TWCERT/CC 資安情資電子報

2021 年 8 月份

電子報序言

台灣電腦網路危機處理暨協調中心(以下簡稱 TWCERT/CC)在行政院資通安全處及國家通訊傳播委員會指導下，推動企業資安通報協處、產品資安漏洞通報、惡意檔案檢測服務及資安情資分享等工作，以提升國家資安聯防能量，並維護整體網路安全。

TWCERT/CC 本月份所發布之資安情資電子報，為透過官方網站、電子郵件及電話等方式接收資安情資，並與國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間資安情資共享，將接收與共享之情資進行彙整、分析與分享，主要分成以下 6 章節：

第 1 章、封面故事：上月 TWCERT/CC 所發布之資安情資中，官網點閱次數最高之情資列為本月份封面故事。

第 2 章、資安小知識：提供資安基礎概念、資安防護指南等知識，以提升大眾資安素養。

第 3 章、資訊安全宣導：針對近期資安議題、TWCERT/CC 服務或配合政府資安政策等進行資安宣導，以提升大眾資安意識。

第 4 章、國內外重要資安事件：研析國內外相關資安情報，及彙整上述方式接收之資安情資，進行分析與分享。範疇包含資安趨勢、國際政府組織資安資訊、社群媒體資安近況、行動裝置資安訊息、軟體系統資安議題、軟硬體漏洞資訊及新興應用資安。

第 5 章、資安研討會及活動：近期舉辦之國內外資安相關研討會、訓練課程及資安競賽等活動資訊分享。

第 6 章、資安情資分享概況：將上月份 TWCERT/CC 每日接收及分享之資安情資，針對對外資安情資分享地區及各項資安攻擊類型進行統計。

目錄

第 1 章、 封面故事

FBI 警告加密貨幣持有人與交易所，對可能發生的攻擊行動提高警覺

美國聯邦調查局日前警告加密貨幣相關利害關係人，要對可能進行的攻擊行動提高警覺，不然可能會發生鉅額金錢虧損。

美國聯邦調查局（Federal Bureau of Investigation, FBI）日前發表資安警示通報，警告加密貨幣產業內的相關利害關係人，包括持有人、交易所與第三方支付平台等，要對近來可能進行的攻擊行動提高警覺，不然可能會發生鉅額金錢虧損。

FBI 是透過 TLP:GREEN 私人產業通告（Private Industry Notification, PIN）發布這項警報；根據 FBI 表示，攻擊者會利用多種不同技巧竊取加密貨幣並進行洗錢，例如詐騙技術支援、SIM 卡偷換攻擊、或透過釣魚攻擊等方式，取得加密貨幣操作者使用的登入資訊，以挾持用戶存取權。

加密貨幣一旦被竊走，由於其高度匿名性，因此只要流進攻擊者控制的加密貨幣錢，包，其流向就非常難以查緝；也因為執法力量難以發揮，因此往往造成受害者的大筆資金一去不返。

FBI 說，在 2020 年 5 月到 2021 年 5 月間，美國資安相關單位觀察到或接獲受害者報案的加密貨幣竊取攻擊事件，大致可分為以下幾個類型：

- 跳過二階段驗證過程，取得受害者的加密貨幣交易所帳號權限；
- 線上支援詐騙：假冒成交易平台的技術支援專線，在電話中詐騙被害人；
- 利用 SIM 偷換攻擊，攔截用戶收到的二階段簡訊驗證碼。

FBI 建議可能成為攻擊目標的相關加密貨幣金融機構，應該特別留意詐騙或釣魚 Email 活動，並且對最近註冊的新帳號活動加強注意。

另外，加密貨幣持有人也應在所有交易所或錢包服務中，啟用二階段登入驗證，不要下載任何不明軟體或使用遠端遙控軟體進行加密貨幣操作，也只透過交易所官方提供的 Email 或電話進行連絡。

- 資料來源：
  1. FBI warns cryptocurrency owners, exchanges of ongoing attacks
  2. FBI Warns Digital Currency Exchanges and Crypto Owners of Possible Threats
  3. FBI San Francisco Warns the Public of the Dangers of SIM Swapping

第 2 章、 資安小知識

2.1.1、勒索軟體辨識與解密工具

1. 簡介

加密勒索軟體 Ransomware 為一種透過資料加密手法讓受害者失去資料存取或系統的控制的惡意程式，且如不支付贖金給犯罪組織，則將無法取回受加密的資料。因犯罪組織利用這種不法模式獲利，也是其被稱為「勒索軟體」的原因。

現今的勒索軟體精密複雜且侵入性強大，透過發展各種攻擊手段與支援多國語言、跨平台等方式感染受害者設備。目前防毒軟體廠商對於部分勒索軟體已有可應對的免費解密工具，如不慎受到勒索軟體攻擊，可先參考本篇第二章節，辨識勒索軟體名稱後，透過第三章節的解密工具清單，搜尋是否有可支援的解密工具。

2. 勒索病毒種類辨識

勒索軟體種類眾多，為了取得對應的解密工具，需先正確地辨識勒索軟體名稱。本篇提供以下線上勒索軟體辨識服務，可透過提供 ‘勒索內容’ (如: 勒索訊息、勒索電子郵件、網站網址等)與 ‘被加密的檔案’ 進行特徵比

對，判定勒索軟體名稱。

(1). ID Ransomware

由 MalwareHunterTeam 提供，可辨識超過 1000 種勒索軟體。使用者可透過上傳加密檔案、勒索訊息(如無勒索訊息，可提供勒索電子郵件、網站網址)，即可進行辨識。網頁上傳介面如圖 1 所示。勒索軟體名稱辨識結果示意圖如圖 2 紅框處所示。網址請參考: ID Ransomware 官網

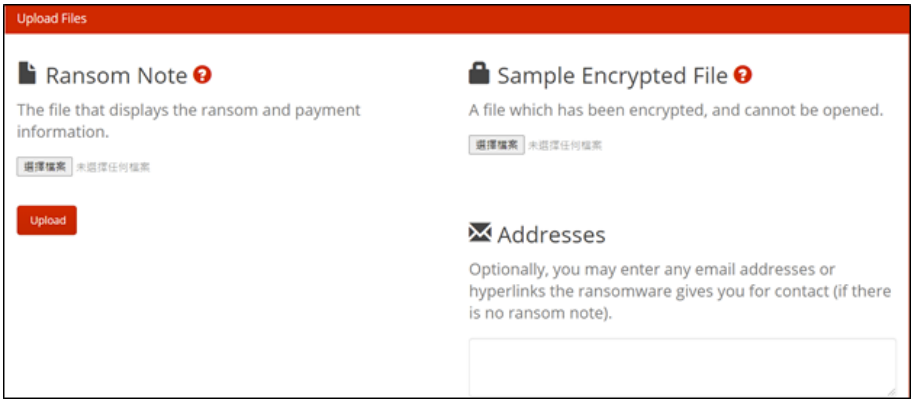


圖 1、ID Ransomware 上傳頁面

圖 2、ID Ransomware 勒索軟體名稱的辨識結果示意圖(紅框處)

2. Crypto Sheriff

由 The No More Ransom Project 提供，可辨識勒索病毒並提供對應的免費解密工具。使用者可透過上傳兩個加密檔案、上傳勒索訊息檔案或是提供勒索訊息內容的電子郵件、網站網址、洋蔥網路網址、比特幣網址，即可進行

辨識。上傳網頁介面如圖 3 所示。結果示意圖如圖 4 所示。

網址請參考: No More Ransom 官網

圖 3、No More Ransom 解碼警長頁面

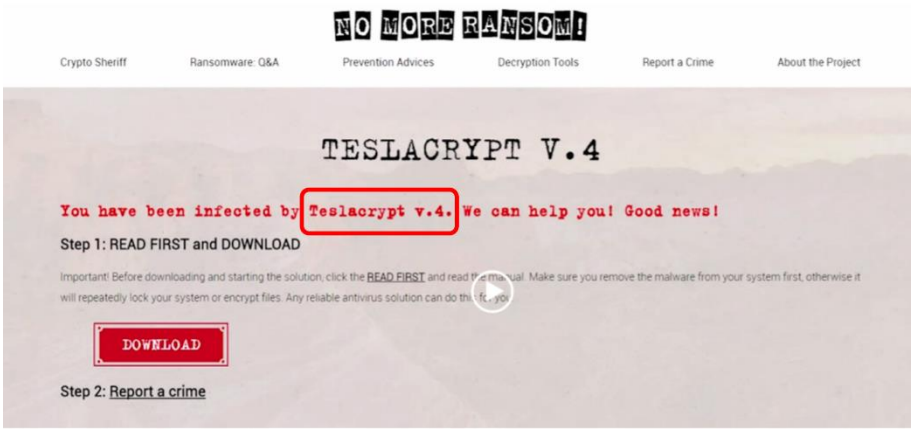


圖 4、解碼警長勒索軟體名稱辨識結果示意圖 (紅框處)

3. 解密工具

勒索軟體名稱確認之後，可透過本章節所提供之解鎖工具網頁清單，搜尋勒索軟體名稱或是瀏覽解密工具清單找到對應的解密工具，少數勒索軟體有機會使用以下工具嘗試解密。勒索軟體名稱辨識方式請參考本篇第二章節。

1. No More Ransom 解鎖工具

由 No More Ransom Project 提供。使用者可透過搜尋勒索軟體名稱(紅框處)或是瀏覽解鎖工具列表(藍框處) (圖 5) ，查看工具使用指南與下載(圖 6) 。

網址請參考: No More Ransom 官網

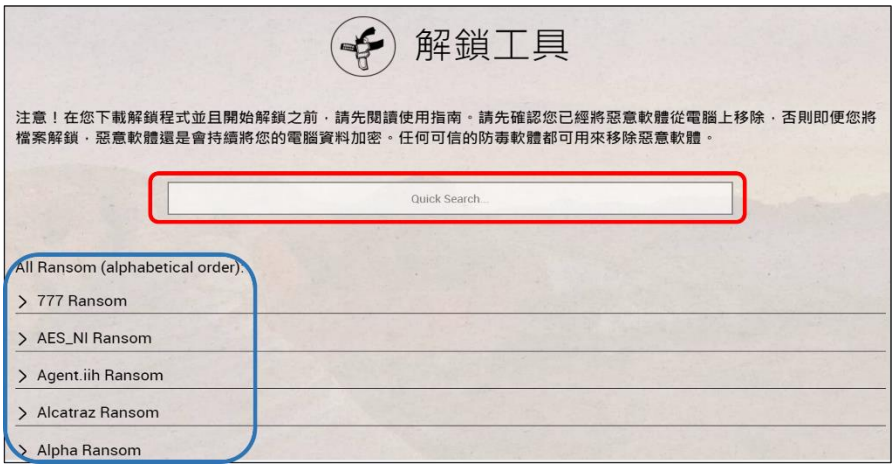


圖 5、No More Ransom 解鎖工具列表與搜尋頁面

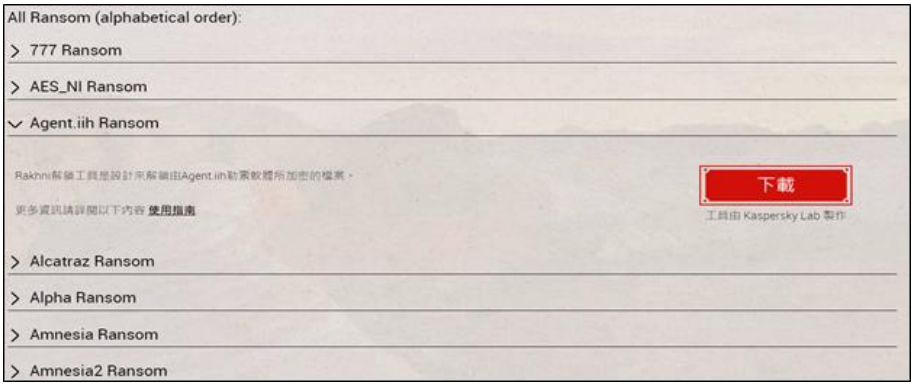


圖 6、No More Ransom 解鎖工具之說明、使用指南與工具下載連結頁面

2. Trend Micro Ransomware File Decryptor

由 Trend Micro 提供。使用者可下載 (綠框處)與執行 RansomwareFileDecryptor 工具，選擇勒索軟體名稱與欲解密的檔案或資料夾進行解密(紅框處)。頁面如圖 7 所示。網址請參考: Trend Micro 官網

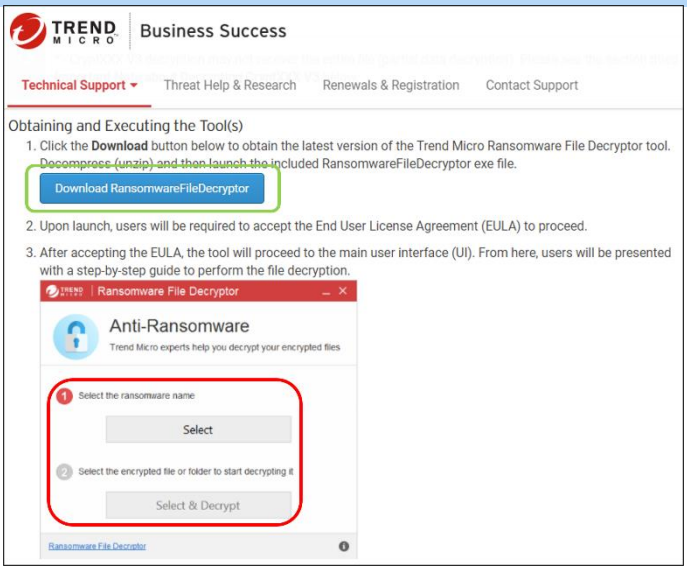


圖 7、Trend Micro Ransomware File Decryptor 下載與說明頁面

3. 卡巴斯基 Free Ransomware Decryptors

由卡巴斯基提供。使用者可瀏覽解密工具列(藍框處)表或是搜尋名稱(紅框處)，下載所需之解密工具進行解密。搜尋畫面與列表如圖 8 所示。

網址請參考: 卡巴斯基官網

圖 8、卡巴斯基 Free Ransomware Decryptor 解密工具搜尋與瀏覽頁面

4. AVG 免費軟體解密工具

由 AVG 提供。使用者可瀏覽解密工具列表(圖 9) (藍框處)，檢視解密工具說明與下載修正程式進行解密(圖 10)。網址請參考: AVG 官網

圖 9、AVG 免費勒索軟體解密工具列表頁面

圖 10、工具說明、勒索訊息畫面與修正程式下載連結 (示意圖)

5. EMSI SOFT Free Ransomware Decryption Tools

由 EMSI SOFT 提供。使用者可瀏覽解密工具列表(藍框處)，下載所需解密工具(圖 11)。網址請參考: EMISI SOFT 官網

圖 11、EMISI SOFT Free Ransomware Decryption Tool 解密工具列表頁面

6. McAfee Ransomware Recover (Mr2)

Mr2 為 McAfee 開發之解密工具，採取指令列介面，且定期更新支援的勒索軟體主類。使用者可透過圖 12 下載安裝 Mr2 (綠框處)，執行後可透過指令檢視支援解密的勒索軟體列表與進行解密，如圖 13 所示。

網址請參考: McAfee 官網

使用 Mr2 破解勒索軟體 Stampado 之範例與說明:

Stampado 勒索訊息如圖 14 所示，內容提示受害者需透過攻擊者電子郵件(圖 14 紅框處)聯繫以取得解鎖碼輸入(圖 14 綠框處)進行檔案解密。

- 1) 啟動 Mr2 後，輸入 ‘MfeDecrypt -list’ 指令(圖 15 綠框處)搜尋 ‘Stampado’ 勒索軟體的解密工具(圖 15 紅框處)
- 2) 執行 ‘MfeDecrypt -get stampado -ver 1.0.0’ 指令下載 Stampado 解密工具。(圖 16 紅框處)
- 3) 執行 ‘MfeDecrypt -about stampado -ver 1.0.0’ 指令查看解密工具使用方式(圖 17 紅框處)。
- 4) 透過 ‘MfeDecrypt -run stampado -ver 1.0.0 -args “-e FileUnlocker64@mail2tor.com’ 命令執行解密工具(圖 18 紅框處)，提供圖 14 紅框處的勒索聯絡電子郵件，取得解鎖碼(圖 18 綠框處)，並於圖 13 的勒索訊息畫面輸入解鎖碼進行檔案解密。

圖 12、McAfee Ransomware Recover (Mr2) 下載頁面

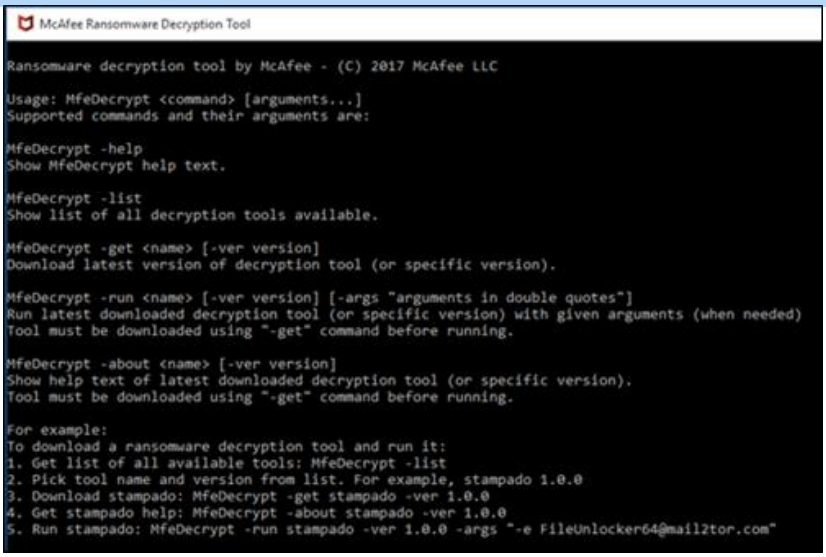


圖 13、Mr2 執行畫面，包含工具指令與說明

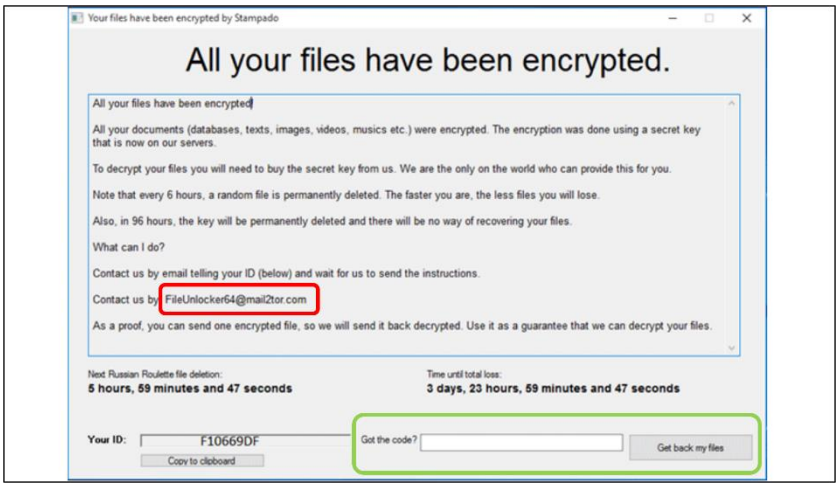


圖 14、Stampado 勒索訊息 (示意圖)

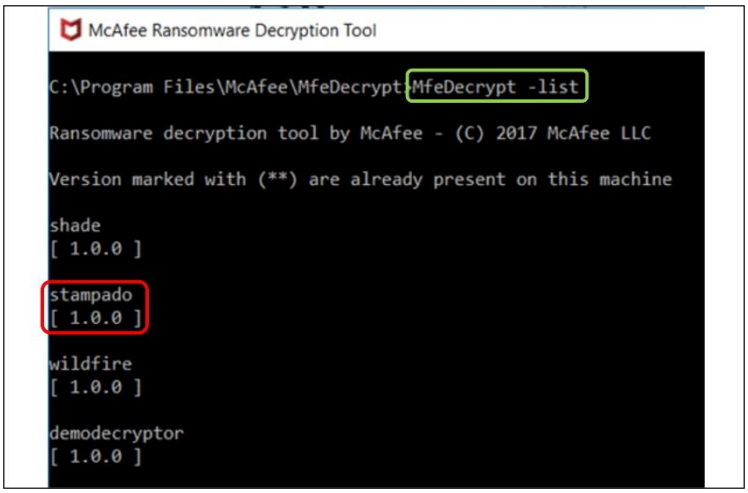


圖 15、Mr2 支援 Stampado 解密與顯示所有勒索軟體解密支援的命令 (示意圖)

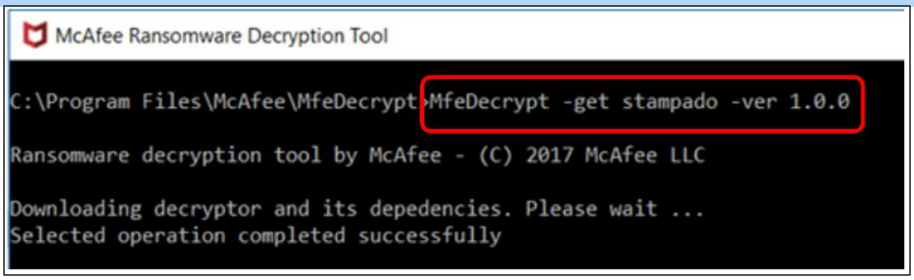


圖 16、下載勒索軟體 Stampado 解密工具的命令 (示意圖)

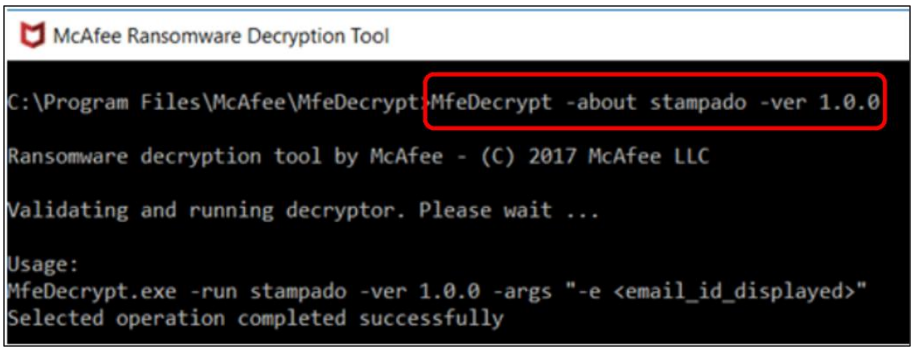


圖 17、Stampado 解密工具命令使用方式 (示意圖)

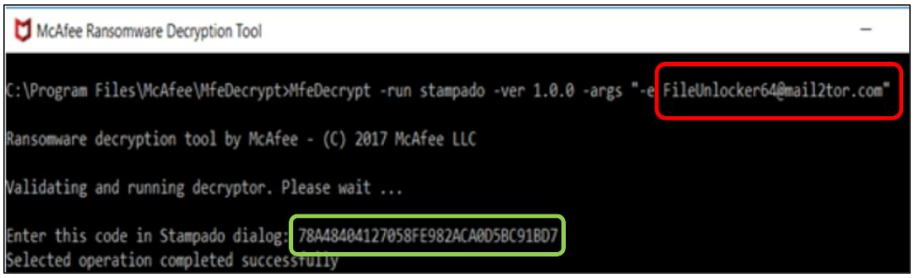


圖 18、取得 Stampado 解鎖碼 (示意圖)

7. Avast Free Ransomware Decryption Tools

由 Avast 提供。使用者可瀏覽解密工具列表(圖 19) (藍框處)，檢視解密工具說明與下載修正程式進行解密(圖 20)。網址請參考: Avast 官網

圖 19、Avast Free Ransomware Decryption Tool 解碼工具列表頁面

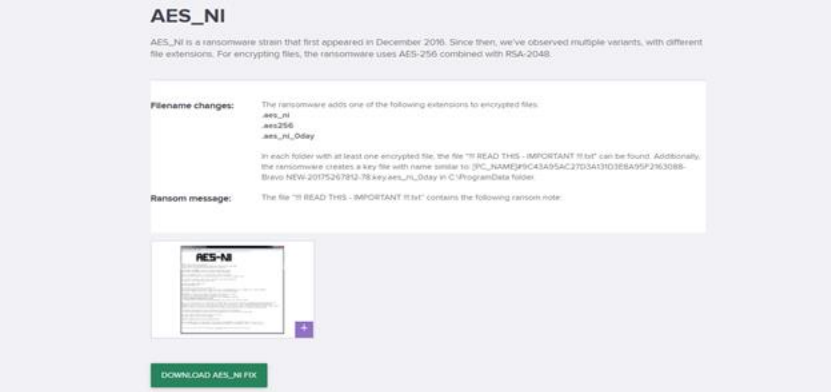


圖 20、解密工具說明、勒索訊息截圖與下載連結 (示意圖)

8. Quick Heal Free Decryption Tool

由 Quick Heal 提供。使用者可下載支援多種勒索軟體解密的工具進行解密(圖 21)。執行工具後，會自動進行掃描加密檔案進行解密。

網址請參考: Quick Heal 官網

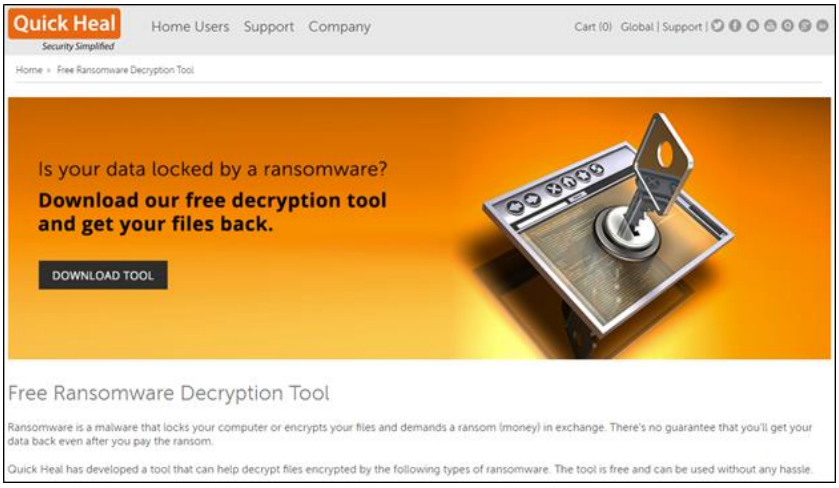


圖 21、Quick Heal Free Ransomware Decryption Tool 解密工具下載頁面

9. MDS Ransomware Decryption Tools

由 MDR 提供。使用者可瀏覽解密工具列表，下載所需解密工具進行解密，如圖 22 所示。網址請參考: MDS 官網

圖 22、MDS Ransomware Decryption Tools 解密工具列表

2.1.2、勒索軟體防護成熟度自評說明 - 使用美國 CISA CSET RRA 軟體模組

1. 簡介

為了因應日益猖獗的勒索軟體攻擊，美國國土安全及基礎設施安全局 (Cybersecurity and Infrastructure Security Agency, CISA) 的資訊安全評估工具 (Cyber Security Evaluation Tool, CSET) 已納入新模組 – 勒索軟體防護機制自評工具(Ransomware Readiness Assessment, RRA)，協助組織診斷自身資安防護機制是否健全與足夠應對勒索軟體攻擊。

CSET 為一評估工具之平台，可協助組織根據不同的成熟度評估模組 (如: ACET、CMMC、EDM、RRA)，系統性的評估組織資訊安全性。而 RRA 則是 CSET 的新增模組，專門用來評估組織應對勒索軟體時的防禦與恢復能力， RRA 亦納入不同等級的勒索軟體威脅防護成熟度，藉以評估組織應對勒索軟體攻擊的狀況。評估結果以透過儀表板的圖形與表格方式呈現評估結果，其中亦包含摘要與細節，提供增強防護之建議。

RRA 評估模組以下列十大防護面向進行組織自評:

1. Robust Data Backup (DB), 備份機制:

檢視備援政策的適當性，如採用定期與自動化資料與系統設定備份，並以安全方式儲存 (加密)等。

2. Web Browser Management and DNS Filtering (BM), 瀏覽器管理與 DNS 過濾機制:

檢視瀏覽器管理與 DNS 過濾機制，即時過濾與可疑惡意域名的連線。

3. Phishing Prevention and Awareness (PP), 釣魚威脅防治:

檢視反釣魚防護機制措施，並定期於組織內進行提升釣魚威脅意識之教育訓練。

4. Network Perimeter Monitoring (NM), 網路邊界監控:

檢視網路邊界監控機制，採用可結合威脅情資與入侵指標(IoC)之網路防護設備，並即時監控與防堵可疑網路流量。

5. Asset Management (AM), 資產管理:

檢視資產管理政策，如定期盤點更新組織資產設備，並移除已不被支援的軟體與硬體設備等。

6. Patch and Update Management (PM), 更新修補管理:

檢視設備軟體與韌體更新管理機制，如定期置換已不被支援的 OS、應用程式及硬體設備等。

7. User and Access Management (UM), 使用者存取控管:

檢視使用者權限管理政策，如採取帳戶最小權限原則、密碼強度政策及監控分析使用者異常行為等。

8. Application Integrity and Allowlist (AI), 應用程式安全性:

訂定組織可允許使用之應用程式清單，並定期檢視應用程式檔案的完整性等。

9. Incident Response (IR), 資安事件應變:

檢視資安事件處理計畫，並定期進行資安事件演練。

10. Risk Management (RM), 風險管理:

檢視組織提升資安威脅意識政策，如定期進行教育訓練與演練等。

RRA 評估項目分為 ‘Basic’、‘Intermediate’與 ‘Advanced’ 三個成熟度等級，旨在提供組織了解目前各等級防護成熟度與改善措施之優先度。建議會員可依序完成 ‘Basic’等級之所有措施之後再持續完善 ‘Intermediate’與 ‘Advanced’ 之防護措施。相關各等級對應之問題可於 ‘Deficiency Report’中檢視，建議措施細節可參照 ‘RRA report’。

2. 安裝與使用說明

美國 CISA 已透過 GitHub 釋出含有 RRA 模組之 CSET 自評工具，TWCERT/CC 建議企業組織利用此工具進行自我評估。以下為安裝步驟與使用說明。

