涉為監控拒通報微軟 斯諾登促國會求交代

NSA瞞漏洞變網災禍首

■美國政府的網絡計劃花費大量資源發展網絡武器，包括用作攻擊敵人的電腦系統及監控通訊等。 網上圖片

今次黑客用作襲擊全球網絡的勒索軟件，被揭發是美國國家安全局(NSA)開發的間諜工具，用於監控網絡及收集反恐情報。網絡保安專家警告，這些由NSA開發的軟件，一旦落入犯罪分子之手，會淪為犯案工具，成為全球安全隱患。曾洩露美國監控資訊的中情局前職員斯諾登，批評NSA是這次網攻始作俑者，指它早知微軟視窗有漏洞，但為方便監控而未有通知微軟修復，促請國會要求NSA交代其「網絡武器」運作情況。NSA未就事件回應。

■斯諾登批評NSA是這次網攻始作俑者。 網上圖片

美國政府的網絡計劃花費大量資源發展網絡武器，包括用作攻擊敵人的電腦系統及監控通訊等，更利用網絡保安漏洞進行攻擊。各界關注情報機關擁有強大網絡武器的風險，民權組織美國公民自由聯盟發聲明指，今次事件凸顯網絡漏洞除可被保安機關加以利用，亦可淪為不法分子的犯罪工具。

「生產危險工具反被利用」

斯諾登認為，只要NSA一早暗中通知微軟有關漏洞，今次全球網攻事件便可避免，批評NSA是罪魁禍首，「生產危險的網絡攻擊工具，現在反被用作攻擊西方國家，令所有人都付出代價。」

全球多個網絡保安專家，亦對NSA未有通報漏洞表示關注。外界相信按一般做法，NSA發現任何網絡漏洞，會經內部程序決定是否將漏洞通報微軟、蘋果及Google等科企，以保障國民及機構安全，但NSA亦可能基於情報目的而選擇隱瞞。

外界以為微軟今年3月安裝軟件堵塞漏洞，是因獲得NSA「通水」，但實際是微軟發現黑客組織Shadow Brokers散播病毒，才自行推出軟件修復。

網絡公司Veracode科技主管衛索帕指出，即使微軟及時推出軟件補救，問題依然存在，因為一般機構需要8周時間才能完成更新，這段期間足以讓犯罪分子開發複雜的攻擊軟件，發動襲擊。 ■路透社/《國際財經時報》/《華盛頓郵報》

防範措施

■備份檔案

勒索軟件最大傷害是令檔案和資料消失，最佳防範方法是將所有資料和檔案，備份到一個完全分開的系統，例如沒有連接網絡的外部硬件或外部伺服器

■對電郵、網站和應用程式(App)保持戒心

在點閱垃圾郵件或瀏覽不熟悉的網站時應保持警惕，切勿下載沒經過官方商店認證的App，並在安裝程式前先閱讀評論，在使用電郵或其他賬戶時啟動雙重認證功能

■使用防毒程式

防毒程式可掃描文件，看下載前是否含勒索軟件，也可封鎖惡意廣告，以及搜尋可能已在電腦或裝置上的惡意軟體

■經常更新軟件

微軟等公司會不時推出軟件更新，修補可用作安裝勒索軟件的漏洞

■絕不付贖金

受害者付贖金只會助長黑客，且不確保可取回檔案

■其他方法

在手機下載Signal程式，加密文字訊息；在電腦啟用蘋果公司FileVault或微軟BitLocker功能，定期更改密碼，瀏覽網頁時使用HTTPS插件，也可考慮使用虛擬私人網絡(VPN)，以及用其他搜尋引擎搜索敏感資料

《華盛頓郵報》《紐約時報》

毒郵件「時速」500萬封傳播

據網絡保安專家指出，今次黑客使用的勒索病毒傳播速度極快，含有該病毒的郵件，以近每小時500萬封的速度發出。歐洲刑警組織(Europol)昨日發表聲明，指今次全球網絡攻擊的規模，達至前所未見的程度，當局必須在在國際層面展開全面調查，才能找出幕後黑手。該組織屬下的歐洲網絡犯罪中心(EC3)，正與受影響國家合作，以減輕所面臨的威脅和幫助受害者。 ■法新社

