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10月 29 星期日
癸卯年九月十五 廿五立冬
大致多雲 幾陣驟雨 氣溫24-27℃ 濕度75-90%
港字第26873 今日出紙1疊5大張 港售10元

追蹤報道

香港數碼港及消費者委員會的電腦系統先後被黑客攻破，盜取了大量機密資料並進行勒索，但事件只是冰山一角，部分企業機構也曾中招。兩名成為黑客「點心」的學校及中小型地產經紀行負責人日前在接受香港文匯報訪問時，訴說與黑客鬥智鬥力經歷。他們所犯的網絡漏洞大忌值得公眾引以為鑑：長年無更新網絡安全系統，以及員工網絡安全意識薄弱，開啟了帶有病毒的連結。有專家表示，黑客是「無差別」入侵各地企業、機構的網絡，香港不少大專院校、中小學、連鎖地產公司、航空公司甚至公營機構都中招，可怕的是即使繳付贖金，黑客仍會食言照舊公開及兜售機密資料，故企業必須提高保安意識。

◆香港文匯報記者 文禮願

機構網安太落後 黑客眼中大活靶

入侵者每日掃描「誰有漏洞」有中學7年無更新系統淪獵物

香港文匯報記者發現，黑客「無差別」發動入侵，看似沒保存太多機密資料的中學，同樣成為黑客獵物。位於九龍區某所中學，去年初遭黑客「洗劫」，盜取了校內多份重要資料。

揭發事件的行政部主任周小姐憶述事發經過時仍猶有餘悸：「當日早上8點如常返到學校打開電腦，發現多份檔案被鎖住，包括一批學生入學紀錄、校方財務賬目，以及過去10年捐助校方的善長名單及聯絡資料。」

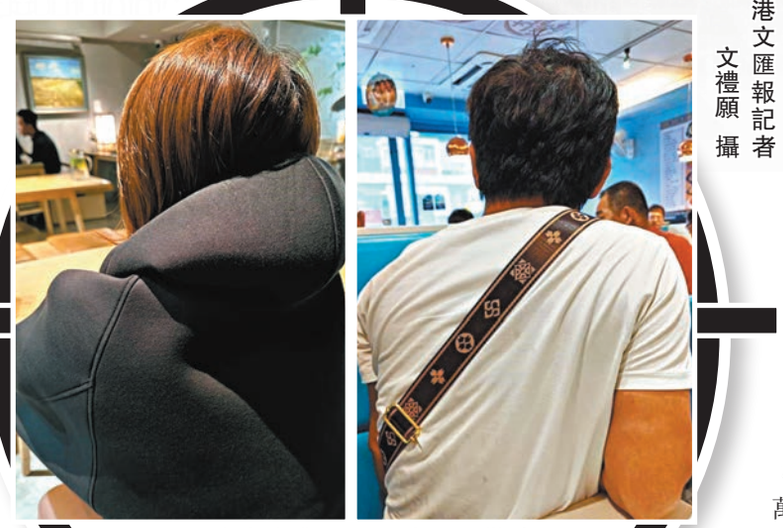
黑客大小通吃 掠校方50萬元

最初，她以為只是中了電腦病毒，馬上找資訊科技部同事來檢查，細查下才發現被黑客盯上。該黑客更單刀直入要挾在兩周內繳交50萬港元贖金，否則將有關資料在網上公開，令校方無地自容。

該校校長及高層知道後震驚，馬上召開緊急會議商討對策。有同事反對付贖金，但又擔心黑客公開學生資料會惹來家長及同學不滿，為免事情鬧大，決定息事寧人，繳付了50萬元贖金了事。

黑客見輕易得手，即指令校方盡快入錢。然而為免身份敗露，黑客拒絕透露其銀行入數賬戶，而是要求校方到尖沙咀一間虛擬貨幣場外找換店（OTC），將50萬元購買加密貨幣Bitcoin，然後存入指定的貨幣錢包內。被嚇得膽戰心驚的周小姐決定代校方完成「任務」。入數後，眾人忐忑不安地等待黑客回覆。黑客收錢後沒有食言，翌日隨即解鎖檔案。

