SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

https://stb.stpi.narl.org.tw/

資安暨智慧科技研發大樓

2023.03.25 (六) —— 2023.03.31 (五)

對拼多多app利用0day漏洞控制使用用戶手機及挖取數據的分析，含分析指南

拼多多透過挖掘手機廠商與雲服務廠商的相關漏洞，並將漏洞技術利用於突破系統限制來挖掘使用者的所有訊息與監控所有傳輸資料，侵犯用戶隱私與盜取用戶資訊，並且安裝後門於手機內將用戶的各項機敏資訊用於廣告使用。

【資料來源：REDDIT, 2023.03.27】

WiFi協議漏洞允許攻擊者劫持網絡流量

研究人員在 IEEE 802.11 WiFi 協議標準的設計中發現了一個安全漏洞，可以利用該漏洞誘使連線中的裝置流量以明文的方式傳輸到指定的裝置，已達到劫持流量冰監控內容的目的，建議使用者可以關心韌體更新進度，儘速更新避免遭受影響。

【資料來源：BLEEPINGCOMPUTER, 2023.03.28】

新的 AlienFox 工具包可竊取數十種雲服務的憑證

SentinelLabs 的研究人員發現一個名為 AlienFox 的新工具包，該惡意程式能針對目前常見的雲端服務提供商中含有配置錯誤或是權限控管不當的主機進行憑證竊取，呼籲管理員須定期檢視內部環境避免設定錯誤使得企業憑證遭受冒用。

【資料來源：SECURITYAFFAIRS, 2023.03.30】

BEC詐騙集團開始轉向竊取真實物品

一些網絡犯罪分子正在轉變他們的商業電子郵件妥協 (BEC) 詐騙方式，不再是偽裝成尋求付款的供應商騙取匯款，現在偽裝成買家來騙取業者提供容易出售的商品並從中獲利，研究人員呼籲企業防護意識須隨時變化，因應不斷變化的攻擊技巧。

【資料來源：DARKREADING, 2023.03.31】