

**CYBERSEC 2024**  
臺灣資安大會

5/14<sub>Tue</sub> — 5/16<sub>Thu</sub>  
臺北南港展覽二館

**Generative  
Future**

Cyber Briefing

# TWCERT服務介紹

林易澍

國家資通安全研究院 經理

# 一、TWCERT/CC簡介



## • Taiwan Computer Emergency Response Team / Coordination Center

- 台灣電腦網路危機處理暨協調中心

中山大學

1998年9月  
TWCERT/CC  
成立於中山大學

TWNIC

2010年1月  
轉由台灣網路資  
訊中心(TWNIC)  
接手維運

國家  
中山科學  
研究院

2014年8月  
改由國家中山  
科學研究院承接

TWNIC

2019年1月  
回到台灣網路資  
訊中心(TWNIC)  
維運

國家  
資通安全  
研究院

twcertcc

2024年1月  
由國家資通安全研究院  
(NICS)負責維運

## TWCERT/CC 服務總覽



### 情資分享

- ① 建立多元情資分享管道，促進跨域資安合作
- ② 彙整國內資安組織情資，持續分享交流



### 應變協調

- ① 協調資安事件處理團隊，協助資安事件應變處理
- ② 漏洞通報及CVE(common vulnerabilities and exposures)審查發放
- ③ 惡意檔案檢測服務



### 國際合作

- ① 參與國際資安組織活動
- ② 建立國內外溝通管道
- ③ 掌握資安威脅趨勢



### 意識提升

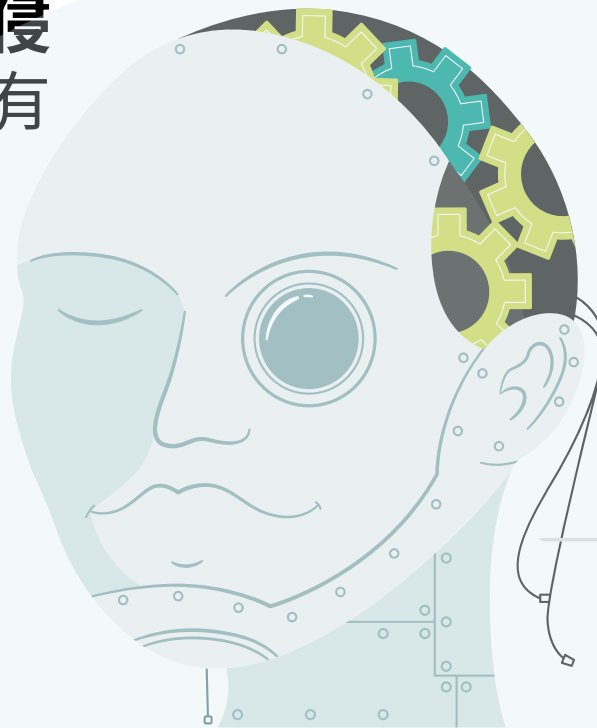
- ① 推動台灣CERT/CSIRT聯盟，強化資安聯防體系
- ② 透過社群媒體與宣導活動，提升民間資安意識