眼見危機終於解除，校方馬上聘請網絡保安專家徹查「受襲」原因，發現漏洞原來出於電腦系統太舊所致。周小姐語帶無奈地說：「校方為了慳錢，7年沒更新系統。」她慨嘆校方並非大企業，一度以為沒什麼資料好偷，沒想到黑客大小通吃，扼緊校方的「死穴」作威脅。經此一役，校長馬上聘請網上保安公司全天候監察電腦系統，同時每年進行至少一次系統測試，確保沒有漏洞。



◆揭發所在中學遭黑客勒索的行政部主任周小姐

◆被黑客勒索80萬元的地產公司股東吳先生

◆香港文匯報記者 文禮願 攝

版本老舊 無升級無支援

專家點評

智慧城市聯盟資訊科技管理委員會主席龐博文指出，太舊的電腦軟件或系統往往難以抵禦黑客入侵，「有些公司或機構現仍沿用2012年的伺服器系統。這類版本太舊的軟件都有一個共通點，就是原廠已不再提供任何支援，即使發生問題亦無法得到安全升級，令黑客有機可乘。」

網絡勒索日漸普遍，過去3年已有百多間企業及機構遭黑客入侵，其中不乏大企業。到底黑客是如何揀選目標？龐博文坦言，「暗網」上的犯罪分子勒索目的無非爲錢，因此沒什麼針對性，犯案往往隨機應變，保安意識相對較低的企業，較易成爲目標，「黑客每日會透過所有社交媒體、即時通訊軟件及電郵發放無數假訊息，誘騙使用者點擊連結，令他們『感染』勒索軟件後進行勒索。」

與此同時，黑客亦會做足功課，每日留意在網上公開的訊息安全漏洞數據庫，了解最新的安全漏洞，然後在「暗網」下載相關的安全漏洞掃描工具，甚或自行編寫有關工具，然後在網絡上發動大規模掃描，只要發現任何機構的網絡設備存在這些漏洞，就會抓緊機會攻擊。

點擊可疑連結 地產公司失逾10萬客戶資料

除了中學外，一間擁有數間分店的連鎖地產公司亦成為黑客目標。股東吳先生透露，事發於2021年中，一名前線同事返回店舖欲打開電腦系統聯絡業主，才發現有關檔案變成一片漆黑。涉事黑客明目張膽留下訊息，稱有關檔案已被鎖定及盜取，索價贖金80萬港元。

由於被盜的資料涉及10多萬客戶，包括業主及租客的地址及聯絡電話，吳先生認為事態嚴重，一度想過報警，惟其他股東擔心事件外洩會影響公司形象，決定按兵不動，並求助IT專家。專家發現，黑客是透過可疑電郵入侵，懷疑是員工不慎開啟問題連結，結果在短時間內感染全體分店的電腦。

黑客最後因為收不到贖金，3個多月後，有關資料被發布在網上兜售，但黑客「留一線」，未有公開地產公司的名字，風波最後不了了之。經此一役，吳先生馬上聘請專人處理公司的重要及機密資料，將之加密。

屋宇署也中招

香港文匯報亦發現屋宇署去年曾被黑客入侵，該署回應查詢指去年1月11日收到政府電腦保安事故協調中心通知「樓宇齊愛護」網站被塗改，已即時關閉該主題網站，並報告事故予資科辦及香港警務處以作出調查，結果發現有關服務供應商未為受影響的網頁伺服器安裝最新修補程式，事件沒有影響該署內部的電腦網絡及系統，今年5月完成全面革新上述主題網站。

欠缺入侵者檢測與即時監控

專家點評

智慧城市聯盟資訊科技管理委員會主席龐博文解釋，黑客往往透過可疑連結「播毒」，只要有一位企業員工不慎點擊了就會「中毒」，更將病毒快速傳染全公司的電腦系統，除鎖上系統內的重要檔案外，有時連備份系統也受感染，令企業陷入癱瘓。

然而，不少企業以爲安裝了防毒軟件再加防火牆就「百毒不侵」，其實是大錯特錯。龐博文指出，防毒軟件主要抵禦部分電腦病毒，防火牆就好比閘門及看更，兩者雖具有一定抵禦力，惜關鍵是欠缺了「入侵者檢測系統」（Intrusion detection system），未能在被入侵的瞬間及時亮起紅燈。

