



資安聯防全面啟動

TWCERT/CC 通報應變小組
沈紀威

大綱

一 近期常見的資安問題

二 日本資安聯防體系

三 TWCERT/CC提供的服務

前言

- 資通科技(ICT)的迅速發展，帶來了便利與智慧化的生活，同時也衍生了資訊安全的疑慮：
 - 對個人而言，造成個資外洩、檔案勒索或財務盜刷。
 - 對單位而言，造成經濟損失、商譽受損或機密外洩。
 - 對國家而言，關鍵資訊基礎設施遭駭，引發政經民心動亂。
- 政府已將資訊安全提升到國家安全的層級，因此，資訊安全的觀念應成為國民的基本素養。

資訊安全與個資保護

■由於資訊化普及，個人資料均以電子檔案方式儲存，個人資料遭竊案例，時有所聞。



小心LINE帳號遭盜用，勿提供四位數簡訊認證碼

國外 團體 訂房 機票 雄獅自由行 航空自由行 郵輪 台灣

熱門國外目的地

東北亞		
韓國	大阪京都	立山雪牆
東京	北海道	九州
東南亞/南亞島國		
泰國	新加坡	吳哥窟
峇里島	長灘島	越南
宿霧	馬來西亞	馬爾地夫
大陸港澳		
香港	澳門	北京
江南水鄉	九寨溝	張家界

團體 國外 台灣

訂房 機票 自由行 航空自由行 高鐵旅行 票券 主題旅遊

*出發地 不限

*出發日期 2017/

旅遊天數 不限

只找

標題：小心LINE帳號遭盜用，勿提供四位數簡訊認證碼

發布時間：2017/3/28 下午 03:30:50

詐騙集團近期透過通訊軟體「LINE」假冒民眾親友，傳送訊息請民眾代收四位數簡訊認證碼，藉此盜用民眾LINE帳號，並向其親友借款詐騙\$。

提醒您，#勿將4位數認證碼告知他人；#接獲親友傳訊息借款，#請當面或電話再次確認，以免受騙。



資料來源:165反詐騙

資訊安全與理財購物

■網路商業活動活絡，同時也成為駭客覬覦詐財的目標，詐騙取財紛爭不斷。

民眾通報高風險賣場排名

排名	內
1	E (電影票券)、拍賣
2	拍賣 件數：16件
3	旅遊 件數：13件
4	生活 件數：10件

資料來源:165反詐騙

「網拍購物真方便！小心惡意詐騙藏其中」偵破趙○棠涉嫌網拍詐欺案

5/26/2017

標題：「網拍購物真方便！小心惡意詐騙藏其中」偵破趙○棠涉嫌網拍詐欺案

副標題：「網拍購物真方便！小心惡意詐騙藏其中」偵破趙○棠涉嫌網拍詐欺案

發布時間：2017/4/28 下午 04:42:03

(一)本局近期發現知名拍賣網站以不明帳號販售最新電子3C產品為名義，向不特定網路買家詐騙，俟被害人匯款後，涉嫌人即失去聯繫不予理會，經本局偵九大隊聲請臺灣橋頭地方法院搜索票，於4月19日前往主嫌趙○棠住居所執行搜索，查扣犯案用手機6支、平板電腦2台、銀行帳戶存簿2本、提款卡2張、桌上型電腦1台、外接式硬碟1個等相關證物，初步統計被害人數66人，詐騙金額新臺幣101萬6千餘元。

(二)犯罪嫌疑人趙○棠於105年底開始利用知名拍賣網站，以「最新旗艦商品，智慧手機、3C商品、穿戴裝置、公仔玩偶」為號招吸引買家，初期正常出貨以建立良好之賣家評價，並私下透過網路通訊軟體與被害人聯繫，待被害人匯款後，即以不堪長期虧損為由一再拖延出貨或退款時間，最後失去聯絡，被害人始警覺遭詐騙。

(三)本局提醒民眾，網路購物有快速便宜的特性，但也成為犯罪者覬覦的目標，為降低被詐騙的風險，除慎選適當交易平台外，應注意賣家評價及選擇使用第三方支付之付款方式進行交易，更避免與賣家私下通訊交易，以保障自身的權益。

資料來源:165反詐騙

資訊安全與商譽維護

■商譽對於企業有其重要性，一旦商譽受損，連帶會影響客戶的信心。

事件	發生時間	個資外洩、損失金額	後續
冒用OO航空	2017年3月	40多人遭詐騙逾300萬	
OO人壽保戶資料外洩	2017年3月	不明 (保戶數約35萬)	
「OOOOOOOO生活」網站	2016年10月	133人遭詐900萬	
OO考生個資外洩	2016年10月	45人遭詐138萬	
「OO函授」學員資料外洩	2016年9月	28人遭騙550萬元	
「OO牧場」等旅館訂房網遭駭	2016年9月	16人遭詐180萬	
OO人壽大量洩漏保戶個資	2016年8月	上百位保戶	
OO銀行寄錯2萬人帳單洩個資	2016年6月	2萬人	罰鍰400萬元
OO投信洩漏客戶個資	2016年2月	電子報會員有7萬9193位	
OO航空行程管理驗證功能出包	2015年12月	業者未透露	
OO旅館集團遭駭	2015年9月	上萬筆	
OO咖啡會員資料被駭	2015年5月	5000筆會員個資	
18家購物網站個資外洩	2014年2月	造成民眾近9000萬元損失	
OOOO網路銀行	2013年5月	5萬多筆	罰鍰400萬元
OOOOO行銷活動網站被駭	2013年2月	150萬筆	

資料來源:消基會

案例1:臉書的一頁式廣告詐騙(1/3)

華視 CTS HD

投訴人: 高雄 楊先生

事由

萬元滑板車賣1688

臉書購物慘遭詐騙

不買對不起自己

獨家 臉書購物詐騙案 半年多達4千件!

19:15 搶救觀光 · 花蓮自由行補助 放寬平日2人同行適用 花蓮 20-26°C

案例1:臉書的一頁式廣告詐騙(2/3)

【STYLENANDA官方3CE MOOD RECIPE唇膏全色迷你套裝】

D-store
約1個月前

特別推薦 🍌
滋潤保溼, 色彩飽滿, 防水持久不沾杯
🍌: 【官方3CE MOOD RECIPE唇膏全色迷你套裝】 咖啡色+紅色 2套共10支僅需NT\$ 998!
限量發售99套, 售完無補. 立即預定吧! 🍌
<http://www.ebuytw.com/stylenanda>

2,908
207則分享 20萬次觀看

#破盤價 #免運費
#貨到付款 #7天鑑賞
冒用原廠圖片影片, 引誘點擊可疑網址, 然而商品與實際不符, 造成民眾財損或被植入惡意程式

STYLENANDA官方3CE MOOD RECIPE唇膏全色迷你套裝
NT\$ 998

已搶購8574件 僅剩21件
距離結束 08 時 42 分 52 秒

免運費 貨到付款 7天鑑賞期

立即購買

案例2:網站遭轉址服務利用的資安風險(1/5)

- 某電商通報其網站被偽冒

1.  .kjm.com.tw
2.  .omap.com.tw
3.  .ufc.com.tw
4.  r.ii9.com.tw
5.  r.jnd.com.tw

這些是可疑網站，都是轉址服務



案例2:網站遭轉址服務利用的資安風險(2/5)

- 網路上有許多提供免費網域轉址服務的網站，為了獲取廣告收入
- 針對申請者的身分認證機制並不嚴謹，不經同意就可將知名網站加工轉換成其他網域
- 網站管理者通常不知道已經遭到利用作為其他用途或加入廣告頁框。



```
1
2 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" "http://www.w3.org/TR/REC-html40/loose.dtd">
3 <html>
4 <head>
5 <title>[REDACTED]/title>
6 <meta name='keywords' content='[REDACTED]'>
7 <meta name='description' content=''>
8 <meta name='revisit-after' content='14 days'>
9 <meta name='robots' content=''>
10 </head>
11 <frameset rows='25,*' frameborder='NO' border='0' framespacing='0'>
12 <frame name='TOP_MENU' src='http://[REDACTED].ufc.com.tw/?PUT=ad' noresize scrolling='no'>
13 <frame name='MAIN' src='http://www.[REDACTED].com.tw'>
14 </frameset>
15 <noframes>
16 <body bgcolor='#FFFFFF' text='#000000'>
17 進入 <a href='http://www.[REDACTED].com.tw'>[REDACTED]</a>
18 </body>
19 </noframes>
20 </html>
```

案例2:網站遭轉址服務利用的資安風險(3/5)



The screenshot shows a Google search interface with the query 'site:ufc.com.tw' in the search bar. Below the search bar, the results are displayed, with a red box highlighting the search results summary: '共約 2,220 項結果, 這是第 2 頁 (搜尋時間: 0.24 秒)'. The results list several websites, including '外掛聯合國', '禿鷹教育網', '豆瓣', 'Yahoo!奇摩電影', 'PCZONE 討論區', 'Post76影音玩樂網', and '騰發科技股份有限公司'. A red box highlights the 'Yahoo!奇摩電影' result, which is the focus of the text on the right.

Google site:ufc.com.tw

全部 圖片 新聞 地圖 更多 設定 工具

共約 2,220 項結果, 這是第 2 頁 (搜尋時間: 0.24 秒)

外掛聯合國
wgun.ufc.com.tw/ ▼
發佈多種免費外掛供玩家選擇且功能強大, 擁有台灣、新馬、香港等免費外掛。

禿鷹教育網
1061513.ufc.com.tw/ ▼
提供線上課程、遠距教學、數位學習、網路會考、落點分析、自傳口試等服務。

豆瓣
1060733.ufc.com.tw/
熱門話題 ····· (去話題廣場). 我的第一份工作 [新] 回首初入社會時 · 1467人參與; 我心目中的國產電影十佳 中國首部電影開拍紀念日 · 5547人參與; 走出故鄉還回得 ...

