【專題四】

淺析金融證券期貨業近期資安事件

葉琨煒（法務部調查局調查官）

壹、前言

近期金融證券暨期貨業者遭受資安攻擊事件頻傳，本文針對近期熱門之「密碼撞庫攻擊」及「偽冒網站或郵件詐騙攻擊」事件進行行為態樣分析，並自證券商端及客戶端分別探討資安攻擊之防禦策略及機制，期能避免此類資安攻擊之再次發生。

貳、密碼撞庫攻擊事件

近期數家證券商向主管機關通報遭受「密碼撞庫攻擊」事件。所謂「密碼撞庫攻擊」係指駭客自他處（例如暗網）取得民眾不慎外流的帳號和密碼，利用民眾使用共通密碼的習性，嘗試登入各大網站及手機應用程式（下稱 APP）。駭客成功登入網站或 APP 後即可非法獲取民眾的權限進行網站或 APP 操作。近期證券商遭受攻擊之事件即為駭客利用密碼撞庫攻擊手法，非法登入投資人之證券暨期貨帳戶，透過複委託功能下單購買香港交易所深藍科技控股股票（股票代號：1950）。

由於本次密碼撞庫攻擊事件受害之範圍既深且廣，而證券市場係我國資本市場的火車頭，其市場之資訊安全維護緊密連結著台灣未來資本市場的發展，為避免再次發生密

碼撞庫攻擊事件，故有深入研究密碼撞庫攻擊之手法及思考未來策應作為之必要。

一、密碼撞庫攻擊行為態樣分析

筆者就自身偵辦多起證券商遭受密碼撞庫攻擊事件之經驗，簡單歸納及分析密碼撞庫攻擊行為態樣如下：

（一）帳號密碼嘗試錯誤率高達一半以上：

由於駭客並非直接入侵證券商資料庫取得投資人帳號密碼，而係由暗網或其他來源取得民眾帳號密碼隨機進行密碼撞庫攻擊，因此密碼撞庫嘗試錯誤率甚高。此外，證券商下單 APP 預設係以身分證字號做為帳號並搭配使用者密碼進行登入，惟據筆者觀察，駭客在密碼撞庫攻擊使用之帳號列表除使用身分證字號外，亦有以電子郵件地址或英文名稱做為帳號，並無一定規則，故可研判駭客所使用之帳號密碼列表係由一至數個的外洩帳號及密碼來源之「大雜燴」所組成。

（二）駭客使用之攻擊來源 IP 位址涵蓋國內及境外：

經彙總分析密碼撞庫攻擊連線來源之 IP 位址，可發現駭客連線來源的 IP 位址除境外 IP 位址外，亦包含國內 IP 位址，深究其原因主係駭客為隱匿自身 IP 位址躲避追查，實案上可能向我國從事網路電信事業之二類電信業者租用 VPN 伺服器做為攻擊跳板使用，因此在證券商伺服器端會顯示來源 IP 位址為國內，藉以更好地偽裝為合法的使用者連線，降低密碼撞庫攻擊被發現的機會及拖延被系統偵測為異常的時間。

（三）來自相同來源 IP 之多帳號嘗試登入：

由於密碼撞庫攻擊事件的本質係以大量之隨機帳號密碼執行登入嘗試，為爭取攻擊時效，駭客常以自動化之工具嘗試密碼登入，密集以多個帳號進行帳號及密碼驗證，因此會出現短時間內自同一來源 IP 位址嘗試登入多個帳號之異常態樣，而與正常投資人之登入行為（即不同帳號來自不同 IP 位址）有所區別。

（四）攻擊證券商之來源 IP 具有共通性：

駭客不僅針對單一證券商進行密碼撞庫攻擊，據筆者觀察，多家證券商

於 110 年 11 月下旬同時遭受密碼撞庫攻擊，且各證券商受攻擊之來源 IP 位址具有共通性，研判為同一駭客集團同時（或於相近的時間）對數個證券商網站或 APP 發動密碼撞庫攻擊。如圖 1 所例，駭客以所持之外洩帳密 A,B,C 同時（或於相近的時間）對甲、乙、丙證券商發動密碼撞庫攻擊，故其攻擊來源 IP 均顯示為同一駭客連線 IP 位址 x.x.x.x，而具有共通性。

