◎資通安全宣導

## ～網路駭客在臺碰壁—第一銀行遭詐領案～

105 年 7 月 11 日（週一）上班後，第一銀行發現該銀行 ATM 遭詐領共達新臺幣八千多萬元，經各分行通報清查後發現，7 月 9 日及 10 日，全臺各地共有 22 家分行 41 台 ATM 遭到詐領，ATM 從吐鈔口接連吐出一疊疊厚鈔，沒有輸入任何密碼，也不需提款卡，甚至不用接觸 ATM 就能領錢，彷彿像電影情節一般，ATM 成了一台源源不絕任意吐鈔的機器。此案為臺灣史上 ATM 遭駭客入侵盜領首例，第一銀行隨即向平日保持聯繫的調查局新北市調查處報案，新北市調查處報請臺北地檢署指揮偵辦，之後才向警方備案，由調查局負責解析駭客犯罪手法，找到遠端遙控的惡意程式及可能的入侵路徑及來源，警方則負責查緝涉案車手及洗錢的犯罪分子，調查局及警方分進合擊，不眠不休地進行蒐查，分別扮演不同的角色分工合作，拼湊這起臺灣史上頭一遭沒有提款卡也能詐領大量現金的犯罪案件全貌。

案發隔天，調查局資安鑑識實驗室人員隨即前往第一銀行總部，並向總行資訊處調取相關電腦軌跡檔（log 檔），該銀行也將發生金額短少的 41 台 ATM 設備，陸續送到調查局的資安鑑識實驗室進行鑑識，希望能夠找到任何蛛絲馬跡，還原駭客可能的入侵路徑。調查局資安鑑識團隊從第一銀行提供的電磁紀錄及設備中，找出 3 支惡意程式及 1 個執行批次檔，經分析惡意程式及批次檔發現：其中「cnginfo.exe」程式主要用來取得 ATM 相關訊息，包括 ATM 系統及吐鈔夾資訊，並可以測試開啟吐鈔開關夾；「cngdisp.exe」 程式及「cngdisp_new.exe」主要的功能就是操作 ATM 吐鈔程式，帶入參數後，可以選擇吐鈔的卡夾槽及吐鈔張數，執行該惡意程式後，就可以吐出鈔票；「cleanup.bat」程式則是一個批次檔的執行程式，透過執行微軟刪除功能的程式 「sdelete.exe」， 清除顯示 ATM 相關資訊的「cnginfo.exe」和控制 ATM 吐鈔功能的「cngdisp.exe」及「cngdisp_new.exe」，試圖抹除犯罪軌跡及相關資料。調查局資安鑑識人員發現上述惡意程式後，更進一步發現在 7 月 9 日至 11 日 ATM 遭詐領期間，ATM 主機有來自一銀倫敦分行電話錄音伺服器的異常連線，但由於倫敦分行並沒有 ATM，理應不該出現這樣的連線紀錄，因此研判駭客極可能透過駭入倫敦分行電話主機，並藉其滲透進銀行

內部網路取得網路管理權限，再藉由內部 ATM 派送主機提供 ATM 更新程式時，將含惡意程式的更新包發送到各 ATM，藉此打開 ATM 遠端連線及控制 ATM 吐鈔。還原駭客入侵犯罪手法 105 年 7 月 9 日至 10 日，駭客集團內多名在臺車手貝某、柏某等人，陸續至第一銀行各分行受駭 ATM 前等候，並藉由犯罪集團之駭客操控該銀行 ATM 使其自動吐鈔，順利取走鈔票後，再將不法所得交由安某等人進行移轉及寄藏，並指派集團內其餘人員負責後續接應及處理。雖然第一銀行在 7 月遭駭客集團詐領，但此集團早在 5 月就已設法入侵該銀行內部網路，搜尋可能漏洞，控制其倫敦分行錄音主機，並且使用海外 IP 與該錄音主機建立異常連線，以非法手段取得網路管理者權限之帳號密碼，瀏覽存取該銀行內部網路伺服器及員工個人電腦等資訊，藉以掌握該銀行內部訊息，逐步蒐集犯案所需資訊，並成功盜取該銀行 ATM 更新程式的派送系統管理者權限，駭客取得派送系統的管理者權限，無疑是將 ATM 的大門打開，可以輕鬆地將遠端連線及吐鈔等惡意程式，透過派送系統植入各分行 ATM。犯罪集團取得派送系統的權限後，陸續將犯案所需之工具程式偽裝成第一銀行 ATM 更新程式的檔案，再利用先前取得之管理者帳號密碼，將遠端連線服務、吐鈔程式及執行批次檔等派送至部分 ATM，直到 7 月開始密集派送至各 ATM，藉以開啟遠端連線服務，並選在假日期間，安排車手到各分行 ATM 等待，犯罪集團之駭客遠端執行吐鈔程式後，由車手順利將鈔票取出。

警方追查車手及贓款流向在調查局追查駭客犯罪手法及入侵來源的同時，警方也透過調閱第一銀行遭駭 ATM 的相關監視器，對於領款之車手進行地毯式的搜索，惟 13 名執行領款的車手在案發後已紛紛離境，但警方發現 2 名車手貝某及柏某在離開前，將房間交給 1 名拉脫維亞籍男子安某，警方隨即掌握該名嫌犯並公布其長相，研判安某來臺目的應該是為了處理後續贓款。安某在發現自己身分曝光後，馬上離開臺北並逃往宜蘭，但在 17 日被眼尖的員警認出，經通報當地派出所支援將安某逮捕到案，安某表示是遭到俄羅斯黑手黨威脅與利誘，才參與本次犯罪活動，並依其供詞順利在臺北市大直維多利亞酒店逮獲另 2 名羅馬尼亞籍詐領案嫌犯，並查獲詐領之贓款。

結語

近年來因應行動通訊、社群媒體、大 數據、雲端科技等資通訊技術的進步，金 融服務也順應時代潮流，在金融數位化、 網路化、行

動化下，雖然使民眾生活更加 便利，也造成一連串資訊安全問題，透過 此次事件或可思考：一、以「白名單」方式控管可在 ATM 系統 中執行的合法程式，及於 ATM 上裝置異常金錢提領預警系統之可行性等。二、盤點組織資訊設備，務使每一設備均納入管理與監控；並即時監控組織內網路運用，發現異常應立即追查到底，排除任何入侵可能性。三、妥善保存管理者權限之帳號密碼，勿因人為疏忽遭竊。資安問題其嚴重性與損害性，往往取決於使用者之資安概念，若能建立良好資訊安全防護概念，如內外網實體隔離、定期更新防毒軟體、檢查電腦有無惡意程式、 網頁，以及郵件開啟前先確認安全性，再 加上完備的網路安全防護及人員管理等作為，盡可能將網路管理及資訊安全做到零死角，將資安風險降到最低，確保資安防護滴水不漏，始可有效防範此類電腦犯罪 再度發生。


*臺中榮民總醫院關心你也提醒你!*