2018 資安年刊

台灣電腦網路危機處理暨協調中心

Taiwan Computer Emergency Response Team/Coordination Center

目錄

第一章、 前言 4

第二章、 資安通報現況與案例 5

第三章、 年度主要資安事件分析 8

3.1、 網頁挖礦程式事件 8

3.2、 手機間諜軟體分析—以 Skygofree 為例 12

3.3、 網路詐騙事件 14

3.4、 家用路由器遭駭客攻擊事件 20

3.5、 透過社交軟體散布詐騙訊息事件 27

3.6、 新加坡醫療資安事件 33

第四章、 情資發布與分享 34

4.1、 漏洞統計數據分析 34

4.2、 駭侵事件分析 35

4.3、 主流產品類別之弱點態樣 36

4.4、 年度主要產品漏洞技術 38

4.5、 常見駭客攻擊特徵 40

第五章、 資安政策與趨勢 40

5.1、 資安通報的挑戰與對策 41

5.2、 台灣資安弱點發布之現況與未來 45

5.3、 亞太地區電腦事故緊急應變團隊營運概要 49

5.4、 台美國家資通安全戰略比較 52

第六章、 TWCERT/CC 漏洞揭露政策 53

6.1、 簡介 53
6.2、 漏洞通報方式 54
6.3、 漏洞揭露方式 54
6.4、 漏洞報告公開時程 54
6.5、 漏洞報告處置流程 54
6.6、 CVE 編號發放規則 55
6.7、 漏洞通報者稱呼及聯繫方式公開 58
第七章、 合作交流與資安推廣 58
7.1、 國際資安組織交流現況 59
7.1.1、 參與亞太區電腦緊急事件回應小組 2018 年網路攻防演練(APCERT CYBER DRILL 2018) 59
7.1.2、 協助「No More Ransom」計畫完成正體中文網頁翻譯 59
7.1.3、 參加 30th FIRST 年會 60
7.1.4、 參與 THE HONEYNET PROJECT ANNUAL WORKSHOP 2018 61
7.1.5、 與 TEAM CYMRU 簽訂合作備忘錄 62
7.1.6、 與 FS-ISAC 簽訂合作備忘錄 62
7.1.7、 參與 OIC-CERT 2018 年網路攻防演練 62
7.1.8、 申請並成為 CVE 編號管理者 (CNA) 63
7.2、 國內資安推廣現況 64
7.2.1、 台灣 CERT/CSIRT 聯盟 64
7.2.2、 資安研討會/座談會協辦/演講 66
7.2.3、 2018 台灣資安通報應變年會成果紀實 68
結語 72
參考資料 73

第一章、 前言

隨著現今資訊科技運用普及與網際網路日益蓬勃發展，資訊通信科技已成為每個人日常生活中的一部分，改變了人類的生活習慣，但在享受舒適生活的同時，也衍生出政治、經濟、社會、科技及軍事等各層面之資安威脅，往往因一時的疏忽，釀成重大損失或無法挽救的地步，資訊安全成了目前社會所關注的重要議題之一。近幾年我國不斷出現機關電腦資料遭竊、帳號密碼遭盜用、金融機構遭駭侵盜領、勒索軟體威脅、電腦病毒發作及網頁遭置換等，資訊網路時代雖然便利，但同時也讓個人與企業暴露於危害之中。層出不窮的資安威脅，日新月異的攻擊手法，不僅影響個人、企業、甚至危害到國家安全，因此，建構一個安全的資訊使用環境，提升企業、人民對於資訊安全的認知，刻不容緩。

由於資安事件態樣多元，被攻擊目標也從傳統的資訊設備不斷延伸到通訊和工業控制設備；被竊取的資訊不僅包括經貿與科技等智慧財產，更擴及國家安全有關的外交、國防等機密。因此，全面的資安防護有必要整合政府國安、資安及通安三方面資安組織之量能，包含國家安全會議國家資通安全辦公室、行政院資通安全處及國家通訊傳播委員會，組成國家資安防護鐵三角，分別從國安、資安及通安等層面，保護國家安全及社會安全，建構國家整體資通安全防護網。

另外「行政院國家資通安全會報」亦設立了「關鍵資訊基礎設施安全管理組」及「資安產業發展組」，來提高資安事件應變之組織層級、強化關鍵資訊基礎設施的安全及提升資安產業的合作量能。相關法規方面，我國政府亦持續完備與落實《資通安全管理法》、《個人資料保護法》等資安法規，並將網路空間治理概念納入《國家安全法》、《數位通訊傳播法》及《電信管理法》等法規修訂。

國家資安聯防體系的建立，包含由國安、國防單位及行政院各部會，分工籌組並整合資安緊急應變小組、資安事件通報及處理小組、資安維運及預警中心、以及情資分享與分析中心等單位，建立以「情報驅動」(資訊分享並協同應變) 的資安聯防架構，提升早期預警、緊急應變及持續維運的能量及效率。

目前我國在民間企業推展資安所面臨的最大困難與挑戰就是：當企業發生資安事件或個

資外洩時，一般都選擇保持沉默，並未告知主責機關或利害關係人，或各企業只在乎營運績效與成本，對於資訊安全並不太重視，也未將其視為應盡之企業社會責任，為了因應這些問題，政府除應完善各種資安法規與規範外，同時亦應有適當的獎勵與罰責，如此才能促進民間企業對資安與個資防護的重視。

資安防護的推動應由政府帶頭做起，並配合軍方、產業界、學界和研究單位共同參與，如此才能共同朝資安聯防之路邁進，以提升台灣自主資安防護的能力，打造我國健全的資安聯防體系。未來資安防護已不再僅僅是政府或專家的責任，每個人都肩負著這項使命，期望未來我們能迎向一個健全的網路環境。

第二章、 資安通報現況與案例

TWCERT/CC 的通報情資來源非常廣泛，除了國內企業組織、學研單位、資安機構，以及駭客社群等組織外，也與國際 CERT/CSIRT、資安相關單位等進行合作，

而在 TWCERT/CC 接收到情資後，會針對該情資進行研判，若為國內資安事件會透過 N-ISAC 通報到相關單位進行處理；若為民間企業組織通報特定資安事件，TWCERT/CC 會直接處理；而若情資屬於國外資安事件，則會通報到國外相關單位協請處理。

本中心 107 年度 1 月至 12 月止，接收來自 20 個國家之資安通報，共計 31,093 筆情資，其中，針對日本 Rakuten-CERT 請 TWCERT/CC 協助處理我國對該公司的惡意攻擊事件之惡意 IP 通報為最大宗(12,322 筆)，其次為美國(10,812 筆)及台灣(7,639 筆)所通報的資安事件，如圖 1 所示。分析其攻擊手法為「嘗試利用 IP 以不同的 Email 進行目標系統登入」，嘗試登入的次數從數十次到上百次之多，有部分帳號已成功登入，研判相關 IP 之主機可能已遭有心人士掌控。

TWCERT/CC 接獲該情資後，陸續透過國家資安資訊分享與分析中心(National Information Sharing and Analysis Center, N-ISAC)完成通報作業，並於 107 年 4 月份電子報中，提醒民眾注意資訊設備的監控措施，若確認該資訊設備已遭入侵，建議重新安裝作業系統，並更新至最新修補程式，若作業系統無法重新安裝，則需執行惡意程式檢測，亦建議需

更換系統使用者之相關密碼；若暫時無異常行為，建議安裝防毒軟體，除需將軟體版本及病毒碼更新至最新版，並需確認病毒碼持續更新設定，另亦需隨時注意與自身設備及系統相關的資安情資。

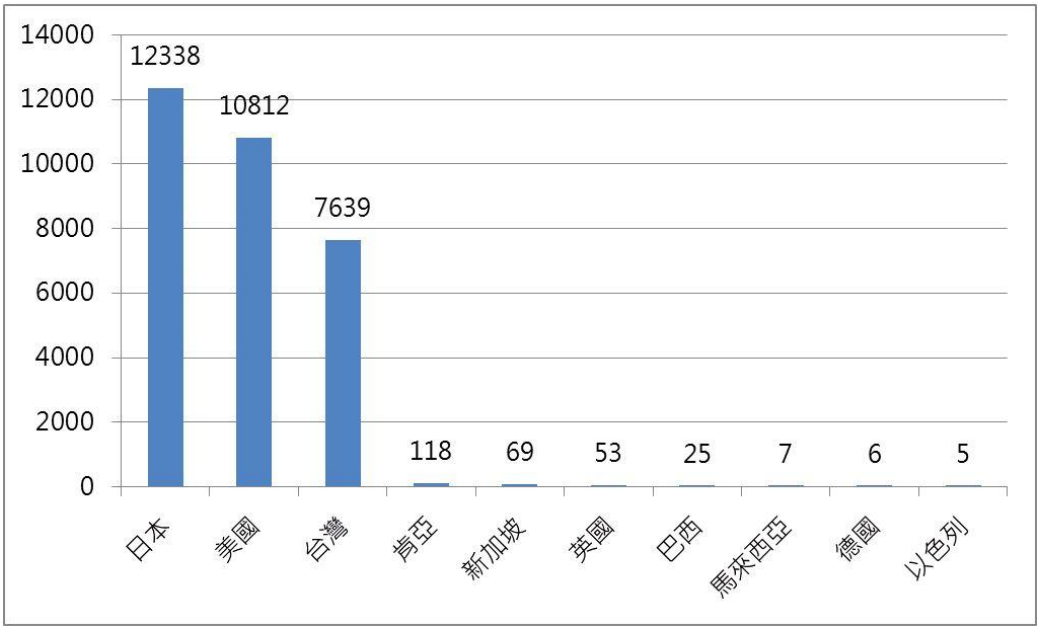


圖 1 通報來源統計圖

1 月至 12 月有效通報筆數合計 31,093 筆，包括國內 7,639 筆及國外 23,454 筆(如圖 2)，其中美國國土安全部(DHS)之自動化資安威脅情資共享計畫(Automated Indicator Sharing, AIS)情資計 4,149 筆，占 13.34%，反釣魚工作小組(Anti-Phishing Working Group, APWG)情資計 3,746 筆，占 12.04%。

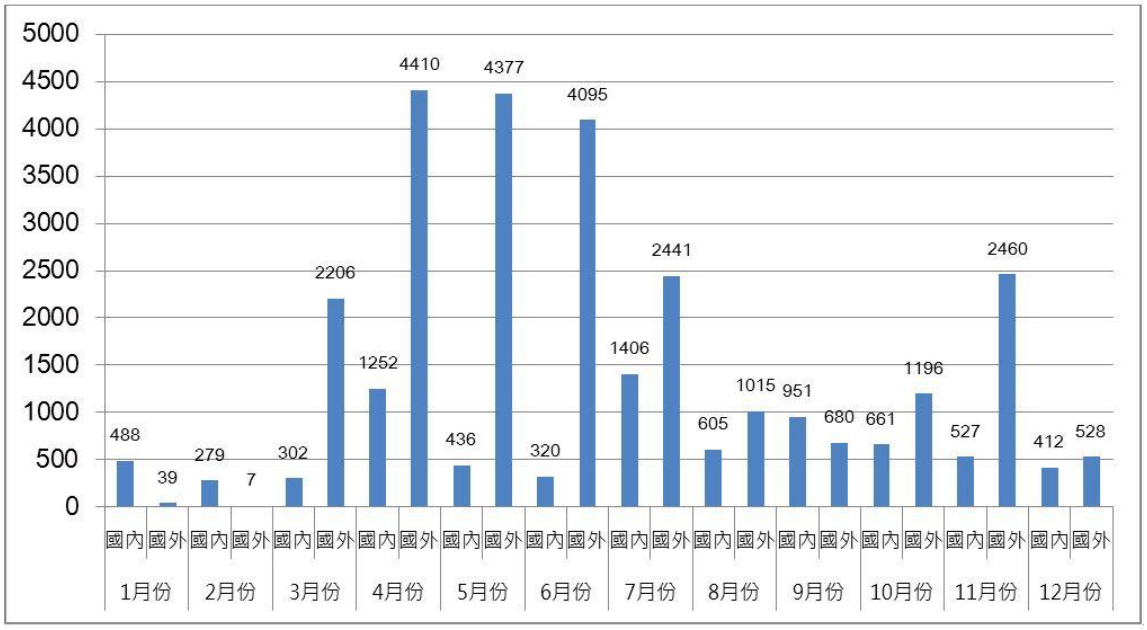


圖 2 通報來源統計圖

TWCERT/CC 針對所接獲之通報情資，會進行攻擊源 IP 所屬國家以及攻擊類型分析，再將情資提供給予相關單位，其中通報對象以台灣為最大宗，占上半年度通報對象 86.7%，美國次之，占通報對象 1.8%(如圖 3)。

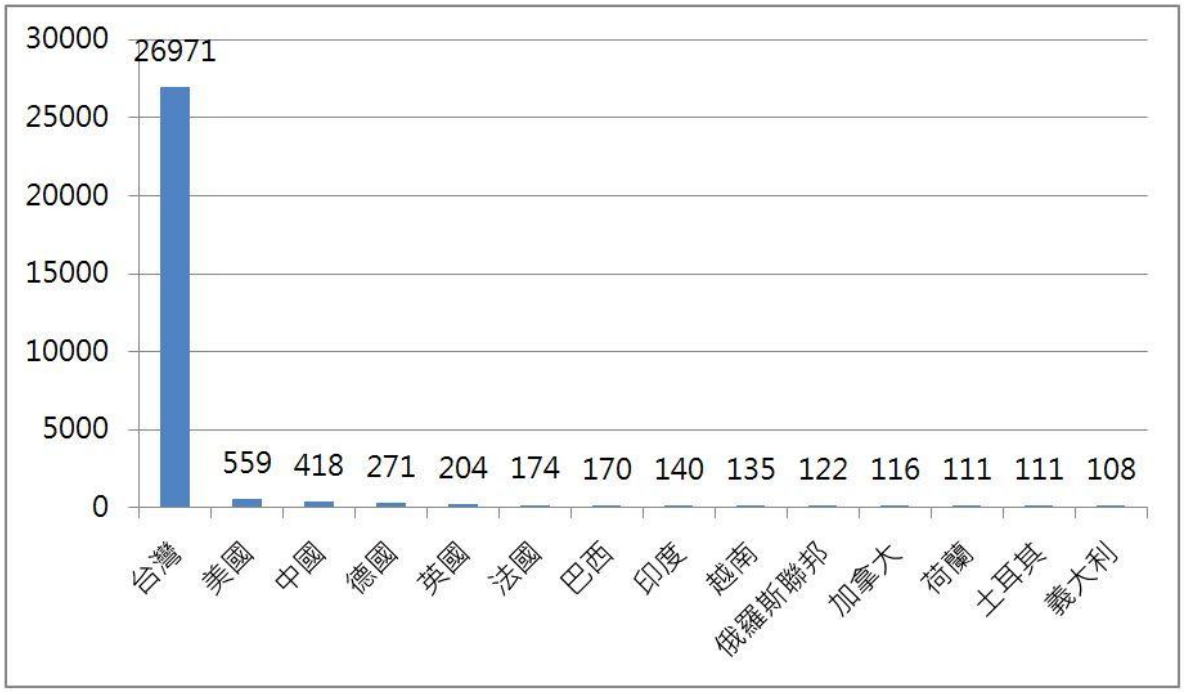


圖 3 通報對象統計圖

若依通報類型做分析，則以對外攻擊為最大宗，合計 25,879 筆(如圖 4)，占 83.23%，其中日本 Rakuten-CERT 通報之情資占對外攻擊類型高達 47.6%。其中對外攻擊類之主要原因

為攻擊源 IP 之主機或資訊設備遭植入惡意程式或遭駭客控制，而對外發送攻擊封包，本年度常見的其它類的攻擊尚包括電子郵件社交攻擊、垃圾郵件、釣魚網頁等網路釣魚攻擊，以及利用系統弱點進行的攻擊行為通報案件，包括網頁置換、系統存在弱點、C&C 及殭屍電腦等。

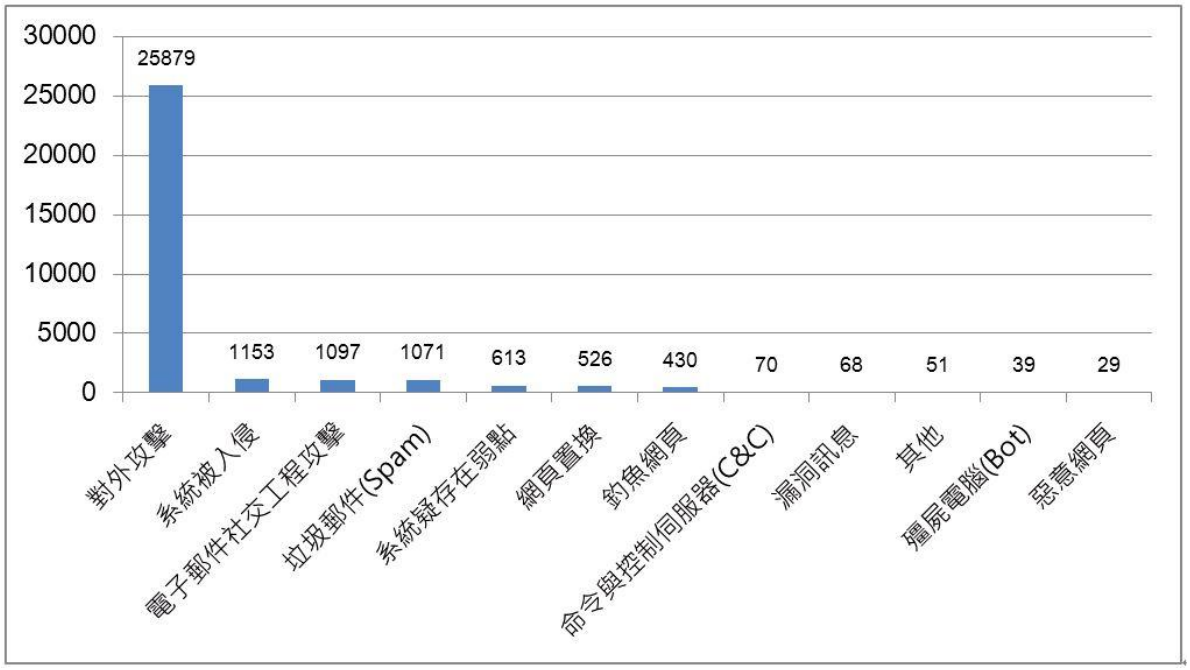


圖 4 通報類型統計圖

第三章、 年度主要資安事件分析

TWCERT/CC 平時除了蒐整國內外資安情資外，亦針對一些近期較夯的資安事件進行分析，並撰寫相關處置建議，讓民眾平時就能提高警覺，若不幸受駭時，亦能即時掌握狀況，快速排解問題。以下將針對網頁挖礦程式、手機間諜軟體、網路詐騙事件、家用路由器安全風險與防護、社交媒體假消息散布，以及新加坡醫療資安事件進行分析與探討。

3.1、 網頁挖礦程式事件

近年來隨著虛擬貨幣的價值飆漲，越來越多人熱衷於虛擬貨幣開採(挖礦)，紛紛建置挖礦機來開採虛擬貨幣，有心人士更將挖礦程式植入網站中，讓網站瀏覽者協助其挖礦，當使用者不慎點選並瀏覽這些網站時，即遭利用成為礦工。

根據知名廣告過濾服務商 AdGuard 在 2017 年 10 月的報告[1]中指出，在全球流量排行榜上前 10 萬名網站中，有 220 個網站暗藏了至少一種 JavaScript 挖礦程式碼，包括 Coinhive、

JSEcoin、CryptoLoot 及 MineMyTraffic 等，不一而足。在這 220 個藏有挖礦程式碼的網站中，以來自美國的網站為最大宗(占 18.66%)，其次是印度(占 13.4%)、第三名則是俄羅斯(占 12.44%)，台灣也有 4 個網站內藏挖礦程式，然經 TWCERT/CC 於 2018 年 3 月進一步追查，已確定該 4 個網站皆已無挖礦行為。

TWCERT/CC 於 2017 年 12 月接獲某國 CERT 情資，揭露台灣有 16 個網站藏有 Coinhive 挖礦程式，經 TWCERT/CC 清查後，發現多屬私人或企業架設之網站，包含某蔬食網站、某租屋網站及某生態介紹網站等。此外，TWCERT/CC 亦主動查找國內其它疑似遭植入挖礦程式的網站，並通報協處。以下茲以 TWCERT/CC 所發現國內某大學系所官方網站遭植入挖礦程式的案例進行說明，陳述 TWCERT/CC 近期處理相關通報與發現台灣網站遭植入惡意挖礦程式案例之攻擊態樣與手法分析，並提供企業與民眾簡易的辨別及防範方法。

在本案例中，該系所網站遭植入 Coinhive 挖礦程式後，同樣會導致瀏覽該網站的使用者，其 CPU 使用率異常飆升(如圖 5 所示)。經分析發現，該網站亦未隱藏用以開發的軟體版本相關資訊(如圖 6 所示)，網頁程式碼中亦含有 Coinhive 挖礦程式及 Coinhive[.]com 註冊的 Site Key(如圖 7 所示)。

