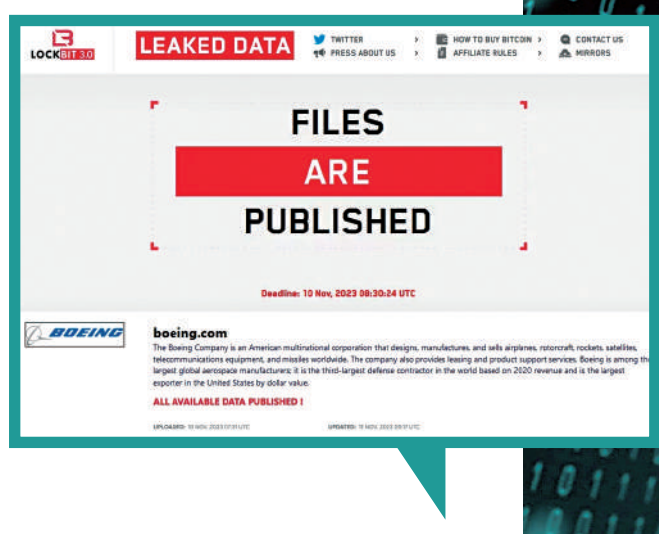
惡意加密數據勒索贖金 受害者遍布全球

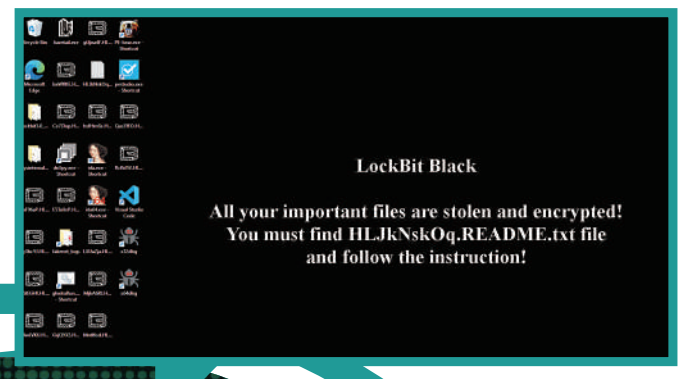
國際網絡犯罪集團Lockbit被摧毀

綜合路透社、彭博社及《衛報》報道：成員包括英國國家打擊犯罪調查局（NCA）和美國聯邦調查局（FBI）在內的國際執法機構聯盟20日宣布，已成功摧毀了全球最臭名昭著的黑客組織Lockbit，並關閉了該組織用於勒索軟件付款的網站。Lockbit通過惡意軟件加密受害人的數據來勒索贖金，在全球有逾2000受害公司或機構，包括波音公司、英國皇家郵政等都曾遭其毒手。

▼Lockbit去年11月索要贖金不成，將波音公司的敏感資料公布。 網絡圖片



▲國際執法機構聯盟在Lockbit的暗網頁面宣示攻佔行動成功。 路透社



◀被Lockbit惡意軟件入侵的電腦，其文件均被加密。 網絡圖片

【大公報訊】Lockbit自2019年開始運營，被美國官員稱為「全球頭號勒索軟件威脅」。根據網絡安全公司Palo Alto Networks的數據，在去年全球近4000起勒索網絡攻擊中，涉及該組織的攻擊佔了23%。美國司法部指，Lockbit在全球範圍內有超過2000個受害者，通過勒索已經獲得逾1.2億美元贖金。

執法人員攻佔黑客網站

在國際執法機構聯盟宣布摧毀該組織前，Lockbit網站已被國際執法人員「侵佔」，其首頁上赫然寫道：「該網站目前已由NCA、FBI和國際執法工作組控制」。一位FBI官員表示，來自英國、美國、法國、日本、瑞士等11個不同國家的執法部門近日聯手進行了「克羅諾斯行動」，查封了Lockbit及其附屬公司用於傳播勒索軟體的1.1萬個網域，並成功破壞了Lockbit的基礎設施及其惡意軟件部署系統。