## 二、資安院運營TWCERT/CC的利基



## ● 積累多年政府資安服務經驗

資安院整合前行政院國家資通安全會報技術服務中心業務，在執行推展公務機關資安駭侵防護及應變協處相關工作已有20餘年經驗



## ● 公私聯防實作經驗

依據「國家資通安全發展方案」，維運N-SOC、N-CERT與N-ISAC國家層級聯防體系，建構事前威脅監控、事中應變與事後情資分享量能



## ● 具備國家層級情資綜整分析能力

資安院協助政府建立國家層級聯防體系，匯集各領域資安事件情資、自研情蒐、國內外情資，商用情資、經整合分析，去蕪存菁綜整有效情資，適時提供各領域參用

## ● 結合多元管道，提升情資質量

資安院可綜整結合N-ISAC、TWISAC、官網公告、電子報等多元管道，快速向民間企業分享資安相關情資，協助民間企業資安防護

## ● 技術能量積累

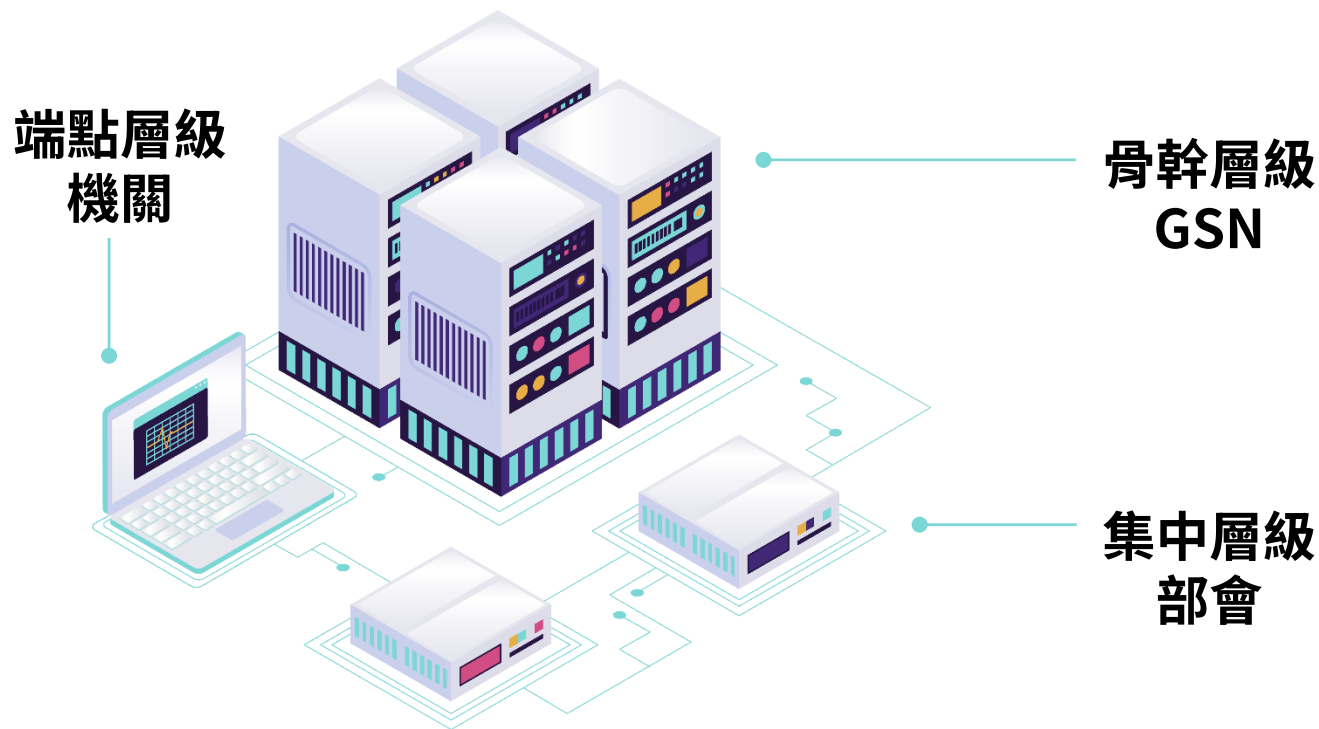
資安院長期協助公務機關執行GSN(Government Service Network)網路駭侵縱深防護作業，具備威脅偵測、事件處理、數位鑑識及情資分析等能力，可將相關技術能量與經驗移轉、分享民間企業