1. 透過美國 CISA 官網或 GitHub 下載並安裝 CSET。請參考: 美國 CISA 官網、GitHub 網站。

2. 啟動 CSET 應用程式。

3. 點選 ‘Start a New Assessment’ 建立新評估專案，如圖 1 所示。

圖 1、建立新評估專案

4. 於 Assessment Options 勾選 ‘Maturity Model’並點擊 ‘Next’ 按鈕，如圖 2 所示。

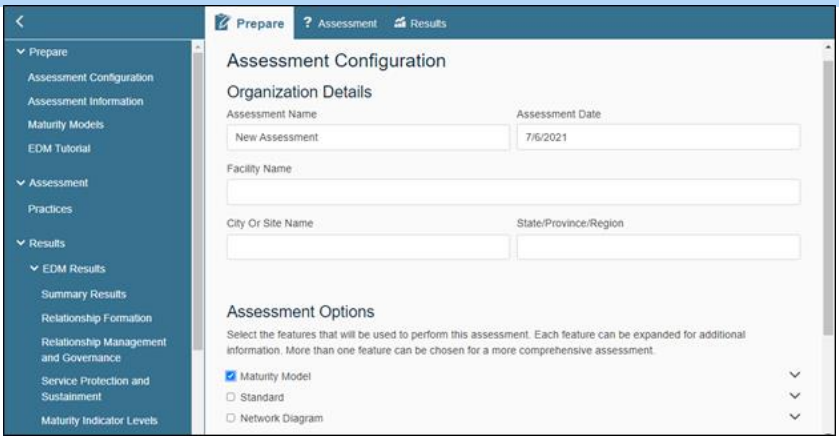


圖 2、選取 Maturity Model

5. 從左邊選單點選 ‘Maturity Models’，並勾選 Ransomware Readiness Assessment 項目，點擊 ‘Next’ 按鈕，如圖 3 所示。

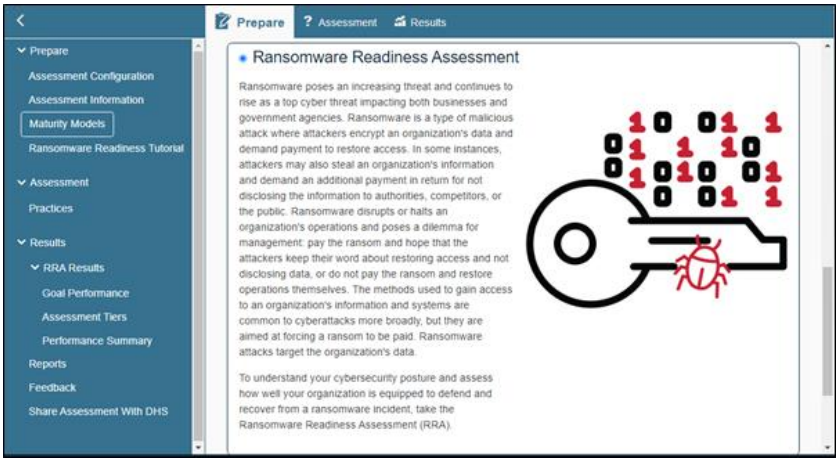


圖 3、選取 Ransomware Readiness Assessment

6. 從左邊選單點選 ‘Assessment’ 的 ‘Practices’ 子項目後，可根據 RRA 之十大項目(表一的 DB、BM、PP、NM、AM、PM、AI、UM、IR、RM)的細節問題進行自評 (藍框處): ‘符合’ 點選 ‘YES’、 ‘不符合’點選 ‘NO’、或是不確定則點擊 ‘旗幟’，完成後點擊 ‘Next’ 按鈕，如圖 4 所示。

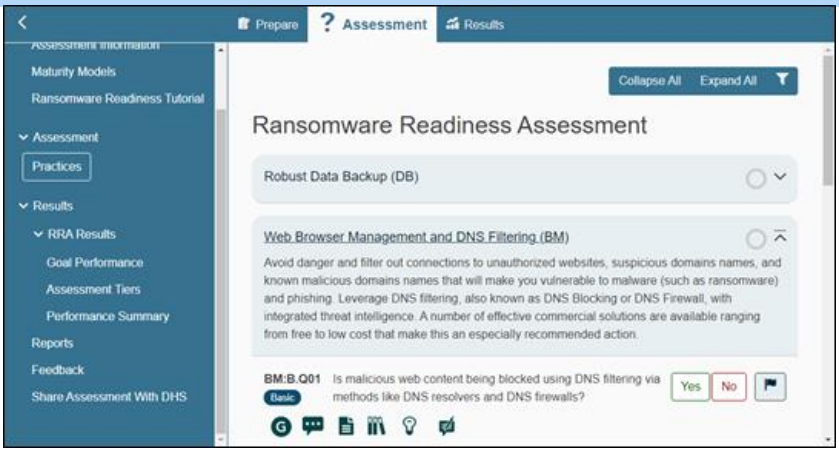


圖 4、自評畫面

7. 評估結果畫面，包含各大項防護措施的達成度 (長條圖與表格)，點擊 'Next' 按鈕，如圖 5、圖 6 所示。

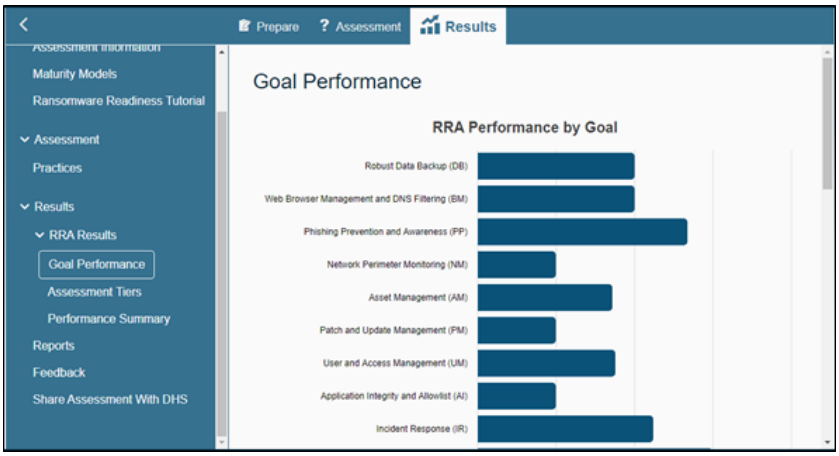
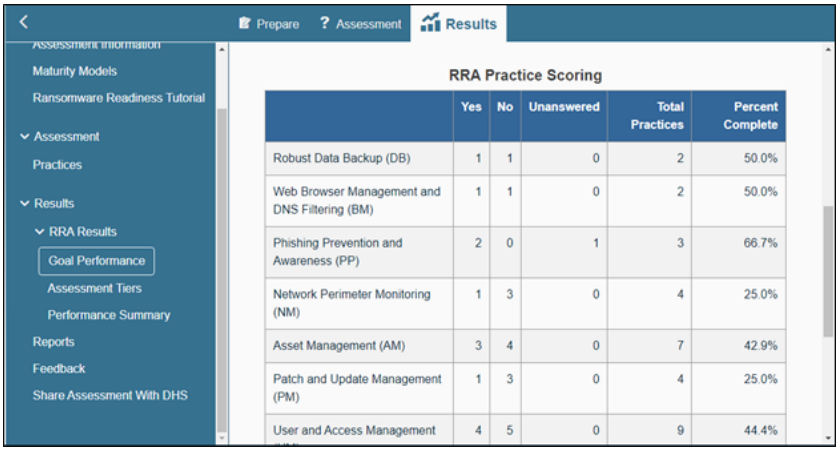


圖 5、各項評估結果 1，(長條圖) (示意圖)



	Yes	No	Unanswered	Total Practices	Percent Complete
Robust Data Backup (DB)	1	1	0	2	50.0%
Web Browser Management and DNS Filtering (BM)	1	1	0	2	50.0%
Phishing Prevention and Awareness (PP)	2	0	1	3	66.7%
Network Perimeter Monitoring (NM)	1	3	0	4	25.0%
Asset Management (AM)	3	4	0	7	42.9%
Patch and Update Management (PM)	1	3	0	4	25.0%
User and Access Management	4	5	0	9	44.4%

圖 6、各項評估結果 2、(表格) (示意圖)

8. RRA 成熟度等級(圖 7)，以及各級防護成熟度評估結果(圖 8、圖

9)。點擊‘Next’。

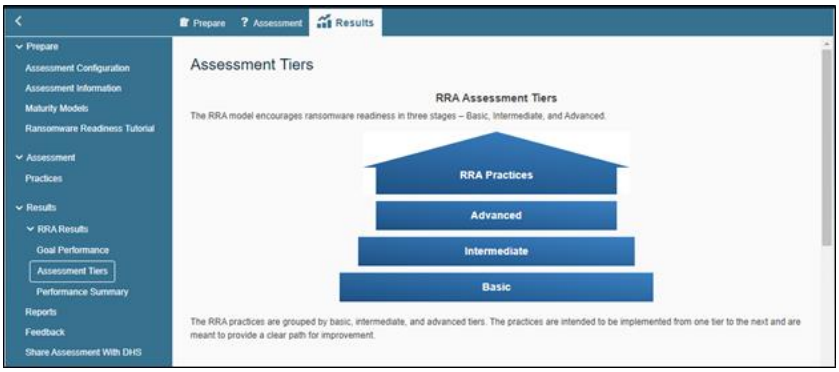


圖 7、RRA 成熟度分級圖

圖 8、‘Basic’、‘Intermediate’、‘Advanced’各級項目成熟度 (長條圖) (示意圖)

圖 9、‘Basic’、‘Intermediate’、‘Advanced’各級項目成熟度 (圓餅圖) (示意圖)

9. RRA 報告下載，如圖 10 所示。

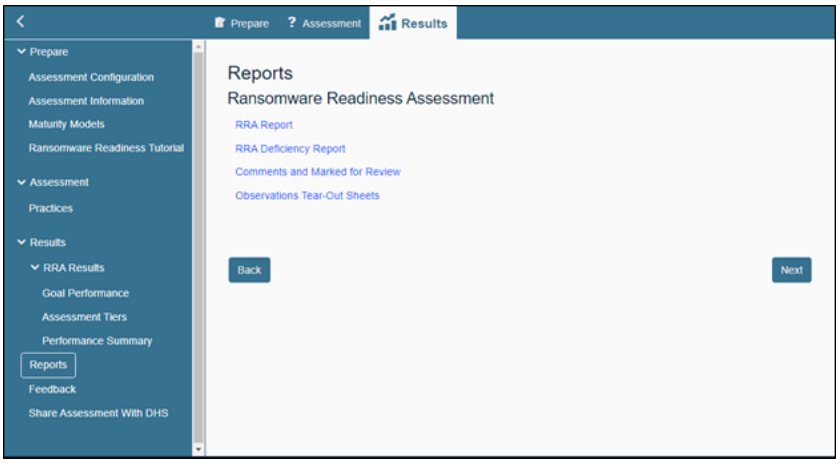


圖 10、RRA 報告下載。

- ‘RRA Report’ 為整體評估報告，包含:
  整體評估分數與各等級成熟度(圖 11)

  - 呈現組織於各等級與總體成熟度概觀。

  各項評估結果(圖 5、圖 6)

  - 呈現 RRA 十大評估項目的各項成熟度。

  建議改善項目(圖 12)

  - 呈現 RRA 十大評估項目最低至最高成熟度排名，提供組織檢視優先改善的項目。

  十大項目完成度(圖 13)

  - 呈現 RRA 十大評估項目的各項完成比例。

  RRA 成熟度分級圖(圖 7)

  - 呈現 RRA 的 ‘Basic’、‘Intermediate’與 ‘Advanced’ 三個等級機制，提供組織了解目前各等級防護成熟度與改善措施之優先度。建議會員可依序完成 ‘Basic’等級之所有措施之後再持續完善 ‘Intermediate’與 ‘Advanced’ 之防護措施。

  ‘Basic’、‘Intermediate’、‘Advanced’各級項目成熟度 (圖 8、圖 9)

- 呈現各等級的成熟度。

各問題的細節、建議措施與參考資料。白底為自評 ‘符合’的項目(圖 14)，紅底為自評 ‘不符合’的項目(圖 15)

- 提供組織了解各問題針對的防護措施內容及參考資訊。

- ‘RRA Deficiency Report’為未達成之防護項目，包含:
  建議改善項目(圖 12)

- 呈現 RAA 十大評估項目最低至最高成熟度排名，提供組織檢視優先改善的項目。

回答 ‘不符合’ 的各個問題清單(依照等級分類) (圖 16)

- ‘Comments and Marked for Review’為自評階段選取 ‘不確定’的項目清單 (圖 17)
- ‘Observations Tear-out Sheet’為含有自評組織的基本資訊頁(圖 18)

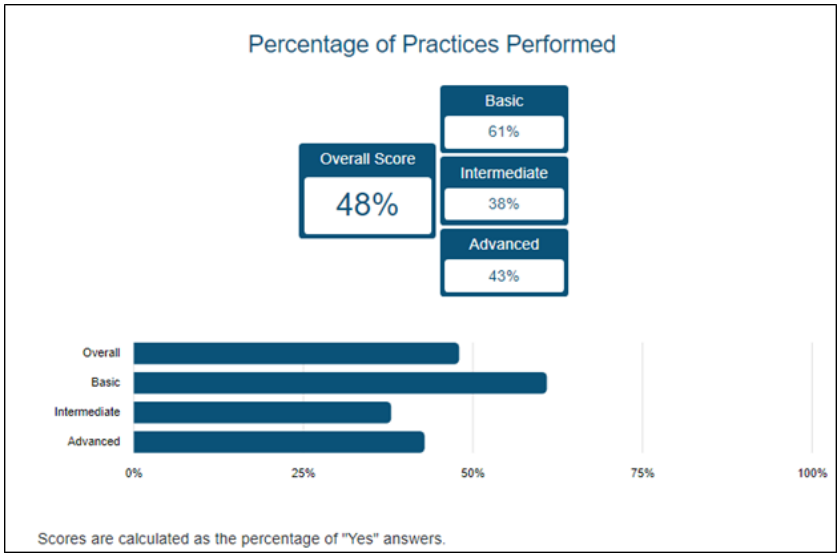


圖 11、整體評估分數與各等級成熟度(示意圖)

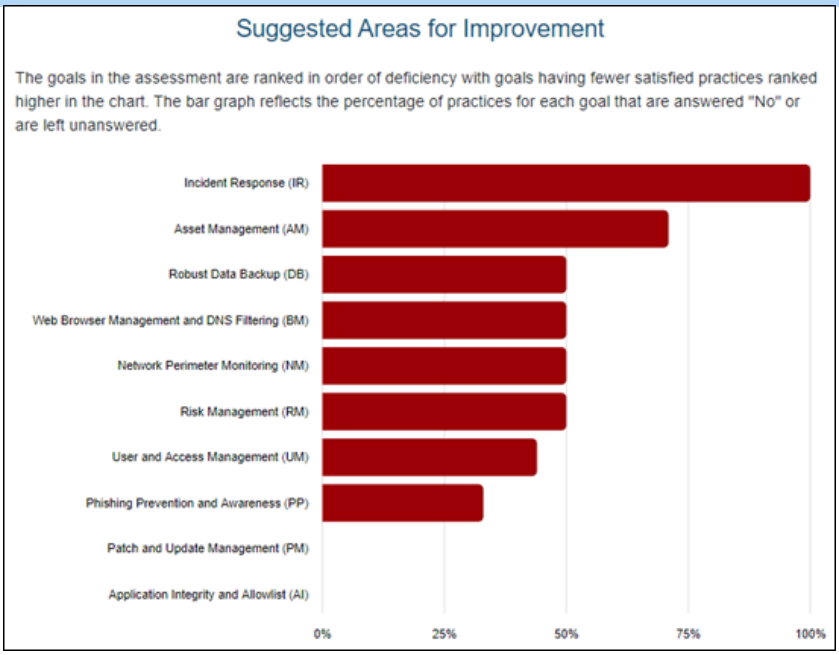


圖 12、建議改善項目(示意圖)

