臺灣一銀 ATM 盜領事件對金融圈帶來最大的震撼就是，原本以為採用 SNA 封閉網路架構的 ATM，可以減緩駭客透過網路入侵的風險，但這次事件反應出這樣的 ATM 其實不安全

文/黃彥棻 | 2016-07-25 發表

第一銀行早在 2013 年下半年就已經評估要淘汰微軟 XP 的舊款 ATM，卻因為深信 ATM 採用封閉網路比較安全的資安迷思，加上預算排擠因素，延緩相關的 ATM 汰換進度。

圖片來源:

iThome

這次臺灣發生第一銀行 ATM 盜領 8,327 萬事件，對許多資安專家而言，發生這樣的資安事件並不稀奇，因為從 2013 年開始，一直到去年，從俄羅斯、東歐、歐洲等，都已經先後發生許多起這樣神乎奇技的 ATM 盜領事件。

先前資安公司推出類似的資安報告，像是荷蘭與俄羅斯資安研究公司 Group-IB 及 Fox-IT 在 2014 年聯合發表的資安報告《AnunAk：APT Against Financial Institutions》中，詳細揭露了這個俄羅斯黑幫集團，利用開源銀行木馬 Carberp，來客製化出專門攻擊銀行和支付系統的惡意程式 Anunak，專攻特定廠牌 Wincor（德利多富）ATM，可竄改銀行吐鈔上限，並可同時遠端遙控多達 52 臺 ATM 吐鈔來盜領金錢。此俄羅斯犯罪集團已經利用相同手法，不只偷遍俄羅斯，也橫行美國與歐洲多國的銀行。

到了 2015 年 2 月，卡巴斯基推出資安報告《Carbanak APT：The Great Bank Robbery》，根據這份報告統計，光在 2013 年晚期，這類 ATM 盜領造成的損失就已高達 10 億美元（約新臺幣 310 億元），其中受駭的銀行更遍布俄羅斯、美國、德國、中國或烏克蘭等。不過，這樣 ATM 盜領事件並不是每一起事件都可以盜領很多錢，像有單一銀行 ATM 損失就高達 730 萬美元（約新臺幣 2.26 億元），其他更多的損失往往是來自直接透過線上平臺轉帳帶來的損失，有銀行光是線上轉帳損失就超過 1 千萬美元（約新臺幣 3.1 億元）。

但即使這樣的 ATM 盜領案例層出不窮地在國際爆發，卻少見臺灣金融業者重視，反而是，像孟加拉央行被盜領的事件，臺灣金融業者關心程度還更高。綜合下來，其實源於幾個臺灣金融業者某些不夠落實、半調子的資安觀點，才導致臺灣的銀行業者缺乏對這類資安事件的心理準備。

迷思 1 臺灣 ATM 使用封閉網路，所以比較安全

所有臺灣的銀行業者，除非是採用 IP ATM 的銀行業者，全部都一致認為，許多臺灣 ATM 還是採用封閉 SNA（Systems Network Architecture）網路架構，ATM 直接透過 SNA 和後端帳務及客戶餘額主機連線，不僅網路傳輸時加密，也使用3DES與後端銀行主機做加密，加上 ATM 業者也會在 ATM 設備安裝防毒軟體強化其安全性。因此，多數銀行業者都會說，臺灣 ATM 使用封閉網路架構，所以比較安全。

事實上，真的如此嗎？一銀的狀況其實也是許多臺灣的銀行業者縮影，如果 ATM 真的是封閉網路，那光是 ATM 軟體升級，就必須透過 ATM 設備工程師，親自拿光碟或隨身碟，到每一臺 ATM 設備升級作業系統。

但是，從一銀的作業模式可以發現，該銀行其實已經有一套更新 ATM 軟體的派送伺服器，像是六月底，一銀更新 ATM 系統時，就是透過網路而非實體升級。

嚴格來說，銀行說的封閉網路只局限在兩個端點，ATM 連到後端帳戶系統，是採用 SNA 封閉的內網架構；ATM 更新伺服器和 ATM 設備，也是 SNA；但是，從外面派送的更新軟體內容到 ATM 更新伺服器時，看樣子就是透過網際網路升級，而非 SNA 封閉網路架構。其實，銀行業者定義的封閉網路並不完整，大部分都是指和後端帳務系統連網的網路架構，但是，更新派送的部份，終究不全然採用封閉網路架構。銀行是否還可以使用封閉網路的字眼，企圖混淆視聽呢？