NCA發言人和美國司法部發言人證實，執法部門已經瓦解了該黑客團夥，並表示行動「仍在進行中」。《衛報》指，兩名Lockbit相關成員分別在波蘭和烏克蘭被捕，另外兩名疑似附屬機構人員在美國落網並被起訴。美國當局還宣布制裁兩名與該組織有關的俄羅斯公民。

另外，執法人員凍結超過200個與該組織有關的加密貨幣賬戶，同時發現了超過1000個解密密鑰，相信有助於幫助Lockbit以往的受害機構找回被鎖定的數據。

收贖金但未刪除受害者檔案

Lockbit使用同名勒索惡意軟件，入侵受害組織的電腦系統，獲取並對其系統上的資料進行加密，然後要求目標支付贖金以解密資料。贖金通常以加密貨幣的形式索取，例如比特幣，這種形式的貨幣更難追蹤，並且接收者可以保持匿名。報道指，Lockbit雖然聲稱收到贖金後會刪除目標機構的數據，但NCA在近期行動中發現，Lockbit說謊，其系統中保留的部分檔案，屬於那些支付過贖金的苦主。

Lockbit的代表沒有回覆評論請求，但其在加密應用程序上稱，該組織的備份伺服器未受到執法行動的影響。

背景神秘 行事猖獗

近年，Lockbit在全球各地橫行霸道，其首要勒索目標是金融、製造業、醫療保健、能源等關鍵基礎設施提供商。去年6月，美國聯邦機構的公告稱，自2020年以來，美國約1700起勒索軟件攻擊均是Lockbit所為，受害者包括「市政府、縣政府、公立高等教育、K–12學校以及緊急服務部門」。該組織在美國總共索要了9100萬美元的贖金。中國工商銀行美國子公司工銀金融、波音公司等都曾在Lockbit的「受害者名單」上。

Lockbit的真實歸屬至今神秘莫測。一些安全分析師認為該團夥的總部位於俄羅斯，但該團夥從未公開表示其歸屬於某個民族國家，也未表示支持任何政府。Lockbit先前在暗網的網站上稱，它「位於荷蘭，完全不關心政治，只對金錢感興趣」。

美國網絡安全公司Analyst1的首席安全策略師迪馬吉奧表示，Lockbit是「勒索軟件組織中的沃爾瑪」，有着像企業一般的經營模式，「可以說是當今最大的勒索軟件團隊」。某種程度上，Lockbit的成功就取決於其「附屬機構」，即志同道合的犯罪團夥。

近年Lockbit 主要攻擊事件

2023年

11月：
- Lockbit攻擊中國工商銀行美國子公司工銀金融，導致部分系統中斷，大量交易無法進行清算。工銀金融被迫支付贖金，以換取解鎖。

10月：
- Lockbit聲稱竊取波音公司的敏感資料，由於沒有收到贖金，Lockbit於11月在網上公布波音超過43G的檔案。

7月：
- Lockbit攻擊日本名古屋港，造成運貨工作停擺2日，日本全國10%的貿易都經由該港。

6月：
- Lockbit聲稱入侵台積電的供應商擎昊科技，並勒索7000萬美元的贖金。

1月：
- 英國皇家郵政的國際出口服務遭Lockbit勒索軟件攻擊，發生嚴重中斷。

2022年

12月：
- Lockbit攻擊了美國加州金融管理局，聲稱竊取了75.3GB的文件；該組織還聲稱攻擊了葡萄牙最大的里斯本港，要求150萬美元的贖金。

8月：
- 全球五大汽車零部件供應商之一德國大陸集團遭Lockbit攻擊，由於未回應贖金要求，該組織於11月公布了部分被盜數據。

大公報整理

黑客勒索猖獗 數碼港也是苦主

【大公報訊】近年來，全球網絡犯罪頻發，黑客活動愈發猖獗。去年，本港的數碼港以及消費者委員會於8月、9月先後遭受黑客入侵，分別被勒索30萬（約235萬港元）及50萬美元（約391萬港元）的贖金。

