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。

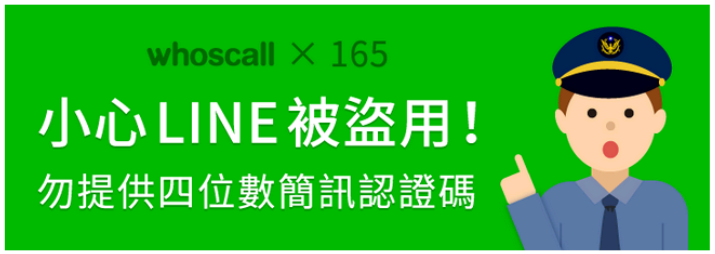
小心LINE帳號遭盜用，勿提供四位數簡訊認證碼

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

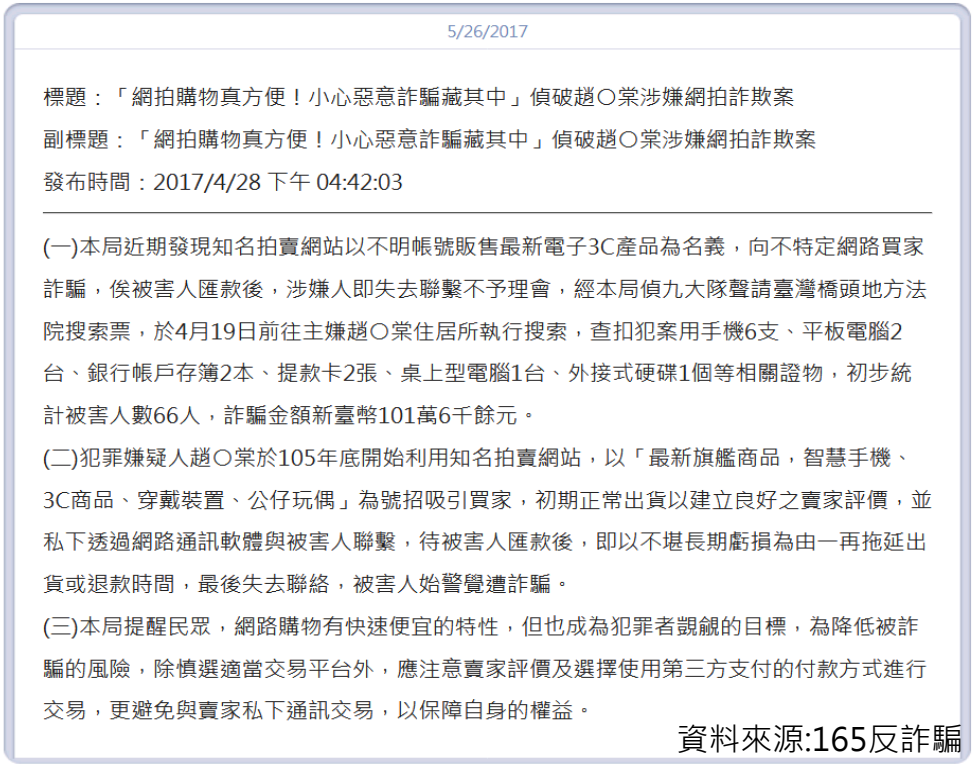
資訊安全與理財購物

■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

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的付款方式進行交易，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）	
「OOOOOOO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)

案例1:臉書的一頁式廣告詐騙(2/3)

#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

案例1:臉書的一頁式廣告詐騙(3/3)

VirusTotal檢測連結	偵測率	title	comment
https://www.virustotal.com/zh-tw/url/2a7949d541c0a80ebbde5cd91791b6db81283cbcf3dc78f84a19a132ed89f7c5/analysis/1522633190/	0 / 67	雙人按摩跳舞毯	廣告不實，說有切水
https://www.virustotal.com/zh-tw/url/45e4a798ff2a9c0325863c19618caf53cb409e1c6202bd0f7b9efb04f297beb8/analysis/1522633348/	0 / 67	內衣折扣店	none
https://www.virustotal.com/zh-tw/url/b6c9ec22b28a75c3db1a03a84be7aab43cbf79d3519d79b07942307fb608f34f/analysis/	5 / 67	HyperX大禮包	假冒知名實況主，並
https://www.virustotal.com/zh-tw/url/4b6349e433cb75d4b0f797694e05723ddc3101da9d8850bd78ccdd7a61b284ed/analysis/1522633506/	0 / 67	巧手折一折紙玩偶	實際收到貨品完全不
https://www.virustotal.com/zh-tw/url/123d4f2de0a771b9d72f1359bf3b99a0ff4f3482cdb3bb46e779c2896c8373f9/analysis/1522633543/	0 / 67	珠寶 手飾 開運飾品	我購買後卻不能退貨
https://www.virustotal.com/zh-tw/url/cea8dbbe809354c68473ed3f9ca35c001f1664620bac11414de70bc962c4ad2b/analysis/1522633578/	0 / 67	【官方正品】2018新款復	none
https://www.virustotal.com/zh-tw/url/41afe831afd830af28561882f92c440bec178cc71b4bea570dce0a00da7281a0/analysis/1522643876/	0 / 67	日本三豐游標卡尺	網站賣日本三豐游標
https://www.virustotal.com/zh-tw/url/3494663fac5764c737bfe4004575e2ef6393f38b5b82da4f06087cb67d65c264/analysis/1522643905/	0 / 67	大禾床飾	商品貨到收款，廣告
https://www.virustotal.com/zh-tw/url/c530a5e55564f670bccc391c512a18d4ad277ba13516a8bd21085d05befd9f57/analysis/1522643942/	0 / 67	官方3CE唇膏	用正版公司的影片匿
https://www.virustotal.com/zh-tw/url/05f364e17d9299c51287f7a8171eeb4b9a9c604a43faedaf4e712738c8910ec3/analysis/1522643974/	0 / 67	榮獲國家精品獎肯定：打	因為公司是大古鐵器