### 網路駭侵縱深防護

惡意程式蒐整

惡意程式分析

駭侵偵測規則

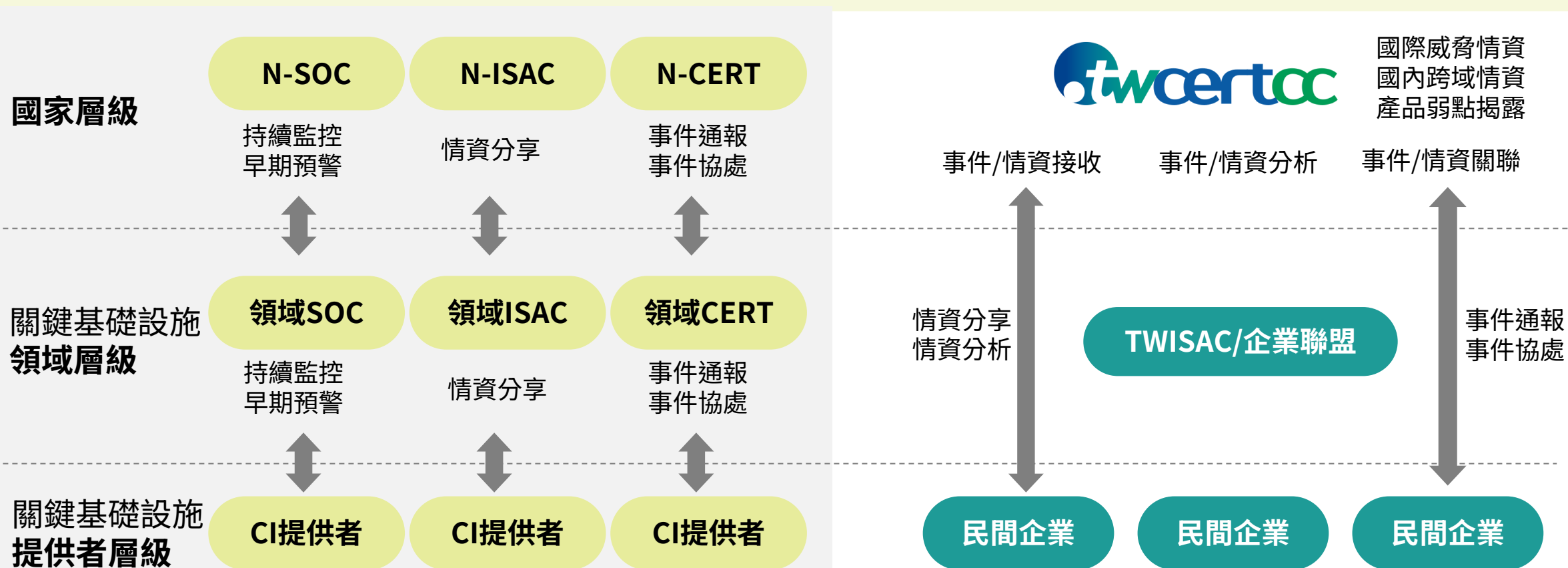




## ● 資安院可作為公私領域間橋樑，強化公私鏈結能量



資安情資交流/資安事件應處



## 三、強化公私協力 深化情資分享



# 擴大服務企業資安



強化公私  
鏈結聯防



公私領域  
情資交流



個資防護  
行政檢查

## ● 民間駭侵事件偵蒐

- 結合長期公務機關資安防護經驗，偵測蒐集民間企業APT攻擊事件，掌握受駭目標，與警調單位合作，協助其事件處理並提供強化建議



- 從公務機關事件調查，主動掌握民間受害事證，
- 從民間資安事件協處，情資回饋公務機關偵測防護，有效強化公私協力鏈結

## ● 對外服務曝險掃描

- 針對對外服務具重大影響弱點(CVE)，透過官網、TWISAC、N-ISAC通知民間企業，同時協助TWISAC會員進行掃描，主動通知未修補會員進行修補

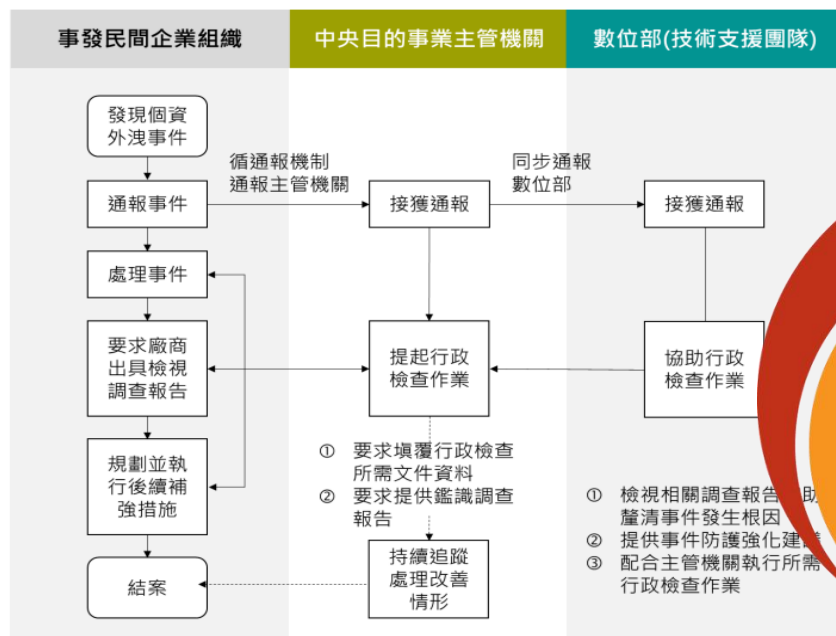
## ● 強化公私領域駭侵情資交流

- 匯集資安事件分析所得、自研情蒐、國內外情資，結合N-ISAC、TWISAC、官網公告、電子報等管道向民間企業分享資安相關情資，提升民間企業資安防護意識
- 鼓勵企業回饋自身事件應處後駭侵情資與惡意程式樣本，配合VirusCheck服務，協助樣本分析與情勢研判，助於其他公私領域防護有效性



## ● 強化個資防護技術面

- 依國發會「防止非公務機關個資外洩精進措施」，訂定非公務機關個資相關系統防護參考基準，具體強化技術面查檢面向
- 協助未來個資會與各中央目的事業主管機關執行民間企業行政檢查作業，就技術面提供強化改善建議



非公務機關個資相關系統防護基準(草案)

系統風險等級	系統風險等級		
	高	中	普
措施內容	一、對外服務系統上線前執行源碼檢測 二、對外服務系統上線前執行滲透測試，並完成漏洞修補 三、每年辦理一次滲透測試作業	一、對外服務系統上線前執行弱點掃描，並完成弱點修補 二、每年辦理一次弱	
系統檢測			

## 四、服務推廣





## ● 鼓勵企業通報

- 提供資安事件相關專業諮詢服務
- 透過廠商評鑑，提供專業服務廠商資訊供企業參考
- 協處特定資安事件，提供強化資安防護改善建議

The screenshot displays the twcertoc website, which is the Taiwan Computer Emergency Response Team / Coordination Center. The header includes the twcertoc logo, navigation links for News, Services, Advocacy, Links, and About us, and a search icon. Below the header, the main content area features a large circular graphic with the title '簡易資安事件通報' (Simple Cybersecurity Incident Reporting). Inside