

twcertcc

2019
資通安全年報



twcertcc

目錄 Table of Contents

第一章、前言 07

第二章、資安威脅趨勢 13

第一節、網路威脅趨勢與防護 14

一、DNS 資安威脅與防護機制 14

二、邊界閘道通訊協定威脅與防範 27

三、網路釣魚樣態與協處機制 32

第二節、IOT 設備與行動應用安全 40

一、物聯網資安威脅與資安檢測 40

二、行動應用 APP 資安威脅與防護 46

第三章、情資分享與漏洞協處 57

第一節、TWCERT/CC 資安情資分享 58

第二節、VIRUS CHECK 惡意檔案分析 61

第三節、資安漏洞協處 64

一、我國產品漏洞概況 64

二、跨域漏洞協處 67

三、資安漏洞協處案例 69

第四章、合作交流與資安推廣 75
第一節、主辦活動 76
一、台灣資安通報應變年會 76
二、台灣 CERT/CSIRT 聯盟交流會議 79
第二節、國際交流 80
一、參與 FIRST 年會 80
二、參與 APCERT 年會 81
三、參與亞太區國際網路安全攻防演練 82
四、參與 APNIC 48 年會 83
第三節、國內交流 84
一、亞太資安論壇 84
二、2019 Cyberspace 聯合研討會 85
三、2019 HITCON Defense Summit 企業安全會議 86
四、iThome CYBERSEC101 資安實務研討會 86

第五章、結語 89

圖目次

圖 2-1 DNS 劫持攻擊示意圖 15
圖 2-2 DNS 快取中毒攻擊 17
圖 2-3 DNS 惡意程式運作比較 18
圖 2-4 分散式反射拒絕服務示意圖 20
圖 2-5 DNS 通道穿越比較示意圖 22
圖 2-6 BGP 劫持 / 錯誤宣告示意圖 28
圖 2-7 全球 IPV4 RPKI 統計圖 (以路由數量計) 31
圖 2-8 國內 IPV4 RPKI 統計圖 (以路由數量計) 31
圖 2-9 網路釣魚示意圖 32
圖 2-10 TWCERT/CC 通報國外網路釣魚處置統計 38
圖 2-11 MIRAI 病毒運作示意圖 41
圖 2-12 QBOT 惡意程式運作示意圖 42
圖 2-13 XORDDOS 惡意程式運作示意圖 43
圖 2-14 廣告惡意 APP 示意圖 49
圖 2-15 網路釣魚 APP 示意圖 50
圖 3-1 TWCERT/CC 資安跨域聯防與情資分享 59
圖 3-2 TWCERT/CC 國際資安情資分享比例 60
圖 3-3 TWCERT/CC 通報事件類型比例 60
圖 3-4 惡意檔案檢測服務 VIRUS CHECK 61
圖 3-5 VIRUS CHECK 檔案檢測風險值比例 62

圖 3-6 CVE 漏洞嚴重等級統計 66
圖 4-1 2019 台灣資安通報應變年會 - 貴賓合影 76
圖 4-2 活動與會者行業別分析 77
圖 4-3 與會者回饋問卷統計分析 77
圖 4-4 AUSCERT 與 TWCERT 交換合作備忘錄 78
圖 4-5 林志鴻博士於 FIRST 年會報告概況 80
圖 4-6 APCERT CONFERENCE 2019 全體合照 81
圖 4-7 丁綺萍副執行長於 WORKING GROUP 交流概況 81
圖 4-8 黃勝雄董事長主持 IPV6 DEPLOYMENT 場次 83
圖 4-9 丁綺萍副執行長主持之 COOPERATION SIG 場次 83
圖 4-10 林志鴻博士於亞太資安論壇報告概況 84
圖 4-11 CYBERSPACE 2019 聯合研討會開幕 86
圖 4-12 WORKSHOP 實務分享現場 86
圖 4-13 林志鴻博士於 HITCON DEFENSE SUMMIT 演講概況 86

表目次

表 2-1 惡意 APP 類型比例 48
表 3-1 TWCERT/CC 審核發布 CVE 統計表 64

twcertcc

2019 台灣電腦網路危機處理暨協調中心資安年報

第一章

前言

TWCERT/CC 為我國企業資安事件通報及協處窗口，透過網路威脅趨勢之研析探討、資安情資分享與漏洞協處、資安活動參與之合作交流與資安推廣等服務，厚植企業資安認知，並且擔任對國外之聯繫窗口，促進國際資安交流合作，共同維護台灣網路安全。

台灣電腦網路危機處理暨協調中心 (Taiwan Computer Emergency Response Team/Coordination Center, TWCERT/CC) 負責推動資訊發展與資安趨勢探討、資安情資分享服務、事件通報協處、國內外資安交流合作以及深化資通安全意識，提供國家整體資安聯防能量，共同維護台灣整體網路安全。

針對近期資訊發展與資安趨勢，網路攻擊方式及類型難以計數，然而許多機制、設備或系統，在近期逐漸成為主要攻擊目標。網路攻擊中，由於網域名稱系統 (Domain Name System, DNS) 的運作是網路運作所必需，許多系統不會防範 DNS 封包，對應的監控及防禦機制也少，導致 DNS 成為攻擊者的首要目標，因此為減少其資安威脅，應進行相關防護作業與 DNSSEC (Domain Name System Security Extensions) 防護機制，加強 DNS 系統的資安防護。

其次，由於網際網路是以路由作為基礎運行，而許多路由都倚賴邊界閘道通訊協定 (Border Gateway Protocol, BGP)，一旦當 BGP 受到威脅，所產生的影響將會相當嚴重，在近年，路由事件有逐漸上升之趨勢，應透過其安全管理功能以及資源公鑰基礎建設 (Resource Public Key Infrastructure, RPKI) 確保 BGP 的安全性，根據台灣網路資訊中心 (Taiwan Network Information Center, TWNIC) 統計，台灣 IPv4 於 2019 年 12 月之 RPKI 通過驗證比例為 74.28%，高於全球。

再者，近年資訊系統於系統面的防護越來越牢靠，然而人性的弱點依舊存在，導致「人」成為在資訊系統的環節中，最為薄弱的一環，也是最受攻擊者歡迎的目標之一，因此針對透過各種形式吸引使用者受騙後獲取不正當利益之網路釣魚 (Phishing) 攻擊，使用者除了應隨時提防可疑訊息外，更可透過反釣魚系統加強防護，如若收到相關訊息，可透過 TWCERT/CC、國際釣魚工作小組 (Anti-Phishing Working Group, APWG) 以及 165 全民防騙網提供相關資訊，從源頭遏

止網路釣魚的發生。

此外，隨著便利性及需求的增加，物聯網(Internet of Things, IoT)逐漸成為生活中的一部分，然而這些過於貼近生活且新興的設備及機制，變成竊取個人隱私和資訊之攻擊者的首選，在物聯網的資安威脅中，許多知名惡意程式透過感染其裝置獲取不法利益，因此應從物聯網設備、通訊及雲端三個體系進行防護，並對產品進行安全性驗證，提升其資安水準以及大眾的信任。而針對行動應用 APP，行動裝置的普及已經逐漸成為人人必備的工具，卻也逐漸成為攻擊者侵入使用者裝置的一大破口，這些惡意的行動應用 APP 主要會產生惡意廣告、網路釣魚、殭屍網路、間諜軟體及下載器等惡意行為，因此，除了使用者應注意並進行相關防護作業外，行動應用 APP 的開發者亦需針對其產品進行檢測，以提升整體行動應用 APP 的資訊安全。

在 2019 年間，TWCERT/CC 持續進行國內外資安情資分享，其情資來源主要包含國際資安組織、國內資安組織，以及各國 CERT 組織。因此在接獲情資後，會依據其地域性分享至境內或境外，境內主要分享對象包括政府單位、網路業者、金融單位、學術單位、其他資安相關組織及國內企業等，而境外分享對象主要為 117 國的 CERT(Computer Emergency Response Team) 與 CSIRT(Computer Security Incident Response Team) 及相關資安組織。此外，亦針對惡意檔案檢測服務 Virus Check 進行系統優化作業，提供以使用者導向為考量之使用平台，並於 2019 年 7 月中旬上線開放予大眾使用，降低惡意檔案對使用者所產生的資安風險。

針對資安事件通報協處，TWCERT/CC 提供資安事件通報之管道，如服務專線、專屬電子郵件信箱及官方網站等通報服務管道，其中，官方網站通報部分，為提升通報及分析效率，依據

事件資訊、內容，分為一般通報和簡易通報，讓民眾可以依據通報資安事件的類型及內容選擇適當的通報模式。除資安事件之外，針對資訊產品漏洞，在 2019 年期間，共計發布國內 27 個通用漏洞揭露 (Common Vulnerabilities and Exposures, CVE) 計畫產品漏洞編號，其產品範圍涵括網通產品、軟體服務系統及物聯網裝置等類型，並且協調相關廠商對其產品進行軟韌體之更新及修補，以提升國內資通訊產品安全性。

為增進資安情資之分享以及資安意識之提升，TWCERT/CC 定期主辦與協辦資安相關活動與會議，並且參與國內外資安交流活動，分享國內外相關資安事件。在 2019 年，主辦 2019 台灣資安通報應變年會，並舉辦「台灣 CERT/CSIRT 聯盟」聯盟會議，除邀請專家進行資安相關專題演講外，亦邀請企業會員單位進行資安案例分享，互通企業間的資安能量，形成良性的交流管道。同時亦協辦國內資安相關活動，分享國內外相關資安事件處理案例及經驗。在國際活動部分，TWCERT/CC 參與多場國際活動以及 APCERT Drill 資安通報演練，並於 FIRST (Forum of Incident Response and Security Teams) 2019 年會等國際資安會議上進行資安議題資訊之發表，向國際 CERT/ CSIRT 專業人員分享成果。

在深化資通安全意識方面，2019 年間定期寄送資安電子報，其項目包含國內外資安新聞、駭侵事件、漏洞資訊、資安研討會 / 活動 / 競賽資訊，提供對資安有興趣之讀者相關資訊。並且在資安資訊宣導部分，TWCERT/CC 持續經營 TWCERT/CC 官網、Facebook、Instagram 和 Twitter 等官方粉絲團。

TWCERT/CC 盼透過資安趨勢研析、情資分享、通報協處以及資安推廣與意識提升，加強國內資安防護及協處之能量，提升整體資安防護能量，提供安全、舒適的網際網路環境給所有使用者。

twcertcc

2019 台灣電腦網路危機處理暨協調中心資安年報

第二章

資安威脅趨勢

為增進大眾對資安議題之了解和關注，TWCERT/CC 配合資安趨勢、資安政策、資安事件與重大駭侵事件等議題，彙整研析相關資安資訊，提供相關資安威脅與防護資訊，強化大眾資安意識，提升資安敏銳度。

第一節、網路威脅趨勢與防護

一、DNS 資安威脅與防護機制

1. 簡介

網域名稱系統(DNS)，是將網址(Uniform Resource Locator, URL)轉換為IP(Internet Protocol)，提供電腦判讀並連線之系統。由於電腦或伺服器本身都是以數字判讀連線位址並通訊，亦即透過每個端點之 IP 位址方能順利與目的端點進行連線。然而，使用者難以記憶如 IP 位址的冗長數字以進行網路連線行為，因此，包含特定文數字的易讀網址就成了方便使用者連線至目標位址時的極佳工具。而將使用者輸入之網址轉換成電腦 / 伺服器可判讀之 IP、令其能夠順利與目標主機進行連線之網路服務，即為網域名稱系統[1]。

2. DNS 資安威脅

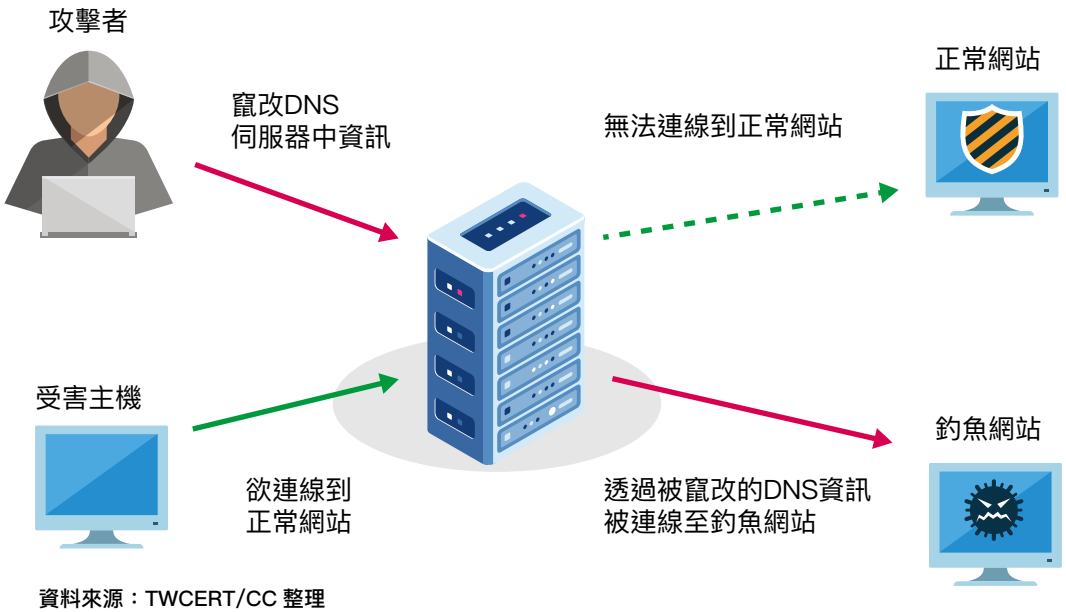
在網路攻擊中，由於 DNS 的運作是長時間不間斷，並且為網路運作所必需的設備及機制，許多企業均不會針對 DNS 封包進行防範，對應的監控及防禦機制也較其他設備及機制更少，因此 DNS 往往是諸多攻擊者的首要目標。在近三年中，受到 DNS 攻擊之企業，其受到每件攻擊之總損失金額逐漸增長，其原因主要是緣於駭客在近年針對 DNS 的攻擊，已不再是往常之暴力攻擊，而是入侵組織內部，進行更為複雜的攻擊，導致受害公司所受害的程度及為了恢復運行而耗費之資源和成本逐年增長。為了避免並減少因 DNS 受攻擊而造成之損失，促使相關組織或企業採取相關因應措施。

針對 DNS 服務的攻擊或利用 DNS 進行攻擊的常見模式，有以下幾種：

(1) **DNS 劫持攻擊（DNS Hijack Attack）**：此攻擊又稱為 DNS 重定向（DNS Redirection）攻擊，主要為駭客入侵或竄改使用者主機所詢問之 DNS 伺服器，導致使用者主機從受害 DNS 伺服器中接收到錯誤的相關資訊，與釣魚網站連線，遭到網路釣魚攻擊[2]。

如圖 2-1 所示，此種攻擊手法主要是藉由主機信任 DNS 伺服器所查詢並回覆的目標網站位址，並以此位址進行連線之作業過程，攻擊者便利用此機制，駭入 DNS 伺服器中，修改其中網站網址所對應的位址，導致使用者收到的位址是攻擊者竄改後的惡意釣魚網站位址。而在收到 DNS 回覆之後，使用者主機會信任其回

圖 2-1 DNS 劫持攻擊示意圖



資料來源：TWCERT/CC 整理

1 TWNIC. “DNS(上)”：https://blog.twnic.net.tw/2019/03/12/2880/（瀏覽日期：2019年10月2日）
2 CactusVPN. “What Is DNS Hijacking? (Your Guide to How to Stop DNS Hijacking)”. Retrieved October 2, 2019, from the World Wide Web: https://www.cactusvpn.com/beginners-guide-online-security/dns-hijacking/

覆資訊，並依據該位址連入釣魚網站中，導致產生個資竊取或感染惡意程式等資安問題。

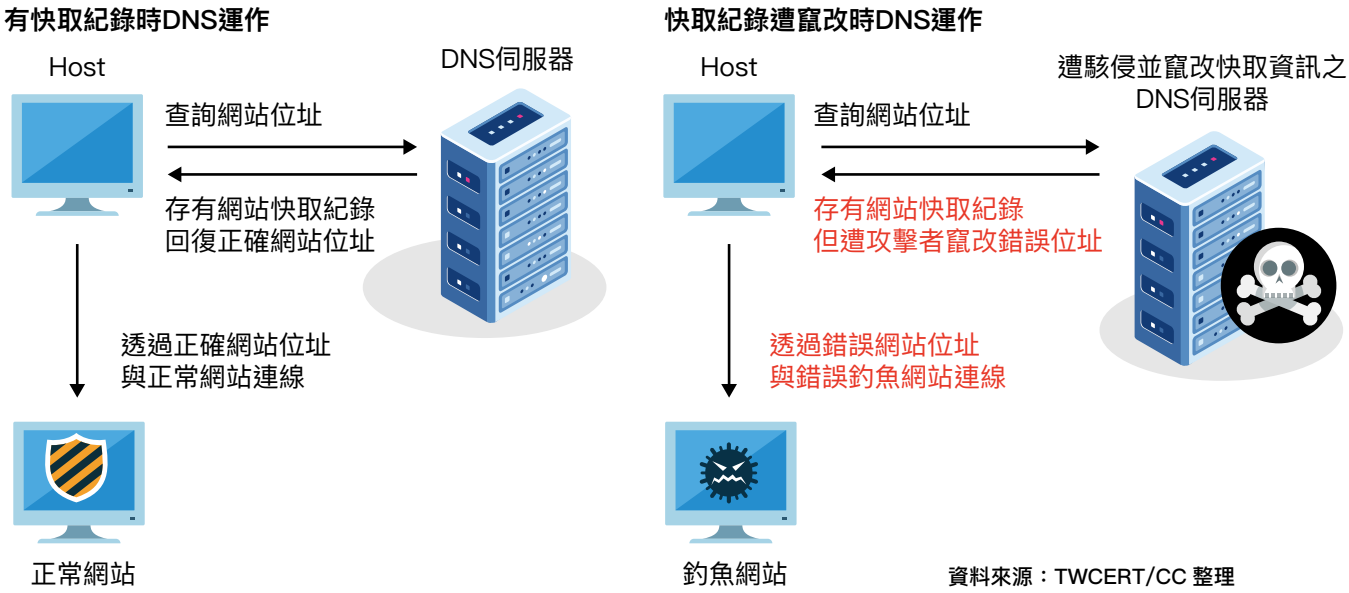
2017 年 1 月到 2019 年第一季間，曾發生針對 13 個國家逾 40 個組織之 DNS 劫持攻擊。該攻擊被稱為「海龜行動 (Sea Turtle)」，藉由劫持 DNS，並將其 DNS 資訊進行竄改，將流量引導至駭客掌控之伺服器，進而騙取受害者的相關資訊及憑證。

(2) **DNS 快取中毒 (DNS Cache Poisoning)**：又稱為 DNS 欺騙 (DNS Spoofing)，主要是針對快取訊息的攻擊手法。攻擊者可以透過各種方式入侵或傳播惡意程式，進入系統竄改快取資訊，將其中的快取目標改為惡意網站，因此若使用者欲連線至快取資訊所紀錄之網站，將會因為信任快取資訊，而被導至惡意網站[3]。

如圖 2-2 所示，DNS 運作為 DNS 伺服器收到請求封包後，會檢查自身是否曾查詢過該網站並存有該網站網址的快取紀錄，如若該 DNS 伺服器存有該網站的快取紀錄，則會直接以快取中的資訊回傳給使用者，讓使用者得以連入目標網站。但攻擊者便可利用此機制，透過駭入 DNS 伺服器，竄改其中快取紀錄中的資訊，將其快取資訊所對應的網站與網址改為攻擊者所控制的釣魚網站。如此，導致 DNS 伺服器確認其快取紀錄，並以該紀錄回傳給使用者時，其所提供的資訊為錯誤的網站位址，使用者主機信任並連入該位址後，將會被導入惡意釣魚網站中，成為網路釣魚的受害者。

在 2018 年 4 月下旬，以太坊錢包 MyEtherWallet 遭到 DNS 快取中毒攻擊，其於知名公共 DNS 服務中的網址 myetherwallet.com 被遭到竄改，其對應的 IP 位址被設定為會竊取 MyEtherWallet 金鑰的惡意伺服器 IP。當使用者被導入該惡意伺服

