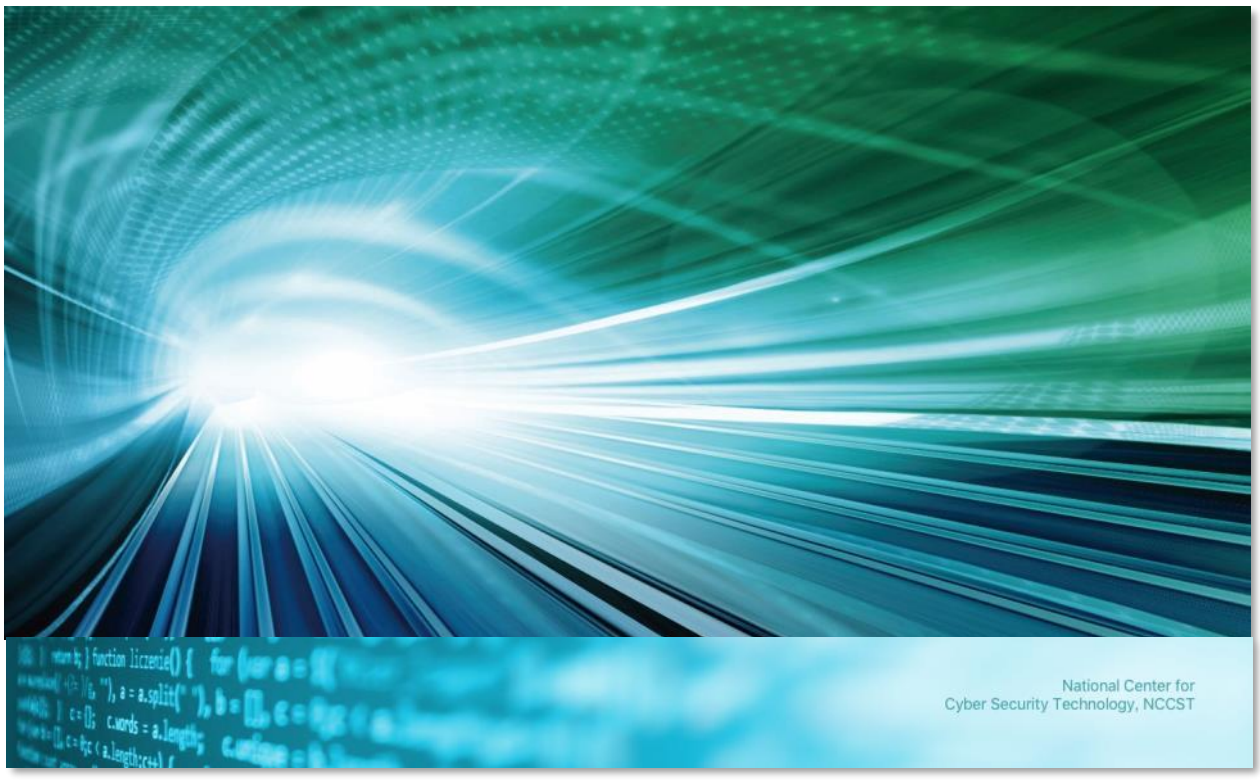
108年第3季資通安全技術報告

Quarterly Technical Report



目　次

圖 目 次

摘要

「第 3 季資通安全技術報告」除分析本季全球資安威脅、政府通報之資安事件外，並提供相對應之防護建議。同時，藉由資安專題之分享與資安技術之研析，提供政府機關(構)於資安風險的關注重點。

「第 3 季資通安全技術報告」分為以下 4 個章節。

●1.資安威脅現況與防護重點

從分析全球資安威脅現況開始，第 1 起案例探討行動支付之程式設計不當與資安缺陷；另一起案例為駭客利用物聯網裝置入侵企業網路。

分析政府資安威脅現況，發現政府機關(構)通報事件原因以「非法入侵」(占 33.52%)類型為主，「網頁攻擊」(占 26.65%)次之。

●2.資安專題分享

研析 FIDO2 (Fast IDentity Online 2)身分認證協議，藉由此議題討論逐漸降低對密碼過度依賴的可能性，另一方面，亦能提供創新的身分認證方式，以降低對密碼管理的成本與負擔。

●3.資安技術研析

本季主題為探討與說明韓國金融詐騙調查分析事件之詐騙經過與後續防範措施，以及惡意程式 Calling Interceptor 下載站偽裝成合法下載頁面，讓使用者在沒有察覺情況下受駭。

●4.結論

本報告透過分析全球與政府之資安事件與統計數據，了解最新資安威脅趨勢與因應之防護重點。資安專題分享 FIDO2 身分認證協議，透過 FIDO2 無密碼化認證技術，將對資安強化有一定成效。此外，透過資安

技術的研析，深入探討惡意程式 Calling Interceptor 下載站偽裝成合法下載頁面，造成韓國金融詐騙資安事件發生，後續防範措施亦可做為後續資安宣導重點。

1. 資安威脅現況與防護重點

本報告藉由檢視當季國內外所發生之資安事件或議題，研析事件發生之主要原因與可能之衝擊與影響。第 3 季(以下簡稱本季)觀測到隨著資通訊科技應用的便利，衍生出貿然使用創新科技，如區塊鏈、行動支付、人工智慧及物聯網(Internet of Things, IoT)等，卻未妥適準備相關資安防護作業。資通訊科技的應用，引領著創新應用與未來趨勢潮流，但潛藏在科技應用背後，可能造成重大衝擊的資安威脅與風險，更應備妥相關因應方案。

在所有資安防範議題中，密碼設定與管理已成為普世價值，但分析政府機關(構)資安事件，使用弱密碼或預設密碼，依然高居駭客成功入侵原因的前 3 名。本章節的事件與議題皆配合整理相關之防護重點，提供組織就相關資安風險或議題進行評估，並依循防護重點進行強化。

1.1 全球資安威脅現況

資通訊科技的進步與隨著網際網路發展而來的各項應用，正逐步改變資安威脅的面向，駭客除使用傳統手法利用系統漏洞或不安全之組態設定進行攻擊外，亦利用科技應用，如行動支付與 IoT 設備等啟動相關入侵行為。

以行動支付發展為例，行政院將 107 年定位為「行動支付」元年，目標是 114 年電子支付普及率能達到 90%。為達成行動支付普及，必須擴大整合支付工具，同時配合相關法規與政策，創造更多應用場域，提供民眾更多資通安全與個資保護之確保，以提高相關參與率。隨著 IoT 設備的廣泛應用，所要考量的攻擊面向，亦包含應用服務、作業系統、硬體(韌體)設備及無線傳輸等相關資安議題。

本季具指標性的案例，將研析行動支付之程式設計不當與資安缺陷；另一起案例為駭客利用 IoT 裝置入侵企業網路。

首先，探討案例為日本 7-11 手機支付 APP 被駭事件，肇因為行動支付之

程式設計不當與資安缺陷。日本 7-11 於 108 年 7 月 1 日推出支付 APP 7pay，傳出駭客利用該 APP 設計不嚴謹缺陷進行攻擊，導致消費者帳號被竊，並盜刷帳號內綁定之銀行支付資訊，消費者銀行帳戶等個資皆存在 7iD 帳號中。自 7 月 3 日起，有多名日本消費者透過推特(Twitter)表示，自身 7pay 密碼遭人竄改後信用卡被盜刷，7-11 接獲消息後隨即緊急暫停 7pay 會員申請機制與支付功能。據日本媒體報導，截至 7 月 4 日，已約有 900 人受害，損失金額約為 5,500 萬日幣。

