網銀遭入侵炒股 下周推防衛計劃

香港文匯報訊（記者 蔡競文）金管局總裁陳德霖昨日在專欄《匯思》中撰文指出，本港網上銀行去年平均每月交易金額達7.3萬億元，金管局下周將推出銀行業的網絡防衛計劃。他更指出，近日有銀行的網上股票戶口被不法之徒入侵，盜用戶口進行股票買賣，銀行事後迅速回應並再提升保安措施，局方亦已與銀行業界商討如何進一步強化防範和偵測可疑網上股票買賣交易的措施。

戶口1100萬 每月交易額7.3萬億

陳德霖表示，網上銀行已變成市民日常生活倚重的環節，香港有提供網上或流動服務的銀行中，近半數客戶都有使用有關服務，網上銀行賬戶已逾1,100萬個，網上銀行的交易額和交易量逐年攀升，去年平均每月處理交易量高達1,700萬宗，金額達7.3萬億元。

今年3月，金管局成立「金融科技促進辦公室」推動金融科技的發展。陳德霖表示，金管局將會在下周舉行網絡安全高峰會，推出銀行業的「網絡防衛計劃」，主要工作包括網絡安全風險和應對能力的評估、人才培訓及業界資訊互享。金管局亦已與銀行業界商討如何進一步強化防範和偵測可疑網上股票買賣交易的措施。

陳德霖指出，近日有香港銀行的個別網上股票戶口被不法之徒入侵，盜用戶口進行股票買賣，估計他們可能由兩個途徑入侵：一是透過網絡在客戶的個人電腦植入惡意程式，盜取其網上銀行密碼；第二個可能是以電腦程式不斷嘗試而「撞中」用戶賬號和密碼。要防範類似的情況，最起碼是選擇較難破解的密碼，並避免以同一組密碼用於所有網上服務。

他指出，銀行事後迅速回應並再提升相關保安措施，加強對股票賬戶的保障，金管局亦已與銀行業界商討如何進一步強化防範和偵測可疑網上股票買賣交易的措施。

密碼「123456」無異開門揖盜

陳德霖表示，黑客的攻擊手法層出不窮，一些新招還包括侵入企業電腦系統後將機密檔案加密，然後勒索比特幣（bitcoin）作解密的「贖金」。金融機構更是黑客重點攻擊目標。金管局去年接獲19宗報告，稱銀行受分佈式阻斷服務攻擊（DDoS，以大流量造成網絡交通阻塞），當中6宗更以實施DDoS作威脅，向銀行進行勒索。幸而銀行服務未有因DDoS而受嚴重影響。

即使「網絡安全」是小學常識科必考，但知易行難，很多人可能意識不到網絡漏洞帶來的殺傷力，對於保障自己網絡安全仍掉以輕心。據一間網絡安全公司統計，去年歐美網民最常用密碼仍然是「123456」，實在與開門揖盜無異。

陳德霖認為，要保持公眾對銀行業的信心，關鍵之一是銀行體系具備應對和處理網絡風險的能力。他指出，上述事件是很好的警示，提醒網絡安全不但要「知」，更重要是「行」，「銀行客戶、金融企業、監管機構三方都應『知行合一』，重視和實踐網絡安全。」

■金管局下周將推出銀行業的網絡防衛計劃。 資料圖片

網絡遇竊兩禍首：懶諗密碼 亂開電郵

專家倡雙重認證加密數據堵塞漏洞

香港文匯報訊（記者 岑志剛）互聯網發展一日千里，人類工作、休憩以及日常生活，都離不開網絡。越來越多企業發展電子商貿，遭受黑客攻擊的風險亦隨之提高。網絡保安公司Verizon昨日發表《數據失竊調查報告2016》，發現高達63%經確認的數據失竊，都是因為密碼太簡單破解所致；而利用附有惡意程式的釣魚電郵，盜取個人資料的「三路攻擊」亦日漸普遍。報告建議用戶應在電腦採取雙重認證、盡快修補保安漏洞、為數據加密及培訓員工了解有關資訊保安事務等。

Verizon向包括澳洲警方等全球67家機構取得資料，分析去年逾2,260宗經確認的數據失竊個案及逾10萬宗保安事故，結果發現89%的攻擊目的是騙取金錢或與間諜活動有關；以勒索軟件進行攻擊的個案數目比去年上升16%，而高達63%經確認的數據失竊都是因為密碼容易破解、沒有更改或被盜取，但很多機構仍嚴重缺乏基本的防禦措施。

