112年第1季資通安全技術報告

Quarterly Technical Report

國家資通安全研究院

National Institute of Cyber Security

目　次

圖 目 次

表 目 次

摘要

「第 1 季資通安全技術報告」除分析本季全球資安威脅、政府通報資安事件外，並提供相對應之資安防護建議。同時，藉由資安專題分享與資安技術研析，提供政府機關需關注之資安風險重點。

「第 1 季資通安全技術報告」分為以下 4 個章節。

●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 起案例為汽車業者全球供應鏈網站漏洞，可能讓駭客輕易獲取機敏資訊；另一起案例為美國禁飛名單於駭客論壇遭公開分享，名單因與國家安全與反恐目的有關恐衝擊擴大。

分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」(占 60.97%)類型為主，排除綜合類型「其他」外，其次分別為「設備問題」(占 10.37%)與「阻斷服務」(占 9.15%)為主要通報類型。

●資安專題分享

資安專題分享主題為 OWASP 十大主動式控制 Top 10 Proactive Controls，提供針對開發人員了解面對每個軟體開發項目均應包含之安全技術，並依重要性排序，以供人員實作時參考使用。

●資安技術研析

資安技術研析主題為星際檔案系統(InterPlanetary File System, IPFS)濫用威脅之攻擊手法探討，由資安事件中揭露多起惡意程式代管服務之防彈主機(bulletproof hosting)加入 IPFS 網路。IPFS 濫用情形有日趨嚴重之情況，管理人員應事先了解其入侵途徑，並防範未然。

●結語

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資安防護重點。資安專題分享 OWASP 十大主動式控制 Top 10 Proactive Controls，提供針對開發人員了解面對每個軟體開發項目均應包含之安全技術。此外，資安技術研析分析星際檔案系統濫用威脅之攻擊手法，管理人員應充分了解其入侵途徑，妥善應對。

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及可能之衝擊與影響。112 年第 1 季(以下簡稱本季)探討全球供應鏈所衍生之相關資安風險與面對雲端服務之風行所應強化之資安防禦。

本章節之事件與議題皆配合整理相關之資安防護重點，提供政府機關就相關資安風險或議題進行評估，並依循資安管理規範與技術防禦進行強化。

1.1 全球資安威脅現況

根據世界經濟論壇(World Economic Forum, WEF)「112 年全球風險報告」調查經濟、環境、地緣政治、社會及科技等 5 大類風險中有關 2 年之短期風險與 10 年之長期風險，科技類之「廣泛之網路犯罪與網路危機(Widespread cybercrime and cyber insecurity)」皆於排名前十位占居第 8 名。因此可見網路犯罪仍為本年度全球的重點風險，再加上「網路犯罪即服務」(Cybercrime-as-a-Service, CaaS)攻擊手法推波助瀾下，使惡意攻擊技術門檻低且日漸猖獗，有心人士藉此擴大攻擊範圍。同時網路犯罪者也藉著提供「網路犯罪即服務」此類產品獲取高利潤，二者間逐漸形成網路攻擊之生態體系。

從全球風險報告得知網路犯罪與網路危機威脅四伏，而駭客攻擊工具取得越趨容易，順應全球化之趨勢，供應鏈夥伴來自世界各地，而如何認證與檢視供應鏈之安全，應嚴陣以待。同時面對雲端服務之普及，未來可能成為主流情況下，相信來自於雲端服務之攻擊將更加白熱化。

本季具指標性案例為汽車業者全球供應鏈網站漏洞，可能讓駭客輕易獲取機敏資訊；另一起案例為美國禁飛名單於駭客論壇遭公開分享，名單因與國家安全與反恐目的有關恐衝擊擴大。

首先，探討案例汽車業者 Toyota 全球供應鏈網站漏洞，可能讓駭客輕易獲

取機敏資訊。一位資安研究員在去(111)年 11 月時開始揭露該公司 Global Supplier Preparation Information Management System (GSPIMS)系統存在嚴重漏洞，GSPIMS 為汽車製造商之網路應用系統，系統允許員工和供應商遠端登錄並管理公司的全球供應鏈，只要得知其中一個系統使用者之電子郵件帳號，就可以成功取得該系統之控制權，該研究員是在一次測試入侵中，發現經由此漏洞，可以任意存取系統內超過一萬多家供應夥伴之資訊，包含帳號細節、機密文件、專案資料及供應商排行與評論等等敏感訊息。

GSPIMS App 是建立在 Angular JavaScript 架構上，使用特定的路徑與功能以決定使用者可以存取那些頁面，此漏洞允許可透過修改 JavaScript 以任意存取頁面。而之所以可以透過任一 Toyota 有效之員工電子郵件地址登入是因為此服務提供一個 JSON Web Token (JWT)身分驗證機制，而此程序只要求輸入電子郵件帳號，不需密碼即可登入。之後再透過系統 API 之漏洞，將可允許入侵者成功創建一使用者帳號後再切換成具特權管理之帳號。汽車業者 Toyota 於 111 年發生數起資安供應鏈遭駭事件，包含針對其供應鏈之網路攻擊與官方連接應用程式之 GitHub 儲存庫(Repository)遭揭露。

第 2 起案例為美國禁飛名單於駭客論壇遭公開分享，遭分享名單中包含超過 150 萬筆與 25 萬筆候選之禁飛紀錄，名單經證實與駭客於不安全伺服器中找到之美國運輸安全管理局(Transportation Security Administration, TSA)禁飛名單相同。這兩個電子表格所包含之個人資料從 108 年開始，包含姓名、別名、護照號碼、出生日期及相關資訊。而這些資料之所以列為機敏資訊是因禁飛名單多涉及國家安全與反恐目的等，因此有其特別意義必須加強保護。

