文匯報 WEN WEI PO www.wenweipo.com

政府指定刊登有關法律廣告之刊物 獲特許可在全國各地發行

2023年9月 23 星期六 癸卯年八月初九 是日秋分

短暫陽光 幾陣驟雨 氣溫28-33℃ 濕度65-90%

港字第26837 今日出紙2疊6張半 港售10元

消委會被黑客入侵時序表

周二（19日）

經過

- 黑客在傍晚開始入侵消委會電腦系統，持續7個多小時，安全系統懵然不知

周三（20日）

- 員工早上上班，無法登入系統才揭發事件
- 消委會即時加強系統的安全措施，防止黑客再次入侵
- 委託鑑證專家進行調查，了解事件及收集相關資料

周四（21日）

- 黑客留下勒索信，要求周六（23日）晚上11時20分前繳交50萬美元贖金，逾期加至70萬美元
- 消委會報警，並主動向個人資料私隱專員公署備案

周五（22日）

- 消委會召開記者會交代事件
- 會方未來數天會接觸可能受影響人士
- 會方堅拒繳交贖金

消委會機密被盜 投訴者訂戶高危

遭黑客入侵7小時 拒交贖金 提醒受影響者防範可疑訊息

黑客無孔不入，繼數碼港被黑客入侵勒索後，香港消費者委員會亦「失守」，其電腦系統日前遭黑客入侵洗劫逾7小時。其間，電腦保安系統儼如「瞓咗」一直沒有發現問題，直至翌日職員上班無法登入系統才揭發，向該會投訴者、《選擇》月刊8,000名訂戶等四類高危人士有資料外洩風險。黑客勒索今晚11時20分前交出50萬美元的贖金，否則加碼至70萬美元，甚至「撕票」。消委會昨日強調絕不繳交贖金，實際受影響人數可能「撕票」後才知曉，呼籲高危人士提高警覺防範可疑連結、電郵或訊息。有電腦專家認為，特區政府應盡快訂立網絡安全法，規定企業機構的存檔及網絡保安要求。

◆香港文匯報記者 張弦、劉明

◆消委會電腦系統遭黑客入侵7小時，被盜65GB資料，近80%系統受破壞。 香港文匯報記者涂穴 攝

香港消委會主席陳錦榮昨日交代被黑客入侵經過。事發於本周二（19日）有黑客入侵該會電腦系統，數據流量較正常多出65GB，但一直未被發現，翌日（20日）上午職員上班才發現電腦系統異常，證實遭黑客以勒索軟件惡意入侵，但為時已晚，近八成系統受到破壞，部分內部資料被盜。

他表示，消委會已即時加強系統安全措施，委託鑑證專家調查，經搶修系統，網上格價工具及熱線服務已回復正常，並於前日上午向警方報案，以及向私隱專員公署備案。

四類人受影響 待「撕票」後始能確認

陳錦榮透露，黑客要求消委會於今日（23日）晚上11時20分前繳交50萬美元（約390萬港元）贖金，若遲交則增至70萬美元（約547萬港元）。消委會強烈譴責黑客的非法活動，強調絕對不會交付贖金，並對事件引起市民不便，深表歉意。

由於不少電腦系統被鎖，消委會至今未能確認被盜的實際數量，估計四類人士較高危，包括員工、前員工和他們的家屬，以及空缺申請者；約8,000名曾向消委會提供信用卡資料的《選擇》月刊訂戶；消費投訴者，以及消委會合作夥伴。消委會總幹事黃鳳嫺補充，現階段仍未能掌握實際受影響人士的身份及數量，估計或要到「撕票」後才能準確知道，希望受影響者諒解，又提醒他們提高警覺，「相關人士對於近日收到的來電、連結、電郵要特別小心處理，以免造成進一步損失。」消委會將全力檢視系統的安全措施、事發因由，以及改善方案。

她強調，消委會多年來投放資源提升網絡保安系統，包括定期進行風險評估及審計，黃鳳嫺表示，該會購買及安裝市面上最佳作業模式的網絡保安方案，並會定期進行風險評估及審計，例如主要系統伺服器的漏洞掃描，資訊科技部門亦全年定期檢視系統問題，已排除是職員錯誤點擊釣魚連結引致中毒，「但大家都明白，現時的科技很厲害，黑客無孔不入，手法層出不窮，即使投放多少資源，亦難以完全防範黑客的不斷入侵及攻擊。」

截至昨日下午5時，個人資料私隱專員公署共接獲1宗涉及消委會資料外洩事件的投訴及8宗查詢。對消委會發現被黑客攻擊後一天才通報公署，私隱專員鍾麗玲表示，公署已展開循規審查，現階段未能判斷消委會在事件中有否違規，又透露公署正制訂修例建議，研究設立資料外洩的強制通報機制以及行政罰款。

專家促立法提升企業安全意識

特區政府資科辦雲端保安及私隱工作小組成員、訊息安全專家龐博文昨日接受香港文匯報訪問時坦言，黑客勒索團夥分布全球，分別在暗網串連組織及分工發動攻擊。事實上，所有網絡保安系統總有新漏洞，團夥發現後便會大規模掃描，尋找使用有關系統的目標進行入侵，「他們入侵電腦系統後，會下載數據並將系統內的數據加密，然後發電郵勒索被入侵的機構，畀贖金才會為加密的數據解鎖。」他認同消委會拒交贖金的做法，「不少例子是交贖金後，仍被黑客將備份資料放在暗網販售。」