圖 5 瀏覽某大學系所網站，會造成 CPU 使用率飆升

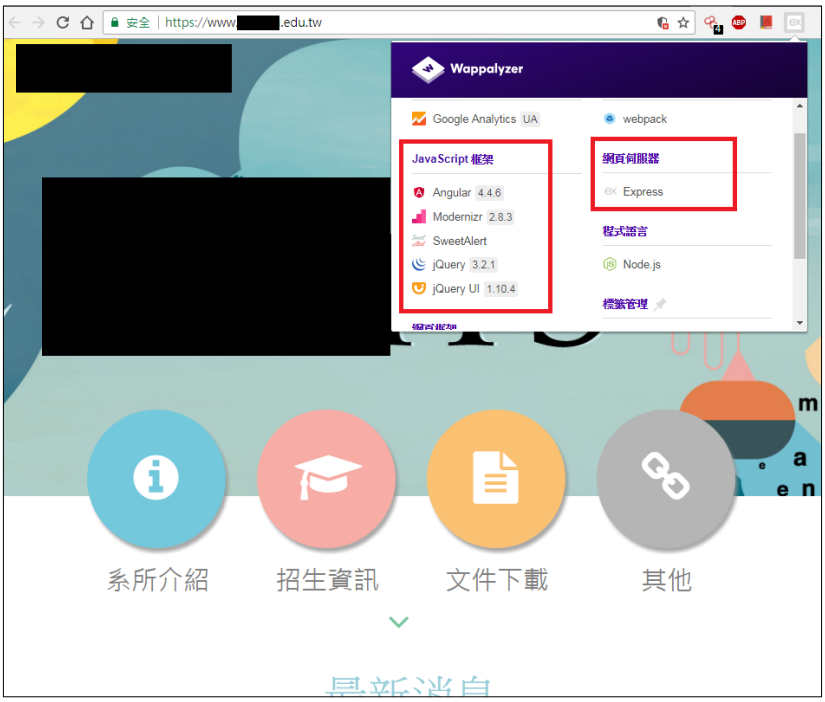


圖 6 該系所未隱藏用以開發網站的軟體版本資訊

圖 7 該系所網站遭植入 Coinhive 挖礦程式及其 Site Key

上述的網頁挖礦攻擊手法被稱之為「挖礦劫持」(Cryptojacking)[2]，使用者需連回虛擬貨幣的伺服器下載挖礦程式，才可以進行挖礦(如圖 8 所示)。

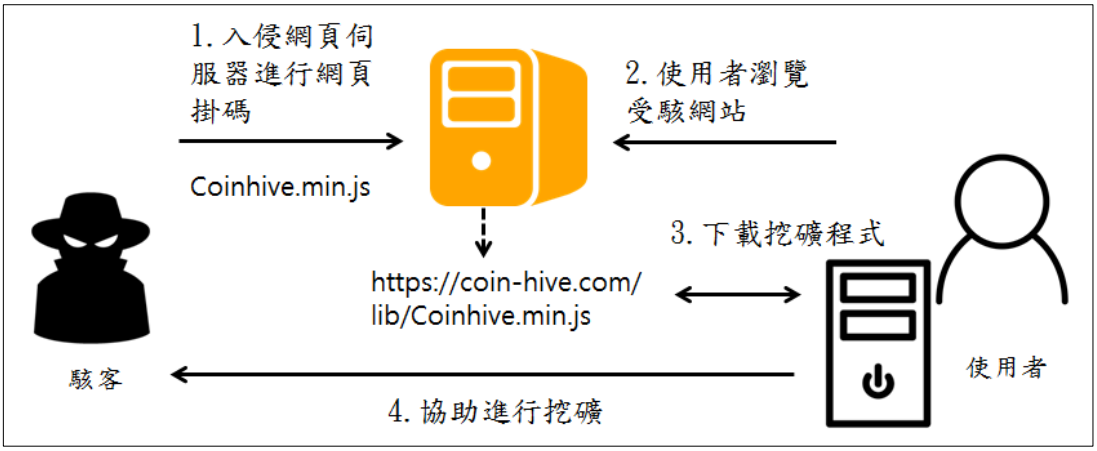


圖 8 Coinhive 網頁挖礦手法

TWCERT/CC 彙整目前常見的挖礦程式碼如下：

- digxmr[.]com/deepMiner.js
- coin-hive[.]com/lib/coinhive.min.js
- crypto-loot[.]com/lib/miner.min.js

根據 TWCERT/CC 的國內通報案例及協處經驗，多數企業網站管理者若未經 TWCERT/CC 通報，皆不知其所有網站已遭有心人士植入挖礦程式。本中心在協助企業移除挖礦軟體時，亦提供企業初步自行檢查網站是否被植入挖礦程式的方法，並提醒企業所應執行的系統安全性檢查與網站應用程式的漏洞修補，以避免再次遭駭客利用挖礦。

針對防範諸如 Coinhive 等挖礦惡意程式之攻擊，TWCERT/CC 提供以下四項防護建議：

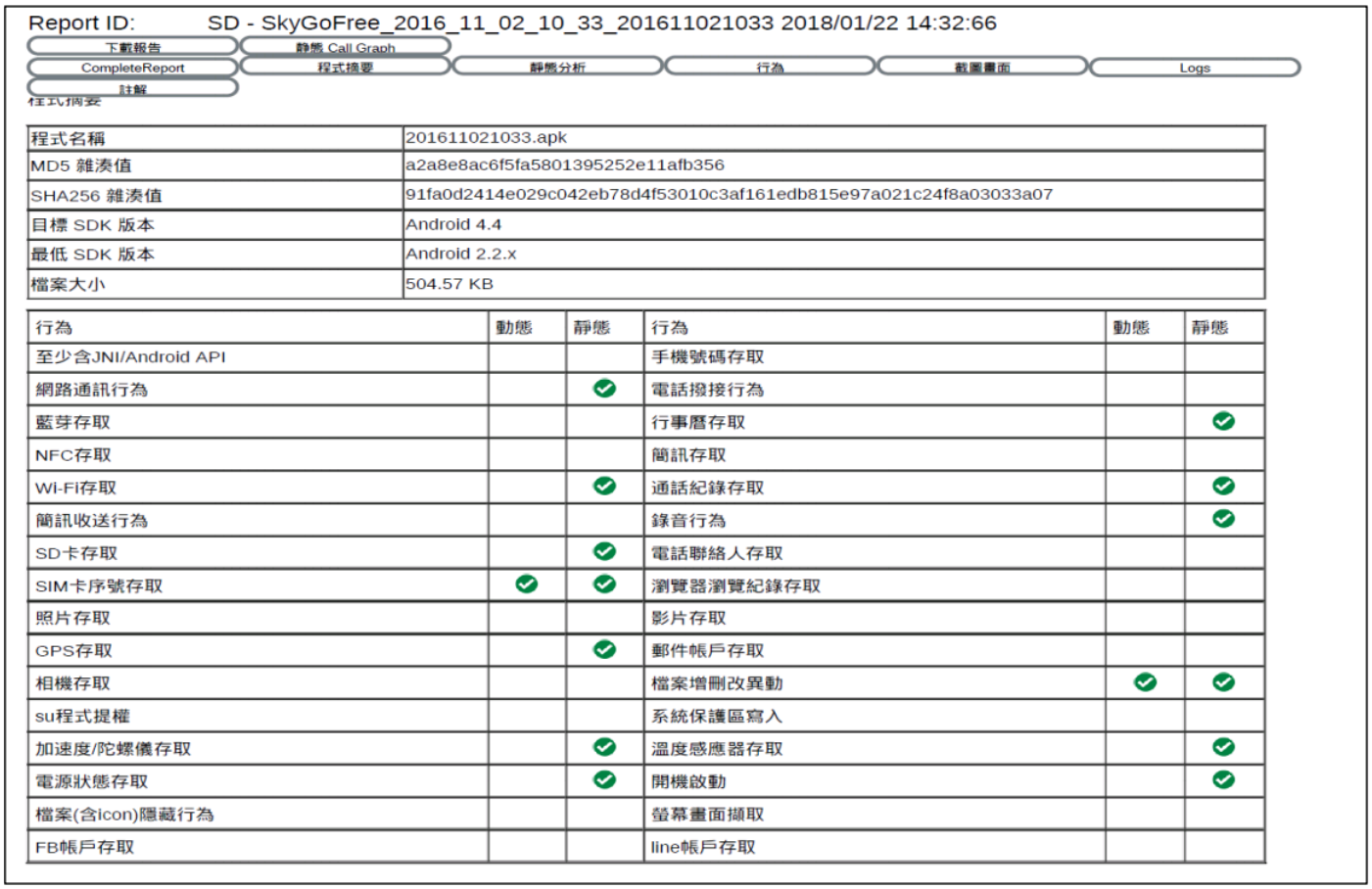
1. 使用者在瀏覽網站時，若在非預期情況下，發現系統效能持續降低，應提高警覺，並依上述案例所提供的檢查方式，查看所瀏覽的網站是否含有挖礦程式，若有，建議應通報 TWCERT/CC。
2. 使用者可於瀏覽器中安裝防止挖礦程式執行的合法外掛程式，例如 AdBlock Plus[3]、Adguard[4]、AntiMiner[5]、MinerBlock[6]或 No Coin[7]，來阻擋已知的挖礦程式。
3. 網站管理者若發現其網站遭植入挖礦程式，應在確認惡意程式碼所在位置後移除之，並全面檢查與強化系統的安全性，以降低再次被利用挖礦的風險。

網站管理者應隱藏網站伺服器、網頁開發框架等系統資訊，避免開啟未使用的通訊埠，

及定期更新防毒軟體、作業系統及應用程式，以降低網站被攻擊利用的風險。

3.2、 手機間諜軟體分析—以 Skygofree 為例

手機可說是現代人最為普及的隨身攜帶行動裝置，而在諸多行動裝置應用程式中，以即時通訊 App 最常為一般使用者所使用，如 Facebook Messenger、WhatsApp Messenger 等。駭客常以社交工程手法誘騙使用者下載安裝手機應用程式，並同意特定存取功能，進而竊取手機資料。2018 年 1 月，網路上公布了一個手機間諜軟體 Skygofree，該軟體能夠記錄行動裝置周遭的聲音、側錄鍵盤及竊取裝置上的 LINE、WhatsApp 或 Facebook Messenger 的通訊訊息記錄。TWCERT/CC 針對 Skygofree 樣本進行惡意行為分析，其竊取手機資料手法為誘使使用者開啟無障礙工具(Android Accessibility)功能，藉以竊取通訊軟體即時訊息畫面，依據 TWCERT/CC 所發布的手機間諜軟體分析—以 Skygofree 為例的文件[8]指出，Skygofree 惡意程式家族的主要惡意行為為目標手機的相關資訊竊取，包含 Wi-Fi 存取、相機存取、加速度/陀螺儀存取、溫度感應器存取、電源狀態存取、SIM 卡序號存取、手機號碼存取、行事曆存取、通話紀錄存取、錄音、郵件帳戶存取、開機啟動、網路通訊、SD 卡存取、GPS 存取、檔案增刪改異動、系統保護區寫入、檔案(含 icon)隱藏及安裝程式。



Report ID: SD - SkyGoFree_2016_11_02_10_33_201611021033 2018/01/22 14:32:66

下載報告 | 靜態 Call Graph | CompleteReport | 程式摘要 | 靜態分析 | 行為 | 截圖畫面 | Logs | 註解

程式摘要

程式名稱	201611021033.apk
MD5 雜湊值	a2a8e8ac6f5fa5801395252e11afb356
SHA256 雜湊值	91fa0d2414e029c042eb78d4f53010c3af161edb815e97a021c24f8a03033a07
目標 SDK 版本	Android 4.4
最低 SDK 版本	Android 2.2.x
檔案大小	504.57 KB

行為	動態	靜態	行為	動態	靜態
至少含JNI/Android API			手機號碼存取		
網路通訊行為		✓	電話撥接行為		
藍芽存取			行事曆存取		✓
NFC存取			簡訊存取		
Wi-Fi存取		✓	通話紀錄存取		✓
簡訊收送行為			錄音行為		✓
SD卡存取		✓	電話聯絡人存取		
SIM卡序號存取	✓	✓	瀏覽器瀏覽紀錄存取		
照片存取			影片存取		
GPS存取		✓	郵件帳戶存取		
相機存取			檔案增刪改異動	✓	✓
su程式提權			系統保護區寫入		
加速度/陀螺儀存取		✓	溫度感應器存取		✓
電源狀態存取		✓	開機啟動		✓
檔案(含icon)隱藏行為			螢幕畫面擷取		
FB帳戶存取			line帳戶存取		

圖 9 Skygofree 行為分析結果

印度政府在 2017 年底由負責蒐集國外情資的印度調查分析局（Research and Analysis Wing, RAW）與直屬印度總理辦公室國安顧問的國家技術研究組織（National Technical Research Organisation, NTRO）亦發出一份報告，指出有 42 個 APP 有資安風險，並通知印度軍方所有官兵與官員刪除這些軟體(如下圖 10)。

圖 10 印度政府指出有 42 個 APP 有資安風險

為防範類似 Skygofree 手機惡意程式之攻擊，TWCERT/CC 建議不要從來源不明的網站下載手機應用程式；安裝手機應用程式時，需確認手機應用程式存取系統功能之必要性及其風險，如有疑慮切勿執行安裝。此外，如非必要，建議關閉 Accessibility 功能，並應確保 Android 作業系統升級至最新版本，以避免類似 Skygofree 等有資安風險之間碟或惡意攻擊。

3.3、 網路詐騙事件

由於電子商務盛行，網路上有愈來愈多的電子商務平台成立，為達商品廣告效益，許多商品利用社群媒體(如：Facebook、Line 等)的高點閱率，進行網路行銷。近期網路上出現大量的惡意賣家，利用上述特性建置一頁式商品廣告頁面，並向社群媒體購買廣告，進行網路行銷詐騙，如圖 11、圖 12 所示。

圖 11 透過臉書散布一頁式廣告連結

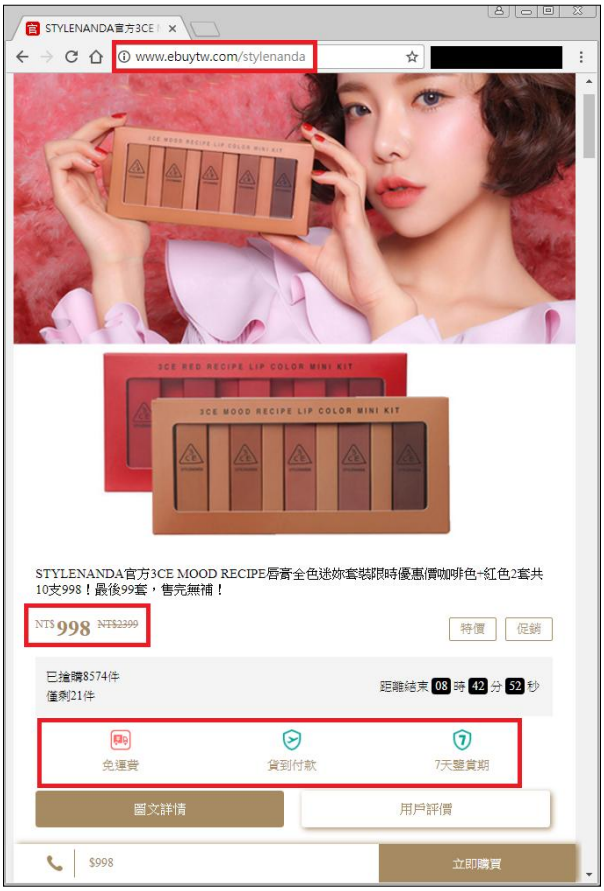


圖 12 一頁式廣告案例

以台灣內政部警政署刑事警察局於 2018 年 3 月 27 日破獲之上海「壹加壹國際物流公司」一頁式詐騙事件為例[9]，負責人與境外詐騙集團合作，由詐騙集團擷取或變造台灣知名人物或電視台官方網站影像，結合時事、八卦等議題書面文字，在臉書粉絲專頁散布「一頁式廣告」連結，以吸引民眾上網瀏覽時點閱廣告，並誘導民眾誤信廣告內容下訂購物。該起一頁式廣告詐騙流程如圖 13 所示。

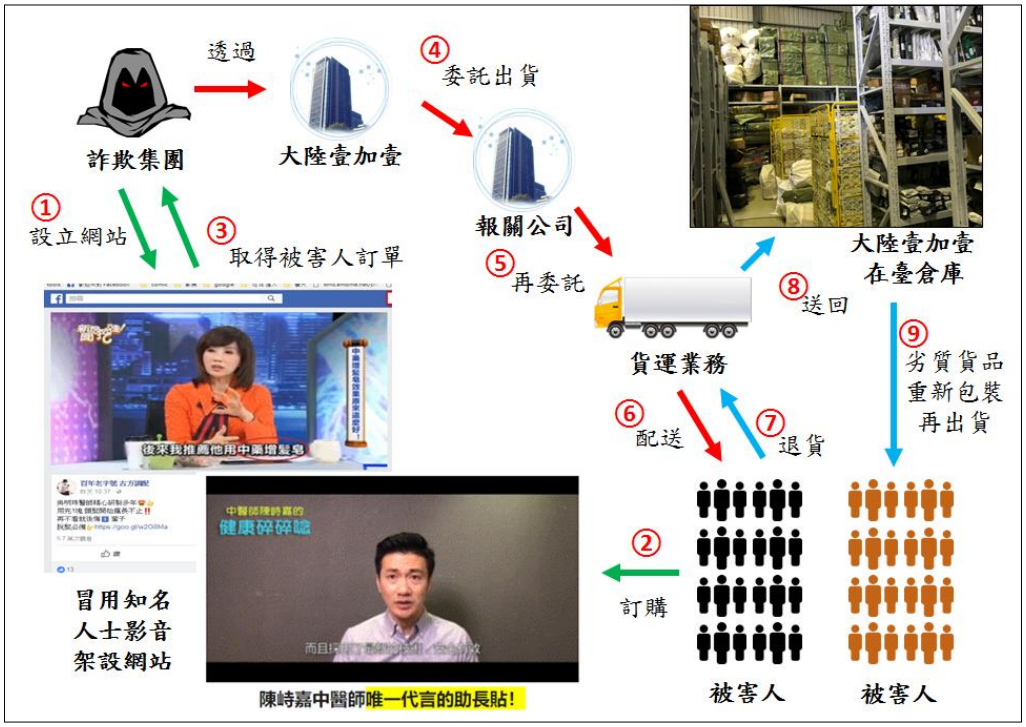


圖 13 一頁式廣告詐騙流程

TWCERT/CC 分析刑事警察局自 2018 年 1 月 29 日起所提供之一頁式廣告網址清單共 937 筆，發現一頁式廣告以夾藏於 Facebook 連結為最大宗傳播方式(計 98 筆)，其網址多以 https://www.facebook.com/[商品相關敘述]，來誘導使用者點選並開啟廣告連結，進而選購商品。進一步清查此類一頁式廣告網址所註冊之國家，並彙整刑事局所提供之詐騙情資後，TWCERT/CC 發現詐騙集團多將一頁式廣告伺服器架設在境外，且以中國大陸居多。此外為躲避查緝，這些廣告的提供者通常在廣告釋出一週後，即再更換其他類型廣告內容，網址也隨之改變，導致追查困難度大幅提升。

雖然 TWCERT/CC 積極將可疑網址通報至所註冊之所屬國家 CERT 組織，但是針對此類通報，國際 CERT 組織通常表示：此種一頁式廣告所連結之網頁大多未含惡意程式碼，不具

資安威脅，故以 CERT 權責角度，無法單以詐騙網頁為由，協助移除相關網頁或阻擋該網域；若單以詐騙網頁為由，移除合法登記註冊之廣告專頁，恐將引起後續糾紛。有鑑於此，TWCERT/CC 目前僅以通報遭駭客利用，並以一頁式廣告方式散布的惡意廣告連結為主(如圖 14 所示)，請求國際 CERT 予以協處，以阻擋惡意連結繼續散布。

圖 14 一頁式廣告遭 Virustotal 檢測出夾帶惡意程式碼

TWCERT/CC 分析 2018 年 3 月份由刑事局所提供之一頁式廣告連結清單，發現僅有 4.08%的廣告連結遭檢測出夾帶惡意程式碼，表示此類廣告存在資訊安全疑慮的情況仍偏低，致使社群平台、廣告業者及各國 CERT 組織直接就源頭下架或阻擋此類詐騙廣告的比例仍偏低。因此 TWCERT/CC 呼籲各國 CERT 組織、檢調單位、社群平台及廣告業者應該將此類一頁式廣告內容的合法性納入協處考量，必要時檢調單位可與 CERT 組織合作追查，以有效阻擋此類廣告的流竄，降低消費者遭到詐騙而蒙受財物損失，或是被駭客植入惡意程式的可能。

針對如何防範透過社群媒體所散布之一頁式廣告詐騙行為，TWCERT/CC 除呼籲社群媒體應重視並審核廣告之內容合法性以外，並彙整此類詐騙廣告特色[10]、目前本中心因應作為，及提供民眾初步防護方式如下：

一、 詐騙廣告六大特色：

- 特徵 1：網頁上未標明公司地址及客服電話，僅留電子信箱。
- 特徵 2：售價下殺 1 折、3 折，明顯低於市場行情。
- 特徵 3：以倒數計時、存貨不多等吸引民眾，但時間、庫存永遠倒數不完。
- 特徵 4：免運費，且號稱有 7 天鑑賞期，並可拆箱驗貨。
- 特徵 5：只能使用貨到付款或信用卡付款(若消費者使用信用卡付款，將有被盜刷的風險)。
- 特徵 6：網頁常有簡體字或中國大陸用語(例如：支付、直郵、郵費、信息)。

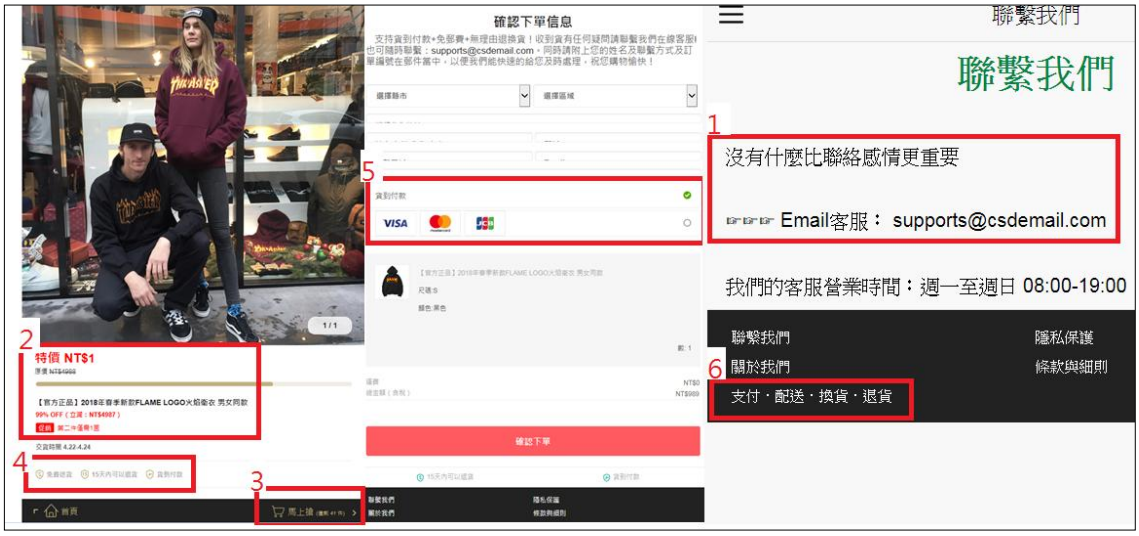


圖 15 一頁式廣告特徵

使用者瀏覽網頁時，若發現上述特徵(如圖 15 所示)，應立即關閉所瀏覽之網頁。

二、 本中心針對一頁式詐騙廣告之因應作為：

1. 密集實施主題式多元宣導

透過 TWCERT/CC 官方網站與臉書專頁及發布新聞稿，宣導民眾勿點擊一頁式廣告購物。

2. 協調國際合作防制

由於一頁式詐騙廣告網址多為國外網域，難以溯源追查，刑事警察局爰自 107 年 1 月 29 日起，按週提供「詐騙反饋平臺」詐騙網址資料予本中心，以協助通報各國 CERT