Yahoo!奇摩電影
1061229.ufc.com.tw/ ▼
含最新電影、電視頻道、線上電影及強檔放送等內容。

PCZONE 討論區
pczone.ufc.com.tw/ ▼
ADSL FTTB CABLE WIFI 3G iPhone iPad Android htc samsung mp3 寬頻網路。

Post76影音玩樂網
pingping.ufc.com.tw > Post76 玩樂網 > 論壇 ▼
總版管 副版管 版務總管組 科林版主 行動組版主 特別行動組版主 行動組特工 見習版主 會員: icon 關大爺; icon bzguy; icon wkhbobby999; icon oyd; icon ...

騰發科技股份有限公司
afartech.ufc.com.tw/ ▼
騰發科技股份有限公司. 騰發科技. 騰發. 網站規劃. 網站設計. 網站程式設計。

遭ufc轉址服務利用的網址就有2220筆

案例2:網站遭轉址服務利用的資安風險(4/5)

The screenshot shows the legitimate CNA website. The browser's address bar contains the URL **www.cna.com.tw**, which is highlighted with a red box. The page header includes the CNA logo and navigation links such as "總覽", "要聞", "國際", "文化", "兩岸", "財經", "科技", "社會", "地方", "生活", "體育", "娛樂", "特企", and "影音". The main content area features a news headline: "[09:20] 財經 / 台積電完成填息 耗費32個交易日" and a sub-headline: "大學指考放榜 查詢錄取校系看這裡". A large image of a building is visible on the left side of the page.

The screenshot shows a phishing website that mimics the CNA website. The browser's address bar contains the URL **1061559.fol.com.tw**, which is highlighted with a red box. The page header includes a logo that looks like CNA and navigation links similar to the legitimate site. The main content area features a news headline: "[09:11] 國際 / 駭客聲援叛變 駭入委內瑞拉官方網站" and a sub-headline: "大學指考放榜 查詢錄取校系看這裡". A large image of an elderly woman is visible on the left side of the page. The footer of the page contains the text **FOL**, which is highlighted with a red box.

案例2:建議措施(5/5)

- 1.電商業者應該經常以自己的網站名稱、網域等關鍵字進行搜尋，是否遭非法冒用，若發現有非網站管理者意願之重製行為，應向網域轉址服務平台反映並通報當地CERT/CSIRT組織或網域管理單位，協助移除。
- 2.使用者應該小心其網站名稱與網址是否有異，勿認為從搜尋引擎找到的連結都是正確的。
- 3.網域轉址服務平台商應對申請者建立更嚴謹的身分驗證機制，以防止有心人士利用網域轉址服務作為網路釣魚用途。

案例3:某電商資料外洩實例

TWCERT/CC接獲企業通報，表示該企業的線上購物客戶，在近數月間頻頻收到詐騙電話，以明確的個人資料及購買商品的資訊，說服顧客重新轉帳匯款。詐騙集團在取得受害者信任後，便誘騙受害者至ATM操作，將款項匯款至指定帳戶中，當時已有多名顧客受害。

- 該受駭購物網站係架設於向服務商所租賃的雲端空間中，相關的連線機制並未採用SSL加密機制。
- 該購物網站的網頁應用程式為委外廠商進行設計與開發，經本中心檢測後，該網頁應用程式存在**多個高風險**的安全問題。

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	74
High	42
Medium	6
Low	23
Informational	3

電商常見的資安問題

台灣許多具實體店面的小型企業，想透過網路進行販售，然而受限於產業規模與型態，企業員工通常不具資訊及資安相關背景，因此其線上購物網站普遍委託網站開發廠商建置，企業對於系統架構與網站設計皆無法掌握，開發商因人力、技術及成本考量，相關的安全測試與檢查常被忽略，普遍存在以下問題：

1. 網站原始碼存在安全漏洞。
2. 相同網站開發商所建置之網站，可能使用相同開發框架，若網站開發商對於網站資訊安全不重視，容易導致企業遭遇類似的資安風險。
3. 網站無防火牆保護或防火牆設定為預設值或設定不正確。
4. 網站伺服器的作業系統及應用程式未安全更新至最新版。
5. 防毒軟體未安裝或未更新至最新病毒碼。
6. 網站資料庫存取未即時監控異常連線。
7. 網站未採用SSL加密機制。
8. 委外廠商不處理(合約沒寫、合約過期了不保固)
9. 網站的管理權限無有效的控管，一般僅使用帳號/密碼管理，無限制管理者的來源。
10. 內部員工電腦遭入侵(社交工程、惡意郵件)。
11. 以上你都知道，但是完全落實的少。

零時差攻擊沒你想的普遍 快調整安全弱點管理優先順序 已知漏洞才是遭駭大宗 資安莫再捨薪輿而逐秋毫

Craig Lawson、Kasey Panetta

安全漏洞遭到利用，至今仍是造成大多數資安缺口的根本原因，絕大多數的資料外洩事件都起源於漏洞遭到駭客利用，其中大部分的攻擊是來自於已知的漏洞，而非零時差攻擊（Zero Day Attack）。

務

2018/9/26

AI帶來機會而非失業 自動化促進資安人才發揮

2018/9/26

底層通訊攸關網路安全性 5G 引進高可信資安設計

2018/9/25

Ruckus Networks 發表亞太區 Wi-Fi 研究報告

2018/9/25

伊頓飛瑞慶在台十週年

2018/9/25

的資料外洩事件都起源於漏洞遭到駭客利用，其中大部分的攻擊是來自於已知的漏洞，而非零時差攻擊（Zero Day Attack）。

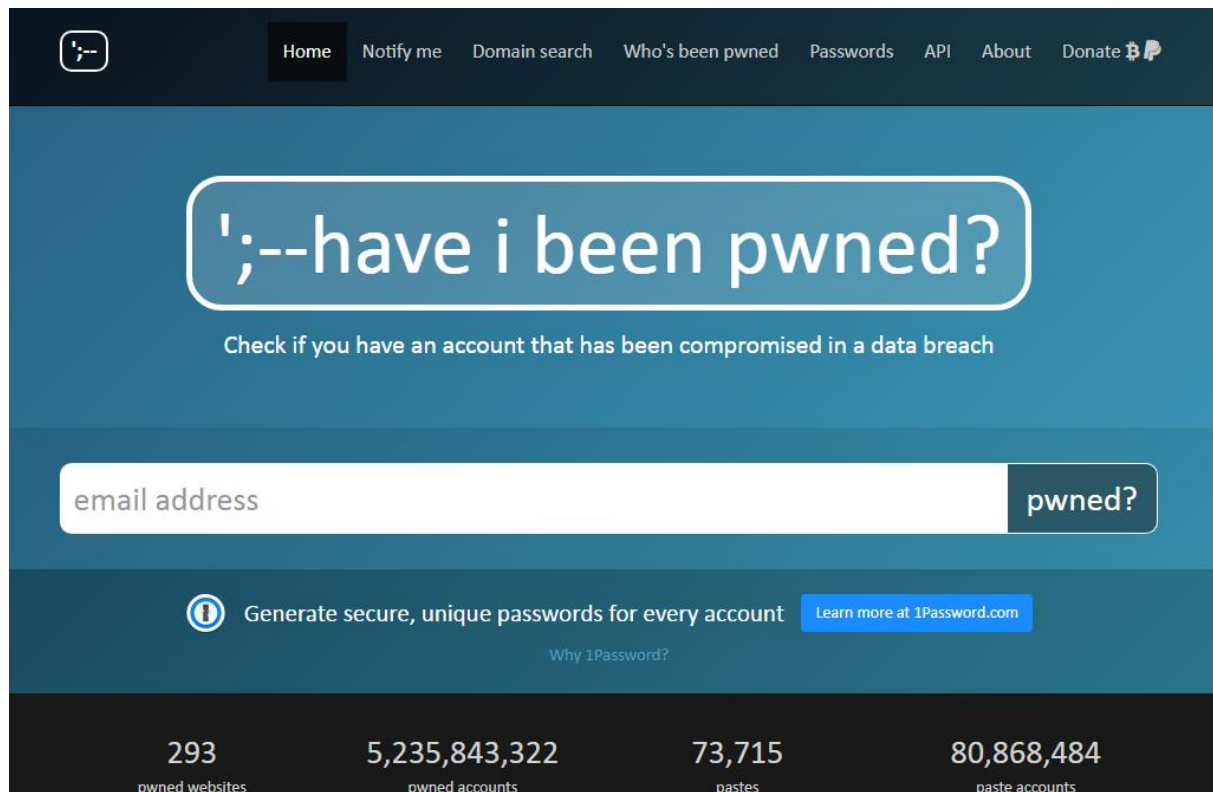
去（2017）年以來WannaCry和Petya勒索病毒攻擊事件肆虐全球，Equifax資料外洩事件也引發極大關注。要吸引媒體注意很容易，但這不應該是安全專業人士最應該擔心的威脅。

安全漏洞遭到利用，至今仍是造成大多數資安缺口的根本原因，絕大多數的資料外洩事件都起源於漏洞遭到駭客利用，其中大部分的攻擊是來自於已知的漏洞，而非零時差攻擊（Zero Day Attack）。

過去10年間，零時差漏洞在所有漏洞佔比中只有約0.4%，因偵測這類漏洞所花費的金錢，和它們真正產生的風險相比實在不成比例。

民眾之資安防護

- 民眾可利用have i been pwned?網站查email是否已外洩



參考資料：<https://haveibeenpwned.com/>

TWCERT/CC主動告知

■ 情資來源

- 外部合作夥伴
- 網路公開清單

放心，我們不是壞人



主旨：請回覆[TWCERT/CC-██████████]股份有限公司所屬電子郵件信箱已遭駭客入侵或鎖定。
收件者：██████████
日期：11/17/17 13:24
寄件者：通報應變小組

