TLP:GREEN

資安威脅案例與企業資安事件通報應變制度簡介

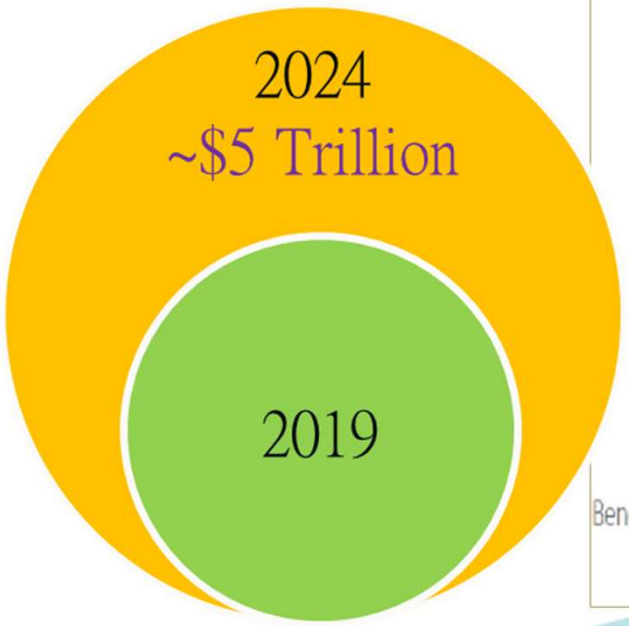
台灣網路資訊中心(TWNIC)

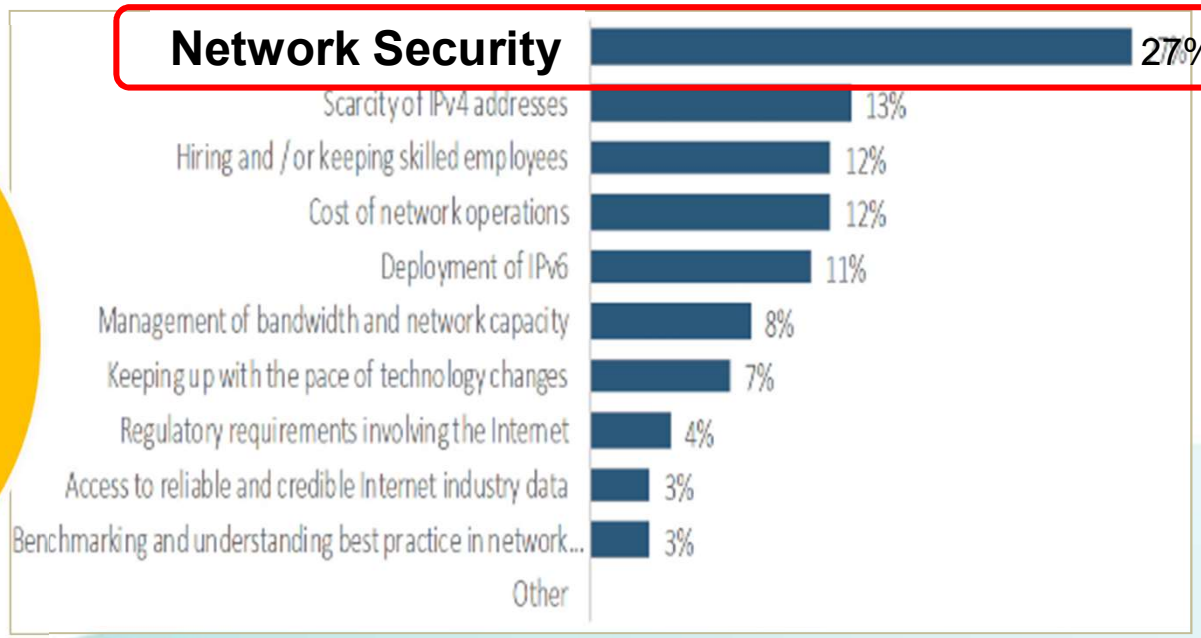
2022.05.31

大綱

- 資安威脅趨勢
- 殭屍網路(挖礦/後門/DDoS)
- 社交工程與變臉詐欺
- 勒索軟體
- 軟體更新
- 資安事件通報應變

資安為數位經濟重要挑戰





- Cost of data breaches due to the Cybercrime
  - $5 Trillion globally in 2024
  - average annual growth of 11%

  [Juniper research, 2019]
- Security is the biggest challenge for internet service provider

  [APNIC, 2018]

主要資安攻擊面向

Applications & Services		• Phishing • SQL-Injection • XSS • …
Data/Storage		• Ransomware • Data Breach • …
Communication Networks		• DDoS • DNS attack • BGP Hijacking • Man-in-the-Middle ….
Computer Systems/Device		• HeartBleed • Rootkit • Fireless Attack…

社交工程與變臉詐欺

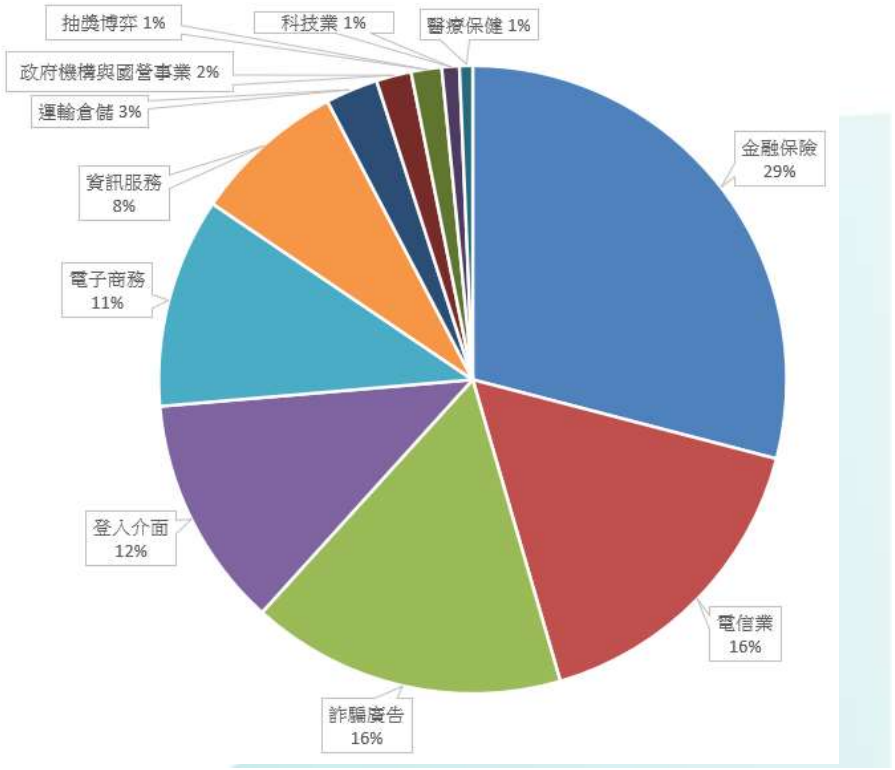
釣魚網站資安威脅

- 釣魚網站偽冒金融、購物、電信網站，以取得帳密、個資為主要目標
- 資安廠商 Vade 於3月發表2021年釣魚攻擊相關統計報告，其中假冒社群媒體的比例首次比其他類別品牌要多
- 2021年，TWCERT/CC統計國內模仿對象則以金融保險最多，電信業次之
- 釣魚網站的處理方式，TWCERT/CC可協助通報國內ISP、國外相關單位處理

Vade統計前20名

1. Facebook（社群媒體）
2. Microsoft（軟體與雲端服務）
3. Crédit Agricole（金融服務）
4. WhatsApp（社群媒體）
5. La Banque Postale（金融服務）
6. Orange（電信服務）
7. Amazon（電子商務）
8. Chase（金融服務）
9. Comcast（電信服務）
10. PayPal（金融服務）
11. DHL（電子商務 / 物流）
12. Netflix（雲端服務）
13. Wells Fargo（金融服務）
14. Rakuten（電子商務）
15. Adobe（雲端服務）
16. OVH（電信服務）
17. LinkedIn（社群媒體）
18. MTB（金融服務）
19. Apple（電子商務）
20. Yahoo（網路服務）

Twcert/CC統計2021釣魚網站偽冒類別



釣魚網站 – 金融

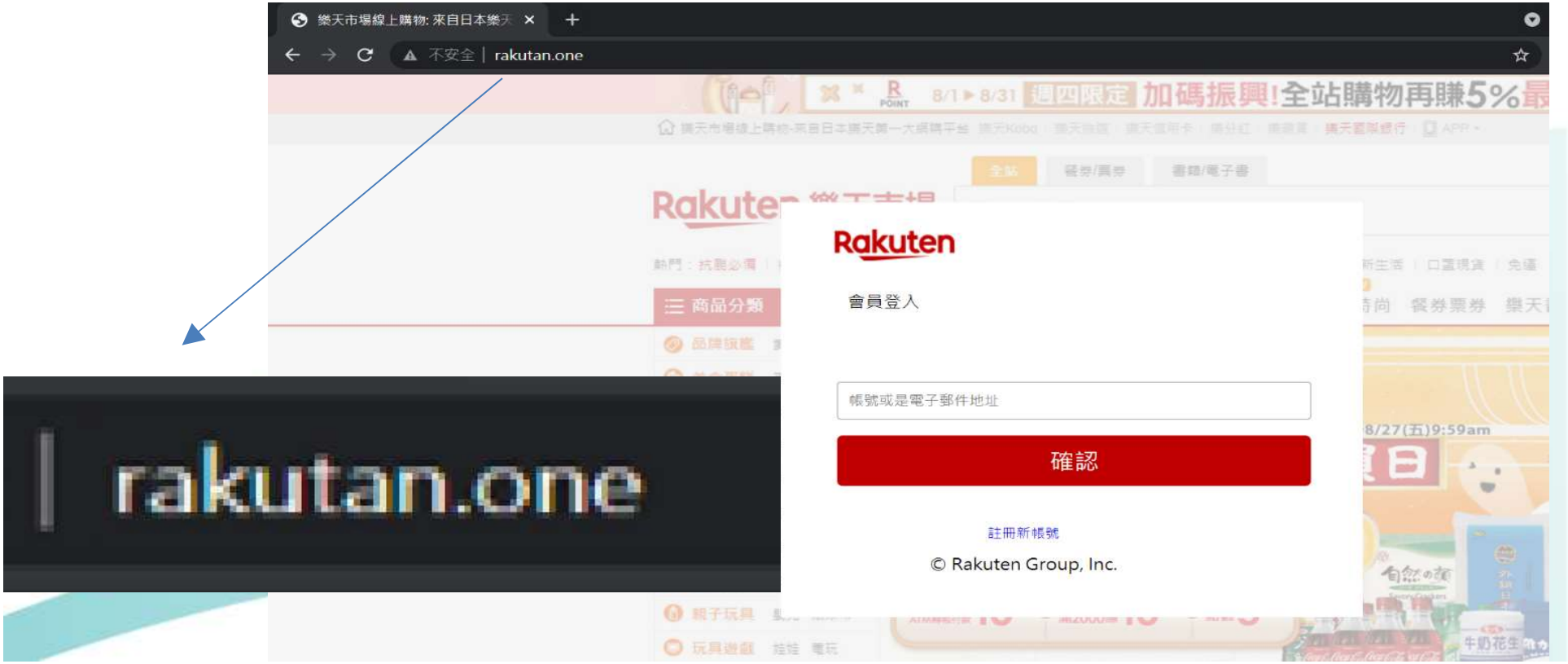
- 110年6月29日接獲通報，有模仿「台中商銀」登入頁面網站
- 網站的IP國家為冰島，通報PhishTank、Netcraft、Browser協助列為黑名單
- www.tcbbanktw.com vs https://www.tcbbank.com.tw/

釣魚網站 – 金融

- 110年8月4日接獲通報，有模仿「中國信託」登入頁面網站
- 網站的IP國家為冰島，通報PhishTank、Netcraft、Browser協助列為黑名單
- www.ctcbcbank.com vs www.ctbcbank.com

釣魚網站－電子商務

- 110年04月06日接獲APNOW通報情資來源，有模仿「蝦皮購物」電子商務業釣魚網站
- 110年8月30日接獲通報，有模仿「樂天市場」電子商務業釣魚網站
- 網站的IP國家為美國，並且通報PhishTank、Netcraft、Browser協助列為黑名單



釣魚網站 – 電信業

- 110年04月15日接獲通報，有模仿「中華電信」登入頁面網站
- 網站的IP國家為美國，並且通報PhishTank、Netcraft、Browser協助列為黑名單

釣魚網站 – 公協會

- 110年6月8日接獲通報，有模仿「高雄市工業會」登入頁面網站
- 網站的IP國家為台灣，通報CISAC協助列為黑名單

變臉詐騙BEC

- 變臉詐騙、Business Email Compromise，也被稱為商務電子郵件入侵
- 利用假造身分的電子郵件，如高階主管，取得下屬/被害人的信任，使其進行轉帳及詐騙金錢財物

新的變臉詐騙媒介

- COVID-19疫情使在家辦公、視訊會議成為常態，美國聯邦調查局（FBI）警告惡意集團趁機進行變臉詐騙
- 駭客冒充CEO或CFO，發送遠端會議的電子郵件，謊稱鏡頭或麥克風問題，只顯示照片，甚至是以Deep Fake技術偽冒音效進行會議
- 透過這些方式要求員工進行匯款動作，也可能利用CEO郵件帳號參與員工遠端會議，蒐集該公司商業資訊
- 也可在遠端會議中送出惡意檔案，讓與會者安裝

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

February 16, 2022

Alert Number
I-021622-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Business Email Compromise: Virtual Meeting Platforms

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

USING VIRTUAL MEETING PLATFORMS FOR BEC ACTIVITY

注意社群軟體使用安全

IG藏漏洞！個資恐外洩 資安專家：快更新

新頭殼newtalk | 郜敏 綜合報導

發布 2020.09.28 | 13:17

TechNews 科技新報

5G OTA Tests
In the Field
GET THE PAPER

零組件 行動裝置 網路 AI 人工智慧 尖端科技 生物科技 能源科技 系列專題 財經 財報快訊 拓

Facebook 又爆個資外洩，5.33 億用戶個資被發布在駭客論

作者 侯 冠州 | 發布日期 2021 年 04 月 04 日 9:57 | 分類 Facebook , 網路 , 資訊安全

分享 分享 Follow 讚 1,240 分享

社群媒體、即時通訊資安議題

- 惡意軟體傳播管道：為釣魚網站連結的傳播主要方式，亦或是更為直接的惡意檔案傳輸，點擊後直接執行
- 機敏資料外洩：社群媒體、即時通訊出現漏洞，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
- 社交工程攻擊：駭客集團在初步蒐集情資後，可鎖定特定具獲利空間族群進行攻擊，例如以金融銀行為對象，亦可主動創建群組，藉由資訊的分享來吸引特定族群參加
- 隱私保護議題：為社群媒體主要被質疑的資安議題

社群媒體與即時通訊的資安案例(1)

- 駭客集團已建立各種由社群媒體與即時通訊取得攻擊可用的資訊管道
  - 成立Facebook進行宣傳惡意網站
  - 註冊假的LinkedIn帳號與知名企業接觸
  - 在Twitter等媒體註冊帳號與被勒索受害者溝通
- MITRE ATT&CK 整理惡意集團的社群媒體使用方式(APT32、Cleaver、Sandworm Team為駭客集團，Fox Kitten則是知名駭客)

ID	Name	Description
G0050	APT32	APT32 has set up Facebook pages in tandem with fake websites.
G0003	Cleaver	Cleaver has created fake LinkedIn profiles that included profile photos, details, and connections.
G0117	Fox Kitten	Fox Kitten has used a Twitter account to communicate with ransomware victims.
G0034	Sandworm Team	Sandworm Team has established social media accounts to disseminate victim internal-only documents and other sensitive data.

