



# TWCERT/CC 資安情資電子報

---

2018 年 1 月份

## 目錄

第 1 章、摘要 .....	1
第 2 章、TWCERT/CC 近期動態 .....	1
第 3 章、國內外重要資安新聞 .....	3
3.1、國內外資安政策、威脅與趨勢 .....	5
3.2、駭客攻擊事件及手法 .....	9
3.3、軟硬體漏洞資訊 .....	9
3.4、資安研討會及活動 .....	11
第 4 章、2017 年 12 月份事件通報統計 .....	22

## 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電子報，電子報中統整上月重要資安情資，包含 TWCERT/CC 近期動態、資安政策、威脅與趨勢、駭客攻擊事件、軟硬體漏洞、資安研討會活動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，白帽駭客能量應釋出，為資安注契機，另銀行執行內稽，著重資安三重點，而為了防止洩密，印度令邊防兵刪微信微博，以及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。

在軟硬體漏洞方面，D-Link 升級 DIR-605L 韌體以解決 HNAP 服務阻斷漏洞；VMware 釋出 4 類升級產品修補多組漏洞；Android 被公布 47 漏洞，其中 Janus 能導致惡意碼以系統身分執行；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 漏洞恐洩漏 private key 及 Bypass 加解密；Cisco 至少二類產品恐遭 ROBOT 攻擊而解密資料，且暫無安全更新；PostgreSQL 初始化導致 Red Hat Enterprise Linux 7 系統權限被接管；Apple 密集更新多款設備，防禦 KRACK 暨劫持智慧家電等攻擊行為；Palo Alto 更新防火牆作業系統 PAN-OS 阻擋組合式攻擊；IoT 殭屍網路 Satori 正大肆攻擊華

為家用型 router ; Citrix 修補多版 XenServer 避免實體機 DoS 。

在資安研討會方面，2018 年 1 月 27 日至 28 日於輔仁大學聖言樓中舉辦「輔大 NISRA Hackathon」競賽。

在 2017 年 12 月事件通報統計方面，分別說明通報來源統計圖、攻擊來源統計圖及攻擊類型統計圖等統計數據，經統計分析後，該月以國外駭客掌握國際相關電郵帳密清單情資為大宗。

## 第 2 章、TWCERT/CC 近期動態

### 2.1、2017 年 12 月 19 日 TWCERT/CC 參加「2018 資安趨勢論壇」研討會

TWCERT/CC 於 2017 年 12 月 19 日參加「2018 資安趨勢論壇」研討會，此次會議是由資安人主辦，參與對象主要為中小企業，此次以金融相關單位為主，針對資安立法的角度、資訊長的角色扮演、銳不可抵的金融科技、全球網際網路威脅等項目為研討內容，TWCERT/CC 陳永佳主任也於此次研討會上針對 TWCERT/CC 於 2017 年度的通報狀況進行分析，並提出未來企業需要特別防範的資安威脅及給予相關建議，以及 TWCERT/CC 可提供民眾的服務內容進行推廣。



以下將列出從 2017 年度資安通報的狀況來看，彙整出對於個人及企業較需注意的 10 項資安威脅防護建議：

#### (1). 個資外洩

- 個人：不輕易將個人資料留於網路上。
- 企業：對客戶資料善盡保護責任，否則可能會因違反個資法而

遭求償，或商譽受損。

(2). 社交工程攻擊

- 開啟郵件及附檔時需小心謹慎，勿開啟不明來源信件，安裝防毒軟體。

(3). 勒索軟體攻擊

- 勿開啟不明來源信件，系統定期更新、資料需備份，安裝防毒軟體。

(4). 網站/系統弱點攻擊

- 系統開發納入源碼檢測、弱點掃描及滲透測試等安全軟體發展流程(Secure Software Development Life Cycle, SSDLC)，並進行系統定期更新。

(5). 釣魚網頁

- 勿點擊不明網頁連結，安裝防毒軟體。

(6). 弱密碼

- 修改預設密碼，定期更新密碼，落實密碼複雜度。

(7). 機密資料外洩

- 資料加密，勿將資料隨意置於雲端或上傳國外惡意程式分析平台。

(8). Webcam、印表機(事務機) 等 IoT 裝置遭控制利用

- 勿使用預設帳密，非必要勿暴露於網路中。

(9). APP 偽冒.