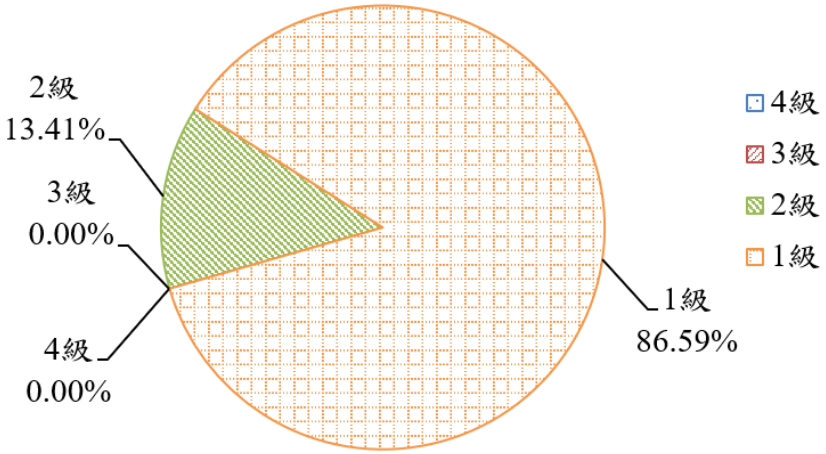
事件發生起因為某航空公司於 Amazon Web Services (AWS)雲端伺服器因

組態配置錯誤，導致駭客可任意存取其資料庫。駭客告訴媒體他們的做法為使用搜尋引擎 Shodan 尋找協助構建、測試及部署軟體之自動化伺服器時發現此份禁飛名單。駭客更聲稱藉由此雲端伺服器組態配置錯誤之漏洞，他們可以任意取消或延遲航班，甚至更換機組員。TSA 事後在調查此事件時，針對機場與航空公司發布一項安全命令，要求就現有安控措施進行強化，特別是在處理敏感資料與個人資訊上。同時也再次強調將繼續與合作夥伴合作，確保其實施安全要求，並保護系統與網路，避免遭受網路攻擊。

綜覽本季全球資安威脅與資安事件，供應鏈全球化，涵蓋不同面向、來源及等級之可能風險，因此如何集中管理供應鏈，制定一致性之管理原則並套用將會是迫在眉睫之課題。而雲端服務因新冠疫情影響，助長其應用範圍，同時從事件中也發現駭客針對不論是雲端服務提供者或客戶皆展開相關攻擊，因此就管理面而言，雲端資料之保護與安全組態設定，應為使用雲端服務前必須列為優先考量議題。

1.2 政府資安威脅現況

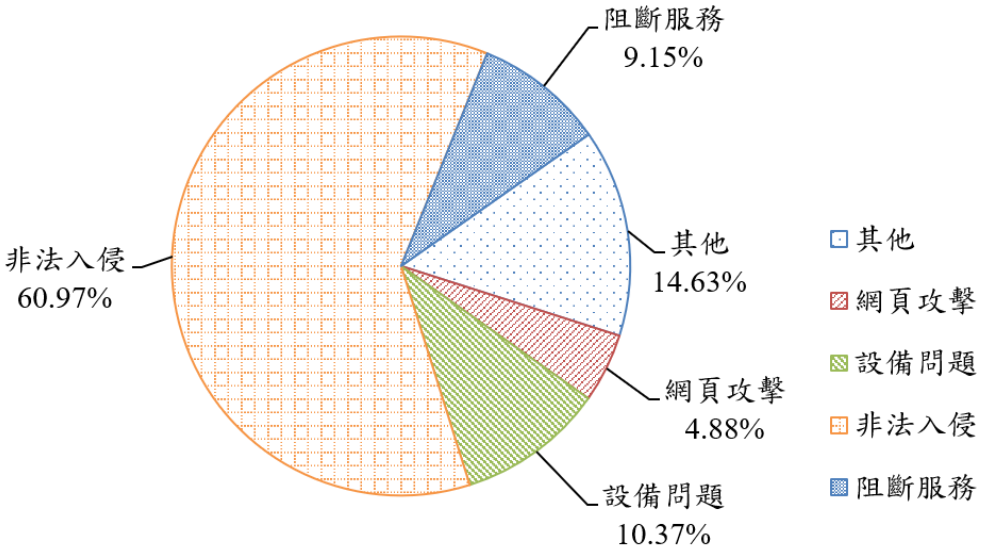
彙整本季所接獲之政府機關通報事件，藉由事件之影響等級、通報類型及事件原因，了解目前政府機關之資安威脅現況。通報事件依「機密性」、「完整性」、「可用性」3 個面向所造成之衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級。彙整事件影響等級，本季公務機關中以 1 級事件占 86.59%為大宗，2 級事件占 13.41%次之，3 級與 4 級通報事件則未發生，相關統計情形詳見圖 1。