社群媒體與即時通訊的資安案例(2)

- 利用行動APP蒐集帳密、個資、企業資料
- RCSAndroid是針對Android的惡意軟體，其存在目的就是為了要蒐集使用者資訊，其行為就有針對社群媒體的攻擊手法

以MITRE ATT&CK 整理RCSAndroid攻擊手法

動作ID	名稱	說明
T1409	訪問存儲的應用程序數據	RCSAndroid可以從流行應用程序收集聯繫人和消息，包括 Facebook Messenger、WhatsApp、Skype、Viber、Line、微信、Telegram
T1429	捕獲音頻	RCSAndroid可以使用設備麥克風錄製音頻
T1512	捕捉相機	RCSAndroid可以使用前後攝像頭拍攝照片
T1414	捕獲剪貼板數據	RCSAndroid可以監控剪貼板內容
T1533	來自本地系統的數據	RCSAndroid可以收集Wi-Fi網絡和在線帳戶的密碼，包括 Skype、Facebook、Twitter、Google、WhatsApp、Mail 和 LinkedIn

社群媒體與即時通訊的資安案例(3)

- 即時通訊的漏洞也是重要議題，尤其行動設備必定安裝即時通訊
- 2021年8月發現駭客釋出強化WhatsApp的助手APP FMWhatsappWhatsApp以改善 WhatsApp 用戶體驗來吸引下載
  - 更好的隱私、自定義聊天主題、訪問其他社交媒體的表情符號包以及使用PIN、密碼等鎖定應用功能
  - 其中包含各種惡意軟體，包括非常難以刪除的xHelper及Triada木馬軟體
- FMWhatsappWhatsApp將下載並啟動多個惡意軟體
  - Trojan-Downloader.AndroidOS.Agent.ic，下載並啟動其他惡意模組
  - Trojan-Downloader.AndroidOS.Gapac.e，安裝其他惡意模組並顯示全螢幕廣告
  - Trojan-Downloader.AndroidOS.Helper.a 執行xHelper安裝程序並在後台運行隱形廣告
  - Trojan.AndroidOS.MobOk.i 為Android設備所有者註冊付費訂閱
  - Trojan.AndroidOS.Subscriber.l 為受害者註冊高級訂閱
  - Trojan.AndroidOS.Whatreg.b 收集信息並請求驗證碼登錄受害者的 WhatsApp 帳戶

社群媒體的資安防護

- 保護在社群媒體上發布的內容
  - 風險威脅
    - 不當的內容、錯誤訊息或發布個人觀點（不是“官方”公司觀點）可能會損害對組織的信任
    - 出於惡意目的劫持，例如重定向到惡意網站
  - 應對作法
    - 確保只有授權人員才能發佈內容
    - 對離職者或調離部門者進行追蹤管理
    - 使用提供良好安全功能的社交媒體平台
    - 確保內容在發布前可以經過審核和授權
    - 使用公司設備創建和發佈內容
    - 制定緊急恢復計劃
- 如何安全使用社群媒體
  - 威脅風險
    - 魚叉式釣魚攻擊
    - 社交工程
    - 身份識別相關威脅
    - 網站應用攻擊
  - 應對作法
    - 依循來自社交媒體平台的安全建議，並設定安全policy。
    - 使用兩步驗證 (2FA) 來保護帳戶。
    - 制定政策並強化存取、網路與端點的控制措施。
    - 供應商與合作廠商管理機制。

即時通訊的資安防護

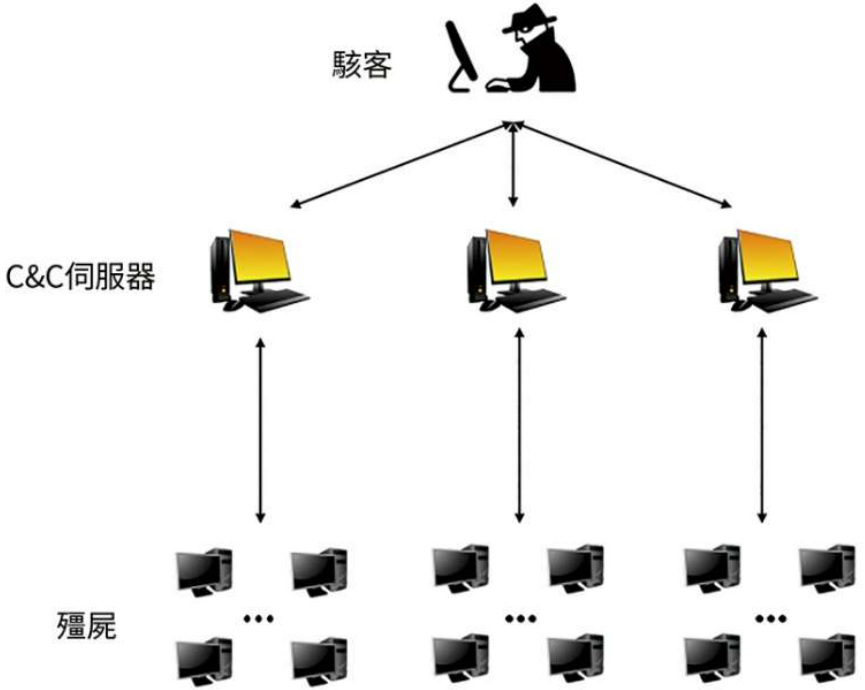
- **不隨意開啟連結**
- 最小化即時通訊軟體的權限設定，如: 關閉自動下載或只允許通訊錄的人員通訊
- 避免透過即時通訊軟體提供機密資料，並確認對方身份
- 定期更新即時通訊軟體
- 封鎖不明使用者的訊息
- 了解即時通訊軟體的安全機制，如: 訊息加密、訊息刪除、雙因子身分驗證、安全設定、雲端備份機制等，並採用適當設定
- 關閉自動接受好友申請與搜尋功能
- 使用即時通訊軟體的設備應啟用螢幕保護程式、使用電腦或網頁板的通訊軟體後確實進行登出
- 企業應明訂即時通訊軟體政策，如: 指定員工使用特定即時通訊軟體、不可傳送企業機密與文件、使用即時通訊軟體的手機應設定自動螢幕鎖定及加密儲存等
- 訂定行動裝置使用管理機制
- 定期舉行員工資安意識教育訓練

殭屍網路(挖礦/後門/DDoS)

殭屍網路架構類型

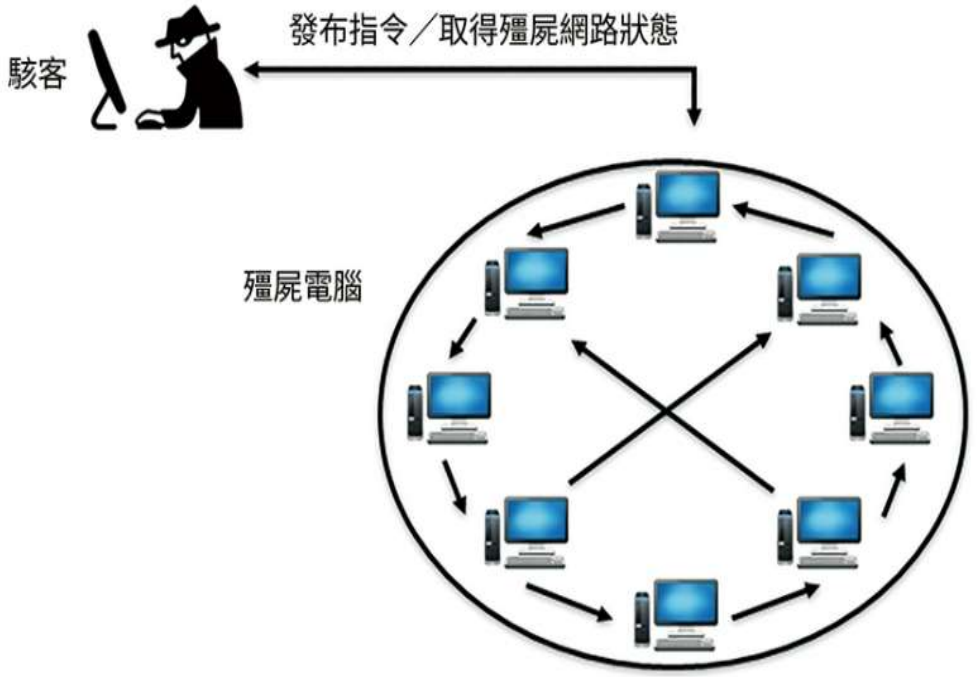
集中式殭屍網路

- 由受感染殭屍電腦(Client)與C&C(Command and Control)伺服器組成
- 透過C&C 伺服器快速將指令傳給殭屍電腦
- 主要的殭屍網路結構方式
- Client與 C&C伺服器間的溝通產生流量異常，較易找到C&C伺服器並清除殭屍網路



P2P (Peer to Peer) 殭屍網路

- 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
- 技術難度較高，但更具彈性
- 要清除殭屍網路，須找到該網路的 Peer List，清除難度較高

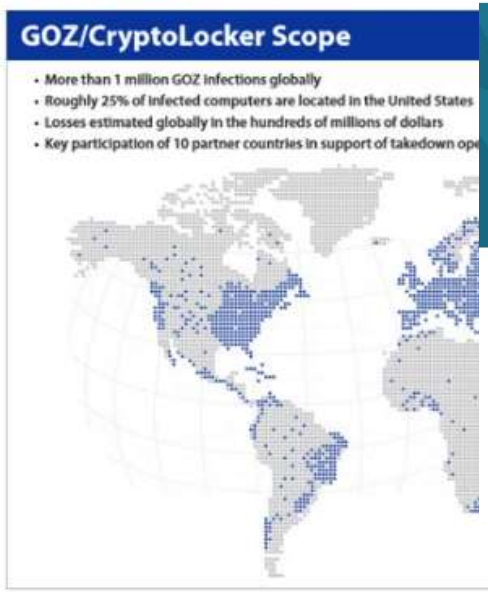


利用殭屍網路發起的攻擊

- **分散式阻斷(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
- **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
- **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
- **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
- **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

DDoS造成危害–不要成為殭屍幫

新|



觀點

您現在位置：首頁 > 觀點

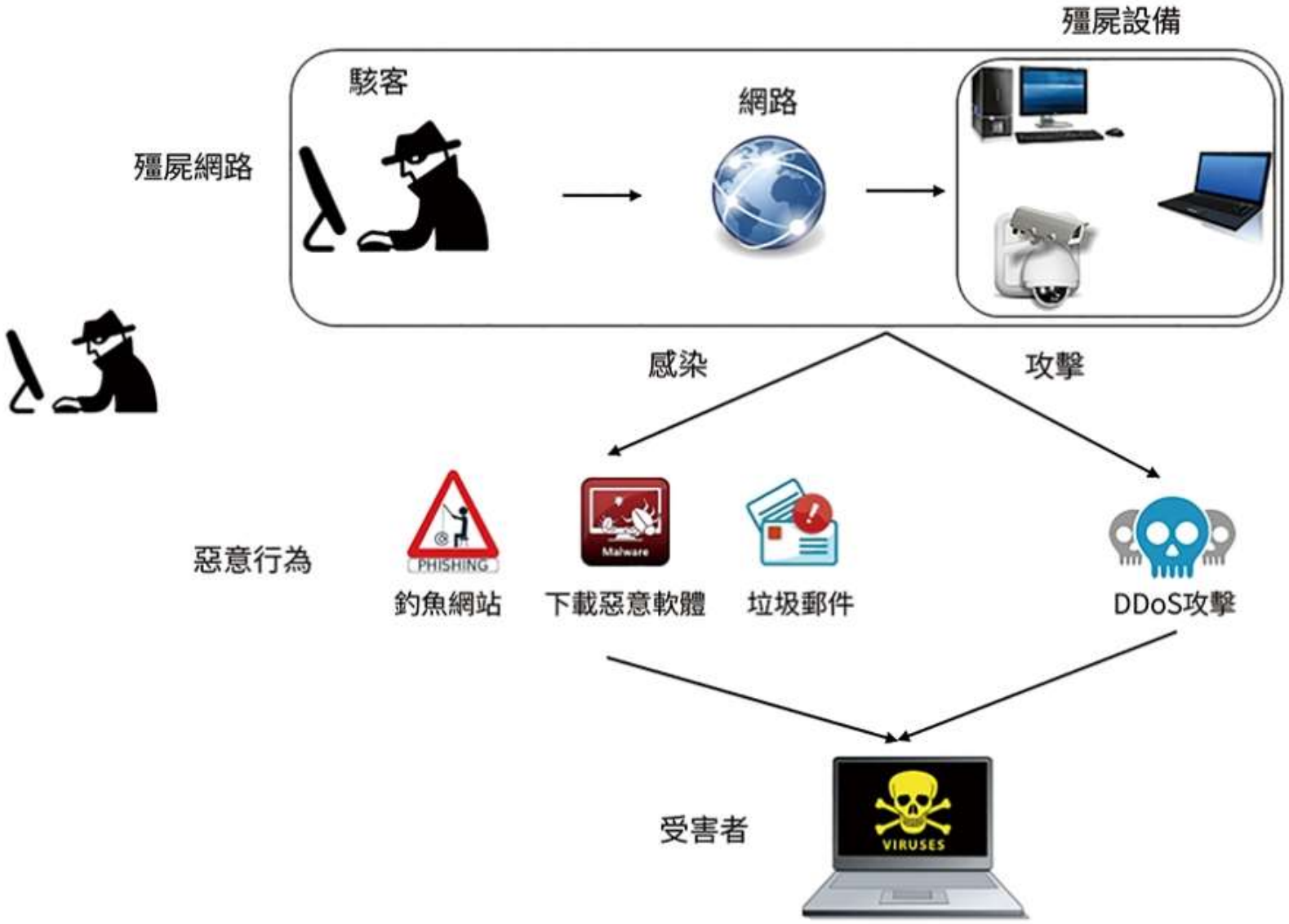
IoT殭屍網路朝P2P化發展&資安建議

2021我國資訊設備遭感染概況

- 2021年，國內ICT設備遭入侵感染，被利用對國外發起超過60萬次資安攻擊
- IoT類：
  - mirai在2020年為主要惡意軟體，在2021已大幅下降
  - conflicker已由Windows擴大至大型IoT設備，如醫療的MRI、CT掃描器
- NAS類：qsnatch針對 NAS設備感染，且持續改進感染方式
- 行動裝置類：android hummer惡意軟體長期占據前三名