- 一頁式廣告連結存在資安風險比例偏低，國際CERT組織難協助移除
- 民眾防範方式：

1. 第三方支付機制，確認貨品無誤再付款
2. 詳閱社群媒體所宣告之隱私權政策，修改廣告偏好，並減少以社群媒體帳號登入其他服務。
3. 安裝廣告阻擋外掛程式，例如Adblock Plus或AdGuard，以阻擋已知的惡意廣告連結。
4. 主動取消追蹤該、檢舉粉絲團
5. 臉書有加入無店面公會，可協助調解消費糾紛

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

案例2:網站遭轉址服務利用的資安風險(2/5)

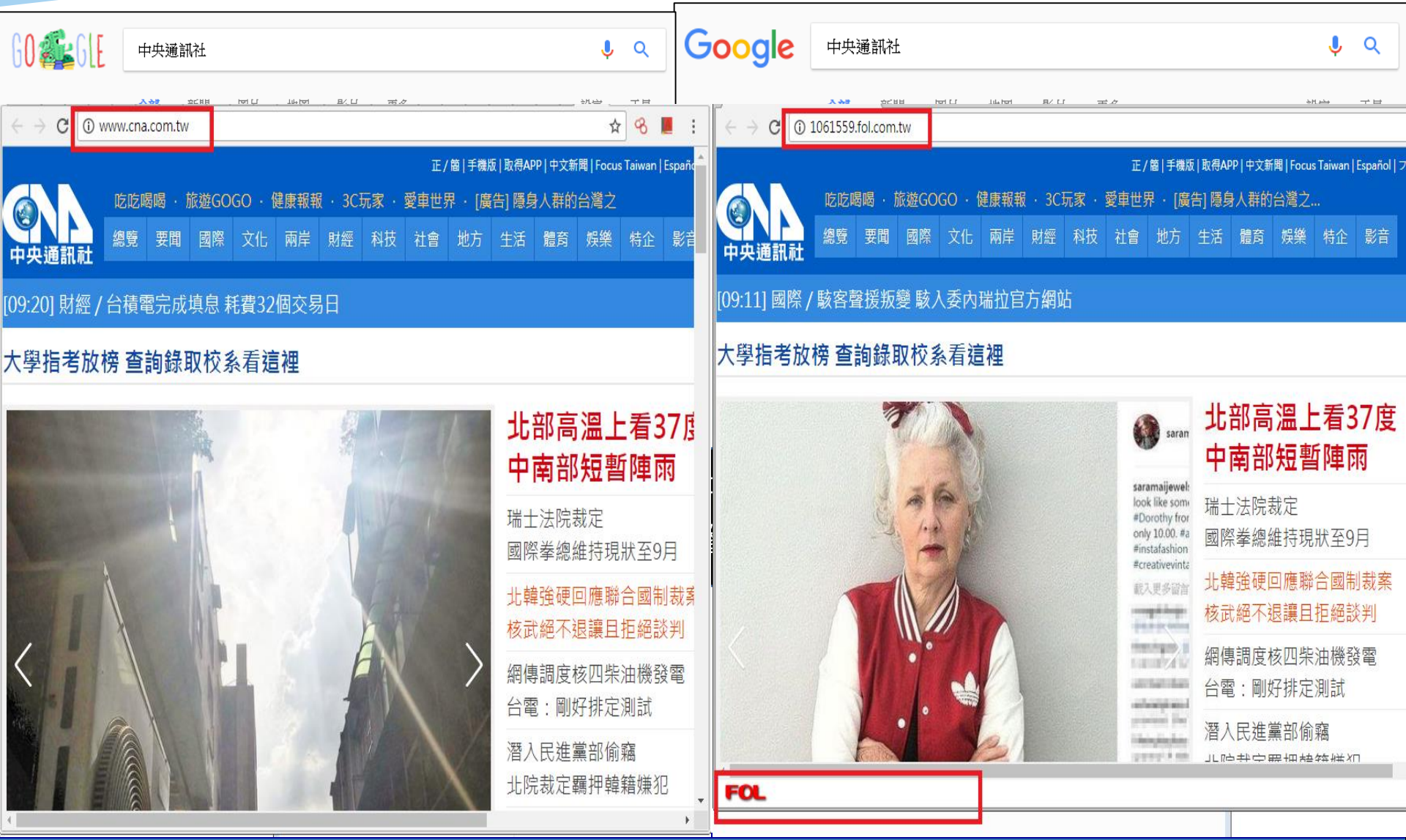
- 網路上有許多提供免費網域轉址服務的網站，為了獲取廣告收入
- 針對申請者的身分認證機制並不嚴謹，不經同意就可將知名網站加工轉換成其他網域
- 網站管理者通常不知道已經遭到利用作為其他用途或加入廣告頁框。


```
<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.0 Transitional//EN' 'http://www.w3.org/TR/REC-html40/loose.dtd'>
<html>
<head>
<title>[redacted]</title>
<meta name='keywords' content='[redacted]'>
<meta name='description' content=''>
<meta name='revisit-after' content='14 days'>
<meta name='robots' content=''>
</head>
<frameset rows='25,*' frameborder='NO' border='0' framespacing='0'>
<frame name='TOP_MENU' src='http://[redacted].ufc.com.tw/?PUT=ad' noresize scrolling='no'>
<frame name='MAIN' src='http://www.[redacted].com.tw'>
</frameset>
<noframes>
<body bgcolor='#FFFFFF' text='#000000'>
進入 <a href='http://www.[redacted].com.tw'>[redacted]</a>
</body>
</noframes>
</html>
```

