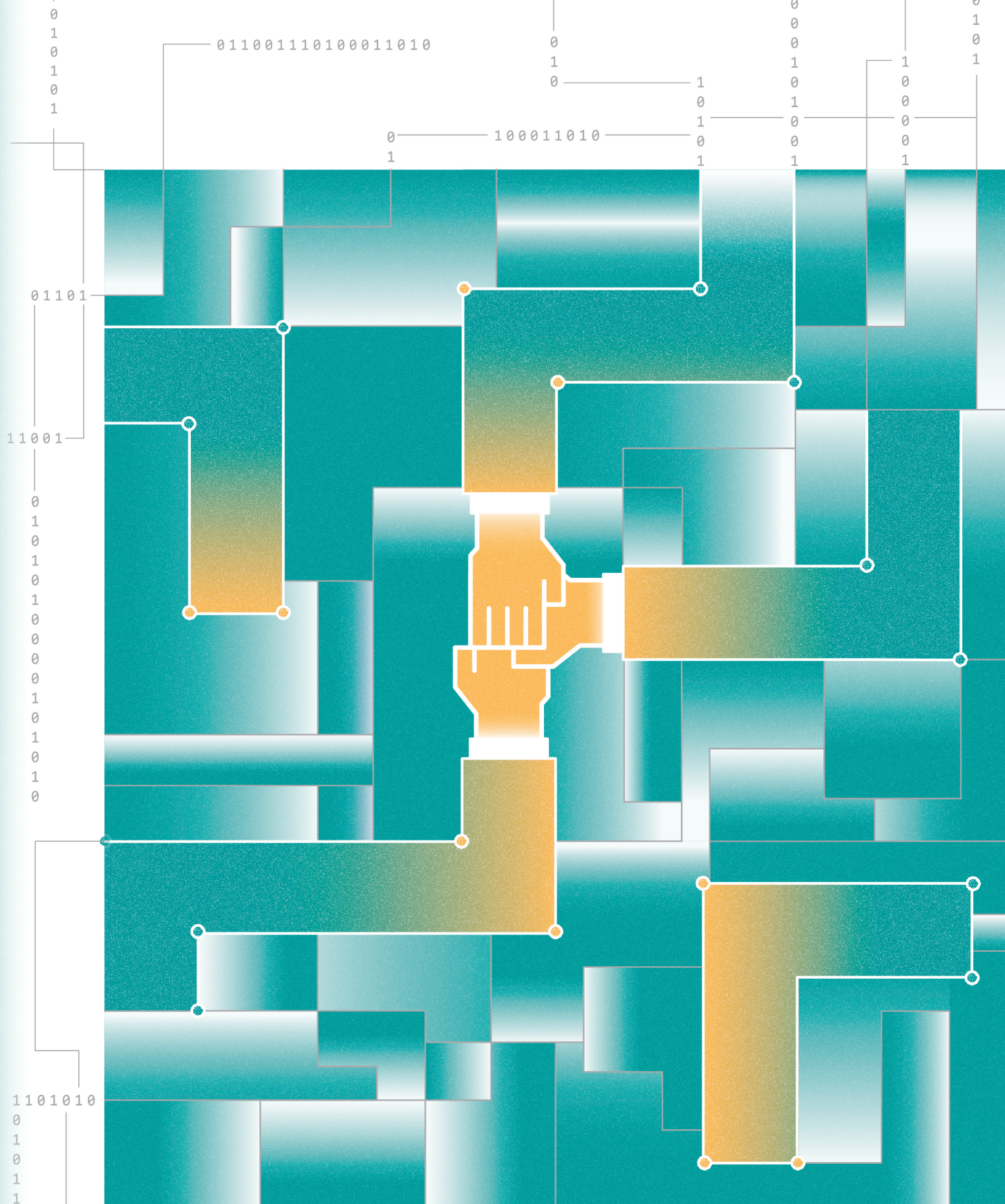


0
1
1
1
0
1
011

1
0
0
0
0
1
0
1
1
0100101
0101
fwwcertac

Cyber Security Annual Report 2021

2021 資通安全年報





10011110100011010

0
1
0
1
0
1

0
1
1
0
1

1101101102

Cyber Security Annual Report 2021

2021 資通安全年報

0
1
1
0
1

11001

0
1
1
0
1

1
0
1
0
1
1

前言

台灣網路危機處理中心暨協調中心 (Taiwan Computer Emergency Response Team/Coordination Center, TWCERT/CC) 是我國企業資安事件通報及協處窗口，負責推動資安情資分享與資安事件諮詢，透過資安事件通報協處、資安趨勢分析、參與國內外交流以及建立資安宣導專區，加強國家資安聯防能量，提升臺灣網路安全。

針對近期資訊發展與資安趨勢，由於 Covid-19 大流行嚴重衝擊了人類的生計，受影響的企業組織為了持續日常營運需要，為員工提供了遠距辦公 (work from home, WFH) 的軟硬體環境，雖然提供了方便，但也提高了資安風險，其中未授權存取及外部入侵是重大的風險類型，而目標式勒索軟體攻擊逐漸成為主要攻擊手法。現今勒索軟體在勒索軟體即服務 (Ransomware as a Service, RaaS) 模式下具備無固定入侵途徑、檔案加密鎖定加上資訊揭露的雙重勒索等特性，且以多種手法進行攻擊。

隨著新的勒索軟體運作模式 RaaS 的出現，勒索軟體已不再只是靠釣魚郵件或是針對幾種漏洞進行入侵，組織的每一個資訊設備與人員皆可能為被利用目標。為提升臺灣資安防護能量，TWCERT/CC 建立勒索軟體防護專區，提供事前防護、事中處理、事後回復各階段措施指南。

其次，Covid-19 大流行導致線上業務急速擴增，使得個資越來越有價值，也凸顯身分驗證對企業組織與消費端的重要性。為提升我國之安全防護能量與增強身分驗證的便捷性和安全性，內政部推行行動自然人憑證 Taiwan Fido (TW-Fido) 服務；而金管會則成立了「金融行動身分識別聯盟」，建立金融 FIDO，以加速推動金融行動身分識別標準化機制，解決與日俱增的全電子化開戶及交易需求。身分驗證與民眾生活息息相關，一旦發生資安問題將影響深遠，因此在任何情況下都不應忽視身分驗證的重要性。

同時，隨著對 IoT 設備的需求增加，新興的設備與機制，變成竊取個人隱私和資訊攻擊首選。由於許多惡意程式會透過感染設備發送攻擊，因此應從 IoT 設備的管理帳號管理與產品安全管理進行防護。為提升 IoT 設備的資安防護能量與提升大眾的信任，政府已委託行動資安聯盟制定 IoT 設備標準與檢測規範，並對產品進行安全性驗證。

此外，受疫情影響，以社群軟體進行生活社交與工作已是現代人的日常，因此社群軟體逐漸成為駭客蒐集機敏資訊、散播惡意軟體以及網路釣魚的最佳管道。落實軟體更新是維護資安的不二法門，而應用越來越廣泛的社群軟體更是如此。為避免讓駭客有機可趁，使用者應盡可能了解社群軟體各項設定的意義並進行安全的選擇。

在 2021 年間，TWCERT/CC 持續進行國內外資安情資通報與分享，總計分享近百萬筆資安情資予相關單位。此外，TWCERT/CC 也持續與國內外資安組織及企業定期並即時地進行情資交流分享，提升臺灣資安聯防能量。TWCERT/CC 亦透過惡意檔案檢測平臺——Virus Check，協助大眾檢測檔案中是否藏有惡意程式，降低遭惡意檔案攻擊之機率。

針對產品資安漏洞，2021 年期間共計接獲超過 160 個資安漏洞，其產品範圍包含軟體服務系統、IoT 設備與伺服器等類型，並且協調相關廠商對其產品進行軟體之更新與修補，以提升國內資通產品安全性。

2021 年期間，TWCERT/CC 主辦台灣資安通報應變年會，並舉辦台灣 CERT/CSIRT 聯盟會議，除邀請專家進行資安相關議題演講外，亦對企業會員進行教育訓練，協助企業提升資安防護能量，建立良好之溝通管道，促進資安情資之分享。同時 TWCERT/CC 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與經驗。在國際交流部分，TWCERT/CC 參與 APDrill 資安通報演練與多場國際活動，進行經驗交流與分享。

在加強資通安全意識方面，TWCERT/CC 於 2021 年期間定期寄送電子報，並分享國內外相關資安新聞、駭侵事件、漏洞資訊以及相關資安研討會、活動等訊息，積極提升大眾資安意識與防護。TWCERT/CC 亦持續經營 Facebook、Instagram 與 Twitter 等官方粉絲團，讓大眾能透過社群平臺，即時獲得資訊安全相關訊息。

信任、交流與分享

TWCERT/CC 透過資安趨勢研析、情資分享、資安事件與漏洞協處、國內外交流合作以及資安宣導，強化我國資安防護與協處之能量，共同維護臺灣的網路安全。

TWCERT/CC 資通安全年報封面以手部的互動線條插畫結合漸層區塊，代表資訊安全維護工作中信任的重要性；背景框線與程式碼以交疊交錯的方式，代表情資交流；底部藍色漸層塊則展現資訊擴散流通與分享。

目次 Contents

前言	02	
壹、資安威脅與防護	08	一、企業組織之資安威脅與防護 (一) 勒索軟體概述與防護建議 (二) 殭屍網路威脅趨勢與防護 (三) 殭屍網路之防護機制
	22	二、消費端應用安全 (一) 身分驗證的技術與發展 (二) IoT 設備安全議題與強化建議 (三) 社群軟體資安威脅與防護
貳、情資分享與漏洞協處概況	34	一、TWCERT/CC 資安情資分享
	41	二、VIRUS CHECK 惡意檔案分析
	45	三、資安漏洞協處 (一) 我國發布之產品漏洞概況 (二) 國際資安事件與漏洞協處案例 (三) 國內資安事件與漏洞協處案例

而整體色彩規劃採用未來主義式配色，呈現資訊科技的進步形象，而手部插畫的部分則添加明亮溫暖的橙黃色，象徵資訊維護，為網路科技增添安全感與人性溫度。

TWCERT/CC 希望藉由 2021 資通安全年報封面設計，將 TWCERT/CC 精神——信任、交流以及分享傳遞給社會大眾。

參、合作交流與資安推廣	56	一、主辦活動
		（一）台灣資安通報應變年會
		（二）台灣 CERT/CSIRT 聯盟交流會議
	64	二、國際交流
		（一）APEC 暨 TELWG 線上大會
		（二）APNIC 52 線上論壇
		（三）2021 APDrill 國際網路安全攻防演練
	67	三、國內交流
		（一）TWCERT/CC 企業資安推廣與分享
		（二）TWCERT/CC 社群資安研討與分享
結語	72	
附錄	74	附錄一、遠距辦公資安防護建議
	79	附錄二、勒索軟體防護檢核表

圖目錄

11	圖 1	直接的勒索病毒運作（左）和 RaaS 運作（右）比較
14	圖 2	集中式殭屍網路
15	圖 3	P2P (Peer to Peer) 殭屍網路
18	圖 4-1	2021 年感染數的逐月 10 大排名
19	圖 4-2	2021 年感染數的逐月 10 大排名
26	圖 5	Mirai 病毒攻擊示意圖
30	圖 6-1	社群軟體
31	圖 6-2	社群軟體
36	圖 7	TWCERT/CC 資安跨域聯防與情資分享
37	圖 8	TWCERT/CC 國際資安事件情資分享比例
38	圖 9	TWCERT/CC 2021 境內情資分享威脅類型比例
39	圖 10	TWCERT/CC 2021 對企業情資分享威脅類型比例
40	圖 11	TWCERT/CC 2021 境外情資分享威脅類型比例
41	圖 12	惡意檔案風險類型
42	圖 13	Virus Check 網站示意圖
43	圖 14	TWCERT/CC 2021 Virus Check 檔案檢測風險值比例
44	圖 15	TWCERT/CC 2021 Virus Check 檢測檔案中高風險檔案類型比例
45	圖 16	TWCERT/CC 2021 接獲漏洞類型
53	圖 17-1	公私部門攜手合作，力抗跨國殭屍網路
54	圖 17-2	公私部門攜手合作，力抗跨國殭屍網路
55	圖 18	TWCERT/CC 勒索軟體防護專區
58	圖 19	台灣資安通報應變年會活動剪影
59	圖 20	台灣資安通報應變年會活動剪影
59	圖 21	台灣資安通報應變年會活動剪影
60	圖 22	聽眾出席行業別分析
60	圖 23	研討會整體滿意度
61	圖 24	2021「台灣CERT/CSIRT 聯盟」交流會議
62	圖 25	2021 第一次「台灣 CERT/CSIRT 聯盟」資安教育訓練實況
63	圖 26	2021 第二次「台灣 CERT/CSIRT 聯盟」資安教育訓練實況
65	圖 27	APNIC 52 線上論壇
66	圖 28	APrill 2021 情境示意
67	圖 29	臺北場「資訊安全防護及案例分享研討會」
68	圖 30	臺中場「資訊安全防護及案例分享研討會」
68	圖 31	彰化場「資訊安全防護及案例分享研討會」
69	圖 32	桃園場「資訊安全防護及案例分享研討會」
69	圖 33	高雄場「資訊安全防護及案例分享研討會」

69	圖 34	資訊安全防護及案例分享研討會（海報）
70	圖 35	介紹 TWCERT/CC 服務暨入會申請流程活動剪影
71	圖 36	台南自動化機械暨智慧製造展
73	圖 37	TWCERT/CC 情資分享與資安服務概要
74	圖 38-1	遠距辦公資安防護指南—企業篇
75	圖 38-2	遠距辦公資安防護指南—企業篇
75	圖 39-1	遠距辦公資安防護指南—員工篇
76	圖 39-2	遠距辦公資安防護指南—員工篇
77	圖 40	遠距辦公資安防護指南—遠距會議篇
78	圖 41	遠距辦公資安防護指南—VPN 篇
79	圖 42	TWCERT/CC 勒索軟體防護專區

表目錄

46	表 1-1	TWCERT/CC 2021 審核發布 CVE 統計表
47	表 1-2	TWCERT/CC 2021 審核發布 CVE 統計表
48	表 1-3	TWCERT/CC 2021 審核發布 CVE 統計表
49	表 1-4	TWCERT/CC 2021 審核發布 CVE 統計表
51	表 2	國際資安情資分享
80	表 3-1	1.1 系統保護面
81	表 3-2	1.1 系統保護面
82	表 3-3	1.1 系統保護面
83	表 4-1	1.2 資料保護面
84	表 4-2	1.2 資料保護面
84	表 5-1	1.3 資安意識面
85	表 5-2	1.3 資安意識面
85	表 5-3	1.4 應變準備面
86	表 6	2.1 事件確認面
87	表 7-1	2.2 應變處理面
88	表 7-2	2.2 應變處理面
89	表 8	3.1 設備恢復面
90	表 9	3.2 事後分享
90	表 10	3.3 檢討改進

PART 1

壹、資安威脅與防護

為提升我國企業與一般民眾之資安意識，以及國內各單位對資安相關議題的了解和關注，TWCERT/CC 配合資安趨勢、資安政策、資安事件與重大侵駭事件等議題，彙整研析，針對企業組織與消費端應用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。

一、企業組織之資安威脅與防護

(一) 勒索軟體概述與防護建議

1. 勒索軟體概述

勒索軟體為一種網路病毒，駭客植入惡意程式至受害者的設備後，控制設備或是加密檔案，隨後要求受害者支付贖金以取回電腦控制權或是受加密的檔案，如著名勒索軟體 WannaCry、Conti 與 Netwalker。勒索軟體散布方式如惡意廣告、釣魚電子郵件與瀏覽論壇文章等管道。

2. 勒索軟體侵害趨勢— RaaS 模式劇烈成長

最早的勒索軟體可追溯到 1989 年的 AIDS 木馬 (AIDS Trojan¹)，在當年的 WHO (World Health Organization) 的 AIDS 會議上，與會人士開啟存放病毒的軟式磁碟片 (floppy disk) 並安裝程式，他們的設備即被感染，被感染的設備起先並無異狀，待重新開機達到 90 次時，病毒會加密設備上全部檔案，並要求受害者以支票支付贖金換取解密金鑰，當時約影響了兩萬人，此病毒也以該會議名稱命名。

相比最早勒索軟體 AIDS 木馬，現今勒索軟體的行為模式已有很大的進化，透過網路或是社交工程的傳播效率更勝以往，支付方式也多以匿名制的虛擬貨幣為主，使攻擊者不易被追查。例如勒索軟體 Conti 透過夾帶惡意附件或惡意連結的釣魚郵件等手法，入侵受害者設備，竊取資料後加密，以此勒索贖金²；以及越來越多駭客利用 Microsoft Office 巨集下載方式，將勒索軟體藏於其中並以附件方式寄送，受害者開啟 office 文件並啟用巨集時，就會自動下載惡意程式並執行。

從開源情資 (Open Source Intelligence, OSINT) 觀測到勒索軟體相關事件數量在 2021 年有劇烈增加的情形，已成爲最主要網路安全威脅。在 2021 年取得贖金前十大勒索軟體中³，大部分爲提供勒索軟體即服務 (Ransomware as a Service, RaaS) 的模式，即買家向勒索軟體開發者購買或租用惡意程式。在過去，駭客團體若想發動勒索軟體攻擊，需開發惡意程式以及贖金談判；在 RaaS 模式中，駭客只需向勒索軟體開發者以租用方式使用勒索軟體發動攻擊，因此整個犯罪生態鏈有了更好的分工，勒索軟體組織可以更專注在勒索軟體開發與運作，租用者專注在贖金談判。RaaS 的出現降低了發動勒索軟體攻擊的門檻，且原本勒索軟體組織從以贖金作爲收入，轉變爲收

取服務費用，駭客組織有相較穩定的地下經濟模式，可用更多心力精進勒索軟體本身。著名勒索軟體組織如 Wizard Spider、LockBit 與 BlackMatter。



2021 年發生多起 BlackMatte 勒索軟體組織勒索企業組織事件，即為勒索軟體組利用利用輕型目錄存取協定 (Lightweight Directory Access Protocol, LDAP) 與伺服器訊息區塊 (Server Message Block, SMB) 協定來存取 AD (Active Director)，進而找到主機並加密資料，甚至清除備份資料，也威脅受害組織將公開竊取的機密資料以索求贖金⁵。而 2021 年底揭露的 Log4j 漏洞，則已有勒索軟體組織利用此漏洞發動攻擊，並以此獲利，由於受影響服務與系統範圍廣，微軟已呼籲用戶立即更新版本並提高警覺⁶。

3. 勒索軟體防護建議—TWCERT/CC 勒索軟體防護專區網站

由上述可知現今勒索軟體在 RaaS 模式下具備無固定入侵途徑與檔案加密鎖定加上資訊揭露之雙重勒索特性。過往面對勒索軟體威脅，可以針對主要入侵途徑進行封阻，加上資料備份以降低危害，但當面對多種攻擊手法時很難防護面面俱到，且機密資料被公開的威脅也無法被消弭，因此應回歸到資安防護的策略思考。台灣電腦網路危機處理暨協調中心 (TWCERT/CC) 建立勒索軟體防護專區網站⁷，提供事前預防、事中處理、及事後回復各階段措施之指南與檢核表：

I . 事前預防

a. 保護系統

- 安裝防毒軟體，並確保作業系統、應用程式等皆為最新版本。
- 強化 AD 伺服器安全，並監控異常狀況。
- 限制 Microsoft Office 巨集。近期 Microsoft 也已預設封鎖來自網路的 VBA 巨集程式，若未來使用者需要使用巨集，會提醒使用者巨集的風險性⁸。
- 設置防火牆，阻擋黑名單連線，避免使用允許任何連線 (Allow Any) 的規則，並只開放對外必要之服務埠，關閉不必要之對外服務埠
- 定期對員工進行社交工程演練以提升組織成員資安意識

- b. 保護資料
 - 定期備份重要資料與重要的系統映像檔
 - 加密保護機敏資料，避免遭竊時被洩漏內容
- c. 準備事件應變計畫
 - 制定並演練事件應變計畫
 - 規劃實際事件發生時聯繫通報的外部單位

II . 事中處理

- a. 識別勒索軟體種類
- b. 緊急應變處置
 - 斷開全部設備的內外網連結
 - 進行資安事件通報，啟動事件處理，確認入侵途徑
 - 啟動應變措施

III . 事後回復

- a. 更換全部帳號密碼，並重置相關憑證
- b. 重新安裝被感染的設備
- c. 還原備份資料

除以上措施外，還可用資訊安全評估工具 (Cyber Security Evaluation Tool, CSET)⁹，針對勒索軟體防護機制進行自評以了解自身組織安全性，以及採取相對應強化措施。此外，為防範內網橫向移動 (Lateral Movement) 的感染力，內網應依功能落實網路分層管理，各層間不能直接連通，彼此間部署網路連線異常偵測與紀錄機制，針對網域中重要伺服器部署內網攻擊偵測機制，避免將內網設定為一整個網路，提高內網複雜度。

