NSA網絡「武器」被盜用 近百國中招

史上最嚴重 黑客全球鎖「腦」勒索

【大公報訊】綜合英國《每日郵報》、法新社、路透社報道：全球99個國家或地區的逾7.5萬台電腦遭受「蠕蟲」式勒索病毒感染，受害者包括歐美和亞洲多國。業界表示，這是有紀錄以來最嚴重的黑客攻擊。黑客利用美國國家安全局（NSA）網絡武器庫中泄漏的黑客工具，製成勒索軟件。目前受災最嚴重的是俄羅斯，雖然本港僅一名市民受到黑客攻擊，政府、醫院等其他部門暫未被波及，但電腦保安事故協調中心13日已就加密勒索軟件，發出「極度危險」保安公告。

這個名爲「想解密／想哭」（WannaCrypt）的電腦病毒主要針對運行微軟系統的電腦，電腦中毒後，用戶資料會被封鎖，而用戶必須向黑客支付價值約300至600美元（約2338至4676港元）的比特幣贖回資料。微軟方面回應稱，已經增加了檢測和保護措施，以防止事件蔓延，並再度呼籲用戶下載補丁、更新系統。

無需經電郵就能進行攻擊

香港電腦保安事故協調中心經理梁兆昌解釋指，今次的勒索軟件有別於過往，它無需利用含有電腦病毒的電郵及網頁這種攻擊的方式，而是直接在互聯網上尋找未有安裝防火牆及防毒軟件等防禦裝置的用戶，經掃描後若發現其電腦有SMB（伺服器信息區塊）漏洞，即可加密檔案，進行勒索。

軟件亦可透過一部「中招」電腦內的資料，攻擊另一部電腦，換言之，如果一間公司的一部電腦受攻擊，就可利用內含的資料，找到同公司的其他電腦，隨時令公司所有電腦遭殃。

本港政府部門運作正常

梁兆昌稱，13日凌晨接獲了一名市民的相關求助，其家用電腦被勒索軟件「想解密／想哭」攻擊，電腦數據被加密，該用戶使用Windows 7，直接使用上網數據機接駁電腦上網，但電腦無安裝防火牆或防毒軟件，用戶也沒定期更新電腦的保安系統。

警方發言人稱，截至13日晚暫未接獲或知悉其他有關勒索軟件的舉報，警方會繼續留意情況，並與政府資訊科技總監辦公室及香港電腦保安事故協調中心保持聯繫。

政府資訊科技總監辦公室也稱暫未收到政府部門事故報告，所有系統正常運作，並強調已加強監察網絡攻擊及其保安威脅。醫院管理局發言人亦表示未收到任何電腦系統事故報告，醫管局電腦系統有多重保安措施，防止病毒攻擊，已要求同事提高警覺，並會密切監察情況。港燈、中電、九巴等本港大型機構均稱，未有受黑客軟件攻擊。

▲意大利多所高校出現病毒感染 網上圖片

斯諾登劍指NSA無視警告

據了解，此次侵襲全球的「蠕蟲」勒索病毒，源自NSA網絡武器庫中泄漏出的黑客工具「永恆之藍」。這批加密軟件於上月被名爲「影子經紀人」的黑客組織盜走。

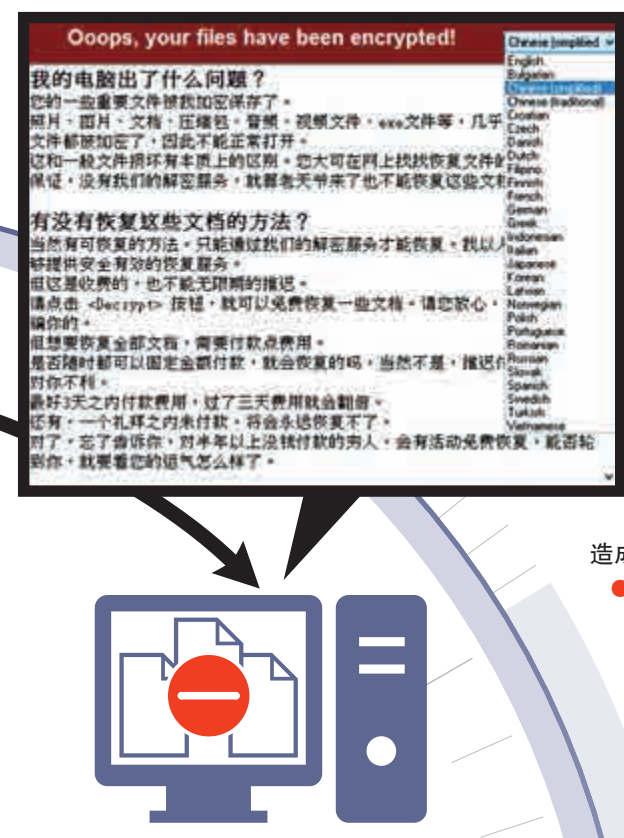
「棱鏡」事件泄密者斯諾登爲此指責NSA難辭其咎。他在推特上寫道：「NSA無視警告，還是製造了可以進行網絡攻擊的危險工具。今天我們知道了其中的代價。」

斯諾登還表示，國會應該就此事向NSA進行詢問，確認後者是否還知道除了微軟以外，其他大型應用軟件的弱點，又是否根據這些弱點編寫過攻擊軟件。

計算機安全專家克盧利也表示，「美國情報機構在微軟軟件中發現了一個安全漏洞，他們的做法並不正派，把這個漏洞保留給了自己，並利用這一漏洞來進行間諜行爲。然後他們自己也遭了殃。」