經初步調查，本次事件基本上是該 APP 存在 2 個明顯問題所導致。第一個問題是用戶註冊時之身分驗證機制，在 iOS 系統開啟 7pay App 要註冊 7iD 會員時，出現用戶只需輸入第一項電子郵件信箱資訊，在沒有輸入其他資料選項情形下，依然可執行下一步，且系統還自動預設以 108 年 1 月 1 日做為生日，並在 APP 會員資料介面說明提到有此預設機制。Android 系統則沒有這個問題，需填寫所有欄位才能繼續。

第二個問題則是密碼重設時，電子郵件信箱輸入驗證機制。7pay App「忘記密碼」申請介面上，僅要求輸入生日與 7iD，且可輸入任意電子郵件信箱來接收重設密碼信。該系統並未比對所輸入之重設密碼電子郵件信箱，與原設 7iD 會員帳號電子郵件信箱是否相同，且因預設生日為 108 年 1 月 1 日機制，更大幅降低猜測難度，使駭客更容易得逞。此 APP 系統之資安設計缺陷包含重設會員密碼或註冊過程，均未搭配 2 階段驗證機制，當重設輸入不同電子郵件信箱時，也無額外驗證機制。

第 2 起案例為俄國駭客利用 IoT 裝置入侵企業網路。微軟(Microsoft)官方部落格於 8 月 5 日指出，有駭客組織正在利用印表機與 Voice over IP (以下簡稱 VoIP)網路電話等企業 IoT 設備，伺機對企業網路發動攻擊。微軟威脅情報中心(Microsoft Threat Intelligence Center, MSTIC)研究人員於 4 月間發現 3 起攻擊行動，駭客連上多台 VoIP 電話、辦公室印表機及影片解碼

裝置，經分析後發現攻擊者企圖利用這些裝置駭入企業網路。其中 2 次攻擊是利用 IoT 裝置的預設密碼，另外一次則是因為裝置韌體未升級到最新版本，而讓駭客有機可乘。研究人員認為，入侵 IoT 裝置之目的，是在企業網路上建立據點，做為未來發動攻擊準備。駭客成功入侵 IoT 裝置後，會執行 tcpdump 軟體來聽取企業子網路的封包流量與內容，並讓裝置與外部中繼站建立連線。攻擊者還會特別列舉管理群組，以便未來發動進一步攻擊。當攻擊者由一台裝置移動到另一台時，均會放置執行遠端控制的 shell script，以便日後持續控制所有接觸過的裝置。

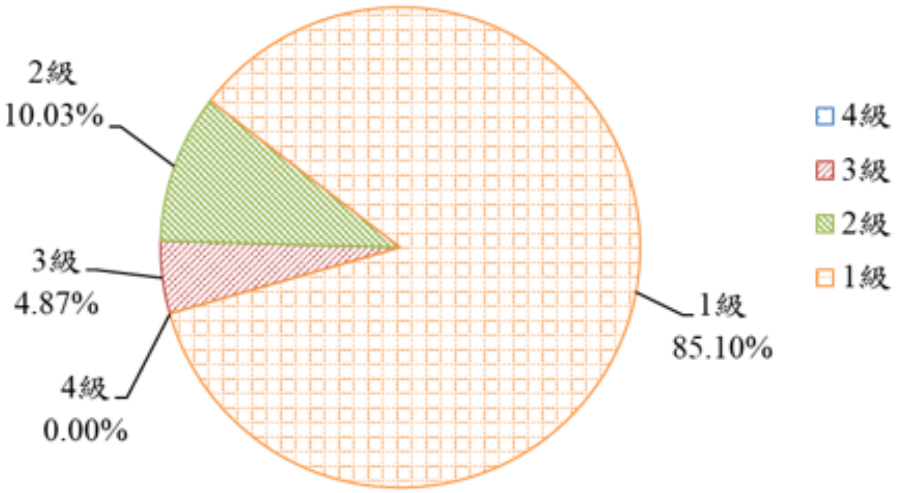
由於上述 3 起攻擊都在初期就被發現，因此尚無法判斷駭客最終目標為何。但微軟判斷這 3 起攻擊均源自一個名為 Strontium 的駭客組織，另一知名的稱號是 Fancy Bear 或 APT 28，是俄羅斯政府所資助之駭客組織。微軟在過去一年，就發出將近 1,400 次與該組織有關的國家級駭客攻擊行動警訊，其中 20%目標為全球非政府組織、智庫或政治團體，其餘 80%攻擊對象包含政府、IT、軍事、國防、醫療、教育及製造產業等。

綜覽本季重大資安事件，駭客鎖定推出行動支付的業者，迅速展開攻擊，最終迫使企業宣告終止使用行動支付 APP 功能。據媒體報導，其競爭者也因上次事件居間獲利，趁勢取得大量新會員。IoT 裝置的盛行，代表日後資安威脅將存在生活中的每一個角落，在使用相關 IoT 設備的便利性時，更應考量到可能發生的資安風險與衝擊。

1.2 政府資安威脅現況

彙整本季所接獲之政府機關(構)通報事件，藉由事件之影響等級、通報類型及事件原因，了解目前政府機關(構)之資安威脅現況。通報事件依資安事件對「機密性」、「完整性」、「可用性」3 個面向所造成的衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級資安事件。彙整事件影響等級，本季以 1 級事件占 85.1%為大宗，2 級事件占 10.03%次之，3

級事件僅占 4.87%，而 4 級資安事件則未發生，相關統計情形詳見圖 1。

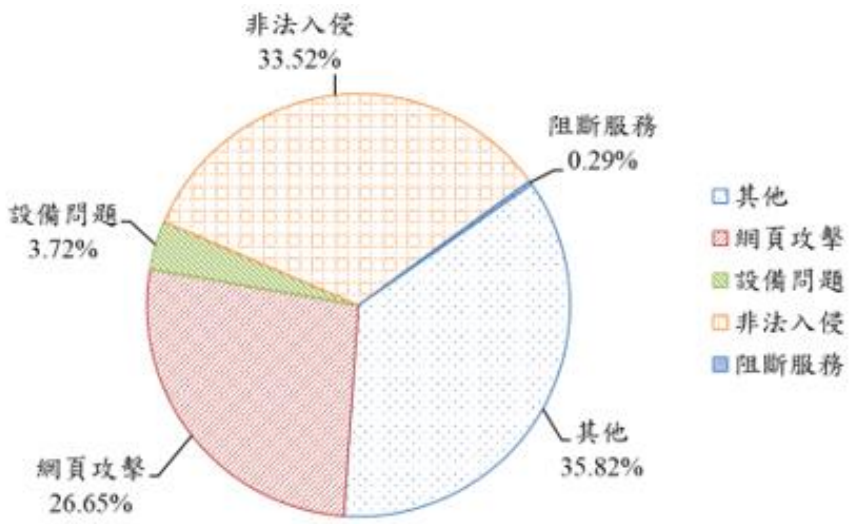


資料來源：本報告整理

圖1　108 年第 3 季資安事件影響等級比率圖

本季 3 級重要資安事件主要為攻防演練通報案件占比居多，多數機關評估在攻擊團隊成功入侵受測目標後，可能造成敏感資料遭洩漏，因此通報為 3 級事件。雖然政府機關(構)仍通報零星勒索病毒攻擊事件，但因未成功入侵重要系統與資料，且因備援與備份政策在機關(構)推廣已見成效，因此所造成之業務影響有限。