案例2:網站遭轉址服務利用的資安風險(3/5)

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)



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

已知的漏洞，而非零時差攻擊（Zero Day Attack）。

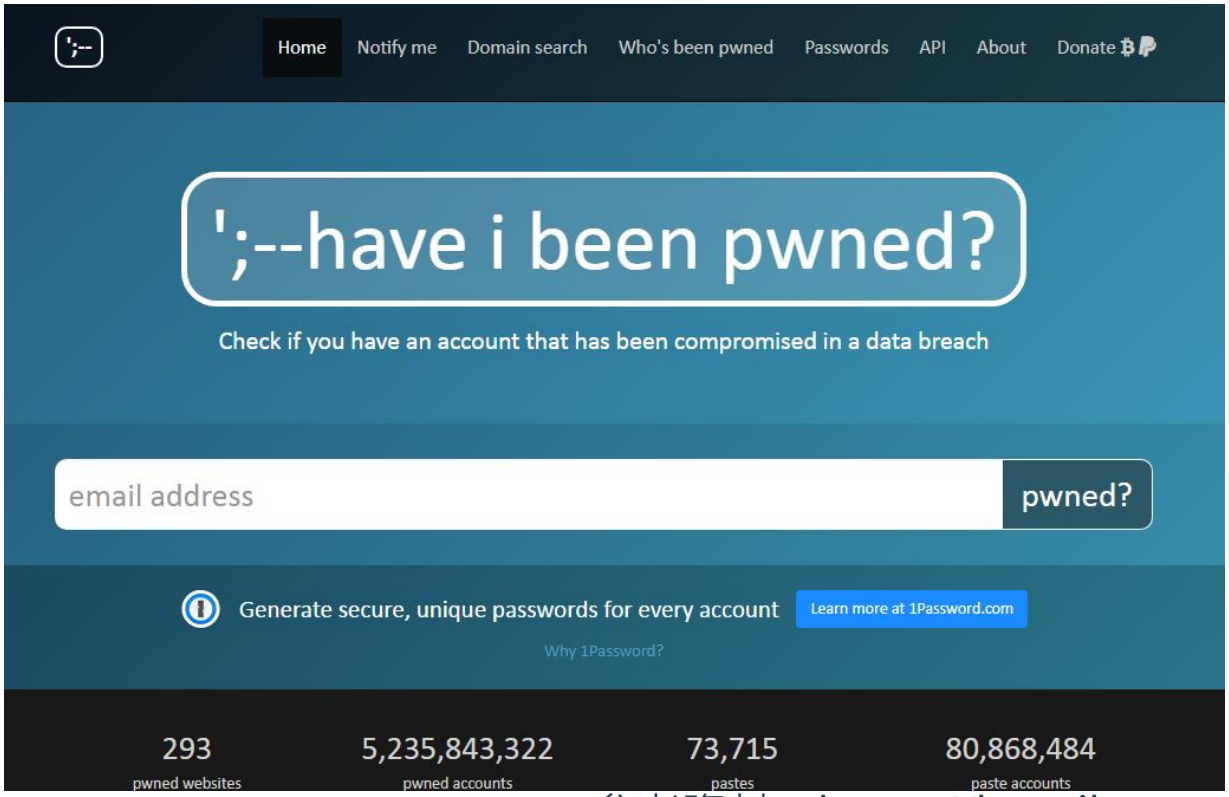
去（2017）年以來WannaCry和Petya勒索病毒攻擊事件肆虐全球，Equifax資料外洩事件也引發極大關注。要吸引媒體注意很容易，但這不應該是安全專業人士最應該擔心的威脅。

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[TWCERTCC-[redacted]]股份有限公司所屬電子郵件信箱已遭駭客入侵或鎖定。

日期： 11/17/17 13:24

收件者： [redacted]

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[redacted]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：「[redacted]」

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（常見的竄改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）。

