臺灣起訴世界首件卡巴耐克集團電腦駭客案

文・圖／張安箴

電腦犯罪手法日新月異，電腦駭客（hackers）們處心積慮利用網際網路的便利，以入侵網站的方式獲取利益。在此同時，有另一群人，同樣有高超的電腦程式能力，被稱為白帽駭客（White Hat Hacker），也想方設法找出網際網路的漏洞，但事先對公司或網站管理者提出警告，以期能在其他駭客還未能入侵前就做好防護。

2010年7月28日，有一位傳奇性的白帽駭客巴納比・傑克（Barnaby Jack）在黑帽駭客大會（Black Hat Computer Security Conference）上做了一個非常有名的示範，他稱之為Jackpotting（中大獎）；他在台上擺了兩台提款機，並利用自己的電腦遠距操控，先對提款機植入惡意程式（malware），然後對其中一台提款機使用自製提款卡提領現金，對另一台提款機則完全不需要任何人近距離碰觸，就能使該提款機在惡意程式的操控下自動吐出現金。他的示範震撼了全世界[1]。

自從Jack的中大獎示範後，電腦駭客集團針對銀行提款機的攻擊也越來越頻繁。在2014年，俄羅斯的資安公司GROUP-IB發布消息指出，從2012年到2014年間，在俄羅斯與烏克蘭發展出一個名為Anunak的駭客集團，用駭入銀行提款機的手法從東歐國家的銀行偷走1,500萬歐元。這個集團的手法是對銀行員工寄出釣魚郵件，使員工誤以為郵件是從俄羅斯聯邦寄出的，等銀行員工誤點開該郵件後，郵件內的惡意程式就使該員工的電腦中毒，之後再從該電腦植入惡意程式到銀行電腦，進而影響銀行提款機，使提款機搞錯提款金額而吐出多於提款金額的錢。

同年，電腦資安公司卡巴斯基實驗室（Kaspersky Lab）收到一家烏克蘭銀行的委託來調查一件銀行提款機在無人提領情況下自動吐鈔導致銀行受害的事件。到2015年，該實驗室發布正式的調查報告指出，他們發現這是一種新型的駭客攻擊手法，稱之為卡巴耐克（Carbanak）。到2016年，卡巴耐克集團已經攻擊全世界超過100家銀行，得手超過10億美金。集團已經曝光的成員包括俄羅斯籍、烏克蘭籍、拉脫維亞籍、羅馬尼亞籍、愛沙尼亞籍、摩爾多瓦籍、澳洲籍與中國籍，已是一個跨國犯罪集團的規模。而僅2016年一年間，已被確認為該集團發動的攻擊案件就已經發生在西班牙的巴塞隆納、馬

德里、阿利坎特、波蘭的華沙、亞塞拜然的巴庫、法國的尼斯、塔吉克斯坦的杜尚貝、白俄羅斯的明斯克、吉爾吉斯與羅馬尼亞等地。這個猖獗全世界的駭客集團全球橫行無阻，卻沒有一個國家能夠破案。

該集團也把矛頭指向臺灣，在2016年5月間，該集團發現我國第一商業銀行倫敦分行的某一個可以連接到外部網路的電話錄音主機系統竟然可以連到銀行內部網路，出現漏洞[2]，故就在5月31日晚上10時36分，入侵該電話錄音主機，並等待時機做進一步的入侵。之後，該集團利用該銀行分行的電話錄音主機連入銀行內部網路，取得該銀行提款機控制現鈔資訊的程式，又植入惡意程式，指定在2016年7月間特定時間段執行強制提款機吐鈔的動作；該集團同時還植入清除程式，以便得手款項後刪除曾經入侵該銀行電腦的所有記錄。

做好準備工作後，該集團就陸續在2016年7月6日到9日間派出15位提款車手自世界各地飛抵臺灣。第一組是從土耳其入境的曼紐肯與艾迪恩，他們在7月10日凌晨2時29分起到11日凌晨0時39分止，依集團指示時間到第一商業銀行雙和分行、埔墘分行、古亭分行、雙園分行、木柵分行等分行提款機前等待惡意程式運作而吐出現鈔，兩人共領得新台幣（下同）2376萬6千元。第二組是從杜拜入境的馬力克與從香港入境的賽克亞瑞與維利科羅，他們三人在7月10日凌晨1時48分起至7月11日凌晨2時24分止，依集團指示時間到第一商業銀行光隆分行、吉林分行、汐止分行、汐科分行、萬華分行等分行提款機前等待惡意程式運作而吐出現鈔，三人共領得1548萬1千1百元。第三組是自香港入境的貝瑞佐夫斯基與柏克曼，兩人自7月10日凌晨0時33分起至11日凌晨2時17分止，依集團指示時間到第一商業銀行北臺中分行、臺中分行、南臺中分行、大里分行、公館分行等分行提款機前等待惡意程式運作而吐出現鈔，兩人共領得1526萬5千5百元。第四組是從土耳其入境的亞克夫、從香港入境的約瑟夫、拉斐克，他們從7月10日凌晨1時51分起至3時3分止，依集團指示時間到第一商業銀行江子翠分行與華江分行等分行提款機前等待惡意程式運作而吐出現鈔，三人共領得264萬元。第五組是從菲律賓入境的譚恩與從澳洲入境的維克特，兩人從7月10日凌晨4時24分起至晚上8時42分止，依集團指示時間到第一商業銀行臺中分行與中港分行等分行提款機前等待惡意程式運作而吐出現鈔，兩人共