1		2		3		4		5		6		7		8		9		10		11		12	
mirai	⟺	mirai	⟺	android. hummer	↑	qsnatch	↑	wannacrypt	↑	android. hummer	↑	pva. intowow	✚	android. hummer	↑	qsnatch	↑	android. hummer	↑	downadup	↑	android. hummer	↑
qsnatch	↑	android. hummer	↑	qsnatch	↑	android. hummer	↓	android. hummer	⟺	qsnatch	↑	wannacrypt	↑	downadup	↑	android. hummer	↓	downadup	↑	android. hummer	↓	downadup	↓
android. hummer	↑	qsnatch	↓	wannacrypt	↑	wannacrypt	⟺	qsnatch	↓	downadup	✚	android. hummer	↓	qsnatch	↑	downadup	↓	virut	↑	virut	⟺	lethic	↑
conficker	↓	wannacrypt	↑	mirai	↓	lethic	↑	virut	↑	wannacrypt	↓	qsnatch	↓	wannacrypt	↓	virut	↑	lethic	↑	lethic	⟺	virut	↓
wannacrypt	↓	lethic	↑	lethic	⟺	conficker	↑	lethic	↓	virut	↓	downadup	↓	virut	↑	lethic	↑	avalanche-andromeda	↑	conficker	↑	conficker	⟺
sality-p2p	↓	conficker	↓	conficker	↓	virut	↑	conficker	↓	conficker	⟺	pva.torrent. kickasstracker	✚	lethic	↑	conficker	↑	conficker	⟺	avalanche-andromeda	↓	avalanche-andromeda	⟺
lethic	⟺	virut	↑	emotet	↑	emotet	⟺	avalanche-andromeda	↑	lethic	↓	virut	↓	avalanche-andromeda	✚	avalanche-andromeda	⟺	avalanche-generic	↑	dltminer	↑	android.bakdoor. prizmes	✚
virut	↑	emotet	✚	virut	↓	avalanche-andromeda	↑	coinminer	↑	avalanche-andromeda	↓	conficker	↓	conficker	⟺	avalanche-generic	↑	sality	↑	avalanche-generic	↓	avalanche-generic	⟺
proxyback	↓	avalanche-andromeda	↑	coinminer	✚	coinminer	⟺	sality	↑	avalanche-generic	✚	pva.torrent. publictorrent	✚	avalanche-generic	✚	mozi	✚	mozi	⟺	sality	↓	sality	⟺
avalanche-andromeda	⟺	sality	✚	avalanche-andromeda	↓	sality	✚	mozi	✚	dltminer	✚	lethic	↓	sality	✚	sality	⟺	dltminer	✚	mozi	↓	dltminer	↓

殭屍網路運作方式


殭屍設備
駭客
網路
殭屍網路
感染
攻擊
惡意行為
PHISHING
Malware
釣魚網站
下載惡意軟體
垃圾郵件
DDoS攻擊
受害者
VIRUSES

影響企業運作的挖礦軟體

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 iThome鐵

新聞

挖礦軟體藏身免費版PC遊戲軟體入侵用戶電腦

包括《NBA 2K19》、《Jurassic World Evolution》等多款遊戲盜版軟體內藏惡意挖礦軟體，並具備關閉防毒軟體等反偵測能力

文/ 林妍溱 | 2021-06-28 發表

讚 6.6 萬 按讚加入iThome粉絲團 讚 137 分享

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 iThome鐵人賽 搜

新聞

惡意程式Dexphot以高明手法躲避偵測，8萬台Windows PC變比特幣挖礦機

Dexphot不但會清空合法行程內容，以便借其外殼執行惡意程式，還會每半小時就改變檔名及型態，以迴避防毒軟體偵測

文/ 林妍溱 | 2019-11-27 發表

讚 6.6 萬 按讚加入iThome粉絲團 讚 1,071 分享

Microsoft iTho

Emotet木馬資安威脅

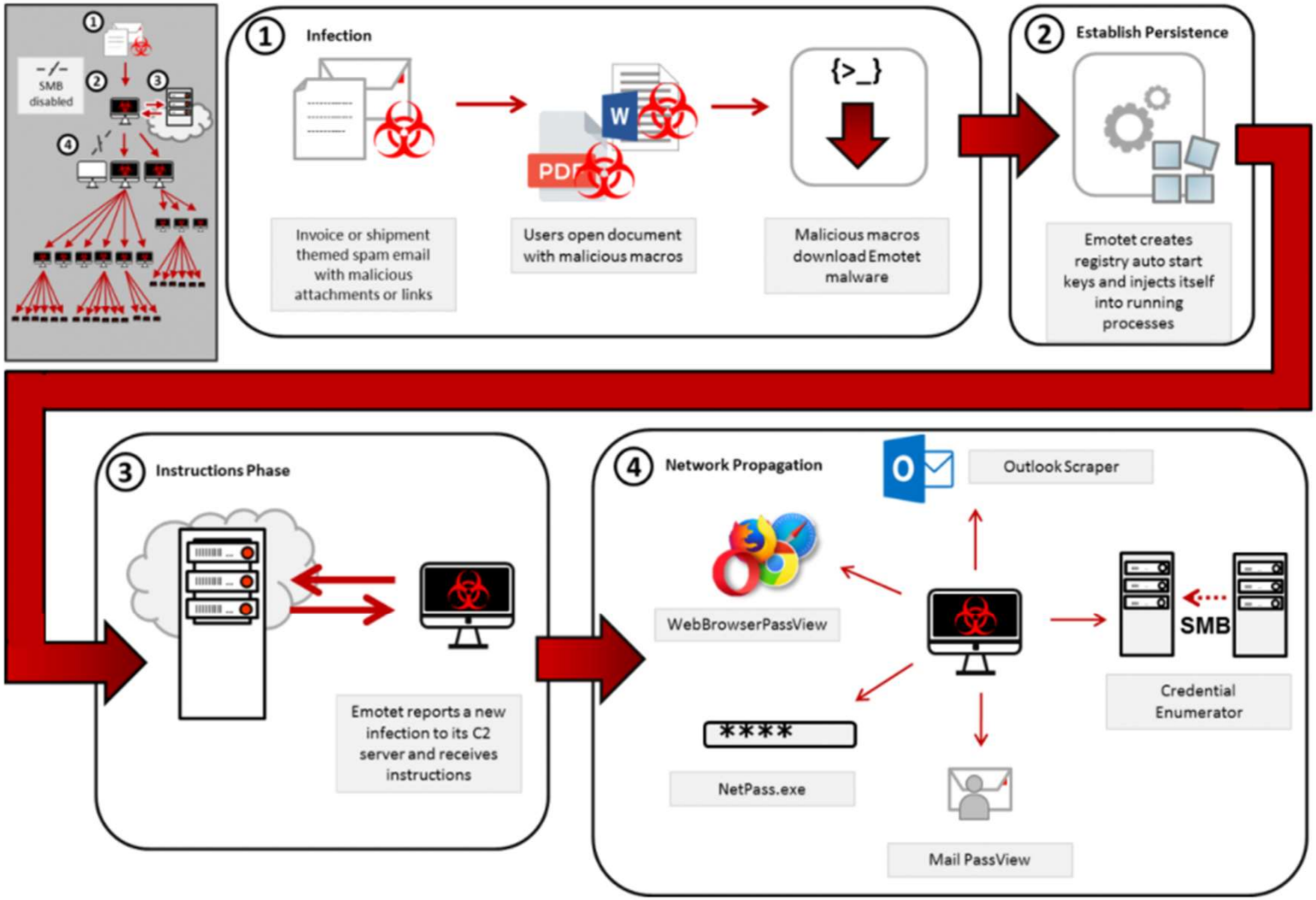
- Emotet是近幾年傳播最廣的惡意軟體之一，最初是以金融類型的木馬出現，但衍化至今，已不限於金融類型
- 功能複雜多樣，感染後可下載多種惡意軟體，如勒索軟體、TrickBot和QakBot，也是Ryuk等駭客組織常用於攻擊的入侵起點
- Emotet主要是垃圾郵件傳播，內含有惡意 Word、Excel 或連結，並結合時事，如氣候環保、Covid-19
- Toyota被勒索攻擊事件，即是從emotet感染開始

Emotet特點

- Wi-Fi spreader，能夠攻擊Wi-Fi網路並傳播
- polymorphic，不斷地改變特徵，可逃避檢測
- 無檔案感染（如Powershell script），感染後的檢測難度升高
- 橫向擴散能力強，例如竊取或破解管理密碼，進行傳播
- Email thread hijacking，從被感染的電腦上竊取電子郵件資訊，偽冒身份回應，使其他人點擊惡意文件、惡意連結

Source: CISA

Emotet攻擊流程示意



Emotet infection chain (*CISA*)

FamousSparrow 攻擊威脅

- TWCERT/CC 接獲國際情資，駭客團體 FamousSparrow 針對包含台 灣、巴西、以色列、加拿大、泰國、英國等 12 個國家之政府、法務機關、飯店、 私有企業及工程領域發起攻擊

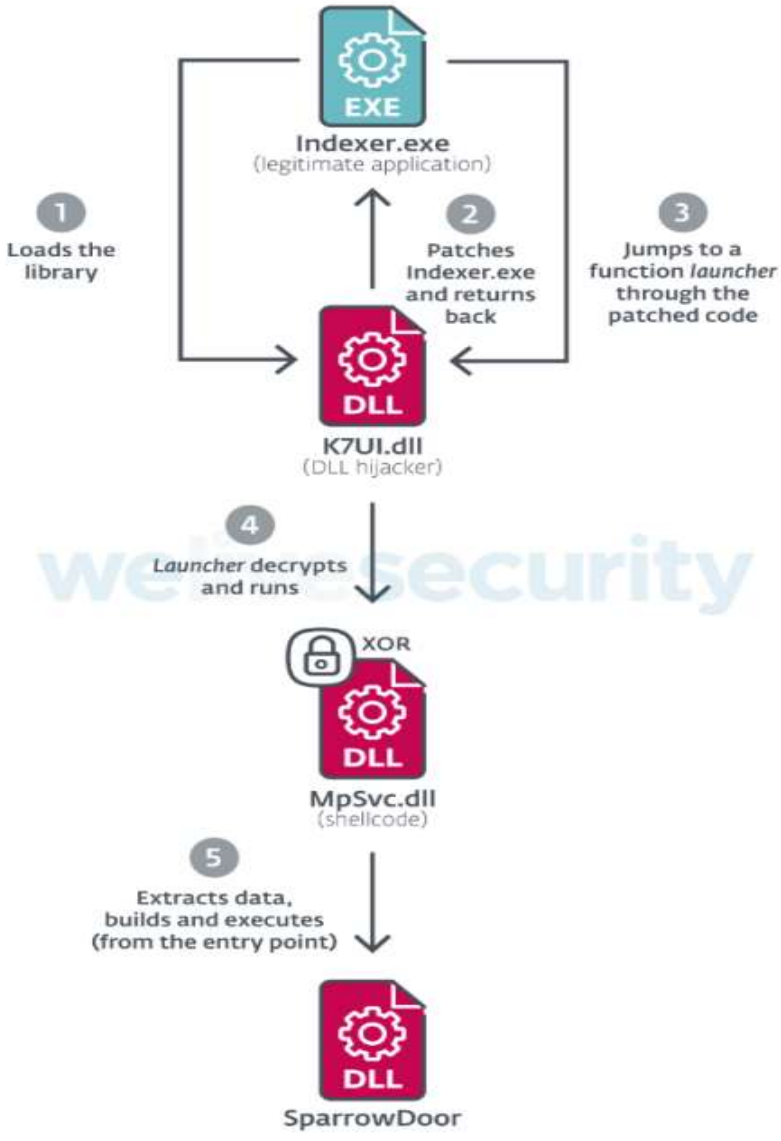
- FamousSparrow 與 DarkHotel、APT28、Rana Group 等駭客組織相似，疑似為情資蒐集為目的，針對飯店訂房系統、通訊領域及航空公司為攻擊對象，進而取得特定對象之行動位置與資訊

FamousSparrow 攻擊手法(1)

- 使用客製化後門程式 ‘SparrowDoor’，並利用包含 SharePoint、Oracle Opera、及 ProxyLogon 等已知遠端任意碼執行漏洞進行攻擊
- FamousSparrow 入侵後會植入以下客製化 工具:
  - Mimikatz 變種，用於破解windows密碼
  - 透過其他工具植入 ProcDump 並用於蒐集 ‘lsass’程序資訊，可用於取 得記憶體的機敏資訊，如身分驗證等資訊
  - Nbtscan，NETBIOS 掃描工具
  - SparrowDoor 後門程式 loader

FamousSparrow 攻擊手法(2)

- SparrowDoor 後門程式為透過以下三個元件植入受害系統
  - Indexer.exe – 正常 K7 computing 執行檔，利用於 DLL hijacking
    - 如果在程序要load一個沒指定絕對路徑的DLL時，Windows會以去尋找這個DLL；攻擊者將惡意的DLL放到這個目錄，惡意DLL就會被程序使用並執行
  - K7UI.dll – 惡意 DLL
  - MpSvc.dll – 已加密腳本，編譯產出與執行後門 PE 檔案



建議防護措施

- 於防火牆部屬規則阻擋與惡意 IP、DN 的連線
- 使用防毒軟體並確保安全控管正常開啟與運行，並及時進行更新
- 檢視系統是否含有 SharePoint、Oracle Opera、Exchange 等或是對外服務與軟 體漏洞，並即時進行安全性更新。如無法進行更新，應避免暴露於網際網路
- 提高安全意識，不隨意開啟可疑連結、來源不明電子郵件、檔案，並於開啟與運行前進行安全掃描，盡可能從可信的來源下載和安裝軟體
- 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

Moriya Rootkit案例 (1)

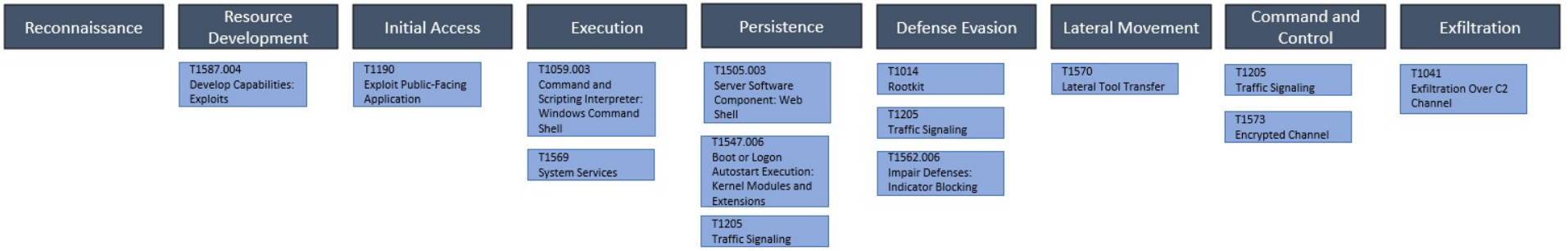
- 中國駭客組織自2019年起，針對非洲、亞洲地區展開 名為“TunnelSnake”駭侵活動，使用新型態後門程式 “Moriya Rootkit”
- Moriya Rootkit具高隱匿性，潛伏於作業系統Kernel層，過濾C2封包，執行指令與回應

Moriya Rootkit 弱點利用與手法

1. 製作特殊PROFIND封包[1587.004]並傳至目標系統觸發漏洞2017-7269 [T1190]
2. 安裝China Chopper後門程式[T1505.003]、Moriya Agent[T1059.003]
3. 、Moriya Driver的Kernel 模組[T1547.006]
4. 由Moriya Driver從Kernel監聽網路封包，將C2封包命令傳遞至Moriya Agent執行，丟棄C2封包以規避遞送至Network Stack被偵測為異常網路流量 [T1562.006]
5. 回傳C2命令執行結果回傳至C2 [T1041]

CVE 漏洞資訊:

CVE 編號	影響版本與型號	影響	CVSS 分數
CVE-2017-7269	Microsoft IIS 6.0	該漏洞主要是 Microsoft IIS(Internet Information Services)6.0 的 WebDAV 服務中，httpext.dll 動態連結函式庫之 ScStorageFromUrl 函式存在緩衝區溢位漏洞，讓遠端攻擊者可透過發送特製的的 PROPFIND 請求封包，導致可執行任意程式碼或造成阻斷服務。	9.8 Critical



Moriya Rootkit 入侵指標

- TunnelSnake駭侵事件除了Moriya Rootkit之外，亦發現有被植入其他惡意程式與工具
- 入侵指標可用於firewall等資安設備，針對性強化防護

