

永遠走在最前面
Always Ahead



淺談智慧型手機資安

掌握先機 即時回應

中華電信資訊技術分公司



大綱

一. 近年智慧型手機安全議題

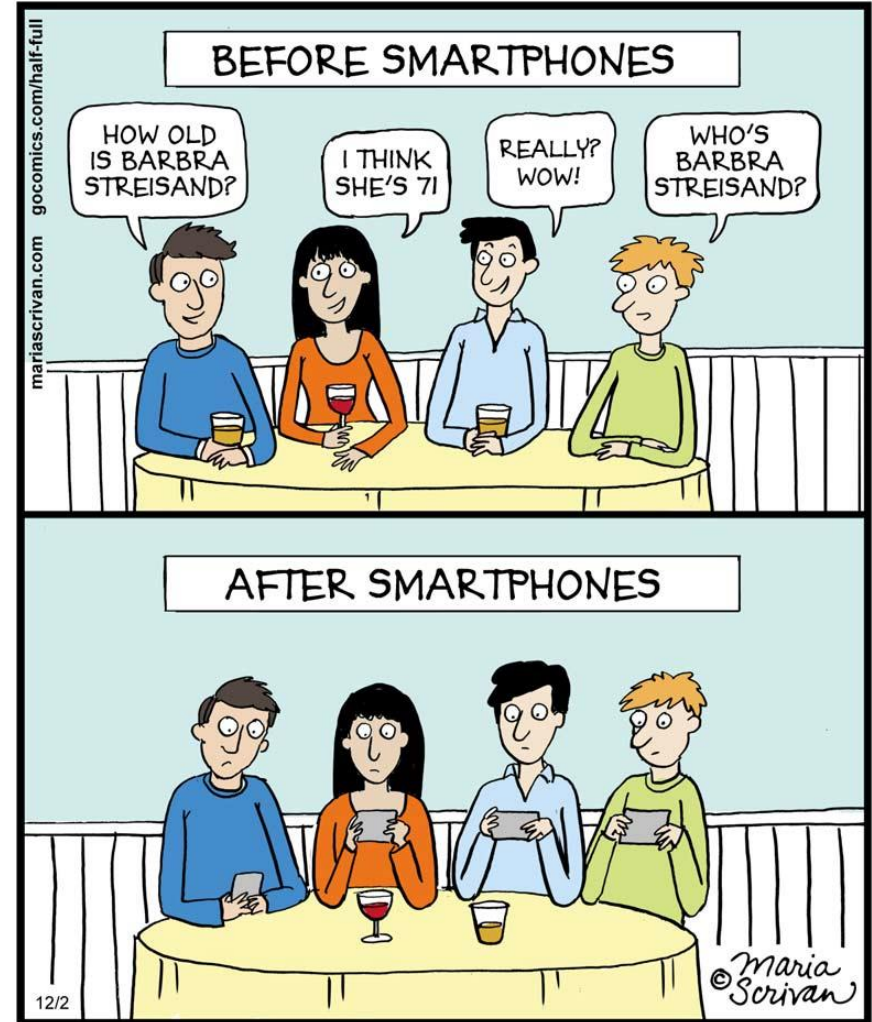
- Android
- iOS

二. 行動支付與其安全性

三. 行動裝置安全強化

四. 結語

幾張圖說明行動裝置帶來的改變



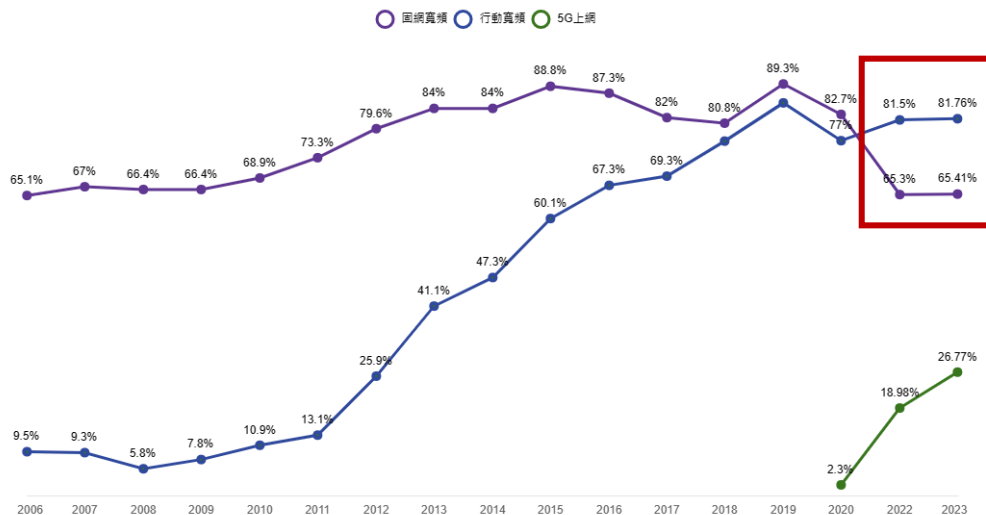
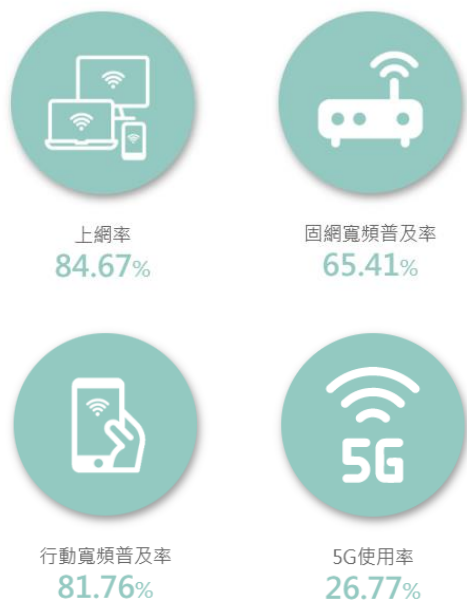
台灣民眾上網率高

TWNIC 2023 台灣網路報告指出

- 18歲以上民眾上網率為 **84.67%**
- 使用行動寬頻上網的比例約為 **81.76%**
 - 行動寬頻的普及率已超越固網寬頻
- 唯行動上網(mobile-only)族群佔 **18.76%**

固網和行動寬頻普及率歷年趨勢

比較2006至2023年的固網寬頻與行動寬頻普及率之歷年趨勢，繼2022年行動寬頻用戶普及率首度超越固網寬頻用戶普及率，今年度兩者的增長率皆大致持平，穩定維持行動寬頻普及率高於固網寬頻普及率的態勢。



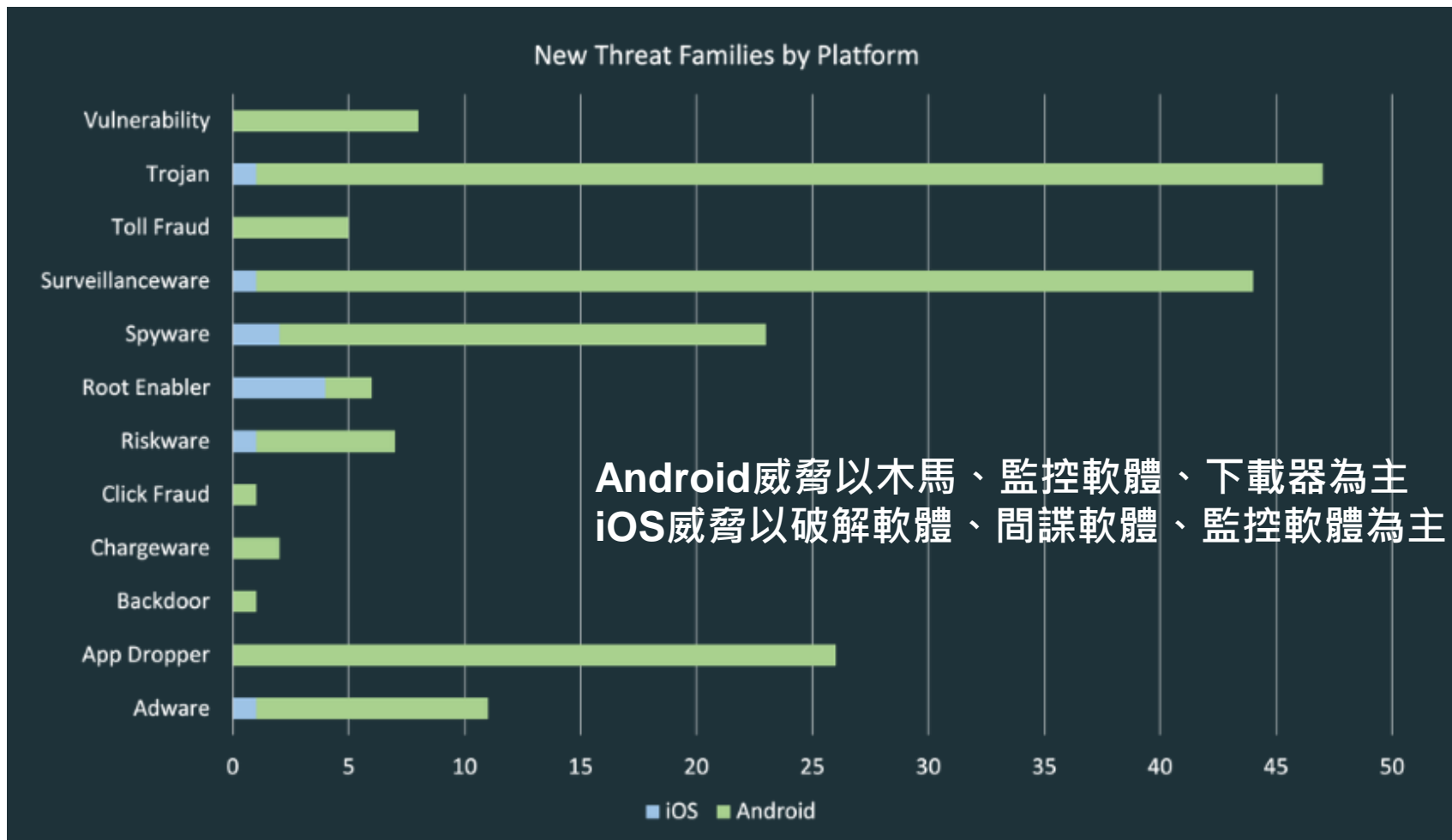
資料來源：2006至2023台灣網路報告，註：本次調查對象為18歲以上民眾；2020及往年調查對象為年滿12歲以上民眾。

資料來源: TWNIC

一、近年智慧型手機 安全議題

- 預估現今全世界有**48.8億人**使用智慧型手機
 - 以全球**80億**人口計算，約占**61%** (Oberlo, 2024)
- 潛在性的資安弱點
 - 2023偵測到**130萬支**行動惡意安裝程式(Kaspersky, 2024)
 - 其中**15.4萬支**為行動銀行木馬(Mobile Banking Trojan)
 - 每分鐘有**113部**手機遺失或被竊(worldbackupday.com, 2024)
- 不安全的App
 - 6500支熱門App中，有**95%**無法通過OWASP MASVS (Mobile Application Security Verification Standard) 安全性標準 (NowSecure, 2023)
 - 54% 網路問題 (App與後端平台通訊可能被竊取)
 - 47% 平台問題 (App間資料交換可能被竊取)
 - 43% 程式問題 (開發時輸出入未妥善驗證、使用不安全的第三方函式庫、未套用程式語言或行動作業系統所提供的安全機制)

2023 Mobile Threat Landscape



資料來源: Lookout



首先看看Android陣營

2022/02 BRATA銀行木馬再現

Android銀行木馬BRATA再度現身，先騙走錢財再重置受害者手機

在2019年被發現的Android銀行木馬BRATA，自去年11月底又開始活躍，資安業者Cleafy在1月24日公布研究，指出發現3個變種，感染區域擴及全球更多國家，其散布主要透過簡訊，誘用戶下載假垃圾郵件防護App

文/ 林妍濤 | 2022-01-26 發表

讚 6.8 高 按讚加入iThome粉絲團 讚 29 分享

安全廠商Cleafy近日發現，一隻名為BRATA的Android木馬程式，除了會騙取用戶銀行帳戶存款外，還會藉由重置用戶手機來躲避偵查。

BRATA為Brazilian RAT Android最初是2019年卡巴斯基發現，因流竄於巴西，針對Android用戶的RAT (remote access trojan) 程式而得名。但之後它擴大到美國及西班牙等地。Cleafy研究人員去年11月起再度偵測到BRATA活動，除了拉丁美洲、義大利等原有區域，並新增英國、波蘭，此外西班牙及中國也有零星個案。

這波感染中，BRATA是透過簡訊誘使用戶下載防護垃圾郵件軟體，而安裝到用戶手機上。這波BRATA活動有3個變種。分析BRATA，研究人員發現在最常見的變種中，惡意程式作者新增了多項新功能，包括回復手機出廠設定、GPS定位、和C&C伺服器之間使用多重傳輸通道 (HTTP、TCP)，以及透過VNC (Virtual Network Computing，具遠端操作及螢幕分享) 及鍵盤側錄功能擷取用戶銀行帳戶密碼等資訊。

為了突破手機既有安全防護，例如限制App存取權限，因此在安裝時，BRATA誘使用戶同意數項權限，包括取得手機輔助服務 (Accessibility Services) 以啟動VNC、蒐集GPS定位紀錄及回復手機出廠設定並刪除裝置所有資料。研究人員指出，回復出廠設定是這隻惡意程式的kill switch功能；當駭客完成匯款，或是發現防毒軟體偵測時，攻擊者即可遠端執行，目的在刪除所有資料以消滅跡證。

事實上已有兩起受害者手機遭到重置，在資料被刪除後受害者即使發現戶頭短少也完全無從追查原因。

最後，BRATA的多重傳輸通道功能則讓它先以HTTP協定和C&C伺服器建立連線、驗證並刪除裝置上的防毒App，再轉換到更有效的WebSocket協定，以便持續從C&C伺服器接收檔案或將蒐集到的手機資訊傳給攻擊者。

常見BRATA木馬APP Icon



BRATA Downloader幾乎不會被防毒引擎偵測(2022/01)



側錄銀行APP操作



資料來源: iThome, Cleafy

2022/03 TeaBot入侵Google Play

TeaBot金融木馬溜進Google Play, 這次它假冒為條碼掃描器

駭客將良性程式QR Code & Barcode Scanner上架到Google Play後, 再要求完成下載的用戶立即更新程式並提供無障礙服務權限, 以於裝置上植入金融木馬TeaBot竊取超過400種程式的登入憑證

文/ 陳曉莉 | 2022-03-02 發表

讚 6.8萬 按讚加入iThome粉絲團 讚 139 分享

資安業者Cleafy本周揭露, 於2021年5月現身的金融木馬程式TeaBot已成功溜進Android的官方程式市集Google Play, 這次它假冒為條碼掃描器QR Code & Barcode Scanner, 並已被下載逾1萬次。

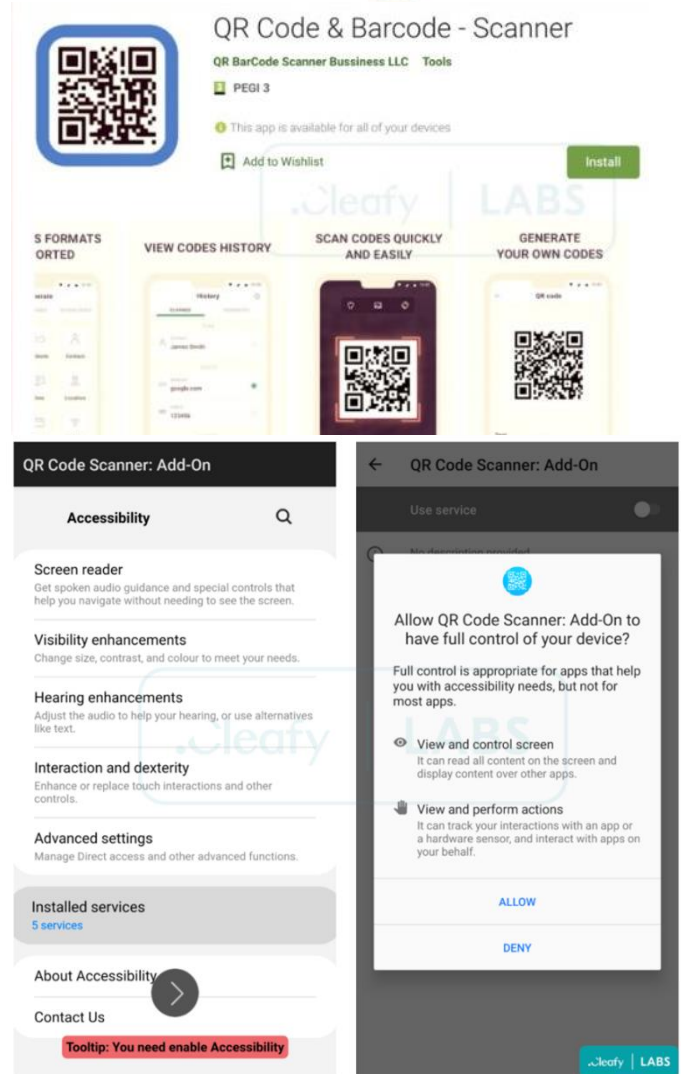
TeaBot之前主要的感染途徑為簡訊網路釣魚, 發送大量的垃圾簡訊以誘導使用者下載假冒為VLC Media Player、DHL或UPS等品牌的程式, 但這些程式都是進駐在第三方的Android市集, 不過, 今年2月才發現的新版TeaBot, 偽裝成條碼掃描器, 成功溜進了Google Play, 由於具備完整的掃描功能, 因而評價良好, 下載量已超過1萬次。

Cleafy指出, Google Play上的QR Code & Barcode Scanner是個良性程式, 但在安裝之後, 它立即會要求使用者進行更新, 而這便是駭客所偽造的更新程序, 以遞送TeaBot。該程式的更新並非直接來自Google Play, 而是要求使用者下載與安裝另一個存放於GitHub上的QR Code Scanner: Add-On程式。

一旦使用者執行了此一偽造的更新, TeaBot便會啟動安裝程序, 要求使用者賦予無障礙服務 (Accessibility Services) 的權限, 以便讓TeaBot得以檢視與控制螢幕, 以及檢視與執行行動, 前者可用來竊取使用者於螢幕上輸入的憑證, 後者則是用來方便駭客執行惡意行為。

新版的TeaBot除了散布方式進化之外, 也擴大了攻擊目標, 從原先鎖定的60個目標, 增加到超過400個, 除了銀行程式之外, 亦囊括保險程式、加密貨幣錢包, 以及加密貨幣交易中心等, 此外, 它還擴充所支援的語言, 能以英文、中文、俄羅斯文或斯洛伐克語來執行安裝說明。

Cleafy提醒, 有鑑於TeaBot透過官方的Google Play散布、僅要求少數的授權, 再加上它是利用之後的更新程序安裝惡意程式, 使得它不僅不會引起使用者的懷疑, 也經常能躲過防毒軟體。值得注意的是, 此一被Cleafy點名的條碼掃描程式依然存在於Google Play上, 不確定Google是否已收到Cleafy的通知。



資料來源: iThome, Cleafy

2022/03 防毒軟體暗藏木馬

安卓用戶快刪除！4款防毒軟體App 暗藏新型惡意木馬病毒、搬光你的錢

2022/03/06 16:51

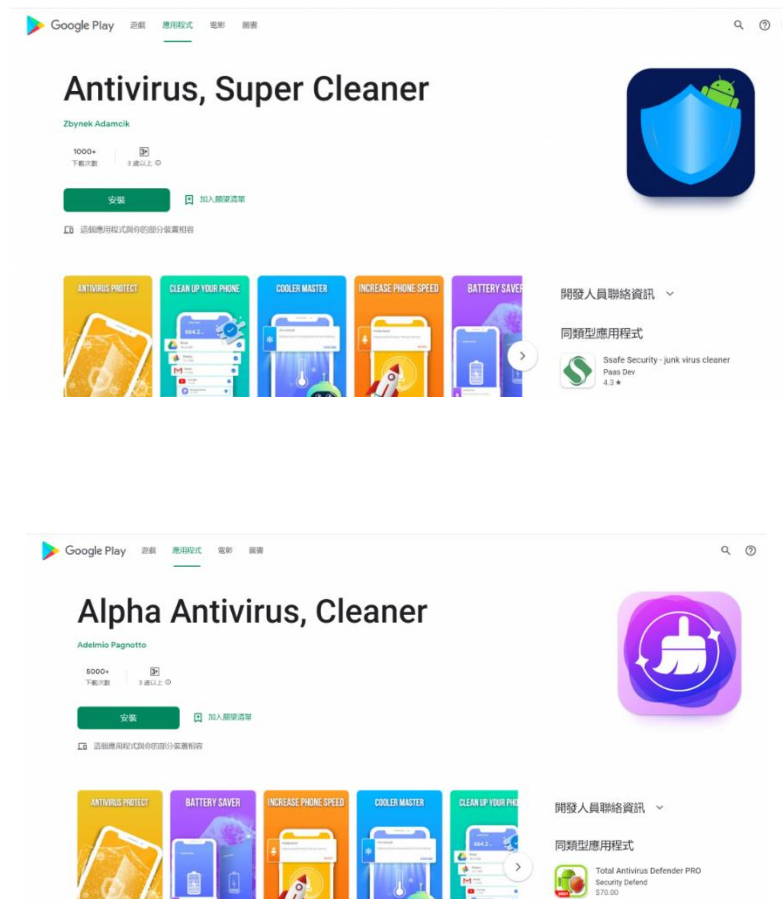
文 / 記者劉惠琴

來自英國網路安全公司NCCGroup 發佈的研究報告，近期發現在Google Play商店平台一款名為「SharkBot」的新型態 Android 惡意木馬病毒出沒，實際上卻是有後門的銀行木馬程式。採用非常狡猾且複雜又陰險的手法，利用隱身在多個假冒為手機防毒軟體的應用程式內，吸引用戶下載，並藉此繞過 Google Play 的安全審查機制。

安卓手機用戶若一旦在不知情的狀況，下載這些已被植入「SharkBot」木馬病毒的應用程式後，裝置就有可能遭受感染，不但能側錄手機鍵盤輸入的資料，攔截手機收到的簡訊內容，甚至還會竊取手機憑證與登錄網銀的憑證，從遠端取得手機裝置系統的權限，並進一步在背後裡，從用戶手機已下載的網路銀行App，暗中透過一套具有啟動自動轉帳匯款功能的系統，趁機搬移用戶銀行裡的存款，牟取不法獲利。

目前已知夾帶有「SharkBot」木馬病毒的四個特定應用程式的名稱，分別為：Powerful Cleaner, Antivirus (下載次數破5萬)、Atom Clean-Booster (下載次數破5千)、Antivirus, Super Cleaner (下載次數破1千)、Alpha Antivirus, Cleaner (下載次數破100)。上述這四款應用成的最新更新日期，於Play商店網頁畫面皆顯示為2022年2月10日，且應用程式簡介資料所用的截圖還全都一模一樣。且截至記者發稿前，這些帶有惡意病毒的應用程式，仍未被Google Play商店強制下架。

安全研究人員建議Android用戶，若曾經在Google Play商店下載過上述這些假冒版的防毒軟體App，務必盡快確認已從手機裝置刪除卸載。不要盲目地相信在Play商店上的應用程式都是沒有安全疑慮與風險，若想要為手機安裝病毒軟體，盡可能地以具有知名度的廠牌為優先考量。



資料來源: 自由時報

2022/03 FB登入憑證竊取程式

可用來竊取臉書憑證的Android程式已被安裝在逾10萬臺裝置上

曾成功上架Google Play一段時間的Craftsart Cartoon Photo Tools暗藏木馬，在安裝過程會出現臉書登入畫面，以誘騙使用者輸入帳密

文/ 陳曉莉 | 2022-03-22 發表

讚 51 分享

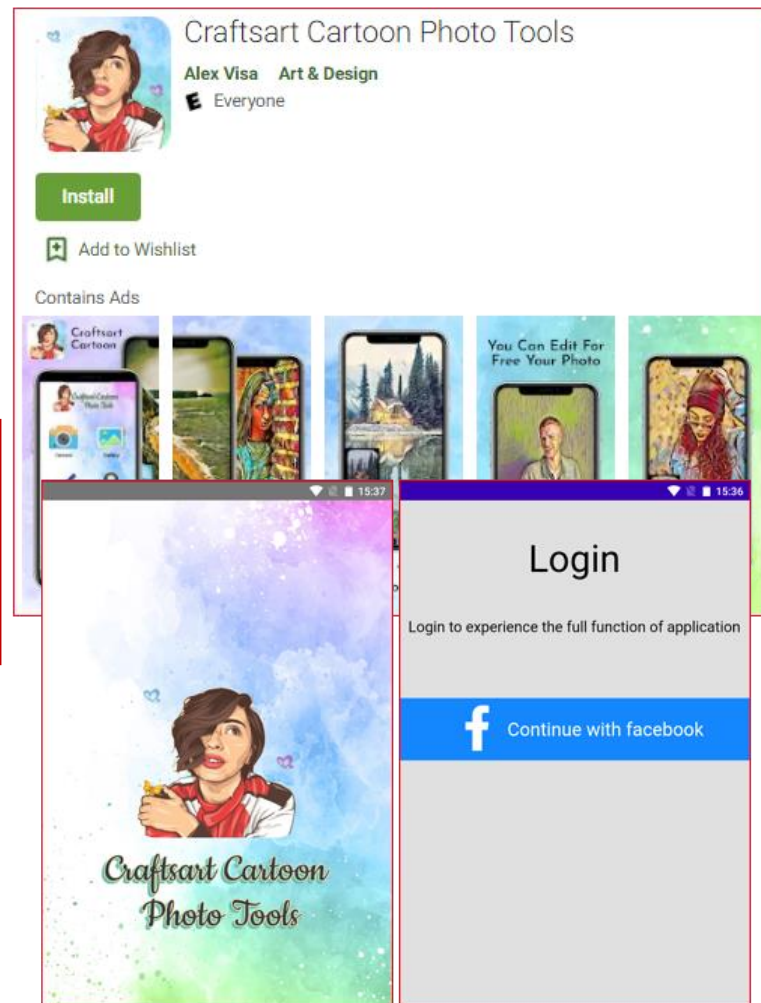
行動資安業者Pradeo本周指出，Google Play上陳列了一款專門用來竊取臉書憑證的惡意程式，該程式的名稱為Craftsart Cartoon Photo Tools，號稱可協助使用者將照片編輯成卡通人物，且已有超過10萬臺Android裝置安裝它。

Pradeo表示，Craftsart Cartoon Photo Tools被嵌入了名為Facestealer的Android木馬程式，當使用者下載並安裝它時，它即會出現臉書的登入畫面，在使用者輸入臉書帳號與密碼時，即將此一憑證傳送到由駭客控制的C&C伺服器。

取得臉書憑證的駭客得以存取受害者的臉書機密資訊，並利用它們來進行金融詐騙、傳送網釣連結或散布假新聞。

至於駭客所掌控的C&C伺服器則是於俄羅斯註冊的網域，且該網域名稱已被使用7年，且與許多惡意行動程式有所關連。

Pradeo在3月21日揭露此事時，該程式仍存在於Google Play上，但截稿時Google已將它下架。曾安裝該程式的使用者除了應儘快將它移除之外，也應該要重設臉書密碼，以取回臉書帳號的控制權。



資料來源: iThome, Pradeo

2022/07 微軟揭露詐騙程式手法

微軟揭開Android收費詐騙程式的面紗

微軟發表有關Android收費詐騙程式 (Toll Fraud) 的研究報告，指出它雖然是Google Play上市占率第二高的惡意程式，卻鮮少有業者分享相關資訊，使得該團隊決定揭露收費詐騙程式的手法，以及如何辨識及預防

文/ 陳曉莉 | 2022-07-01 發表

讚 507 分享

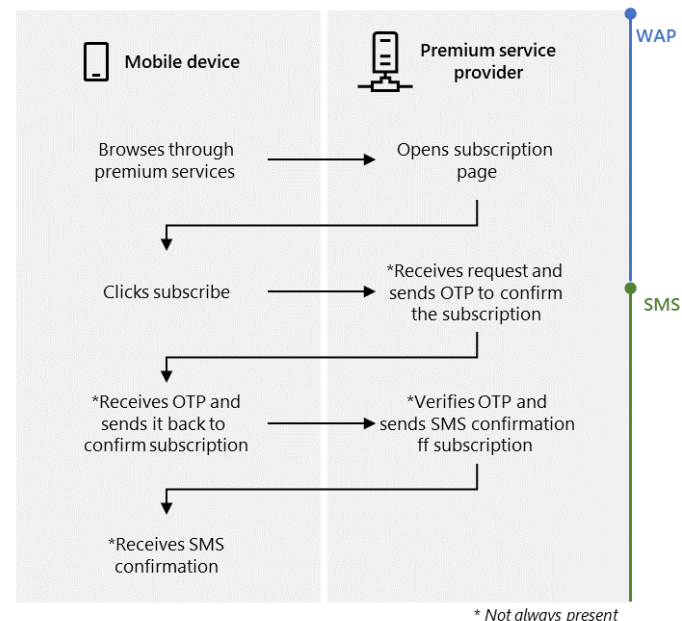
Google在2017年至2019年間，總計自Google Play上移除了1,700款含有Joker惡意程式的Android程式，Joker即為收費詐騙的惡意程式家族，根據Google今年第一季的統計，在Google Play上出現的惡意程式中，最多的是占了47.3%的間諜程式，其次即是收費詐騙程式，占了34.8%。

收費詐騙的手法一般是鎖定特定的電信網路，將使用者導向一個訂閱網站，並按下訂閱，之後按月由使用者的電信帳單付款，這中間使用者幾乎都是毫無察覺的，一直到發現帳單上的異樣。