(二) 殭屍網路威脅趨勢與防護

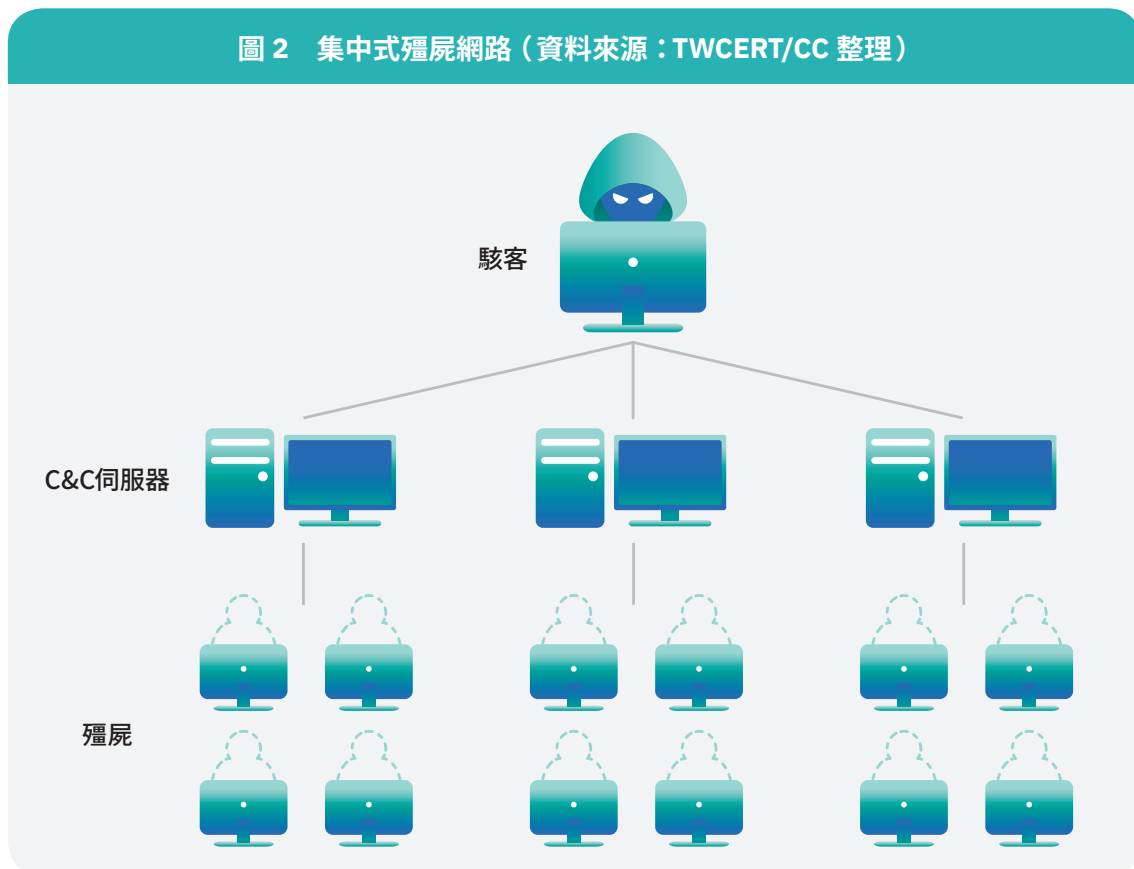
1. 殭屍網路簡介

殭屍網路是由受惡意程式感染設備所組成的網路，其規模可能超過數百萬臺設備，攻擊者可操縱殭屍網路發起攻擊，如阻斷網路、散布惡意程式以及發送垃圾郵件等攻擊行爲。散布惡意程式，發送垃圾郵件等攻擊行爲。臺灣常見殭屍網路病毒如 Qsnatch、Mirai 與 Conficker 等惡意軟體。殭屍網路主要可以分爲兩種架構類型：

I . 集中式殭屍網路

運作結構由受感染殭屍電腦 (Client) 與 C&C (Command and Control) 伺服器組成。駭客能透過 C&C 伺服器快速地將攻擊指令傳送給殭屍電腦，此種架構的殭屍網路執行速率較快，至今仍是主要的殭屍網路結構方式。集中式殭屍網路由於 Client 與 C&C 伺服器之間的溝通頻繁容易產生異常流量，因此網路安全人員較易找到 C&C 伺服器並將其清除，使殭屍網路失效。

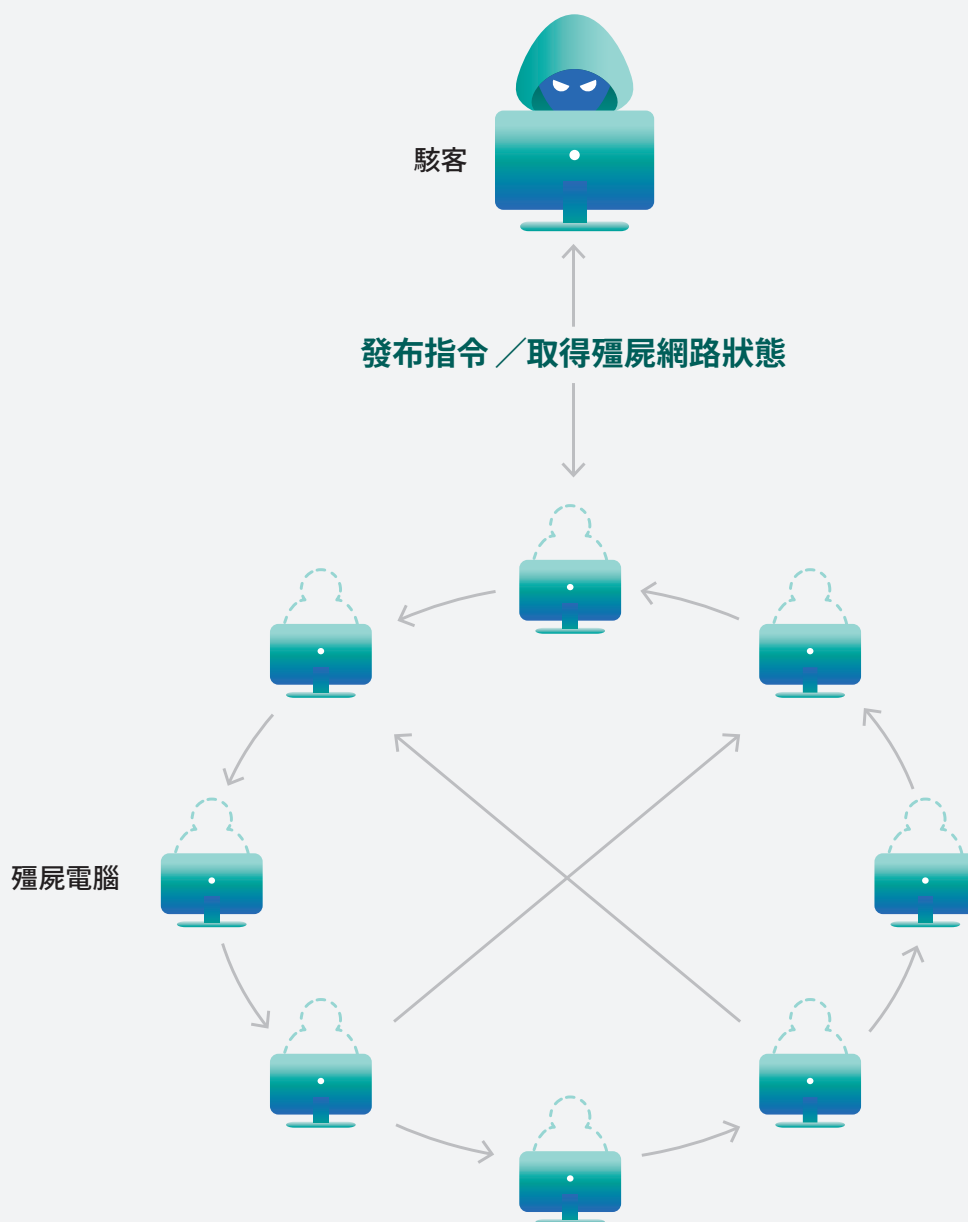
圖 2 集中式殭屍網路 (資料來源：TWCERT/CC 整理)



II . P2P (Peer to Peer) 殭屍網路

運行 P2P 殭屍網路的特色在於殭屍網路中的各個節點設備彼此共享命令和訊息，沒有固定的 C&C 伺服器。P2P 殭屍網路實施技術難度較高，但更具彈性。每個殭屍節點設備都擔任 C&C 伺服器角色傳遞消息，也同時扮演 Client 角色獲取訊息。P2P 殭屍網路的各節點依靠鄰居清單 (Peer List) 選擇任一鄰居進行溝通，因此要清除殭屍網路，須找到該網路的 Peer List，清除難度較高。

圖 3 P2P (Peer to Peer) 殭屍網路 (資料來源：TWCERT/CC 整理)



2. 殭屍網路的威脅

不管是技術或是成本層面，運行殭屍網路的門檻都不高，在暗網 (Dark Net) 上已提供各種租售方案，數十美金即可由駭客組織代為發動殭屍網路，例如進行小規模 DDoS 流量攻擊。在許多合法網站和 YouTube 上都有大量技術教學。再加上識別出殭屍網路攻擊者很困難，導致殭屍網路難以阻絕。利用殭屍網路發起的攻擊¹⁰ 包括：

I . 分散式阻斷 (Distributed Denial-of-Service attack, DDoS) 攻擊

DDoS 攻擊需要發起大量的流量或是服務請求，故殭屍網路最為適合被用於 DDoS 攻擊。

II . 挖礦

加密貨幣是通過求解加密的數學方程式而取得，需要大量的 CPU 運算或是磁碟空間，故透過殭屍網路的建立，讓大量設備協助參與挖礦，可讓攻擊者賺取大量金錢。

III . 資訊窺探

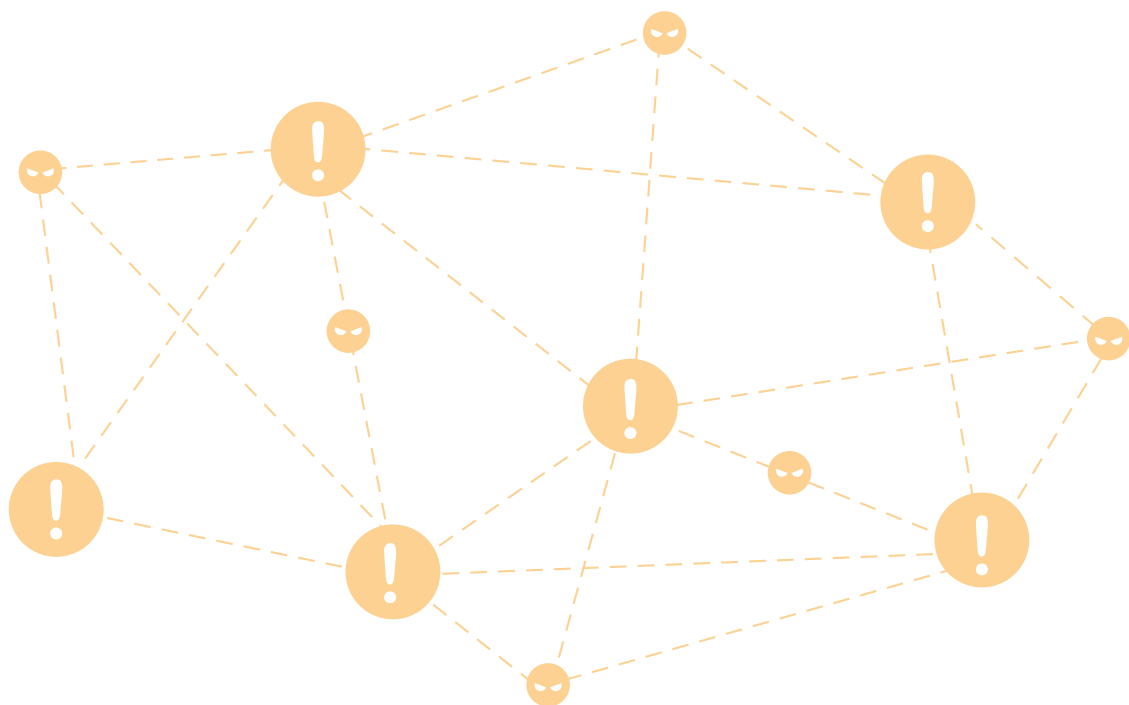
殭屍網路可用於監視網路流量，可以被動地收集資訊，也可以主動地將惡意代碼注入 HTTP 流量。

IV . 阻塞 (Bricking) 攻擊

阻塞攻擊會將感染後的 IoT 設備刪除軟體模組，使其變得無用或阻塞，攻擊者可能會在多階段攻擊中使用阻塞攻擊，隱藏發起主要攻擊時可能留下的線索。

V . 垃圾郵件

殭屍網路從網站，論壇等任何用戶輸入其電子郵件地址的地方收集資料，用於創建帳戶和發送垃圾郵件。



3. 我國殭屍網路感染狀況分析

本報告依據 TWCERT/CC 的情資來源通報的殭屍網路情資，進行惡意軟體家族分類統計，觀察殭屍惡意軟體對我國的影響狀況以及趨勢。2021 年主要變化（如圖 4）為 Mirai 與 Qsnatch 威脅大幅降低；Android-hummer 是入榜唯一的行動裝置惡意軟體，具不易移除的特性；利用 Windows 系統漏洞攻擊的威脅持續，如已擴展至較為大型的物聯網設備，尤其是以醫療為主的 MRI 機器、CT 掃描器等的 Conficker 與新上榜的 downadup；以信件為主要傳播手段的 Lethic 仍持續上榜，顯示須更強化社交工程防護意識。

與國際趨勢相比，國際上的殭屍惡意軟體變化很快，新出現的殭屍惡意軟體很快會上榜¹¹；國內殭屍軟體變化不大，且多為存在已久之惡意軟體家族，例如 sality 與 virut 等在國外曾經造成重大威脅的惡意軟體。故在資安作為上，應更落實軟體更新，重視老舊版本軟體更版，以及強化防護機制。

圖 4-1 2021 年感染數的逐月 10 大排名 (資料來源：TWCERT/CC 整理)

月份 名次	1月	2月	3月	4月	5月	6月						
1	mirai	↔	mirai	↔	android.hummer	↑	qsnatch	↑	wannacrypt	↑	android.hummer	↑
2	qsnatch	↑	android.hummer	↑	qsnatch	↑	android.hummer	↓	android.hummer	↔	conficker/downadup	↑
3	android.hummer	↑	qsnatch	↓	wannacrypt	↑	wannacrypt	↔	qsnatch	↓	qsnatch	+
4	conficker/downadup	↓	wannacrypt	↑	mirai	↓	lethic	↑	virut	↑	wannacrypt	↓
5	wannacrypt	↓	lethic	↑	lethic	↔	conficker/downadup	↑	lethic	↓	virut	↓
6	sality	↓	conficker/downadup	↓	conficker/downadup	↔	virut	↑	conficker/downadup	↓	lethic	↓
7	lethic	↔	virut	↑	emotet	↑	emotet	↔	andromeda	↑	andromeda	↔
8	virut	↑	emotet	+	virut	↓	andromeda	↑	coinminer	↑	avalanche-generic	+
9	proxyback	↓	andromeda	↑	coinminer	+	coinminer	↔	sality	↑	dltminer	+
10	andromeda	↔	sality	↓	andromeda	↓	sality	+	mozi	+	sality	↓
		排名上升：	↑	排名下降：	↓	排名持平：	↔	新惡意軟體：	+			

圖 4-2 2021 年感染數的逐月 10 大排名 (資料來源：TWCERT/CC 整理)

月份 名次	7月	8月	9月	10月	11月	12月
1	pva.intowow	android.hummer	conficker/downadup	conficker/downadup	conficker/downadup	conficker/downadup
2	conficker/downadup	conficker/downadup	qsnatch	android.hummer	android.hummer	android.hummer
3	wannacrypt	qsnatch	android.hummer	virut	virut	lethic
4	android.hummer	wannacrypt	virut	lethic	lethic	virut
5	qsnatch	virut	lethic	andromeda	andromeda	andromeda
6	pva.torrent.kickasstracker	lethic	andromeda	avalanche-generic	dltminer	android.bakdoor.prizmes
7	virut	andromeda	avalanche-generic	sality	avalanche-generic	avalanche-generic
8	pva.torrent.publictorrent	avalanche-generic	mozi	mozi	sality	sality
9	lethic	sality	sality	dltminer	mozi	dltminer
10	andromeda	mozi	coinminer	vpnfilter	android.bakdoor.prizmes	mozi

排名上升：
 排名下降：
 排名持平：
 新惡意軟體：

(三) 殭屍網路之防護機制

殭屍網路是發起多種大規模攻擊的基礎，亦是攻擊階段的惡意工具下載機制，若能防範將可起到降低後續更嚴重資安危害的效果。針對國內殭屍網路感染特性，提供以下建議：

I . 定期的安全意識培訓計畫

提升設備管理人員之資安意識，教導使用者／員工識別惡意連結或附件，以避免感染殭屍惡意軟體。

II . 建立完善軟體更新程序，保持防毒軟體最新狀態並定期掃描網路

如 Conficker、Salinity 等，皆是針對 Windows 作業系統為主要對象，這幾個存在已久的惡意軟體對國內危害仍大，有兩個可能，一是惡意軟體持續更新變種；二則是舊版 Windows 作業系統仍然存在，或是更新速度不夠快。唯有持續重視安全性更新，並且淘汰不再被維護的作業系統或軟體才是最有效的方法。

III . 汰換已超過產品生命週期、無法取得安全性更新之產品

物聯網裝置近年來已有多起被利用進行大流量攻擊的案例，這些裝置可能因運算效能不足或是資安防護較弱而成為目標，Mirai 僅是利用預設密碼便造成極大的危害，而物聯網裝置通常具有同類型大量部署的特性，即使不再有預設密碼的問題，只需某個品牌產品出現問題，即可一次攻陷大量相同裝置，且相較電腦主機已具有成熟的中控式更新機制，物聯網裝置的安全性更新更要加強重視，一旦物聯網裝置已超過產品生命週期無法取得更新，就應啟動產品汰換機制，不讓存在弱點的裝置繼續暴露在風險中。

IV . 選購符合資安規範之設備

資安標準的制定對裝置安全具有良好的效果，例如行動應用資安聯盟所制定之影像監控系統（IP camera）的物聯網資安標準已頗有成效，故選購產品時，選擇通過資安標準認證的產品較有保障。

V . 部署入侵偵測系統（Intrusion detection system，IDS）與端點保護方案

保護方案盡可能包括 rootkit 檢測能力，可以監控內部網路封包與流量是否有異常，當發現異常時，自動通報給資訊安全管理人員並採取措施，阻止惡意網路。

VI . 產品設計導入安全性規範

研製相關連網裝置的廠商也應與時俱進。從產品的設計開始就應導入安全性規範，落實資安檢測，除了可避免未來要耗費更多時間修補問題，亦能讓使用者更加安心使用廠商之產品。



二、消費端應用安全

(一) 身分驗證的技術與發展

1. 單因子身份驗證技術與議題

身分驗證是確認使用者能否取得系統資源的關鍵，也是許多敏感應用得以安全運作的基礎，由於不同使用環境之需求，身分驗證技術越來越多樣化發展。身分驗證的三大要素，說明如下：

I . 所知之事 (what you know)

帳號密碼是最原始、使用最廣泛的身分驗證技術。例如登入網路服務時，使用者輸入「所知」的帳號及密碼，由遠端伺服器審核使用者身分，對通過身分驗證的使用者提供相關服務。

隨著資通訊技術的發展，使得人們越來越依靠各種應用程式來完成工作。當使用者被迫記住許多複雜和頻繁需要變更的密碼時，由於不堪負荷，因此許多使用者會冒險使用相同或相似的密碼、弱密碼，而網路伺服器一旦遭攻陷，儲存在內的使用者密碼也可能遭到外洩。這種僅依賴使用者知道的祕密，來保護系統的存取權限，已無法提供安全的防護。

II . 所持之物 (what you have)

驗證使用者是否「擁有」或「持有」某樣已通過認證的東西。例如使用者持有的一次性密碼 (One Time Password, OTP)、門禁卡、識別證、數位憑證等，是一種常見的身分驗證手段。

例如簡訊 OTP 為目前常見應用在高風險交易的「所持之物」身分驗證，其風險在於駭客能利用假簡訊騙取受害者個資，以及當手機遭駭入裝置惡意軟體後，駭客可透過惡意軟體發動中間人攻擊¹²，進而取得控制。例如我國曾發生駭客集團偽造銀行 APP 更新通知，發送 OTP 驗證碼與詐騙連結，誘使受害者點擊連結輸入銀行帳號密碼，並成功盜款¹³。而國外曾發生過利用能攔截簡訊 OTP 的行動裝置惡意軟體 SpyEye，進而從中獲取不法所得¹⁴。

III . 所具之形 (what you are)

利用使用者身體獨一無二的特徵（如指紋、靜脈、眼睛虹膜或視網膜等）進行身分驗證，廣泛應用在行動裝置登入、門禁系統等應用環境中。

由於可應用在身份驗證的生理特徵，必須要滿足「永久性」及「可測量性」，隨著 AI 技術的發展，導致生物特徵被盜用或是偽造的風險提高。例如有研究團隊指出駭客能透過偽造的指紋，欺騙智慧型手機上的指紋掃描儀，進而竊取受害者的金融帳戶資訊¹⁵。此外，當生物辨識的結果被轉換成資料儲存，若被不法分子取得，則可能侵犯個人隱私。例如遠距進行生物辨識的技術（如人臉辨識）被廣泛使用時，就可對其進行跟蹤，危害該生理特徵擁有人的安全。相較於其它身份驗證機制，由於生物辨識綁定的是使用者本身，故隱私外洩是生物辨識驗證技術獨有的風險。

2. 多因子身分認證機制發展

隨著急速擴增的雲端應用服務與線上業務，網路帳號越來越有價值，導致帳號密碼外洩，或是藉由網路釣魚獲得個資與生物識別事件不斷，因此僅使用單一身份驗證方式已無法確保其安全強度。為強化身份驗證之安全，使用兩種或多種不同的機制，來驗證使用者身分的多因子認證（multi-factor authentication, MFA），成為目前最重要的身分驗證方法。

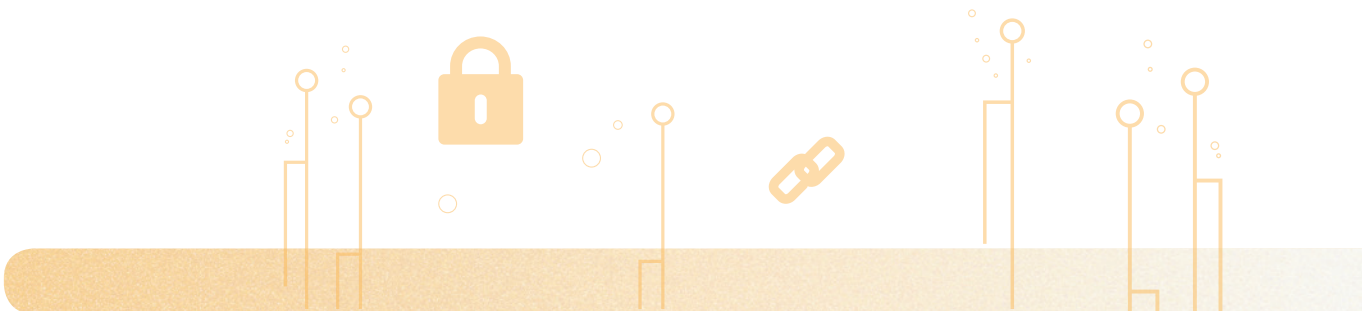
常見多因子驗證如雙重驗證／兩步驟驗證（two-factor authentication, 2FA），其驗證機制為 TOTP（Time-based One-Time Password）¹⁶與帳號密碼做搭配。TOTP 是基於時間的一次性密碼，其運作模式為使用者透過 TOTP 手機應用程式連結帳號，當使用者每次使用服務，在輸入帳號與密碼後，其連結之 TOTP 手機應用程式依據使用者使用之服務與登入時機產生一組一次性驗證碼。每一個驗證碼只能使用 30 秒，之後使用者會取得新的一次性驗證碼。常見 TOTP 應用程式如 Google Authenticator 應用程式與 Microsoft Authenticator 應用程式。生物辨識與憑證亦為常見多因子身份驗證方式，例如我國內政部移民署所設置的入出國自動查驗通關系統（e-Gate Enrollment System），以護照（所持之物）搭配人臉辨識（所具之形）技術，讓旅客能自助、便捷、快速的入出國。