this circle is a form with three input fields: a text field, an email field labeled '電子信箱 E-mail', and a text area labeled '事件狀況描述 Description'. A blue button labeled '我要通報' (I want to report) is positioned at the bottom of the circle. To the left of the circle, there are four icons representing different services: International Collaborative Cyber Defense, Cross-National Cyber Intelligence Exchange, Entrepreneurial Cybersecurity Incident Referral, and Cyber Intelligence Collection and Cybersecurity Outreaches. Each icon is accompanied by its respective service name in both Chinese and English. At the bottom of the page, there are three buttons: '申請加入聯盟' (Apply to join the alliance), 'PGP KEY', and '連絡我們' (Contact us).



- 免費惡意檔案檢測服務

- 透過沙箱對惡意程式進行動態分析，並判斷是否有異常



## ● 協助漏洞發布

- 持續參與美國MITRE之通用漏洞揭露 (Common Vulnerabilities and Exposures, CVE®) 計畫，以CVE編號管理者(CVE Numbering Authorities, CNA)身分審核並發布CVE編號



The screenshot shows the twocertoc website's TVN (Taiwan Vulnerability Note) page. The page features a navigation bar with links to News, Services, Advocacy, Links, and About us. Below the navigation bar, there is a breadcrumb trail: 首頁 / 資安服務 / 台灣漏洞揭露平台 (TVN) / TVN (Taiwan Vulnerability Note) 漏洞公告. The main heading is "TVN (Taiwan Vulnerability Note) 漏洞公告". There are links for "TVN (English Version)" and "TVN 漏洞公告 RSS 訂閱". A button labeled "全部" is present. Below this, a table lists four vulnerabilities.