Microsoft 365 Defender團隊說明，駭客通常是利用無線應用通訊協定 (Wireless Application Protocol, WAP) 來展開收費詐騙，WAP是個付款機制，讓消費者可訂閱網站服務並透過電信帳單付款，詐騙手法始於必須讓使用者透過電信網路連至提供付費服務的網站，之後使用者還必須點擊訂閱按鍵，有時會收到必須回傳給電信業者的一次性密碼以確認訂閱，但有些電信營運商則不要求使用者回傳一次性密碼。

因此，駭客會想辦法關閉手機的Wi-Fi連線或等待使用者切換至行動網路，再偷偷地連至訂閱頁面，藉由程式自動點擊訂閱按鍵，攔截系統傳送的一次性密碼，再將密碼回傳給電信營運商，並取消訂閱的簡訊通知。這一連串的手法有些複雜，但並非無法辦到。

而為了進駐Google Play，駭客經常使用熱門類別且方便植入木馬的開源程式，例如桌布程式、通訊程式或編輯程式等，而且一開始上傳至Google Play上的版本是乾淨的，直到下載量達到一定的數目，之後便藉由更新機制動態地載入惡意程式碼，同時還會刻意區隔原本程式與惡意流量，以避免被偵測。



微軟建議收費詐騙預防之道：

1. 避免自不可靠來源下載安裝App
2. 不隨意提供簡訊、存取系統通知欄位，或是存取無障礙服務的授權
3. 下載前最好先瀏覽該App的評論
4. 安裝惡意程式偵測方案
5. 裝置過保/失去安全更新時考慮換機

資料來源: iThome, 微軟

2022/11 螢幕鎖定繞過漏洞



device is locked

2022/12 3款App藏有資安漏洞

ETtoday新聞雲 > 3C家電

2022年12月06日 21:17

3C家電

3C焦點

家電

筆電相機

手機平板

遊戲APP / 科技生活

快刪除！3款APP藏資安漏洞 逾200萬用戶 恐被「遠端竊個資」

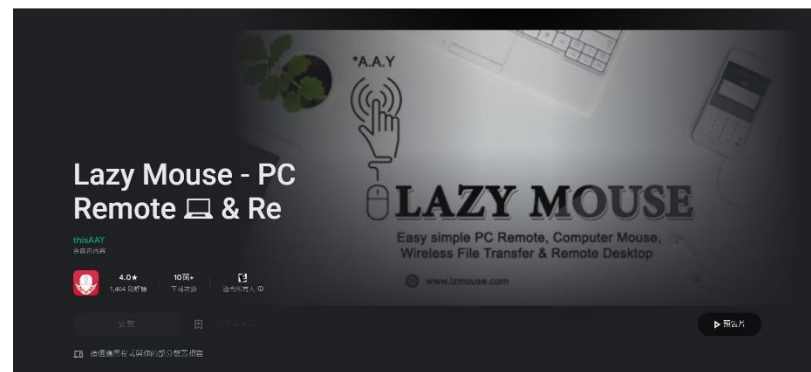
記者閔文昱／綜合報導

美國新思科技 (Synopsys) 的網絡安全研究中心 (CyRC) 近期調查發現，有3款可在Google Play商店下載的APP存在嚴重缺陷問題，導致這些APP用戶的敏感個資恐被駭客輕易竊取。目前這3款APP在Google Play的下載量已超過 200 萬次。

綜合外媒報導，被查出有資安漏洞的APP分別為「Lazy Mouse」、「PC Keyboard」以及「Telepad」，這3款應用程式都屬工具類APP，Android用戶下載後可透過手機遠端操控電腦的鍵盤或滑鼠。目前3款APP仍被廣泛使用，CyRC雖已多次聯繫3款APP的開發者，但都還未收到回覆。

CyRC表示，根據調查發現，3款APP的身份驗證機制薄弱，且含有不安全的通信漏洞，讓駭客能夠輕易從APP中查看用戶在電腦輸入內容，藉此盜取密碼等個資，目前已知有資安問題的版本為Telepad 1.0.7 及更早版本、PC Keyboard 30 及更早版本、Lazy Mouse 2.0.1 及更早版本。

另外，CyRC還發現，這3款APP總共有多達7個資安漏洞，其中4個的CVSS漏洞危險程度評分高達9.8分（滿分 10 分），其餘3個則為5.1 分，而3款APP都已超過2年沒更新，意味著開發人員似乎無意解決這些問題，因此CyRC也呼籲，有下載這3款APP的用戶盡快刪除，以免個資被盜用。



CyRC Vulnerability Advisory: Remote code execution vulnerabilities in mouse and keyboard apps

Posted by [Mohammed Alshehri](#) on Wednesday, November 30, 2022

CVE-2022-45477, CVE-2022-45478, CVE-2022-45479, CVE-2022-45480, CVE-2022-45481, CVE-2022-45482, CVE-2022-45483 are remote code execution vulnerabilities in three popular mouse and keyboard apps.

Overview

The Synopsys Cybersecurity Research Center (CyRC) has exposed multiple vulnerabilities in three applications that enable an Android device to be used as a remote keyboard and mouse for their computers.

Lazy Mouse, Telepad, and PC Keyboard are keyboard and mouse applications that connect to a server on a desktop or laptop computer and transmit mouse and keyboard events to the server. The free and paid versions of these three apps have a combined total of more than two million downloads from Google Play.

資料來源: Etoday, Synopsys

2023/04 變色龍Android惡意軟體

新發現的「變色龍」Android 惡意軟體，會假冒為銀行、政府、加密貨幣 App

◎發布日期：2023-04-21

字型大小： 小 中 大   

發布單位:TWCERT/CC

更新日期:2023-04-21

點閱次數:2419

資安廠商 Cyble 旗下的資安研究人員，近日新發現一個 Android 惡意軟體「Chameleon」；這種惡意軟體會假扮成銀行、政府單位或加密貨幣交易所發行的 App，用以對使用者發動各類駭侵攻擊。

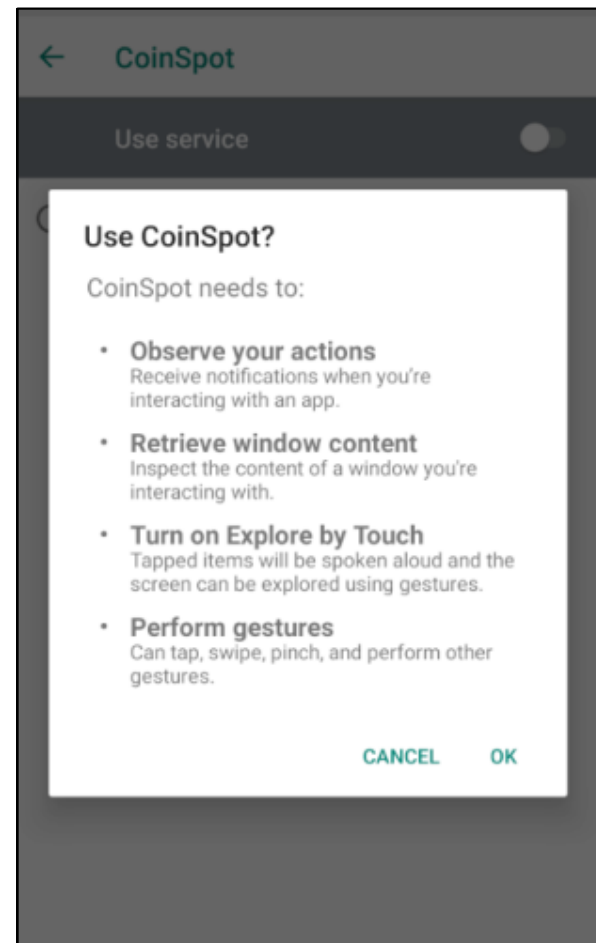
據 Cyble 資安專家指出，Chameleon 鎖定波蘭與澳大利亞境內的 Android 行動裝置使用者發動攻擊，目前已假冒為澳大利亞某政府單位、波蘭 IKO 銀行與 CoinSpot 加密貨幣交易所。

報告也說，Chameleon 會在執行時進行多種檢查，以逃避各種資安防護軟體與機制的偵測。舉例來說，Chameleon 會檢查感染的 Android 裝置是否已經 root (越獄) 或開啟 debug 模式，以防遭分析人員執行。

如果感染的環境是「正常」的，Chameleon 會要求使用者授予多種輔助使用權限，並且停用 Google Play Protect 保護機制，也不讓使用者自裝置中刪除該 App；接著 Chameleon 會連線到其控制伺服器，傳送受感染裝置的版本、型號、Root 狀態、所在國家、精確地理座標等資料。

接著 Chameleon 會決定要假扮成哪種服務，在前景中以 webview 開啟該服務真實的 URL，載入其網站內容，但在背景載入惡意程式碼，以執行各種惡意功能，包括竊取 cookie、執行鍵盤輸入內容錄製程式、注入釣魚網頁內容、竊取手機解鎖密碼或手繪圖樣、竊取透過簡訊傳來的單次有效密碼，以通過二階段登入驗證等等。

建議 Android 用戶在下載安裝任何 App 時，應只從 Google 官方 Play Store 挑選評價優良的正版軟體下載，勿自任何第三方應用程式商店或不明來源連結下載任何應用程式。



資料來源: TWCERT/CC, Cyble

2023/05 手機出廠前已被感染

ETtoday新聞雲 > 3C家電

2023年05月23日 13:52

3C家電

3C焦點

家電

筆電相機

手機平板

遊戲APP / 科技生活

安卓手機要注意 報告：近900萬支手機出廠前就感染惡意病毒

記者陳俐穎／綜合報導

資安公司趨勢科技最新調查發現，50個不同品牌的多達890萬部手機在出廠前就感染了惡意軟體。安全公司Sophos的研究人員將這個惡意軟體命名為「Guerrilla」，除此之外，也在Google Play中的15個App中發現此軟體。

Guerrilla打開一個後門，使受感染的產品定期與遠程命令和控制服務器通訊，以檢查是否有任何新的惡意更新可供它們安裝，能夠收集有關用戶的數據。

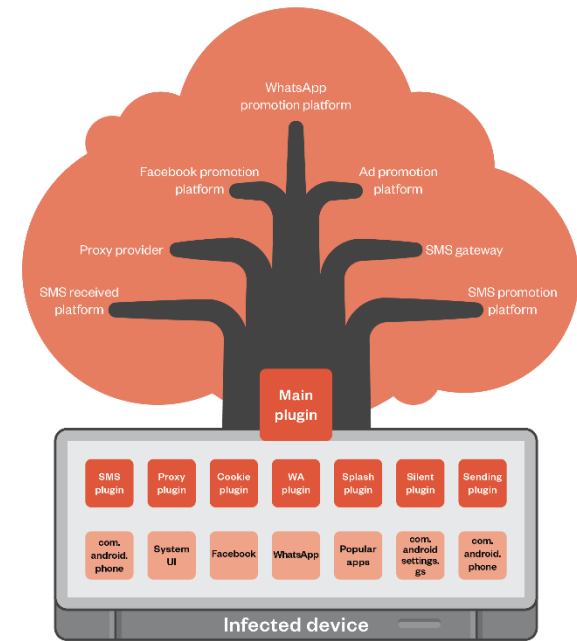
趨勢科技稱這些惡意軟體的背後操作者為「Lemon Group」，他們會將這些數據出售給廣告商。Guerrilla會在用戶的裝置上偷偷安裝廣告，這些軟體就會讓用戶的手機耗盡電池並降低用戶體驗。

趨勢科技研究人員表示，這些惡意團夥，主要涉及大數據、營銷、廣告公司做的一些業務，主要業務涉及大數據的利用，分析海量數據和相應的廠商出貨特徵，從中獲取不同的廣告內容。不同時間不同用戶，數據配合詳細軟體推送。

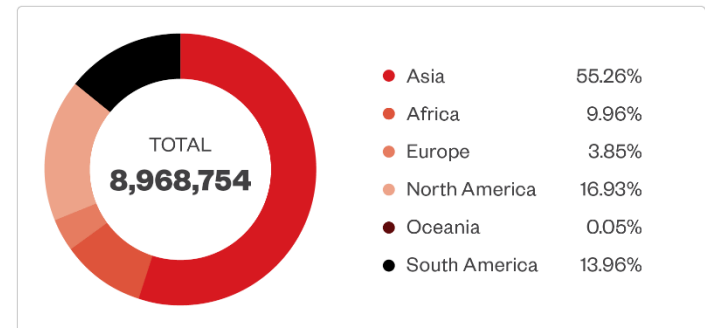
目前受感染手機最集中的國家是美國，其次是墨西哥、印度尼西亞、泰國和俄羅斯，不過目前趨勢科技沒有確定受影響的品牌。

第二份報告由TechCrunch發布，報告中提到，透過亞馬遜銷售的幾款Android電視盒，都帶有惡意軟體。據報導，這些電視盒是帶有h616的T95型號，向命令和控制服務器報告，就像Guerrilla服務器一樣，可以遠端安裝想要的任何應用程序。此款惡意軟體稱為clickbot。它會在後台偷偷點擊廣告來產生廣告收入。

Cybercriminal Business on Infected Devices



©2023 TREND MICRO



©2023 TREND MICRO

資料來源: Etoday, 趨勢科技

2023/05 畫面錄影App成監聽工具

● 應用軟件 應用軟件 Android App

保安公司警告 Android 畫面錄影程式 更新後成 黑客監聽工具

作者
唐美鳳

發佈日期
2023-05-28

閱讀時間
3分鐘

字體大小
A A A

分享

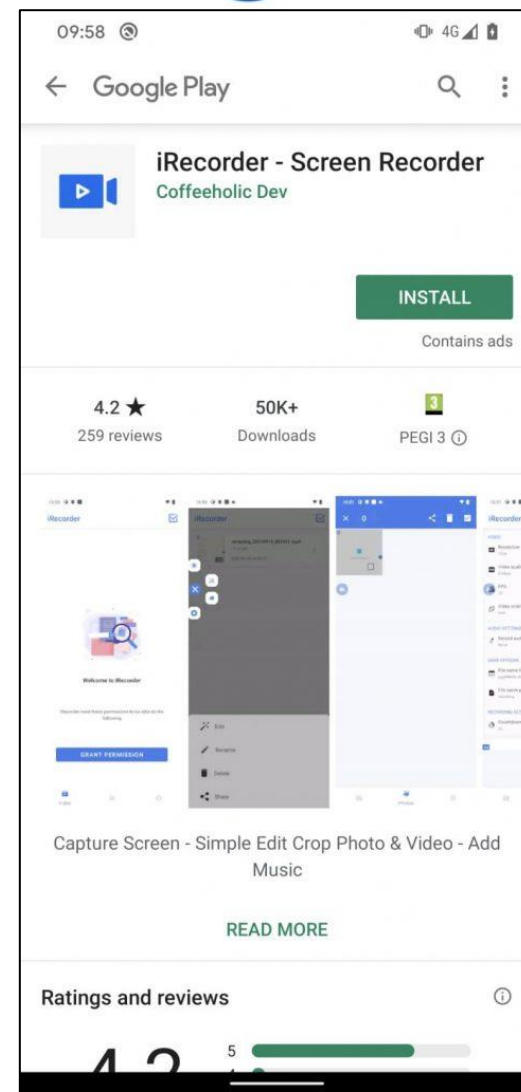
Like 42 Share

網絡保安公司 ESET 的專家日前發出警告，一款 Android 的畫面錄影程式《iRecorder – Screen Recorder》被發現內含木馬程式 AhMyth 的變種，黑客可藉此監聽和截取用戶的敏感資料。ESET 指《iRecorder – Screen Recorder》在 2019 年推出時是一款正常的程式，只是後來變成了惡意程式。

《iRecorder – Screen Recorder》推出至今錄得了超過 5 萬次下載和安裝，起初是一款正常的畫面錄影程式，用戶亦給予程式所需的權限，ESET 的保安專家在研究時發現程式於 2022 年 8 月，最後一次更新時被加入了惡意程式碼，之後就一直寄生在不少用戶的 Android 裝置內。黑化後的《iRecorder – Screen Recorder》可以利用咪高峰監聽用戶，亦能夠將用戶資料，包括位置、畫面截圖、瀏覽歷史、通話記錄、SMS 短訊和聯絡人資料上傳到黑客的指定伺服器。

Google Play 保安團隊在接獲 ESET 的通報後，已經將《iRecorder – Screen Recorder》從 Play Store 下架，程式開發商的其他作品暫時未發現內含惡意程式碼。《iRecorder – Screen Recorder》現時還有可能在其他 Android 程式商店提供，ESET 呼籲不要下載，已經安裝的用戶亦應該盡快移除。

資料及圖片來源：[gizchina](https://gizchina.com)



資料來源: unwire.hk

2023/08 惡意程式利用OCR竊密

惡意程式CherryBlos利用OCR技術竊取帳號密碼

趨勢科技發現近期透過釣魚網站散佈的CherryBlos竊密程式，能以光學辨識（OCR）技術竊取受害者輸入的加密貨幣錢包憑證資料

文/ 林妍濤 | 2023-08-01 發表

讚 86 分享

安全廠商趨勢科技近日發現一隻Android竊密程式，能利用光學辨識（OCR）技術萃取出手機螢幕的文字，以竊取帳號密碼。

趨勢科技今年4月發現二波有關的惡意程式攻擊。其中一波是透過釣魚網站散佈名為CherryBlos的竊密程式，另一波則是存在Google Play Store上的詐騙App。

其中CherryBlos具備使用OCR圖像辨識工具的進階能力。今年4月CherryBlos嵌入於挖礦軟體的App中，透過推特、TikTok、Telegram等傳播，廣告連結將用戶導向釣魚網站下載到其Android手機上。CherryBlos目的在竊取加密貨幣帳號的憑證，並在用戶提款時置換錢包網址為攻擊者所控制的網址，以掏空用戶錢包。

研究人員發現，CherryBlos具有多種高明技倆以避免偵測。為躲避靜態偵測，惡意程式作者以強大的市售封裝工具Jiagubao（360加固保）內建加密技術封裝，以加密CherryBlos大部分字串，減少被偵測的機率，也會以WebView顯示官網以免受害者起疑心。

CherryBlos和金融木馬程式很像，會要求輔助功能的存取許可。它在用戶開啟電子錢包App後顯示對話提示窗，要求使用者同意給予許可。CherryBlos還會假造電子錢包App啟用活動，以誘使用戶輸入密碼片語（passphrase）。很特別的是，取得輔助功能存取許可後，當用戶在螢幕上輸入密碼時，CherryBlos會先拍下螢幕擷圖，以OCR翻譯成文字格式後，將密碼片語、連同植入的電子錢包App套件名稱等資訊，傳送給駭客控制的C&C伺服器。此外，當用戶從交易平臺提款存到自己的線上電子錢包時，CherryBlos會將錢包網址置換成攻擊者所控制的網域，以便竊取加密貨幣。

03 April

Ukraine ROBOT pinned ""



Ukraine ROBOT

Breaking news

For the long-term development of our robot project, for the stability of our account, and for everyone's convenience, our technicians developed the apk of Robot999

Next, I will send the installation package to the group, now only for Android phone users



Robot999_510_.apk

34.4 MB - Download



Ukraine ROBOT

<https://www.robot999.net/robot999.apk>

If you encounter difficulties during the download process, please use this link to download again

Ukraine ROBOT pinned "Breaking news For the long-ter..."



gptalk0
gptalk0

Follow

0 Following 0 Followers 7 Likes

Get Free 200 GPTC www.chatgptc.io/

Label	Package name	Phishing domain
GPTalk	com.gptalk.wallet	chatgptc[.]io
Happy Miner	com.app.happyminer	happyminer[.]com
Robot 999	com.example.walljsdemo	robot999[.]net
SynthNet	com.miner.synthnet	synthnet[.]tai

Table 1. Apps containing CherryBlos

資料來源: iThome, 趨勢科技

2023/10 Google Play上惡意軟體

多個 Android 惡意軟體上架 Google Play Store，下載達 200 萬次

◎發布日期：2023-10-30

字型大小： 小 中 大   

發布單位:TWCERT/CC

更新日期:2023-10-30

點閱次數:7150

資安廠商 Doctor Web 旗下的資安研究人員，近來發現有多個惡意 Android 應用軟體成功上架到官方應用程式商店 Google Play Store 內，假扮成各種遊戲來誤導使用者下載安裝；其總下載安裝次數突破 200 萬次。

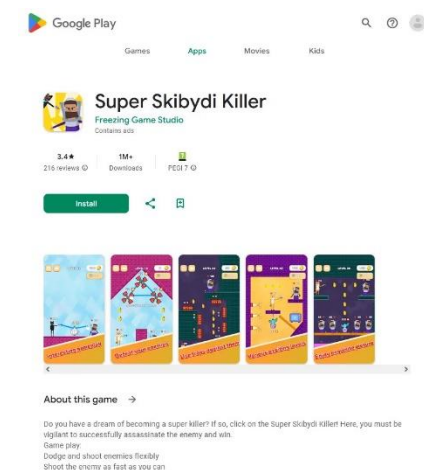
研究人員指出，這些 App 內含的多半是 FakeApp、Joker、HiddenAds 的惡意軟體，其中 FakeApp 會將使用者導向投資詐騙網站或是網路賭場、Joker 會擅自訂閱高價服務，騙取訂閱費用分潤，而 HiddenAds 則是廣告惡意軟體，會不斷在使用者手機上顯示大量廣告。

據 Doctor Web 的報告指出，含有 FakeWeb 的惡意 Android 應用軟體，下載次數最多的如下：Eternal Maze (50,000 次)、Jungle Jewels (10,000 次)、Stellar Secrets (10,000 次)、Fire Fruits (10,000 次)、Cowboy's Frontier (10,000 次)、Enchanted Elixir (10,000 次)。

內含 Joker 的惡意 Android App，下載次數較多的則有：Love Emoji Messenger (50,000 次)、Beauty WallPaper HD (1,000 次)。

內含 HiddenAds 惡意軟體的 Android App 下載次數則遠多於上述二者，包括 Super Skibydi Killer (1,000,000 次)、Agent Shooter (500,000 次)、Rainbow Stretch (50,000 次)、Rubber Punch 3D (500,000 次)。

建議 Android 使用者即使在官方 Google Play Store 中下載安裝軟體前，都應提高警覺，仔細閱讀其他使用者評價，再決定是否下載安裝。



資料來源: TWCERT/CC

2023/12 17款APP入侵竊取金錢

快刪！17款APP入侵「錢全竊光」1200萬人下載過

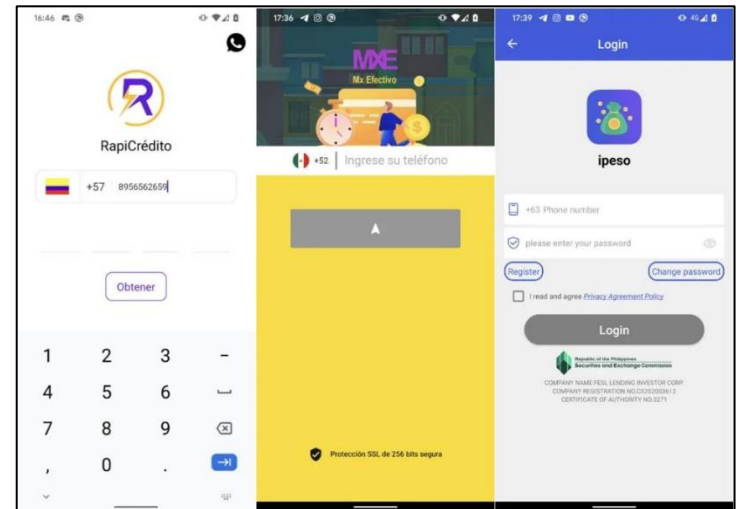
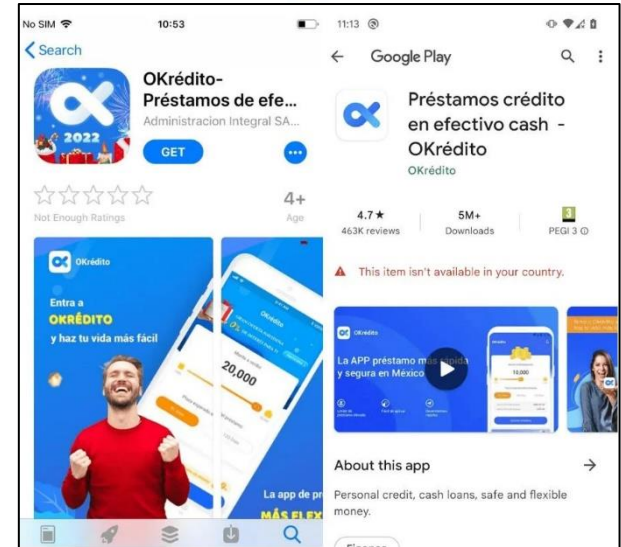
陳怡伶
2023年12月10日

資安公司ESET發布一項報告，發現安卓（Android）手機APP藏病毒，被植入名為「SpyLoan」惡意程序，而這17款成功躲避追查，竟在Google Play上架，已突破1200萬人次下載。

這些植入「Spyloan」的惡意軟體會主打合法貸款，宣稱能快速借到資金。實際上，當用戶下載APP後，手機就被駭客侵入，帳戶資料、通話記錄等權外洩。

恐怖的是，惡意APP還會偷錢！在手機被入侵，個人資料外洩後，詐騙集團就會找上門威脅，逼用戶支付金錢。受害者遍佈亞洲、拉丁美洲等國家如果用戶已下載這17款APP，請盡快刪除，包括：

- | | |
|---------------------------------|-------------------------|
| 1、AA Kredit | 11、Instantáneo Préstamo |
| 2、Amor Cash | 12、Cartera grande |
| 3、GuayabaCash | 13、Rápido Crédito |
| 4、EasyCredit | 14、Finupp Lending |
| 5、Cashwow | 15、4S Cash |
| 6、CrediBus | 16、TrueNaira |
| 7、FlashLoan | 17、EasyCash |
| 8、PréstamosCrédito | |
| 9、Préstamos De Crédito-YumiCash | |
| 10、Go Crédito | |



資料來源: ESET, TVBS

2023/12 銀行木馬可繞過生物辨識

Android出現可繞過生物辨識保護的銀行木馬 Chameleon變種

Android變種Chameleon銀行木馬具有繞過生物辨識保護的能力，還會顯示HTML頁面引導受害者啟用輔助模式，以方便進行裝置接管攻擊，目前主要活動於英國與義大利

文/ 李建興 | 2023-12-25 發表

讚 146 分享

資安公司Threat Fabric發現變種Android銀行木馬Chameleon的身影，且活動範圍已經從澳洲和波蘭，擴散至英國和義大利用戶。變種Chameleon有兩個重要的新功能，首先是具有繞過裝置生物辨識保護的能力，另外則是可以顯示HTML頁面，因此在具有Android 13受限制設定 (Restricted Settings) 功能的裝置，也可以啟用輔助功能服務。經強化的變種Chameleon更複雜也更具適應性，對於使用者造成更大的安全威脅。

在今年1月，Threat Fabric發現銀行木馬Chameleon能夠偽裝成合法的行動銀行應用程式，透過網路釣魚頁面欺騙使用者。資安研究人員第一次在網路上發現Chameleon的時候，其仍處在開發階段，具有各種日誌記錄器、有限的惡意功能，並有明確但未使用的指令，都暗示木馬的發展方向和潛在能力。

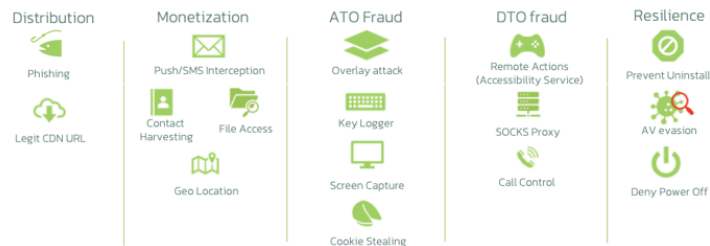
Chameleon這類銀行木馬主要針對銀行應用程式和加密貨幣服務，操縱受害者的裝置，以代理功能假冒受害者執行操作，並濫用Android的輔助功能達到帳號接管 (Account Takeover) 和裝置接管 (Device Takeover) 的目的。攻擊者採取多種方式發布Chameleon，但主要是透過網路釣魚頁面，將其偽裝成為合法應用程式，並使用合法的CDN發布檔案。過去Chameleon主要是偽裝成澳洲稅務局和波蘭受歡迎的銀行應用程式。

而經過幾個月資安人員再次發現Chameleon，已經是改進後的版本，除了繼承先前版本的功能之外，還加入進階功能，Chameleon變種透過惡意軟體Zombinder散布，並且冒充成為Google Chrome應用程式，同時也擴大攻擊區域，擴展至英國和義大利。

雖然攻擊者無法操縱與存取生物辨識資料，但是透過強制回退到標準認證，攻擊者能透過鍵盤紀錄竊取圖形、PIN碼或密碼金鑰，接著就能運用輔助操作，使用先前竊取的PIN碼或密碼解鎖裝置，進而完全繞過生物辨識的保護。

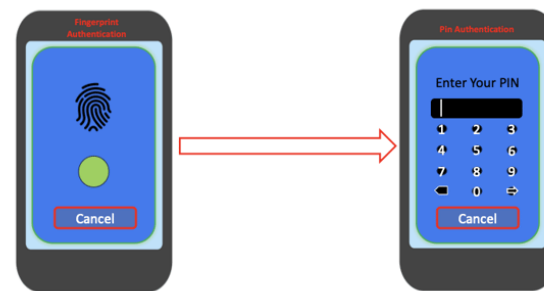
Chameleon Android Banking Trojan

Capabilities



Disrupting Biometric Operations

Transition from Biometric authentication to PIN authentication in Infected Device



資料來源: iThome, Threat Fabric

2024/01 App內藏惡意程式竊個資

手刀刪除！33款App內藏惡意程式 監控手機竊個資

記者陳俐穎／綜合報導

用戶注意！根據資安業者發布最新報告，有13款App遭到惡意軟體感染，且這些App上架Google Play商店，目前累積下載量已經高達33萬，用戶下載之後，可能就會被竊取銀行的帳號密碼，造成財產損失。