此外，資安事件通報類型依其所發現之異常情形，包含非法入侵、網頁攻擊、設備問題、阻斷服務及其他，其中，以「非法入侵」(占 33.52%)類型為主，另外針對特定機關(構)之網頁攻擊事件亦在通報事件中占比第二，詳見圖 2。

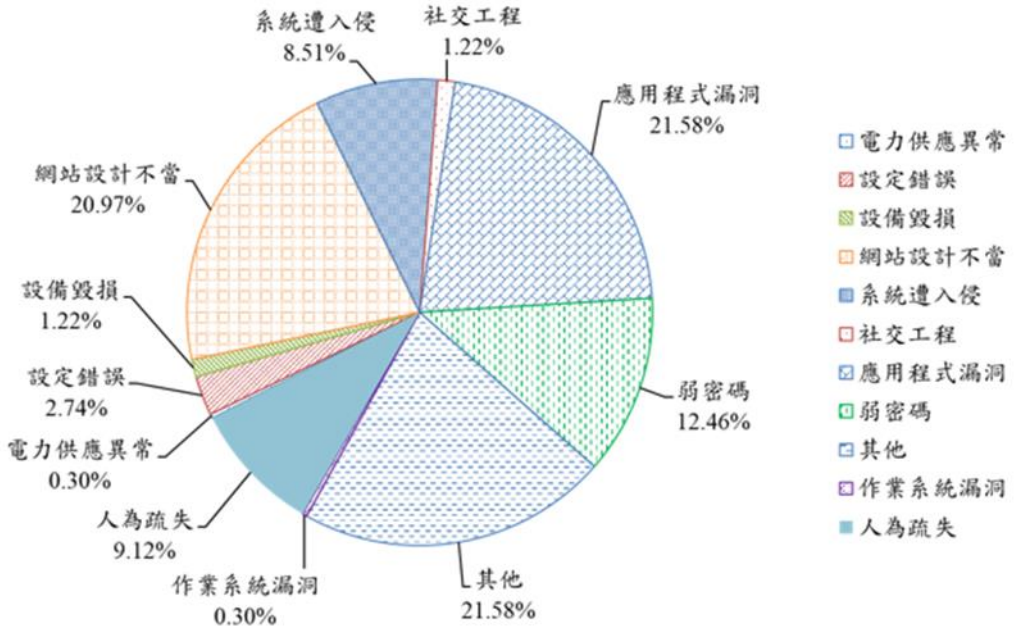


資料來源：本報告整理

圖2　108 年第 3 季資安事件通報類型比率圖

最後，分析通報事件發生原因，以應用程式漏洞(21.58%)與其他(21.58%)為主，其次分別為網站設計不當(20.97%)、弱密碼(12.46%)、人為疏失(9.12 %)、系統遭入侵(8.51%)、設定錯誤(2.74%)、設備毀損(1.22 %)、社交工程(1.22%)、作業系統漏洞(0.3%)及電力供應異常(0.3%)，詳見圖 3。本季事件之應用程式漏洞此次為機關(構)在攻防演練與實際通報資安事件中，高居首位，顯見應用程式漏洞已成為系統應用最大威脅。當應用程式急就章上線，或是在系統開發時未依安全系統發展生命週期之原則進行把關，則問題往往出現在正式環境維運時，進而影響業務之持續性。

分析相關資安事件發生原因，仍持續發現機關(構)委外廠商維護帳號使用預設密碼或弱密碼情況，駭客透過暴力破解方式，成功入侵機關(構)資訊設備。再者部分機關(構)內部伺服器帳號密碼與存取權限控管不當，造成橫向擴散導致災情擴大。因此，如何依資通安全管理法規定，委外辦理資通系統之建置、維運或資通服務之提供，選擇適當之受託者，並監督其資通安全維護情形，以避免資安事件發生疑慮。



資料來源：本報告整理

圖3　108 年第 3 季資安事件原因比率圖

1.3 資安防護重點

分析本季全球資安威脅現況，行動支付等創新應用科技與 IoT 設備的普及，因為資安防護等級與措施並未追隨這些科技應用發展的腳步，導致相關資安事件屢見不鮮，而疲於應付。

分析政府機關(構)通報的 3 級資安事件可看出，駭客藉著成功入侵機關(構)資通系統，竊取個人資料或機敏性資料。另外，資安事件關於資通系統的漏洞發生比率高，也寓示資通訊或資安人員在評估使用或維運資通系統的資安方案應該更為謹慎，如評估資通系統安全等級後，相關部署、組態設定、維運及資安檢測都應定期檢視其風險等級。密碼安全設定仍是資通系統防護的第一道門檻，雖政府強力宣導不使用預設密碼或弱密碼，但分析資安事件中，不論是委外廠商或政府機關(構)仍陸續發生有密碼遭竊或破解情況發生。

綜整以上資安威脅現況，提供資安防護建議如下：

●存取設定與密碼管理

– 依據存取控制政策，界定資通系統重要等級，訂定最小權限存取原則。

– 變更資通系統預設密碼，檢視密碼複雜度，並避免共用密碼。

– 導入創新或多重身分認證機制，提供存取登入效率並降低密碼外洩風險。

●物聯網資安管理

– 依循政府所訂定之系統開發資安規範，開發相關系統與 APP。

– 系統與 APP 上線前，必須經各項資安檢測，包含網頁、作業系統、網路服務、通訊、軟體、硬(韌)體及密碼安全等。

– 提供與選擇通過不同等級的 IoT 資安標章驗證之產品，並定期更新與檢視資安設定。

●行動支付安全

– 行動支付 APP 應從 Play 商店或官網下載，以避免下載偽冒 APP。

– 啟用行動支付前，應詳讀相關隱私保護條款，並了解與配合系統安全設定。

– 定期更新 APP 程式，修補程式漏洞。

2. 資安專題分享_FIDO 身分認證協議

現今網路時代，密碼依然是主流認證方式。而近年來為防範密碼外洩或遭惡意破解，使用者被要求遵循密碼資安規範，包含密碼長度、複雜度、使用期限及變更頻率等，再加上身分認證概念逐漸普及，認證系統資安要求也提升複雜性，造成系統管理者或使用者密碼管理上之困擾。

Google 曾在 108 年初，發表幾項需要注意的資安趨勢，其中值得關注的包含攻擊者將對較弱的雙因素認證(Two-Factor Authentication)方法進行攻擊，像是透過網路釣魚攻擊獲取帳號密碼資訊，或是攔截簡訊服務(SMS)的一次性驗證碼(OTP)等，因此 Google 預測，更多的服務應該會陸續採用更能對抗釣魚或其他攻擊的身分認證機制，如採用 FIDO (Fast IDentity Online, FIDO)聯盟所推出之身分認證協議等，透過公私鑰進行身分認證，讓使用者獲得更強大防範網路釣魚攻擊與帳戶遭竊的保護。

Google 進一步預測，108 年無密碼登入將會成為主流，FIDO 聯盟致力於推動無密碼身分認證技術，本報告將針對 FIDO 聯盟推出的 FIDO2 身分認證協議進行說明。