3. 公開金鑰架構之身分認證發展

從傳統簡單的使用者和密碼組合，逐漸發展到多因子認證，身分驗證技術不斷地在演進。然而伺服器漏洞問題造成密碼外洩、密碼強度不足以及使用者帳號密碼管理問題層出不窮，為解決上述問題，並改善使用者須經多重階段身份驗證才能使用服務的不便利性，作為目前最炙手可熱的新興身份驗證標準 FIDO (Fast Identity Online)，受到各界極大的期待。

FIDO 標準由 FIDO 聯盟¹⁷制定，該標準建立於公開金鑰加密 (Public Key Cryptography) 架構，以此進行多重因子驗證以及生物特徵認證。FIDO 機制為使用者先透過生物特徵驗證個人裝置，如筆電或智慧型手機，通過驗證後，與應用服務帳號註冊至 FIDO 伺服器中取得一組專屬於該設備、使用者帳號的公鑰與私鑰 (public-private keys)。私鑰存放於使用者的設備，並由生物認證機制保護，而 FIDO 伺服器僅保存使用者的公鑰。由於 FIDO 架構採取公私鑰分散式存放，並且 FIDO 不再留存使用者密碼，從而最大限度地減少了機敏資料與帳戶密碼外洩的可能性。FIDO 標準除了強化身分認證安全性外，由於其適用於任何 FIDO 認可的設備、服務與網站，標準化的身分認證規範能方便業者部屬，而不再需要記住複雜的密碼，僅須進行生物辨識的認證方式也助於提升使用者體驗。

FIDO 聯盟迄今已發布了三種使用者身分驗證規範，包括以透過結合生物辨識等認證途徑，讓使用者無密碼登入的 FIDO UAF (FIDO Universal Authentication Framework)，支援雙因子驗證的 FIDO U2F (FIDO Universal Second Factor) 以及對 web 支援並綜合無密碼及雙因子驗證的最新身分驗證規範 FIDO2¹⁸。



4. 我國身分驗證規範

I . 行動自然人憑證 Taiwan Fido (TW-FidO)

由內政部推行的 TW-Fido 服務，用以改善過去仰賴自然人憑證或申請帳號密碼使用政府網路服務的做法。TW-Fido 採用生物特徵辨識方式驗證，使用者透過手機 App 綁定自然人憑證後，即可以生物辨識，透過免密碼方式，快速驗證登入多個政府網站，取得個人服務。TW-Fido 目前僅供政府機關試辦，尚未開放商業應用¹⁹。

II . 金融行動身分識別標準化機制 (金融 FIDO)

由金管會推動，透過金融 FIDO 標準，未來用戶在不同金融機構使用服務時，透過綁定的行動裝置、生物特徵進行身分驗證，不需要再使用實體卡片或帳號密碼重複認證²⁰。

III .IoT 設備之身分驗證資安規範

隨著 IoT 市場的蓬勃發展，IoT 設備逐漸成爲生活中的一部分，然而 IoT 設備的安全性問題層出不窮，許多低成本 IoT 設備使用低強度的身分驗證機制，增加潛在資安風險。爲強化 IoT 設備之身分驗證保護機制，FIDO 聯盟制定「FIDO Device Onboard」(FDO) 規格²¹，爲自動化、安全的 IoT 設備定義新標準，以便可以安全地與其雲端或內部管理平臺進行通訊。我國已有業者推出符合 FDO 規範的解決方案，協助 IoT 開發人員打造符合 FDO 標準的安全產品²²。

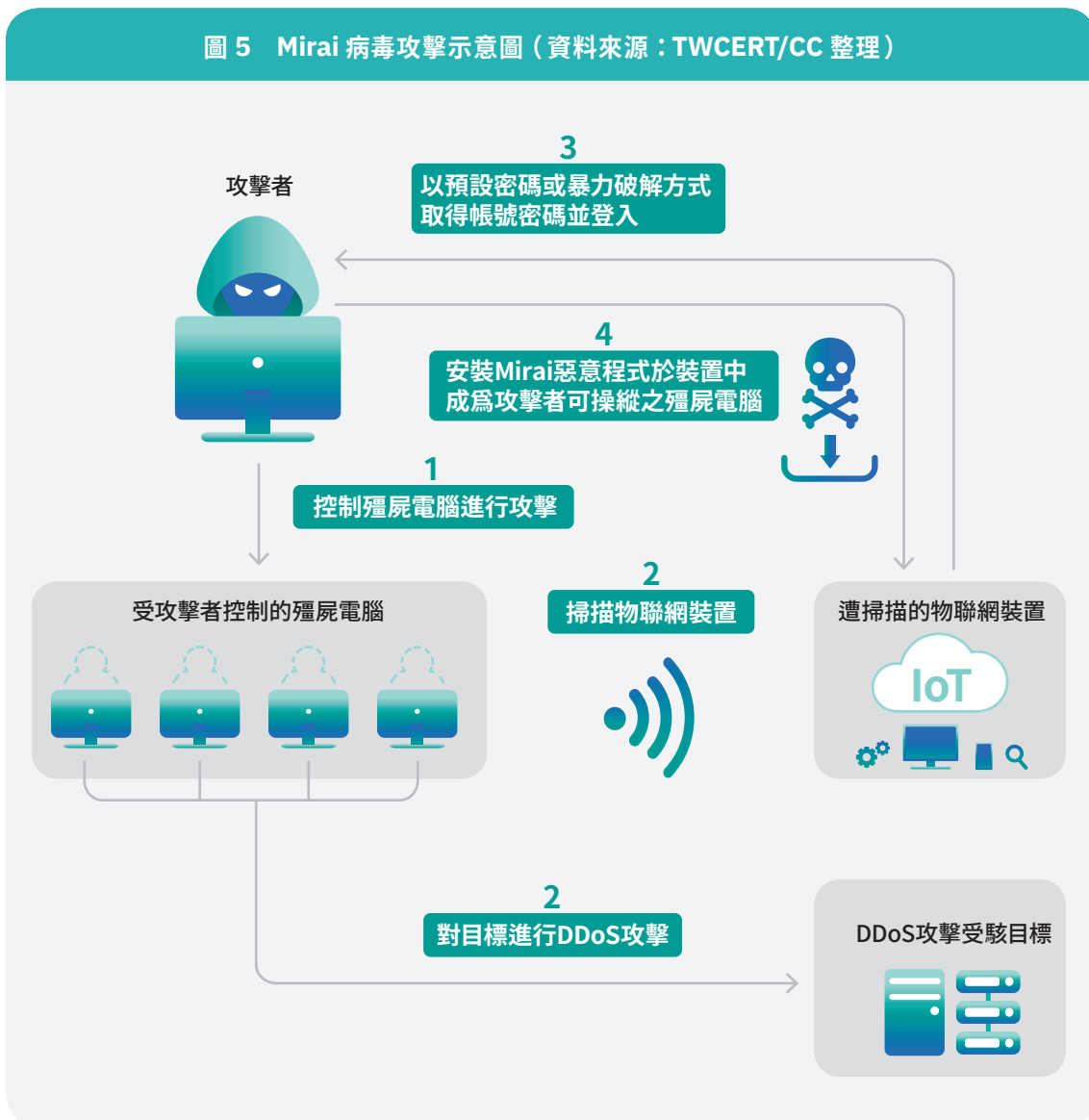


(二) IoT 設備安全議題與強化建議

1. IoT 設備安全議題

近年來物聯網日趨深入人們的生活當中，大量傳統設備增加聯網功能，也讓駭客有更多機會利用 IoT 設備弱點，入侵設備植入惡意程式，發送垃圾郵件、發動 DDoS (分散式阻斷服務, Distributed Denial-of-Service attack)、竊取個人資料以及散播病毒，使 IoT 設備成員殭屍網路一員。例如著名惡意軟體 Mirai 所構建的殭屍網路，其殭屍大軍主要由數十萬台網路攝影機與其他物聯網裝置，能同時發動數百 Gbps 的 DDoS 攻擊流量，癱瘓受攻擊目標²³。

圖 5 Mirai 病毒攻擊示意圖 (資料來源：TWCERT/CC 整理)



常見 IoT 設備如網路攝影機、智能燈泡、掃地機器人；基於安全監控的需求，網路攝影機通常透過網際網路提供 24/7 全天候的監視服務。加上由於影像處理所需，網路攝影機亦具有相較高於其它 IoT 設備的計算能力和良好的網路流量輸出，因此成為駭客竊取個人隱私和攻擊的首要目標。

例如從著名的網站²⁴上可以發現，臺灣有上百支網路攝影機影像遭公布在網站上，供全球觀賞，其中攝影的地點包括辦公室內部、工廠作業區、民宅客廳、餐廳、會議室、診所、營業場所等地的即時影像。因此有心人士透過網頁瀏覽器即可觀看各式的即時影像。IoT 設備之資安問題包括：

I . 使用者資安意識不足

大多數 IoT 設備預設使用了眾所週知的預設使用者帳號及密碼，並允許在安裝設定過程中不需要更改預設密碼，加上使用者新設定的密碼保護性低，駭客能透過網路掃描取得 IoT 設備的廠牌及型號後，利用預設密碼表或暴力破解連網裝置的登入帳號及密碼，完成入侵。例如惡意軟體 Mirai 就是利用網路攝影機設備預設帳號及密碼的弱點，使用了數十個使用者帳號及密碼的組合對物聯網設備進行簡單的暴力攻擊，從而建立殭屍網路²⁵。

27

II . 雲端資料儲存庫安全性不足

許多 IoT 設備應用會連結雲端服務上的應用軟體或服務，例如雲端監控可以讓使用者將影像傳送到雲端影像資料庫儲存，實現雲端循環錄影，並讓使用者在稍後隨時回放。因此即使駭客無法直接連接到使用者的網路攝影機，駭客也可以對雲服務發動攻擊竊取影像資料，例如 2021 年曾發生雲端安全監視系統遭駭客入侵一案，導致數十萬則安全監控影像被外洩²⁶。

III . 產品本身安全性不足

除了常見的密碼猜測攻擊外，利用 IoT 本身的資安漏洞也是常見的駭客入侵手法。例如研究人員曾發現某些網路攝影機的漏洞，不僅可以讓攻擊者透過中間人攻擊截取雲端伺服器與攝影機之間的串流影像，還可以讓攻擊者將攝影機的合法韌體替換成藏有後門版本的韌體²⁷。

2.IoT 設備資安強化建議

綜合前述所提到的資安議題，包括隱私議題、預設密碼、脆弱密碼、錯誤設定、雲端資安、設備弱點等，對 IoT 設備使用者提出以下建議：

I . 修改預設帳號，提高密碼強度，並避免與其它設備使用相同密碼。

II . 使用支援雙因子認證 (Two-factor authentication, 2FA) 的設備，如此一來除非駭客有能力獲得另一組安全碼，否則即使駭客破解設備的帳號與密碼組合也無法登錄，可以大幅降低網路攝影機遭駭客入侵的機會。

III . 確保 IoT 設備的韌體版本都更新至最新版本，關注廠商所發布的資安訊息，及時安裝所有的漏洞修補程式。

IV . 保護網路並加強網路安全，例如不要在沒有任何資安防護措施 (如防火牆等) 保護的情況下，將網路攝影機直接曝露在網際網路上，避免資料外洩，或是駭客藉由入侵網路攝影機進入主要網路，造成其它系統受害。對網路攝影機所使用的網路進行隔離 (例如放置在虛擬區域網路)，使之與主要網路分離，是一個較好的解決方法。

V . 使用 SSL 或 WPA2 對網路連線進行加密，以防範中間人攻擊並避免機敏資料在傳送過程中遭竊。

VI . 選擇通過資安檢測的 IoT 設備。物聯網設備資安標準與檢測認證，已成為政府重視的一大焦點。政府委託行動資安聯盟²⁸制定了物聯網設備之資安標準與測試規範，例如消費性網路攝影機資安標準暨檢測規章、門禁系統資安標準暨檢測規章等，以全面提升消費性設備的安全與防護能量。

（三）社群軟體資安威脅與防護

1. 社群軟體安全議題

社群軟體²⁹為網路時代主要社交工具之一，人們透過社群軟體進行生活社交與工作交流，已是現代人的日常。因此社群軟體所具備即時通訊、資訊分享、快速傳播、社群影響、商業內容等特性，在駭客集團眼中已成為蒐集資訊的最佳管道，導致資安議題層出不窮，帶來的損害也日益增加。社群軟體主要資安議題為：

I . 惡意軟體傳播管道

藉由有趣或熱門時事的標題，或是偽裝成一般合法應用程式，吸引使用者點擊，進而成功進行釣魚攻擊，或是更為直接的惡意檔案傳輸，點擊後直接執行。例如 2021 年駭客釋出強化 WhatsApp 的助手 APP FMWhatsapp 來吸引下載安裝，以改善 WhatsApp 用戶體驗，例如更好的隱私、自定義聊天主題以及使用其他社交媒體的表情符號等應用功能。安裝 FMWhatsapp 後，木馬程式開始收集設備訊息並將其發送到其命令和控制伺服器，該伺服器回覆一個藏有惡意軟體的下載連結，隨後木馬程式將下載並啟用惡意軟體進行攻擊³⁰。

II . 社群軟體之漏洞問題

社群軟體出現漏洞，潛藏的洩漏機密風險極高，亦有案例是透過社群媒體 APP 的漏洞，監控 APP 內所有的行為與訊息記錄，造成企業重要機敏資料外洩。例如近期最知名的是 2021 年 4 月 Facebook 因 API 漏洞遭入侵所造成數億筆個資外洩。

III . 針對性社交工程攻擊

駭客集團在初步蒐集情資後，在社群軟體中創建假帳號，鎖定特定族群，觀察其中可能獲取下一步攻擊資訊的對象，進行攻擊。例如 2021 年研究人員發現 TA456 駭客集團在網路上創建假 Facebook 帳號，並與攻擊目標的員工建立長達 8 個月的聯繫，取得信任後，藉由電子郵件寄送帶有惡意程式的檔案給受害者，竊取個資³¹。

2. 社群軟體資安防護

雖說社群軟體服務有各種資安事件的發生，但並非不重視資安議題，其軟體功能皆具備安全考量，例如社群軟體提供點對點的加密功能（End-to-End Encryption，E2EE），只有收發訊息兩端能使用專屬金鑰加解密訊息。但點對點的加密方式仍非完全安全，還是存在中間人攻擊的可能性³²，所以必須搭配其它認證機制來加以強化，例如結合手機來進行多層次的證認，並於使用新設備登入時必須進行確認等防護機制，加強安全。

此外，各國針對社群軟體資安議題十分重視，也有相關的國際資安規範^{33 34 35 36 37 38}。以下提出相關建議：

I . 軟體管理

透過正式管道下載社群軟體，並定期更新軟體。

II . 帳號密碼管理

定期更新並使用高強度密碼，並避免所有平臺都使用同一組帳號密碼。當使用電腦或網頁板的社群軟體後應確實進行登出。亦使用兩步驗證（2FA）來保護帳戶。

III . 帳號連結管理

確認有哪些平臺帳號連結至社群軟體，若帳號已無使用，應關閉其帳號，避免被駭客利用來存取與其連結的帳號。

圖 6-1 社群軟體



Pinterest



TikTok



YouTube



LinkedIn



Facebook



Messenger



Instagram



WhatsApp

IV . 隱私權限管理

關閉自動接受好友申請與搜尋功能，以及有限度的公開個人資料，當公開的資料越多，就越有可以被駭客以社交工程手法攻擊。

V . 最小化權限設定

如關閉社群軟體上的自動下載功能或只允許通訊錄的人員通訊。

VI . 訊息內容管理

避免透過社群軟體提供機密資料，並確認對方身分，以及封鎖不明使用者的訊息與不隨意開啟連結。

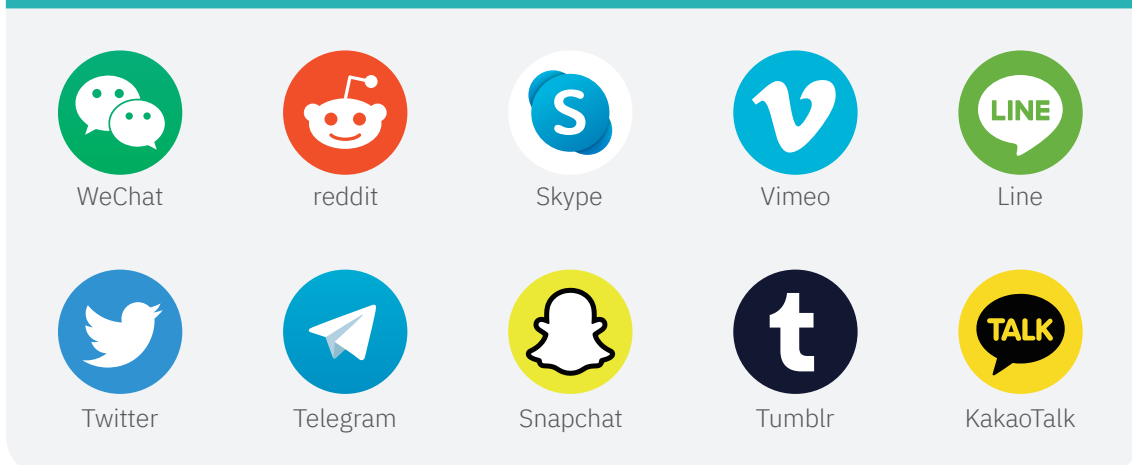
VII . 設定安全機制

例如對訊息加密、訊息刪除、雙因子身分驗證、安全設定、雲端備份機制等進行適當設定，並注意社交平臺與對於安全的控管政策。

VIII . 減少曝光個資

由於社群平臺漏洞造成個資外洩的問題掌控權並不在使用者，因此使用者應注意盡可能減少將個資曝露於社群軟體。

圖 6-2 社群軟體

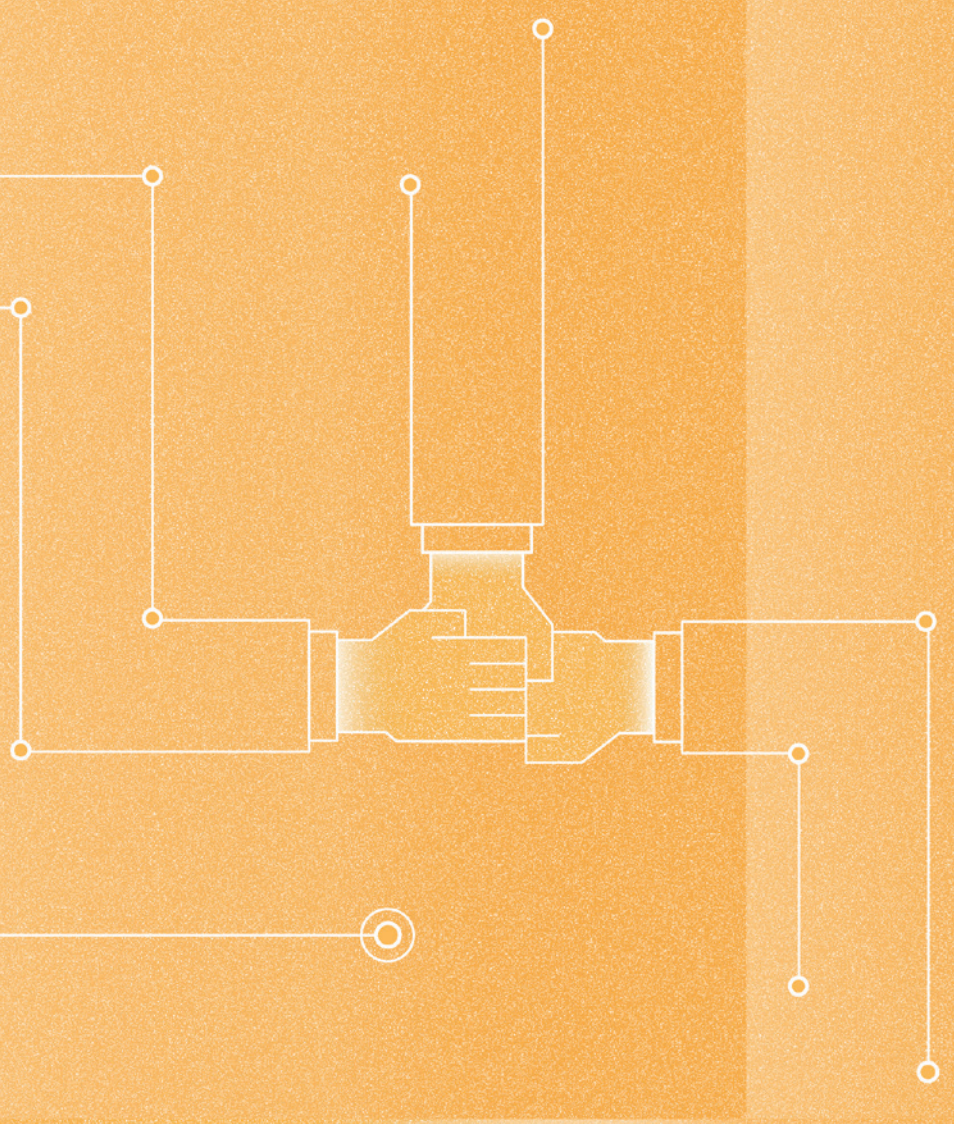


參考書目

- 1 ransomware.org. “The AIDS Trojan: The First Ransomware Attack” : <https://ransomware.org/what-is-ransomware/the-history-of-ransomware/#evolution-of-ransomware>
- 2 ENISA. “ENISA Threat Landscape 2021” : <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>
- 3 ransomwhe. : <https://ransomwhe.re/>
- 4 Trendmicro. 〈勒索病毒即服務 (RaaS): 推波助瀾了大量攻擊〉 : <https://blog.trendmicro.com.tw/?p=69932#more-69932>
- 5 tenable. “Active Directory is Now in the Ransomware Crosshairs” : <https://www.tenable.com/blog/active-directory-is-now-in-the-ransomware-crosshairs>
- 6 iThome. 〈微軟警告 Log4j 漏洞風險並未消褪，要有長期抗戰準備，美 FTC 也呼籲企業與合作廠商立即行動，不然將提告〉 : <https://www.ithome.com.tw/news/148739>
- 7 TWCERT/CC. 勒索軟體防護專區 : <https://antiransom.tw/>
- 8 THE VERGE. “Microsoft to block Office VBA macros by default” : <https://www.theverge.com/2022/2/7/22922032/microsoft-block-office-vba-macos-default-change>
- 9 CISA. 〈勒索軟體防護成熟度自評說明 – 使用美國 CISA CSET RRA 軟體模組〉 : <https://antiransom.tw/pdf/CISACSETRRA.pdf>
- 10 CrowdStrike. “Botnets Explained” : <https://www.crowdstrike.com/cybersecurity-101/botnets/>
- 11 Spamhaus Malware Team. : <https://www.spamhaus.org/>
- 12 NordVPN. 〈什麼是中間人攻擊?〉 : <https://nordvpn.com/zh-tw/blog/zhongjianren-gongji/>
- 13 iThome. 〈假冒銀行釣魚簡訊詐騙規模擴大，繼國泰世華、台新銀行後，中國信今日也出現遭冒名的狀況，金融業者民眾可千萬注意〉 : <https://www.ithome.com.tw/news/142711>
- 14 iThome. 〈透過簡訊執行二次驗證不再安全，美國國家標準技術研究所建議別再使用〉 : <https://www.ithome.com.tw/news/112845>
- 15 TechNews. 〈AI 偽造指紋登場，指紋解鎖還安全嗎?〉 : <https://technews.tw/2018/12/27/ai-generated-fingerprints-could-soon-fool-biometric-systems/>
- 16 WANcatServer. 〈用 TOTP 擺脫簡訊驗證碼：安全好用的兩步驟驗證〉 : <https://wancat.cc/post/totp/>
- 17 Wikipedia. “FIDO Alliance” : https://en.wikipedia.org/wiki/FIDO_Alliance
- 18 HENNGE. 〈FIDO 是什麼？無密碼時代的來臨〉 : <https://hennge.com/tw/blog/what-is-fido.html>
- 19 行動自然人憑證 : <https://fido.moi.gov.tw/pt/>
- 20 金融監督管理委員會〈「金融行動身分識別聯盟」正式成立，加速提升數位金融服務的安全與便利〉 : https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0&mcustomize=news_view.jsp&dataserno=202106150002&dtable=News
- 21 EDN. “IoT security update: The FDO standard scores an early design win” : <https://www.edn.com/iot-security-update-the-fdo-standard-scores-an-early-design-win/>

