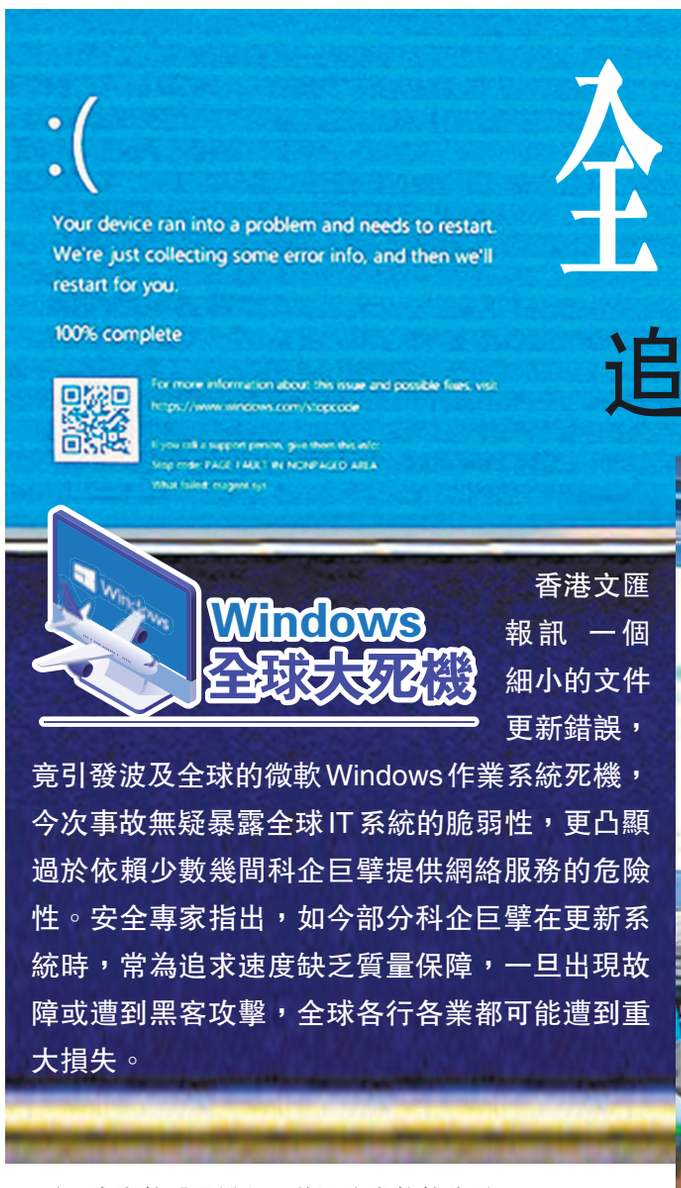


全球網絡依賴少數科企巨擘肇禍

追求速度忽視質量 暴露系統脆弱不堪一擊

香港文匯報訊 今次事件「元兇」、美國防毒軟件公司CrowdStrike，在全球擁有約2.9萬個客戶，包括近300名福布斯財富榜500強的大型企業。研究公司Gartner數據顯示，按照收入計算，CrowdStrike去年已佔全球安全軟件市場約15%份額，僅次於微軟的40%。Windows更是全球數以億計電腦使用的作業系統，長期支援航企、數碼支付和緊急服務等多個後端系統運作。

專家：網絡互聯牽一髮動全身

CrowdStrike官方聲明承認，今次事故源自一個名為「C-00000291*.sys」的問題文件，隱藏在安全產品更新中，該文件運行時引發Windows系統報錯，觸發「藍屏死機」。倫敦大學學院電腦科學教授瓦賽克指出，如今各間企業已習慣使用科企巨擘的雲端伺服器，而非自家系統滿足運算需求，「科技網絡變得龐大、複雜且相互關聯，這才牽一髮而動全身。」

