維基解密揭黑客軍火庫 入侵全球手機板腦

CIA「入屋」電視假熄機真竊聽

洩密網站「維基解密」昨日公佈近9,000份據稱是美國中央情報局(CIA)的機密文件，揭露局方與外國情報機構聯手，研發逾千種惡意軟件、木馬程式和病毒，入侵智能手機、平板電腦等流動裝置，竊取WhatsApp和微博通訊，蘋果公司iPhone、iPad以及Android和微軟視窗系統產品無一倖免。其中，三星電視被入侵後，會呈現「假關機」狀態，暗中錄取用戶在房間內的通話。

■黑客會透過研發惡意軟件，控制多款電子設備。 網上圖片

「維基解密」表示，名為「7號保險庫」(Vault 7)的文件屬於中情局網絡情報中心，編制時間介乎2013至2016年。若文件屬實，將是中情局歷來最大洩密事件。白宮和中情局未確認文件真偽，但有前情報人員和網絡安全專家均指，當中的計劃代號是中情局所慣用。中情局除了與美國國家安全局(NSA)交換情報和黑客技術之外，亦有與澳洲、加拿大、新西蘭和英國軍情五處(MI5)等國家的機構緊密合作。

竊微博WhatsApp訊息

文件顯示，中情局人員可透過黑客軟件程式，控制美歐等地大量企業的電子設備，包括蘋果iOS、Andriod和微軟手機，還有三星智能電視，把它們變成竊聽器。在一個名為「哭泣天使」的計劃中，中情局和MI5試驗入侵三星F8000智能電視系列產品，令它們處於屏幕沒有畫面的「假關機」狀態，實際上是監聽和錄音，再傳送至中情局的伺服器。文件又指，黑客可繞過WhatsApp、Telegram、Signal和微博的加密技術，竊取用戶私人訊息。The Intercept網站則認為，中情局不是直接攻擊上述軟件，而是入侵並騎劫整部手機，從中竊取用戶的社交通訊。

蘋果稱已修補相關漏洞

「維基解密」發佈文件時形容「CIA的軍火庫已失控」，通過一系列「武器化的黑客工具」，前所未有地控制全球智能設備。為免黑客軟件流傳，「維基解密」未有計劃披露詳情，又批評今次洩密反映中情局未能妥善保管網絡攻擊工具，或會外流至其他黑客手中。

蘋果昨發聲明，表示中情局文件所提及的保安漏洞，在最新的iOS版本已修補，承諾將迅速解決其他漏洞。微軟和三星僅稱會調查事件。民權組織「電子前哨基金會」總裁科恩批評，中情局得知相關軟件和裝置有保安漏洞後，不但沒協助企業改善問題，更利用漏洞監聽公眾。曾揭露NSA大規模監控計劃的前中情局僱員斯諾登指，美國政府刻意讓電子產品留有保安漏洞，「(這些做法)不計後果，令人啞然」。

■路透社/法新社/美聯社/《紐約時報》/The Intercept網站

■CIA試驗入侵三星F8000智能電視系列，令它們處於「假關機」狀態。 網上圖片

■CIA(右下)與軍情五處(左下)及NSA(上)等機構緊密合作。 資料圖片

趁漏洞未修復 發動「零日攻擊」

「維基解密」洩露懷疑是中情局的文件顯示，當局是利用程式上的「零日」(Zero Day)漏洞入侵並控制裝置，亦即在軟件工程師發現相關漏洞、繼而修復問題前，便發動攻擊，藉此將智能手機和智能電視等變成監控工具，例如將三星智能電視調校至「假關機」模式，從而監聽現場人士的對話。

企業「捉蟲」冀盡快更新軟件

「零日」漏洞是指一些軟件開發者在除蟲過程中，未能發現的程序錯誤，一般而言，企業會鼓勵外界專家揭發相關問題，從而可及早藉更新軟件等途徑修復漏洞。由於相關問題愈快修復愈好，因此得名「零日」漏洞。若「維基解密」公開的文件內容屬實，便意味中情局掌握大量未被發現的程式漏洞，令不少軟件面臨被入侵的風險。

為監聽用戶的私人通訊，中情局針對相關漏洞開發了大量惡意軟件和病毒，並將它們植入至相關裝置上，改變程式的運作方式。除了令三星智能電視進入「假關機」狀態之外，中情局亦利用了Android系統和蘋果iOS系統的「零日」漏洞施襲，甚至控制智能汽車。■《每日鏡報》/《泰晤士報》/《衛報》

偷用外國軟件 留「指紋」嫁禍

根據「維基解密」公開的文件，中情局(CIA)設有專責部門，收集俄羅斯等其他國家的網絡攻擊手段。由於中情局在美國總統特朗普上任前，曾經指控俄黑客在大選前入侵民主黨電郵系統，協助特朗普勝出，特朗普陣營因此質疑，民主黨被入侵可能是中情局嫁禍俄羅斯黑客的自編自導事件；但也有網絡安全專家認為，與俄羅斯關係密切的「維基解密」是故意在特朗普團隊「親俄」醜聞沸騰之際，公開密件，為俄羅斯及特朗普開脫。

中情局網絡情報中心轄下的「遙距發展部門」(RDB)有一個名為UMBRAGE的小組，專門偷取外國研發的惡意軟件。中情局不但能夠運用這些軟件進行攻擊，更可誤導目標，讓對方以為攻擊來自研發軟件的國家，如同留下其他人的指紋。