保安事故顯示9種犯罪橋段

報告又指出，85%成功的網絡攻擊，都是利用報告中提及的常見十大程式漏洞。95%的數據失竊及86%的保安事故可歸納為9種犯罪橋段，包括誤用行為如密碼太簡單、網絡程式攻擊、遭犯罪軟體攻擊等（見圖）。

Verizon亞太區網絡安全總監黃財明昨日表示，不少用戶設置的個人密碼過分簡單，甚至只沿用系統預設密碼而沒有重設密碼，容易被攻擊者入侵；保安事故中的「其他錯誤」有26%涉及把敏感資料發送到錯誤的收件人，包括公司資料處理不當、IT系統配置錯誤，以及手提電腦與智能電話等失竊等。

黃財明又指，「三路攻擊」日漸普遍，騙徒會先發出附有惡意連接或附件的釣魚電郵，然後會將惡意軟件下載至電腦，盜取個人資料，最後利用盜取的資料進行更多攻擊，如登入網上銀行或零售商店等網站。

釣魚郵件7賤招 30%上鈎

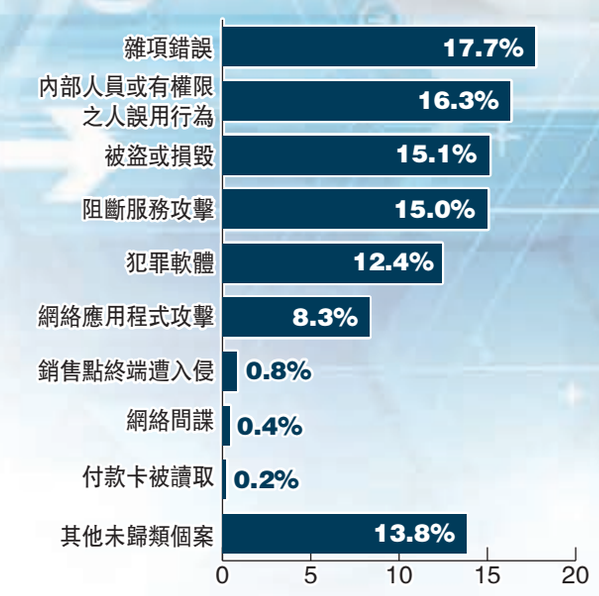
黃財明表示，「網絡釣魚」數字大幅增加，今年有30%的釣魚郵件被打開，相比2015年的23%有明顯上升；而被點擊的郵件中，13%更打開了惡意附件或連接，讓網絡罪犯得以透過惡意軟件犯案。他指「網絡釣魚」過往主要涉及網絡間諜活動，但今年已擴展至9種犯罪橋段中的7種。

黃財明又說，網絡犯罪速度愈來愈快，在93%的個案中，攻擊者只需數分鐘甚至數十秒，就能把系統攻陷；而在28%的個案中，數據在幾分鐘內便被偷取；但70%個案用戶或企業需要數月，甚至數年時間才能發現，由遭入侵到發現的時間差更有擴大趨勢。

Verison建議用戶應採用雙重認證，並且鼓勵登入社交網絡應用程式時也採用；盡快修補已知的漏洞；為數據加密並審查所有登入記錄以偵察惡意活動；以及培訓員工保安意識等。


■Verizon發表《數據失竊調查報告2016》，發現密碼太容易破解，釣魚電郵盜取資料日漸普遍。左起黃財明、葉照長、謝梅鶯。 岑志剛 攝

網絡攻擊9種常見犯罪橋段



資料來源：《數據失竊調查報告2016》
製表：記者 岑志剛

「三路攻擊」手法

一種新出現的「三路攻擊」正日趨普遍，而且已經影響到不少機構。這種攻擊包括：

■發出附帶惡意連接或附件的釣魚電郵。

■把惡意軟件下載至個人電腦，從而建立立足點，然後經其他惡意軟件來探取秘密及要盜取的內部文件（亦即網絡間諜活動），或把檔案加密以進行勒索。有時惡意軟件會透過鍵盤記錄來盜取多個應用程式的登入資料。

■利用盜取的登入資料進行更多攻擊，例如登錄到銀行或零售商店等第三者網站。

商業間諜案95%源自銷售點

香港文匯報訊（記者 岑志剛）黑客行為涉及商業犯罪。Verizon亞太區網絡安全總監黃財明表示，被攻擊和入侵的電腦，涉及的數據失竊主要包括顧客用戶資料、付款卡數據，甚至是產品設計圖。報告發現，95%數據失竊都涉及銷售點終端遭入侵。