- 用戶：勿安裝不明來源 App。
- 開發商：上線前需進行安全檢測。

(10). DDoS 攻擊

- 用戶：弱點與惡意程式檢測，並安裝防毒軟體，以避免成為 DDoS 攻擊幫兇。
- 企業：建置 DDoS 防護機制。

## 第 3 章、國內外重要資安新聞

### 3.1、國內外資安政策、威脅與趨勢

#### 3.1.1、AKAMAI 發布「2017 年第三季網際網路現狀——安全報告」

Akamai Technologies, Inc.發布的「2017 年第三季網際網路現狀——安全報告」最新資料顯示，網路應用程式攻擊無論在每一季或年度皆明顯持續增長。同時，對 Mirai 殭屍網路與 WireX 惡意軟體的進一步研究分析指出，攻擊者可能利用物聯網和 Android 裝置建立日後的殭屍網路大軍。



資料來源：

<http://technews.tw/2017/12/05/q3-state-of-the-internet-security-report/>

#### 3.1.2、密碼規則的盲點與未來可能發展

數位身分識別將是未來所有新興科技都要共同面對的問題。回到管理風險角度來看，組織應該依據提供服務的特性，面對威脅的狀態，風險評估的結果，選擇複合性的安全規則，並採取既「分工」又「合作」的策略，才能有效的解決「變更密碼」的問題，此外，必須瞭解密碼強度的目的是保護密碼，防範用戶身分遭到盜用，所以重點一定要放在效果，如果誤將手段當成目的，那勢必是事倍功半、徒勞無功。



資料來源：

[https://www.informationsecurity.com.tw/article/article\\_detail.aspx?tv=&aid=8549&pages=2](https://www.informationsecurity.com.tw/article/article_detail.aspx?tv=&aid=8549&pages=2)

### 3.1.3、總統：白帽駭客能量應釋出 為資安注契機

總統蔡英文於 2017 年 12 月 11 日在總統府經國廳出席「府會資安週」開幕式，提到打造國家級資安機制等 3 大目標；她也說，台灣有一群年輕充滿活力的白帽駭客，這股創新和創業能量應該被釋放出來，為台灣資安產業注入新的契機。



資料來源：

<http://www.cna.com.tw/news/aip/201712110074-1.aspx>

### 3.1.4、防洩密 印度令邊防兵刪微信微博

印度安全機構向中印邊境部隊下達指令，要求軍人刪除中國的APP，並將手機格式化。



資料來源：

<http://www.chinatimes.com/newspapers/20171201000741-260309>

### 3.1.5、顧立雄：銀行內稽 三重點大翻修

金管會近期將全面翻修銀行內稽內控規定，將「強制」資產規模達一兆以上的銀行，須設獨立法遵和資安單位，並落實吹哨者保護機制，全面納入「金融業(銀、保、證)」三業內稽內控。



資料來源：

[https://udn.com/news/story/7239/2847267?from=udn-ch1\\_breaknews-1-cate6-news](https://udn.com/news/story/7239/2847267?from=udn-ch1_breaknews-1-cate6-news)

### 3.1.6、中國主辦世界互聯網大會 強調網路主權

中國大陸官方舉辦的世界互聯網大會，再次提到全球網路治理及建構網路空間命運共同體的「四項原則」和「五點主張」，並表示全球網路治理體系變革進入關鍵時期。



資料來源：

<https://tw.appledaily.com/new/realtime/20171203/1252552/>

## 3.2、駭客攻擊事件及手法

### 3.2.1、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

專為政府、國防、重大基礎設施提供 IT 安全服務的 Fox-IT 上周坦承曾於 2017 年 9 月遭中間人 ( Man-in-the-Middle, MitM ) 攻擊。