圖 2–2 DNS 快取中毒攻擊



資料來源：TWCERT/CC 整理

器時，該伺服器會藉此取得使用者的錢包金鑰，並將其錢包中的金流導入攻擊者的多個私人錢包位址中。在攻擊開始後的短短三個小時內，其私人錢包便已接收共 179 筆交易，總計 216.06 個以太幣，在當時換算約莫 152,000 美元[4]。

（3） **DNS 惡意程式**：此種攻擊手法，主要是針對使用中的主機，駭客透過各種管道如社交工程等方式，散布惡意程式。當受害主機感染惡意程式後，其會在未經使用者授權之情況下修改主機 DNS 設定，將使用者導入駭客設立之惡意網站，以賺取不法利益[5]。

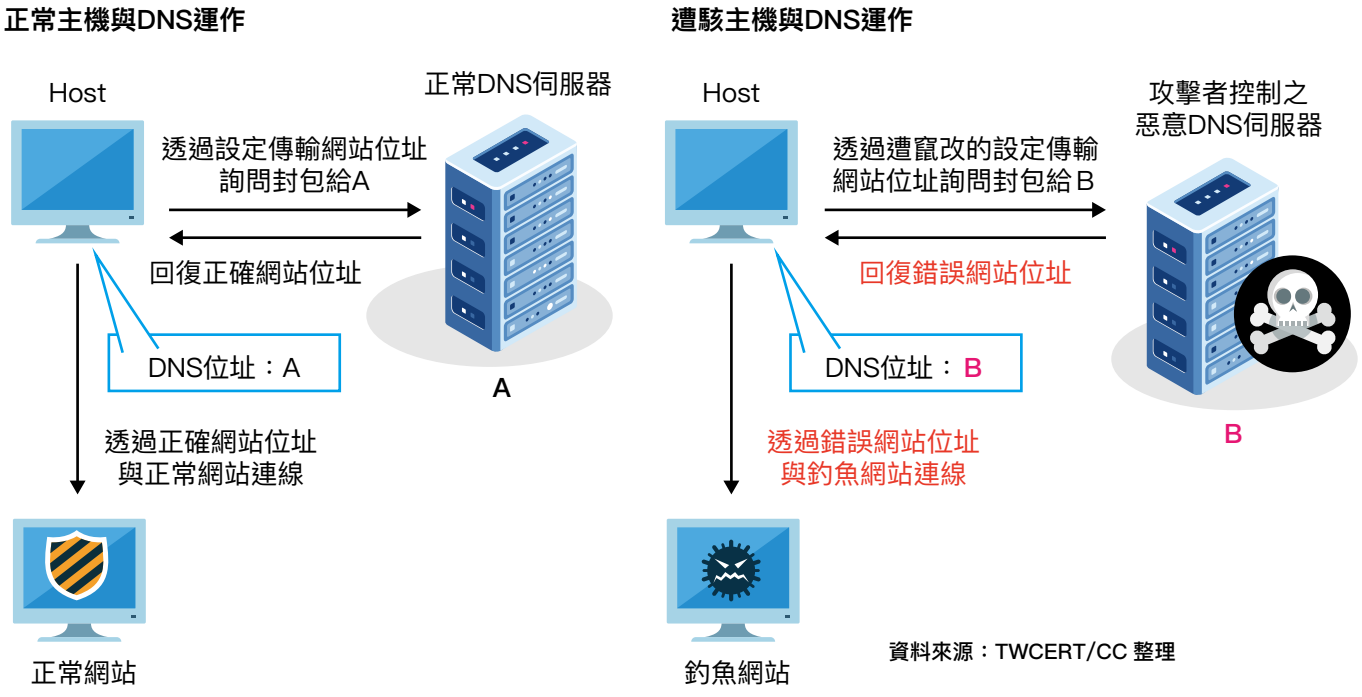
3 CloudFlare. “What is DNS cache poisoning? DNS spoofing”. Retrieved October 3, 2019, from the World Wide Web: https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

4 CoinDesk. “$150K Stolen From MyEtherWallet Users in DNS Server Hijacking”. Retrieved October 9, 2019, from the World Wide Web: https://www.coindesk.com/150k-stolen-myetherwallet-users-dns-server-hijacking

如圖 2-3 所示，當主機在進行網路連線時，都會設定其所欲使用的 DNS 伺服器及其位址，包括公共的 DNS 服務及 ISP 業者所提供的 DNS 伺服器，並且會依此設定傳輸 DNS 查詢請求給指定的伺服器，然後再依據其回覆進行連線作業。然而，攻擊者便可透過此機制，以多種管道，如釣魚郵件、惡意檔案下載等方式，讓主機感染惡意程式並受到攻擊者控制後，竄改主機系統所設定之 DNS 伺服器位址，改為攻擊者可控的惡意 DNS 伺服器，而不知情的使用者在進行 DNS 查詢後，該惡意伺服器會回覆惡意釣魚網站之位址，而非正確的網站位址，讓使用者因此連入釣魚網站中而蒙受損失。

在 2019 年 7 月，一款名為 Extenbro 的新興 DNS 變更木馬惡意程式被發現。

圖 2-3 DNS 惡意程式運作比較



資料來源：TWCERT/CC 整理

此款惡意程式在感染受害主機後，會替該主機額外添加數個惡意 DNS 伺服器，除了會竊取流經該惡意 DNS 伺服器的封包資訊，以及將受害者導入釣魚網站外，Extenbro 甚至會阻止受害主機與任何安全性或防護系統的網站進行連線，避免使用者下載可對付該惡意程式的防護軟體。甚至，該惡意程式會關閉受害主機的 IPv6 連線，強制使用惡意 DNS 伺服器，進而成功進行網路釣魚及資料竊取等惡意行為[6]。

(4) **DNS 洪水攻擊 (DNS Flooding Attack)**：此種攻擊主要是針對 DNS 服務的分散式阻斷服務攻擊 (Distributed Denial-of-service Attack, DDoS)，駭客透過大量的殭屍網路，向 DNS 伺服器提出大量網域解析要求，導致 DNS 伺服器無法負荷過量的解析要求，中斷 DNS 伺服器的服務[7]。

在 2016 年 10 月，美國某網路服務供應商的 DNS 服務，遭 Mirai 殭屍網路進行大量的 DNS 洪水攻擊。依據專家估計，此次攻擊之流量應有達到 1.2 Tbps。如此巨量的數據湧入其 DNS 伺服器，導致了北美網路 DNS 服務的中斷，使用者無法連接如 Twitter、CNN、eBay、App Store、PayPal 等大型知名網站[8]。

(5) **分散式反射拒絕服務 (Distributed Reflection Denail-of-service, DRDoS)**：此種攻擊主要目標並非 DNS 本身，而是透過 DNS 服務對目標受害者進行攻擊之手法。攻擊者會偽冒受害者的 IP 位址，對 DNS 伺服器進行解析請求。而這些 DNS 服務回覆

5 資安趨勢部落格. “讓57萬台電腦遇駭的駭客集團ROVE DIGITAL (DNS Changer開發者) 近10年的起落”：https://blog.trendmicro.com.tw/?p=1919（瀏覽日期：2019年10月2日）

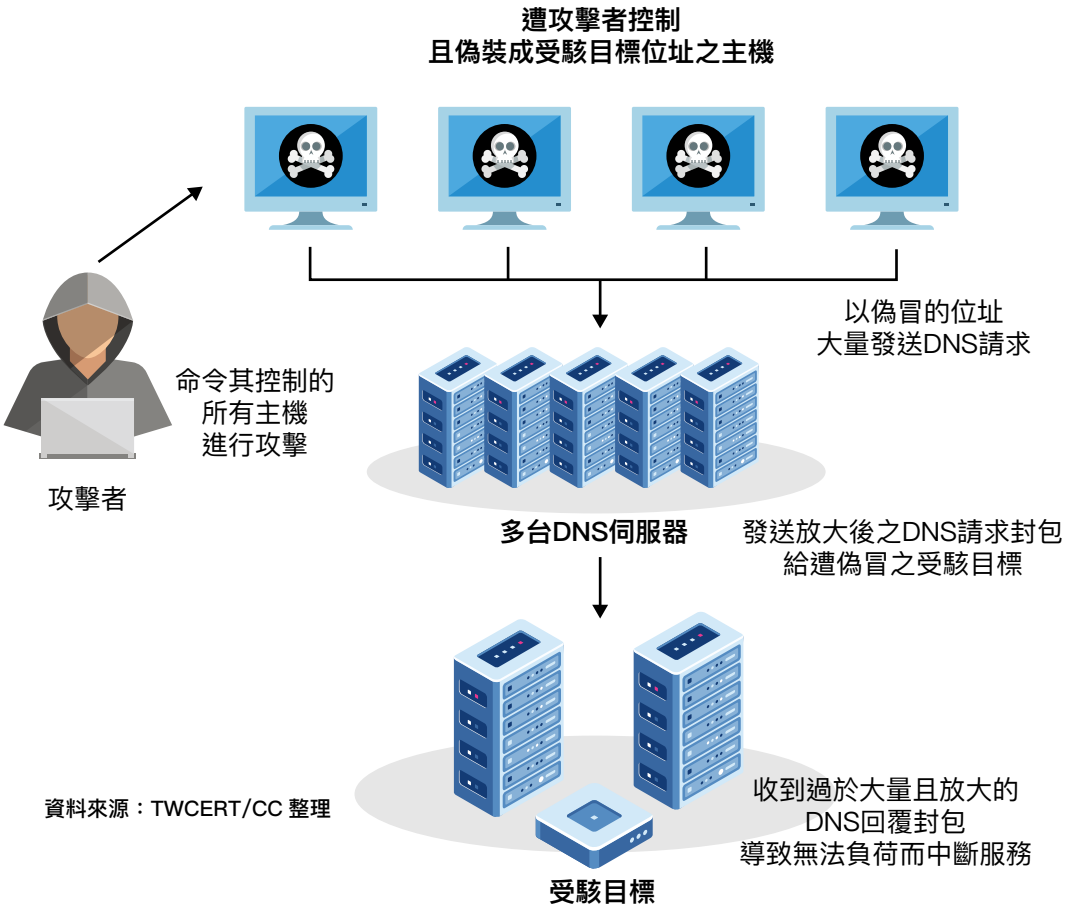
6 Malwarebytes Labs. “Meet Extenbro, a new DNS-changer Trojan protecting adware”. Retrieved October 3, 2020, from the World Wide Web: https://blog.malwarebytes.com/trojans/2019/07/extenbro-a-new-dns-changer-trojan-protecting-adware/

7 CloudFlare. “抵抗DDOS攻擊”： https://www.cloudflare.com/zh-tw/ddos/（瀏覽日期：2019年10月2日）

之封包大小會因攻擊者請求之類型而放大，並寄往受害主機，導致大量放大後之回覆封包被傳送給受害主機，使得受害主機因無法負荷大量訊息而中斷服務[9]。

如圖 2-4 所示，此種攻擊手法是透過某些特定類型之 DNS 請求，在回覆時因其中資訊的增加而導致回覆封包的大小較請求時的封包大。對一般的 DNS 請求而言，此機制導致的封包放大並不會影響主機的運作，但攻擊者卻可利用此機制，先透過多台受駭且受攻擊者控制的主機，將這些主機的位址偽裝成攻擊受駭目標所在位址，並對各大 DNS 伺服器發送大量且會放大類型之 DNS 查詢請求，而這些

圖 2–4 分散式反射拒絕服務示意圖



資料來源：TWCERT/CC 整理

DNS 伺服器在接收封包後，會將如此大量且放大的回覆封包傳送給遭偽冒的受駭目標。在此機制下，即便攻擊者控制發送攻擊的主機數量不多，但經過放大後，卻足以超過受駭目標的負荷量，導致其服務中斷。此外，由於受害目標所收到的封包來源為知名 DNS 服務業者的 IP，如 Google、IBM、CloudFlare，因此無法進行有效的阻擋，導致此種攻擊手法較難以防範。

國內一公共DNS服務，在2019年2月，遭駭客進行分散式反射拒絕服務攻擊，當日 DNS 查詢量超過 11 萬次 / 秒，並且其查詢量約為 70Mbps，但回覆之流量卻高達 130Mbps。根據其資訊，一般查詢與回應之比例約為 1:0.8，但該次攻擊時，其查詢與回應比例竟達 1:1.86。

管理者在發現流量的異常後，立即請相關單位於路由器封鎖其來源 IP，以排除該攻擊流量，順利將 11 萬次 / 秒之查詢量降至一半以下。然而，除了與相關單位溝通協助進行白名單及限速作業外，為了因應未來可能重複出現之類似攻擊，該單位提出增加伺服器及更換相關路由器之可能解決辦法，以預防愈發多元且針對性的攻擊手法。

(6) **DNS 通道穿越 (DNS Tunneling)**：此種手法主要是透過 DNS 本身屬於必要且基本的服務，因此很少會對 DNS 進行過濾之動作，使得駭客將通訊或傳輸等封包，包裝成 DNS 的封包進行傳輸，因此產生了一段隱蔽的通道，進行遠端控制或資料傳輸等作業 [10]。

8 CloudFlare. “Inside the infamous Mirai IoT Botnet: A Retrospective Analysis”. Retrieved October 9, 2019, from the World Wide Web: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/#toc-3

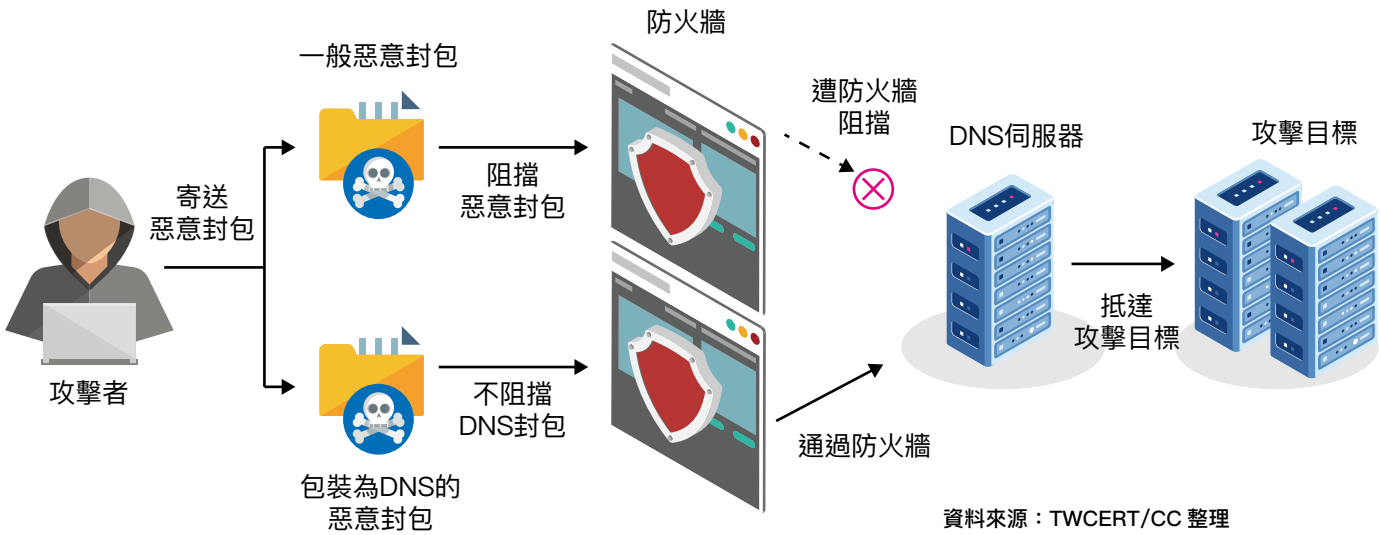
9 Arturai. “DRDOS Attacks”. Retrieved October 2, 2019, from the World Wide Web: https://www.arturai.com/en/support/faqs/drdos-attacks

10 TWNIC. “DNS安全防護探討”：https://blog.twnic.net.tw/2018/01/31/273/（瀏覽日期：2019年10月4日）

如圖 2-5 所示，由於許多企業或組織為防範受到惡意攻擊，均會建立足夠防護能量的防火牆，對惡意封包進行阻擋及攔截。然而，由於許多企業或組織有建立 DNS 伺服器於其中，並且 DNS 服務是進行網路行為時必須使用的協定，因此往往該防火牆不會阻擋 DNS 封包。而攻擊者便透過此機制，將惡意封包偽裝成 DNS 封包進行傳送，導致攻擊目標所建立之防火牆因辨認為 DNS 封包而不多加以阻擋，可順利通過防火牆，並在進入企業內部網路後，可透過其連接眾多伺服器的內部網路，從 DNS 伺服器傳播至攻擊目標的主機或伺服器中，順利進行惡意攻擊。

在 2019 年 4 月，伊朗駭客進階持續性威脅 (Advanced Persistent Threat, APT) 組織—OilRig，透過 DNS Tunneling 保護和控制對中繼站通訊的相關資訊。OilRig 被發現至少從 2016 年開始，便透過 DNS Tunneling 和其中繼站進行通訊，並透過木馬程式盜取資料。由於大部分的設備都允許使用 DNS，因此此 APT 組織利用

圖 2-5 DNS 通道穿越比較示意圖



資料來源：TWCERT/CC 整理

DNS 查詢特殊子網域，將其相關命令傳送至伺服器中，並且透過不同的子網域，傳送不同的數據進行資料的竊取。但由於駭客必須在中繼站和入侵工具之間傳送大量的 DNS 查詢，因此，若對網路流量進行監控，便可發現駭客的蹤跡，進而阻止惡意程式的盜竊行為 [11、12、13、14、15、16]。

3. DNS 系統防護

針對 DNS 的安全防護，除了相關防護設備之外，必須從 DNS 的系統本身進行基本的資安防護，其防護方法有下述幾種 [17]：

(1) **伺服器關閉不必要的 DNS 存取功能：**許多伺服器都預設開啟 DNS 服務，但對於一般不需要 DNS 的伺服器應關閉 DNS 服務，防火牆也應針對 DNS 進行控管，關閉不必要的 DNS 存取。

(2) **落實弱點漏洞修補、存取管控：**DNS 伺服器應即時更新版本，以達到其漏洞或弱點修補之動作，並且落實 DNS 伺服器的存取管控機制，例如正確的 DNS 遞迴查詢設定或 Administrator 權限設定等。

11 SecurityAffairs. “Analyzing OilRig’s malware that uses DNS Tunneling”. Retrieved October 9, 2019, from the World Wide Web: https://securityaffairs.co/wordpress/84125/apt/oilrig-dns-tunneling.html
12 CactusVPN. “What Is DNS Hijacking? (Your Guide to How to Stop DNS Hijacking)”. Retrieved October 2, 2019, from the World Wide Web: https://www.cactusvpn.com/beginners-guide-online-security/dns-hijacking/
13 CloudFlare. “What is DNS cache poisoning? DNS spoofing”. Retrieved October 3, 2019, from the World Wide Web: https://www.cloudflare.com/learning/dns/dns-cache-poisoning/
14 資安趨勢部落格. “讓57萬台電腦遇駭的駭客集團ROVE DIGITAL (DNS Changer開發者) 近10年的起落”：https://blog.trendmicro.com.tw/?p=1919（瀏覽日期：2019年10月2日）
15 CloudFlare. “抵抗DDOS攻擊”：https://www.cloudflare.com/zh-tw/ddos/（瀏覽日期：2019年10月2日）
16 Arturai. “DRDOS Attacks”. Retrieved October 2, 2019, from the World Wide Web: https://www.arturai.com/en/support/faqs/drdos-attacks

(3) **指向組織內部 DNS 伺服器：**若組織本身有架設 DNS 伺服器，則組織內部主機應指向該組織內部之 DNS 伺服器，以減少透過外部 DNS 伺服器造成的資安威脅。

(4) **落實 DNS 網路管理及 DNS Log 紀錄分析：**DNS 伺服器管理者，應做好其網路管理功能，以及 DNS Log 的記錄和分析，並將各類型的服務狀態、查詢或回應等進行分析，若有任何異常，應納入異常監測管理，可及早發現外部對 DNS 的異常行為。

(5) **採取適當 DNS 防護措施：**針對 DNS 伺服器，應採取適當的防護措施，例如採取黑 / 白名單等方式，進行其查詢行為之過濾等，方可提升 DNS 伺服器自身防護能量。

