跨國交易漏洞 招連環盜款

黑客肆虐銀行 SWIFT評倫保安毒瘤

今年接連發生金融黑客入侵銀行系統事件，其中孟加拉央行早前爆出被盜用身份，匯走存於紐約聯邦儲備銀行的8,100萬美元(約6.3億港元)存款，引起外界關注業界網絡保安。銀行業界現時透過環球銀行金融電訊協會(SWIFT)系統進行跨國交易，連串黑客事件令外界憂慮，SWIFT或已變成金融保安「最弱一環」，淪為不法之徒利用的工具。

■香港文匯報記者 余家昌/黎耀康

SWIFT成立於1973年，由比利時等10個發達國家的央行共同管理，董事局成員則由大型銀行代表出任，是1萬多間成員銀行跨國交易的重要媒介。SWIFT的運作機制並不透明，有前員工透露，SWIFT依賴電子代碼核實客戶身份，但不設額外認證機制，故只要黑客成功盜取代碼，便能為所欲為，保安較一般銀行寬鬆得多。

侵SWIFT冒銀行指示匯款

黑客今年1月12日進入SWIFT系統，冒充厄瓜多爾銀行Banco del Austro(BDA)，指示美國富國銀行及花旗銀行把BDA在該行的存款，匯到多個不知名戶口。富國信以為真，其後10日進行最少12次交易，造成1,200萬美元(約9,319萬港元)損失。

BDA一個月後控告富國，指後者沒即時報告可疑交易，應賠償損失款項，又稱花旗已賠償180萬美元(約1,398萬港元)。富國反駁稱是按SWIFT指示行事，認為BDA需自行承擔電子代碼外洩損失。SWIFT則稱對事件不知情，已跟涉事銀行聯絡。

僅2400人 SWIFT資源不足

SWIFT前高層多伊爾指出，銀行業界一般對被黑客入侵秘而不宣，以免損害形象，甚至產生保安系統易被攻破的印象，BDA事件反映無論是SWIFT或銀行業界，均對黑客入侵的情況不甚了解。由於不少牽涉黑客入侵事件的銀行均私下解決損失，估計實際情況較現時所知嚴重得多。

SWIFT承認正調查多宗黑客入侵事件，促請客戶報告類似個案，國際清算銀行(BIS)去年亦發表報告，建議業界加強交換網絡攻擊的資訊，減低金融機構面對的風險。英倫銀行及瑞典央行已要求國內所有銀行，加強對SWIFT電子代碼的保安，不過SWIFT人力資源部門前主任蘭布雷希特指，SWIFT由大型銀行控制，加上人手只有2,400人，資源嚴重不足，難以強制要求成員通報黑客入侵資訊。

■花旗銀行成黑客目標，據稱賠償厄瓜多爾銀行逾千萬。 網上圖片

■SWIFT已成金融保安「最弱一環」，淪為不法之徒利用的工具。 設計圖片

歐元區銀行運作流程

發送付款指示

– 歐元區大部分銀行支付皆以Target 2支付系統完成，25個歐洲國家共1,800間銀行使用
– 當一間銀行透過Target 2向另一銀行支付款項，付款銀行在所屬國家央行的賬戶會被扣款，收款銀行在所屬國央行賬戶結餘增加
– 每次付款，交易雙方都是依據電子訊息，「環球銀行金融電訊協會」(SWIFT)負責驗證和加密訊息

SWIFT驗證

– 付款方利用SWIFT系統加密支付訊息，再傳至SWIFT網絡
– 完成驗證後，SWIFT向Target 2平台發送訊息
– 有關訊息通過安檢後，Target 2發出結算確認，並由SWIFT送往收款方


■孟加拉央行今年2月遭黑客盜款逾6億。

SWIFT促銀行速報可疑交易

環球銀行金融電訊協會(SWIFT)系統自去年起至少3次遭黑客入侵，其中孟加拉央行更損失8,100萬美元(約6.3億港元)。SWIFT為應對保安漏洞及解決SWIFT與銀行溝通不足問題，周二宣佈於本周內制訂新保安計劃，以重建SWIFT的信譽。

指黑客侵銀行網絡盜密碼

SWIFT要求使用協會系統的銀行改善資訊分享，盡速向SWIFT回報可疑交易，同時加強系統保安及增加使用可偵測黑客入侵的軟件。SWIFT則會向銀行提供遏止入侵所需工具，以及制訂更嚴格準則，評定銀行對系統的保護是否足夠。

SWIFT上周五指出，其網絡、服務及軟件均沒受入侵事件影響，相信黑客闖入銀行網絡，取得銀行SWIFT密碼後，再假裝銀行發出指示，將資金轉至黑客戶口。SWIFT總裁萊布蘭特指有關國家沒足夠技術保護銀行，令黑客得逞，又稱SWIFT無法獨自負責系統保安。萊布蘭特進一步稱，銀行業須創造一個適合的「生態系統」，包括實施第三方服務提供者認證要求等，以保障服務提供者及合作夥伴的質素。

