TWCERT/CC 資安情資月報

106 年 11 月份

臺灣電腦網路危機處理暨協調中心

Taiwan Computer Emergency Response Teams / Coordination Center

目錄

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、資安威脅、資安趨勢、駭客攻擊事件、軟硬體漏洞及資安事件通報統計分析等資訊。

TWCERT/CC 近期動態，本中心於本月辦理中日工程研討會。

在資安政策方面，美公布決策準則，處理資安漏洞，而台灣強打資安 產值拚 550 億，並擬訂標準，防堵物聯網資安漏洞，另為了防駭客星、臺 9 國簽訂資安聯防。資安威脅方面，US-CERT 警告 WINDOWS 的 ASLR 含有可接管系統的臭蟲，另 US-CERT 與 FBI 警告：小心四處流竄的北韓駭客工具 FALLCHILL，GOOGLE 公布常見帳號竊取手法，網路釣魚比駭客入侵更嚴重，另十多款防毒軟體隔離恐失效，AVGATER 漏洞能縱放被封鎖的惡意程式，而空白 WORD 暗藏木馬，俄國駭客組織用微軟 DDE 協定攻擊散佈惡意程式。資安趨勢方面，新版 OWASP 十大網站安全風險排名出爐，微服務風潮帶來三大新安全風險，另 4 成公司查不到攻擊的駭客　金融業最常被盯上，而醫療領域 IOT 應用帶來安全新隱憂。

在駭侵事件方面，美國服飾商 Forever 21 顧客信用卡資料外洩，而英國典當業之電商購物網站客戶資料遭駭，Uber 也證實遭駭，5700 萬筆資料外洩，另加入 LINE@會員、分享好友， 即可獲得折價券」，勿貪小便宜，避免個資遭竊，偵測工具 KRACK Detector，可用來避免有心人士利用 WPA2 弱點進行 KRACK 攻擊。

在軟硬體漏洞部分， Microsoft 釋出 11 月之安全更新；Oracle 緊急釋出更新修復 Identity Manager 漏洞；OracleTuxedo 軟體平臺存在嚴重漏洞 JoltandBleed；Linux Kernel 內 ALSA 定序介面、

waitid()系統呼叫存在弱點導致系統權限遭剽竊；Linux kernel 經檢測 USB 驅動程式漏洞多達數十項；IEEE P1735 規範之加密流程出現 7 漏洞，將危及電子設計智財權；OpenSSL 釋出新版修補資料外洩漏洞；LibreOffice 釋出新版修補記憶體寫入錯誤；Apache 釋出 OpenOffice4.1.4 版修補漏洞；EMC 修補 ScaleIO 與 RSA® Authentication Manager 數個漏洞；特定 Intel 處理器技術多組漏洞導致代碼執行或提權事件。

在資安研討會及活動部分，2017 年 12 月 12 日至 15 日於台大醫院國際會議中心舉辦「2017 Taiwan Internet Forum-與你我有關的資訊安全」，另 2017 年 12 月 19 日於台北文創大樓舉辦「2018 資安趨勢論壇」，另 2017 年 12 月 21 日及 2017 年 12 月 28 日分別於中國文化大學進修推廣部、NTC.im 人才培訓中心召開白帽駭客認知班訓練課程。

在本月份事件通報統計部分，分別介紹通報來源統計圖、攻擊來源統計圖及攻擊類型統計圖等統計數據，另接獲大量疑因遭駭客以電子郵件社交工程攻擊方式所獲之電子郵件帳號及密碼外洩清單。

第 2 章、TWCERT/CC 近期動態

2.1、106 年 11 月 22 日 TWCERT/CC 辦理中日工程研討會

本次研討會邀請松下株式會社產品安全中心林永熙主幹技師，為了讓林先生對 TWCERT/CC 有初步了解，首先針對 TWCERT/CC 於國內所負責任務及內部業務進行相關介紹，接著林先生則針對自己過往的經驗、日本資安培育狀況及 Panasonic 內部 PSIRT 維運經驗進行分享。Panasonic 內部產品除了大家所熟悉的一般家電之外，目前著重開發的產品為車載零組件，大約佔了總產品的 80%。