(6) **實施 DNSSEC：**為了強化 DNS 協定自身之弱點，實施 DNSSEC 可減少其如偽冒等資安風險。

(1)、DNSSEC 防護機制

網域名稱系統安全擴充 (Domain Name System Security Extensions, DNSSEC)，是用以解決 DNS 資訊遭駭客竄改的問題，透過數位簽章的簽署和驗證，可以知道該資訊是否遭到偽冒，以減少其資安風險。

此外，該機制也會透過 NSEC (Next Secure)，針對使用者收到之「該網址 / 網頁不存在」之訊息進行驗證，以避免駭客竄改資訊，導致使用者與某些特定網站無法進行連接。

除了數位簽章以及 NSEC 機制之外，DNSSEC 也使用了 EDNS (Extension Mechanisms for DNS) 技術。該技術主要是為了提升 DNS 安全性，將舊有的 DNS 封包中的格式，延伸出更多的區段，並將所需的特徵值放入其中，用以增加 DNS 資料傳輸的完整及安全性 [18]。其機制包括：

A. **數位簽章**：透過數位簽章，DNSSEC 可以確保使用者所收到的資訊都未經駭客竄改，是正確的 DNS 資訊。此機制主要是在 DNS 伺服器收到相關請求後，將回覆的訊息透過雜湊函式 (Hash Function) 進行運算，將其變成雜揍摘要 (Digest)，再將其摘要以及 DNS 訊息，以密鑰進行加密並回傳。使用者收到後，透過 DNS 伺服器的密鑰解密，取得其 DNS 訊息以及雜湊摘要，並將明文 DNS 訊息透過同樣的雜湊函式運算，若運算後所得到之雜湊摘要和所收到之雜湊摘要相同，則可證明該訊息未被竄改。

B. NSEC：透過 NSEC，可針對連網時「該網址／網站不存在」訊息之真偽進行驗證。此機制會將所有網頁之網址記錄於資料庫中，並將其依照網址的字母順序進行排序。因此當顯示網址不存在的訊息時，該機制便會比對該網址與資料庫中的網址，以及比對其前後資訊。例如 b.com 會被排序在 a.com 之後及 c.com 之前，當使用者查詢 b.com，卻收到不存在訊息時，該機制會查詢資料庫，在 a.com 和 c.com 之間是否有 b.com 的網址存在。若無，則代表該網址確實不存在 [19]。

C. EDNS：為因應越來越多之功能，並且維持過往 DNS 封包的形式，因此建立了 EDNS。此機制主要是將舊有的 DNS 封包，延伸出更多的區段，例如過往的封包大小，在加上了數位簽章的資訊後已不足以負荷，因此 EDNS 機制便可將其封包大小上限進行提升，可將 DNSSEC 所期望的特徵值和資料內容，完整地納入封包並進行傳輸。

18 TWNIC. “DNS(下)” ： https://blog.twnic.net.tw/2019/04/10/3216/（瀏覽日期：2019年10月13日）
19 APNIC Labs. “DNSSEC Validation Rate by country (%)”. Retrieved October 14, 2019, from the World Wide Web: https://stats.labs.apnic.net/dnssec

透過數位簽章、NSEC 以及 EDNS 的運作，DNS 服務可透過 DNSSEC 的建置，而達到三項的安全保證：

A. **資料完整性** (Data Integrity)：透過相關驗證，確保傳輸的 DNS 是真實的，並未遭到駭客竄改，以防止因經過修改的 DNS 封包，而導致使用者誤入惡意網站。

B. **來源可驗證性** (Origin Authentication of DNS Data)：確保該 DNS 回覆為真實的 DNS 伺服器所發送，而不是駭客偽冒 DNS 伺服器所發出的假訊息，以避免使用者因收到的偽冒回覆封包而蒙受損失。

C. **可驗證不存在性** (Authenticated Denial of Existence)：由於駭客可透過偽冒的訊息，讓主機取得「該網頁 / 網址不存在」的資訊，導致使用者無法順利與該網站進行連線。而 DNSSEC 可驗證該網址是否真的不存在，或是收到假冒的資訊。

DNSSEC 主要用以解決 DNS 劫持攻擊、DNS 快取中毒，以及 DNS 惡意程式中偽冒的 DNS 伺服器等攻擊手法，能透過上述機制，達到較佳的 DNS 資安防禦。但 DNSSEC 對於其他相關攻擊，例如洪水攻擊、通道穿越，以及分散式反射拒絕服務等，都較難以全面性的進行防禦，必須藉助相關單位或設備 / 系統的建置，方能針對其他攻擊模式進行防護。

此外，相關業者針對 DNSSEC，也提出幾許問題須待改善，主要為在建置了 DNSSEC 後，使用者進行網路連線時，其失敗率較未建置 DNSSEC 時高；其二，為了提高其安全性，DNSSEC 擴增了其封包之欄位，將其所需之相關特徵值都納入其中，但也導致封包大小的增加，使得建置 DNSSEC 後，消耗的頻寬因其封包大小的增加而上升；其三，便是由於 DNSSEC 未能完全防禦所有 DNS 相關攻擊手法，因此相關業者除了建置 DNSSEC 之外，同時也必須增加相關設備或系統之建置，

以達到最佳的 DNS 防禦效益，然而，如此也導致了企業成本的上升。

因此，若要令 DNSSEC 真正普及，除了提升 DNSSEC 對相關業者之吸引力外，同時必須解決或降低上述問題之影響，方能讓業者真正願意建置 DNSSEC，落實 DNSSEC 的高普及率。

二、邊界閘道通訊協定威脅與防範

1. BGP 概述

邊界閘道通訊協定 (BGP)，是一種網路路由協定 (Routing Protocol)，提供網際網路的自治系統網域內，彼此之間傳遞封包的最佳路徑，以達到在最佳資訊傳遞速度和品質。

BGP 協定主要是透過 Bellman-Ford 距離向量路由演算法，以計算每個自治域的連接設備 (BGP Speaker)，透過不斷更新路由資訊，學習並繪製出網路最佳路由的相關拓撲 [1、2、3]。

2. BGP 資安威脅

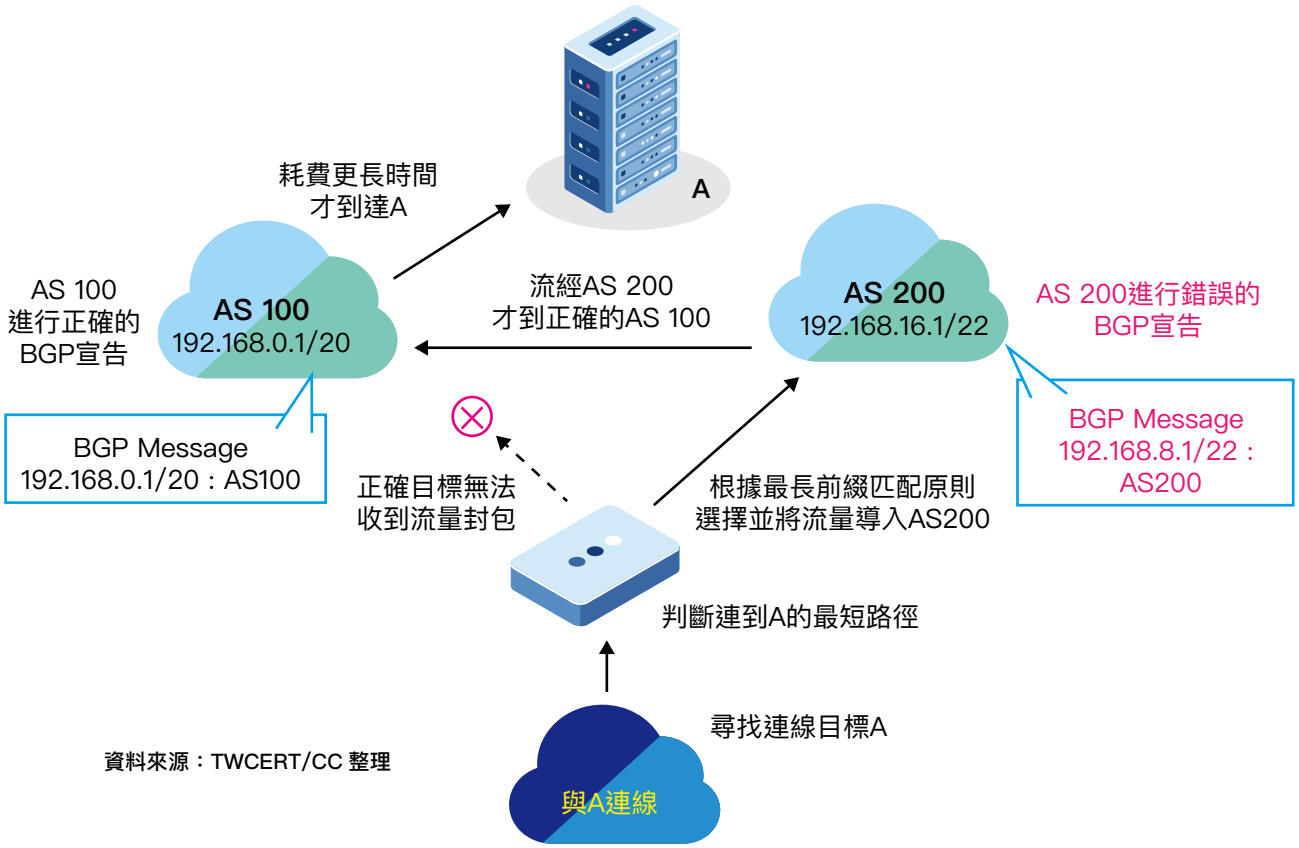
BGP 劫持是在 BGP 協定中，最為常見也最被廣泛討論的安全威脅。此種威脅模式主要是源因於一個錯誤的前綴資訊的宣告，也就是一個自治系統向外部區域宣告了應不屬於自身的前綴資訊，導致欲使用該 IP 位址區段的使用者因為其錯誤的宣告，而被引導至錯誤的目的地 [4]。

如圖 2-6 所示，每個自治系統 (Autonomous system, AS) 都會分配到專屬於自身的 IP 位址

1 NSRC. “BGP for All”. Retrieved July 30, 2019, from the World Wide Web: https://learn.nsrc.org/bgp
2 CLOUDFLARE. “What Is BGP? | BGP Routing Explained”. Retrieved July 30, 2019, from the World Wide Web: https://www.cloudflare.com/learning/security/glossary/what-is-bgp/
3 Wikipedia. “Border Gateway Protocol”. Retrieved July 30, 2019, from the World Wide Web: https://en.wikipedia.org/wiki/Border_Gateway_Protocol
4 黎松, 諸葛建偉, & 李星. (2013). BGP 安全研究. 軟件學報.

區段，然而，在圖中的 AS 200 卻錯誤宣告自身原本應為 192.168.16.1/22 的 IP 區段，宣告為 192.168.8.1/22，導致其區段與 AS 100 所屬之 192.168.0.1/20 有部分重疊。因此，當有使用者欲與目標伺服器 A 連線時，傳輸過程中的路由在判斷最短路徑時，卻因該機制為依據最長前綴匹配原則進行判斷，因此在兩者都匹配的狀態下，選擇前綴較長的 AS 200 為目標進行傳輸，而後方才在另一次的路由判斷中，將封包傳輸至真正最短路徑的 AS 100 中，再行傳輸至目標伺服器 A。如此，在這樣的傳輸中，由於路徑先經過 AS 200 才到 AS 100，將會導致傳輸時間拉長，傳輸效率低落，甚至當 AS 200 為惡意的攻擊者時，更可以監聽流經 AS 200 的所有封包，竊取其中的機敏資訊。

圖 2-6 BGP 劫持 / 錯誤宣告示意圖



資料來源：TWCERT/CC 整理

根據 MANRS (Mutually Agreed Norms for Routing Security) 的統計，在 2019 年中，路由的運作中斷事件總計 13,580 件，其中，共有 10,309 個自治系統產生了一次以上的路由事件。其中，平均每月約有 1131.67 次的路由事件，但於 2018 年的統計，顯示該年度僅 12,600 次路由事件，平均每月 1,050 次路由事件。與前一年相比，可以看到從 2018 到 2019 年中，路由事件的數量成長率為 7.78%，有逐漸增長的趨勢。

BGP 劫持事件發生頻繁，並且往往會因為微小的失誤而嚴重影響大量網路之服務品質，甚至導致服務中斷，若不幸為惡意之 BGP 劫持行為，更可能讓使用者在不知情的情形下蒙受損失，這些都是網路業者應極力避免產生或遭受影響之嚴重資安威脅。

3. BGP 資安威脅防禦機制

(1) BGP 安全管理功能

為增加 BGP 的安全性，以及減少意外造成之路由安全威脅和風險，有幾項針對 BGP 協定的設置可以減少因意外造成的路由問題：

A. 需限制最大路由數量 (Prefix-Limit)，限制接收的路由資訊之網段數量一此種限制對減少全表路由洩漏以及自身內存耗盡等問題富有助益，或限制自身宣告的網段數量，可以減少因配置錯誤等造成之路由問題之影響程度。

B.BGP 路由管理應注意並防護駭客偽造網段、欺騙他人來源 IP 位址之惡意行為，例如反欺騙 (Anti-Spoofing) 機制。

C. 除了驗證來源 IP 位址之外，應同時具備 BGP 宣告網段正確性之驗證，例如資源公鑰基礎建設 (Resource Public Key Infrastructure, RPKI) 機制。

(2) RPKI 防護機制

有鑑於 BGP 劫持事件以及路由錯誤設定的情形經常發生，網際網路工程任務組

(Internet Engineering Task Force, IETF) 訂定了一用以解決大部分路由相關安全問題的資源公鑰基礎建設 (RPKI) 標準。RPKI 標準主要適用於保護網際網路路由基礎建設，提供將網際網路號碼資源資訊連結到信任錨 (Trust Anchor) 的方法，也就是連接到一個可信的第三方並進行相關的驗證，以確保資訊的正確性 [5]。

為確保路由資訊的正確性，RPKI 允許單位發布路由來源授權 (Route Origin Authorization, ROA)，用以證明所收到的路由資訊中的 IP 位址和 ASN(AS Number) 是正確的組合。ROA 本身是一個經過加密簽章的物件，標明了 ASN 和 IP 地址及前綴資訊的對應關係，當一個自治系統發布了一個前綴資訊時，便可以透過 ROA 去驗證該自治系統是否有權利發布這個前綴資訊 [6]。

RPKI 標準可以透過認證網際網路資訊，以作為確保路由安全的一種模式。此標準允許區域網際網路註冊管理機構的成員可簽發 RPKI 資源憑證以及列出其持有的網際網路號碼資源，並存於 RPKI 資料庫中，而這些資源便可以提供驗證，作為安全性的有效證據。亦即當一路由接受到新的路由資訊宣告時，若該自治系統已經部署了 RPKI，便可以自 RPKI 資料庫中下載新路由資訊宣告的憑證以及 ROA 資訊，從而判斷此路由資訊宣告是否有效，減少路由錯誤以及防止大部分的 BGP 劫持 [7]。

根據美國國家標準暨技術研究院的統計數據，2019 年 12 月初，全球 IPv4 路由數量之 RPKI 統計，約有 17.80% 的路由申請 ROA 並通過驗證，約 82.20% 之路由數尚未申請 ROA、亦即並未施行 RPKI，如圖 2-7 所示 [8]：

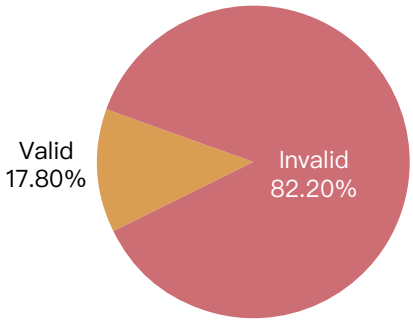
在台灣 RPKI 主要由國家通訊傳播委員會推動，其 RPKI 目前主要的憑證授權中心為台灣網路資訊中心 (TWNIC)，TWNIC 會向其會員，也就是其資源持有者發放憑證，並且持有者可以透過 TWNIC 的管理系統進行 RPKI 相關資源的增修以及

操作。

自台灣 RPKI 開始施行後，直到 2019 年 8 月中，以台灣 IPv4 路由數量統計，目前已有 91.3% 申請 ROA 並通過驗證，如圖 2-8 所示 [9]：

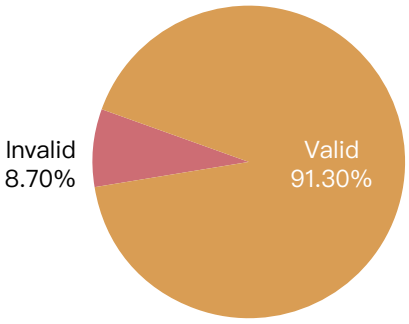
台灣的 RPKI 申請並通過驗證之比例，遠高於全球的 15.62%，可見台灣對路由安全有足夠之警覺性外，同時也願意為了增進自身之網路安全和品質，與國家通訊傳播委員會以及 TWNIC 攜手合作，減少 BGP 路由問題，強化台灣的網路安全體系。

圖 2-7 全球 IPv4 RPKI 統計圖（以路由數量計）



資料來源：[8]

圖 2-8 國內 IPv4 RPKI 統計圖（以路由數量計）



資料來源：[9]

5 財團法人台灣網路資訊中心. (2018年). “資源公鑰基礎建設(Resource Public Key Infrastructure，RPKI) 的介紹”：https://blog.twnic.net.tw/2018/04/30/824/ (瀏覽日期：2019年8月7日)

6 財團法人台灣網路資訊中心. (2018年). “路由來源授權(Route Origin Authorization，ROA)的介紹”：https://blog.twnic.net.tw/2018/05/30/928/ (瀏覽日期：2019年8月7日)

7 財團法人台灣網路資訊中心. (2018年). “資源公鑰基礎建設(RPKI)進行路由起源授權(ROA)於國際推行”：https://blog.twnic.net.tw/2018/03/29/710/ (瀏覽日期：2019年8月7日)

8 NIST. “Global Prefix/Origin Validation using RPKI”. Retrieved August 07, 2019, from the World Wide Web: https://rpki-monitor.antd.nist.gov/index.php?p=0&s=0

9 TWNIC. “ROUTING SECURITY AND RPKI 路由安全與資源公鑰基礎設施” ： https://opm.twnic.net.tw/33rd/presentation/2-3.pdf (瀏覽日期：2019年12月30日)

三、網路釣魚樣態與協處機制

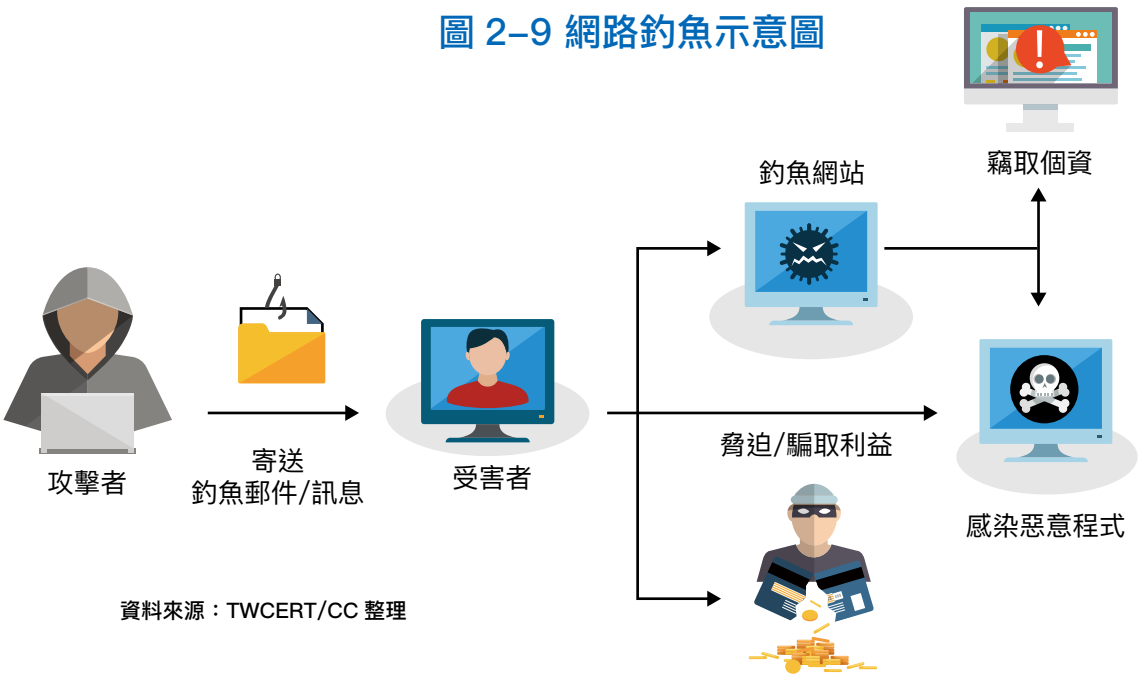
1. 簡介

網路釣魚 (Phishing) 為社交工程攻擊的一種模式，主要是指駭客利用人性的弱點，透過偽造的電子郵件或欺騙之偽造網站，誘導使用者提供個人資訊或使用者的金融資訊或帳號密碼等，讓駭客得以從中獲取不正當之利益。