進行分析處置。

三、 本中心針對如何減少遭一頁式廣告詐騙之初步防護建議：

1. 使用者可利用第三方支付機制，確認貨品無誤再付款，並選擇評價良好、具有實體店面的賣家，以增進交易安全之保障。
2. 使用者應詳閱社群媒體所宣告之隱私權政策，修改個人之廣告偏好，並減少以社群媒體帳號登入其他服務。
3. 使用者可於瀏覽器安裝廣告阻擋外掛程式，例如 Adblock Plus 或 AdGuard，以阻擋已知的惡意廣告連結。
4. 使用者若發現不法臉書粉絲團散布詐騙廣告，應該主動取消追蹤該粉絲團(如圖 16 所示)，或者進一步向臉書檢舉該頁面散布不實廣告(如圖 17 所示)，以減少接收惡意廣告的機會。

圖 16 暫停追蹤可疑的臉書粉絲團

圖 17 透過臉書封鎖及檢舉粉絲專頁

3.4、 家用路由器遭駭客攻擊事件

近來全球發生數萬起家用路由器遭駭客攻擊事件：駭客入侵路由器並竄改網域名稱系統設定(DNS)，將使用者網路連線導至惡意網站，並誘導 Android 系統使用者下載惡意程式，竊取其銀行帳戶、手機通聯紀錄等敏感資訊，該事件以南韓、日本、中國、香港及台灣等亞洲地區國家為主要攻擊目標[11][12]。2018 年 5 月，台灣居易科技公司(DrayTek)所生產的路由器弱點被揭露[13]，導致用戶的 DNS 設定遭駭客竄改，並將連接該路由器用戶的網址導向惡意伺服器，使駭客得以用釣魚網站蒐集用戶的資訊，受影響的家用路由器超過 25 款；同月 Cisco 公司亦發現專門攻擊家用路由器及網路儲存設備的 VPNFilter 病毒，影響超過 50 萬個網路裝置[14]，顯見駭客已鎖定家用路由器進行攻擊。

卡巴斯基實驗室研究人員在 2018 年第一季的 APT 攻擊趨勢報告[15]中表示，家用路由器已成為駭客愈來愈常攻擊的標的。2018 年 3 月起，趨勢科技與卡巴斯基分別不約而同地偵測到了因家用路由器遭駭侵並導致使用者行動裝置遭植入惡意 APP 之攻擊案例(趨勢科技命名為 XLoader、卡巴斯基命名為 Roaming Mantis、行政院國家資通安全辦公室技術服務中心命名為少爺[16])，其攻擊手法皆為竄改使用者家用路由器之 DNS 設定，當使用者以行動裝置連接該受駭路由器上網時，會將使用者連線導到惡意伺服器，並誘騙使用者下載安裝惡意 APP

程式，如圖 18 所示。

圖 18 劫持家用路由器的駭侵手法

駭客成功入侵一般家用路由器後，會竄改路由器的 DNS 設定。一旦有使用者之行動裝置透過該受駭路由器上網，將會出現提示視窗誘導使用者於行動裝置上安裝應用程式。為了增加行動裝置惡意程式的安裝率，駭客會利用使用者正在瀏覽的網頁，結合「請安裝 Facebook 擴展工具包提升安全性及流暢性」或「請安裝最新版 Chrome 應用程式以提升安全性及流暢性」等有關安全與效能的重要文字，來取信使用者。

例如當使用者正在瀏覽 securelist.com 網站時，會跳出提示視窗「securelist.com says: To better experience the browsing, update to the latest chrome version.」，讓使用者誤認為是原廠網站對用戶系統效能與安全提升的建議，便進行下載與安裝。取信使用者的內容支援多達 27 種語言，包含英文、日文及正體中文等，如圖 19、圖 20 所示。

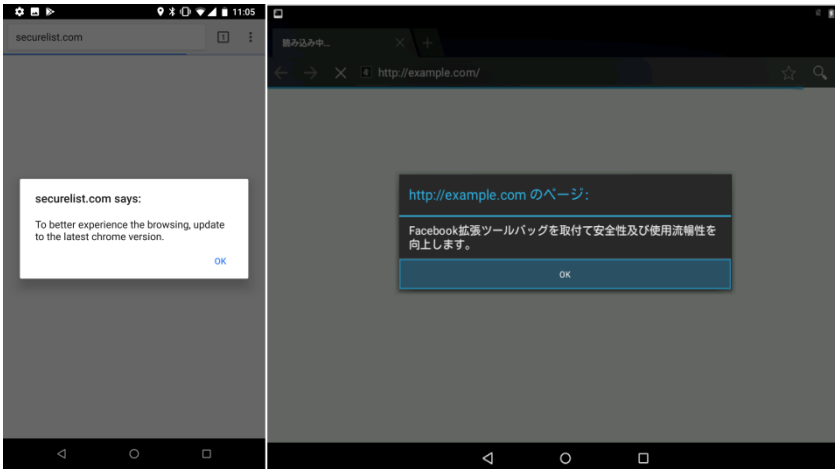


圖 19 誘導使用者安裝 APP 更新之英文、日文版提示視窗

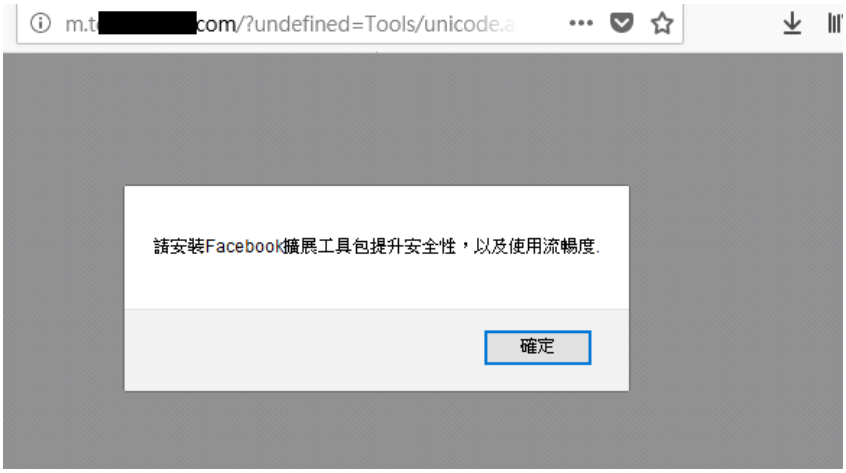


圖 20 誘導使用者安裝 APP 更新之正體中文版提示視窗

駭客所提供的 chrome.apk 或 facebook.apk 行動裝置惡意程式，將於安裝時要求 SMS 簡訊、通聯紀錄、網路、錄音功能及外部儲存裝置等存取權限。

除了竊取行動裝置用戶的資訊外，該惡意程式在開啟時亦會利用詐騙方式盜取受害者帳號密碼。當裝置被喚醒時將跳出「Google 帳號危險 認證後使用」的提示視窗，在使用者點擊確認後，會啟動瀏覽器開啟釣魚網頁誘騙使用者輸入姓名、生日與身分證號，如圖 21 所示。

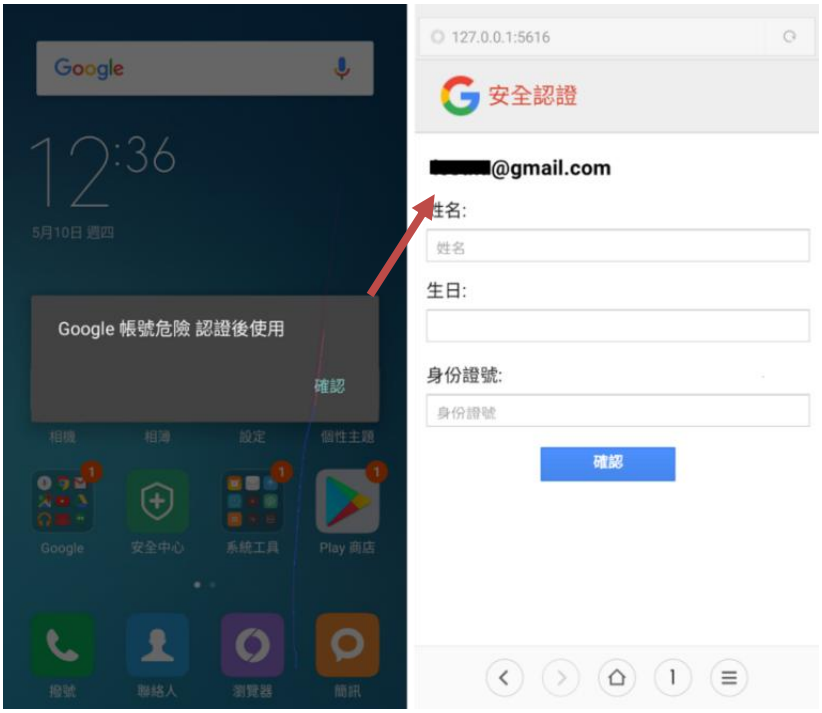
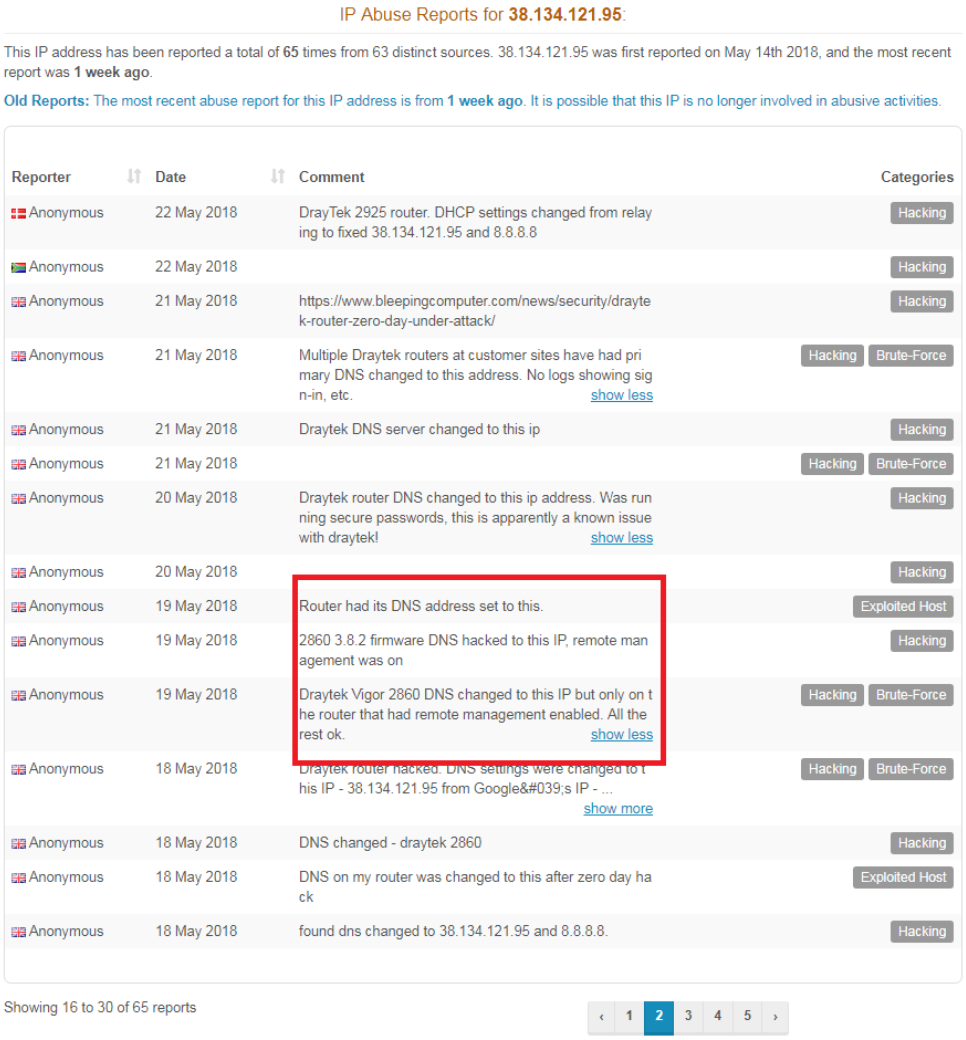


圖 21 駭客偽冒 Goolge 安全認證網站騙取使用者資料

無獨有偶，2018 年 5 月開始有歐洲用戶投訴台灣居易科技(DrayTek)所生產的路由器，其 DNS 伺服器位址無故遭設定為 38.134.121[.]95，而提供檢測惡意 IP 及網域之 AbusedIPDB 組織亦陸續於 5 月 14 日起收到 65 次 DNS 位址遭竄改的通報[17]，並將此 IP 列為惡意的 DNS 網域，如圖 22 所示。



IP Abuse Reports for **38.134.121.95**:

This IP address has been reported a total of **65** times from 63 distinct sources. 38.134.121.95 was first reported on May 14th 2018, and the most recent report was **1 week ago**.

Old Reports: The most recent abuse report for this IP address is from **1 week ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	Date	Comment	Categories
Anonymous	22 May 2018	DrayTek 2925 router. DHCP settings changed from relaying to fixed 38.134.121.95 and 8.8.8.8	Hacking
Anonymous	22 May 2018		Hacking
Anonymous	21 May 2018	https://www.bleepingcomputer.com/news/security/draytek-router-zero-day-under-attack/	Hacking
Anonymous	21 May 2018	Multiple Draytek routers at customer sites have had primary DNS changed to this address. No logs showing sign-in, etc. show less	Hacking Brute-Force
Anonymous	21 May 2018	Draytek DNS server changed to this ip	Hacking
Anonymous	21 May 2018		Hacking Brute-Force
Anonymous	20 May 2018	Draytek router DNS changed to this ip address. Was running secure passwords, this is apparently a known issue with draytek! show less	Hacking
Anonymous	20 May 2018		Hacking
Anonymous	19 May 2018	Router had its DNS address set to this.	Exploited Host
Anonymous	19 May 2018	2860 3.8.2 firmware DNS hacked to this IP, remote management was on	Hacking
Anonymous	19 May 2018	Draytek Vigor 2860 DNS changed to this IP but only on the router that had remote management enabled. All the rest ok. show less	Hacking Brute-Force
Anonymous	18 May 2018	Draytek router hacked. DNS settings were changed to this IP - 38.134.121.95 from Google's IP - ... show more	Hacking Brute-Force
Anonymous	18 May 2018	DNS changed - draytek 2860	Hacking
Anonymous	18 May 2018	DNS on my router was changed to this after zero day hack	Exploited Host
Anonymous	18 May 2018	found dns changed to 38.134.121.95 and 8.8.8.8.	Hacking

Showing 16 to 30 of 65 reports

‹ 1 2 3 4 5 ›

圖 22 網路設備之 DNS 位址無故遭設定為 38.134.121[.]195

居易科技已證實韌體存在弱點，讓駭客有機會竄改路由器的 DNS 設定，但該弱點細節並未公開。該事件受影響的路由器超過 25 款，為此居易科技 5 月 18 日緊急發布安全更新通知[13]，並建議用戶主動檢查路由器之 DNS 設定、啟用 TLS 1.2 的加密連線及關閉遠端管理者存取權限，在此 TWCERT/CC 呼籲使用者應儘速檢查並安裝最新版軟韌體。

除了駭客劫持路由器並竄改 DNS 設定的駭侵手法外，Cisco 旗下的威脅情報組織 Talos 在 2018 年 5 月 23 日及 6 月 6 日的研究中[14][18]，揭露了 VPNFilter 惡意程式，發現該惡意程式已攻擊全球 54 個國家並影響超過 50 萬個裝置，包含 Linksys、MikroTik、NETGEAR、ASUS、D-Link、中興、華為與 TP-Link 等品牌的路由器，以及 QNAP 網路儲存裝置。

多數家用路由器都是採用嵌入式的 Linux 平台，並配備精簡版的 Unix 程式套件 BusyBox。研究人員從目前受駭狀況推測，駭客係透過掃描網路上使用 BusyBox 的裝置，檢測其是否開

啟 Telnet 或 SSH 之遠端控制服務，再暴力破解路由器密碼成功後植入 VPNFilter。遭植入 VPNFilter 裝備會連到 Photobucket[.]com 或 ToKnowAll[.]com 下載變造過的圖檔來取得 C&C 伺服器 IP 位址，成功連上 C&C 後會下載其他監控程式。不同於其他物聯網裝置惡意程式(例如 Mirai)，VPNFilter 會修改家用路由器之非揮發性記憶體(Non-Volatile Memory)內容，並透過 Linux 的排程指令 crontab 將 VPNFilter 加入到例行性工作排程中，達到常駐於家用路由器的目的。因此，即便使用者將路由器重新開機，仍無法將惡意程式完全移除。

若路由器遭植入 VPNFilter 惡意程式，與其連接的網路流量都將遭受監控進而造成連網資料外洩，例如使用者之帳號、密碼或銀行帳戶等敏感資訊。目前美國聯邦調查局(FBI)已取得美國法院的命令，將存取 ToKnowAll[.]com 等惡意網域名稱的連線都導入 sinkhole，以阻絕受駭裝置與駭客的聯繫管道[19]。

TWCERT/CC 提醒，隨著越來越多物聯網裝置應用在日常生活中，相關的使用與控制皆是透過家用路由器來連接網際網路，家用路由器已成為駭客的主要攻擊對象。使用者必須了解家用路由器和相關物聯網設備連接網際網路所可能帶來的資安風險，物聯網設備所帶來的便利性與安全性才能兼顧。

針對近期家用路由器遭駭侵事件，TWCERT/CC 提出以下 7 項防護建議：

1. 選擇安全可靠的路由器廠牌，並隨時關注相關資安新聞，及即時更新原廠發布之軟、韌體，以封鎖駭客對已知漏洞攻擊的管道。
2. 修改家用路由器預設帳號及密碼，且應避免使用 admin、12345678 或 password 等容易猜測的弱密碼組合，建議使用混合英文、數字及符號，並且超過 8 個字元長度的強密碼。
3. 使用者應參考原廠路由器說明書，隨時檢視家用路由器(以 Asus WL-500gP V2 為例)之 DNS 伺服器 1 與 DNS 伺服器 2 之設定是否遭竄改(如圖 23 所示)，若遭竄改為非預期之設定(例如被改為 38.134.121[.]95)，應立即修正。台灣常使用的 DNS 伺服器為中華電信(168.95.192[.]1、168.95.1[.]1)或 Google 提供之 Public DNS (8.8.8[.]8、8.8.4[.]4)。

圖 23 確認家用路由器之 DNS 設定

4. 為防止駭客透過路由器遠端進入使用者的網路，應停用路由器內不必要的功能，例如通用隨插即用(UPnP)、WPS、Telnet/SSH 遠端管理功能，並限制 WEB 遠端管理的連線 IP。

5. 啟用家用路由器(以 Asus WL-500gP V2 為例)之防火牆基本防護功能(如圖 24 所示)。

圖 24 啟用家用路由器之防火牆功能

6. 若要防止惡意程式(例如 VPNFilter)常駐於路由器中，使用者可將家用路由器重置/回復出廠設定，再進行安全設定與更新。系統重置通常可以使用迴紋針或類似物品，按壓設備上的「reset」標示按鈕五至十秒鐘，以完成此動作。須注意系統重置會導致設備

所有的使用者設定都將消失。

家用路由器設備供應商應鼓勵漏洞通報，積極修補其產品的資安漏洞，並即時進行產品漏洞揭露，讓使用者掌握所用設備的資安風險，以維護品牌形象及商譽。

3.5、 透過社交軟體散布詐騙訊息事件

在台灣，透過社交軟體傳遞訊息已逐漸取代傳統的撥打電話、傳簡訊等通信方式，社交軟體已成為個人、企業甚至政府機構的重要即時溝通管道，社交軟體的高使用率，也吸引駭客或有心人士利用來散布詐騙訊息及惡意連結的管道。

假的商品優惠資訊或免費貼圖下載邀請訊息，常利用知名品牌名義加上限時或限地區優惠的文字，吸引消費者點選。以「星巴克母親節限定優惠僅有一天」假冒訊息事件為例，有心人士以「starbuckscoffee」等字樣，配合標題上的R等文字，讓使用者誤認該優惠廣告為星巴克官方帳號所發布(如圖 25 所示，偽冒資訊辨認方式請見該咖啡業者官方網站說明[20])。無獨有偶，2018 年 6 月 7 日起，有心人士以「臭跩貓愛嗆人(台灣限定篇)」限時可愛貼圖免費下載活動[21]，並以使用者不易察覺有異的短網址連結(如圖 26 所示)，誘騙使用者點擊，當使用者點選該連結後，會出現特製的下載頁面，並進一步以「分享 10 位好友即可下載」等字讓使用者協助其擴大散布，以增加該惡意連結的點擊數。當使用者點選下載後，實際上並沒有貼圖可下載，但帳號資料已經被給有心人士蒐集，進而讓對方得以販售所蒐集的使用者帳號，作為後續廣告及不法應用。