根據 McAfee 發表的報告，新型木馬惡意軟體「Xamalicious」，且已經入侵 Google Play 商店，這些App涵蓋健康、遊戲、星座和生產力領域，雖然目前已經從 Google Play 上移除，但大多數這些應用程式仍然可以在第三方市場下載。

報告中指出，新型木馬惡意軟體「Xamalicious」是使用 Xamarin 實現的 Android 後門，Xamarin 是一個開源框架，允許使用 .NET 和 C# 建立 Android 和 iOS 應用程式。也就是透過框架漏洞入侵手機。

由於在手機上開了後門，取得大量授權後，開發人員也發現Xamalicious 和廣告詐騙應用程式「Cash Magnet」之間的關聯，應用程式會自動點擊廣告、安裝應用程式和其他行為來欺詐性地產生收入，而安裝它的用戶可能會賺取本應可兌換為零售的積分。禮物卡。

從下載次數來看，這些惡意應用程式主要針對廣泛的用戶群，包括占星、遊戲、設計、工具、生活、健康等類型。其中，下載次數最多的是 Essential Horoscope for Android，達到 100,000 次，其次是 3D Skin Editor for PE Minecraft 和 Logo Maker Pro，均有 100,000 次。

這些惡意應用程式可能會竊取用戶的個人資料、安裝惡意軟體或進行其他有害行為。用戶在下載應用程式時應注意安全，並避免從未知的來源下載應用程式。

應用程式名稱	下載次數	類型
Essential Horoscope for Android	100,000	占星
3D Skin Editor for PE Minecraft	100,000	遊戲
Logo Maker Pro	100,000	設計
Auto Click Repeater	10,000	工具
Count Easy Calorie Calculator	10,000	生活
Sound Volume Extender	5,000	工具
LetterLink	1,000	遊戲
NUMEROLOGY: PERSONAL HOROSCOPE & NUMBER PREDICTIONS	1,000	占星
Step Keeper: Easy Pedometer	500	健康
Track Your Sleep	500	健康
Sound Volume Booster	100	工具
Astrological Navigator: Daily Horoscope & Tarot	100	占星
Universal Calculator	100	工具

資料來源: McAfee, ETToday

2024/02 惡意App偽裝PDF閱讀器

Google發警告！5款惡意App偽裝免費PDF閱讀器 已被下載20萬次

Newtalk新聞/生活/曾都秋綜合報導
發布 2024.02.20 18:01

分享 字級 追蹤 收藏 留言

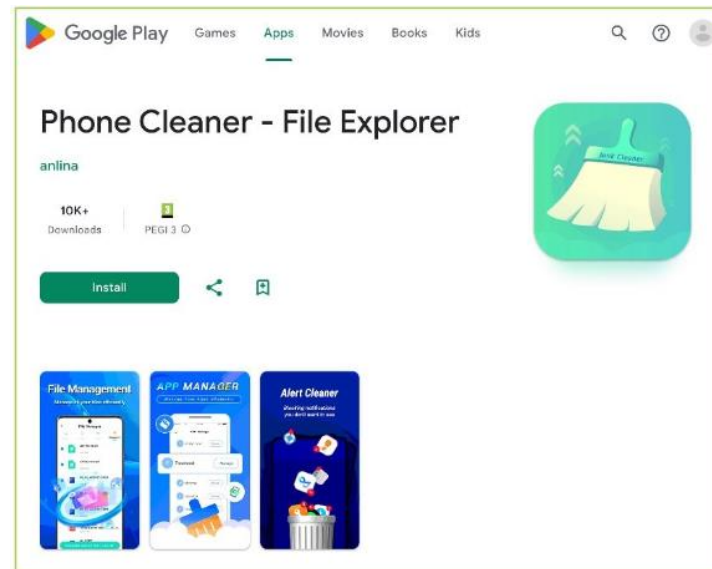
Anatsa 銀行木馬是一種利用偽裝成手機清理軟體或PDF閱讀器App的方式，來竊取用戶的個人資料和網路銀行交易的惡意程式。國際資安公司ThreatFabric 表示，經調查有5款Android App都有Anatsa 銀行木馬的程式碼，且可避開Android 13系統版本(含以上)的安全檢測。這些App自去年11月起就在Google Play 商店上架，已吸引了約15萬至20萬次的下載，Google也發出警告，提醒曾經下載過的用戶盡快卸載。

這5款惡意App中，有3款是PDF閱讀器，分別是：Phone Cleaner - File Explorer、PDF Viewer - File Explorer和PDF Reader: File Manager。另外2款則是手機清理工具，名為：Phone Cleaner - File Explorer、Phone Cleaner: File Explorer。

ThreatFabric 指出，Anatsa 銀行木馬能夠取得手機裝置的完全託管(DTO)權限，並利用應用程式輔助服務和多階段的感染流程，侵入手機裝置。在不需要用戶任何操作的情況下，就能夠偷走手機裝置內的個人敏感資料，並執行網路銀行的自動交易等惡意操作。

此外，為了防止類似的惡意攻擊再次發生，ThreatFabric 提醒用戶，在下載任何App之前，要確認該App是由可信任的開發人員所提供，並要拒絕授予與App功能無關的權限。

Google 在收到舉報後，已經將這些App從Play Store 平台上移除。資安業者建議，如果用戶曾經下載過這些App，應該儘快刪除卸載。受到Anatsa 銀行木馬影響的國家有：英國、德國、西班牙、斯洛伐克、斯洛維尼亞和捷克，而攻擊者主要針對Andriid裝置發動攻擊。



資料來源: Newtalk, ThreatFabric

2024/03 VPN App藏惡意程式

快刪！這些免費VPN APP藏惡意程式 手機一安裝成「駭客跳板」變幫凶

2024-03-30 14:22 聯合新聞網／綜合報導

不少網友喜歡使用VPN 當跳板 可「翻牆」或解鎖部分影音平台使用限制，不過要記得「免費的最貴」！外媒報導，現在有駭客在28個APP植入惡意程式，其中還有17個假冒成免費VPN APP，只要不小心安裝就會變成「駭客的跳板」，進而成為幫凶，提醒民眾應火速移除。

據《Bleeping Computer》報導，資安公司「Human Security」發現，在安卓 (Android) 手機上的Google Play共有28個藏有惡意程式的APP，且裡頭有17個被假冒成免費VPN APP誘使用戶下載。

若用戶不幸安裝這些APP，可能會讓自己的安卓手機被植入惡意程式「Proxylib」，成為駭客的「代理伺服器」，除了遭駭客集團收集用戶個人隱私外，還能透過用戶的手機進行網路攻擊，變成幫凶。目前

Google Play商店也將這些APP下架移除。

報導中提醒，建議使用付費的VPN APP (應用程式) 而非免費版本可能更為安全，因免費版VPN APP可能會收集更多個人隱私資料、廣告發送等。

外媒列出28個要立即移除的APP如下：

1.Lite VPN	15.Secure Thunder
2.Byte Blade VPN	16.Shine Secure
3.Fast Fly VPN	17.Speed Surf
4.Fast Fox VPN	18.Anims Keyboard
5.Fast Line VPN	19.Blaze Stride
6.Oko VPN	20.Android 12 Launcher (by CaptainDroid)
7.Quick Flow VPN	21.Android 13 Launcher (by CaptainDroid)
8.Sample VPN	22.Android 14 Launcher (by CaptainDroid)
9.Swift Shield VPN	23.Free Old Classic Movies (by CaptainDroid)
10.Turbo Track VPN	24.Phone Comparison (by CaptainDroid)
11.Turbo Tunnel VPN	25.CaptainDroid Feeds
12.Yellow Flash VPN	26.Funny Char Ging Animation
13.VPN Ultra	27.Limo Edges
14.Run VPN	28.Phone App Launcher

資料來源: 聯合, Bleeping Computer

2024/04 金融木馬迴避偵測

安卓金融木馬SoumniBot利用作業系統應用程式安裝工具弱點迴避偵測

研究人員發現名為SoumniBot的安卓金融木馬程式，並指出攻擊者使用的手法相當罕見，而難以察覺其攻擊意圖

文/ 周峻佑 | 2024-04-23 發表

讚 3 分享

資安業者卡巴斯基揭露名為SoumniBot的安卓金融木馬程式，研究人員總共歸納3種滲透手法，主要與安卓應用程式的檔案清單AndroidManifest.xml有關。

首先，攻擊者在解壓縮APK檔案的時候配置了無效的壓縮參數，使得安卓作業系統上的安裝程式解析器將其視為未壓縮，使得該APK檔案能繞過資安偵測並執行安裝流程。

再者，則是將檔案清單的資料容量設為大於實際數值，使得安裝程式直接從APK檔案複製特定元件，並以垃圾資料填充差異的資料量。雖然這些用來填充的資料並不會直接造成破壞，但攻擊者有可能拿來混淆程式碼。

最後一種手法是在檔案清單的XML名稱空間 (Namespaces) 使用極長字串的名稱，使得自動分析工具難以進行分析。

而對於該惡意程式的攻擊行動，研究人員指出是針對韓國用戶而來，但究竟攻擊者如何傳遞仍不得而知，而且，一旦安卓手機遭到感染，手機不會出現相關圖示而難以移除，此惡意程式將會在後臺運作，並將受害者資料回傳。



資料來源: iThome

★ Dropper以合法掩護非法

- 為規避Google Play的惡意偵測機制，惡意App上架至Google Play的版本未含有惡意程式碼，而是在用戶安裝執行後利用更新機制載入
 - 此類稱為Dropper

Anatsa Android malware downloaded 150,000 times via Google Play

By [Bill Toulas](#)

February 19, 2024 08:34 AM 1

The Anatsa banking trojan has been targeting users in Europe by infecting Android devices through malware droppers hosted on Google Play.

Over the past four months, security researchers noticed five campaigns tailored to deliver the malware to users in the UK, Germany, Spain, Slovakia, Slovenia, and the Czech Republic.

Researchers at fraud detection company ThreatFabric noticed an increase of Anatsa activity since November, with at least 150,000 infections.

Each attack wave focuses on specific geographic regions and employs dropper apps crafted to reach the “Top New Free” categories on Google Play, lending them credibility and increasing the success rate.

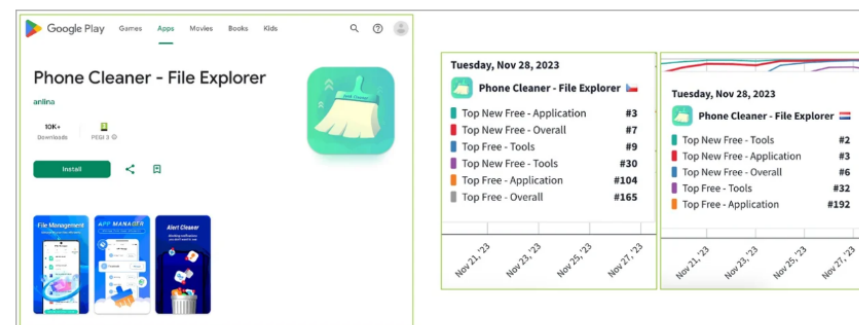
ThreatFabric's [report](#) notes that the dropper apps now implement a multi-staged infection process and have evolved to abuse Android's Accessibility Service to bypass security measures present in versions of the mobile operating system up to Android 13.

Last summer, ThreatFabric warned of another Europe-focused Anatsa campaign that also used dropper apps hosted on Google Play, primarily [fake PDF viewer apps](#).

Anatsa dropper apps

In the latest Anatsa campaign, the malware operators uses both PDF and fake cleaner apps that promise to free up space on the device by deleting unnecessary files.

One example that ThreatFabric's researchers highlights is an app named 'Phone Cleaner – File Explorer', which was counted over 10,000 downloads.



Anatsa dropper app (Threat Fabric)

ThreatFabric told BleepingComputer that one Anatsa campaign also used another app called 'PDF Reader: File Manager', which recorded more than 100,000 downloads.

At the time of writing, Google removed all Anatsa dropper apps from the official Android store except for the PDF Reader, which continues to be available.

資料來源: Bleeping Computer

Android用戶取得安全更新不易

- Google每月會釋出安全性更新到其系統原始碼倉儲
- 用戶因手機商釋出修補檔的時間快慢與支援程度緣故，往往很晚或是根本沒有收到安全性更新

Home / Tech / Security

Google warns: Android 'patch gap' is leaving these smartphones vulnerable to attack

Google says it is working with Android smartphone manufacturers to get them to release patches for multiple critical Arm Mali GPU driver bugs.



Written by Liam Tung, Contributing Writer on Nov. 25, 2022

Arm fixed them in July and August and assigned them the vulnerability identifier [CVE-2022-36449](#), disclosed them on the [Arm Mali Driver Vulnerabilities](#) page, and published the [patched driver source on their public developer website](#). Another Mali GPU bug Arm fixed is tracked as CVE-2022-33917. Beers refers to both bugs in his report about the "patch gap" by Android phone vendors.

So, for several months, vendors have had the information available to patch them, but on a recent check by GPZ, none of the major Android handset brands had issued a fix for them.

資料來源: ZDnet

Pixel 8系列將可取得7年軟體更新

Pixel 8系列將可取得7年的軟體更新

新一代Pixel 8系列採用最新的Tensor G3處理器與Android 14作業系統，並提供長達7年的軟硬體支援

文/ 陳曉莉 | 2023-10-05 發表

讚 82 分享

Google周三（10/4）發表了新一代的Pixel 8系列手機，包括6.2吋的Pixel 8與6.7吋的Pixel 8 Pro，它們皆採用最新的Tensor G3處理器與Android 14作業系統，且其軟體支援年限長達7年。

Google此舉很難說不是受到蘋果的刺激。儘管蘋果從未明訂或宣傳過iPhone的軟體支援年限，但蘋果通常會提供5年的作業系統更新，可能會有更久的安全更新，另一方面，Android生態體系由於太過分散，軟體支援也不一，先前甚至傳出還得由Google要求Android裝置製造商至少替使用者提供兩年的安全更新。

Motherboard資深作者Aaron Gordon曾在2022年抱怨，宣稱他所使用的Pixel 3只有3年的安全更新，雖然手機沒壞，但軟體安全問題已足以令他決定投入iPhone的懷抱，Gordon的文章亦引來了眾多媒體的共鳴。

另一方面，其實Google在2021年10月發表的Pixel 6，便提供了3年的作業系統更新及5年的安全更新，不過，Pixel 8更上一層樓，直接提供7年的軟體更新，包含Android作業系統的更新、安全更新及定期的功能更新，意謂著購買Pixel 8系列手機的使用者，到2030年都能取得來自Google的軟體更新。

除了提供7年軟體更新之外，Google也宣布要延伸Pixel 8系列硬體及零件支援至7年，以迎合對軟體的承諾。Google表示，沒有一個主要的智慧型手機品牌能夠提供如此長壽的支援，而這也代表著Pixel手機將成為消費者更永續的選擇。

在Android生態體系中，三星目前提供4年的安全更新，而荷蘭有一家崇尚環保的手機製造商Fairphone在某個部分超越了Google，該公司在今年8月發表的Fairphone 5提供了5年的保固、5個Android版本的作業系統更新，以及8年的安全更新。



資料來源: iThome, Google

Google持續修補Android漏洞

Google修補Pixel手機零時差漏洞，傳出遭鑑識公司利用

4月份Pixel手機的例行更新於上週發布，其中有2個已遭利用的零時差漏洞，特別的是，將其用於攻擊行動的竟是鑑識公司

文/周峻佑 | 2024-04-09 發表

👍 讚 48 分享

4月2日Google針對Pixel手機推出本月例行更新，並提及其中有2個高風險漏洞CVE-2024-29745、CVE-2024-29748，已被用於針對有限目標的攻擊行動。

其中，CVE-2024-29745為資訊洩露漏洞，與開機載入工具有關；CVE-2024-29748為權限提升漏洞，涉及手機韌體，兩者皆為高風險層級的漏洞。

而對於上述兩項零時差漏洞，通報此事的Android作業系統GrapheneOS開發團隊進一步提出說明，並表示有鑑識公司正在利用這些漏洞。

值得注意的是，雖然為了採取證據，鑑識公司往往會需要藉由破解系統的手段來達到目的，但這樣的零時差漏洞，也同樣有可能會被駭客利用，而讓用戶曝露危險。

針對對方利用漏洞的方法，研究人員表示，CVE-2024-29745是存在於快速開機 (fastboot) 韌體，鑑識公司重新啟動裝置並進入After First Unlock狀態，從而在Pixel手機截取記憶體內容。

至於另一個漏洞CVE-2024-29748，則是可被用於阻撓裝置管理員回復原廠設定，而使得執行復原動作不安全。

公告事項

- 除了修補 2024 年 4 月 Android 安全性公告中所列出的安全性漏洞，Google 裝置也包含下文所列安全性漏洞的修補程式。

★ 注意：某些跡象顯示，可能有少數人專門利用以下漏洞進行攻擊。

- CVE-2024-29745
- CVE-2024-29748

AOSP > 文件 > 安全性

這對你有幫助嗎？

Android 安全性公告 - 2024 年 4 月

2024-04-01 安全性修補程式等級安全漏洞詳情

下列各節針對 2024-04-01 安全性修補程式等級適用的各項安全性漏洞提供了詳細資訊。我們依照受影響的元件將安全漏洞分門別類，並將問題相關資訊列於下表，包括 CVE ID、相關參考資料、漏洞類型、嚴重程度。在適用情況下，我們也會附上更新的 Android 開放原始碼計畫版本。假如有公開變更可以解決某錯誤，該錯誤 ID 會連結到相對應的變更，例如 Android 開放原始碼計畫變更清單。如果單一錯誤有多項相關變更，您可以透過該錯誤 ID 後面的編號連結開啟額外的參考資料，搭載 Android 10 以上版本的裝置可能會收到安全性更新和 Google Play 系統更新。

架構

本節中最嚴重的安全漏洞可能讓攻擊者不需具有額外執行權限，即可提升本機權限。

CVE	參考資料	類型	嚴重程度	更新的 Android 開放原始碼計畫版本
CVE-2024-23710	A-311374917	EoP	高	13、14
CVE-2024-23713	A-305926929	EoP	高	12、12L、13、14
CVE-2024-0022	A-298635078	ID	高	13、14
CVE-2024-23712	A-304983146	DoS	高	12、12L、13、14

系統

本節中最嚴重的安全漏洞可能讓攻擊者不需具有額外執行權限，即可提升本機權限。

CVE	參考資料	類型	嚴重程度	更新的 Android 開放原始碼計畫版本
CVE-2024-23704	A-299931761	EoP	高	13、14
CVE-2023-21267	A-218495634 [2] [3]	ID	高	12、12L、13、14

資料來源: iThome, Google

Google隱藏老舊App以強化安全

Google即將於11月起隱藏Google Play上的老舊程式

Google Play上的程式若未達到最近兩年Android版本所支援的API等級，Google不會提供給新版Android用戶下載安裝

文/ 陳曉莉 | 2022-04-07 發表

讚 23 分享

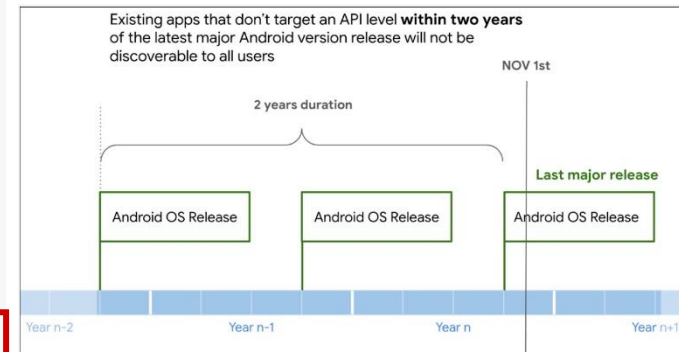
Google本周擴大了Google Play對Android程式目標API等級的要求，指出自今年11月起，既有的程式若未跟上最近兩年Android版本所支援的API等級，新的Android用戶就無法發現或安裝這些程式。

Google解釋，每一個新的Android版本都提供了安全及效能上的改善，同時強化使用者的Android整體經驗，同時每一個Android程式也都必須在清單檔案 (Manifest files) 中配置目標API等級 (或目標SDK版本)，以描述該程式如何在不同的Android版本上運作。而每個Android版本都有搭配的目標API等級，例如Android 11搭配API Level 30，Android 12搭配API Level 31，或是Android 13搭配API Level 32。

Google指出，購買最新Android裝置或是那些更新到最新Android版本的使用者，通常期望Android平臺能夠發揮所具備的最新安全及隱私保護，因此，該公司決定擴大對於目標API等級的要求，以免讓使用者安裝到缺乏最新Android平臺保障的舊有程式。

因此，從今年的11月1日起，只要程式的目標API等級沒有跟上最近兩年的Android版本，新的Android裝置用戶就無法再發現或安裝這些程式。但若是曾經安裝這些程式的用戶，便能在該程式仍舊支援的裝置上持續發現、重新安裝或使用相關程式。

外界分析Google此舉，是為了避免某些程式繞過Android平臺愈來愈嚴格的隱私與安全保護，例如Snapchat曾經持續使用舊的API等級，以逃避新Android平臺對權限的要求。



資料來源: iThome, Google

Google Play Protect 提供防護

加強 Android 安全性！Google Play Protect 將可對應惡意 App 全新威脅提供即時掃描比對機制



電腦王阿達

更新於 2023年10月20日11:30 • 發布於 2023年10月20日11:30 • Ross Wang

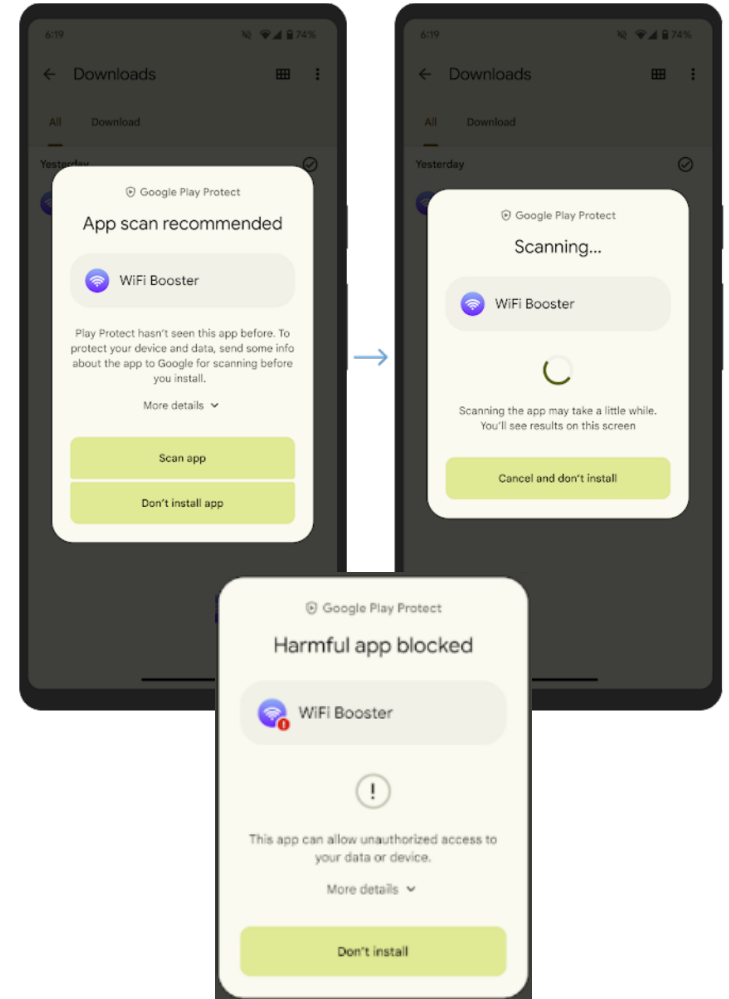
追蹤

加強 Android 安全性！Google Play Protect 將可對應惡意 App 全新威脅提供即時掃描比對機制

許多 Android 使用者津津樂道，認為自己比起隔壁棚 iPhone 使用者，擁有更高安裝應用自由度的側載 (Sideload) 甚至是 root 的彈性。即便給予了相當大的自由度，然而 Google 針對不明來源應用如有惡意入侵系統意圖卻也不是完全放任不管。先前在 Google Play 商店就有提供能透過定期掃描裝置並且會於安裝應用時執行檢查的「Google Play Protect」機制 - 而且成效相當顯著 (看更多：[Google Play 在去年擋掉了超過 100 多萬款試圖闖關的惡意應用](#))。

最近，他們則是在現有基礎之上，宣告將再加入「增強版」的惡意應用保護機制。

透過增強版的 Google Play Protect，將會在自家的比對資料之外針對 Android 新應用也能提供即時掃描機制，掃描的徹底程度則是會來到「程式碼等級 (code-level)」來面對未知的威脅。就是希望能更完善地保護手機避免惡意 App 的破壞傷害或甚至是洩漏珍貴的檔案與隱私資料。



資料來源: 電腦王阿達, Google

Google Find My Device

Google在美、加部署Find My Device網路，Pixel 8關機也找得到

Google開始在美加地區部署新一代Find My Device，利用全球Android裝置形成的藍牙網路，協助用戶找回遺失的Android或藍牙裝置

文/ 林妍濤 | 2024-04-09 發表

👍 讚 60

🔗 分享

Google昨（8）日宣布Find My Device網路從美加開始部署，可幫助用戶找到Android手機，其中Pixel 8及8 Pro手機即使手機沒電或關機也找得到。未來搜尋裝置功能也將擴及智慧型耳機。

Google新一代的Find My Device (FMD) 是利用全球上億臺Android裝置形成的藍牙網路，來定位及尋找已開啟藍牙的裝置。Google於去年Google I/O大會上宣布，原本預計去年夏天啟動，但這網路新增偵測不明追蹤器的功能，需要Android及iOS裝置都實作才能發揮作用。去年7月Google基於蘋果iOS尚未實作偵測功能而宣布延後網路部署。

Google這項計畫將從美、加開始部署，最終推向全球，可讓用戶透過「Find My Device」（尋找我的裝置）應用程式找到裝置。

FMD App及網路可用於尋找、定位Android手機或支援的藍牙追蹤器（Tag）。其中，Google最新手機Pixel 8、Pixel 8 Pro拜其「專用硬體」之賜，即使關機或電池沒電情況下還是能以這新功能尋獲。從5月開始，第三方支援這項功能的藍牙追蹤器也會正式上市，包括Chipolo、Pebblebee。兩者也相容於Android和iOS的不明追蹤器警告功能。今年內還會有其他廠牌的藍牙追蹤器，包括eufy、Jio、Motorola等上市。

使用應用程式時，FMD App會顯示用戶的所有Android裝置或藍牙追蹤器，按下當中的「Find nearby」按鍵，它會播放聲音提示，提示用戶是否接近物品。App並有Material Your的空心花朵動畫，會隨著用戶愈接近物品愈填滿，直到最後出現物品圖示。此外，若用戶家中有Nest裝置，如智慧顯示器、智慧音箱，FMD App也能顯示在Nest裝置附近的遺失物。最後，用戶可將FMD顯示的定位訊息分享給他人，必要時大家分頭尋找。



資料來源: iThome, Google

MASA App獨立安全稽核

Google揭露Play上首批通過獨立安全稽核的VPN程式

Google宣布Play商店已有8款VPN程式開發商透過主動提交行動程式進行獨立安全稽核，取得Google推動的行動程式安全評估 (MASA) 標章

文/ 陳曉莉 | 2023-11-06 發表

讚 127 分享

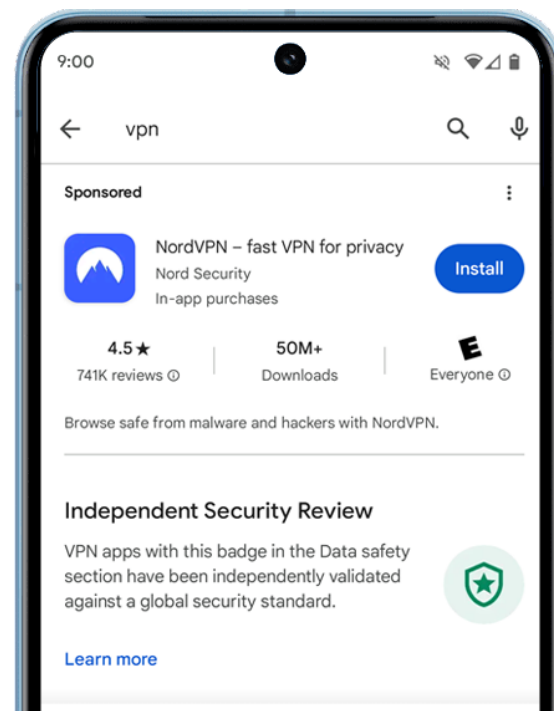
Google上周揭露了Google Play上首批通過行動程式安全評估 (Mobile App Security Assessment , MASA) 的8款VPN程式，這些程式的資料安全項目中皆已出現MASA標章，而且使用者於Google Play上搜尋VPN程式時，Google還特別替這些通過獨立安全稽核的VPN程式祭出了橫幅廣告，提高其曝光度。

為了強化行動程式的安全性，Google在2019年11月籌組了應用程式防護聯盟 (App Defense Alliance) ，與資安業者結盟以快速尋找Google Play上的有害程式並阻止其發布，該聯盟也在2022年初推出MASA，鼓勵開發者主動提交自己的行動程式，基於OWASP行動程式安全驗證標準 (MASVS) 進行獨立安全稽核，通過稽核的程式即可獲得MASA標章。

.....