特區政府正就網絡安全法進行研究，雖然不少黑客都是跨境犯案，未必受到香港法例規管，但龐博文認為，立法有助提升企業的網絡安全意識，以及釐清責任，能起一定阻嚇作用。他建議有關的法例應細分為不同範疇，包括數據分類法、跨境數據法等，規定企業必須將不同數據，按敏感度分類存放，而跨境數據法則規定一些敏感資料不能放在海外伺服器內。

可能受影響四類人士及資料

- ◆員工、前員工及其家屬，以及應徵者資料（包括身份證號碼、住址、出生日期和履歷）
- ◆《選擇》月刊訂戶資料，包括約8,000名曾提供信用卡資料的訂戶
- ◆投訴者資料，但因投訴處理系統用一套獨立運作的系統，相信只有小部分投訴人資料外洩
- ◆消委會合作夥伴，包括公司地址、電話、電郵或手機號碼

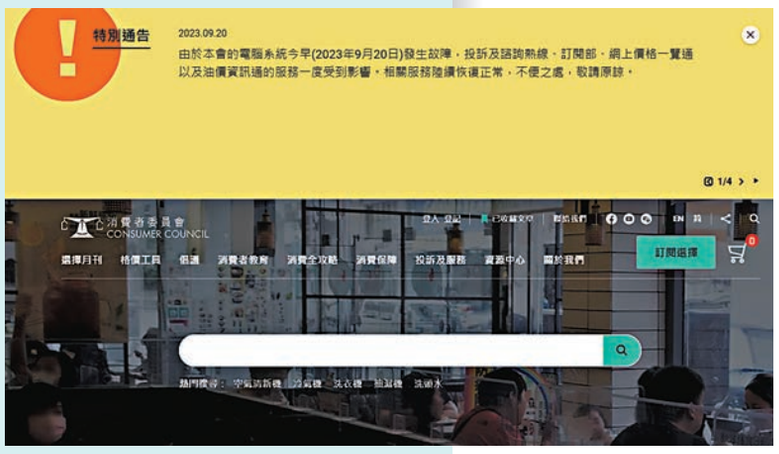
為保障個人資料私隱，相關人士應採取以下措施：

- ◆重設及定期更改網上賬戶密碼，並啟用多重認證功能（如有）
- ◆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，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否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

如有疑問，可致電消委會熱線（2929 2222）查詢

◆資料來源：消委會

◆整理：香港文匯報記者 張弦



▲消委會網頁公布顯示該會的電腦系統發生故障。

無24小時監控 翌日始知被夜襲

專家之言

香港消委會電腦系統雖然已安裝高效網絡安全系統，但仍中招，訊息安全專家龐博文昨日接受香港文匯報訪問時懷疑，該系統欠缺24小時全天候監測功能，「中招的系統好多時是夜晚被入侵，要翌日上班才發現。但事實上，目前有安全監控中心提供24小時監控服務。即時發覺就可立刻處理，抵抗入侵，將受影響範圍減至最小。」

龐博文認爲，各機構除了要增加系統安全檢測和提高警覺，不要點擊可疑電郵外，還有多種方法防範，包括系統內的數據應定期備份，並將數據分類，如客户、員工、合作夥伴及財務等資料分開存放，不要集中放在同一伺服器內，以免被黑客一次過打包盜取，如果分開儲存，對方只能下載部分資料，增加盜取所有資料的難度，「太麻煩會減低黑客下載資料的意慾。」

◆香港文匯報記者 劉明

政府正支援公營機構築牢三重防線

香港文匯報訊(記者 劉明)香港接連有企業及機構被黑客入侵，香港特區政府資訊科技總監黃志光昨日強調，事件反映網絡安全事故無處不在，特區政府循三方面保護數據，系統大部分都集中在私有雲端平台上管理，通過中央互聯網通訊站與互聯網接觸，其中有多層網絡安全保安技術，可24小時監測系統流量和發出警報，亦能攔截電郵內的惡意附件及連結，可抵禦日常隨機攻擊；但公營機構並不在保護範圍內，故已向有關企業及機構提供技術支援。

黃志光在會見傳媒時表示，特區政府不時偵察到企圖入侵政府系統的攻擊行為，但均成功阻截。原因是政府有三重數據保護防線，當中包括多層網絡安全保安技術如防火牆、偵測入侵和應變系統，可24小時監測系統流量和發出警報，亦隔除電郵內惡意附件和連結。

定期評估 培訓員工應變

在制度方面，要求部門嚴格遵守網絡安全指引，系統投入服務前做安全評估審查，每兩至三年須再做審查。政府並已要求部門成立電腦保安事故應變小組，一旦發生事故須即時通報資科辦，並要向私隱專員公署和警方網罪科匯報。最後是員工培訓，公務員須定期接受應變訓練，資科辦和警方網罪科亦有演練，並與海內外機構交換情報等。

不過，有關的規定未包括公營機構。黃志光強調，公私營機構都有責任保護資料系統和數據，各機構要保障網絡系統安全，有需要可向電腦保安事故協調中心求助，而資科辦亦設有平台為相關部門的網絡系統提供審計及入侵偵測，以盡早跟進未做好的修補工作。

督印：香港文匯報有限公司地址：香港仔田灣海旁道7號興偉中心2-4樓 電話：28738288 傳真：28730657 採訪部：28738260 傳真：28731451 發行中心：28739889 廣告部：28739888 傳真：28730009 承印：三友印務有限公司 地址：香港仔田灣海旁道7號興偉中心2-3樓