



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

賽門鐵克端點安全行動版，有效防護暗藏在行動APP中的惡意OCR資料滲透

2025年3月25日發布

[點擊此處可獲取--最完整的賽門鐵克解決方案資訊](#)

最近安全研究發現，Google Play 和 iOS App Store 上有超過 20 個 APP 有暗藏惡意 OCR 的技術來擷取和滲透敏感資料，稱為「SparkCat」。這些 APP 會掃描本機和雲端儲存，針對加密金鑰、密碼和財務文件，然後將資料傳送至 AWS 控制的伺服器。

iOS 惡意軟體：複雜的威脅

我們的主要焦點是 iOS，因為它對企業安全有影響。這些 APP 內的惡意框架：

- 當使用者開啟支援視窗時被啟動，允許檔案存取。
- 使用 OCR 掃描檔案，尋找敏感關鍵字，包括加密復原金鑰。
- 將識別出的檔案滲透到由 C&C 基礎架構控制的 Amazon 主機伺服器。

值得注意的是，並非所有的 APP 版本都會受到影響，這顯示是一種供應鏈攻擊，在開發過程中的某個階段被注入惡意程式碼。

為何這項研究引人注目

- 大規模迴避--惡意軟體繞過 Apple 安全審查，在 App Store 上維持一年以上未被偵測到。
- 隱身伎倆--攻擊者利用合法的網路服務來逃避偵測。
- AI 驅動的滲透--機器學習在擷取和傳輸敏感資料的過程中扮演重要角色，顯示行動威脅的複雜性達到新的水準。
- 超越靜態偵測--傳統的安全工具無法偵測到這些威脅，突顯出行為驅動安全方法的必要性。

賽門鐵克如何保護客戶

儘管惡意軟體採取隱蔽方式，賽門鐵克的行動威脅防禦 (MTD) 仍能及早識別並降低威脅：

- 網路完整性政策使用 WebPulse 網頁信譽分析將 C&C 伺服器標示為可疑。
- 不需要的 APP 政策會偵測到試圖滲透敏感資料受感染版本應用程式。
- 以行為為基礎的偵測識別出靜態簽章以外的風險，在公開披露之前標記高風險活動。

有趣的是，在這些行為被大肆報導之前，我們的系統已經在其他應用程式中發現這些行為，最早可追溯至 2024 年 1 月。我們也標記原始研究未涵蓋的受感染應用程式之風險行為，包括攻擊者 AWS 存取金鑰 ID 及嵌入惡意函式庫和框架的秘密金鑰。

持續的風險需要不間斷防護機制

這些應用程式在 iOS App Store 上仍然活躍，如此增加供應鏈攻擊的可能性。然而，開發人員必須整合惡意框架--直接或透過 Xcode 等特洛伊木馬工具。這表示單靠靜態偵測並不足夠；必須動態分析每個應用程式版本的高風險行為。

關鍵要點：僅靠 App Store 的自我審核機制是不夠安全

企業的行動保護需要主動、動態的安全性來防止資料遺失。當威脅的複雜程度和規模持續演進時，僅依賴 Apple 或 Google 的自我審核機制是不夠安全。

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。



關於賽門鐵克 (Symantec)

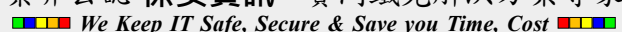
賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom, 美國股市代號 AVGO, 全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED), 特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系, 讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性, 有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者, 致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝, 同時也大大降低交易複雜性。Symantec 持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, 以及基於比原廠更熟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、可以提供良好諮詢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。

業界公認 保安資訊--賽門鐵克解決方案專家


服務電話：0800-381500 | +886 4 23815000 | <http://www.savetime.com.tw>