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

STARGate(* 星際之門) 的 Mobile Insight(行動鑑識) 能有效防止惡意 APP 下載到手機

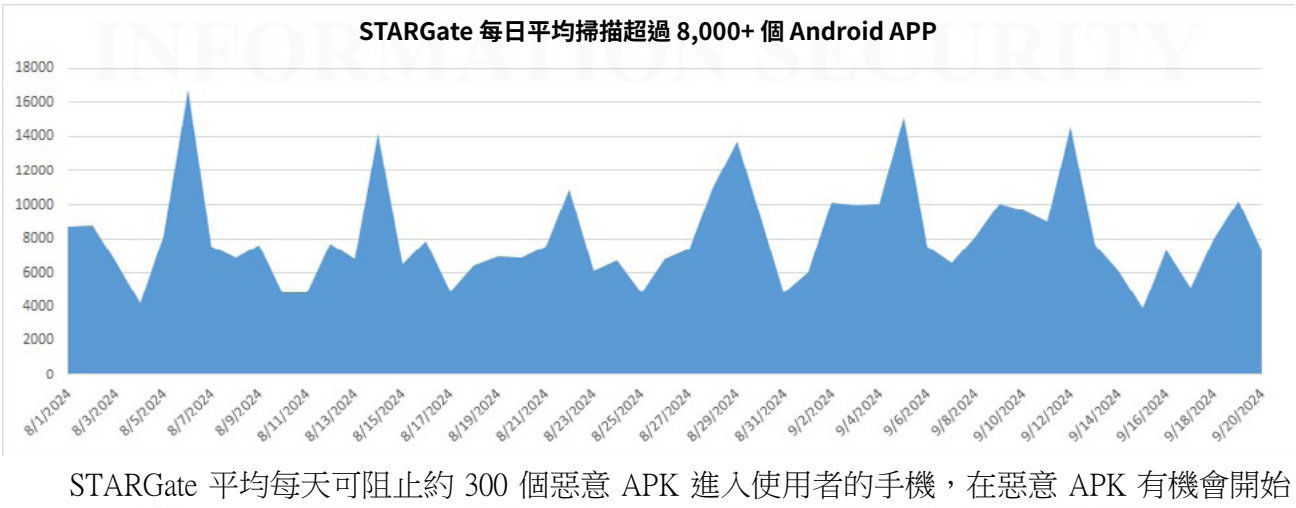
2024 年 10 月 1 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

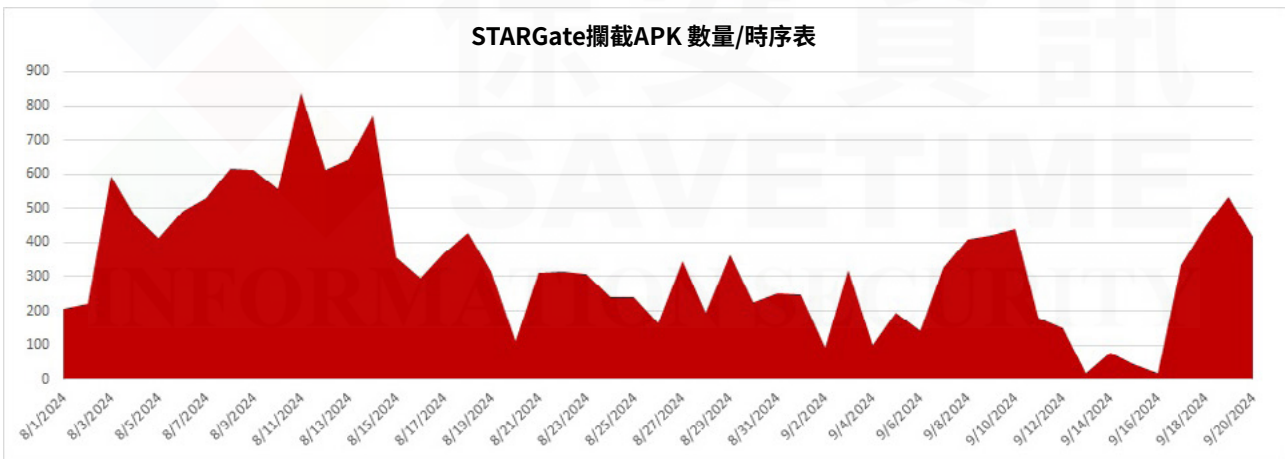
手機與行動裝置上的網路釣魚和 QR 碼／圖碼 (英語：Quick Response Code；全稱為快速回應圖碼) 詐騙正在增加，正如我們在 2024 年 7 月的防護公報中所討論。防止惡意 APP 下載至使用者的手機，可為我們的客戶提供額外且必要的保護層。

STARGate 是一個先進的網路防禦平台，可在賽門鐵克企業產品的廣泛範圍內提供威脅偵測與靜態內容分析。其中 Mobile Insight(行動鑑識) 的功能，可在賽門鐵克產品 (例如：Symantec CloudSOC、Symantec Messaging Gateway 或 Symantec Protection Engine) 的閘道層 (Gateway layer) 上阻止內嵌於 Android Package Kit (APK) 先前未見的手機與行動裝置上的威脅。STARGate 會根據已部署實例的匿名資訊，使用 machine-determined 的機器學習平台特色來識別好或壞的 Android APP。STARGate Mobile Insight 使用與我們的行動威脅防禦系統相同的關係式深度學習解決方案。

目前 STARGate 每日平均掃描超過 8,000+ 個 Android APP，涵蓋及其 Symantec Enterprise 產品。



STARGate 平均每天可阻止約 300 個惡意 APK 進入使用者的手機，在惡意 APK 有機會開始之前就將其阻擋。



Android 行動監視範例

「com.nexipaytoken.app」套件就是這樣一個惡意 Android APP 的範例。此惡意應用程式以「Nexi」品牌自居（Nexiis 是合法的歐洲數位支付解決方案）。一旦部署到用戶的手機上，該應用程式就有能力執行以下動作：

- 連接至指揮與控制 (C&C) 伺服器以接收指令
- 開啟攝影機
- 擷取通話記錄
- 啟動電話通話
- 鎖定裝置
- 開啟系統設定以解除某些安全機制的限制
- 開啟網址並執行自動點選動作
- 下載其他 APP
- 擷取螢幕截圖
- 開啟或解除安裝特定 APP
- 刪除、傳送簡訊至指定的目標號碼
- 顯示覆蓋視窗，有可能模仿合法網頁
- 建立虛假通知

STARGate Mobile Insight 在閘道層將這個 Android 套件識別為 Mobile Spy，防止惡意 APP 下載到使用者的手機。

欲瞭解有關防護亮點：有效抵禦複雜攻擊鏈的威脅情報--STARGate(*星際之門)，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，以及基於比原廠更孰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、可以提供良好諮商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**。