中招家庭用Windows 7 警:勿交贖金不建議格式化

「WannaCry」肆虐 港現18宗勒索

香港文匯報訊（記者 文森）本港對勒索軟件「WannaCry」嚴陣以待。政府資訊科技總監辦公室在昨日的聯合記者會上表示，暫未接獲任何政府部門的事故報告，指重要資料主要存放在雲端及伺服器，勒索軟件難以攻擊，重要文件亦「每分每秒在備份」。生產力促進局繼日前收到2宗「WannaCry」勒索舉報，昨日再收到15宗，連同警方接獲的1宗報案，至今共收18宗勒索舉報。醫管局指已做好應變措施。創新及科技局局長楊偉雄呼籲市民保持冷靜，因為今次事件不單是電腦保安問題，亦是電腦罪案問題。

■警方聯同香港生產力促進局及政府資訊科技辦公室召開記者會，跟進「WannaCry」勒索病毒事件。左一為黃家偉，左二為林偉喬。 香港文匯報記者潘達文 攝

電腦保安中心支援中小企

政府資訊科技總監辦公室、香港生產力促進局及警方昨日召開記者會。副政府資訊科技總監（基礎設施及營運）林偉喬表示，已向各政府部門發出網絡保安指引，另香港電腦保安事故協調中心負責向中小企提供支援，協助香港整體應對保安威脅，同時協調中心會與其他國家及地區交換網絡安全情報，以掌握病毒變種及處理方法等資訊。

林偉喬續指，昨日為發現勒索軟件後的首個工作天，不排除未來有更多電腦受感染，會繼續觀察情況。他並指已經要求政府部門備份文件，預計這兩天完成。

香港生產力促進局總經理黃家偉表示，至今共收到17宗求助個案，當中15個是家庭用戶，均使用Windows 7作業系統，而另外2宗則為商業用戶，分別使用Windows Server 2008及Windows 7作業系統，局方亦另收到160至170宗查詢及求助個案。

警:中招後應聯絡警方

警方呼籲「中招」者不應按指示繳交贖金，因黑客並無答應肯定解封，而交贖金只會助長黑客的犯罪行為，且不建議格式化電腦，因有可能毀滅證據，提醒市民中招後應盡快聯絡警方及專家。警方指，警方設立熱線2860-5012，方便市民就「WannaCry」勒索軟件查詢及舉報。

醫院病歷存伺服器

醫管局資訊科技及醫療信息主管張毅翔表示，醫院約五萬部電腦暫未受感染，病人資料和病歷全部儲存在中央伺服器，並非在個人電腦中，相信即使有電腦受感染，只需清洗「中毒」的電腦即可，不會為醫療系統帶來大影響。該局亦已成立特別事故應變小組，增撥人手協助同事檢查電腦。該局目前未有接獲公立醫院電腦系統受有關軟件影響的報告。

■政府跨部門記者會講WannaCry攻擊及勒索。 香港文匯報記者潘達文 攝

電腦保安中心：應常更新電腦

香港文匯報訊（記者 文森）勒索軟件「WannaCry」在全球各地攻擊電腦系統，香港電腦保安事故協調中心經理梁兆昌昨日接受電台訪問時形容，「WannaCry」比以往的勒索軟件更具侵略性，會主動在互聯網搜尋目標，再強行攻擊，並將電腦檔案加密，因此沒有更新及直接接駁互聯網的電腦均屬高危。他提醒市民要恒常更新電腦和設定防火牆。

梁兆昌表示，昨日新增的「中招」個案之中，當中至少有三宗沒有更新電腦及修補程式。不過，電腦即使已安裝防火牆，只能抵擋外間的攻擊，如內聯網有一部電腦受攻擊，即使其他電腦已安裝防火牆，整個內聯網的電腦亦會很大機會同樣被加密。

若受攻擊 應拔走網線

他指「WannaCry」發展成熟，暫時未有方法將已被勒索軟件攻擊的檔案解密，建議用戶開啟電腦前中斷上網連線，檢查視窗作業系統，若安全性保護並非處於最新狀態，最好先作更新，並應安裝防火牆和防毒軟件，若發現電腦受到勒索軟件攻擊，應第一時間拔走上網線。

專家：亞洲電郵大量「地雷」 日產日立中招


■亞太多地中招，印尼有醫院的輪候取票機停用。 美聯社

昨日是周一工作天，勒索軟件「WannaCry」在亞太地區進一步蔓延，日本和韓國都有政府網絡或企業受影響，其中至少兩間日本大企業中招。

日本非牟利電腦維修組織稱，全國共有約2,000部電腦被入侵。汽車生產商日產昨日承認，數個部門成為攻擊目標，但未影響營運。日立電機發言人則表示，由於受到網絡攻擊，公司內部系統發生故障，出現電郵收發困難、無法打開附件等情況，事件與「WannaCry」有關，但黑客暫未要求他們繳付贖金，公司正在安裝軟件搶修。據報日本亦有醫院和個人電腦感染「WannaCry」。