- 22 ACW.〈初探物聯網安全趨勢下 PUF 晶片安全發展機會〉：<https://www.acw.org.tw/Events/Detail.aspx?id=13>
- 23 維基百科.Mirai (惡意軟體)：[https://zh.wikipedia.org/zh-tw/Mirai_\(%E6%81%B6%E6%84%8F%E8%BD%AF%E4%BB%B6\)](https://zh.wikipedia.org/zh-tw/Mirai_(%E6%81%B6%E6%84%8F%E8%BD%AF%E4%BB%B6))
- 24 insecam.“Insecam–Live cameras directory”：<http://www.insecam.org/>
- 25 Kim Quach.“Default Username And Password In Internet of Things”,Bachelor Degree Project in Information Technology with a Specialisation in Network and System Administration,University of Skovde,2018.Available at：<https://www.diva-portal.org/smash/get/diva2:1252229/FULLTEXT01.pdf>
- 26 Cybersecurity Insider.“Hackers breach systems of Cloud based Security Camera company Verkada”：<https://www.cybersecurity-insiders.com/hackers-breach-systems-of-cloud-based-security-camera-company-verkada/>
- 27 ESET.“D-Link camera vulnerability allows attackers to tap into the video stream”：<https://www.welivesecurity.com/2019/05/02/d-link-camera-vulnerability-video-stream/>
- 28 行動應用資安聯盟聯盟：<https://www.mas.org.tw/>
- 29 Wikipedia.“Social software”：https://en.wikipedia.org/wiki/Social_software
- 30 bleepingcomputer.“Malicious WhatsApp mod infects Android devices with malware”：<https://www.bleepingcomputer.com/news/security/malicious-whatsapp-mod-infects-android-devices-with-malware/>
- 31 T 客邦.〈資安趨勢部落格—駭客集團靠一個美女健身教練假帳號，布局數月騙到了國防承包商員工帳號〉：<https://www.techbang.com/posts/88850-zian-detailed-how-the-hacking-group-tricked-defense-contractor>
- 32 Wikipedia.“Man-in-the-middle attack”：https://en.wikipedia.org/wiki/Man-in-the-middle_attack
- 33 NCSC.“Social media: protecting what you publish”：<https://www.ncsc.gov.uk/guidance/social-media-protect-what-you-publish>
- 34 NCSC.“Social Media: how to use it safely”：<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>
- 35 CISA.“Guidelines for Secure Use of Social Media by Federal Departments and Agencies”：<https://www.energy.gov/sites/prod/files/maprod/documents/SecureSocialMedia.pdf>
- 36 ENISA.“Recommendations for Online Social Networks”：<https://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks>
- 37 NCSC.“Choosing an enterprise instant messaging solution”：<https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/choosing-an-enterprise-instant-messaging-solution>
- 38 NCSC.“Using third-party applications on devices”：<https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/using-third-party-applications-on-devices>

PART 2



貳、情資分享與 漏洞協處概況

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。

一、TWCERT/CC 資安情資分享

在 2021 年期間，TWCERT/CC 總計分享近百萬筆之資安情資予相關單位，包含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。情資來源主要為國際資安交流組織、國內資安相關組織、國內企業組織，以及各國電腦緊急應變小組（Computer Emergency Response Team，CERT）組織等相互交流的訊息。

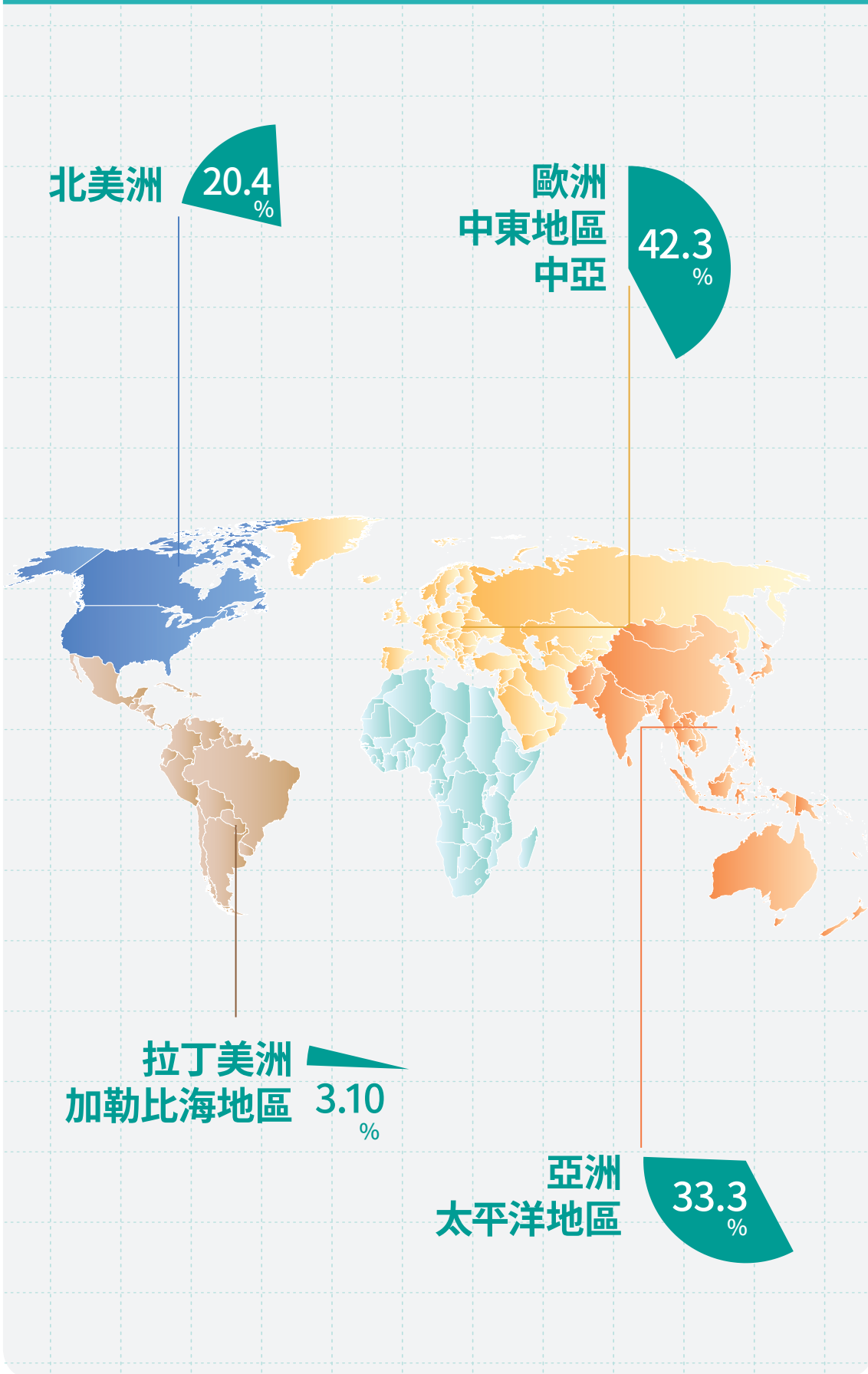
收到資安通報後，TWCERT/CC 會依據通報中心之對象進行情資分享。依國內外對象區分，國內分享對象主要包含政府單位、網路業者、金融單位、學術單位、台灣駭客協會 HITCON 等資安組織，以及諸多國內企業；國外分享對象為 150 餘國家的 CERT/CSIRT 單位及相關資安組織。此外，為提升情資警示及分享效率，TWCERT/CC 通報系統與國家資安資訊分享與分析中心（National Information Sharing and Analysis Center，N-ISAC）、美國自動化資安威脅情資共享計畫（Automated Indicator Sharing，AIS）、反釣魚工作小組（Anti-Phishing Working Group，APWG）等國內外資安組織介接，定期並即時地進行情資分享互通交流，提升情資分享效能與提升聯防能量。

在 TWCERT/CC 所接獲並進行通報的情資中，以接受國際情資後分享至國內相關單位之數量為最大宗。而接收國內情資，將國內情資或資安訊息分享至國外的情資數量中，其通報的國家眾多，最多的為歐洲、中東、中亞區域地區之國家，其次為亞洲、太平洋地區之國家，第三則為北美、南極洲地區之國家，其詳細比例如圖 8。



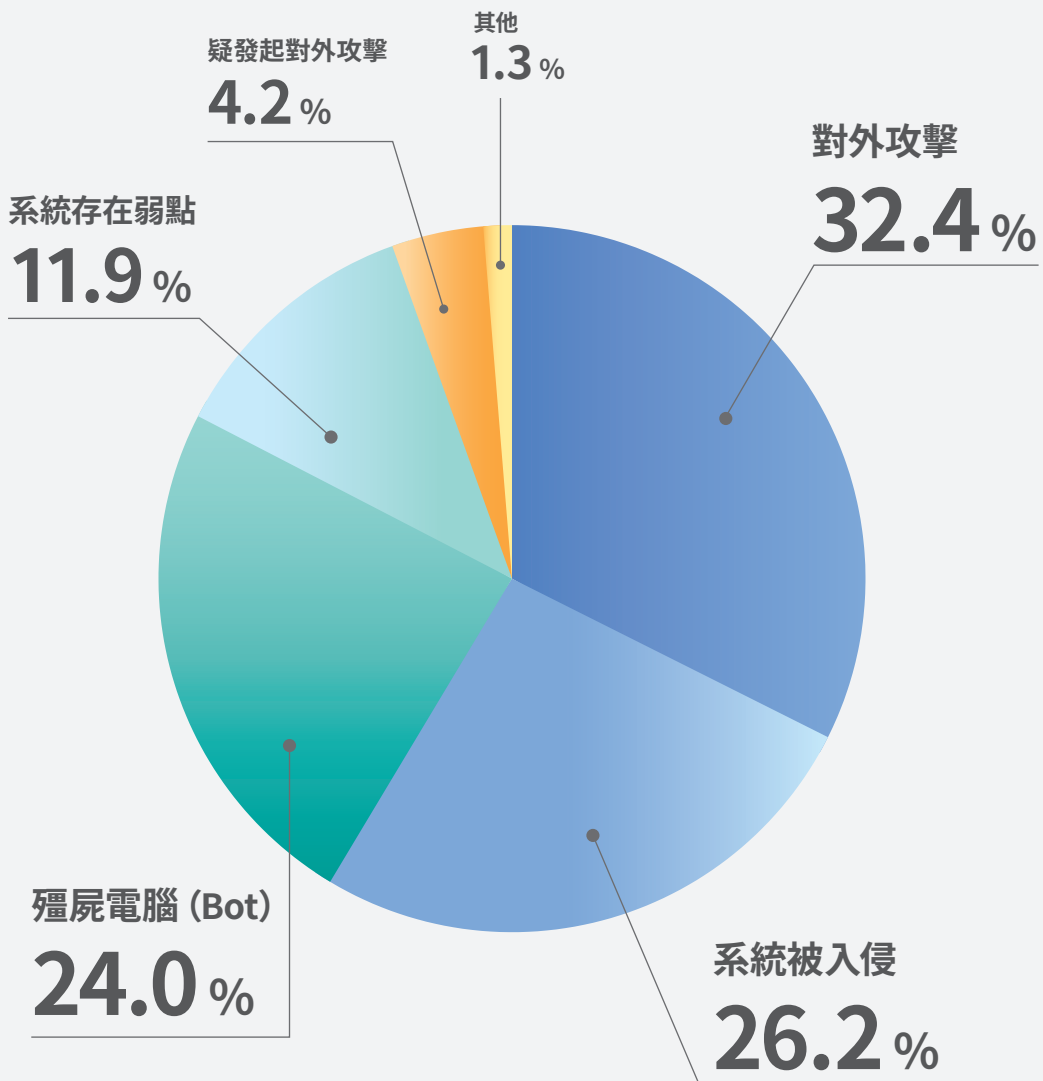
圖 7 TWCERT/CC 資安跨域聯防與情資分享（資料來源：TWCERT/CC 整理）

圖 8 TWCERT/CC 國際資安事件情資分享比例 (資料來源：TWCERT/CC 整理)



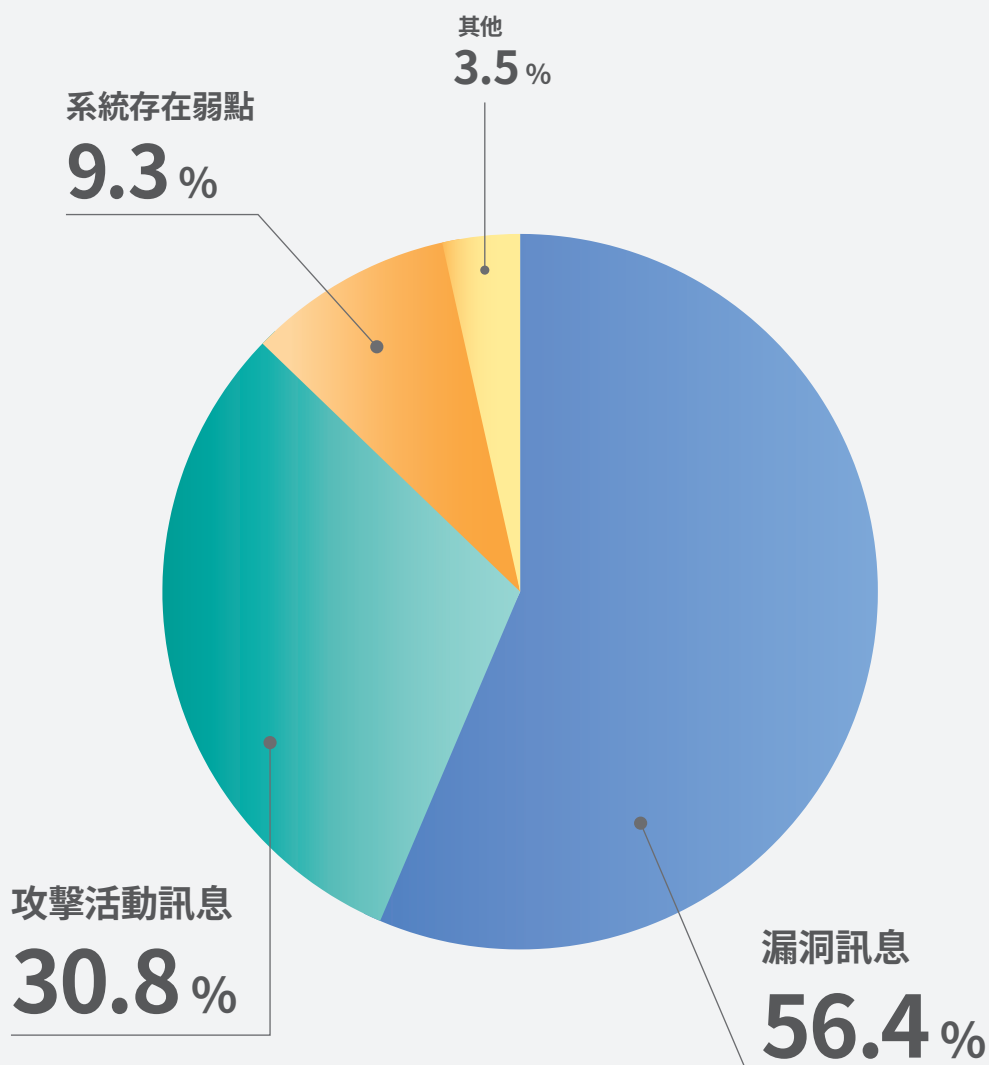
TWCERT/CC 針對其攻擊類型及方式進行區分，接獲並通報國內組織的資安事件類型比例，前三項分別為對外攻擊、系統被入侵與殭屍電腦，代表有大量遭入侵的系統被利用作為攻擊用途，或是成為殭屍網路的一員，其他事件類型包含攻擊活動類型、漏洞訊息與疑發起對外攻擊。與 2020 年相比，系統疑存在弱點有些微比例下降，但存在弱點即有被入侵風險，故亦需注意。

圖 9 TWCERT/CC 2021 境內情資分享威脅類型比例 (資料來源：TWCERT/CC 整理)



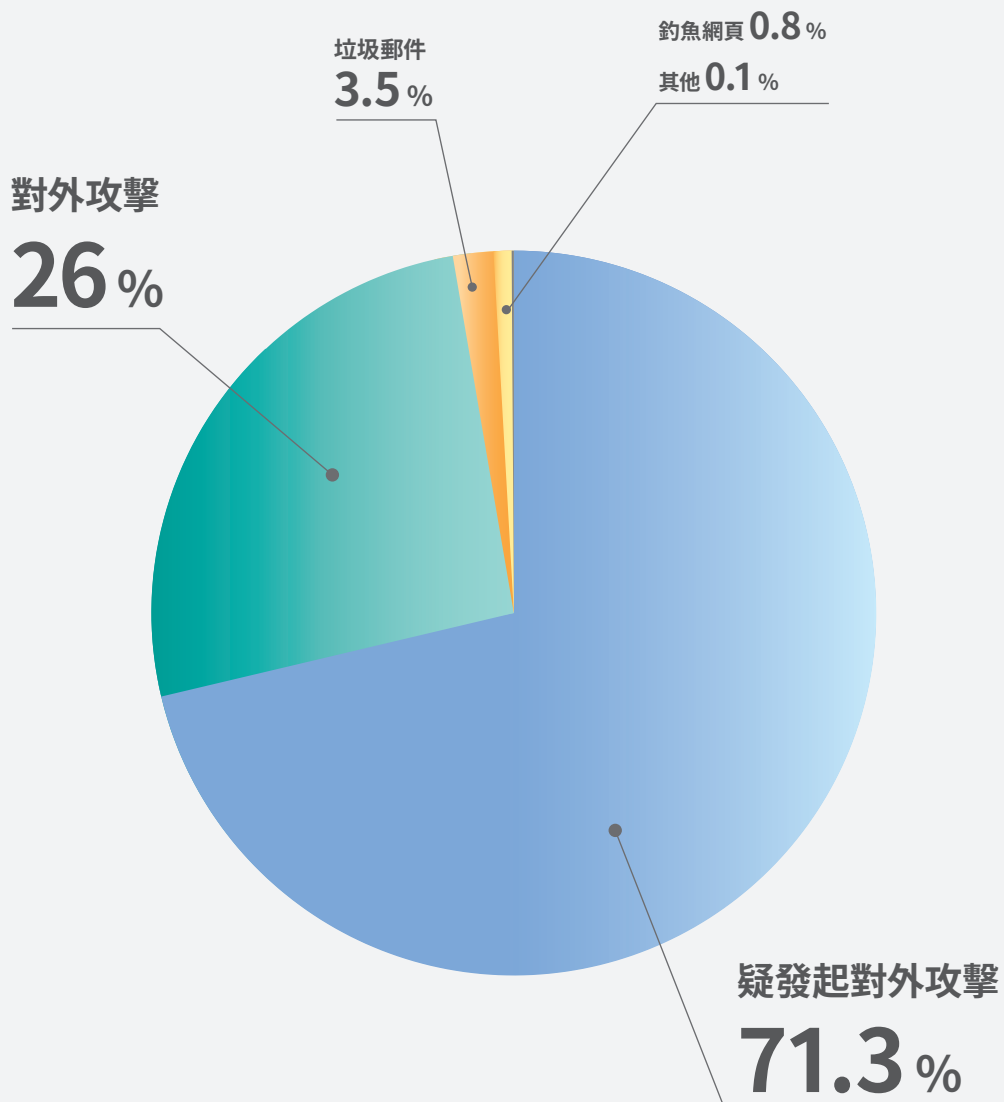
而針對對國內企業組織分享資安事件類型，前兩名為漏洞訊息與攻擊活動訊息，顯示 TWCERT/CC 持續協助企業及時掌握最新資安訊息，強化防護能量與臺灣資安漏洞處理防護系統，提升臺灣產品安全性，第三名則為系統疑存在弱點，代表臺灣仍有大量系統有被入侵的風險，顯示企業組織對資訊安全意識仍需加強。對企業情資分享威脅類型其他包含分析報告與疑發起對外攻擊。

圖 10 TWCERT/CC 2021 對企業情資分享威脅類型比例（資料來源：TWCERT/CC 整理）



對國際單位分享的資安事件類型前三名為疑發起對外攻擊、對外攻擊與垃圾郵件 (Spam)，主要為國際組織間之企業組織系統或主機因受攻擊者操控，導致其被利用對外發起惡意攻擊行為，或是對外寄送未經允許之垃圾郵件。與 2020 年相比，無論國內或國外其對外攻擊比例皆上升，顯示國內外組織受惡意程式攻擊日趨嚴重。對境外情資分享威脅類型其他包含網頁木馬、系統疑存在弱點，命令與控制伺服器 (C&C) 與殭屍電腦 (Bot)。