資料來源：本報告整理

圖1　112 年第 1 季通報事件影響等級比率圖

整體通報事件類型，以「非法入侵」(占 60.97%)類型為主，排除綜合類型「其他」外，「設備問題」與「阻斷服務」類型次之，詳見圖 2。

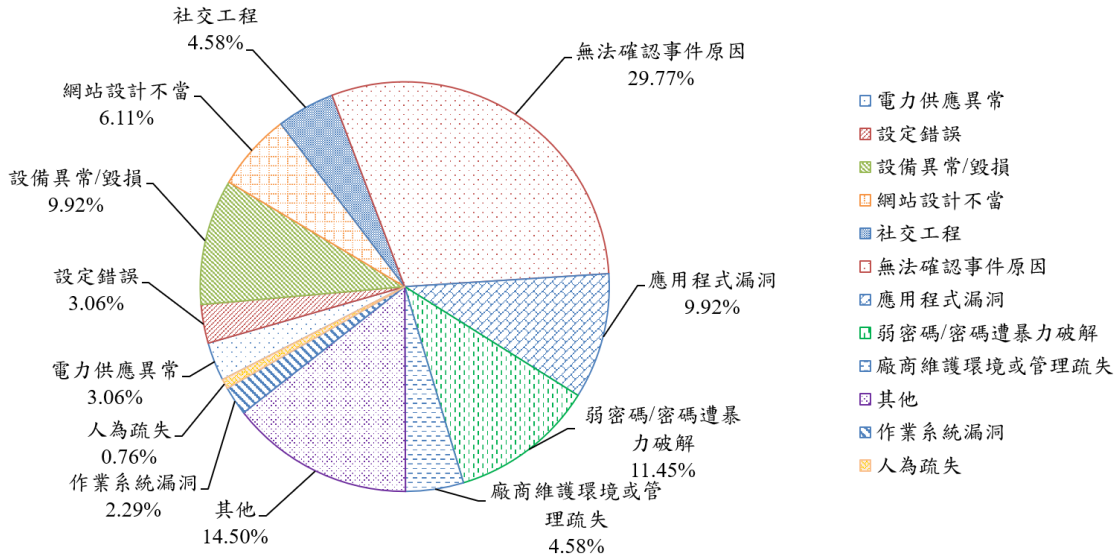


資料來源：本報告整理

圖2　112 年第 1 季通報類型比率圖

通報事件之阻斷服務於本季相較於上季有攀升之趨勢，此類攻擊通常具備針對性與具備特定攻擊意義，且最大目的在於阻斷目標對象之服務或網路之正常運作，而非常見之竊取資料或入侵系統。因阻斷服務經常利用殭屍網路進行攻擊，除考量能即時偵測該攻擊與儘速回復正常運作外，亦應強化用戶端、網路及物聯網等設備防護避免成為僵屍網路利用工具。

分析通報事件發生原因，透過公務機關資安事件原因比例圖，詳見圖 3，可發現事件原因以無法確認事件原因(29.77%)為主要原因，其次分別為其他(14.50%)、弱密碼/密碼遭暴力破解(11.45%)、設備異常/毀損(9.92 %)、應用程式漏洞(9.92 %)、網站設計不當(6.11%)、社交工程(4.58 %)、廠商維護環境或管理疏失(4.58 %)、電力供應異常(3.06 %)、設定錯誤(3.06 %)、作業系統漏洞(2.29 %)及人為疏失(0.76 %)。本季無法確認事件原因與其他之比例仍居不下原因，除事件調查後仍無法發現原因外，有二大主因為系統逕行下架與無相關紀錄檢視，其中又系統逕行下架高居首位，資安事件發生後，管理人員因系統下架未能妥適保留證據，導致無法確認事件發生原因。系統遭下架可能是因評估設備老舊或已無使用需求，但也常造成無法於第一時間進行事件根因調查。機關內部老舊或已無使用需求之設備應訂定維運與汰換之標準程序，若發生資安事故時，應有證據留存之作法。另外，針對無相關紀錄檢視之事件，其機關應依遵循資通安全管理法要求之資通系統防護基準，應訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。



資料來源：本報告整理

圖3　112 年第 1 季資安事件發生原因比例圖

分析第 1 季通報類型與通報事件中，發現有網通設備遭揭露存在任意文件寫入(Arbitrary Write)與其他身分驗證繞過漏洞等，攻擊者不需通過身分驗證即可針對該設備進行攻擊，機關應針對所擁有之設備檢視是否在受影響範圍，並關注韌體升級等訊息，同時關閉與限制相關服務之存取，避免因設備漏洞遭受刺探式攻擊。

1.3 資安防護重點

分析本季全球資安威脅現況，全球供應鏈因每一供應鏈或廠商之資安韌性不同，造成管理上之困難。雲端服務之風險根據網通廠商 Palo Alto Networks 所發表之 2023 雲端原生資安狀況報告(2023 State of Cloud-Native Security Report)指出，在新冠疫情期間，各公私單位雲端服務使用增長達 25%以上，而有 78%受訪單位表示將雲端服務之安全責任分散至各部門，而非以單一資安團隊因應，另有 47%表示旗下員工並不完全了解雲端服務對應之資安責任。

國內部分，發現雲端服務遭利用為攻擊平台，近期追查機關事件中，揭露

駭客使用雲端服務架設中繼站，藉此規避防護阻擋並隱匿行蹤，如利用 Google Cloud Platform (GCP)、AWS、Cloudflare 及 DigitalOcean 等雲端平台，使用合法 IP 位址與域名進行資料竊取，將惡意傳輸流量隱藏於合法流量中，使資安防護偵測機制無法於第一時間察覺其惡意行為。

綜整以上資安威脅現況，提供資安防護建議如下：

●全球供應鏈之資安管理

– 組織應主動盤點所有供應鏈，分析其服務或連網等可能威脅，隨時確認供應鏈範圍與風險可接受度。

– 強化供應鏈權限申請、審核及存取管理，確保只提供其特定角色對應之權限。

– 積極保護資訊本身，不提供過多資訊予供應鏈，並應定期檢視資料分享機制。

●雲端服務之資安管理

– 應審慎評估雲端平台使用需求，考量部署具備內容分析之資安偵測機制，隨時監控雲端服務之安全性。

– 機敏資料放置於雲端時，應採取加密機制，且應針對雲端服務訂定一致性之安全組態設定與存取規則，如最小權限、持續驗證及日誌留存機制等。

– 依雲端服務之屬性，訂定相關威脅指標以進行域名分析與阻擋。

2. 資安專題分享_OWASP Top 10 Proactive Controls 概述與實作介紹

近來資安事件頻傳資通系統遭入侵，追究其根本原因為資通系統存在安全性漏洞。分析其漏洞肇因大部分為開放源碼或程式碼不安全導致。政府機關資安聯防情資也常見相關入侵攻擊，針對網頁應用程式之攻擊行為高居不下，可見駭客無所不用其極尋找可入侵之破口，而對外之公開網站或應用系統則為常見之目標。加上不論是內部自行開發或委外人員，可能未接受完整之安全程式碼撰寫訓練，因此在開發 Web 應用程式時常出現關鍵資安控制措施之缺失。