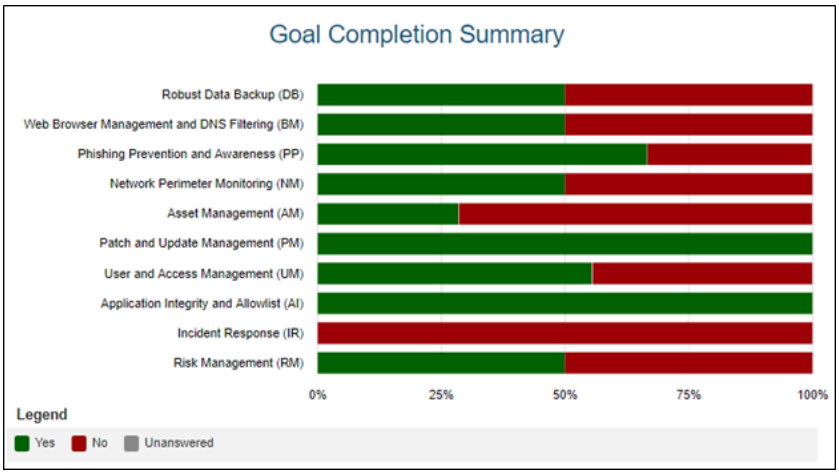


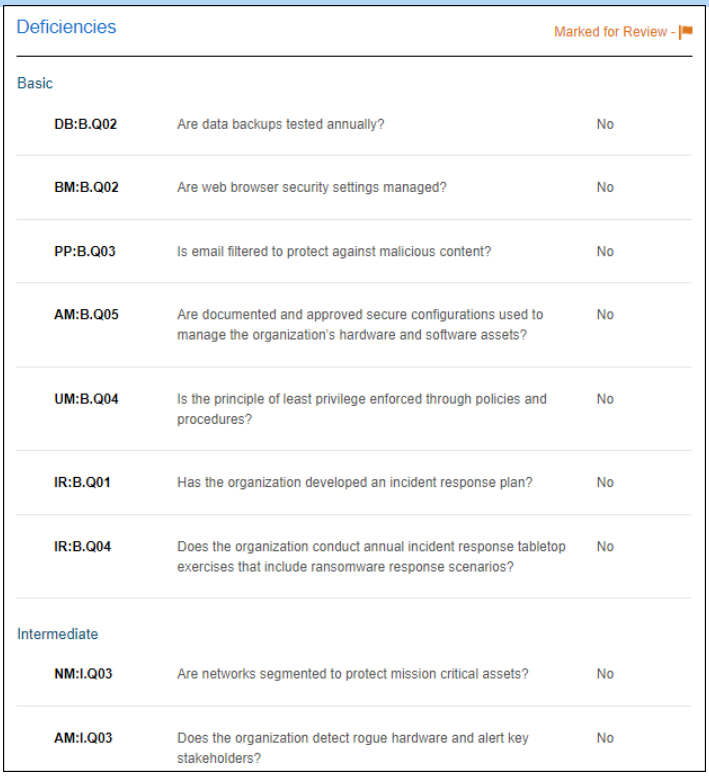
圖 13、十大項目完成度(示意圖)

Identifier	Practice	References
DB:B.Q01	Are important systems and data backed up daily to an offsite location with the ability to restore multiple versions back at least 30 days?	NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-1, CP-2, CP-9, CP-10 NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems: This publication assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle. CIS Control 11 - Data Recovery: Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state. Protecting Data from Ransomware and Other Data Loss Events: A Guide for Managed Service Providers to Conduct, Maintain, and Test Backup Files, National Cybersecurity Center of Excellence (NCCoE), 2020. CRR Supplemental Resource Guide Volume 1 Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process.

圖 14、自評 為‘符合’的項目與細節說明

DB:B.Q02	Are data backups tested annually?	NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. CP-1, CP-2, CP-9, CP-10 NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems: This publication assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle. CIS Control 11 - Data Recovery: Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state. Protecting Data from Ransomware and Other Data Loss Events: A Guide for Managed Service Providers to Conduct, Maintain, and Test Backup Files, National Cybersecurity Center of Excellence (NCCoE), 2020. CRR Supplemental Resource Guide Volume 1 Asset Management Version 1.1: This guide is intended for organizations seeking help in establishing an asset management process.

圖 15、自評為 ‘不符合’的項目與細節說明



Deficiencies — Marked for Review -

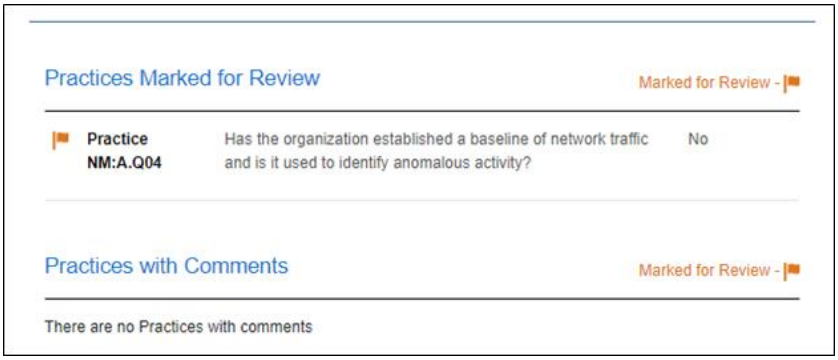
Basic

DB:B.Q02	Are data backups tested annually?	No
BM:B.Q02	Are web browser security settings managed?	No
PP:B.Q03	Is email filtered to protect against malicious content?	No
AM:B.Q05	Are documented and approved secure configurations used to manage the organization's hardware and software assets?	No
UM:B.Q04	Is the principle of least privilege enforced through policies and procedures?	No
IR:B.Q01	Has the organization developed an incident response plan?	No
IR:B.Q04	Does the organization conduct annual incident response tabletop exercises that include ransomware response scenarios?	No

Intermediate

NM:I.Q03	Are networks segmented to protect mission critical assets?	No
AM:I.Q03	Does the organization detect rogue hardware and alert key stakeholders?	No

圖 16、自評為 ‘不符合’的項目清單 (依照等級分類) (示意圖)



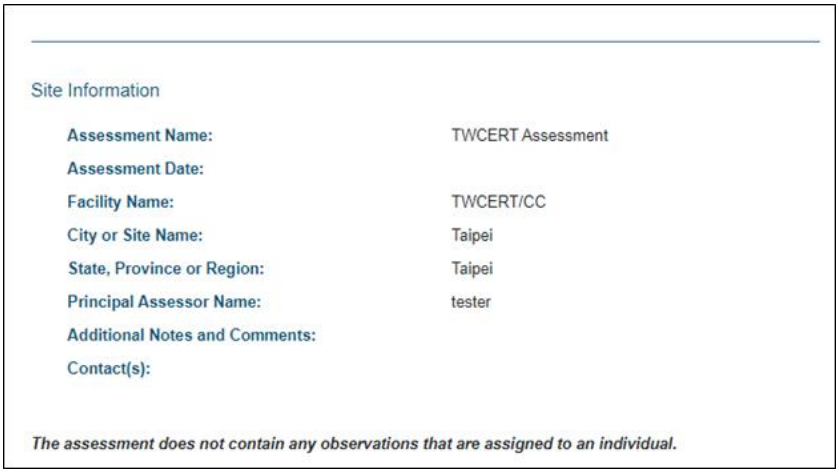
Practices Marked for Review — Marked for Review -

Practice NM:A.Q04	Has the organization established a baseline of network traffic and is it used to identify anomalous activity?	No

Practices with Comments — Marked for Review -

There are no Practices with comments

圖 17、自評階段選取 ‘不確定’的項目清單(示意圖)



Site Information

Assessment Name:	TWCERT Assessment
Assessment Date:	
Facility Name:	TWCERT/CC
City or Site Name:	Taipei
State, Province or Region:	Taipei
Principal Assessor Name:	tester
Additional Notes and Comments:	
Contact(s):	

The assessment does not contain any observations that are assigned to an individual.

圖 18、自評組織的基本資訊(示意圖)

- 資料來源：
  1. NCCIC ICS CYBER SECURITY EVALUATION TOOL
  2. Downloading and Installing CSET
  3. Ransomware Readiness Assessment CSET v10.3

2.1.3、勒索軟體防護之網路資源彙整

1. Stop Ransomware
2. NO MORE RANSOM
3. 刑事局與趨勢科技合作 無償提供電腦版瀏覽器防詐軟體
4. 美國 CISA CSET RRA-勒索軟體防護機制自評工具

- Ransomware Readiness Assessment CSET v10.3
- Downloading and Installing CSET
- NCCIC ICS CYBER SECURITY EVALUATION TOOL

5. 線上勒索軟體辨識服務

- ID Ransomware
- Crypto Sheriff 解碼警長

6. 解密工具

- No More Ransom 解鎖工具
- Trend Micro Ransomware File Decryptor
- 卡巴斯基 Free Ransomware Decryptors
- AVG 免費軟體解密工具
- EMSI SOFT Free Ransomware Decryption Tools
- McAfee Ransomware Recover (Mr2)
- Avast Free Ransomware Decryption Tools
- Quick Heal Free Decryption Tool

- MDS Ransomware Decryption Tools

第 3 章、 資訊安全宣導

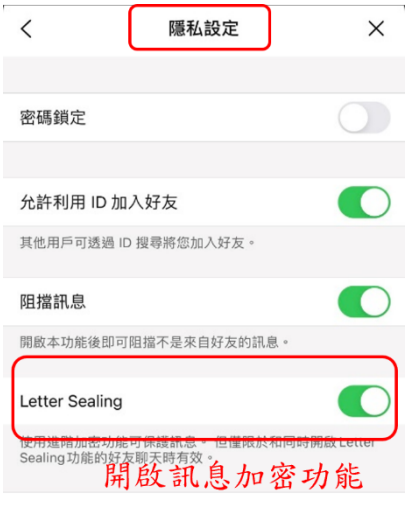
LINE 安全性設定檢視宣導

LINE 是台灣人最常使用的通訊軟體之一，若安全性方面沒有做好管控，可能會造成資訊外洩、帳號遭有心人士入侵等風險，以下說明用戶該如何檢視 LINE 帳號的安全。

請依下列步驟檢視 LINE 帳號的安全性：

1.請至 LINE app 的主頁->設定(齒輪)->隱私設定，檢視【Letter Sealing】是否被關閉，預設應為開啟，如果是被關閉，請立即開啟。

- Letter Sealing 為針對訊息進行點對點加密技術（End to End Encryption），是一種訊息保護的功能，僅有對話雙方才能閱讀訊息內容。



2.請至 LINE app 的主頁->設定(齒輪)->我的帳號，檢視【允許自其他裝置登入】的設定是否開啟，如果有開啟，請執行第 3 點檢視【登入中的裝置】。

3.請至 LINE app 的主頁->設定(齒輪)->我的帳號，檢視【登入中的裝置】，是否有陌生的裝置登入。如果有陌生的裝置登入，表示帳號被駭風險很高，請先截圖留存畫面，再將該陌生裝置登出，並執行第 4 點。

4.請至 LINE app 的主頁->設定(齒輪)->我的帳號，將【允許自其他裝置登入】的設定關閉。

提醒：請勿於社群軟體討論公務或重要事務。

- 資料來源：
  1. Letter Sealing

第 4 章、 國內外重要資安事件

4.1、資安趨勢

4.1.1、資安廠商發表 2021 年第一季駭侵攻擊報告，攻擊量較去年同期增加 17%

資安廠商發表 2021 年第一季駭侵攻擊統計報告指出，各種駭侵攻擊活動的數量，較去年同期相比，增加 17%。

資安廠商 Positive Technologies 日前發表 2021 年第一季駭侵攻擊統計報告，報告中指出各種駭侵攻擊活動的數量，較去年同期相比，增加 17%；如果是跟上一季（2020 年第四季）相較，增加幅度為 1.2。

在所有攻擊活動當中，針對組織發動的佔 88%，針對個人的佔 12%。

以攻擊的目的來看，針對組織發動的攻擊中，資料竊取佔 62%、詐財佔 43%、激進駭客活動（Hacktivism）佔 9%、利用企業資源發動其他攻擊佔 2%；而企業被竊取的資料中，31% 為個人機敏資訊、24% 為智慧財產權、23% 為登入資訊、醫療資訊、客戶資料庫、付款卡片資訊等各佔 6%。

針對個人發動的攻擊活動，69% 是為了取得個人資訊，24% 為了詐取財物、11% 為激進駭客活動；個人被竊取的資料中，51% 為登入資訊、23% 為個人機敏資訊、12% 為通訊內容、6% 為金融卡或信用卡資訊%，其他類則為 8%。

被攻擊的組織類型，政府機關佔比最高，達 12%、其次是製造業佔

11%、科學與教育機構佔 11%、醫療保健機構佔 8%、IT 產業佔 8%、金融業佔 7%、電信業佔 6%、其他產業佔 26%。

從攻擊手法來看，利用惡意軟體發動的攻擊數量，不論機構或個人都佔 58%、利用社交攻擊手法，機構佔 52%，個人佔 89%。

值得注意的是，針對政府機關發動的勒贖攻擊，近年來有日益增加的趨勢；觀察政府機關所有攻擊事件中，勒贖攻擊佔所有惡意軟體攻擊的比例，去年（2020 年)第一季到第四季分別為 28%、26%、37%、54%，而到今年（2021 年）第一季已高達 70%。

- 資料來源：
  1. Cybersecurity threatscape: Q1 2021
  2. Cyber incidents on the rise as ransomware accounts for two thirds of all malware attacks

4.1.2、資安廠商調查指出，54% 勒贖攻擊受害者接受過釣魚攻擊防護訓練

資安廠商調查指出，在遭到從釣魚郵件開始進行勒贖攻擊的受害者中，有 54% 都接受過釣魚攻擊防護訓練。

資安廠商 Cloudian 日前發表調查報告指出，釣魚郵件攻擊是勒贖攻擊者用以發動攻擊的主要手法，各大企業組織也普遍舉辦釣魚攻擊防護訓練；然而在遭到從釣魚郵件開始進行勒贖攻擊的受害者中，有 65% 都接受過釣魚攻擊防護訓練。

Cloudian 針對 200 位近兩年來曾遭勒贖攻擊的各大公私組織中 IT 部門決策者進行調查，得到的調查結果顯示，傳統的勒贖攻擊防護機制是無效的；調查結果摘要如下：

- 24% 的勒贖攻擊，透過釣魚攻擊開始發動；
- 54% 的受害者公司，都曾針對員工舉辦過釣魚郵件防護訓練；
- 49% 的受害者，原本就建置有類似攻擊的防護系統；
- 31% 的勒贖攻擊從公有雲開始發動；
- 44% 的公司在儲存資料時有進行即時加密；
- 43% 的公司會限制內部資料或主機的存取權。

此外，調查也顯示勒贖攻擊者的反應速度極快，有 56% 的受害者表示，勒贖攻擊者能在 12 小時內完全控制該公司的資料，並且要求支付贖款；30%

受害者表示在 24 小時內發生；而超過一半以上的受害者表示，勒贖攻擊對該公司的財務、日常運作、員工、顧客和公司聲譽造成顯著損害：

- 對員工造成損害：59%；
- 對公司財務造成損害：58%；
- 對公司營運造成衝擊：57%；
- 對顧客造成影響：57%；
- 對公司聲譽造成負面影響：52%。