名稱	說明
HTTP Scanner	探索目標網絡中的網路伺服器
DCOM Scanner	連結至遠端HOST並嘗試解析所有網路介面之位置
Bouncer	此後門程式可接收特定PORT連線，提供遠端控制與橫向移動
Custom PSExec	此為客製化PSExec工具，可讓攻擊者與目標主機上創建服務
Earthworm	此工具可創建受害主機與攻擊設備之間的通訊通道
Termite	此工具可提供於受害主機上傳檔案等功能
TRAN	此工具可提供主機間的檔案傳輸功能

Hash值
48307C22A930A2215F7601C78240A5EE
A2C4EE84E3A95C8731CA795F53F900D5
5F0F1B0A033587DBCD955EDB1CDC24A4
C1159FE3193E8B5206006B4C9AFBFE62
DA627AFEE096CDE0B680D39BD5081C41
07CF58ABD6CE92D96CFC5ABC5F6CBC9A
9A8F39EBCC580AA56D6DDAF5804EAE61
39C361ABB74F9A338EA42A083E6C7DF8
DE3FB65461EE8A68A3C7D490CDAC296D
EAC0E57A22936D4C777AA121F799FEE6
D745174F5B0EB41D9F764B22A5ECD357
595E43CDF0EDCAA31525D7AAD87B7BE4
9D75B50727A8E732DB0ADE7E270A7395
3A4E1F3F7E1BAAB8B02F3A8EE20F98C9
47F2D06713DAD556F535E523B777C682
45A5D9053BC90ED657FA90DE0B775E8F

Moriya Rootkit 建議措施

- 確認對外服務伺服器無存在CVE-2017-7269之漏洞
- 對外服務伺服器應定期進行安全性更新
- 部屬防毒軟體，並定期更新病毒碼以即時偵測與隔離可疑檔案
- 實施網路分段區隔並監控流量

勒索軟體

勒索軟體攻擊

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 iThome鐵人賽 搜

打破框架，淬鍊精華

數位轉型攻略系列III：IT 即戰力　租虛擬主機架站，再附信箱　14.2%企業願意聘用大資料人才

新聞

去年美國當地學校受到77次的勒索軟體攻擊，光是停機成本就損失66億美元

過去勒索軟體駭客並不特別青睞教育單位，相關攻擊案件在2018年只有10件，但2019年就激增到96件，2020年也有77件，同時駭客也愈趨鎖定大型學校為目標

文/ 陳曉莉 | 2021-09-01 發表

讚 6.6 萬 按讚加入iThome粉絲團 讚 98 分享

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 iThome鐵人賽 搜

新聞

駭客公布50萬組Fortinet VPN用戶帳號與密碼，74個國家受影響，臺灣第二嚴重

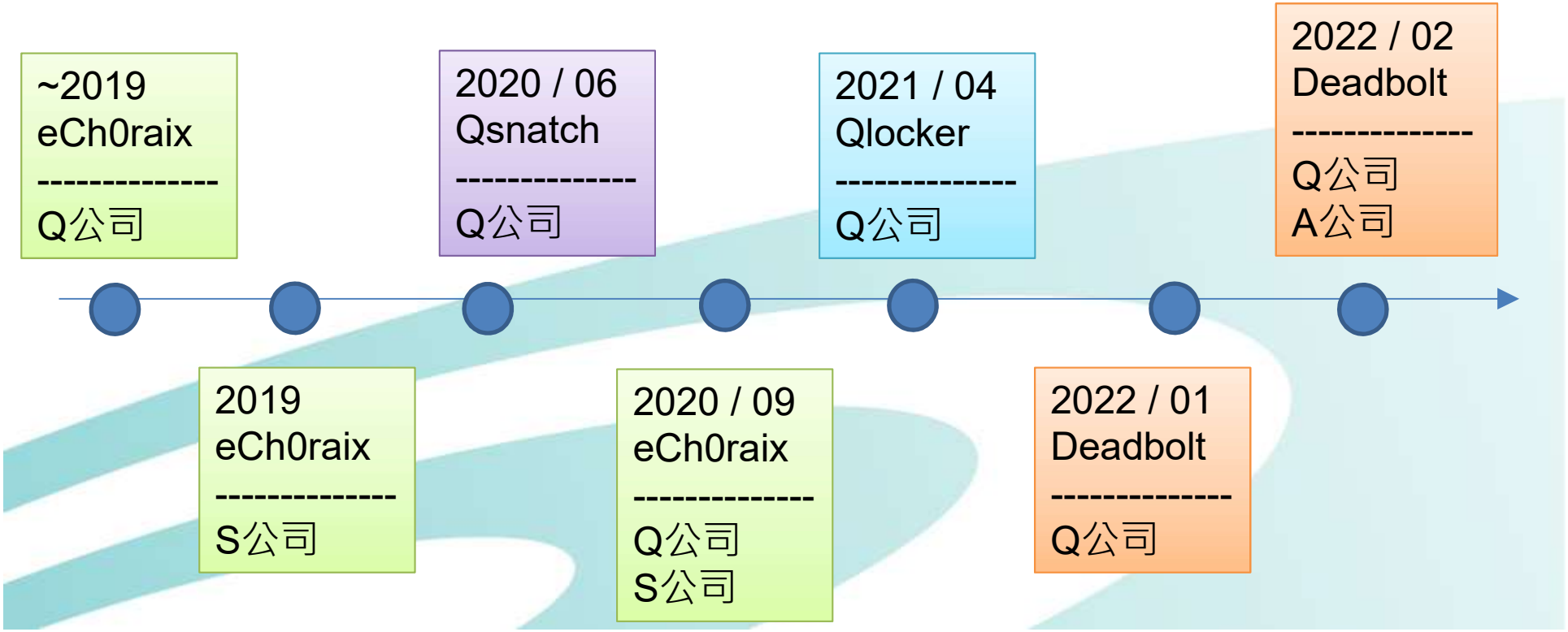
Fortinet早在2019年便提供修補的CVE-2018-13379漏洞，現在傳出被駭客濫用導致大批FortiGate SSL-VPN裝置的存取帳號與密碼外洩，而且官方也提醒，就算是已完成修補的用戶仍不可輕忽，事後仍需重設所有的密碼，並啟用雙因素認證，修補才算圓滿

文/ 陳曉莉 | 2021-09-09 發表

讚 6.6 萬 按讚加入iThome粉絲團 讚 783 分享

勒索軟體威脅NAS安全日益嚴重

- NAS因其設備用途，做為儲存與共用資料的重要企業服務，成為資安攻擊目標，並針對性的開發勒索軟體
- 入侵途徑：漏洞、外網曝露、安全設定錯誤(帳密過於簡單)



攜手公私部門，力抗跨國殭屍網路

Deadbolt勒索軟體

- 入侵途徑
  - 攻擊暴露於外網的 NAS，劫持 NAS 登入畫面
  - 不恰當的安全設定，“The System Administration service can be directly accessible from an external IP address via the following protocols: HTTP”
- 安全建議
  - 關閉 Port Forwarding ，關閉NAS 系統管理的8080、443
  - 關閉 QNAP NAS 的 UPnP，ASUSTOR的SSH、SFTP 功能
  - 更改ASUSTOR遠端Web存取預設port
- 解密工具：服務不完整的解密機制
- TWCERT/CC協處
  - 自2022年1月以來陸續接獲通報，QNAP與ASUSTOR NAS設備遭勒索軟體入侵，提供諮詢服務
  - TWCERT/CC協助將使用者通報內容提供廠商分析，並協助將廠商修補資訊通報國外、分享於官網、社群媒體

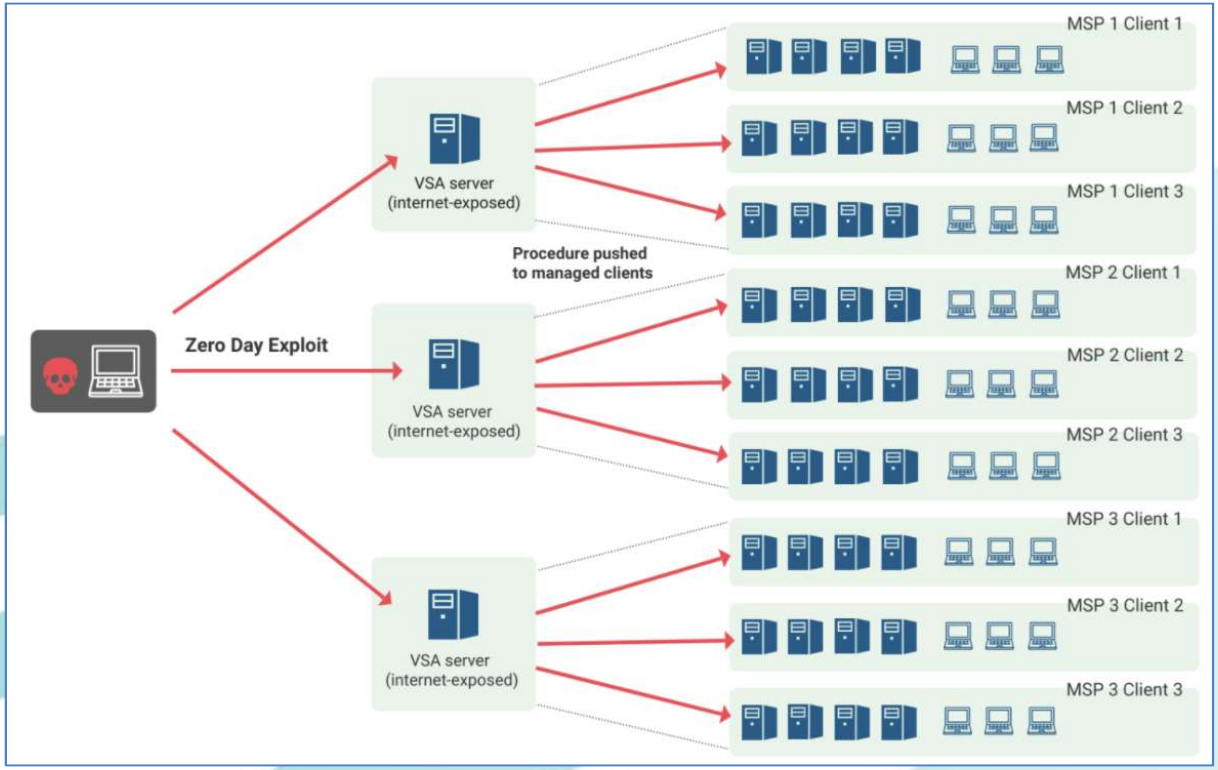
- Discovery
- T1018 Remote system discovery
- Initial Access
- T1133 External Remote Services
- T1190 Exploit Public-Facing Application
- Credential Access
- T1110.001 Brute Force: Password Guessing
- Impact
- 1486 Data encrypted for impact
- 1489 Service stop

REvil 產業鏈攻擊與勒索攻擊 (1)

- REvil自2019年起針對電信、金融及製造業等20個領域發起攻擊，甚至鎖定Vmware ESXi伺服器及釋出用來加密NAS裝置的Linux版加密工具
- 美國託管軟體開發業者Kaseya駭客入侵
- 全球11國傳出災情，60家VAS客戶遭到波及，導致1,500家下游廠商受到影響，REvil駭客則聲稱已加密數百萬個系統並要求高達7,000萬美元之贖金以提供解密工具
- REvil 7月13日消失匿跡、但於近日(9月)重現蹤影，VT亦收到新REvil惡意程式樣本

REvil 產業鏈攻擊與勒索攻擊 (2)

- Kaseya事件為透過CVE-2021-30116之身分驗證資訊接露之嚴重漏洞入侵VAS伺服器，並透過雲端服務提供者自動散播勒索軟體



REvil 產業鏈攻擊與勒索攻擊 (3)

1. 觸發Kaseya VAS伺服器之漏洞 (CVE-2021-30116, 當時為0-day漏洞)
2. 植入包含Microsoft Defender舊版執行檔與加密使用的dll之壓縮檔 'agent.crt'至hotfix路徑下，後續自動推播至MSP用戶端
3. 透過Powershell命令關閉設備防護與偵測機制
4. 將Microsoft Defender舊版執行檔置換設備上原有之執行檔，並於運行後載入加密使用之dll至記憶體中 (DLL side-load攻擊)
5. 加密檔案並植入勒索訊息

REvil 產業鏈攻擊與勒索攻擊 (4)

- ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Impact
T1190 Exploit Public-Facing Application	T1059.001 Command and Scripting Interpreter: Powershell	T1574.002 Hijack Execution Flow: DLL Side-Loading	T1574.002 Hijack Execution Flow: DLL Side-Loading	T1562.001 Impair Defenses: Disable or Modify Tools	T1049 System Network Connections Discovery	T1486 Data Encrypted for Impact
				T1140 Deobfuscate/Decode Files or Information		
				T1070.004 Indicator Removal on Host: File Deletion		
				T1574.002 Hijack Execution Flow: DLL Side-Loading		

REvil 產業鏈攻擊與勒索攻擊-小結(5)

- REvil 為近年最有名之勒索駭客團體，採取RaaS經營模式，雖隱匿一段時間，但近日重現，並出現新型態勒索惡意程式
- 建議措施
  - 對外設備之軟硬體應定期更新至最新版本以及時修補漏洞
  - 加密所有內部機敏資訊
  - 定期進行檔案備份
  - 評估採用高權限控管架構 (PAM)

Lockbit 2.0 勒索軟體 (1)

- Lockbit 勒索軟體為一種勒索軟體既服務 (RaaS)，原為ABCD病毒
- 2021年6月推出2.0強化版，可透過Windows Server群組原則自動加密整個網域下設備
- 全球已有多國遭受勒索攻擊影響

表一、LockBIT 2.0 功能與特性

Tor 中的管理員面板
解密工具功能的自動測試
阻止可能破壞加密過程的進程啟動
進階的通訊埠端口掃描
自動清除受感染網路中的日誌
通過 Wake-on-Lan 自動啟動電腦
能使用在受害網路中連接的印表機印出需要的文件
在受害網路中的自動散播
刪除可用於備份還原的影子備份

Lockbit 2.0 勒索軟體 (2)

- Lockbit 2.0也納入 “StealBIT”模組，聲稱擁有世界上最快資料加密與竊取速度

- 加密100G資料僅需4分半
- 上傳100G資料僅需20分鐘

PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130	110468
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156	109700

Comparative table of the information download speed of the attacked company

Testing was made on the computer with a speed of Internet of 1 gigabit per second

Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode	drag'n'drop	Time spent for downloading of 10 GB	Time spent for downloading of 100 GB	Time spent for downloading of 10 TB
Stealer - StealBIT	83,46 MB/s	Yes	Yes	Yes	1M 59S	19M 58S	1D 9H 16M 57S
Rclone pcloud.com free	4,82 MB/s	No	No	No	34M 34S	5H 45M 46S	24D 18M 8S
Rclone pcloud.com premium	4,38 MB/s	No	No	No	38M 3S	6H 20M 31S	26D 10H 11M 45S
Rclone mail.ru free	3,56 MB/s	No	No	No	46M 48S	7H 48M 9S	32D 12H 16M 28S
Rclone mega.nz free	2,01 MB/s	No	No	No	1H 22M 55S	13H 48M 11S	57D 13H 58M 44s
Rclone mega.nz PRO	1,01 MB/s	No	No	No	2H 45M	1D 03H 30M 9S	114D 14H 16M 30S

Lockbit 2.0 勒索軟體 (3)