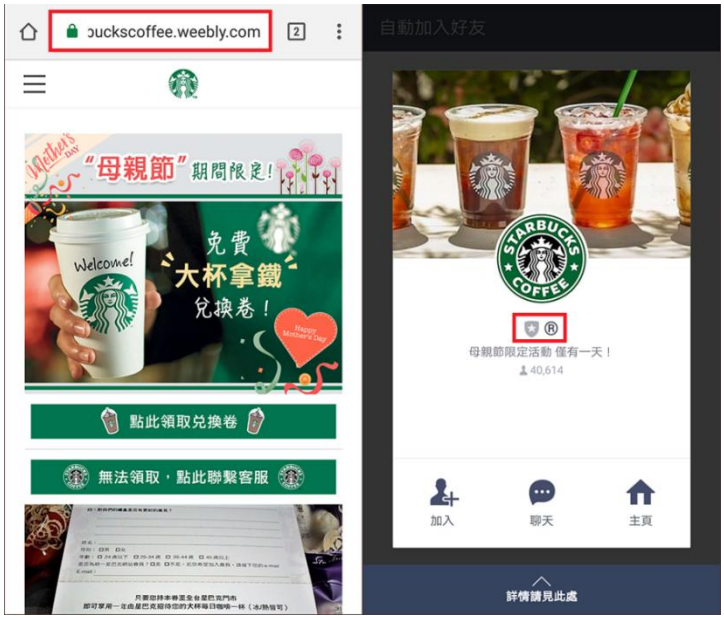


圖 25 偽冒的知名商品優惠廣告案例

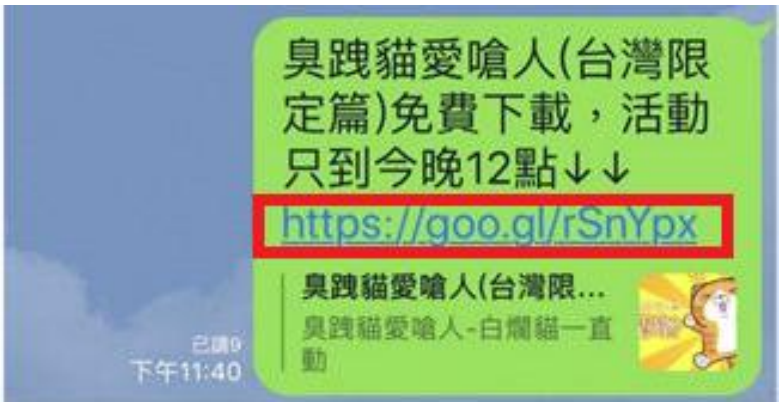


圖 26 社交軟體接收詐騙訊息案例

假的貼圖下載邀請訊息，常以「分享活動」的方式要求使用者分享給更多用戶，以增加詐騙訊息散布的機會(如圖 27、圖 28 所示)，並以「未邀請者無法下載」等限制，導致使用者為了取得貼圖，而分享給其他用戶，然而此詐騙訊息所提供的短網址連結 hxxps://goo.gl/rSnYpx 所對應的真實網址是 hxxps://qoo607041.wixsite.com/catcat，並非是 LINE 貼圖的官方連結網址 hxxps://store.line.me/，故使用者於分享後也無貼圖可下載。

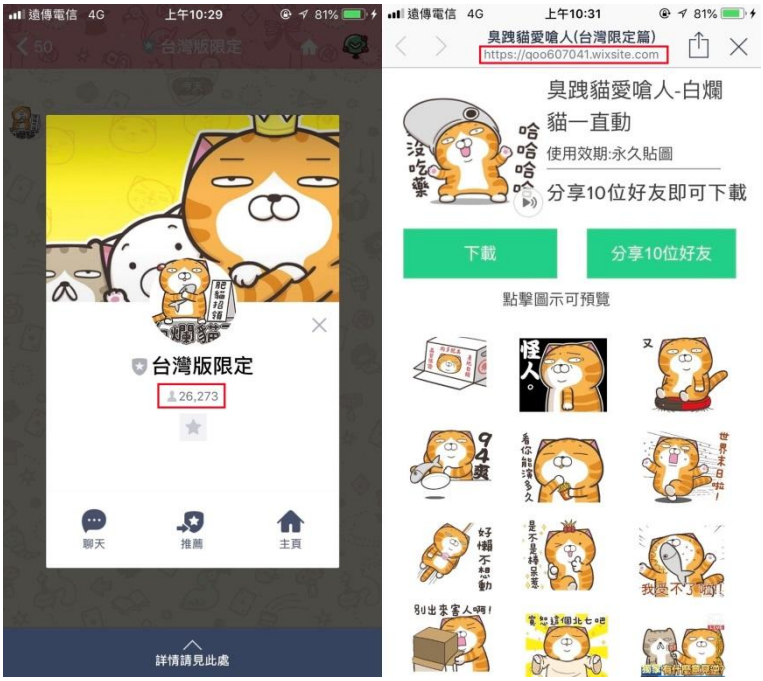


圖 27 假的貼圖帳號(已有 26,237 人被騙加入好友)

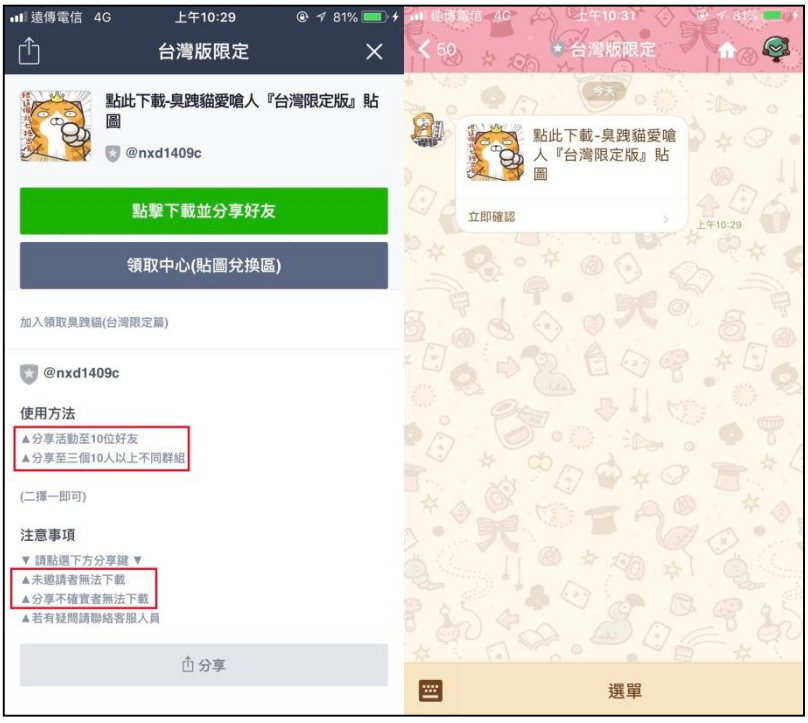


圖 28 詐騙貼圖下載案例(一般皆要求分享多個好友或群組)

有心人士從今年 6 月 7 日起，透過 Google URL shortener 的短網址服務來掩飾其惡意網址，經由 Google 短網址點擊次數分析結果顯示，截至 7 月 16 日已有超過百萬人次點擊此詐騙貼圖下載短網址，如圖 29 所示。

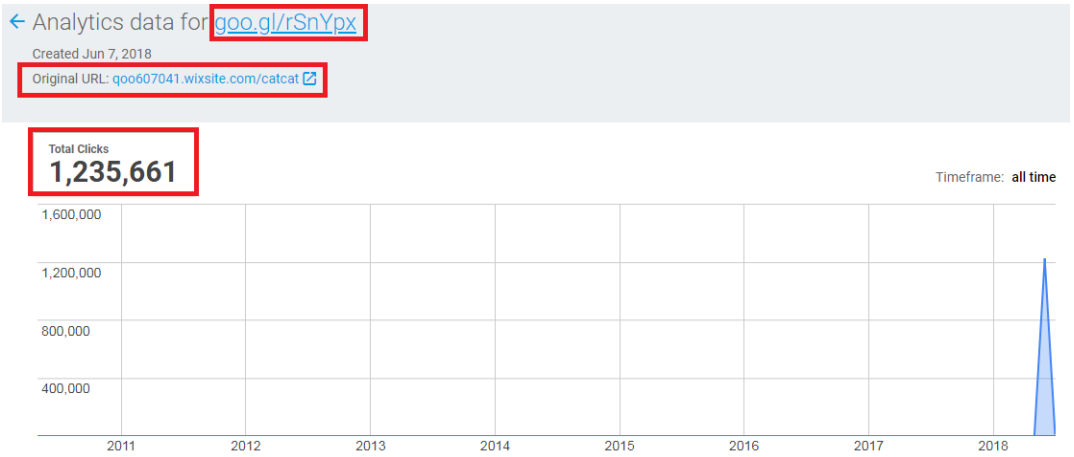


圖 29 Google 短網址點擊次數統計

進一步分析該詐騙貼圖訊息的點擊者，主要是來自台灣的使用者，其次數竟高達 1,053,047 次(如圖 30 所示)，日本計 4,232 次，美國 2,274 次，使用者主要透過 Android 及 iPhone 等行動裝置點擊該連結，此結果顯示台灣的社交軟體用戶常使用有趣且傳神的貼圖來聊天，故社交軟體貼圖廣告對台灣的用戶有致命的吸引力。

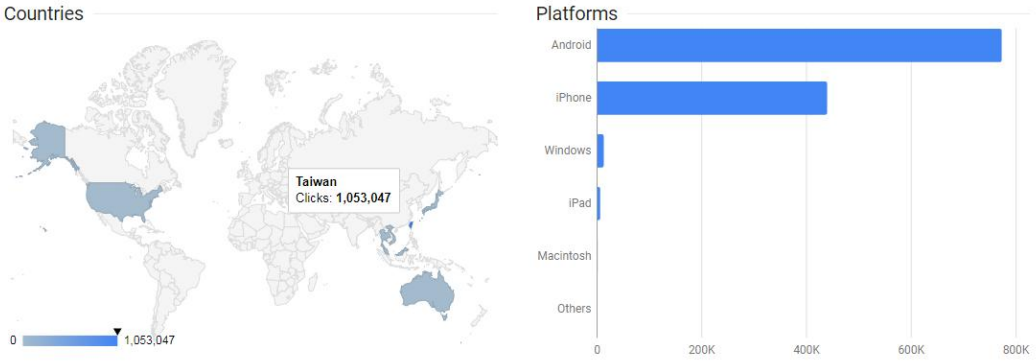


圖 30 臭跩貓詐騙網址受害來源統計

近來社交軟體儼然成為駭客進行網路攻擊的新途徑，相關詐騙與攻擊案例，經彙整分析如下：

- 透過社交軟體傳遞惡意或釣魚網站連結，誘導使用者點擊並下載安裝惡意程式或誘騙使用者登入應用服務系統，以竊取用戶帳號密碼。
- 透過社交軟體傳遞具有觸發惡意程式的貼圖、圖片或小額付款連結等，造成使用者中毒、資料外洩或財產損失。

- 社交軟體的帳號密碼遭破解，並遭冒用，以騙取好友信任，詐騙好友購買點數卡，造成友人財產損失。
- 透過社交軟體散布免費貼圖或優惠商品訊息，致使用者帳號遭蒐集販售，造成使用者遭廣告干擾，甚至受騙招致財產損失。

從上述案例發現，惡意軟體或連結常針對社交軟體用戶喜好與習慣，再配合優惠商品訊息或精美的貼圖引誘使用者點擊，可在極短時間內達到大規模散布之目的。社交軟體被應用來進行釣魚與散布惡意程式的新途徑[22]，經分析可能原因如下：

- 運用人性弱點誘騙使用者點擊惡意連結
- 比起以往透過電子郵件散布垃圾郵件進行網路釣魚，使用者面對的廣告或詐騙訊息可能都是來自於使用者的好友或關注的品牌，在這樣的氛圍下，用戶容易認為這些網址連結是安全的，點擊率相對提高。
- 社交軟體提供用戶大量的個人資料
- 社交軟體公開資訊通常包含使用者喜好、聯絡人資訊，比起入侵電子郵件才能獲取這些資訊，駭客更易於透過社交軟體進行網路釣魚攻擊。
- 行動裝置的防護機制較缺乏
- 目前行動裝置的資安防護相對於個人電腦較少，惡意連結及木馬程式，透過行動裝置入侵後再成功攻擊個人或企業電腦的機會將提高。

因此，使用者對於使用與接收社交軟體訊息時，應隨時提高警覺，審慎評估社交軟體訊息內容的真實性，以避免受害。針對近期頻傳社交軟體散布詐騙訊息事件，TWCERT/CC 提出以下 5 項防護建議：

1. 當收到短網址連結時應確認寄件者身分及真實網址，若有疑慮切勿點擊。以 Google 短網址為例，若網址為 hxxps://goo.gl/rSnYpx，則在網址後加上.info，如圖 31 所示，即可檢視短網址的真實網址內容。

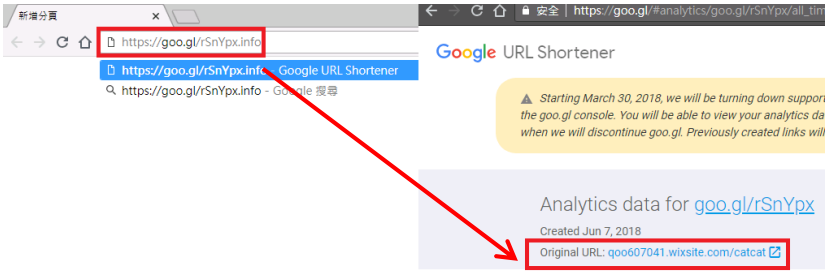


圖 31Google 短網址還原方法

2. 了解社交軟體的帳號類別與特性[23]，例如 LINE@帳號即分為灰色的一般帳號盾牌、經認證帳號的藍色盾牌以及 LINE 官方帳號的綠色盾牌等三種(如圖 32 所示)，若使用者收到來自非正式官網或經認證帳號所傳送之商品優惠與下載連結訊息，使用者應該提高警覺，使用者應該提高警覺[24]。

圖 32LINE 帳號類別

3. 隨時關注國內、外資安新聞、刑事局 165 反詐騙網站的訊息及新興詐騙手法，若不小心已將可疑帳號加為好友，應檢查是否具有假帳號詐騙特徵，若有，應立即檢舉並封鎖。若接到有釣魚網址連結的訊息，則可通報 TWCERT/CC 以協助移除該連結，避免該釣魚連結持續散布，致更多使用者受害。
4. 若非必要，使用者應關閉社交軟體及電信商之小額付款功能[25]，以避免誤按不明網路付款連結，並注意信用卡及電信費用帳單明細，若有異常交易紀錄，應立即向發卡公司及電信服務商反應，以避免財務損失。
5. 使用者應詳閱社交軟體的隱私權政策與個資揭露設定，若非必要項目應關閉。例如 LINE 允許手機通訊錄自動加入好友、允許好友邀請、個人化廣告、阻擋訊息及訊息加密(Letter Sealing)等服務，如圖 33 所示。

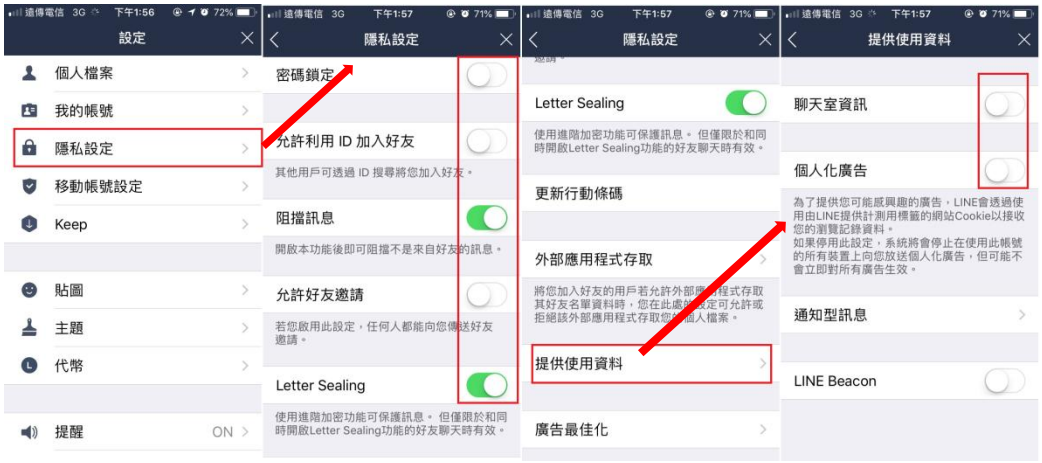


圖 33 LINE 的隱私設定

3.6、 新加坡醫療資安事件

2018 年 7 月 20 日新加坡衛生部(Ministry of Health, MOH)對外表示新加坡醫療保健集團遭駭[26][27][28]，導致 150 萬人的非醫療個人資料(包含姓名、身分證字號、地址、性別、種族及生日)，以及 16 萬名病患的處方等資料遭非法存取及複製。負責管理公共醫療機構 IT 系統的整合健康資訊系統公司(Integrated Health Information System, IHiS)於發現新加坡醫療保健集團資料庫異常活動後，立即封鎖異常存取連線，並更換全系統的帳號密碼，新加坡醫療保健集團亦提供專屬網站讓民眾查詢受害情況，使整起資料外洩事件的影響得以降低。此外，新加坡網路安全局(The Cyber Security Agency of Singapore, CSA)也依據 IHiS 所提供的資訊進行評估，並依該國網路安全法(Cybersecurity Act)擴大要求其它關鍵資訊基礎設施(Critical Information Infrastructure, CII)同步提升資安防護等級與範圍，整體流程堪稱完善嚴謹。

針對此類事件，TWCERT/CC 整理 SingCERT[29]所提防護建議，做為台灣企業評估重要系統資安防護的參考：

1. 定期檢視網域管理者帳戶及權限：網域管理者擁有其網域的管理最高權限，因此須定期控管帳號權限，若發現異常的管理者帳號應刪除之。
2. 非經授權的遠端存取行為：注意資料庫存取的語法限制，當發生異常的資料庫查詢行為，應有警告機制並注意系統日誌、資訊安全日誌有無異常紀錄。系統及資料庫登入

密碼應使用強密碼並定期更換，另應對於重要系統的登入採取多因子認證。

3. 加強管控長時間運行的終端設備：若終端設備長期處在不關機的狀態下，應設有監控或惡意行為偵測機制，另針對未使用的資通訊設備應移除，以減少終端設備遭駭客利用，而成為入侵途徑。
4. 以白名單方式限制使用者可執行的應用程式、服務及來源網路位址：以白名單方式限制用戶可執行的應用程式及服務，可以防止其他未經許可惡意軟體的執行，另針對重要系統亦應以白名單方式限制可連線使用者的來源網路位址。
5. 更新修補程式並保持系統更新：適時更新作業系統及應用程式相關修補程式，可以避免駭客使用已知的漏洞或惡意程式進行攻擊，針對防火牆與防毒軟體等系統防護設備也需定時更新，以確保系統的最佳防護效力。
6. 定期稽核並落實實體隔離防護機制：已實施實體隔離安全防護機制的企業，針對其實體隔離網路架構及隔離機制實際執行情形應定期稽核，並且將所有可連線的設備皆納入風險評估的範圍。

第四章、 情資發布與分享

為提升我國民眾資安意識，TWCERT/CC 於每月發布電子報，統整上月重要資安情資，包含 TWCERT/CC 近期動態、資安政策、威脅與趨勢、駭客攻擊事件、軟硬體漏洞、資安研討會活動及資安事件通報統計分析等資訊。TWCERT/CC 所發布資安情資，除了以電子郵件方式提供電子報訂閱者，另發布於官方網站、Facebook 及部落格等，以利不同閱讀習慣之民眾皆可順利閱覽。

4.1、 漏洞統計數據分析

本年度所發布產品漏洞類型統計如圖 34 所示，其中代碼執行(Code execution)類型之漏洞為最大宗，其次則為提權(Gain privilege)及資料洩漏(Gain information)等種類之漏洞。

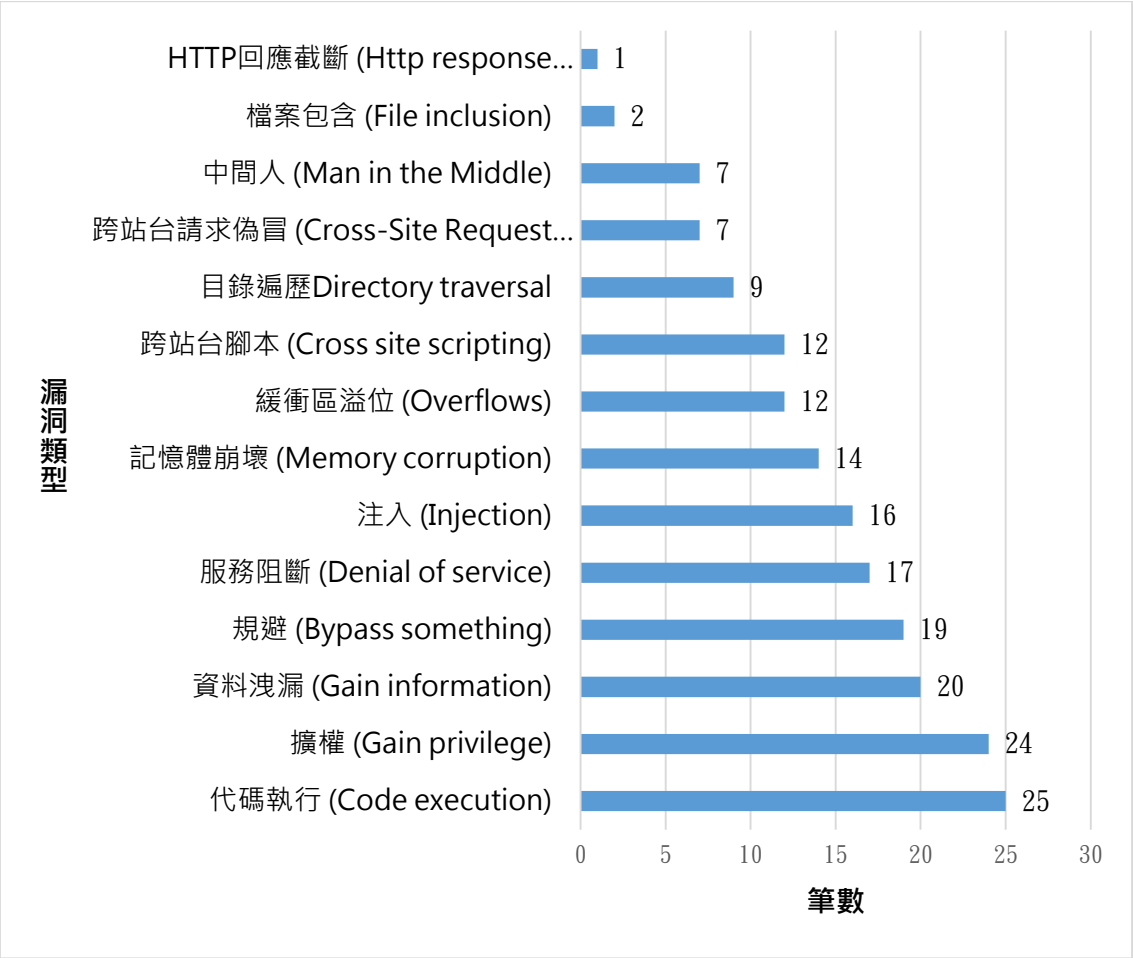


圖 34 產品漏洞類型統計

4.2、 駭侵事件分析

由今年本中心所蒐整之駭侵事件中，可看出今年度約有五分之一的駭客攻擊事件主要針對金融領域進行攻擊，如各地銀行所使用 SWIFT 系統遭駭、銀行感染勒索病毒，或是銀行客戶誤連入釣魚網頁導致個人資訊及信用卡號等財務資訊遭竊等，皆是時有耳聞。