本單位是TWCERT/CC（台灣電腦網路危機處理暨協調中心），為非營利組織，負責與國內外各資安組織協同合作執行民間資安事故通報與應變作業，以維護臺灣整體網際網路安全。

日前接獲通報，發現██████████公司所屬電子郵件信箱已遭駭客入侵或鎖定，可能會遭受社交工程攻擊，或被利用為散發垃圾郵件之帳號等，請協助所屬用戶確認並解決相關問題，以免遭有心人士利用。

遭攻擊郵件信箱：「██████████」

TWCERT/CC建議處置方式：

請向所屬用戶宣導並協助處理下列事項：

- 1.請定期更新電子郵件信箱密碼，避免帳號密碼遭竊取。
- 2.勿點選來路不明的郵件或檔案、連結，即使信件來自熟識帳號亦應確認真偽。
- 3.注意信件寄件者帳號信箱是否正確（常見的竊取電子郵件手法包含字型混淆（英文、數字）、字元加減及位置調換等方式來欺騙使用者）。
- 4.定期保持作業系統及防毒軟體更新。

若有任何疑問歡迎來電詢問。

GOOGLE IT!



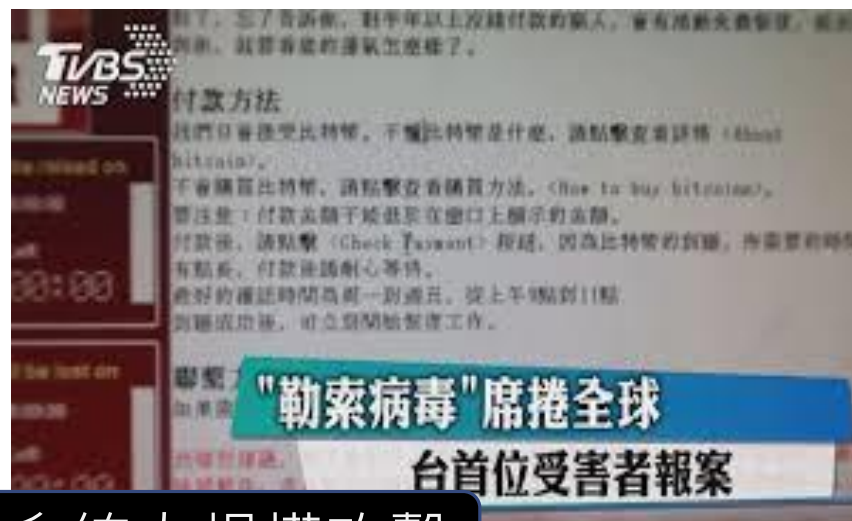
你的名字



二、日本資安聯防體系 Nippon CSIRT Association



駭客有發動對同類型受害人進行大規模攻擊的趨勢



鎖定特定對象或系統大規模攻擊

全球ATM崩潰倒數計時？傳駭客將進行大規模侵略

資訊專家安全研究員布萊恩克雷布斯 (Brian Krebs) 透露, FBI接獲消息, 表示今日ATM可能遭到大規模攻擊, 請民衆注意。

870 讚 9 分享 推文 分享

By 財經組, 台灣英文新聞 - 編輯
2018/08/16 14:58



SWIFT平台被駭金額前5高銀行



銀行名稱 (時間)	被駭金額
孟加拉央行(2016.2)	8100萬美元
台灣遠東商銀(2017.10)	6000多萬美元
俄羅斯央行 (2016年初)	3100萬美元
厄瓜多某銀行 (2015.1)	1200萬美元
烏克蘭某銀行(2016.6)	1000萬美元

資料來源：綜合外電 製表：編譯楊美宜

資安通報管道?

從2016年起

- 銀行ATM攻擊盜領
- 證券業集體遭DDoS勒索
- 新型態的勒索軟體(如WannaCry、Petya等)
- 旅行社大量個資外洩
- 物聯網設備遭攻擊利用
- 銀行SWIFT系統遭駭

以上資安攻擊案例都與我們日常生活息息相關，一般人皆能體會119於生命財產受威脅時的重要性，企業主們是不是也該想一想，發生**資安**攻擊事件時，您們的**通報管道**在哪裡？→CERT或CSIRT

CSIRT是什麼？

■ Computer Security Incident Response Team, CSIRT.

CSIRT在一開始並非稱為CSIRT，而是CERT (Computer Emergency Response Teams)

■ 在國際上有關電腦緊急應變小組名詞，包括：

- CERT or CERT/CC (Computer Emergency Response Team / Coordination Center)
- **CSIRT (Computer Security Incident Response Team)**
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

■ 功能

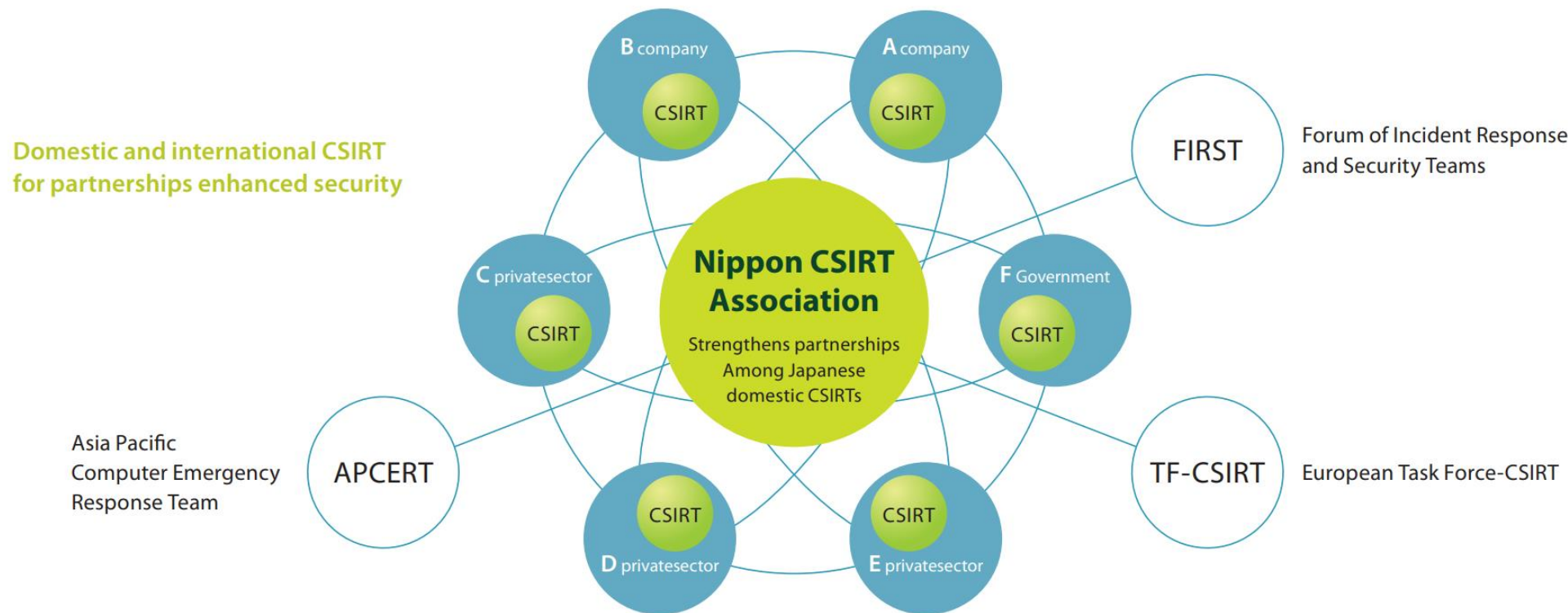
負責電腦相關安全事故對應處理之團隊。平時負責協助組織內安全相關政策的施行與資安訓練，並作為組織的安全代表與外部進行情資交流；一旦有事件發生，必須有能力確實掌握狀況應變，將災害減至最輕，有必要時須向管理階層報告。

資料來源：中央研究院、CERT/CC

日本CSIRT協會(1/2)

■ 日本CSIRT協會(Nippon CSIRT Association, NCA)

- ✓ 2007年3月由JPCERT/CC協助籌組的非政府組織，2018年9月28日公布成員數達312個企業
- ✓ 主要任務：成員間彼此共享資安情資、資安事件應變處置作為



日本CSIRT協會(2/2)

- 日本CSIRT協會(Nippon CSIRT Association, NCA)
 - ✓ 資安聯防：與成員進行**聯合資安演練**，分享防禦措施
 - ✓ 舉辦研討會：該協會**舉辦研討會**活動，以支持企業建立新的CSIRT，並提供企業資安改善建議措施
 - ✓ NCA出版物：**CSIRT Starter Kit (即CSIRT建置指引)**
 - ✓ Working Groups：NCA會員彼此可以與其他任何會員組成一個工作小組，彼此互相解決問題

日本CSIRT協會成員

■ 日本CSIRT協會成員(Nippon CSIRT Association, NCA)