黃財明指出，店舖的銷售點終端系統，可能同時用作處理文書、上網等其他用途，如果員工保安意識不足，不慎在網上下載惡意軟體或打開釣魚電郵，可能令系統被入侵，令客戶的信用卡交易資料失竊，建議有關企業應安裝電腦保安修補程式，小心選擇雲端服務提供者等。

報告又指出，47%數據失竊都涉及製造業，可視為網絡間諜行為。他提到，有個案利用犯罪軟件，盜取製造業公司的產品設計圖，最終新產品被競爭者搶先推出市場，「有公司自己設計新產品，但發覺競爭對手快過他們推出！」他指，轉售產品設計圖有利可圖，容易成為黑客目標。

海盜偷客戶提單 方便劫船

眾多個案中最誇張的，莫過於涉及海盜事件的資料盜竊。黃財明說，國際上的海盜行為出現轉變，專門搶劫運載高價值貨物如珠寶的船隻。他們分析數據後發現，被搶劫的船隻的海運提單，事前被黑客入侵下載，相信海盜是利用提單鎖定目標。

勒索軟件攻擊比例激增至39%

香港文匯報訊（記者 鄺慧敏、岑志剛）《數據失竊調查報告2016》指出，85%成功的網絡攻擊，都是利用報告中提及的常見十大程式漏洞；而可歸納為9種犯罪橋段當中，以勒索軟件進行攻擊的個案正在上升，佔「犯罪軟體」一項的39%，較2014年增加了16個百分點。Verizon亞太區網絡安全總監黃財明認為，有關個案升幅屬不算多，但估計未來會有持續上升趨勢。香港資訊及系統保安專業人員協會顧問龐博文指出，勒索軟件愈來愈普遍，而且勒索軟件有利可圖，故個案上升屬正常情況，預計未來有更多人中招。

勒索比特幣 無法追蹤流向

龐博文指出，勒索軟件主要是令電腦中毒，把電腦內的文件封鎖，用戶需繳付比特幣才能解鎖，但現時勒索軟件愈來愈普遍，而製造勒索軟件的門檻不高，黑客只要進入地下網絡，便能購買製造勒索軟件的編碼。

他又指出，勒索軟件有利可圖，因現時各國政府未有禁止比特幣，又無法追蹤比特幣的去向，比特幣成為安全的收取款項途徑，更有中國製的勒索軟件教導電腦用戶如何購買比特幣，顯示不法之徒具有組織性。

龐博文說，最近於地下網絡出現能入侵電視盒子及手機的相關病毒，相信勒索軟件將會擴散至其他電子產品之中，呼籲市民切勿掉以輕心，建議減少使用盜版軟件、不要開啟來歷不明的電郵及經常備份。他又促請各國政府監管比特幣，以打擊勒索軟件。

民建聯立法會議員葛珮帆表示，勒索軟件背後是無本生利的行為，強調市民及企業若不幸「中招」，應立即報警助警方找出幕後黑手，又要求政府主動接觸更多中小企，讓他們了解網絡安全之重要性。

輕失網遊道具 重則遭狂碌卡

話你知

網絡雖然爲市民帶來方便，但亦有不法之徒利用網絡保安漏洞犯罪，包括網上遊戲盜竊、「釣魚」電郵及勒索軟件等，市民一不小心隨時墮入陷阱，得不償失。早年的網絡犯罪多爲網上遊戲盜竊，例如遊戲賬戶被人非法使用，賬戶所擁有「道具」及「金幣」被人非法轉移到其他賬戶，買賣「賬戶」、「角色」、「道具」時出現詐騙等。

另外，「釣魚」電郵也是網絡犯罪之一。不法之徒向電郵用戶發出「釣魚」電郵，訛稱是某機構的職員，並誘導用戶瀏覽一些仿眞度極高的虛假網站，例如假冒銀行網頁，並試圖令銀行客戶登入網站，以騙取用戶的個人資料，包括地址及信用卡號碼等，不少市民因而損失慘重。

此外，新興加密勒索軟件「Locky」肆虐。據香港電腦保安事故協調中心統計，今年2月至3月底，已收到38宗「Locky」個案，受害機構多爲中小企及非牟利組織。「Locky」透過垃圾郵件入侵電腦，用戶一旦打開文件，病毒便入侵電腦，檔案會被加密而無法打開，並會在用戶的電腦桌面登出勒索告示，要求索取1元至4元比特幣，即約數千至數萬元，用戶需繳交贖金才能打開電腦檔案。

■記者 文森