不少媒體業開始譴責NSA，指此前美國政府和NSA一直表示發展網絡項目主要爲了防護和安保。但此次事件揭露，美國政府及附屬機構，一直在研發可以進行攻擊的網絡項目。NSA目前尚未對此事予以置評。

◀遭到黑客「蠕蟲」式勒索病毒感染的微軟系統電腦畫面 網上圖片



勒索軟件圖解

（法新社）

全球遭黑客網攻的國家及地區

- 紅色為最嚴重地區
- 黃色為較嚴重地區
- 綠色為受影響地區

來源：美國TechCrunch科技網站

黑客勒索事件 Q&A

病毒肆虐範圍有多大？

●已有99個國家或地區受影響，相關案件達7.5萬多起。

哪些重要部門或公司受影響？

●英國公共衛生體系「國民醫療服務系統」是重災區之一，導致英國數十間醫院被迫取消手術，工作人員指恐造成病人「吃盡苦頭，甚至死亡」。

●俄羅斯受災比其他國家都嚴重。該國內政部上千部電腦受到攻擊，但已將病毒感染限於局部。俄羅斯第二大移動電話網絡Megafon，也表示受到病毒影響。

●西班牙電信巨擘Telefonica、伊維爾德羅拉電力公司及公用事業的天然氣公司、德國鐵路系統及葡萄牙電信公司和聯邦快遞也都受到不同程度影響。

幕後黑手是誰？

●上月，名為「影子經紀人」的黑客組織聲稱從美國國家安全局盜走了「EternalBlue」黑客軟件。他們此後還曾試圖在網上拍賣這些加密軟件。專家指，這批軟件正是造成此次黑客襲擊的元兇。這讓「影子經紀人」看起來最像此次事件的幕後黑手，但他們已於上月8日選擇公開這些軟件的密碼，這意味着，網上任何一個黑客都能獲取並使用這些軟件。「影子經紀人」稱，公布密碼是對美國總統特朗普的「抗議」。

為何用比特幣支付？

●近年來比特幣以虛擬貨幣的形式嶄露頭角後，使其成為洗錢或網絡犯罪的工具，主因是採用匿名交易，且毋須任何正式金融機構經手。

（英國廣播公司）

中國高校成災區 大批畢業生論文被黑

【大公報訊】駐北京記者馬琳報道：有黑客近日鎖定Windows系統漏洞進行勒索病毒攻擊，「疫情」已波及99個國家或地區，中國內地和中國台灣都未能幸免，大量企業、高校等內網環境用戶中招。

自本月12日開始，Onion、WNCRY兩類勒索病毒變種在中國逐步爆發，感染用戶主要集中在企業、高校等內網環境。其中，校園網是重災區，多所高校出現病毒感染。大量學生的畢業論文等重要資料被病毒加密，只有支付贖金才能恢復。面臨畢業答辯的學生紛紛表示「辛辛苦苦碼了一年的論文沒被學校掛掉，反而被黑客掛掉了」。

金山毒霸安全中心指，從目前監控到的情況來看，中國內地全網已經有數萬用戶感染，QQ、微博等社交平台上也是哀鴻遍野。另外，全國多地的中石油加油站也無法進行網絡支付，只能改用現金。

中國寶島台灣也是此次病毒攻擊的重災區。台灣媒體稱，台灣是僅次於俄羅斯與烏克蘭，遭攻擊程度最嚴重的地區之一。有人報料稱，病毒「猖狂」得連公司電腦的進出廠刷卡系統也不放過，要交「贖金」才能打開。

獵豹安全專家李鐵軍向大公報記者指出，此次大範圍病毒感染主要還是用戶的安全防範意識不夠，廣泛存在未修補的系統漏洞造成的。微軟公司今年3月已經處於安保原因要求用戶下載升級補丁，但「顯然，很多人沒當回事」。李鐵軍說，這次事件對廣大互聯網用戶是一個深刻的教訓，安全防範不能只停留在口頭上，要主動發現漏洞並及時修復。另外對於國家機構用戶，還應該組織一支隊伍模擬攻擊，加強防黑客能力。

英公立醫院緊急轉移病人

【大公報訊】據英國《每日郵報》、中央社報道：英國公共衛生體系「國民醫療服務系統」（NHS）12日遭大規模黑客網絡襲擊，目前已有數十家醫院受到影響，救護車無法進行正常調配，多地的醫院因擔憂急症病人出現危機，已將他們轉移至其他治療地點。不少醫院還取消了病人正常的預約求診，並強烈呼籲，民眾如果沒有重大疾病，暫時不要前往醫院求診。

英國首相文翠珊指，這起襲擊事件並不是專門針對英國公共衛生體系的，目前也沒有證據表明患者的數據遭到泄露。英國國家網絡安全中心將與國民保健制度數字中心密切合作，以幫助受到影響的醫療機構，確保患者的安全。

報道指，醫療機構遭遇勒索軟件攻擊要求付錢案例與日俱增。美國去年亦有三家醫院以同樣方式遭黑客襲擊。其中，去年二月，美國洛杉磯的荷里活長老會醫學中心被迫付出相當1.7萬美元（約合13.26萬港元）的比特幣贖金，才讓院內電腦系統恢復正常。安保公司Avast專家克魯斯泰克說：「勒索軟件變得特別惡劣，尤其感染像醫院這樣的機構，這會讓人命置於險境。」

▲英國數十家醫院遭受黑客攻擊之後，緊急轉移病人 網上圖片