SONY-JP-SIRT	SONY Japan Security Incident Response Team
SPSV-CSIRT	Sony Payment Services CSIRT
SRIG-CSIRT	Sumitomo Rubber Industries Group Computer Security Incident Response Team
SSNB-CSIRT	SBI Sumishin Net Bank Computer Security Incident Response Team
START	Symantec Tactical and Advanced incident Response Team
STARTIA-CSIRT	STARTIA GROUP Computer Security Incident Response Team
SUMISEI-CSIRT	SUMISEI Computer Security Incident Response Team
SUMITEM-CSIRT	SUMITEM Computer Security Incident Response Team
SuMiTPFC-CSIRT	SuMiTPFC Computer Security Incident Response Team
SURUGA CSIRT	SURUGA bank CSIRT
SWC-CSIRT	The Sumitomo Warehouse Co., Ltd. Computer Security Incident Response Team
TAKENAKA-SIRT	TAKENAKA Security Incident Response Team
TC-CSIRT	Tokyo Century Computer Security Incident Response Team
TDC-CSIRT	TDC-CSIRT
TDU-CSIRT	Tokyo Denki University CSIRT
TEIJIN-CSIRT	TEIJIN Computer Security Incident Response Team
TEPCO-SIRT	TEPCO Security Incident Response Team
TG-CSIRT	TOKYO GAS CSIRT
TIS-CSIRT	TIS-CSIRT
TKK-CSIRT	TOKYU CORPORATION-CSIRT
TMC-SIRT	Toyota Motor Corporation Security Incident Response Team

NCA成員行業別

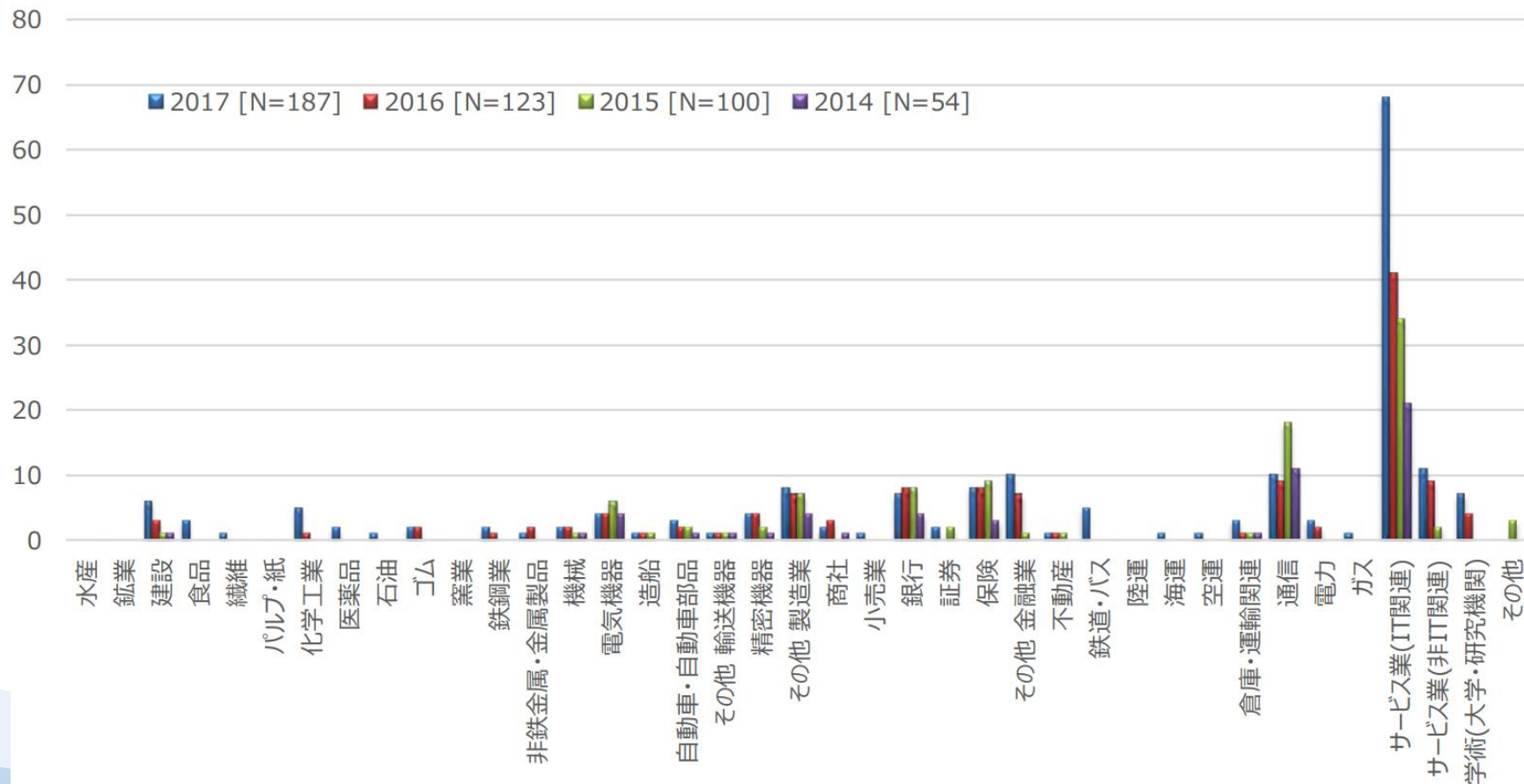


図 1 : 加盟組織の業種

來源 : http://www.nca.gr.jp/imgs/nca_teams_2017.pdf

小結

2015年日本政府制定相關的網路策略指導方針，鼓勵日本企業考慮設置CSIRT團隊，且同年度日本發生民眾個資的大規模外洩事件，刺激了日本企業紛紛建立企業內CSIRT團隊。