針對網路釣魚，可以彙整成以下性質[1]：

- **欺騙性**：建造一個與實際存在網站相仿之釣魚網站，或是透過一個與實際郵件地址相似的電子信箱進行釣魚郵件的發送，並加強其真實程度以增加成功之機率。
- **針對性**：現今電子商務、網路銀行等線上金融服務盛行，雖然增加使用之便利性，但也成為網路釣魚的目標之一。

圖 2-9 網路釣魚示意圖



資料來源：TWCERT/CC 整理

- **多樣性**：為取信使用者，網路釣魚會結合其他服務或將某些服務連結到真正遭偽冒網站中，提高服務之真實性。
- **仿真性**：雖然網路釣魚的數量相當多、仿造的品質也愈發精良，但釣魚者並不會利用大量資源去建造一個相同的網站，因此即便仿冒的再相似，都會有其缺陷，而使用者必須透過觀察力和警覺性，去避免遭受釣魚攻擊及損失。

而駭客為了欺騙使用者並取得不法利益，通常有兩種攻擊手法—釣魚郵件以及釣魚網站，用以獲取不正當之利益[2]。

(1) **釣魚郵件 / 釣魚簡訊**：偽冒受害者信任的人、組織，或是中獎通知、物流訊息等吸引使用者之內容，引誘使用者提供如帳號密碼等個人資訊。甚至當使用者點擊連結後，便會遭受惡意程式的感染及入侵，除了電腦的損壞外，更會有資訊竊取及洩漏等威脅，甚至發生資安勒索事件[3]。

(2) **社群媒體釣魚**：隨著如 Facebook、Instagram、Twitter 等社群媒體的盛行，許多駭客會在社群媒體中發布如抽獎、免費提供服務等吸引大眾的資訊，讓使用者於該釣魚貼文中留言或點擊內文中的釣魚連結，並提供個人資訊給駭客，甚至受騙下載惡意檔案，成為網路釣魚的受害者[4]。

1 電腦時代. (2013年) “遏制網路釣魚行為的法律措施: https://www.lunwendata.com/thesis/2013/24349.html （瀏覽日期：2019年9月2日）
2 GoDaddy. “什麼是網路釣魚？”：https://tw.godaddy.com/help/what-is-phishing-346 （瀏覽日期：2019年9月2日）
3 臺灣大學. “釣魚/詐騙信件手法解析”： https://www.cc.ntu.edu.tw/mailtips/index.html （瀏覽日期：2019年9月2日）
4 PhishLabs. “Why Social Media is Increasingly Abused for Phishing Attacks”. Retrieved September 15, 2019, from the World Wide Web: https://info.phishlabs.com/blog/how-social-media-is-abused-for-phishing-attacks

(3) **釣魚網站：**最基本的釣魚網站會配合釣魚郵件 / 訊息內容，致使使用者受騙提供如姓名、電話、地址等個資。精緻的釣魚網站，會假冒大型知名網站，並申請極為相似的網址，甚至偽冒電子商務或網路銀行類型網站，竊取使用者的帳號密碼，或販售虛假 / 仿冒的商品，騙取資金。另外有些釣魚網站會散布惡意程式，導致電腦遭感染而蒙受損失[5]。

2. 網路釣魚防護

(1) **網路釣魚基本防護**

針對網路釣魚，使用者可透過以下幾項基本防護，提高自身警覺注意相關細節，減少上當受騙機率[6、7]：

A. **勿點擊不明連結及附件：**網路釣魚通常都會在訊息中附上連結或檔案 / 附件供使用者下載，作為個資竊取或惡意程式散布方式之一。因此，當使用者收到相關郵件 / 訊息，可先將其中網址 / 檔案透過資安組織提供之檢驗工具驗證，以免誤入釣魚陷阱中。

B. **勿讓他人遠端操作電腦 / 下載檔案：**某些釣魚信件宣稱使用者的電腦已遭他人入侵或遭惡意程式感染，並告知對方可協助處理，要求允許遠端控制自身電腦或下載防護程式。若使用者收到此類型郵件，除必須先查詢對方身分之外，若真不幸遭到感染 / 入侵，應尋求可信之組織 / 企業協助。

C. **注意郵件地址及內容：**一般網路釣魚郵件多會仿冒實際組織 / 企業之電子郵件地址或相關資訊，因此使用者可仔細觀察電子郵件相關資訊，是否拼寫或標點符號等有誤，避免上當受騙。

D. **注意網站網址及內容資訊**：無論是否使用 https 的網站，使用者均可留意網站之網址資訊，注意是否有增減任何標點符號或拼寫錯誤，以及該網頁中是否有實際網站不存在或應有卻未出現之功能，若有任何與實際網站迥異之處，應避免繼續瀏覽及提供任何相關資訊，同時也需檢驗是否有遭到惡意程式的入侵。

E. **隨時更新應用程式及作業系統**：為了防止層出不窮的釣魚攻擊，不論是作業系統或瀏覽器等應用程式，必須配合相關企業 / 組織進行系統更新，以達到最新之防護能量。

(2) **反釣魚系統**

反釣魚 (Anti-Phishing) 系統，主要辨別釣魚郵件及釣魚網站等，在使用者觸及時提出警告，並將其阻擋或封鎖，減少使用者因網路釣魚而蒙受損失之機率。為防範網路釣魚，各家網路業者紛紛推出相關防範系統，其提供之產品或服務主要分為以下幾種[8、9]：

A. **防止相似域名**：紀錄網際網路上大部分實際使用之網站和對應之網址，並且在觸及到釣魚網站時，與資料庫中網址進行比對和驗證，減少因極相似之網域而產

5 資安人.（2012年）.“教你分辨釣魚網址分身術！”：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=6813（瀏覽日期：2019年9月3日）

6 Norton.（2019年）.“如何防護五種常見的網路釣魚詐騙？”：https://www.jadespring.com.tw/如何防護五種常見的網路釣魚詐騙.html（瀏覽日期：2019年9月10日）

7 臺北市政府警察局.（2019年）.“網路釣魚騙術解析與防治？”：https://police.gov.taipei/News_Content.aspx?n=8D43510FCC9EE11C&sms=87415A8B9CE81B16&s=1B8350AAB6B0C4D0（瀏覽日期：2019年9月10日）

8 APWG. “Sponsoring Solutions”. Retrieved September 10, 2019, from the World Wide Web: https://apwg.org/sponsoring-solutions/

9 Infosec. “Top 16 Anti-Phishing Resources”. Retrieved September 10, 2019, from the World Wide Web: https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-countermeasures/top-16-anti-phishing-resources/#gref

生的網路釣魚攻擊。

B. 郵件驗證 / 過濾：除將電子郵件在傳輸時進行加密外，會透過包含大量數據之資料庫，對電子郵件驗證並過濾信件內容，防止使用者受到釣魚信件之威脅。

C. 網頁過濾：透過被發現以及潛在威脅之大量釣魚訊息，可以有效阻擋惡意的或已被認定為網路釣魚之網站，提升網路釣魚的識別性和過濾效率。

D. 加強驗證機制：除雙因素認證外，許多資安企業提出了更多因素認證方式，例如生物辨識或線上簽名等，甚至提出涵蓋整體組織，以防止有非組織內部人員登入並竊取資料。

E. 檢驗使用者資訊：有網路業者提供軟體服務，會掃描裝置中是否存在不明或惡意程式，並將其卸載，或是透過程式從暗網等搜尋該使用者的相關資訊是否已遭竊，並立即提出警訊以避免傷害擴大。

F. 使用者意識培訓：透過軟體、網站或社群媒體，定期提供使用者關於網路釣魚的相關知識，甚至定期進行相關培訓課程，不論是針對企業還是個人，都可因為防範意識的提高，而減少遭到網路釣魚之機率。

現今許多網路業者均紛紛推出反釣魚程式產品，例如趨勢科技，Google、Netcraft、PhishTank 等均推出反釣魚軟體，每款軟體所提供功能不盡相同，但都可以作為防範網路釣魚的工具，降低網路釣魚帶來的威脅。

3. 網路釣魚通報協處機制

在網際網路上，有相當多的組織都接受使用者的網路釣魚通報，一來可以即時將資訊傳輸給被仿冒成攻擊者 / 攻擊方所屬之網路業者，二來可以建立起屬於

自身的網路釣魚資料庫，並透過數位分析和預測，隨時針對網路釣魚進行即時防護，維持使用者及企業的使用品質，減輕網路釣魚帶來的威脅和負擔。

(1)、 國外通報協處

反網路釣魚工作小組 (APWG) 是國際上對網路釣魚極具公信力之組織，協助網路釣魚之通報和協處運作。APWG 提供網路釣魚通報服務，每月會接收超過 10 億筆相關資訊，並將其透過所屬國家或處理機構進行通報，要求相關單位關閉或處理網路釣魚事件，希冀能減少甚至消除網路釣魚等惡意行為 [10]。

在台灣，由國家通訊傳播委員會 (National Communications Commission, NCC) 督導之 TWNIC 負責維運 TWCERT/CC，也與 APWG 合作，固定分享及通報網路釣魚情資，自 2019 年起，TWCERT/CC 已接受 APWG 組織通報超過百筆之情資，並協助將其釣魚網站 / 釣魚郵件等，經查證後通知相關業者，請負責之網路業者進行關閉或處理行為，減少網路釣魚受害量。

(2)、 國內通報協處

在台灣，為防止詐騙事件之猖獗，內政部警政署建立 165 反詐騙諮詢專線，提供民眾在收到類似詐騙之訊息或電話時，可以即時透過該諮詢專線進行查證，以免因歹徒之誘騙或威脅而蒙受損失。而其詐騙報案及宣導之範疇自然包括網路釣魚事件，例如：某快遞業者的釣魚簡訊或詐騙中獎通知等，都可經過該防詐騙專線進行驗證。同時，警政署也建立 165 全民防騙網，將其所收到之相關資訊以及事

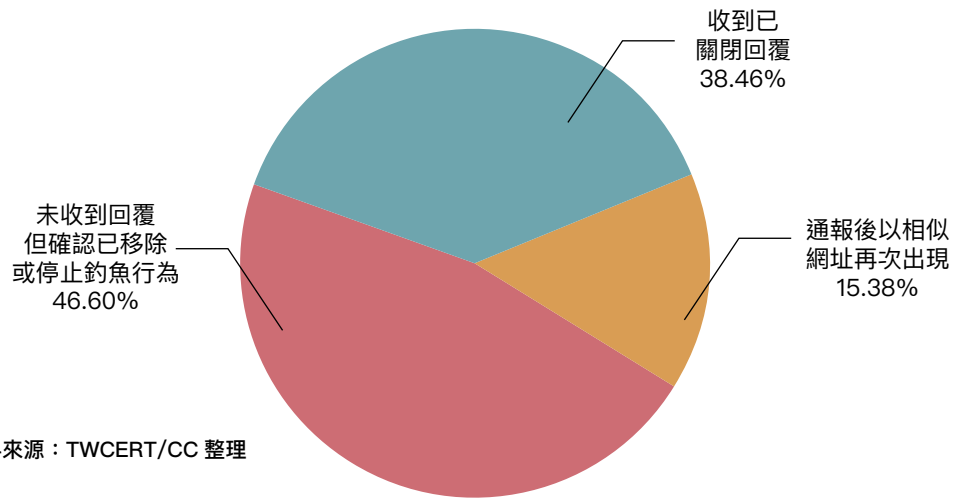
10 APWG. “Anti-Phishing Working Group”. Retrieved September 10, 2019, from the World Wide Web: https://apwg.org

件等，公告於該網站中，除了對民眾宣導勿輕信詐騙手法外，更提供一個提升民眾警覺和查驗方式之極佳管道，減少民眾遭受詐騙之威脅 [11]。

(3)、 網路釣魚通報協處統計

TWCERT/CC 組織擔任台灣與國際間資訊安全訊息傳遞及協處之橋樑，除接收國內企業或民眾之通報，同時也接收國外針對台灣之資安通報。針對網路釣魚，已協調國內外組織，通報為數不少之釣魚網站 / 釣魚郵件。若收到關於台灣網域或 IP 之網路釣魚訊息，都會針對其內容通知如 TWNIC、網路業者、學術單位或政府等單位，針對網路釣魚進行相關處理。而若自台灣組織或民眾收到關於他國之釣魚網站 / 釣魚信件，也會通知他國之 CERT 組織或該國之網路業者，請對方進行相關處理。

圖 2–10 TWCERT/CC 通報國外網路釣魚處置統計



資料來源：TWCERT/CC 整理

根據 TWCERT/CC 統計資訊，通報至國外之釣魚網站情資，有約 38.46% 之國際 CERT 組織及企業回覆已收到其通報並關閉該釣魚網站，約 15.38% 之釣魚網站被關閉後透過相似之網址再度出現，剩餘之釣魚網站雖未收到關閉回覆，但經確認已移除或停止網路釣魚行為。詳細資訊如圖 2-10：

網路釣魚是一種無國界之資安問題，必須串連使用者、企業、通報組織以及相關負責單位之合作，方能進行最為迅速、精確且完整之網路釣魚處理機制，致力於消弭網路釣魚行為，完備網際網路的資訊安全。

11 內政部警政署. “內政部警政署165全民防騙網” ： https://165.npa.gov.tw/#/（瀏覽日期：2019年9月10日）

第二節、IoT 設備與行動應用安全

一、物聯網資安威脅與資安檢測

1. 簡介

1. 物聯網惡意程式威脅

近年來，物聯網日趨深入人們的生活當中，同時林林總總的物聯網裝置，也讓駭客有更多機會利用裝置出廠時就已存在的弱點，植入惡意程式，利用受到惡意程式感染的設備 ，用以濫發垃圾郵件 (Spam)、發動分散式阻斷服務攻擊 (DDoS)、散播病毒或蠕蟲，以及竊取個人資料，大大提高物聯網的資安風險。

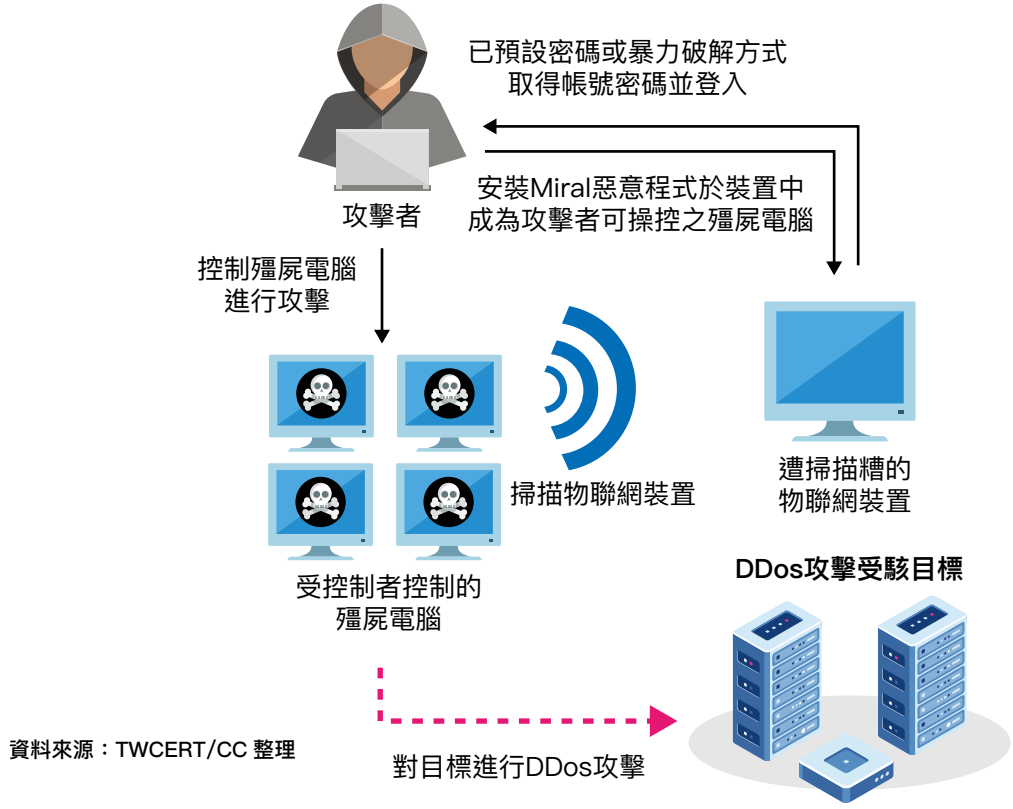
物聯網惡意程式大抵透過傳播 (Propagation)、感染 (Infection)、命令與控制傳達 (Command and Control Communication) 和進行攻擊 (Execution of Attacks) 等四個步驟執行 [1]。而物聯網惡意程式種類及數量相當多，也都可能對物聯網產生重大的危害，例如下述較為知名的幾個物聯網惡意程式：

(1) Mirai

此惡意程式在 2016 年 9 月 18 日，攻擊法國主機供應商 OVH 遭遇超過 1TB 流量的攻擊；9 月 21 日，知名資安部落格 Krebs on Security 亦受到 DDoS 攻擊，流量達 665GB。同年 10 月 21 日，提供動態 DNS 服務的 Dyn DNS 遭受大規模的 DDoS 攻擊，甚至導致 GitHub、Twitter、Airbnb、Reddit、Freshbooks、Heroku、SoundCloud、Spotify 和 Shopify 等網站一度癱瘓 [2、3、4]。

如圖 2-11 所示，Mirai 病毒本身使用 Telnet 協定並透過掃描方式，找出仍使用原

圖 2–11 Mirai 病毒運作示意圖



資料來源：TWCERT/CC 整理

1 Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Dominik Breitenbacher, Asaf Shabtai, and Yuval Elovici. (2018). “N–BaIoT: Network–based Detection of IoT Botnet Attacks Using Deep Autoencoders”. Retrieved June 24, 2019, from the World Wide Web: https://arxiv.org/pdf/1805.03409.pdf

2 鄭進興.（2017年6月）.“分散式阻斷服務攻擊防護策略探討”：http://www.myhome.net.tw/2017_06/p03.htm（瀏覽日期：2019年6月24日）

3 CLOUDFLARE. “What is the Mirai Botnet?”. Retrieved June 24, 2019, from the World Wide Web: https://www.cloudflare.com/learning/ddos/glossary/mirai–botnet/

4 Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever,Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, Yi Zhou. (2017, August 16). “Understanding the Mirai Botnet”. Retrieved June 24, 2019, from the World Wide Web: https://storage.googleapis.com/pub–tools–public–publication–data/pdf/f822124cae127fdde5f613b3beb6e0929c800e09.pdf