2.1 FIDO2 身分認證協議

FIDO 聯盟成立於 101 年 7 月，是一個開放的業界組織，其主要目標為推動新的身分認證標準，以降低對密碼的過度依賴。FIDO 聯盟期通過開放標準，以改變身分認證的屬性。藉由此開放性標準，提供比密碼與 SMS OTP 更安全且消費者更易於使用，同時服務提供商更易於部署與管理的身分認證方式。

為達成容易使用、隱私安全及標準化之目的，FIDO 聯盟致力於以下核心任務：

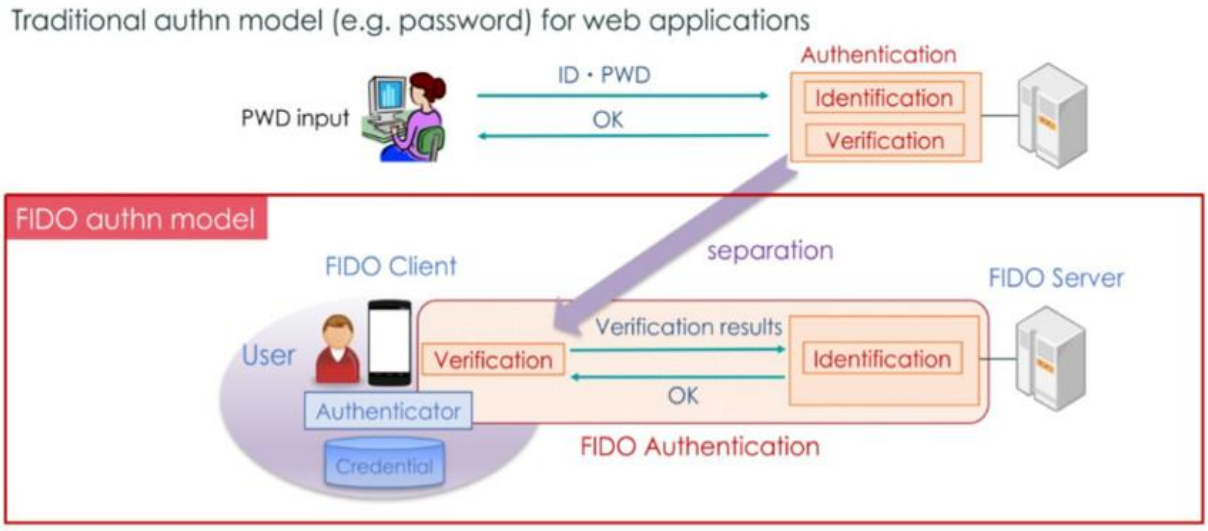
●制定發展相關技術規範，定義一個具開放、可擴展且相容的機制，以減

少使用密碼進行身分驗證的依賴。

●運用產業驗證計畫，以確保在全球範圍內能成功採用該規範。

●將成熟的技術規範提交給公認的標準制定組織，以進行正式標準化。

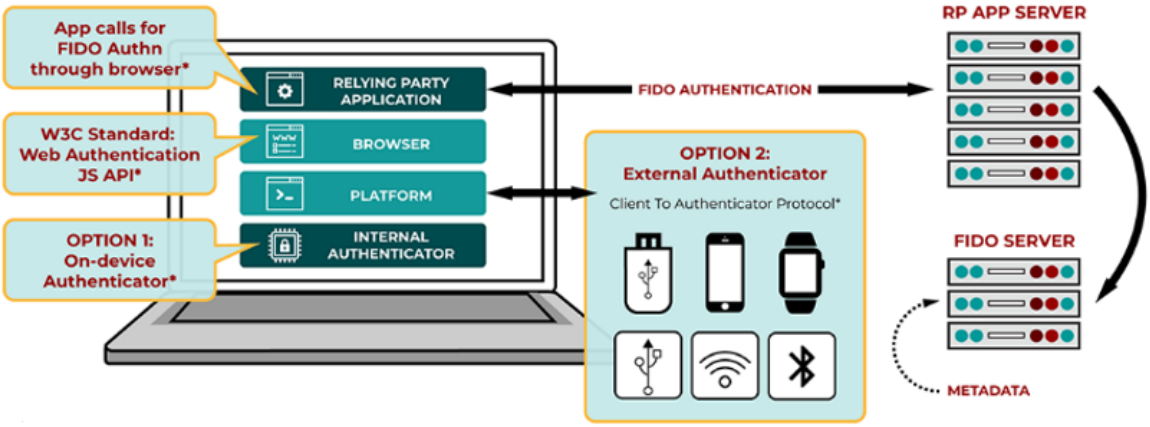
FIDO 聯盟於 107 年提出 FIDO2，主要概念是運用認證器(Authenticator)將驗證與識別拆開，先以生物辨識或 PIN 碼認證使用者，再經由公開金鑰達成身分識別，詳見圖 4。



資料來源：FIDO Alliance

圖4　FIDO2 身分認證模型

為達上述目的，FIDO2 由 WebAuthn(Web Authentication, WebAuthn)與 CTAP(Client-to-Authenticator Protocol, CTAP)等 2 種協議組成，由於 WebAuthn 被全球資訊網協會(World Wide Web Consortium, W3C)接受且定為共通性標準，各大瀏覽器陸續支援，相容性亦大幅提升。WebAuthn 內建於瀏覽器的 Web API(javascript)，用於 FIDO 認證；CTAP 內建於平台(OS)，允許使用外部的認證器進行無密碼認證、2 次認證或多因子認證，FIDO2 身分認證方式詳見圖 5。



資料來源：FIDO Alliance, FIDO2 project

圖5　FIDO2 身分認證方式

2.2 FIDO2 資安議題與採用建議

由於在 FIDO2 中，認證器的功能包含儲存生物特徵或 PIN 碼，以認證使用者、產生金鑰對，並儲存私鑰及運算身分識別時所需之資訊。因此認證器為 FIDO2 安全之核心，為確保認證器之安全，FIDO 聯盟發展認證器安全驗證計畫(Authenticator Security Certification Program)，並分為 3 個主要安全等級，詳見圖 6。

等級	定義	進階要求
L3+	可抵擋實體攻擊的裝置 (Captured Devices)	抵擋晶片等級之攻擊
L3		抵擋電路板等級之攻擊
L2+	具備受限制的運作環境 (Restricted Operation Environment, ROE)	通過黑白箱檢測
L2		抵擋不安全的OS(運算)
L1+	任意符合FIDO功能之軟體或硬體	抵擋不安全的OS(資料)
L1		無

