 MacOS 上 SEP 的 IPS 網路防護技術也為賽門鐵克的瀏覽器保護解決方案提供支援。瀏覽器防護將賽門鐵克 IPS 網路保護導入谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器。

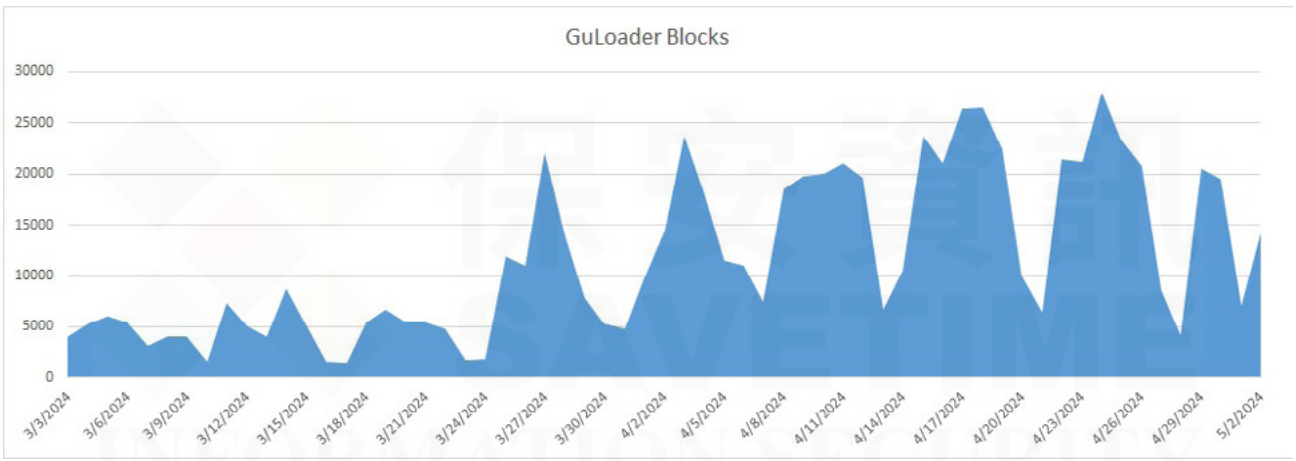
賽門鐵克 IPS 主要功能包括：

- IPS 引擎可以在該端點的網路層、檔案層和更深入的程序層等不同階層，精準檢測和攔截網路威脅活動。
- 遍佈全球的賽門鐵克威脅情資團隊，對當今影響企業網路威脅提供無與倫比的分析，並透過特徵碼資料更新來增強賽門鐵克 IPS。
- IPS 特徵碼集每週 5 天、每天透過 LiveUpdate 更新。這些特徵碼通常會主動阻止威脅的傳播，特徵碼每天都會更新，以改進目標式攻擊類型的 IPS 防護。
- IPS 利用 WebPulse 網頁脈衝專利技術，基於網址／網域／IP 分類來阻止已知釣魚網站和惡意軟體網域。賽門鐵克 WebPulse 服務依靠全球智慧型網路來識別威脅、威脅工件和惡意網路活動。
- 入侵預防的稽核特徵 (IPS Audit Signatures) 提供客戶自行微調 IPS 防護的自訂靈活性。
- 端點 IPS 為賽門鐵克 EDR 提供網路可見性，使威脅獵手團隊和事件回應人員能夠獲得豐富的網路資訊。

## 以防護 GuLoader 實例來驗證 IPS 實績

GuLoader 是近年非常氾濫的一種惡名昭章的惡意軟體下載器，因其在全球各地傳播各種不同的惡意軟體而聞名。某些情況下，它會載入 Agent Tesla 惡意竊密程式，而在其他情況下，它可能會下載 Remcos 遠端存取木馬。在我們最近的防護公報中了解有關 GuLoader 的更多資訊。