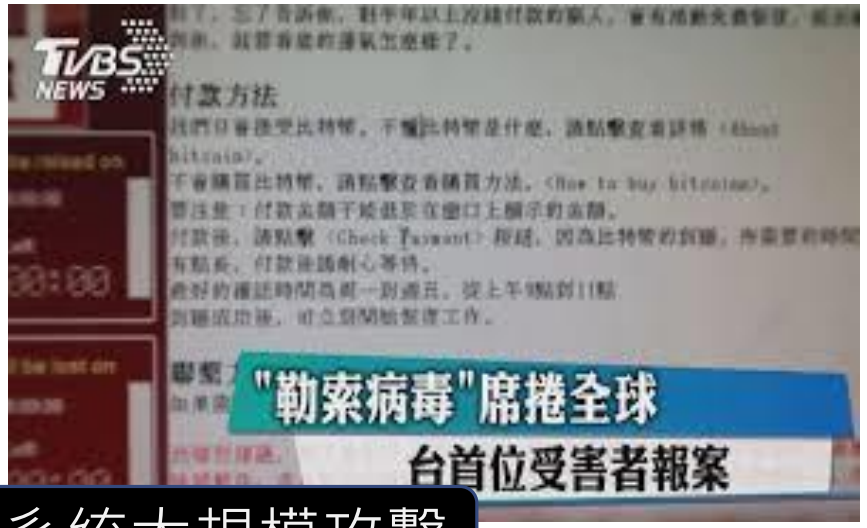
4.定期保持作業系統及防毒軟體更新。

若有任何疑問歡迎來電詢問。

GOOGLE IT!

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

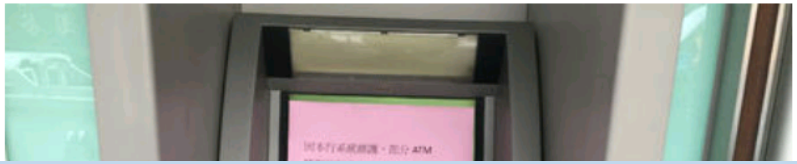
首頁 / 財經

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，請民眾注意。

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：編譯楊芙宜

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)

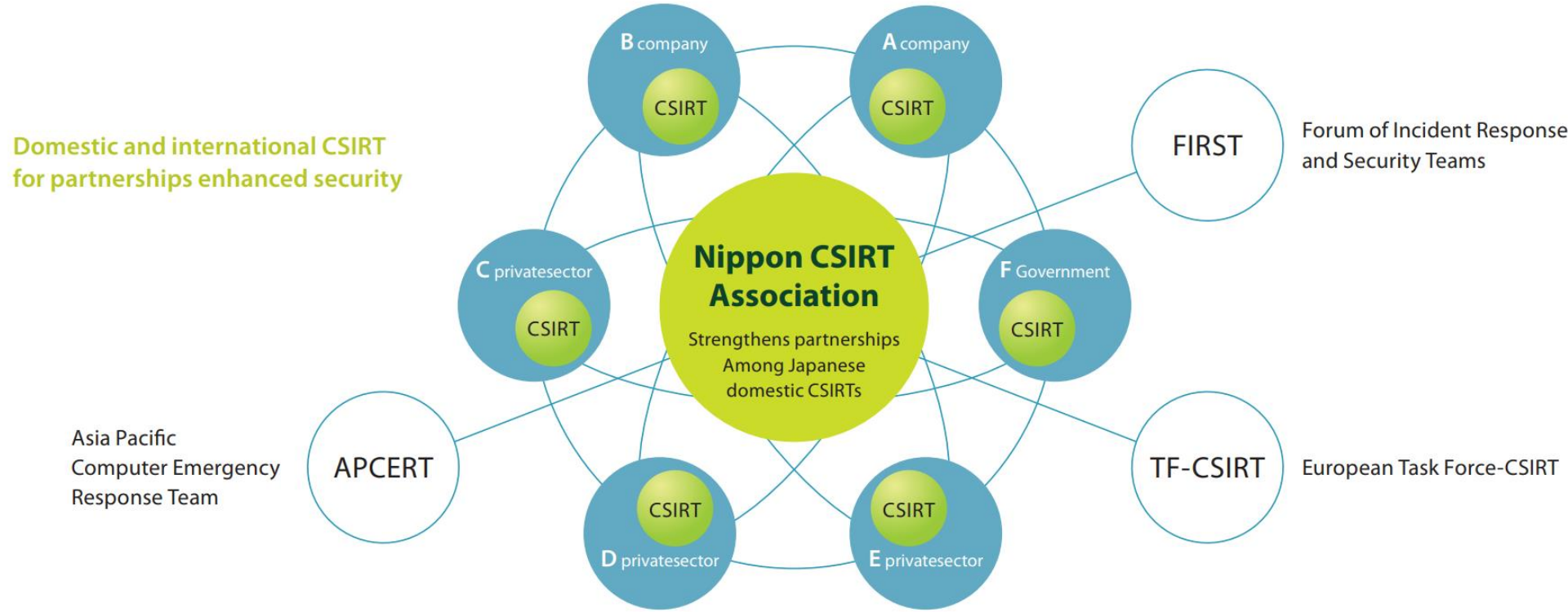
- 在國際上有關電腦緊急應變小組名詞，包括：
  - CERT or CERT/CC (Computer Emergency Response Team / Coordination Center)
  - **CSIRT (Computer Security Incident Response Team)**
  - IRT (Incident Response Team)
  - CIRT (Computer Incident Response Team)
  - SERT (Security Emergency Response Team)
- 功能