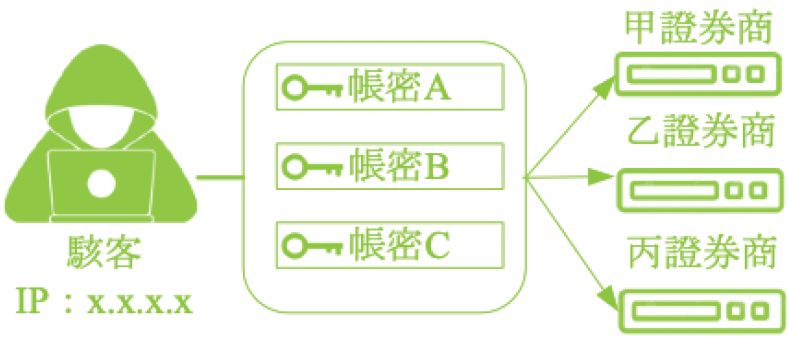

圖 1　密碼撞庫攻擊之示意圖

二、防止密碼撞庫攻擊之用戶端防禦機制

在網路普及的時代，密碼撞庫攻擊將隨之增加，為防止再次發生密碼撞庫攻擊導致投資人證券帳戶遭盜用，金融監督管理委員會（下稱：金管會）於 110 年 12 月 14 日發布新聞稿，提醒民眾應妥善保管證券期貨網路下單之帳號密碼，呼籲自用戶端提升資訊安全，此外並責成臺灣證券交易所（下稱：證交所）及臺灣期貨交易所督導證券商及期貨商強化 3 項措施，以維投資人權益，茲列舉如次：

（一）提供網路下單服務之證券商，應於網路下單登入時落實採多因子認證方式，確認為本人登入：

所謂「多因子認證方式」係指除帳號密碼以外，需輔以可鑑別使用者身分之其他方式，包含下單憑證、綁定裝置、一次性密碼（OTP）及生物辨識等機制。由於密碼撞庫攻擊駭客所知悉者僅投資人之帳號密碼，因此多因子認證方式可有效防止駭客僅憑帳號密碼即入侵使用者帳戶。

（二）加強宣導客戶應使用優質密碼設定及定期更新使用者密碼：

使用複雜度高的密碼能避免投資人的密碼遭駭客暴力破解，加強宣導客戶更新密碼則可降低密碼撞庫攻擊的成功率，惟密碼撞庫攻擊成功的本質在於利用密碼的共通性，故如客戶於外洩來源使用相同的帳號密碼，縱然密碼

複雜度夠高，則仍可能遭駭客撞庫成功。至於加強宣導客戶定期更新密碼，如客戶存僥倖心態不予定期變更，恐難以達成降低密碼撞庫攻擊的成功率。

（三）證券期貨商應分析異常的登入原因、異常 IP 位址登入時通知投資人：

當證券期貨商發現有異常嘗試登入的情形時，即時通知投資人注意異常情況，俾利投資人採取更改密碼等防禦作為，有助於保障投資人帳戶安全，惟如投資人怠於採取積極作為，即可能錯失防禦密碼撞庫攻擊之時機。

三、密碼撞庫攻擊整體防禦暨情資橫向流通計劃

綜上觀之，現行在針對密碼撞庫攻擊事件的防範仍限於用戶端防禦機制，然如果僅依賴用戶端防禦機制，恐受限於用戶端之執行程度，致無法將其發揮至最大成效，故筆者認為亦可建置證券商端防禦機制，並結合前述之用戶端防禦機制，完善整體資本市場之資安防護網。

經瞭解，現行證券市場如有委託人不如期履行交割義務時，證券商應依臺灣證券交易所股份有限公司證券經紀商申報委託人遲延交割及違約案件處理作業要點向證交所申報違約，證交所接獲證券商違約申報後將其內容轉知其他證券商，並將相關違約資訊上傳聯合徵信平台，供同業及異業即時瞭解投資人信用狀況，有效控管投資人信用風險。