圖 11 TWCERT/CC 2021 境外情資分享威脅類型比例 (資料來源：TWCERT/CC 整理)



二、VIRUS CHECK 惡意檔案分析

為協助企業與民眾降低社交攻擊盜取機敏資料與入侵系統，TWCERT/CC 建置惡意檔案檢測系統 (Virus Check)，提供企業和民眾上傳可疑檔案，以判別是否為惡意檔案。使用者上傳檔案後，Virus Check 透過靜態檢測與動態檢測，根據檔案行為或特徵判讀檔案風險類型，判別是否為惡意檔案，並與國網、趨勢科技、奧義智慧、TEAMT5 合作，進行深度檢測提升準確度。

圖 12 惡意檔案風險類型 (資料來源：TWCERT/CC 整理)

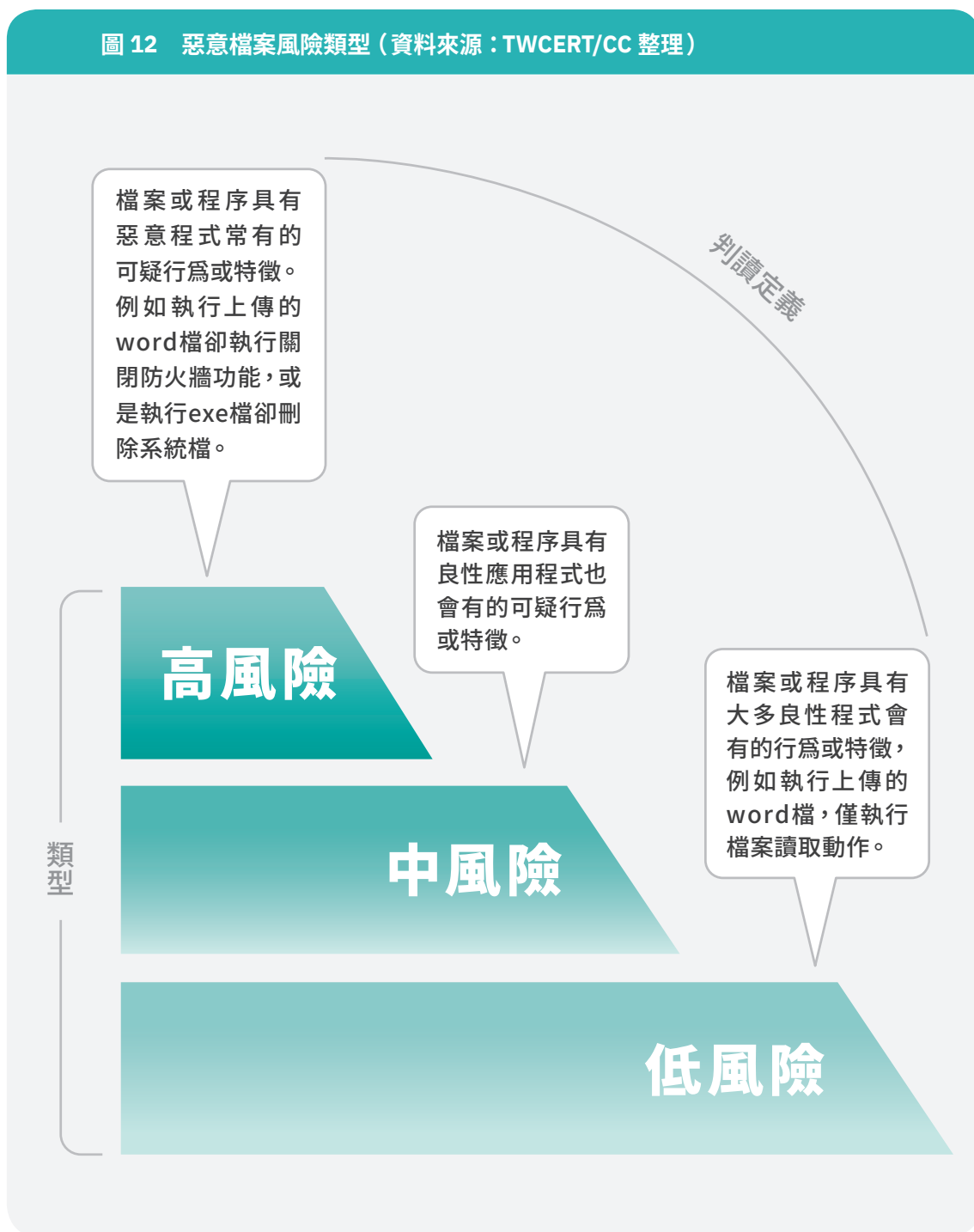
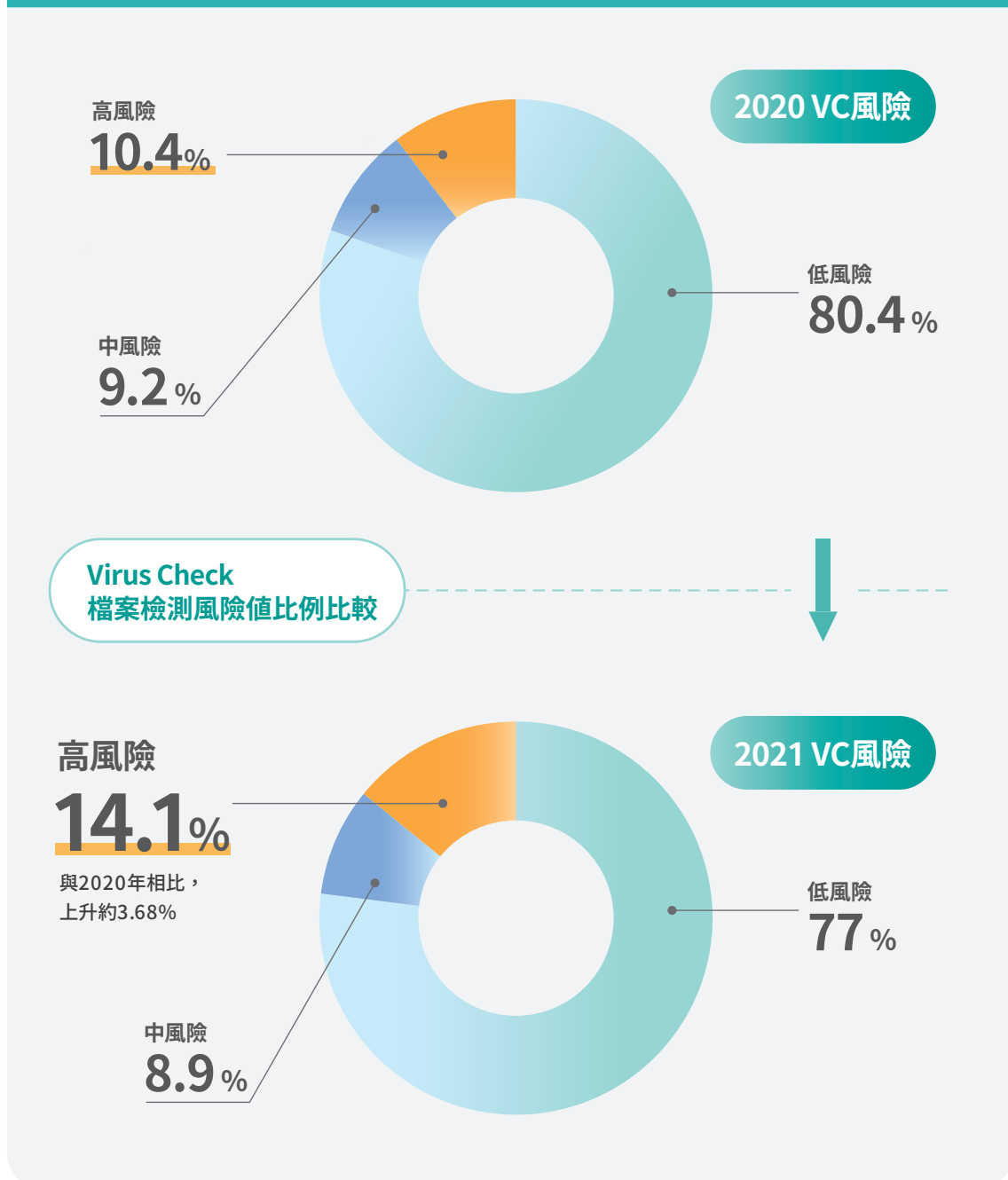


圖 13 Virus Check 網站示意圖



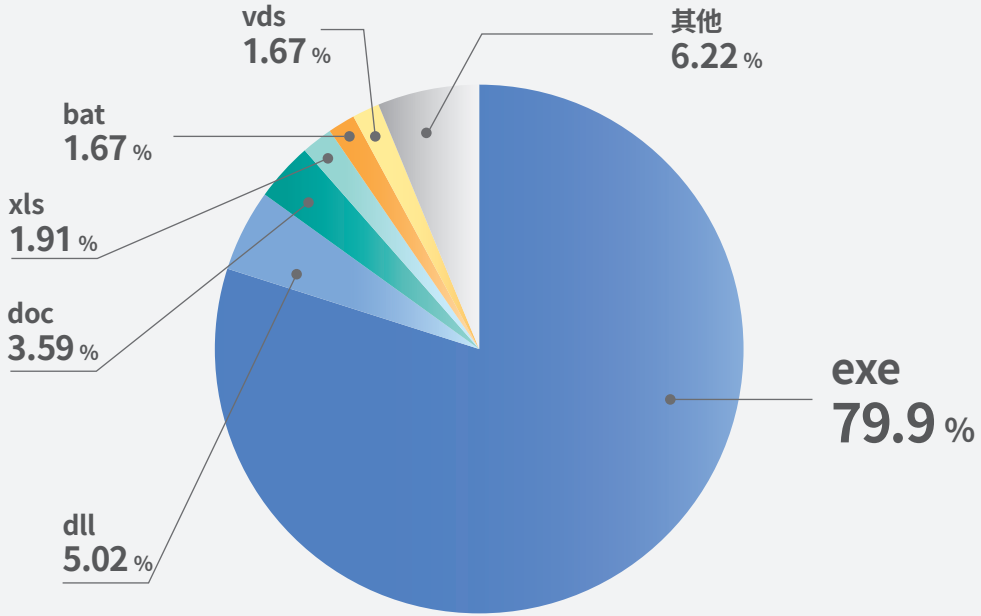
在 2021 年期間，TWCERT/CC 接獲逾上千筆檔案，與 2020 年相比，高風險檔案比例上升約 3.68%。

圖 14 TWCERT/CC 2021 Virus Check 檔案檢測風險值比例 (資料來源：TWCERT/CC 整理)



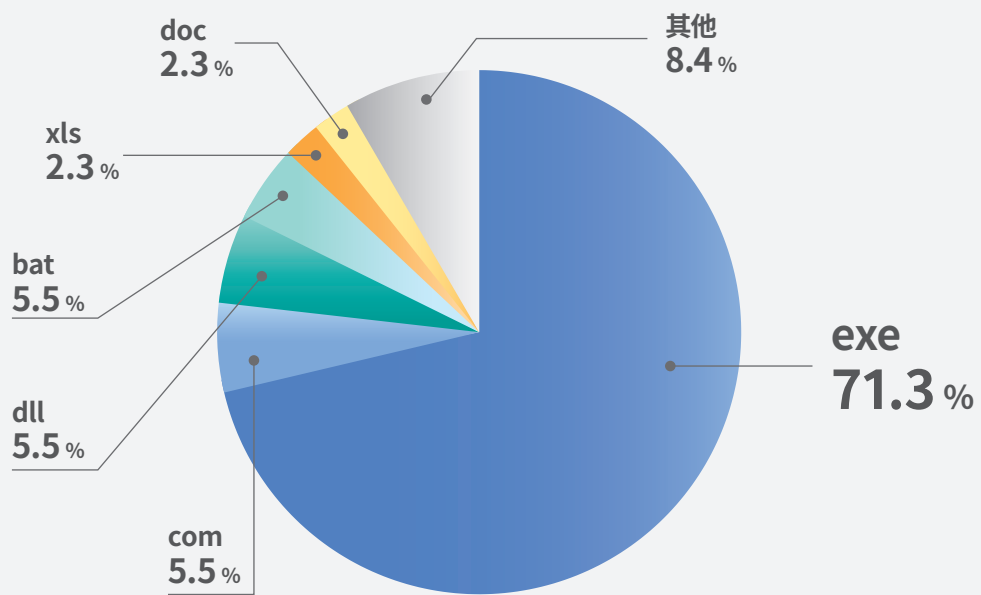
針對中高風險之檔案類型，2021 年 1 月至 12 月期間，共計逾 400 多個檔案中，數量最多前三名為可執行檔 exe 檔、可執行檔 com 檔與動態連結函式庫 dll 檔。與 2020 年相比，可執行檔 exe 檔仍舊佔大宗。

圖 15 TWCERT/CC 2021 Virus Check 檢測檔案中高風險檔案類型比例 (資料來源：TWCERT/CC 整理)



2020 中高險檔案比例

Virus Check 檢測檔案
中高風險檔案類型比例比較



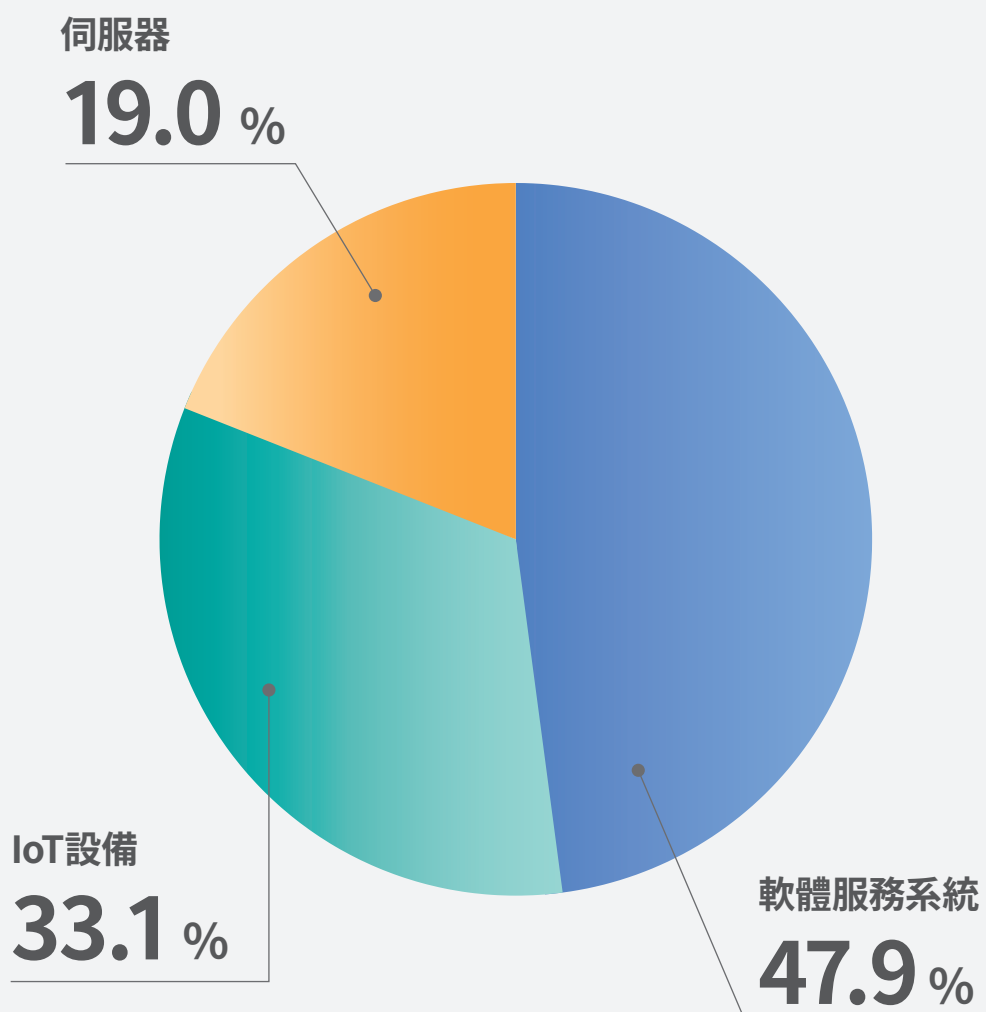
2021 中高險檔案比例

三、資安漏洞協處

(一) 我國發布之產品漏洞概況

在 2021 年期間，TWCERT/CC 總計接獲約 167 個漏洞通報，佔比最多為軟體服務系統。大部分漏洞通報來源為公司自身通報，而漏洞類型最多者為 Broken Access Control (權限控制失效)，顯示許多平臺未將使用者權限做有效管理，駭客能透過此漏洞、修改平臺任意帳號，甚至修改權限，植入惡意軟體於系統中。

圖 16 TWCERT/CC 2021 接獲漏洞類型 (資料來源：TWCERT/CC 整理)



TWCERT/CC 2021 審核發布 CVE 統計如下表

表 1-1 TWCERT/CC 2021 審核發布 CVE 統計表 (資料來源：TWCERT/CC 整理)

類型	產品類別	數量	編號
軟體服務系統	員工入口網站	3	CVE-2021-22850、CVE-2021-22851、CVE-2021-22852
	人薪系統	3	CVE-2021-22853、CVE-2021-22854、CVE-2021-22855
	網站平臺系統	2	CVE-2021-22847、CVE-2021-22849
	財產管理系統	3	CVE-2021-22856、CVE-2021-22857、CVE-2021-22858
	Web 公文系統	2	CVE-2021-22859、CVE-2021-22860
	郵件歸檔稽核系統	1	CVE-2021-22848
	電子簽核平臺	3	CVE-2021-28171、CVE-2021-28172、CVE-2021-28173
	智慧下單系統	1	CVE-2021-28174
	POS 系統	4	CVE-2021-30170、CVE-2021-30171、CVE-2021-30172、CVE-2021-30173
	電子簽核系統	1	CVE-2021-30174
	播課系統	1	CVE-2021-32544
	雲端辦公室平臺	2	CVE-2021-32539、CVE-2021-32540
	交易系統	3	CVE-2021-32541、CVE-2021-32542、CVE-2021-32543
	網站後臺管理	1	CVE-2021-32538
	門禁考勤系統	2	CVE-2021-35961、CVE-2021-35962

表 1-2 TWCERT/CC 2021 審核發布 CVE 統計表 (資料來源：TWCERT/CC 整理)

類型	產品類別	數量	編號
軟體服務系統	企業數位學習平臺	6	CVE-2021-35963、CVE-2021-35964、CVE-2021-35965、CVE-2021-35966、CVE-2021-35967、CVE-2021-35968
	出勤打卡系統	5	CVE-2021-37211、CVE-2021-37212、CVE-2021-37213、CVE-2021-37214、CVE-2021-37215
	安控元件	1	CVE-2021-37909
	行動入口網	2	CVE-2021-37912、CVE-2021-37913
	教務行政系統	9	CVE-2021-41563、CVE-2021-41564、CVE-2021-41565、CVE-2021-41566、CVE-2021-41567、CVE-2021-41568、CVE-2021-41974、CVE-2021-41975、CVE-2021-41976
	出納帳務管理系統	1	CVE-2021-42337
	教學平臺系統	4	CVE-2021-42329、CVE-2021-42330、CVE-2021-42331、CVE-2021-42332
	線上學習測驗平臺	4	CVE-2021-42333、CVE-2021-42334、CVE-2021-42335、CVE-2021-42336
	出納帳務管理系統	1	CVE-2021-42337
	政府組態基準設定與檢測	1	CVE-2021-42338
	圖書館管理自動化軟體	2	CVE-2021-42838、CVE-2021-42839

表 1-3 TWCERT/CC 2021 審核發布 CVE 統計表 (資料來源：TWCERT/CC 整理)

類型	產品類別	數量	編號
軟體服務系統	教育訓練管理系統	3	CVE-2021-43358、CVE-2021-43359、CVE-2021-43360
	政府組態基準設定與檢測	1	CVE-2021-44159
	健檢報告查詢系統	1	CVE-2021-44160
	行動動態密碼系統	1	CVE-2021-44161
	文字客服系統	3	CVE-2021-44162、CVE-2021-44163、CVE-2021-44164
	神網電腦終端防護系統	2	CVE-2021-45916、CVE-2021-45917
伺服器	網路服務伺服器	35	CVE-2021-28175、CVE-2021-28176、CVE-2021-28177、CVE-2021-28178、CVE-2021-28179、CVE-2021-28180、CVE-2021-28181、CVE-2021-28182、CVE-2021-28183、CVE-2021-28184、CVE-2021-28185、CVE-2021-28186、CVE-2021-28187、CVE-2021-28188、CVE-2021-28189、CVE-2021-28190、CVE-2021-28191、CVE-2021-28192、CVE-2021-28193、CVE-2021-28194、CVE-2021-28195、CVE-2021-28196、CVE-2021-28197、CVE-2021-28198、CVE-2021-28199、CVE-2021-28200、CVE-2021-28201、CVE-2021-28202、CVE-2021-28203、CVE-2021-28204、CVE-2021-28205、CVE-2021-28206、CVE-2021-28207、CVE-2021-28208、CVE-2021-28209

表 1-4 TWCERT/CC 2021 審核發布 CVE 統計表 (資料來源：TWCERT/CC 整理)

類型	產品類別	數量	編號
IoT 設備	網路攝影機	5	CVE-2021-30165、CVE-2021-30166、CVE-2021-30167、CVE-2021-30168、CVE-2021-30169
	網路儲存裝置	31	CVE-2021-32506、CVE-2021-32507、CVE-2021-32508、CVE-2021-32509、CVE-2021-32510、CVE-2021-32511、CVE-2021-32512、CVE-2021-32513、CVE-2021-32514、CVE-2021-32515、CVE-2021-32516、CVE-2021-32517、CVE-2021-32518、CVE-2021-32519、CVE-2021-32520、CVE-2021-32521、CVE-2021-32522、CVE-2021-32523、CVE-2021-32524、CVE-2021-32525、CVE-2021-32526、CVE-2021-32527、CVE-2021-32528、CVE-2021-32529、CVE-2021-32530、CVE-2021-32531、CVE-2021-32532、CVE-2021-32533、CVE-2021-32534、CVE-2021-32535、CVE-2021-37216
	多點視訊控制器	1	CVE-2021-32536
	音效卡驅動程式	1	CVE-2021-32537
	無線會議室投影機	1	CVE-2021-37911
	BAS 控制器	13	CVE-2021-41290、CVE-2021-41291、CVE-2021-41292、CVE-2021-41293、CVE-2021-41294、CVE-2021-41295、CVE-2021-41296、CVE-2021-41297、CVE-2021-41298、CVE-2021-41299、CVE-2021-41300、CVE-2021-41301、CVE-2021-41302
	無線路由器	2	CVE-2021-37910、CVE-2021-41289