  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 Securitey 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

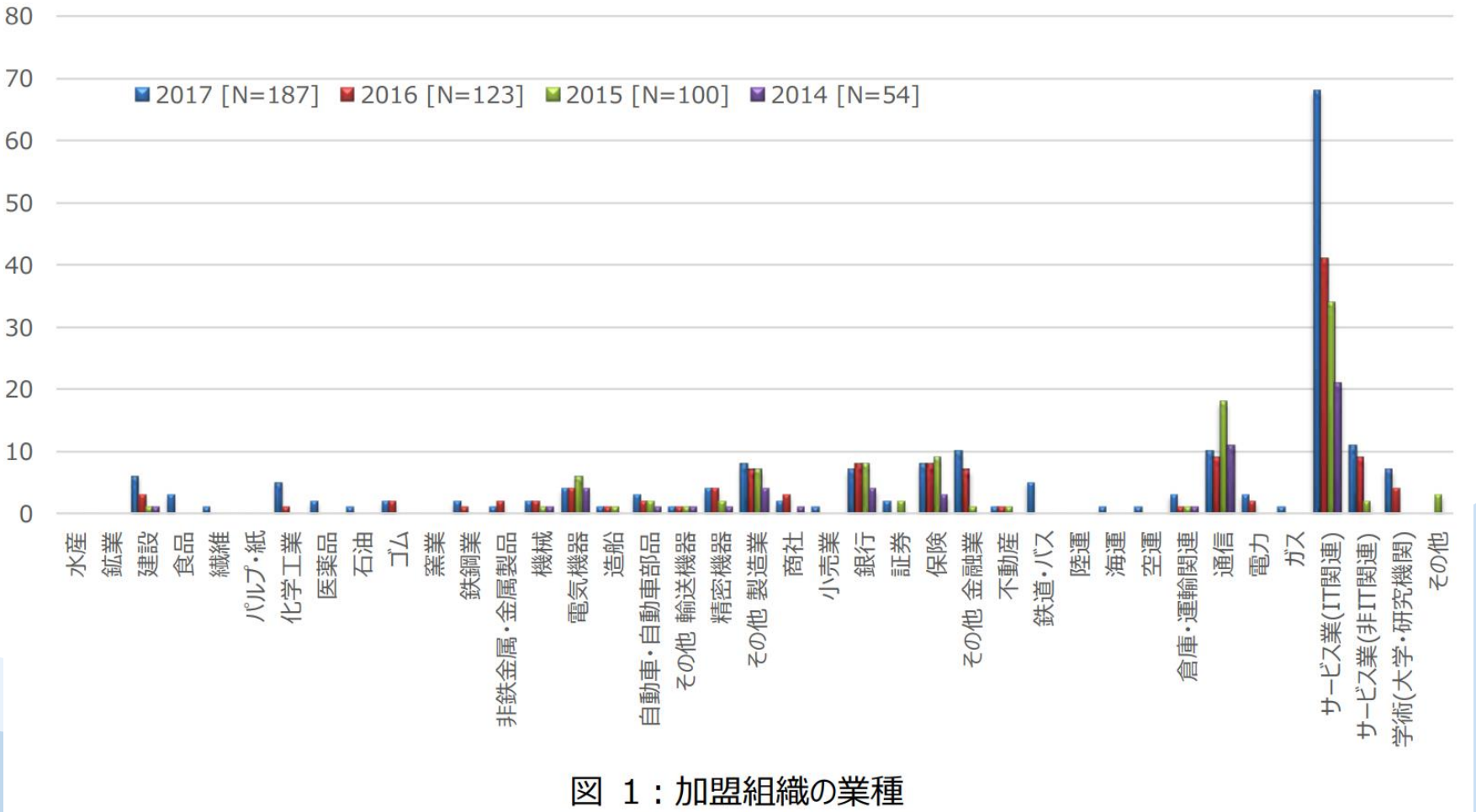


図 1：加盟組織の業種

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

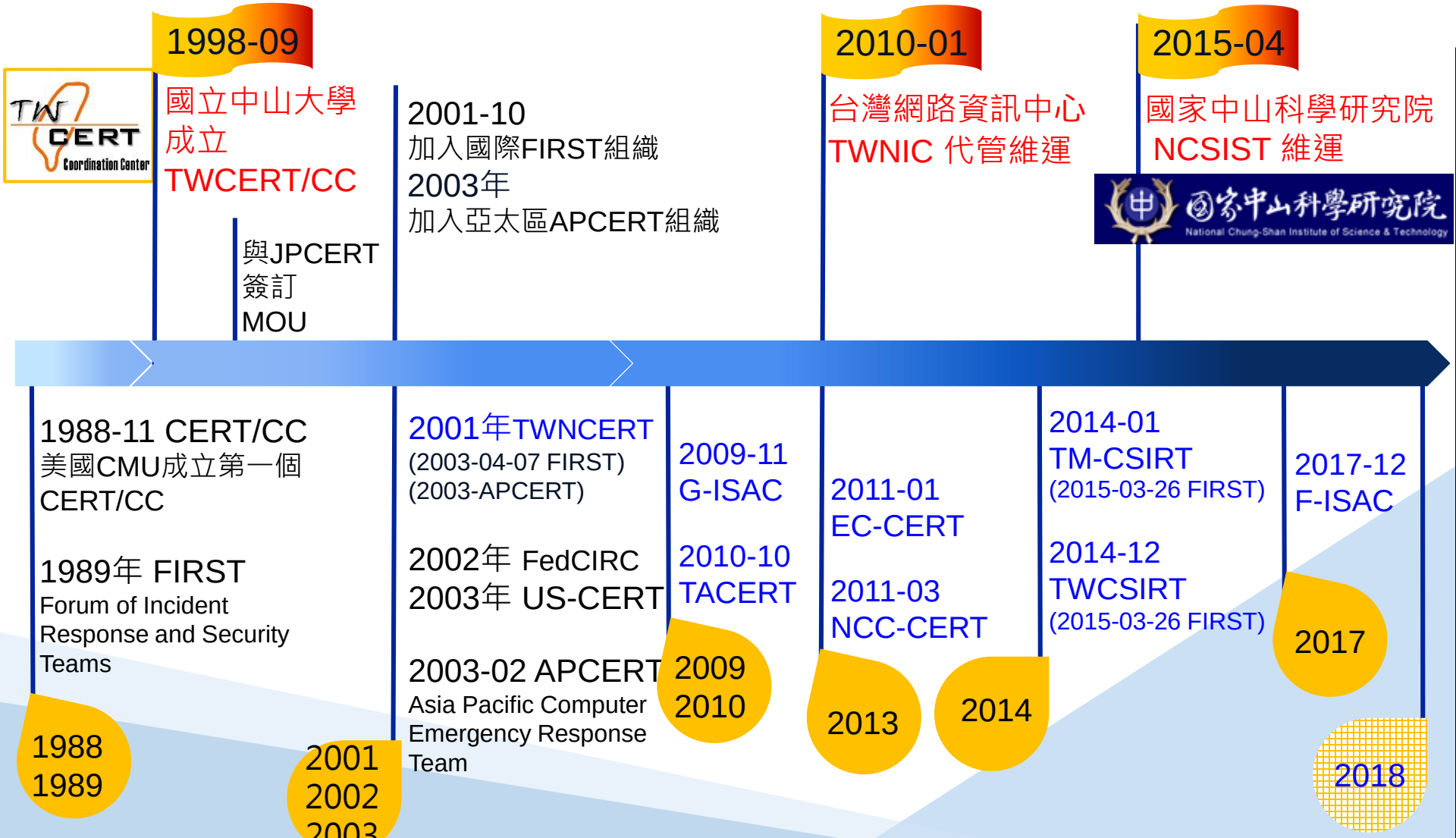
國內

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。