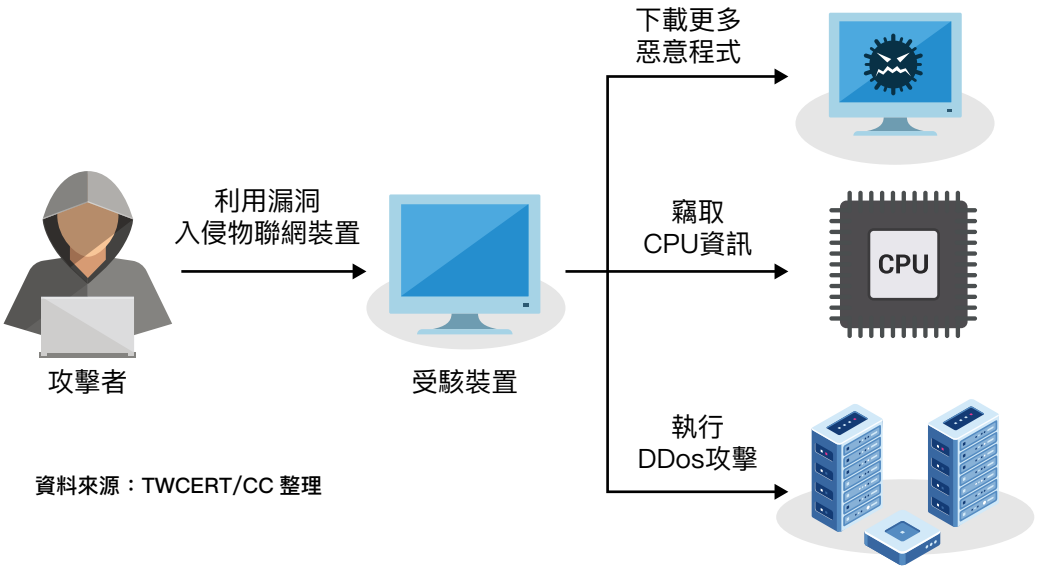
廠帳號密碼設定的物聯網裝置，以多組裝置出廠預設使用者名稱和密碼嘗試登入，登入成功後針對特定 IP 在特定期間發動 DDoS 攻擊；並可繼續發掘其他可被攻破的物聯網裝置，製造新的 Botnet，大幅擴張駭侵規模。

(2) Qbot

此種惡意程式最為人知的事蹟是 2014 年曾發動大規模 DDoS 攻擊。

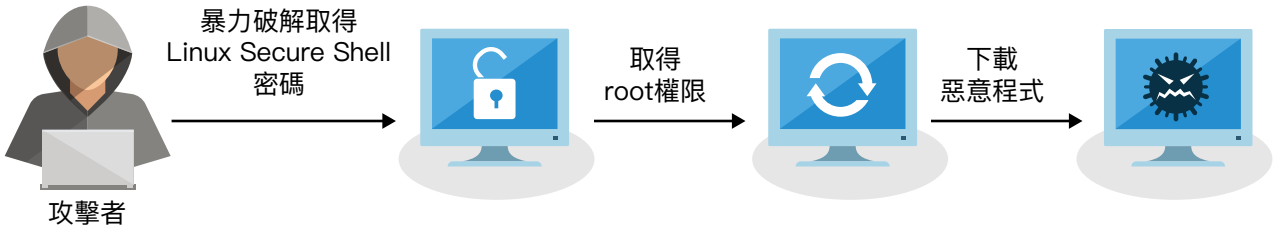
如圖 2-12 所示，此惡意程式在先前的版本會利用 Shellshock 漏洞 (CVE-2014-6271) 來入侵裝置，然後再透過遠端指令遙控被入侵的裝置發動 DDoS 攻擊，或者再下載其它惡意檔案到被入侵的裝置，且具有利用常見使用者名稱與密碼組合來暴力攻擊路由器的功能，同時能從受感染的裝置收集 CPU (Central Processing Unit) 資訊。新版的感染方式改為使用可公開取得的 Metasploit 漏洞攻擊模組，並支援更多 DDoS 遠端遙控指令，以及一些虛擬貨幣和後門功能，同時還會在裝置上植入

圖 2-12 Qbot 惡意程式運作示意圖



資料來源：TWCERT/CC 整理

圖 2-13 XorDDOS 惡意程式運作示意圖



資料來源：TWCERT/CC 整理

惡意程式，移除競爭對手的殭屍病毒[5、6]。

(3) XorDDOS

圖 2-13 所示，XorDDOS 會以暴力攻擊法取得 Linux 機器上 Secure Shell 服務的密碼，進而取得存取權限。攻擊者一旦登入系統，就會使用 root 權限執行 Bash shell 指令碼，開始下載並執行惡意程式的二進位檔案[7]。

2. 物聯網資安風險與防護

由於物聯網資安牽涉設備、通訊、雲端等三個體系的整體防護，使得物聯網資安需要軟硬體生態系的合作[8]：

5 Trend Labs 趨勢科技全球技術支援與研發中心.（2019年4月11日）.“Bashlite IoT 惡意程式新增挖礦與後門功能，專門攻擊 WeMo 品牌裝置”：https://blog.trendmicro.com.tw/?p=60149（瀏覽日期：2019年6月25日）

6 Symantec Security Response.（2016年9月22日）.“有越來越多DDoS 攻擊利用IoT裝置”：https://www.symantec.com/connect/tr/blogs/ddos-iot-0?page=1（瀏覽日期：2019年6月25日）

7 Akamai.（2015年10月5日）.“Akamai 研究發現XOR DDoSbotnet透過被入侵的Linux機器”：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=8178（瀏覽日期：2019年6月25日）

8 顧馨文.（2019年3月5日）.“資安攻擊事件頻傳　物聯網安全防護湧現商機”：https://www.2cm.com.tw/2cm/zh-tw/market/ED01FA5446EB47D6AC9D01313211A803（瀏覽日期：2019年6月25日）

(1) **設備安全**：物聯網設備包括感測器、通訊元件等硬體及作業系統、應用程式、儲存資料等。為了增進產品資訊安全，許多廠商加入了晶片認證與安全防護、設備授權與認證等功能，但也帶來了老舊設備無法植入新安全功能的資安隱憂。

(2) **通訊安全**：物聯網通訊組成包含通訊網路、通訊協定、網路設備等，並可能包含有線 / 無線或者開放 / 封閉以及不同協定的網路；其防護則包括存取控制、防火牆 / 入侵偵測、通訊加密等。不安全的網路通訊會讓攻擊者有機會從通訊過程中擷取資訊，進而竊聽或造假。

(3) **雲端安全**：許多物聯網應用會連結雲端服務上的應用軟體或服務，故必須確保雲端服務之應用安全及資料安全。此外，整體物聯網體系的資訊安全也極為重要，包括設備的驅動程式管理、補丁的更新、政策與稽核管理、活動監視及安全地移除軟體等。

因此，我國資策會智慧網通系統研究所曾經參考美國國土安全部所提出之「發展物聯網系統資訊安全策略原則」，提供下列的思考方向[9]：

(1). 系統若能在設計就考慮各種威脅與中斷之狀況與相對應處理方法，日後營運時資安事件將會大大降低；就算發生，也可避免緊急採購昂貴資安產品來補強。

(2). 持續修補更新與漏洞管理，可以降低資安威脅，故應在設計階段考慮故障設備對系統之影響、各項產品使用期限、以及維修成本等面向；當資安軟體更新失能時，製造商必須衡量召回之費用與被攻擊的損失風險。針對前述問題，可參考美國國家通訊與資訊管理委員會 (National Telecommunications and Information Administration, NTIA) 所提出的物聯網更新與修補流程。

(3). 許多界定漏洞、偵測不法、資安事件處理回應機制、損失或中斷回復機制的資訊

安全實務，可運用於物聯網系統，就此可參考美國國家標準技術研究所 (National Institute of Standards and Technology, NIST) 所制定的風險管理參考框架 (NIST Cybersecurity Risk Management Framework)，在現有的資安防護實務基礎上，更進一步的實踐資安防衛，並參與資安漏洞分享平台，即時接收最新資安威脅與漏洞以保持警戒。

(4). 應參考不同系統或供應商的環境與需要，設計、操作物聯網裝置，並以系統可承受影響的程度，決定採用適當的風險管理方法；工業及企業系統並須針對連網裝置，設定身分識別與認證。

物聯網系統各階段供應商的漏洞，會影響整個系統的資訊安全，因此開發者與製造商需要知道整個供應體系之軟硬體及其可能產生之漏洞，廠商亦需提供清楚的軟硬體元件、模組、版本、漏洞等資訊，以利風險管理。

3. 強化設備檢測和認證

物聯網設備資安產業標準與檢測認驗證，已成為政府重視的一大焦點； 2018 年 6 月，國家通訊傳播委員會與經濟部整併物聯網資安標準及測試規範，以及無線射頻通傳設備資安檢測技術指引，於同年 12 月正式發布物聯網設備資安驗證標章制度，並委由台灣資通產業標準協會

9 馮明惠、吳國華. “物聯網資訊安全特性與原則初探”：http://www.twcloud.org.tw/files/file_pool/1/0i227610614524406609/4.pdf（瀏覽日期：2019年6月25日）

10 羅正漢.（2019年3月19日）. “【臺灣資安大會直擊】最新臺灣資安產業標準發展現況揭露，已有5家認可實驗室正式上路”：https://www.ithome.com.tw/news/129458（瀏覽日期：2019年6月25日）

11 黃雅琤.（2019年3月19日）.“臺灣物聯網產品資安認驗證制度介紹–活絡產業標準 擴展國際鏈結”：https://s.itho.me/cybersec/2019/slides/twpavillion/0319_臺灣物聯網產品資安認驗證制度介紹_TAICS_黃雅琤副處長.pdf（瀏覽日期：2019年6月25日）

核發「物聯網資安標章」並進行實驗室及產品稽核管理業務[10、11]。

我國目前已完成影像監控系統的資安標準及測試規範、具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引、智慧巴士資通訊系統資安標準與智慧高效率照明系統技術規範，以全面提升物聯網設備的安全及防護能量[12、13、14、15]。

透過標準、制度帶動臺灣物聯網產品之資安水準，將進一步強化我國產品在國際上的競爭力。政府目前致力於推動國內物聯網資安測試實驗室成立，以完備認驗證制度，同時也會輔導製造商取得產品認證，進而推動國內公部門將物聯網設備資安標準納入採購規範及共同供應契約，並公告通過資安標準認證的產品，作為一般民眾採購時的參考，進一步提升民眾消費認知。未來將致力推動物聯網設備資安標準逐步成為國家標準，並促成國際標準相互認證。

二、行動應用 APP 資安威脅與防護

1. 簡介

APP 是應用程式 (Application) 的縮寫，是一軟體應用程式 (Software Application)，其主要是在智慧型手機或行動裝置中所使用的應用程式，並且針對不同的平臺與作業系統，產生不同類型的行動應用 APP。

根據美國的行動應用 APP 數據及分析平臺 App Annie 之統計，2018 年整體行動應用 APP 下載量已經超過 1,940 億次，相較於 2016 年成長了約 35%，APP 的相關支出也超過了 1,010 億美元，其相較 2016 年之成長幅度達到了 75%，隨著行動裝置的普及，未來行動應用 APP 的下載量將持續上升[1]。

然而，正因為行動應用 APP 的廣受歡迎，使得駭侵或病毒散布的目標逐漸轉向行動裝置的 APP 上，並且藉由使用者對 APP 的信任，透過行動應用 APP 進行惡意行為，從而獲取不法利益。

1. 行動應用 APP 資安威脅

行動應用 APP 的資安威脅，統稱為惡意行動應用程式 (Malicious Mobile Applications)，透過吸引使用者的某些功能或活動，誘使使用者下載並安裝該 APP，然而，在使用者安裝了惡意 APP 之後，其可能會自動安裝惡意程式以竊取行動裝置中的資訊，甚至修改裝置內資訊或相關設定[2]。

在眾多的惡意 APP 中，比例最高的為工具類型之 APP，佔全體惡意 APP 數量的 39.1%；第二名為生活風格類型之 APP，佔全體惡意 APP 數量的 14.9%；第三名為娛樂類型之 APP，佔全體惡意 APP 數量的 7.3%，詳細資訊如表 2-1[3]：

此外，根據 Check Point 針對台灣之資安統計報告，在 2018 年期間，行動裝置相關的資安攻擊，佔居台灣五大攻擊中的第二名，並且坦言未來將會越來越多針對行動裝置的攻擊，例如在 2018 年發現一款名為 AdultSwine 的惡意程式，該惡意程式被植入於 APP 商店中逾 60 款的兒童遊戲類 APP，導致這些 APP 會跳出色情廣告以及假防毒軟體等詐騙訊息，在該商店中，含

12 台灣資通產業標準協會.“標準及測試規範”：http://www.ifantech.net/taics/Validation04.aspx?validateType_id=14&Type=1（瀏覽日期：2019年6月25日）

13 台灣資通產業標準協會.“智慧巴士資通訊系統資安標準–第一部：一般要求”：https://www.taics.org.tw/userfiles/file/20181226/20181226150501_34065.pdf（瀏覽日期：2019年6月28日）

14 經濟部能源局.（2019年1月4日）.“發光二極體先進照明推廣補助計畫作業要點”：https://www.moeaboe.gov.tw/ECW/populace/Law/Content.aspx?menu_id=3326（瀏覽日期：2019年6月28日）

15 經濟部能源局.（2019年1月14日）.“公告修正「智慧高效率照明系統技術規範」，並自即日生效。”：https://www.moeaboe.gov.tw/ECW/populace/Law/Content.aspx?menu_id=5793（瀏覽日期：2019年6月28日）

---

1 App Annie. “The State Of Mobile 2019”. Retrieved November 4, 2019, from the World Wide Web: https://www.appannie.com/en/go/state-of-mobile-2019/

表 2-1 惡意 APP 類型比例

惡意APP類型	百分比
工具	39.1
生活風格	14.9
娛樂	7.3
社交	6.2
音樂	4.3
益智遊戲	4.2
照片與影片	4.2
動作遊戲	4.1
書籍與參考	3.2
教育	2.6
其他	9.9

資料來源：TWCERT/CC 整理

有 AdultSwine 的 APP 總計已經被下載超過 700 萬次，顯示行動應用 APP 的威脅在未來將會持續增加[4]。因此，台灣行動裝置使用者應需多加注意，避免成為惡意 APP 之受害者。因此，台灣地區在 2018 年仍有一定之惡意 APP 攻擊數，雖僅稍高於全球平均，但台灣行動裝置使用者仍需多加注意，避免成為惡意 APP 之受害者。

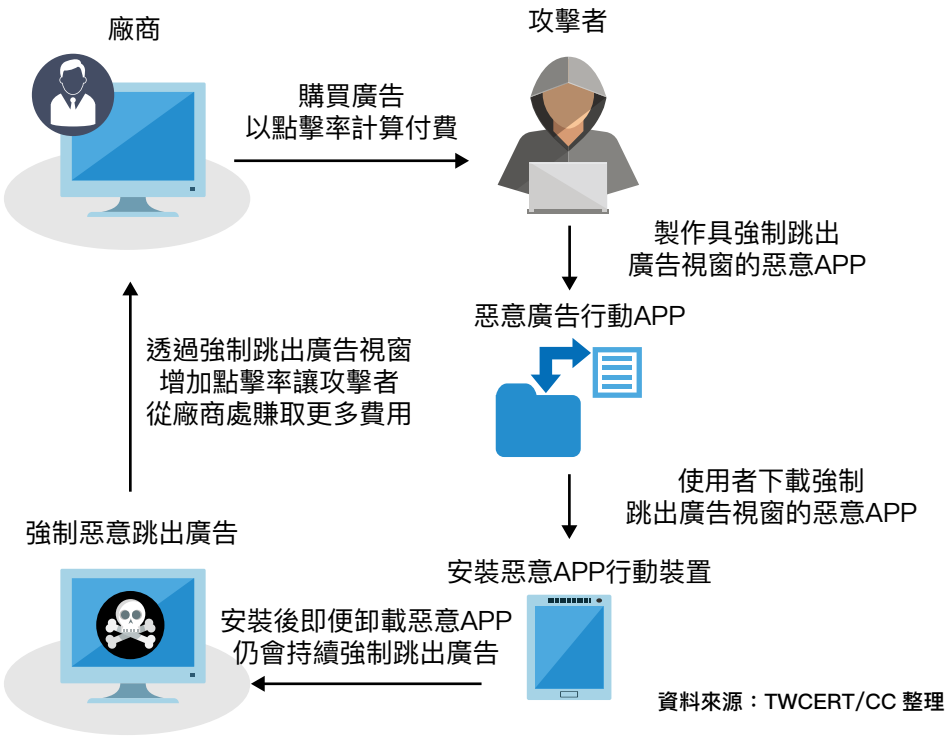
2. 行動應用 APP 資安威脅及案例

隨著 APP 數量以及使用者將機敏資訊存於行動裝置的比例增加，惡意 APP 對使用者的威脅以及損害程度逐漸提升。然而，除了個人使用者之外，同時由於個人自備裝置 (Bring Your Own Device, BYOD) 在企業內的逐漸普及，企業同樣也遭受惡意 APP 入侵並竊取公司機密資訊的威脅，這些惡意 APP 可被分為以下五種類型[5]：

(1) **廣告 (Adware)**：經常偽裝成一般合法應用程式，其行為通常涉及到第三方的購買行為，例如透過自動廣告點擊提升其點擊率，讓廠商獲取資金等。

如圖 2-14 所示，許多攻擊者會透過 APP 強制跳出廣告視窗，以賺取第三方購買廣告的更多費用。因此，當使用者發現在下載行動應用 APP 後，若有廣告出現在

圖 2-14 廣告惡意 APP 示意圖



使用者未授權或不應出現的狀況時，甚至行動裝置的運行速度突然變慢，以及電池量耗用突然加速，極有可能是下載並遭到了廣告惡意 APP 的侵襲。

(2) **網路釣魚 (Phishing)**：此種類型之惡意 APP 主要是將使用者導入一釣魚網站，並

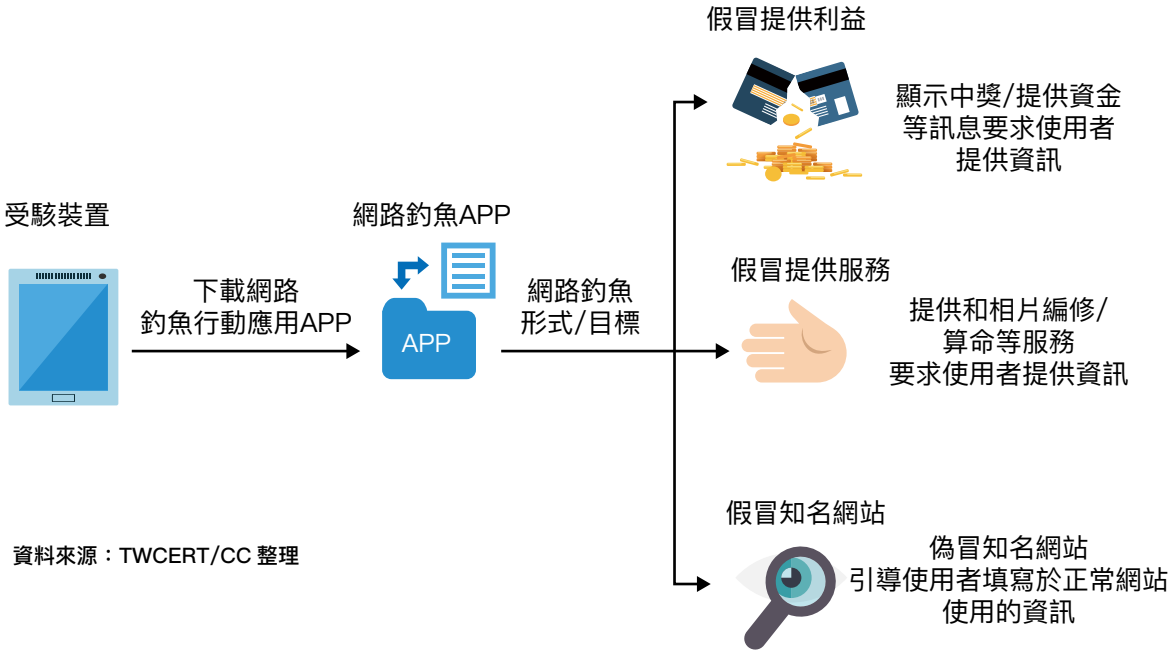
2 cloudHQ. “Malicious Mobile Apps: The New Threat To Small Businesses”. Retrieved November 5, 2019, from the World Wide Web: https://blog.cloudhq.net/malicious-mobile-apps-the-new-threat-to-small/

3 Symantec. “Internet Security Threat Report Volume 24”. Retrieved November 8, 2019, from the World Wide Web: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