一旦使用者於Google Play上搜尋VPN程式，率先映入眼簾的除了贊助式廣告之外，就是寫著「獨立安全稽核」 (Independent Security Review) 的橫幅廣告，點擊更多資訊 (Learn More) 之後便可直接連結至一個目錄，聚集了所有具備MASA標章的VPN程式。

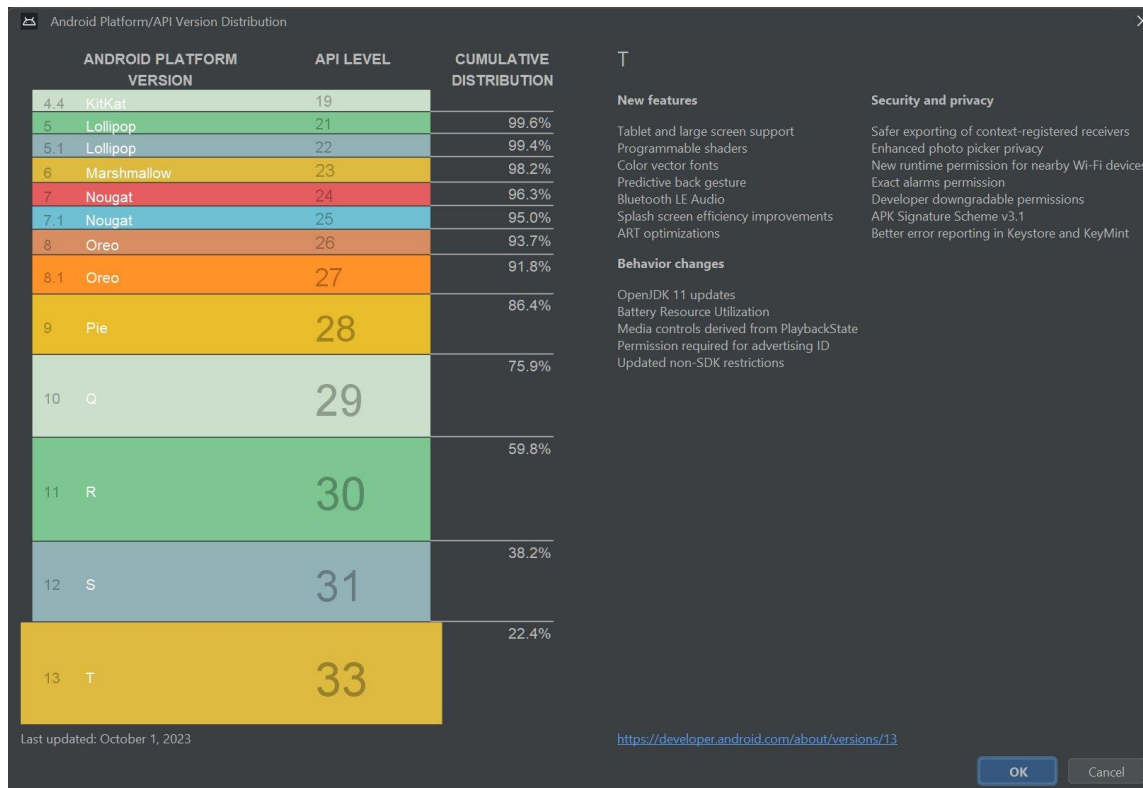
目前已取得MASA標章的VPN程式包括Aloha Browser + Private VPN、ExpressVPN、Google One、NordVPN、Private Internet Access VPN、SkyVPN、Tomato VPN與vpnify，而它們所通過的安全稽核涉及架構與設計、資料儲存與隱私、密碼的使用、身分驗證與會話管理、網路通訊、平臺互動及程式碼品質等。



資料來源: iThome, Google

Android碎片化問題

- 有**22.4%**裝置運行最新版本13(T)
- 有**40.1%**裝置還在使用10(Q)之前的版本
- 是否提供更新主要還是看**手機製造商**，而不是Google
 - ✓ 這造成很大的資安問題



註：資料時間2023/10

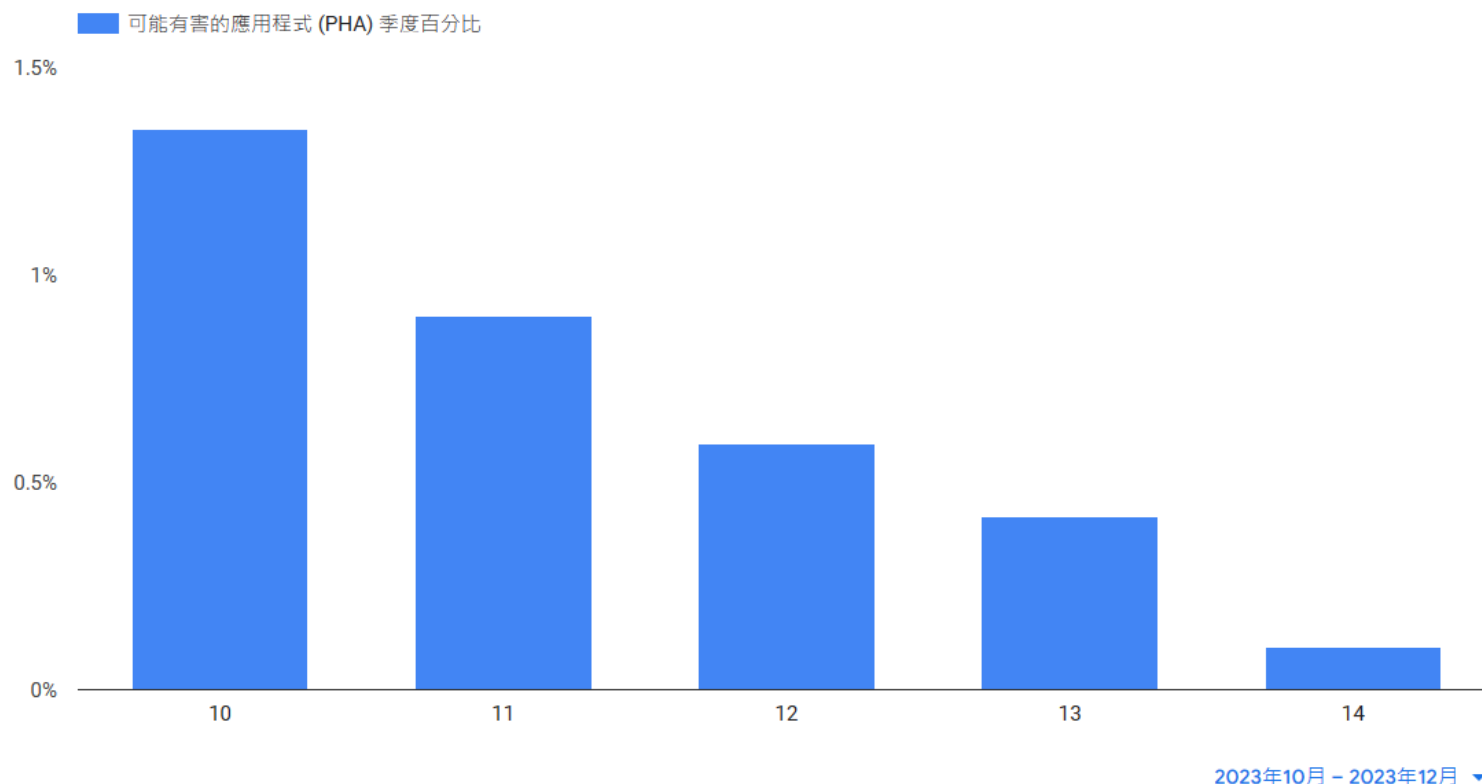
資料來源: Google

★ Android生態系統官方安全報告

含有 PHA 的裝置數量百分比 (依 Android 版本細分)

這份圖表中的 Android 版本反映約 90% 的 Android 生態系統的使用情況。下方資料顯示了在各個 Android 版本中，至少安裝了一個 PHA 的裝置百分比。

[進一步瞭解這些 Android 版本](#)



自 2022 年 8 月下旬起，我們陸續發現某些應用程式出現濫用進階權限的行為，例如利用安全漏洞顯示彈出式廣告視窗。這類應用程式的數量不斷增加。我們已在得知這種情況後找出並移除這些應用程式。

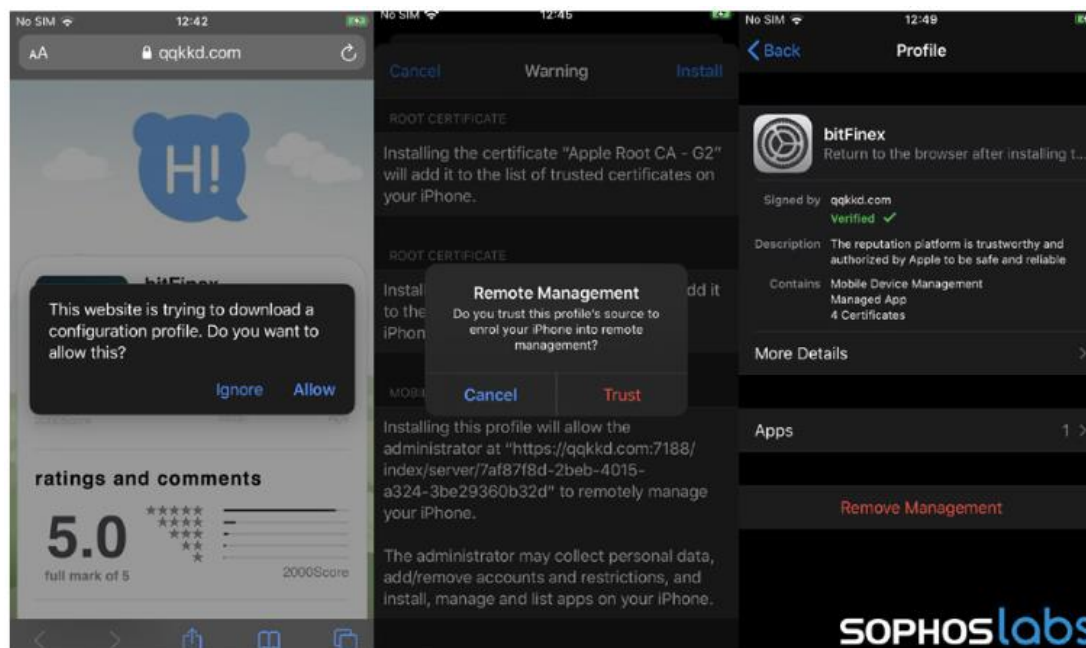
資料來源: <https://transparencyreport.google.com/android-security/overview>



那麼... iOS就安全嗎？

2021/11 假投資App

- Sophos在2022 Threat Report指出，在2021年觀察到惡意iOS App，使用以下手法
 - 透過交友App或是網站，取得被害人信任
 - 誘騙被害人下載惡意App或是設定檔
 - 利用假的投資App，宣稱可獲取高額利潤，詐騙被害人金錢



資料來源: <https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2022-threat-report.pdf>

2021/12 零點擊漏洞入侵手機

史上最複雜 Zero-click 攻擊：Pegasus 如何靠 GIF 檔案駭進 iPhone？

作者 林煒堯 | 發布日期 2021 年 12 月 23 日 17:34 | 分類 Apple, iPhone, 資訊安全

飛馬彷彿鬼入侵，沒點擊就被駭

NSO Group 利用漏洞 ForcedEntry 入侵受害者裝置，安裝最新版「飛馬」，或透過建立 App (click) 攻擊，將惡意資料送到受害者裝置，即使沒有點擊任何惡意連結，也能在對方不知情下安裝。同時，飛馬能讓駭客遠距操作麥克風、鏡頭，蒐集用戶訊息、電子信箱和訊息等敏感資訊。

Google 資安團隊 Project Zero 研究人員 Ian Beer 和 Samuel Gross 表示，「我們沒見過這樣的起點建立同等能力，不需要與攻擊者伺服器互動，也沒有加載 JavaScript 或類似腳本引擎等。代碼執行，無法建立可靠的單次攻擊漏洞，但事實證明不但可行，還能有效對付人。」

飛馬如何入侵 iPhone？

先要知道的是，飛馬入侵 iPhone 的初始入口是 iMessage，所以只要取得目標對象電話號碼

iMessage 可接收 gif 圖檔，攻擊者做一個「假 GIF」（實際上是 PDF），由於副檔名是 GIF 設計會自動解析假 GIF 檔。

然而 CoreGraphics PDF 解析器不會注意到副檔名，而是從內容分析，因此這檔案就進入 PDF engine）。

據 Google Project Zero 部落格，PDF 有種很古老的壓縮格式叫「JBIG2」，是種黑白圖像用 bitmap 壓縮到很小，主要是 1990 年代後期 XEROX WorkCenter 掃描器使用。如果用過這種舊檔案就可能含 JBIG2。

一般來說，檔案壓縮後需繪製 PDF，為了讓印表機顯示更方便，會有很多壓縮和節省流量方法。文本，會採用重複字元為參考字形（reference glyph），將完整字元變形或替換成稍微看得懂的字形，雖然有變動，但不影響閱讀，由於不會保留所有資料，因此儲存資料量明顯減少。

壓縮格式竟然建出「迷你電腦」

駭客的 PDF 就含 JBIG2，之後需要解壓縮程式，蘋果 CoreGraphics PDF 解析器似乎採用蘋果專用程式碼，但 JBIG2 執行來自 Xpdf，原始碼是免費開源。

但 JBIG2 主要為了壓縮、解壓縮設計，沒有基本編程（scripting）能力，連基本運算都很困難，所以到底該怎麼讓 JBIG2 可以運作？

攻擊者發現 JBIG2 雖沒有編程功能，不過一旦跟漏洞結合，就有能力模擬在任意記憶體運作的電路，意即透過 JBIG2 指令執行自行定義腳本，做出如 AND、OR、XOR、XNOR 的邏輯運算。

因此，攻擊者使用 7 萬條 JBIG2 指令和邏輯開建構出迷你電腦架構，有暫存器、加法器和比較器，可做基本運算，雖不像 Javascript 那麼快，但運作原理相同。

Project Zero 部落格指出，有了這台迷你電腦，就可透過 JBIG2 bootstrap 進入「沙盒」（SandBox）模擬電腦環境，之後透過模擬環境試跑真正的攻擊程式。

研究人員直言，「整件攻擊在這非常奇怪、模擬的環境執行。非常不可思議，也非常可怕。」

蘋果開吉、美國列入黑名單

由於這行為太惡劣，為防止更多濫用行為及損害使用者，造成資安問題，蘋果 11 月 23 日提告 NSO Group，並發出永久禁令，禁止其使用任何蘋果軟體、服務或裝置，還要求超過 75,000 美元賠償金。美國當局也將該公司列入出口管制黑名單。

飛馬今年 7 月遭指控入侵和竊聽世界各地記者、維權人士和企業高層的智慧手機，影響遍及多平台。後來監控名單流出，超過 5 萬筆電話號碼，含 189 名記者、85 位維權人士、65 名企業高層、600 多位政治人物和外交情報官員，甚至還有法國總統馬克宏等國家元首，震驚全球。

資料來源: 科技新報

2022/01 HomeKit漏洞

● 商業科技 資訊保安

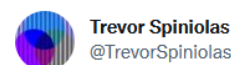
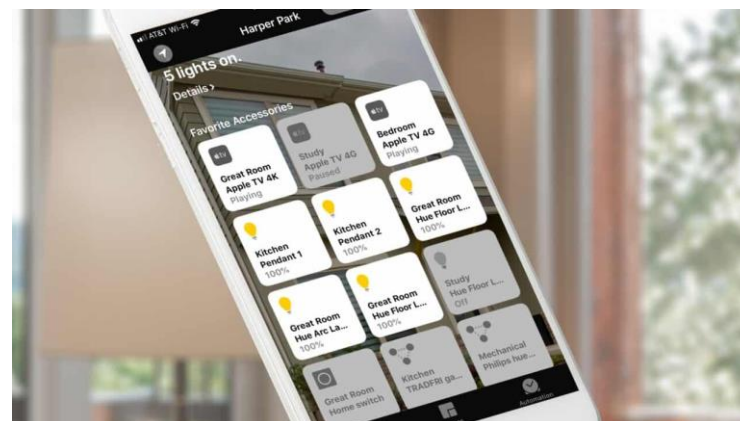
HomeKit 出現嚴重漏洞 Apple 去年 8 月得悉至今還未修復

網站 The Verge 日前報導指開發者 Trevor Spiniolas 在去年發現一項 HomeKit 有關的嚴重漏洞，並且向 Apple 作出匯報，Apple 在 8 月 10 日就知悉漏洞的存在，又著 Spiniolas 不要在 2022 年初之前將漏洞公開。然而 Spiniolas 指 Apple 並未有及時處理，漏洞由 iOS 14.7 發現至最新的 iOS 15.2 依然存在。

根據 Spiniolas 的說法，如果將 HomeKit 裝置的名稱設定到約 50 萬字，就會令 iOS 系統出現崩潰，同時陷入無止境的重啟狀態。雖然一般用戶都不會將名字設定成 50 萬字，但在 iOS 15 之前的系統版本，第三方案式擁有修改 HomeKit 裝置名字的權限，所以只要有人刻意搞局，就會令用戶的 iOS 裝置無法使用。

更惡劣的是 iCloud 能自動備份和還原 HomeKit 裝置名稱，令連接同一 iCloud 帳號的裝置都會因為同步而遭殃。此外，還有其他利用漏洞的方式，例如透過邀請加入家庭網絡去令其他裝置中招。仍然使用 iOS 14 或更早版本系統的裝置，要防範漏洞可以將 iCloud 同步關閉，或者將 Home Controls 從控制中心移除，將流動局限於 Home 程式而非整個 iOS 系統。

來源：[theverge](https://theverge.com)



Four months ago I discovered and reported a serious denial of service bug in iOS that still remains in the latest release. It persists through reboots and can trigger after restores under certain conditions.
trevorspiniolas.com/doorlock/doorl...

下午3:49 · 2022年1月1日 · Twitter for iPhone

資料來源: unwire.hk, @TrevorSpiniolas

2022/01 可偽裝關機的木馬

● 商業科技 資訊保安

iOS 木馬工具假扮關機 暗地開啟 鏡頭錄音監控

外界普遍認為採用封閉式系統的 iPhone 保安能力較高，不過安全研究機構 ZecOps 最近開發了一款名為 NoReboot 的木馬工具，不但能夠在無聲無息地以前置鏡頭和咪高峰監控用戶，還是 Apple 無法通過系統更新修復解決，用戶自保方法是避免越獄，並且只在 App Store 安裝程式。

由 ZecOps 研發的 NoReboot，是安全研究人員用作驗證概念的木馬工具，它能夠偽造出關閉 iPhone 的假象，欺騙裝置已經重新開機，這樣就能繞過 iOS 透過重新開機將惡意代碼清除的保安手段。只要不法份子將 NoReboot 整合到惡意程式，就能開啟前置鏡頭和咪高峰，在用戶不知情下攝錄和錄音監控，由於用戶以為 iPhone 已經關機，所以無法透過 iOS 狀態列知道鏡頭和咪高峰正在使用。

安全研發人員表示 NoReboot 並非利用系統漏洞的惡意程式，而是透過控制 InCallService、SpringBoard、Backboardd 後台守護進程，去脅持 iPhone 重新開機的控制權，以達到偽裝模擬開關機畫面，讓用戶以為 iPhone 已經重新啟動過。ZecOps 表示受到 NoReboot 攻擊的 iPhone，只要連接網絡就有機會被持續監控，甚至進行其他黑客行為。由於 NoReboot 未涉及系統漏洞，所以 Apple 無法通過更新修復，而且所有 iOS 版本都受到影響。




來源：[techeblog](https://techeblog.com)



資料來源: unwire.hk, zecOps

2022/01 Safari漏洞外洩瀏覽紀錄

Safari 有漏洞，用戶 Google 帳號資訊、歷史瀏覽紀錄恐外洩

作者 邱健芯 | 發布日期 2022 年 01 月 17 日 11:23 | 分類 Apple, iOS, iPadOS     138 

網路詐騙偵測解決方案開發商 Fingerprints 近期在部落格寫道，iOS 15、iPadOS 與 macOS 15 新 Safari (Safari 15 版) 出現嚴重漏洞，恐讓使用者個資與歷史瀏覽紀錄外洩。

Fingerprints 指出，這項漏洞是源自 Safari 瀏覽器 IndexedDB API 出現錯誤，資料顯示「IndexedDB 是為用戶端的儲存用 API，可用於大量結構化資料，並透過索引功能高效率搜尋資料」。

Safari 漏洞可允許任何使用 IndexedDB 的網站，追蹤用戶瀏覽的其他網站；舉例透過漏洞，當使用者從 Google 頁面轉到其他網頁瀏覽時，網頁就可存取 Google 帳號資訊。

這不僅意味不受信任或惡意網站能竊取用戶資訊，也代表用戶資訊赤裸裸攤在陽光下供人瀏覽。

有些人可能會想，那開啟 Safari 私密瀏覽模式就可以了？Fingerprints 也分析，這種情況下 Safari 15 私密瀏覽模式也無法防止個資外洩。

Safari 15 使用者該如何保護自己？Fingerprints 指出，使用者如果不採取嚴格防護措施，無法保全個資；如果使用者想保護自己，方式之一是預設阻止所有 JavaScript，並僅在信任的網站允許，但這會讓瀏覽網頁時相當不便。

另一種方式就是不要用 Safari，改用別的瀏覽器。



● 應用軟件 應用軟件 iOS App

修正 Safari IndexedDB 漏洞 iOS、iPadOS、macOS 同步更新



保安研究專家去年發現 Safari 瀏覽器的 IndexedDB API 漏洞，不法份子可以利用特別編寫的網站去取得網民的瀏覽歷史，還有登入過的 Google 帳號資料。這個影響用戶私隱的嚴重漏洞，在日前釋出的 iOS 15.3、iPadOS 15.3 和 macOS 12.2 得到修正。

除了修復 Safari 15 的 IndexedDB 漏洞，Apple 還同時堵塞了多個讓惡意程式執行任意程式碼，還有獲得系統權限的漏洞。由於今次系統更新對裝置的安全性有重大幫助，Apple 罕有地在更新訊息中加入「建議所有用戶安裝」的字眼。

除了 iOS、iPadOS 和 macOS，Apple 亦同步推出 watchOS 8.4 和 tvOS 15.2 的更新，以解決這些裝置的 Safari 15 漏洞。

來源：[Apple](#)

資料來源: 科技新報, unwire.hk

2022/10 iOS繞過VPN建立連線

iOS 16依然繞過VPN建立連線，洩露用戶資訊

先後有研究人員證實iOS 15、iOS 16都會繞過VPN和蘋果伺服器通訊，恐導致用戶資訊外洩，而且這類情況也同樣發生在Android

文/ 林妍濤 | 2022-10-18 發表

讚 1,556 分享

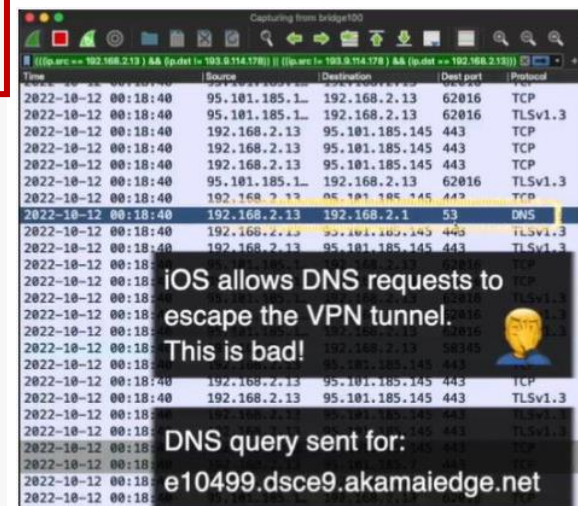
8月間一名研究人員指控蘋果刻意讓iOS 15繞過VPN和蘋果伺服器通訊。本周另一個安全團隊發現，到了iOS 16，這個問題仍然存在，手機啟用VPN後，用戶資訊仍然洩露。此外，Android也會繞過VPN和Google服務伺服器建立通訊。

研究人員Tommy Mysk及其團隊上周公布在安裝iOS 16.0.3的iPhone上，如何在開啟ProtonVPN後洩露用戶訊息的實驗。根據Mysk張貼的影片，當iPhone或iPad用戶開啟VPN下使用Apple Maps，攻擊者可以輕鬆查詢到他的IP位址、或DNS查詢目的地等資料。

Mysk說明，駭客其實只要一臺Mac和Wireshark封包分析軟體，就可以透過將目標裝置連到Mac同一個Wi-Fi網路，輕鬆監控任何裝置的網路流量。

8月間另一名研究人員披露蘋果刻意未將所有App導入VPN引發重視，當時研究人員實驗的是較舊版的iOS 15.4及15.5版，Mysk的實驗顯示在最新的iOS 16也有這問題。

研究人員對9to5mac表示，他相信蘋果是刻意這麼做的。上述App需要經常和蘋果伺服器建立連線，像是Find My及通知，因而研究觀測到的流量超出預期。不過研究人員認為，這些流量還是加密狀態，因此用戶資訊還是安全的。



資料來源: iThome, Tommy Mysk

2023/06 利用iMessage攻擊竊密

不知名的惡意程式利用iMessage攻擊iPhone用戶

卡斯基發現部分員工iPhone被植入新型間諜軟體，感染指標包括手機「資料使用」項顯示有BackupAgent的行程，也可能無法安裝iOS更新

文/ 林妍濤 | 2023-06-02 發表

讚 23 分享

安全廠商卡斯基基本周揭露有人以一個全新、不知名的惡意程式攻擊iPhone用戶，並企圖蒐集用戶行為資訊，受害者包含卡斯基員工。

該公司是在檢查公司內部無線網路時，發現員工iPhone有異常活動，隨後利用國際特赦組織開發的Mobile Verification Toolkit (MVT) 發現特定入侵指標。該公司並將這起攻擊行動命名為Operation Triangulation。

卡斯基執行長Eugene Kaspersky指出，調查分析才剛開始，尚無法得知這樁攻擊的完整面貌。目前僅知，攻擊行動是攻擊者傳送有惡意附件的iMessage給受害者，再利用多個已知iOS漏洞安裝惡意軟體。攻擊過程無需用戶任何動作，只要點選訊息即可安裝惡意程式，並啟動後續下載最終植入間諜軟體。該公司說，其中一個漏洞是蘋果去年12月就修補的CVE-2022-46690，是一個中度風險越界寫入 (out-of-bounds write) 漏洞。

一旦用戶iPhone被植入間諜軟體，就會開始蒐集iPhone中的麥克風錄音、iMessage的相片、定位及其他多種活動的資料，再送到外部伺服器上。卡斯基目前還在研究這間諜軟體，可以確定的是Operation Triangulation和之前已知的iOS間諜軟體，包括Pegasus、Predator或Reign都不同。

雖然受限於iOS設計，這個惡意程式無法長期在iPhone內長期滲透，但是卡斯基分析多個受害手機顯示，可能手機重開機會再度感染惡意程式。他們追查到最早感染時間為2019年，但到2023年6月，攻擊仍在進行中。最新近被感染的iOS版本為15.7版。

資料來源: iThome

2023/06 詐騙程式上架App Store

● 商業科技 資訊保安

成功突破 Apple 防線 假冒 Trezor Wallet 程式現身 App Store 騙錢

作者
唐美鳳

發佈日期
2023-06-22

閱讀時間
3分鐘

字體大小
A A A

分享

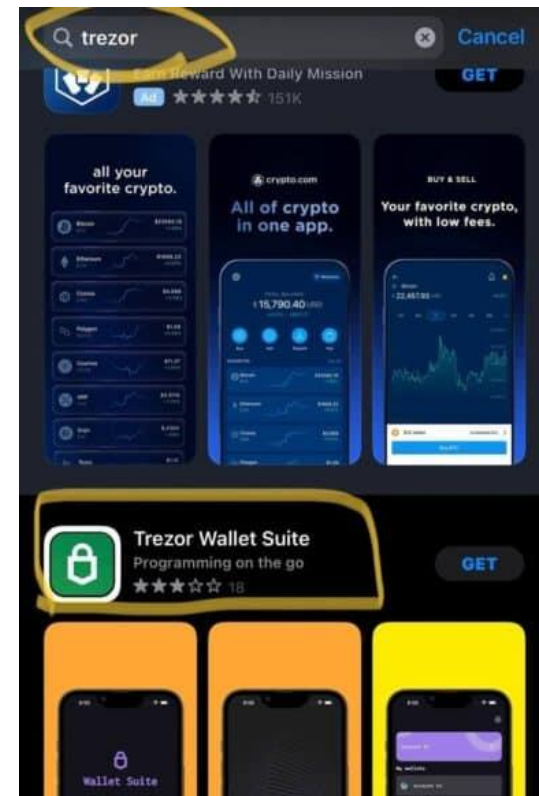
👍 讚好 26

🔗 分享

隨著加密貨幣技術日趨普及，相關的手機錢包程式亦越來越多，有不法之徒趁機推出假冒程式嘗試詐騙用戶，最近有一款甚至逃過 Apple 人員的審查，成功登陸 App Store。日前律師 Rafael Yakobi 在 Twitter 提醒網民，假冒的 Trezor Suite Lite 在 App Store 成功上架，更成為了搜索的榜首。

Yakobi 是專門協助加密貨幣相關開發者、投資者和組織的律師團隊 The Crypto Lawyers 成員，他日前在 Twitter 提醒網民一款名叫 Trezor Wallet Suite 的詐騙程式，在過去數星期成功在 App Store 上架，相信已經有數以千計 iPhone 或 iPad 用戶下載和受騙。Yakobi 建議最近曾經下載 Trezor 錢包的用戶，盡快確認是否下載了正版的 Trezor Suite Lite，而並非冒牌的 Trezor Wallet Suite。

詐騙程式 Trezor Wallet Suite 會要求用戶提供當遺失私鑰時，用作恢復的助記詞 (Seed Phrase)，並向程式的營運者開放所有加密資產的權限，在 Yakobi 的帖文下至少有一名用戶聲稱中招。在 Yakobi 發出警告後不久，涉事程式已經被下架，暫時未知為何冒牌貨能夠成功突破 Apple 防線和上架。



資料來源: unwire.hk

2023/09 漏洞被用來安裝間諜程式

蘋果上周修補的3個漏洞是被用來安裝Predator間諜程式

加拿大公民實驗室與Google威脅分析小組調查顯示，埃及政府疑似透過商業間諜軟體業者的協助，利用蘋果9月21日修補的零時差漏洞，在該國總統候選人的iPhone手機植入間諜程式Predator

文/ 陳曉莉 | 2023-09-25 發表

讚 85 分享

蘋果於上周四（9/21）緊急更新了3個已遭駭客濫用的零時差漏洞，提報漏洞的加拿大公民實驗室（Citizen Lab）與Google威脅分析小組分別在隔天揭露了攻擊場景，指出遭到攻擊的是手持iPhone的埃及總統候選人Ahmed Eltantawy，駭客利用相關漏洞在Eltantawy的手機上植入了間諜程式Predator。

公民實驗室說Predator的開發商是Cytrox，Google則說是Intellexa，這是因為有資安業者認為，Intellexa是由包括Cytrox、Nexa Technologies與WiSpear等商業間諜軟體業者共同設立的聯盟，共同開發與銷售Predator，目的是與打造Pegasus間諜程式的NSO Group相抗衡。不過，不管是Cytrox或Intellexa，都已經在今年7月被美國列入禁止商業往來的實體名單（Entity List）中。

Predator的功能與Pegasus類似，在成功植入手機後，它們即可存取手機內部的所有資料，從訊息、電話、照片到密碼，還可以隱藏程式，也能監控手機位置，或是啟動手機鏡頭與麥克風。

公民實驗室指出，曾擔任埃及議員的Eltantawy是在今年3月宣布要參選埃及總統，以取代現任總統Abdel Fattah el-Sisi的專治與鎮壓國家治理手段，之後Eltantawy的家人與支持者即開始受到各種騷擾與逮捕，Eltantawy則懷疑自己的手機受到危害，因而主動找上了該實驗室。

上周蘋果所修補的3個漏洞，分別是可用來執行任意程式的WebKit漏洞CVE-2023-41993，可繞過簽名驗證的CVE-2023-41991，以及可擴充本地端權限的CVE-2023-41992。

根據公民實驗室的調查，Eltantawy是在今年的8到9月間從iPhone造訪了幾個沒有使用HTTPS加密傳輸的網站，當時他使用的是Vodafone Egypt的行動網路，卻悄悄的被轉向到存放Predator的惡意網站。

PREDATOR IN THE WIRES

Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions

By Bill Marczak, John Scott-Railton, Daniel Roethlisberger, Bahr Abdul Razzak, Siena Anstis, and Ron Deibert

September 22, 2023 [Arabic translation](#)

Apple has [just issued an update for Apple products](#) including iPhones, iPads, Mac computers, and Apple Watches. We encourage all users to immediately update their devices.

