■英國國家醫療服務系統是網攻重災區。 法新社

「意外英雄」揭鎖死鍵阻擴散「WannaCry 2.0」堵漏洞

病毒變種升級 今恐爆第二波

勒索軟件「WannaCry」肆虐全球，英國一位年僅22歲的網絡安全專家發現「kill switch」(鎖死鍵)功能，防止病毒繼續擴散，成為輿論關注焦點。他受訪時警告，黑客將試圖破壞相關功能，感染更多電腦，更指新一輪攻勢可能最快在今日展開。報道指，病毒已出現變種「WannaCry 2.0」，傳播速度更快。

■印尼網絡保安部門召開記者會，講解今次黑客襲擊。 路透社

這位「意外英雄」來自英國西南部，任職網絡安全公司Kryptos Logic，但未有透露名字，僅以其微博twitter賬戶名「MalwareTech」自稱。他11歲時迷上電腦科技，自學成才，放棄攻讀大學，改而在科技網誌撰文和編寫軟件。他表示，上周五看到英國國家醫療服務系統(NHS)等多家機構受網絡攻擊的報道後，開始研究勒索軟件的樣本，發現每次惡意病毒感染電腦後，會試圖聯繫一個特定網址，但這域名並沒註冊。於是他試試花費10.69美元(約83港元)註冊，來看哪些電腦會聯繫他，讓他掌握病毒擴散的程度，並無意中找到病毒中隱藏的kill switch開關，停止病毒傳播。

繳贖金恐洩銀行資料

與此同時，美國網絡安全公司Proofpoint的28歲研究員赫斯亦着手研究，同樣發現了勒索軟件內的kill switch功能，他和MalwareTech其後分享雙方發現，聯手制止病毒擴散。赫斯形容，全球網絡安全專家發揮團隊合作精神，應該同被視作英雄。不過赫斯警告，黑客可能會推出沒有kill switch的新版本軟件，可能在這一兩天或本周內再發動類似網絡攻擊。

MalwareTech正和同事蒐集受入侵的IP位址名單，交給執法部門，通知電腦遭感染但仍未知情的用家，他指黑客正嘗試升級勒索軟件，堵塞kill switch漏洞。勒索病毒導致受害人檔案被鎖，但美國國土安全部表示，向黑客繳付贖金不代表他們會解鎖檔案，只會令黑客取得銀行資料等私隱。

註冊域名無阻傳播

內地傳媒也引述國家網絡與信息安全信息通報中心緊急通報，已變種的「WannaCry 2.0」已出現， 與之前版本不同，變種版取消了kill switch，無法通過註冊域名來阻止其傳播，而且傳播速度可能更快，促請網民盡快升級微軟視窗系統，已感染病毒的電腦應立即斷網，避免進一步傳播。黑客研究網站The Hacker News引述網絡安全企業卡巴斯基分析師報道，他們的團隊發現一些沒有kill switch的病毒版本，除非全部高危電腦已更新系統，否則新一波攻勢會更難阻止。

■《衛報》/美聯社/英國《太陽報》/法新社/《每日郵報》

港企開機前須先斷網備份更新

香港文匯報訊(記者 文森) 香港已收到兩宗受「WannaCry」攻擊的個案。今日是事件爆發後首個上班上學日，香港電腦保安事故協調中心表明將潛藏爆發危機，呼籲中小企和市民如不知電腦是否已更新至最新版本，開機前應先關掉網絡。

生產力促進局資訊科技及業務流程總經理黃家偉透露，協調中心前日和昨日各收到一宗市民遭黑客勒索的報告，兩事主均是個人用戶，使用Windows 7視窗系統。他形容，兩個案均屬高危情況，沒設置防火牆，亦未有更新系統至最新版本。

香港資訊科技商會資訊保安召集人范健文、互聯網協會網絡保安及私隱小組召集人楊和生指出，市民可利用4個步驟預防，包括確定無線路由器及防火牆已設定攔截來自任何互聯網連至Port 139及145的互聯網流量；在開電腦前，拔掉上網線或關掉無線路由器。此外，把重要檔案備份至外置儲存裝置，完成後把裝置離線；使用視窗已更新至最新版本的電腦。完成以上步驟後，才把電腦重新接上互聯網。

資訊科技界立法會議員莫乃光指出，是次勒索軟件具有「蠕蟲」病毒特點，會主動尋找網絡內未有更新系統至最新版本的電腦，呼籲市民不要掉以輕心，即使現時不中招，亦不代表能避過下一波攻擊。他更擔心中小企和個人用家被攻擊，特別是部分中小企使用微軟舊系統多年未更新，亦無內部資訊科技部門或員工處理網絡保安。

全球20萬部電腦中招

歐洲刑警組織(Europol)表示，截至昨日全球共有20萬部電腦遭「WannaCry」勒索軟件攻擊，影響逾150個國家或地區共10萬個機構。各地企業電腦技術人員昨日加緊更新保安軟件，以免員工今日上班一開機就遭感染。