(二) 國際資案事件與漏洞協處案例

1. 微軟 Exchange Server 漏洞

TWCERT/CC 接獲國際情資指出，微軟於 2021 年 3 月釋出 4 個微軟 Exchange Server 漏洞與安全性更新，我國與該漏洞相關情資總計近 400 筆 IP 受駭，相關受害 IP 已全數通報完畢：196 家企業、C-ISAC 195 筆。因該漏洞影響重大，亦發布相關漏洞資訊給聯盟成員和相關 ISAC 成員，以達聯防目的；同時亦發布相關新聞通知民眾和企業注意並更新。

2. Pulse Secure VPN 軟體的漏洞

TWCERT/CC 接獲國際情資指出，疑似有 UNC 2630 駭客組織利用 Pulse Secure VPN 軟體的漏洞 (CVE-2021-22893 0-day 漏洞) 攻擊美國國防產業、研究機構及設備製造單位。TWCERT/CC 接獲我國企業仍未修補漏洞之 IP 名單進行通報，相關受害 IP 已全數通報完畢，共通報 27 家企業，請其盡速進行安全性更新修補漏洞，並將此漏洞資訊分享給聯盟成員和相關 ISAC 成員，以達聯防之目的。

3. 美國燃油管道系統 Colonial Pipeline 遭勒索攻擊情資分享

TWCERT/CC 接獲國際情資指出，美國最大燃油管道系統 Colonial Pipeline 發布聲明稿，稱遭到俄國 DarkSide 勒索軟體組織攻擊，導致東海岸佛羅里達、紐約、德州等 18 州的燃油管道作業停擺，經濟損失嚴重。TWCERT/CC 與國際組織溝通了解狀況，在獲得相關事件威脅情資資訊後，隨即進行情資分析與整理，並將此漏洞資訊分享給 CERT/CSIRT 聯盟成員和相關 ISAC 成員 (T-ISAC、E-ISAC、N-ISAC 等)，以達重要資安情資分享、資安聯防之目的。

4. 國際資安情資分享通報

TWCERT/CC 多次接獲國際資安組織通知及通知我國具有資安漏洞的資訊系統情資。TWCERT/CC 為避免漏洞遭駭客利用，造成國內相關單位或企業受駭侵，隨即進行情資彙整與分析；並將此漏洞資訊分享給 CERT/CSIRT 聯盟成員和相關 ISAC 成員 (T-ISAC、E-ISAC、N-ISAC 等)，及相關企業組織，以達重要資安情資分享，資安聯防之目的。

表 2 國際資安情資分享 (資料來源：TWCERT/CC 整理)

月份	情資說明	具漏洞的 IP 數
110/06	Sonic Wall unpatched and end-of-life (EOL) 8.x firmware	62
110/08	Exchange Server	633
110/09	Fortinet VPN credential leaks	719
110/11	SQL Injection	195

(三) 國內資安事件與漏洞協處案例

1. 仿冒銀行登入頁面的釣魚網站通報

TWCERT/CC 陸續接獲仿冒銀行登入頁面的釣魚網站通報，駭客透過簡訊通知銀行客戶釣魚網址，意圖竊取帳密資訊等個資，再進一步竊取帳戶之金錢。TWCERT/CC 隨即進行釣魚網站通報，累計通報 81 筆釣魚網站通報，受害範圍涵蓋國內 6 間銀行。並依照調查局和刑事警察局之來函，同步請 ISP 業者協助屏蔽相關釣魚網頁，避免更多民眾受害。因本次通報受害對象眾多，TWCERT/CC 已於官網發布提防假冒銀行之網路釣魚詐騙的資安小知識宣導，提醒民眾多加防範相關釣魚手法。

2. 某光電駭侵相關情資分享報告

TWCERT/CC 亦接獲某科技公司通報，發現系統存在可疑檔案與連線紀錄，提供相關可疑檔案進行分析協處，分析後了解為透過 MS Proxy Logon 漏洞之駭侵事件，所幸該公司及早發現入侵之跡象，未擴大受害情況。經通報單位同意，TWCERT/CC 將相關入侵威脅指標 (Indicator of Compromise, IoC) 的研究報告分享給聯盟成員和相關 ISAC 成員，以達聯防之目的。

3. 某 PC 製造企業遭勒索攻擊情資分享

我國知名 PC 製造企業遭受 Sodinokibi (REvil) 勒索軟體攻擊，TWCERT/CC 深怕此攻擊亦會針對國內相關或其他企業發動，便積極與有關企業聯繫，期望能獲得相關事件資訊，分享給其他企業以達到聯防之目的。TWCERT/CC 透過聯盟成員的協助聯繫與說明，獲得受駭企業授權分享此次資安事件相關威脅指標等資訊。彙整相關資訊，包含中繼站資訊、病毒資訊、駭客入侵威脅指標 (Indicator of Compromise, IoC)、駭客入侵攻擊策略 (Tactics, Techniques and Procedures, TTPs) 及主機重建確認事項等情資資訊與建議，提供分享給聯盟成員相關 ISAC 成員以利進行相關防護與自我檢測。

4. 公私部門攜手合作，力抗跨國殭屍網路

QNAP 透過 TWCERT/CC 與調查局聯繫，並主動提供相關受駭 Qsnatch 惡意樣本及全球受駭 IP 清單。經調查局追查，發現全球受

駭裝置總數約 6 萬 3,000 筆，經長時間監控，未發現該駭客組織有進一步的駭侵行爲。TWCERT/CC 居間協調國內電信業者協助通知國內 2,419 名受駭用戶，移除惡意程式及手動更新系統軟體，其他非屬臺灣管轄範圍的受駭裝置，由台灣網路危機處理暨協調中心協助向國際組織通報。

調查局感謝台灣網路危機處理暨協調中心等共同打擊不法殭屍網路，落實全球資通安全，並立下新里程碑。

圖 17-1 公私部門攜手合作，力抗跨國殭屍網路（資料來源：TWCERT/CC 整理）

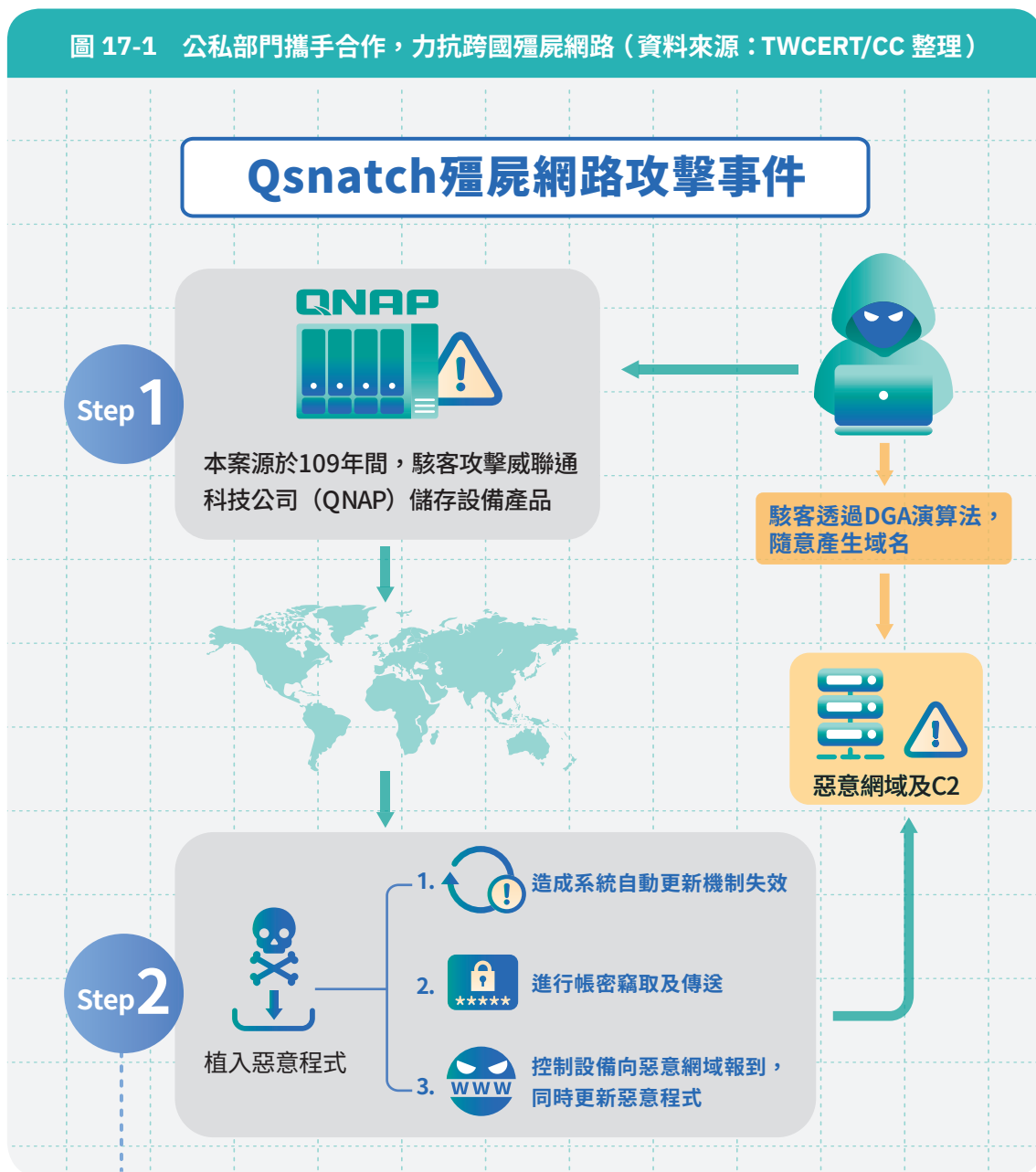
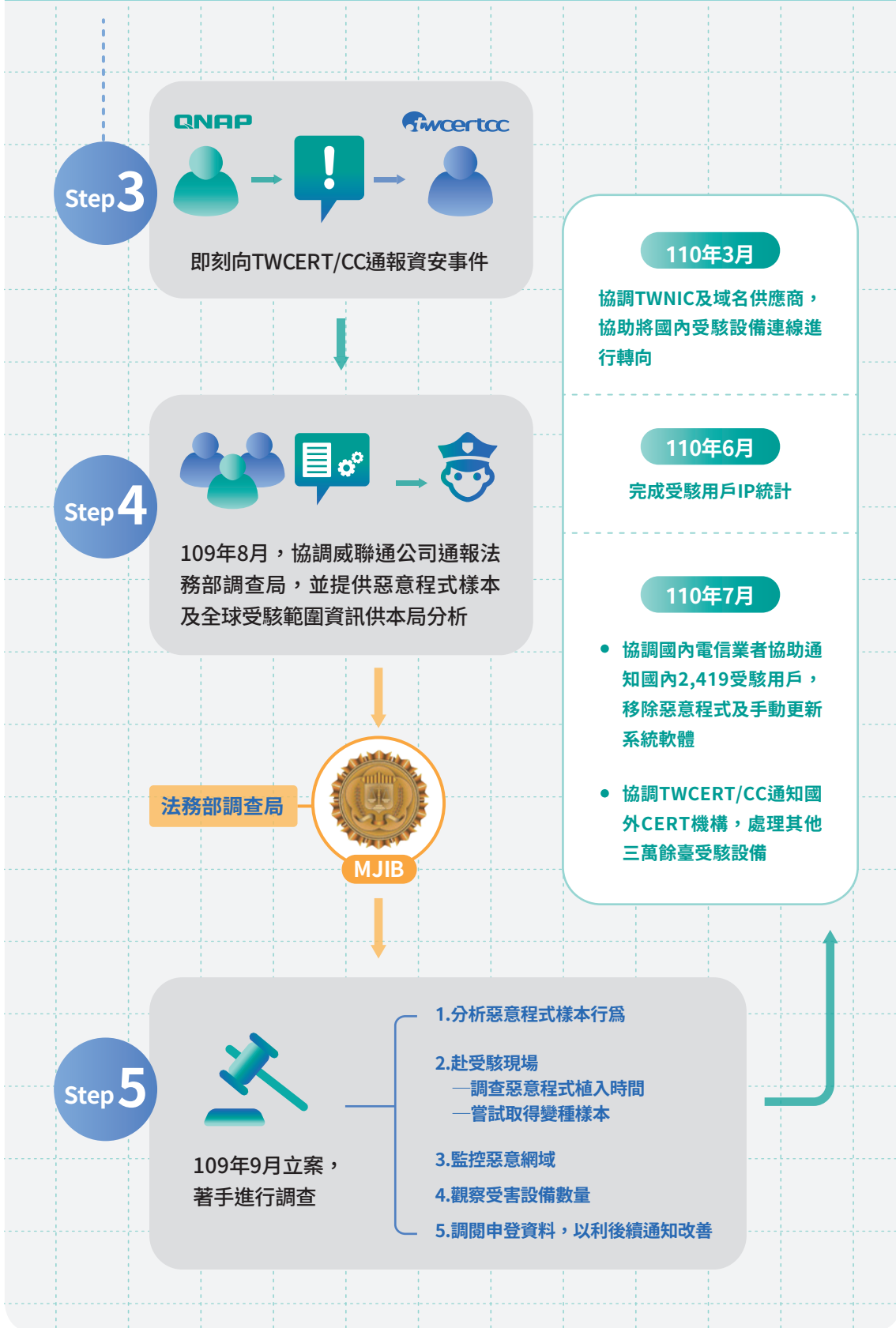


圖 17-2 公私部門攜手合作，力抗跨國殭屍網路（資料來源：TWCERT/CC 整理）



- 幫助國內企業組織對抗勒索軟體，TWCERT/CC 設立勒索軟體防護專區
在行政院國家資通安全會報與國家通訊傳播委員會（NCC）的支持下，TWCERT/CC 於官網新增設了勒索軟體防護專區，並設計了獨立的入口網站（antiransom.tw），提供臺灣企業組織使用，事前預防、事中處理與事後回復的因應，都讓企業能更有著手方向，並在每個階段提供相對應的指南、資源與自評等內容，更設計了檢核表，幫助企業透過更簡單的方式，來檢視自身的行動。

圖 18 TWCERT/CC 勒索軟體防護專區

勒索軟體防護專區

什麼是勒索軟體
勒索軟體是一種惡意軟體，以加密設備上的文件來威脅受害者，要求受害者支付贖金（通常是加密貨幣）才能解密文件。並不斷演變出新的變種，或與其他惡意軟體結合形成更有威脅的攻擊行為，而影響到服務或企業的正常運作。

事前預防
勒索軟體攻擊預防措施
了解更多

事中處理
被勒索軟體攻擊時的應變措施
了解更多

事後回復
回復階段的作法
了解更多

資安事件報案
法務部調查局
service@mjb.gov.tw
刑事警察局
cib.noransom@cib.npa.gov.tw

資安事件通報
TWCERT/CC
資安事件通報
https://www.twcert.org.tw/

指導單位：NCSST 行政院國家資通安全會報 National Information & Communication Security Taskforce
國家通訊傳播委員會 NATIONAL COMMUNICATIONS COMMISSION

Email: twcert@cert.org.tw | 隱私權及安全政策 | 使用說明

Copyright © TWCERT/CC 台灣電腦網路危機處理暨協調中心 2021-2022

PART 3

參、合作交流與 資安推廣

一、主辦活動

(一) 台灣資安通報應變年會

2021 年台灣資安通報應變年會活動除了以往的宣導資安通報意識外，更強化臺灣公私部門「超前布署，及早資安聯防」的概念與執行作法，針對事前、事中、事後資安應變防護、企業建置資安相關政策或組織、國內 ISAC 組織之經驗分享。

本次活動以「跨域聯防—建構韌性安全的數位環境」為核心主題，邀請國家通訊傳播委員說明了 5G 萬物聯網時代的安全供應鏈管理與 NCC 的 3 個創新作為。同時，面對全球共通的勒索攻擊威脅，規劃了國際座談「他山之石：他國如何做到公私聯防，提升資安綜效」，由台灣網路資訊中心黃勝雄董事長主持，邀請日本 JPCERT、印度 CERT-In 與泰國 ThaiCERT 進行與談。現場還邀請了奧義智慧與鴻海研究院進行議題分享。



圖 19 台灣資安通報應變年會活動剪影（資料來源：TWCERT/CC 整理）

除此之外，亦邀請國家資通安全會報技術服務中心主持高峰座談會，與日月光集團、華碩電腦與威聯通探討高科技業的資安防禦關鍵與可行的聯防之道。



圖 20 台灣資安通報應變年會活動剪影

在眾多與會者中，高科技產業為大宗，佔 28%，其餘依序為製造業與政府單位。多數與會者全程參與年會，對兩場專題座談與專題演講非常有興趣，更認為本次應變年會對企業及未來資安政策制定意義相當重大，超過 99% 的民眾期待明年再次參加資安應變研討會。



圖 21 台灣資安通報應變年會活動剪影

圖 22 聽眾出席行業別分析 (資料來源：TWCERT/CC 整理)

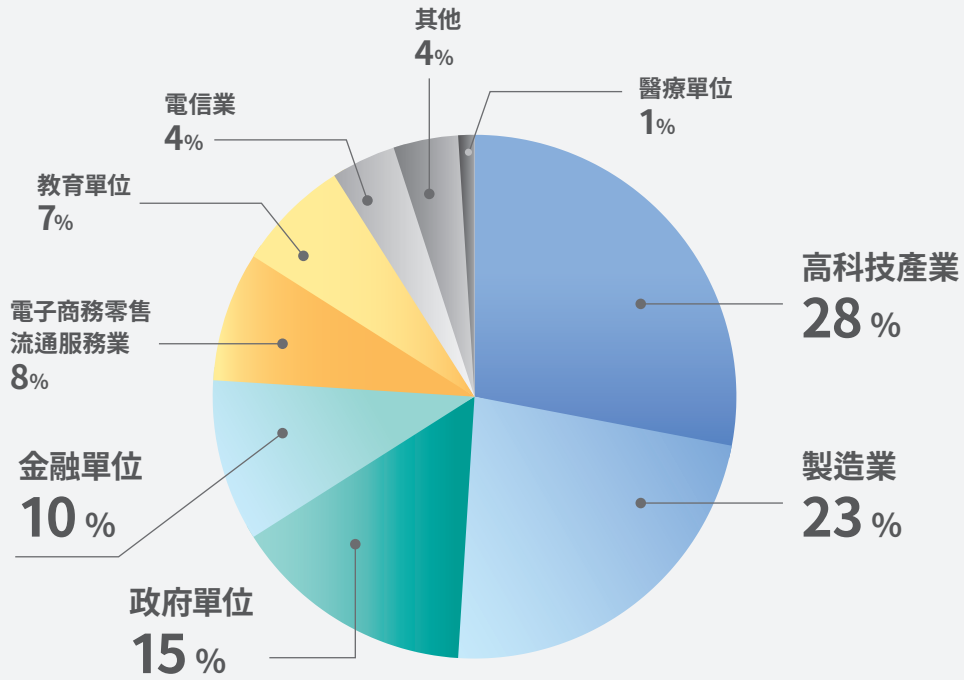
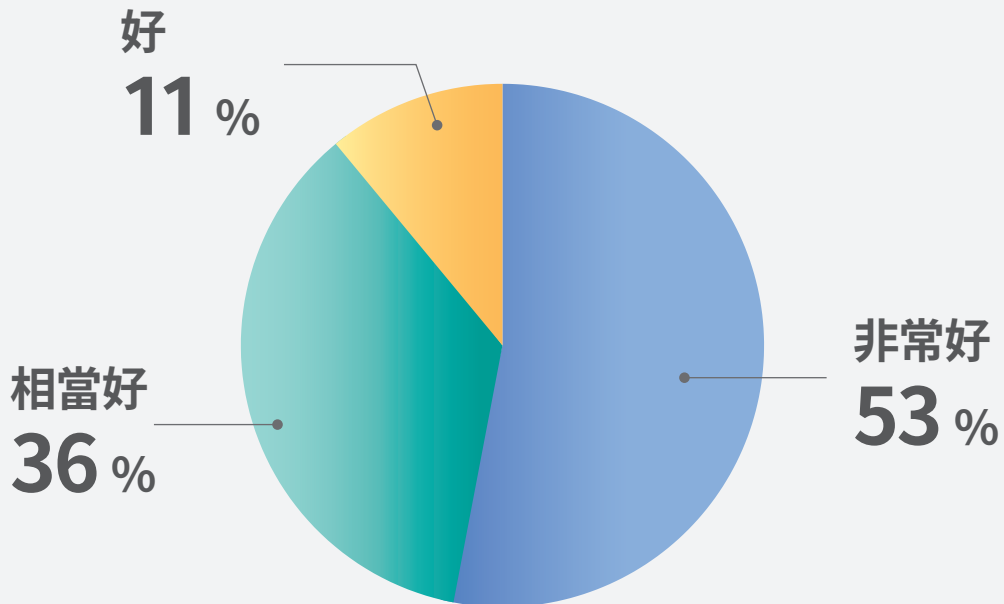


圖 23 研討會整體滿意度 (資料來源：TWCERT/CC 整理)



從整體統計分析顯示，此次台灣資安通報年會已確實達到宣傳資安意識、提升品牌認知、增添資安通報意願與強化臺灣公私部門「超前布署，及早資安聯防」的概念與執行作法之目的。

(二) 台灣 CERT/CSIRT 聯盟交流會議

為讓臺灣各 CERT/CSIRT 和企業單位有固定聯繫管道、互通國內資安情資交流，由 TWCERT/CC 整合國家電腦事件處理中心 (Taiwan National Computer Emergency Response Team, TWNCERT)、國家通訊暨網際安全中心資安通報應變平臺 (NCCSC C-CERT)、台灣學術網路危機處理中心 (TANet Computer Emergency Response Team, TACERT)、經濟部商業司及民間企業單位等，共同組成之「台灣 CERT/CSIRT 聯盟」，結合產業與民間社群能量進行資安意識推廣。

2021 年度除了召開聯盟成員會議，分享資安新訊和聯盟成員進行資安資訊交流外，亦舉辦二場教育訓練，協助聯盟成員提升資安能力，強化臺灣資訊安全的防護網。

1. 聯盟成員會議

共有 42 個單位、73 個成員參與，本次會議邀請 TeamT5 杜浦數位及華碩電腦，分享近期資安議題、漏洞通報機制與 CVE 申報經驗分享。統計本次聯盟會議的會後滿意度調查，參與學員的整體滿意度為 4.63；而對於本次會議邀請講者分享內容滿意度為 4.61（本滿意度調查採 5 分法尺度）。