Key Findings

- Between May and September 2023, former Egyptian MP Ahmed Eltantawy was targeted with Cytrox's Predator spyware via links sent on SMS and WhatsApp. The targeting took place after Eltantawy publicly stated his plans to run for President in the 2024 Egyptian elections.
- In August and September 2023, Eltantawy's Vodafone Egypt mobile connection was persistently selected for targeting via network injection; when Eltantawy visited certain websites not using HTTPS, a device installed at the border of Vodafone Egypt's network automatically redirected him to a malicious website to infect his phone with Cytrox's Predator spyware.
- During our investigation, we worked with Google's Threat Analysis Group (TAG) to obtain an iPhone zero-day exploit chain (CVE-2023-41991, CVE-2023-41992, CVE-2023-41993) designed to install Predator on iOS versions through 16.6.1. We also obtained the first stage of the spyware, which has notable similarities to a sample of Cytrox's Predator spyware we obtained in 2021. We attribute the spyware to Cytrox's Predator spyware with high confidence.
- Given that Egypt is a known customer of Cytrox's Predator spyware, and the spyware was delivered via network injection from a device located physically inside Egypt, we attribute the network injection attack to the Egyptian government with high confidence.
- Eltantawy's phone was additionally infected with Cytrox's Predator spyware two years prior, in September 2021, via a text message containing a link to a Predator website.

資料來源: iThome, Citizen Lab

2024/01 瀏覽網站顯示中毒警告？

iPhone中毒訊息是真的嗎？iOS 檢測木馬程式或中毒警告該怎麼辦

iOS教學, iPhone教學 / 2024-01-23 / 作者: 瘋先生 / iOS中毒, iPhone中毒檢測, iPhone掃毒, iPhone病毒, iPhone病毒掃描, 病毒掃描

iPhone中毒或被黑現象是怎麼回事？

相信很多 iPhone 用戶瀏覽特定網站或網頁時，會很常跳出「你的iPhone已經被病毒感染」、「發現病毒！正在拖慢你的iPhone速度」、「注意！發現病毒！你的iPhone受到x個病毒的嚴重破壞」、「危險！您的iPhone正訪問成人網站已被黑，且找到x個病毒！」等中毒或iPhone被黑、被入侵等警告訊息。

甚至有些會倒數計時造成你更恐慌，甚至有些還會好心提示，只要點擊下方按鈕刪除所有病毒或檢測，最後直接引導到 App Store 下載 App 的頁面。千萬不要傻傻去下載 VPN 就以為能防毒啊，有不少用戶不懂裝上後，導致 Siri 等功能都無法正常使用。

有些顯示更誇張，左上角還偽造 Apple Security 安全標誌，直接顯示 iPhone 病毒會嚴重破壞 iPhone SIM 卡，導致你的聯絡人、照片、數據和應用，甚至連同電池也會被感染造成損壞，對於不懂的用戶看到這消息肯定嚇死。

實際這些並不是真的 iPhone 中毒，其實是「欺騙性廣告 (Deceptive Advertising) 」，由網頁廣告代碼自動偵測手機型號，並不是真實 Safari 網頁有掃毒能力可以掃描 iOS 系統，更何況 App Store 也不讓任何一款防毒工具上架，也讓惡意廣告商可趁機藉由人性會因「警告提示文字」造成恐慌，讓你以為真的 iPhone 中毒，近一步誘導下載特定的 App，就能夠達到誘導欺騙目的。



1. 不要破解手機(越獄)
2. 不要點擊不明連結
3. 不要安裝來路不明的App
4. 開啟阻擋廣告
5. iPhone沒有掃毒、防毒App!

資料來源: 瘋先生

2024/02 木馬程式嘗試竊取個資

2024.02.20 | 資訊安全

iPhone 用戶注意！竊取「Face ID、銀行帳戶」木馬程式出現，4招防護措施快看

首款收集受害者Face ID的木馬程式GoldDigger出現了，正在以Android、iOS用戶為攻擊目標。犯罪集團如何展開攻擊？民眾如何預防？

網路安全公司Group-IB在近期指出，研究團隊發現全世界第一款收集受害者臉部辨識資料的木馬程式——GoldDigger，正在針對iPhone用戶發動攻擊，以竊取使用者的銀行帳戶、電子支付資訊、身分證件等個人資料。

Group-IB表示，由於懷疑GoldDigger將成為亞太地區日益嚴重的威脅，已立即向相關部門發出警報，保護客戶免受損害。

從Android攻擊到iOS系統！木馬程式GoldDigger恐怖在哪？

早在去年7月份，Group-IB就已經在部落格揭露GoldDigger的存在。犯罪組織GoldFactory最初以Android設備為目標，並且針對越南50多家金融機構的網路銀行、加密錢包進行攻擊；隨著惡意程式不斷繁衍進化，GoldDigger現在出現了iOS版本，攻擊範圍也延伸至越南、泰國以外的亞太地區。

Group-IB的研究人員發現，GoldDigger的iOS版本能夠收集臉部辨識資料、身分證件並攔截手機簡訊（Android版本具備相同攻擊手法），駭客利用偷來的生物辨識數據，進一步採用AI驅動的深偽技術（Deepfake），未經授權就能夠成功存取受害者的銀行帳戶。Group-IB推測，這是新型態的貨幣盜竊技術。

與GoldDigger相關受害者可能已經出現。今年2月，有消息指出一位越南民眾完成應用程式（App）發起的請求驗證，其中包含臉部辨識掃描，結果遭竊取大約4萬美元的資金。Group-IB認為：「我們目前沒有任何證據表明GoldPickaxe（GoldDigger的變體）在越南也有散布，但根據新聞提到的『臉部掃描』，再加上GoldFactory在該地區活躍的事實，我們懷疑犯罪分子已經開始在越南使用GoldPickaxe，預計當地很快就會出現更多案例。」

.....

Group-IB發現，GoldFactory犯罪分子主要結合「網路釣魚」技術發動攻擊。

舉例來說，在泰國，犯罪集團透過冒充政府當局身分，說服受害者使用當地最受歡迎的通訊軟體LINE互加好友並開始對話。在聊天過程中，犯罪分子會發送惡意連結，誘導民眾安裝某款號稱「數位退休金」的詐騙App，聲稱能夠以數位的方式領取退休金，或者假冒「泰國政府資訊入口網站」的App，實際在不知不覺中偷走所有機敏資料。

還有另一種詐騙情境：詐騙集團會廣撒電費退稅的詐騙簡訊，一旦收件人點開連結，就會被立刻導向LINE，並將犯罪分子添加為好友。接下來的詐騙手段就跟前者一致了，民眾乖乖遵循指示、安裝惡意應用程式，然後個資遭竊。



1. iOS、Android用戶儘快將手機系統升級至最新版本
2. 不要隨便點擊來路不明的網路連結
3. 謹慎授權第三方App使用Face ID資料
4. 不要安裝TestFlight上的應用程式，資安風險高

資料來源: 數位時代

2024/04 間諜軟體鎖定特定人士

蘋果呼籲92國用戶小心傭兵間諜軟體

針對商業間諜軟體企圖入侵特定iPhone用戶的攻擊行動，蘋果宣布會以電子郵件發布威脅通知 (threat notification) 給高風險用戶，也建議所有用戶啟動iPhone或iPad的封閉模式 (Lockdown Mode) 以預先阻斷惡意軟體入侵途徑

文/ 林妍濤 | 2024-04-12 發表

讚 194

分享

蘋果本周對印度等92國產品用戶發出警告通知，要用戶小心防範傭兵間諜軟體 (mercenary spyware) 的攻擊，竊取用戶重要資訊。

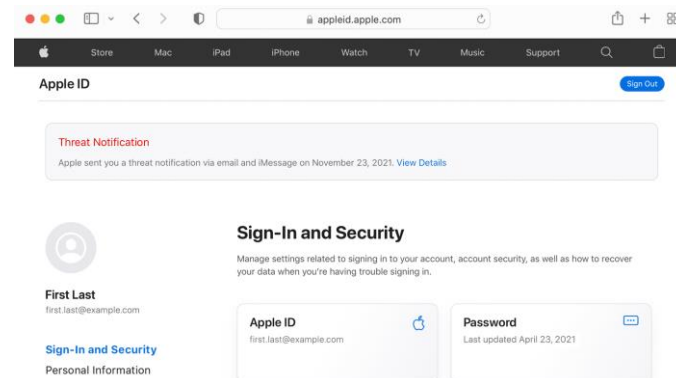
印度《經濟日報》及《路透社》周四報導，蘋果以電子郵件發布威脅通知 (threat notification) 給有風險的用戶。蘋果說，已偵測到某名用戶正遭到鎖定，傭兵間諜軟體試圖遠端駭入和特定Apple ID關聯的iPhone。

蘋果警告用戶，傭兵間諜軟體是基於特定用戶身分或其從事的工作發動攻擊，雖然難以100%確定，但蘋果有高度信心 (已發生攻擊) ，要用戶不要掉以輕心。

蘋果周四稍晚也在官網公布關於威脅通知的資訊。這通知是為了告知並協助可能遭傭兵間諜軟體鎖定的用戶而設計。這類軟體由專門開發監控軟體的公司開發，並銷售給政府、情報機關等客戶以監控特定個人，如記者、人權運動、政治人物或外交人員。傭兵間諜軟體使用者絕大多數是國家或國家駭客。蘋果特別點名以色列業者NSO Group開發的Pegasus作為舉例。

這是蘋果第二次發布和傭兵間諜軟體威脅通知。去年10月蘋果也曾警告用戶小心「國家資助」 (state sponsored) 的竊密攻擊，不過這次已移除了這個字眼。

安全專家多次偵測到記者、歐美官員或政治人物等人iPhone被植入Pegasus以蒐集情資。蘋果本周在給用戶的通知中並未說明攻擊者、攻擊型態或何時發生的攻擊。



- 1.升級到最新版作業系統
- 2.設立passcode
- 3.Apple ID使用強密碼及雙因素驗證
- 4.只從Apple Store下載App
- 5.線上服務使用強密碼
- 6.不要點選來路不明的網頁連結或附件

資料來源: iThome, Apple

2024/04 拼音輸入法潛藏資訊洩漏

多款拼音鍵盤輸入法存在漏洞，有可能向攻擊者洩漏輸入內容

加拿大公民實驗室 (Citizen Lab) 指出，廣泛受到中國用戶採用的拼音輸入法，與雲端架構的通訊上存在弱點，而有可能讓攻擊者得知用戶輸入的內容並進行監控

文/ 周峻佑 | 2024-04-25 發表

讚 6 分享

開發者為了能讓中文輸入法應用程式能預測使用者接下來可能會輸入的文字，往往透過雲端提供相關功能，但若是沒有充分的保護措施，這種輸入法很有可能被攻擊者當作監控軟體，或是另類的「鍵盤側錄工具」。

對此，加拿大公民實驗室 (Citizen Lab) 對於中國市面上常見的拼音輸入法著手進行調查，他們針對9家供應商的Windows、iOS、安卓版輸入法程式進行檢測，結果發現，除華為以外的供應商，他們提供的輸入法軟體都存在漏洞，而能被攻擊者得知用戶輸入的內容。

研究人員估計，約有近10億使用者會受到上述輸入法的弱點影響。因為，光是搜狗、百度、科大訊飛 (iFlytek) 的輸入法，在中國第三方輸入法市占就超過95%，約有10億人使用。

另一方面，榮耀、Oppo、小米裝置預載的輸入法，也曝露上述危險，而這3個廠牌的智慧型手機去年在中國擁有近50%市占。

對此，他們向所有輸入法供應商通報漏洞，大多數都做出回應並進行修補。值得注意的是，百度修補了他們獲報最嚴重的漏洞，但仍有部分尚未處理；對於QQ拼音的部分，騰訊宣稱將在今年第1季升級旗下產品採用HTTPS通訊，但截至4月1日，研究人員發現該公司並未發布新版修補相關漏洞。

Device manufacturer	Own	Sogou	Baidu	iFlytek	iOS	Windows
Samsung	XX	✓*	XX	N/A	N/A	N/A
Huawei	✓*	✓	N/A	N/A	N/A	N/A
Xiaomi	N/A	X*	XX	XX	N/A	N/A
OPPO	N/A	X	XX*	N/A	N/A	N/A
Vivo	✓*	X	N/A	N/A	N/A	N/A
Honor	N/A	N/A	XX*	N/A	N/A	N/A

資料來源: iThome, Citizen Lab

2024/04 合法第三方iOS市集上線

首家合法的第三方iOS市集AltStore PAL上線

AltStore PAL類似蘋果的網頁發布 (Web Distribution) 功能，讓歐盟地區使用者可直接自第三方網站下載iOS程式

文/ 陳曉莉 | 2024-04-18 發表

15 讚

在歐盟《數位市場法》(Digital Markets Act) 迫使蘋果於歐洲經濟區開放第三方市集與外部支付後，由獨立開發者Riley Testut打造的第一家合法第三方iOS市集AltStore PAL於本週三 (4/17) 上線了，它鼓勵任何通過蘋果公證的行動程式透過該市集發布，為了支付蘋果所要求的核心技術費用 (Core Technology Fee)，AltStore PAL每年將向使用者收取1.5歐元。

Testut過去就曾打造第三方iOS市集AltStore，只是AltStore並不合法，而AltStore PAL則是通過蘋果認證的第三方市集，目前僅提供了兩個程式，都是由Testut所開發，分別是任天堂模擬器Delta，以及可於背景執行的剪貼簿管理程式Clip。

AltStore PAL也是個開源的市集，市集中的所有行動程式都是由開發者自行代管的，一旦所開發的程式經過蘋果的公證，開發者就可下載一個替代遞送封包 (Alternative Distribution Packet, ADP)，再將它上傳到自己的伺服器上。而若要透過AltStore PAL遞送，開發者則必須建立一個「來源」(Source)，這是個JSON檔案，內含上傳至公開URL的程式元資料，只要使用者將此一Source加入AltStore PAL中，就可在AltStore PAL上看到來自該Source的所有程式。

Testut說明，Source是AltStore PAL的核心概念，可完全地去中心化，在AltStore PAL上所看到的所有程式，都是由使用者主動添加Source而出現的，該機制同樣也允許開發者自行推廣程式，並將使用者導至開發者網站。

AltStore PAL類似蘋果所推出的網頁發布 (Web Distribution) 功能，讓使用者可直接自第三方網站下載程式，Testut坦承，它們的確是同樣的概念，與其說是市集，AltStore PAL更像是一個美化過的側載工具，它只負責讀取JSON檔案，而且會在程式更新時自動通知使用者。

Testut鼓勵那些遭到蘋果App Store審核機制拒絕的獨立開發者透過AltStore PAL來遞送程式，而只要安裝iOS 17.4及以上版本的歐盟地區使用者則可直接透過AltStore網站來安裝AltStore PAL。



資料來源: iThome, AltStore

iOS漏洞也持續在修補

蘋果緊急更新iOS與macOS等平臺，修補3個已遭濫用的零時差漏洞

蘋果在9月21日緊急修補的3個零時差漏洞涉及不同平臺，目前已知的針對性攻擊行動則都鎖定使用iOS 16.7以前版本的iPhone

文/ 陳曉莉 | 2023-09-23 發表

讚 933 分享

蘋果周四 (9/21) 緊急更新了macOS、iOS、iPadOS、watchOS及Safari，修補3個已經遭到駭客濫用的零時差漏洞。

此次蘋果所修補的安全漏洞分別是CVE-2023-41991、CVE-2023-41992與CVE-2023-41993，其中的CVE-2023-41991允許惡意程式繞過簽名驗證，此一漏洞同時存在於macOS、iOS、iPadOS及watchOS上。CVE-2023-41992則為核心漏洞，允許本地端駭客擴充權限，亦同時存在於macOS、iOS、iPadOS及watchOS上。

CVE-2023-41993漏洞位於WebKit中，其網頁內容處理功能可能導致任意程式執行，主要影響iOS、iPadOS與Safari。

雖然上述漏洞涉及不同的平臺，但迄今所發現的攻擊行動皆是鎖定iOS 16.7以前的iOS版本，顯示實際遭到攻擊的裝置為iPhone。此外，相關漏洞都是由加拿大公民實驗室 (Citizen Lab) 的Bill Marczak與Google威脅分析小組的Maddie Stone所提報。

本月上旬蘋果才修補了兩個亦是由公民實驗室發現的零時差漏洞，當時駭客利用這兩個漏洞入侵了iPhone，並植入Pegasus間諜程式。今年以來蘋果所修補的零時差漏洞數量已達到16個。

Apple security updates and Rapid Security Responses

Name and information link	Available for	Release date
iOS 17.4.1 and iPadOS 17.4.1	iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later	21 Mar 2024
iOS 16.7.7 and iPadOS 16.7.7	iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation	21 Mar 2024

iOS 17.4.1 和 iPadOS 17.4.1

2024 年 3 月 21 日發行

CoreMedia

適用於：iPhone XS 和後續機型、iPad Pro (12.9 吋，第 2 代和後續機型)、iPad Pro (10.5 吋)、iPad Pro (11 吋，第 1 代和後續機型)、iPad Air (第 3 代和後續機型)、iPad (第 6 代和後續機型)，以及 iPad mini (第 5 代和後續機型)

影響：處理影像可能導致執行任何程式碼

說明：改進輸入驗證機制後，已解決超出界限的寫入問題。

CVE-2024-1580：Google Project Zero 的 Nick Galloway

WebRTC

適用於：iPhone XS 和後續機型、iPad Pro (12.9 吋，第 2 代和後續機型)、iPad Pro (10.5 吋)、iPad Pro (11 吋，第 1 代和後續機型)、iPad Air (第 3 代和後續機型)、iPad (第 6 代和後續機型)，以及 iPad mini (第 5 代和後續機型)

影響：處理影像可能導致執行任何程式碼

說明：改進輸入驗證機制後，已解決超出界限的寫入問題。

CVE-2024-1580：Google Project Zero 的 Nick Galloway

資料來源: iThome, Apple

蘋果與安全人員合作找出弱點

蘋果讓研究人員找出130多項iPhone重大漏洞

為了更快找出影響iOS的安全漏洞，蘋果已連續四年透過安全研究裝置方案以及漏洞獎勵計畫，與外部安全研究人員合作抓漏，現在蘋果宣布明年度的安全研究裝置方案正式開放外界申請加入

文/ 林妍濤 | 2023-08-31 發表

讚 903 分享

iPhone 15公布在即，蘋果再次強調iPhone的安全性，昨（30）日公布過去4年來，蘋果在和安全研究人員合作下，修補了iPhone超過130項重大漏洞。

蘋果從2019年起，在安全研究裝置方案（Security Research Device Program）下提供特別準備的iPhone給參與計畫的研究人員，允許他們找出iOS安全漏洞而無需苦苦繞過種種安全防護。最重要的是，在這計畫下通報的任何漏洞，都會列入蘋果安全獎勵方案給予獎金。蘋果指出，自4年前推行以來，SRDP研究人員共發現130項高影響性的重大安全漏洞，研究發現使蘋果得以實作緩解方案以保護iOS平臺。單單在過去6個月內，研究人員發現就有36項列為漏洞，受影響元件涵括XNU核心、核心擴充程式、XPC服務。

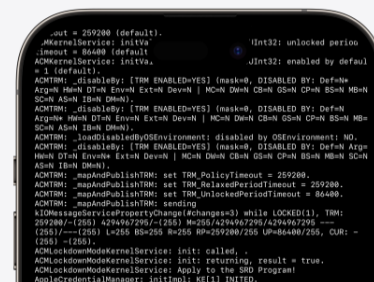
有些在本方案找到的安全漏洞也拿到了蘋果頒發的抓漏獎勵。歷來透過SRDP，蘋果共針對100多項漏洞頒發50萬美元獎金，獎金中位數約為1.8萬美元。

今年SRDP計畫又開始了。今年SRDP的核心主體是一為安全研究特製的iPhone 14 Pro，加上一些相關工具，供研究人員可以使用，他們可以選擇任何策略來設定或關閉iOS的進階安全防護，這些防護在平常iPhone上是不可能為一般用戶關閉的。

在這項方案中，蘋果允許研究人員安裝和啟用核心快取、以任何權限執行任意程式碼，包括以平臺或以根權限。他們也可以設定SNVRAM變項、安裝和啟動iOS 17上的SPTM（Secure Page Table Monitor）及TXM（Trusted Execution Monitor）。而即使一些通報的漏洞已經先行修補過，參與者仍然可以在特製的iPhone上持續其研究。

How it works.

The Security Research Device (SRD) is a specially fused iPhone that allows you to perform iOS security research without having to bypass its security features. Shell access is available, and you can run any tools, choose your own entitlements, and even customize the kernel. Using the SRD allows you to confidently report all your findings to Apple without the risk of losing access to the inner layers of iOS security. Plus, any vulnerabilities that you discover with the SRD are automatically considered for [Apple Security Bounty](#).



資料來源: iHome, Apple

快速安全更新 (Rapid Security Update)

蘋果釋出第一批修補零時差漏洞的快速安全更新

蘋果快速安全更新以自動安裝模式，針對最新版iOS、iPadOS及macOS裝置修補零時差漏洞

文/ 林妍濤 | 2023-05-02 發表

蘋果昨 (1) 日釋出第一批快速安全更新，以修補最新版iOS、macOS的零時差漏洞。

蘋果是在去年6月公布macOS Ventura時宣布快速安全更新 (Rapid Security Update)，這是在常規的安全更新以外，針對iOS及macOS已經遭到濫用的漏洞釋出的緊急安全修補程式，類似微軟的例外安全更新 (out-of-band security update)。

根據蘋果說明，快速安全更新僅提供給最新版iOS、iPadOS及macOS，將從iOS/iPadOS 16.4.1與macOS 13.3.1開始。用戶iPhone、iPad及Mac電腦會自動安裝快速安全更新，一般不需重新啟動裝置，必要時會有提示用戶重啟。當安裝完成在系統顯示的軟體版本碼後會出現英文字母，例如iOS 16.4.1 (a)、iPadOS 16.4.1 (a)或macOS 13.3.1(a)。

iOS用戶可以透過「設定」>「一般」>「軟體更新」>「自動更新」下的「安全回應&系統檔案」開啟或關閉。Mac電腦上，該功能位於蘋果選單下的「系統設定」>側邊欄的「一般」>右方的「軟體更新」>「自動更新」中的「顯示細節資訊」中，啟動「安裝安全回應與系統檔案」可以開啟接收。若用戶選擇關閉或不安裝，用戶裝置會在下一次的常規軟體更新中獲得這些安全更新。

不過蘋果並未說明這波快速安全更新修補的是什麼漏洞。Techcrunch報導，間諜軟體開發商如QuaDream及NSO Group都曾經開發濫用iOS或Mac漏洞的竊密程式，以服務其政府客戶。此外，上周安全廠商Cyble也發現一隻macOS竊密程式Atomic macOS Stealer (AMOS)，後者可透過漏洞或釣魚網站散布並攻擊Mac電腦用戶。



資料來源: iThome, Apple

2022 App Store安全稽核報告

去年蘋果審核逾610萬個程式，有170萬個被打回票

根據蘋果2022年App Store安全稽核報告，有5.7萬個不安全iOS App即使被拒於App Store門外，仍透過第三方案式市集散布

文/ 陳曉莉 | 2023-05-17 發表

讚 30 分享

蘋果本周公布了2022年的App Store安全稽核狀況，指出去年總計審核了超過610萬個程式，拒絕了其中的170萬個，通過審核的比例為72%。

根據蘋果的統計，App Store團隊平均每周審核逾10萬個程式，接近90%的程式會在提交的24小時內進行審核，去年總計審核了逾610萬個程式，並有18.5萬名開發者是首次提交程式至App Store。

行動程式要登上App Store前會面臨許多安全關卡，先是Xcode會系統性地檢查程式是否使用合法技術並符合App Store的最低要求，在開發者將程式上傳至App Store Connect之後，再檢查程式是否採用私有的APIs或含有已知惡意程式，最後才由App Review團隊來確保它符合蘋果的品質與安全標準。

從蘋果提供的數據可看出，去年有27.8%的程式被拒於App Store門外，當中有40萬個程式是因為侵犯使用者隱私而遭拒，另有超過15.3萬個程式則是因垃圾訊息、抄襲或誤導而被打回了票，還有近2.9萬個程式則是因隱藏或未紀錄其功能而遭拒。

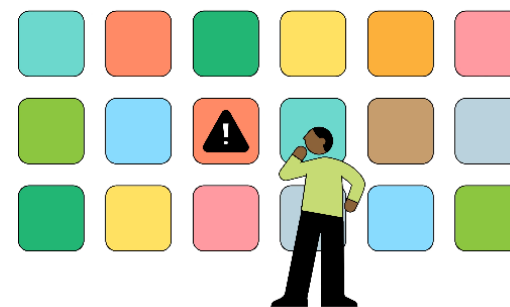
此外，去年也有不少惡意程式企圖闖關，有的程式可自第三方服務來竊取使用者憑證，有的則是偽裝成無害的金融管理平臺，之後卻可變身為其它程式。蘋果去年封鎖或移除了2.4萬個相關程式。

值得注意的是，蘋果特別強調該公司的把關，讓5.7萬個不可靠的程式未能登上App Store，這些程式雖然支援iOS與iPadOS，卻不是透過App Store散布，而是來自於其它的第三方案式市集，且它們可能危害使用者的安全及隱私。



UPDATE
May 16, 2023

App Store stopped more than \$2 billion in fraudulent transactions in 2022



Today, Apple announced that in 2022, the App Store prevented over \$2 billion in potentially fraudulent transactions, and rejected nearly 1.7 million app submissions for failing to meet the App Store's high standards for privacy, security, and content.

資料來源: iThome, Apple

iOS / iPadOS版本分佈

- 截至2024/02有**66%**裝置運行iOS 17，僅**11%**裝置運行iOS 15前版本；近4年發表的裝置有**76%**運行iOS 17
- 因為OS與硬體都是Apple設計，故更新推出速度較Android快

iOS and iPadOS usage

As measured by devices that transacted on the App Store on February 4, 2024.

iPhone



76% of all devices introduced in the last four years use iOS 17.



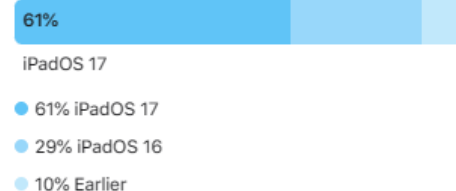
66% of all devices use iOS 17.



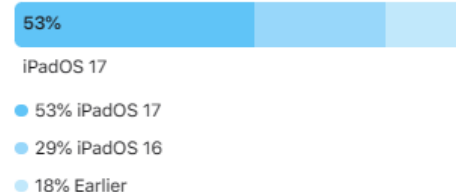
iPad



61% of all devices introduced in the last four years use iPadOS 17.



53% of all devices use iPadOS 17.