筆者參考上述證券實務上違約風險管控之作法，建議將密碼撞庫攻擊的情資透過金融資安資訊分享與分析中心（F-ISAC）之情資分享平台進行橫向，達成跨證券商及跨業之橫向資安聯合防禦機制，以收最大之綜效。茲就本文提出之密碼撞庫攻擊整體防禦暨情資分享計劃說明如下：

（一）證券商端防禦機制：

針對前述密碼撞庫攻擊行為所可能產生之異常連線態樣，筆者建議各證券商應建立系統警示機制，具體做法可參考本文第貳章節態樣分析一及三，建立如「同一來源 IP 位址之多帳號嘗試登入失敗」之警示規則，如發現符合警示規則之異常事件，透過 SIEM 於第一時間內，通報資安管理人員。所謂 SIEM，全名為 Security Information and Event Management（安全資訊事件管理系統），其主要功能在於透過分析系統紀錄（Log），識別反常的網路行為，並發出異常告警通知資訊人員。資安人員可將前述警示規則導入 SIEM 系統，SIEM 即可不間斷地分析使用者連線紀錄，透過此方式自動化

監控是否有符合警示規則的異常網路行為產生，如識別出異常事件，即可適時將異常情形以電子郵件或簡訊通報資安人員，由資安人員進行確認後，對異常來源 IP 位址進行阻斷，以此方式即可自動化防禦流程，降低資訊人員之負擔，也可針對可疑之密碼撞庫攻擊行為做出即時的反應及處理。此外，警示規則參數臨界值（例如單一 IP 位址嘗試登入失敗之帳號數量）宜衡酌各證券商實際日常連線狀況妥為設定，以降低 SIEM 系統誤判率。

（二）跨證券商暨跨業之密碼撞庫攻擊情資分享：

有鑒於前述遭受密碼撞庫攻擊之證券商，其攻擊 IP 的來源位址具有共通性，爰筆者建議借鏡證交所對全市場通報投資人違約交割暨於聯合徵信平台公告違約供異業風險控管之做法，透過現有之 F-ISAC 之情資分享平台供證券商分享密碼撞庫攻擊 IP 情資，具體流程詳如圖 2。

當某甲證券商透過內部 SIEM 系統確認發生密碼撞庫攻擊時（流程 1），可透過程式介接或以人工方式，上傳密碼撞庫攻擊 IP 位址情資至 F-ISAC 情資分享平台（流程 2），F-ISAC 情資分享平台收到情資後，再將攻擊 IP 位址之情資即時分送各平台會員（流程 3），各證券商收到密碼撞庫攻擊 IP 位址情資後，便可即時比對自家網站或 APP 系統是否有來自相同 IP 位址之可疑密碼撞庫行為，如有發現即可即時進行阻斷，若暫無發現亦可將獲通報之 IP 設為可疑黑名單，防範可能發生之下一波密碼撞庫攻擊。

透過以上的情資分享方式，當某證券商遭受密碼撞庫攻擊時，可即時將攻擊 IP 位址情資分享給其他證券商或其他金融業者進行預警，進行密碼撞庫攻擊的聯合防禦，達成跨證券商及跨業之資安橫向防護，降低密碼撞庫攻擊波及之範圍及減少客戶之災損。

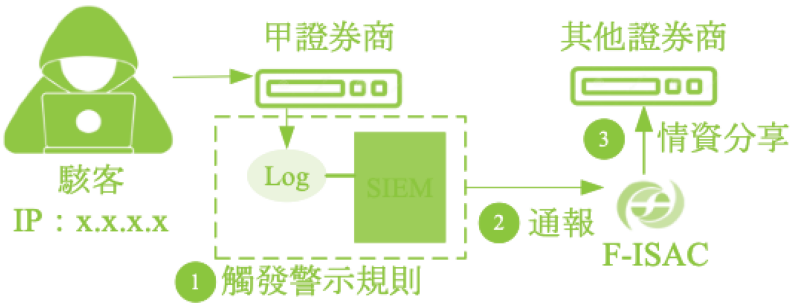

圖 2　密碼撞庫攻擊整體防禦暨情資分享計劃架構圖

參、偽冒網站或郵件詐騙攻擊

除了前面提到的密碼撞庫攻擊外，駭客另一種常見的攻擊手法係利用民眾普遍欠缺資安意識的弱點，製作假可亂真的釣魚網站與釣魚郵件，誘騙民眾點選網站或郵件中的連結，輸入其帳號密碼，藉此方式取得民眾的帳號密碼資訊，進一步入侵至民眾證券帳戶或網路銀行，冒用民眾身分進行下單，或甚至將財產移轉，造成民眾經濟上之損失，此種攻擊手法稱為偽冒網站或郵件詐騙攻擊。

