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

健全的底層邏輯，可以應對千變萬化的世局：賽門鐵克無須更新也能防護最新的Emotet零時差攻擊

2022 年 11 月 29 日發布

安全研究人員早在 2014 年就首次發現 Emotet 銀行木馬，現已證明它是威脅領域中最受歡迎且最強悍的木馬之一。最初是一支單純的銀行惡意軟體，試圖從受害者那裡竊取敏感的銀行相關訊息，後來的版本逐漸引入了新的模組化功能和感染媒介，包括垃圾郵件、惡意軟體交付服務（包括其他銀行木馬和勒索軟體）和隱身修改。美國國土安全部甚至表示，Emotet 是他們見過的成本最高、破壞性最強的惡意軟體之一。

Emotet 已經經歷幾個活動顯著下降的平靜時期，大概是在當局緊追不捨或者可能是由於內鬥或結構重組的時候。然而，在 11 月初，Emotet 背後的參與者發起一場新的惡意電子郵件攻擊行動，其中包括新的 URL 格式和個人化的登錄頁面，似乎是從休眠的活火山復發一樣。在此特定實例中，電子郵件包含負責下載 Emotet 的 Excel 附件，該 Excel 檔案利用社交工程，需要用戶輸入才能成功執行惡意內容，有效地讓毫無戒心的用戶感染。

雖然有許多不同的方法可以防禦像 Emotet 這樣的惡意軟體（正如我們在11 月 2 日的 Emotet 公告中所指出的那樣），但最好的方法當然是主動阻止它，無需更新簽章、定義檔、規則等，不過需要更新相對應的安全產品才能生效。雖然肯定沒有網路安全供應商敢於在每次威脅來襲時都聲稱主動防禦，但在這種情況下，啟發式保護是幾個月前使用過去變種的多種特徵、進階的叢集技術和經過我們惡意軟體分析團隊的大量努力，賽門鐵克產品無需任何更新即可阻止這些以前未發現的新 Emotet 變種。

賽門鐵克已提供零時差保護，具體偵測如下：

檔案型(基於回應式樣本的病毒定義檔)防護：

- XLM.Downloader!gen1
- XLM.Downloader!gen2
- XLM.Downloader!gen4
- CL.Suspexec!gen128

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**。