資料來源: Apple



其他/共通的安全性議題

• 硬體弱點影響Android/iOS兩大行動系統平台

逾20款安卓手機恐陷駭客攻擊漏洞！Google曝2招避險

2023/03/18 12:00
文 / 記者吳佩樺

Google Project Zero 資安團隊公布由三星在2022年底至2023年初生產的Exynos數據晶片出現18個零時差漏洞，包括Google、三星、vivo等手機皆採用，總計超過20款以上安卓手機都有可能遭受駭客攻擊。

據稱當中4個最嚴重的漏洞將允許網路至基頻的遠端程式攻擊，駭客只需得知手機號碼就能展開攻擊，不用跟使用者互動。從公布的名單，多款暢銷手機都入列，包括Google Pixel 6、Pixel 7系列，以及三星S22系列、A53等。

三星對此回應，去年底收到Google Project Zero的通知，已經針對漏洞提供所有客戶修復版本，相關問題已經解決。Google也說，Pixel手機在3月的安全更新將陸續獲得修復。

Google Project Zero提出建議，對自己手機安全有疑慮者，建議關閉VoLTE跟WiFi通話兩功能，藉此避免被駭。

●可能受影響的設備

●三星→S22、M33、M13、M12、A71、A53、A33、A21s、A13、A12 和 A04系列

●Google→Pixel 6、7系列及6a

●vivo→S16、S15、S6、X70、X60、X30系列

●任何使用Exynos Auto T5123 晶片組的車輛

蘋果 Mac 驚爆有無法修復的漏洞！近三代電腦全中槍

2024/03/26 10:36
文 / 記者黃肇祥

蘋果 Mac 電腦驚傳存在無法修復的安全漏洞，包含最新發表的 M3 晶片在內，近三代的產品全都中槍。

根據外媒《ars TECHNICA》引述一份最新論文指出，蘋果自製晶片包含 M1、M2 以及 M3 在內，皆存在名為「GoFetch」的安全漏洞，可以讓駭客竊取 Mac 電腦內的安全密鑰。最麻煩的地方是，漏洞來自於晶片內的「微架構」缺陷，因此無法直接進行修復。

目前唯一的解法是透過第三方安全軟體的防禦措施來緩解，但報告也提到，此作法會降低 M 系列的效能表現，其中又以 M1、M2 影響最多。主要是因為，與本次漏洞密切關連的資料預取器（DMP），在 M3 機型上是可以由開發者選擇停用的，M1、M2 則沒有設計這項機制。

儘管如此，不過外媒《9to5mac》表示一般使用者無須擔憂，因為要成功透過 GoFetch 展開進攻，駭客首先要先誘騙受害者安裝惡意軟體，而且研究人員更發現，惡意軟體必須持續運行長達 54 分鐘至 10 小時不等，代表說，想要進攻此漏洞並不是那麼容易。



資料來源: 自由時報

外接裝置的風險

外國研發竊取資料Lightning線【有片睇】作為資安滲透測試工具



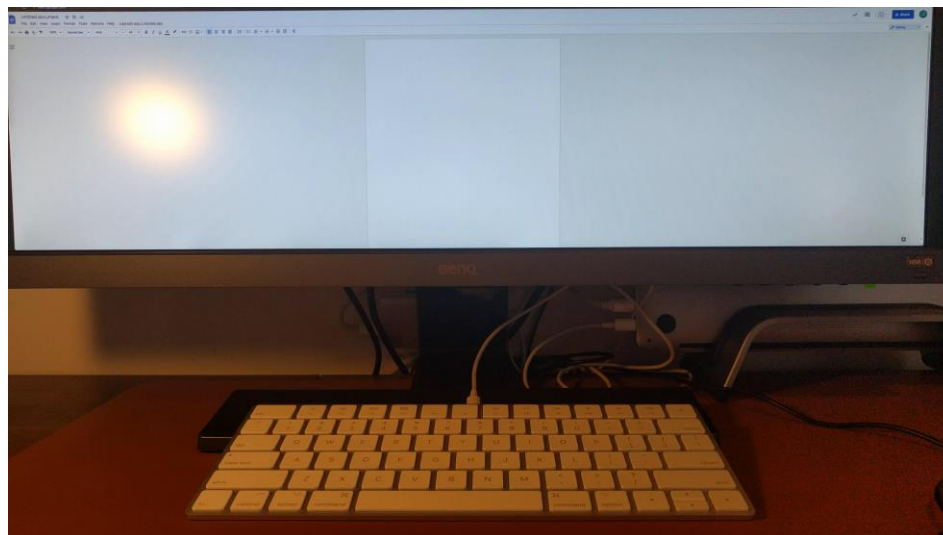
從外表上完全分不出那條有做過手脚

近日外國資訊安全研究人員 MG 研發了一條 Lightning 充電線。你可能會問，Lightning 充電線有甚麼特別？原來這條 Lightning 的充電線，可以竊取用戶在裝置上的資訊，而且看起來跟普通的 Lightning 充電線一模一樣，令人防不勝防。

據外媒報道，該充電線名為「OMG 充電線」，是開發用來作測試滲透工具使用，早在 2019 年已經在 DEFCON 駭客會議上發表，今次此款是新版本，該外國資訊安全研究人員表示已經將此款充電線量產，並由網絡安全供應商 Hak5 售賣。

該充電線內含一個駭客晶片，只要連接到你的裝置上，並且在裝置上輸入資訊，該 OMG 充電線便可以竊取用戶輸入的資訊，包括密碼、文字都會被紀錄。而且有心人還可以購買 Thunderbolt/USB-C 轉接頭，就算 iPad 或 Mac 都可用。

MG 表示，這條 OMG 充電線在網絡上面有售，雖然研發的原意是用作測試滲透，但有心人還是有可能用來做惡意工具，偷取用戶的個人資料。



資料來源: unwire.hk, motherboard

惡意廣告與社交工程攻擊(1/2)

17黑客快閃行動！發2銀行「釣魚簡訊」 6 天捲千萬：彼此不認識

記者邱中岳／台北報導

2021/10/02

刑事局接獲民眾報案，近日接連收到「國泰世華網路銀行」簡訊，內容顯示帳號異常要對方輸入帳號密碼，最後民眾戶頭存款全被用領，估計有2家銀行，61名民眾上當，估計損失上千萬，警方也在9月27日逮捕設計相關釣魚簡訊的嫌犯17人，才發現原來是主嫌「網路號召」的臨時犯罪集團。

警方調查，33歲的莊姓主嫌在網路號召17人組「臨時犯罪集團」，從2021年開始冒用「國泰世華網銀」的釣魚簡訊，內容寫道「【國泰世華】您的銀行帳戶顯示異常，請立即登入綁定用戶資料，否則帳戶將凍結使用」。

有被害人一時沒注意登入假網銀頁面，並輸入網路銀行帳號以及密碼，莊嫌等人取得資料後隨即將被害人銀行帳戶轉至人頭帳戶，被害人帳戶瞬間被清空，莊嫌等人等錢到手後，再將錢送入水房進行洗錢作業。

警方指出，從2021年1月27日至29日，國泰世華銀行客戶被害26人，損失671萬，2月份台新銀行客戶被害35人損失409萬，2起案件共計61人被害，損失金額達1080萬元。

警方經過數月調查，最後鎖定莊姓嫌犯等17人涉案，最後前往台中逮人，並起獲手機、電腦、分享器、存摺以及提款卡、對帳表、現金50萬元，訊後依照詐欺、《組織犯罪條例》等罪嫌將莊嫌等人送辦。

警方指出，莊姓主嫌私立大學資訊相關科系畢業，在網路號召有同樣背景的17名嫌犯，並且組成犯罪集團，從製作假網站以及釣魚簡訊，並隨機發送給不特定人士。



被害人受害之過程



資料來源: ETtoday

惡意廣告與社交工程攻擊(2/2)

● 科技娛樂 生活科技

滙豐銀行釣魚短訊騙案 六旬男子 被騙\$275萬



短訊騙案層出不窮，最近有人報案揭發，有騙徒假冒香港上海滙豐銀行發出「網絡釣魚」短訊，並誘騙市民點擊進入偽冒銀行網站的連結，輸入帳戶資料及密碼，騙徒其後再將受害人戶口內的款項提走，而其中一名六旬男子更損失\$275萬港元。滙豐提醒若收到類似偽冒手機短訊，不要點擊或提供任何個人資料。

近日有騙徒假冒香港上海滙豐銀行發出「網絡釣魚」短訊，短訊內指其戶口出現異常，或無故新增了收款人等異動，吸引當受害人點擊進入偽冒銀行網站的連結，再誘騙受害人輸入帳戶資料及密碼。騙徒其後再將受害人戶口內的款項提走。由於短訊透過滙豐銀行的電話號碼發出，令人不虞有詐直接點擊，其中一名六旬男子更因此損失 \$275 萬港元。

滙豐銀行澄清該行與偽冒手機短訊及網站並無任何關係，並提醒如果收到類似偽冒手機短訊，不要點擊任何連結或提供任何個人資料。滙豐亦重申其香港網址為 <http://www.hsbc.com.hk>。若要使用任何銀行服務，亦應在瀏覽器上輸入正確網址。而現時滙豐正與有關方面合力關閉偽冒網站。

以下為有關偽冒手機短訊及網站的截圖：

偽冒手機短訊

A new payee has been added today. If this was not you, visit: <https://secure-hk.com/hsbc>

A new payee has been added today. If this was not you, visit: <http://authorise-support-host.com>

A new payee has been added today. If this was not you, visit: authorise-hk-payment.com

A new payee has been added today. If this was not you, visit: <http://authorise-host-support.com>

提高警覺慎防釣魚簡訊

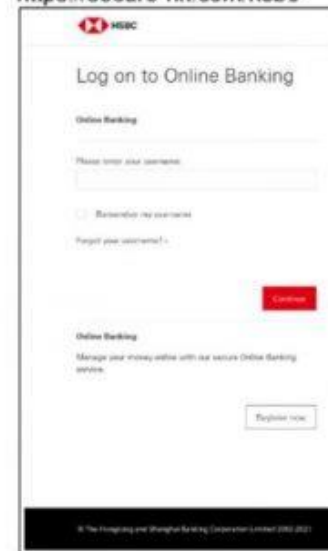
1.短網址

2.註冊類似域名

看到輸入欄位要求填入
帳號、密碼要再次確認

偽冒網站

<https://secure-hk.com/hsbc>



<http://authorise-support-host.com>



資料來源: unwire.hk

App連線安全

- 有些App的通訊未採用加密
- 或是即使採用了加密連線，也沒有驗證憑證有效性
- 或是使用過舊TLS版本
- 下場：機敏資料被竊聽



從App資安檢測經驗，看國內App開發3大常見問題

對於臺灣行動App的開發，有哪些常見安全問題？安華聯網在他們檢測過的國內400支左右App中，當中包含4成是金融領域App，2成是政府單位，其他還包括行動支付、教育、醫療與運動產業，發現3類常見風險最容易發生。若對應OWASP Mobile Top 10的風險類別，分別是不安全的資料儲存 (Insecure Data Storage)、不安全的傳輸行為 (Insecure Communication)、用戶端程式碼品質問題 (Client Code Quality)。

其中又以前兩種最嚴重，都有近50%比例有此狀況存在。不論企業自行開發或是委外，都應該要及早注意。

資料傳輸不安全

大多數App都有網路通訊能力，需要與雲端伺服器應用程式去取得對應的資料，但在連線過程當中，很多開發人員往往會忽略相關安全。此時可能有3個狀況，包括：未以加密方式 (HTTPS) 傳輸敏感性資料，未檢查憑證來源，以及使用過舊的TLS版本。

他解釋，部分開發人員不知道要採用HTTPS加密連線傳輸，僅用明文HTTP傳送資料，如此一來，經由這種方式傳輸的帳號密碼資料，都很容易被看光。

而他更要提醒的是，雖然現在大家開始知道要採用HTTPS，但還是有些地方要注意。例如，一旦App未檢查連線安全性，此時，駭客可以運用中間人攻擊，讓App以為跟伺服器連線，實際卻是跟駭客電腦連線，這將導致訊息被竊改、資料遭竊，以及被植入惡意程式等風險。

探究其原因，在於開發者疏於檢查憑證，導致App無法識別伺服器的真假，因此在實驗室檢測的過程中，還是可以看到傳輸的資料內容。

不僅如此，他觀察到有客戶對於HTTPS認知甚少，因為開發者使用了老舊且不安全的TLS 1.0，並在TLS採用了RC4演算法。

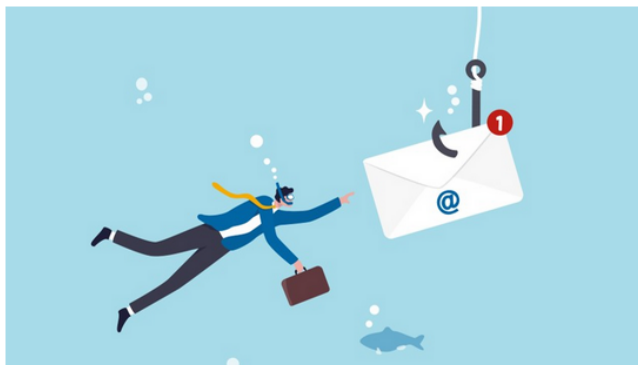
把惡意連結藏在QR Code (1/2)

電郵中嵌入惡意QR Code的新型釣魚手法

2021 / 12 / 03 作者：國際瞭望
分類：發展, 社群, 資安
Tags：QR code, 即時訊息, 國際瞭望, 網路釣魚



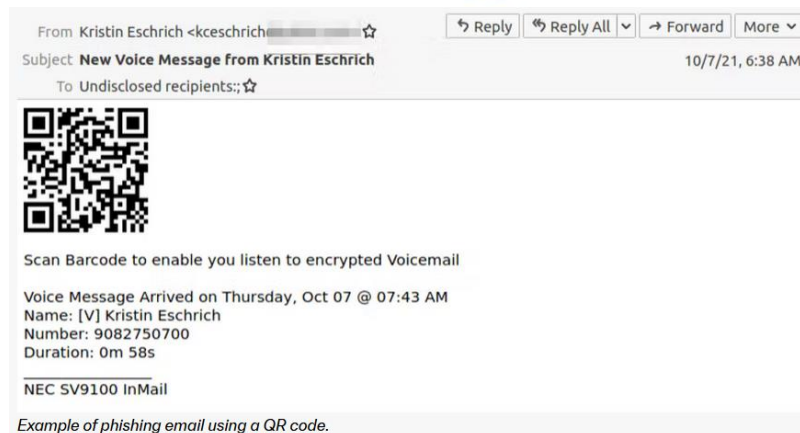
[← 回到上一頁](#)



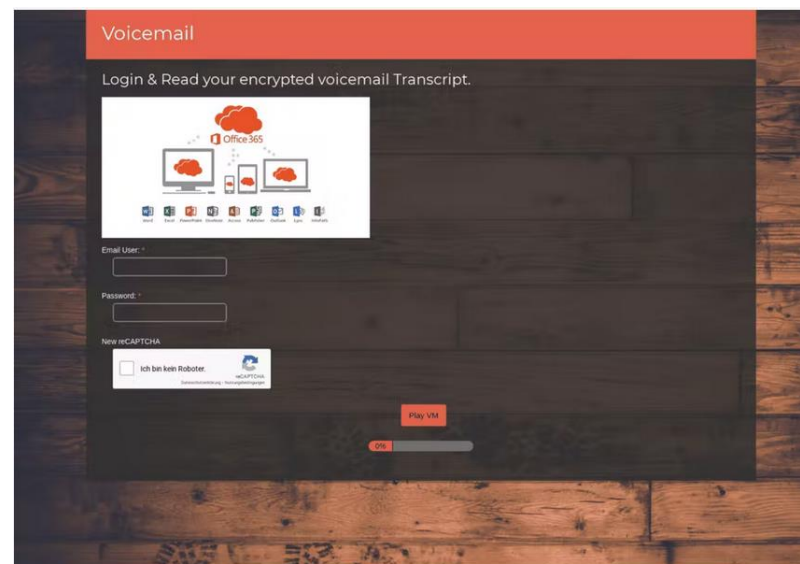
電郵安全公司Abnormal Security近期揭露一款利用QR Code行騙的釣魚手法，詐騙犯透過在電郵中嵌入惡意QR Code誘使收件人掃描，以躲避一般可掃描惡意網址連結及相關附件之防護機制。

非營利組織商業改進局 (Better Business Bureau , BBB) 溝通長 (Chief Communication Officer , CCO) Katherine Hutt分析，QR Code之所以能成為詐騙犯的避險機制有兩大原因：其一，在COVID-19疫情期間，以非接觸式的QR Code提供資訊，有助於減少肢體接觸及病毒傳播；其二，幾乎所有手機鏡頭都不需下載特定App就能掃描QR Code。此外，一般使用者不會像檢查電腦惡意軟體那般仔細查看手機，詐騙犯正是利用人們的這項心理因素。

部分惡意QR Code將收件人重新導向試圖竊取個資或憑證的釣魚網站，另一些則誘使收件人啟動支付App或關注惡意社群媒體帳號，這些詐騙案的共同點都是希望受騙者在未仔細檢查的情況下立刻掃描QR Code。



Example of phishing email using a QR code.



Example of the Microsoft credentials phishing page.

資料來源: TWNIC, Abnormal Security

把惡意連結藏在QR Code (2/2)

QR Code 別亂掃，FBI 示警：恐落入駭客圈套

作者 邱偉志 | 發布日期 2022 年 01 月 20 日 12:39 | 分類 科技生活, 資訊安全 [分享](#) [分享](#) [Follow](#)

自新冠肺炎疫情爆發後，對台灣民眾來說，進入公共場所掃簡訊實聯制 QR Code 已成為日常；不過根據美國 FBI 最新公告，現在有許多網路犯罪分子會篡改 QR Code 連結，將 QR Code 重新定向到會竊取用戶個資的惡意網站，偷走用戶的帳戶登錄資訊或財物訊息等。

智慧手機普及後，QR Code 讓使用者用手機鏡頭掃描讀取，迅速進入網站、下載 App 頁面，或支付之用。就技術來說，QR Code 立意良善，讓企業合法利用 QR Code 達到非接觸式支付或資訊提供體驗，因此新冠肺炎疫情爆發後，QR Code 更頻繁地使用。

FBI 發現，許多網路犯罪分子利用這項技術，篡改 QR Code 連結，讓不知情使用者掃描 QR Code 後導向惡意網站。FBI 也發現，篡改過的 QR Code 還有可能嵌入惡意軟體，讓有心人士掌握受害者行動裝置位置，以及財務資訊。

那要如何防範這情況發生？

FBI 建議使用者，每次掃描 QR Code 後，都要留意網站 URL 位址看起來是否為真；但要注意的是，惡意網址通常看起來與真實網址很像，駭客通常用不同拼寫網址，或讓網址字母更改位置混淆。

如果掃完 QR Code 後有要求登入個人資訊，尤其銀行帳戶等財務資訊等，都要更小心謹慎。

FBI 也建議使用者，如果想下載 App，不要掃描 QR Code 導向下載頁面，直接利用手機應用程式商店（App Store、Google Play 商店）搜尋應用程式，是比較安全的做法。

資料來源: 科技新報

APP後台配置不當、資料外洩

23 款 Android App 配置不當，多達 1 億筆使用者個資網上看光光

作者 Evan | 發布日期 2021 年 05 月 24 日 10:44 | 分類 Android, app, Google 

多款 Android App 因不當配置而導致 1 億多筆使用者敏感個資外洩，這可能使他們淪為惡意攻擊者牟利的肥羊。

「由於在將第三方雲端服務設定並整合到應用程式時，並未遵循最佳實踐，結果導致上億使用者個資外洩。」Check Point 研究人員 20 日分析報告表示，「雖然在某些情況下，這種類型的錯誤只會影響一般使用者，但實際上開發人員也會因此招致攻擊。不當配置會讓使用者個資和開發人員的內部資源（例如對更新機制、儲存等資源的存取權限）面臨風險。」

分析報告是對 Google Play 官方商店 23 款 Android App 的研究結果，其中一些 App 下載量從 1 萬到 1,000 萬不等，例如 Astro Guru、iFax、Logo Maker、Screen Recorder 和 T' Leva 等 App。

據 Check Point 指出，這些問題源於對即時資料庫、推送通知和雲端儲存金鑰的不當配置所致，進而導致電子郵件、電話號碼、聊天訊息、位置、密碼、備份檔、瀏覽器歷史記錄和照片的外洩。

研究人員將重要服務存取金鑰內嵌 App，為攻擊者敞開長驅直入大門

研究人員舉例指出，由於安哥拉（非洲國家）計程車叫車 App T' Leva 沒有在身分認證關卡做好保護資料庫，致使研究人員輕易獲得用戶個資，包括司機和乘客之間交流的訊息，以及乘客全名、電話號碼、目的地和接送地點。

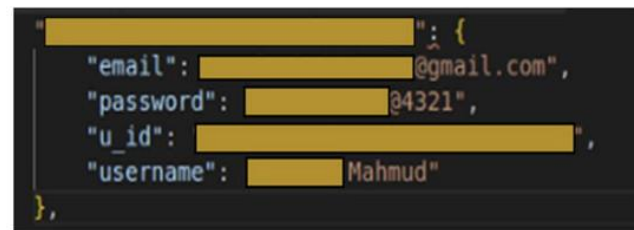
此外，研究人員發現，App 開發人員在 App 直接嵌入發送推送通知和存取雲端儲存服務所需金鑰。這不僅會讓惡意攻擊者假藉開發人員的名義向所有使用者發送惡意通知，甚至還能藉此將毫無戒心與防備的使用者導向至網路釣魚頁面，淪為更複雜威脅的切入點。

同樣地，將雲端儲存存取金鑰嵌入 App，無異與其他攻擊打開長驅直入的大門，這樣的攻擊，攻擊者可將雲端儲存的所有資料竊取到手，研究人員便在 Screen Recorder 和 iFax 這兩個 App 成功展開攻擊，並拿到螢幕錄影檔與傳真文件。

Check Point 指出，只有少數 App 負責任地立即變更，以呼應這次安全揭露，這意味著其他 App 使用者仍然容易受詐騙和身分盜用等可能威脅的影響，更不用說駭客可能利用被盜密碼騙取其他帳號了。

「當前受害者基本上易受許多不同攻擊媒介的攻擊，例如偽造攻擊、身分盜用、網路釣魚和服務盜用等。」Check Point 行動研究經理 Aviran Hazum 說。「這次研究揭露令人不安的現實狀況：App 開發人員不僅將用戶個資置於風險下，並讓自身個資也有風險之虞。」

- 23 Android Apps Expose Over 100,000,000 Users' Personal Data



Email, Password, Username and ID of a user on Logo Maker

```
public void create() {
    try {
        Client v1 = new Client(new Credentials("XXXX", "XXXX"));
        this.client = v1;
        v1.setRegion(Region.getRegion(Regions.US_WEST_1));
        this.createEndpoint(Definitions.pushFBToken);
    }
    catch (Exception v0) {
        Helper.Log("create error: " + v0.getMessage() + "====" + Definitions.pushFBToken);
    }
}
```

Credentials to Push Notification services embedded into an application

資料來源: 科技新報, thehackernews.com



智慧型手機威脅種類與危害

智慧型手機威脅類型



後門 (Backdoor)

- 允許潛在有害、遠端控制等行為的惡意程式



付款詐騙 (Billing Fraud)

- 以故意欺騙方式讓受害人付款的惡意程式，如未經使用者同意發送簡訊或撥打電話



間諜軟體 (Spyware)

- 未經使用者同意發送個人機敏資訊的惡意程式(如收集位置、通話紀錄等)



服務阻斷 (Denial of Service)

- 讓裝置發送封包癱瘓網站或服務的惡意程式



惡意下載 (Hostile downloaders)

- 本身不一定造成裝置損害，但會下載其他惡意程式



釣魚 (Phishing)

- 假冒合法網站或服務，騙取使用者資料的惡意程式



提權濫用 (Elevated Privilege Abuse)

- 提升權限，突破沙盒封鎖或是裝置安全限制的惡意程式，如偷取憑證或防止解除安裝屬於此類



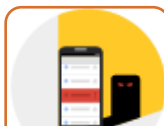
勒索軟體 (Ransomware)

- 取得裝置或資料控制權，以此要脅受害人付款贖回的惡意程式



破解程式 (Rooting)

- 破解手機的程式，可能是惡意程式也可能不是



垃圾郵件 (Spam)

- 利用受害裝置發送垃圾訊息或郵件的惡意程式

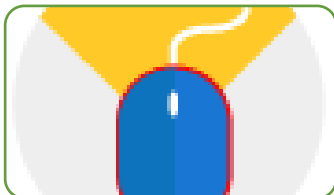


木馬 (Trojan)

- 偽裝成合法程式(如遊戲)卻背著使用者執行其他工作的惡意程式

行動裝置上嫌惡程式類型

Mobile Unwanted Software (MUwS)



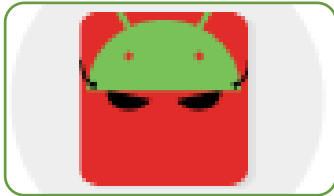
點擊詐欺 (Click fraud)

- 未經使用者同意代操作，自動對廣告點擊、觸碰、產生流量的應用程式
- 向廣告主詐取廣告費



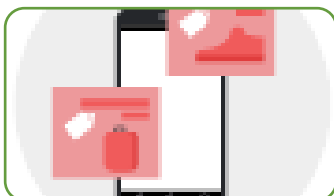
資料收集 (Data collection)

- 未通知、徵得使用者同意即收集、傳輸個人資料的應用程式
- 如：手機號碼、Email信箱、第三方帳號ID、其他個資等



偽裝 (Impersonation)

- 透過偽裝成另一支應用程式，讓使用者以為正在使用該APP
- 如：偽裝成知名APP、防毒軟體等騙取付費、偽裝成網銀APP騙取帳號



干擾式廣告 (Disruptive ads)

- 顯示會對使用者造成困擾或是對裝置功能造成干擾的廣告的應用程式
- 如：蓋版、跳出視窗等

參考資料: <https://developers.google.com/android/play-protect/phacategories>

★ 行動惡意軟體的攻擊途徑

● Android系統感染途徑

- ✓ 惡意App繞過Google檢查上架到Google Play Store
- ✓ 非官方的App市集
- ✓ 惡意下載連結/透過網址誘騙使用者安裝

● iOS 系統感染途徑

- ✓ 惡意App繞過審核機制上架到App store(相對較少)
- ✓ 透過網址與盜取的開發者憑證散播
- ✓ 惡意的描述檔
- ✓ 惡意下載連結/透過網址誘騙使用者安裝

行動惡意軟體造成的危害

加密勒索

- 駭客加密手機資料 如通訊錄、簡訊、照片等，要求贖金

木馬/間諜軟體

- 竊取手機上的個資等重要資料，或攔截交易簡訊，追蹤使用者地理位置跟每日行程

綁架挖礦

- 駭客透過APP或網站進行挖礦，賺取虛擬貨幣，另有造成手機CPU過熱甚至電池膨脹之隱憂

二、行動支付及安全性

行動支付普及化(1/2)

疫情帶動近 7 成民眾結帳用行動支付



陳怡樺 · Yahoo財經特派記者

2022年1月26日 · 2分鐘 (閱讀時間)

根據資策會產業情報研究所 (MIC) 公布 2021 年行動支付消費者調查發現，去年行動支付常用度首次達到 69%，相當接近第一名的實體卡 74%和現金 71%。過去行動支付在台灣無法普及有一個原因正是信用卡太方便，但去年行動支付不僅連續三年成長，和實體卡的差距也從 2019 年的 26%縮小到 5%。

反映出疫情因素加速消費者使用行動支付的習慣養成，政策目標有望達成。另一個重要的指標是消費者偏好，調查顯示，去年消費者首選行動支付的偏好度大幅提升，從前年 37%成長至 50%，反倒是消費首選實體卡的比例從 35%降到 26%，差距幅度急遽增加。

而調查也特別針對去年全國三級警戒疫情期間的消費者行為研究，發現常用的實體卡和行動支付都有接近 6 成，行動支付還是疫情期間消費者使用頻率增加最多的，至於現金同樣降幅最大，常用比例只有 38%，有過半消費者表示減少了現金使用頻率。

進一步針對行動支付的使用場域分析，排名依序為便利商店 (70%)、網路商店 (56.3%)、量販店 (55.8%)、超級市場 (51%)、連鎖餐飲 (47%)。MIC 資深產業分析師胡自立表示，前三名的成長與疫情驅動實體交易轉移到線上都有關。

至於去年行動支付用戶在「使用頻率」、「平均消費金額」與「單次最高消費金額」三部分也都有明顯成長，每次均消費金額超過 1000 元的族群成長至 12%，單次消費金額超過 3000 元的行動支付用戶，也從 2020 年 10%大幅成長到 27%，可以看出民眾的習慣已經漸漸改變。

➤ 【產業地圖圖解】台灣「電子支付與純網銀」產業地圖

2023 / 05 / 23 生活產業, 產業情報, 零售產業, 電商產業

- 💡 「電支雙雄」街口支付&一卡通使用人數雙雙突破560萬，「電支新星」全支付使用人數搶進TOP 3
- 💡 2022年電支匯兌業務年增103.5%最高，全支付2022Q4交易額超越一卡通&玉山銀行
- 💡 純網銀商品走向多元化，蝦皮、綠界、拍付、LINE Pay、藍新、foodpanda晉身電支預備軍

截至2023年3月底，全台共計10家專營電支機構及20家兼營電支機構(含銀行及中華郵政)，總使用人數(未歸戶)年增39.3%至2,332.3萬人。依各電支機構使用人數排名，前3大業者分別為街口支付(使用人數603.0萬、年增8.3%)、一卡通票證(使用人數564.8萬、年增17.0%)以及2022年8月開業的全支付(使用人數313.8萬)。

另一方面，同樣做為普惠金融的重要加速器，台灣純網銀市場主要由連線商業銀行(LINE Bank)、樂天國際商銀以及將來銀行共同構成。截至2023年第一季，3家純網銀數位帳戶數量分別達148.8萬戶、15.9萬戶及29.6萬戶，其中帳戶數量最高的LINE Bank已成為全台數位帳戶數第3高的銀行，僅次於台新與國泰世華銀行。

支付金融為商業底層基礎設施，加上其中所蘊含的大量消費數據，吸引零售電商集團、電信通訊/網路遊戲/社群平台及交通票證機構積極參戰。未來流通研究所爬取台灣主要電支&純網銀業者營運數據與競合脈絡，繪製「電子支付&純網銀」產業地圖，做為觀測整體產業走向的重要基礎。

資料來源: Yahoo、未來流通研究所

行動支付普及化(2/2)

台灣「電子支付 & 純網銀」產業地圖

累計使用人數 603萬人 TOP1

街口電子支付

全台用戶數最多&交易額最高電支品牌

使用人數	603.0萬	交易總額	389.6億
匯兌總額	420.6億	儲值總額	773.9億
營收總額	3.6億	稅後淨利	-2.6億
營業費用	2.8億	合作銀行	27家