一、近期偽冒網站或郵件詐騙攻擊案例分享

圖 3 是近期民眾受到釣魚簡訊詐騙的一則新聞案例，110 年間國泰世華銀行的多名用戶收到了一封詐騙簡訊，謊騙用戶的帳戶出現異常而將遭到凍結，並要求立即點選簡訊中的下方「www.cathay-bk.com」的連結，該連結點擊後出現如圖 4（左）的詐騙網站，多名用戶輸入身分證字號、用戶代號及網銀密碼後，輸入的個資即會被駭客所蒐集，短短 3 天內駭客集團取得了 21 人個資及盜領 300 萬元新台幣之「豐碩戰果」。

圖 3　假國泰世華帳戶凍結簡訊案例。（取材自蘋果新聞）

二、駭客攻擊手法解析

自前述案例，可以發現駭客慣用的詐騙手法係先以詐騙簡訊或電子郵件方式發送釣魚連結，傳送至被害人手機後，以聳動的標題（如：帳戶即將被凍結）或利誘的方式（如：給予優惠點數），騙取被害人點擊釣魚連結，將被害人引導至駭客集團所預先設計好的釣魚網站，由於釣魚網站外觀幾乎與官方網站頁面無異，被害人往往不疑有他而輸入自身的個資、帳號及密碼等，掉入駭客集團所布置好的陷阱。駭客集團藉此方式蒐

集民眾個資、取得被害人網銀帳密後，即可冒用被害人身分登入網路銀行，將被害人網路銀行下的款項轉帳至駭客所控制的人頭帳戶，進而取得贓款，此時當被害人發現受騙上當時，往往款項已經被駭客轉出帳戶，此時再想追回款項已經為時已晚。駭客詐騙手法流程詳見圖 4（右）。

圖 4　國泰世華詐騙網站與駭客詐騙取財流程。（取材自 IT home 網路新聞）

三、客戶端防範駭客攻擊的策略

針對上述駭客攻擊的手法，一般客戶應該如何擬定防範策略呢？筆者認為不妨從圖 4 右方的駭客攻擊手法的流程進行思考。首先，駭客散布釣魚連結的方式，依照筆者辦案的經驗，十之八九係經由電子郵件或是簡訊，因為這兩種媒介對駭客集團來說經濟效益最高，花費最少，且可以達到廣布於眾的目的，這可比向 Google 買廣告「宣傳」其釣魚網站要便宜許多，且能低調較不易被發現。因此建議一般投資人收到電子郵件或是簡訊時，都必須保持高度的警覺，尤其是來自陌生來源的電子郵件或簡訊，務必仔細的查驗（查驗的方式請詳下章節）。

其次，當投資人收到可疑的電子郵件或簡訊時，關鍵在於請勿點擊電子郵件或簡訊中的連結，因為單純的閱覽電子郵件或簡訊內容並不會造成手機被駭侵，但當民眾誤信電子郵件或簡訊的內容為真，而點擊內容中的連結時，這才是真正手機受駭的關鍵。復以圖 3 為例，單純的打開簡訊並閱覽有關帳戶凍結的內容並不會造成手機被駭客入侵，真正會造成手機被駭的起點，應是自民眾誤信該帳戶凍結的內容為真，實際點擊「www.cathay-bk.com」的連結而輸入其網路銀行帳號密碼開始。