Fox-IT 特定網域遭駭客接管達約 10 小時，其中 Fox-IT 用戶的登入憑證及電子郵件流量遭接竊取及攔截。

2017 年的 9 月駭客利用有效憑證登入第三方的網域名稱註冊商，存取並變更 Fox-IT.com 的 DNS 紀錄，將流量導至駭客控管的伺服器上。

駭客目標為 Fox-IT 的 ClientPortal 檔案交換服務，並攔截了 9 名用戶的登入憑證、10 個檔案、一個電話號碼、一些名字與電子郵件帳號。

Fox-IT 展開全面的內部調查，尋找駭客取得有效 DNS 憑證的管道，並表示 DNS 服務供應商並未啟用雙因素認證，駭客只要結合帳號及密碼就能存取管理介面。

TWCERT/CC 建議 Fox-IT 產品使用者檢視 2017 年 9 月至今寄送至 Fox-IT 之電子郵件以及 ClientPortal 網路登入憑證等活動紀錄是否異常，並注意近期可疑之電子郵件來源，以免遭駭客利用。



資料來源：

<https://www.ithome.com.tw/news/119682>

<https://arstechnica.com/information-technology/2017/12/hackers-steal-s>

[ecurity-firms-secret-data-in-brazen-domain-hijack/](https://arstechnica.com/information-technology/2017/12/hackers-steal-s)

### 3.3、軟硬體漏洞資訊

#### 3.3.1、D-Link 升級 DIR-605L 韌體以解決 HNAP 服務阻斷漏洞

友訊公司 DIR-605L 300Mbps 無線寬頻路由器存在弱點，駭客可藉此送出長字串讓 HNAP 元件視作密碼處理，從而導致 DoS，D-Link 因此而升級對應之韌體。



資料來源：

<https://vuldb.com//?id.110110>

#### 3.3.2、VMware 釋出 4 類升級產品修補多組漏洞

VMware 對 4 款產品測出弱點，如網路虛擬化與安全平台 NSX for vSphere、適用 Mac 的 Fusion、Workstation(Linux、Windows 版)及雲端虛擬桌面 Horizon View 俱存風險，駭客可藉此 Input Validation 瑕疵竊資；另越界讀寫記憶體、大量 buffer 溢位、空指標 dereference、DLL 劫持等漏洞，皆用以遂行 DoS 及代碼執行，影響層面涵蓋實體機 OS 與 VM，VMware 就相關版本軟體提供對應之安全更新。

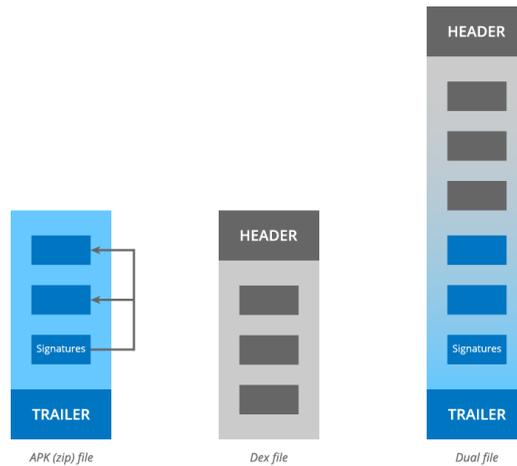


資料來源：

<https://www.vmware.com/security/advisories/VMSA-2017-0018.html>

### 3.3.3、Android 被公布 47 個漏洞，其中 Janus 能導致惡意碼以系統身分執行

Google 成立的 Open Handset Alliance 負責維護開發 Android，2017 年 12 月份安全公告列出 47 個漏洞散落於多項元件與架構，駭客可由近端或遠端進行探勘，藉此獲得高級權限且任意執行程式碼，並獲得隱私資料，另因 APP 代碼要在 Android 裝置執行，須先編譯然後打包成 Android 能識別並執行的應用程式套件 APK(Android application package)，有效的 APK 為 archive 檔案格式，APK 內包含被編譯的代碼 DEX(Dalvik Executable)、resources、assets、憑證、清單，APK 檔基於 ZIP 格式，與 JAR 檔案構造相似，Janus 漏洞利用 Android 特性，攻擊者若插入惡意 code 至簽章證明之 DEX，甚可藉 system 權限隨意執行程式，Google 已就相關版本軟體研製安全更新，但多數用戶須等待製造商(OEMs)修補檔尚需數月，顯有大批智慧機仍處風險之中。