點 2022年新增5萬點，共計25萬個支付點

股 街口金融科技

策 ① 目標2025年轉虧為盈
② 以日本為首，拓展跨境旅客付款服務
③ 推動JKO Fintech Hub金融服務

累計使用人數 565萬人 TOP2

一卡通

全台小額匯兌&儲值金額最高電支品牌

使用人數	564.8萬	交易總額	235.5億
匯兌總額	816.0億	儲值總額	1,763.1億
營收總額	5.7億	稅後淨利	-1.8億
營業費用	5.2億	合作銀行	24家

點 累計使用通路據點POS數逾44萬個

股 聯邦銀行、國發基金、高雄市政府、高捷

策 ① 目標2025年轉虧為盈
② 進入iPASS 3.0，推動iPASS APP上線
③ 建構數據中台，強化數據分析運用

累計使用人數 314萬人 TOP3

全支付

以成為台灣第1家獲利電支品牌為目標

使用人數	313.8萬	交易總額	90.9億
匯兌總額	0.25億	儲值總額	39.1億
營收總額	3,136.6萬	稅後淨利	-3.3億
營業費用	4.1億	合作銀行	15家

點 與百大品牌合作，超過10萬個支付點

股 全聯實業

策 ① 提高代理收付金額，推出金融商品
② 拓展全聯周邊據點，擴張消費場景
③ 增加合作支付通路，吸引年輕用戶

*依2023Q1各電支機構「使用人數」排序

累計使用人數 221萬人 TOP4

悠遊卡公司

預計2024年上市，積極佈局海外市場

使用人數	221.4萬	交易總額	45.1億
匯兌總額	9.4億	儲值總額	61.6億
營收總額	16.6億	稅後淨利	6,032.3萬
營業費用	8.0億	合作銀行	18家

點 逾35萬個支付據點(含悠遊卡)

股 悠遊卡投控、台北市政府、台北捷運

策 ① 增加連鎖商家&大型百貨支付點
② 積極佈局日/韓/星/馬等海外市場
③ 2024規劃推出「悠遊付附隨卡」

累計使用人數 182萬人 TOP5

玉山商業銀行

使用人數	181.7萬	交易總額	163.8億
匯兌總額	0	儲值總額	4.1億

點 與台灣Pay共享通路，超過25萬支付點

策 強化境內及境外(如淘寶)整合收付服務

累計使用人數 139萬人 TOP6

全盈支付

營收總額	1,719.5萬	交易總額	35.4億
匯兌總額	1,177.2萬	儲值總額	4.4億

點 超過10萬股 全家、玉山、台新、拍付

策 發展嵌入式金融、生態圈與數據賦能

累計使用人數 110萬人 TOP7

愛金卡

營收總額	8.5億	交易總額	61.7億
匯兌總額	4.2億	儲值總額	19.6億

點 超過20萬個支付點 股 統一超商

策 結合統一超點數生態圈、推出金融商品

累計使用人數 103萬人 TOP8

歐付寶

營收總額	7,098.0萬	交易總額	16.2億
匯兌總額	1.2億	儲值總額	6,785.4萬

股 歐買放(同步持股綠界科技)

策 強化跨境電商金融&外籍移工匯款服務

累計使用人數 50萬人 TOP9

橘子支

營收總額	1,060.1萬	交易總額	52.6億
匯兌總額	4.5億	儲值總額	5.9億

點 超過9萬個支付點 股 遊戲橘子

策 擴大服務範圍&遊戲場域外溢消費管道

累計使用人數 26萬人 TOP10

中國信託商業銀行

使用人數	25.5萬	交易總額	2.8億
匯兌總額	0	儲值總額	30.3萬

股 中國信託金融控股

策 結盟產業領導品牌，擴大支付生態圈

累計使用人數 6.6萬人 TOP11

簡單行動支付

營收總額	1,797.4萬	交易總額	5,818.3萬
匯兌總額	2.3億	儲值總額	610.1萬

股 藍新科技(智冠集團)

策 推出收款設備，跨足實體支付場景

累計使用人數 3.5萬人 TOP12

國際迪

營業費用	4,033.0萬	交易總額	0
匯兌總額	176.2萬	儲值總額	81.1萬

股 拍付國際(PChome集團)

策 持續發展與其他業者合作，降低成本

連線商業銀行(LINE BANK)

帳戶數量	148.8萬戶	淨收益	-3.95億	稅後淨利	-20.1億
營業費用	19.2億	資本適足率	44.64%	存款餘額	417.5億

股 LINE Financial、北富銀、渣打銀行、台灣大哥大、聯邦銀行

策 推出信貸、產險等多元金融商品，強化獲利能力及拓展服務廣度

樂天國際商業銀行

帳戶數量	15.9萬戶	淨收益	2,077.1萬	稅後淨利	-5.4億
營業費用	6.8億	資本適足率	140.36%	存款餘額	197.8億

股 國票金融控股、樂天銀行株式會社、樂天CARD株式會社

策 發展日本旅遊生態圈&跨境金融服務，強化放款業務&拉高存放比

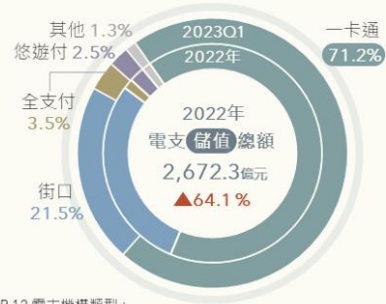
將來商業銀行

帳戶數量	29.6萬戶	淨收益	-4,734.9萬	稅後淨利	-10.0億
營業費用	11.8億				

股 中華電信、兆豐銀行、新光集團、全聯

策 完成產品建設，聯手股東發展生態圈

2022年 & 2023Q1 電支核心業務市佔率

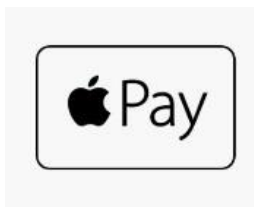


TOP 12 電支機構類型: ●電商&資訊類 ●交通類 ●實體零售類 ●銀行兼營 ●純網銀

資料來源: 未來流通研究所

●兩大主流模式

- ✓行動支付：行動裝置綁定信用卡作為支付工具
- ✓電子支付：有獨立電子支付帳戶，進行交易或轉帳
- ✓可以是其中一種，也可以同時支援兩種模式



行動支付(實體信用卡虛擬化)

- 把實體信用卡虛擬化成為手機信用卡，讓支付更安全方便
 - ✓例如：Google Pay、Apple Pay
- 使用者必須綁定信用卡才能使用
- 金流流向與實體信用卡支付模式雷同，並未改變原有生態系



資料來源：
數位時代

電子支付(帳戶儲值、點數)

- 使用者在網路平台開通儲值帳戶
 - ✓ 如LINE、悠遊付、街口等網路平台
- 使用者不一定需要綁定銀行帳戶與信用卡
- 金流不會經過 Visa 與 MasterCard 等信用卡組織與收單銀行，對原有支付生態系造成影響



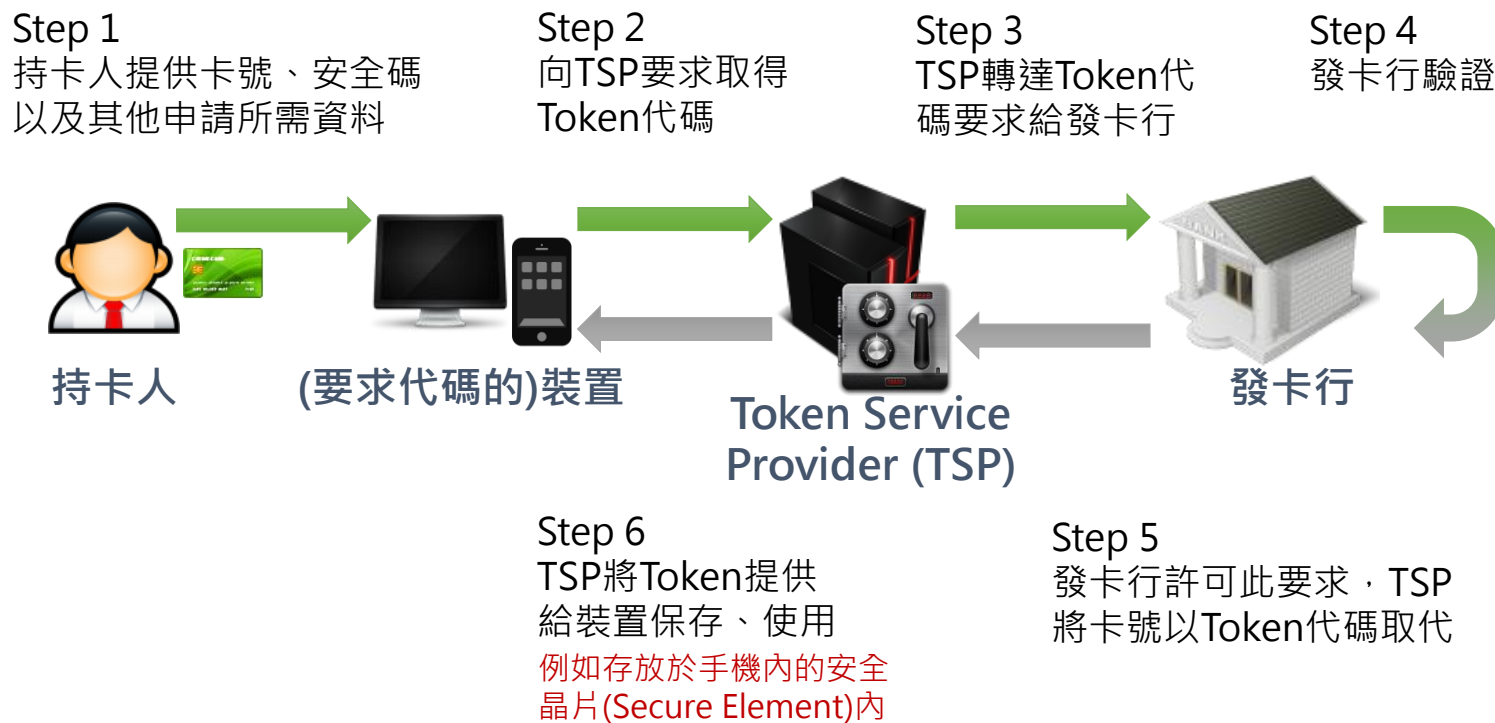
資料來源：
數位時代

代碼化(Tokenization) (1/3)

- 實體信用卡虛擬化背後技術
- 由EMVCo組織提出
 - ✓ Visa + MasterCard + EuroPay
- 藉由一串虛擬的數位帳號、或一個可以被安全儲存於行動裝置內的Token代碼，來取代傳統塑膠卡片上的帳號資訊
- 卡號資訊、刷卡人身分保密，較傳統消費方式安全

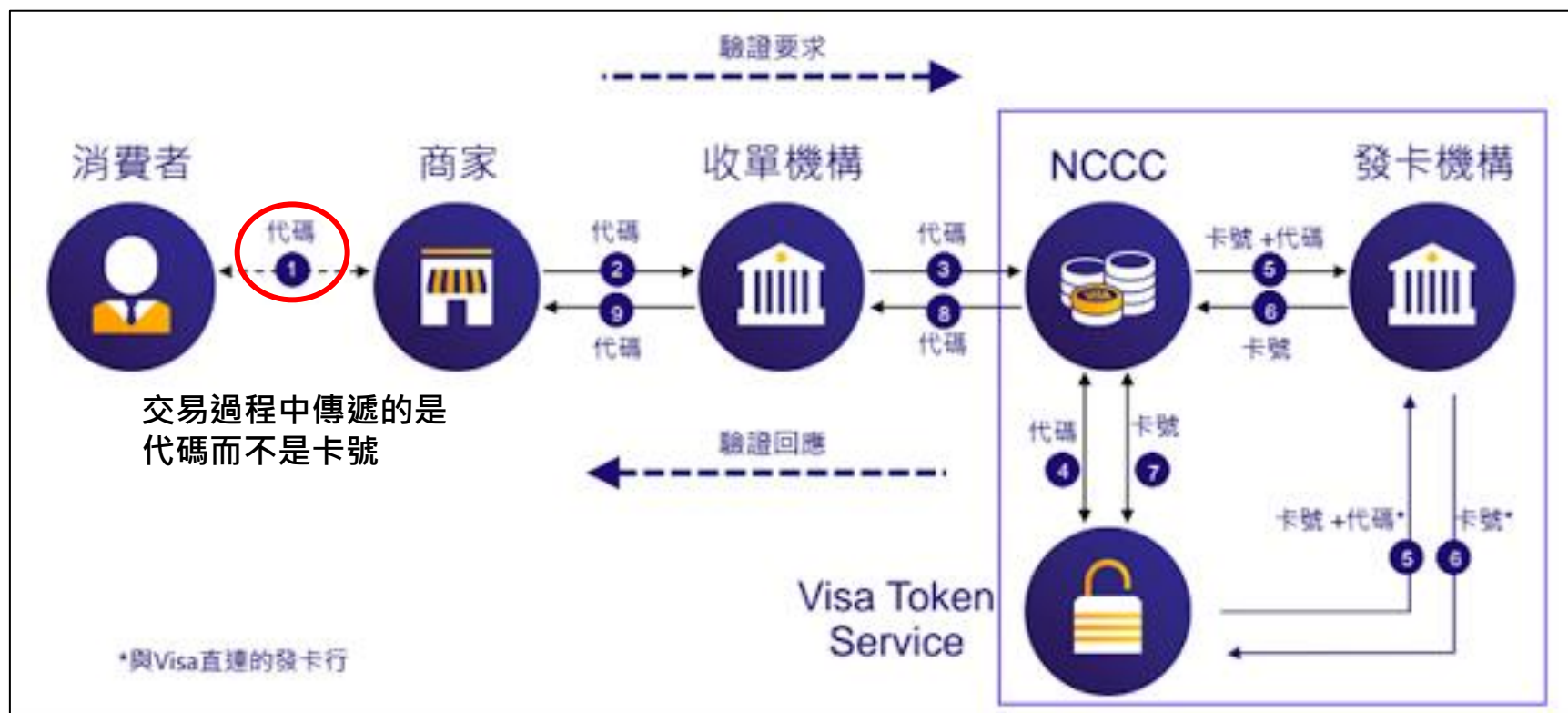
代碼化(Tokenization) (2/3)

●Token代碼如何產生



代碼化(Tokenization) (3/3)

●Token如何使用於交易(以Visa為例)



Token Service Provider只知代碼與卡號的對應及發卡行，
不知刷卡者身分，無個資問題

資料來源：Visa

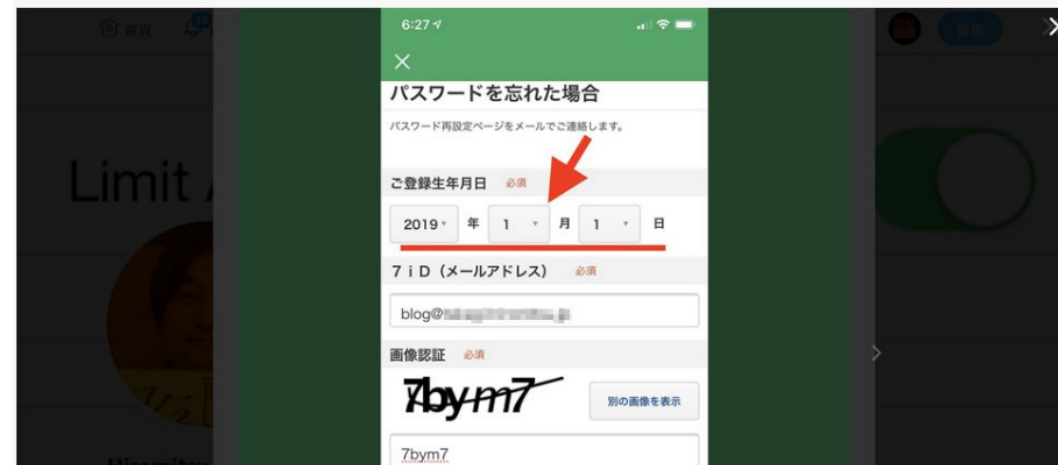
7Pay用戶遭竄改密碼並盜刷

密碼重設功能不嚴謹，缺乏驗證，日本7Pay用戶遭竄改密碼並盜刷

7月第一天才剛推出7pay的日本7-Eleven，隔日就被民眾爆出自己的7Pay密碼遭人竄改，導致App綁定的信用卡遭人盜刷的問題，而日本網路上也有研究員指出，該系統的密碼重設與身分驗證機制不夠嚴謹。

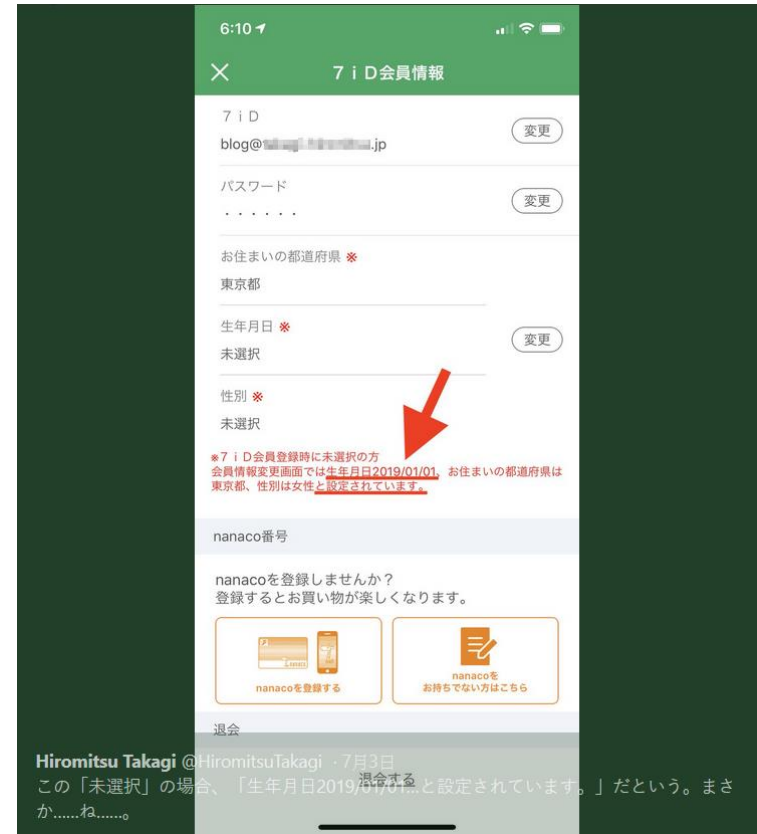
文/ 羅正漢 | 2019-07-07 發表

按讚加入iThome粉絲團



關於日本7-Eleven「7Pay」的重設密碼功能，因其身分驗證機制不夠嚴謹，導致已有數百用戶帳戶讓人盜用進而盜刷的事件，日前7&i控股（Seven & I Holding）與7pay均已在官方網站已發出公告，並表示從7Pay上線後隔日，就陸續收到用戶反應遭人盜刷的狀況。到底7pay App的身分認證與密碼重設機制，出現了那些嚴重的問題？各界都很關心。

對於實際操作過程的弱點，已經有許多日本民眾在網路上討論。例如，在7月3日，日本一名研究員高木浩光（Hiromitsu Takagi）在Twitter上，就指出了7iD會員登入的相關問題。根據他的貼文，在iOS系統開啟7pay App要註冊7iD會員時，一開始的介面上會有7iD（電子郵件信箱）、居住地區、生日與性別的欄位，但是，用戶只要輸入第一項的電子郵件信箱，在沒有輸入生日等選項的情形下，依然可以執行下一步。



消費者若需重設密碼，只要輸入生日(預設2019/01/01)、手機號碼及任一電子郵件信箱，系統即會將重設郵件寄到該信箱內

資料來源: iThome, @HiromitsuTakagi

冒用個資綁行動支付盜刷

冒用個資騙銀行客服 綁行動支付再盜刷

詹淑雲 / 桃園報導 發布時間：2020-11-26 12:57 更新時間：2020-11-26 21:16

銀行 行動支付 盜刷 客服 個資

詐騙集團出新招！這回是掌握被害人個資，謊稱是持卡人，騙過銀行客服人員更改留存的行動電話及電子信箱，綁定行動支付，盜刷約200萬財物。

撥打電話到銀行客服中心，詐騙集團冒用持卡人資料，成功騙過銀行客服人員修改行動電話號碼和電子信箱，再綁定行動支付盜刷信用卡。桃園檢警日前分別在桃園、新竹逮捕3名涉案嫌犯，並起獲大批贓證物。

桃園地檢署襄閱主任檢察官趙燕利表示，「竄改後的門號來申請電子支付，諸如Apple pay、Google pay這些等等，並以竄改之後的門號及電子信箱做為接收銀行端認證簡訊及訊息的工具。」

地檢署表示，以蕭男、江男、林女等人為首的犯罪集團，自今年8月起，陸續假冒銀行信用卡持卡人更改資料進行盜刷，初步清查有14位被害人，損失將近2百萬元。

民眾表示，「個資被盜用的話，銀行又沒有好好把關的話，說實在的我們一般老百姓會很不放心。」

金管會銀行局副局長林志吉表示，「要更改的話，並不是基本個資就足以更改，問你更私密的資料。譬如說三個月的繳款去哪裡繳款，我們可能要再來釐清說，銀行在這個過程當中有沒有疏失。」

銀行局表示，若民眾沒有疏失，被盜刷金額，由銀行自行吸收負責。全案檢察官偵訊後，向桃園地方法院聲押蕭、江2人獲准，也聯繫相關發卡銀行，緊急改善持卡人透過客服變更資料的徵信流程。



資料來源: 公視

孫盜刷花光阿公百萬養老金

偷看密碼！12歲孫狂刷百萬「買到戶頭剩5元」 養老金全沒阿公哭了

圖文/CTWANT

2022/04/13

大陸河南省鞏義市一名12歲小祥（化名）日前跟阿公出去吃飯，結果得知了阿公的支付密碼，之後居然在網路上狂買東西，把阿公戶頭裡23萬人民幣（約新台幣105萬元）養老金，花到剩不到5元。阿公哽咽，「心疼，心太疼了。」

根據陸媒《九派新聞》報導，小祥母親氣炸表示，一回家看到家裡一堆大大小小的箱子瞬間傻眼，快遞箱裡有玩具、氣炸鍋、夾板等，還有好幾箱是盲盒，不知道裡面裝了什麼東西，這些全是兒子拿阿公戶頭裡的錢網購的。

小祥透露，去年9月跟阿公去吃飯，意外得知阿公的支付密碼，之後看到什麼想買就買，「我買了筆記型電腦、蘋果手錶、華為的VR眼鏡等。」他為了不被家人發現，還把東西存放在快遞站，直到家長發現戶頭剩不到5元去查，才得知一切。

檢視紀錄，小祥共買了61件商品，除了筆電、手錶，甚至還買「卡丁車」，但現在不知道車子的下落。家人循線追查，發現小祥都跟某個直播主買東西。對此直播主表示，對小祥有印象，是單場消費破3萬人民幣（約新台幣13.7萬）的一個大哥。

養老的錢被孫子花光，小祥阿公眼眶紅了，「心疼的，不是心疼（孫子），是心太疼，現在的狀態處於晚上、白天都不知道，腦子已昏。」目前家人已透過平台聯繫商家退貨退款，希望可以將傷害降到最低。



資料來源: CTWANT

行動支付安全嗎？ (1/2)

- 綁卡盜刷：使用者卡號、個資沒保護好
 - ✓ 盜刷犯使用偷來的個資，欺騙信用卡公司更改註冊電話
 - ✓ 使用偷來的卡號、安全碼註冊卡片，收取驗證碼簡訊
 - ✓ 成功綁定信用卡至手機，進行盜刷行為
- 電支盜刷：登入憑證外洩、帳號重設機制問題
 - ✓ 帳號、密碼外洩被冒用盜刷
 - ✓ 密碼重置機制驗證不嚴謹，導致帳戶被攻擊者接管
- 信用卡掉了會被綁定行動支付盜刷嗎？
 - ✓ 有難度，綁定信用卡至手機需經簡訊驗證
(除非是前述的情況)
- 手機掉了或被偷時，行動支付會被盜刷嗎？
 - ✓ 有難度，刷卡時需要失主的指紋或是密碼驗證

行動支付安全嗎？ (2/2)

- 是否可能透過木馬病毒盜取手機上Token代碼？
 - ✓ 有難度，首先你需要取得手機最高權限
 - ✓ 再來還要破解儲存Token代碼的獨立安全晶片(硬體級別的漏洞)
- 可以用支援行動支付的穿戴式裝置(Apple Watch)盜刷嗎？
 - ✓ 有難度，裝置會偵測穿戴情形，若脫下需要密碼解鎖才可再次使用
- 到底有沒有被盜刷的可能？
 - ✓ 如果對方可同時取得手機及指紋或密碼的話，可能
 - ✓ 接觸對象是頭號嫌犯，應不難抓
 - ✓ 另一個可能是系統設計出了狀況(像是7Pay)

降低行動支付盜刷的風險

降低風險

- 密碼不共用(行動支付的密碼通常只有幾個位數)
- 開啟生物辨識(臉部、指紋)
- 解除不常使用的支付APP信用卡綁定
- 小心騙取帳號密碼、個資的釣魚網站
- 不安裝來路不明的APP
- 不破解裝置

降低損失

- 開啟刷卡通知(APP推播、簡訊、Email)
- 專卡專用

三、行動裝置安全強化

系統安全 (1/2)

- 系統的漏洞只能靠原廠的修補更新(Patch)
- 不管是Android或是iOS，還是需要時常檢查是否有安全更新
 - ✓ 鮮少有堅不可破的系統，勤勞點比較實在
- iOS的更新比較不需要擔心
 - ✓ 基本上前後幾代的機種都可以持續收到安全更新
 - ✓ 2018年販售的iPhone Xs仍可更新至最新版17.x
- Android比較棘手
 - ✓ Android的更新需要仰賴製造商與電信商來協助(生命週期約2年)
 - ✓ 只有Google自家Pixel系列的手機可以保證收到定時更新
 - ✓ 大廠(Samsung, Sony...等)比較會跟著Google腳步推出更新
- 怎麼檢查呢！？

系統安全 (2/2)

設定 > 關於手機 > Android 版本



設定 > 安全性 > 安全性更新



註：可能隨機種不同，路徑也不一樣

App的安裝及管理 (1/6) – Android

- 只使用官方的Google Play Store來安裝App
- 安裝前請詳閱公開說明書
 - ✓ 詳細檢視App所需要的權限 – Android 6.0後的系統可針對相關權限做控管
 - 人體感測器
 - 日曆
 - 相機
 - 聯絡人
 - 位置資訊
 - 麥克風
 - 電話
 - 簡訊
 - 儲存空間

設定>應用程式>特殊應用程式存取權
>安裝不明應用程式

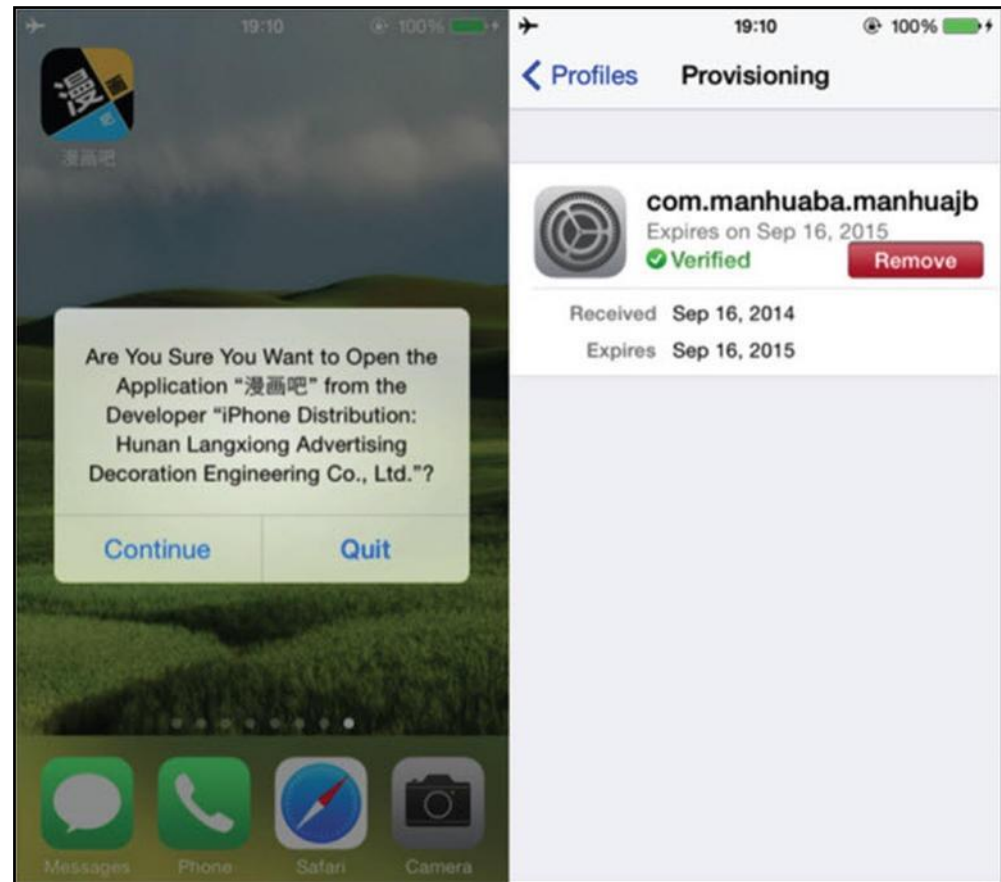
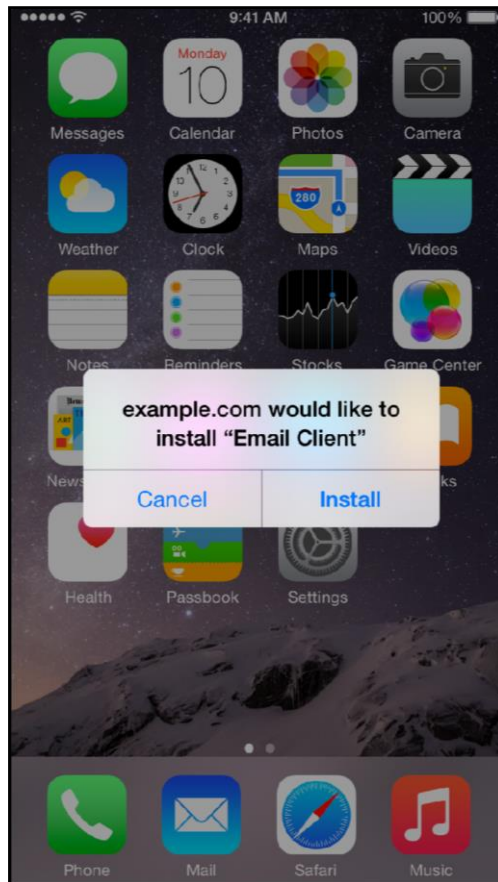