承前述，當民眾不慎已經點擊了釣魚連結，是否即代表手機已經在駭客的控制之中？答案應為否定。因為在本局偵辦的過往案例中，當民眾點擊釣魚連結後，大致會有兩種情況。第一種：駭客在釣魚連結中暗藏木馬程式，當被害人點擊釣魚連結後，手機會提示是否下載執行該木馬程式，此時如果民眾有所警覺，即可拒絕該木馬程式的執行並刪除已經下載的木馬程式，而順利地自駭客所佈下的陷阱中「脫逃」。第二種：當被害人點擊釣魚連結後，會將被害人引導至駭客集團精心設計的偽冒網站，誘使民眾在偽冒網站中輸入個資，此種攻擊方式意在取得民眾的個資，騙取民眾主動輸入，而不需要另外設計木馬程式讓使用者下載，相對於第一種方式，駭客集團會比較省工，也較不會因為需另外下載木馬程式而觸發被害人的警覺。回到國泰世華銀行的案例中，當被害人點擊前揭惡意連結後，會被引導至駭客集團模仿國泰世華網路銀行 APP 所製作的假網頁，誘使使用者輸入其網銀帳密，此種攻擊手法屬於筆者前述的第二種情況，由於駭客集團意在騙取個資，在假網頁中夾藏惡意程式的機會較低，如果此時民眾有所警覺，不要輸入網銀帳號密碼，旋即退出該釣魚網頁，民眾的個資即不會有外洩或手機遭駭客控制的情形。

最後，當民眾未察覺而於釣魚網站輸入其帳號密碼時，此時應如何處理？筆者建議應立即更換網銀密碼，此外，投資人使用之其他手機應用服務，例如手機證券期貨下單 APP 等，如果使用與網銀相同密碼者，亦應一併更換。惟實案上，多數民眾直至網路銀行款項遭駭客盜領收到簡訊通知才驚覺受駭。遇此情況，筆者建議應循「金融機構辦理警示帳戶聯防機制作業程序」，親自前往開戶銀行櫃台告知遭詐騙，經金融機構櫃檯人員確認身分及瞭解被詐騙事由後，由民眾填寫切結書並撥打 165 反詐騙報案電話通知警方，開戶銀行會協助將「警示帳戶通報單」傳真至受款銀行通報窗口，受駭民眾隨後應向警察機關報案完畢。

四、釣魚連結及網站的查驗方式

承前述，筆者實不建議投資人直接點擊電子郵件或是簡訊內容中的連結進入網路銀行介面或是證券登入頁面。此時，較安全的方式應係查詢官方網站，並從官網網站首頁進行登入，或是經由官方提供之 APP 進行登入。或有投資人認為一概不點擊電子郵件或是簡訊內容中的連結似乎有些本末倒置，是否有一些可以用以查驗網站是否是「正牌貨」還是「冒牌貨」的方法呢？答案是有的，以下就聽筆者娓娓道來～

在網路的世界中，網站會有一組 IP 位址，使用者可以透過 IP 位址來找到對應的網站，換句話說，IP 位址形同於真實世界中的門牌號碼，不過 IP 位址係以小數點相隔的

4 組數字組成（例如：218.32.90.68），實在太難記憶了，為了讓網站瀏覽者更好記，就產生了「網域」的概念，有了網域，網站瀏覽者就不需要再記憶 IP 位址，只要在網址列輸入網域，就可以找到對應的網站。以國泰世華銀行官方網站為例，其網站 IP 位址為：218.32.90.68，網域名為「www.cathaybk.com.tw」。相較 IP 位址而言，網域名稱是不是好記很多呢。值得一提的是，網域有一定的組成規則，由右至左分別為頂級域（Top-Level Domain, TLD）、次級網域（Second-Level Domain, SLD）及子網域（Sub Domain）。頂級域為網域中最高層級的組成，大家所熟知的「.tw」、「.com」及「com.tw」均屬頂級域。前述國泰世華銀行網域「www.cathaybk.com.tw」所屬頂級域即為「com.tw」。頂級域由特定域名管理機構所管理，並有權力發放次級網域給申請者。目前台灣網域即是由財團法人台灣網路資訊中心（TWNIC）所管理，但目前因應國內商業網路的發展，TWNIC 已開放部分民間公司（主要為 ISP 業者，例如中華電信）代理發放次級網域給申請者，因此獲得 TWNIC 授權的民間公司亦有發放次級網域的權力。而所謂次級網域，即是網域申請者向域名管理機構所申請使用的「註冊名稱」，概念上如同公司在網路世界的註冊商標，為讓網站瀏覽者可以加深記憶，常見會使用公司的英文縮寫做為註冊名稱。在「www.cathaybk.com.tw」的網域中，「cathaybk」即為國泰世華銀行所申請的次級網域。最後，在「www.cathaybk.com.tw」中最左方的「www」係網域持有者可自行設定的服務名稱，俗稱為子網域，不需向域名管理機構申請。

