



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

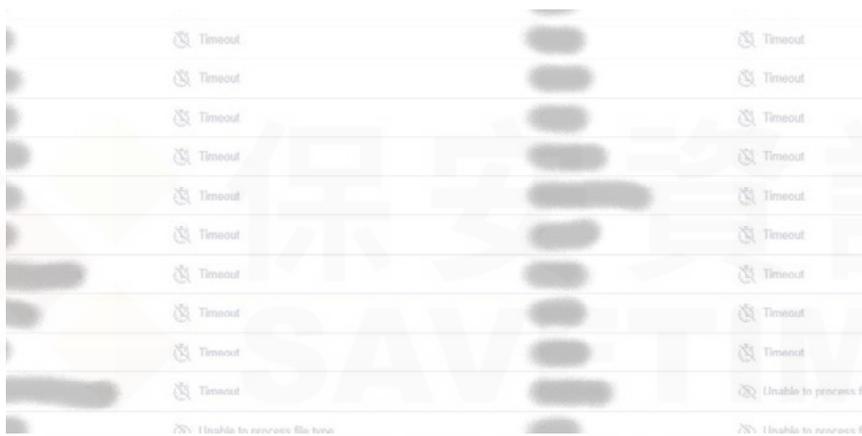
# 『模擬』 Android阻斷服務攻擊 (DoS)

2023 年 5 月 15 日發布

[點擊此處可獲取--最完整的賽門鐵克解決方案資訊](#)

在我們 7x24 的日常工作中，我們會不斷監控異常和跡象，這些異常和跡象可能顯示存在試圖逃避安全檢測的全新威脅或經過修改的威脅。我們的自動化系統最近提醒我們注意一個問題，即在檢測特定 Android 手動安裝包 .APK 的樣本時，我們的雲端掃描明顯變慢。快速瀏覽一下就會發現，幾個有問題的樣本也對更廣泛的自動化掃描系統效能產生輕微影響。

VirusTotal 其他供應商似乎受到的不利影響更大，在分析期間顯示逾時 (Timeout)，這實際上看起來像是一次行動裝置的分散式服務阻斷 (DDoS) 攻擊。



深入研究樣本顯示了以下特性：

- 每個容器樣本都包含大量（最多 32K）、很小的檔案
- 這些很小的檔案包含看起來像隨機字串的內容，並且似乎沒有被 APK 使用
- APK 本身似乎是自動化產成
- 手動安裝包名稱似乎也是隨機自動生成
  - \* hbjvuoxxuhyfbnvxt.d.xgbesgyxslvkkccgozbi.deomdyhhwgeraghfzrds
  - \* dknmmohvktzcmoplths.yrrnbpuvictwiefeycz.gtwxbuikrwakaehwpazg

透過行為分析，我們確定這些 APK 樣本主要是廣告軟體／灰色軟體，和其他可能不需要但不全然是惡意的程式，被統稱為潛在有害程式 (Potentially Unwanted Applications, PUAs)。其中某些連接到遠端伺服器以取得跟廣告相關的設定或與管理推送通知或位置服務的部份軟體開發套件 (SDK) 整合。

迄今為止，我們已經看到超過 11,000 個此類樣本（每個樣本包含超過 30,000 個檔案）。我們相信它們可能是某種測試--因此標題中使用『模擬』這個詞彙--但很難確定這種測試是由安全研究人員，還是有惡意意圖的人士所進行。

學習和適應的能力對於一家安全公司的成功非常重要，我們立即修改我們的自動化程序，以便更有效地分析這些樣本，有效地克服之前觀察到的處理性能下降。

賽門鐵克的端點安全企業版 (SESE)／端點安全完整版 (SESC) 內含防護 IOS／Android 的最先進防護技術，[請點擊此處](#)瀏覽更完整的資訊。

個別的內含在 SES／SESC 賽門鐵克行動裝置威脅防禦型錄最新版下載，[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](http://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, 以及基於比原廠更熟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。

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>