- 入侵途徑
  - LockBIT 2.0通常利用暴露於網路設備、軟體漏洞進行攻擊，近期澳洲的勒索事件為利用Fortinet FortiOS及FortiProxy產品漏洞入侵受害組織。

表 2、CVE-2018-13379 漏洞說明與建議措施

CVE 編號與影響	影響設備與版本	建議措施	CVSS 分數
CVE-2018-13379	啟用 web-mode 或 tunnel-mode 的 Fortinet Forti OS 6.0~6.0.4，5.6.3~5.6.7，5.4.6~5.4.12、FortiProxy 2.0.0, 1.2.0~1.2.8, 1.1.0~1.1.6, 1.0.0~1.0.7	1. 升級設備韌體至最新版本 2. 無法升級韌體時的暫時排除方式為關閉 SSLVPN 3. 如無法升級韌體且無法關閉 SSLVPN 者，應使用雙因子身分認證組防止駭客利用此弱點	9.8 (嚴重)

Lockbit 2.0 勒索軟體 – 小結 (3)

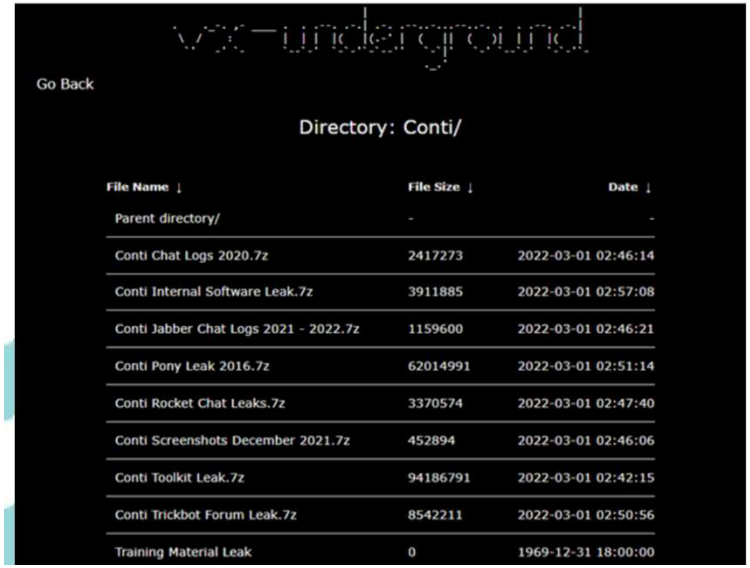
- LockBIT 2.0含有強大的攻擊能力與特性，包含自動透過Windows群組原則感染其他設備以及快速的加密與上傳能力
- 盡速更新前述之Fortinet FortiOS及FortiProxy漏洞的安全性更新
- 對外設備之軟硬體應定期更新至最新版本以及時修補漏洞
- 關閉非必要的服務如135、139、445、3389等高風險port
- 定期進行檔案備份

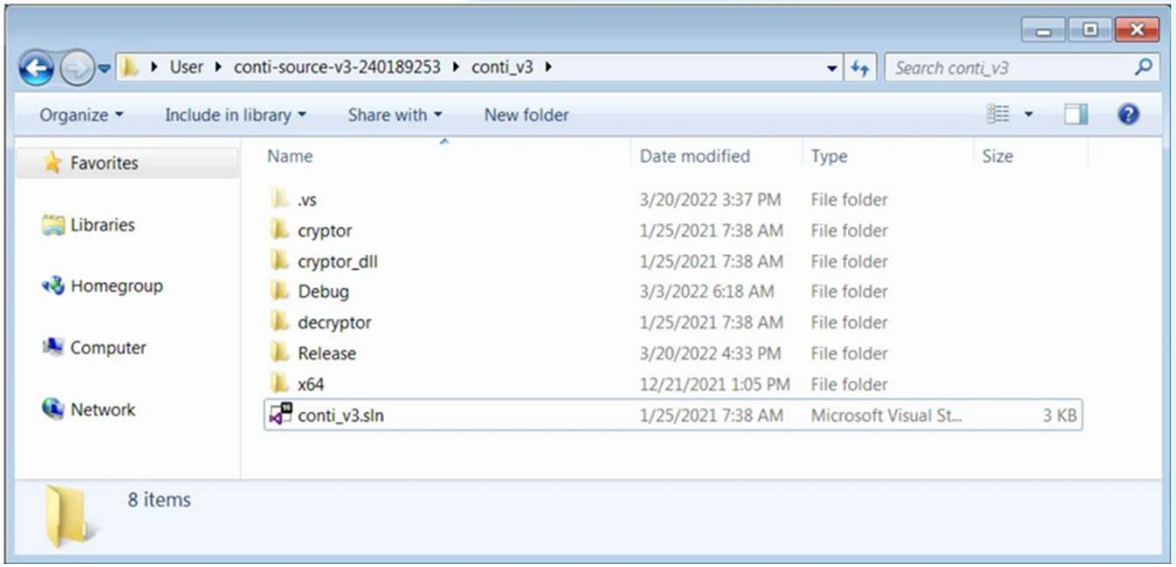
勒索軟體Conti介紹

- 最早於2019年首次發現的Conti勒索軟體類型，是目前主流的 Ryuk 勒索軟體家族的最新變種型態
- 勒索軟體即服務（ransomware-as-a-service）的模式
- 透過TrickBot、BazarLoader等後門程式散布，針對大型企業、政府機關，且是2021年ICS環境最嚴重的勒索軟體
- CISA於2021年9月首次針對Conti發出警告，於今年3月再度更新警告
- 資安廠商NordLocker 的研究報告指出[8]，統計該公司所處理之2020-2021的勒索攻擊，前十大勒索軟體第一就是Conti，有 450 起案例
- 國內則於2020、2021年皆有知名大廠遭到Conti攻擊

Conti資料外洩事件

- 俄羅斯與烏克蘭的戰爭，Conti勒索團體官方宣布支持俄羅斯，導致Conti成員產生分歧
- 烏克蘭陣營的Conti成員在twitter公布內部資料，包含勒索教學、入侵工具、C2 IP等，總共洩漏近170,000 條內部聊天對話、原始碼等資料
- 這樣的洩漏可以讓資安研究人員研究更多針對性防禦措施，但可能因此催生出新的勒索軟體，如同Hidden Tear的洩漏造成Pandora等勒索軟體使用相關原始程式





Conti攻擊流程


Conti attack chain
Conti 攻擊流程
透過包含google文件連結的釣魚信件、帳號濫用、對外開放的服務和已知漏洞等方式取得初始訪問
其中含惡意連結會指向BazarBackdoor loader，取得BazarBackdoor
執行遠端系統掃描，攻擊 Active Directory
Adfind
NetScan
ShareFinder
使用Windows Command Shell或應用程式API進入網路，並利用Web Shell持續訪問服務
使用Cobalt Strike操作BazarBackdoor
執行遠端系統掃描
權限提升
Mimikatz
防禦迴避
PCHunter
獲取憑證
PowerShell Empire: Kerberoast
MITRE ATT&CK
TA0001 Initial Access
T1078 Valid Accounts
T1190 Exploit Public-Facing Application
T1566 Phishing
TA0007 Discovery
T1018 Remote system discovery
T1033 System owner/user discovery
T1057 Process discovery
T1083 File and directory discovery
T1082 System information discovery
TA0002 Execution、TA0003 Persistenc
T1059.003 Command and Scripting Interpreter: Windows Command Shell
T1106 Native API
T1505.003 Server Software Component: Web Shell
TA0004 Privilege Escalation
T1078.002 - Valid accounts: domain accounts
TA0005 Defense Evasion
T1055.001 Process Injection: Dynamic-link Library Injection
T1140 Deobfuscate/Decode files or information
TA0006 Credential Access
T1552 Unsecured credentials
T1555 Credentials from password stores
經由SMB橫向擴散尋找目標
AnyDesk
連結C2 server
Cobalt Strike
使用Rclone、WinSCP等工具將數據外洩到Mega等雲端儲存空間
Conti 勒索軟體加密資料
加密資料，並使用WMI阻止系統回復
TA0008 Lateral Movement
T1021.002 Remote services: SMB/Windows admin sha
T1080 Taint Shared Content
T1570 Lateral tool transfer
TA0011 Command and Control
T1071 Application Layer Protocol
T1219 Remote access software
TA0010 Exfiltration
T1567.002 Exfiltration over web service: exfiltration to cloud storage
TA0040 Impact
T1486 Data encrypted for impact
T1489 Service stop
T1490 Inhibit system recovery

Conti相關漏洞與工具

MITRE ATT&CK TA0007 - Discovery

- ADfind.exe：一種命令行工具，用於查詢 Active Directory 並收集有關網絡中的用戶、網絡和系統的信息 。
- BloodHound：提供可能的攻擊路徑的 Active Directory 工具 。
- Invoke-Kerberoast： MITRE ATT&CK T1558.003 竊取或偽造 Kerberos 票證的 PowerShell 腳本：Kerberoasting 。
- NtdsAudit：審計 Active Directory 數據庫的工具。
- PowerTools：用於網絡發現和權限提升的攻擊性 PowerShell 腳本集合。
- ShareFinder： PowerTools 中的一個 PowerShell 腳本，用於搜索和列出共享文件。
- Rubeus：用於原始 Kerberos 交互和濫用的開源工具集 。
- SharpView： PowerView 的 .NET 端口，一個用於 AD 的 PowerShell 腳本
- WinPwn：用於 Windows 自動滲透測試的 PowerShell 腳本。

MITRE ATT&CK TA0004 - Privilege Escalation

- dazzleUP：權限提升漏洞掃描器。
- PEASS-ng：多平台提權框架。
- Watson：用於列出權限提升漏洞的缺失更新掃描器。

MITRE ATT&CK TA0006 - Credential Access

- Invoke-SMBAutoBrute：用於強制獲取憑據的 PowerShell 腳本。
- Net-GPPPassword：明文憑證和數據收集器。
- SharpChromium：用於收集 cookie、歷史記錄和登錄憑據的 Google Chrome 和 Microsoft Edge 的數據提取工具。

MITRE ATT&CK TA0011 - Command and Control

- Anydesk：用於遠端桌面控制。
- Atera：一種遠端監控軟體(RMM)，用收集用戶資訊。
- GOST (GO Simple Tunnel)：以GO語言實現的安全通道，可以設置port監聽和代理轉發。

MITRE ATT&CK TA0010 - Exfiltration

- Filezilla：使用 FTP 服務進行數據洩露的工具 。
- Mega：一種被濫用於數據洩露的雲存儲服務 。
- rclone：使用雲存儲服務進行數據洩露的命令行工具。

編號	CVE編號	編號	CVE編號
1	CVE-2015-2546	18	CVE-2019-1405
2	CVE-2016-3309	19	CVE-2019-1458
3	CVE-2017-0101	20	CVE-2020-0609
4	CVE-2017-0199	21	CVE-2020-0638
5	CVE-2018-8120	22	CVE-2020-0688
6	CVE-2019-0543	23	CVE-2020-0787
7	CVE-2019-0708	24	CVE-2020-0796
8	CVE-2019-0841	25	CVE-2020-1472
9	CVE-2019-1064	26	CVE-2020-5135
10	CVE-2019-1069	27	CVE-2021-1675
11	CVE-2019-1129	28	CVE-2021-1732
12	CVE-2019-1130	29	CVE-2021-21985
13	CVE-2019-1215	30	CVE-2021-22005
14	CVE-2019-1253	31	CVE-2021-26855
15	CVE-2019-1315	32	CVE-2021-34527
16	CVE-2019-1385	33	CVE-2021-44847
17	CVE-2019-1388		

*根據Conti外洩資訊整理

Conti防護建議

Common attack techniques	Defenses
釣魚信件安裝後門 • 透過不安全釣魚信件進行安裝後門 **獲得初始訪問權限** • 帳號被盜用 • 透過Trickbot、BazarBackdoor訪問系統 **弱點遭利用** • 對外開放存取程式存在漏洞，可以被加以利用 • 例如: 利用Log4j的Powershell、Proxyshell等已知漏洞進行攻擊 **橫向擴大攻擊範圍** • 對網路進行滲透掃描 • 使用Cobalt Strike和C2 server進行連線控制 • 尋找安全層級較弱的主機進行攻擊 **勒索軟體執行加密** • 透過AnyDesk等工具將機敏資料傳送到外部 • 機敏檔案被加密	**資安意識** ✓ 提高安全意識，不隨意開啟可疑連結、來源不明電子郵件、檔案。 **存取控制** ✓ 針對外部來源的使用者，使用多重身份驗證。 ✓ 實施網絡分段和過濾流量，減少勒索軟體傳播的可能。 **系統更新** ✓ 使用專業的防毒軟體並確保安全控管正常開啟與運行，並及時進行更新。 ✓ 定期對軟體和應用程式進行漏洞評估，並進行修補和更新。 **網路監控** ✓ 調查任何未經授權的應用程式，尤其是遠程桌面或遠程監控的管理程式。 **資料保全** ✓ 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

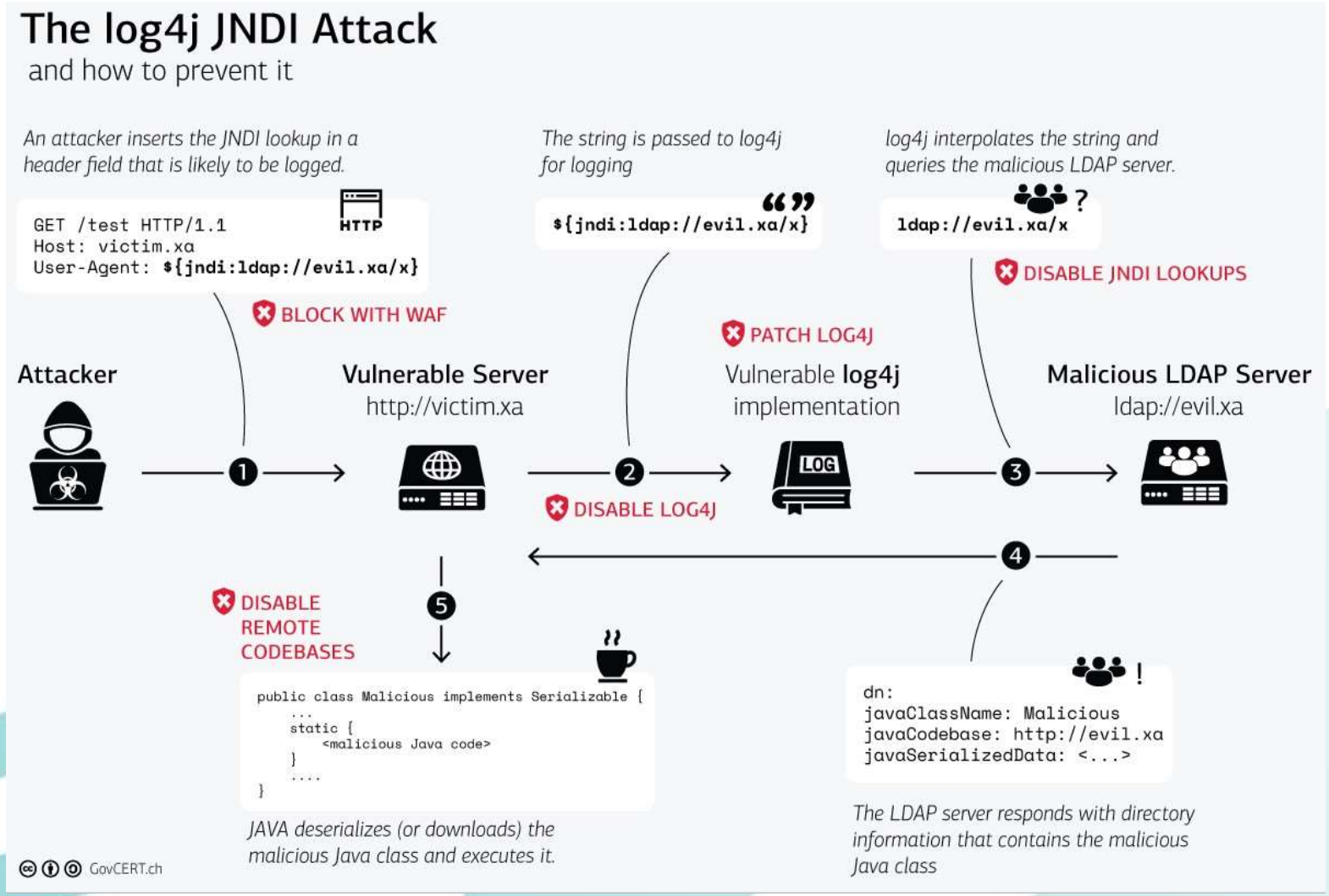
漏洞更新相關事項

- 各資安單位、新聞常會提醒重大漏洞需進行更新，公司常因各種狀況而難以更新
  - 服務無法立即停止、系統老舊、無外包維護、難以確保更新後服務正常運行
- 漏洞仍是建議第一時間完成更新，但若有困難，應進行更新評估作業，
- 解讀漏洞
  - CVSS :
    - Base Score : 7.2 HIGH
    - Vector : CVSS:3.1/**AV:N**/AC:L/**PR:H**/UI:N/S:U/**C:H/I:H/A:H**
- 範例
  - **CVE-2021-38639和CVE-2021-36975**皆屬於本地端執行的漏洞，雖然在CVSS評分上會比遠端執行低，但因其影響大部份的Windows版本
  - 難以更新時，可考量其本地端發動攻擊特性，進而考量該漏洞主機位置，評估對應作法

