近期國際駭客入侵事件樣態及資安防護注意事項

一、 近期國際駭客入侵事件： 108.1.3

發布日期	資安威脅分析報告	說明
107/12/26	F-ISAC 資安威脅分析報告(60)-PandaBanker 惡意程式分析	資安公司Cylance於2018年10月9日發布研究報告，內容包含駭客組織利用Panda Banker惡意程式，攻擊美國、加拿大及日本的金融機構用戶。 報告指出當受害者瀏覽特定金融機構網頁時，於瀏覽器中注入惡意腳本，目的為竊取受害者機敏資料，如銀行帳戶、信用卡與網路錢包資訊等。
107/10/30	F-ISAC 資安威脅分析報告(35)-會員分享利用 IQY 進行社交工程攻擊案例	近期F-ISAC會員分享郵件防護系統攔截到的夾帶附檔可疑郵件，經分析攻擊手法，與今（2018)年8月資安設備廠商「proofpoint」發布「Marap」惡意程式攻擊活動報告相似。 本案係透過社交工程發送釣魚郵件夾帶附檔，附檔格式為 PDF 檔案內嵌「.iqy（Microsoft Excel Web Query）」，觸發後會執行 Power Shell 連線至惡意中繼站下載惡意程式，蒐集主機及受害者金融相關資訊後，透過中繼站伺服器（Command and Control，簡稱 C&C）傳出，以利駭客進行入侵，造成受害者損失。
107/10/15	F-ISAC 資安威脅分析報告(31)-會員分享「利用 Microsoft Publisher 附檔進行社交工程攻擊」分析	F-ISAC 會員分享兩封可疑郵件，經初步分析為「偽冒」外部公司、公司內部使用者及相同之網域，以進行社交工程攻擊。本次夾帶的附檔格式為「MS Publisher」，與一般常見的手法不同，主要目的是避開資安設備攔阻，以增加入侵成功機率。
107/10/8	F-ISAC 資安威脅分析報告(29)-北韓惡意網路活動-HIDDEN COBRA-FASTCash	依據美國電腦網路緊急應變中心（United States Computer Emergency Readiness Team，簡稱 US-CERT）於美國時間 2018 年 10 月 2 日發布之「北韓

		惡意網路活動」。公告指稱,「FASTCash」為北韓政府用來攻擊特定金融機構ATM 系統的手法代號，且可歸類於「HIDDEN COBRA」活動。 「FASTCash」可歸類於 ATM 盜領(ATM Cash-out)攻擊手法，犯罪組織利用偽冒的磁條卡，針對特定金融機構帳戶於本地或遠端 ATM 進行盜領，且能繞過既有的控管或提領限制，在短時間內大規模盜領，最終造成金融機構重大損失。
107/8/22	F-ISAC 資安威脅分析報告(24)- 印度 ATM 盜領及 SWIFT 盜轉事件	英國路透社(Reuters)於 2018 年 8 月 14 日報導印度 Cosmos 銀行遭駭[1]，駭客在 8 月 11 日(週六)分別於全球二十多個國家，透過自動櫃員機(ATM)進行 14,849 筆交易，盜領金額總計達 8.05 億盧比，另有 1.39 億盧比則是透過 SWIFT 系統轉 帳到香港公司，該行整體損失高達 9.44 億盧比。
107/8/22	F-ISAC 資安威脅分析報告(23)-美國聯邦調查局(FBI)發布 ATM 盜領警報	美國聯邦調查局（Federal Bureau of Investigation，簡稱 FBI)發布「ATM 盜領告警訊息」，內容主要說明 FBI 警告金融犯罪集團近期可能對銀行或支付卡處理中心發動 (ATM cash-out) 攻擊，利用偽冒磁條卡片，在短時間內進行大規模的盜領。

詳細資料可參考 F-ISAC 發布日期所發布(或編號)之資安威脅情資。

二、 綜合研析與防護建議

國際駭客組織常見手法係利用社交工程及資通系統重大漏洞，針對金融機構進行入侵作業，並利用惡意 Windows 執行檔、Command-Line 應用程式及其他檔案以網路探測金融機構重要營運系統（如 ATM、SWIFT、網路下單及客戶資料庫等），並竊取系統或主機敏感資訊再內網橫向移動，進而非法的登入重要營運系統，進行大規模盜領、SWIFT 盜轉、下單系統加密勒索及竊取客戶資料庫於暗網市場販售等行為，最終導致金融機構重大損失。建議加強資安防護措施如下：

(一) 定期檢視並監控特權帳號之活動。

(二) 定期針對管控機制進行驗證作業，確保機制正常運作且有效。

(三) 監控交易系統是否有異常行為（如嘗試同時間多點登入或是非上班時間嘗試登入）。

(四) 監控系統是否有異常之執行程序，或建立應用程式白名單，防止惡意程式之執行。

(五) 強化系統介接之安全防護或監控機制，防止因中間人攻擊造成之交易偽冒或竄改。

(六) 強化管理者帳戶之認證機制，強化密碼強度或採用雙因素認證。

(七) 監控是否有對外之異常連線，或建立連線白名單。

(八) 建立防毒閘道，過濾郵件附件或網路下載內容。

(九) 定期進行弱點掃描，並依風險評估等級，及時更新或修補系統漏洞。

(十) 定期進行社交工程演練，強化人員資安意識。

(十一) 訂定事件應變處理計畫，落實事件管理機制，以強化網路資安事件處理時效。

三、 春節期間注意事項

(一) 原則禁止遠端連線，禁止由外部連線至銀行內部營運區進行系統維護作業，若真有緊急需要，應加強監控管理，例如：身分驗證、授權人工確認等。

(二) 加強各類異常情形之監控，包括資訊系統異動、防毒防駭事件警訊、internet 存取紀錄、派版軟體及病毒碼更新設備等之監控處置。

(三) 加強高風險交易之管控，如啟動人工覆核或確認機制等。

(四) 評估關閉連假期間無須運作之資訊設備或系統。

(五) 加強資安防護，設置緊急聯絡窗口，發生重大資安事件，依通報規定進行通報。