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

木馬程式 Masslogger 再度成為駭客圈青睞的焦點

2025 年 6 月 17 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

木馬程式Masslogger 重出江湖

木馬程式 Masslogger 至少從 2020 年就開始活躍，這幾個月來全球各地的各種威脅組織和獨立行動者利用這隻惡意程式所發動攻擊明顯增加，目標是各行各業以及公共組織。

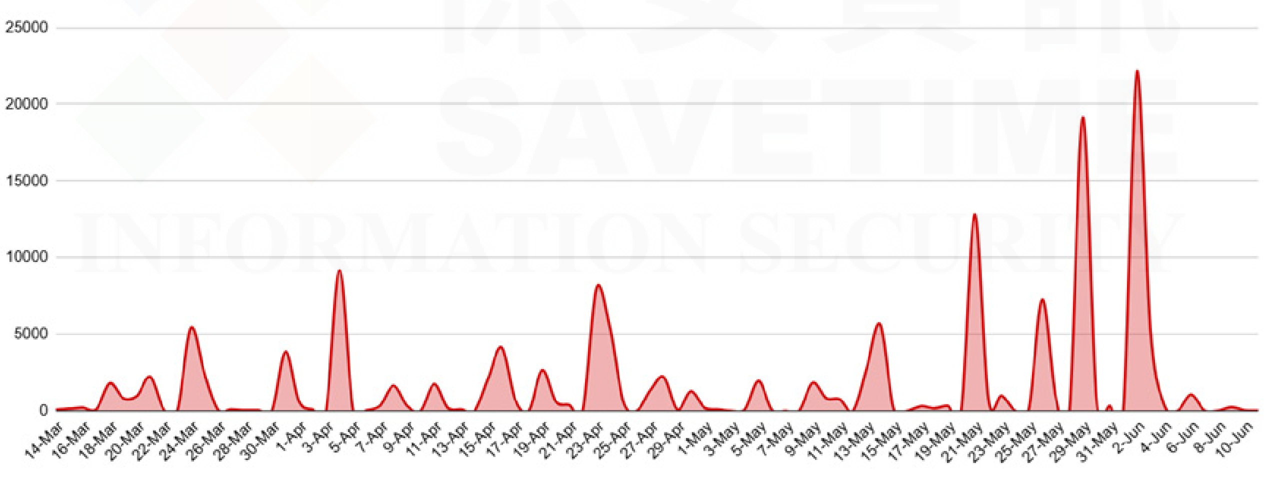
雖然不同的攻擊行動和攻擊者所偏愛的戰略多所不同，但 MassLogger 涉入的攻擊始終遵循一種有跡可循的模式：社交工程的網路釣魚電子郵件、隱蔽的執行技術，以及從受感染的系統中擷取敏感憑證。

在透過電子郵件發動初始攻擊後，大多數的攻擊行動會採用直截了當的方法--以詐術附加壓縮檔內含木馬程式 Masslogger 的二進位檔案。然而，更老練的攻擊者通常會擴充此方法，利用 JavaScript、VBScript、Batch 或 PowerShell 等腳本式的惡意程式載入器，以及 NSIS 和 SCR 等可執行格式的替代方案，來繞過安全軟體的偵測並提高有效酬載的執行成功率。