去年8月，黑客入侵香港數碼港，盜取逾400GB的機密資料，涉及現職、離任僱員，以及應徵者的個人資料，並勒索30萬美元的贖金。在贖金要求被拒絕後，被盜資料於次月遭「撕票」，被上傳暗網。洩漏的資料包括數碼港的季刊、財政預算、租賃協議、單據、核數文件等，以及包括數碼港公司的董事局會議資料、合作公司資料和招標及合約文件和多個政府部門的文件。

繼數碼港資料外洩後，消費者委員會的電腦系統緊接着於去年9月遭黑客入侵，八成系統遭到破壞，包括8000名《選擇》月刊訂戶在內的四類人士的資料恐將外洩。消委會被勒索交付50萬美元贖金。

消委會主席陳錦榮表示，在數碼港遭入侵後，儘管消委會亦檢查網絡系統安全，提高警惕，但仍被黑客侵入。電腦保安專家鄭利明稱，此次事件側面反映出相關機構低估了黑客的耐性及科技手段，凸顯職員的網絡安全意識不足。

26億彩票獎金成夢幻 美國男子怒告威力球

【大公報訊】據NBC報道：美國華盛頓一名男子去年1月在威力球彩票網站上發現，自己購買的號碼中了頭獎，獎金是3.4億美元（約26.6億港元）。然而當他前去兌獎時卻被告知，網站當時發生錯誤，公布的號碼為測試用，並非中獎號碼。男子憤而決定提告。

奇克斯於2023年1月6日購買了一張威力球彩票，但他並未觀看次日的開獎直播，而是於1月8日在彩票網站查詢，看到自己的號碼中了頭獎。當他前往零售商兌獎時，工作人員卻告知他的號碼與中獎號碼不匹配。他又去了華盛頓特區彩票和博彩辦公室（OLG），但再次遭到拒絕。

奇克斯隨後聯繫律師起訴了威力球，對象包括彩票承包商陶弟公司，包含違反契約、疏忽、精神損失、詐欺等，向威力球公司求償3.4億美元。

陶弟公司表示，本次的烏龍事件是因「技術失誤」造成。1月6日至9日期間，該公司的團隊正在測試網站，「意外」將一組用於測試的號碼一連掛在網站上3天，而這組號碼正巧跟奇克斯的號碼相同。

奇克斯的律師埃文斯表示，目前並未看到任何證據證明，承包商確實是因「錯誤」而將那組號碼放在網站上。他還引用了愛荷華州類似事件的先例，當時的承包商承認了錯誤，並支付了獎金。「這不只是網站上的號碼問題，而是關乎彩票機構的公信力。」

▲馬里蘭州一家便利店外的威力球標牌。 法新社

外國人遲交稅 或失日本永久居留權

【大公報訊】據日本時報報道：日本出入國在留管理廳正考慮修改《出入境管理和難民認定法》，外國人獲得日本永久居留資格後，如果故意逃稅或多次未按時繳納稅款，可能被取消或變更永久居留資格。

報道指，依照日本現行制度，獲得永久居留權的外國人沒有時間或行業限制。截至2023年6月，日本境內具有中長期居留資格的外國人數超過322萬人，其中超過88萬人擁有永久居留權，佔27%。目前針對擁有永久居留權的外國人，即使屢次不納稅或繳納社會保險金；或多次犯法而被判處1年以下有期徒刑，也不會失去永久居留權。

日本政府本月宣布，將推出新的「育成就勞制度」取代現行的「技能實習制度」，預期會有更多外國勞工獲得永久居留權。因此日本出入國在留管理廳考慮上述新措施，以控制獲得永久居留權的外國人數量，並預計向本屆國會提出相關法案。

根據新規定，在日本有永久居留資格的外國人，若反覆蓄意不繳納或延遲繳納稅金或社會保險金等，或是被處以1年以下有期徒刑的話，出入國在留管理廳將可以撤銷或更改其永久居留權。另外，日本政府也計劃設立通報制度，讓地方政府的職員等通報未履行繳稅等義務的外國人。

▲日本擬訂政策控制本國獲永居外國人的數量。圖為行人走過東京新宿區。 法新社