針對大眾運輸業進行攻擊者也是不在少數，如航空公司及購票系統遭駭導致個資外洩等事件也屢見不鮮。此外，政府單位及關鍵資訊基礎設施亦為容易遭受攻擊的目標，各國政府皆需加強此些相關單位的資安防護能力，以免造成嚴重損失。

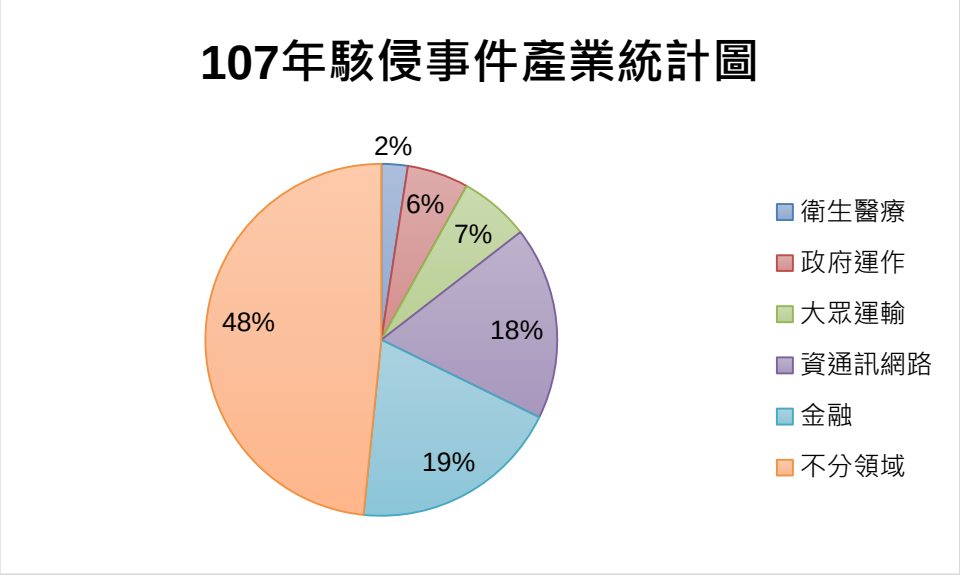


圖 35 107 年駭侵事件產業統計圖

4.3、 主流產品類別之弱點態樣

本年度主流資訊產品包含中央處理器、物聯網、行動裝置、通訊軟體、作業系統及一般應用程式等，分別遭揭露多種類型之弱點，詳述如下：

1. 中央處理器 (Central Processing Unit, CPU)：

今年最特殊的硬體式漏洞，首先推熔毀(Meltdown)、鬼魅(Spectre)，利用 branch instruction 推測性執行特點，實行旁道分析，其後 Spectre 有 3 個變體版，6 月出現 Lazy FP state restore，亦可竊取浮點運算單元運算資料，此係 CPU 結構設計為追求運算效率所衍生之副作用，全面影響 Intel 產品。

2. 物聯網 (Internet of Things, IoT)：

除智慧手機以外，一般人不常直接操作 IoT 設備，更罕見去檢查系統狀態，舉凡網安設備、路由器、基地台、IP camera、NAS、印表機、智慧家電、IP Phone 等皆在此列，話說多數 IoT 為顧及成本與運算效率，其韌體設計採用輕量型嵌入式作業系統，旨在提供商品基本服務，欠缺足夠安全機制，當然也無法安裝防毒軟體，故先天防禦力偏低，因設計缺失，無法過濾可疑 HTTP request 輸入值，常觸發 Command Injection、DoS、XSS，或者因權限配置不當或預設帳密，造成 bypass 驗證、CSRF、Directory Traversal，而獲得控制權，弱點曝光率高廠商為 D-Link、華碩、MikroTik、

Pelco Sarix、LG、VelotiSmart、Foscam、QNAP 等，其中 QNAP 修補頗落實。

3. 行動裝置：

手機、平板、智慧錶雖屬 IoT，然其專屬個人且密集使用之特性，故單獨彙整漏洞概情，漏洞多與 OS 有關，主流者乃谷歌 Android 與蘋果 iOS、tvOS、watchOS，且搭配各種 APP，架構上形似一般電腦，但沒有嚴謹的權限配置政策，所謂權限非不同帳號分級授權，而是不同 APP 對各項資源存取應遵守合宜控管，智慧機操作者應該只限物主，其他人就算偷到手也無法輕易破解而使用其功能，而曾經發生過的勒索軟體、執行惡意碼、個資外流、bypass 密碼錯誤稽核等，皆是原廠預裝 APP 之弱點結合權限不當所導致。

4. 通訊軟體：

WhatsApp、Telegram、Skype、Signal、PyBitmessage 之共同特性是通訊過程加密，故可防禦傳送內容遭中間人竄改，置入惡意訊息，即時通雖然也是應用軟體，但能跨桌機與行動裝置，支援於多種平台運行，故其漏洞所能影響作業環境更多元，漏洞皆出在資料傳送以外軟體行為，例如 DLL hijacking、RCE、DoS，造成更新器安裝到假程式、欺騙用戶下載挖礦程式、訊息內容、本機儲存明文資料、長字串癱瘓程式等事件。

5. 作業系統及一般應用程式：

這是數量最龐大的弱點來源，無法臚列所有軟體，除 OS 外，諸如 email、文書影像編輯、播放器、網站開發、防毒程式皆屬此類，為用戶直接操作介面，使用功能之主體，主要漏洞形式為 Memory Corruption，無論是 Use-after-free、Out-bound read/write、Overflow，皆可能衍生後續 DoS、RCE、權限擴張、訊息外洩，但均源自惡意操弄記憶體，如 Microsoft Dynamic Data Exchange (DDE) Protocol 可被惡意程式利用而進行感染。

4.4、 年度主要產品漏洞技術

本年度漏洞資訊統整中，遭受最多漏洞威脅的產品包含 Adobe 產品、CPU、IoT 及行動裝置，皆曾發生漏洞被利用導致嚴重威脅之情事，分別詳述如下：

1. Adobe 產品：

現今幾乎無獨立運作的主機，故作業系統、應用程式、網站服務關係密切，任何入侵均無法端賴特定漏洞，特地舉 Adobe 產品為例，是因其涉及多次駭客行動，其 InDesign、Photoshop 均可觸發 Memory Corruption，Dreamweaver 觸發指令注入，然無甚損失，Acrobat Reader 因 Double Free 漏洞，可被連鎖探勘，在 Windows 擴權執行任何 exe 檔，因被駭客成員上傳給防毒平台進行測試才曝光；至於 Flash Player，永遠有修補不盡的 Type Confusion、Use-after-free 缺點，今年分別在朝鮮半島、中東卡達、俄羅斯烏克蘭區域衝突中，三度成為資安攻擊主角，針對特定族群之 Windows 主機下手。

2. CPU：

執行硬體旁道分析，駭客需實體操作受害主機，通常亦須具備管理者權限，方可執行特定工具，能做到如此程度，也是對自己的實驗設備下手，稱不上資訊犯罪，故 Meltdown、Spectre、Lazy FP state restore 應屬學術案例，非典型入侵途徑。

3. IoT：

雄邁監控雲端服務 XMeye P2P Cloud，曾經捲入 2016 年 Mirai DDoS，咎其因為內建帳密 admin/空值、明文流量等，且漏洞延續迄今，台灣約有 15,000 該廠設備，仍有惡化成殭屍網路風險。另具管理權限的駭客，經 port 37215 攻擊華為家用型路由器，曾於 12 小時內感染 20 餘萬設備，形成大規模殭屍網路 Satori，肆虐阿根廷、美、義、德、埃及、土耳其、烏克蘭、委內瑞拉和秘魯等國。至於國廠居易 DrayTek 28 型 Vigor 路由器漏洞，據報少數設備遭不明人士竄改 DNS，指向中國大陸 IP(38.184.121.95)，且查無任何系統紀錄，必然是 bypass 帳密驗證程序，直接存取組態值。

上述物聯網資安事件，根本原因在於攻擊者容易獲得控制權，無論是透過中間人攻擊或者 bypass 驗證，甚至撈取密碼檔加以破解，最恐怖者乃寫死預設帳密。

另針對 Wi-Fi Protected Access II (WPA2)協定而設計之金鑰重安裝攻擊 KRACK(Key Reinstallation Attack)，取得中間人位置後重放交握加密訊息，重設 nonce 值為 0，駭客需身處 Wi-Fi 範圍內，始得奏效；以及針對 TLS session 加密機制弱點設計的 Bleichenbacher 式威脅回歸 ROBOT(Return Of Bleichenbacher's Oracle Threat)，須佔據中間人位置且建立十萬至數百萬之鉅量 TLS 連線，分析截獲 TLS 流量，耗時甚久。故 KRACK、ROBOT 具理論可行性，而較無實用性，對 IoT 甚無威脅。

4. 行動裝置：

Android 面臨 Janus 漏洞探勘，會藉 System 權限執行程式；某些元件被惡意檔案觸發弱點後可擴權執行代碼；另可利用 Man-in-the-Disk(MitD)弱點，突破沙箱，從外部貯存器植入間諜軟體 Triout。

iOS 上安全飛地處理器 SEP(Secure Enclave Processor)，無法紀錄外接鍵盤密碼錯誤次數，故有暴力破解機會；某些元件會造成代碼執行，取得核心權限；另藉 Siri 視障輔助功能，對 iPhone 以電話或簡訊連絡，顯示系統通知訊息時，發生 UI 衝突，迴避 Screen Lock 安全鎖，可實體侵入手機，竊取各類隱私；CoreText 元件處理印度 Telugu 文字則引發 DoS。

華為智慧機被安裝惡意程式後，可遭攻擊者略過權限認證，於聲控距離內，語音觸發 Soundtrigger 模組，喚醒休眠控制目標裝置發簡訊或撥電話。

Samsung 手機內建簡訊軟體，因排程訊息(SCHEDULED TEXT)功能錯誤，在用戶不知情下外傳圖庫區照片給通訊錄內友人。

智慧機被入侵都不脫本機操作條件，無論用戶不慎胡亂安裝 APP，或是攻擊者直接取得手機，故未曾發生大規模事件，但設計瑕疵的確存在，至於 Telugu 文字造成 DoS，僅限印度地區，也稱不上威脅，至於主動送出照片，更無關入侵，根本就是程式邏輯問題。

4.5、 常見駭客攻擊特徵

根據分析，目前駭客攻擊有多個常見特徵，包含各階段任務明確、惡意程式高級化及駭客組織專業分工，分別詳述如下：

1. 各階段任務明確

首先利用魚叉式社交工程，誘騙受害者開啟檔案。接著在檔案中嵌入惡意程式，例如 Office 檔案內必然嵌入 Flash Player 物件，在開啟的同時瞬間觸發弱點。這些惡意程式會避開 ASLR (Address space layout randomization)機制，及微軟 DEP (Data Execution Prevention)或 CFG (Control Flow Guard)，執行 Shellcode 後連線 C&C，並下載及植入後門程式，在作業系統背景執行服務。

2. 惡意程式高級化

終極 Payload 危害最為嚴重，且其功能設計精緻完整，已具有初級 AI，能判斷是否有防毒軟體，適時轉移或自毀滅跡，並能主動休眠，監控受害者 I/O。

3. 駭客組織專業分工

社交工程布局嚴密，誘餌設計逼真，需要包裝行銷專長，惡意檔案觸發漏洞後能精準執行 Shellcode，顯示對作業系統軟體工程極精通，聰明的後門程式，則須熟悉各種 UTM 防護樣式，才能安全存活，必然是團隊合作成果。

第五章、 資安政策與趨勢

進年來資安意識抬頭，各國對於資安事件所帶來的衝擊逐漸開始重視，紛紛制定資訊安全相關法規來規範企業或組織，企業需對於資安防護不完善，導致發生資安事件時，客戶蒙受嚴重的損害而有所負責。目前各國及企業分別亦有成立資安事件應變團隊，各團隊之間也經常彼此互助合作，透過溝通協調、情資交流的方式，建立資安聯防機制，以即時掌握資訊安全現況，並加速資安事件處置效率，底下將介紹 TWCERT/CC 所觀察到資安通報面臨的挑戰以及因應對策、亞太地區電腦事故緊急應變團隊營運概要、台美國家資通安全戰略比較，及台灣資安弱點發布之現況與未來進行探討。

5.1、 資安通報的挑戰與對策

駭客針對一般民眾上網習慣，常將熱門新聞議題、關鍵字或影片等民眾有興趣的內容，利用社交網站、即時通訊軟體或電子郵件等管道散布惡意程式或釣魚網站連結。因現階段台灣民眾資安意識仍薄弱，即便瀏覽器或防毒軟體已針對相關可疑網路行為提出警告，仍有民眾不以為意，繼續其網路瀏覽作業。因一般民眾較重視資訊的「獲得」，不在意資訊來源是否「安全」，且普遍有「電腦中毒沒關係，只要移除或重灌，問題就可解決了」的觀念。雖然，表面上看起來問題已被「解決了」，但是實際上問題產生的原因並未被排除，一般民眾不會細究發生資安事件的背後原因，並尋求正確的解決方式，導致相同資安事件重複發生。

TWCERT/CC 在接獲來自國內外的資安通報後，經確認受駭單位為我國企業或民眾，TWCERT/CC 將直接聯繫受駭單位進行資安事件通報，並依事件影響程度協助處理。常見接獲通報之單位對於通報之案件多以不處理、或僅以表面排除等消極態度因應。常因該單位未澈底解決問題而再次出現類似的資安問題，甚至部分單位對 TWCERT/CC 執行通報業務及所通報的內容存疑，而將通報資訊歸類為詐騙集團訊息或垃圾郵件，以致駭侵事件資訊無法即時傳遞給受害單位進行早期處理，可能造成後續重大的損失。

資安事件能否儘快排除，減少損失，主要的關鍵在於事件通報與應處程序能否順利推動，TWCERT/CC 在執行資安事件通報與協處業務上所遇到的問題大致可區分為「資安意識不足」以及「法規的限制」等兩大類別，常見狀況列舉如下。

(一)資安意識不足

1.對資安事件可能造成危害的嚴重性認知不足

企業或民眾於接獲資安通報後，常因相關資安問題尚未造成其損失，而對事件排除之處置態度不積極(如程式修訂或系統漏洞修補等)。

例如：針對企業網站遭置換之資安通報(如揭露於 zone-h 或被通報為釣魚網頁)，常見受駭單位僅以移除遭置換的網頁因應，未細究網頁遭換之原因(如對系統進行完整安全檢測)，導致本中心再次接獲該單位網頁被置換之情資。

2.資訊與資安能力不足，以致無能力修正系統的資安問題

大部分中小企業的網站係委託軟體開發商建置，企業本身對系統架構與設計並無掌握及不了解，另軟體開發商因人力、技術及成本考量，系統安全測試與檢查常被忽略。因此，在接獲資安事件通報時，即使 TWCERT/CC 已於通報資訊中提供處置建議，企業亦無能力處理或無法確認委託商處理狀況。

例如：TWCERT/CC 通報案例中，有許多小型企業由實體店面跨足網路商店，其線上購物網站普遍委託軟體開發廠商建置。當接獲資安通報時，常因系統建置完成後，開發商已無責任，而無法立即協助修訂，導致問題排除時間延長，甚或因該問題尚未造成企業立即的損失，而不修正。

3.不知道系統需要安全更新或修補系統漏洞，導致資安事件發生

一般企業或民眾因資訊能力或資安意識不足，不了解安全更新是資安防護的重要工作。絕大多數的駭侵事件起源於系統漏洞遭到駭客利用，其中大部分的攻擊是來自於已知的漏洞，而非零時差攻擊[30]。另因企業或民眾所建置之系統對於舊環境或元件相依性重，擔心修補更新後會造成原系統不穩定或損壞[31]，而對資安通報所述之漏洞問題未及時修補或更新意願不高。

例如：2017 年 5 月全球發生 WannaCry 勒索軟體，即是透過微軟已於 3 月公告的漏洞進行攻擊[32]，若用戶能及時修補這個漏洞，相信將可降低該事件的攻擊風險。

4.不知道發生資安事件應該通報，並可尋求協助

國內一般企業與民眾普遍對資安通報與協處資訊認知不足，目前尚存有家醜不外揚觀念，對於本身遭受資安事件時，大部分民眾僅以重新安裝作業系統的方式處理，而非找出資安事件原因，另外同時也輕忽網路上所發生的資安事件，因而錯失早期防護的時機，導致類似資安事件重複發生。

針對資安意識不足而造成資安通報與協處程序的挑戰，TWCERT/CC 建議之改善對應策略如下：

1.強調資安通報等級及資安事件影響程度

為使企業或民眾明瞭相關單位所通報資安事件的嚴重性，通報內容可強調事件的

影響等級及分級標準資訊，並提供該資安事件相關新聞與參考資料。

2.鼓勵企業開發軟體時，納入安全軟體發展流程

企業的資訊系統開發過程中，應要求開發人員納入源碼檢測、弱點掃描及滲透測試等安全軟體發展流程(Secure Software Development Life Cycle, SSDLC) [33]。若需委外廠商開發時，除了考量開發成本外，也應將資安檢測納入驗收條件，並建議找資安信譽優良的廠商合作，以免因小失大，影響企業商譽。

3.提供有效解決方案建議

企業及民眾除了注意漏洞修補、更新程式相關取得管道或問題緩解資訊外，也應確認解決方案之相容性問題。

另可建議進行漏洞修補前置測試，例如，將修補程式安裝於備援系統中運行，以確認修補程式的安裝不會對正式系統造成任何非預期的後果。

4.建立單位資安聯繫管道，時刻掌握資安情資

單位應建立資安專責聯繫管道，負責接收與回報資安情資與資安事件，平時多關注相關資安新聞、漏洞發布資訊等資安情資(如加入 TWCERT/CC 臉書粉絲專頁及訂閱 TWCERT/CC 電子報等)，適時參與資安研討會以了解最新的資安威脅趨勢與防護技術，並將所獲情資對內部員工進行宣導，以培養員工之資安意識。當內部發生資安事件時，協助員工進行事件排除，並可依事件影響等級對外通報及尋求協助(如向 TWCERT/CC 通報)，以求事件之快速排除。

(二)法規的限制

1.TWCERT/CC 針對通報的問題之驗證無法源依據

由於 CERT 通常屬民間之非營利組織，因法規關係，除通報網頁置換或釣魚網頁等可直接檢視外之案件外，部分接獲之通報案件所述之通報問題無法即時或有授權可驗證情資是否正確，難以確認通報情資正確性，若不經求證之通報而造成誤報，將造成受通報單位之不便，更使通報單位之可信度受質疑。

例如:有大量屬於台灣用戶的電子郵件帳號及密碼遭到公布在其他國家之網站上,並無法得知被公布之原因。當 TWCERT/CC 接獲該情資時,若嘗試驗證其帳號密碼之正確性時,可能遭質疑有入侵嫌疑。

2.系統代管或開發商處理資安事件態度消極

系統開發商或託管商認為其開發的產品遭通報有資安疑慮時,為了避免事件擴大影響其公司開發系統的品質遭質疑,卻僅關閉或移除問題資料,且不願意讓其客戶知道此事件。

例如:資訊系統開發商或託管商表達不應該將產品問題通報其客戶,應直接通報至該業者。

3.受害單位認為即使有影響其他人也無所謂

當企業或民眾接獲資安通報後,即使說明此通報可能造成的影響,仍不願意修補。

例如:企業或民眾購置的網路監視器遭公布於 Insecam 網站時,即使了解若未修正相關設定,可能遭駭客植入惡意程式,成為殭屍網路的一員攻擊其他設備,但是企業或民眾認為不是攻擊自己,因此不認為有影響。

針對法規上的限制而造成資安通報與協處程序的挑戰,TWCERT/CC 建議之改善對應策略如下:

1.提供通報問題驗證方式

受限於資安情資驗證時,須經當事者同意,因此,通報單位如能協助整理相關驗證方式之資訊,由受通報單位自行確認,便無觸法疑慮。

2.公布通過資安檢測的合格開發商資訊

當企業或民眾需要委託系統開發商建置其系統或網站時,可透過公開資訊網站查詢經過資安檢測認證合格的開發商,形成良性競爭關係。

3.強化資安政策及法令規範

應該修訂法律規範,若確實有資安疑慮時,應該配合修正,以避免成為加害者。

綜上所述,TWCERT/CC 進行通報業務時,面對之挑戰不外乎企業或民眾資安意識不足,

導致資安問題重視程度低落，若能將基本資安觀念推廣達到全民化，如此不論企業或個人都將有效減少資安事件發生，以建立良好之資安環境。

5.2、 台灣資安弱點發布之現況與未來

現今網路上最常使用的資安漏洞資料庫，是由美國 MITRE 公司負責營運維護的「通用漏洞揭露」(Common Vulnerability and Exposures, CVE)平台，CVE 為美國國土安全部網路安全和通信辦公室所贊助的計畫。當資通訊產品之軟、韌體被發現運算邏輯等影響機密性、完整性或可用性的設計缺失時，得以透過 CVE 平台，將所有已知漏洞資訊和安全風險的名稱標準化，並賦予漏洞編號。截至 2018 年 12 月 10 日，CVE 共有來自 14 個國家(澳大利亞、奧地利、加拿大、中國、法國、德國、以色列、日本、荷蘭、俄羅斯、南韓、台灣、英聯合王國、美國)的 93 個漏洞編號授權單位參與。

CVE 漏洞審查與編號分配需由經 MITRE 公司核可的「漏洞編號授權單位」執行。為了讓每一個 CNA 彼此在溝通、管理及發布漏洞時能有一致的標準，MITRE 制定「漏洞編號授權單位規章」(CVE Numbering Authorities (CNA) Rules)[34]，弱點編號是由「弱點編號授權單位」(CVE Numbering Authorities, CNA)負責弱點審核與編號賦予，「漏洞編號授權單位」分為三種類別，分別就其所負責維護管轄之範疇，進行 CVE 審核及編號分派。CNA 之組織架構如圖 36 所示，說明如下：

1. 主漏洞編號授權單位(Primary CNA)：

   亦即 MITRE 公司，負責授予 Root CNA CVE 編號區段、維護整體 CVE 編號清單並且對外公布，同時也擔任各個 Root CNA 間溝通管道。

2. 根漏洞編號授權單位(Root CNA)：

   擔任 Primary CNA 與 Sub CNA 間的協調者，協助 Primary CNA 維護所轄範圍內產品，供應商或產品的 CVE 審核與編號分派發布作業，且有義務主動告知 Primary CNA 其所發布之漏洞資訊更新。Root CNA 通常是由地區的協調中心或特定領域資訊分享與分析中心擔任，例如電腦網路危機處理小組 (Computer Emergency Response Team, CERT)、資訊分享與分析中心 (Information Sharing and Analysis Center, ISAC)