Panasonic 也有產品安全相關處置方案，產品出售前會進行威脅分析及黑箱測試，開發人員在完成產品開發後，會進行威脅分析，若發現產品中存在威脅時，會依產品開發程序立即自行處理並解決，而在產品售出後，若使用者或開發人員發現產品漏洞，則相對應的事件處置包括：在第一時間希望可取得確認漏洞的證明(Proof of Concept, POC)，來讓技術人員了解事件狀況，再針對手上擁有的資料進行相對應的分析與問題的修正，並取得第三方的認可後，例如通報事件之相關單位，最後則針對此事件公開解釋，讓民眾能了解事件的真相及處理的結果。林先生也表示:「Panasonic 的 PSIRT 目前僅針對該公司相關產品的安全性進行相對應的確保，但未有漏同獎勵(Bug Bounty)機制，因 Panasonic 於世界各地之工廠都有自己的產品線，各產品線不一定都會認可 Bug Bounty 機制。」

此外，日本在 NCA(National CSIRT Association)會推廣的這麼順利，且企業也逐漸在成立內部的 CSIRT/PSIRT 組織，主要是因為日本有許多企業會派遣公司內部資深資安專家，協助 NCA 的運作，且協助推廣 CSIRT/PSIRT 等資安事件應變團隊建置，林先生建議：「TWCERT/CC 可先從較熟悉的公/協會著手，先向公/協會進行 CSIRT 建置推廣，並請公/協會協助推廣予底下的企業。」

林永熙講師分享 Panasonic 內部 PSIRT 維運

林永熙講師與 TWCERT/CC 主任陳永佳進行交流研討

TWCERT/CC 主任陳永佳致贈禮品予林永熙講師

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、發現資安漏洞如何處理 美公布決策準則

路透社報導，外界批評，美國政府過於經常將偵測到的漏洞累積起來，以保持能力對電腦系統發動攻擊，而將網路暴露於危險之中。華府試圖處理這些批評，才會公布這些準則。

白宮網路安全協調員喬伊斯（Rob Joyce）表示，這些經過修改的規定是用來解釋眾多聯邦機構權衡利弊，決定是否保密漏洞的程序。這些規定被公布在白宮官網上。他在華府阿斯本研究所（Aspen Institute）活動上表示，這些是「全世界最複雜」的規定，使美國和其他國家比起來與眾不同。

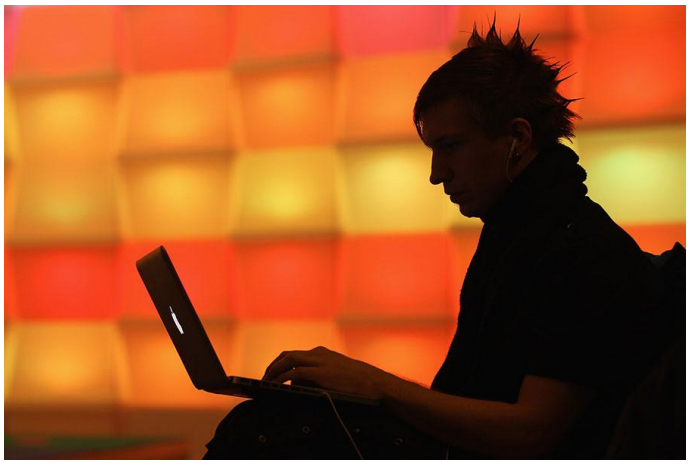
在前總統歐巴馬任內，美國政府制定了機構間的審查程序，來決定如何處理主要由國家安全局（NSA）等情報機構發現的企業技術漏洞。這個過程旨在平衡執法機構和美國情報機構之間的需求。情報機構喜歡入侵公司的電腦系統，以警告製造商在罪犯和其他駭客入侵之前修補漏洞。

川普執政團隊的新規定解釋了漏洞審查過程，以及哪些機構參與這個過程。這些機構包括情報機構和一些文職部門，比如商務部、財政部、能源部和國務院。

國家安全局被列為這個跨機構小組的「執行秘書」，其任務是協調爭議。如果分歧不能調和，這個小組將就是否披露某個漏洞進行投票表決。

新規定也要求跨機構小組發佈年度報告，其中部份內容將公開。報告將列出發現漏洞的數量、保密的數量和披露的數量。

新規定中也標明，有關某個漏洞是否保密的決定，每年都將重新考慮。喬伊斯指出，逾 90%的漏洞最終都被披露，但是批評者說，漏洞分享得太慢，而且大多數嚴重漏洞常常被保密，而若是嚴重漏洞被駭客早一步利用，則有可能造成嚴重後果，例如今年爆發的「想哭」勒索病毒，該病毒襲擊全球 150 個國家，導致醫院的電腦系統癱瘓、工廠營運混亂，這造成人們對政府保密網路漏洞做法的批評聲浪增大。