■ 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。

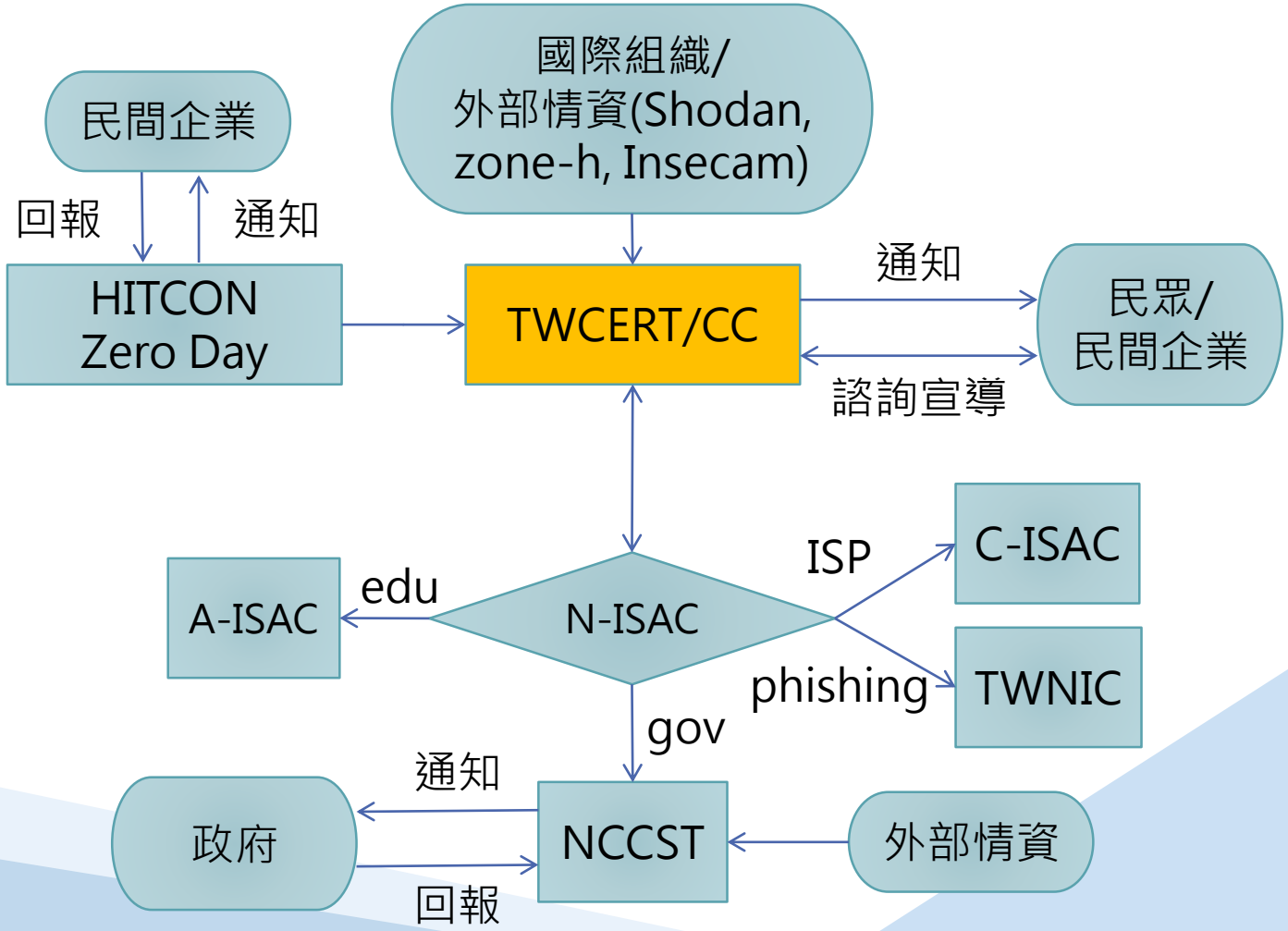
■ 交流合作

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。

■ 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


國際組織/
外部情資(Shodan,
zone-h, Insecam)
民間企業
回報
通知
HITCON
Zero Day
TWCERT/CC
通知
諮詢宣導
民眾/
民間企業
A-ISAC
edu
N-ISAC
ISP
C-ISAC
phishing
TWNIC
gov
通知
政府
NCCST
外部情資
回報