調查也指出，勒贖攻擊造成的受害者財務損失，並不只有支付贖金而已：

- 55% 的受害公司會支付勒款；平均支付金額為 223,000 美元，更有 14% 支付超過 500,000 美元；
- 因為勒贖攻擊造成其他的額外損失，平均為 183,000 美元；
- 資安相關保險僅能彌補所有勒贖攻擊損失的 60%；
- 支付了贖金後，僅有 57% 企業能夠取回所有資料。

- 資料來源：
  1. Cloudian Ransomware Survey Finds 65% of Victims Penetrated by Phishing Had Conducted Anti-Phishing T
  2. Phishing continues to be one of the easiest paths for ransomware

4.1.3、調查指出修復高危險性漏洞所需時間，六個月內自 197 天增至 246 天

資安廠商的調查報告指出，各家廠商修復高危險性資安漏洞所需的時間，在最近 6 個月內，自 197 天增加到 246 天。

資安廠商 NTT Application Security 日前發表的最新 AppSec Flash Report 調查報告指出，各家廠商修復高危險性資安漏洞所需的時間，在最近 6 個月內，自 197 天增加到 246 天。

這份報告主要調查資安漏洞在得到修復前的空窗期長度，因為在空窗期之內，漏洞很可能遭駭侵者用以發動駭侵攻擊。

最新的報告指出，自今年（2021）年初到六月底的半年期間，雖然最主要的五大類漏洞的平均修復日期和過去差別不大，但各種應用程式的漏洞修復空窗期，明顯都拉長了。資安廠商稱「這是常見漏洞修復的系統性失敗」。

根據 NTT Application Security 的資安專家指出，今年上半年一月到六月間，所有漏洞的平均修復需時，自年初的 205 天略為減少到六月的 202 天；而高度危險性的資安漏洞修復需時，卻從年初的 194 天大幅增加到六月的 246 天，多了快要 2 個月。

至於各類型、各種危險程度漏洞的修復比率，也自今年年初的 54%，下降到六月底的 48%；高危險性漏洞的修復比率，更是從年初的 50% 大幅下降

到六月底的 38%。

該報告也分析了各種應用程式類型的漏洞出現比例。工具類應用程式中，有高達 65% 至少含有一個嚴重資安漏洞，為所有應用類型之冠。

報告也說，教育、製造、零售、批發商等產業的漏洞修復空窗期，在近期也拉長了 4%；醫療產業的空窗期則拉長了 2%。至於金融保險產業的空窗期則略有改善，減少了 2%。

- 資料來源：
  1. AppSec Flash Report
  2. Average time to fix high severity vulnerabilities grows from 197 days to 246 days in 6 months: repor
  3. The moment you realize software security can unleash business potential.

4.1.4、Twitter 公布調查報告，開啟二階段登入驗證之用戶比例低

Twitter 近日公布調查報告，指出其活躍用戶中，已啟用二階段登入驗證功能的用戶比例極低，僅有 2.3%。

全球大型社群平台 Twitter 近日公布其 2020 年度透明度調查報告，其中關於用戶資安的部分統計數字指出，自 2020 年 7 月到 12 月為止，其活躍用戶中，已啟用任何一種二階段登入驗證功能的用戶比例極低，僅有 2.3%。

如同許多大型社群或網路服務一樣，Twitter 為防止日益猖獗的帳號竊取事件，提供二階段登入驗證功能；用戶在登入服務時，除了須輸入原有的帳號與密碼外，還需要另外輸入一組隨機產生的登入驗證碼，才能順利登入並使用服務。

Twitter 提供的二階段登入驗證，其隨機驗證碼可以透過簡訊、第三方驗證碼產生軟體，或是硬體隨機驗證碼產生器來取得；在 2.3% 啟用二階段登入驗證的用戶中，有高達 79.6% 的用戶選擇使用簡訊接收驗證碼，30.9% 使用第三方驗證碼產生軟體，使用硬體隨機驗證碼產生器的用戶比例僅有 0.5%。

不過，統計數字也指出，採用二階段登入驗證的用戶比例，在調查期間內還略為增加了 9.1%。

資安專家指出，二階段驗證碼的使用率低落，並不只是 Twitter 一家業者獨有的現象，而是資訊服務產業面臨的共同問題；由於二階段驗證碼的操作過程，比起傳統只需帳號密碼的登入方式更為複雜，也不夠直覺，因此許多

不夠重視自身資安防護的用戶，就不願採用二階段登入驗證功能。

即使是採用了二階段登入驗證的用戶，也有極高比例透過手機門號接收透過簡訊傳來的二階段登入驗證碼；但資安專家指出這仍有風險，因為駭侵者很可能會利用 SIM-Swap 攻擊來取得用戶手機門號的使用權，直接攔截傳來的二階段登入驗證碼。

- 資料來源：
  1. Twitter reveals surprisingly low two-factor auth (2FA) adoption rate
  2. Account Security

4.2、新興應用資安

非惡意挖礦 App 大規模針對 Android 用戶進行詐騙

資安廠商近日發現，超過 170 支 Android App 會鎖定對加密貨幣感興趣的用戶進行詐騙。

資安廠商 Lookout 旗下的研究人員近日發現，近來有超過 170 支 Android App 會鎖定對加密貨幣感興趣的用戶進行詐騙，但由於 App 本身沒有任何惡意軟體程式碼或惡意行為，因此反而很難偵測。

這些「非惡意」詐騙 App 的詐騙行為，是發生在 App 之外；這些 App 多宣稱可以幫用戶進行付費雲端挖礦，但實際上向用戶收了錢，卻不會真正提供任何雲端挖礦服務，用戶花了錢卻無法得到任何承諾的服務，因此也算是一種詐騙。

但由於這些 App 本身沒有進行任何惡意活動，包括沒有惡意軟體酬載安裝、不含任何惡意程式碼、不竊取任何用戶裝置上的資訊，也不會進行任何掃瞄；正因如此，各種惡意軟體防阻機制，不會把這些 App 視為惡意軟體而加以防範，反而讓這類軟體能成功進行詐騙活動。

Lookout 的資安專家，把這 170 支 Android App 分為兩類：前一類稱為 BitScam，其開發框架非常簡單，任何沒有開發經驗的人，也能用這個框架和 SDK 做出一支詐騙 App；另一類則稱為 CloudScam ，其開發框架則是用 Java 製作，需要有程式寫作能力的人才能操作。但兩種框架都能產生這種「非惡意」、不含任何惡意程式碼的詐騙挖礦 Android 應用程式。

Lookout 指出，這 170 支 Android 應用程式中，有 25 支成功在 Google Play Store 上架，其餘則在各種規模較小的第三方應用程式商店內上架；據該公司統計，被這些「非惡意」詐騙挖礦 App 詐騙的受害者多達 86,000 人以上，遭詐騙金額則超過 350,000 美元。

在 Google Play Store 上架的這類詐騙軟體，目前已遭 Google 下架；對加密貨幣挖礦有興趣的用戶，在選擇挖礦服務並安裝軟體時，應特別提高警覺。

- 資料來源：
  1. Lookout Unearths Android Crypto Mining Scams
  2. Non-Malicious Android Crypto Mining Apps Scam Users at Scale

4.3、國際政府組織資安資訊

4.3.1、美國資安主管機關 CISA 推出勒贖攻擊防護評估指南

美國聯邦政府資安主管機關 CISA，近日推出勒贖攻擊防護評估指南，供各公私單位參考，以對抗日益嚴重的勒贖攻擊。

美國聯邦政府資安主管機關網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA），近日推出「勒贖攻擊防護評估指南」（Ransomware Readiness Assessment, RRA），供各公私單位參考，以對抗日益嚴重的勒贖攻擊。

這份勒贖攻擊防護評估指南，是一系列可用以進行自我資安評估的工具，各單位可以依照此指南進行評估，了解自身對於勒贖攻擊的防護程度；特別適用於針對資訊科技（Information Technology）、營運科技（Operational Technology）、工業控制系統（Industrial Control System）資產的勒贖攻擊防護。

在 RRA 的 Wiki 頁面上，CISA 指出：「RRA 同時也提供各單位一條清楚的資安防護提升路線圖，包括各種基本、中等與進階防護的評估用問題。」

RRA 評估工具目前已整合在 CISA 提供的「資安評估工具」（Cyber Security Evaluation Tool, CSET）之中，成為 CSET 的多種資安防護程度評估模組之一。

CISA 表示 RRA 擁有以下特色，可以用來幫助各單位有效對抗勒贖攻擊：

- RRA 可幫助各單位以系統性、有條理且可重覆執行的方式，來評估其資安防護能力，特別是針對勒贖攻擊防護相關的資安標準與最佳執行實務；
- RRA 可用以指導 OT、IT 系統的資產管理與操作者，以系統化的流程來評其系統的資安防護措施，以對抗勒贖攻擊，甚至還提供圖表與表格的分析儀表板，便於檢視各種簡化與詳細資安資訊。

- 資料來源：
  1. CSET 10.3.0 Release Notes
  2. cisagov/cset
  3. CISA releases new ransomware self-assessment security audit tool

4.3.2、美國聯邦調查局發出警訊，提防駭侵者對東京奧運發動攻擊

美國聯邦調查局發出資安警訊，指出即將開幕的東京奧運，以及與奧運相關的個人或組織，近期很可能會面臨駭侵者針對性的攻擊。

美國聯邦調查局（Federal Investigation Bereau，FBI）日前發出資安警訊，指出即將開幕的東京奧運，以及與奧運相關的個人或組織，近期很可能會面臨駭侵者針對性的攻擊，應提高資安防護準備。

在 FBI 近期發表的「私人產業通報」（Private Industry Notification, PIN）中指出，可能的攻擊行動類型，將包括勒贖攻擊、分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）、社交工程攻擊、釣魚詐騙活動、局內人威脅阻斷或騷擾運動賽事轉播、機敏資料之竊取、洩漏、佔有，或是阻斷、影響奧運活動依賴的基礎設施運作等等。

另外，FBI 也說，奧運賽事期間的運動競技、媒體轉播環境、人員住宿、交通、票務與安保措施很可能也會受到駭侵攻擊事件的衝擊。

FBI 指出，目前的情報並不足以證實有某些特定團體，意圖針對特定奧運項目發動何種攻擊；但與奧運相關的直接或間接關係人、組織等，都應該針對其網路與數位環境做好資安防護整備工作。

FBI 說，像奧運這類高知名度的大型活動，往往會成為駭侵團體的攻擊目標，藉以獲取不法金錢利益、製造混亂、加強該團體的知名度、影響主辦單位或執法者的形象，或是宣揚其意識形態。

FBI 指出，2018 年的平昌冬季奧運，就發現疑似有駭侵團體，針對將於 2018 年 2 月 9 日舉辦的開幕典禮進行駭侵攻擊，目標是要破壞開幕典禮的運作；同樣有大批參與該屆冬季奧運的南韓官員、民眾、各國運動員、合作伙伴等相關個人或組織遭到駭入。

- 資料來源：
  1. Potential for Malicious Cyber Activities to Disrupt the 2020 Tokyo Summer Olympics
  2. FBI: Threat actors may be targeting the 2020 Tokyo Summer Olympics

4.3.3、美國國家安全局提供遠距工作者無線設備資安防護指南

美國國家安全局發表最新資安指南，針對遠距工作情境下各種無線連線裝置的使用，提供多個防範資安攻擊破壞的安全使用指引。

美國國家安全局（National Security Agency，NSA）於 2021 年 7 月 29 日，發表最新的資安指南；該指南針對遠距工作情境下各種無線連線裝置的使用，提供多個防範資安攻擊破壞的安全使用指引。

該局提供的指引，主要是提供給美國政府旗下如國家安全系統（National Security System）、國防部（Department of Defense）、國防工業與技術基礎（Defense Industry Base）等單位的遠距工作者遵循之用，但也適用於所有官方與民間單位的遠距工作者。

NSA 在指南中指出，駭侵者可以透過藍牙、公眾 Wi-Fi 無線網路、近場通訊（NFC）等方式攻擊各類資訊裝置，造成個人與組織資料、登入資訊與裝置的危害。

該指南要求遠距工作者如有可能，避免連線到任何公眾 Wi-Fi 無線網路，應盡量以企業組織或個人的 Wi-Fi 連線進行加密安全連線，以提高連線安全性；必須使用公眾 Wi-Fi 網路時，特別不需要密碼即可連線的無限制網路時，更應提高警覺。

NSA 指出，即使是需要密碼才能使用的公眾 Wi-Fi 無線網路，其資料傳輸也未必經過加密，且駭客很可能握有解密用的金鑰；因此在使用公眾 Wi-Fi

連線時，最好使用公私單位或個人的 VPN 連線，進一步對傳輸資料進行加密，以提高安全性。

此外，裝置上開放的藍牙連線與 NFC 近場傳輸功能，也有可能遭不肖人士用於駭入裝置並竊取資訊，遠距工作者也應特別注意不明裝置的連線要求。

NSA 在指南中建議用戶，應保持裝置上作業系統與各種軟體更新至最新版本、使用有效的防毒防駭軟體，並在各項服務上使用多階段登入驗證；如果是經常必須連線到無法信任的網路服務（特別是行動裝置），應該經常重新開機。。

- 資料來源：
  1. Securing Wireless Devices in Public Settings
  2. NSA Issues Guidance on Securing Wireless Devices in Public Settings
  3. NSA shares guidance on how to secure your wireless devices

4.4、社群媒體資安近況

4.4.1、駭侵者公開社群平台 Gettr 用戶個資，近 87,000 用戶受害

甫於七月初推出的社群平台 Gettr，上線不過短短一周，已遭多次駭侵攻擊；近 87,000 名用戶各項個資遭到公開。

甫於今年（2021）七月四日，即美國國慶日當天推出的親川普社群平台 Gettr，上線不過短短一周，傳出已遭至少兩次以上駭侵攻擊；近 87,000 名用戶各項個資在某駭侵相關論壇上遭到公開。

資安媒體 HackRead 取得這批遭竊資料後，加以分析並清除重覆資料，指出共有 76,382 名 Gettr 用戶的個資，在這波攻擊行動中遭到曝光；被公開的用戶資料欄位，包括：用戶使用狀態、所在地、註冊的用戶名稱、出生年月日、Email 地址等。

HackRead 也指出，被竊資料中並不包含用戶登入使用的密碼資訊。

Gettr 是由美國前任總統川普的前發言人 Jason Miller 所推出的全新社群平台，其立場傾向極右保守的川普路線；推出後吸引相當多全球各地川普支持者註冊使用。

據 HackRead 指出，Gettr 從 7 月初推出上線至今，還不到一個星期，至少已遭大規模駭侵攻擊達兩次以上；包括在一堆出後就遭不明人士在其討論區中張貼大量不堪入目的色情圖片與影片，網站上前川普幕僚的知名人士，如創辦人 Jason Miller、Steve Bannon、前國務卿 Mike Pompeo、國會議員 Mojorie Taylor Greene 等人的個人檔案內容也遭惡搞。

駭侵者甚至還在相關論壇上指出，「要入侵 Gettr 是非常容易的」，強調他們只是為了好玩，並沒有政治目的。

Gettr 在接受 HackRead 訪問時強調，註冊 Gettr 無需輸入詳細個資，Gettr 也無意像其他社群平台一樣，透過用戶個資牟利；該站目前已修復遭駭侵者利用的漏洞，後續未曾發生其他入侵事件。

- 資料來源：
  1. Hackers leak scraped data of 87,000 GETTR users
  2. The Trump Team’s New Social Media Platform Is Already Flooded With Hentai

4.4.2、曾駭入 TikTok、Snapchat 的駭客，因 Twitter 駭侵攻擊在西班牙被捕

一名在去年七月犯下 Twitter 名人帳號挾持案件的嫌犯，於日前在西班牙遭到逮捕。

一名在去年七月犯下 Twitter 名人帳號挾持案件的嫌犯 Joseph O′Connor，於日前在西班牙遭到逮捕；他也曾經犯下挾持其他社群平台如 TikTok 和 Snapchat 上帳號的罪行。

Joseph O'Connor 是英國籍，現年 22 歲，他和 Mason Sheppard （又名 Chaewon，19 歲，英國籍）、Nima Fazeli（又名 Rolex，22 歲，美國籍）、Graham Ivan Clark（又名 Kirk，美國籍）等其他三人，在去年 7 月時以 SIM swap 與社交工程等方式，成功駭入 Twitter 的內部管理系統，並且挾持多達 130 個名人與著名公司的 Twitter 帳號，並利用這些帳號發布比特幣詐騙訊息；嫌犯假稱任何匯進指定錢包的比特幣，都可以收到兩倍的匯回款，以此吸引被害人匯款。

在去年的攻擊事件中，被挾持用來發布詐騙訊息的名人或知名公司帳號，包括時為美國總統民主黨候選人的 Joe Biden、Amazon 執行長 Jeff Bezos、美國前總統 Barrack Obama、特斯拉執行長 Elon Musk、前紐約市長 Michael Bloomberg，以及著名投資大師 Warren Buffet，以及全球最大的加密貨幣交易所 Binance、蘋果公司、另一家加密貨幣交易所 Coinbase、共享交通公司 Uber 等。

該次帳號挾持與比特幣詐騙攻擊中，嫌犯控制的比特幣錢包位置，在 24 小時內收到 383 次比特幣轉入，得到近 13 枚比特幣，當時的幣價相當於 117,000 美元。

這些嫌犯也將透過 Twitter 內部系統竊得的超短帳號（如@dark、@w、@l、@R9、@50、@vague）等，在相關社群平台上販售。

這四人目前都被指控多項駭侵罪名。

- 資料來源：
  1. TikTok, Snapchat account hijacker arrested for role in Twitter hack
  2. Who’s Behind Wednesday’s Epic Twitter Hack?

