手機行動裝置上的威脅形勢不斷進化，磨刀霍霍向加密貨幣使用者

2025 年 7 月 29 日發布

隨著加密貨幣市場創下歷史新高，特別針對加密貨幣愛好者和使用者的手機行動裝置上的威脅也大幅增加。詐騙者以各種不同的方式利用人們對數位資產日益增加的興趣。威脅方式可能從簡單的簡訊網路釣魚攻擊 (誘騙使用者洩露機密資料) 到惡意 APP(專門竊取私密金鑰和加密錢包憑證)。

過去這幾年來，攻擊者越來越專注於手機行動裝置，將其視為取得使用者所持加密貨幣的最便捷途徑之一。本公告概述最近一些手機行動裝置威脅的趨勢，以及攻擊者針對行動加密貨幣使用者所採用的技倆。

簡訊網路釣魚攻擊又稱為 Smishing

簡訊網路釣魚攻擊，是指網路犯罪份子利用簡訊服務的文字訊息誘騙手機使用者透露敏感資訊。簡訊網路釣魚攻擊也可能引誘使用者點擊惡意連結，進而導致任意有效酬載的執行。在加密貨幣的世界中，簡訊網路釣魚攻擊已經成為針對加密貨幣使用者最熱門的技倆之一，這主要是由於行動裝置在日常生活中的廣泛使用。在所觀察到的網路釣魚詐騙中，攻擊者通常會冒充合法加密貨幣平台的知名品牌，目的是讓受害者相信訊息的真實性，進而損害他們的加密貨幣資金。

山寨加密貨幣錢包和挖礦 APP

另一種常見導致加密貨幣資產受損的手法是散佈冒充合法供應商的偽造加密貨幣交易所、錢包或挖礦 APP。這些惡意 APP 透過各種途徑，包括直接網路釣魚、第三方 APP 商店、社交媒體上的貼文／廣告或偽裝成合法服務的詐欺網站／儲存庫，傳播給加密貨幣使用者。在行動裝置上安裝後，攻擊者會透過鍵盤側錄技術或冒充受害者熟悉的合法加密貨幣錢包 APP，從特定加密貨幣錢包中竊取憑證。

Crypto-Clipping 惡意軟體

此手機行動裝置上的惡意軟體稱為 Crypto-Clipper，具有截取剪貼簿資料的功能，主要針對加密貨幣的錢包地址。在偵測到使用者複製加密貨幣錢包地址進行交易的活動後，惡意軟體會將其取代為攻擊者控制的地址。在成功取代加密貨幣錢包地址後，加密貨幣會直接轉移到攻擊者的錢包，造成受害者的財務損失。此類惡意軟體通常透過從非官方來源下載、特洛伊木馬或其他假冒的 APP 所散佈。

使用 OCR(光學字元辨識) 技術從影像中擷取資料

行動威脅領域最近一項發展，是惡意應用程式能夠在光學字元識別 (OCR) 技術的協助下，竊取加密貨幣資訊。最近幾種利用 OCR 竊取加密貨幣相關資訊的惡意軟體有 SpyAgent、SparkCat 以及新發現的 SparkKitty。這些惡意軟體變種能夠掃描本機裝置儲存區和雲端儲存庫中的加密貨幣資訊。涵蓋加密錢包憑證、私鑰、恢復短語 (recovery phrase)，甚至是以影像檔儲存的財務文件。一旦有找到，惡意軟體就會運用 OCR 技術從影像檔案中擷取敏感資訊，隨後將其傳送到威脅份子所控制的伺服器。

加密錢包種子短語(seed phrase)的收集成為重點

種子短語 (seed phrase，也稱為恢復短語 (recovery phrase) 或助記詞 (Mnemonic phrase))，助記詞是一組 12、15、18、21 或 24 個單詞 (符合 BIP39 標準)，用來生成私鑰。它是私鑰的可讀形式，方便人類記憶與備份。助記詞可以恢復錢包內的所有私鑰，因此必須妥善保管，不可洩漏。當加密貨幣錢包遺失或無法在之前使用的行動裝置上存取時，種子短語對於復原加密貨幣錢包非常重要。種子短語實際上被視為主備份金鑰，允許完全恢復加密貨幣錢包的存取權。因此，它也需要額外的保護步驟，以隨時保持安全性，例如：建議使用物理離線儲存。但實際上，加密貨幣使用者通常會將種子短語儲存為本機磁碟機上的影像。無論是透過竊取資訊的惡意軟體、社交工程或其他途徑而言，這種高風險的行為大大增加竊取的威脅。Crocodilus 是最近專門針對收集和滲透錢包種子短語的惡意 APP 家族之一。