領得347萬4千元。第六組是從土耳其入境的巴比、烏爾蘇與阿爾謝，三人從7月10日凌晨3時10分起至11日上午6時48分止，依集團指示時間到第一商業銀行興雅分行、西門分行、忠孝路分行與五股分行等分行提款機前等待惡意程式運作而吐出現鈔，三人共領得2,265萬1千元。此集團在兩天內總共盜領得8,327萬7,600元。

上開取款車手完成取款後就將款項留在住宿旅館等待銷贓車手取款，並陸續在7月10日至13日間，出境至香港、杜拜、加拿大、土耳其與韓國等地。其中車手頭巴比收集第二組與自己的第六組的贓款後放在兩個行李箱，藏在臺北車站地下一樓東出口前的置物櫃內。在此同時，集團派出銷贓車手7人，包括7月9日從香港入境的洛夫斯基、7月11日從澳門入境的莎琪蘇娃與從杜拜入境的安德魯、7月13日自深圳入境的保羅與自土耳其入境的雷納斯、7月16日自韓國入境的潘可夫與自加拿大入境的米海爾等。洛夫斯基負責收取第一組曼紐肯與第四組亞克夫提領的贓款，並與莎琪蘇娃會合後，將贓款置放在白色行李箱中，前往寒舍艾美酒店510號房藏放。保羅與車手頭巴比會合後，一同將510號房的行李箱運至臺北火車站地下一樓東出口前置物櫃內，其後兩人就在7月13日離境。安德魯負責至君悅酒店1547號房收取第三組貝瑞佐夫斯基取得的贓款，帶往臺北市民生東路的出租套房藏放。潘可夫與米海爾則負責到臺北火車站取出藏放贓款的行李箱，運往臺北市敬業路的維多利亞酒店715號房，等待洗錢指示。

從上述該集團細膩的犯罪手法與分工，大概可窺知為何其能橫行各國犯罪而無人能查獲。

但在7月10日晚間8點，當曼紐肯與艾迪恩出現在第一商業銀行的古亭分行收取款項時，剛好被前來提款的民眾發覺提款機上有未取走的6萬現鈔在吐鈔口，民眾想要提醒兩人故拉住其中一人，該車手因心慌拉扯而掉落自己的信用卡在現場，倉皇離開。民眾因而記下計程車號並報警。檢察官立即與調查局、刑事警察局、臺北市政府警察局成立專案小組，並逐步從清查計程車號、信用卡號開始，進而調閱相關人士的入出境紀錄、城市監視器錄影畫面、旅館入住記錄等，在短期內花費大量人力、物力過濾龐大資訊，最終將此集團部分成員與詳細做案手法揭露於世。

集團成員安德魯、潘可夫與米海爾因快速的查緝動作，尚未出境就遭逮捕並遭起

訴，並起出贓款7748萬5100元，等於追回93.4%的犯罪所得。其餘集團成員雖已離境潛逃，但經我國警方向國際刑警組織發出訊息後，各國也協助展開追緝行動，因而能在白俄羅斯逮捕車手頭巴比。亦因該集團成員首次被捕，羅馬尼亞、歐洲刑警組織、白俄羅斯、摩爾多瓦、泰國等國也來台進行相關案件的司法互助調查。

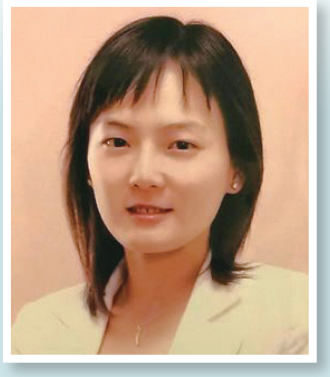
本案起訴後獲得臺北地方法院支持，對安德魯、潘可夫、米海爾均判處有期徒刑5年之重刑。上訴後經高等法院改判安德魯4年10月有期徒刑、潘可夫4年6月有期徒刑、米海爾4年8月有期徒刑。本案在2017年8月24日因最高法院駁回上訴而確定。

這個案件成功的追訴，為我國在國際刑事偵查領域寫下新的扉頁，並使各國追緝卡巴耐克駭客集團的僵局獲得突破，實為跨國司法互助的良好範例。（本專欄策畫／法律學系蔡英欣教授）

註：

[1] Jack 其後也關注糖尿病患者胰島素注射器以及心律調整器，他示範了遠距入侵個人胰島素注射器調高劑量，還有遠距入侵個人心律調整器，並使心律調整器產生電擊致人死傷。他希望生產這些儀器的公司能加強資安控管。

[2] 銀行使用有連接網路的儀器若有連接到銀行內部網路的就不能同時連接到外部網路，以免遭到駭客利用攻擊。



張安箴小檔案

民國 82 年畢業於臺大法律系，曾任立法院國會助理、月旦法學雜誌編輯、律師、苗栗地方法院學習司法官，現任臺北地檢署檢察官。

88 年取得美國賓州大學法學碩士、比較法學碩士，在美留學期間曾任賓州參議院參議員 Stewart Greenleaf 的法務助理，以及美國第三巡迴法院法官 Norma Shapiro 的法官助理。98 年取得輔仁大學口譯暨筆譯研究所文學碩士。

任職台北地檢署期間專辦智慧財產權案件、毒品案件、詐騙集團案件、婦幼案件、執行案件等，目前擔任公訴組重金庭專責檢察官，曾負責蒞庭中興銀行掏空案、國華人壽掏空案、幸福人壽掏空案等。