「有入侵者檢測系統就好比閉路電視（CCTV），可及時發現是否遭人入侵，並提出警告。若同時配合24小時即時安全監控中心，即可在發現入侵者之同時，及時發起抵禦、驅逐、追蹤甚至取證，令入侵者知難而退。」他說。

就範幫襯「代繳贖金」恐遭加碼再勒索

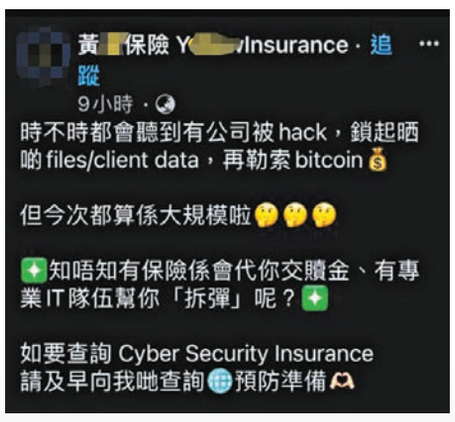
黑客入侵企業勒索除引發洩密災難外，更嚴重影響公司聲譽，損失往往難以估計。因應市場需要，近來愈來愈多公司提供「網上保安保險」，企業投保後一旦被黑害入侵，即會獲得一筆補償，更有聲稱是中介的公司近日不斷在社交媒體賣廣告，聲稱只要幫襯其「服務」，即使遇上黑客勒索，都可以「代為繳付贖金」，及「代為向黑客談判」。有法律界人士及立法會議員均擔心此舉會助長黑客氣燄。

翻查資料，在美國支付贖金給黑客或犯罪組織，通常被視為違法行為。大律師陸偉雄表示，代付贖金在香港雖然不屬犯法，但在道德層面上「此風不可長」，「罪犯不會因為你交了贖金一次而放過你，下次可能再勒索過。」

民建聯立法會議員葛珮帆表示，傳統保險業有存在代付贖金及代為談判的動作，但大多是應對遇上海盜勒索之類，然而到今時今日，勒索軟件在網絡上並無時間和空間限制，以繳付贖金企圖抑制事件的做法並不太可行，「有好多例子顯示即使受害者付上贖金後，被盜用的資料依然遭人放上『暗網』販賣，間接令其他黑客意識到某些企業原來願意就範，更加向其埋手苛索。」

隨着網上勒索個案加劇，她建議特區政府考慮立法禁止及明確表明政府機構絕不會向黑客談判及繳付贖金。

立法會議員陳沛良表示，網絡勒索個案近年愈趨普遍，往往令企業招致重大損失，保險界近年有提供各類「網上保安保險」，惜受歡迎程度只是一般。他認為有必要加強教育，令企業意識到買定保險，有助在出事時可獲得專業意見評估。



◆有自稱是保險中介的公司稱可代客人向黑客談判及繳付贖金。

逼苦主「打爆機」拍裸照出賣朋友

黑客成功發起網絡勒索後，除了開天殺價要求天價贖金外，部分勒索花樣更匪夷所思，包括要求受害者拍攝10張裸照、交出10個朋友的聯絡資料供黑客蹂躪，有人更會要求受害人下載某隻電腦遊戲軟件，並在短時間內「打爆機」為止，才會提供密碼，讓受害人為資料文檔解鎖。

交贖金一樣「撕票」

智慧城市聯盟資訊科技管理委員會主席龐博文透露，由於不少企業遭入侵後極為無助，部分人為免事件鬧大影響公司聲譽，傾向用錢解決，息事寧人，但他並不贊成繳付贖金，只因不少黑客不守信用，即使收到贖金仍然「撕票」，在網上公開盜取回來的機密資料。

「曾有國際知名公司於2017年被勒索軟件勒索後雖有支付贖金，但黑客斷斷續續放售資料，時隔6年、今年仍持續把被盜的客戶資料放上『暗網』轉賣，每套資料售價由最初的幾十萬美金，減至現時12美金。」他舉例說。

根據香港警方最新數字顯示，單是今年首7個月，涉及網上勒索的案件已達172宗，盜用電腦的案件為203宗，而去年網上勒索案件多達155宗。今年2月，警隊的網罪科推出「防騙視伏App」（Scameter+）流動應用程式，協助市民辨識詐騙及網絡陷阱。

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