羅兵咸永道會計師事務所網絡安全專家伊韋日奇表示，勒索軟件感染部分客戶的電腦，須臨時停用電腦以進行緊急修復。印尼雅加達一間醫院證實有400部電腦遭入侵，干擾病人登記程序，亦難以找到病人病歷。新加坡數碼簽名服務公司MediaOnline一名技術員操作失誤，導致兩間商場的12部電腦遭感染，幸好這些電腦沒與商場或其他客戶的系統連接。

歐洲刑警負責人溫賴表示，這次攻擊獨特之處，在於勒索軟件擁有蠕蟲病毒特質，可透過一部電腦自動傳播至整個網絡，規模前所未見。他稱當局正與美國聯邦調查局(FBI)合作找出幕後黑手，估計不止一人犯案。在上周的攻擊當中，亞洲地區受影響的電腦相對較少，但新加坡網絡安全專家卡拉姆表示，要準備今日上班後可能會出現更多感染個案，包括網絡釣魚電郵攻擊。

分析指，「WannaCry」肆虐全球是因為一系列條件所造成，包括微軟視窗系統很多用戶未及時安裝3月推出的更新，加上病毒能在大學、企業或政府網絡快速傳播，形成一場「完美風暴」。 ■路透社/法新社/美聯社

鐵路核電站或成目標

「WannaCry」上周感染了全球多個國家和地區的公私營機構電腦，包括醫院、工廠和政府部門等等。專家警告，這只算是「小兒科」，下一波攻擊可能針對核電站、鐵路和水壩等重要基建，後果不堪設想。

美國亞利桑那州的電腦專家艾森表示，病毒一直潛伏在互聯網，伺機施襲，「今日有1萬部電腦遭感染，明天可能就多達1億部」，若黑客攻擊水壩、橋樑、鐵路和核電站系統，將導致電網和交通癱瘓。

部分電腦專家認為，這次攻擊可能是俄羅斯或烏克蘭黑客所為。網絡安全公司SentinelOne保安策略主管格羅斯曼指，3/4勒索軟件攻擊均由俄烏黑客策劃，但他不忘指出，若非美國國家安全局(NSA)入侵軟件外洩，今次事件根本不會發生。

■有傳下一波攻擊針對核電站、鐵路和水壩等重要基建，後果不堪設想。 法新社

黑客僅獲20萬贖金

黑客向受害電腦用戶勒索比特幣，專家估計相關款項可多達7.7億英鎊(約77.2億港元)，但據報截至前晚，黑客只收到2萬英鎊(約20.1萬港元)贖金。 ■哥倫比亞廣播公司/《星期日郵報》

英醫療大亂 醫生警告恐奪命

英國國家醫療服務系統(NHS)是網攻重災區，英格蘭48個醫療機構的電腦系統受感染，在蘇格蘭則有13個，包括全英最大的巴茲保健和國民信托。很多手術和預約需要臨時取消，病人要轉送至其他未受影響的醫院，有醫生警告，病人的生命會因而受到威脅。英國內政大臣盧綺婷前日表示，相關問題大部分已解決，但認為當局應加強防範。

■《星期日電訊報》

■受影響病人吐苦水。 網上圖片

■內地大學電腦室有多部電腦中招。 網上圖片

內地1.8萬個IP受感染

「WannaCry」令中國教育、銀行、交通等多個行業也遭受不同程度影響。國家網際網路應急中心專家建議，廣大用戶要及時更新視窗系統已發佈的安全更新，定期在不同的存儲裝置上備份數據。

截至昨日10時30分，國家網際網路應急中心已監測到約242.3萬個IP地址遭受攻擊；被該勒索軟件感染的IP地址數量近3.5萬個，其中中國境內IP約1.8萬個。國家網際網路應急中心博士、高級工程師高勝表示，該勒索軟件對於企業局域網或內網的主機系統破壞性尤其嚴重。「由於大量內網主機沒有及時更新或使用XP系統，因此一旦有一台主機被感染，將造成網內大規模擴散。」 ■新華社

YouTube教製勒索軟件 素人可變黑客

傳統黑客攻擊手法一般是透過入侵電腦，盜取受害人個人資料圖利，但這做法技術要求較高，相反使用勒索軟件的技術難度低得多，利潤亦更可觀，因此近年愈來愈多黑客改用勒索軟件。視頻網站YouTube上更有不少製作勒索軟件教學，部分影片甚至附有連結，讓不法之徒可輕易用16英鎊(約161港元)購買勒索軟件。

《星期日泰晤士報》發現多個提供勒索軟件教學片段的賬號，YouTube接報後已經停用其中一個頻道，並刪除多段教導製作勒索軟件的視頻。

贖金「市價」4個比特幣

勒索軟件使用方法簡單，加上比特幣等難以追查去向的加密虛擬貨幣，讓外行人也能輕易成為「網絡大盜」。網絡安全機構Crypsis Group的高級董事指，以前黑客起碼要有少許創造力及伎倆，「現在根本毋須擁有任何技術也能做到。」

現時勒索軟件受害者當中，約一半會就範支付贖金，Crypsis Group調查顯示，贖金「市價」由一個比特幣(約1,700美元，即約1.3萬港元)，至30個比特幣(約5.1萬美元，即約39.7萬港元)不等，中位數是4個比特幣，市值接近7,000美元(約5.5萬港元)。 ■《星期日泰晤士報》/《紐約時報》