資料來源：

<https://thehackernews.com/2017/12/android-malware-signature.html>

### 3.3.4、Google 更新 Chrome 修補 37 漏洞

Google 於 2017 年 12 月修補 Chrome 大量弱點，解決前版受漏洞造成之風險，諸如巨量溢位、使用釋放後記憶體、超限讀寫、URL 偽造等。駭客可藉此取得遠端系統控制權，對各類元件模組進行多種攻擊模式，Google 提供修補版本供下載，惟基於資安顧慮，漏洞細節均未公開。



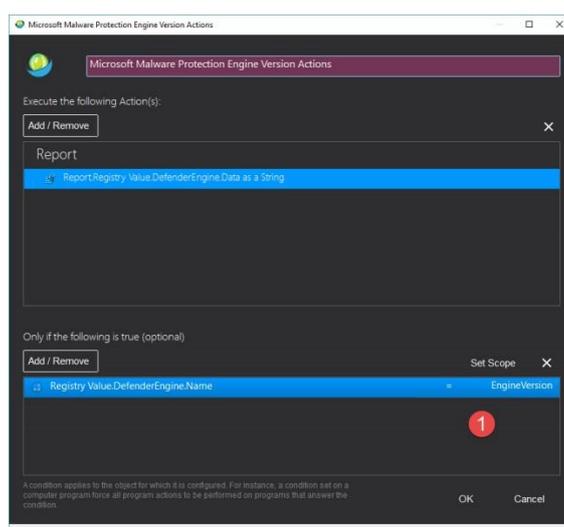
資料來源：

<https://chromereleases.googleblog.com/2017/12/stable-channel-update-for>

[-desktop.html](#)

### 3.3.5、Microsoft 緊急修補 Malware Protection Engine 防止嚴重 RCE 事件接管系統權限

微軟開發之惡意軟體防禦引擎 (Malware Protection Engine, MPE) 具核心級資安性能，如即時偵掃、檢測、清除等防毒防護機制，內建於主流 server 暨 windows 軟體，囿於 MPE 運作時恐觸發 memory corruption，接續衍生 Remote Code Execution，駭客可全權接管系統控制，任意增刪帳號、檔案、程式，該公司已提供 MPE 1.1.14405.2 版且自動部署更新，因 Microsoft 不按常態地修補 memory corruption 漏洞，趕在每月例行「Patch Tuesday」前僅僅數日緊急公開，且保證該漏洞修補前尚未遭在野濫用，顯見危險程度不容小覷。



資料來源：

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CV>

[E-2017-11937](#)

### 3.3.6、F5 更新 BIG-IP 防止 Double Free Memory 與 CCA2 攻擊

F5 公司開發 BIG-IP 眾多網管產品(LTM、AAM、AFM、Analytics、APM、ASM、DNS、Link Controller、PEM)，使用共同技術協定，故同樣弱點將落在多款設備，其中 Traffic Management Microkernel 在處理惡意構造封包時當掉，服務重啟時間內呈現網管擱置流量狀態；另第 2 版 CCA，即適應性選擇密文攻擊(Adaptive Chosen-Ciphertext Attack)，針對 RSA 加密信號有逐次還原明文能力，對 Client SSL profile 預設啟動 RSA key exchange 形成洩密威脅，駭客若掌握網路流量或介入中間位置，可能造成 DoS 與獲悉隱密資料，F5 就相關版本軟體提供對應之安全更新。



資料來源：

<https://support.f5.com/csp/article/K21905460>

### 3.3.7、OpenSSL 公布 2 漏洞恐洩漏 private key 及 Bypass 加解密

開放原始碼的軟體函式庫套件 OpenSSL，主要以 C 語言撰寫，用途為落實 SSL、TLS 協定以避免遭竊聽，現存在 2 項弱點，駭客藉 rsaz\_1024\_mul\_avx2() 之蒙哥馬利乘法程序觸發 overflow，獲得密鑰資訊；另經由製造 handshake 錯誤狀態，引發 OpenSSL 1.0.2b

