逾8000人資料恐外洩 勒索50萬美元

黑客攻陷消委會 各部門高度戒備

繼數碼港遭黑客入侵導致資料外洩後，消費者委員會的電腦系統也遭黑客以勒索軟件攻擊，事發於本周二（19日）傍晚，黑客入侵時間長達七小時，成為最近一個多月內第二宗網絡安全入侵事件，公營機構網絡安全人人自危。

消委會昨日表示，本周三發現被入侵時，八成系統已遭到破壞，包括8000名《選擇》月刊訂戶在內的四類人士資料恐將外洩，同時被勒索50萬美元。消委會前日已報警，並強調絕不會繳交贖金，但被盜取的資料內容可能要等被「撕票」才知。政府高度關注近期兩宗公營機構網絡安全事故，已經主動聯絡兩個機構並提供技術支援協助，其他部門續高度戒備。

大公報記者 王亞毛 賴振雄

▲消委會昨日舉行記者會交代電腦系統被黑客攻擊詳情。

消委會資料外洩 四類人士高風險

- 員工、前員工及其家屬、空缺申請人：例如身份證號碼、住址、出生日期和履歷
- 《選擇》月刊訂戶：當中包括約8000人曾向消委會提供信用卡資料
- 消費投訴人士：相關個人資料
- 消委會合作夥伴：例如公司地址、電話、電郵，部分或存有手機號碼

資料來源：消費者委員會

限今晚11時20分前付贖

消委會昨日舉行記者會交代事件表示，其職員於本周三（20日）早上發現無法登入電腦系統，調查發現，系統在前一天傍晚6時左右被攻擊。該勒索軟件概述已從消委會電腦系統盜取某些內部資料，包括員工及客戶數據，以及其他內部紀錄。消委會主席陳錦榮表示，黑客勒索要求消委會於今晚11時20分前，繳交50萬美元贖金，折合約390萬港元，若遲於該時間則須繳交70萬美元，折合547萬港元。

消委會在被入侵的7個多小時內，系統數據流量較正常多出65GB。就是否涉及個人資料外洩及其覆蓋範圍，仍在調查中，但從風險評估，四類人士包括消委會員工及家屬、8000名《選擇》月刊訂戶、投訴人士，以及消委會合作夥伴的資料恐遭洩露。據了解，八成系統已遭到破壞。

消委會將提醒受影響人士

消委會總幹事黃鳳嫺強調，絕對不會交付贖金。專家也已初步掌握事件來源，而所洩露資料的具體內容和範圍，可能要等被「撕票」才知，希望市民諒解。消委會未來數天會接觸可能受影響人士，提醒相關人士務必提高警覺，若收到可疑連結、電郵或訊息，切勿開啟或點擊，加強保障網絡安全。

陳錦榮表示，在日前數碼港遭黑客入侵事件發生後，消委會已即時檢視網絡系統安全，提高警惕，但仍不幸被黑客攻擊，形容黑客的手段一日千里，很難保證系統百分百安全。

香港資訊科技商會榮譽會長方保僑接受《大公報》記者查詢表示，系統在被入侵時間內多出的65GB數據流量，相信是黑客侵入電腦後，盜走資料時所用的流量，「其實現時電腦網速足夠快，一般同時間使用電腦的職員也未必能察覺到，問題在於消委會對其系統防火牆的設定，是否能監測到流量使用的異常狀況。」

據報道，有私人企業被黑客入侵後，遭勒索數十萬元，經討價還價後，交付十多萬元，原以為事件完結，取回資料後，發現部分資料不翼而飛。有資訊科技專家稱，絕對不能交付贖金，黑客發現受害人會付款，就會在暗網交換資料，曾經有公司交贖金後，一個月內被勒索28次，勒索沒完沒了。