或是發展成熟的研究機構。

3. 子漏洞編號授權單位(Sub CNA)：

Sub CNA 通常由產品開發商擔任，通常是擁有明顯的客戶群且已具備資訊安全顧問諮詢能力的廠商，負責自身產品相關的漏洞維護作業。Sub CNA 對於發布之漏洞有資訊更新，應主動告知 Root CNA。而目前已成為 CNA 之單位列舉部分於表 1 中，詳細可參閱[34]。

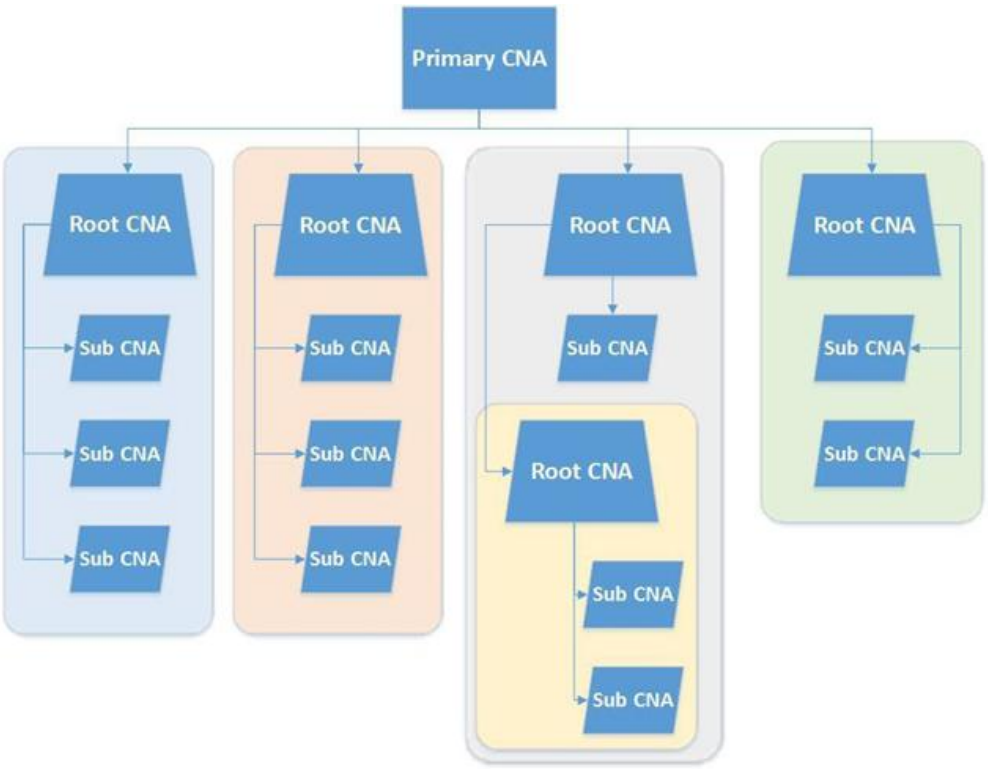


圖 36 CNA 組織架構圖

表 1. CNA 列表

CNA 種類	數量	單位名稱
Primary CNA	1	MITRE Corporation
Root CNA(含 National CERT and Industry CERTs)	7	CERT/CC, CyberSecurity Philippines – CERT, ICS-CERT, Distributed Weakness Filing Project, JPCERT/CC, KrCERT/CC, TWCERT/CC
Sub CNA(含 Vendors and Projects, Vulnerability Researchers, Bug Bounty Programs)	85	包含 Apple Inc., Adobe Systems Incorporated, Android (associated with Google Inc. or Open Handset Alliance), Apache Software Foundation, ASUSTOR Inc., Facebook, Kaspersky Labs, QNAP Systems Inc., Synology Inc., Trend Micro, Inc.等。

根據 MITRE 的「漏洞編號授權單位規章」，漏洞發布運作流程分為五個步驟，依序為申請 CVE ID 區段、CVE ID 保留、CVE ID 分派、CVE 通報及 CVE 發布(如圖 37 所示)。TWCERT/CC 將依據前述漏洞發布運作流程，成為台灣資通訊產業之漏洞揭露服務提供者。

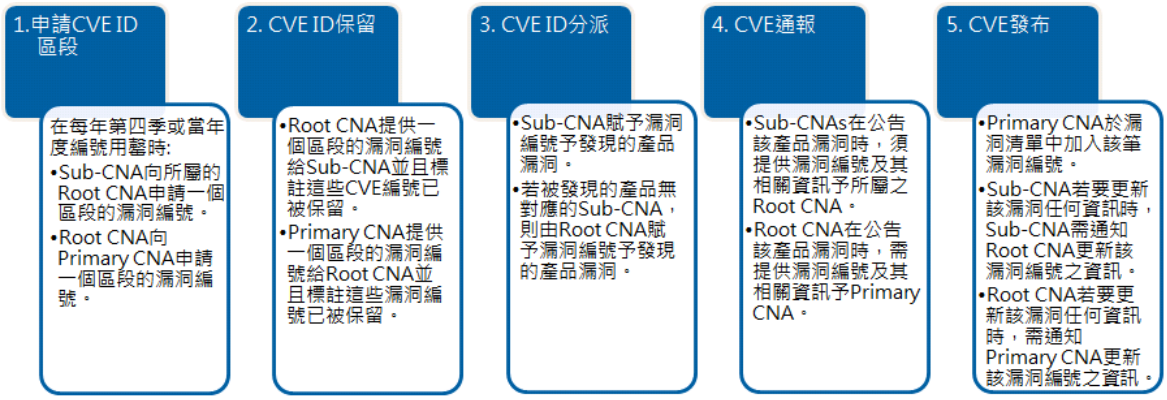


圖 37 漏洞發布運作流程[35]

舉例來說，當 CNA 接收到資通訊產品被發現存在漏洞時，首先會評估該漏洞是否有主責的 CNA。若有，則將此漏洞提供予該產品主責之 CNA 進行漏洞審核作業、編號分派與發布；若無主責 CNA，則逕由接收到訊息之 CNA 或 MITRE 依漏洞編號發布流程進行處理。

目前台灣有三家資通訊產品廠商為 Sub CNA，分別是群暉科技 (Synology Inc.)[36]、威聯通科技(QNAP Systems, Inc.)[37]及華芸科技(ASUSTOR Inc.)[38]，均可處理與發布該公司

產品所發現的漏洞編號，其餘台灣廠商的產品漏洞則由 TWCERT/CC 發布。台灣資通訊產業發達，素有科技島之稱，所研發販售之資通訊產品已在國際市場上廣為銷售，為協助台灣廠商重視 CNA 漏洞發布機制，提升產品的安全性，爰此，TWCERT/CC 已申請成為 Root CNA，協助我國資通訊產品漏洞的審核及漏洞編號發布，來協助相關廠商掌握其產品漏洞並及早修訂。

依 MITRE 之 CVE 漏洞編號賦予規定，TWCERT/CC 會於每年第四季，向 MITRE 申請隔年度將使用的 CVE ID 區段，來保留給台灣廠商使用。這些 CVE ID 除了分配給前述三個台灣 Sub CNA 使用之外，若 TWCERT/CC 接獲其它台灣廠商之軟、韌體產品漏洞情資，且該產品並無適當的 CNA 主責時，TWCERT/CC 將擔任與軟、韌體製造商之間的協調窗口，積極通報該產品廠商相關漏洞資訊並提醒進行漏洞修補，以利廠商維護其產品的品質與商譽。在確認接獲通知之廠商已確實掌握該漏洞情資後，TWCERT/CC 也將協助審核此漏洞情資與相關修訂情形，並賦予 CVE ID 及漏洞發布。

若由台灣的 Sub CNA 或 TWCERT/CC 所協助審核之漏洞有任何資訊更新，如最新的漏洞修補建議與版本等，本中心亦將協助提供漏洞內容更新予 MITRE，以維護 CVE 計畫漏洞揭露資料庫之全球一致性。

針對國內外所發現有關台灣廠商所開發之資通訊產品漏洞發布作業，TWCERT/CC 提出「漏洞處理框架(Vulnerability Handling Framework)」，以確保國內外資安研究機構、漏洞懸賞計畫或其他 CERT/CSIRT 組織在發現台灣產品疑似存在相關資安漏洞時，能夠有漏洞通報管道及負責發布漏洞編號的單位(如圖 38 所示)。

當 TWCERT/CC 接獲國內某產品存在新資安漏洞之通報後，若該漏洞符合 MITRE 所定義之漏洞規則，TWCERT/CC 將循「漏洞處理框架」，將漏洞相關資訊通報該產品廠商，待廠商研擬出安全更新或緩解措施後，TWCERT/CC 會協助進行此漏洞審查及編號賦予，最後將於 CVE 漏洞資料庫進行更新發布。

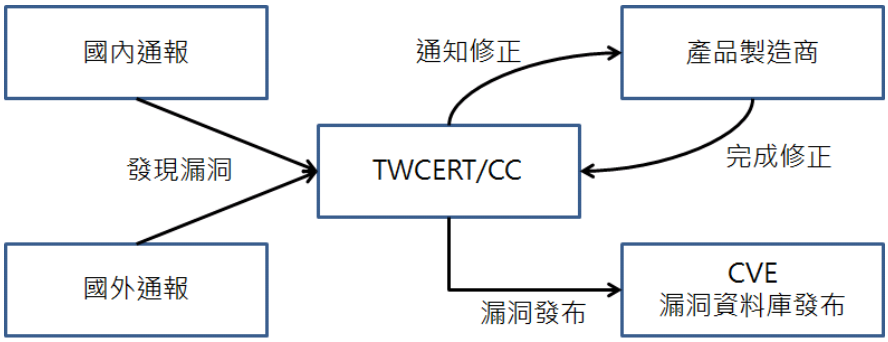


圖 38 漏洞處理框架

5.3、 亞太地區電腦事故緊急應變團隊營運概要

APCERT 是亞太區電腦事故緊急應變組織的協作機構，於 2003 年由澳大利亞、中國大陸、日本、韓國、台灣等國家的電腦事故緊急應變機構發起成立，主要願景為透過國際合作來維護亞太地區網路空間的安全與可信任度[39][40]。APCERT 從創始時的 12 個經濟體 15 個團隊，至目前已成長為 21 個經濟體 30 個團隊的規模，是當前亞太區最具公信力的電腦事故緊急應變協調組織(成員分布如圖 39 所示)。目前台灣的 TWCERT/CC、TWNCERT 及 EC-CERT 等三團隊為 APCERT 會員。

圖 39 APCERT 成員分布圖

APCERT 為了讓會員間可以有更多彼此交流的機會，以達到國際聯防效益，及讓會員有管道可汲取其他團隊經驗來提升自我能量，除每年固定舉辦年會之外，並成立了包括誘捕網(TSUBAME)、資訊交換(Information Sharing)、會員關係(Membership)、組織政策(Policy,

Procedure, and Governance)、教育訓練(Training)、病毒緩解(Malware Mitigation)及資安演練(Drill)等 7 個工作小組[41]。茲簡要說明 APCERT 各工作小組的目的與工作內容如下：

1. TSUBAME WG[42]：

成立於 2009 年，由 JPCERT/CC 所主導，負責透過封包流量監測系統 TSUBAME 來監測亞太地區可疑的掃描活動，並將所觀察到之攻擊態勢分享給相關組織。

2. Information Sharing WG：

成立於 2011 年，由 CNCERT/CC 所主導，負責識別來源資訊對 APCERT 會員的可用性，並分享給其他會員，亦積極強化成員間情資交換的機制、協議及基礎設施。

3. Membership WG：

成立於 2011 年，由 KrCERT/CC 所主導，負責審視目前各會員能力及執行適當協調工作，同時持續拓展多方合作關係，挖掘潛在會員，並協調新組織加入 APCERT。

4. Policy, Procedures, and Governance WG：

成立於 2013 年，由 CERT Australia 所主導，負責訂定方針及協助 APCERT 營運時所需要的組織與章程，並調查各會員的能力發展狀況。

5. Training WG：

成立於 2015 年，由 TWNCERT 所主導，負責全面化的教學及訓練作業的建立，幫助會員發展、運作與改進事故緊急應變管理能力，平時也舉辦資安教育訓練供會員參與。

6. Malware Mitigation WG：

成立於 2016 年，由 MyCERT 所主導，負責分享 APCERT 各成員所分析之惡意程式情資，並探討不同經濟體可能遭受攻擊的動機與特色，同時強調透過協同合作並共享惡意程式的緩解方法，減少 APCERT 各經濟體遭受惡意程式感染的機會。

7. Drill WG：

成立於 2017 年，由 ThaiCERT 所主導，負責協助當年度領導資安演練的 CERT 進行 APCERT 年度資安演練，並維護資安演練所需的手冊、流程及工作文件等。

APCERT 年度資安演練均設定主題，2018 年之主題為「物聯網上的惡意程式導致資料外洩」(Data Breach via Malware on IoT)[43]，除了 APCERT 的 20 個經濟體(澳大利亞、孟加拉、汶萊、中國大陸、台灣、香港、印度、印尼、日本、韓國、寮國、澳門、馬來西亞、蒙古、緬甸、紐西蘭、新加坡、斯里蘭卡、泰國和越南)共 27 個 CSIRT 參加之外，並邀請伊斯蘭合作組織所屬電腦事故緊急應變組織(Organization of the Islamic Cooperation- Computer Emergency Response Team, OIC-CERT)的 5 個國家(埃及、摩洛哥、奈及利亞、阿曼、巴基斯坦)之 CSIRT 一同參與[8]。

台灣 TWCERT/CC、TWNCERT 及 EC-CERT 三團隊於 APCERT 各工作小組之參與情況如下表 2 所示。

表 2. 目前台灣加入 APCERT 工作小組情況

	TWCERT/CC	TWNCERT	EC-CERT
TSUBAME	V	V	V
Information Sharing	-	V	-
Membership	-	V	-
Policy, Procedures, and Governance	-	V	-
Training	V	V	-
Malware Mitigation	V	V	-
Drill	V	V	-

電腦事故緊急應變團隊平時除了依循其資安事故處置流程，進行事故應處外，橫向協調合作更是電腦事故緊急應變團隊必須具備的功能：對外需了解全球的電腦事故緊急應變團隊所具備的能量，並積極參與國際資安組織與活動，推展雙邊及多邊國際合作關係；對內則需具有與政府機關、研究機構、服務運營商與資訊安全廠商等之橫向協調能力，藉由全面的網路安全聯防，完善資安早期預警與事故迅速排除機制。

根據美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)所提出之電腦安全事故應處指南(Computer Security Incident Handling Guide)[44]，資安事故應變與處理程序循環包含準備(Preparation)、發現與分析(Detection & Analysis)、控制移除與復原(Containment, Eradication & Recovery)、後續活動(Post-Incident Activity)等四大階段(如圖 40)。

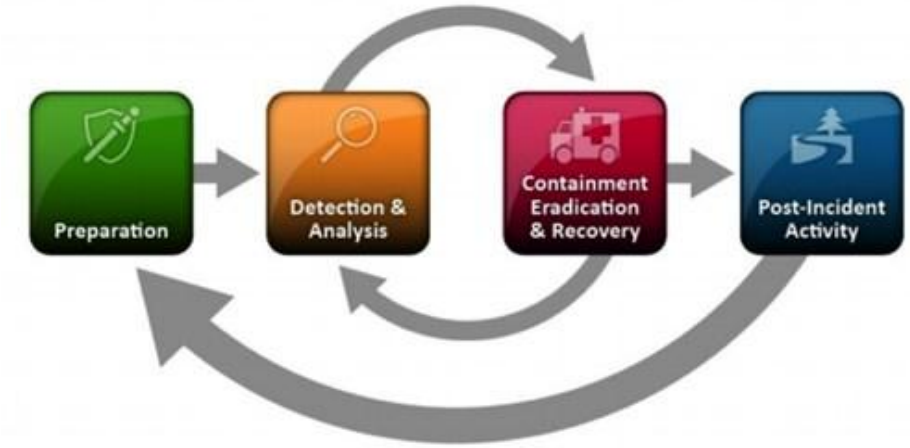


圖 40 資安事故處置循環[48]

此外，網路攻擊事故常具跨國性質，事故的處理已不再是憑一己之力就可解決；透過積極參與各 CERT(如 APCERT、FIRST 等)，及時了解各國所面臨的網路攻擊與威脅樣態，並與各組織分享應處程序、技術與方法，方能使我國融入國際網路安全聯防體系，發揮網路聯防成效。

5.4、 台美國家資通安全戰略比較

2018年9月，國家安全會議國家資通安全辦公室發布我國第一本國家資通安全戰略報告，報告以「資安即國安」戰略為上位指導方針，闡述戰略之形成、願景、目標、推動策略，並將透過持續優化國家資安機制、強化國家資安體系運作效率及完備資安自主產業生態體系等三大努力方向予以落實；同月美國亦提出「美國國家資安戰略(National Cyber Strategy of the United States of America)」報告，宣示未來 15 年美國資安戰略的四大支柱(pillars)，並將透過保護美國網路系統之運作與資料安全捍衛其國土，藉由培育及促進美國國內之數位經濟與創新力求其繁榮，並且強化與盟邦及合作夥伴間的關係，打擊網路惡意行為，維護網路環境的開放、可信與安全。

透過比較我國國家資通安全戰略報告「資安即國安」與「美國國家資安戰略」報告，可見台、美國家資通安全戰略類似與相輔相成之處，在於政府領導機制、關鍵基礎設施之資安問題、數位經濟發展，以及打擊經濟犯罪維護自由價值等四大面向，而我國也將本諸蔡總統於一〇七年國慶談話中所揭示之國家安全整體布局，由確保民主制度及社會經濟正常運作，

同時重整並全新布局我國全球經貿戰略的角度出發，根據「系統導向、軟硬整合、軍民合一、國際鏈結」等四大方向，執行我國經濟及安全能力的建構與提升，並落實於我國資安體系之建構和運作中，以積極回應美國印太戰略，同時增進國內產官學界及國外盟邦之合作關係，快速提升我國科技水準及研發能量，持續在國際資安聯防體系中肩負責任並提供實質貢獻。

第六章、 TWCERT/CC 漏洞揭露政策

針對國內外所發現有關台灣廠商所開發之資通訊產品弱點發布作業，TWCERT/CC 提出「弱點處理框架(Vulnerability Handling Framework)」，以確保國內外資安研究機構、漏洞懸賞計畫或其他 CERT/CSIRT 組織在發現台灣產品疑似存在相關資安弱點時，能夠有弱點通報管道及負責發布弱點編號的單位。今年 TWCERT/CC 已經 MITRE 核准成為台灣之弱點編號授權單位 - Root CNA，協助 MITRE 審核及分配台灣廠商設計開發的資通訊軟、韌體產品所通報資安弱點的 CVE ID，可在漏洞訊息尚未揭露下，協助台灣廠商早期掌握與即時弱點修訂。當 TWCERT/CC 接獲國內某產品存在新資安弱點之通報後，若該弱點符合 MITRE 所定義之弱點規則，TWCERT/CC 將循弱點處理框架，將弱點相關資訊通報該產品廠商，待廠商研擬出安全更新或緩解措施後，TWCERT/CC 會協助進行此弱點審查及編號賦予，最後將於 CVE 弱點資料庫進行更新發布。

當今企業不僅需要提供各種多元的服務與應用，更得對抗日趨複雜的資安威脅。TWCERT/CC 鼓勵台灣資通訊產品開發商致力於增進其產品的安全性，建議產品開發商應該積極的看待弱點發布機制，即時修補所發現之產品弱點，並通知使用者進行更新，讓使用者享受產品功能之餘，不用擔心產品弱點遭利用而進一步引發資安事件。

6.1、 簡介

做為可信的漏洞通報中介單位，本中心自 2018 年起參與美國 MITRE 之通用漏洞揭露(Common Vulnerabilities and Exposures, CVE®)計畫 ，申請成為 CVE 編號管理者 (CVE Numbering Authorities, CNA)，並建置台灣漏洞紀錄 (Taiwan Vulnerability Note, TVN)平台，透過協助國內外廠商處理產品漏洞，以儘快完成漏洞緩解及修補，避免有心人士利用產品漏

洞造成使用者遭駭之情況發生。

以上的努力，均為共同維護台灣整體網路安全穩健，從安全、便利、效能三面向來推動資通安全，以逐步實現建構網路安全環境之願景。

6.2、 漏洞通報方式

漏洞通報者可將漏洞細節報告及相關佐證資料寄至 cve@cert.org.tw，本中心將於接獲資料後進行後續處理流程。

若欲使用 PGP KEY 先行將檔案加密再寄給本中心，請使用本中心公開之 PGP KEY (網址：https://twcert.org.tw/subpages/aboutus/pgp_key.aspx, KeyID： 1E9D1F1B)。

6.3、 漏洞揭露方式

本中心之漏洞揭露及處置方式，係根據 CVE®官方所公布之 CVE 編號管理規則 (網址：https://cve.mitre.org/cve/cna/rules.html)及中華民國法律規定。各項規範若有說明不足處，TWCERT/CC 保留最終解釋權。

6.4、 漏洞報告公開時程

任何通報至本中心之漏洞報告，將於通報日期起 45 個日曆天內公開報告之基本資料，包含主旨、通報日期、事件日期、影響產品、簡要描述、通報人等資訊，例如於 2018 年 8 月 1 日接獲通報，則最晚於 2018 年 9 月 14 日公開上述資訊。

漏洞報告中所闡述之詳細漏洞利用方式等技術細節，則於該漏洞有明確漏洞緩解方式、廠商已公告修補版本，或確認該報告提及之漏洞無須處理後公開，不設定強制公開時間。

本中心有權利可於判斷漏洞影響程度後，決定是否延後各項資訊之公開時程，以及公開內容之詳細程度。

6.5、 漏洞報告處置流程

本中心於接獲漏洞通報後之處置流程如圖 41 所示。漏洞通報者發掘漏洞，並通報漏洞技術細節至本中心，本中心接獲漏洞通報後，首先進行初步判斷，確認漏洞報告之內容是否足夠，若尚有缺漏處則請漏洞通報者補充，確認無須補充後，本中心發放此漏洞通報一 TVN 編

