



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

與時俱進的賽門鐵克靜態資料掃描器之 .NET 模擬器，再老練的駭客也討不到便宜

2024 年 9 月 24 日發布

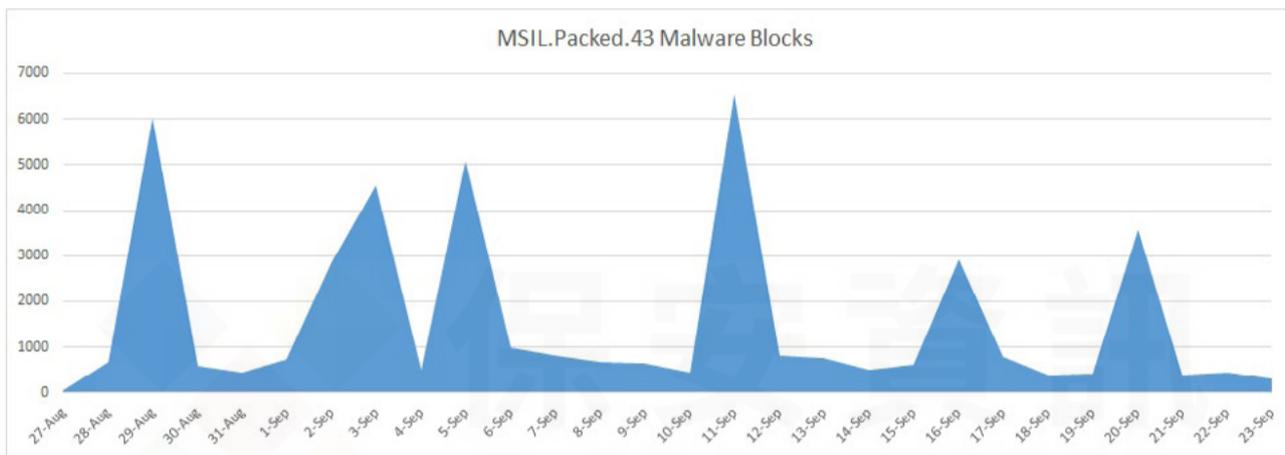
[點擊此處可獲取--最完整的賽門鐵克解決方案資訊](#)

在現今快速演進的威脅環境中，網路攻擊已變得越來越複雜。Snake Keylogger、Formbook 和 Lokibot 等惡意軟體最近變種活動更加頻繁，並採用各種傳送方式，例如：釣魚電子郵件、惡意附件和偷渡式下載。這些技術最終會部署惡意的 .NET 有效酬荷，對組織造成重大風險。

.Net 是微軟在 2000 年代初推出的軟體開發框架，主要是為了讓程式設計更容易。支援 C#、VB.NET 等多種語言，.NET 程式會編譯成 Microsoft Intermediate Language (MSIL：中繼語言有時也稱為通用中間語言 (CIL))。執行時，即時編譯器 (JIT) 會將 MSIL 轉譯為機器程式碼。雖然 .NET 架構的設計初衷是為了幫助軟體工程師，但網路罪犯很快就找到濫用其功能以謀取自身利益的方法，他們通常使用特殊工具來混淆 .NET 應用程式的原始程式碼，以增加理解逆向工程和分析程式碼的挑戰性。

我們在 2024 年 5 月的公告中討論過賽門鐵克靜態資料掃描技術：SDS--Symantec Static Data Scanner，其中包含模擬器，是它主要功能之一。SDS 實際上包含好幾個模擬器，其中一個是進階的 .NET 模擬器，專門用來有效偵測並解除這些隱藏的威脅。它可發現隱藏在合法功能中的惡意程式碼，發現不尋常的修改或新增內容。它會模擬應用程式的執行，識別標準方法 (例如：Application.Run) 內的異常情況。最後它會在威脅發生時偵測並解除威脅，將潛在損害降到最低。

賽門鐵克持續成功阻擋數以千計以「MSIL」開頭的 .NET 惡意軟體攻擊。以下是上述 Snake、Formbook 和 Lokibot 攻擊的最新範例。



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](#)。

欲深入瞭解賽門鐵克的端點多層次防護解決方案中「檔案檢測技術」如何保護裝置，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、可以提供良好諮詢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。

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>