4.5、行動裝置資安訊息

4.5.1、Google 下架 9 個會竊取用戶 Facebook 密碼的 Android App

Google 自 Google Play Store 下架了 9 款 Android App，因這些 App 遭資安專家發現，會用特殊方式竊取用戶的 Facebook 密碼。

Google 日前自 Google Play Store 中下架了 9 款 Android App，其合併下載次數高達 580 萬次；原因是這些 App 遭資安專家發現，會用特殊方式竊取用戶的 Facebook 密碼。

這些被下架的 App 都是相當熱門的應用類型，像是相片特效編輯、加框、運動健身、星座、Android 系統整理加速、移除垃圾檔案等等，用這些功能解除用戶心防，吸引用戶下載。

這些惡意 App 竊取用戶 Facebook 登入帳號密碼的方式也很一致，就是要求用戶輸入其 Facebook 登入資訊，以移除 App 內顯示的廣告；雖然在用戶登入時出現的是真正的 Facebook 登入頁面，但在同一個 WebView 元件中，還會另外載入由駭侵者的控制伺服器植入的 JavaScript 程式碼，以攔截用戶輸入的登入資訊。

這支 JavaScript 程式在獲取用戶的 Facebook 登入資訊後，會再將登入資訊傳回控制伺服器，之後惡意軟體還會竊取用戶存在瀏覽器中的 Cookie。

資安專家也指出，雖然該惡意程式碼目前只竊取 Facebook 登入資訊，但可以隨時透過控制伺服器，變更要竊取的登入服務對象；因此用戶在其他服務的登入資訊也很有可能早被竊取得手。

這九個被 Google 下架的 Android App 分別是 PIP Photo、Processing Photo、Rubbish Cleaner、Inwell Fitness、Horoscope Daily、App Lock Keep、Lockit Master、Horoscope Pi、App Lock Manager。Android 用戶應立即檢查自己是否有下載這些惡意 App 並儘速移除。

- 資料來源：
  1. Android trojans steal Facebook users' logins and passwords
  2. Apps with 5.8 million Google Play downloads stole users' Facebook passwords

4.5.2、Android 惡意軟體 Vultur，會透過 VNC 遠端遙控協定竊取用戶密碼

資安專家發現全新的 Android 惡意軟體，會透過可遠端進行遙控操作的 VNC 協定，記錄用戶在手機上的一切操作，同時竊取鍵盤輸入字元與密碼。

荷蘭資安廠商 ThreatFabric 旗下的資安專家，日前發現一個全新的 Android 惡意軟體 Vultur，會透過可遠端進行遙控操作的 VNC 協定，記錄用戶在手機上的一切操作，同時竊取鍵盤輸入字元與密碼。

Vultur 最早是於 2021 年 3 月時被 ThreatFabric 的資安專家觀察到其活動。ThreatFabric 在報告中說，Vultur 變種自其他 Android 惡意軟體；原先的惡意軟體會在用戶開啟其他正常軟體進行登入時，覆蓋一層假冒的登入頁面，藉以騙取用戶輸入的帳號與密碼。

Vultur 的作法則有所有不同。它會在受感染的 Android 手機上開啟一個 VNC 伺服器，並於背景執行；由於 VNC 原本的功能，就是將電腦設備的畫面傳到另一台電腦上，並使用另一台電腦進行遠端遙控，因此感染 Vultur 的手機，其操作畫面就會被傳送到駭侵者設立的控制伺服器錄製下來，Vultur 幕後的駭侵者即可取得各種 app 的登入帳號與密碼。

據 ThreatFabric 的分析，目前遭到 Vultur 感染的 Android 手機，多為先前遭到另一支惡意軟體 Brunhilda malware 感染的受害者；Brunhilda malware 過去曾出現在 Google Play Store 軟體商店中若干 app 之中，其功能之一就是「酬載」其它的惡意軟體程式碼。

用戶的 Android 裝置若是感染 Vultur，Vultur 會試圖欺騙用戶給予完整的

手機控制權限；一旦成功，Vultur 即可取得完整的手機控制權。另外，當用戶想要移除內含 Vultur 惡意程式碼的 app 時，Vultur 會自動按下「回上頁」按鈕。

用戶如果在 Android 的通知面板中看到一個執行中的螢幕分享程式，名為「Protection Guard」的話，就是遭到 Vultur 的感染；另外，Vultur 也會在受害者的手機中，透過 VNC 遠端遙控功能，安裝更多惡意軟體。

- 資料來源：
  1. Vultur, with a V for VNC
  2. New Android malware records smartphones via VNC to steal passwords

4.6、軟體系統資安議題

4.6.1、建議關閉無列印需求 Windows 伺服器的列印暫存區服務

美國資安主管機關發布資安通報，針對嚴重 0-day 漏洞 PrintNightmare，要求沒有列印需求的 Windows 伺服器，應關閉列印暫存區服務，以免遭到攻擊。

美國政府資安主管機關「網路安全暨基礎設施安全局」（Cybersecurity and Infrastructure Security Agency, CISA），日前發布資安通報，針對極嚴重的 0-day 漏洞 PrintNightmare，要求沒有列印需求的 Windows 伺服器，應關閉列印暫存區服務（Windows Print Spooler），以免遭到攻擊。

這個漏洞原先被辨識為 CVE-2021-1675，微軟也在六月發行的 Patch Tuesday 每月資安修補包中予以修補完成；然而在六月底時資安專家發現，微軟的修補程式在 Windows Server 2019 上並未解決問題；後來在一家中國資安廠商發展出的攻擊概念實作程式碼流出後，外界才發現這個存於 Windows Print Spooler 中的 0-day 漏洞。

該 0-day 漏洞的嚴重程度屬於非常危險的等級，駭侵者可利用此漏洞，在受駭系統上遠端執行任意程式碼；目前這個 0-day 暫時被命名為 PrintNightmare。

CISA 於 7 月 1 日發表資安通報，建議 Windows 所有系統管理者，關閉沒有列印需求的網域控制器或其他伺服器系統上的 Windows Print Spooler 服

務，以免遭到駭侵者利用此漏洞發動攻擊。

CISA 說，網域控制器或 Active Directory 的系統管理員，可以參考微軟於今年（2021 年）1 月發表的指南，關閉未使用的 Windows Print Spooler 服務。

- 資料來源：
  1. PrintNightmare, Critical Windows Print Spooler Vulnerability
  2. Security assessment: Domain controllers with Print spooler service available
  3. CISA: Disable Windows Print Spooler on servers not used for printing

4.6.2、全球逾千家企業遭 REvil 勒索軟體攻擊，建議落實資安防護

REvil 勒索軟體攻擊對象涵蓋全球各大領域產業，影響逾千家企業，台灣多家大型企業也曾受駭，建議企業落實資安防護措施，提升員工資安意識，以免遭勒索軟體攻擊而造成損失。

近年來俄羅斯駭客組織 REvil 逐漸壯大，在勒索軟體的排行中名列前茅，被列為最危險的勒索軟體之一，該駭客組織自 2019 年起，針對全球從製造業、金融業到電信業等 20 個領域進行攻擊。

REvil 專門鎖定全球各地企業進行勒索攻擊，台灣多家企業也深受其害，光是 2021 年國內就已有如電腦大廠、電子代工製造大廠以及半導體封測大廠旗下孫公司等，數家大型企業接連遭遇 REvil 勒索軟體攻擊，並被駭客要求支付高額贖金。

REvil 甚至已開始針對 Linux 平台。今年五月，資安公司 Advanced Intelligence 的研究人員表示，REvil 推出了 Linux 加密工具，在 NAS 設備上也能運行。六月，該公司研究人員發現另一 Linux 版本的 REvil 勒索軟體，鎖定 VMware ESXi 伺服器及釋出用來加密 NAS 裝置的 Linux 版的加密工具。

TWCERT/CC 近日接獲國際情資，2021 年 7 月 2 日美國資訊科技管理業者 Kaseya 遭到 REvil 發動勒索軟體攻擊，導致全球各地上千家企業受害。迄今已有十一國傳出災情，堪稱受害企業最多的單一一起勒索軟體攻擊事件，也是史上規模最大與最嚴重的供應鏈攻擊。駭客的目標為託管服務提供商

(MSP)，這些公司主要客群為中小型企業，透過襲擊這些 MSP 業者便能進一步入侵企業客戶的內網。

根據 Kaseya 與網路安全研究人員，犯案的是一個月前成功勒索大型肉品加工商 JBS 價值一千一百萬美元比特幣的俄羅斯駭客組織 REvil。REvil 於本事件利用 Kaseya 的虛擬系統管理(VSA)軟體之 0-day 漏洞，並藉由此管道透過託管服務提供商散播勒索軟體(圖 1)。美國國土安全部的網路安全與基礎建設安全局(CISA)與 Kaseya 皆聲明建議 Kaseya 使用者立即關閉其 VSA 伺服器。

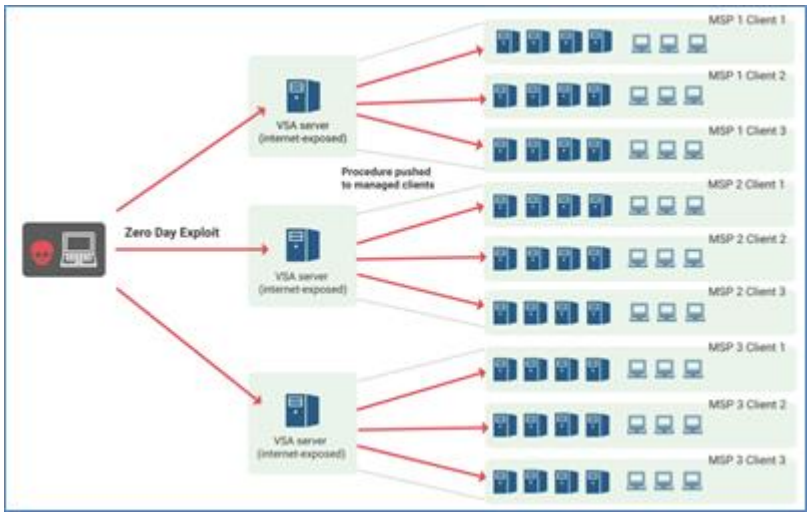


圖 1、Kaseya 產業鏈攻擊示意圖

- 建議採取資安強化措施

1. 立即關閉 Kaseya VSA 伺服器。Kaseya 預計於 7/5(美國時間)釋出漏洞修補更新檔案(官方更新釋出連結)，屆時建議立即進行安全性更新。
2. 建議透過入侵偵測工具(VSA Detection Tools)掃描系統設備是否已存在入侵跡象。
3. 駭客的勒索訊息含有惡意連結，切勿開啟任何連結。
4. 定期進行檔案備份，並遵守備份 321 原則：

➢ 1) 資料至少備份 3 份

- 2) 使用 2 種以上不同的備份媒介
- 3) 其中 1 份備份要存放異地

5. 不論是個人或企業，建議都應做好事前預防措施以及被感染後的應變措施，可參考勒索軟體防護指南。
6. 若企業不幸遭遇駭侵事件，可尋求資安專業單位協助處理，並即時向相關單位進行資安通報，TWCERT/CC 亦為企業通報及協助之單位。

- 資料來源：

1. Important Notice July 4th, 2021
2. VSA Detection Tools
3. REvil ransomware hits 1,000+ companies in MSP supply-chain attack
4. 勒索軟體防護指南
5. Vmware ESXi Virtual Computers Targeted by the REvil Ransomware's New Linux Encryptor

4.6.3、發生過遠端資料刪除事件的 WD NAS，再被發現新的 0-day RCE 漏洞

WD NAS 儲存裝置，又被發現新的 0-day 漏洞，不但會被植入一個永久的後門，而且還能遠端執行任意程式碼。

上個月在全球發生不明攻擊，導致用戶儲存資料被完全刪除的 Western Digital 的 NAS 儲存裝置，又被發現新的 0-day 漏洞；這次的漏洞不但會讓駭侵者以 root 身分，在用戶設備植入一個永久的後門，而且還能遠端執行任意程式碼。

這個 0-day 漏洞發生在 Western Digital 執行「My Could 3」作業系統的 My Cloud 儲存裝置中，而這個版本的 My Cloud 3 作業系統早已無法獲得 Western Digital 的更新與支援。

Western Digital 表示，My Cloud 3 已在數年前由新版的 My Cloud 5 作業系統取代，而新版 My Cloud 5 已經修復此一漏洞；但據資安專家表示，新版的 My Could 5 取消很多舊版 My Cloud 3 中的功能，用戶若將其 NAS 自 My Cloud 3 升級至 My Cloud 5 ，會有很多原本使用的功能出現錯誤而無法繼續使用，因此用戶的升級意願並不高；在舊版作業系統早就停止支援更新的情形下，將會使得該漏洞的潛在威脅程度更為提高。

不過不願升級 My Cloud 3 的用戶，也不是完全沒有希望；有資安專家推出了自己撰寫的修補檔案，My Cloud 3 的用戶可以自行下載安裝。但這個版本有個重大缺點，就是如果用戶重新啟動其 NAS 裝置，本修補程式就會失效；用戶必須再次安裝該修補程式才行。

- 資料來源：
  1. Microsoft Issues Emergency Patch for Windows Flaw
  2. rdomanski/Exploits_and_Advisories

4.6.4、造成 REvil 勒贖攻擊全球 1,500 家企業的零日漏洞，將獲 Kaseya 修補

駭侵團體 REvil 針對 Kaseya VSA 伺服器發動的全球性勒贖攻擊活動，所使用的 0-day 資安漏洞，即將在近日由 Kaseya 推出修補程式予以修補。