TVN ID	標題	CVE ID
TVN-202404014	鎧書全球科技 ArmorX Android APP - MFA Bypass	CVE-2024-4303
TVN-202404013	雲發互動科技有限公司 Super 8 livechat SDK - Cross-site Scripting	CVE-2024-4302
TVN-202404012	新夥伴科技 N-Reporter 與 N-Cloud - Os Command Injection	CVE-2024-4301
TVN-202404011	醫位資訊 FS-EZViewer(Web) - Sensitive Data Exposure	CVE-2024-4300

## ● 協助漏洞發布

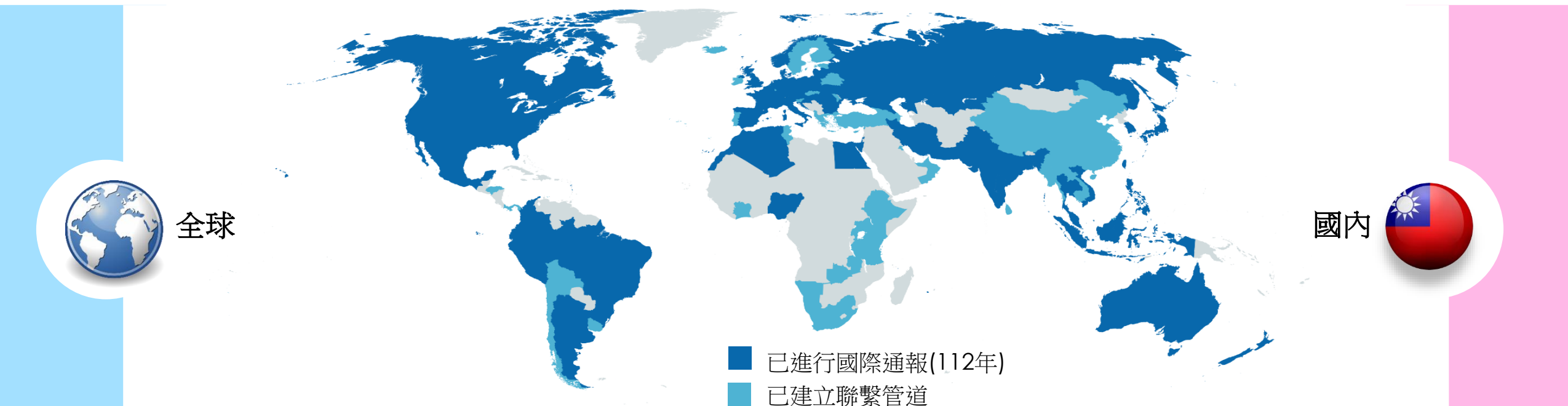
- 持續參與美國MITRE之通用漏洞揭露 (Common Vulnerabilities and Exposures, CVE®) 計畫，以CVE編號管理者(CVE Numbering Authorities, CNA)身分審核並發布CVE編號

### ASUS 無線路由器 - OS Command Injection

TVN ID	TVN-202404006
CVE ID	CVE-2024-1655
CVSS	8.8 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
影響產品	ExpertWiFi EBM63 韌體 3.0.0.6.102_32645(不含)以前版本 ExpertWiFi EBM68 韌體 3.0.0.6.102_44384(不含)以前版本 RT-AX57 Go 韌體 3.0.0.6.102_22188(不含)以前版本
問題描述	ASUS 部分無線路由器型號存在 OS Command Injection 漏洞，允許通過身分鑑別之遠端攻擊者，可藉由發送特製請求執行任意系統指令。
解決方法	更新 ExpertWiFi EBM63 韌體至 3.0.0.6.102_32645(含)以後版本 更新 ExpertWiFi EBM68 韌體至 3.0.0.6.102_44384(含)以後版本 更新 RT-AX57 Go 韌體至 3.0.0.6.102_22188(含)以後版本
漏洞通報者	William Shi
公開日期	2024-04-15