程式設計人員會在應用程式上線前進行源碼檢測與弱點掃描，因此 OWASP 組織所提出之十大應用程序安全風險(Top 10 Web Application Security Risks)可協助辨識上線與維運時可能之風險，惟此方式未完整提供開發人員如何在開發過程中各階段之安全實作方式。在現今網路威脅不斷升溫情況下，為了讓開發人員在專案之初始階段便具備完整之資安防護概念與實作概念，OWASP 十大主動式控制 Top 10 Proactive Controls(以下簡稱 OPC)提供針對開發人員了解於每個軟體開發項目均應包含之安全技術，並依重要性排序，以供人員實作時參考使用。

以下將針對 OWASP 之 OPC 專案進行概述，並提供開發人員實作方向，藉此提升撰寫程式之安全程度。

2.1 OPC 專案與項目說明

OPC 專案主要目標為訓練開發人員具備安全開發能力，對於有些具備開發能力，但並未包含安全開發素養之人員是相當良好之參考素材，此十大主動式安全控制措施更可廣泛應用於各種應用程式中，每項控制項目提供項目概略說明，描述需要考量之實務議題等，OPC 十大工作項目依 OPC 列表之編號與重點分別為 C1 定義安全需求，藉由初始時定義應用程序之安

全要求，避免潛在漏洞威脅；C2 使用知名且積極維護之安全框架與函式庫，協助開發人員更有效地達成安全目標；C3 資料庫存取安全，旨在定義安全查詢、安全組態、安全認證及安全通訊，以確保資料存取安全；C4 使用資料編碼與跳脫等技術，以防禦注入攻擊(Injection Attack)、跨站腳本攻擊(Cross-Site Scripting, XSS)；C5 驗證所有輸入，確保只接受正確且有效之資料輸入；C6 實作數位身分，透過不同身分等級之驗證，確認欲存取之主體真確性；C7 執行存取控制，確認授權之真確性；C8 保護各處資料，透過正確保護資料方式，避免機敏資料外洩；C9 實作安全日誌與監控，安全日誌維運時可用於調校與診斷應用系統之運作，並於事件時檢視惡意行為之軌跡；C10 處理所有錯誤與例外，正確回應任何異常與錯誤，確保應用程式之安全。而最佳實作實踐，則說明如何以最好之規範進行實作與案例。專案項目亦提供應預防之漏洞說明，如避免出現已知之十大風險或通用缺陷列表(Common Weakness Enumeration, CWE)之漏洞等。另外，可從所提供之參考文獻，如 OWASP 備忘表(Cheat Sheet)，由各種不同應用系統專家於不同領域所創建，可供開發人員參考使用。最後專案項目列出不同項目之工具，藉由介紹能提供輔助之工具軟體或資源，提升安全整備度。

OPC 十大工作項目，詳見表 1，以下將依其重要順序說明開發時之關注重點與實作建議。

表1　OPC 列表

編號	英文名稱	譯名
C1	Define Security Requirements	定義安全需求
C2	Leverage Security Frameworks and Libraries	使用安全框架與函式庫
C3	Secure Database Access	資料庫存取安全

C4	Encode and Escape Data	資料編碼與跳脫
C5	Validate All Inputs	驗證所有輸入
C6	Implement Digital Identity	實作數位身分
C7	Enforce Access Control	執行存取控制
C8	Protect Data Everywhere	保護各處資料
C9	Implement Security Logging and Monitoring	實作安全日誌與監控
C10	Handle All Errors and Exceptions	處理所有錯誤與例外

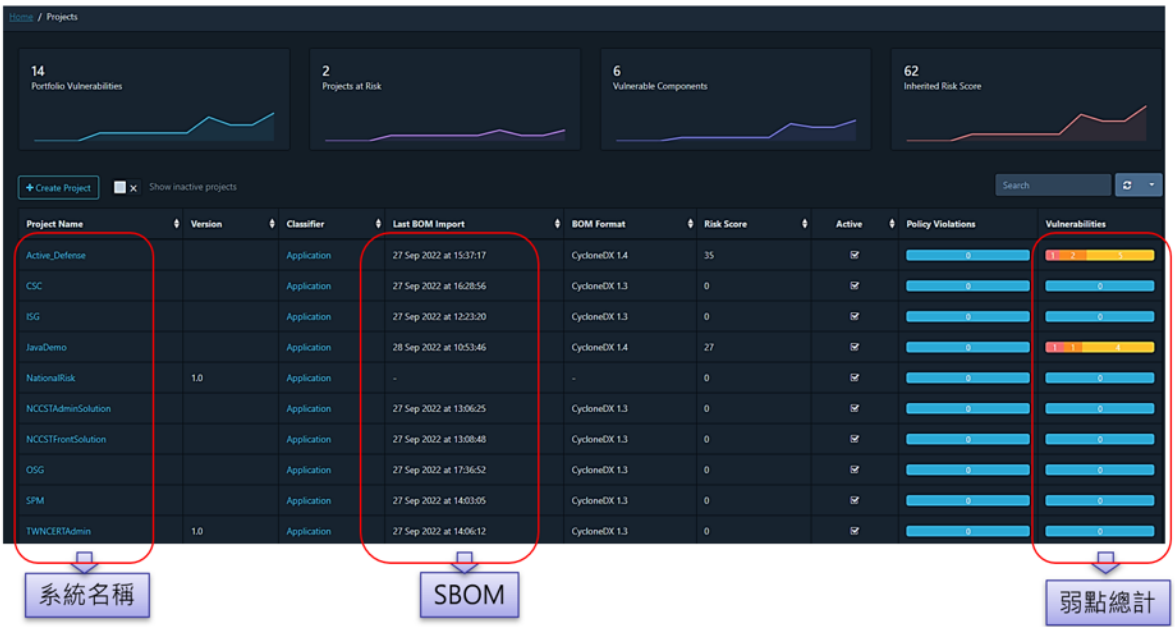
●C1.定義安全需求：定義安全需求以解決特定之安全問題或符合各種安全規範。定義安全需求為關鍵步驟，於開發新應用程式或版本更新時，若無妥善定義安全需求，將可能導致存在脆弱性之程式或後續需要花費更多時間進行漏洞修補。