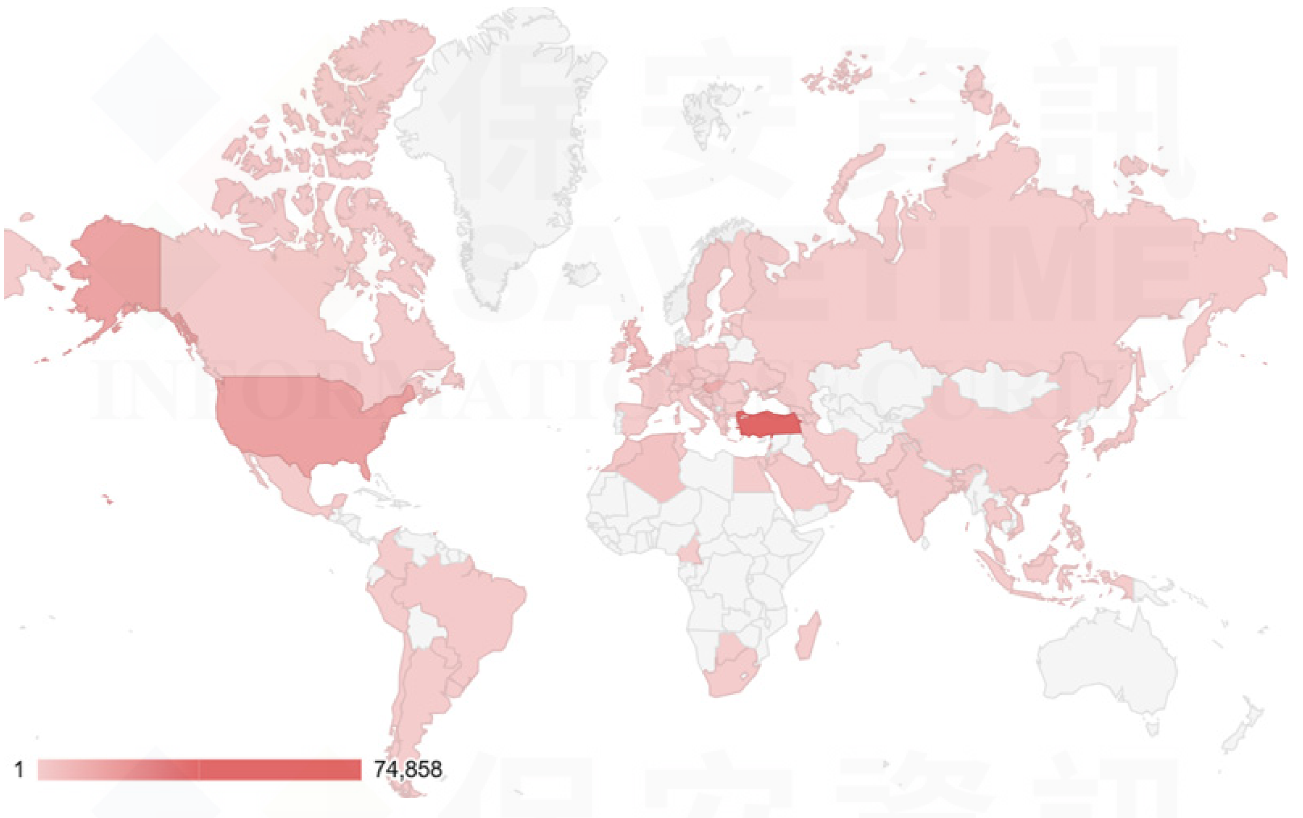
在過去半年，MassLogger 活動一直持續，並在多個地區觀察到幾次急劇的飆升。我們的資料顯示，儘管每日的偵測通常持平，但週期性的峰值 (特別是在五月底和六月初)，顯示出較大的波動。

土耳其是最受影響的國家，防毒引擎偵測到的次數超過 74,000 次，其次是美國以及數個歐洲和拉丁美洲國家。此分佈情況顯示廣泛的機會主義目標策略，很可能是利用當地化的誘餌和利用遭入侵的基礎設施進行傳送。

MassLogger 偵測趨勢



MassLogger 偵測熱圖



鎖定憑證為目標

MassLogger 是一款普通的憑證竊取惡意軟體，其設計目的是在嘗試滲透敏感用戶資料時隱藏其行蹤。它的目標是廣泛的憑證來源，包括網頁瀏覽器、電子郵件用戶端 (例如：Outlook 和 Thunderbird)、FTP 應用程式 (例如：FileZilla)、VPN 軟體等。

此威脅支援多種通訊方法做為外洩手段。常見的技術包括透過 SMTP(電子郵件) 傳送竊取的資料、透過 FTP 上傳或使用 HTTP POST 請求傳送至攻擊者控制的伺服器。在某些自訂變種中，攻擊者透過利用 Telegram Bot API 將 MassLogger 配置為使用 Telegram bots 來滲透日誌。這可讓惡意軟體直接將竊取的資料傳送到操作者的聊天帳戶，使用加密且看似合法的 HTTPS 流量，試圖繞過防火牆並逃避網路監控。

MassLogger 操控者最近使用的 Telegram 殭屍權杖範例：

- bot7341689230:AAHymAZAjTKDwQdX3qK2HITohVFwhbvLPIc
- bot7398536732:AAFG_GQm2-o0UoJEIV0aVrSPCtyqz5VEliU
- bot7646451386:AAGgex98cq9UD2k8MPa66b
- bot8004081294:AAEeQb3kkdq-mgW3gSkEAnMJX0fU078688E
- bot8185619395:AAFoycueqDVSZD7Vj-U3AfAuKB5byVNAYJU。