圖 24 2021「台灣 CERT/CSIRT 聯盟」交流會議

2. 「台灣 CERT/CSIRT 聯盟」資安教育訓練（一）

本次教育訓練講師由 TWCERT/CC 團隊擔任，針對資安事件通報與 IoC 應用實務，帶領聯盟成員進行實機操作。本次活動共計 31 個單位、46 位與會者參加，針對本次教育訓練，參與學員的整體滿意度 4.83，課程內容滿意程度 4.70，講師專業滿意程度 4.80（本滿意度調查採 5 分法尺度）。



圖 25 2021 第一次「台灣 CERT/CSIRT 聯盟」資安教育訓練實況

3. 「台灣 CERT/CSIRT 聯盟」資安教育訓練（二）

本次教育訓練，講師以威脅獵捕為題，帶學員們實務動手來學習體驗，如何在企業內部找出可能的駭客攻擊軌跡，帶領聯盟成員進行實機操作。本次活動共計 24 位與會者參加，針對本次教育訓練，參與學員的整體滿意度 4.85。



圖 26 2021 第二次「台灣 CERT/CSIRT 聯盟」資安教育訓練實況

二、國際交流

2021 年 TWCERT/CC 參與多場國際交流會議，以了解國際資安發展之趨勢和現況，藉此會議提升自身的資安能量，並提升國際聯防與 TWCERT/CC 資安通報之分析、處理及資安意識推廣能量。參加之會議包含亞太網路資訊中心（Asia-Pacific Network Information Centre, APNIC）主辦之 APNIC 論壇、FIRST（The Forum of Incident Response and Security Teams）Conference 2021 以及 NatCSIRT 2021 等會議。除參與國際會議外，TWCERT/CC 亦於 APEC 暨 TELWG 線上大會中分享我國跨國聯防之資訊、於 APNIC 52 線上論壇中分享我國之 ProxyLogon 侵駭案例，並參加 2021 APDrill 國際網路安全攻防演練，以下為詳細介紹。

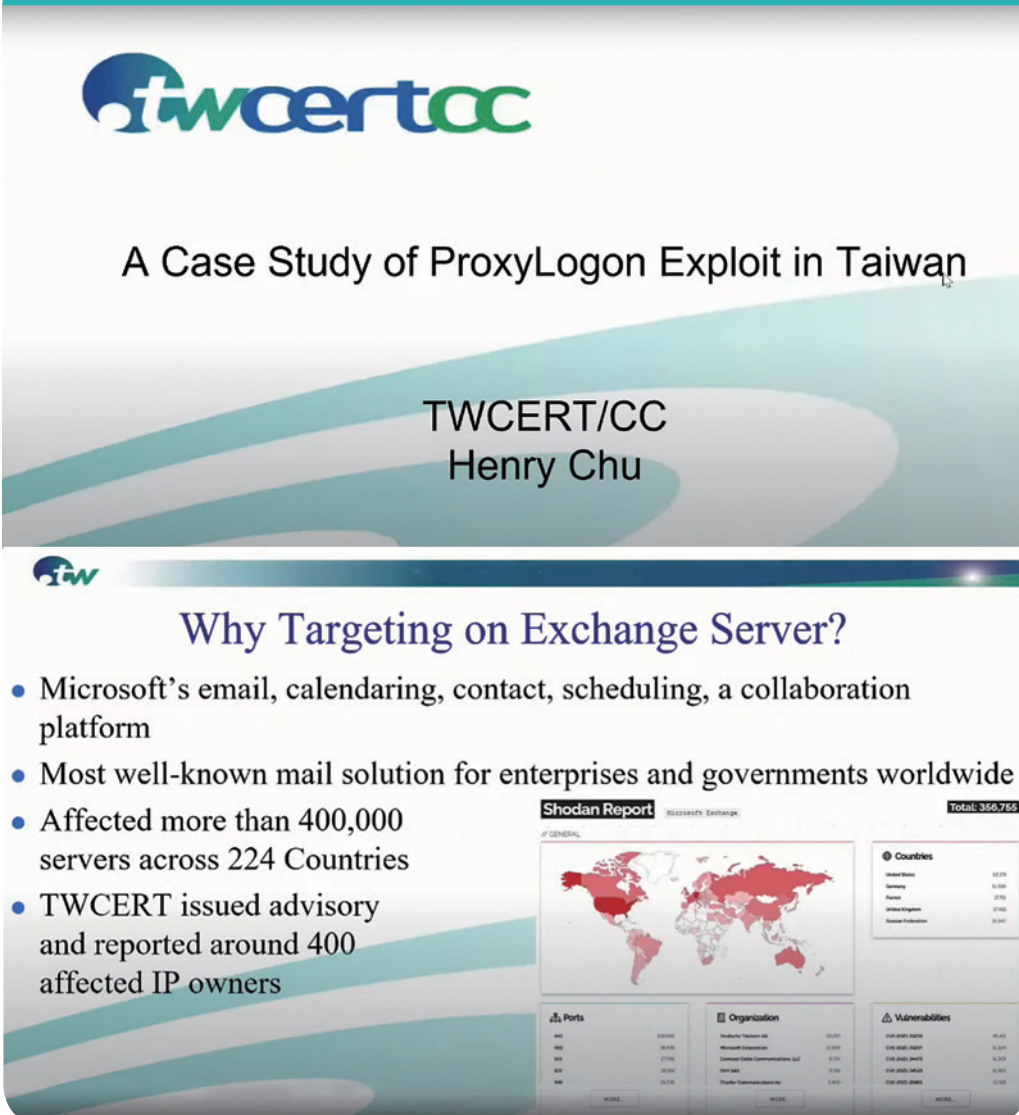
（一）APEC 暨 TELWG 線上大會

亞太經濟合作會議（APEC）之電信暨資訊工作小組（TELWG）會議主要目的是針對亞太 21 個經濟體，於目前在通訊領域發展現況進行報告。其中 APEC Security and Prosperity Steering Group（SPSG）小組主要為促進網路資訊安全與網路犯罪防治。本次會議 TWCERT/CC 前往國家通訊傳播委員會（NCC）共同參與，亦於 SPSG 小組分享中，提供促進我國資訊安全和在跨國領域資安聯防中之相關服務資訊的分享。

（二）APNIC 52 線上論壇

參與本次 APNIC First Security 1 & 2 場次演講，主題為「A Case Study of ProxyLogon Exploit in Taiwan」，Proxylogon 為微軟 Exchange 最嚴重漏洞之一，2021 年初廣泛被多個駭客組織利用於全球駭侵攻擊。本次演講意旨為透過臺灣實際駭侵事件協處進行案例分享，與全球資安專業人士進行經驗交流與分享。

圖 27 APNIC 52 線上論壇 https://www.youtube.com/watch?v=sn_oIgm1mLc
(資料來源：TWCERT/CC 整理)



twcertcc

A Case Study of ProxyLogon Exploit in Taiwan

TWCERT/CC
Henry Chu

Why Targeting on Exchange Server?

- Microsoft's email, calendaring, contact, scheduling, a collaboration platform
- Most well-known mail solution for enterprises and governments worldwide
- Affected more than 400,000 servers across 224 Countries
- TWCERT issued advisory and reported around 400 affected IP owners

Shodan Report Microsoft Exchange **Total: 356,765**

Countries

United States	10,279
Germany	6,536
France	2,976
United Kingdom	2,740
Canada	2,544

Ports

443	239,005
444	69,116
445	27,794
447	23,242
448	23,278

Organization

Reductive Network AG	21,271
Microsoft Corporation	17,891
Comcast Cable Communications, LLC	17,816
VeriSign	17,102
Charter Communications Inc	16,612

Vulnerabilities

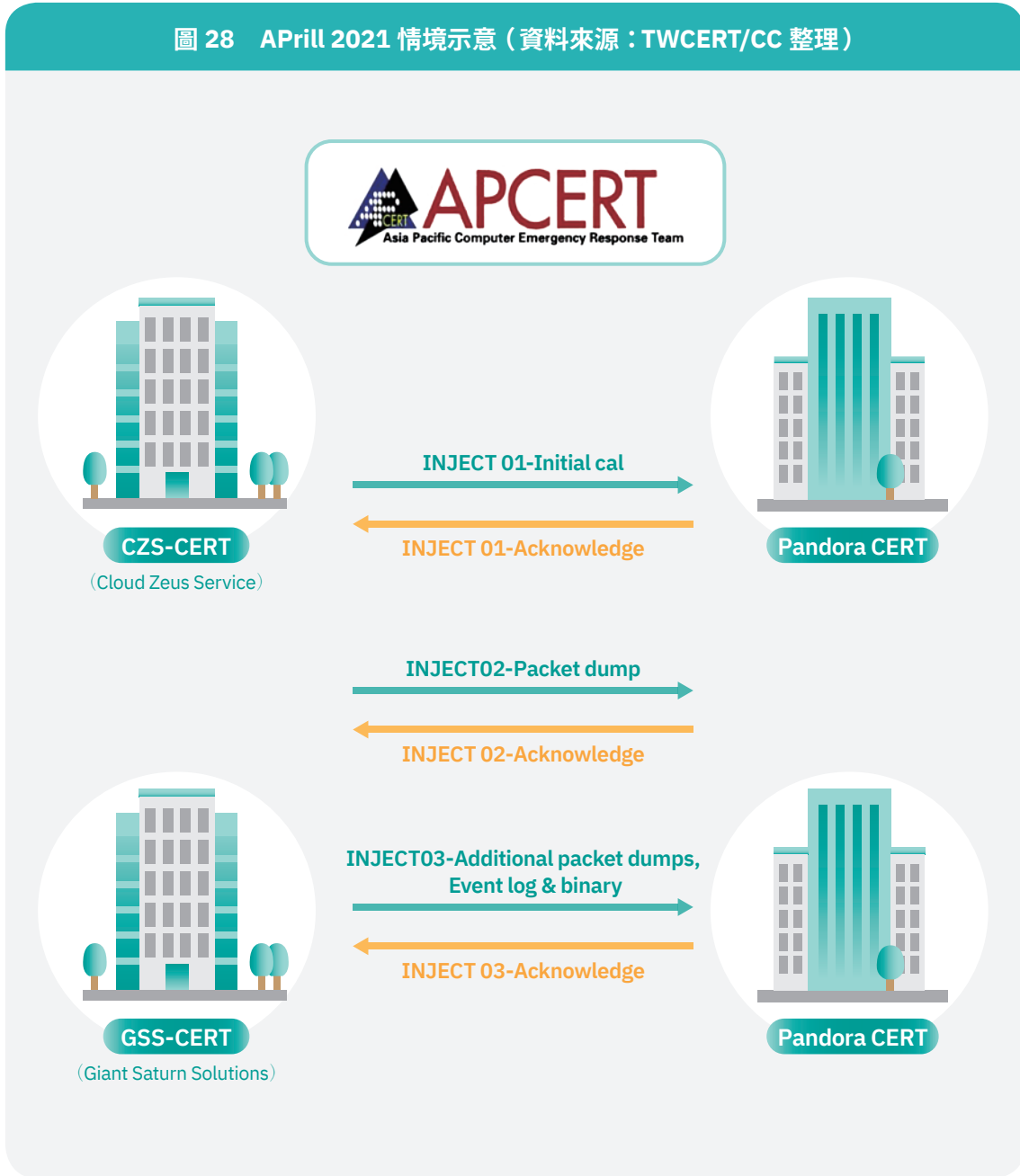
CVE-2020-14725	45,402
CVE-2020-14727	16,319
CVE-2020-14728	14,311
CVE-2020-14729	14,311
CVE-2020-14730	12,311

65

(三) 2021 APDrill 國際網路安全攻防演練

APDrill 為 APCERT 組織成員每年固定會舉辦的一次資安通報演練，TWCERT/CC 作為 Drill 工作小組成員，每年皆會參與亞太地區通報演練活動並與相關工作小組成員進行演練活動規劃討論。本年度 Drill 活動由 KrCERT/CC 主導策劃，並舉行參與成員演練主題討論會議 (PreDrill)，討論訂出今年度演練主題為「產業鏈釣魚攻擊」，並決議出演練中所需要進行分析情資的項目，包含檔案雜湊值 (Hash) 與釣魚郵件分析、相關情資整理及統整情資後的分享模式等。

圖 28 APDrill 2021 情境示意 (資料來源：TWCERT/CC 整理)



TWCERT/CC 參與 2021 APDrill 國際通報協處演練，和各國 CERT 成員進行演練主題為「產業鏈釣魚攻擊」，總共有來自 19 個 APCERT 亞太經濟體參與，台灣電腦網路危機處理暨協調中心 (Taiwan Computer Emergency Response Team /Coordination Center, TWCERT/CC) 作為臺灣參與此次 APCERT Drill 演練的代表團隊之一，認真達成每個階段的任務目標，為 25 個參與單位中唯一於時間內完成本次演練各任務的團隊。透過參與國際合作的大型演練有助於 TWCERT/CC 優化情資分享流程及事件應變能力，強化臺灣資安能量的同時促進資安跨域聯防的正向發展。

三、國內交流

(一) TWCERT/CC 企業資安推廣與分享

因資安議題相當廣泛，爲了協助企業組織更精確地提升該產業之資安防護能量，TWCERT/CC 常與各產業協會合作交流，針對特定產業領域，進行演講或交流，藉此提升該產業成員及組織之資安意識與能量。

首先 TWCERT/CC 針對中小企業需求，分別與桃園市中小企業協會、台中市電腦商業同業公會、國立中山大學、彰化電腦商業同業公會與臺北市中小企業協會合作，於 5 個縣市各舉辦一場「資訊安全防護及案例分享研討會」，總計逾百人參與研討會，整體表現皆具高滿意度。



圖 29 臺北場「資訊安全防護及案例分享研討會」

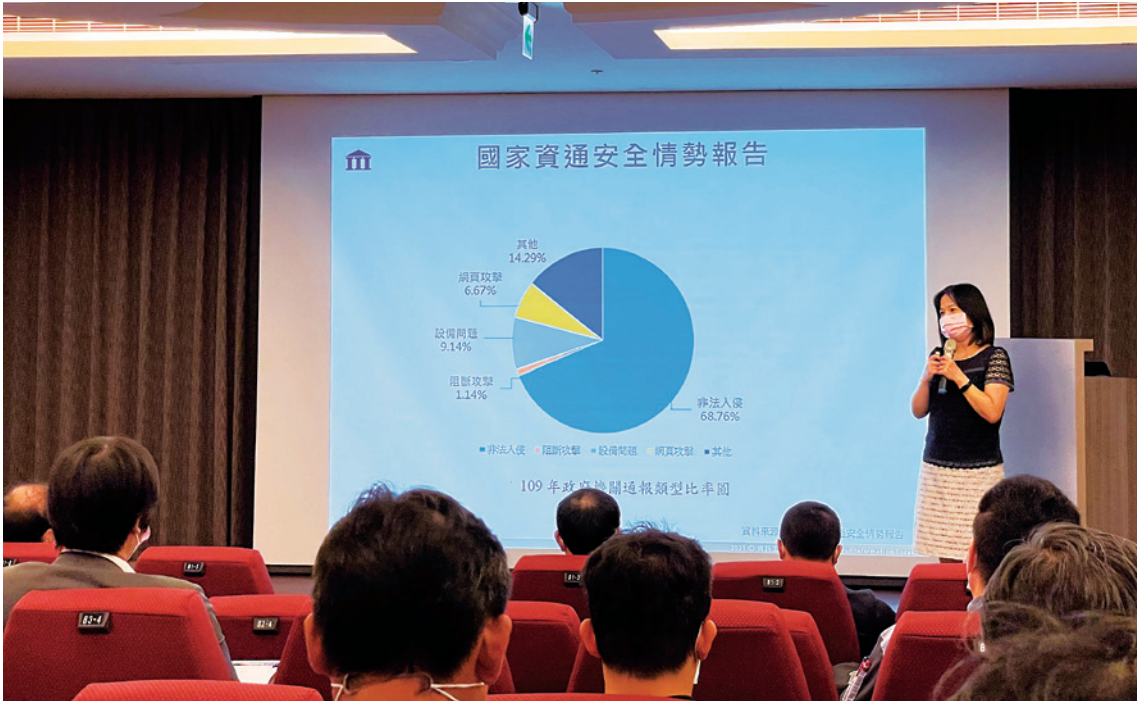


圖 30 臺中場「資訊安全防護及案例分享研討會」



圖 31 彰化場「資訊安全防護及案例分享研討會」



圖 32 桃園場「資訊安全防護及案例分享研討會」

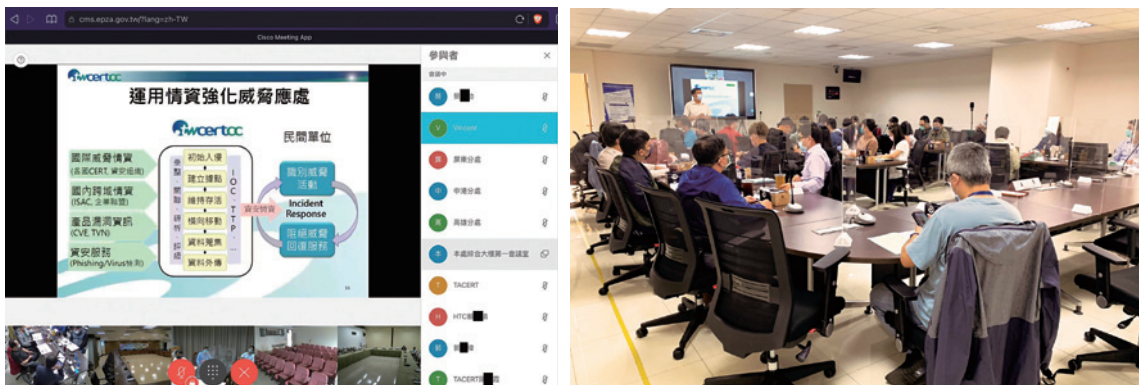


圖 33 高雄場「資訊安全防護及案例分享研討會」



圖 34 資訊安全防護及案例分享研討會（海報）

除了與公協會合作舉辦研討會外，TWCERT/CC 亦積極協助政府提升企業組織強化資安情資分享，提升資安事件通報應變能量。TWCERT/CC 作為講師參與證交所針對上市上櫃公司資安人員或主管，所舉辦的資安宣導說明會，介紹 TWCERT/CC 資安聯盟服務暨入會申請流程及技術分享，共 168 人參與，透過證交所對上市、櫃公司推廣，以吸引更多會員參與。



圖 35 介紹 TWCERT/CC 服務暨入會申請流程活動剪影

(二) TWCERT/CC 社群資安研討與分享

TWCERT/CC 除參與對企業推廣資安服務的活動外，亦共同推廣單位參與多場國內交流會議，期許提高 TWCERT/CC 組織的國內外知名度，以利逐步提高企業信任度，包含台灣資安大會以及第三十一屆全國資訊安全線上會議 (CISC)，並參與特定社群的資安會議，以針對特定領域之資安相關議題進行演講交流，例如 2021 自動化機械暨智慧製造展 (臺南展)、2021 TWNIC「IPv6 暨資安推廣講座」與 HITCON Pacific 2021，以下為詳細介紹：

1. 2021 自動化機械暨智慧製造展 (臺南展)

TWCERT/CC 主要參與「智慧製造資訊專區」之活動，此專區結合 5G、SI、ERP、CRM、資安、硬體等眾多智慧製造跨領域能量，建立 5G 智慧製造資訊鏈，向南臺灣製造業相關業者進行資安宣導與資安服務推廣。

本次活動除了擺攤近距離推廣 TWCERT/CC 服務內容，吸引民眾了解 TWCERT/CC 之服務外，更於現場推廣 FB 粉絲團與資安電子報的訂閱，期望參觀民眾能長期關注資訊安全之議題。除此之外，TWCERT/CC 也舉辦「資安防護及案例分享研討會」，邀請數聯資安分享「自動化機械製造數位轉型資安面面觀」之主題，和關心智慧製造與數位轉型衍生之資安問題的製造業者共同討論相關轉型案例與資安議題。此外 TWCERT/CC 亦於座談會中推廣說明「TWCERT/CC 相關的資安服務」，獲得高滿意度。

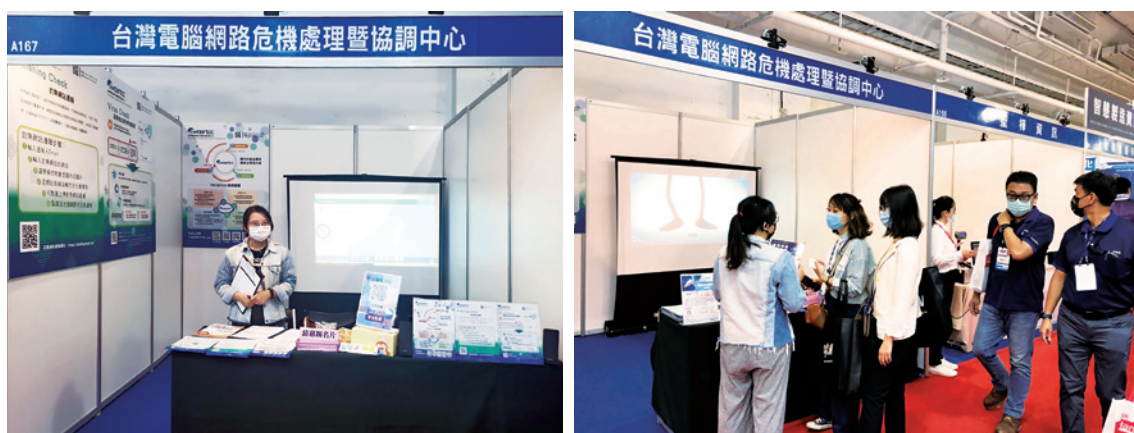


圖 36 台南自動化機械暨智慧製造展

2. 2021 TWNIC「IPv6 暨資安推廣講座」

此活動由 TWNIC 及 TWCERT/CC 主辦，並由高雄市電腦商業同業公會及 (ISC)² Taipei Chapter 共同協辦。活動安排 IPv6 應用服務介紹與資安議題演講，針對情資通報、IPv6 應用情境以及 IPv6 網路安全進行探討，並以座談會形式分享 IPv6 網路建置以及服務經驗。

3. HITCON Pacific 2021

TWCERT/CC 作為協辦單位參與由社團法人台灣駭客協會之 HITCON Pacific 2021 線上研討會。TWCERT/CC 於 HITCON Pacific 2021 中介紹 CVE 漏洞態勢、審查與揭露機制，由資安漏洞生命週期，探究漏洞未被有效修補的根因，並建議除 CVSS Base Metric 外，亦將 Temporal/Environmental Metric 納入考量，綜合評估 Exploit 成熟度、修補程式有效性、系統關鍵性等外部因子，做優先度評級，以配置資源進行有效的資安漏洞處理。藉由漏洞資訊與資安情資回饋強化，將可促進資安威脅的防禦綜效。