後續版本 handshake 函數，SSL\_read()和 SSL\_write()被不當呼叫，使資料繞過加解密運算，OpenSSL 僅就 1.0.2 系列軟體提供升級檔案。



資料來源：

<https://www.openssl.org/source/>

### 3.3.8、Cisco 至少二類產品恐遭 ROBOT 攻擊而解密資料，且暫無安全更新

經證實 Cisco 旗下 ACE、ASA 系列網管產品因具有 TLS session 加密機制弱點，駭客得改版 Bleichenbacher attack，開展 ROBOT(Return Of Bleichenbacher's Oracle Threat)攻擊形式，針對 RSA 密鑰交換特性，發送上百萬查詢連線以截獲其回應，比較 Transport Layer Security 架構中有效與無效 PKCS#1 padding 之旁道訊息，逐次推敲還原 RSA PKCS#1 v1.5 加密區塊，最終目的為取得明文，Cisco 暫無對應此弱點之更新，刻正調查 8 款產品是否受累，另 13 類產品無恙。



資料來源：

<http://www.kb.cert.org/vuls/id/144389>

### 3.3.9、PostgreSQL 初始化導致 Red Hat Enterprise Linux 7 系統 權限被接管

Red Hat Enterprise Linux 7 系列作業系統存在共同弱點，本機駭客探勘 PostgreSQL 初始化 script 之 Race condition 漏洞，直接擴權至 root，取得完整控制權，Red Hat 就各版軟體提供相應安全更新。



資料來源：

<https://securitytracker.com/id/1040007>

### 3.3.10、Apple 密集更新多款設備，防禦 KRACK 暨劫持智慧家電等攻擊行為

Apple 檢測多項弱點散落數類產品，駭客可對 AirPort 基地台發動 Key Reinstallation Attack 竊取且竄改封包數據；或利用 HomeKit 輸入驗證瑕疵，入侵智慧家電，隨意操縱連線資產；還可藉特製資料影響 Safari、iTunes、iCloud 之 WebKit 與 Wi-Fi 晶片，觸發 Memory Corruption 以執行任意碼；並趁 Apple push notification service 元件發生憑證隱私瑕疵，追蹤受害者隱私，Apple 就各版裝置 OS 與 firmware 提供對應安全更新。



資料來源：

<https://support.apple.com/en-us/HT208326>

### 3.3.11、Palo Alto 更新防火牆作業系統 PAN-OS 阻擋組合式攻擊

Palo Alto Networks 發展多種防火牆設備，其作業系統 PAN-OS 存在多重弱點，尤其舊版管理介面遭受 server-side request forgery，解析已匯入惡意資料將使防火牆連線攻擊者並洩漏隱私訊息；或者運行中 GlobalProtect gateway 被迫轉為 DoS 狀態；駭客甚至能發動組合式攻擊，觸發 PHPSESSID cookie 反序列化、panAuthCheck 驗證 bypass 等連串錯誤，取得對 '/php' 資料夾與 '/php/utils/router.php'、'/usr/local/bin/genindex\_batch.sh' 二腳本檔寫入能力，後續假 root 身分執行命令；另封包擷取管理元件亦

