賽門鐵克的郵件安全服務，成功瓦解 Lokibot竊密程式的詭計

2022 年 12 月 22 日發布

多年來，我們已多次發布有關 Lokibot 竊密程式的訊息--最近一次在 12月14日P2。至少可以追溯到 2015 年，Lokibot 透過永無止境的垃圾郵件攻擊行動進行傳播。這些壞蛋為數眾多且水平不一。Lokibot 通常利用附加在電子郵件中的惡意 PDF、RFT 和 Office 檔案作為感染媒介，並使用常見的報價、航運、銀行、SWIFT 外匯轉帳、發票和支付相關的社交工程主旨，Lokibot 試圖從包括瀏覽器在內的數百個應用程式中竊取憑證、FTP 用戶端、電子郵件用戶端、SSH 用戶端、加密貨幣錢包和密碼管理軟體。Lokibot 可能會使用幾種不同的打包工具來進行混淆，但最終必須在執行主要有效籌載之前將自己解壓縮到記憶體，終究還是會被發現。

賽門鐵克持續導入各種先進防護技術來預防及攔阻 Lokibot 的入侵意圖。縱深防禦 (多層次防護) 不僅僅是一個概念，它確實是保護您的組織的唯一方法。攻擊者整天不停歇地尋找您防禦機制中的弱點，即使是相對非頂尖的攻擊者--只要秉持純粹的僥倖或者莫名的好運--最終也會在您的一個或多個防護或流程機制中找到漏洞。但要找到一種能穿越多層防護的方法是一項更具挑戰性的任務。最好的防禦當然是主動防禦，在攻擊發生之前就已經牢固地進行保護。查看過去幾週我們的遙測監控系統清楚地表明多個 Lokibot 垃圾郵件攻擊行動，被賽門鐵克的多層次主動防禦技術所完全攔截，該防護技術集也成功攔截其他不同的威脅家族與種類。

賽門鐵克擁有領先業界的 **零時差** 保護技術，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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Packed.NSISPacker!g14

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)。

表列的檔案型檢測技術不僅適用於我們的電子郵件安全服務 (ESS)，還適用於所有採用我們檔案型檢測保護技術的賽門鐵克產品，包括 Symantec Endpoint Protection (SEP)、Data Center Security (DCS)、儲存保護、伺服器保護、網頁安全雲端服務和網頁安全閘道器 (SWG) 等。

要了解有關賽門鐵克雲端郵件安全服務的更多資訊，**請點擊此處下載我們型錄及簡報檔**。

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**。