結語

隨著網際網路的發展與 IoT 應用擴大，病毒傳播的管道也變得更多元，從社群媒體、即時通訊，以及智慧家庭都可能產生資安威脅，不論個人、企業組織，乃至國家單位，都有可能是受駭目標。

2021 年持續受到 Covid-19 影響，企業組織與大眾之工作與生活皆受到廣泛影響。企業組織為維持營運，大幅採用遠距辦公或是在家辦公，因此各種網路服務用量大增，身分驗證與遠端存取相關應用的漏洞與網路攻擊也大幅增加，助長勒索即服務 RaaS 的犯罪模式。為防範資安問題，企業組織應定期進行系統更新、安裝防護軟體、妥善做好權限管理與對員工進行社交工程演練等措施，並參考 TWCERT/CC 勒索軟體防護專區，針對各階段措施指南進行相關資安檢核。

社群媒體與即時通訊，在疫情時代進行生活與工作社交的應用更加廣泛，大眾應避免將個資曝光於社群軟體上，以及避免下載、點擊或開啟不明的檔案與連結，對可疑檔案透過 TWCERT/CC 的 Virus Check 系統檢測，降低因惡意檔案帶來的資安風險。隨著雲端應用與 IoT 設備的蓬勃發展，IoT 設備已成為人們日常生活中的一部分，為提高消費性產品之資安防護能量，政府已制定相關法規以確保產品之安全性，使用者選購產品時，應選擇通過資安檢測之產品以降低資安風險。

除了惡意程式外，資通訊產品之資安漏洞也是極大的威脅來源，TWCERT/CC 參與 MITRE 的 CVE 計畫，為臺灣地區之 CNA，接收國內產品的資安漏洞情資，審核後提供 CVE 編號並發布。為協助企業提升產品安全性，TWCERT/CC 持續優化漏洞通報流程，並且提供廠商漏洞緩解及修補諮詢，以降低產品漏洞造成受害的影響層面及範圍。

資訊社會的時代，單打獨鬥的資安防護模式已無法對抗快速且複雜的資安攻擊，為強化資安情資分享效率與聯防能量，維護我國之資通訊安全，TWCERT/CC 持續擴大與國內外資安組織合作，建立資安情資交流管道，同時為因應 STIX 改版，將進行相關情資通報功能改版，優化情資分享流程與平臺，以加強情資分享之效率。TWCERT/CC 亦積極主協辦及參與國內外組織交流合作，增加資安通報協處能量，並協同公私部門資源，協助處理企業資安事件及提供企業資安事件處理參考指南，以增強企業資安應變能力，增進企業對 TWCERT/CC 信任度。

此外，為增加網路使用安全性，提升企業與大眾之資安意識不容忽視，TWCERT/CC 持續收集國內外資安政策、威脅與趨勢、駭客攻擊事件、軟體漏洞及資安情資分享統計分析等資訊，研擬中英文專題月報與規劃製作資安宣導影片等，藉由多方管道，包括每月電子報、Line 與 Facebook 等社群媒體提供即時的資安新聞與預警，並結合公協會、資安社群、政府單位等舉辦資安主題研討會活動與教育訓練，將資安訊息傳遞給更多使用者，期盼提升整體網路安全，讓所有人都能使用安全便利的網路環境。

圖 37 TWCERT/CC 情資分享與資安服務概要

資安跨域聯防與情資分享

- 資訊去識別化 (Anonymization)
- 遵守情資交換協定 (Traffic Light Protocol, TLP)，確保妥適運用

釣魚網站協處

- 跨境協處偽冒企業網站之釣魚網站
- phishingcheck.tw

惡意檔案檢測

- 檢測可疑檔案，避免機敏檔案外洩
- 整合靜態檢測與沙箱 (Sandbox) 之動態分析機制，檢知潛藏惡意程式
- viruscheck.tw

TLP 情資交換協定

-  RED 限與會者
-  AMBER 限參與者組織內
-  GREEN 限資安社群間
-  WHITE 公開資訊



釣魚網站通報
Report



惡意檔案檢測服務
Virus Check

遠距辦公資安專區

- 因應遠距辦公資安需求，提供個人、企業、VPN、線上會議等安全小錦囊

勒索軟體防護專區

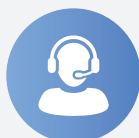
- 因應勒索軟體威脅，提供事前預防、事中處理與事後回復之指南與檢核表
- <https://antiransom.tw>

TWCERT/CC 台灣電腦網路危機處理暨協調中心

TWCERT/CC是我國企業資安事件通報及協處窗口，將提供企業資安事件諮詢及協調協處服務，推動資安情資分享、舉辦資安宣導活動，厚植企業資安認知，亦為我國對國外CERT組織聯繫窗口，促進國際資安交流合作，共同維護臺灣網路安全，提升臺灣整體資安防護能量。



國際資安事件聯防
International
Collaborative Cyber
Defense



跨國資安情報交流
Cross-National Cyber
Intelligence Exchange



企業資安通報轉介
Entrepreneurial
Cybersecurity Incident
Referral



情資收集資安宣導
Cyber Intelligence
Collection and
Cybersecurity
Outreaches

附錄一、遠距辦公資安防護建議

由於受 COVID-19 持續影響，許多企業仍實施居家辦公或是採取混合辦公模式，即員工能選擇在家上班或是至辦公室。企業為了讓員工遠距辦公時，仍能迅速因應企業可能遭遇之各種緊急事件與保障遠距存取企業內部網路的安全性，紛紛導入遠端視訊會議（video-teleconferencing，VTC）相關系統與虛擬私人網路（Virtual Private Network，VPN），但也增加了資安的潛在風險。因此為避免發生資安事件，企業在實施遠距辦公同時，企業與員工應積極做好資安準備，守護企業重要商業資產的安全性。

為協助企業降低實施遠距辦公帶來的資安風險，TWCERT/CC 分別針對企業、員工、遠距會議以及 VPN 提出相關資安防護指南，如下：

企業篇：

圖 38-1 遠距辦公資安防護指南—企業篇（資料來源：TWCERT/CC）

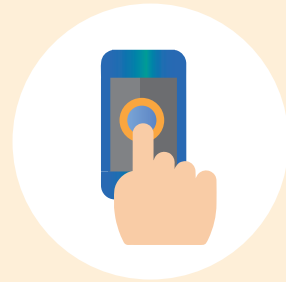
使用高安全性的設備、系統與軟體

企業須選用安全之設備、系統與軟體，提供員工遠距作業使用，並留存日誌以檢核異常使用。使用安全的網路連線（例如：VPN）和安全的遠端會議系統進行討論，可避免機敏資訊外洩。



多重認證機制

建立多重認證，並要求員工在遠距工作時，透過多重身份認證後，方能操作企業內部系統。



定期審核授權狀況

企業需定期確認使用者帳號及其權限，避免有陌生帳號或不當被利用之帳號竊取內部資訊。



圖 38-2 遠距辦公資安防護指南—企業篇（資料來源：TWCERT/CC）

強化資安政策，提高資安警覺

強化企業既有的資安政策，設定資安問題處理流程，以利快速處理各種突發的資安狀況，減低損害。定期提醒員工在家工作資安相關注意事項，提升企業全體人員的資安警覺。



定期更新與備份

定期更新系統版本，以獲得最新資安防護，並定期備份資料於安全設備中，減少資安事件發生時的損失。



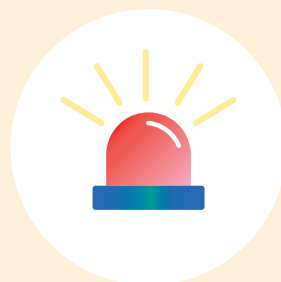
75

員工篇：

圖 39-1 遠距辦公資安防護指南—員工篇（資料來源：TWCERT/CC）

時時保持警覺

隨時對惡意郵件或軟體保持警覺心，看見有疑慮的郵件或連結，請勿點擊。如遇可能的資安問題即時警示相關人員進行確認與處理。



使用安全的網路設備

使用安全的家用網路以及無已知漏洞的網路連線設備。



圖 39-2 遠距辦公資安防護指南—員工篇（資料來源：TWCERT/CC）

避免被竊取資訊的可能

設定裝置閒置時鎖定並進行磁碟資訊加密，線上會議結束後，務必將相關設備關閉（例如：麥克風、視訊鏡頭）。



及時更新軟體避免漏洞

及時更新使用之系統與各應用軟體的版本。



使用強密碼

相關密碼設定使用強密碼，例如含英文大小寫以及數字，並且不使用生日、電話等易破解之資訊作為密碼。



遠距會議篇：

圖 40 遠距辦公資安防護指南—遠距會議篇（資料來源：TWCERT/CC）

選用無資通安全疑慮的視訊會議軟體

企業選用遠距會議軟體時，需考量其安全性，避免使用有資安漏洞和疑慮的軟體，落實資安防護。

**限制會議參與者**

所有會議建議設定密碼限制，並由會議發起人於會議開始前確認參與成員的身分。

**選擇可信賴的下載軟體管道**

在可信賴的官方網站或 App Store 下載軟體，以避免安裝到含有惡意程式的偽冒軟體或 APP。

**避免在公開社群分享會議連結**

請直接提供與會者連結，如此可以最大限度地避免不相關的人員得知會議並混入會議中竊取商業機密。

**謹慎確認會議邀請與連結**

來路不明的會議邀請或連結，極有可能是惡意連結，請勿點選避免受駭。

**謹慎使用螢幕共享的功能**

會議中若需使用螢幕共享的功能，需限制特殊指定人士才可使用該功能。

**更新至最新的軟體版本**

視訊會議軟體皆會因應各種資安漏洞進行修補更新，隨時更新到最新版本，可以確保使用上的安全。

**確保使用設備的安全性**

使用者參與線上視訊會議的資訊設備以及網路連線方式，皆需符合企業訂定之資安標準（例如：限定使用資訊設備、不使用免費網路連線等）。



VPN 篇：

圖 41 遠距辦公資安防護指南—VPN 篇（資料來源：TWCERT/CC）

選擇信譽良好的 VPN 廠商

由於 VPN 系統可直接存取企業內部網路，因此若 VPN 廠商信譽不良，可能不當存取企業機敏資訊或日誌紀錄，導致機敏資訊洩漏。

**建立多重認證機制**

建立多重認證，並要求員工在遠距工作時，透過多重身份認證後，方能進行後續作業。

**監控 VPN 的使用狀況**

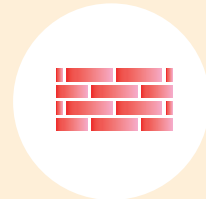
監控並記錄 VPN 的使用狀況，定期檢核日誌以及早發現異常使用。

**具備完善的加密機制**

選擇足夠安全的加密機制，進行資訊的加密傳輸，如 RSA-2048 或 AES-256 等，以避免資料外洩。

**搭配防火牆或防護軟體**

使用的 VPN 伺服器建議搭配相關防護措施，阻擋未經授權的連線，避免惡意程式流向主機。

**避免使用免費 VPN 服務**

免費的 VPN 服務內含較多廣告，部分廣告有夾帶惡意程式的風險，亦有個資外洩的疑慮。

**參考資料**

TWCERT/CC 遠距辦公資安專區：
<https://www.twcert.org.tw/tw/lp-142-1.html>

附錄二、勒索軟體防護檢核表

為協助企業評估對勒索軟體時的防禦與恢復能力，TWCERT/CC 彙整國內外資源，建立勒索軟體防護檢核表，以提供企業做檢核之依據。企業可於 TWCERT/CC 官網勒索軟體防護專區的事前預防、事中處理與事後回復查詢此檢核表。



基礎項目：

企業在防護勒索軟體時的一般性原則，確認事前的技術預防是否已達成，事中、事後則是建議事項或再確認處理動作是否遺漏。

進階項目：

當較大規模的企業具備多網段、AD 管控、虛擬平臺等複雜的網路環境，除了達成基礎項目需外，建議落實進階項目，以獲得更好的防護效果；同時，在資產方面也產生重要性的排序需求，可快速釐清事件處理順序，減輕影響與提升系統回復的效率。

1. 事前預防階段 [TLP: WHITE]

1.1 系統保護面

表 3-1 1.1 系統保護面

子面向	基礎項目	進階項目	檢核欄
1.1.1 防毒軟體	1.1.1.1 啟用病毒碼即時更新功能	-	
	1.1.1.2 每週 1 次全系統掃描	-	
	1.1.1.3 防毒軟體為啟用防護狀態	-	
	1.1.1.4 隨身碟等儲存設備連接電腦時，應執行防毒掃描	-	
1.1.2 軟體更新	1.1.2.1 Windows 啟用系統安全性更新的自動更新功能	-	
	1.1.2.2 Windows 更新功能應啟用「更新其它的 Microsoft 產品」	-	
	-	1.1.2.3 確認應用軟體更新狀態，並保持最新狀態	

表 3-2 1.1 系統保護面

子面向	基礎項目	進階項目	檢核欄
1.1.2 軟體更新	1.1.2.4 防毒軟體中控、AD 伺服器、資產管理系統之作業系統與應用服務皆應保持最新的更新狀態	-	
1.1.3 群組原則	-	1.1.3.1 定期確認 AD 伺服器、資產管理系統之群組原則或工作排程，是否有不正常異動狀況	
1.1.4 應用軟體	1.1.4.1 停用 Microsoft office 巨集功能，僅在必要時使用	-	
1.1.5 網路服務	1.1.5.1 每季執行 1 次網路服務 port 掃描，並確認每個 port 皆為必要服務所開啟，否則應關閉	-	
	1.1.5.2 每季執行 1 次網路服務弱點掃描，並修正所有高、中風險弱點	-	

表 3-3 1.1 系統保護面

子面向	基礎項目	進階項目	檢核欄
1.1.6 網路分段 區隔	-	1.1.6.1 實施網路分段區隔並監控流量	
1.1.7 防火牆	1.1.7.1 阻止任何與已知惡意 IP、URL 的對外連線行為	-	
	1.1.7.2 禁止使用允許任何連線的規則	-	
	1.1.7.3 只允許與對外服務的 IP、DN 進行連線	-	
1.1.8 權限設定	1.1.8.1 管理者以外使用者，給予可執行工作之最小權限	-	
	-	1.1.8.2 查看和管理所有使用戶帳戶的使用情況，並禁用非活動帳戶	
	-	1.1.8.3 實施多因子身份認證	

1.2 資料保護面

表 4-1 1.2 資料保護面

子面向	基礎項目	進階項目	檢核欄
1.2.1 資料 備份	1.2.1.1 定期執行資料備份，且備份間隔不長於 1 個月	-	
	1.2.1.2 依照 3—2—1 備份原則，3 份備份、2 種儲存媒體、1 個不同的存放地點	-	
	1.2.1.3 資料備份所存在的媒體或電腦，至少有 1 份以未連接網路的方式存放	-	
	1.2.1.4 依不同作業系統（如 Windows、Linux）特性調整資料備份作法	-	
1.2.2 系統映像 檔	-	1.2.2.1 重要的虛擬機與伺服器應備份映像檔（image file），且比照資料備份規則執行	
1.2.3 資料加密	1.2.3.1 對重要資料存放時應進行加密	-	

表 4-2 1.2 資料保護面

子面向	基礎項目	進階項目	檢核欄
1.2.4 安全存取	-	1.2.4.1 建立可存取重要資料的應用程式清單	
	-	1.2.4.2 啟用 Windows 受控資料夾存取功能 (controlled folder access)，限制只有安全的應用程式才能存取特定資料夾	
1.2.5 資產清單	-	1.2.5.1 盤點資產，並訂定關鍵資產清單	

1.3 資安意識面

表 5-1 1.3 資安意識面

子面向	基礎項目	進階項目	檢核欄
1.3.1 教育訓練 / 演練	1.3.1.1 基礎資安知識	-	
	1.3.1.2 勒索軟體攻擊介紹	-	

表 5-2 1.3 資安意識面

子面向	基礎項目	進階項目	檢核欄
1.3.1 教育訓練 / 演練	1.3.1.3 釣魚攻擊介紹， 識別可疑郵件、附檔、 連結、網頁	-	
	1.3.1.4 社交工程攻擊介 紹	-	
	-	1.3.1.5 定期進行 社交工程演練	

1.4 應變準備面

表 5-3 1.4 應變準備面

子面向	基礎項目	進階項目	檢核欄
1.4.1 應變規劃	1.4.1.1 規劃資安事件 發生時，各層級員工分 工、通報流程、連絡方 式等		
1.4.2 應變演練	-	1.4.2.1 定期執行 應變演練，確認成 效	
1.4.3 協處單位	1.4.3.1 準備資安事件發 生時，可尋求協助的外 部資安單位、警調之清 單與連絡方式	-	

2. 事中應變階段檢核表 [TLP: WHITE]

2.1 事件確認面

表 6 2.1 事件確認面

子面向	基礎項目	進階項目	檢核欄
2.1.1 發現回報	2.1.1.1 內部自行發現，蒐集資訊並提交報告	-	
	2.1.1.2 收到外部異常警告或事件通報，蒐集資訊並提交報告	-	
2.1.2 感染勒索軟體跡象	2.1.2.1 硬碟使用率大幅提升	-	
	2.1.2.2 CPU 或記憶體使用率大幅提升		
	2.1.2.3 受影響的檔案被修改副檔名	-	
	2.1.2.4 設備螢幕上顯示勒索訊息	-	
2.1.3 評估決策	<p>2.1.3.1 根據事件報告，評估事件性質，依結果遞交相關部門人員，如經確認，觸發應變流程。</p> <p>事件性質評估面向為：受影響資料擁有者層級、受影響資料重要性、受影響主機數量、利害關係人影響性，如客戶、產品使用者等。（此項目因企業性質差異，僅提供原則性建議）</p>	-	

2.2 應變處理面

表 7-1 2.2 應變處理面

子面向	基礎項目	進階項目	檢核欄
2.2.1 防止擴大	2.2.1.1 斷開受感染設備與所有網路的连接，若為 sub-domain 或是多台設備，從 switch 層級斷開網路	2.2.1.2 若無法斷開受駭設備與網路连接，則將主機斷電。（此步驟可能影響資料保存與證據維護，謹慎採用）	
2.2.2 報案與通報	2.2.2.1 依應變計劃之內部通報流程，進行通報以啟動應變作業，並記錄事件經過	-	
	2.2.2.2 將被加密的檔案與勒索信件拍照存檔，並向警方備案	-	
	2.2.2.3 透過 TWCERT/CC 官網通報 (twcert.org.tw) 或 Email:twcert@cert.org.tw 進行資安事件通報進行資安事件通報。	-	
	-	2.2.2.4 確保通報或對外溝通管道之機密安全性，防範引起攻擊者警覺	

表 7-2 2.2 應變處理面

子面向	基礎項目	進階項目	檢核欄
2.2.3 事件協處	2.2.3.1 由外部專業資安團隊協助處理	-	
2.2.4 影響確認	2.2.4.1 盤點可能受影響設備，執行防毒軟體掃描，並確認是否受駭	-	
		2.2.4.2 依據預先定義之關鍵資產清單，評估優先查證影響程度的順序	
2.2.5 事件處理	2.2.5.1 依勒索軟體名稱、副檔名等分辨病毒類型，尋找解密工具	-	
	2.2.5.2 確認資安事件發生根因，予以排除	-	
2.2.6 利害關係人	2.2.6.1 讓內部或外部的利害關係人瞭解事件，並提供可減輕事件影響的協助	-	

3. 事後回復階段檢核表 [TLP: WHITE]

3.1 設備恢復面

表 8 3.1 設備恢復面

基礎項目	進階項目	檢核欄
-	3.1.1 依據關鍵資產清單及 2.2.4.2 受駭影響評估結果，排 定資產恢復優先順序，以及對 高重要性資產的資安保護規劃	
3.1.2 重置該設備的所有 密碼、憑證	-	
3.1.3 使用備份資料進行 還原	-	
3.1.4 重新恢復的設備安 裝防毒軟體，並執行全系 統掃描	-	

3.2 事後分享

表 9 3.2 事後分享

基礎項目	進階項目	檢核欄
3.2.1 將事件相關資料通報 TWCERT/CC，協助分享給國內企業，防止更多企業受害	-	

3.3 檢討改進

表 10 3.3 檢討改進

基礎項目	進階項目	檢核欄
3.3.1 依受駭原因，於事件應變後，規劃管理層面對應改善措施並執行	-	

參考資料

- 1.CISA.“I’VE BEEN HIT BY RANSOMWARE!”：
<https://www.cisa.gov/stopransomware/ive-been-hit-ransomware>
- 2.CISA.“Rising Ransomware Threat ToOperational Technology Assets”：
https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_
- 3.CISA.“Ransomware_Threat_to_OT_Assets_508C.pdf STOP RANSWM
WARE”：
<https://www.cisa.gov/stopransomware>
- 4.JENNER&BLOCK.“Memo What We Urge You To Do To Protect Against The
Threat of Ransomware”：
<https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf>
- 5.NCSC.“Mitigating malware and ransomware attacks”：
<https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>
- 6.No Moew Ransom.<如何預防勒索軟體攻擊？>：
https://www.nomoreransom.org/zht_Hant/prevention-advice.htm
- 7.TWCERT 官網.<事前預防 勒索軟體防護指南>：
<https://antiransom.tw/page-1.html>
- 8.TWCERT 官網.<事中處理 勒索軟體防護指南>：
<https://antiransom.tw/page-2.html>
- 9.TWCERT 官網.<事後回復 勒索軟體防護指南>：
<https://antiransom.tw/page-3.html>

出版單位：財團法人台灣網路資訊中心

資通安全年報 . 2021= Cyber security annual report 2021 /
台灣電腦網路危機處理暨協調中心主編

ISBN 978-986-06247-3-1 (精裝) NT\$: 200



Cyber Security Annual Report 2021

2021 資通安全年報

出版者：財團法人台灣網路資訊中心

書名：2021 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 臺北市松山區八德路四段 123 號 3 樓

電話：(02)2528-6786

承製單位：紫晶數位有限公司

版次：初版

出版日期：2022 年 7 月

定價：新臺幣 200 元整

I S B N : 978-986-06247-3-1

本文件之智慧財產權屬台灣電腦網路危機處理暨協調中心所有。

10100011010

100011010

101010

1101101100011101010

01010

0
1
0
|
1
0

0
1
0
1
0
1

|
1
0
1
0
1
|

|
1
0
1
1

0
1
0
0
0
0
1
0
1
0
0
1

1101010

01101102

11001

00111



台灣電腦網路危機暨處理協調中心

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 105305, Taiwan (R.O.C)

<https://www.twcert.org.tw/tw>
+886-2-2528-6768

ISBN 978-986-06247-3-1



NT 200