實作案例為可透過需求討論或誤用案例(Misuse Cases)等活動發展安全需求，藉由參考如 OWASP 應用安全確認標準(Application Security Verification Standard, ASVS)等安全需求檢核表，預先確認已包含功能與非功能之安全措施，並規劃應用於 Web 應用程式與服務之設計、開發及測試使用。

●C2.使用安全框架與函式庫：使用具公信力且積極維護之框架或函式，並優先使用框架既有之安全功能特性，如能提供企業應用程式身份驗證、授權及其他安全功能之 Java/Java EE 框架 Spring Security 或 Flask Security 等，同時亦能藉由封裝函式庫，以減少攻擊面。

最佳實作包含建立並維護軟體物料清單(Software Bill of Materials, SBOM)，隨時關注函式庫與組件維持最新狀態，使用工具如 OWASP 關聯性檢視工具(Dependency Track/ Check)或 Retire.JS 等工具以追蹤 SBOM 之清單、相依性及漏洞。舉資安院使用 Dependency Track 為例，詳如圖

4，以圖示化方式呈現 SBOM 列表與漏洞。



資料來源：本報告整理

圖4　Dependency Track 示意圖

●C3.資料庫存取安全：確保對資料庫存取設定適切之身分驗證程序與組態。實作規範包含開發人員應先熟悉資料庫管理系統(DBMS)所提供之建置指引，符合安全組態設定，建立資料庫存取之安全服務或連結通道，如傳輸或 API 介接時之驗證與加密要求。同時使用參數綁定等技術防禦 SQL Injection 攻擊，可參考 OWASP 查詢參數備忘表(Query Parameterization Cheat Sheet)設定。

●C4.資料編碼與跳脫：編碼與跳脫主要是將特殊字元轉換為某種不同但等價之形式，用以防範跨站腳本攻擊，例如可參考使用 OWASP 防範跨站腳本攻擊備忘表(XSS Prevention - Stopping XSS in your web application)。

●C5.驗證所有輸入：預設所有輸入資料皆是不安全的，確保惟符合格式之資料才得以輸入。通則之實作規範為限制所有類型之輸入應用大小，其他重點包含應納入驗證語法有效性(Syntax validity)與語意有效性

(Semantic validity)，語法有效性為資料符合預期形式，如常見之身分證字號組成字元，以列表建立字元白名單或黑名單，在此例因建立黑名單恐曠日費時，可採取白名單作法。而語意有效性，以資料輸入範圍之合理性為例，如開始日期必須早於結束日期。

實作建議亦可藉由利用開發框架與函式庫提供之驗證功能，驗證資料類型、長度要求、整數範圍及空數值檢查等，自動化工具可運用 OWASP HTML Sanitizer、Java Hibernate Validator 及 PHP filter functions 等。

●C6.實作數位身分：建置數位身分鑑別機制，包含身份鑑別與會話(Session)管理，驗證主體所提出之身分，同時協助伺服器維護使用者所提出之身分狀態，且無需重複進行身分驗證。實作之身份驗證可參考 NIST 800-63b 數位身分指引(Digital Identity Guidelines)文件所提出之三個鑑別器保證等級(Authenticator Assurance Level, AAL)，決定所應用程式之身分識別要求。

●C7.執行存取控制：此程序重點為授權，確認准駁之請求，同時應注意授權程序並不等同於身分驗證程序，存取控制之要求可能必須在不同應用層中展現。存取控制(授權)設計建議原則，應提前設計相關機制，並具備其一致性之存取控制方式，例如，應強制所有請求皆需透過存取控制檢查，可考慮應用 Java Filter 確保所有網頁請求皆通過特定存取控制檢查邏輯。一致性存取控制原則應預設最小權限原則，僅提供依權責任務之必要存取權限，若發生系統錯誤或異常時，應拒絕任何存取權限進行，且若有新功能上線時，若組態尚未安全設定，應不允許任何存取服務。另一項實作存取控制重點為日誌紀錄之設定與儲存，特別是錯誤存取日誌，應依嚴重等級檢視且積極管控處理。

●C8.保護各處資料：惡意攻擊者可以透過多種方式從資通系統或公開網站相關服務應用程式中竊取資料，特別是敏感與機密資訊，對程式開發人

員首先應從資料分類分級開始，確認可能會處理、利用之資料機敏等級，再設計對應之保護原則。實作規範包含應用程式保密管理，如站台憑證、SQL 連線密碼等，透過適切之加密方式保護靜態資料，使用經過認證之加密演算法進行資料傳輸或處理、利用時之保護。特別應針對設計於行動式設備之應用程式，行動式設備由於其特性，機敏資料應設計儲存於特別目錄，並加以保護。

●C9.實作安全日誌與監控：對於程式開發人員，應記錄任何正常與異常行為，協助定義行為基準值，辨識與基準值不同之異常狀態以利追後續任何漏洞或安全議題。惟在設計所需儲存之日誌內容項目時，除非經過審核，不應記錄任何敏感或機密資料，例如，個人資料、交易訊息等。

