

安全神話破滅 黑客無聲入侵iPhone

經iMessage傳送惡意代碼 用戶不點擊亦中招

魔高一丈

【大公報訊】綜合美聯社、CNN、《衛報》報道：加拿大網絡安全監督組織「公民實驗室」（Citizen Lab）13日公布，至少從今年2月起，以色列網絡情報集團NSO就利用蘋果程式漏洞「無聲」入侵iPhone等移動設備，即使用戶未點擊惡意短訊或連結也會中招。此消息一出，蘋果方面急忙對相關漏洞進行緊急修復，並敦促用戶盡快升級最新iOS 14.8操作系統。

蘋果定於美國當地時間14日上午舉行今年最大的新品發布會，加拿大多倫多大學網絡安全監督組織公民實驗室13日指出，他們今年3月在沙特阿拉伯一名政治活動人士的iPhone記錄中發現，其手機在2月已遭以色列NSO集團的間諜程式「飛馬」（Pegasus）入侵，而且沒有任何可見跡象，因此向蘋果公司提出警告。

蘋果：普通用戶不受影響

公民實驗室研究人員雷頓表示，這次事件係首次經確認並分析的「零點擊」攻擊，用戶即使未點擊惡意文件或連結，裝置也會遭到黑客入侵，蘋果旗下的iPhone、MacBook以及Apple Watch等16.5億部裝置全部受到影響。

據介紹，由於蘋果手機自帶的通訊服務iMessage會自動呈現接收到的圖像文件，因此黑客在向用戶傳送包含惡意代碼的圖像文件後，無需用戶進行任何操作便可在裝置內安裝「飛馬」程式。

其後，「飛馬」可以激活用戶的相機、麥克風，甚至紀錄電郵、通話以及諸如WhatsApp等加密程式的聊天紀錄，並傳送給NSO集團的客戶。公民實驗室將這入侵技術稱為ForcedEntry。

蘋果安全工程和架構主管克爾斯蒂克當日表示，在發現iMessage的漏洞後，已經迅速在iOS 14.8系統中進行修復以保護用戶。他還補充道，這一類型的網絡攻擊極為複雜，需要花費數百萬美元開發而且可使用時間短，通常用於攻擊特定的個人，並不針對絕大部分普通民眾，但沒有點名NSO集團。

對於此次事件，NSO集團並未正面回應，僅表示：「NSO集團將繼續為世界各地的情報和執法機構提供拯救生命的技術，以打擊恐怖主義和犯罪。」

NSO集團近年來是非不斷，早在2019年10月，社交媒體巨頭Facebook就聲稱，旗下通訊程式WhatsApp遭到NSO集團的「零點擊」攻擊，

有1400名用戶受到影響，該公司並向美國聯邦法院提起訴訟。

公民實驗室研究員馬爾扎克表示，由於眾多聊天程式會自動幫連結建立預覽或快取功能，以提升用戶體驗，「許多聊天程式已不可抗拒地成為攻擊軟目標」，相關程式應當加強安全性。

Facebook曾向NSO集團提訴

此外，今年7月，非政府組織「禁忌故事」、國際特赦組織與17間國際媒體合作調查顯示，NSO集團將「飛馬」程式賣給全球40個國家約60個客戶，監控名單上5萬個電話號碼遍布全球50多國，現已確定1000多個持有人身份，多為政要、記者和活動人士。此外，名單上還有189名來自路透社、美聯社、《紐約時報》和半島電視台等媒體機構的記者。

《華盛頓郵報》亦指，有14名現任或前任國家領導人的手機可能曾被人以「飛馬」程式監視。名單中包括3名在任總統：法國總統馬克龍、伊拉克總統薩利赫、南非總統拉馬福薩，10名現任及前任總理，以及摩洛哥國王穆罕默德六世。



▲以色列網絡情報集團NSO被指「無聲入侵」蘋果產品。美聯社



▲蘋果系統出現重大安全漏洞。路透社

Facebook網友評論

- 何永樂：**每次有新機推出，都會有重大保安漏洞
- Chan Joe：**啲好安全(的評論)唔見晒
- San Ka：**每次有新機出前，電量總會亂咁計，自動reboot，唔係約好無人信囉
- Chen Liwei：**說真的，當Android手機平板功能追上iPhone之後，還會堅持iOS作業系統的應該不多了

颶風「尼古拉斯」登陸 得州油企恐再停擺

【大公報訊】綜合CNN、美聯社報道：熱帶風暴「尼古拉斯」14日增強為一級颶風後，沿美國得克薩斯州海岸登陸，當天已導致得州50.3萬用戶停電，許多航班被迫取消，學校也已停課。登陸數小時後，「尼古拉斯」減弱為熱帶風暴，並向路易斯安那州移動。氣象學家警告，它將持續帶來重大洪水威脅。

「尼古拉斯」14日以每小時120公里、相當於12級大風的速度登陸得州，在沿岸地區掀起超過1.5公尺的巨浪，為得州休斯敦帶來460毫米的降雨，使南部腹地面臨山洪威脅。得州州長阿博特表示，人們要做好洪水及龍捲風來臨的準備，並宣布17個郡與3個城市進入緊急狀態。

剛剛遭受颶風「艾達」肆虐的路州這次也會受到影響，而該州直到目前仍有9.3萬戶尚未從此前的斷電中恢復。路州州長愛德華茲說：「豪雨是當前最主要的問題，14到16日，路州南部累積降雨量可能高達152至254毫米」。

8月下旬，「艾達」曾對墨西哥灣石油生產和煉油設施造成嚴重破壞，成為近15年來對美國墨西哥灣原油產出破壞力最大的颶風。目前仍有近50%的美國離岸油井處於停工狀態，「尼古拉斯」令當地石油產業再度面臨停擺。受此影響，國際油價14日激增至一個半月以來的新高。



▲美國得州民眾13日保護自己的臉免受風沙侵襲。美聯社

「飛馬」入侵iPhone過程



來源：《衛報》

裁定谷歌限制競爭 韓國重罰14億

【大公報訊】綜合韓聯社、法新社報道：韓國公正交易委員會（KFTC）14日表示，谷歌涉嫌向智能手機製造商強加自家安卓操作系統，限制移動操作系統市場競爭，因此向其開出2074億韓圓（約13.76億港元）罰單。KFTC表示，這是該機構有史以來開出的金額第9高的罰單。

自2016年7月開始，KFTC就對谷歌公司展開反壟斷調查。該組織9月14日表示，谷歌濫用其在智能終端領域的支配地位，要求智能手機製造商在簽署關於應用商店許可和早期訪問操作系統的關鍵合約時，亦須簽署「反碎片化協議」（AFA）。根據該協議，谷歌不允許設備製造商使用修改過的安卓系統。



▲谷歌公司在美國加州的辦公大樓。法新社

KFTC表示，這種做法有助於谷歌鞏固其主導地位，且破壞了智能設備操作系統的開發創新。因此，KFTC下令禁止谷歌強迫設備製造商簽訂「反碎片化協議」，並對其處以2074億韓圓罰款。

另外，韓國國會8月31日以壓倒性票數通過被稱為「反谷歌法」的《電信商業法》修正案，自9月14日起正式實施。該法案禁止大型應用商店運營商要求程式開發者使用商店內置支付系統，同時不得以不合理理由延遲批准程式上架，或將其從商店中剔除。違例者將面臨公司韓國營業額3%以內的罰款。該法案標誌著韓國成為全球首個禁止谷歌和蘋果等強制開發者使用其支付系統的國家。