官網、電子郵件、電話多元通報管道

TW CERT Coordination Center

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


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）：

聯絡電話：

電子郵件：

受影響設備資料

IP位置：

網域名稱：

設備廠牌、型號：

已裝置之安全機制：

防火牆：

防毒軟體：

入侵偵測系統：

入侵防禦系統：

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。

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

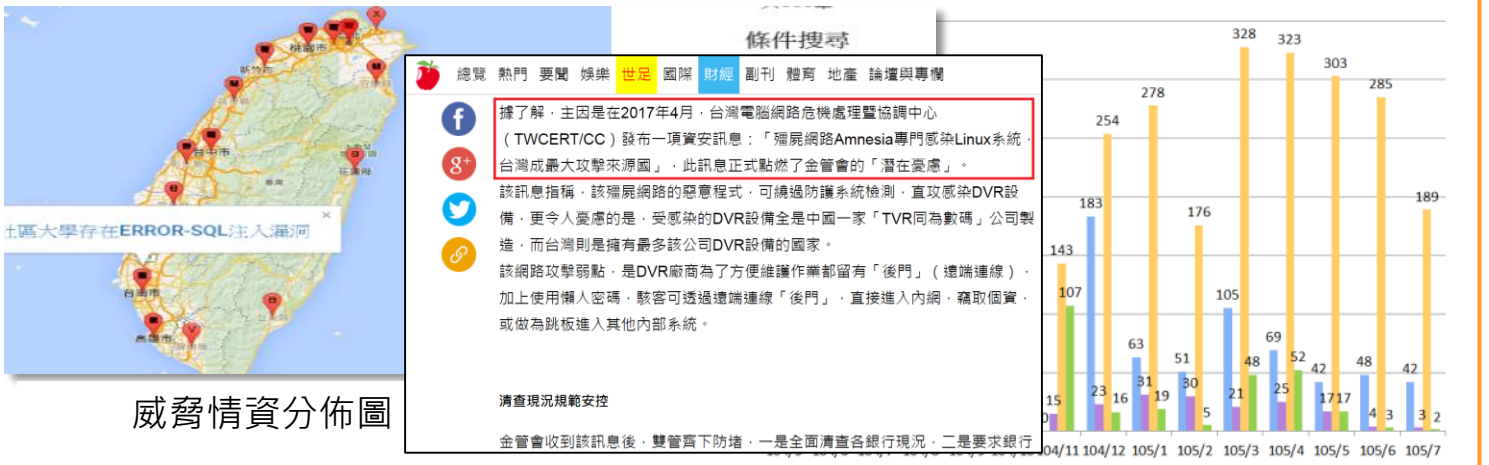
MARS

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。

情資發布-威脅預警情資

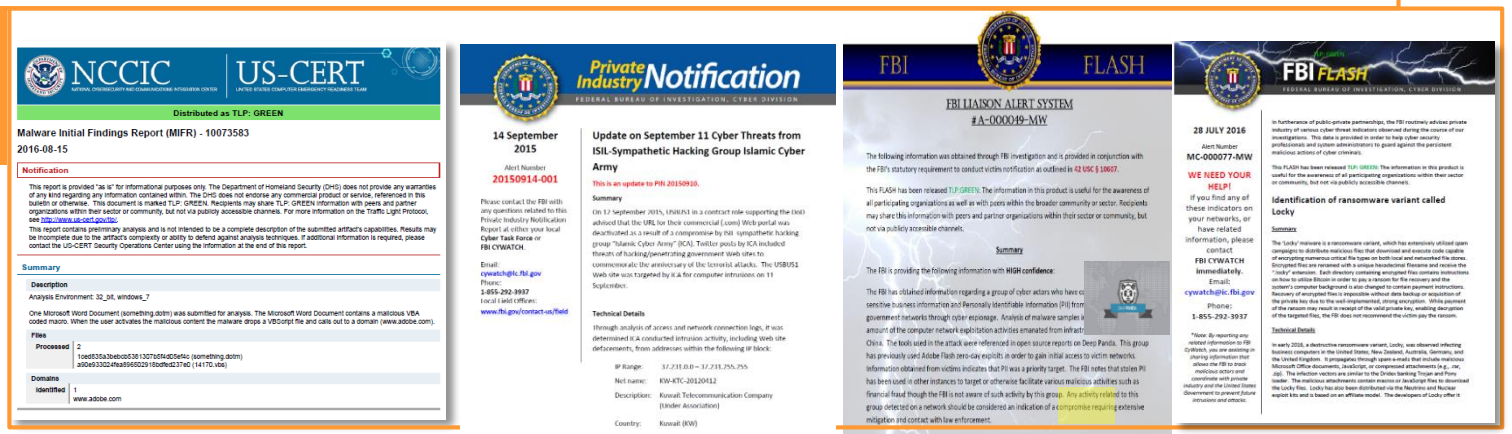