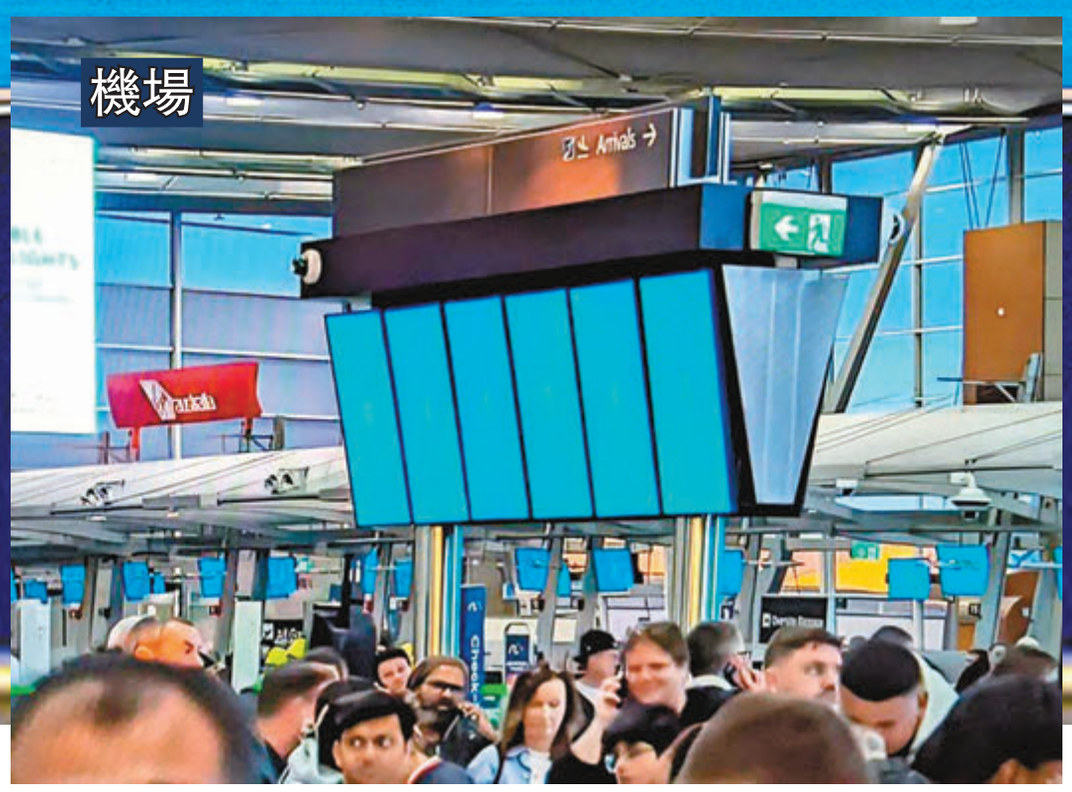
智庫「戰略與國際研究中心」顧問格斯特爾分析稱，現時許多網絡設備供應商，都使用名為「持續整合及持續交付自動化」（CI/CD）的開發流程，相當於階段性的應用程式更新，全數由工具測試並自動部署到伺服器中。但更新過程中一旦出錯且未被發現，錯誤代碼便會透過雲端系統，傳送給大量客戶。

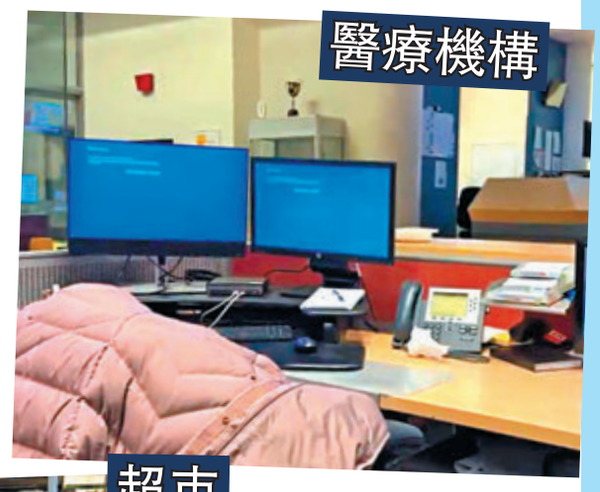
靠第三方更新系統成漏洞

格斯特爾指出，許多用戶依賴科企巨擘的產品，往往會遵照提示允許自動更新，但用戶根本沒有足夠資源和時間，檢查每個系統更新後的內容，「各國都依賴少數技術供應者，爭分奪秒測試作業系統和軟件更新情況，我們創建了一個有漏洞的系統，那就是依靠第三方提供用戶自己不知情的系統更新。」

英國安全服務公司Quorum Cyber創辦人查羅斯基指出，「IT行業部分供應商更新系統時，根本沒有分析細微的改變有何影響。他們為追求速度而走捷徑，缺乏足夠的測試。我們無條件地信任一些運行作業系統所必不可少的技術，這種做法是錯誤的。」

