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

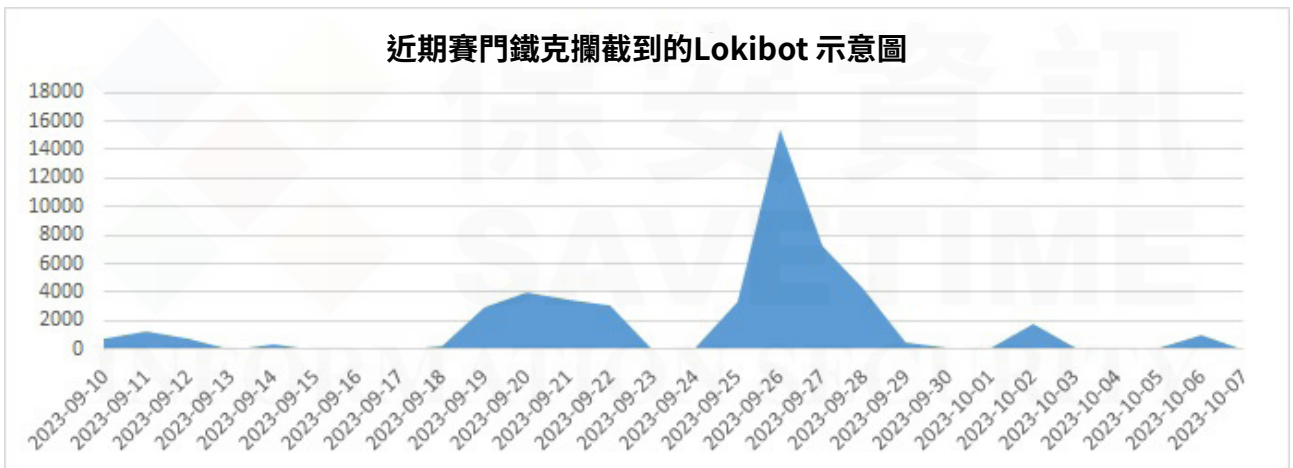
Lokibot仍然是一個危險

2023 年 10 月 10 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

Lokibot 竊密程式的歷史可以追溯到 2015 年左右，至今仍然非常活躍，它透過持續發動一連串的垃圾郵件行動進行傳播，通常利用電子郵件中附加的惡意 PDF、RTF 和 Office 文件作為感染媒介，並使用報價、運輸、銀行、SWIFT、發票和支付相關的社交工程主旨，Lokibot 試圖從數百個應用程式中竊取憑證，包括瀏覽器、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，並可能使用幾種不同的打包方法進行混淆，但最終在執行主要有效籌載之前會將其自身解壓縮到記憶體中，這通常是安全產品會攔截它的地方。

賽門鐵克最近觀察到新的攻擊行動中出現各種主旨的電子郵件，包括報價、付款確認、新合約、採購訂單等。



像往常一樣，電子郵件包含一個附件，可以是壓縮檔案（rar、gz 等）或 Microsoft Office 文件。不論是哪種狀況下，實際的 Lokibot 有效籌載的可執行檔都可以寄生在附件檔裡面。以下範例顯示一封附件包含 .gz 檔案的電子郵件--這是使用 gzip 壓縮技術壓縮的檔案。

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 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer.Lokibot
- Infostealer.Lokibot!12
- Infostealer.Lokibot!16
- Infostealer.Lokibot!22
- Infostealer.Lokibot!34
- Infostealer.Lokibot!43
- Infostealer.Lokibot!gm
- Scr.Malcode!gen59
- Scr.Malcode!gdn32
- Scr.Malcode!gdn34
- Bloodhound.RTF.12
- Bloodhound.RTF.20
- Exp.CVE-2017-11882!g5
- Exp.CVE-2017-11882!g6
- ISB.Downloader!gen60
- ISB.Downloader!gen68
- Web.Reputation.1
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1
- SONAR.SuspBeh!gen667

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：

- System Infected: Bad Reputation Process Request 4

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。
欲瞭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。
欲深入瞭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。

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**。