因此，要判斷網路連結是否為釣魚網址，可以查驗網路連結的域名是否正確，其中又以頂網域及次級網域的比對最為關鍵。圖 5 顯示國泰世華銀行網域與詐騙網域「www.cathay-bk.com」之比較。就頂網域部分，詐騙網域之頂網域為「.com」，與國泰世華銀行網域之頂網域「com.tw」並不相同。另就次級網域部分，詐騙網域之次級網域為「cathay-bk」，與國泰世華銀行網域之次級網域「cathaybk」亦不相同，且詐騙網域的次級網域與國泰世華銀行所使用的次級網域高度雷同，容易造成使用者的混淆，惟如被害人具有警覺性及查驗網域異同的能力，仍應能發覺兩者之不同。

末就釣魚網頁的查驗方式，則幾乎與釣魚連結的查驗方式相同，最可靠的方式仍為查驗網頁上方的網址列，判斷網址中所顯示的網域是否正確，千萬不可「眼見為憑」，單以頁面的相似程度進行判斷，因為以目前的網站製作技術，僅需參考官方網站的網頁框架，即可製作出以假亂真的釣魚網頁，因此筆者建議如要判斷網站的真偽，查驗網域仍然是最佳的不二法門。

圖 5　釣魚詐騙網域查驗方法

五、證券商端防禦機制

根據筆者的經驗，由於投資人普遍資安意識仍有不足，如僅從客戶端防範偽冒網站或郵件詐騙攻擊，恐無法根本杜絕此類攻擊造成的危害，因此仍仰賴證券商端偕同客戶端進行防禦，目前證券商或金融機構對於偽冒之釣魚網站多採取網路宣導的方式提醒投資人注意。除此之外，筆者建議證券商或金融機構得透過 FISAC 或司法偵查機關積極向財團法人台灣網路資訊中心（TWNIC）請求下架釣魚網站，避免投資人誤入釣魚網站。

肆、結語

未來 10 年新興科技將帶來更深的資安威脅，在後疫情時代，普羅大眾對數位化需求有增無減，然而享受科技的同時，資訊安全是不可不重視的議題。由於資本市場為國家經濟發展之櫥窗，為維持經濟的穩定發展，金融業的的資安議題更是重中之重。

近期證券商網站及 APP 系統之密碼撞庫攻擊已成為駭客入侵投資人證券帳戶之主要攻擊手法之一，現行金管會已針對密碼撞庫攻擊之用戶端防禦機制建立相關機制，然用戶端防禦機制仍需仰賴用戶之積極作為，為完善整體金融環境之資安防護，建議建置證券商端之防禦機制，並結合前述之用戶端防禦機制，以期達成跨證券商暨跨業的聯合資安防禦，降低密碼撞庫攻擊波及之範圍及減少客戶之災損，打造一個資安無虞的金融環境。

此外，面對數位科技的蓬勃發展，現代人依靠手機完成日常生活起居已成不可逆的趨勢，駭客已經逐漸將資安攻擊重心轉往個人的手持裝置，並利用一般民眾普遍欠缺資安意識的弱點，以簡訊或電子郵件各類傳輸媒介，向民眾發送惡意連結，竊取民眾個資

進而入侵手持裝置中的各類電子下單及電子支付工具盜取款項，造成民眾鉅額的經濟上損失。面對日益嚴峻的個人資安威脅，客戶端應提升資安的防護意識，多一份小心，面對可疑的簡訊或電子郵件，應盡量避免點擊內容的連結，選擇自官方網站登入，會是較為安全的選擇。對於造訪的網站，應仔細查驗網站的網域是否正確。惟有建立正確的資安觀念，才能防護好個人的資訊安全，不讓駭客有可趁之機。證券商端除多向投資人宣導資安概念及公布偽冒網站資訊外，亦得積極尋求下架偽冒網站的管道，避免其投資人誤入釣魚網站。