以log4j漏洞防護為例

- 2021年12月發現了log4j漏洞，因其套件被廣泛使用，影響巨大受到高度重視，且立即被利用進行攻擊
- 編號為CVE-2021-44228，CVSS為critical最高10分，不需權限、遠端發動、攻擊方式簡單，可操控系統、取得資料，還可再影響其它服務
- log4j使用JNDI(Java Naming and Directory Interface)的API介面連結資料庫，而JNDI介接多種資源，包括LDAP(Lightweight Directory Access Protocol)服務
  - LDAP用於將資料做結構性整合，例如企業內的姓名、電話、電子郵件的目錄等，另一個常見用途是做單一登入(single sign on)的主要模組
- 漏洞問題是log4j允許任意的JNDI與LDAP的請求，且未加以檢查，當攻擊者將惡意網址放入JNDI的查詢字串中，log4j會將網址內含的程式碼下載並執行，且可攻擊到相關的其它服務

Log4j緩解與防護措施



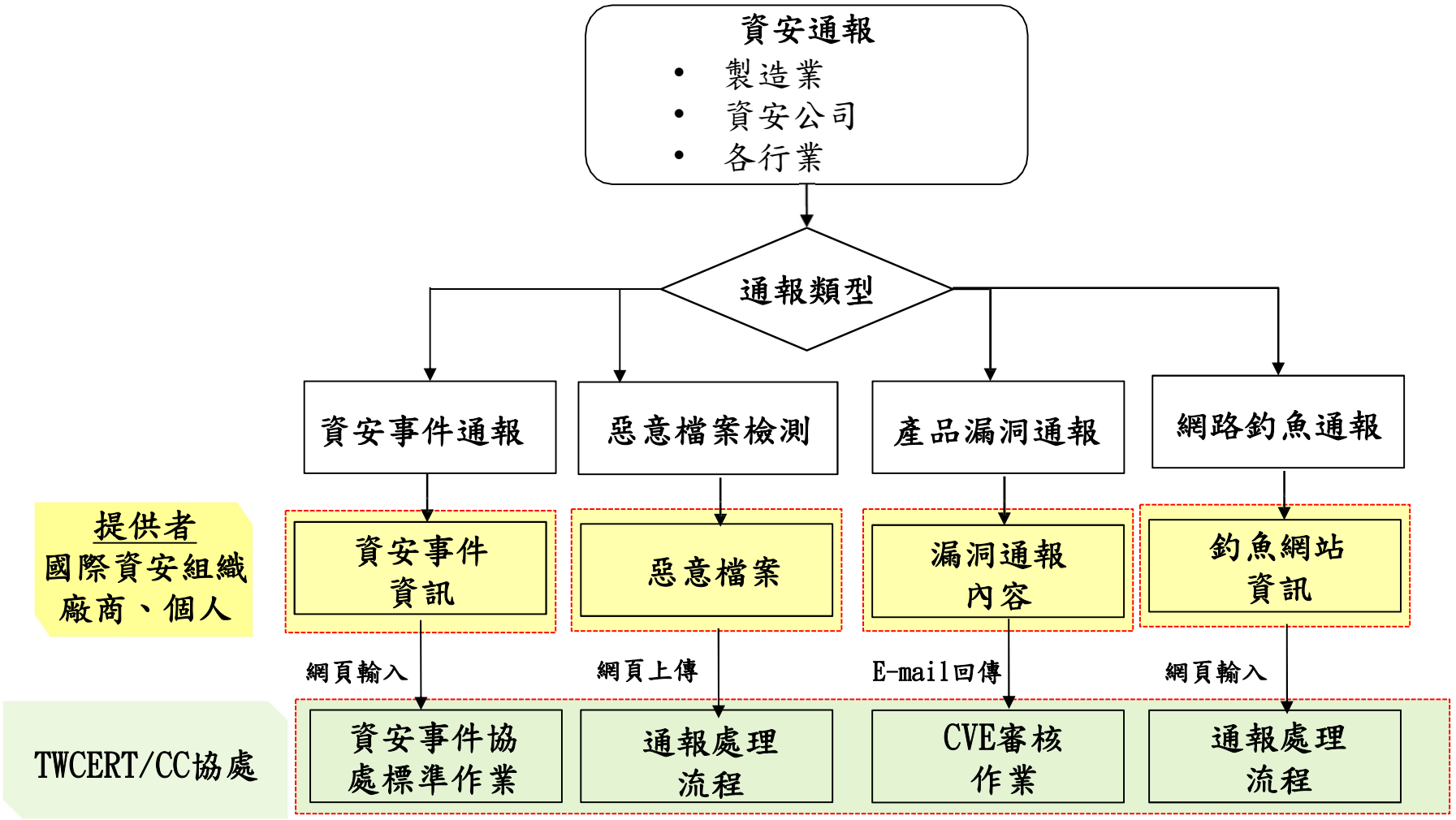
Source : Swiss CERT

Log4j漏洞更新狀況仍不理想

- iThome 5/8的文章，資安廠商Rezilion發現網際網路仍有9萬多個應用程式仍包含舊版Log4j
- Google服務Open Source Insights，在4月20日的調查結果中，存在Log4j漏洞的套件有17,840個，其中已經修補的只有7,140個，近60%還曝險
- Sonatype公布的Log4j下載追蹤資料，自去年12月10日以來，Log4j被下載超過4500萬次，有39%下載舊版本。以4月20日來看，過去24小時內從Maven Central套件庫下載Log4j版本將近41.3萬次，其中有36%仍然存在Log4Shell漏洞
- 未修補原因
  - 難以確認所開源軟體中的元件清單與版本
  - 老舊專屬軟體

資安事件通報應變

資安通報架構


資安通報
製造業
資安公司
各行業
通報類型
資安事件通報
惡意檔案檢測
產品漏洞通報
網路釣魚通報
提供者
國際資安組織
廠商、個人
資安事件
資訊
惡意檔案
漏洞通報
內容
釣魚網站
資訊
網頁輸入
網頁上傳
E-mail回傳
網頁輸入
TWCERT/CC協處
資安事件協
處標準作業
通報處理
流程
CVE審核
作業
通報處理
流程

資安服務概要

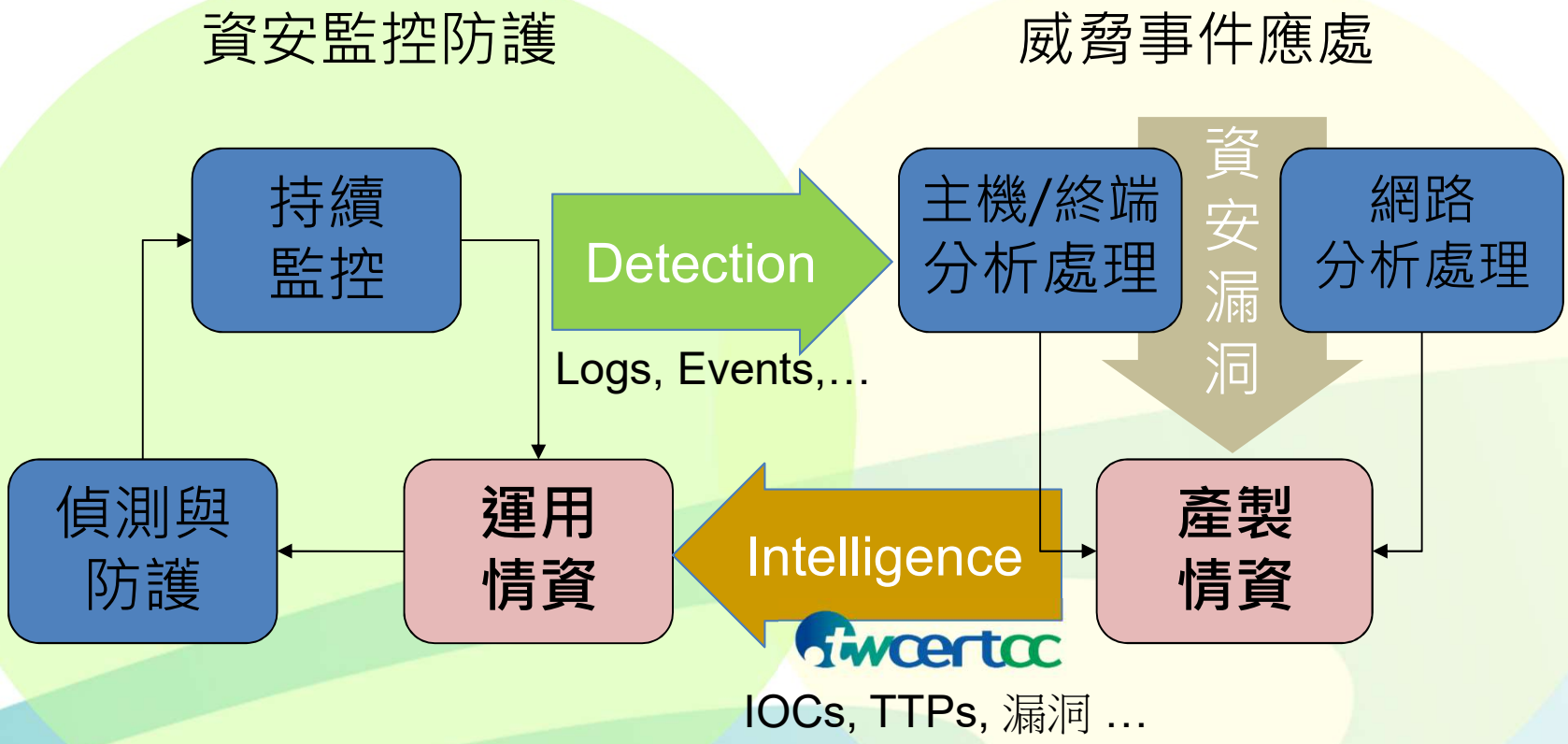
- **資安跨域聯防與情資分享**
  - 資訊去識別化 (Anonymization)
  - 遵守情資交換協定 (Traffic Light Protocol, TLP)，確保妥適運用
- **釣魚網站協處**
  - 跨境協處偽冒企業網站之釣魚網站
  - phishingcheck.tw
- **惡意檔案檢測**
  - 檢測可疑檔案，避免機敏檔案外洩
  - 整合靜態檢測與沙箱(Sandbox)之動態分析機制，檢知潛藏惡意程式
  - viruscheck.tw