資料來源：FIDO Alliance

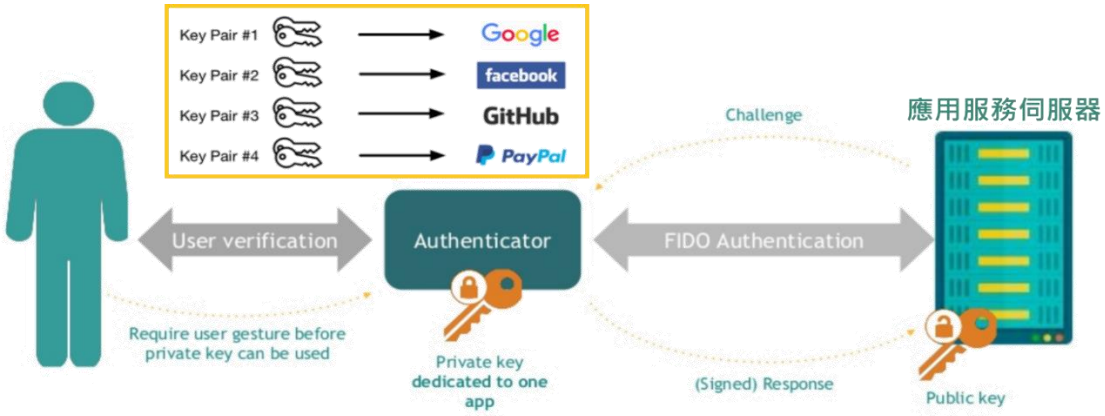
圖6　認證器之安全等級

此外，FIDO 聯盟也提供 Metadata Service(MDS)資料庫，維護認證器資訊與版本，以查看認證器 URL、最後更新時間、雜湊值及設備識別碼等資訊，讓使用 FIDO2 的伺服器與使用者，得以確認該認證器目前的安全狀態，詳見圖 7。

資料來源：FIDO Alliance

圖7　認證器狀態

另一方面，為進一步保障使用者隱私，認證器在註冊階段會對不同應用服務產生不同的金鑰對，並將公鑰傳送給應用服務伺服器進行註冊，防止攻擊者追蹤使用者在不同應用服務的相關紀錄，詳見圖 8。



資料來源：FIDO Alliance

圖8　FIDO2 註冊階段流程

FIDO2 為新一代的身分認證協議，其運用公開金鑰技術來取代傳統的密碼共享，並已被 W3C 訂為 Web 認證之標準，預計後續的應用範圍將逐步擴大。認證器為 FIDO2 安全之核心，認證器資安防護之有效性與生物辨識之準確率，將可能影響 FIDO2 後續推動之成效，其資安議題值得持續觀察。

密碼外洩、破解之資安事件頻傳，即使企業提供類似電信簡訊與電話語音執行二次驗證，也傳出屢遭網路釣魚與中間人的攻擊。要如何解決密碼設定或管理上種種問題，多年來有不同的見解與爭論。

逐步捨棄傳統密碼，轉向無密碼登入儼然已成為身分認證的趨勢，未來顯而易見將更加廣為運用在生活中所有需要身分認證的環境。惟使用者除因多年來已習慣使用密碼設定，對無密碼登入的安全與隱私保護仍存在一定疑慮。建議可透過政府身分認證之政策，協同產業之發展計畫，推廣使用者之用戶體驗。

3. 資安技術研析_惡意程式 Calling Interceptor

本季所探討的資安技術研析，是概述韓國金融詐騙調查分析事件。在此案例中駭客利用台灣 IP 建立惡意 APK 下載站，下載站偽裝成 Google Play 商店 APP 下載頁面，APP 偽冒對象為韓國行政安全部警察廳的手機反間諜服務。此種受害情況擴散原因，通常是因為惡意程式下載站偽裝成合法下載頁面，使用者往往缺乏警覺心，且要等到有一定數量的受害者後，惡意程式才會被揭露。

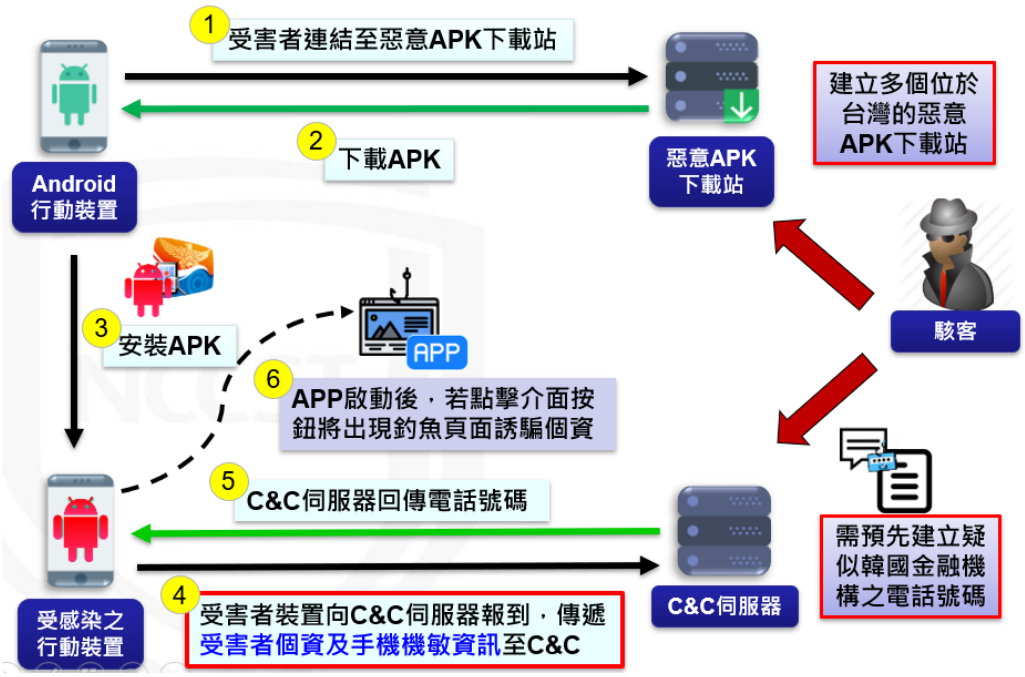
以下將說明韓國金融詐騙調查分析事件之詐騙經過與後續防範措施。

3.1 案例分析與追蹤

108 年 TWNCERT 接收到情資，駭客利用台灣 IP 建立惡意 APK 下載站，偽冒對象為韓國行政安全部警察廳的手機反間諜服務。韓國警察廳推出的反間諜 APP，主要在檢測手機內是否存在惡意 APP，並將每次檢查的結果寫入 history.xml 中，而偽冒的反間諜 APP 會逐一搜尋已安裝於手機內的 APK 是否包含 whowho 及 whoscall，如果有的話則會跳出建議解除安裝頁面，並且將部分手機機敏資訊寫入至 ALLCC.xml 中。

為確認是否有其他位於台灣的惡意下載站，技服中心建立惡意手機木馬下載站掃描模組，擴大追蹤駭客犯罪情形。首先利用掃描工具探測鄰近網段，追蹤惡意 APK 下載站使用 IP，並嘗試取得樣本，確認是否為同一族群的惡意程式，偵測結果發現數個相同樣態木馬 APK 的下載站，惡意 APK 仿冒對象除韓國警察廳的反間諜軟體外，還包含韓國各家金控業者的信用貸款服務及韓國資安業者 BTWorks 的防釣魚軟體等。部分惡意 APK 分析結果，C&C 所在位置為韓國，於是通知 KrCERT 處理位於韓國的 C&C 伺服器，並請求提供 C&C 方面相關資訊。此次調查之可疑 IP，皆來自於同一個網路平台服務業者。透過網路平台服務業者的 RouterOS 軟體路由器查看目前正在連線的用戶，發現遠端連線至追查目標主機的來源 IP