前總裁：SWIFT保安落後

然而，部分批評者認為SWIFT應更積極行動，例如審查系統客戶，發現不符合保安要求時，將其剔除出服務名單。SWIFT前總裁施蘭克則指，SWIFT保安改進追不上黑客愈趨複雜的犯罪手法，提議SWIFT採用「不正常交易偵測器」，阻延有問題的訊息，或是將系統與銀行網絡分開。


■孟加拉央行行長拉赫曼(中)引咎辭職。

■國際黑客組織「匿名者」目的是推翻資本主義。

反資本主義黑客癱瘓倫交所網站

國際黑客組織「匿名者」的菲律賓分支，早前入侵倫敦證券交易所(LSE)網站，導致網站癱瘓超過2小時。倫敦警方表示未接獲有關報告，LSE則拒絕評論。專家相信交易系統沒受影響，亦沒有機密資料失竊。

在倫交所網站被入侵前，「匿名者」曾聲稱入侵了土耳其證券交易所和紐約泛歐證券交易所的網站，目的是抗議全球銀行業和金融機構。「匿名者」聲稱，他們成功攻擊的目標包括瑞士央行、委內瑞拉央行和三藩市聯邦儲備銀行。

網絡保安公司CyberInt專家邁爾稱，「匿名者」其中一個目的是推翻資本主義，「反對不公義及虛偽建制」，又指近期連串入侵暴露了多間金融機構的系統保安存在漏洞。

歐央行設即時警報系統

全球近年發生多宗針對銀行系統的大型網絡攻擊，導致巨大損失。有見及此，歐洲央行最近設立首個即時網上警報系統，自2月起收集歐元區內18間最大型銀行的數據，準備明年擴展至受歐央行管轄的130間銀行。

孟加拉央行2月遭黑客入侵，轉走8,100萬美元(約6.3億港元)。歐洲央行隨即試行實時警報系統，收集歐元區18間最大銀行的網絡入侵事件資料，儲入數據庫。歐央行副行長米肖稱，行方主要收集造成巨額損失，以及嚴重打擊銀行聲譽的「顯著入侵事故」，分析黑客攻擊的趨勢，預先警告可能成為入侵目標的銀行，又計劃與美國聯儲局及英倫銀行等分享情報。

孟加拉央行遭盜款經過

2015年	
3月15日	黑客利用假名，在菲律賓中華銀行(RCBC)馬卡蒂分行開設4個戶口。
2016年	
2月4日	黑客向紐約聯儲銀行發出至少35項環球銀行金融電訊協會(SWIFT)虛假支付指示，涉及9.51億美元(約73.71億港元)，其中4項支付要求獲批，8,100萬美元(約6.3億港元)被轉至RCBC，另一筆2,000萬美元(1.55億港元)則轉入斯里蘭卡泛亞銀行。其餘30項涉及8.5億美元(約65.88億港元)的交易指示，因收款人資料不明，紐約聯儲銀行拒執行。
2月5日	孟加拉央行董事胡達發現，用作列印SWIFT交易確認的打印機紙盒全空，以人手列印後，發現數十宗可疑交易。同時，有人以「Jessie Christopher Lagrosas」假名，從RCBC櫃枱提取2,270萬美元(約1.76億港元)，存入以「William Go」假名開設的RCBC戶口。
2月6日	胡達發現連接SWIFT系統的銀行終端機軟件沒反應，後來發現收據顯示，紐約聯儲銀行將拒執行的數十項匯款要求傳回孟央行。
2月8日	孟央行官員發現有5項未經批准的SWIFT驗證訊息送出，顯示大筆款項被轉入RCBC及斯里蘭卡泛亞銀行。

黑客測中東銀行保安

美國網絡保安公司FireEye的專家指出，有黑客向中東多間銀行發送一批包含惡意程式的電郵，一旦打開附件，程式會盜取銀行網絡資料，包括客戶密碼及銀行電腦採用的軟件。專家表示，黑客這種手法較罕見，明顯是「預先偵測潛在入侵目標」，為進行欺詐轉賬要求作準備。

中東及非洲最大銀行卡塔爾國家銀行(QNB)的網絡系統早前遭黑客入侵，大量客戶名字及賬戶密碼更被上載到互聯網。FireEye發言人表示，遭黑客發送惡意電郵的銀行並不包括QNB，但沒透露涉及的銀行名稱和所屬國家。發言人又稱，惡意程式已將資料傳回黑客的伺服器，表示部分銀行的網絡系統已遭感染。


■美國網絡保安公司FireEye調查黑客事件。