網路威脅態勢

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



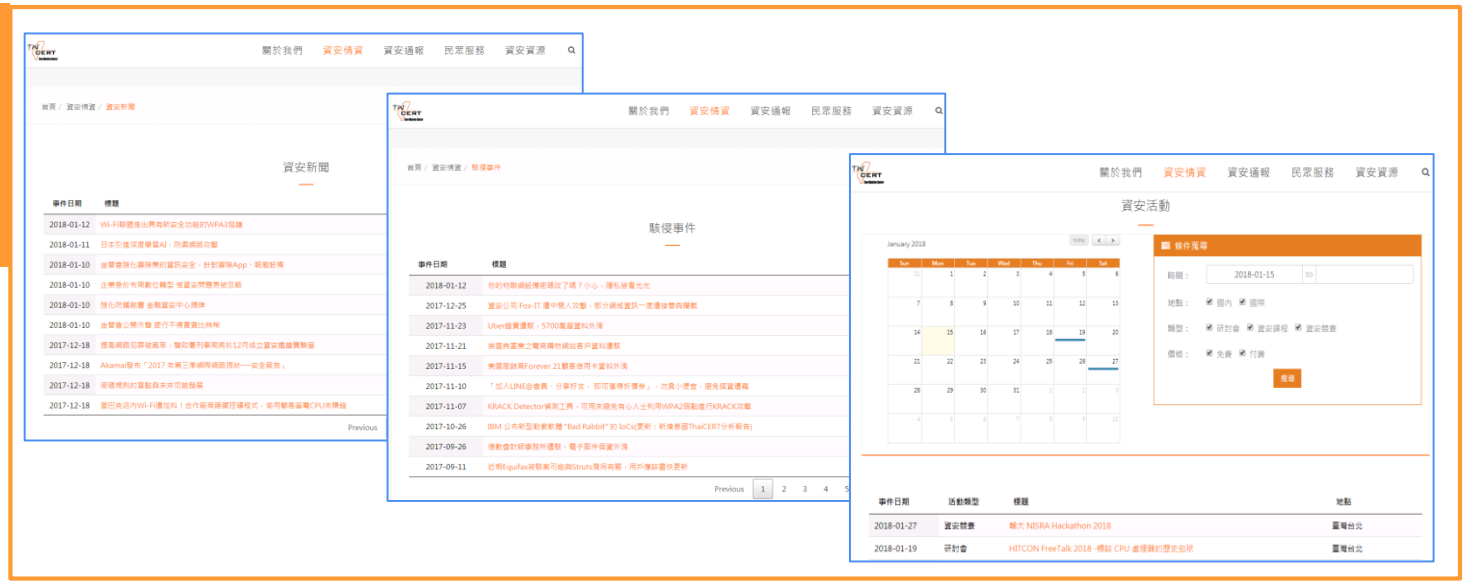
威脅情資分佈圖

國外合作交流威脅警訊



情資發布-資安訊息

資安新聞
駭侵事件
活動訊息



資訊產品漏洞
及解決方案

情資發布-資安刊物

資安電子報

http://twcertcc.blogspot.tw/

免費電子報訂閱

資安年報

情資發布-技術文件

CSIRT組織
技術文件/手冊

專題彙整分析
技術研究報告

資安情資發佈管道

Mailing List

Please Join Us!!

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

台灣電腦網路危機處理暨協調中心 - TWCERT/CC

Blog

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!

Thanks!

Q & A

資安月報訂閱

Facebook