分別來自中國、韓國及俄羅斯等國家。經由技服中心分析後，發現攻擊流程詳見圖 9。



資料來源：本報告整理

圖9　殭屍網路攻擊流程圖

3.2 攻擊流程與分析

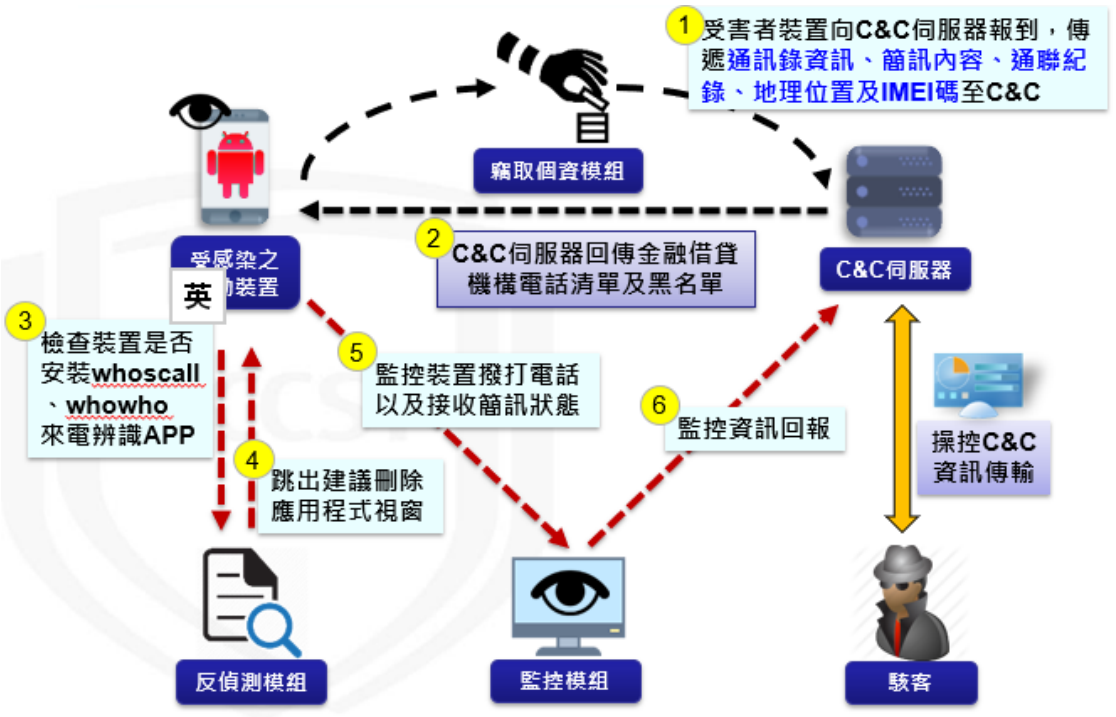
駭客使用的網頁伺服器軟體主要為 Microsoft IIS 與架站軟體(Apache+PHP+MySQL)整合包，架站軟體整合包所使用的語言皆為韓文，通常被韓國的使用者用來簡單、快速地架設 Web 伺服器，包含 APMSetup 與 KebiHome。

本案例掌握的惡意程式 Calling Interceptor，主要可分為 A、B 等 2 種樣態(詳見圖 10)，偽冒韓國行政安全部警察廳的反間諜 APP 屬於 Type A，其 APK 之行為流程圖詳見圖 11。

	Type A	Type B
啟動模組	主程式: \classes.dex C&C API: \lib\armeabi-v7a\libhelper.so	主程式 + C&C API: \classes.dex
詐騙MP3存放位址	\assets\r.zip	\assets\
反偵測模組	刪除 whoscall/whowho APP	停用 whoscall/whowho APP
竊取個資模組	竊取裝置資訊、通訊錄、 簡訊、個資及通話紀錄	竊取裝置資訊、通訊錄、 簡訊、個資及通話紀錄
監控模組	■ 監聽裝置撥打\接聽電話狀態 ■ 監控裝置發送\接收簡訊狀態	■ 監聽裝置撥打\接聽電話狀態 ■ 監控裝置發送\接收簡訊狀態
詐騙MP3模組	不比對借貸機構電話號碼清單 不播放詐騙MP3	比對借貸機構電話號碼清單 播放詐騙MP3

資料來源：本報告整理

圖10 惡意程式樣態

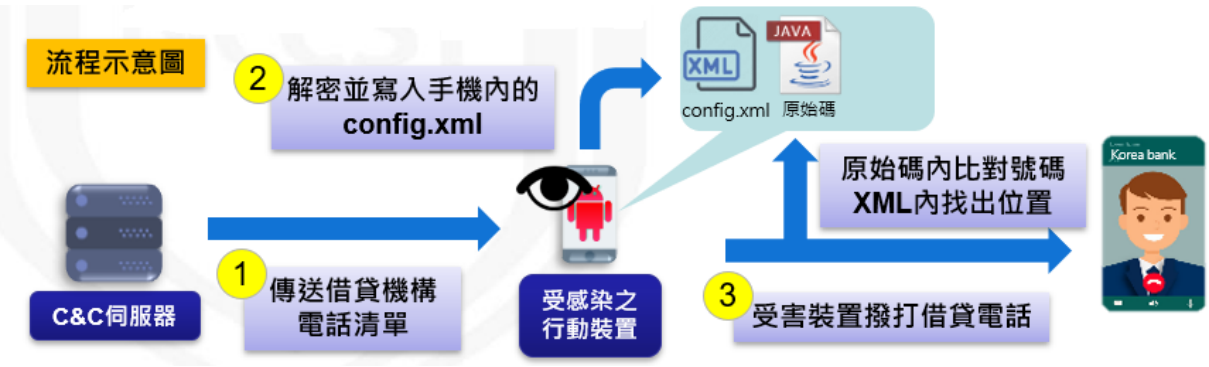


資料來源：本報告整理

圖11 Type A 之 APK 行為流程圖

另一惡意程式偽裝成韓國聯合社區信用合作社的 APP 誘騙使用者下載安裝，此攻擊樣態為 Type B。惡意程式感染行動裝置後，會竊取受害者個資與手機機敏資訊，經 AES 加密傳送至 C&C 伺服器完成報到，C&C 伺服器會定時更新借貸機構電話號碼與黑名單資訊在 URL 上，而受害裝置則可經由 URL 取得，大約有 5,000 筆韓國金融借貸機構之電話號碼與偽冒來電資訊，以及經查已被民眾舉報為惡意來電之黑名單等資訊。

此惡意程式夾帶 50 個預先錄製好的詐騙音訊檔，命名皆為韓國金融借貸相關名稱，詐騙流程一開始收到並解密出 C&C 伺服器傳送的號碼清單，惡意程式監控受害裝置是否有撥打電話，若受害裝置確實有撥打電話，則會將該電話號碼與韓國金融單位電話進行比對，若吻合則撥放對應的 MP3 詐騙音訊檔，詳見圖 12。