對應 MITRE ATT&CK 框架的攻擊戰略

以下是最近觀察到的木馬程式 Masslogger有效酬載對應到 MITRE ATT & CK 框架的戰術和技巧：

- 執行 (TA0002)：透過排程任務／工作 (T1053)、指令與腳本編譯器 (T1059)，特別是 PowerShell (T1059.001、T1086) 與 base64 編碼的有效酬載執行惡意行為。同時利用 Native API (T1106) 和 Shared Modules (T1129) 來動態載入和執行程式碼。
- 持續性／常駐能力 (TA0003)：透過排程任務／工作 (T1053) 和註冊表 Run 機碼／啟動資料夾 (T1060、T1547.001) 建立持續性，將惡意指令碼置入啟動目錄。此外，它還會修改註冊表 (T1112)、建立或操控 Windows 服務 (T1543.003)，並包含使用 Bootkits (T1542.003) 的預先作業系統啟動 (T1542) 支援。
- 權限提升 (TA0004)：透過程序注入 (T1055) 和存取權限操控 (T1134) 獲得提升的執行權限。也會使用「建立或修改系統程序」(T1543) 及「開機或登入自動啟動執行」(T1547) 維持系統層級服務的持續性。
- 防禦規避 (TA0005)：使用 Rootkit (T1014) 元件、混淆檔案或資訊 (T1027)、軟體封裝 (T1027.002、T1045) 及程序注入 (T1055) 來避免偵測。它會在執行時解除混淆內容 (T1140)、隱藏惡意視窗 (T1143、T1564.003)，並採用指標刪除 (T1070)、修改註冊表 (T1112) 和停用或修改工具 (T1562.001)。它還運用反射式程式碼載入 (T1620)，並使用隱藏檔案和目錄 (T1564.001) 隱藏生成物。
- 憑證存取 (TA0006)：嘗試透過作業系統憑證轉存 (T1003)、檔案中的憑證 (T1081) 及註冊表中的憑證 (T1214) 收集憑證。它會搜尋不安全的憑證 (T1552)，且會竊取 Web Session Cookies (T1539)。
- 搜尋 (TA0007)：查詢註冊表 (T1012)、搜尋系統網路組態 (T1016)、執行進程搜尋 (T1057)、系統資訊搜尋 (T1082) 以及檔案與目錄搜尋 (T1083)。它還會檢查已安裝的軟體 (T1518)，並透過偵錯程式偵測使用沙箱規避技術。
- 收集 (TA0009)：使用本機系統資料 (T1005)、電子郵件收集 (T1114) 和自動收集 (T1119) 收集敏感檔案和資料。收集的資料會透過 (T1560.002) GZip 進行壓縮。
- 指揮與控制 (TA0011)：透過應用層通訊協定 (Application Layer Protocol，T1071) 建立 C2 通訊，使用動態解析 (Dynamic Resolution，T1568) 建立彈性的基礎架構，並使用加密通道 (Encrypted Channel，T1573) 加密通訊。
- 影響 (TA0040)：可透過資料破壞 (T1485) 進行破壞行動，並可能從事資源劫持 (T1496)，影響系統效能或可用性。

Symantec 的防護

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Enc!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g483

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。

基於端點偵測與回應(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資訊，請參閱此鏈接：https://github.com/Symantec/threathunters/tree/main/Trojan/IcedID
- 賽門鐵克的端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

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：

- CL.Suspexec!gen*
- Downloader
- Hacktool
- ISB.Downloader!gen*
- ISB.Heuristic!gen*
- ISB.Houdini!gen7
- JS.Redirector
- MSIL.Packed.*
- Packed.NSISPacker!g*
- Phish.ScptML.L
- Scr.Malarchive!gen*
- Scr.Malcode!gdn*
- Scr.Malcode!gen*
- Scr.Mallnk!gen*
- Scr.xSense!gen*
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Trojan.Malautoit!g*
- Trojan.Malcab
- Trojan.xSense.C
- Web.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B
- Heur.AdvML.C

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：

- Wudit: Untrusted Telegram API Connection

欲了解啟用賽門鐵克端點安全完整版 (SESC) 上的「自適應防護」透過管理受信任應用程式所執行的潛在風險行為來減少攻擊面，請點擊此處。

要了解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。

欲了解 Carbon Black Endpoint，請點擊此處。

欲了解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

欲深入了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。

欲深入了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。

欲深入了解賽門鐵克的端點多層次防護解決方案中「進階機器學習」防護技術，請點擊此處。

欲了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。

Symantec
A Division of Broadcom

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。

保安資訊
KEEPSAFE
INFORMATION SECURITY

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，以及基於比原廠更熟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**。