防護 GuLoader 的實績，是賽門鐵克 IPS 保護價值的常態而非特例。阻止 GuLoader 相關網路流量可防止下載和執行攻擊鏈後期階段的酬載。IPS 每天能檢測並阻止成千上萬 GuLoader 活動。




## IPS攔截到GuLoader的數量/時序表

我們再看看每週活躍的其他威脅類別，以及它們被 IPS 阻擋的次數。在過去 7 天裡，SEP 的網路防護引擎 (IPS) 總共攔截了 5.57 萬次攻擊，涵蓋 51.06 萬個受保護端點。其中 82.8% 的攻擊是在執行有效載荷之前的感染前階段就被攔截的。

- 在 1.103 萬個端點上阻止了 1890 萬次掃描 Web 伺服器漏洞的嘗試
- 在 1.423 萬個端點上阻止了 1160 萬次利用 Windows 作業系統漏洞的嘗試
- 在 3.67 萬台 Windows 伺服器上阻止了 920 萬次攻擊
- 在 67.5K 個端點上阻止了 190 萬次掃描伺服器漏洞的嘗試
- 在 14.6K 個端點上阻止了 818.1K 次掃描 CMS 漏洞的嘗試
- 在 48.7 千個端點上阻止了 150 萬次利用應用程式漏洞的嘗試
- 阻止了 186.1K 個端點上 420 萬次攻擊，這些攻擊試圖將用戶重導向到攻擊者控制的網站
- 透過 11.3K 個端點阻止了 150 萬次挖礦嘗試
- 在 107.4K 個端點上阻止了 810 萬次惡意軟體 C&C 嘗試
- 在 538 個端點上阻止了 56.5K 次加密劫持嘗試

按一下此處了解有關在桌上型電腦和伺服器上啟用 IPS 的更多資訊。

按一下此處了解有關整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站。

別家都沒有的功能？試試使用賽門鐵克瀏覽器保護功能保護您的瀏覽器。

---

**2024/04/30**

## GuLoader惡意軟體下載器，涉入針對俄語系國家的網路攻擊

已觀察到一名威脅者利用不同的社交工程手法發動兩起電子郵件攻擊行動，這些行動都有 Guloader 涉入的跡象。這兩起電子郵件攻擊行動都針對俄語系國家，例如：俄羅斯、白俄羅斯、吉爾吉斯和哈薩克的產業。

在一封電子郵件 (主旨：СПЦ №130 подписанная Belarus) 中，他們冒充一家從事製藥和保健行業的俄羅斯大型公司。該公司有多個業務部門，包括藥品行銷、零售連鎖藥店和醫藥產品製造。攻擊者使用類似銷售的社交工程手法，夾帶一個壓縮附件檔 (СПЦ №130 от 12.04.2024 подпис.7z)，並誘使受害者執行其中偽裝成產品特性摘要的惡意二進位檔案 (СПЦ №130 от 12.04.2024 подпис..exe)。

在分析上述攻擊情境時，賽門鐵克在公開來源中發現另一個惡意壓縮檔 (Доверенность Транзит Хоргос.7z)，其中包含完全相同的 GuLoader 有效酬載。因此，作者似乎也在使用不同的電子郵件方案開展並行活動 (儘管目前還無法獲得該電子郵件)。根據其名稱，威脅者試圖用與霍爾果斯貨物過境相關的法律檔案引誘受害者。霍爾果斯是哈薩克和中國邊境上的一個重要地點，因其作為主要陸港和新絲綢之路經濟帶上的樞紐而聞名，促進中國、中亞和歐洲之間的大量貿易和物流業務。

GuLoader 是一種惡名昭章的惡意軟體下載器，因其經常涉入世界各地的攻擊行動被用於傳播各種惡意軟體而聞名。在本案例中，它正在載入 Agent Tesla 惡意竊密程式，但也可能下載 Remcos 遠端存取木馬。

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)。

**自適應防護技術(包含於SESC)：**

- ACM.Untrst-RunSys!g1

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Trojan Horse

### 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**。