●Android 6.0或以後的系統內建應用程式權限管理機制



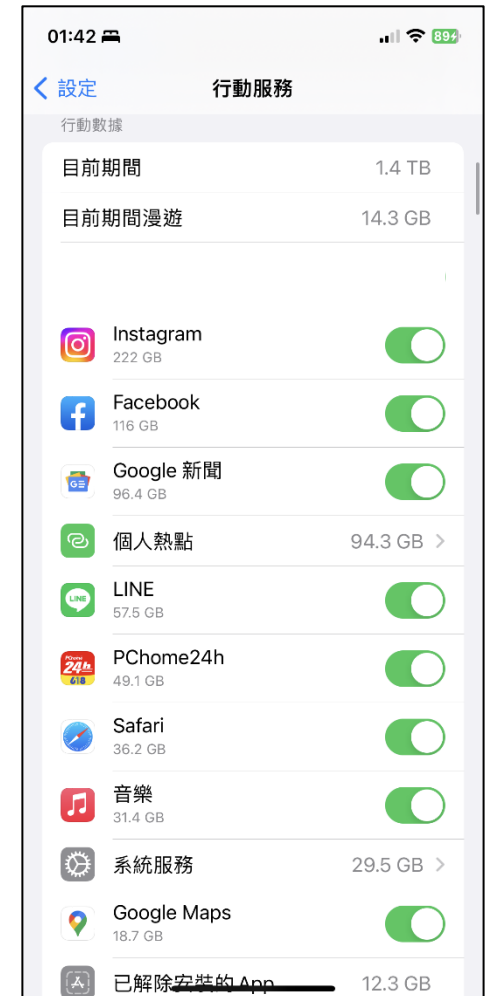
App的安裝及管理 (3/6) – iOS

- 使用官方的App Store來安裝App
- 小心突然冒出來的安裝提示按鈕



App的安裝及管理 (4/6) – iOS

●iOS比起Android，提供了更細緻的權限管控機制



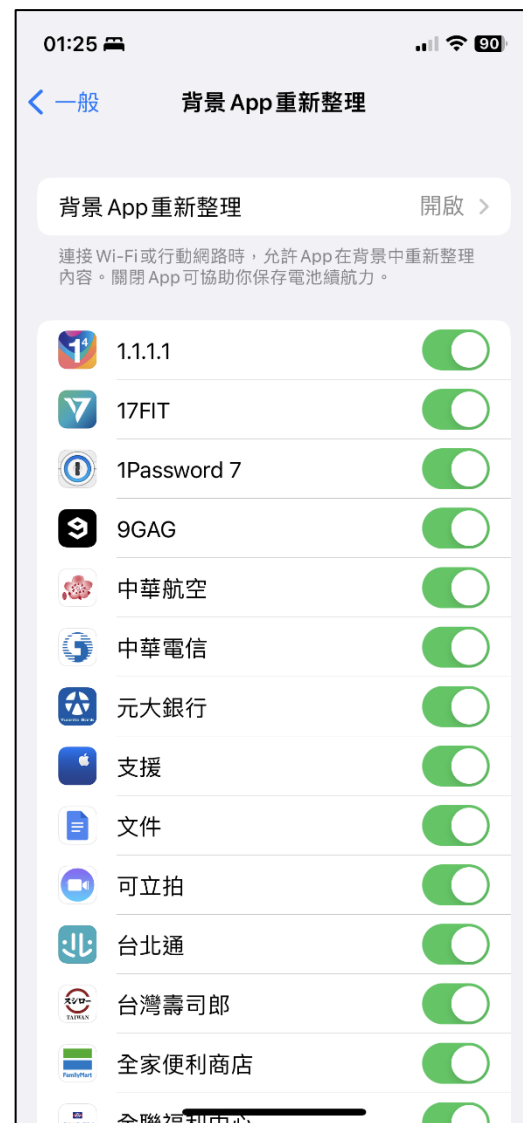
App的安裝及管理 (5/6) – 背景活動

●Android

- ✓ 根據廠牌不同，可能有不同的客製化方式
- ✓ 多半透過系統監控應用程式活動狀況，及設定閒置時間後，讓App進入休眠模式
- ✓ 可以手動關閉背景程式
 - 但是有一些預載的service可能關不掉

●iOS

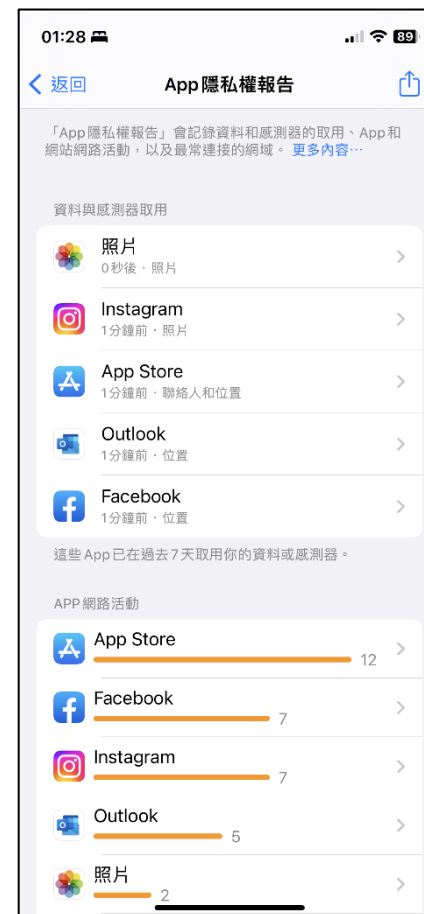
- ✓ 類似的方式，但是額外提供了管理介面，可以針對App去做個別控管



App的安裝及管理 (6/6) – App隱私

●iOS App隱私權報告

✓ 設定>隱私權與安全性>App隱私權報告



系統管理組態檢查

● 定時的檢查手機的安全相關組態設定

✓ Android:

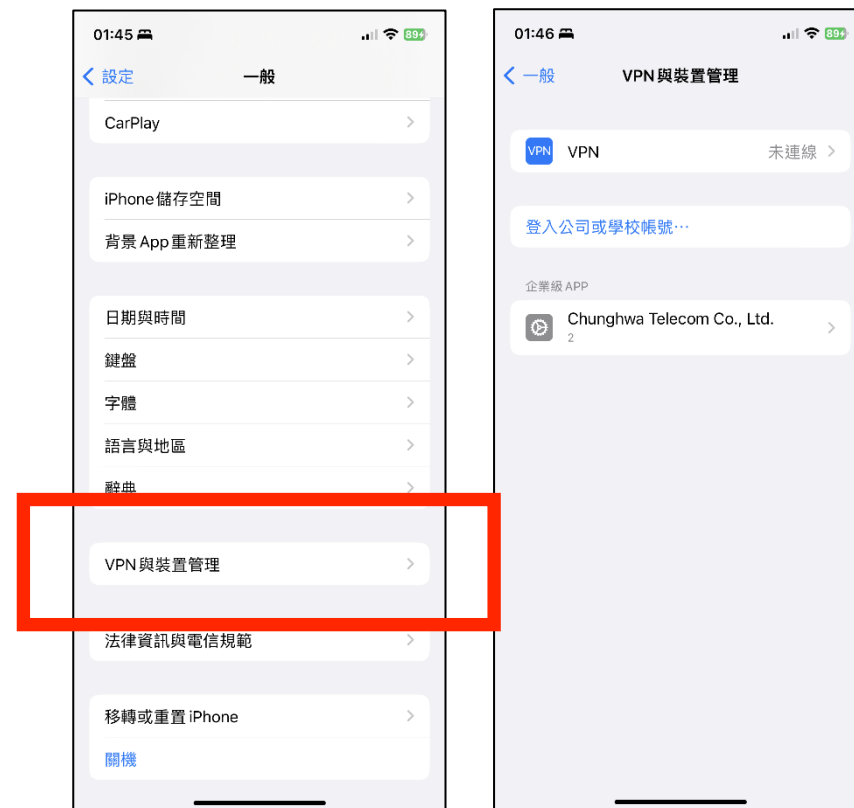
□ 裝置管理員

□ 帳戶與同步



✓ iOS :

□ VPN與裝置管理

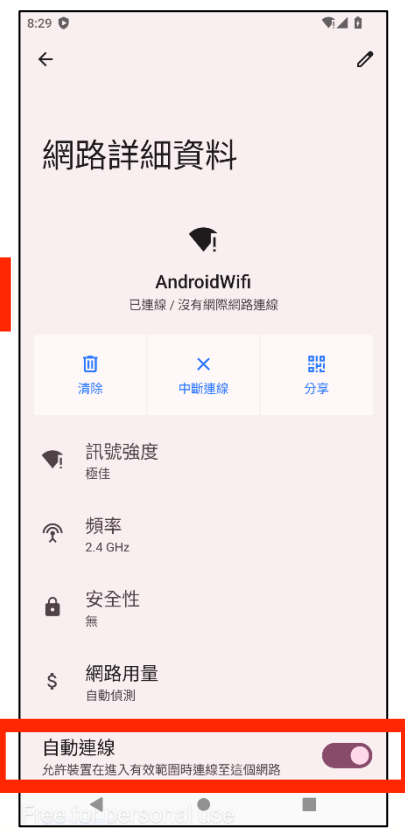
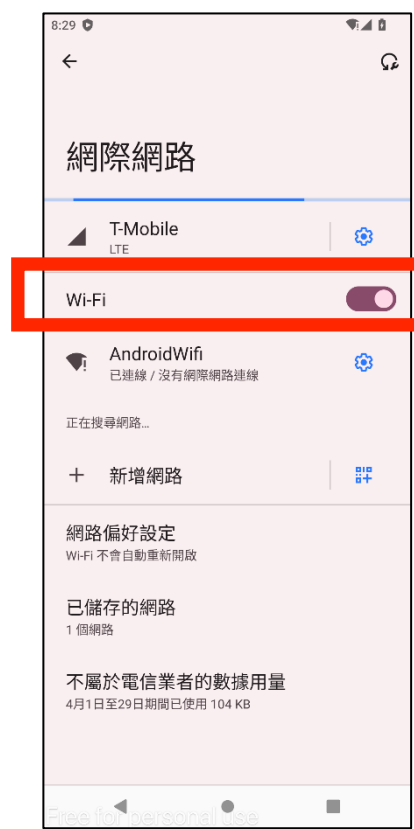


● 避免使用不知名的免費Wi-Fi

- ✓ 現在咖啡店、餐廳...等開放公共空間多半有免費Wi-Fi可以使用
- ✓ 常見的Wi-Fi基地台有三種方式提供服務
 - 無密碼
 - 共用密碼(一般咖啡廳、餐廳等)
 - 跨站認證機制(大專院校無線網路漫遊、中華電信CHT Wi-Fi等)
- ✓ 免費的最貴
- ✓ 連到居心不良的Wi-Fi基地台會有什麼風險?
 - 帳號密碼盜用
 - 個人資訊被竊取

行動上網安全 (2/2)

- 停用自動加入網路功能
- 關閉自動掃描可用網路功能
- 無需使用Wi-Fi時，請關閉Wi-Fi功能



★ 行動安全防護原則



認證的App來源

- 避免安裝未簽署的App，只從官方App Store下載App
- App要求存取授權時確認其合理性，特別是擁有讀取簡訊能力的App可能會想辦法繞過簡訊認證



行動作業系統安全

- 不要在與手機網綁的帳號(iCloud/Gmail)使用弱密碼
- 避免以破解(JailBreak/Android Root)方式使用行動裝置
- 將手機系統版本更新到最新版



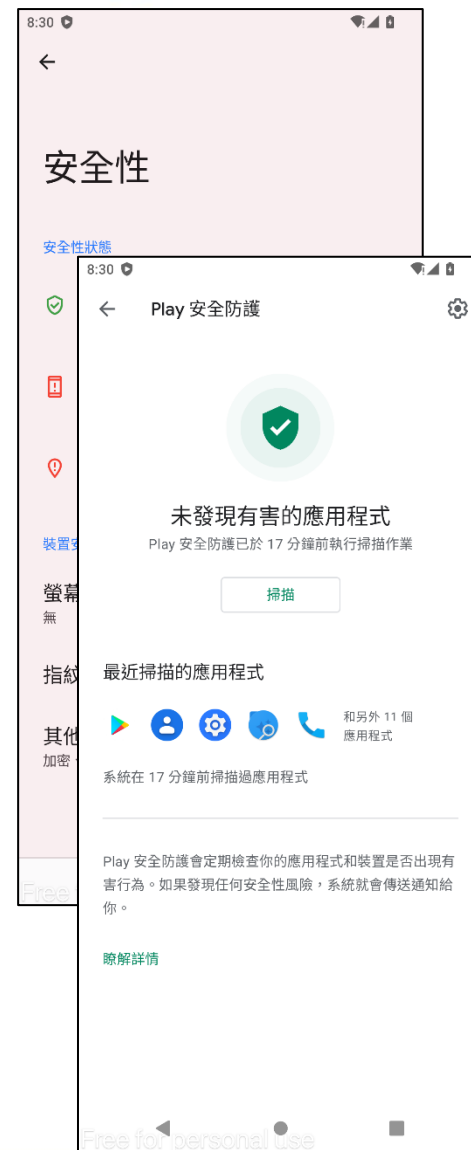
連線與使用環境安全

- 避免將重要資料存放在SD卡上，可能會被其他App存取
- 停用Wi-Fi自動連線，避免手機自動使用不安全的無線網路



防護軟體

- 考慮安裝有效的手機防護App



裝置的连接也需要注意

- 一般來說，手機插上電腦或有能力讀取手機儲存空間的裝置後，會出現以下兩種提示畫面：



Android



iOS

充電還是受駭？

● 攻擊者可能會使用的方式



畅充 freecharge 亲，手机没电了？看这里哟！

- ios系统的手机用户须 **点击信任按钮**
解锁手机屏幕，弹出窗口后点击“信任”按钮，即可享受免费高速充电服务。
- android系统的手机用户须 **打开USB调试模式**
 - 解锁手机屏幕，弹出“是否允许计算机调试”窗口后点击“允许”按钮，即可享受免费高速充电服务。
 - 部分用户如使用“仅充电”功能或拒绝安装推荐APP，将无法享受免费高速充电服务。

温馨提示
IOS用户已安装APP如无法使用，请进入“设置”→“通用”选项→“描述文件”或“设备管理”→“选择该文件”→点击“信任”，即可打开APP话费。

畅充充电助手，帮助android手机用户快速开启高速充电服务。

仅19K
下载畅充充电助手
扫我一键开启USB调试模式

高速充电使用须知
Fast Charging Operation Instruction

关注畅充科技官方微信
扫我进入精彩活动

其餘安全設定建議 (1/6)

● 手機應開啟加密機制

✓ iOS系統預設都是開啟的

- 每台裝置都有獨一無二的硬體密碼保護

✓ Android系統v6或以後

- 基本上預設都開啟裝置加密了
- 如果沒開... 請自己打開
- 別忘記SD卡也要開啟加密機制

設定 > 安全性 > 其他安全性設定 > 加密和憑證



其餘安全設定建議 (2/6)

● 設定密碼鎖定避免盜用

✓ 不要設定簡單的密碼(4位數容易破解)

□ 新版iOS預設使用6位數密碼保護

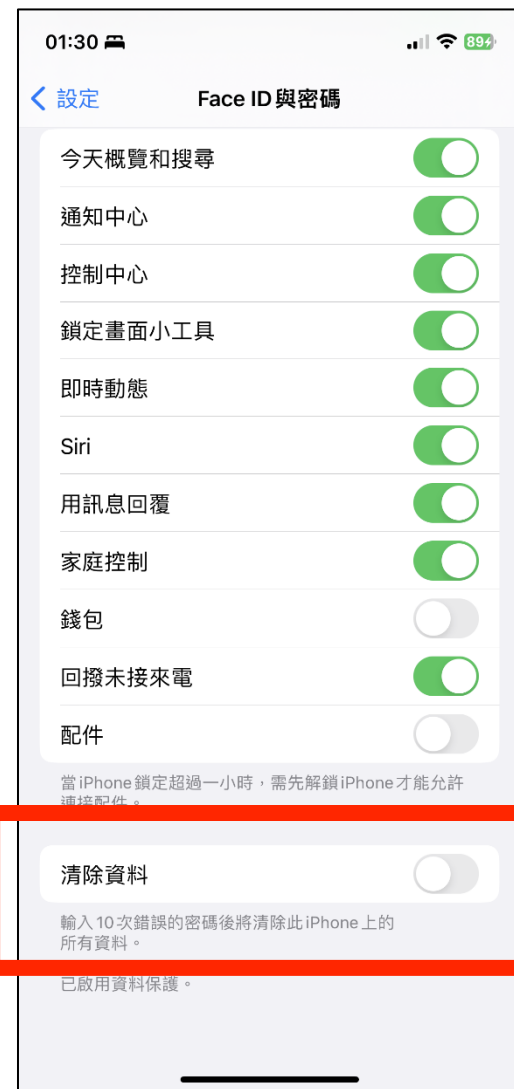
□ 可以的話請同時設定生物辨識

• 指紋辨識

• 臉部辨識

✓ 設定自動Wipe機制(iOS)

□ 密碼猜錯10次，手機會自動清除資料

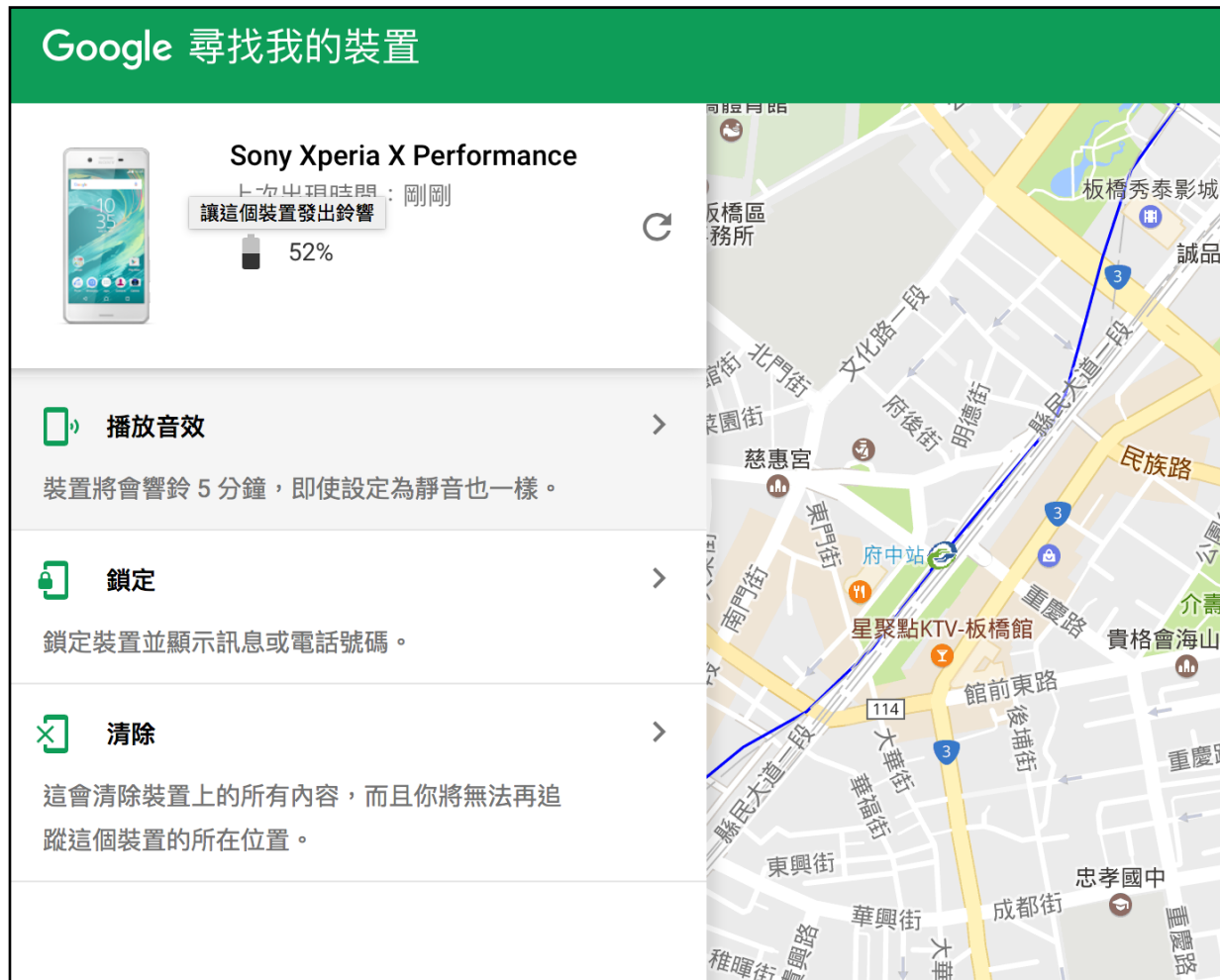
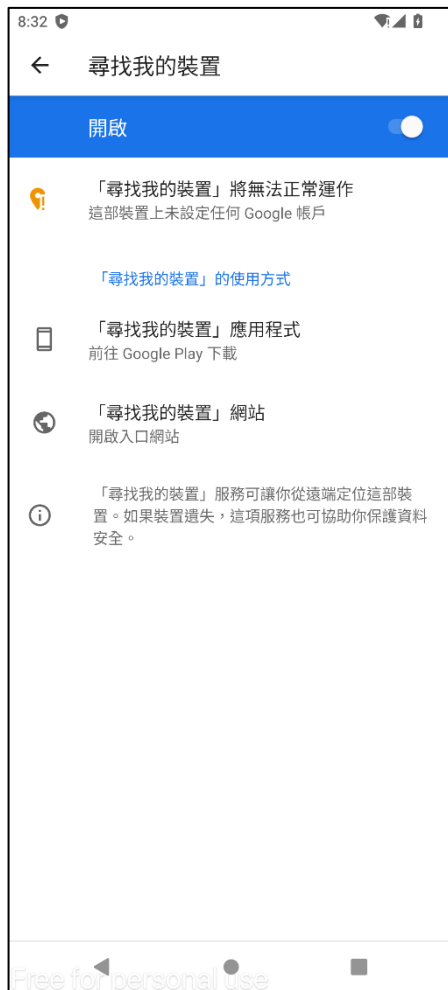


其餘安全設定建議 (3/6)

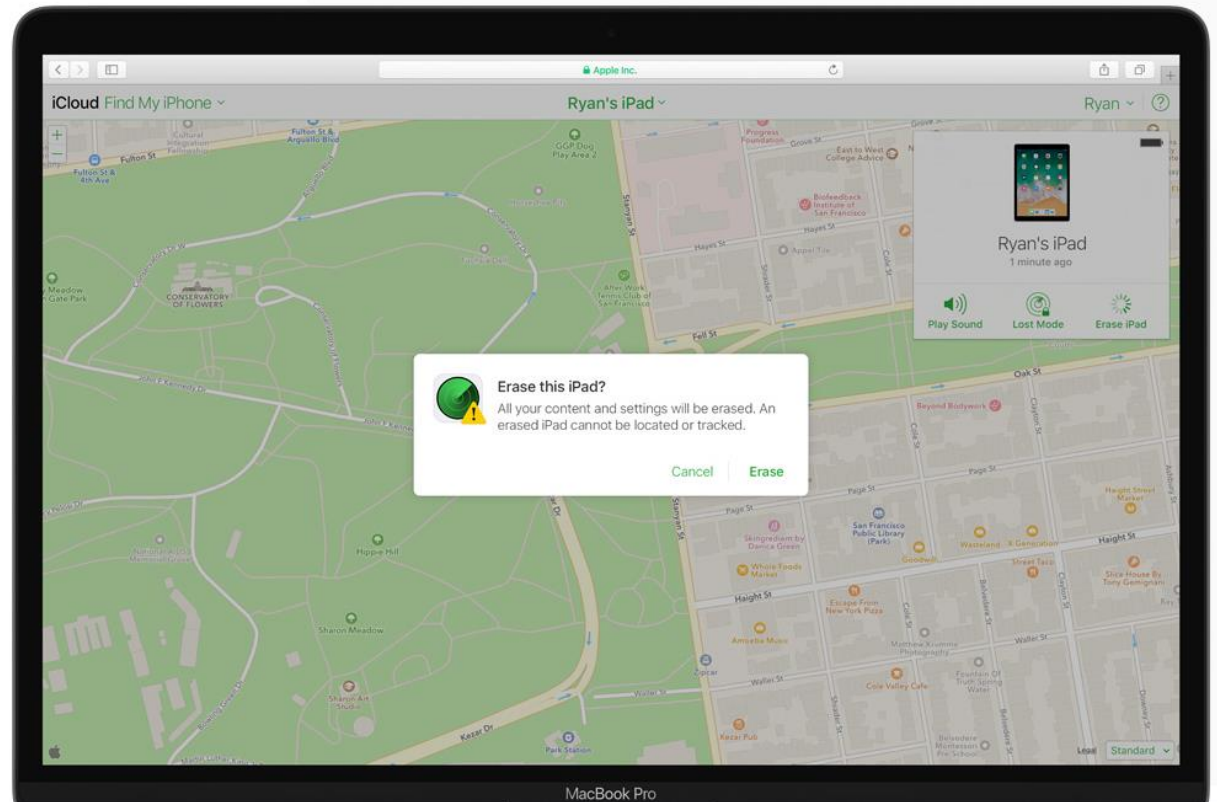
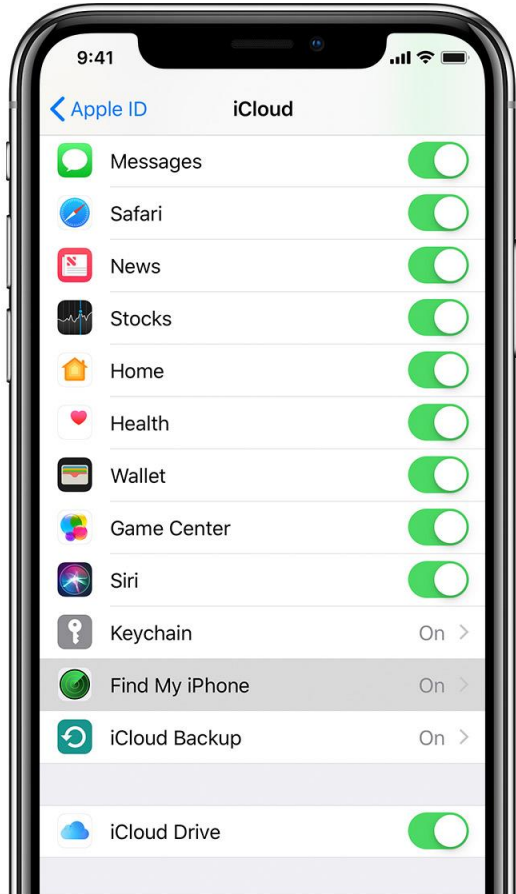
- 啟用手機製造商提供的Find My Phone功能
 - ✓ 可以遠端清除裝置
 - ✓ 可以遠端定位裝置
- 啟用Google原生的裝置管理員功能
 - ✓ <https://www.google.com/android/devicemanager>
 - ✓ 可以遠端清除裝置
 - ✓ 可以遠端定位裝置
- 帳號密碼也要保護好...
 - ✓ Find My iPhone勒索案例近幾年開始出現

其餘安全設定建議 (4/6)

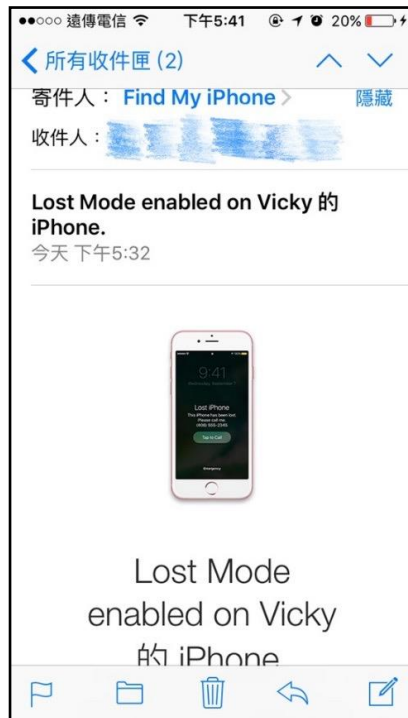
設定 > 安全性 > 尋找我的裝置



其餘安全設定建議 (5/6)



其餘安全設定建議 (6/6)



四、結語

結語

- 工作、上網、娛樂均與智慧型手機密不可分，且手機較個人電腦存有更多的**私密資訊**，駭客會嘗試透過**漏洞**、**惡意APP**、**釣魚**等管道侵入
- 智慧型手機應注意保持更新至**最新的作業系統與軟體版本**，以降低資安風險
- 智慧型手機使用上要注意養成良好習慣，**不安裝來路不明APP**、對於**釣魚簡訊**、信件、下載連結應**保持強烈警覺心**



中華電信
Chunghwa Telecom

報告完畢
敬請指教

Thank You!