有 RCE 風險，Palo Alto 升級各版 PAN-OS 解決相關風險。

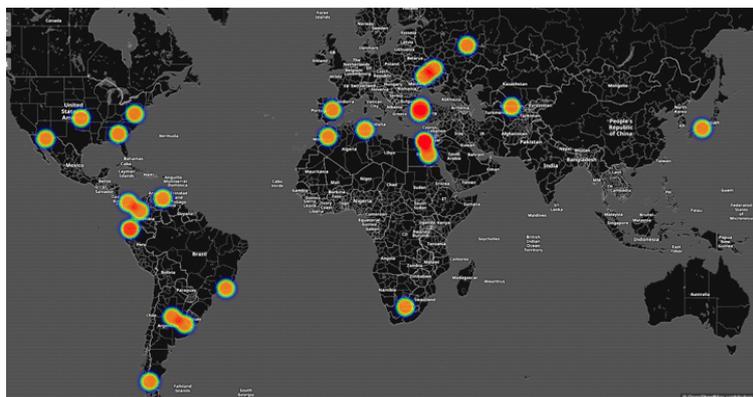


資料來源：

<http://securityadvisories.paloaltonetworks.com/Home/Detail/102>

### 3.3.12、IoT 殭屍網路 Satori 正大肆攻擊華為家用型 router

Satori 原意為日本禪宗「開悟」，然在此情境則無禪意，由於華為家庭路由器韌體設計存在弱點，駭客可注入 shell meta 字元 "\$()"，構成有效之惡意 request，通過 port 37215 及 UPnP 設計所形成之漏洞，針對性 HG532 觸發其更新行為，趁機引發 RCE 攻擊，目前已影響數十萬設備，儘管華為提供安全性建議，惟 Mirai 原始碼已公諸於世，仍應擔心其他變種 IoT 殭屍網路竄起。



資料來源：

<https://research.checkpoint.com/good-zero-day-skiddie/>

### 3.3.13、Citrix 修補多版 XenServer 避免實體機 DoS

XenServer 系列產品使用改良式快速模擬器 Quick Emulator (Qemu)，將所有硬體零件虛擬化，如 CPU、BIOS、IDE 硬碟控制器、VGA 顯示卡、USB 控制器、網卡，以實踐全面虛擬的 HVM (Hardware Virtual Machine) 客體主機，而 HVM 在 Intel 處理器 x86 架構下，用戶若為本機客體 VM 系統管理者，可能觸發 VGA 模擬器之緩衝區溢位、分頁表控制失誤，幾乎皆導致實體機 hypervisor 或 OS 失能，亦會衍生擴權後不當執行程式並取得資料等結果，而在 XenServer 7.2 及 7.1 LTSR CU1 有嚴重弱點，受到惡意操作將 crash 實體機，Citrix 就各版軟體提供對應修補壓縮檔。



資料來源：

<https://support.citrix.com/article/CTX230624>

### 3.4、資安研討會及活動

時間	研討會/課程 名稱	研討會相關資料
2018/01/27- 01/28	輔大 NISRA Hackathon 2018	<p>【資安競賽】輔大 NISRA Hackathon 2018</p> <p>主辦單位：NISRA</p> <p>活動對象：台灣各大學，在學學士生與在學碩士生</p> <p>日期：2018年01月27日(六) - 2018年01月28日(日)</p> <p>地點：輔仁大學聖言樓 SF648 SF651(新北市新莊區中正路 510 號)</p> <p>線上報名連結：  <a href="https://nisra.kktix.cc/events/hackathon2018">https://nisra.kktix.cc/events/hackathon2018</a></p> <p>活動概要：</p> <p>生活中常常會遇到一些小困擾，儘管偶爾會閃過「如果有.....就好了」的念頭，但很少有人真的付諸行動。而所謂的「駭客精神」，就是實際上動手解決我們所遇到的問題。解決方法可能不太完整、有點醜、甚至莫名其妙，但卻是有效的。</p> <p>於是，我們舉辦 Hackathon，希望藉由這場活動聚集一群充滿熱情的人，以小組合作的形式向目標共同邁進，利用程式改善我們的生活。</p> <p>我們鼓勵初次參賽者發揮駭客精神，只要具備基礎程式能力，歡迎帶上新穎的點子與熱忱！活動的過程中，可以和教練們進行資訊技術的交流，教學相長。你有什麼想改變世界的好點子嗎？利用這 28 小時告訴我們吧！</p>

## 第 4 章、2017 年 12 月份事件通報統計

本中心每日透過官方網站、電子郵件、電話等方式接收資安事件通報，2017 年 12 月收到通報計 941 筆，以下為各項統計數據，分別為通報來源統計圖、通報對象統計圖及通報類型統計圖。