■我們應仿效日本CSIRT聯盟之精神，以利資安聯防

1. 向台灣民間企業推廣資安通報應變機制之重要性
2. 輔導企業建置CSIRT
3. 廣邀台灣CSIRT加入台灣CERT/CSIRT聯盟

TWCERT/CC 角色

與國外資安組織互惠合作及情資共享，並加速事件通報與協處，提升台灣整體資安聯防能量。

國外



國內

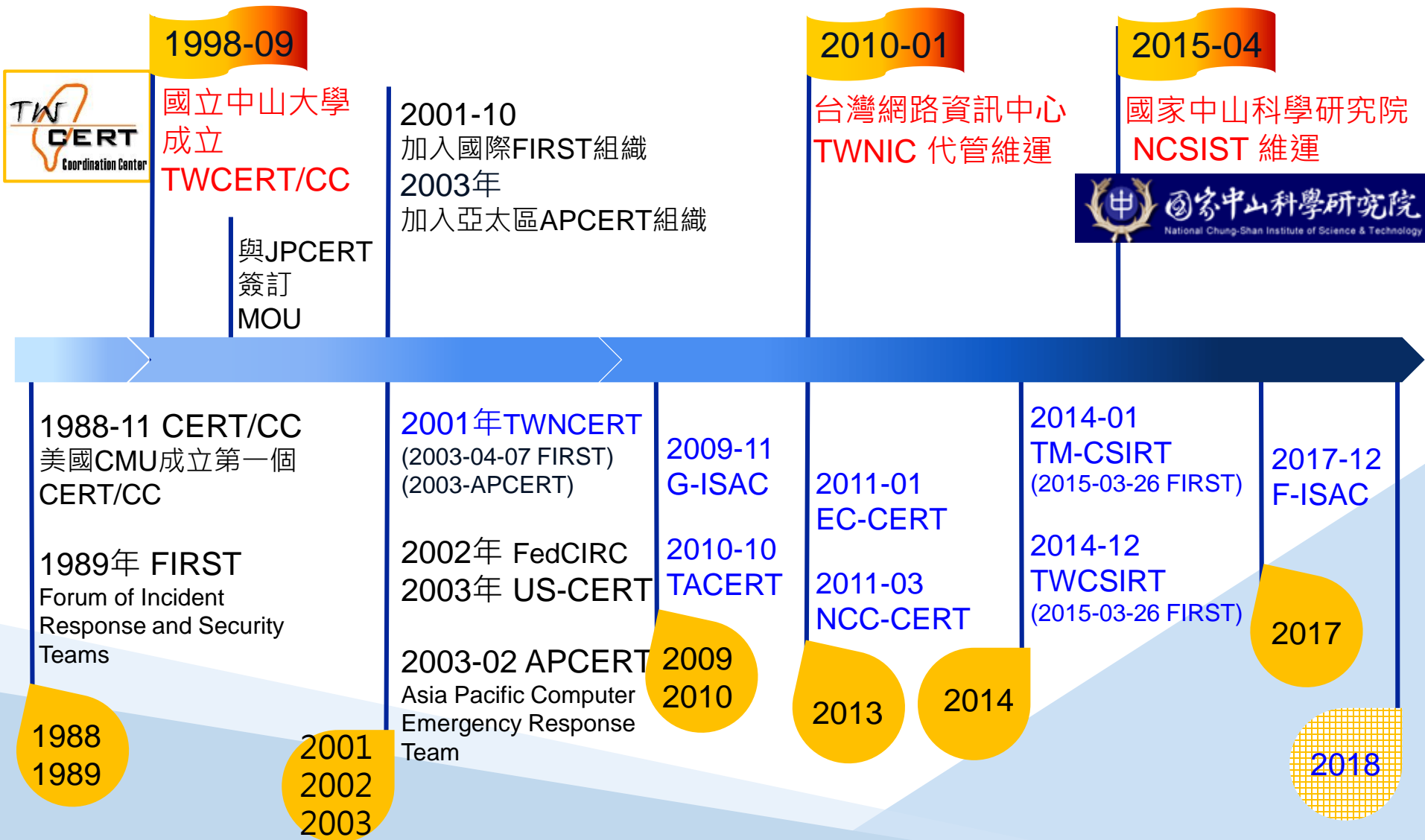


介接國內資安應變組織，強化資安事件處理能量，縮短應變時效。

負責推動國內民間資安事件通報處理、舉辦資安宣導活動。

三、TWCERT/CC提供的服務

TWCERT/CC 歷史沿革



TWCERT/CC業務

■ 應變協調

協助國內企業/產業公會成立CERT/CSIRT，建立資安事件處理團隊，協調國內外資安事件通報與應變處理。

■ 交流合作

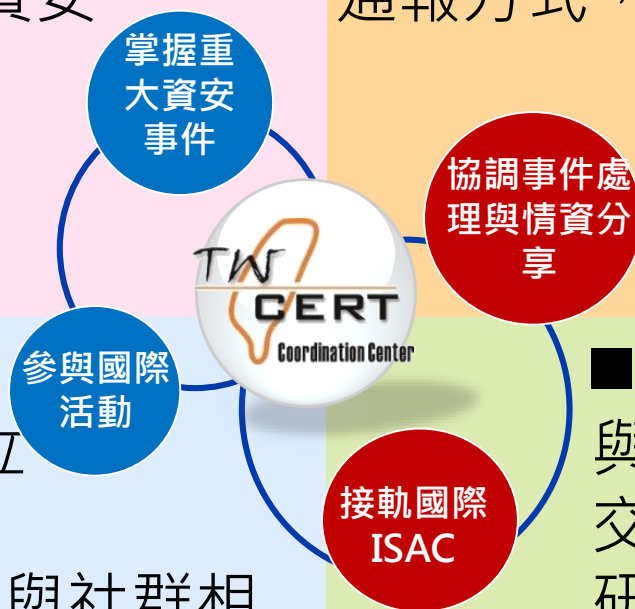
與國際CERT組織建立雙邊合作關係，參與國際與國內資安組織與社群相關活動，發表資安研究報告，掌握資安最新發展趨勢。

■ 通報處理

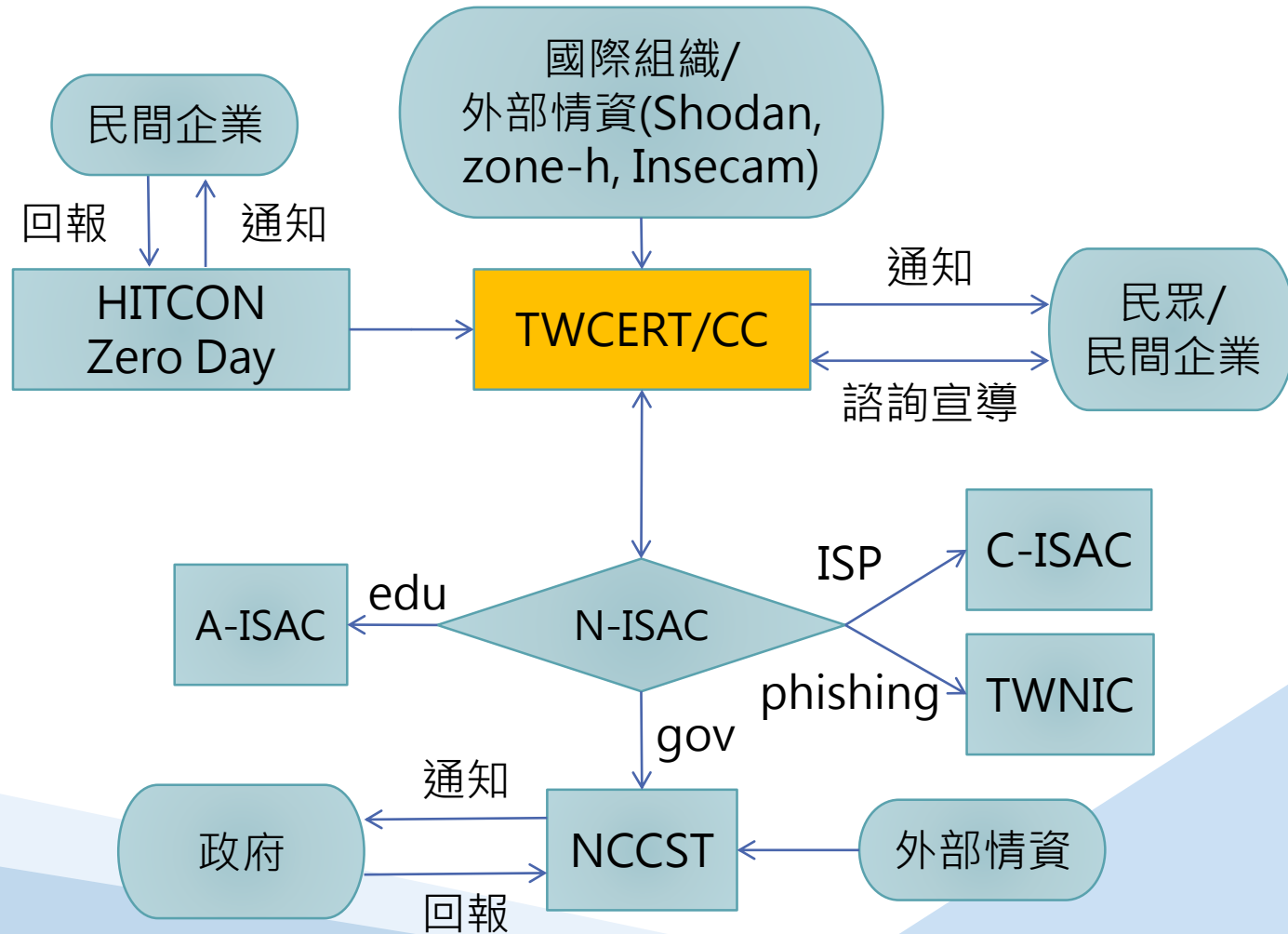
提供民間企業團體和個人多元通報方式，根據事件緊急的程度給予相應的技術諮詢、處置建議與協助。

■ 情資發佈

與國際資安組織合作交流分享情資，彙整研析追蹤、掌握國內外重大資安事件發展，推測研判網路威脅態勢，提供決策單位參考。



通報協處流程



官網、電子郵件、電話多元通報管道



官 網： www.cert.org.tw

電 話： 0800-885-066
(02)2377-6418

電子信箱：twcert@cert.org.tw

官網一般通報介面

官網進階通報介面

官網一般通報介面

通報人（機關）：

例：TWCERT/CC

聯絡電話：

例：02-23776418 #212

電子郵件：

例：twcert@cert.org.tw

IP位置：

例：127.0.0.1

+

網域名稱：

例：<https://www.twcert.org.tw>

+

事件說明：

官網進階通報介面 (1/2)

步驟 1：填寫資安事故基本資料

通報人（機關）：

通報人（機關）

聯絡電話：

聯絡電話

電子郵件：

電子郵件

受影響設備資料

已裝置之安全機制：

IP位置：

例：127.0.0.1

+

網域名稱：

例：https://www.twcert.org.tw

+

設備廠牌、型號：

設備廠牌、型號

已裝置之安全機制：

防火牆：

防火牆

防毒軟體：

防毒軟體

入侵偵測系統：

入侵偵測系統

入侵防禦系統：

入侵防禦系統

其他：

其他

官網進階通報介面 (2/2)

步驟 2：評估事件影響等級

機密性衝擊：

國家機密資料遭洩漏

完整性衝擊：

國家重要資訊基礎建設系統或資料遭竄改

可用性衝擊：

國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作

跨單位衝擊：

衝擊之單位影響國家重要資訊基礎建設系統

步驟 3：資安事故發生過程

事件分類：

未知

事件說明：

應變措施：

TWCERT/CC對通報內容之安全管控

■ 通報內容接收

- 通報網站採用SSL加密機制，可提供安全的通報平台。
- 提供PGP加密公鑰，若企業機關(構)或民眾有機敏資訊欲提供時，可透過電子郵件並使用PGP加密方式通報。

■ 通報內容處理

- 通報網站管理及資料庫內容的存取控制僅限本中心通報應變組人員。

■ 通報情資分享

- 事件分析後，僅針對入侵手法、攻擊特徵進行保留，對於企業機關(構)及民眾需保護的資料及隱私將去識別化，不擅自對外提供或公開。
- 報告完成後，將與當事人確認內容是否合宜，並於當事人同意後始能提供第三方單位參考運用。

TWCERT/CC服務項目

■ 情資整合

TWCERT/CC平時除了主動蒐整國內外資安情資外，亦與國內外資安組織進行情資交流，並將最新情資發布於官網及FB。

The screenshot shows a news article on the iThome website. The title is "【MIS必看】WannaCry勒索病毒猖獗！上班第一天如何處理病毒未爆彈？TWCERT/CC教你6步驟自保". The article text begins with "WannaCry事件發生後的第一個上班日，也就是星期一，恐怕才會有企業災情發生。因此，TWCERT/CC工程師也緊急測試目前各方提出的預防方法，整理了一個6步驟企業自保策略。". Below the article, there is a social media share bar and a comment section. The TWCERT/CC logo and name are visible in the bottom left corner of the screenshot.

The screenshot shows an email from TWCERT/CC. The subject is "各位台灣CERT/CSIRT的同仁您好，我是TWCERT/CC，與您分享USCERT最新分享之Wannacry勒索軟體之STIX情資". The email body contains the following text: "各位台灣CERT/CSIRT的同仁您好：我是TWCERT/CC分析師。在此分享USCERT對這次Wannacry勒索軟體事件，16日提供之STIX(如附件)與參考連結。Indicators Associated With WannaCry Ransomware". There is a "Description" section that reads: "Initial reports indicate the hacker or hacking group behind the WannaCry campaign is gaining access to enterprise servers through the exploitation of a critical Windows SMB vulnerability. Microsoft released a security update for the MS17-010 vulnerability on March 14, 2017. Additionally, Microsoft released patches for Windows XP, Windows 8, and Windows Server 2003 operating systems on May 13, 2017. According to open sources, one possible infection vector may be through phishing." A "參考連結" (Reference link) is provided: "https://www.us-cert.gov/ncas/alerts/TA17-132A". The email concludes with "以上 感謝您" and "敬祝 平安".