實作建議應先實施編碼(Encoding)，針對任何風險字串進行記錄前之編碼與驗證，以防止日誌注入(Log Injection)攻擊，針對日誌之完整性，設計權責區隔之存取機制，且偵測任何篡改行為。維運日常之安全日誌，應使用標準且常用之日誌架構(Logging Framework)，例如 Apache Logging Services 或 SLF4J with Logback，並運用各種形式之自動化工具進行監控與日誌審查。

●C10.處理所有錯誤與例外：如何正確處理應用程式所出現之錯誤與異常狀況，首先要考量當異常狀況發生時，任何敏感資訊應妥善地被保護，而不因錯誤處理過程可能導致機敏資訊外洩或長時間無法提供服務。因此在程式設計時，若出現錯誤時，向使用者所揭露地資料應為最小訊息，但仍足夠讓使用者正確回應。實作規範應以集中方式管理任何異常資訊，避免程式碼內重複出現 Try/Catch 等程式區塊。自動化工具可使用 Error Prone，為程式碼靜態分析工具，可與程式建置流程整合，能找出更多程式碼潛在錯誤。

綜上所述，妥善運用 OPC，將可從中學習安全系統開發知識與防禦技術，

同時參考此專案所提供之自動化工具或備忘表，將可使開發過程更具效率，並預先於設計開始至每一階段皆致力於減緩漏洞發生之情況。以 OPC 預設安全之概念再搭配 OWASP Top 10 協助上線前與維運時辨識出可能風險，可相輔相成完成基於安全設計之原則。

3.資安技術研析_星際檔案系統濫用威脅分析

本季探討之資安技術研析為星際檔案系統(InterPlanetary File System, IPFS)濫用威脅之攻擊手法探討，多家資安公司觀測資安情勢指出，駭客開始使用防彈主機(bulletproof hosting)加入 IPFS 網路，防彈主機因提供網路或域名服務且不限制使用者上傳與發布之內容，因此會特意設於境外，以規避本地網路監督或法律追責，大多會被使用於發送垃圾郵件或其他非法服務，由資安事件中亦揭露多起惡意程式代管服務之防彈主機加入 IPFS 網路。此外，垃圾郵件(Mailspam)中常見之惡意後門程式，如 AgentTesla、LokiBot 及 Remocs 等，亦發現開始使用 IPFS 網路節點作為下載站之軌跡。

本院於觀測政府領域惡意電郵偵測機制，偵測出可疑惡意電子郵件約在1~3%區間，若再回溯關聯分析發現 IPFS 相關惡意電子郵件，以 111 年度平均約占 0.2%左右，整年 IPFS 相關惡意郵件占比率雖不高，惟若以年度長期觀測與統計，111 年濫用 IPFS 之釣魚攻擊郵件(Phishing)與惡意程式垃圾郵件攻擊數量明顯可見其逐月上升趨勢，分析發現 IPFS 濫用情形有日趨嚴重之情況，管理人員應事先了解其入侵途徑，並防範未然。

以下將概述 IPFS 之功能，並分析濫用威脅趨勢與案例。

3.1 星際檔案系統簡介與可能威脅濫用

有別於傳統之主從式架構，IPFS 為一點對點(Peer-to-peer, P2P)分散式檔案系統，主要用於實現檔案之分散式儲存、共享及持久化之網路傳輸協定。傳統網際網路檔案傳輸，以集中式主從架構之 HTTP 協定進行，因此若伺服器停擺或連線中斷，則無法傳輸檔案。運用 IPFS 檔案系統，則可輕易利用多個網路節點上傳送，因此內容將可以分散式存放且維持其存續性。

IPFS 自問世以來，廣泛應用於各項網路服務，如串流平台、網路文獻典藏

及線上市集等，現今也被視為一項新興 Web3 技術，如新創公司 Fleek.co，該公司去中心化開放式之 Web3 開發者平台已被大量廣泛使用，產品包含各式 IPFS 與區塊鏈服務，可窺見未來可能取代傳統雲端平台如 AWS 與 DNS 基礎設施等 Web2 服務。

IPFS 於網路中各檔案預設使用 SHA256 演算法建立其雜湊值，以辨識是否為相同檔案，傳遞內容時不僅可節約頻寬用量，且因其分散式架構可避免單點故障並防止分散式阻斷服務(DDoS)攻擊，另一 IPFS 服務被廣泛利用之原因為可運用星際命名系統 IPNS (InterPlanetary Name System)將網路域名(DNSLink 機制)對應至特定 IPFS 之內容定址 Content ID (CID)，以方便人們以易記的網址取代 CID 複雜的雜湊值。對使用者而言，可透過安裝軟體成為 IPFS 網路節點或使用公開 IPFS 閘道經 HTTP 協定以 CID 取得資料。

多起資安事件顯示駭客利用多項 IPFS 服務展開惡意攻擊，如設立釣魚網站、或於合法服務中暗藏惡意程式及利用 IPFS 作為通訊管道，以進行惡意 C2(Command and Control)命令控制。

舉最熱門之釣魚網站攻擊手法演示為例，詳見圖 5。

資料來源：本報告整理

圖5　IPFS 釣魚網站攻擊概述

IPFS 釣魚網站之所以無法於第一時間阻擋最主要的原因為其去中心化之特性，如內容雜湊定址、檔案分散儲存至多個網路空間及結合 URL 轉址導

向，導致無法即時追蹤分析特定 URL 特徵，並進行攔截。雖然部分 IPFS 閘道服務商，已開始針對此類釣魚網頁或惡意程式下載進行過濾阻擋，惟只需變更 IPFS 閘道，CID 內容保持不變，則依然可瀏覽與存取資料，因此無法成功以域名黑名單進行連線阻擋。