4 IThome. “臺灣遭受惡意程式攻擊現況揭露，竟是Botnet攻擊最多國家”： https://www.ithome.com.tw/news/129187（瀏覽日期：2019年11月8日）

5 Charge Defense. “Types of Mobile Malware”. Retrieved November 5, 2019, from the World Wide Web: https://www.chargedefense.com/tips-tricks/infographic-types-of-mobile-malware/

圖 2-15 網路釣魚 APP 示意圖



資料來源：TWCERT/CC 整理

且誘使使用者輸入相關資訊，以竊取個人資料或相關憑證。

如圖 2-15 所示，透過釣魚 APP，攻擊者可顯示中獎資訊、服務提供等方式，要求使用者提供個人資訊，甚至偽冒知名網站，引導使用者填寫帳號密碼或個人資料，以竊取相關資訊。因此，若使用者在下載並安裝行動應用 APP 後，突然收到關於贏得獎品、帳戶或訂閱服務遭到停止，並且未確實告知原因，必須緊急採取行動以解決問題等，都極有可能遭到網路釣魚 APP 的駭侵。此時使用者除了提高警覺、不能依照訊息的指示操作或提供個資外，更需立即將可能的網路釣魚 APP 卸載。

(3) **殭屍網路 (Bots)**：此種惡意 APP 可以在行動裝置後台運作，往往不被使用者察覺，可以和殭屍控制主機 (Botmaster) 進行聯繫和執行命令。

若使用者在下載並安裝 APP 後，其行動裝置容易產生連線中斷、網路無法連接，或是在未經使用者授權的情況下，行動裝置自動安裝或移除任何 APP、電話撥號、簡訊或電子郵件的傳送，則該行動裝置極有可能下載到殭屍惡意 APP，並且遭其感染。

(4) **間諜軟體 (Spyware)**：將使用者的裝置或行為資訊，例如簡訊、電子郵件、電話紀錄、錄音、聯絡人、地理位置、圖片，以及相關狀態等訊息，加以監控和記錄，並且將上述資訊分享給遠端的伺服器。

若使用者在下載並安裝行動應用 APP 後，發現行動裝置有奇怪或可疑之行為，例如行動裝置在未被使用者使用的情況下自動啟動、關閉或發出不尋常之聲響，或是行動裝置的電量及數據使用量消耗突然增加，甚至在進行電話溝通時容易聽到可疑的蜂鳴聲或噪音，都有可能為行動裝置感染間諜軟體之故，此時使用者除了將可疑的行動應用 APP 移除外，也必須檢查內部是否有被安裝或放置可疑的檔案或程式，並將所有可疑檔案進行移除和卸載。

(5) **下載器 (Downloader)**：此種程式自身並非惡意程式，但會隱身於 APP 中，負責下載其他的惡意程式到使用者行動裝置中，是其他惡意 APP 執行惡意行為中的過程工具。

當使用者下載並安裝 APP 後，行動裝置產生問題最明顯的即為出現未經使用者授權下載之 APP 或檔案，此外，亦有可能受感染之行動裝置產生非使用者使用造成之電池耗用、網路流量，以及額外費用等，都可能為行動裝置遭惡意下載器感染所產生之情形。

3. 行動應用 APP 防護

惡意 APP 難以完全防範，因此使用者在下載行動應用 APP 之前，必須考慮下述幾點：

(1) 定期更新行動裝置作業系統版本或相關軟體、應用程式之版本，以配合廠商進行相關漏洞修補及增加防護能量。

(2) 從信用良好的應用程式商店，如 Google Play Store 或 App Store 等商店下載行動應用 APP，避免從第三方下載 APP。

(3) 許多惡意 APP 會偽冒知名品牌 / 企業，騙取使用者信任，因此使用者需檢查並識別該 APP 確實為該品牌 / 企業所屬。

(4) 使用者在下載並安裝 APP 前，必須針對其所要求的任何授權仔細閱讀，避免提供非 APP 功能外的授權或洩漏行動裝置中的機敏資料。

(5) 若使用者擔憂遭自身難以識別之惡意程式感染及入侵，則可以安裝行動安全應用程式，除了警告已辨識為惡意 APP 的應用程式外，更可將行動裝置中的企業資料或機敏資料隔絕，達到機密資訊不外漏的目的。

(6) 為了減少行動裝置或資料因惡意 APP 遭到破壞之問題，建議使用者需定期備份手機中的機敏或重要資訊。

根據美國的 Web 應用安全非營利組織 OWASP 所提出的 Mobile Top 10，提出了開發者對於行動應用 APP 的開發，必須注重並避免的 10 項安全項目[6]：

(1) **平臺使用不妥當** (Improper Platform Usage)：主要為開發者未確實使用平臺安全控管機制，為了防止平臺使用不妥當的行為，在行動應用 APP 開發時，必須在伺服器端實踐安全編碼 (Secure Coding) 以及安全相關設置。

(2) **不安全的數據存取**(Insecure Data Storage)：因開發者並未針對行動裝置所儲存的機敏資訊進行管控所造成。因此，開發者必須避免使用較差的加密資料庫，或若未針對數據進行適當的防護，應設定必須透過特殊的工具方能針對數據進行存取的行為。

(3) **不安全的通訊**(Insecure Communication)：駭客可能透過系統或設備的漏洞以竊取行動應用 APP 數據傳輸中的機敏資料。因此開發者必須將 SSL（Secure Sockets Layer）除了身分驗證外，也用於機敏資訊傳輸時所用，或是使用可信的憑證中心所提供的簽章，以防止因通訊不安全造成的損失。

(4) **不安全的身分驗證**(Insecure Authentication)：開發者必須避免較弱的身分驗證模式，直到驗證成功才將相關數據加載到行動裝置上，以確保相關數據或程序都是在通過身分驗證後方可使用。

(5) **不足夠的加密法**(Insufficient Cryptography)：開發者除盡量避免在行動裝置上儲存任何機敏資訊外，更應使用經過驗證且未來 10 年內都經得起考驗的加密標準進行加密。

(6) **不安全的授權**(Insecure Authorization)：開發者應僅使用後端伺服器中的訊息進行驗證，而避免使用來自於行動裝置的權限資訊進行授權驗證。

(7) **較差的程式碼品質**(Poor Code Quality)：此種類型的問題，本身並不一定是安全問題，但容易引發安全的漏洞，因此開發者必須確保在開發團隊中，都維持一致的

6 OWASP. “Mobile Top 10 2016-Top 10”. Retrieved November 11, 2019, from the World Wide Web: https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

編碼方式。

(8) **程式碼竄改 (Code Tampering)**：由於行動應用 APP 被安裝在行動裝置中，大部分數據都置於行動裝置中，因此駭客便有可能入侵後竄改行動應用 APP 中的程式碼，或是更動記憶體中資訊、使用的應用程式介面 (Application Programming Interface, API) 等，經常作為網路釣魚之用。因此，開發者必須提供驗證機制，檢測該行動應用 APP 是否曾經遭到他人竄改，並執行適當處置行為。

(9) **逆向工程 (Reverse Engineering)**：駭客可能透過某些工具針對 APP 進行反組譯解析，或是從中得到該 APP 的相關資訊、機敏資料甚至得到其程式碼，同時也可以針對所得的資訊對後端系統進行攻擊等。因此，為了防範逆向工程，開發者必須使用混淆工具，將其程式碼、字符表等資料進行混淆處理，避免輕易遭到逆向工程的威脅。

(10) **額外功能 (Extraneous Functionality)**：許多開發者為方便進行程式的修改或安全的控管，因此會在 APP 的程式碼中留下與 APP 本身功能無關的其他功能。通常這些額外的功能並不會告知使用者，並且此種額外功能往往都不具惡意，不會讓使用者的個人權益遭侵害。但某些功能卻可能被駭客所利用，用於入侵並竊取相關資訊。因此，為了防範此資安問題的發生，通常需透過相關資安專家針對該行動應用 APP 進行程式碼的檢查，例如檢查其配置，避免有任何隱藏功能；檢查 APP 中的測試程式碼或檢查所有 Log 資訊，確保無過多關於後端系統的資訊被寫入 Log 中。

由於行動應用 APP 的數量隨著行動裝置的蓬勃發展，其數量逐年快速上升，導致

許多病毒或駭侵手法都從電腦轉往行動裝置，但由於 APP 的數量過多，難以確實的進行相關檢測，因此，除了使用者需注意並維持行動裝置的安全外，開發者亦必須針對所開發之 APP 進行全面之檢測，以避免因程式碼撰寫或安全性未落實等原因，造成使用者的不安全。並且為了提升自身 APP 之安全性以及提供使用者信任，建議可尋求相關資安檢測實驗室進行 APP 的驗證，除可以協助提高其安全外，亦可讓使用者能放心使用該 APP。

twcertcc

2019 台灣電腦網路危機處理暨協調中心資安年報

第三章

情資分享與漏洞協處

為降低資安之威脅以及影響範圍，TWCERT/CC 透過接收國內外資安通報外，同時亦進行跨域資安情資分享，完善國內情資分享與協處，更提供靜態及動態之惡意檔案檢測服務，以及資安漏洞通報服務，強化國內資安防衛能量。

第一節、TWCERT/CC 資安情資分享

在 2019 年 1 月至 12 月期間，TWCERT/CC 總計分享逾 110 萬筆之資安情資予相關單位進行處理，包括來自國際、欲針對國內 IP 位址進行協處與警示的通報，以及來自國內、欲針對國內其他單位或國際 IP 位址進行協處與警示的通報。情資來源主要為包括 13 個國際資安交流組織、國內資安相關組織，以及各國 CERT 組織，而國內分享對象主要包括政府單位、網路業者、金融單位、學術單位、台灣駭客協會 (HITCON) 等資安組織，以及諸多國內企業，國外分享對象為 117 國家的 CERT/CSIRT 組織及其他相關資安組織。此外，為提升情資警示及分享效率，更透過系統的優化，與國家資安資訊分享與分析中心 (National Information Sharing and Analysis Center, N-ISAC)、AIS(Automated Indicator Sharing)、APWG 等國內外資安組織介接，定期並即時分享駭侵事件、產品漏洞及資安預警等資安情資，縮短處理情資來源時程，提升情資分享效能。

一旦接收來自國際的通報，此來源往往係針對國內之 IP 位址，因此會檢閱其國內 IP 位址所屬對象後，告知相關權責單位進行處理；而來自國內的通報，大部分均屬針對國際 IP 位址的通報事件，少部分為國內其他單位之 IP 位址，因此，將會針對其通報之 IP 位址進行確認，一旦確認該位址屬於他國，則告知該國 CERT 組織或該 IP 位址所屬之單位進行處理。如此，除了可建立跨境資安通報橋樑外，更可針對欲通報對象，進行精確之聯繫及處理，以達到提升國內資安防護及協處能量之目標。

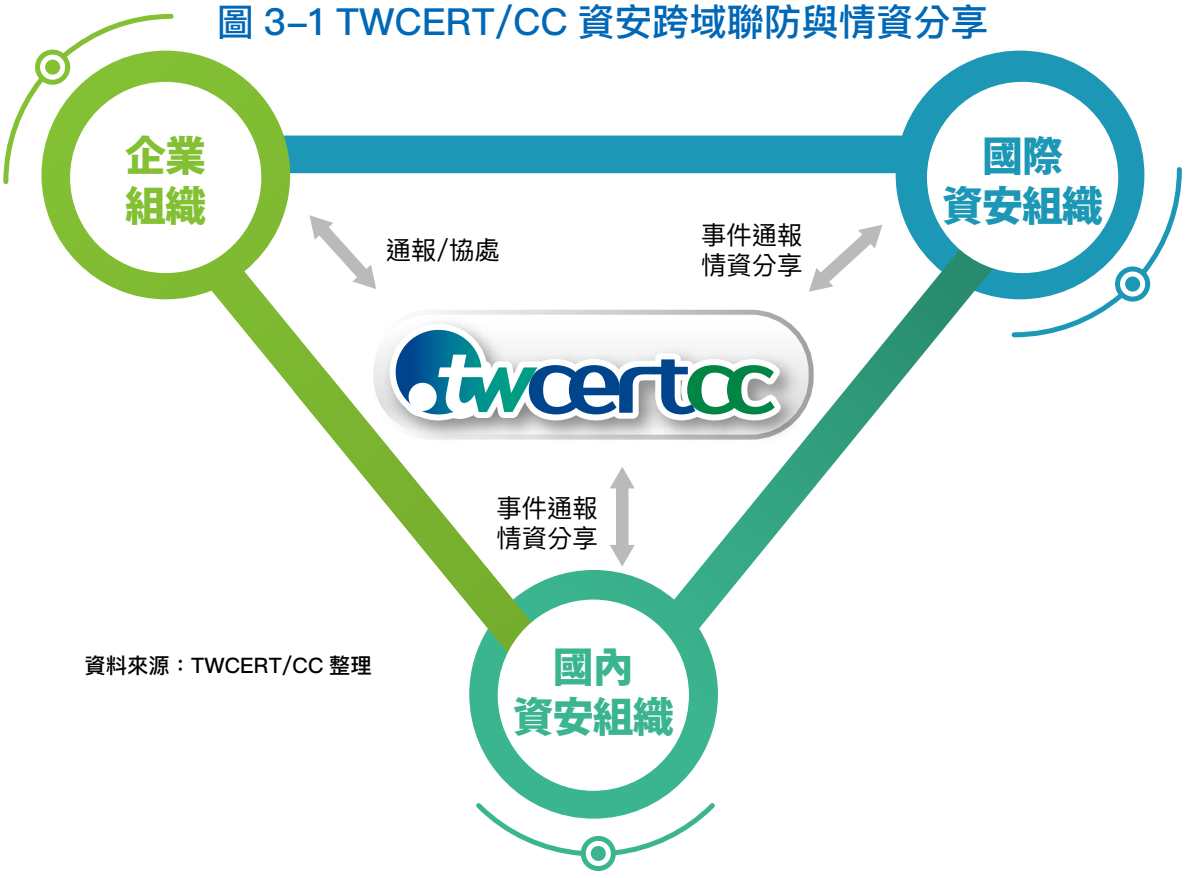
在 TWCERT/CC 所接獲並進行通報的情資中，以接收國際情資後分享情資至國內相關單位之數量為大宗。而接收國內情資，將國內發現或資安資訊分享至國外的情資數量中，其通報的國家眾多，以區域網際網路註冊機構 (Regional Internet Registry, RIR) 管理區域區分，最多的為屬於亞洲及太平洋地區國家之亞太網路資訊中心 (Asia Pacific Network Information Centre,

APNIC)，其次為屬於歐洲、中東、中亞地區之歐洲網路資訊中心(R seaux IP Europ ens Network Coordination Centre, RIPE NCC)，第三則為屬於北美、南極洲等地區之美洲網際網路位址註冊組織(American Registry for Internet Numbers, ARIN)，接著依序為拉丁美洲及加勒比地區網際網路地址註冊管理機構(Latin America and Caribbean Network Information Centre, LACNIC)及非洲網路資訊中心(African Network Information Centre, AFRINIC)其詳細比例如圖 3-2：

在逾 110 萬筆之情資中，TWCERT/CC 會針對其攻擊類型及方式進行區分，並提供給相關單位，除了方便相關單位針對該事件類型進行處理外，同時也易於後續統計分析，提供未來資安威脅預警之用。

其主要通報類型，主要分為受害者系統被駭客入侵、受害主機被當作殭屍電腦進行惡意行

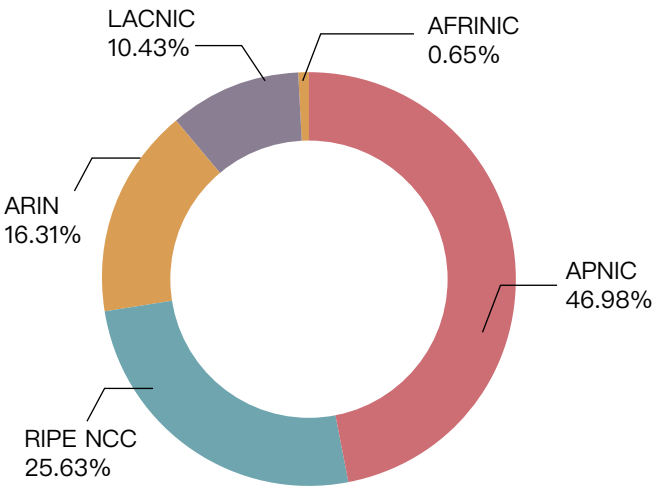
圖 3-1 TWCERT/CC 資安跨域聯防與情資分享



資料來源：TWCERT/CC 整理

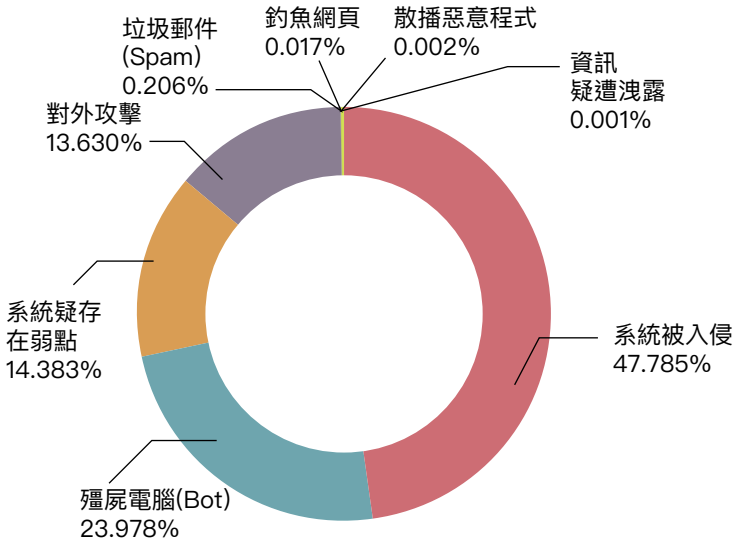
為、系統被發現存在可能會遭駭客利用之弱點，以及可能遭利用對外攻擊等類型。在眾多類型中，接獲並通報的資安事件類型比例最高者為系統被入侵，其次則為殭屍電腦，第三為系統疑存在弱點，其詳細比例如圖 3-3：

圖 3-2 TWCERT/CC 國際資安情資分享比例



資料來源：TWCERT/CC 整理

圖 3-3 TWCERT/CC 通報事件類型比例



資料來源：TWCERT/CC 整理

第二節　Virus Check 惡意檔案分析

為協助民眾檢測潛藏於檔案中之惡意程式，以及減少機敏資料外洩問題，TWCERT/CC、國家高速網路與計算中心及趨勢科技攜手合作，建置惡意檔案檢測服務系統 Virus Check[1]。並且為提升大眾使用效能及滿意度，已根據相關使用回饋及系統檢視，進行使用者介面改善、程式碼修改及壓力測試，提供以使用者為導向的檢測系統平台，並於 2019 年 7 月中旬上線開放予大眾使用。

Virus Check 可透過靜態及動態的惡意程式檢測方式，達到全方位的檢驗，與防毒軟體相輔相成，強化檔案安全檢測。靜態分析是透過研究並分析程式碼內容，找出其中唯一的程式碼作為辨識特徵之病毒碼，搭配防毒軟體中之掃描功能，方能自電腦或檔案中，確認是否有惡意程

圖 3-4 惡意檔案檢測服務 Virus Check

資料來源：[1]

1　TWCERT/CC. “惡意檔案檢測服務Virus Check” ： https://viruscheck.tw （瀏覽日期：2019年7月16日）

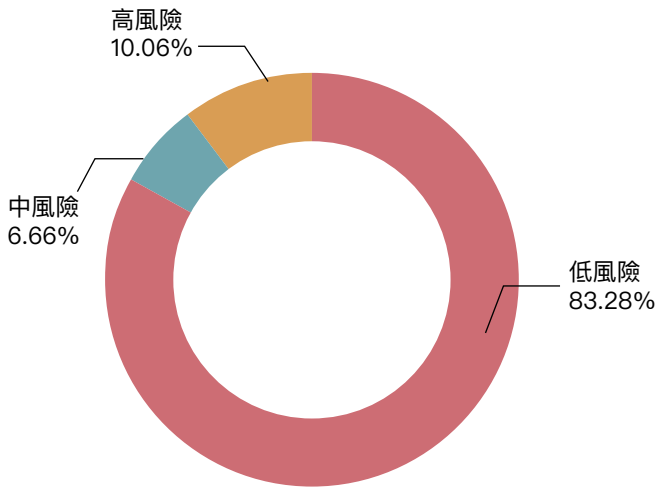
式潛藏於其中。

相對於透過特徵值分析惡意程式的靜態分析方法，動態分析方法是將惡意程式置於一個幾乎外部隔絕的沙箱 (SandBox) 環境中，觸發惡意程式實際執行，觀察並紀錄該惡意程式的行為。動態分析本身是著重於惡意程式執行時的行為觀察，即便駭客將惡意程式的程式碼進行更動，則因其執行時仍然進行對受害電腦產生影響的惡意行為，因此不會被混淆分析，仍然可以判斷出該程式為惡意程式。