TWCERT/CC服務項目

■ 教育訓練

企業組織內部應定期舉辦資安教育訓練，提升員工資安意識，TWCERT/CC亦協助企業舉辦資安教育訓練，分享近期資安威脅及防護作法。



TWCERT/CC服務項目

MARS

為了避免機密性資料外洩，TWCERT/CC與國家高速網路與計算機中心合作開發惡意樣本檢測平台(Malware Analysis & Report System)，提供惡意樣本上傳檢測，並於10分鐘內可取得檢測報告。

The screenshot shows the MARS web interface for uploading malware samples. The page title is "惡意樣本檢測系統" (Malware Analysis & Report System). It includes navigation links for "惡意樣本上傳", "檢測進度查詢", "使用說明及規範", and "常見疑難". The main section is "惡意樣本上傳" (Malware Sample Upload). It features a system reminder: "系統提醒: 您所上傳的檔案可於 10 分鐘內完成檢測。" (System reminder: Your uploaded files can be scanned within 10 minutes). Below this, there are instructions for file types: "檔案上傳 (必須欄位, 限制20MB內, 可接受檔案類型: scr, ppt, doc, pdf, xls, xlsx, xlm, xltm, pptx, pptm, potm, docx, docm, dotm, exe, msi, dll, js, vbs, sys, bat, com, htm, html, odt, odp, ods, odg, oob, zip)(內含檔案數量上限為10個)" (File upload (required field, limited to 20MB, supported file types: scr, ppt, doc, pdf, xls, xlsx, xlm, xltm, pptx, pptm, potm, docx, docm, dotm, exe, msi, dll, js, vbs, sys, bat, com, htm, html, odt, odp, ods, odg, oob, zip) (maximum number of files included is 10)). There is a "選擇檔案" (Select file) button and a note: "未選擇任何檔案" (No files selected). A ZIP password field is present with the instruction: "ZIP密碼 (非必填欄位, 若您上傳的檔案為ZIP檔, 且有使用密碼加密, 請於本欄位填入密碼以利系統將檔案解壓縮, 若無則不需填寫, 請確認密碼無誤, 若密碼錯誤導致無法正確檢測檔案, 本系統不負相關責任。)" (ZIP password (optional field, if you upload a ZIP file and use password encryption, please enter the password in this field to facilitate system decompression, if none, no need to fill, please confirm the password is correct, if the password is wrong and causes the file to be incorrectly scanned, the system is not responsible). Below the ZIP password field is an "E-mail" field with the instruction: "E-mail (非必填欄位, 如需本中心主動寄送檢測結果給您, 請填寫電子郵件, 若無填寫則請自行到檢測進度查詢頁面取得檢測結果。)" (E-mail (optional field, if you need the center to actively send you the scan results, please fill in your email, if not, please go to the scan progress query page to get the results). There is also a "備註" (Remarks) field with the instruction: "備註 (非必填欄位, 限200字元, 供您備人筆記, 會於查詢及寄送檢測結果時提供備註給您)" (Remarks (optional field, limited to 200 characters, for your notes, will be provided when you query and receive scan results). At the bottom, there are "取消送出" (Cancel) and "確認送出" (Confirm) buttons, with a note: "※點選確認送出則視為同意使用說明及規範" (Clicking confirm submit is considered agreement to the terms and conditions). Footer information includes: "請使用Chrome、Safari、Firefox、Edge或IE 10瀏覽本站, 以獲得最佳顯示" (Please use Chrome, Safari, Firefox, Edge or IE 10 to browse this site for the best display), "惡意樣本檢測系統為台灣電腦網路危機處理暨協調中心及財團法人國家實驗研究院國家高速網路與計算中心共同提供之線上惡意樣本分析服務。" (The malware sample detection system is a joint service provided by the Taiwan Computer Network Crisis Management and Coordination Center and the National Experimental Research Institute of National High-Speed Network and Computing Center), "免付費服務電話: 0800-885-066", "E-Mail: twcert@cert.org.tw", "Website: https://www.twcert.org.tw", and "Copyright © TWCERT/CC 台灣電腦網路危機處理暨協調中心 1998-2017".

The screenshot shows the "檢測進度查詢" (Detection Progress Query) page. It features a search bar with the event ID "TWCERT-MAL-20170531133634KEGPb" and a search button. Below the search bar is a table with the following data:

檔名	事件編號	上傳時間	檢測進度
TreeSizeFreeSetup.exe	TWCERT-MAL-20170531133634KEGPb	2017-05-31 13:37:00	檢測完成

Below the table, there is a "初步檢測結果" (Preliminary Detection Results) section. It states: "61 家防毒軟體中, 有 0 家檢測到該檔案為惡意樣本。" (In 61 antivirus software, 0 detected the file as a malware sample). There is a "檢測結果" (Detection Results) section with a "下載檢測報告(PDF)" (Download Detection Report (PDF)) button. To the right of this section is a traffic light icon showing a green light, labeled "低風險" (Low Risk). Below the traffic light, there is a "檔案資訊" (File Information) section with the following details:

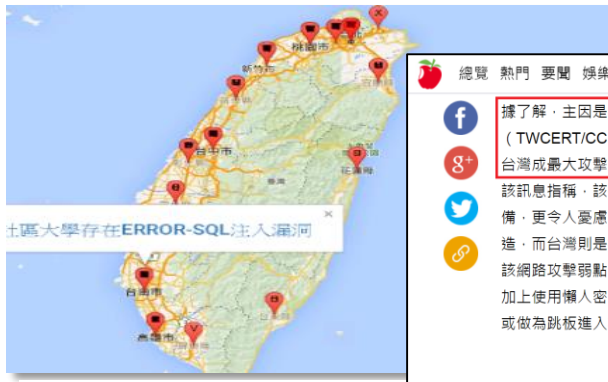
- SHA256: 570e6e029a6698eacc0d417966d1555f3f123ac95f71159bb38ed52d4507e
- SHA1: 441f439910fa9f13a33f9b19f99979628232a365
- MIME TYPE: application/x-pe-app-32bit+386
- MD5: 17ca6530ab4454aee0c2a63a7f9639f4

Below the file information, there is a "風險值 (最高為100, 風險值越大則代表該檔案為惡意的可能性越高)" (Risk Value (Maximum 100, the higher the risk value, the higher the possibility of the file being malicious)) section. It includes a "風險值範圍: 0~25為低風險; 30~60為中風險; 70~100為高風險" (Risk value range: 0~25 is low risk; 30~60 is medium risk; 70~100 is high risk) and "檔案風險值: 0" (File risk value: 0). At the bottom, there are two sections: "系統登錄檔行為(+)" (System log behavior (+)) and "檔案存取行為(+)" (File access behavior (+)).

情資發布-威脅預警情資

網路威脅態勢

彙整、研析及追蹤國內外重大資安事件發展，研判網路威脅態勢



威脅情資分佈圖

條件搜尋

總覽 熱門 要聞 娛樂 世足 國際 財經 副刊 體育 地產 論壇與專欄

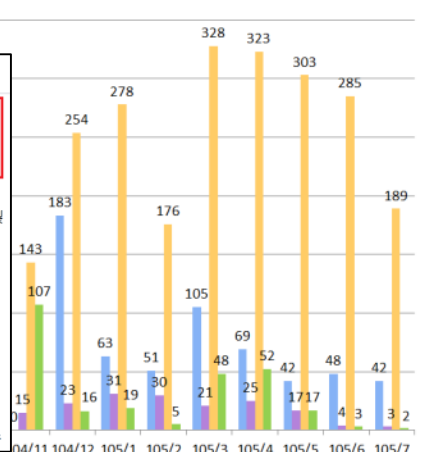
據了解，主因是在2017年4月，台灣電腦網路危機處理暨協調中心 (TWCERT/CC) 發布一項資安訊息：「殭屍網路Amnesia專門感染Linux系統，台灣成最大攻擊來源國」，此訊息正式點燃了金管會的「潛在憂慮」。

該訊息指稱，該殭屍網路的惡意程式，可繞過防護系統檢測，直攻感染DVR設備，更令人憂慮的是，受感染的DVR設備全是中國一家「TVR同為數碼」公司製造，而台灣則是擁有最多該公司DVR設備的國家。

該網路攻擊弱點，是DVR廠商為了方便維護作業都留有「後門」(遠端連線)，加上使用懶人密碼，駭客可透過遠端連線「後門」，直接進入內網，竊取個資，或做為跳板進入其他內部系統。

清查現況規範安控

金管會收到該訊息後，雙管齊下防堵，一是全面清查各銀行現況，二是要求銀行



國外合作交流 威脅警訊

NCCIC US-CERT

Distributed as TLP: GREEN

Malware Initial Findings Report (MIFR) - 10073583
2016-08-15

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. This DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise. This document is marked TLP: GREEN. Recipients may disseminate TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. For more information on the Traffic Light Protocol, see <http://www.us-cert.gov/ncas/tlp>.

This report contains preliminary analysis and is not intended to be a complete description of the submitter's attack capabilities. Results may be incomplete due to the inherent complexity or ability to perform against analysis techniques. If additional information is required, please contact the US-CERT Security Operations Center using the information at the end of this report.

Summary

Description

Analysis Environment: 32_bit_windows_7

One Microsoft Word Document (something.docx) was submitted for analysis. The Microsoft Word Document contains a malicious VBA coded macro. When the user activates the malicious content the malware drops a VBScript file and calls out to a domain (www.a300e.com).