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

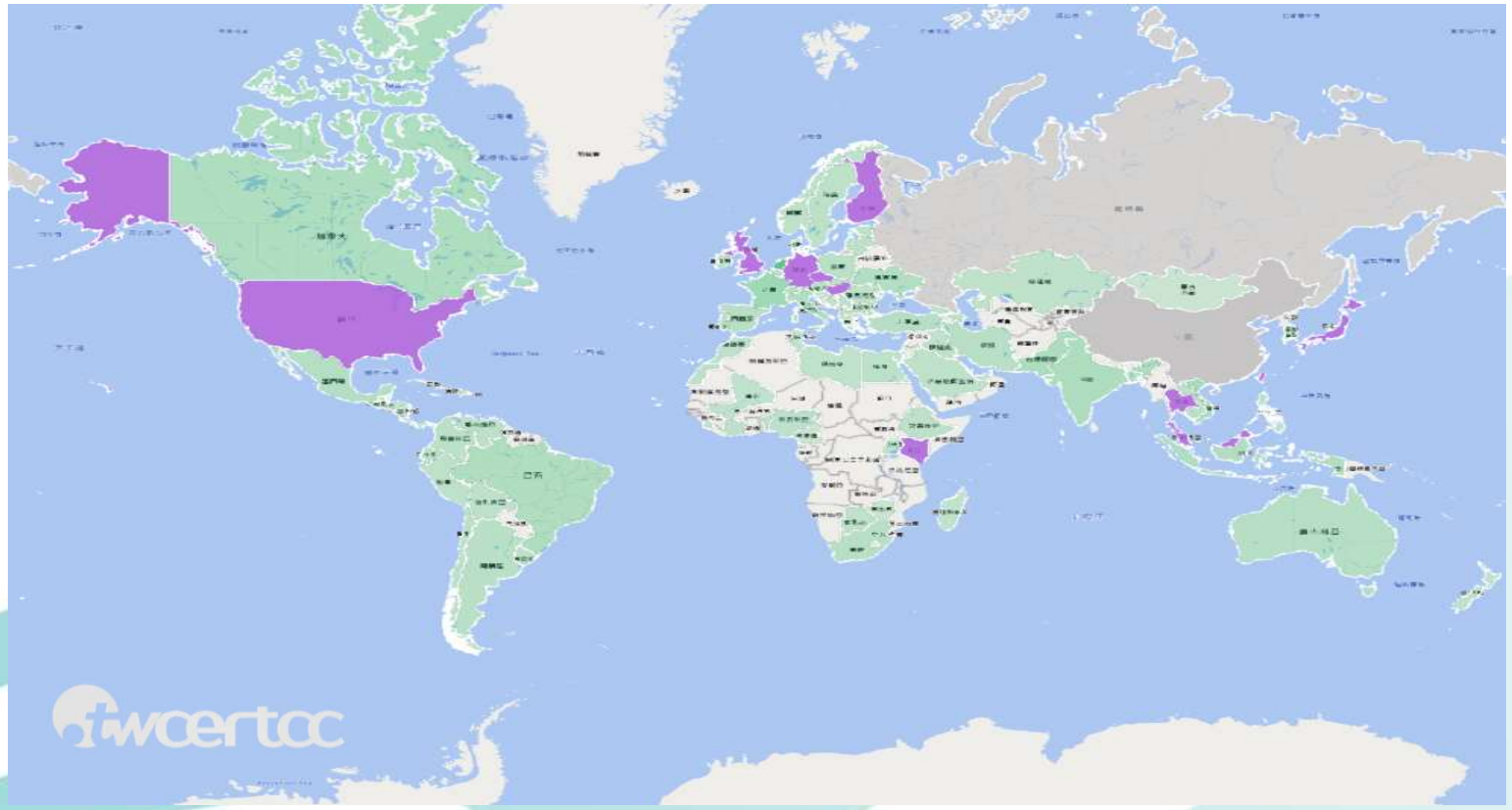
資安跨域聯防與情資分享

資安監控防護 vs. 威脅事件應處

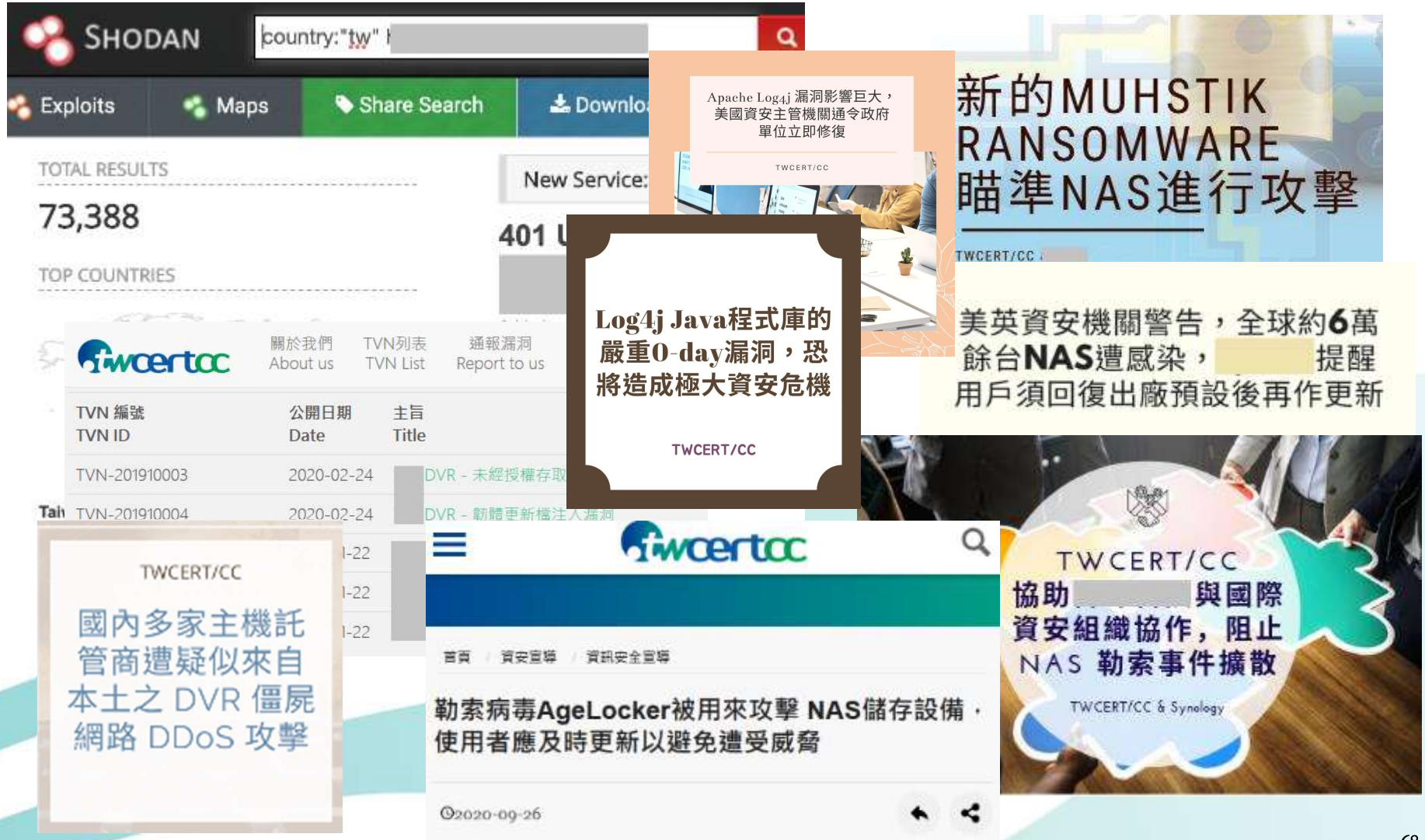


資安情資處理概況

- 2020年累計處理超過150萬筆資安情資
- 對境外分享百餘國，近20國作雙向情資分享

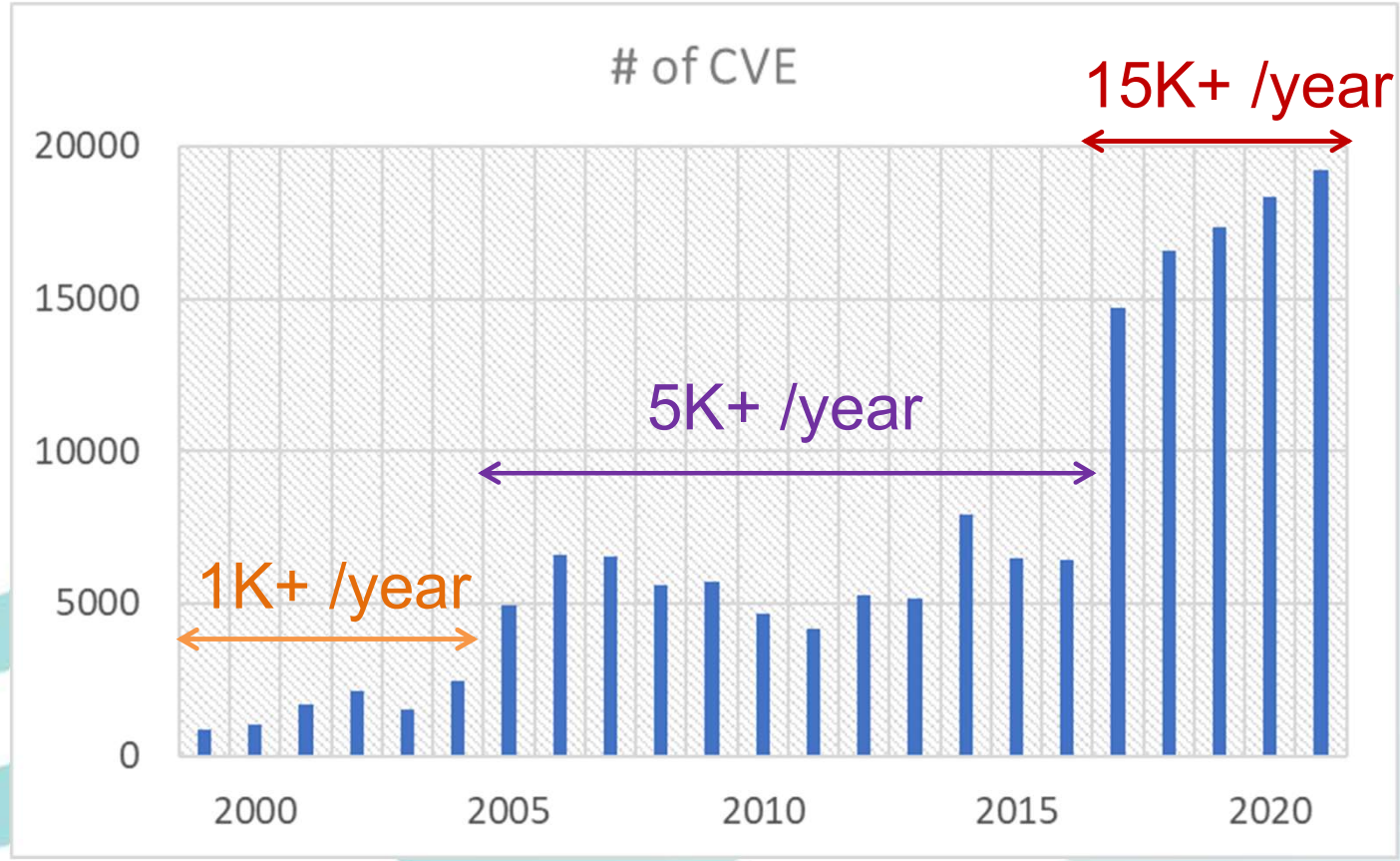


產品漏洞遭利用發動資安攻擊



資安漏洞急遽增加

- 2021年已揭露超過1.9萬個 CVE 資安漏洞
- FIRST指出，多數單位1個月僅能修復5%~20%已知漏洞

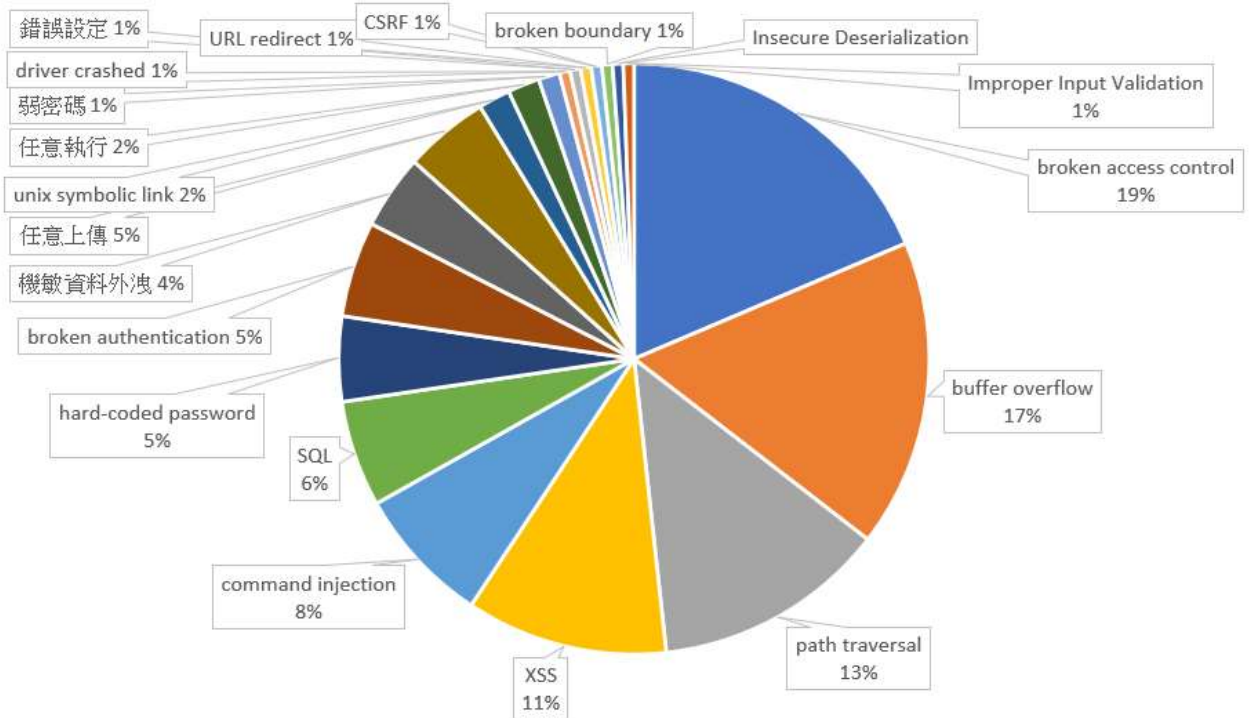


Source: CVE Details

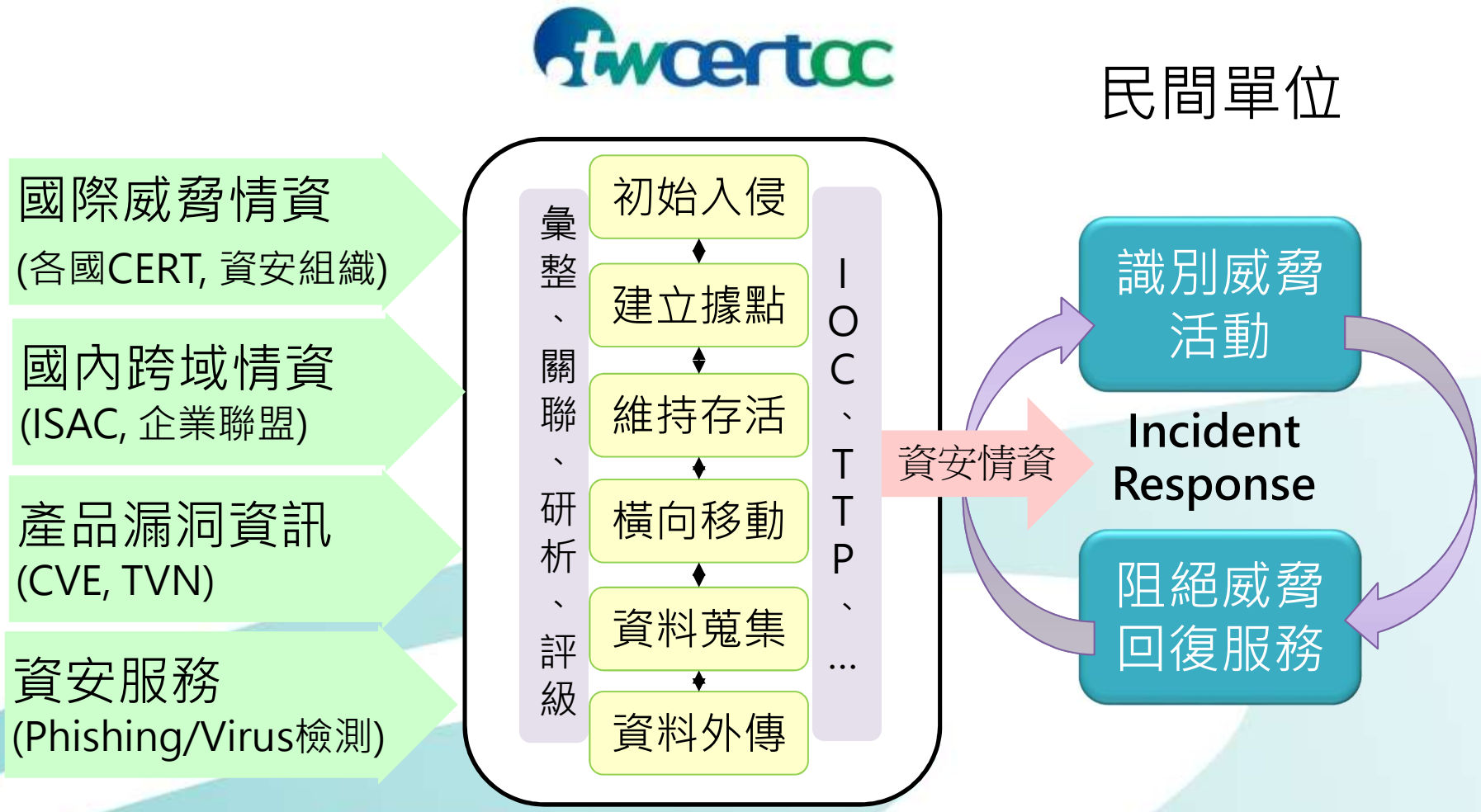
CVE漏洞處理概況

- TWCERT/CC 已審核並發布超過200個CVE漏洞編號
- 2021年已審核並發布167個CVE
  - 產品類型：軟體平台-78、IOT裝置-54、資訊主機-35
  - 嚴重程度：Critical-42、High-40、Medium-83
  - 威脅類型：Broken access control、buffer overflow、Path traversal