號，並於 45 個日曆天內於 TVN 平台中公布漏洞基本資訊。

接著，本中心將漏洞報告提供產品廠商，由產品廠商確認漏洞資訊，本中心則協助產品廠商及漏洞通報者傳遞漏洞資訊、漏洞修補結果驗證之確認訊息。

最後，待三方皆確認漏洞修補完成或有相對應漏洞緩解方法後，本中心將把漏洞技術細節公布於 TVN 平台中。

若接獲之漏洞報告資訊有下述情況，本中心有權決定暫停或停止處理該份報告，包括「不足以確認漏洞內容或發生原因、違反官方 CVE 編號管理規則 (CVENumbering Authorities (CNA) Rules)、無法聯繫漏洞通報人釐清細節等。」。

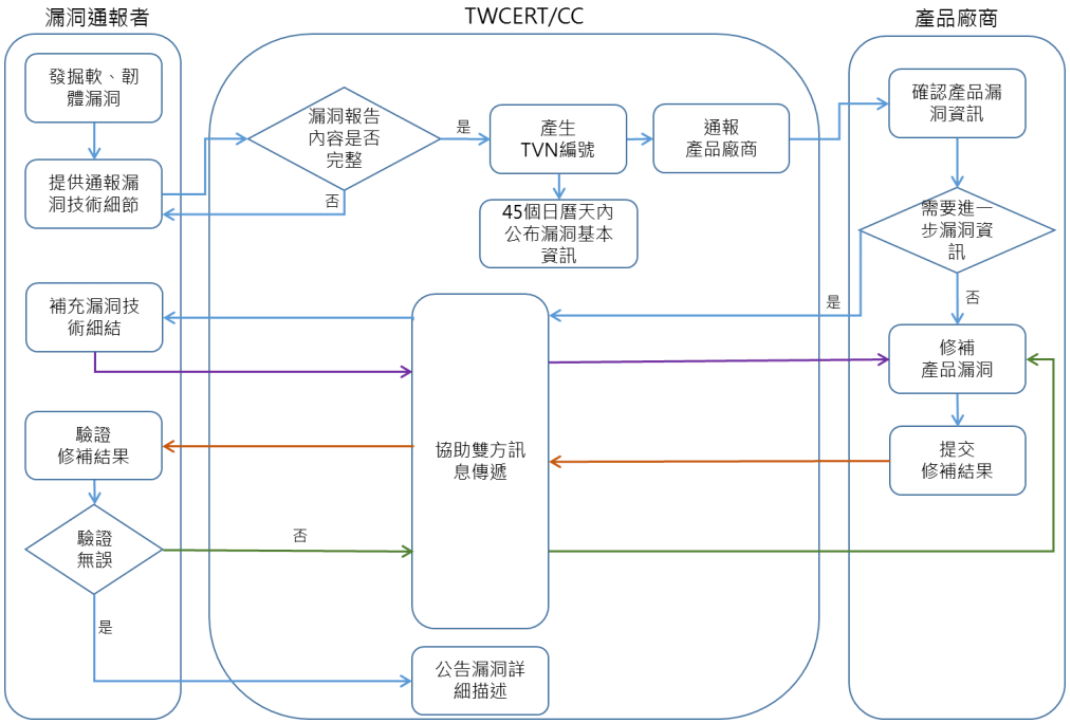


圖 41 漏洞報告處置流程

6.6、 CVE 編號發放規則

若在漏洞報告處理流程中，於漏洞通報者、本中心或是產品廠商對於所發現的漏洞欲申請 CVE 編號，將由三方共同確認是否通過官方定義之 CVE 編號發放規則，如圖 42 所示。一旦確認符合申請 CVE 編號之資格，則由三方確認資訊後，由本中心發放 CVE 編號給該漏洞。

CVE 編號發放規則包含三個數量計算判斷 (Counting Decision, CNT)及五個資格判斷

(Inclusion Decisions, INC)，CNT 是用來判斷該 Bug 可分成幾個漏洞處理，INC 則是判斷該漏洞是否可以被發布，因此，一個 Bug 必須經過判斷八個條件皆符合後，才能確認其中包含幾個漏洞，以及每個漏洞是否可發放 CVE 編號，也就是說，有可能會有無法發放 CVE 編號給某一漏洞的狀況發生。

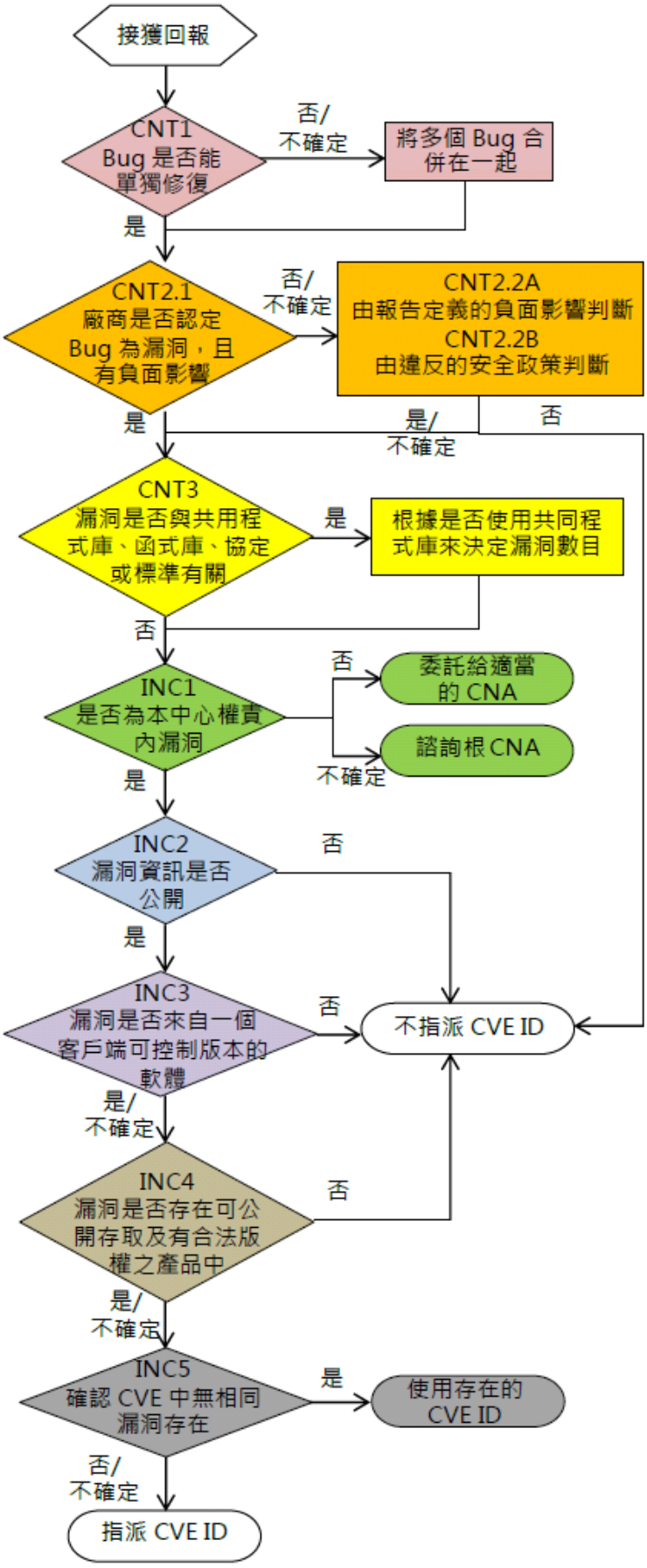


圖 42 CVE ID 發放規則

6.7、 漏洞通報者稱呼及聯繫方式公開

本中心於公開漏洞通報紀錄時，會一併將漏洞提報者之稱呼公開，該稱呼可為，且不限於暱稱或單位名稱等，以確保發掘漏洞的功勞可歸功於此漏洞通報者，若漏洞通報者不希望稱呼被公開，可於任何時間告知本中心，本中心將協助修改並顯示為匿名。

本中心擔任漏洞通報者與產品廠商間的協調者，協助雙方確認漏洞細節及修補進度等事項，若產品廠商在接獲漏洞報告後需要對漏洞通報者進一步詢問細節，本中心將先行詢問漏洞通報者是否願意提供電話或電子郵件等聯繫方式至產品廠商，若是，則將由產品廠商直接聯繫漏洞通報者以確認漏洞細節，惟仍須告知本中心漏洞修補狀況，以利更新漏洞報告資訊；若否，產品廠商則無法直接聯繫漏洞通報者，並由本中心擔任產品廠商及漏洞通報者間溝通橋樑。

完整 TWCERT/CC 漏洞揭露政策請至本中心官網公開文件下載。

更多資訊請參考 CVE 計畫網站：https://cve.mitre.org/

第七章、 合作交流與資安推廣

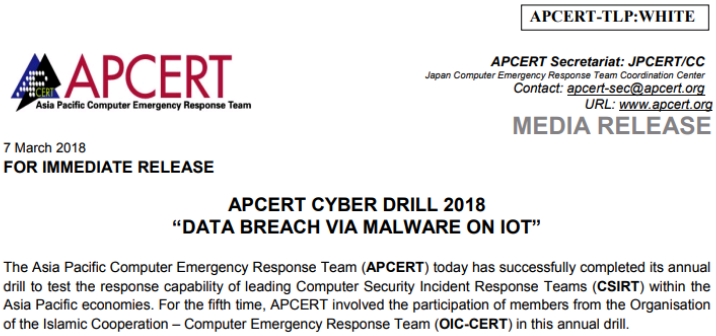
TWCERT/CC 平時積極與國際資安組織協同合作，目前為 FIRST 資安事件應變小組論壇(Forum of Incident Response and Security Teams)及 APCERT 亞太區電腦緊急事件回應小組(Asia Pacific Computer Emergency Response Team)會員，定期參與每年盛大年會及網路攻防演練，透過定期參與這些活動，了解各國事件應變團隊運作狀況、汲取資訊防護及資安威脅新知、並提升資安事件應變能量。除了與國際資安組織交流外，TWCERT/CC 亦於本年度分別舉辦兩次台灣 CERT/CSIRT 聯盟第四次及第五次工作會議，以促進國內資安組織交流。

此外，TWCERT/CC 亦於平時配合企業組織/產業公協會舉辦資安座談會、研討會及教育訓練，希望能透過這些活動來提升民間資安意識，推廣 TWCERT/CC 服務內容、資安通報的重要性促進民眾通報意願，並且也於今年舉辦 2018 年台灣資安通報應變年會，以企業無可避免的資安管理責任為此次會議主軸。

7.1、 國際資安組織交流現況

7.1.1、 參與亞太區電腦緊急事件回應小組 2018 年網路攻防演練(APCERT CYBER DRILL 2018)

TWCERT/CC 於 3 月 7 日參與一年一度之亞太區電腦緊急事件回應小組 2018 年網路攻防演練(APCERT CYBER DRILL 2018)，並於演練中擔任腳本設計及參與實際演練。本年度之演練主題為「透過 IOT 病毒導致資料外洩(DATA BREACH VIA MALWARE ON IOT)」，APCERT 之官方新聞稿請參考：https://www.apcert.org/documents/pdf/APCERTDrill2018PressRelease.pdf。



APCERT-TLP:WHITE

APCERT
Asia Pacific Computer Emergency Response Team

APCERT Secretariat: JPCERT/CC
Japan Computer Emergency Response Team Coordination Center
Contact: apcert-sec@apcert.org
URL: www.apcert.org

MEDIA RELEASE

7 March 2018
FOR IMMEDIATE RELEASE

APCERT CYBER DRILL 2018
"DATA BREACH VIA MALWARE ON IOT"

The Asia Pacific Computer Emergency Response Team (**APCERT**) today has successfully completed its annual drill to test the response capability of leading Computer Security Incident Response Teams (**CSIRT**) within the Asia Pacific economies. For the fifth time, APCERT involved the participation of members from the Organisation of the Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**) in this annual drill.

圖 43 APCERT Cyber Drill 2018

7.1.2、 協助「No More Ransom」計畫完成正體中文網頁翻譯

TWCERT/CC 於 106 年 5 月成為「拒絕勒索軟體(No More Ransom)」計畫夥伴，並於日前協助完成正體中文網頁之翻譯。

「拒絕勒索軟體」計畫是由荷蘭國家警察高科技犯罪單位 (National High Tech Crime Unit of the Netherlands' police）、歐洲刑警組織歐洲網路犯罪中心 (Europol' s European Cybercrime Centre）、卡巴斯基資安公司 (Kaspersky Lab) 及麥考菲資安公司 (McAfee) 所共同創立。該計畫目的為幫助勒索軟體的受害者，使他們在不用付贖金的狀況下也可以回復被加密的檔案。

若民眾發現電腦中了勒索病毒，可以先至此網站進行查詢是否已有解鑰可使用，若有，則可順利將遭加密的檔案還原。我們並不建議付贖金。付贖金給網路罪犯只能確認勒索軟體有效，並不能確保你可因此拿到所需的解鑰。

The No More Ransom Project:

https://www.nomoreransom.org/zht_Hant/index.html

圖 44 No More Ransom Project

7.1.3、 參加 30th FIRST 年會

資安事件應變小組論壇(Forum of Incident Response and Security Teams, 簡稱 FIRST)是國際最大的非營利資安組織，每年定期會舉行重要的國際資安會議。第 30 屆年會於 2018 年 6 月 24 日至 6 月 29 日間舉辦，此次年會由馬來西亞國家資訊安全局(NATIONAL CYBER SECURITY AGENCY, NACSA)及馬來西亞電腦緊急應變小組協調中心(CYBERSECURITY MALAYSIA)於馬來西亞吉隆坡舉行。

為了因應日新月異的網路資安事件，FIRST 成立於 1990 年，今年度 FIRST 會員已超過 420 個組織，包含政府機構、私人企業、學術研究單位等，遍佈美洲、歐洲、亞洲等，而台灣電腦網路危機處理暨協調中心(TWCERT/CC)亦為 FIRST 組織的正式成員，亦出席此次年會。會中，本中心積極與各國之 CERT/CSIRT/PSIRT 組織會員互動，以交流國際最新資安態勢，並參與各項會員活動、議題討論及訓練課程。

圖 45 參與 FIRST 2018 年會

7.1.4、 參與 THE HONEYNET PROJECT ANNUAL WORKSHOP 2018

The Honeynet Project Workshop 為非營利組織，每年由全球不同的分會舉辦年會並探討最新誘捕網趨勢，今年則於 2018 年 7 月 9 至 10 日由台灣分會於台大集思會議中心舉辦。TWCERT/CC 羅文翎分析師受邀參與年會進行專題報告，並以「Development of Honeynet projects in APCERT」為題進行分享，介紹 APCERT 相關工作小組所進行的誘捕網專案之發展現況。

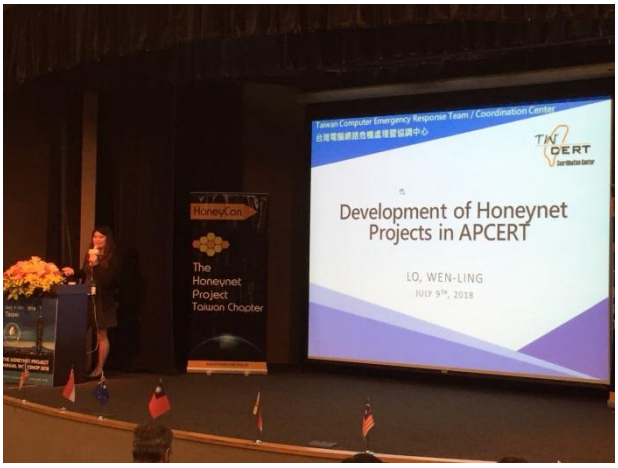


圖 46 THE HONEYNET PROJECT ANNUAL WORKSHOP 2018 演講

7.1.5、 與 TEAM CYMRU 簽訂合作備忘錄

為建構國際資安聯防體系，TWCERT/CC 與長期關注網路惡意行為的 TEAM CYMRU 建立合作機制，互享資安情資，以挖掘並降低我國電腦網路對外之惡意連線，打造安全可信賴的網路空間。

圖 47 TEAM CYMRU logo

7.1.6、 與 FS-ISAC 簽訂合作備忘錄

為建構國際資安聯防體系，TWCERT/CC 與長期關注金融領域資安情資的 FS-ISAC (Financial Services Information Sharing and Analysis Center)建立合作機制，互享資安情資，以提升我國資安防護能量。

圖 48 FS-ISAC logo

7.1.7、 參與 OIC-CERT 2018 年網路攻防演練

本中心於 9 月 18 日獲邀，參與一年一度之伊斯蘭合作組織電腦緊急事件回應小組(the Organisation of The Islamic Cooperation – Computer Emergency Response Teams, OIC-CERT)2018 年網路攻防演練 (OIC Drill 2018)，本年度之演練主題為「加密貨幣風險及緊急威脅 (Crypto-currencies Risks and Emerging Threats)」。

此次主辦單位為阿曼國家電腦緊急應變小組 (Oman National CERT, OCERT)，演練內容包含資安通報處置、惡意鑑識及資料情蒐等情境題，讓參與的 CERT 熟悉高風險資安威脅，以及應處方式。

圖 49 OIC-CERT 2018 年網路攻防演練

7.1.8、 申請並成為 CVE 編號管理者 (CNA)

本中心自 2018 年起參與美國 MITRE 之通用漏洞揭露 (Common Vulnerabilities and Exposures, CVE®)計畫，已完成申請並成為 CVE 編號管理者 (CVE Numbering Authorities, CNA)，並建置台灣漏洞紀錄(Taiwan Vulnerability Note, TVN)平台（建置中），透過協助國內外廠商處理產品漏洞，以儘快完成漏洞緩解及修補，避免有心人士利用產品漏洞造成使用者遭駭之情況發生。

CVE 編號管理者 (CVE Numbering Authority, CNA) 為一志工組織，可為來自世界各國之國家 CERT、產業 CERT、研究機構、漏洞提報組織或廠商等。每個 CNA 都有不同的權責範圍，並有權限可以對權責範圍內之產品漏洞發布 CVE ID，以及後續對 CVE ID 的內容進行維護。

目前全球 CNA 列表請參考官網。

(https://cve.mitre.org/cve/request_id.html#cna_participants)

以上的努力，均為共同維護台灣整體網路安全穩健，從安全、便利、效能三面向來推動資通安全，以逐步實現建構網路安全環境之願景。

TWCERT/CC 漏洞揭露政策：https://twcert.org.tw/subpages/ServeThePublic/public_document_details.aspx?id=65

7.2、 國內資安推廣現況

7.2.1、 台灣 CERT/CSIRT 聯盟

TWCERT/CC 除了主/協辦資安會議、座談會及講座外，並於 105 年主導成立「台灣 CERT/CSIRT 聯盟」，聯盟成員除主要之政府 CERT 外，也納入國內相關資安企業，透過定期會議互通國內各界資安情資與資安應處經驗分享，並邀請我國資安主管機關行政院資安處長官以貴賓身分參加，以協助政府了解全台資安態勢樣貌、推動資安政策與強化國內各界資安防護能量，建構我國安全網路使用環境。TWCERT/CC 於「台灣 CERT/CSIRT 聯盟」之推廣除邀請現階段已具有資安事件處理團隊(CERT/CSIRT)之企業加入外，另外 TWCERT/CC 也積極邀請國內具資安監控技術與服務(Security Operation Center, SOC)之企業加入聯盟，本年已陸續增加了安碁資訊、果核數位、德欣寰宇科技、安華聯網、晶元光電及德安資訊等六家企業，目前聯盟成員共計 15 個單位(如表 3)。

107 年 7 月 4 日召開「台灣 CERT/CSIRT 聯盟」第 4 次工作會議(如圖 50)，會中請勤業眾信 DTTW-CSIRT 陳威棋協理分享「資安攻防演練與應變實務」講座，讓企業了解如何利用與規劃攻防演練來了解與強化企業的應變機制，另外會中亦針對各單位近期處理資安事件通報所遇問題進行探討，及聯盟成員分享重要資安事件處理心得與成果，藉此交流學習不同情境之事件處理作法。

107 年 10 月 3 日召開「台灣 CERT/CSIRT 聯盟」第 5 次工作會議(如圖 50)，除了各單位分享近期資安事件處理經驗外，亦特別邀請工研院資通所卓傳育副組長分享「資安整合服務平台-智慧製造篇」，為經濟部工業局 107 年新興資安產業生態系推動計畫，包含：「打造資安強化示範場域，創造需求帶動資安產業發展；提供安全軟體開發工具服務，厚植產業安全開發能量；鼓勵發展自主新興資安解決方案，聚焦主動安全強化；輔導廠商落實資安健檢；按需求採購，上架安全軟體開發工具；按場域或產品需求執行專業滲透測試服務，紅隊演練、藍隊防禦、紫隊監控；新興或跨域整合資安解決方案上架整合平台提供服務。」，讓聯盟成員藉由此機會了解這些資訊，並協助推廣此計畫給所需要的單位。

圖 50 台灣 CERT/CSIRT 聯盟第 4 次及第 5 次工作會議

表 3 台灣 CERT/CSIRT 聯盟成員(依筆劃排序)

聯盟成員中文名稱	聯盟成員英文名稱
台灣電腦網路危機處理暨協調中心	TWCERT/CC(Taiwan Computer Emergency Response Team / Coordination Center)
台灣學術網路危機處理中心	TACERT(Taiwan Academic Network Computer Emergency Response Team)
台灣電腦安全事件應變中心	TWCSIRT(Taiwan Computer Security Incident Response Team)
安華聯網科技股份有限公司	Onward Security
安碁資訊股份有限公司	Acer Cyber Security Inc.
果核數位	Digicentre
晶元光電股份有限公司	EPISTAR
國家電腦事件處理中心	TWNCERT(Taiwan National Computer Emergency Response Team)
國家通訊傳播委員會	NCC-CERT(National Communications Commission Computer Emergency Response Team)
電子商務資安服務中心	EC-CERT(Electronic Commerce – Computer Emergency Response Team)

聯盟成員中文名稱	聯盟成員英文名稱
德安資訊股份有限公司	Athena Information Systems
德欣寰宇科技股份有限公司	TSC CAPITAL GROUP
群暉科技 - 產品安全事件應變團隊	Synology-PSIRT(Product Security Incident Response Team)
勤業眾信 - 台灣數位安全事件應變團隊	DTTW-CSIRT(Deloitte Taiwan Computer Security Incident Response Team)
趨勢科技股份有限公司	TM-CSIRT(Trend Micro Computer Security Incident Response Team)

7.2.2、 資安研討會/座談會協辦/演講

為了提升民間企業的資安意識，並讓民間企業了解發生資安事件時，有專業的資安諮詢管道，藉由參與國內資安相關會議深入民間企業及產業公會，宣導資安意識的重要性，及資安事件通報的好處與必要性，作為強化民間企業資安防護環境的前線，TWCERT/CC 今年主/協辦資安相關會議、講習、座談會等，共計 17 場次，其中有 5 場次除配合各會議主題進行相關資安議題發表外，亦於活動會場擺設 TWCERT/CC 業務與資安宣導攤位，利用和與會民眾面對面互動，進行民眾資安意識推廣並讓民眾更了解 TWCERT/CC 的服務項目與內容。

2/7 電腦稽核協會台北月例會

3/19 中小企業總會員工教育訓練

3/28 資訊安全前瞻商機研討會

4/25-27 2018 亞太資訊安全論壇

5/2 健行科技大學資工系資安講習

5/2-3 2018 駭客任務-資安戰役及 IRCON

6/27 TiEA 資安講座-資安防禦最前線

7/9-10 Honeynet Project Annual Workshop 2018

7/10-12 2018 國際資訊安全組織臺灣高峰會

7/27-28 HITCON Community

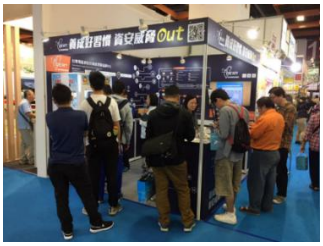
8/18 2018 神盾盃網路奪旗競賽

8/19 107 年度高中職資安種子教師研習營

9/29 TDOH Conf.