Files

Processed: 2
1000532a30e00701107f0d40e10c (something.docx)
a300e320a4661660201f00e0e2170c (14176.vbs)

Domains Identified

1
www.a300e.com

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

14 September 2015

Alert Number: 20150914-001

Please contact the FBI with any questions related to this Private Industry Notification Report at either your local Cyber Task Force or FBI C/Watch.

Email: ciwnot@fbi.gov
Phone: 1-855-292-3937
Local lead office: www.fbi.gov/contact-us/field

Update on September 11 Cyber Threats from ISIL-Sympathetic Hacking Group Islamic Cyber Army

This is an update to FBI 20150910.

Summary

On 11 September 2015, INHOA's in a contract role supporting the Iraq advised that the ISIL, via their commercial (non) military unit, re-identified as a result of a compromise by the ISIL-sympathetic hacking group "Islamic Cyber Army" (ICA). Testers probed for ICA indicator threats of back-gateways government back site to compromise the addresses of the terrorist attacks. The USDOJ Web site was targeted by it as for computer intrusion on 11 September.

Technical Details

through analysis of access and network connection logs, it was determined that a coordinated intrusion activity, including web site defacements, from addresses within the following of block:

IP Range: 37.218.0.0 - 37.218.255.255
Net name: KW-ATC-20120412
Description: Kuwait Telecommunication Company (Kuwait Association)
Country: Kuwait (KW)

FBI FLASH

FBI LIAISON ALERT SYSTEM #A-000049-MW

The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as defined in 42 USC § 10617.

This FLASH has been received TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as peers within the broader sector or community, but not via publicly accessible channels.

Summary

The FBI is providing the following information with HIGH confidence:

The FBI has obtained information regarding a group of cyber actors who have conducted an access intrusion and remotely identifiable information (RIF) from government networks through cyber espionage. Analysis of malware sample is amount of the computer network exploitation activities emanated from Iran and China.

The tools used in the attack were referenced in open source reports on Deep Panda. This group has previously used Adobe Flash files via exploits in order to gain initial access to victim networks. Information obtained from victim indicators that it was a primary target. The FBI notes that since RIF has been used in other instances to target or otherwise facilitate various malicious activities such as financial fraud though the FBI is not aware of such activity by this group. Any activity related to this group detected on a network should be considered an indication of a compromise requiring extensive mitigation and contact with law enforcement.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

28 JULY 2016

Alert Number: MC-000077-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact FBI C/WATCH immediately. Email: ciwnot@fbi.gov
Phone: 1-855-292-3937

Identification of ransomware variant called Lucky

Summary:

The Lucky ransomware is a ransomware variant, which has extensively utilized open source tools to determine network files that download and execute code capable of encrypting files. The ransomware is a variant of the ransomware known as Lucky. Encrypted files are renamed with a unique hexadecimal filename and receive the "Lucky" extension. Each indicator containing encrypted files represents the source of an encrypted file. It is possible without data backup or restoration of the private files to the well implemented, strong encryption. While payment of the ransom may result in receipt of the valid private key, disabling decryption of the targeted files, the FBI does not recommend the victim pay the ransom.

Technical Details:

In early 2016, a decryption ransomware variant, Lucky, was observed affecting financial institutions in the United States, New Zealand, Australia, Germany, and the United Kingdom. It propagates through open source tools that include malicious Microsoft Office documents, PDF files, or compressed archives (e.g., ZIP, JAR). The malicious vectors are similar to the Lucky ransomware and may include malicious attachments or open source code. The ransomware variant is identified as Lucky File. Lucky has also been distributed via the Network and Security response file search based on an offline model. The availability of such files is the ransomware variant.

情資發布-資安訊息

資安新聞 駭侵事件 活動訊息

The screenshot displays three overlapping views of the CERT website. The leftmost view shows the '資安新聞' (Security News) section with a list of articles. The middle view shows the '駭侵事件' (Incidents) section with a list of security incidents. The rightmost view shows the '資安活動' (Security Activities) section, featuring a calendar for January 2018 and a list of events.

事件日期	標題
2018-01-12	Wi-Fi聯盟推出具有新安全功能的(WPA3)協議
2018-01-11	日本引進高階學習AI，防範網路攻擊
2018-01-10	台灣資安協會舉辦的資安安全，針對網路App，經驗分享
2018-01-10	企業應於有風險位轉型 增資安防護措施
2018-01-10	強化內線偵查 金融資安中心應辦
2018-01-10	資安會公開外幣 銀行不得買賣比特幣
2017-12-18	提高網路位置精準度，駭客利用精準度於12月成立資安協會贊助
2017-12-18	Akamai發布「2017年第三季網路趨勢報告—安全報告」
2017-12-18	宏碁將利用點點點非中央控制板
2017-12-18	臺巴酒店Wi-Fi漏洞利用 合作商業聯盟認證，商用駭客設備CPU攻擊

事件日期	標題
2018-01-12	你的物聯網設備被修改了嗎?小心,隱私被曝光
2017-12-25	資安公司 Fox IT 遭中國人攻擊,駭客組織宣稱「壹壹壹壹壹壹」
2017-11-23	Uber遭駭攻擊,5700萬乘客資料外洩
2017-11-21	美國內閣之神鬼降臨地獄駭客資料外洩
2017-11-15	美國聯邦政府Forever 21駭客使用卡資料外洩
2017-11-10	「加入LJNF會員,分享研究,即可獲得好康」,免費小遊戲,避免駭客攻擊
2017-11-07	KRACK Detector 駭客工具,可用來避免有心人士利用WPA2駭客進行KRACK攻擊
2017-10-26	IBM 公布駭客駭客駭客「Bad Rabbit」的 IoT更新,新增美國ThaCERT分析報告
2017-09-26	傳動會計師事務所遭駭,電子郵件被外洩
2017-09-11	利用Equifax駭客可能與Stuxnet有關,用戶應注意更新

事件日期	活動類型	標題	地點
2018-01-27	資安競賽	駭木 NSRA Hackathon 2018	臺灣台北
2018-01-19	研討會	HTCC Free Talk 2018- 網路 CPU 處理器的資安攻防	臺灣台北

資訊產品漏洞 及解決方案

The screenshot displays the '漏洞資訊' (Vulnerability Information) section of the CERT website. It features a table listing various security vulnerabilities and their solutions, along with a detailed article about VMware vulnerabilities.

發佈日期	標題
2018-01-12	Juniper 停機Junos OS、ScreenOS、Junos Space等網路設備管理軟體10個項漏洞
2018-01-10	Linux Kernel eBPF 檢點器存取控制出錯
2018-01-10	VMware 公布5款產品相關漏洞並推出大型更新
2018-01-09	防火牆系統Sonicwall 介電辦法遠端特種payload
2018-01-08	Schneider Electric 升級Pelco VideoXpert 企業版防止Directory Traversal不當存取
2018-01-06	全球CPU資訊Spectre與Meltdown 層層分析式漏洞威脅(更新技服中心資訊, 解決方案、影響資訊)
2018-01-06	Synology 升級MailPlus Server
2018-01-05	IBM更新WebSphere 底層資料洩露漏洞
2018-01-04	Mozilla 升級Thunderbird 解決RSS Feed 相關漏洞
2018-01-03	Samsung 氣管線線路用存取權SOP 改善保護權

VMWARE 公布5款產品相關漏洞並推出大型更新

VMware 於 2018 年 1 月 10 日 宣布 5 款 產品 相關 漏洞 並 推出 大型 更新。這些 漏洞 包括 在 VMware Workstation、VMware Player、VMware ESX/ESXi、VMware vCenter Server 和 VMware Horizon 中發現的漏洞。這些漏洞可能導致拒絕服務、信息洩露和系統損壞。VMware 建議用戶立即更新其產品以修補這些漏洞。

情資發布-資安刊物

資安電子報

<http://twcertcc.blogspot.tw/>



免費電子報訂閱

台灣電腦網路危機處理暨協調中心 - TWCERT/CC

2018年1月15日 星期一

107年1月份TWCERT/CC資安情資電子報

第1章、摘要

為提升我國民眾資安意識，TWCERT/CC於每月發布資安情資月報，月報中統整上月重要資安情資，包含TWCERT/CC近期動態、資安政策、資安趨勢、駭客攻擊事件、軟體漏洞及資安事件通報統計分析等資訊。

TWCERT/CC近期動態，本中心於上月參加「2018資安趨勢論壇」研討會，

在資安政策方面，台備駭客能量應構出為資安法契機，另銀行執行內裡，著重資安三重點，而為了防止洩密，印度令邊防兵則做信傳，另中國主辦世界互聯網大會，強調網路主權。資安趨勢方面，AKAMAI發布「2017年第三季網際網路現狀—安全報告」，另密碼規則的盲點與未來可能發展。

在駭客攻擊事件方面，資安公司Fox-IT遭中間人攻擊，部分網域資訊一度遭接管與攔截。

在軟體漏洞部分，D-Link升級DIR-605L韌體以解決HNP服務阻斷漏洞；VMware釋出4種升級韌體修補多組漏洞；Android被公布47漏洞，其中Janus能導致惡意通訊以系統身執行；Google更新Chrome修補37漏洞；Microsoft緊急修補Malware Protection Engine防止嚴重RCE事件接管系統權限；F5更新BIG-IP防止Double Free Memory與CCA2攻擊；OpenSSL公布2漏洞恐洩private key及Bypass加解密；Cisco及此二種產品通過POC被駭客駭取資料，另駭客安全更新；PostgreSQL初始化導致系統更新多數設備，防禦KRACK駭客系統PAN-OS阻擋組合式攻擊；IoT設備多版XenServer避免資安漏洞。