勒索軟件攻擊急增50%

美國電訊商Verizon上月發表年度報告，顯示涉及勒索軟件的網絡攻擊個案去年大增50%，其中金融服務、醫療服務及政府部門成為黑客3大攻擊目標，而勒索軟件更成為第5種最常用的惡意軟件，較2014年只居第22位大幅上升。

報告研究逾80個國家發生的2,000宗網絡入侵事件，顯示網絡間諜活動日益猖獗，佔黑客入侵網絡事件的20%，來自中東和東歐的黑客活動亦有上升趨勢。其中黑客愈來愈傾向攻擊中小企，中小企遭攻擊個案佔整體達61%，較前年多8個百分點。

同時，黑客更將目標擴大至「物聯網」，攻擊連接網絡的設備，例如在美國總統就職典禮前數日，入侵華盛頓警方系統，關掉所有攝錄鏡頭，並攻擊三藩市公共交通網絡的讀票機。此外，不少黑客利用自動工具攻擊網絡，以及出租或出售惡意軟件予其他黑客，以防自己被發現。 ■英國《金融時報》

美兩醫院曾交贖金 改手寫存檔

部分國家的醫院今次遭受網絡攻擊，英國國家醫療服務系統(NHS)更是重災區。事實上，醫療機構遭網絡勒索早有前科，由於涉及病人生死，黑客相信醫院會盡快交贖金。美國洛杉磯荷里活長老會醫學中心去年2月曾被黑客入侵，需付出相當於1.7萬美元(約13.2萬港元)的比特幣，才能取回電腦控制權。

該醫院行政總裁斯特凡內克表示，當時醫院電腦內的檔案全被惡意加密，最快和最有效的還原方法是繳付贖金，取得解密鑰匙，院方為讓醫院運作回復正常，因此支付贖金。在技術人員協助下，院方數日後重新控制電腦系統。斯特凡內克強調沒有醫療服務受影響，亦沒有醫院記錄外洩，但此後院方改用紙筆為病人記錄存檔。

美國堪薩斯心臟醫院去年也曾受黑客入侵，但交付贖金後，對方只解封部分資料，以圖敲詐更多金錢，院方拒絕，自此便無法讀取部分數據。 ■《衛報》

■美國民眾對NSA的監控表達不滿。 路透社

英專家「救世」：註冊網域名可解鎖

勒索軟件WannaCry對全球網絡進行攻擊，災情蔓延至99個國家和地區，不過英國一名網絡安全專家卻意外發現，只需花費10.69美元(約83港元)註冊隱藏在WannaCry的網域名稱，便可啓動「鎖死鍵」功能，防止災情進一步擴散。不過，已受感染的電腦不會因而復原，勒索軟件的其他版本仍可傳播病毒。

該名專家透過微博twitter賬戶「@MalwareTechBlog」表示，勒索軟件是藉着未被註冊的網域名稱，從而令病毒傳播，又指危機仍未解除，黑客可改寫程式碼再次發功，故民眾需盡快更新系統。該專家又坦言今次發現純屬偶然，自己在註冊網域名稱時沒察覺它可擋下病毒，是在事後才知道。 ■法新社/《衛報》

■有網站以地圖方式展示受影響國家及地區。網上圖片

G7財長會 籲加強合作反「黑」

在意大利巴里召開的七大工業國集團(G7)財長會議，昨日舉行最後一天會議，集中討論黑客入侵電腦系統，對全球銀行體系和金融業的威脅，與會代表呼籲各國合作對抗網絡攻擊。適逢全球電腦網絡遭勒索軟件大規模攻擊，東道主意大利財長帕多安形容這次討論「不幸地來得非常及時」。

路透社獲得的G7財長會議聲明草案文本，指網攻對經濟構成的威脅愈來愈大，應列為優先處理項目，並呼籲各國盡快分享情報，及早找出金融系統的弱點。此外，聲明還建議各國推出措施，加強獨立金融企業的網絡安全。 ■法新社/路透社

■G7財長會議討論黑客入侵，適逢網攻事件發生。 美聯社