2018 11/2 2018 賽門鐵可資安論壇

11/29 中華航空保安緊急應變處置研討會



11/28-12/3 107 資訊月

12/13-14 HITCON Pacific

圖 51 資安研討會及座談會辦理狀況

7.2.3、 2018 台灣資安通報應變年會成果紀實

TWCERT/CC 於 10 月 3 日於集思台大會議中心舉辦『2018 台灣資安通報應變年會-企業無可避免的資安管理責任』，今年的會議是 TWCERT/CC 成立以來所舉辦最盛大的資安研討會，今年參與人數多達 450 人，比起去年增加了 100 多名與會者，也代表越來越多人開始對資安重視，以及對 TWCERT/CC 的認識。

今年的會議是以企業無可避免的資安管理責任為主軸，本次研討會共有 11 場精彩議程，上午分別進行兩場 Keynote 及座談會，下午則分別以電子商務資訊安全及資安事件應處策略進行分場研討，另外，在會議議程中間休息時間，亦特別邀請到 9 家資安廠商/社群前來分享資安防護策略及資安治理理念，研討會場邊設有 15 家資安廠商/社群/單位，以提供一個讓聽眾與廠商近距離接洽的機會，另外也有攤位集點換贈品及抽獎的活動。參與此場會議主要目的是，讓聽眾了解『資安防禦與管理之因應之道』、『如何自主建置資安事件應變團隊』、『資安通報的重要性及好處』，以及『面臨資安管理法之應對方式』。

在當今的網路世代，資安問題將愈來愈受重視，企業經營時，更應考量必要的資安防護，並制定完善的資安政策及通報應變標準作業流程，才能面對席捲而來的資安威脅與挑戰。上午場由國家中山科學研究院營運長蔡嘉芳進行開幕致詞，以及國家通訊傳播委員會主委詹婷怡進行貴賓致詞，兩人均談到本次活動舉辦的重要意義與主要目的，以及數位時代所帶來的風險。其中通訊傳播委員會主委詹婷怡亦表示：「隨著重大資安事件愈來愈頻繁，國人應如何強化與改善資安防禦措施及資安緊急應變機制，國家也應建立資安聯防體系，並提升整體資安防禦能量，以因應瞬息萬變的資安威脅。」。

行政院資安處副處長徐嘉臨於 Keynote 場次演講 - 「資通安全管理法及子法實施說明」，針對全球所面臨的資安威脅趨勢，以及國際間多件重大的資安事件進行分享，並說明「資通安全管理法」及其 6 個子法實施內容，包含各公務機關、關鍵基礎設施提供者、公營事業、政府捐助之財團法人被賦予的責任，積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，確保國家安全與公共利益。

另外，此次特別邀請到亞太網路資訊中心（Asia-Pacific Network Information Centre，

APNIC）的資深網際網路安全專家 Adli Wahid 擔任 Keynote 演講者，主講「Security Collaboration Beyond Your Traditional Borders（跨越傳統邊界的網路安全合作）」，Adli 先生以多年國際資安合作的經驗，分享自身在 APNIC 及 FIRST 協助各國家建置資安事件應變中心的心得，於會中提及當前的網路攻擊事件已經超越國界，攻擊事件也橫跨企業與社群，但由於各國政府之間各自為政，加上官僚習氣，彼此間的信任基礎薄弱，不願意分享各國所發生的資安事件資訊，這都造成資安事件在各國間重複的發生，如今透過 CERT/CSIRT、APCERT、FIRST、DFAT 等組織之間的協同合作，互通訊息與經驗交流分享，才能夠打破國界，讓資安事件得以減少並盡速加以解決。並特別強調組織間在進行情資交流時應建立彼此的信任之上，且應以共同建立穩健安全的網路環境為目標，互助合作，建立資安聯防體系。

在 Adli Wahid 精彩的演講後，則以座談會的方式針對「面臨網路新時代資安威脅之因應對策」主題進行探討，由行政院資安處徐副處長擔任主持人，APNIC Adli Wahid、經濟部中小企業處主任秘書陳國樑、TWCERT/CC 主任陳永佳，以及奧義智慧創辦人吳明蔚擔任與談人，與聽眾以當前面臨的資安威脅，政府與民間企業之間合作方式、資安事件的通報案例、中小企業如何在有限資源下把資安做好、資安法規範的細節等議題進行研討與交流。

下午場則分成兩個主題同時進行，「電子商務資訊安全」與「資安事件應處策略」，其中以「電子商務資訊安全」主題，TWCERT/CC 沈紀威分析師主講「資安聯防全面啟動」，分享近期常見的幾種網路詐騙手法，及建議相關防護措施與電商及消費者，並也介紹日本健全的資安聯防體系 CSIRT 聯盟及 TWCERT/CC 現階段持續推動的台灣 CERT/CSIRT 聯盟運作方式及目的，宣導資安聯防的重要性。

EC-CERT 正工程師林耕宇主講「從電子商務資安事件，來看通報與應變聯防之作為」，說明台灣電子商務所面對的資安風險，分享資安攻擊的四大階段，以及網路攻擊的常見手法，應如何建立智慧情資與通報聯防機制，在處理資安事件時，應從不同面向來處理，並建構關聯的分析模組，且提及企業應注重政策與管理、情資與通報、鑑識與杜絕、應變與處理四個面向，以落實電商資安事件的處理。

賽門鐵克首席資深技術顧問張士龍主講「數位科技資安聯防人人有責！」，依據 2018 賽

門鐵克網路威脅分析報告，分析出常見的各種網路威脅形式，並提出資安監控服務、基礎架構防護、資安顧問服務等三種資訊安全防護鐵三角概念，接著以新加坡 SingHealth 醫療系統遭到駭客入侵為例，說明事件發生的經過，並也介紹 WhiteFly 駭客組織，及他們採用的攻擊方式，讓參與此議程的聽眾能有所警覺，藉以提升聽眾的資安意識。

工研院資通所卓傳育博士 / 副組長主講「電商系統之主動安全防禦策略」，說明電子商務安全的六個面向、電子商務主要面對的威脅，及如何將電子商務威脅減至最低，並透過數件重大網路安全事件為例，說明如何主動做好資安防禦，且也於會中推廣資安整合服務平台。

下午場另一個主題是以「資安事件處理策略」為主軸，安碁資訊資深經理孫明功主講「新世代資安防護管理中心（Intelligent SOC）」，介紹區域聯防中心整體架構，如何透過 SOC 進行集中監控，從異常徵兆中發現資安事件，並應用機器學習演算法進行偵測，進行整體分析，達成全方位的資安防護。

合勤投控資訊服務處游政卿協理主講「知己知彼、百戰不殆－建構合宜的資安防禦體系」，分析各種威脅樣態與防護機制，如何防治進階持續性威脅，並介紹了合勤資安的防護架構，分析各種駭客的行為，並針對各種不同的攻擊樣態，給與相關的防護建議。

群暉科技事件應變團隊負責人江瑞敏主講「產品的資安守門員 - PSIRT 產品安全事件應變團隊任務」，首先介紹群暉科技的歷史與 NAS、OS 等相關產品線、群暉的產品資安事件應變團隊（Product Security Incident Response Team，PSIRT），並且說明群暉在面臨資安事件時，PSIRT 如何進行相關的應變作業，及如何與國際間各大網路安全單位合作，加入事件處置效率，以達資安聯防的目的。

勤業眾信聯合會計師事務所陳威棋協理主講「如何有效建置資安應變機制與資安事件調查團隊」，特別提及在數位創新時代，速度是決勝的關鍵，在面對駭客攻擊時，快速的反應速度是事件應處的關鍵，各國也陸續研擬相關法規，針對資安事件通報與應變之要求，有嚴格的規範。並也介紹如何建置資安應變機制與事件調查團隊。

在面對資安威脅多變的世代，企業內部的資安政策應落實，伴隨著企業內部業務及資安風險的變動，資安政策也應做相對的調整，相信聽眾在參與此次會議後，對於資安通報應變、

跨界資安合作將有更進一步的理解與應用，並將所學的知識帶回企業，讓企業內部的資安防護體系及資安政策的建構上能更完善。

圖 52 貴賓合影

圖 53 會議進行狀況

圖 54 廠商攤位

圖 55 Lighting Talk

圖 56 座談會

圖 57 上午場司儀籌備

圖 58 上午報到

圖 59 上午報到

圖 60 中場休息

圖 61 演講狀況

圖 62 閉幕抽獎

圖 63 閉幕抽獎合影

結語

在面對網路攻擊手法愈趨多樣化的世代，人們的資安意識逐漸抬頭，當企業受到一波又一波網路攻擊的影響後，企業對於資安防護也逐漸開始重視，許多國家也開始擬定相關的資安法規，嚴格要求企業遵循規範，若企業違反規定，將遭受鉅額罰款，商譽造成損害，影響企業整體的生產力，因此企業也不得不開始對自己的資安防護負責。

資安在企業內部所扮演的角色可為兩大面向，一是以企業本身研發產品的資訊安全為導向，平時隨時掌握產品是否存在漏洞，若產品有漏洞，是否有妥善完成修補及發布修補資訊，以此目標運作的團隊則稱為產品資安事件應變小組 (Product Security Incident Response Team，PSIRT)；另一個面向則是以企業本身對內及對外的資安防禦體系為主，企業內部的多層次的資安防護架構是否完善，小至個人電腦，大至企業所建構的防火牆設備等，皆需持續監控是否有受駭的跡象，除了實體防禦外，亦須持續修正企業內部資安管理政策及資安通報應變機制，確保所有的 SOP 皆能解決現階段的資安問題，另外亦需定期辦理資安教育訓練、資安稽核等，以此目標運作的則稱為電腦網路危機緊急應變處理團隊 (Computer Security

Incident Response Team, CSIRT)，服務的對象則包括企業內部員工、合作夥伴、客戶服務。

企業在有限的經費下做資安投資，在投資前應做企 -業內部資訊系統盤點，了解每個系統的風險影響等級，以企業內部重點資訊系統進行防護，以發揮最大的功效，然而資安防禦體系的建構應隨著新興的資安威脅而有所調整，才能即時因應新型態的駭客攻擊。

參考資料

[1] Adguard. (2017, October 12). “Cryptocurrency mining affects over 500 million people. And they have no idea it is happening.”, Retrieved March 7, 2018, from the World Wide Web: https://blog.adguard.com/en/crypto-mining-fever/

[2] Enisa. (2017, November 10). “Cryptojacking - Cryptomining in the browser”, Retrieved February 7, 2018, from the World Wide Web: https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser

[3] Adblockplus. “Adblock Plus”, Retrieved February 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/adblock-plus/cfhdojbkjhnklbpkdaibdccddilifddb?hl=zh-TW

[4] Adguard. “AdGuard 廣告阻擋器”, Retrieved February 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/adguard-adblocker/bgnkhhnnamicmpeenaelnjfhikgbkllg?hl=zh-TW

[5] Tunghobrens. “Anti Miner - No 1 Coin Minerblock”, Retrieved February 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/anti-miner-no-1-coin-mine/ibhpgkhoicjhklmbhdoeikeggbeejonj

[6] CryptoMineDev. “minerBlock”, Retrieved February 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl

[7] Keraf. “No Coin - Block miners on the web!”, Retrieved February 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/no-coin-block-miners-on-t/gojamcfopckidlocpkbelmpjcgmbgjcl

[8] TWCERT/CC. (2018, March 16). “手機間諜軟體分析—以 Skygofree 為例”, Retrieved April 7, 2018, from the World Wide Web: https://www.twcert.org.tw/subpages/ServeThePublic/public_document_details.aspx?id=51

[9] 刑事警察局. (2018, March 29). “「詐騙爛貨復活倉儲！滿坑滿谷肚臍貼！」偵破臉書一頁式廣告販售偽劣貨詐欺案”, Retrieved April 7, 2018, from the World Wide Web: https://www.cib.gov.tw/News/Detail/34194

[10] 台北市政府警察局防制詐騙中心. (2018, January 11). “新興詐欺手法專案報告 六大特徵，破解一頁式廣告詐騙!”, Retrieved April 7, 2018, from the World Wide Web: http://themes.gov.taipei/ct.asp?xItem=380501579&ctNode=45816&mp=10800d

[11] Kaspersky Lab. (2018, April 16). “Roaming Mantis uses DNS hijacking to infect Android smartphones”, Retrieved June 7, 2018, from the World Wide Web: https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/

[12] Trend Micro. (2018, April 17). “XLoader Android Spyware and Banking Trojan Distributed via DNS Spoofing”, Retrieved June 7, 2018, from the World Wide Web: https://blog.trendmicro.com/trendlabs-security-intelligence/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing/

[13] Dray Tek. (2018, May 18). “Notification of Urgent Security Updates to DrayTek routers”, Retrieved June 7, 2018, from the World Wide Web: https://www.draytek.com/en/about/news/2018/notification-of-urgent-security-updates-to-draytek-routers

[14] Talos. (2018, May 23). “New VPNFilter malware targets at least 500K networking devices worldwide”, Retrieved June 7, 2018, from the World Wide Web: https://blog.talosintelligence.com/2018/05/VPNFilter.html

[15] Kaspersky Lab. (2018, April 12). “APT Trends report Q1 2018”, Retrieved June 7, 2018, from the World Wide Web: https://securelist.com/apt-trends-report-q1-2018/85280/

[16] 行政院國家資通安全會報技術服務中心. (2018, June 7). “14 萬韓製路由器與行動裝置遭少爺駭客掌控”, Retrieved June 7, 2018, from the World Wide Web: https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=en&RSSType=news&seq=16110

[17] AbuseIPDB. “IP Abuse Reports for 38.134.121.95”, Retrieved June 7, 2018, from the World Wide Web: https://www.abuseipdb.com/check/38.134.121.95

[18] Talos. (2018, June 6). “VPNFilter Update - VPNFilter exploits endpoints, targets new devices”, Retrieved June 7, 2018, from the World Wide Web: https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

[19] The New York Times. (2018, May 27). “F.B.I.’s Urgent Request: Reboot Your Router to Stop Russia-Linked Malware”, Retrieved June 7, 2018, from the World Wide Web: https://www.nytimes.com/2018/05/27/technology/router-fbi-reboot-malware.html

[20] Starbucks. (2018, January 24). “網路及 Line 謠傳活動澄清公告”, Retrieved June 7, 2018, from the World Wide Web: https://www.starbucks.com.tw/stores/allevent/show.jspx?n=1016

[21] TrendMicro. (2018, June 26). “臭跩貓免費貼圖假訊息,2 萬多人上當（內含最新 LINE 詐騙列表:假官網真詐騙 免費貼圖 裝熟詐騙 網路釣魚）”, Retrieved July 13, 2018, from the World Wide Web: https://blog.trendmicro.com.tw/?p=55845

[22] Calyptix. (2018, August 17). “Social Media Threats: Facebook Malware, Twitter Phishing, and More”, Retrieved June 7, 2018, from the World Wide Web: https://www.calyptix.com/top-threats/social-media-threats-facebook-malware-twitter-phishing/

[23] LINE. (2017, October 9). “LINE@方案與帳號種類大解析”, Retrieved June 7, 2018, from the World Wide Web: http://at-blog.line.me/tw/archives/42220884.html

[24] LINE. (2018, May 27). “破解假帳號詐騙四大特徵！”, Retrieved July 7, 2018, from the World Wide Web: http://at-blog.line.me/tw/archives/75713444.html

[25] TrendMicro. (2018, March 15). “FinTech 浪潮盛行 區塊鏈應用成駭客眼中新寶”, Retrieved July 17, 2018, from the World Wide Web: http://www.trendmicro.tw/tw/about-us/newsroom/releases/articles/20180320034209.html

[26] Ministry of Health, Singapore. (2018, July 20). “SingHealth's IT System Target of Cyberattack”, Retrieved August 16, 2018, from the World Wide Web: https://www.moh.gov.sg/content/moh_web/home/pressRoom/pressRoomItemRelease/2018/singhealth-s-it-system-target-of-cyberattack.html
[27] Ministry of Communications and Information, Singapore. (2018, August 6). “Statement by Mr S Iswaran, Minister-in-Charge of Cybersecurity, on the cyber-attack on SingHealth’s IT system, during Parliamentary Sitting, 6 August 2018”, Retrieved August 14, 2018, from the World Wide Web: https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/8/statement-by-mr-s-iswaran-on--cyber-attack-on-singhealth-it-system-during-parl-sitting-on-6-aug-2018
[28] StraitsTimes. (2018, July 20). “SingHealth cyber attack: How it unfolded”, Retrieved August 16, 2018, from the World Wide Web: https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html?utm_campaign=Echobox&utm_medium=Social&utm_source=Facebook&xtor=CS1-10#Echobox=1532093927
[29] SingCERT. (2018, July 20). “Technical Advisory on Measures For Protecting Customers’ Personal Data”, Retrieved August 9, 2018, from the World Wide Web: https://www.csa.gov.sg/singcert/news/advisories-alerts/measures-for-protecting-customers-personal-data
[30] NetAdmin, “已知漏洞才是遭駭大宗　資安莫再捨薪輿而逐秋毫”, Retrieved Jan. 15, 2018 from the World Wide Web: http://www.netadmin.com.tw/article_content.aspx?sn=1801030010
[31] iThome, Jan. 11, 2018, “你的 Windows 更新了嗎？當心防毒軟體和修補程式不相容導致無法更新”, Retrieved Jan. 15, 2018 from the World Wide Web: https://www.ithome.com.tw/news/120464
[32] Microsoft, May 14, 2017, “為協助抵禦大規模惡意勒索病毒的侵襲，請用戶立即安裝微軟於三月釋出的安全性更新 MS17-010”, Retrieved Jan. 15, 2018 from the World Wide Web: https://news.microsoft.com/zh-tw/windowsdefender/#sm.0000535813159xdpuvym8a1p5ik3g
[33] 許登傑, “淺談安全軟體發展”, Retrieved Jan. 15, 2018 from the World Wide Web: http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=2115
[34] MITRE Cooperation. (2018, January 1). “Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA) Rules Version 2.0”, Retrieved May 7, 2018, from the World Wide Web: https://cve.mitre.org/cve/cna/CNA_Rules_v2.0.pdf
[35] MITRE Cooperation. (2018, April 27). “Request CVE IDs”, Retrieved May 7, 2018, from the World Wide Web: https://cve.mitre.org/cve/request_id.html
[36] Synology Inc. “對資訊安全的持續承諾”, Retrieved May 7, 2018, from the World Wide Web: https://www.synology.com/zh-tw/company/news/article/CNA_join/%E5%B0%8D%E8%B3%87%E8%A8%8A%E5%AE%89%E5%85%A8%E7%9A%84%E6%8C%81%E7%BA%8C%E6%89%BF%E8%AB%BE
[37] QNAP Systems, Inc. (2017, August 31). “QNAP 獲得授權參與 CNA 計畫，保護資安不遺餘力”, Retrieved May 7, 2018, from the World Wide Web: https://www.qnap.com/zh-tw/news/2017/qnap-%E7%8D%B2%E5%BE%97%E6%8E%88%E6%AC%8A%E5%8F%83%E8%88%87-cna-%E8%A8%88%E7%95%AB-%E4%BF%9D%E8%AD%B7%E8%B3%87%E5%AE%89%E4%B8%8D%E9%81%BA%E9%A4%98%E5%8A%9B

[38] Asustor Inc. “New CNA - Asustor”, Retrieved May 7, 2018, from the World Wide Web: https://cve.mitre.org/data/board/archives/2017-10/msg00026.html

[39] APCERT. “About APCERT”, Retrieved September 20, 2018, from the World Wide Web: http://www.apcert.org/about/index.html

[40] APCERT. “Background”, Retrieved September 20, 2018, from the World Wide Web: http://www.apcert.org/about/background/index.html

[41] APCERT. “APCERT Annual Report 2017”, Retrieved September 20, 2018, from the World Wide Web: https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2017.pdf

[42] JPCERT/CC. “TSUBAME (Internet threat monitoring system)”, Retrieved September 16, 2018, from the World Wide Web: https://www.jpcert.or.jp/english/tsubame/

[43] APCERT. “APCERT Drill 2018- Data Breach via Malware on IoT”, Retrieved September 27, 2018, from the World Wide Web: https://www.apcert.org/documents/pdf/APCERTDrill2018PressRelease.pdf

[44] NIST. (2018, August 6). “Computer Security Incident Handling Guide”, Retrieved September 14, 2018, from the World Wide Web: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

2018 資安年刊

發　行　者：TWCERT/CC 台灣電腦網路危機處理暨協調中心

總　編　輯：陳永佳

副 總 編 輯：吳專吉

編 撰 小 組：羅文翎、沈紀威、王蓮淨、藍秉華、黃暖婷、蕭亦筑、李幸秋

地　　址：台北市大安區和平東路三段 170 號

電　　話：0800-885-066

E - M a i l：twcert@cert.org.tw

官　　網：https://twcert.org.tw

FB 粉絲專頁：https://www.facebook.com/twcertcc/

發 布 日 期：中華民國 107 年 12 月 25 日

台灣電腦網路危機處理暨協調中心

Taiwan Computer Emergency Response Team/Coordination Center