專家:付贖反惹黑客再來

方保僑亦稱，不應該向黑客支付贖金，因為黑客事件不時發生，公營機構被勒索後，幾乎一定會遭「撕票」，即使支付10次贖金，黑客都有可能仍持有資料的備份。

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，以及職員的網絡安全意識不足，「不太了解的人不會想這麼多，尤其是節假日前後更易發生類似事件，有些假扮節日慶賀或大抽獎的電郵，進入後才發現是釣魚網站。」

資訊科技總監黃志光強調，政府各部門現時在技術、制度及員工培訓方面都有多項措施保障網絡系統安全，資科辦和警方網罪科有進行演練。就近日接連發生兩宗網絡安全事故，資科辦有進行分析並通報政府部門。他稱政府系統的保安措施現時足夠，間中受到不同類型的攻擊或企圖入侵，但都被防禦系統阻截。

個人資料私隱專員鍾麗玲表示，截至昨日下午5時，共接獲1宗涉及消委會受黑客入侵引起的投訴和及8宗查詢，以及與數碼港事故有關的24宗投訴和52宗查詢。私隱公署非常關注事件，並會視乎情況決定是否啟動調查、發調查報告或發執行通知，要求更正缺失，目前未有進一步資料，難以判斷消委會是否有違規情況。

警方昨晚回覆《大公報》查詢表示，前日（21日）接獲相關機構職員報案，指懷疑電腦系統被入侵，案件列作「有犯罪或不誠實意圖而取用電腦」，交由網絡安全及科技罪案調查科跟進，暫未有人被捕。

懷疑個人資料被盜 自保貼士

- 重設及定期更改網上賬戶密碼，並啟用多重認證功能（如有）
- （如曾提供信用卡資料）通知信用卡公司該卡或已被盜用，及／或申領更換信用卡
- 定期審視銀行月結單及銀行發出通知，以確定是否有任何未經授權或可疑活動
- 留意個人電郵或賬戶有沒有不尋常的登入及收發信息紀錄
- 收到不明來歷或可疑的來電、短訊或電郵時要提高警覺，切勿隨意打開附件或披露個人資料
- 如收到聲稱代表消委會的來電、短訊或電郵，應核實來源，如有疑問，可致電消委會官方熱線（2929 2222）查詢。此外，消委會並不會從以上途徑索取用戶的賬戶號碼、密碼及登入資料等信息，或提供連結要求閣下進行交易
- 對網絡釣魚及其他詐騙行為提高警覺

持有個人資料的機構 防黑客貼士

- 採取資料管治和機構性措施：機構應制定針對資料管治和資料保安的內部政策和程序，包括委任合適的領導人員負責資料保安，及提供足夠的培訓予工作人員
- 定期進行風險評估：在啟用新系統和新應用程式前，以及在啟用後定期進行資料保安風險評估
- 採取一系列的技術上及操作上的保安措施
- 妥善管理資料處理者：機構須採取合約規範方法或其他方法，以防止轉移予資料處理者的個人資料在未獲准許或意外的情況下被查閱、處理、刪除、喪失或使用
- 適時採取資料保安事故發生後的補救措施，從而減輕對機構及受影響人士可能造成的傷害
- 定期監察、評估及改善資料保安政策的遵從情況

資料來源：私隱專員公署

近三年網上勒索及盜用電腦案件

年份	網上勒索（宗）	盜用電腦案件（宗）
2021	158	142
2022	155	192
2023*	172	203

註：不包含裸聊勒索 *1月–7月

資料來源：警務處公共關係部

◀黑客入侵消委會電腦系統，包括八千名《選擇》月刊訂戶在內的四類人士資料恐將外洩。

科技專家：肆意妄為 歐美黑客居多

拆局 數碼港、消費者委員會先後被黑客入侵電腦系統，並遭黑客勒索，不少市民質疑，本港公私營機構網絡安全不足。有資訊科技專家指出，黑客以來自歐美的較為著名，相信今次事件是黑客以漁翁撒網方法行事。專家提出，不少公營機構只是依賴防毒軟件和防火牆，不足以防範黑客入侵。