## ● 國際情資交流

- TWCERT/CC作為我國與國際資安溝通的橋樑，目前已經與110個CERT組織建立聯繫管道



## ● 國內情資交流

- TWCERT/CC同時為國內N-ISAC成員接收國內各領域資安事件情資通報，協助民間企業組織加入資安聯防行列
- TWCERT/CC為協助民間企業組織提升自我防護能量，組成「台灣CERT/CSIRT聯盟」，不定期透過TWISAC分享資安情資

## ● 國內情資交流

- 根據情資類型，目前共分為4種

### 漏洞情資

- 針對CVE分數達8.8之資安漏洞發布情資，提醒企業組織儘整完成更新
- 每週蒐整KEV公告遭利用之漏洞，讓企業了解近期常用之弱點
- 外部情資通報企業設備存在之安全性漏洞

### IoC情資

彙整各情資單位提供IoC情資，不定期提供予會員

### 攻擊活動預警

研析外部通報我國企業攻擊事件情資，發現共通性攻擊活動，發布攻擊活動預警，協助企業提早防範駭客攻擊活動

### 攻擊事件通報

接獲外部情資/偵測發現攻擊事件情資，將攻擊事件相關資訊提供予受駭企業進行應處，以降低事件影響



## ● 以攻擊事件通報為例

- 接獲外部情資/偵測發現攻擊事件情資，將攻擊事件相關資訊提供予受駭企業進行應處，以降低事件影響



TLP:AMBER

Thank you – we have some further feedback for [REDACTED]

- The implications of this intrusion are not limited to the single device (CHROMA-LP-01):
  - Attached is an updated log\_shell file that includes PowerShell commands run by the threat actors on the same device/account. It includes the commands previously shared, as well as significant new commands. This appears to now include the use of utility Rubeus for kerberoasting, and therefore, **potential extensive dumping of password hashes, including for privileged accounts**. Some of the Kerberos tickets listed only use RC4 encryption, which may be easily cracked.
  - Based on this, a domain-wide credential reset may be advised. Credentials for, at least, the 8 accounts that appear to have been kerberoasted should likely be reset, accordingly, as well as the 'uyen.pham' account.
  - These commands, and their output, should be evidence that the device was indeed compromised.
- Antivirus is unlikely to detect the malware retroactively, if it didn't already detect the initial infection. Although it sounds like the device was already wiped, in the event that a forensic image was captured, we are outlining some specific detection opportunities below:

## 攻擊事件通報

TLP: AMBER

TWCERT-TWISAC-202403-00

[REDACTED] 資訊設備疑似遭植入Gootloader惡意程式感染

敬啟者您好

TWCERT/CC接獲通報，發現與貴單位有關之EWA情資，相關資訊如下述，請協助進行處理。

本中心於近日接獲外部情資，發現貴單位資訊設備疑似遭Gootloader惡意程式感染，Gootloader為一種木馬惡意軟體，近期發現為作為勒索軟體攻擊的第一階段，請儘速檢視設備是否有受駭情況，相關資訊如下：1. 來源IP：91.229.248.112 2. 作業系統：[REDACTED]-01 with OS Microsoft Windows 11 Pro 3. 使用者名稱：u[REDACTED] 4. 網域名稱：[REDACTED].[COM].[REDACTED]TW 5. 惡意程式回報時間：3/2 /2024 09:50:35 UTC。惡意程式執行的PowerShell指令如附檔「log\_shell.zip」。