比特幣難用 黑客僅收39萬

韓國網絡振興院則指，自13日起韓國共有8家企業報告感染「WannaCry」病毒，請求技術支援，當中共有13宗疑似中毒，但未最終確認。韓國的政府和公共機構暫未報告受感染。韓國殺毒軟件公司Ahn Lab公佈，12日至昨日下午2時，共發現187台受害電腦。韓國的網絡安全企業強調，病毒傳播需要一定的時間，因此不能放鬆警惕。目前被發現感染病毒的IP地址數量不斷上升。部分網吧、餐廳等小型商舖也不斷發現被感染。

澳洲網絡安全部門昨日稱，全國只有3間企業被攻擊，醫療系統等重要基建均未受影響。新西蘭則暫時倖免於難，但當局已加強網絡保安措施。

協助執法機關追蹤罪犯使用加密貨幣的英國初創企業Elliptic總裁史密斯稱，自上周五勒索軟件攻擊開始以來，黑客只合共收到約值5萬美元(約38.9萬港元)的比特幣，隨着黑客警告會提高贖金要求，預計支付金額會增加，但以如此大規模的網攻，收到的贖金明顯偏少，除了因人們聽從保安專家和政府呼籲拒交贖金外，亦由於不少受影響公司不懂如何購買及支付比特幣。

網站超連結傳播變種

對於「WannaCry」是否已出現變種，專家的意見不一。香港電腦保安公司Network Box創辦人之一加澤利稱，團隊發現利用網站傳播的新變種，只要點擊被植入惡意程式的網站超連結，電腦就會立即被感染。不過，亦有專家指大部分新變種個案都並不屬實。加澤利透露，亞洲多間大企業其實也遭到「WannaCry」攻擊，但都不願意公開承認，又形容區內電郵系統內仍有大量「地雷」。 ■法新社/路透社/美聯社/CNBC

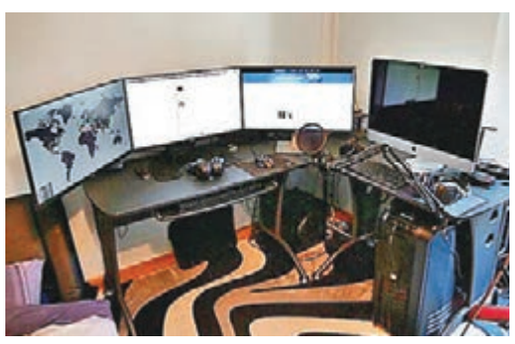
「意外英雄」曝光 憂黑客報復


■哈欽斯

英國一名22歲電腦安全專家在誤打誤撞下，成功阻止「WannaCry」蔓延，英國傳媒報道，他原來是網絡保安公司Kryptos Logic工程師哈欽斯，他自稱不愛上課，因此常常走堂學習電腦知識，還喜歡滑浪。自身份曝光後，企業都爭着邀請哈欽斯跳槽，但他表示無意轉工，據報老闆更出錢請他到洛杉磯旅行，獎勵他擊退「WannaCry」。

《每日郵報》報道，哈欽斯擔心黑客得知他的名字後更易向他報復，他與父母及弟弟一起居住，害怕黑客查出他的地址，「他們什麼也做得出」。哈欽斯指出，曾有一名網絡安全網誌作家在身份曝光後，有人將海洛英寄上門嫁禍，甚至收到死亡恐嚇，哈欽斯擔心會步這名專家的後塵。

自「WannaCry」爆發後，哈欽斯連續3日與病毒搏鬥，其間只睡了5小時，他聲稱自己只離開房間一次，未有機會與家人談話，不清楚他們是否知道自己所做的事。哈欽斯擔心，「WannaCry」或會暗地設下「後門」，可能會引爆新一輪混亂。 ■《每日郵報》


■哈欽斯房間設有多部電腦。 網上圖片

微軟:美洩系統漏洞 破壞力如「戰斧」失竊

黑客利用視窗作業系統漏洞，發動勒索軟件攻擊用家，視窗生產商微軟的主席史密斯前日批評，各國政府非但不向微軟通報系統漏洞，反而暗中收集和儲存有關資料，導致黑客有機可乘，「WannaCry」正敲響警鐘。他形容美國當局儲存的電腦系統漏洞外洩，破壞力好比美軍的「戰斧」巡航導彈被盜。

專家普遍認為，「WannaCry」惡意程式利用了美國國家安全局(NSA)研發的黑客工具，史密斯在網誌稱，現今社會面對兩種主要網絡安全威脅，分別是獲國家支援的行動以及有組織犯罪，「WannaCry」是兩者融合的結果，這種情況出乎各界預料，令人擔心。

史密斯指出，政府收集電腦系統漏洞的問題早已有跡可尋，例如洩密網站「維基解密」曾經公佈美國中情局掌握的系統漏洞。如今NSA收集的漏洞外洩，結果導致全球微軟客戶受到影響。

推動數碼公約 促用戶更新

史密斯認為即使在網絡世界，政府也應該遵守現實的規例，換言之應以監管武器的方式對付電腦系統漏洞。他表示微軟打算推動締結《數碼日內瓦公約》，要求政府向軟件供應商匯報漏洞。史密斯還批評部分機構未有更新系統，助長了病毒擴散，並指出黑客攻擊日趨複雜，如果用戶不更新系統，就無法保護自己。 ■法新社