- 當新的CVE漏洞發布時，TWCERT/CC同步公告漏洞預警資訊並通知ISAC、企業聯盟等，以預先進行相關防範



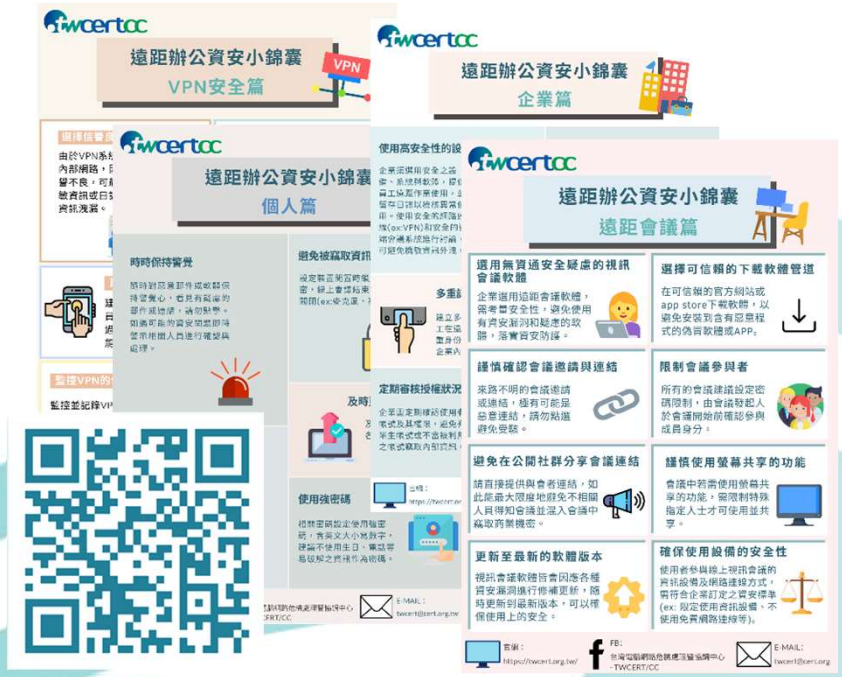
運用情資強化威脅應處


國際威脅情資
(各國CERT, 資安組織)
國內跨域情資
(ISAC, 企業聯盟)
產品漏洞資訊
(CVE, TVN)
資安服務
(Phishing/Virus檢測)
彙整、關聯、研析、評級
初始入侵
建立據點
維持存活
橫向移動
資料蒐集
資料外傳
IOC、TTP、…
資安情資
民間單位
識別威脅活動
Incident Response
阻絕威脅回復服務

資安防護專區

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

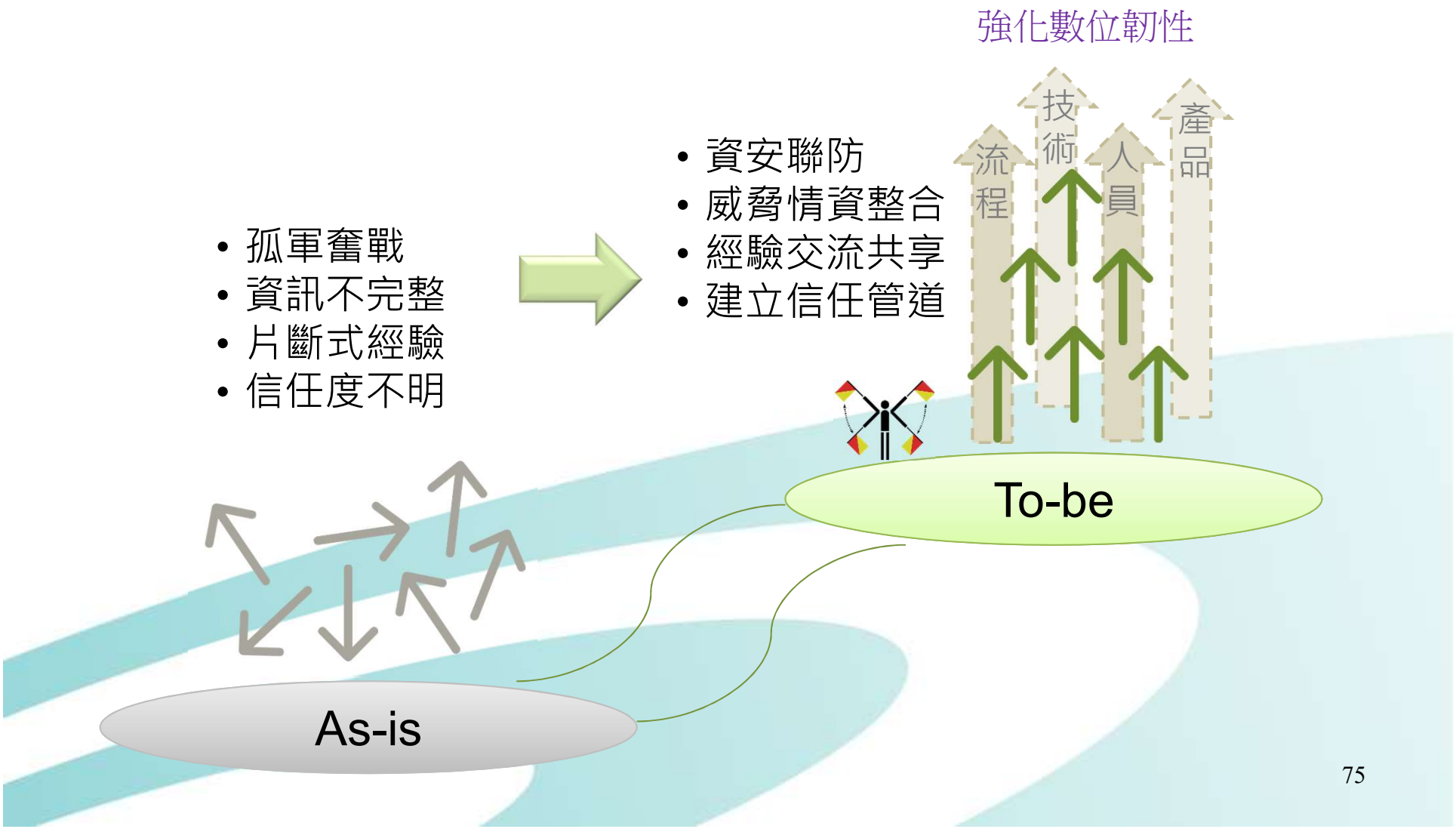
資安服務概要-人員面

- 藉由教育訓練、資安分享會議/論壇等，提升人員資安意識，強化資安威脅防護，減緩資安事件衝擊，並透過交流活動促進成員合作

- 舉辦資安教育訓練
  - ✓ 威脅防護課程 (社交工程，人員防護，勒索軟體)
  - ✓ 資安實務研討
- 資安經驗分享
  - ✓ 國內外資安新聞
  - ✓ 資安趨勢與駭侵事件
  - ✓ 資安經驗分享
- 成員交流活動
  - ✓ 聯盟成員交流
  - ✓ 合作議題討論
  - ✓ 建立聯繫管道

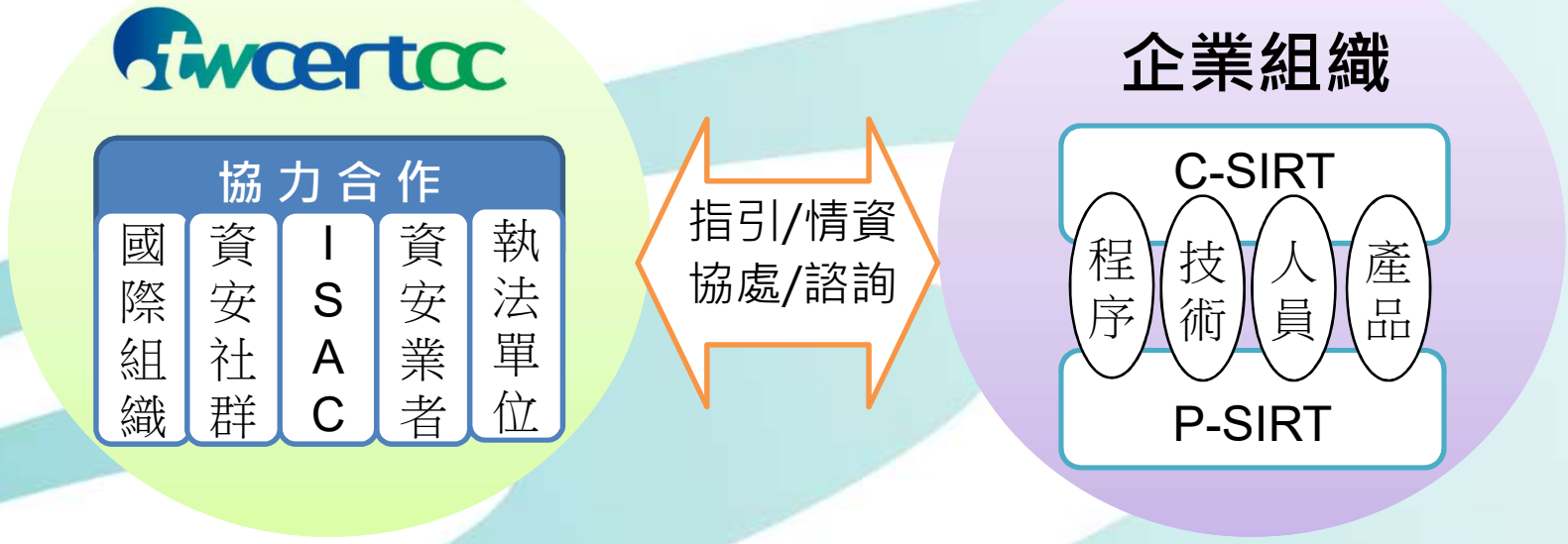
TWCERT/CC 資安聯盟

TWCERT/CC 資安聯盟目標



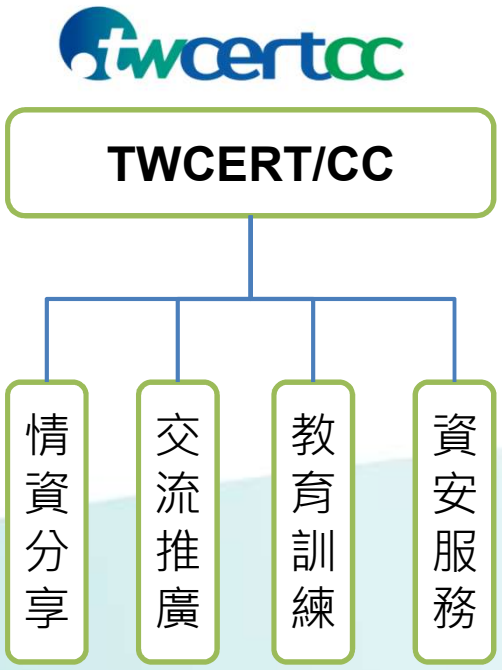
TWCERT/CC 資安聯盟定位

- 目的
  - 為強化企業資安聯防，藉由資安聯盟，進行威脅情資共享，促進資安經驗交流與聯防，冀於流程、技術、人員、產品等面向，強化整體數位韌性
- 會員資格
  - CERT/CSIRT組織、資安業者、一般企業、教育學術單位、公協會、法人團體等
- 作法：與國內外資安單位合作，協助強化企業資安防護

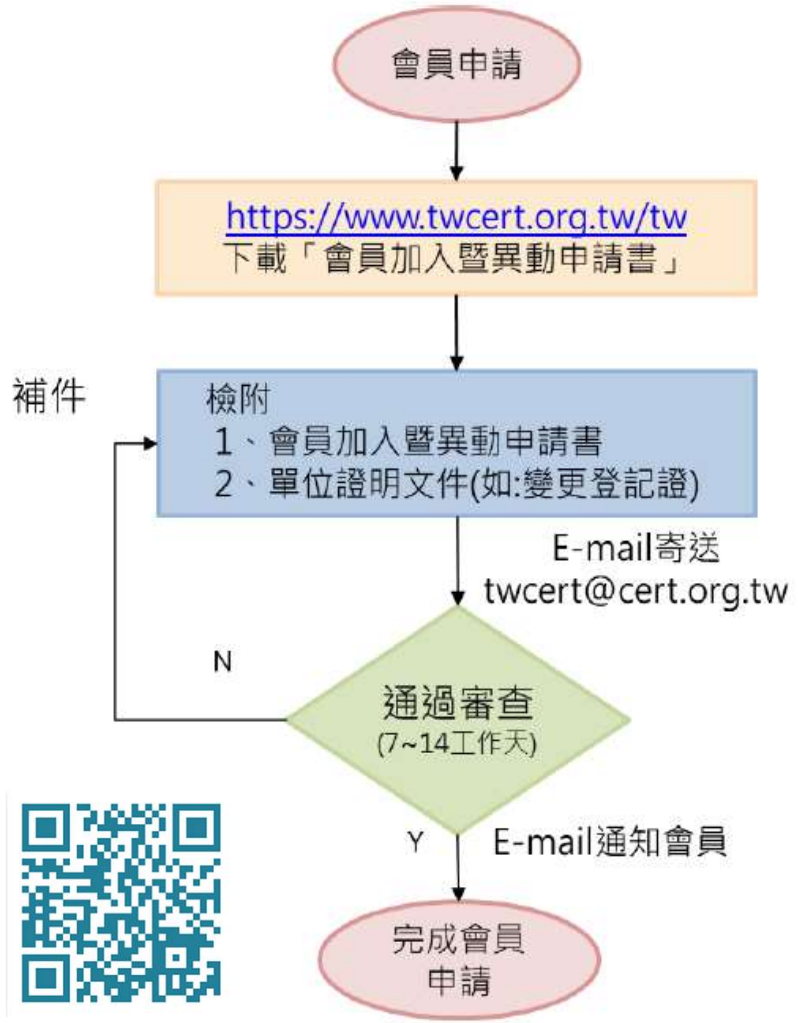


TWCERT/CC 資安聯盟運作機制

- 建立信任管道，促進企業經驗交流與資安聯防
- 參與本聯盟會議與活動，並分享近期重大資安事件處置狀況
  - TW-ISAC 平台
  - E-mail與Line 群組
- 會員可獲取 TWCERT/CC之資安情資，參與教育訓練、資安趨勢研討與交流等活動，以**技術**、**產品**、**流程**、**人員**等4大面向，促進民間資安防護強化



TWCERT/CC 聯盟入會說明



「台灣 CERT/CSIRT 聯盟」會員申請暨異動申請書

申請日期：民國＿＿＿年＿＿＿月＿＿＿日

會員基本資料			
機關/單位統編		證券代號	□上市 □上櫃
機關/單位名稱*			
會員新申請或異動申請(異動時請填寫有異動的欄位)			
□新申請或□異動資料			
機關/單位負責人*			
聯絡人資料*	姓名/職稱		
	Email		
	電話	(　　)　　#	
對外 IP/網段資料* (如:1.11.22.121、1.11.222.128/25 供通用計費安管資通報)	□新增 □刪除		
會員終止申請			
□本機關/單位提出終止申請，原因：			
會員同意暨簽名或用印			
□*已閱讀、瞭解並同意本申請書所註明之注意事項，及台灣 CERT/CSIRT 聯盟會員規章，詳見 TWCERT/CC 網站(twcert.org.tw)。			
機關/單位部門主管簽名 或 機關/單位用印*		申請人簽名*	
(申請或異動時，請附上工商/變更登記證或相關文件)		(請申請人親簽)	

官網/社群/電子郵件多元服務管道

PGP KEY
TWCERT/CC PGP Public Key
Key ID : 0x1E9D1F1B

官　網：www.twcert.org.tw
社群媒體：www.facebook.com/twcertcc/
電子信箱：twcert@cert.org.tw

Thank You!