資料來源：本報告整理

圖12 受害裝置遭詐騙流程

3.3 Calling Interceptor 映射 MITRE ATT&CK

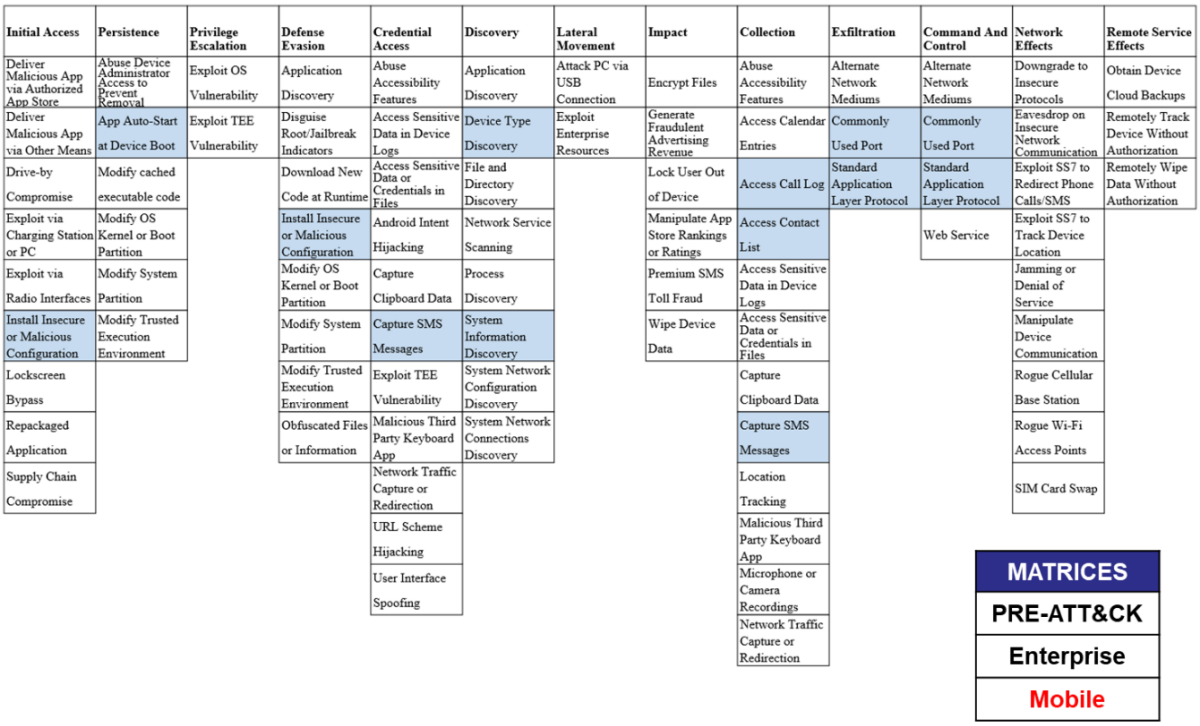
後續彙整此事件相關 Log 紀錄與網路流量的 IP 進行分析，已經下載惡意 APK 的受害者 IP，以韓國占最大宗。調查網路平台服務業者疑似被駭客租用的主機，共發現 11 台相同樣態 APK 下載站的虛擬機。總計 17 種樣本，詳見圖 13。

原始檔名	MD5	樣態
kb.apk	7c331166146d1a9b4cf92e7a66590e96	A
cyber.apk	7c331166146d1a9b4cf92e7a66590e96	A
123kb.apk	e512f1ca8fdcaf5f4d8045c1e049912c	B
sinhanBank.apk	a4e890f4cca9f5304842545487786370	A
cyber.apk	f164a68339d7e352e32249fe8af778e4	A
123kb.apk	d8d5489004f7b0721c1213427d4b084f	B
123kb.apk	7032ddf9433d97a1e9b9a0780bbfa66e	B
kb.apk	ceb9524a78ced562bfdce4aa0b4edf39	B
kb.apk	e587fa5d2178c276dcd5603951eba2db	B
cyber.apk	fa0fc66e93b7cb75cd033a75876d87c1	A
123kb.apk	1f81f7f4838cbcc95e4bcd123603abf3	B
hyundai.apk	1780bba8065295945aa110cdc41806b0	B
123hana.apk	84b1278705cf2888b4bf623ff164e493	B
kb.apk	0b26fd95e20b79f24a8f725a6b52467c	B
123sbibank.apk	7129b551bd7e83cc1205ad755f253d7c	B
hana.apk	c8e2c1e74d4c8f663eb60744371008bc	B
sbibank.apk	d8a7ea8b9ec7f7414aba64690fd275ae	B
saemaul.apk	5c67be66ec75d8bbddfe00e67ad40d62	B

資料來源：本報告整理

圖13 下載站樣本資訊

第 2 季季報資安技術研析主題曾就攻擊者行為資料庫 MITRE ATT&CK 進行概述與說明，透過 ATT&CK 針對攻擊流程的定義，說明相關網路攻擊手法，提供政府機關與企業，更方便地理解攻擊者行為帶來的資安風險，以及早進行相關防範。特別將此惡意程式 Calling Interceptor 以攻擊者行為資料庫 MITRE ATT&CK 進行相關圖解，詳見圖 14、圖 15 及圖 16。



Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Collection	Exfiltration	Command And Control	Network Effects	Remote Service Effects
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Abuse Accessibility Features	Application Discovery	Attack PC via USB Connection	Encrypt Files	Abuse Accessibility Features	Alternate Network Mediums	Alternate Network Mediums	Downgrade to Insecure Protocols	Obtain Device Cloud Backups
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Disguise Root/Jailbreak Indicators	Access Sensitive Data in Device Logs	Device Type Discovery	Exploit Enterprise Resources	Generate Fraudulent Advertising Revenue	Access Calendar Entries	Commonly Used Port	Commonly Used Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Drive-by Compromise	Modify cached executable code		Download New Code at Runtime	Access Sensitive Data or Credentials in Files	File and Directory Discovery		Lock User Out of Device	Access Call Log	Standard Application Layer Protocol	Standard Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Exploit via Charging Station or PC	Modify OS Kernel or Boot Partition		Install Insecure or Malicious Configuration	Android Intent Hijacking	Network Service Scanning		Manipulate App Store Rankings or Ratings	Access Contact List		Web Service	Exploit SS7 to Track Device Location	
Exploit via Radio Interfaces	Modify System Partition		Modify OS Kernel or Boot Partition	Capture Clipboard Data	Process Discovery		Premium SMS Toll Fraud	Access Sensitive Data in Device Logs			Jamming or Denial of Service	
Install Insecure or Malicious Configuration	Modify Trusted Execution Environment		Modify System Partition	Capture SMS Messages	System Information Discovery		Wipe Device Data	Access Sensitive Data or Credentials in Files			Manipulate Device Communication	
Lockscreen Bypass			Modify Trusted Execution Environment	Exploit TEE Vulnerability	System Network Configuration Discovery			Capture Clipboard Data			Rogue Cellular Base Station	
Repackaged Application			Obfuscated Files or Information	Malicious Third Party Keyboard App	System Network Connections Discovery			Capture SMS Messages			Rogue Wi-Fi Access Points	
Supply Chain Compromise				Network Traffic Capture or Redirection				Location Tracking			SIM Card Swap	
				URL Scheme Hijacking				Malicious Third Party Keyboard App				
				User Interface Spoofing				Microphone or Camera Recordings				
								Network Traffic Capture or Redirection				

MATRICES
PRE-ATT&CK
Enterprise
Mobile

資料來源：本報告整理

圖14 Calling Interceptor 惡意程式 MITRE ATT&CK Matrix

Software: Calling Interceptor

Description	本木馬家族以韓國為主要攻擊目標，通常偽冒成韓國各家金控業者、信用貸款服務、政府、資安業者等APP，誘騙民眾下載安裝。主要竊取受害者個資及手機機敏資訊、監控撥打電話，當受害裝置撥打借貸機構電話時，木馬將攔截通話，以撥放MP3詐騙音訊檔取代，並回報狀態至C2，再讓駭客或所屬的詐騙集團運用此手機木馬結合電話詐騙手法。
Aliases	(None)
Techniques	• Install Insecure or Malicious Configuration • App Auto-Start at Device Boot • Capture SMS Messages • Device Type Discovery • System Information Discovery • Access Call Log • Access Contact List • Commonly Used Port • Standard Application Layer Protocol
Group	FatKitten
References	(None)