倡引入「滲透測試」檢視系統偵察力

有網民質疑，事件會否涉及「國家級」黑客入侵，目的並非勒索金錢，旨在打擊香港的國際形象。資訊科技專家，香港智慧城市聯盟創辦人楊全盛向大公報分析，國際知名的黑客一般來自歐美或俄羅斯，屬於個體戶或小團隊，其手法往往是漁翁撒網，攻擊不同國家或地區的公私機構，也不排除有其他私人機構已經中招，只是沒有通報。

至於入侵的方法，香港資訊科技商會榮譽會長方保僑向《大公報》指出，一般是透過電郵或短訊，發放釣魚網站的超連結，所以保安篩查之餘，也要提高員工的日常保安意識，不要胡亂打開電郵中的連結，不常使用的檔案要上鎖等。

坊間已有不同方案，協助監測和攔截系統檔案遭大量刪除、增加檔案等活動。他建議，消委會提升網絡安全時，引入「滲透測試」，以扮演攻擊者的「紅隊」和防守者的「藍隊」，檢視系統是否可偵察攻擊。

政府數據不同層級加密保護

政府資訊科技總監黃志光表示，政府系統大部分都集中在政府的私有雲端平台上管理，並通過中央互聯網通信集接觸互聯網，數據保護亦有不同層級的加密，並有防火牆、偵測入侵和應變系統，24小時網絡監測系統流量和發出警報，能夠攔截電郵的惡意附件及連結。

大公報記者賴振雄

舉一反三 防黑客入侵

透視鏡

蔡樹文

消委會被攻破電腦系統，並勒索50萬美元贖金。這是繼數碼港電腦系統遭黑客入侵後，另一個半官方機構遭黑客入侵。

一連串網絡入侵事件，為香港網絡安全敲響警鐘。網絡安全是一個沒有硝煙的戰場，關係到國家安全及民生福祉。消委會8成電腦系統受到破壞，是嚴重事件。我們明白，在與黑客的鬥爭中，往往出現「道高一尺，魔高一丈」的情況，躲在暗角的黑客，會不斷尋找網絡弱點進行攻擊。

黑客在消委會電腦系統「逗留」7小時期間，不斷進進出出，我們必須反思，消委會的電腦系統有沒有發出預警？若有預警，有沒有採取即時防禦措施？若電腦防止黑客入侵系統根本沒有預警，或者7小時後才被發現，說明問題更加嚴重。

舉一反三，特區政府不同部門的防黑客入侵系統及技術，是否與消委會及數碼港類似？若是，便必須採取措施，防止類似情況發生，絕不能掉以輕心。

投訴需上載交易文件 或涉信用卡資料

記者實測 在消費者委員會電腦系統被黑客襲擊事件中，《選擇》月刊訂戶、消費投訴人士的資料有可能被盜取。大公報記者昨日實測，模擬訂閱《選擇》月刊及向消委會投訴，提交投訴資料時，需要上載交易文件等，或涉及信用卡資料，訂閱時除了提供姓名和電郵，要透過第三方的「傳款易」（PayDollar）系統，輸入信用卡資料內容。

大公報記者模擬，向消委會投訴不良商戶，填報表格時，主要提供商戶及相關交易內容，牽涉個人資料的部分，包括交易文件、溝通紀錄、交易的相關相片及授權書，並要上載相關檔案作為證據，檔案內若有地址和電話等內容，一旦被黑客公開，後果可大可小。

香港資訊科技商會榮譽會長方保僑回應《大公報》查詢時指出，訂閱戶透過「傳款易」系統，輸入的信用卡資料，由於屬第三方的系統，黑客無法取得信用卡後的安全碼，但部分網上交易平台並不需要核對安全碼，所以基於風險，仍建議用戶停用有關信用卡。

倘證消委會招損失 可民事索償

立法會資訊科技及廣播事務委員會議員、執業大律師容海恩表示，投訴人或訂閱戶若出現金錢損失，可循民事索償，但必須提出舉證，證明損失來自今次事件。而消委會可以受害者身份，及已做足電腦保安措施作為抗辯理由。

大公報記者賴振雄