3.2 IPFS 相關惡意郵件威脅趨勢與案例分析

有鑑於政府機關面臨釣魚郵件與惡意程式垃圾郵件攻擊提升，以下將針對釣魚郵件攻擊與惡意程式利用合法平台散布之相關案例進行說明。

IPFS 釣魚郵件攻擊，主要藉由合法服務之閘道服務域名、雲端硬碟資料夾、目標郵件帳號及 Google 翻譯服務，將惡意檔案置放於這些服務上，因此建立惡意連結之方式更加彈性。釣魚郵件攻擊案例，駭客會先於 IPFS 系統上建置釣魚網頁，接著將釣魚網頁網址利用 Google 翻譯服務進行轉址，產生含合法服務域名與憑證之釣魚網址，詳見圖 6。

資料來源：本報告整理

圖6　利用 IPFS 合法服務掩飾非法網址

在使用者端，駭客會偽冒機關名稱，例如發現以「密碼更新或帳號更新」

等主旨，企圖騙取政府機關人員帳號密碼，事件範例如下，詳見圖 7。

資料來源：本報告整理

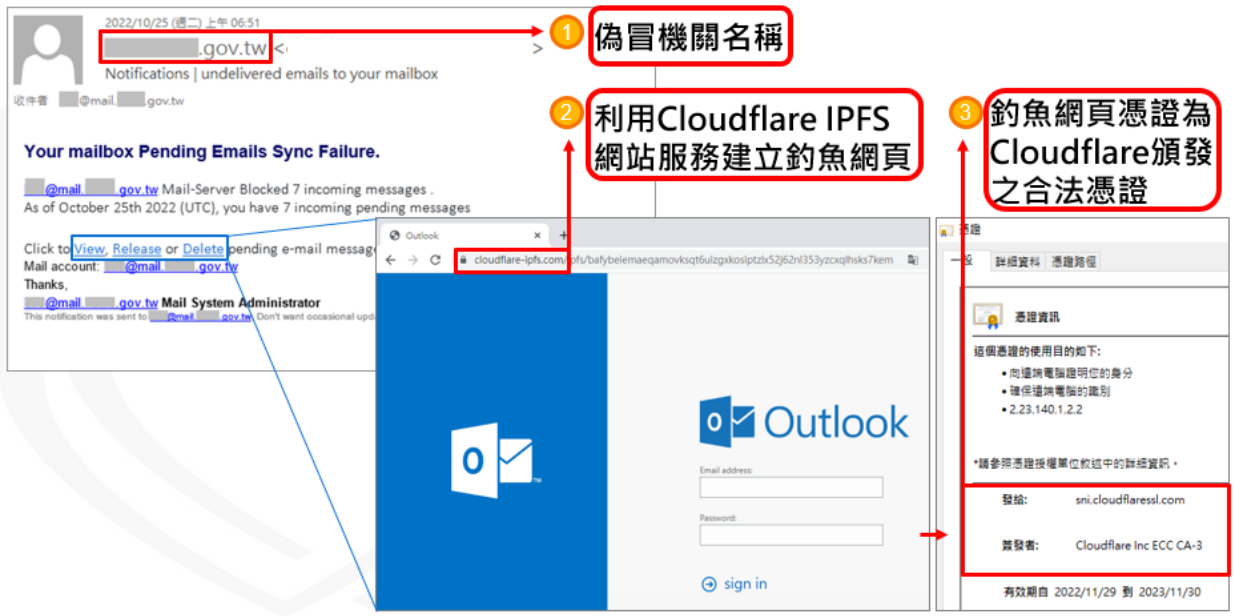
圖7　潛藏惡意連結之郵件

透過 IPFS 建立之釣魚網頁，網址可透過 Google 翻譯服務進行轉址，產生合法服務域名(*.translate.goog)與憑證之釣魚網址，因此將無法即時偵測其行為，駭客得以成功隱匿其非法意圖。事件範例如下，詳見圖 8。

資料來源：本報告整理

圖8　利用翻譯服務轉址功能取得合法憑證之網址

另一事件案例為惡意程式利用合法平台散布，駭客利用後端採用 IPFS 儲存檔案之第三方網頁託管服務，如 Cloudflare 來建立釣魚網頁以取得合法服務域名與憑證。該事件案例之駭客同樣偽冒機關名稱，寄出「郵件寄送失敗」等主旨之惡意社交工程郵件，範例詳見圖 9。



