113年12月號

公務機密
資訊安全維護

林業及自然保育署
臺東分署

公務機密 資訊安全維護

目錄

安卓惡意軟體FakeCall出現新手法，用戶聯繫銀行的電話會轉介到詐騙人員以便進行後續攻擊

文/周峻佑 | 2024-11-04發表

自2022年卡巴斯基揭露專門透過語音網路釣魚（vishing）從事攻擊行動的惡意軟體FakeCall，過程中駭客會冒充銀行撥打電話引誘受害者上當，提供個人金融資料而受害，如今此惡意軟體的攻擊行動再度升溫，引起研究人員關注。

資安業者Zimperium表示，他們近期發現此惡意程式的攻擊手段出現顯著變化。照理來說，攻擊者藉由網路釣魚引誘安卓使用者下載APK檔案之後，此安裝檔會將第二階段的惡意酬載（即FakeCall）植入受害裝置，從而接收C2命令執行各種誘騙使用者的作業，但研究人員指出，近期的FakeCall出現數種過往未曾出現的做法。

其中一種是名為Screen Receiver的元件，攻擊者藉此監控螢幕為開啟或是關閉，這麼做的目的，就是避免洩露程式碼當中存在的惡意行為。另一種叫做Bluetooth Receiver的元件，也有類似的功能，主要是監聽受害裝置的藍牙連線狀態，但究竟攻擊者會如何運用，目前仍不得而知。

而對於安卓惡意程式頻繁濫用的無障礙服務，新的FakeCall則是更進一步，整合基於Accessibility Service而成的新服務，使得攻擊者不僅能控制操作介面，甚至可從螢幕顯示的內容捕捉機敏資訊。

除此之外，攻擊者也能藉此監控受害者撥打電話的行為，或是指定在特定情況下自動提供權限，甚至能進一步讓攻擊者遠端控制受害裝置。

值得留意的是，這款惡意程式還會尋求使用者授權，設置為預設的撥打電話應用程式，一旦使用者同意，該惡意程式就會在使用者嘗試聯繫金融機構時，重新將通話導向攻擊者控制的詐騙號碼，但在此同時手機仍會顯示用戶撥打的金融機構號碼，從而讓攻擊者有機會騙得受害者的財務資訊，洗劫他們的金融帳戶。

國際警方破獲逾2.2萬個惡意IP，逮捕41名嫌犯

圖片來源:國際刑警組織

文/陳曉莉 | 2024-11-06發表

國際刑警組織（Interpol）周二（11/5）揭露Synergia II行動（Operation Synergia II）的成果，指出已查獲了超過2.2萬個與網路威脅相關的惡意IP，並逮捕41名嫌犯。

Synergia II主要鎖定網路釣魚、資訊竊取及勒索軟體等惡意活動，結合了全球95個國家的執法機構，並與Group-IB、趨勢科技、卡巴斯基與Team Cymru等資安業者合作，藉由資安業者在追蹤非法網路活動上的專業，來識別全球的惡意伺服器。

該行動的期間為今年4月1日至8月31日，Interpol與資安研究人員在這期間，總計發現了3萬個可疑的IP位址，關閉了其中的2.2萬個裝置，確認了逾100名嫌犯的身分，逮捕了當中的41名。其中，香港有1,037個伺服器被關閉，蒙古有一臺伺服器被查扣，澳門也有291臺伺服器被關閉，也涉及馬達加斯加及愛沙尼亞。

樂天信用卡27萬筆個資外洩　工程師盜賣獲利逾4萬被訴

記者 潘千詩 報導
發佈時間：2024/10/09 12:29
最後更新時間：2024/10/09 12:38

28歲吳姓工程師原在台灣樂天信用卡公司服務，涉將公司27萬筆客戶的個資，販售給4名網友，獲利新台幣4萬5985元。台北地檢署今（9）日依涉犯《刑法》妨害電腦使用罪起訴吳男，依《個人資料保護法》起訴4名網友。

檢方調查，吳男於2023年11月14日至2024年2月6日間，趁公司電腦系統汰換報廢、軟體更新、設定等機會，將客戶資料複製並暫存在公司電腦共用資料夾，再寄到私人電子郵件信箱，並在臉書刊登「我持有銀行個資，意者私訊」訊息，吸引2名羅姓及王姓、柳姓共4買家。

檢方還發現，吳男涉利用過去曾從事協助貸款送件業務，取得3客戶身分證及健保卡影本，利用電腦軟體將客戶證件變造成自己的大頭照。經樂天公司內部稽核時發現此事，即報警處理，警方循線查獲。

圖為台灣樂天信用卡玫瑰金卡。（圖／翻攝自樂天信用卡臉書）

每月一常識

新版個人資料保護法與過去有很大的不同，新法進一步擴大了個人資料的保護範圍，並且讓所有產業一體適用；新法甚至首度增加團體訴訟，而且違法的罰則也加重了，企業老闆要負更大的責任。接下來，我們以60個Q&A，快速帶你認識新版個人資料保護法

Q8 個資法規範哪些個人資料的運用行為？

A 個資法規範個人資料蒐集、處理及利用，從資料蒐集開始，以至資料的處理、利用，整個過程都必須符合個資法的規定，確保不侵犯個人隱私權，以及合理使用個人資料。

文/iThome

氣炸鍋也會監視？外媒曝：中國製廚具會將個資回傳

2024/11/11 13:02

英國媒體報導，一個消費者倡議組織警告，有些氣炸鍋可能將敏感個人資料傳輸到中國；倡議人士說，這種廣受歡迎的廚房器具正引發愈來愈多隱私疑慮。

「每日電訊報」（Daily Telegraph）日前報導，英國消費者倡議組織「選哪個？」（Which?）研究員發現，中國製氣炸鍋會將資料傳回在中國的伺服器。與這些氣炸鍋相關的智慧型手機應用程式（APP）也企圖在缺乏明確理由的情況下取得錄音許可。

這個組織發現，資料蒐集「常常超過產品發揮功能所需的必要範圍」。

這個組織測試了中國小米、Aigostar、Cosori等公司製造的氣炸鍋，發現小米和Aigostar用來遠端控制氣炸鍋的手機應用程式都將個資傳到中國。這些應用程式在隱私政策中表明了資料蒐集一事。

「選哪個？」表示，小米的智慧家庭應用程式可與其氣炸鍋連線，曾企圖連結社群媒體臉書（Facebook）和TikTok的數位追蹤器。

Aigostar的應用程式也企圖取得用戶性別和生日等個資。

上述3款連線應用程式都企圖取得用戶的精確位置和錄音許可。

根據利茲海德食品研究（Leatherhead Food Research）資料，目前約半數英國家庭有氣炸鍋。

美國共和黨籍聯邦參議員克魯茲（Ted Cruz）去年警告，許多消費者不知道自己的廚房器具可能會蒐集哪些個資。

他說：「我不認為美國人民希望氣炸鍋蒐集他們的資料…他們至少有權知道氣炸鍋是否在監視他們。」

2021年，總部位於美國的網路設備公司思科（Cisco）的安全研究員發現，Cosori網路連線氣炸鍋有漏洞，可讓駭客遠端控制，但這個缺陷後來獲得解決。

小米發言人告訴「選哪個？」，其智慧家庭應用程式雖試圖取得錄音許可，但這「不適用於小米智慧氣炸鍋，因為它不直接透過語音指令和視訊聊天來運作」。

Cosori發言人說：「我們將隱私視為優先要務，按照我們的內部合規要求，智慧型產品必須遵守通用資料保護規則（GDPR）。」
Aigostar則未置評。