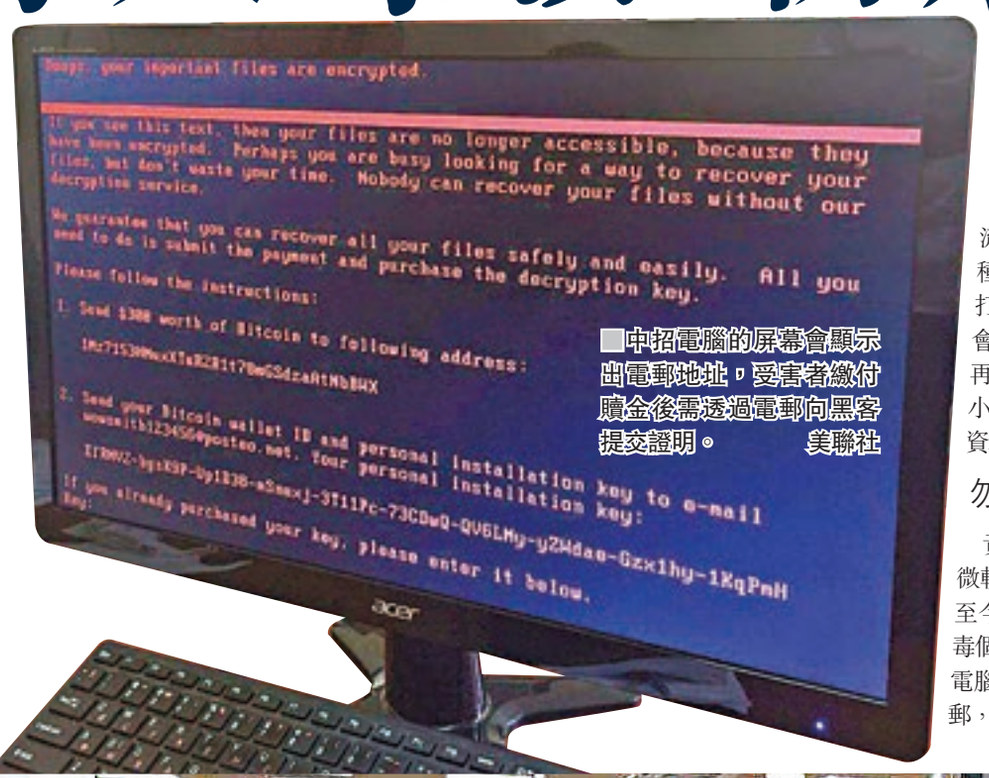
2000電腦網絡受襲 切諾核遺址中招

新病毒大爆發 勒索全球企業

當全球電腦用家對勒索軟件「WannaCry」仍猶有餘悸之際，新一輪網絡攻擊前日起再次席捲歐美及亞太地區，多國政府和企業均成為目標，朱古力大廠吉百利、航運巨頭馬士基集團紛紛中招，其中烏克蘭及俄羅斯災情最嚴重。黑客利用微軟Windows系統的漏洞入侵並控制系統，令電腦死機，用戶須向黑客以比特幣支付300美元(約2,340港元)贖金換取解鎖。防毒軟件商卡巴斯基將新病毒稱為「ExPetr」，專家指微軟早前為Windows推出了保安升級，相信有助堵截病毒入侵。



■中招電腦的屏幕會顯示出電郵地址，受害者繳付贖金後需透過電郵向黑客提交證明。 美聯社

港1宗查詢 中招電腦資料難復原

香港生產力促進局資訊科技及業務流程部總經理黃家偉表示，今次的變種病毒會以電郵寄出釣魚郵件，用戶打開後有機會中毒，無更新軟體的電腦會立即受攻擊，並嘗試透過中毒電腦，再將病毒散播。由於今次會在中毒後一小時才知道，其間病毒或已散播，電腦資料可復原的機會甚微。

勿開不明來歷電郵 直接刪除

黃家偉指，今次發現的病毒主要針對微軟視窗系統，電腦保安事故協調中心至今收到一宗查詢，香港及亞洲未有中毒個案，建議市民、公司及機構定期更新電腦軟件，切勿打開一些不明來歷的電郵，並直接刪除。電腦要安裝防毒軟件及作離線備份，暫時難以評估香港面對的風險。

香港電腦保安事故協調中心發出指引，表示一種新的變種加密勒索軟件正快速散播，中心提供的解決方案包括安裝最新的保安更新程式、確保已設置防火牆或寬頻路由器，且沒有開放SMB服務。