大學聖言樓中舉辦「離六 NISRA

術計劃、攻擊來源統計圖及攻擊類

掌握國際相關電郵帳號清單情資

關於我自己



台灣電腦網路危機處理暨協調中心 - TWCERT/CC

主辦推動資安事件通報、教學資源提供及相關宣導活動等多項工作，透過與國內外資安組織、學術機構、民間社群及私人企業多元合作，本中心將持續推動各項網路安全事務，以確保我國整體網路安全及關鍵資訊基礎設施之穩定可靠。

更多資訊請上官方網站：
<https://www.twcert.org.tw>

檢視我的完整簡介

資料目錄

▼ 2018 (1)

▶ 一月 (1)

107年1月份TWCERT/CC資安情資電子報

▶ 2017 (12)

▶ 2016 (3)

文章分類

資安情資月報

熱門文章

資安年報

2017資安年刊

- 3 | 前言
- 6 | 資安聯防新思維
- 7 | 台灣CERT/CSIRT聯盟
- 10 | 資安通報應變與情資分享機制
- 12 | 資安通報現況與案例
- 13 | 2017年資安通報現況
- 2 | 2017年資安通報案例
- 31 | 年度資安事件分析
- 32 | 網路監視器之資安風險
- 34 | 證券商DDOS攻擊勒索事件
- 37 | 勒索軟體攻擊事件與WANNACRY勒索軟體行為分析

- 40 | SASL認證暴力破解攻擊事件
- 42 | 遠東商銀SWIFT系統遭駭事件
- 45 | 網頁遭置換攻擊事件
- 49 | 情資交換平台TWCERT-ISAC
- 50 | 情資交換平台(ISAC)
- 50 | 惡意樣本檢測系統(MARS)
- 53 | 自動化資安通報系統
- 54 | 資安通報工單系統
- 49 | 合作交流與會議活動
- 22 | 國際資安組織交流成效分析
- 26 | 2017年台灣資安通報應變年會成果紀實
- 55 | 結語

2017 TWCERT/CC 資安年刊



2017資安年刊

前言

網路世界為人類帶來便利，相對而言也帶來了風險，因此資訊安全成了現今社會所關注的重要議題。資訊安全並沒有完成，則有可能發生許多不可預測的損失。身處網路資訊洪流中，從網路購物、金融、通訊、娛樂、教育、醫療、電訊、網路服務及各種應用等，資訊與網路已滲透到人類生活的各個角落，且多與國家安全息息相關。

為了提升我國資安意識，TWCERT/CC於民國87年11月由中山大學成立，民國99年1月由台灣網路資訊中心(Taiwan Network Information Center, TWNIC)接手經營。自103年8月起改由國家中山科學院承接，並於104年4月正式改組為「台灣網路資訊安全辦公室」下屬單位。為了提升台灣整體資安防護能力，台灣網路資訊處理暨協調中心(TWCERT/CC)主辦推動資安事件通報、資安教學資源提供及相關宣導活動等多項工作，藉由政府與民間團體與國內外CERT/CSIRT、資安組織、學術機構、民間社群及私人企業等多元合作，並進行資源整合，共同維護台灣網路安全。

隨著資安意識的普及，資安事件通報與資安事件處理，已成為資安防禦體系中不可或缺的一環。TWCERT/CC訂定通報機制，以處理各類資安事件之通報與處理，並提供多項情資、諮詢與通報服務。透過與國內外資安組織、學術機構、民間社群及私人企業等多元合作，以確保我國整體網路安全及關鍵資訊基礎設施之穩定可靠。

本報係由台灣網路資訊處理暨協調中心(TWCERT/CC)主辦推動資安事件通報、資安教學資源提供及相關宣導活動等多項工作，藉由政府與民間團體與國內外CERT/CSIRT、資安組織、學術機構、民間社群及私人企業等多元合作，並進行資源整合，共同維護台灣網路安全。

隨著資安意識的普及，資安事件通報與資安事件處理，已成為資安防禦體系中不可或缺的一環。TWCERT/CC訂定通報機制，以處理各類資安事件之通報與處理，並提供多項情資、諮詢與通報服務。透過與國內外資安組織、學術機構、民間社群及私人企業等多元合作，以確保我國整體網路安全及關鍵資訊基礎設施之穩定可靠。

1

情資發布-技術文件

CSIRT組織 技術文件/手冊

關於我們 資安情資 資安通報 民眾服務 資安資源

本中心為了讓台灣的企業組織/產業公會於建立電腦安全事件應變小組(Computer Security Incident Response Team, CSIRT)時，了解應處理的問題和界定的事項，並且提供在企業/產業中建立事件應變計畫時應遵循的程序，作為建立電腦安全事件應變小組時的參考，特制定此參考指引文件。

相關下載連結條列如下：

1. 民間企業組織/產業公會CSIRT建置實務指引(草案)v1.0
2. TWCERT資通安全通報應變作業綱要(草案)

若您有對此文件有疑問或建議，歡迎填寫問卷或來信本中心，我們將竭誠為您服務。



專題彙整分析 技術研究報告

資安技術研析

資安健檢與資安鑑識實務分析

摘要

TWCERT/CC 蒐整國內外資安健檢與鑑識相關作業程序、方法與常用之檢測輔助工具，研究相關的實作技術，並配合不同的受檢標的，於實務上規劃檢測實驗室之資安健檢與資安鑑識之施行方式。可提供各單位內部重要核心資訊系統，執行資安健檢作業確保核心系統的安全性，執行資安鑑識作業可協助各單位於資安事件發生時，釐清事件原因並進行風險控管，以減少災害損失，經由資安健檢與資安鑑識作業，來強化各單位之資通安全防護能力。

關鍵字：資安健檢、資安鑑識

資安技術研析

分散反射式阻斷服務(DrDoS)攻擊

分散反射式阻斷服務(DrDoS) 攻擊研析

TWCERT/CC
翁興國顧問

摘要

分散式阻斷服務(DDoS)攻擊，最近幾年已演化成向分散反射式阻斷服務(DrDoS)攻擊模式發展，攻擊規模逐年創新高且大多採用散播攻擊向量，已形成顯著的不對稱攻擊效果。

有鑑於 DrDoS 攻擊之演化趨勢，現階段尚有多種通訊協議後續可能被大幅利用，可演化出不同型態的 DrDoS 攻擊，本報告研析反射攻擊之發展趨勢與分類方法，以及 12 種以 UDP/TCP 為基礎之通訊協定的工作原理，並針對其應戰時可能的反射放大攻擊，評估後續可能發生之反射攻擊威脅，以與後續評估大量家用設備連上物聯網時，可能需面對之資安威脅及強化安全防護策略之參考。

關鍵字：分散式阻斷服務(DDoS)攻擊，分散反射式阻斷服務(DrDoS)攻擊、殭屍網路(Botnet)、放大節(Amplifier)、反射器(Reflector)

台灣電腦網路危機處理暨協調中心 - TWCERT/CC
8月22日

專題彙整分析 - ATM駭侵事件分析

近期台灣發生了ATM遭駭導致巨額現金遭竊之事件，也讓ATM相關資安議題在台灣浮上了水面，那國際上是否有類似的事件發生過呢？又該如何避免呢？本報告將針對近期發生的ATM駭侵事件進行分析。

第1章

台灣電腦網路危機處理暨協調中心 - TWCERT/CC
7月18日

專題彙整分析 - 勒索病毒個案探討及防範應變建議

勒索病毒個案探討及防範應變建議 近年來，國人電腦遭感染勒索病毒的數量快速上升，本章節中將分享一則遭勒索病毒勒索的個案，並介紹應如何防範。

關於我們 資安情資 資安通報 民眾服務 資安資源

遠東銀行遭駭事件惡意程式分析報告

類別：技術分析報告 / 創建日期：2017-10-31 15:33:35 / 最後更新：2017-11-01 09:32:04 / 瀏覽次數：201

本分析報告針對遠東銀行遭駭客人提單中，bitsran.exe、RSWoox.tmp、mmpeng.exe、BspIvov32.exe等惡意程式分析，其中bitsran.exe與RSWoox.tmp為惡意勒索程式，而mmpeng.exe與BspIvov32.exe為後門程式。

檔案下載

1. TWCERTCC-MIFR-2017007.pdf

資安情資發佈管道

Mailing List



Please Join Us!!



Facebook

台灣電腦網路危機處理暨協調中心 - TWCERT/CC

2018年1月15日 星期一

107年1月份 TWCERT/CC 資安情資電子報

第1章、摘要

關於我自己



Blog

台灣電腦網路危機處理暨協調中心 - TWCERT/CC

結論

隨著系統變得越來越複雜，針對相同性質企業組織/產業所進行大規模攻擊亦有越來越集中的趨勢，可預見的是幾乎沒有單一組織能夠完善一切安全措施來預防每一個潛在的資安事件。

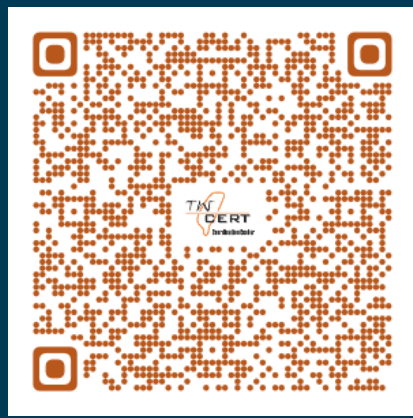
- 提升民間企業通報意願
(讓我們知道哪裡失火了)
- 體認網路攻擊技術係不斷演進，故需與其他CERT/CSIRT合作聯防
(哪裡窗戶沒關大家記得關、怎麼關)
- 需反覆精進通報機制與事件處理流程
(了解別人怎麼關，有更好的方法?)



達成高效益及高效率之事件處理與聯防體系!



資安月報訂閱



Thanks!

Q & A

Facebook