七月初由駭侵勒贖團體 REvil 針對 Kaseya VSA（Virtual System/Server Administrator）伺服器平台發動的全球性勒贖攻擊活動，所使用的 0-day 資安漏洞，即將在近日由 Kaseya 推出修補程式予以修補。

這次針對 Kaseya VSA 伺服器的攻擊行動範圍極大。全球有相當多用戶都使用 Kaseya VSA 來管理企業組織之內的眾多電腦設備，包括雲端版本或安裝於客戶端的 Kaseya VSA 伺服器。據資安廠商 TruSec 指出，由於一台 Kaseya VSA 伺服器之下會管理眾多設備，只要該伺服器遭到攻擊得逞，轄下所有管理的電腦設備均無法倖免。

據 Kaseya 表示，此波遭到攻擊的是該公司約 60 個客戶，但其中相當多的「管理服務供應商」，使用 Kaseya VSA 透過網路提供設備管理服務給更多規模較小的客戶，因此受害者多達 1,500 家以上企業。根據 Kaspersky 的報告指出，該公司觀察到的攻擊次數超過 5,000 次，受害企業遍及全球 22 個國家，災情最嚴重的國家為美國與義大利。

根據資安專家報導指出，原本 REvil 對受害企業提供解碼工具的勒贖金額高達 7,000 萬美元，但目前已經「降價」為 5,000 萬美元；但也有個別企業自行與 REvil 接觸，贖金也有低至 50,000 美元的案例出現。

Kaseya 在攻擊事件發生前已經知道這次攻擊使用的 0-day 漏洞 CVE-2021-30116，但並未及時推出修補程式，以致發生規模如此龐大，僅次於 SolarWind 的攻擊事件；該公司已提供緊急處理原則指南，並且承諾將儘快推出修補程式。

- 資料來源：
  1. Important Notice July 7th, 2021
  2. On Premises VSA Startup Readiness Guide - July 7th, 2021
  3. REvil ransomware attack against MSPs and its clients around the world
  4. REVil is now asking for $50 million (lower than previously reported $70 million).
  5. Kaseya Patches Imminent After Zero-Day Exploits, 1,500 Impacted

4.6.5、國內網路產品製造大廠修復路由器密碼硬編寫暨多個 RCE 嚴重漏洞

國內網路產品製造大廠日前推出無線路由器新版韌體，修復先前遭發現的密碼硬編寫與多個其他漏洞；該款產品用戶應即更新韌體。

國內網路產品製造大廠日前推出無線路由器產品 DIR-3040 的新版韌體，同時修復先前遭發現的密碼「硬編寫」(Hard Code)錯誤與多個其他漏洞；該款產品用戶應立即更新韌體，以排除這些錯誤，降低遭駭侵攻擊的風險。

這些錯誤係由 Cisco 旗下的資安專家發現，一共有 5 個漏洞，分列如下：

- CVE-2021-21816：系統 log 檔（Syslog）資訊洩露漏洞；
- CVE-2021-21817：Zebra IP Routing Manager 資訊洩露漏洞；
- CVE-2021-21818：Zebra IP Routing Manager 密碼硬編寫漏洞；
- CVE-2021-21819：Libcli 指令注入漏洞；
- CVE-2021-21820：Libcli 測試環境密碼硬編寫漏洞。

其中 CVE-2021-21818 和 CVE-2021-21820 這兩個漏洞屬於密碼硬編寫漏洞，也就是將系統登入所需的密碼，直接寫在程式碼中；駭侵者將可以透過特制的網路連線要求，觸發這個漏洞並通過登入驗證，直接進入用戶的 DIR-3040 路由器控制界面，並且發動進一步的攻擊，例如利用此裝置對外發動

DoS 攻擊，或是遠端執行任意程式碼。

CVE-2021-21819 是個嚴重的作業系統指令注入漏洞，也可讓駭侵者遠端執行任意程式碼；另外駭侵者還可利用此漏洞，在用戶的 DIR-3040 路由器中建立一個隱藏的 telnet 服務，並且利用硬編寫在路由器程式碼中的密碼進行登入。

- 建議採取資安強化措施

  針對這些漏洞進行修補的新版韌體已經發布，版本號碼為 V.1.13B03 Hotfix；若用戶的 DIR-3040 路由器韌體版本號碼為 V1.13B03 與更舊的版本，務必立即更新，以防駭侵者利用這些漏洞發動攻擊。

- 資料來源：

1. DIR-3040 :: Rev. Ax :: FW v1.13B03 :: CVE-2021-21816 / CVE-2021-21817 / CVE-2021-21818 / CVE-2021-21
2. Vulnerability Spotlight: Multiple vulnerabilities in D-LINK DIR-3040
3. D-Link issues hotfix for hard-coded password router vulnerabilities
4. TechSupport

4.6.6、LockBit 勒贖軟體現可利用群組原則，自動加密 Windows 網域下所有電腦

資安專家發現，新版 LockBit 勒贖軟體，可透過 Windows Server 設定的群組原則，自動加密整個 Windows 網域下的所有電腦。

資安專家發現，新版 LockBit 勒贖軟體 2.0 版多出數項新功能，其中一項可透過 Windows Server 設定的群組原則，自動加密整個 Windows 網域下的所有電腦。使用 Windows Server 管理旗下所有電腦的企業網域管理員，應特別提高警覺。

LockBit 勒贖軟體出現於 2019 年 9 月，是一個「勒贖軟體即服務」(Ransomware as a service），想要發動勒贖攻擊的人，可以「租用」他們的服務，並且設定要攻擊的對象。

一旦勒贖攻擊成功令受害者支付贖款，租用服務的人可以得到 70%~80% 的贖金，LockBit 的開發團隊則會收取其餘的贖款做為佣金。

近年來，LockBit 的勒贖攻擊相當猖獗，其團隊成員為了「促銷」，也在許多駭侵相關論壇主動提供各種「支援」；在許多駭侵相關論壇紛紛禁止勒贖相關主題貼文後，LockBit 的活動便轉到該團體自己設立的資料洩露網站中。

在該團體網站中，最近公布的 LockBit 2.0 最新功能中，即包括可利用群組原則，自動感染 Windows 網域控制站旗下所有 Windows 電腦的功能；攻擊

者不必自行撰寫程式碼進行勒贖軟體「布署」，只要取得 Windows Server 網域控制器的存取權，就會自動進行布署。

執行時，LockBit 2.0 會自動產生新的群組原則設定檔，並且禁用 Microsoft Defender 的即時防護功能，避免布署活動遭到阻斷。

- 資料來源：
  1. MalwareHunterTeam @malwrhunterteam
  2. LockBit ransomware now encrypts Windows domains using group policies

4.7、軟硬體漏洞資訊

4.7.1、QNAP 修復 HBS 3 備份應用程式的嚴重漏洞

QNAP 發表資安通報，修復可能造成駭侵者提升權限、遠端執行任意程式碼的漏洞；QNAP NAS 用戶應立即更新，以降低遭駭風險。

台灣網路儲存設備（Network Attached Storage, NAS）大廠威聯通（QNAP），日前發表最新資安通報，修復一個可能造成駭侵者提升權限、遠端執行任意程式碼的嚴重漏洞；QNAP NAS 用戶應立即依照資安通報內的指示更新系統軟體，以降低遭到駭侵攻擊的風險。

得到修復的嚴重漏洞，其 CVE 編號為 CVE-2021-28809，屬於存取控制不當漏洞，存於 QNAP NAS 內建的資料備份暨還原應用程式 HBS 3 Hybrid Backup Sync 之中。

該漏洞的危險程度分級為最高等級的「嚴重」（Critical），其發生主因是由於程式內的錯誤，造成 NAS 系統無法有效阻擋駭侵者取得系統資源；駭侵者可藉由這個漏洞，提升自身執行權限，遠端執行任意程式碼，或是在未經管理者授權的情形下，任意讀取系統內儲存的各種資料。

QNAP 雖然在日前才發布資安通報，但又表示下列版本的 QNAP NAS 作業系統 QTS 中的 HBS 3 早已完成修復；這些 QTS 和對應的 HBS 3 版本如下：

- QTS 4.3.6: HBS 3 v3.0.210507 與其後版本

- QTS 4.3.4: HBS 3 v3.0.210506 與其後版本
- QTS 4.3.3: HBS 3 v3.0.210506 與其後版本

另外 QNAP 也表示，執行 QTS 4.5.x 與 HBS 3 V16.x 版本的用戶，其軟體不存有此漏洞，因此不必擔心駭侵者透過此漏洞發動攻擊。

- CVE 編號：CVE-2021-28809
- 影響產品/版本：
  - QTS 4.3.6: HBS 3 v3.0.210507 之前版本。
  - QTS 4.3.4: HBS 3 v3.0.210506 之前版本。
  - QTS 4.3.3: HBS 3 v3.0.210506 之前版本。
- 解決方案：升級至下列版本
  - QTS 4.3.6: HBS 3 v3.0.210507 與其後版本
  - QTS 4.3.4: HBS 3 v3.0.210506 與其後版本
  - QTS 4.3.3: HBS 3 v3.0.210506 與其後版本
- 資料來源：

1. Improper Access Control Vulnerability in Legacy HBS 3 (Hybrid Backup Sync)

QNAP fixes critical bug in NAS backup, disaster recovery app

4.7.2、微軟七月 Patch Tuesday 資安修補包，修復 117 個漏洞

微軟於日前推出 2021 年 7 月 Patch Tuesday 每月資安修補包，微軟各系統用戶應立即更新。

微軟於日前推出 2021 年 7 月 Patch Tuesday 每月資安修補包，一共修補多達 117 個漏洞，其中更有 9 個 0-day 漏洞；微軟各系統用戶應立即更新，以避免遭駭侵者利用這些漏洞發動攻擊。

以漏洞危險程度評級來說，在這 117 個得到修補的資安漏洞中，有 13 個屬於「嚴重」（Critical）等級，1 個屬於「中度」（Moderate）等級，103 個「重要」（Important）等級。

以攻擊手法分類的話，在 117 個漏洞中，有多達 44 個屬於遠端執行任意程式碼、32 個為執行權限提升、14 個為資訊洩漏、12 個為服務阻斷、8 個是安全功能遭跳過、7 個是屬於詐騙類型。

值得注意的是，這 117 個漏洞中，有 9 個是屬於 0-day 即時漏洞，其中有 4 個已遭駭侵者大規模利用於攻擊活動之中；包括先前廣泛用於攻擊的「PrintNightmare」（CVE-2021-34527）。其他 3 個已遭大規模濫用的 0-day 漏洞分別如下：

- CVE-2021-33771：Windows 核心執行權限提升漏洞；
- CVE-2021-34448：指令碼引擎記憶體崩潰漏洞；

- CVE-2021-31979：WIndows 核心執行權限提升漏洞。

其餘詳細的更新資訊，可以參考微軟隨此次更新修補包一併推出的資安通報列表。

由於這次微軟修補的漏洞中，有相當多嚴重漏洞，更包括已被大規模濫用的 0-day 漏洞，因此微軟各種產品的用戶與系統管理員，應立即依照各系統的指示與更新功能，安裝並修補這些漏洞，以免遭到駭侵團體鎖定，利用尚未修補的已知漏洞發動攻擊。

- CVE 編號：CVE-2021-33771、CVE-2021-34448、CVE-2021-31979
- 解決方案：依照各系統的指示與更新功能，安裝並修補漏洞。

- 資料來源：
  1. Windows 10 KB5004237 & KB5004245 cumulative updates released
  2. Microsoft July 2021 Patch Tuesday fixes 9 zero-days, 117 flaws

4.7.3、Apple 修復已遭大規模濫用的 iPhone、Mac 0-day 漏洞

Apple 推出 iOS 14.7.1、iPad OS 14,7.1 與 macOS Big Sur 11.5.1，修復遭駭侵者用於攻擊的 0-day 資安漏洞。

Apple 近日緊急推出 iOS 14.7.1、iPad OS 14.7.1 與 macOS Big Sur 11.5.1，修復一個據信已遭駭侵者大規模用於攻擊的 0-day 資安漏洞；擁有這類裝置的用戶，應立即升級至最新作業系統版本。

得到修補的 0-day 漏洞，其 CVE 編號為 CVE-2021-30807，發生在 IOMobileFramebuffer 的核心延伸組件；由於這個組件的記憶體處理錯誤，駭侵者可利用此漏洞，以核心權限遠端執行任意程式碼；不過要利用此漏洞，駭侵者必須先取得裝置的登入權限。

這個漏洞的 CVSS 危險程度評分為 7.5 分，危險程度分級為「高」等級。

Apple 在近期發出的資安通告中指出，該公司已經獲悉這個 0-day 漏洞可能已遭駭侵者用於大規模駭侵攻擊行動，但目前尚無具體攻擊事件的相關情報。

這個漏洞是由匿名的發現者提供給 Apple，Apple 於 7 月 26 日推出 iOS、iPad OS、macOS 的更新版本，修復此一漏洞。

受此 0-day 漏洞影響的 Apple 各類產品，範圍和數量極廣且多；包括各型 Mac 桌上型與筆記型電腦、iPhone 6s 與所有後續機種、iPad Pro 全系列、iPad Air 2 與後續所有機種、iPad 第五代與所有後續機種、iPad mini 4 與所有後續

機種、iPod Touch 第七代等，全都含有該 0-day 漏洞；這些機型的用戶，應立即更新作業系統。

- CVE 編號：CVE-2021-30807
- 影響產品/版本：各型 Mac 桌上型與筆記型電腦、iPhone 6s 及後續所有機種、iPad Pro 全系列、iPad Air 2 及後續所有機種、iPad 第五代及後續所有機種、iPad mini 4 及後續所有機種、iPod Touch 第七代等。
- 解決方案：立即更新作業系統至最新版本。

- 資料來源：
  1. About the security content of macOS Big Sur 11.5.1
  2. Apple fixes zero-day affecting iPhones and Macs, exploited in the wild

4.7.4、Apple 修復可能造成 iPhone Wi-Fi 功能損壞之嚴重 RCE 資安漏洞

Apple 推出 iOS 14.7 更新版，修復可能損壞 iPhone、iPad Wi-Fi 連線功能的漏洞；該漏洞亦可能讓駭侵者遠端執行任意程式碼。

Apple 日前推出 iOS 14.7 更新版，修復一個可能損壞 iPhone、iPad、iPod 等 iOS 裝置 Wi-Fi 連線功能的嚴重漏洞；該漏洞亦可能讓駭侵者遠端執行任意程式碼。

該漏洞的 CVE 編號為 CVE-2021-30800，是由資安研究人 Cark Schou 發現的 0-day 嚴重漏洞；其發生原因是因為 iOS Wi-Fi 安全檢查機制的漏洞；駭侵者可以透過特製含有「%@」特殊字元的 Wi-Fi SSID（例如 DDDD%x%x%x%@），來誘發此一漏洞，可造成 iOS 裝置的 Wi-Fi 連線功能故障而無法使用，甚至在重新開機後亦不能恢復正常。

Wi-Fi 連線功能被破壞的 iOS 裝置，僅能進入系統設定選單，刪除所有網路連線設定，清除有問題的 SSID 名稱後，才能恢復正常連線；但該漏洞亦可導致駭侵者遠端執行任意程式碼，發動進一步的駭侵攻擊。

攻擊者可以在人潮眾多的地方，設立無須密碼，可自由使用的公眾 Wi-Fi 熱點，誘使已將 iOS 裝置的 Wi-Fi 連線設定為自動加入新 Wi-Fi 熱點的用戶連入，進一步發動駭侵攻擊。