助理政府資訊科技總監(網絡安全及標準)潘士強表示，政府內部有多重措施保護電腦系統，市民的電腦如受病毒侵襲，可報警及向電腦保安事故協調中心求助。創新及科技局局長楊偉雄稱，經過上次WannaCry的經驗，政府已更新視窗系統，作出防禦漏洞的保護，他又指電腦保安事故協調中心已發出指引，讓市民、機構可以小心應付。

■綜合報道


■切爾諾貝爾核事故遺址的輻射監控系統受影響，需改為人手操作。資料圖片


■烏克蘭超市電腦受襲，顧客大排長龍。 路透社

攻擊力勝WannaCry 建檔「perfc」當疫苗

「ExPetr」除了利用美國國家安全局(NSA)發現的Windows漏洞「Eternal Blue」，還有多種入侵系統的方式，攻擊手段比「WannaCry」多。分析認為，「ExPetr」設計更為成熟，但主要針對企業，因此未有太多一般用家電腦受到影響。

報道指，新病毒利用烏克蘭程式MeDoc的軟件升級功能散播，另外，附帶惡意巨集程式的微軟Word文件也可能是傳播途徑。專家還發現，「ExPetr」使用了NSA的「Eternal Romance」工具遙距控制目標電腦。病毒一旦進入目標系統，就會搶奪管理權限，迫使電腦在最少一小時後重新啟動，屆時病毒就會加密檔案。與一般勒索軟件不一樣，「ExPetr」主要目標是企業常用的檔案，而非影像及視訊檔。

已更新電腦亦受波及

此外，病毒能夠感染同一個區域網絡內所有電腦，因此即使部分電腦早前已經安裝更新，只要同一網絡內其他電腦中招，已經更新過的電腦也可能受波及。

中招電腦的屏幕會顯示出電郵地址，受害者繳付贖金後需透過電郵向黑客提交證明，黑客收到後就會提供能解密檔案的密碼。不過，電郵註冊網站已關閉黑客的戶口，意味他們不能以此核實付款，因此專家呼籲受害者切勿繳付贖金。

為免遭到「ExPetr」毒手，專家提出自救方法。病毒啟動加密程序前，會先在系統內搜尋一個檔案，假如它已經存在，病毒就會退出加密程序。因此，只要用戶在「C:\Windows」文件夾建立一個唯讀檔，並把它命名為「perfc」，其作用將如同疫苗，能阻止「ExPetr」運作。此外，「ExPetr」在加密軟件的同時，會展示虛假的「CHKDSK」程式執行畫面，讓用戶誤以為系統正在檢查硬碟，只要用戶此時拔除電腦電源，就能中止加密程序。

■英國廣播公司/WIRED網站


■基輔國際機場工作人員檢視受襲情況。 路透社

人手操作貨櫃裝卸 馬士基無法接訂單

總部設於丹麥的航運商馬士基是網攻最大受害者之一，它們的貨櫃碼頭營運商APM Terminals遭攻擊，荷蘭鹿特丹碼頭的工人被迫改以人手操作裝卸系統。馬士基商務總裁克萊克昨日指，公司暫不能接受新訂單。至於系統被入侵前不久接收的訂單，處理上亦出現問題。克萊克續指，暫時未知公司業務何時才能恢復正常。

以手機聯絡工人

鹿特丹貨櫃港在歐洲規模最大，每年處理超過4.61億噸貨物，APM Terminals管理當中兩座碼頭，發言人博伊德稱，公司的電話及互聯網線路故障，需以手機聯絡工人，但他強調碼頭不會暫停運作，昨日會繼續處理4,500個貨櫃。博伊德指出APM Terminals在全球管理76座碼頭，只有部分受網攻影響，但全部都會投入運作。

印度政府最大貨櫃港、位於孟買的尼赫魯港，其中一個由馬士基旗下公司管理的碼頭受影響。為免貨櫃堆積，有關方面正清出額外空間。 ■路透社/法新社

中招機構

航運巨頭馬士基

食品公司億滋國際

物流公司TNT快遞

挪威國家安全部門

法巴銀行房地產分支

法國建材公司聖戈班集團

俄羅斯銀行業

俄羅斯國家石油公司

俄羅斯鋼材生產商耶弗拉茲

烏克蘭電網及銀行業

烏克蘭基輔鮑里斯波爾國際機場

德國郵政

德國護膚品牌Beiersdorf印度分支

德國零售商麥德龍的烏克蘭分店

美國默克藥廠

美國糖果商Mars

英國家品公司利潔時印度分支

全球最大廣告商、英國廣告集團WPP

路透社

最先傳出災情的是烏克蘭，當地政府網絡系統、基輔國際機場、地鐵系統及多間銀行前日中午起受到襲擊，連切爾諾貝爾核事故遺址的輻射監控系統亦受到影響，需改為人手操作。烏克蘭政府最初把責任歸咎俄羅斯黑客，但未幾俄國企業亦傳出遭受攻擊，當中俄羅斯國營石油公司要改用後備系統。