正在發展的 SIM 卡挾持攻擊／SIM卡交換攻擊 (Sim Swapping) 趨勢

SIM 卡挾持攻擊或稱 SIM 卡交換攻擊 (Sim Swapping) 是一種網路攻擊，威脅者在未經授權的情況下取得受害者電話號碼的控制權。這可以透過誘騙行動電話服務供應商將受害者的電話號碼移植到攻擊者控制的 SIM 卡上來實現。對大多數加密貨幣使用者而言，簡訊傳送的 2FA(雙因素驗證) 是存取加密貨幣交易所和錢包的主要安全機制。當攻擊者取得受害者電話號碼的控制權時，他們可以截取時效性高的 2FA 驗證碼，並取得存取持有其加密資產的錢包之權限。

預載 APP 的危險

正如今年早些時候媒體所報導，未經核准的製造商在低階智慧手機上，預載的惡意 APP 對手機行動裝置上之加密貨幣用戶構成另一個重大威脅。這些裝置經常模仿受歡迎的智慧型手機品牌，甚至採用相似的裝置名稱。例如：最近披露的事件包含模仿流行 WhatsApp 和 Telegram 訊息聊天工具的惡意 APP，一般使用者在購買新手機時很可能不會質疑這些 APP 的存在。交付的惡意軟體能夠竊取敏感的使用者資料，並更改聊天對話中分享的加密貨幣位址。

對照 MITRE ATT&CK 策略和技術知識庫的攻擊鏈

威脅份子利用各種 MITRE ATT&CK 對應的攻擊手法，針對行動加密貨幣使用者進行攻擊，以獲取財務利益，其中一些技術包括：

- 初始存取：應用程式版本控制：T1661--駭客可能會推送更新給先前正常的應用程式，以加入惡意程式碼。
- 初始存取：驅動式惡意入侵：T1456--攻擊者可能會透過使用者在正常瀏覽過程中所瀏覽的網站來存取系統。
- 初始存取：網路釣魚：T1660--攻擊者可能發送惡意的內容給使用者，以存取他們行動裝置。
- 初始存取：SIM 卡交換：T1451--攻擊者可能透過將受害者的電話號碼轉移或交換給他們控制的 SIM 卡及行動裝置，以取得行動裝置的存取權。
- 初始存取：供應鏈入侵：T1474--為了入侵資料或系統，攻擊者可能會在最終消費者收到產品之前，篡改產品或產品交付機制。
- 收集：剪貼簿資料：T1414--惡意使用者可能會濫用剪貼簿管理程式 API，以取得複製到裝置剪貼簿的敏感資訊。
- 收集：輸入擷取：鍵盤記錄 T1417.001--惡意份子可能會記錄使用者的按鍵動作，以便在使用者輸入憑證或其他資訊時擷取這些資訊。
- 收集：螢幕截取 T1513--攻擊者可能使用截取螢幕來收集目標裝置的其他資訊，例如：在前台執行的應用程式、使用者資料、憑證或其他敏感資訊。
- 滲透：透過 C2 頻道滲透：T1646--攻擊者可能透過現有的指揮與控制通道滲透資料，進而竊取資料。
- 影響：資料操控：傳輸資料竄改：T1641.001 T1641.001--為了操控外部結果或隱藏活動，攻擊者可能會更改傳送至儲存庫或其他系統的資料。舉例：Clipper 惡意軟體活動。

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 偵測到的惡意程式名稱及有效對應的防護機制：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- AdLibrary:Generisk
- Android.Reputation.1
- Android.Reputation.2
- AppRisk:Generisk

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

欲了解有關賽門鐵克的重要主機防護系統：Data Center Security(DCS) 更多資訊，請點擊此處。
欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，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**。