美國大選過後，情報機關一致指控俄國黑客入侵民主黨電腦，暗助特朗普一把，成為媒體報道焦點。不過佐治亞州選舉機構去年也曾發現，當地選舉系統曾經被懷疑來自國土安全部的網絡入侵。 ■《衛報》

研干擾汽車系統 或欲暗殺司機

「維基解密」聲稱，中情局在2014年10月研究干擾汽車控制系統的方法，雖然目的並不清楚，但可能目的是暗殺司機。現時大部分車輛均配備電子剎車控制系統，同時設有加速器、安全氣袋、轉向及車門控制裝置，全部由感應器及電腦控制，容易遭黑客入侵。

不過報道指，黑客入侵汽車系統根本不是新事物，例如2014年有兩名黑客遙距入侵一輛吉普車Grand Cherokee的娛樂系統。雖然車廠其後加強保安措施，但同類威脅仍然存在。 ■《華盛頓觀察家報》

■熄燈後

■熄燈前

美國紐約自由女神像的底座前晚突然停電，只有王冠及火炬繼續發光。經過數小時搶修，自由女神像在午夜前恢復供電。

不少網友對今次停電議論紛紛，有人懷疑是當局故意，藉此支持昨日的「無婦女節」抗議活動。「無婦女節」由婦女團體發起，目的是在國際婦女節當日，呼籲各界關注女性面對的經濟及社會不平等。

■英國廣播公司/美聯社

防黑客小貼士

系統更新

即使中情局沒有入侵裝置，用家也應時常更新智能手機或電視的硬件及軟件，以免遭受其他惡意軟件攻擊

文件指出舊式的Android 4.0系列手機較易被入侵，故用家應盡早轉用新款Android手機，同時換上較難破解的密碼

蘋果公司前日也為iPhone推出軟件更新，填補文件所列出的多項漏洞

膠貼防護

黑客可以利用軟件，暗中開啟電腦的鏡頭和咪高峰，用家可參考facebook創辦人朱克伯格，用膠紙覆蓋鏡頭。雖然看似兒戲，卻能有效防止被偷拍

因為咪高峰即使被遮蓋仍可收音，故應避免購買可上網的智能語音助理系統或電視

移除電源

文件顯示即使關上智能電視，黑客仍可竊聽用家的日常對話

為防萬一，用家可中斷裝置的網絡連線、移除電源和避免在電視旁進行敏感對話，也應減少購買產品安全較差廠商的產品

保持警戒

雖然多數用家不會成為中情局目標，但不要胡亂點擊來歷不明的網絡連結或電郵附件

《每日郵報》/美國有線新聞網絡/美聯社

潛駐德總領館 曾網攻中國

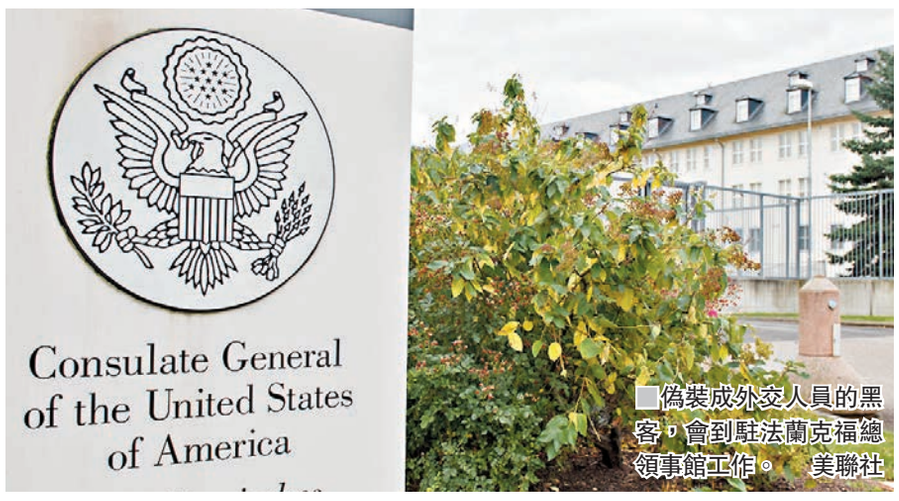
「維基解密」的文件揭發，美國駐德國法蘭克福總領事館，竟然是中情局(CIA)的秘密行動基地。隸屬中情局的黑客偽裝成外交人員潛入德國，曾在領事館內向中國等地發動網絡攻擊。中情局的內部指引不但教導這些黑客如何隱藏身份，也提供瑣碎的生活小貼士。德國政府表示嚴肅關注事件。

美國駐法蘭克福總領事館是全球最大的美國領事機構，被派往當地的黑客會獲發外交護照及國務院銜頭，他們在領事館研發惡意軟件，用以攻擊歐洲、中東及非洲的目標。德國傳媒報道，中情局、國家安全局、軍方秘密人員等都把領事館當成基地。另外，美國也在法蘭克福建立龐大的哨站及空殼公司網絡。

中情局為身在德國的黑客提供詳盡指引，讓他們能順利進入領事館，又要求他們切勿將電子儀器或敏感資料留在無人看管的酒店房間，以免機密外洩。

致黑客旅遊貼士：勿到油站用膳

另外，當局也列出一系列旅行貼士，內容輕鬆，如同旅遊雜誌，例如建議黑客乘搭漢莎航空，理由是酒精飲品免費，若不幸乘坐聯合航空則「為你致哀」。文件又提醒黑客抵埗後別忘了洗澡，並說：「假如你在周日早上抵德，會發現大部分商店(尤其食品店)都休息……不建議到油站用餐。」 ■德國之聲



■偽裝成外交人員的黑客，會到駐法蘭克福總領事館工作。 美聯社