吉百利廠系統癱瘓全面停產

「ExPetr」其後散播至全球各地，專家估計截至昨日，全球約有2,000個電腦網絡受到攻擊。吉百利成為澳洲首間中招的企業，其塔斯馬尼亞朱古力工廠的電腦系統前日癱瘓，全面停止生產，昨早仍未恢復。吉百利母公司億滋國際漏夜發聲明稱，多個地區的員工都匯報指系統出現技術性問題，暫時未知原因。

跨國律師行歐華律師事務所的澳洲分部僱員向當地傳媒稱，他們的電腦系統被鎖上，無法使用。澳洲航空的預訂系統前日一度失靈，但據報與勒索軟件無關。

襲美醫療系統 多間醫院取消手術

黑客還入侵了美國賓夕法尼亞州Heritage Valley醫療系統，當地多間醫院要取消原定的手術。

根據比特幣數據網blockchain.info，超過30名受害人已經向黑客支付贖金。分析指，「ExPetr」傳播的條件之一，相信是必須與目標系統有直接網絡連接，病毒的擴散速度昨日放緩，原因可能是烏克蘭與外國的網絡連結有限。

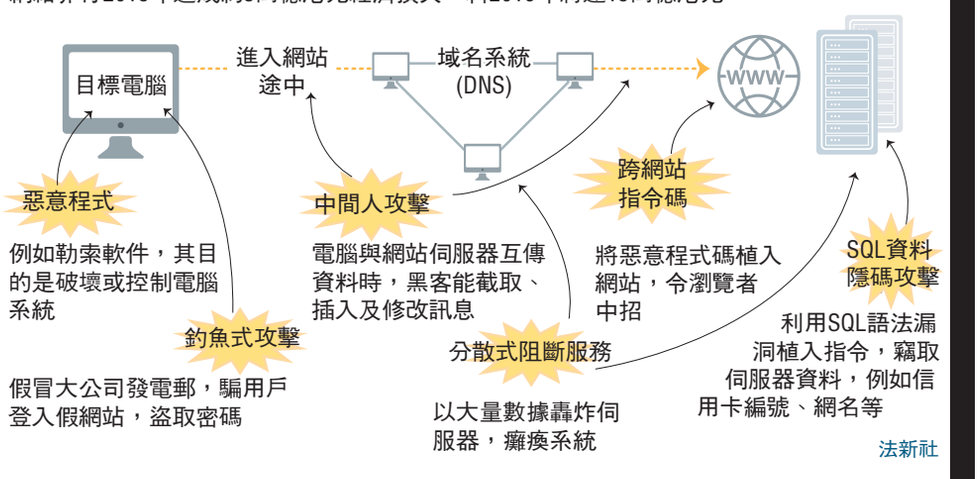
「ExPetr」含有美國國家安全局(NSA)開發的程式碼「Eternal Blue」，與上月肆虐全球的「WannaCry」一樣。微軟發言人稱，新病毒有多種傳染途徑，他們不久前為Windows XP至Windows 10系統推出安全升級「MS17-010」，有助堵截其中一種。另外，用戶收到不明來歷檔案或超連結時應提高警惕，勿隨便打開。

■美聯社/法新社/路透社/《紐約時報》


■烏克蘭銀行櫃員機中招，職員一臉無奈。 路透社

網攻手法層出不窮

網絡罪行2015年造成約3萬億港元經濟損失，料2019年將達15萬億港元



法新社

卡巴斯基：非舊病毒變種

外界起初以為，黑客使用的是去年首次出現的勒索軟件「Petya」，但專家後來發現「Petya」的加密能力更強。網絡安全公司卡巴斯基認為，新病毒並非「Petya」的變種，而是前所未見的勒索軟件，又指出他們的字串(string)接近，但功能不同。

科技界仍未統一新病毒的名稱，除了「ExPetr」，部分人仍稱之為「Petya」，也有人使用「NotPetya」和「GoldenEye」。香港電腦保安事故協調中心昨日亦指病毒名稱為Petwrap，或Petya、NotPetya、Nyetya等。

■綜合報道