迷思 2 XP 即使終止延伸支援，在封閉網路也安全

目前臺灣銀行業者 ATM 作業系統的主流，除了在 2013 年新採購的 ATM 多是內建微軟 Windows 7 以上的作業系統外，許多舊款的 ATM 大多採用在 2014 年 4 月 8 日就終止延伸支援的 Windows XP Professional（簡稱 XP)，以及在 2016 年 1 月 12 日終止延伸支援的 Windows XP Professional Embedded（簡稱嵌入式 XP）作業系統。

從一銀事件來看，目前有438 臺 ATM 採用微軟 XP 作業系統，只有 2013 年之後採購的 54 臺 ATM，是採用 Windows 7 作業系統。其實，第一銀行早在 2013 年下半年，就已經在評估，要汰換用了 7～10 年的老舊 ATM 設備。但是，為什麼一銀到現在還有過半以上的 ATM，仍使用微軟 XP 的老舊 ATM 呢？合理推論就是，即便是使用微軟 XP，但封閉網路會降低駭客透過網路入侵 ATM 的風險，難保一銀有許多已經超過 10 年使用期限的硬體 ATM 設備，在其他預算排擠效應下，遲遲無法升級或汰換。

早在 2 年多前，ATM 設備商 NCR 臺灣及香港區總經理區萬康便曾受訪指出，針對使用終止支援作業系統的銀行業者，應該要參考由信用卡公司提供的 PCI 規範。首先，建議使用終止支援作業系統的 ATM 設備，只允許白名單的應用連線，確保系統的完整性；其次，雖然不限時間，銀行必須要有清楚、合理的設備或產品升級計畫，以 ATM 使用工業主機通常可以耐用 7～10 年，超過 10 年不汰換，就是一個不合理的升級計畫。

從一銀事件看來，ATM 設備端並沒有只允許白名單應用連線；再者，推測一銀仍有超過 10 年未汰換的 ATM 設備，都讓自家 ATM 風險往上升。甚至於，我們也應該譴責，如果有任何業者的商用系統，還在使用微軟 XP 這種軟體孤兒，這些業者都不道德。

迷思 3 銀行資安稽核做得好，防駭能力一定好

有許多資安專家表示，臺灣金融業者的確是在資安設備採購上，投資最多金錢的產業，加上監理機關高度控管，不論是一年 N 次的內稽和外稽，都讓金融單位的資安像是銅牆鐵壁般的安全。

事實證明，臺灣金融業資訊部門花太多時間應付相關稽核，包含資安稽核，卻缺乏足夠的防駭思維，最明顯的例子就是，僅有少數金融機構有半獨立的資安部門；甚至僅有少數的金融業者，在銀行內有自己的資安事件處理團隊（IR Team）。

畢竟，目前也只有富邦金控有聘請專長打擊網路和科技犯罪的前警政署資訊室主任李相臣，擔任富邦金控資訊處長，負責相關的資安事宜而已，其他多數金融業者，仍把資安部門視為資訊部門的附屬品，更不會把資安能力視為提升公司營運能力的重要環節時，資安人員在銀行內無法出頭，更不用奢望有專門的資安團隊可以有心力鑽研怎麼防駭客，怎麼做好資安事件處理。

迷思 4 臺灣人不懂怎麼駭入 ATM，就比較安全

第一銀行董事長蔡慶年在 7 月 18 日的記者會上宣布，將要全數汰換舊款 Wincor Pro Cash 1500 的 ATM 設備，此時也有資安研究人員想協助了解是否有新手法的可能，但可惜是設備代理商不願意出借設備，並向銀行業者說明一旦出借，代理商將不會針對該銀行的 ATM 設備的漏洞進行升級、維修。

事實上，這臺設備已經可以在網路上購買，而且在俄羅斯還有許多中國的地下論壇，早就針對此次一銀受駭的 ATM 廠牌 Wincor，有專屬的發文專區，從最基本的操作說明、操作手冊、操作介面，甚至如何遠端入侵的攻擊手法等，形同是半公開在網路上，有心人士一定找得到。

從此類鴕鳥心態，以為只要臺灣人不懂如何攻擊 ATM，就表示臺灣不會發生這類 ATM 攻擊事件；到代理商惡劣自保心態等，都讓真正的資安技術交流地下化，最後的結果就是，當俄羅斯人、中國人知道怎麼攻擊 Wincor ATM 時，臺灣人因為不知道如何攻擊，更不懂得如何防護，只能作為刀俎上的魚肉，任人宰割罷了。

資料來源：iThome