因此，Virus Check 系統能夠有效將靜態分析與動態分析結合，並與國家實驗研究院高速網路與計算中心及趨勢科技合作，以全面且完整地對檔案進行檢測，減少惡意程式對使用者的威脅。

在此系統中，使用者可將系統接受之檔案類型上傳，系統會將檔案透過靜態及動態檢測，並於短時間內即可產出初步報告，若該檔案被系統判定為風險值較高，則會進行深度檢測，提

圖 3-5 Virus Check 檔案檢測風險值比例



資料來源：TWCERT/CC 整理

供檢測報告，供使用者下載。

此系統除可提供使用者隨時檢測檔案是否有惡意程式感染，更可建立國內專屬之惡意程式資料庫，為國內資安廠商防護情資來源之一。

從開放大眾使用開始的約半年期間，總計收到數千筆的上傳檔案，在 Virus Check 系統初步檢測中，多數為低風險的檔案，其次為高風險檔案，詳細比例如下：

除此之外，為了提高台灣整體資安防護能量、減少感染惡意程式之風險，除了不要下載來路不明之檔案，對於下載之檔案，最好透過檢測系統完整分析，避免電腦遭到惡意程式之威脅。台灣資安能量，需要大家共同參與和努力。

第三節 資安漏洞協處

一、我國產品漏洞概況

TWCERT/CC 參與美國非營利組織 MITRE 之 CVE 計畫，擔任台灣區 CVE 編號管理者 (CVE Numbering Authorities, CNA)，接收、審核及發布資安漏洞 CVE 編號，以降低資安漏洞對使用者及廠商所可能帶來的威脅。

2019 年期間，總計接獲逾 10 項產品、超過 25 個漏洞之資安通報，其漏洞類型涵蓋網通產品、物聯網裝置以及軟體服務系統。對於因 MITRE 資安漏洞因規範，無法取得 CVE 編號者，亦會提供 Taiwan Vulnerability Note (TVN) 編號予通報者，並在確認漏洞修補完畢後進行公開。

在 2019 年間，TWCERT/CC 接獲並發布之 CVE 統計如下表：

表 3-1 TWCERT/CC 審核發布 CVE 統計表

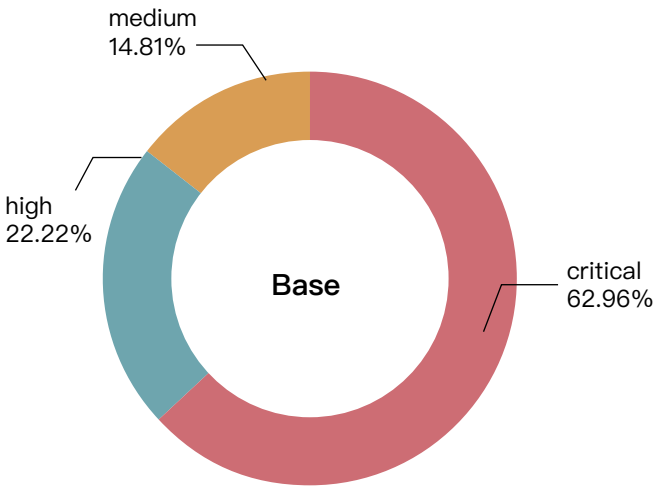
公開日期	CVE	CVSS分數	嚴重等級	漏洞類型	產品類型
2019-05-09	CVE-2019-9882	8.8	High	郵件歸檔稽核系統的 CSRF 漏洞，導致攻擊者可以修改白名單	網通產品
2019-05-09	CVE-2019-9883	8.8	High	郵件歸檔稽核系統的 CSRF 漏洞，導致攻擊者可以使特定帳號取得管理權限	網通產品
2019-07-02	CVE-2019-11062	9.8	Critical	數位學習平台含有 Command Injection 漏洞	軟體服務系統
2019-07-02	CVE-2019-9886	9.1	Critical	校園綜合平台含有任意檔案下載漏洞	軟體服務系統
2019-07-25	CVE-2019-9884	9.8	Critical	校園綜合平台含有存取控制缺陷漏洞	軟體服務系統
2019-07-25	CVE-2019-9885	9.8	Critical	校園綜合平台含有未經授權的 SQL Injection 漏洞	軟體服務系統

2019-08-21	CVE-2019-11060	7.4	High	智慧管家含有未被控制的資源消耗漏洞	物聯網裝置
2019-08-21	CVE-2019-11061	10.0	Critical	智慧管家含有存取控制缺陷漏洞	物聯網裝置
2019-08-21	CVE-2019-11063	10.0	Critical	智慧家庭App 含有存取控制缺陷漏洞	物聯網裝置
2019-08-21	CVE-2019-11064	9.8	Critical	網路攝影機存在遠端管理員帳號與密碼揭露漏洞	物聯網裝置
2019-08-21	CVE-2019-13405	9.8	Critical	網路攝影機存在遠端任意啟動 Android Debug Bridge 漏洞	物聯網裝置
2019-08-21	CVE-2019-13406	7.5	High	網路攝影機存在遠端任意安裝APK漏洞	物聯網裝置
2019-08-21	CVE-2019-13407	6.1	Medium	網路攝影機存在反射型XSS	物聯網裝置
2019-08-21	CVE-2019-13408	7.5	High	網路攝影機存在任意檔案下載漏洞	物聯網裝置
2019-09-25	CVE-2019-15067	9.8	Critical	智慧行動電源存在不安全的驗證機制	物聯網裝置
2019-09-25	CVE-2019-15068	9.8	Critical	智慧行動電源存在權限控制缺陷	物聯網裝置
2019-09-25	CVE-2019-15069	9.8	Critical	智慧行動電源存在不安全的驗證機制	物聯網裝置
2019-10-17	CVE-2019-13409	9.8	Critical	行動視訊會議系統含有 SQL Injection 漏洞	軟體服務系統
2019-10-17	CVE-2019-13410	7.5	High	行動視訊會議系統含有機敏資料暴露漏洞	軟體服務系統
2019-10-17	CVE-2019-13411	10.0	Critical	光纖通訊網路 3097 埠允許遠端執行任意指令	網通產品
2019-10-17	CVE-2019-13412	9.3	Critical	光纖通訊網路 3097 埠允許攻擊者透過特定指令讀取任意檔案	網通產品
2019-10-17	CVE-2019-15064	9.8	Critical	光纖通訊網路含有存取控制缺陷漏洞	網通產品
2019-10-17	CVE-2019-15065	9.3	Critical	光纖通訊網路 6998 埠允許攻擊者透過特定指令讀取任意檔案	網通產品
2019-10-17	CVE-2019-15066	10.0	Critical	光纖通訊網路 6998 埠允許遠端執行任意指令	網通產品
2019-11-20	CVE-2019-15071	6.1	Medium	電子郵件系統頁面下存在 XSS 漏洞	軟體服務系統
2019-11-20	CVE-2019-15072	6.1	Medium	電子郵件系統登入頁面下存在 XSS 漏洞	軟體服務系統
2019-11-20	CVE-2019-15073	6.1	Medium	電子郵件系統頁面下存在 Open Redirect 漏洞	軟體服務系統

在發布的眾多漏洞中，透過 MITRE 的漏洞評鑑系統 (Common Vulnerability Scoring System, CVSS) 針對漏洞進行嚴重性等級的評判，並以數字方式呈現該漏洞之嚴重性，再佐以低 (Low，0.1~3.9)、中 (Medium，4.0~6.9)、高 (High，7.0~8.9) 以及嚴重 (Critical，9.0~10.0) 四種等級區分，以協助使用者或相關組織評估該漏洞之修復優先等級。在所有漏洞中，其基本矩陣群組 (Base Metrix Group) 數值平均為 8.8 分，在 0 至 10 分之級距中數值偏高，即表示這些漏洞有一定之嚴重性，使用者或相關組織必須針對 TWCERT/CC 及 CVE 網站上所發布之訊息進行漏洞處理，避免因資安漏洞遭受攻擊。2020 年上半年期間 CVE 漏洞嚴重等級統計如圖 3-6 ：

為了降低國內資安漏洞所帶來的威脅，TWCERT/CC 透過 TVN 及 CVE 編號供廠商、組織或使用者進行資安漏洞檢視，避免因漏洞而蒙受損失。在此環節中，所有角色均環環相扣，必須有辛勤且高技術能量的通報者，積極配合、努力修補產品漏洞的廠商，以及接獲情資後配合廠商進行漏洞修補的相關組織，如此，方能大幅提升國內資安漏洞防護之能量。

圖 3-6 CVE 漏洞嚴重等級統計



資料來源：TWCERT/CC 整理

二、跨域漏洞協處

1. NAS 產品遭資安威脅

2019 年 7 月期間，TWCERT/CC 接獲國內廠商情資，表示全球各地陸續有 NAS (Network Attached Storage) 產品資料遭遇加密勒索事件，其手法為駭客暴力破解預設帳號及密碼，取得管理員權限後，將檔案加密並對受害者勒索贖金。

在了解全盤狀況後，TWCERT/CC 隨即協助該廠商針對此資安威脅事件進行國際協處工作。收集各種資訊、依據 IP 對應位置，通知該國 CERT 協助撤下中繼站，並建議下列強化措施及進行宣導：

(1) 啟用防火牆功能，僅在必要時開啟對外網路埠。

(2) 啟用雙重驗證機制，阻斷惡意來源嘗試登入的可能。

(3) 停用系統預設的「Admin」帳號。

(4) 使用強度較強的密碼，並啟動密碼強度限制規則。

(5) 啟用自動封鎖來阻擋嘗試登入次數過多的 IP。

(6) 啟用多版本備份，將 NAS 中的檔案備份至本地、遠端、公有雲等地，並在過程執行安全加密，限制存取權限。

(7) 執行安全性諮詢為系統做完整的安全性評估。

廠商後續回報受攻擊用戶數量明顯趨緩，有效遏止事件擴散，本次與國際資安組織展開合作協處工作並順利完成，有效遏阻全球 NAS 勒索事件擴散。

2. 虛擬私人網路 (Virtual Private Network, VPN) 資安漏洞

2019 年 8 月期間，TWCERT/CC 接獲國際資安組織通報，有駭客組織利用 Pulse Connect Secure VPN 的 CVE-2019-11539 資安漏洞進行大規模掃描攻擊，針對國內多個政府單位、法人、ISP 業者、企業及學術單位等有使用該 VPN 產品之組織進行攻擊及威脅。

在接獲通報後，立即與通報方進行接洽，告知可以針對此次資安事件進行受影響單位進行通報及建議其處置方式，請對方提供該公司所檢測到使用該 VPN 產品的所有 IP，以利後續通報作業。

而通報方總計提供 217 個使用 Pulse Connect Secure VPN 產品之相關 IP，TWCERT/CC 立即針對所有 IP 查詢其所對應之單位或組織，並找出相對應的資安管理者及聯繫方式，以加速溝通及儘速解決該資安事件。

經緊急處理，通報使用該 VPN 產品的 6 個政府單位、11 所學術單位、9 個 ISP、7 個企業及 2 個法人單位，共計 35 個相關單位，建議使用單位需針對該 VPN 產品進行產品的升級，以避免遭到大規模掃描攻擊而造成損失。

此事件中，TWCERT/CC 為國內企業資安事件通報窗口，作為國內與國際組織的溝通橋樑，彙整國內外之情資並予以進行通報，以達到全球化的資安聯防，減少資安事件損失，並提升整體資安防禦能量。

3. 晶片韌體資安漏洞

TWCERT/CC 接獲國際組織通知，國內某積體電路 (Integrated Circuit, IC) 設計大廠所設計之晶片韌體含有資安漏洞，由於通報方為國際組織，較難順利與目標廠商建立確切之聯繫管道，因此詢問是否能協助建立兩方之溝通橋樑。

經努力與廠商溝通，並獲得其信任後，提供國際組織所發現之相關漏洞資訊，請廠商儘速修補可能因系統開發過程中設計不良導致的資安漏洞。

廠商獲得漏洞情資後，在三方協作下，迅速完成漏洞修補，並對其客戶發布安全更新檔，避免因該漏洞而造成資安問題之範圍擴散，進而影響公司商譽。MITRE 也已於 2019 年 5 月 13 日公開該晶片韌體漏洞共 8 個 CVE 編號，本次 TWCERT/CC 充分展現協調中心的角色，協助國內科技產業解決產品資安漏洞。後續 TWCERT/CC 將利用推廣活動及社群媒體，將成功案例對國內企業說明，建立企業對 TWCERT/CC 之信任度。

三、資安漏洞協處案例

1. 郵件稽核系統具跨站請求偽造 (Cross-Site Request Forgery, CSRF) 漏洞

2019 年 3 月中旬，TWCERT/CC 接獲某郵件稽核系統之資安漏洞通報，通報者表示該系統存有 CSRF 漏洞，可能致使攻擊者透過該漏洞進行相關資訊及設定之竄改。

在收到該通報後，立即與通報者進行聯繫及確認相關詳細內容，並彙整該系統之相關資訊及漏洞資訊，也針對通報者之請求，檢驗並確認該漏洞是否適於申請 CVE 編號。同時亦儘速與廠商進行接洽，將所整理之相關資訊告知該廠商，並請對方儘速修補漏洞。

經 TWCERT/CC 與廠商和通報者三方積極聯繫及溝通，在廠商告知已修補完畢後，隨即將該資訊告知通報者，請求通報者針對其所通報之系統漏洞進行複測，以確保該系統達到完整的修補。

通報者確認已完成漏洞修補後，立即將該漏洞資訊公告於 TVN 網站中，提醒相關系統的使用者進行系統更新，若使用者未對 CSRF 攻擊進行相關防護，則可能因該漏洞受到攻擊而竄改資

訊等惡意行為。同時也提醒使用者為了減少該漏洞所產生之資安威脅，請配合該廠商進行相關模組及系統的更新，方能減少相關漏洞所造成的影響及損失。

經過驗證，該漏洞共可申請 CVE-2019-9882 及 CVE-2019-9883 兩個編號，並完成 MITRE CVE List 更新。

此次事件中，TWCERT/CC 作為企業與通報者之間的溝通橋樑，減少企業對通報者不信任或通報者難以直接對企業進行聯繫之問題，並蒐集彙整相關資訊，讓企業在收到 TWCERT/CC 提供的訊息和建議後，能儘快針對其產品或系統中的漏洞進行修補，以防止企業及其使用者因資安漏洞而蒙受損失，提升國內之相關資安防護能量。此外，作為台灣區之 Root CVE，可接受個人或組織之任何資安通報，可在 TWCERT/CC 及 MITRE 同時公告下，達到最佳的提醒成效。

2. 網路自動櫃員機 (Web Automated Teller Machine, Web ATM) 元件具 DLL Hijacking 漏洞

2019 年 3 月，TWCERT/CC 接獲通報某金融單位之 Web ATM 元件，因使用已遭公告具有資安漏洞之開源打包軟體 NSIS (Nullsoft Scriptable Install System)，使得該單位之 Web ATM 出現 DLL 劫持 (Dynamic Link Library Hijacking) 漏洞。

NSIS 是一款受歡迎之 Windows 開源打包軟體，用以包裝及發布程式執行檔，由於其具有高自訂性及使用簡潔，因此已被相當多的應用程式所運用。然而，該打包軟體已被公告具有 DLL Hijacking 的資安漏洞，並無針對其載入的函式庫進行相關資安保護機制，導致該金融單位因使用該軟體，而產生了相關之系統漏洞。

收到通報後，立即通報該金融單位，並搭建通報者和該金融單位之溝通橋樑，透過彼此提

供之資訊進行彙整分析，以及對該金融單位之可能資安問題進行建議，並更新其元件以修補資安漏洞。

此外，為防止使用者因該漏洞遭到資安攻擊，已於 TVN 網站進行相關漏洞及修補之公告，而該金融單位亦於該單位網站上公告提醒使用者，請使用該 Web ATM 的使用者從其官方網站上下載新元件進行更新。

除該金融單位外，針對 NSIS 之使用者，亦於 TVN 網站中提醒相關使用者儘速進行更新，並透過新版之 NSIS 軟體將其打包及發布之應用程式進行重新打包，以避免使用 NSIS 之相關系統或應用程式仍有 DLL Hijacking 資安漏洞。

3. 學習管理平台具命令注入漏洞

於 2019 年 5 月下旬，TWCERT/CC 接獲通報某廠商開發之學習管理平台，在通報者檢測後發現該產品存有命令注入漏洞 (Command Injection)，讓攻擊者可透過該漏洞執行任意指令及上傳 webshell，對該系統造成嚴重之影響。

收到該通報後，發現使用該產品相關單位分佈較廣，因此立即將該情資通報給政府、學術、金融資安組織及受漏洞影響之企業，請針對該攻擊進行相關防護。

除了進行資訊之通報外，已將該系統和漏洞之相關資訊進行彙整和分析後，儘速將情資通報給該平台廠商，並與該廠商之研發總監聯繫及溝通、提供相關的修補建議，請求對方盡快針對該漏洞進行修補，避免該產品遭到攻擊者利用該漏洞造成其嚴重的損失。

經過廠商修補及通報者數次複測，在 6 月中旬接獲通報者告知其相關漏洞均完成修補，並在進行嚴謹之檢測後，亦確認該系統及所有受影響之單位均已修補完畢。同時取得 CVE-2019-

11062 編號，並於 TVN 和 MITRE CVE 網站公告該漏洞相關資訊，提醒相關使用者儘速將該系統版本升級，以達到較完善之資安防護。

此次事件中，TWCERT/CC 作為國內之資安通報協調中心，在收到任何資安情資後，會確認其影響範圍，並將該情資通報給相關單位或資安組織，降低使用者因資安漏洞所受到之影響及損失，提升企業對資安問題的重視和防護，完備國內之資安能量。

twcertcc

2019 台灣電腦網路危機處理暨協調中心資安年報

第四章

合作交流與資安推廣

為掌握資安發展趨勢，增加互助合作對象，TWCERT/CC 透過積極參與國際重要資安會議、跨國網路安全演練及實務經驗交流等活動，強化資安協處效率，更可拓展我國能見度，提升整體國內外資安聯防能量。

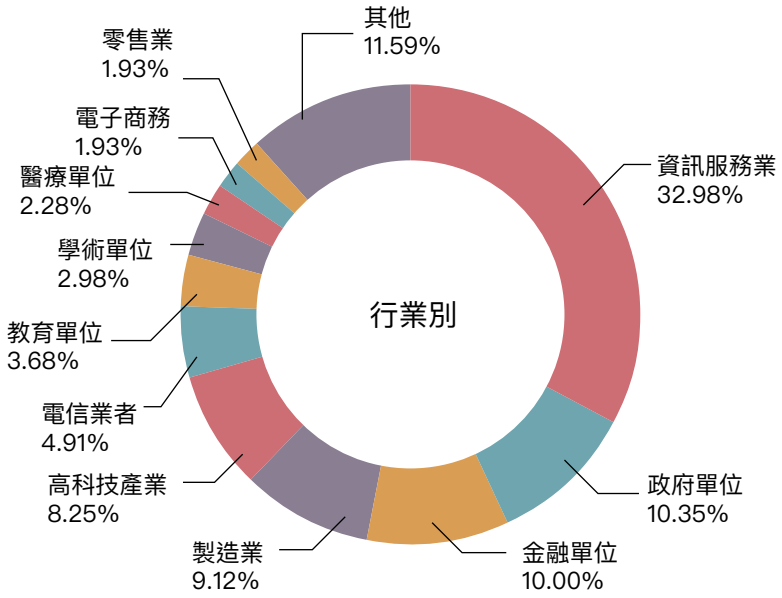
第一節、主辦活動

一、台灣資安通報應變年會

為提升國內企業及組織的資安意識，TWCERT/CC 主辦台灣資安通報應變年會，用以強化資安通報流程及相關協處作業。在此活動中，特請國家通訊傳播委員會鄧惟中委員、國家安全會議廖述煌主任、行政院資通處簡宏偉處長、澳大利亞 CERT 組織 AusCERT (Australia's Pioneer Cyber Emergency Response Team) 代表 Geoffroy Thonon、美國在台協會 (American Institute in Taiwan,