非牟利組織網絡威脅聯盟負責人丹尼爾稱，今次事件或促成監管機構加強審查科企，「對於完全依賴微軟作業系統的企業，它們要思考如何平衡統一使用作業系統的好處和風險。至於CrowdStrike，它或不得不同意外部監管人員介入、調查今次事件的始末。」





等……

「藍屏之亂」揭美炒作「中俄黑客論」荒謬

匯眼天下

郭燁

一場源於美國內部的「藍屏之亂」，讓全球無數企業運作癱瘓、航空交通大亂，再次讓人類意識到高度電腦化社會原來有多麼脆弱。不過諷刺的是，美國近年在預設會引起嚴重資訊安全事故的「假想敵」時，矛頭都只會指向所謂的「中國和俄羅斯黑客」，卻完全忽略了最大的「敵人」原來竟最可能會出在自己家門內，今次事件正正凸顯了美國那種凡事皆抱有被害妄想、無事不抹黑中俄的操作是有多麼的不切實際和荒謬。

不少讀者應該還記得，今年初美國政客和媒體就曾經炒作過一場中國起重機的「安全威脅」，聲稱在美國港口大量使用的中國製貨櫃起重機，被植入所謂的秘密通訊設備，可能會讓中國監視和收集美國進出口材料的情報云云，美國總統拜登更為此下令斥資200億美元（約1,562億港元），要將所有中國製起重機更換成美國製的起重機。

又例如去年7月，美國官員亦曾經聲稱，中國黑客可能已經將惡意代碼植入到美國各地控制電網、通訊系統和供水系統網絡中，「讓中國可以切斷美國軍事基地的水電和通訊，從而中斷或延緩美國的軍事部署或再補給行動」。

近年在美國，類似的中國或俄羅斯的資訊安全威脅論可說是多不勝數，美國官員和媒體三不五時就想着俄羅斯黑客什麼時候會「襲擊」美國的醫療設施，或是設想着如何「應對」中國黑客對美國軍事設施的「威脅」。以至於美國政府內的所謂「網絡戰士」在這次「藍屏之亂」發生後，第一個反應就是去研究事件是不是中俄黑客所為。

更離譜的是，《紐約時報》在事件後發表的一篇分析文章，竟然硬是要將今次完全由美國科技企業人為錯誤所導致的「藍屏之亂」，拉扯到中俄威脅論之上，文章宣稱是要探討今次事件對維持「數碼韌性」（Digital Resilience，意指快速適應任何已知或未知的資訊安全事件引致的環境變化，並從中恢復的能力）的意義，但當中卻沒有討論到應該如何防止這類人為錯誤的重演，或是事故發生後應對方法等眞知灼見，反而以大篇幅不斷重複講述一些所謂中俄黑客入侵美國電腦系統的「案例」，或者美國政府如何「致力防範」中俄黑客的舉措。

文章最後更聲稱，今次事件能夠讓不法之徒知道要從何處下手去讓美國企業和機場癱瘓，甚至更點名指事件可讓中俄領導人「找到如何在美國選舉年引發混亂及干預選舉的詳細路線圖」。

如果美國政府能夠將花在抹黑中俄的精力，放在更認眞看待自家企業引發資訊安全事故的風險，制定好相關預防和處理機制，今次「藍屏之亂」說不定就不會發生，即使發生了損害也可大大減輕。不過正正就是這種凡事皆抱有被害妄想、無事不抹黑中俄的思維，讓美國上下都只顧向外尋找從不存在的「假想敵」，看不到最大資訊安全風險原來一直潛伏在自己家門內。

Windows佔電腦市場七成份額 「用家硬食科企貪婪壟斷後果」

香港文匯報訊 今次死機事件影響全球，凸顯微軟Windows作業系統在個人電腦市場近乎壟斷的地位。市場份額追蹤機構StatsCounter數據顯示，截至今年4月，在全球電腦桌面系統中，Windows佔比達73.5%。蘋果公司開發的OS X以14.7%位居第二。Linux雖然是多數IT開發人員首選作業系統，但普通用戶相對較難操作，佔比只有3.88%。

非牟利組織NextGen Comparison行政主任拉吉斯批評，微軟在作業系統領域採取「供應商鎖定」策略，意味用戶想要切換其他供應商時，成本相當昂貴，還會面臨業務運營中斷的風險，「幾十年來，微軟的做法阻礙了公共和私營部門實現IT能力多元化，如今全球許多人都被迫承擔科技巨擘貪婪的後果。」