資料來源：本報告整理

圖15 Calling Interceptor 惡意程式 MITRE ATT&CK Software

Domain	Tactic	ID	Name	Use
mobile	Initial Access, Defense Evasion	T1478	Install Insecure or Malicious Configuration	使用者必須開啟「允許安裝未知的應用程式」之設定
mobile	Persistence	T1402	App Auto-Start at Device Boot	在設備啟動時自動啟動
mobile	Collection, Credential Access	T1412	Capture SMS Messages	攔截手機簡訊回傳至C2 Server
mobile	Discovery	T1419	Device Type Discovery	取得用戶手機設備IMEI、型號、Android版本
mobile	Collection	T1433	Access Call Log	蒐集通話紀錄並回傳至C2 Server
mobile	Collection	T1432	Access Contact List	蒐集通訊錄號碼並回傳至C2 Server
mobile	Discovery	T1426	System Information Discovery	監控通話資訊並回報至C2 Server
mobile	Command And Control, Exfiltration	T1436	Commonly Used Port	以HTTP的8080 Port向C2 Server報到與傳輸資料
mobile	Command And Control, Exfiltration	T1437	Standard Application Layer Protocol	用戶端手機以HTTP主動發送請求指令，C2依照用戶端的請求回應擴散簡訊所需的資料

資料來源：本報告整理

圖16 Calling Interceptor 惡意程式 MITRE ATT&CK Techniques

經由本案例分析結果得知，當受害者手機感染此惡意程式後，駭客將會監控手機狀態，並撥放釣魚借貸 MP3 取信於受害者，再由駭客所屬的詐騙集團撥打詐騙電話以騙取帳戶金錢。

此次韓國多家金融機構受駭，代表金融服務相關之身分認證機制仍需強化，駭客集團可利用木馬與電話詐騙取得的個資，透過電話假冒民眾向銀行申請借貸。駭客是否能成功假冒民眾申請借貸，銀行對於借貸者身分如何進行審慎驗證與查核將會是資安關鍵議題。為防堵網路銀行帳戶遭盜領事件，除需加強宣導使用者之資安意識，銀行應對線上金融交易採高標準之身分認證與安控機制，將相關詐騙風險降至最低。

4. 結論

本報告透過日本 7-11 手機支付 APP 被駭事件與俄國駭客利用 IoT 裝置入侵企業網路，分析因為程式設計不當，相關要求規範未從程式開發時就將資安概念導入，造成客戶個資外洩與商譽損失。另外 IoT 的普及，也引起駭客鎖定攻擊的興趣，藉由利用 IoT 裝置的預設密碼與裝置韌體未升級到最新版本等弱點，進而駭入到內部網路。國內部分，分析政府資安威脅現況，發現事件原因以「非法入侵」類型為主，其次為「網頁攻擊」，造成非法入侵的原因，使用預設密碼或弱密碼為部分肇因。針對本季全球與政府所面臨的主要資安威脅，本報告就「存取設定與密碼管理」、「物聯網資安管理」及「行動支付安全」方面，提出資安防護建議。

資安專題分享新興網路身分認證協議 FIDO2，概述無密碼化認證技術。密碼管理長久以來是資安領域重要的議題，卻也常存在設定不當與外洩風險，透過 FIDO2 無密碼化認證技術，將對資安強化有一定成效。

此外，透過資安技術的研析，深入探討惡意程式 Calling Interceptor 下載站偽裝成合法下載頁面，造成韓國金融詐騙事件發生，駭客利用台灣 IP 建立惡意 APK 下載站，偽裝成 Google Play 商店 APP 下載頁面，APP 偽冒對象為韓國行政安全部警察廳的手機反間諜服務，將非法行為隱藏在合法程式背後。

下一季「資通安全技術報告」，除持續分析全球與國內政府機關之資安威脅現況，以及蒐集新興資安議題，提供技術研析觀點，從國內外情資與相關研究人員角度提供防護重點。資安專題將探討軟體定義網路(SDN)所帶來的資安威脅與特性，並研擬相關防護建議。

資安相關活動

本季行政院資通安全處辦理多項資安相關活動，活動細節說明如下：

◆ N-ISAC 定期會議

本次 N-ISAC 會議為 108 年第 2 次一般會員會議，報告議題包含 N-ISAC 與 N-CERT 執行情形，以及邀請教育部(A-ISAC)、TWCERT/CC 及台南區域聯防中心進行經驗分享。

專題分享為近期資安情勢與資安事件案例分享，首先由行政院資安處分享近期重大資安事件案例，並針對政府機關資安防護之弱點提出改善建議。報告中分享供應鏈攻擊案例，駭客通常鎖定供應鏈中資安防護較弱的環節進行攻擊，藉由入侵特定軟/韌體開發公司或人員電腦，進行竄改程式或下載連結等行為，造成大範圍的感染與擴散。對應之防範建議則有定期檢視網站所屬資料夾之存取與操作權限，依最小權限原則授權，以降低遭利用上傳惡意程式之風險。同時應確實掌握機關建置之系統維運情形，落實資訊資產盤點，確認應下架之系統均落實下架處置，以減少資安漏洞暴露於網際網路風險。

接著由調查局與技服中心針對新興之網路犯罪樣態，如境外組織租用我國網路服務，針對他國進行惡意活動之情事以及其攻擊流程與技術細節進行說明。此外亦透過 N-ISAC 會議宣導，由於 10 月國慶與 109 年 1 月總統大選等重大活動，預期資安攻擊活動可能會增加，提醒各會員需提高警戒，加強資安防護工作，確實掌握資安事件通報與應處情形，以降低潛在攻擊活動之衝擊。

◆ 政府領域資安聯防監控說明會

政府領域資安聯防監控說明會主要是針對政府領域聯防監控情資回傳作業說明，協助各機關之資通安全人員依資安法聯防監控應辦事項，建置資通

安全威脅偵測管理機制，並依指定方式回傳資料。說明會共辦理 2 場，參加對象為資通安全責任等級 A 級與 B 級政府機關之資通安全人員。

說明會介紹與說明聯防監控情資收容類型與格式、聯防監控情資回饋、聯防監控作業辦理及聯防監控情資回傳等作業，同時包含後續辦理事項與時程說明，將於 108 年 12 月正式完成聯防監控連通測試，正式回傳監控情資，包含「資安監控事件單」與「關聯分析事件單」。109 年起，每月回傳「健康狀態統計單」，並至管考系統更新資安監控資訊。

以聯防監控格式為例，領域聯防監控作業配合資安法應辦事項要求，於 109 年起採 STIX 格式回傳監控情資，舊版情資封裝格式將收容至 108 年底後停用，主要為資安設備所觸發活動資訊，缺乏良好資安事件與威脅情資承載能力。新版情資封裝格式現行為 N-CERT、N-ISAC 及 N-SOC 使用，主要提供資安事件與資安威脅情資等高階情資封裝能力、彙整與分析網路威脅情資(Cyber Threat Intelligence, CTI)，藉此提高資安聯防與情資分享效益。