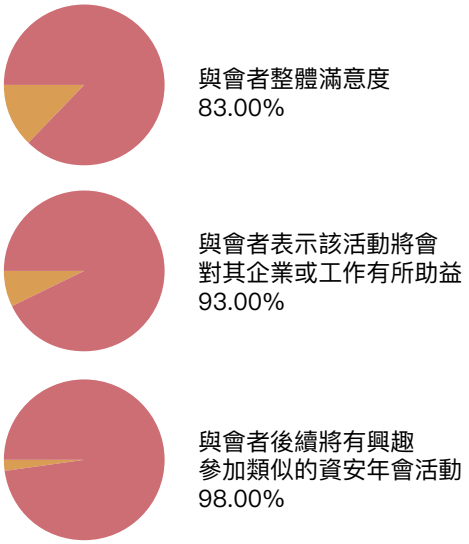
圖 4–1 2019 台灣資安通報應變年會 – 貴賓合影。**資料來源：TWCERT/CC 整理**

圖 4-2 活動與會者行業別分析



資料來源：TWCERT/CC 整理

圖 4-3 與會者回饋問卷統計分析



資料來源：TWCERT/CC 整理

AIT) 代表 Engen Ryan、趨勢科技 方家慶研究員、IBM 李承達專家等產官界貴賓蒞臨指導、案例分享，參展廠商 15 家，與會人數共約 420 人。

在眾多與會來賓中，以資訊服務業為大宗，佔總人數 32%，其依序為政府單位、金融單位、製造業及高科技產業等。

此外，根據回饋問卷統計，針對 2019 台灣資安通報應變年會，與會者整體滿意度達 83%，其中約有 93% 的與會者表示該活動將會對其企業或工作有所助益，更有 98% 的與會者表示後續將有興趣參加類似的資安年會活動。

而從整體統計分析顯示，此次台灣資安通報應變年會確已達到擴散資安意識、提升品牌認

知，以及增添資安通報意願之目的。

並且於此次會議中，TWCERT/CC 與 AusCERT 代表進行合作備忘錄 (Memorandum of Understanding, MoU) 交換儀式，提升國際間的情資共享及資安聯防能量，同時也提升台灣在國際資安組織間的參與度，加深企業對 TWCERT/CC 的信賴程度，增進協同合作的機會及品質，優化國內的資安應變能力。

圖 4–4 AusCERT 與 TWCERT 交換合作備忘錄。**資料來源：TWCERT/CC 整理**

二、台灣 CERT/CSIRT 聯盟交流會議

為有效強化資安防禦體系，即時網路安全情資交流，TWCERT/CC 進行召集，與由產、官、學等共計 25 個單位會員，共同組成「台灣 CERT/CSIRT 聯盟」，以提升國內資訊安全之聯合防護能量。並且為提升各單位之防護能量，此聯盟定期召開「台灣 CERT/CSIRT 聯盟」交流會議，成員彼此分享國內外資安情資及資安事件協處實務經驗。

於 2019 年 7 月中旬，召開 2019 年度第一次聯盟交流會議，邀請台灣駭客協會邱銘彰理事以「AI Security」為核心概念進行專題分享，使大眾在這人工智慧時代中，更了解其資安威脅及防禦機制。此外，也邀請與會成員進行資安通報協處案例及成果經驗分享，讓彼此都能學習更多的執行模式及資安情資，相互交流並強化國內資安聯防體系之防禦能量。

在 2019 年 11 月中旬，召開了 2019 年度第二次聯盟交流會議，並邀請 HITCON ZeroDay 翁浩正總召，以「台灣資安漏洞趨勢」為主題進行探討及提供相關處置建議，降低資安漏洞對國內政府、學術及企業單位所帶來的威脅。此外，也邀請與會者進行資安通報協處案例及成果經驗分享，提升聯盟會員間的資安情資分享、資安能量互通，建立資安單位間的良性交流循環，進而達到強化國內資訊安全環境之目的。

第二節、國際交流

一、參與 FIRST 年會

事件處理與資安小組論壇 (The Forum of Incident Response and Security Teams, FIRST) 是全球最大的資安事件通報應變及安全組織，主要為協調國際間 CERT/CSIRT 組織，進行國際資安情資交流，研擬資安共通規範。

在 2019 年中旬 FIRST 在英國愛丁堡召開第 31 次年會，超過 80 個國家、1,100 名資安相關人員與會。此會議中，其議程分為事件處理 (Incident Response)、管理 (Management) 及技術 (Technical) 三部分，另提供高達百場的資安會議與工作坊，TWCERT/CC 組長林志鴻博士亦於該大型國際會議中進行演講，發表其資安威脅研究，分享台灣的資安防護經驗。

此次與會，透過國際大型會議的交流及分享，掌握最新資安技術與趨勢，借參與資安討論會議，與其他 CERT 組織建立直接聯繫管道，提升未來情資交流及協同合作效率，強化跨域資安聯防能量。

圖 4-5 林志鴻博士於 FIRST 年會報告概況。**資料來源：TWCERT/CC 整理**

二、參與 APCERT 年會

亞太區電腦網路危機處理小組 (Asia Pacific Computer Emergency Response Team, APCERT)[1] 為亞太地區 CERT 組織重要聯盟，於 2003 年創立，邀集位於亞太地區的國家或企業 CERT 組織參與，用以建立亞太區 CERT 組織間的穩定情資分享、事件通報及事件協處配合，形成具成效的區域性電腦網路應變組織，促進資安事件處理的合作與發展。

於 2019 年下旬，參與由新加坡電腦網路危機處理小組 (The Singapore Computer Emergency Response Team, SingCERT) 主辦之 APCERT Conference 2019。在此年會中，針對 APCERT 的八個工作小組 (Working Group, WG) 進行年度狀況說明及未來規劃，並由成員 CERT 組織報告其該年度之資安事件趨勢和處理情形，提供協處經驗予其他成員參考並學習。

圖 4–7 丁綺萍副執行長於 Working Group 交流概況。**資料來源：TWCERT/CC 整理**

圖 4–6 APCERT Conference 2019 全體合照。**資料來源：[1]**

1 SingCERT. APCERT 2019. Retrieved October 2, 2019, from the World Wide Web: https://www.apcert2019.sg

三、參與亞太區國際網路安全攻防演練

APCERT 每年舉辦一次年會，讓眾成員國或成員組織彼此共享 CERT 運營、事件協處經驗、資安情資等資訊，相互交流以提升亞太地區整體資訊安全。

於 APCERT 中，有諸多由多個 CERT 成員國所建立的工作小組，彼此進行不同的資安項目計畫，透過成員加入後彼此合作，達成單一成員難以完成的作業。其中，APCERT Drill 工作小組會於每年舉辦資安演練，在選定主題後由各成員建立演練的題目，並且以此演練當該主題事件發生時，各成員該如何應對、通報及協處，以將其威脅將至最低。

在 2019 年的資安演練中，其主題為「企業網路的無聲災難性資源耗損 (Catastrophic Silent Draining in Enterprise Network)」，該情境模擬當有企業的伺服器因含有漏洞，導致被攻擊者入侵，更遭攻擊者透過該伺服器寄送帶有惡意程式的釣魚郵件給不知情的受害者，因此該企業欲尋求 CERT 組織的協助。而所有參與演練之成員須針對其層層題目進行檢閱、解析及協處，進而提升成員的協處能量及應變能力，當真實事件發生時可大幅降低事件所帶來的影響。

TWCERT/CC 於此次演練中，擔任玩家及觀察者的角色，並根據此次模擬金融企業遭攻擊者透過 CVE-2018-7600 漏洞，入侵內部數位學習平台後取得權限，並利用員工個資寄送釣魚郵件之相關情境，進行資安事件協處及經驗累積。而此情境共計五個階段、七種不同的攻擊手法，整體演練時間共計約三個小時。

透過此次演練活動之參與，除了增加於國際間之能見度之外，更可透過彼此討論、交流，建立與 APCERT 其他成員之間的互信基礎，以及透過演練的經驗與學習，優化 TWCERT/CC 的國際通報協處的效率及能量。

四、參與 APNIC 48 年會

亞太網路資訊中心 (APNIC) 是負責掌管亞太地區的 IP 位址和 AS 編號發放的機構。而該機構會定期召開會議，進行網路管理的技術及意見交流，對 IP 位址及 AS 號碼的相關政策進行探討，以更加深入且優化其政策。

此次 APNIC 48 會議是於 2019 年下旬，在泰國清邁舉行，其內容涵括網際網路維運、技術及發展等，進行經驗的分享及現況報告，以深入了解亞太地區各國的網際網路發展及運作狀況與政策。

在此會議中，TWNIC 暨 TWCERT/CC 董事長黃勝雄博士主持進行 IPv6 部署及相關資訊之 IPv6 Deployment 會議研討，針對亞太地區各國 IPv6 部署、狀態及經驗進行分享及探討。而 TWNIC 暨 TWCERT/CC 副執行長丁綺萍則負責主持網際網路問題探討及治理之 Cooperation SIG 專題演講，探討包括網路與管轄權、IP 位址與網路司法關係等議題。

圖 4–8 黃勝雄董事長主持 IPv6 Deployment 場次。**資料來源：TWCERT/CC 整理**

圖 4–9 丁綺萍副執行長主持之 Cooperation SIG 場次。
資料來源：TWCERT/CC 整理

第三節、國內交流

一、亞太資安論壇

於 2019 年 5 月初，TWCERT/CC 組長林志鴻博士參與亞太資安論壇，講述網路威脅新事態與跨域聯防資訊。

隨著網際網路的蓬勃發展，資安攻擊事件及網路犯罪層出不窮，其對企業及個人所造成的損失不斷增加，因此，資訊安全逐漸受到人們的重視，許多廠商也紛紛推出資安防禦設備，提供使用者或企業更多的安全防護機制與能量。然而，如何將建置的資安防禦系統從「有做」轉為「有效」，是相當重要的一個議題。

圖 4–10 林志鴻博士於亞太資安論壇報告概況。**資料來源：TWCERT/CC 整理**

為了讓防禦系統真的「有效」，應思考該防禦系統究竟是「治標」還是「治本」？要防禦何種類型的攻擊？攻擊樣態是否改變？偵測規則為何？等等問題，以及最重要的是攻擊來源是否有透過相關單位處理。此外，諸多資安防禦都牽涉到跨域聯防，必須透過多組織、多國之間的互助，方能達到最佳的防禦效果。而 TWCERT/CC 與國際許多資安組織均有合作關係，因此可透過這些組織掌握第一手的資安資訊，達到跨域聯防的重要效益。並且如若國內企業或組織遭到境外 IP 攻擊，亦可通報資安事件，會將資訊去識別化後轉給國際相關單位進行處理，以便從源頭杜絕資安事件的發生及影響。

在 2019 年第一季，TWCERT/CC 已通報逾 20 萬餘筆情資，並提供相關資安警訊情資。此外，針對資安漏洞部分，TWCERT/CC 目前為 MITRE 的 Root CNA，為 MITRE 組織認證之 CVE 編號授權及發放單位，可對資安漏洞進行審核並發放 CVE 編號。若未來有任何漏洞欲取得 CVE 編號者，不需透過美國 MITRE 進行通聯及審核，可直接通報 TWCERT/CC 進行審核，並於確認後發放 CVE 編號。

二、2019 Cyberspace 聯合研討會

於 2019 年 10 月中旬，TWNIC 暨 TWCERT/CC 副執行長丁綺萍與 TWCERT/CC 組長林志鴻博士參與 2019 Cyberspace 聯合發表會。該活動分為 Workshop 及研討會議程，研討會由丁綺萍副執行長作為開幕嘉賓致詞，林志鴻博士則於 Workshop 議程中講述資安重點威脅與跨域聯防相關資訊。

該活動以數位創新、數位健康與智慧城市為主題，針對現今連網普及的數位環境，提供可能的資安威脅情境分享，並闡述當前國內與國際跨域聯防的合作狀況及發展，企盼增加國內資安防禦及聯防能量。

圖 4–11 Cyberspace 2019 聯合研討會開幕。
資料來源：TWCERT/CC 整理

圖 4–12 Workshop 實務分享現場。
資料來源：TWCERT/CC 整理

TWCERT/CC 透過本次活動的參與，分享當前與國際間情資交換現況，並透過相關情資說明區域聯防與推廣資安通報的重要性，期待透過企業及相關單位的積極通報，降低國內資安事件風險，同時提供大眾與企業對資安威脅的認知，共同提升國內資安防禦能量。

三、2019 HITCON Defense Summit 企業安全會議

於 2019 年 11 月中旬，TWCERT/CC 組長林志鴻參與 HITCON DEFENSE Summit 企業安全會議。此活動主要是針對諸多企業常見的資安問題進行探討，並邀請多位資安專家及產品顧問，進行經驗分享與交流，以提升諸多企業的資安防護意識及防護能量。

圖 4–13 林志鴻博士於 HITCON Defense Summit 演講概況。**資料來源：TWCERT/CC 整理**

而 TWCERT/CC 組長林志鴻博士也於此活動中，闡述資安威脅與防禦的趨勢與防護建議，讓與會人員對企業資訊安全有更深入的認識，以降低企業受到資安威脅之比例。

四、iThome CYBERSEC101 資安實務研討會

於 2019 年 11 月下旬，TWNIC 暨 TWCERT/CC 副執行長丁綺萍參與 iThome CYBERSEC101 資安實務研討會。該研討會將其議程分別依序以識別 (Identify)、防禦措施 (Protect)、偵測威脅機制 (Detect)、攻擊因應 (Respond) 以及災害復原 (Recover) 等五大資安防禦功能面向區分，並針對各個面向進行深入的探討及分享，得以完整檢視企業資安防禦全貌。

丁綺萍副執行長也受邀參與 Recover 之專題演說，透過相關資安案例探討分析，說明現今企業所面對的資安威脅，以及當資安事件發生時，企業除了需降低受害層面、儘速恢復正常運作外，如何藉此提升企業的資安防禦能量，將是未來企業重要課題。

twcertcc

2019 台灣電腦網路危機處理暨協調中心資安年報

第五章

結語

當前網路與資訊連結蓬勃發展的時代，單打獨鬥的資安防護模式已無法對抗快速且複雜之資安攻擊，透過國內企業、政府單位、資安社群團體及資安公司間的攜手合作，以及和國際資安組織間的互助協處及情資分享，共同建立資安防護網，共同維護並提升網路安全，達成提供安全可靠的資通訊環境之願景。

隨著網際網路、行動裝置、個人電腦以及自動化設備的蓬勃發展，資訊安全逐漸成了人們日常生活中的一部分，從家用網路、行動裝置，到智慧家庭，都可能產生資安威脅，甚至這些威脅也延伸到使用者所屬的組織和企業中，因此，對於資安的重視是保障個人隱私及安全的重要意識之一，人人都應積極面對與防護。諸多國際組織都紛紛針對資訊安全提出規範及法規，引領使用者及企業加強其資安防護能量，避免在資訊發達的時代中，因資安威脅而蒙受損失。包括網際網路協定中的 DNS，可透過 DNSSEC 進行相關的防護作業和機制，避免攻擊者利用 DNS 協定本身以及建置上的漏洞，產生資安威脅。BGP 協定上的問題，則可透過 RPKI 機制進行防護，透過有公信力的第三方進行驗證，達到對 BGP 協定的監督，減少因 BGP 造成的資安問題。此外，隨著行動裝置及物聯網的逐漸盛行，相關的產品及應用程式紛紛問世，而為了增加大眾在使用相關設備及軟體時的安全性，因此可透過政府或可信的單位進行檢測，除了確保產品本身的安全無虞外，更可增添使用者的信任，建造更方便且安全的網路及生活環境。

資訊安全的範圍極廣，從時常聽聞的電腦病毒、勒索病毒，到詐騙的網路釣魚，甚至透過各種工具及系統漏洞進行的駭侵攻擊，都可能造成受害者不小的損失。因此，為防範資安問題的產生，除了定期進行系統更新、安裝防護軟體，以及避免下載、點擊或開啟不明的檔案及連結外，對可疑的檔案應透過相關系統檢視後方進行相關作業，Virus Check 系統在 2019 年 7 月中旬開放大眾使用以來，便已檢測數千筆的檔案，並且經檢測後，發現其中約 10% 的高風險檔案，知會使用者應立即予以刪除，降低惡意檔案感染主機的成功機率。但資安攻擊形式及手法多不勝數，沒有 100% 的防禦方式，因此除了針對資安進行事前防禦外，也應制定或了解當資安事件產生時的應變措施，包括通報相關單位、尋求資安組織的協助、以及針對受害主機進行備份、隔離等減少受害層面之措施。TWCERT/CC 在 2019 年間，已自 13 個國際資安組織、

CERT 組織及各式來源，經手並通報協處逾 110 萬筆之資安情資，並將資安情資分享予國內之政府單位、網路業者、金融單位、學術單位等相關組織，以及國外 117 個國家之 CERT/CSIRT 組織和相關資安組織，成為國內與國際之間的通報及溝通橋樑，促進資安事件的通報協處效率，提升國內整體資安防護能量。

此外，為了在瞬息萬變的資訊安全領域中，成功建立足夠的防護能量，除了常見的防火牆、防毒軟體、防護系統、監控系統等工具外，同時也必須針對新興的攻擊模式、攻擊對象進行即時的應變措施，不論是使用者或企業都應對相關資安組織所提供或發布之相關情資進行檢閱，並將其延伸至自身所使用的裝置及系統，對可能產生的資安問題進行即時的預警及應對措施。TWCERT/CC 於 2019 年間總計分享 182 則國內外資安新聞、34 則駭侵事件、53 則資安漏洞資訊，以及 55 則資安研討會 / 活動 / 競賽等資訊，即時提供企業及大眾資安訊息並予以警示，讓相關單位及人員能在第一時間進行防護作業。

資訊安全並沒有一般大眾或企業所認知的遙遠，但也沒有想像的如此艱難，許多資安問題都可透過足夠的知識、經驗及定期且即時的情資，建立足夠的防護網。即便不幸成為資安問題的受害者，亦有許多組織可協助處理相關資安問題，降低受害的影響層面及範圍。

為因應資訊安全的快速變化和趨勢，TWCERT/CC 將持續擴大與國內外資安組織合作，擴增資安情資來源，同時也將積極主協辦及參與國內外合作交流活動，增進與國際間之資安情資分享與能量，確立情資交流管道。目前已有多方管道可提供使用者進行資安問題之協處及惡意程式檔案之檢測，未來將持續優化系統，同時亦藉由更多公私單位的資安合作，增加資安通報協

處能量。TWCERT/CC 也將持續透過官方網站、電子報及相關社群媒體，提供即時的資安新聞及預警，並結合公協會、政府單位等，將資通訊安全訊息傳達給更多使用者，提升大眾及企業資安意識，增進國內整體網路安全，讓所有處在網路世界中的所有人與組織都能有安全便利的網路環境。

2019資通安全年報

出版者：財團法人台灣網路資訊中心

書名：2019 資通安全年報

主編：台灣電腦網路危機處理暨協調中心

指導單位：國家通訊傳播委員會

地址：105412 台北市松山區八德路四段 123 號 3 樓

電話：(02)2528–6786

版次：初版

出版日期：109 年 6 月

定價：新台幣 1,000 元整

ISBN ：978–986–992–390–3


twcertcc

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team Coordination Center

105台北市松山區八德路四段123號3樓
3F., No. 123, Sec. 4, Bade Rd., Songshan Dist.,
Taipei City 105, Taiwan, R.O.C.
T +886-2-2528-6786
www.twcert.org.tw

ISBN 978-986-992-390-3