彭博通訊社科技專欄作家歐爾森還指出，全球的雲端運算和網絡安全服務市場，主要由微軟的Azure、亞馬遜的AWS以及Google主導，「當只有3間企業主導這一市場，一個小問題就能衝擊全球。」歐爾森建議各地應制訂法案，要求關鍵行業的企業至少使用兩款獨立的作業系統負責核心業務，其中一款系統發生故障時，另一個系統可維持運作。

騙徒趁混亂扮「修復員」偷用戶資料

香港文匯報訊 微軟Windows系統「死機」事故期間，有黑客趁機偽裝稱微軟職員，或是涉事防毒軟件公司CrowdStrike的技術員工，聲稱可協助用戶修復電腦，趁機騙取用戶個人資料和銀行賬戶訊息。澳洲等地政府呼籲民眾，務必依照CrowdStrike的指引修復電腦系統。

澳洲網絡情報機構澳洲訊號局指出，當局發現網絡上出現惡意網站和非官方應用程式，聲稱可以幫助用戶恢復電腦系統。若用戶不慎點擊釣魚鏈接，黑客可能竊取用戶的個人資料。澳洲網絡安全事務部長奧尼爾也在社媒X提醒，當地民眾需提高警惕，仔細識別企圖詐騙的做法。

美國網絡安全與基礎設施安全局警告稱，黑客或詐騙者會試圖欺騙用戶可以修復電腦，趁機竊取用戶電腦中的資料，甚至凍結電腦系統。CrowdStrike行政主任庫爾茨稱，公司已公開事故的解決方案，以及更新後的防護措施，請大家保持警惕。

專家倡企業制訂無網絡應急方案

香港文匯報訊 全球許多企業面對死機事故措手不及，長時間影響業務進度。路透社引述專家分析，事件凸顯許多企業沒有作好IT系統故障的應急計劃。專家建議企業吸取教訓，同時重視IT團隊的故障修復與網絡安全保護能力，設法保證企業緊急運作。

快速復原備份數據

美國私立南方衛理公會大學網絡安全研究所主任桑頓表示，許多企業需要存儲並調用大量數據，依賴互聯網存取備份存在風險，「如果企業的數據存儲中心位於偏遠地區，最好為其安排一條受外部干擾較少的專用線路。數據應急復原不但要全面，更要快速，企業要有能力馬上恢復過去一周、一天，甚至一小時的備份資料。」

英國國家網絡安全中心前負責人馬丁認為，各間企業或組織可以檢查IT系統的網絡彈性，確認這些系統是否設有故障保護機制，「現時的問題是，我們有能力應對網絡攻擊等安全風險，但網絡出現故障時，我們的修復能力不足。」

《金融時報》創新科技編輯特倫希爾稱，極端情況下，各間企業必須作好完全無法使用網絡的應急方案，「他們要盡快恢復正常服務，這通常需要敬業且有變通能力的員工合作，許多航企員工馬上改用手寫登機牌便是例子。」

加醫療服務嚴重受阻 改用紙筆記日程

香港文匯報訊（特約記者 成小智 多倫多報道）微軟Windows作業系統上周五（7月19日）大崩潰，加拿大全國各地醫療體系的服務受到影響，由於電腦作業和網絡系統無法正常運作，各地醫療網絡透過社交媒體向病人通報暫停服務情況和最新信息。

取消非緊急手術

位於安大略省的全國最大醫院網絡UHN有部分系統受阻，多間醫院盡量維持臨床治療安排，但病人遇到延誤是無可避免。多間醫院發言人表示電子醫療記錄系統發生故障數小時，工作人員轉向採取應急程序，並繼續為病人提供適切治療。不過，非緊急手術需要取消，連帶一些例行健康檢查如抽血程序亦無法進行。

卑詩省醫院不得不改用筆和紙來管理記錄和日程安排，並制訂應急計劃確保醫療保健服務繼續運行。衛生廳長迪克斯表示，微軟「死機」影響該省約5萬台醫療電腦裝置，軟件故障改變工作人員日常工作模式，但必須確保原有醫療安排、實驗室工作和飲食訂單等服務盡量如期進行，並且密切監測防止出錯。

紐芬蘭省衛生廳表示，這次故障影響其用於管理患者護理和財務的主要資訊系統Meditech，但各醫療保健機構盡可能提供護理服務。加拿大成癮與心理健康中心（CAMH）的一些電腦系統受到影響，但仍能保持大多數診所照常營運，只有部分面對面和虛擬門診服務需要取消。