



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

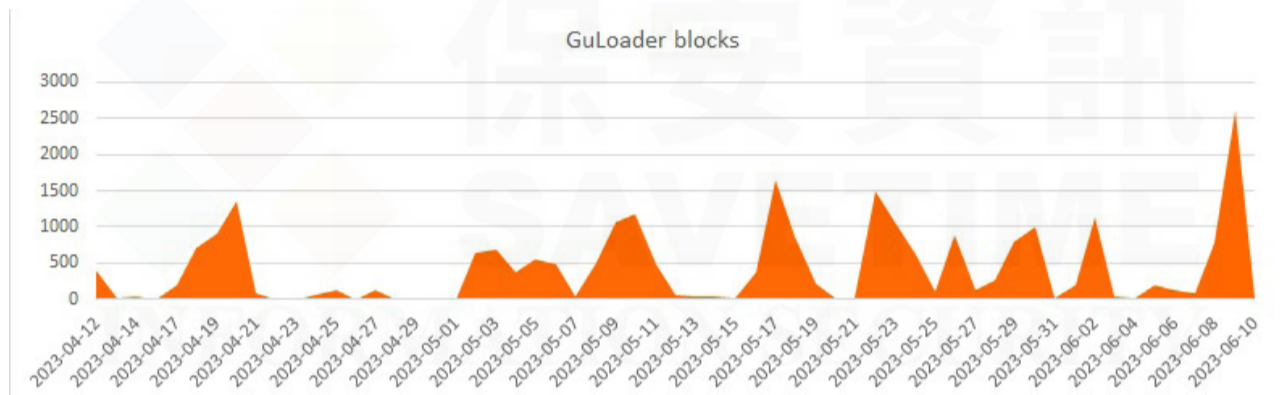
再次檢視GuLoader進階下載器

2023年6月12日發布

[點擊此處可獲取--最完整的賽門鐵克解決方案資訊](#)

我們在今年3月發布一份關於 GuLoader 的防護亮點公告P8，在上週五觀察到活動激增後，這是一個簡短的追蹤，以確認它仍舊嘗試做不法行為，並且仍然成功的被 Symantec 防護產品主動攔截。

回顧一下，GuLoader 是一種基於 shellcode 的進階下載器，它使用各種反分析技巧來試圖逃避檢測並使逆向工程更加困難，其目標是提供一系列惡意軟體，包括但不限於勒索軟體、竊密程式、銀行木馬、遠端存取木馬 (RAT) 和代理 (proxy)。GuLoader 主要透過各種不同主旨的垃圾郵件進行傳播，包括帶有其他惡意軟體連結的版本，或者在某些情況下直接包含嵌入式腳本的附件，該腳本會試圖在使用者系統上構建 PowerShell 腳本並執行它。最終的有效籌載也各不相同，但 FormBook、Agent Tesla、NanoCore 和 Netwire 是最常見。



賽門鐵克為 GuLoader 提供多個零時差防保護。以下是目前的前 10 名：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Exp.CVE-2017-11882!g7
- Packed.NSISPacker!g14
- Scr.Malcode!gen19
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.B!200
- Heur.AdvML.C

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)。

欲深入瞭解更多有關於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](#)。

欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請[點擊此處](#)。

欲瞭解更多有關於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](#)。

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, 以及基於比原廠更熟悉用戶環境的優勢能提供更快更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。

業界公認 保安資訊--賽門鐵克解決方案專家

■ ■ ■ We Keep IT Safe, Secure & Save you Time, Cost ■ ■ ■

服務電話：0800-381500 | +886 4 23815000 | <http://www.savetime.com.tw>