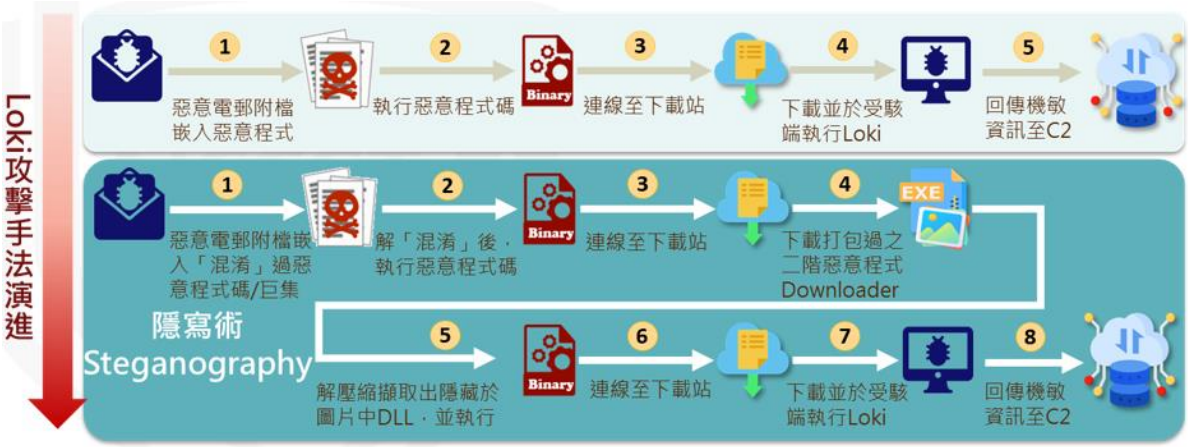
資料來源：本報告整理

圖9　利用合法網站服務取得合法憑證之網址

以上概述 2 種駭客於 IPFS 系統上建立釣魚網頁後，接續如何取得合法憑證網址之案例，經過合法平台掩護之釣魚網頁得以成功誘騙使用者點擊社交工程郵件連結，植入惡意程式於受駭者電腦後，竊取電腦機敏資訊。

在相關事件案例中也發現惡意程式攻擊有發展進化之趨勢，以往垃圾郵件散布之惡意程式多將 2 階後門程式透過圖像隱寫術(Steganography)編碼，並潛藏於惡意程式之資源區塊中，俟程式執行後再將資源解密與載入。惟通常此類型惡意程式，包含 1、2 階後門程式故檔案較大，較容易被資安防護系統偵測。現今分析資安事件中惡意程式演進案例，駭客會大幅縮減 1 階惡意程式之檔案大小做為下載器(Downloader)，再利用合法雲端平台與系統存放惡意程式作為下載站，透過連線合法網站下載 2 階後門程式，如 IPFS 系統、Discord 遊戲平台等。以縮減檔案大小與利用合法平台方式，藉此提升惡意程式存續性，並進行橫向擴散。以某事件為資訊竊取惡意程式 LokiBot 為例，駭客於惡意社交工程郵件附檔夾帶 1 階惡意程式為下載器，另將 2 階惡意程式(LokiBot)放置於 IPFS 系統上，攻擊流程詳見圖

10。



資料來源：本報告整理

圖10 1、2 階後門程式演進攻擊方式

IPFS 盛行原因為其新興應用服務，如可分散式儲存檔案協助數位典藏、具備網路頻寬用量節約之優點，且分散式架構能避免網站遭分散式阻斷服務攻擊而應用廣泛。但也因被駭客鎖定利用，大量運用合法服務以掩護其非法意圖，造成網路釣魚攻擊事件不斷。因其觸發方式多半透過社交工程手法，因此建議應持續加強內部資安意識宣導，於使用電子郵件、社群媒體或瀏覽器時，皆應強化相關防護動作。

4. 結語

本季具指標性案例為汽車業者因全球供應鏈網站漏洞，可能讓駭客輕易獲取機敏資訊。一位資安研究員揭露該公司網路應用系統存在嚴重漏洞，只需該系統使用者之電子郵件帳號，就可以成功取得該系統之控制權。針對供應鏈因全球化關係，致供應鏈邊界不斷擴展，首要之務應依其業務依存與關鍵性訂定管理規範，持續監督風險發生可能性。另一起案例為美國禁飛名單於駭客論壇遭公開分享，事件發生起因為某航空公司於 Amazon Web Services (AWS)雲端伺服器因組態配置錯誤，導致駭客可任意存取其資料庫，且之所以列為機敏資訊是因禁飛名單多涉及國家安全與反恐目的等，有其特別意義必須加強保護。雲端服務提供者亦歸屬於供應鏈之一環，為避免資安事故發生資料恐外洩之虞，建議機敏資料有加密後再置放於雲端之基本防護概念；另應針對雲端服務訂定一致性之安全組態設定與存取規則，如最小權限、持續驗證及日誌留存等管理機制。

國內部分，分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」類型為主，排除綜合類型「其他」外，其次分別為「設備問題」與「阻斷服務」為主要通報類型。針對本季全球與政府所面臨之主要資安威脅，本報告就「全球供應鏈之資安管理」與「雲端服務之資安管理」提出資安防護建議。而面對阻斷服務資安事件之升溫，機關對系統之可用性管理應加強，除於阻斷服務攻擊一開始時能快速偵測外，備援機制亦應妥善規劃，建議應維運具彈性之備援資源服務廠商與系統，於事件發生時提供即時之最小服務水準。

資安專題分享主題為 OWASP Top 10 Proactive Controls 概述與實作介紹，OPC 專案主要目標為訓練開發人員具備安全開發能力，共有十大主動式安全控制措施，可廣泛應用於各種應用程式中，每項控制項目提供項目概略說明，描述需要考量之實務議題等，藉由所提供之最佳實作，進行實作案例實踐。同時關注應預防之漏洞說明，如避免出現已知之十大風險或通用

缺陷列表漏洞等。建議系統開發人員，除關注系統是否有未修補之漏洞，亦應於系統開發期間，規劃導入 OWASP Top 10 Proactive Controls 專案概念，建立預設安全之資安防護等級。

另外，資安技術研析主題為星際檔案系統濫用威脅之攻擊手法探討，由資安事件中揭露多起惡意程式代管服務之防彈主機加入 IPFS 網路，垃圾郵件中常見之惡意後門程式，亦發現開始使用 IPFS 網路節點作為下載站之軌跡。觀測政府領域惡意電郵偵測機制，若以年度長期觀測與統計，111 年濫用 IPFS 之釣魚攻擊郵件與惡意程式垃圾郵件攻擊數量明顯可見其逐月上升趨勢，分析發現 IPFS 濫用情形有日趨嚴重之情況。星際檔案系統濫用，運用合法服務以掩護其非法意圖，造成網路釣魚攻擊事件不斷，因此建議應持續加強內部資安意識宣導，於使用電子郵件、社群媒體或瀏覽器時，皆應強化相關防護動作。