這個漏洞出現在 iPhone 6s 與所有後續機種、所有 iPad Pro 機種、iPad Air 2 與所有後續機種、iPad （第五代）與所有後續機種、iPad mini 4 與所有後續機種、iPod touch （第七代），作業系統版本則為 iOS 或 iPad OS 14.7 之前所

有版本。

各種 iOS、iPad OS 裝置用戶，應立即更新至 iOS、iPad OS 14.7 或更新版本，以避免遭駭侵者透過此漏洞發動攻擊；暫時無法更新作業系統版本的用戶，則可以進入設定頁面，取消「自動加入熱點」功能也可以。

- CVE 編號：CVE-2021-30800
- 影響產品/版本：iPhone 6s 與所有後續機種、所有 iPad Pro 機種、iPad Air 2 與所有後續機種、iPad （第五代）與所有後續機種、iPad mini 4 與所有後續機種、iPod touch （第七代），作業系統版本則為 iOS 或 iPad OS 14.7 之前所有版本。
- 解決方案：更新至 iOS、iPad OS 14.7 或更新版本，或進入設定頁面，取消「自動加入熱點」功能。

- 資料來源：
  1. 關於 iOS 14.7 和 iPadOS 14.7 的安全性內容
  2. Apple fixes bug that breaks iPhone WiFi when joining rogue hotspots
  3. After joining my personal WiFi with the SSID (@vm_call twitter)

第 5 章、 資安研討會及活動

趨勢科技 LetsTalk Online EP6: OT 資安疫情炎上 工業資安的最佳效能防毒	
活動時間	**2021.8.25 2:00pm-2:50pm**
活動地點	**線上研討會**
活動網站	**https://www.digitimes.com.tw/seminar/TM_20210825/**
活動概要	 **主辦單位：趨勢科技** 詳細活動議程及報名資訊，請參閱活動網站。 工控系統已是駭客的新興鎖定的攻擊目標，相關的資安問題和管理也成為顯學。 這次邀請到 TXOne Networks* 探討以下幾個重點議題： ● 從 Kesaya 事件看終端防毒的需求與重要性： -我們是如何解決 POS 和 ATM 的資安需求 ● 為什麼針對製造業-ICS 的防毒設計要有所不同? 製造效能至上主義、我們學得會製造基準嗎、零信任基礎、終端防毒對新舊設備的可適用性 ● 談談油電吧！ -由作業系統的漏洞造成的煉油廠/電廠資安疑慮 -就算有單向的防火牆防護，駭客如何滲透，並對已經裝防毒但沒有定期更新病毒碼的機台進行攻擊

工業發展 安全領航 SECURE OT SUMMIT 2021	
活動時間	**2021 年 8 月 26,27 09:00 – 12:30**
活動地點	**線上研討會**
活動網站	**https://m.fortinet.com.tw/site/secure-ot-2021/**
活動概要	 **主辦單位：FORTINET** 詳細活動議程及報名資訊，請參閱活動網站。 在工業 4.0 的浪潮下，製造業紛紛投入轉型以期在數位時代維持競爭力，卻也替企業帶來了 OT 與 IT 網路融合的相關挑戰。隨著企業轉型這些網路營運方式的變化必須考量到網路資安的最佳實踐方案，建立一個可見、可控並持續監控的環境，來解決工業 4.0 下的資安風險，使企業能更有效率適應業務、產業和技術的未來變化。 Fortinet 匯集業界權威講師，以實務經驗提供大家一個完整的解決方案，邀請你 8 月 26、27 日兩天上午，與我們線上相聚。 -活動報名截止日為 8 月 20 日 (五)。主辦單位將視報名狀況提前或延後線上報名時間。 -參加方式：線上活動。完成報名後，另行寄發直播連結；活動當天請於議程開始前登入。 -關於活動有任何問題請來信: secureotsummit_taiwan@fortinet.com

ISO 27001 資訊安全管理系統主導稽核員訓練課程	
活動時間	**9/6-9/8、9/16-9/17（共計五日）**
活動地點	**中華民國資訊軟體協會 訓練教室（台北市承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjY0OQ==**
活動概要	CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 詳細活動議程及報名資訊，請參閱活動網站。 課程說明： ISO 27001 目前已是國際資訊安全管理的準則及規範，更是各國企業組織展現其在資訊安全管理能力的最佳證明！取得「ISO 27001 資訊安全管理系統主導稽核員專業證照」，將代表個人在資安管理上，建置與稽核的專業能力受到肯定，所學將可實際運用在資訊安全領域的技術職、管理職；參加者將從課程中得到如何協助企業組織建立、稽核 ISO/IEC 27001:2013 資訊安全管理系統照。 ● 課程對象： -資訊安全管理人員、內部稽核人員、電腦稽核人員 -ISO/IEC 27001 輔導人員及將提供資訊安全管理系統輔導之顧問 -IT 部門、MIS 部門、財務稽核部門同仁 -有志瞭解 ISO27001 標準規範、知識應用及取得國際專業個人證照者 ● 講師：BSI 台灣分公司專業合格之講師授課（具備 ISO/IEC 27001 主導稽核員資格） ● 教材：英、中對照教材及試卷 ● 證書：BSI 原廠授證。課程測驗通過後，將由 BSI 台灣分公司授予證書；測驗未通過者，本會則將發「結業證書」乙只。 ● 活動聯絡人和聯絡方式：廖資深專員 Email: Maureen.liao@ cisanet.org.tw Tel: (02)2553-3988 Ext：388

資訊軟體稽核	
活動時間	**9/29 09:30-16:30（共計 6 小時）**
活動地點	**中華民國資訊軟體協會 訓練教室（台北市承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjY0OA==**
活動概要	CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 詳細活動議程及報名資訊，請參閱活動網站。 ● 課程大綱： 1、SSDLC 程式開發安全 2、資訊系統委外開發 RFP 資安需求 3、網站攻防實務 ● 課程對象： -參與系統或軟體開發之相關人員 -軟體專案經理、系統架構師、系統分析師 -程式設計師、軟體測試人員 -以上人員需具備 1 年以上系統軟體開發經驗 ● 活動聯絡人和聯絡方式：廖資深專員 Email: Maureen.liao@ cisanet.org.tw Tel: (02)2553-3988 Ext：388 -每班至少 10 名學員始得開班授課，未達人數將退還繳交學費 -以上課程、內容及主講者，主辦單位保留最終變更及調整之權利

【資安學院】政府受駭案例與反思	
活動時間	**10/21 18:30-21:30（共計 3 小時）**
活動地點	**中華民國資訊軟體協會 訓練教室（台北市承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjY0NQ==**
活動概要	CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：** 詳細活動議程及報名資訊，請參閱活動網站。 ● 課程大綱： -政府企業資安威脅種類 -資安攻擊入侵思維 -實際案例 1：我國重要油品事業近期遭勒索病毒案 -實際案例 2：其它政府機關遭駭客入侵案 -個人資安防護議題 ● 課程對象： -企業資訊部門 -提供資訊安全服務之業務、專案、技術與決策等主管及人員 -對本課程有興趣，欲提升資安專業知能者。 ● 活動聯絡人和聯絡方式：廖資深專員 Email: Maureen.liao@ cisanet.org.tw Tel: (02)2553-3988 Ext：388 -每班至少 10 名學員始得開班授課，未達人數將退還繳交學費 -以上課程、內容及主講者，主辦單位保留最終變更及調整之權利

【資安學院】資安事故處理實務	
活動時間	**10/27（三） 09:00-17:00（共計 7 小時）**
活動地點	**中華民國資訊軟體協會 訓練教室（台北市承德路二段 239 號 6 樓）**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjY0NA==**
活動概要	CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C. **主辦單位：中華民國資訊軟體協會** 詳細活動議程及報名資訊，請參閱活動網站。 ● 課程說明：本課程設計除透過瞭解資安事故處理生命週期，藉以學習當資安事故發生時如何進行資安事故處理程序之外，並由資安事故處理以及數位鑑識處理之實務操作，讓結業學員學習到包含數位證據保全有效性之資安事故處理實務。 ● 課程大綱：端點勒索軟體與 APT、網站入侵、雲端線上服務、行動與物聯網裝置、資料庫和資料外洩等事故案件解析、報告撰寫。 本課程需自備筆電、並具備 VMware 環境 ● 課程對象： 資安(訊)主管 資訊安全管理人員 系統管理人員 網路管理人員 具備 1 年以上實務操作經驗與資安事件調查知識尤佳 ● 活動聯絡人：廖資深專員 Email: Maureen.liao@ cisanet.org.tw Tel: (02)2553-3988 Ext：388 每班至少 10 名學員始得開班授課，未達人數將退還繳交學費 以上課程、內容及主講者，主辦單位保留最終變更及調整之權利

第 6 章、 2021 年 7 月份資安情資分享概況

本中心每日透過官方網站、電郵、電話等方式接收資安情資，以下為各項統計數據，分別為對外資安情資分享地區統計圖及資安情資分享類型統計圖。

分享地區統計圖為本中心所接獲之資安情資分享中，針對資安情資所屬地區之分享比率，如圖 1 所示；分享類型統計圖則為本中心所接獲的資安情資分享中，各項攻擊類型之比率，如圖 2 所示。

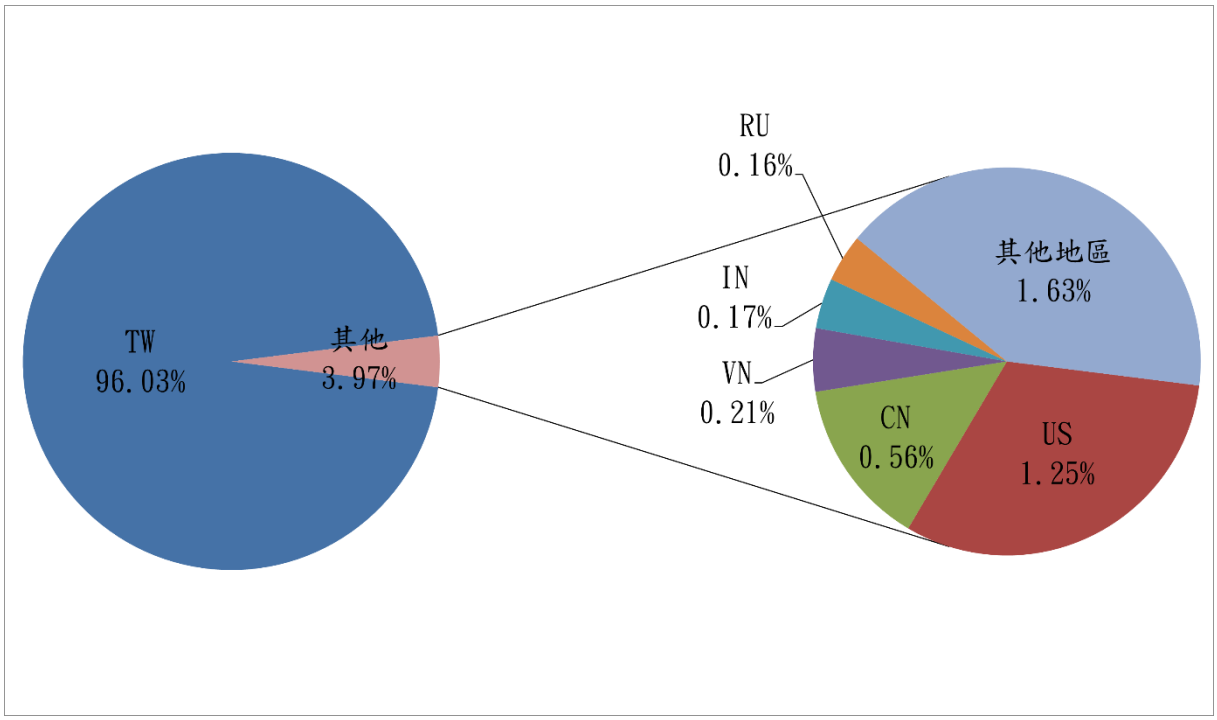


圖 1、分享地區統計圖

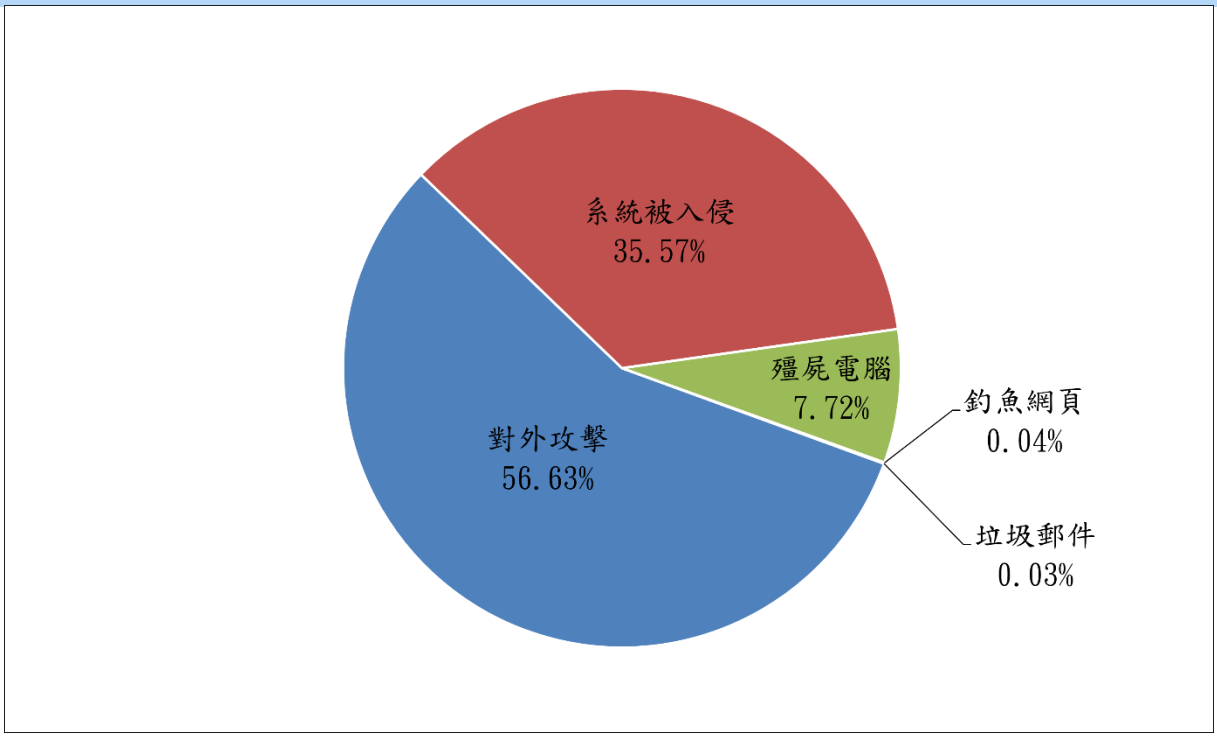


圖 2、分享類型統計圖

發行單位：**台灣電腦網路危機處理暨協調中心**
(Taiwan Computer Emergency Response Team / Coordination Center)

出刊日期：**2021 年 8 月 10 日**

編輯：**TWCERT/CC 團隊**

服務電話：**0800-885-066**

電子郵件：**twcert@cert.org.tw**

官網：**https://twcert.org.tw/**

痞客邦：**http://twcert.pixnet.net/blog**

Facebook 粉絲專頁：**https://www.facebook.com/twcertcc/**

Instagram：**https://www.instagram.com/twcertcc/**

Twitter：**@TWCERTCC**