通報來源統計圖為各國遭受網路攻擊，且發起攻擊之 IP 為我國所有之 IP，並向本中心進行通報之次數，如圖 1 所示；通報對象統計圖為本中心所接獲之通報中，針對通報事件責任所屬國家之通報次數，如圖 2 所示；通報類型統計圖則為本中心所接獲的通報中，各項攻擊類型之筆數，如圖 3 所示。

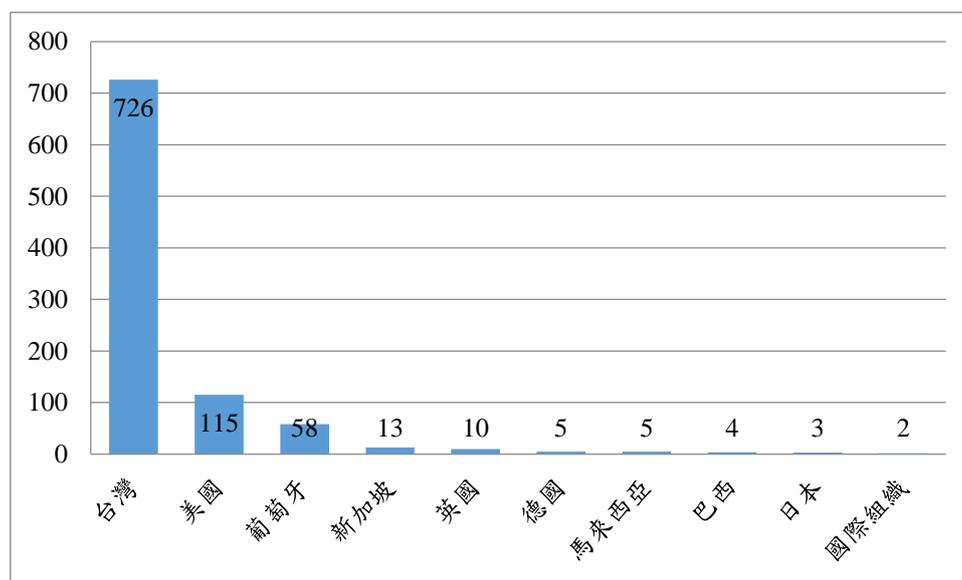


圖 1、通報來源統計圖

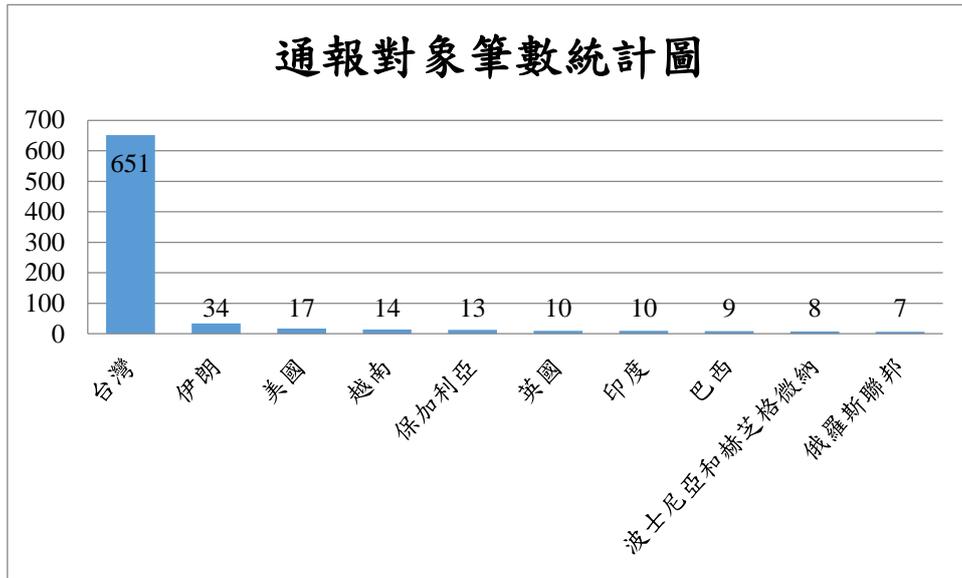


圖 2、通報對象統計圖

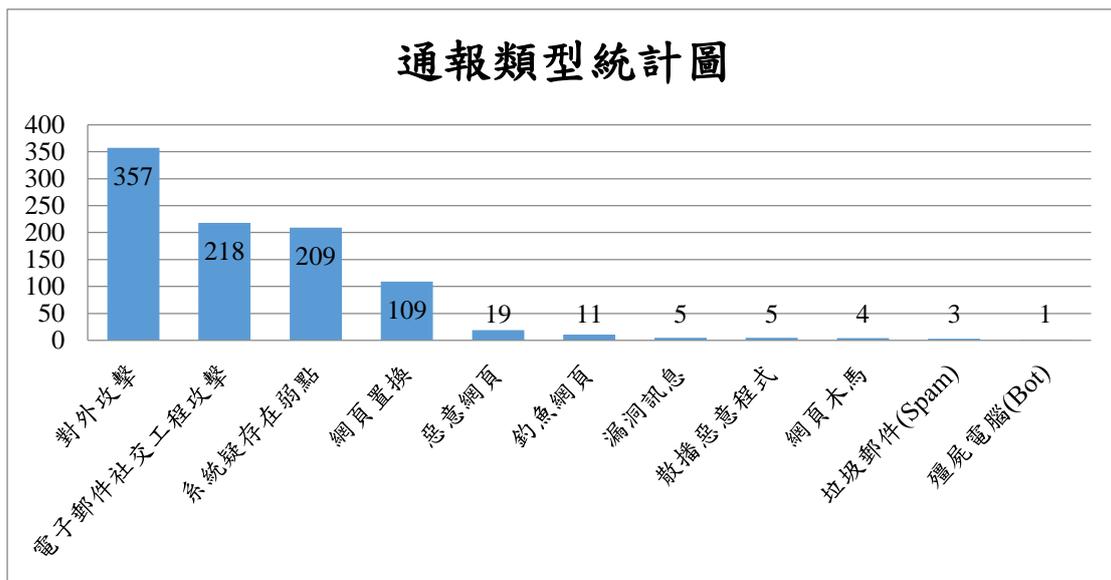


圖 3、通報類型統計圖

2017 年 12 月通報主要來源以來自合作單位提供之國外駭客掌握國際相關電郵帳密清單情資為大宗，TWCERT/CC 從數千筆清單中篩選出台灣「\*.tw」相關網域，內含有全台眾多大型及中小型企業共計 217 組機關單位，總計有 261 筆帳密，並透過網路及全球 Whois

查詢網域登記的資料聯繫電子郵件所有者，或是網域所有者以進行處理。資訊外洩主要原因依據國際資安團隊分析多為網路釣魚郵件、釣魚網站、資料庫遭侵入與植入惡意軟體如鍵盤側錄等第三方攻擊，其中以釣魚郵件威脅最大，且上述外洩因素皆可能互為因果，使用者不可不防。TWCERT/CC 建議用戶定期更新電子郵件信箱密碼，避免帳號密碼遭竊取。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。並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），最後務必定期保持作業系統及防毒軟體更新。

除通報至政府資安資訊分享與分析中心(G-ISAC)外，本中心亦針對 zone-h 情資以電子郵件或電話方式通知相關單位進行處理，本月約有 55%單位完成修正，建議大家應於平常保持良好之防護習慣，於事前勤更新相關弱點及漏洞，事發時立即處理，後續本中心仍持續提醒相關用戶對於所收到之事件通報進行相關處理，以減少駭侵事件發生時所造成的損害。

發行單位：台灣電腦網路危機處理暨協調中心

〈 Taiwan Computer Emergency Response Team / Coordination Center 〉

出刊日期：2018 年 1 月 20 日

編 輯：曾佩雅

服務電話：03-4115387

市話免付費服務電話：0800-885-066

電子郵件：twcert@cert.org.tw

官 網：<https://www.twcert.org.tw/>

粉絲專業：<https://www.facebook.com/twcertcc>

資安電子報訂閱：<http://i-to.cc/S5HzJ>

如有任何疑問或建議，歡迎您不吝指教。