。 若有任何問題或是入侵IoCs等資訊願意分享給我們以利聯防，歡迎與我們聯繫，謝謝您。

受害者IP: 91.229.248.112

受害者Port: 0

受害者Protocol: 0

◎建議措施：

- 盤點與檢視相關設備系統，判定是否遭入侵並植入惡意程式，導致可疑連線行為。
- 若確認系統已遭入侵，請調查該主機遭入侵之途徑，針對遭攻擊之弱點進行修補。
- 請勿開啟未受確認之電子郵件附件。
- 系統上所有帳號需設定強健的密碼並定期更換，非必要使用的帳號請將其刪除或停用。
- 安裝防毒軟體並更新至最新病毒碼，開啟檔案前使用防毒軟體掃描郵件附檔。
- 確實更新防火牆並阻擋惡意中繼站。
- 加強內部宣導與防範駭客利用電子郵件進行社交工程攻擊。

◎參考資料：

- <https://www.kroll.com/en/insights/publications/cyber/deep-dive-gootloader-malware-infection-chain>
- <https://redcanary.com/threat-detection-report/threats/gootloader/>
- <https://www.mandiant.com/resources/blog/tracking-evolution-gootloader-operations>

# 服務推廣：個資外洩通知


## ● 個資外洩通知

- 定期檢視個資販售的論壇(含暗網)，若有疑似個資遭販售之行情，會主動通知會員確認是否屬實

BreachForums > Marketplace > Sellers Place > **SELLING** INT CORP ~2TB of fresh DATA Mark all as read Today's posts

**INT CORP ~2TB of fresh DATA**  
by DISPOSSESSOR - Thursday February 15, 2024 at 08:51 PM

**DISPOSSESSOR**



GOD User

**GOD**

Posts: 27  
Threads: 9  
Joined: Nov 2023  
Reputation: 110

02-15-2024, 08:51 PM #1

Dear colleagues, our big team is selling ~2TB of fresh data exfiltrated from servers due cybersecurity breach  
Company name: Mechema Chemicals International Corp.  
Website: <https://www. .com/>  
Stock Symbol: . TWO - | Stock Price & Latest News | Reuters. - <https://www.reuters.com/markets/companies/ .TWO/>  
Part of files will be posted on leak blog website: <https://dispossessor.com>  
Part of files recorded on video website: <https://cybertube.video/web/index.html#!...e66321ab72>  
News: <https://cybernewsint.com/theft-and-discl...m-company/>

**Company Information**  
INT CORP. is a Taiwan-based company principally engaged in the manufacturing, trading, import and export of oxidation catalysts. The Company's principal products include cobalt acetates, manganese acetates, cobalt compounds, manganese compounds, cobalt bromides, manganese bromides, cobalt metals and manganese metals. The Company is also engaged in the production and trading of magnetic materials and raw materials of batteries, as well as the cyclic utilization of waste oxidation catalysts. The Company mainly distributes its products in domestic market and overseas markets, including the People's Republic of China (the PRC), Korea, Thailand, Malaysia and Indonesia.  
Address: TAOYUAN, 328, Taiwan  
Contact Information +886

**INT CORP. Board members involved in data breach:**  
Lung Tsai Yen - Chairman of the Board, General Manager  
Wenxun Cai - Executive Deputy General Manager, Head of Finance & Accounting  
Suzhen Cai - Manager-Administration  
Yuangdong Xu - Director  
Wenzhi Yan - Director  
Guoguang Ye - Director  
Shen Yuan Chen - Independent Director  
Meng-Hsiu Lee - Independent Director  
Gaojin Wang - Independent Director

Based on the results of data analysis, the company evades taxes. A taxpayer in Taiwan who has, by fraudulent or other illegitimate means, evaded taxation is liable to no more than five years in prison and up to NT\$10,000,000 in fines. The source - <https://www.hcct.gov.tw/en/home.jsp?id=3...ntpath=0,3&>

[Reply](#)



## 五、結語



國家  
資通安全  
研究院



2024年1月

由國家資通安全研究院  
(NICS)負責維運

加強與各主管機關、企業、公協會及國外組織  
鏈結及合作，進一步提升企業資安韌性

採取主動蒐集、主動協處、主動分享等主動服務的  
精神及機制，主動察覺民間企業受害事件，協助企  
業妥適應處資安事件

持續鼓勵民間企業加入TWCERT/CC會員

# Thank you for your attention



國家資通安全研究院

National Institute of Cyber Security