WannaCry始作俑者 威脅洩中俄伊朝核武計劃

黑客組織揚言 揭Windows 10漏洞

■Shadow Brokers聲稱擁有從未公開的Windows 10“零日”漏洞。　網上圖片

黑客組織Shadow Brokers早前洩露美國國家安全局(NSA)網攻工具，造就勒索軟件“WannaCry”肆虐全球。該組織日前揚言，計劃自下月起出售另一批惡意軟件程式碼，令黑客可入侵全球最廣泛使用的電腦、軟件及手機。Shadow Brokers除威脅公開涉及中國、俄羅斯、伊朗和朝鮮的核武和導彈計劃外，亦表示會披露“SWIFT”全球銀行交易系統的資料，以及微軟作業系統Windows 10中從未公開的“零日”(Zero Day)漏洞。

微軟表示，已留意到Shadow Brokers的最新聲明，指微軟網絡保安團隊正監察潛在威脅，從而採取適當行動。美國國土安全部亦展開提升網絡保安意識的運動，敦促科技業界盡快下載微軟在3月份發佈的更新，以堵塞“WannaCry”用以發動攻擊的漏洞。

售入侵工具央行資料

Shadow Brokers在網誌表示，只要任何人願意付出所需價錢，便可以獲取科技界中最重大的商業秘密，它表示會設立每月資料庫，出售入侵網頁瀏覽器、網絡路由器及手機的工具，以及公開從各國中央銀行竊取得來的資料，將於下月披露更多詳情。

英醫院服務大致恢復

“WannaCry”被指與朝鮮黑客組織Lazarus有關，但歐洲刑警組織表示，目前仍在調查，不宜過早下定論，又指受襲的英國醫院、歐洲車廠以至俄羅斯的銀行，目前情況已經穩定。

英國國家醫療服務系統(NHS)是今次網攻的重災區，多個電腦系統癱瘓，部分病人需轉送至其他醫院。NHS英格蘭全國事故總監雷恩斯伯里前日表示，病人無需再從急症部門分流出去，大部分服務已接近恢復正常。不過，多間醫院仍未能全面提供服務，倫敦聖巴塞洛繆醫院需取消預約，警告病理及診斷服務會受阻延。諾福克郡一間醫院的電腦需要升級，藥劑部門只能局部提供服務。　■路透社/法新社

利用相同漏洞 黑客暗挖虛擬幣

專家表示，早在“WannaCry”肆虐前，一款電腦病毒已經利用相同的Windows系統漏洞，自上月底以來潛入20多萬部電腦，暗中種植“礦工”，協助黑客開採新興虛擬貨幣“墨內羅幣”(Monero)。網絡安全公司Proofpoint主管卡倫貝爾表示，黑客或已從中賺取逾100萬美元，遠多於從“WannaCry”攻擊中獲取的贖金。

國際專家早前已懷疑，朝鮮黑客集團Lazarus是“WannaCry”的幕後黑手。

網絡安全企業卡巴斯基上月初指出，Lazarus一個負責敲詐金錢的小組，在歐洲一個伺服器中安裝惡意軟件，開採墨內羅幣。外界估計，上月底藉病毒開採墨內羅幣的攻擊，也是朝鮮所為。

卡倫貝爾表示，歐洲上月初的個案、上月底開採墨內羅幣的病毒，以及現時“WannaCry”勒索事件三者相信互有關連，因為全球墨內羅幣“礦工”數目不多。　■路透社

“Jaff”勒索軟件 圖侵港府電腦不遂

香港文匯報訊（記者　文森）繼勒索軟件“WannaCry”，再有惡意軟件企圖入侵香港政府電腦系統。政府資訊科技總監辦公室日前表示，近日在萬多條寄往政府用戶的可疑電郵中，約有100條送達用戶郵箱，並確認為現時在互聯網非常活躍的“Jaff”勒索軟件，但該惡意軟件不會主動攻擊其他電腦，政府電腦系統運作暫無影響。

電腦保安事故協調中心亦收到一宗“Jaff”勒索報告，黑客要求用戶繳付約2.8萬港元贖金。中心指“Jaff”的電郵主題有固定格式，由一個單字及一組隨機數字組成，中間隔以底線，例如“Copy_12345”。中心建議用戶定期備份電腦檔案及安裝防毒軟件。

11歲神童入侵藍牙 玩具熊變“武器”

美國11歲電腦神童保羅日前在荷蘭一個資訊安全會議上，示範如何入侵與會者的藍牙裝置，以操縱一隻智能玩具熊成為網攻武器。綽號“網絡忍者”的保羅來自得州奧斯汀，是一名初中學生。他在會議上透過WiFi和藍牙技術，把玩具熊接上雲端，以接收及傳送訊息。他其後把信用卡大小的“Raspberry Pi”微型電腦，插入自己的手提電腦，掃描場內可供使用的藍牙裝置後，下載了數十個電話號碼，包括多名高級官員的號碼。保羅接着利用電腦程式語言Python，透過其中一個號碼入侵玩具熊，除了開啓它的燈光外，更在現場觀眾間錄下一段簡訊。　■法新社