- http://www.cna.com.tw/news/aopl/201711160067-1.aspx

（資料來源：臺灣中央通訊社）

3.1.2、政院強打資安 產值拚 550 億

行政院資安處與科技會報辦公室明 11 月 21 日起將召開兩天的資安產業策略會議，探討國內資安產業技術、人才等及全球發展趨勢，並聽取各界意見。

知情官員表示，防毒軟體大廠趨勢科技去年度資訊安全總評報告顯示，去年網路勒索病毒造成全球企業損失高達 10 億美元，台灣遭受此攻擊次數排名全球前 20%，屬高資安風險國家。另一家防毒軟體大廠賽門鐵克（Symantec）今年 4 月網路資安報告也顯示，我國資料外洩程度居全球第五名，更高居亞洲榜首，資安已是不容忽視的

嚴峻課題。

因此，行政院最新核定的第五期國家資通安全發展方案，也決定從資安角度，確保數位國家安全。方案共有四大推動策略，包括推升資安產業自主能量、孕育優質資安菁英人才、完備資安基礎環境及建構國家資安聯防體系，以加強我國資安防禦體系。

在推升資安產業自主能量方面，知情官員表示，我國去年資安產業產值約 344 億元，規模不大，且年營收逾 5 億元者以系統整合業者居多，顯見創新研發能量待提升。

方案設定目標 2020 年前，國內資安產業總產值可達 550 億元，作法包括將符合安全標準的國內廠商資安產品，納入政府採購的共同供應契約，藉政府機關優先採用國內資安產品。

政府機關同時可作為國內資安產品的實驗場域，回饋產品的使用建議，進而促進關鍵資安技術及產品研發品質的提升。

第五期國家資通安全發展方案重點

項目	內容
四大推動策略	●推升資安產業自主能量 ●孕育優質資安菁英人才 ●完備資安基礎環境 ●建構國家資安聯防
預期效益	●帶動資安產值達550億元 ●建立千人資安應變小組，整備國家資安人力資源 ●完備數位時代的法制基礎，建構安全可信賴的網際生態體系 ●完成關鍵資訊基礎設施領域及六都區域聯防體系，厚植國家防禦能量
推動時程	2017年–2020年

資料來源：行政院　　邱金蘭／製表

- https://udn.com/news/story/7238/2828439

（資料來源：臺灣聯合新聞網）

3.1.3、新版 OWASP 十大網站安全風險排名出爐，微服務風潮帶來三大新安全風險

政府和資安業者都會關注 OWASP（The Open Web Application Security Project ，開放網站應用程式安全專案）歸納出的十大網路資安風險（OWASP Top 10），原本今年四月推出一套 Top 10 風險候選版，但遭社群推翻，並於九月重新徵詢社群意見後，於 11 月 20 日推出 2017 年 OWASP Top 10 正式版。

新版 OWASP Top 10 有 3 個全新的資安風險，包括：針對各平臺常見的 XML 外部處理器漏洞（XML External Entity,XXE）、針對 Java、PHP 或 Node.js 等平臺常見的不安全的反序列化漏洞（Insecure Deserialization），以及「紀錄與監控不足風險」（Insufficient Logging & Monitoring）。他指出，XML 外部處理器漏洞就是實際調查會員提供的 Log 和 API 後，才統計歸納出來的風險類型，而不安全的反序列化攻擊以及紀錄與監控不足風險則是社群回饋看到的風險類型。這三個新入圍的資安風險和越來越多微服務的興起有關係，在強調快速提供服務的過程中，有許多需要嚴謹資安驗證和授權的程序，都因此被忽略才會造成類似敏感資料外洩的結果。

分析 OWASP Top 10 的名單，2017 年排名第一名的注入攻擊（Injection）也是 2013 年版的第一名，但這不只是傳統大家認知道的 SQL Injection（隱碼攻擊），包括所有的 SQL、NoSQL、作業系統以及 LDAP 的注入攻擊，通常會發生在惡意的程式語法在輸入時，沒有經過妥善的檢查和驗證所造成的資安風險。

第二名就是無效身分認證（Broken Authentication），許多應用程式經常需要處理身分認證及 Session 管理，但導入方式若不正確，反而可能會讓駭客取得密碼、金鑰、Session 令牌，或者是利用其他導入時的錯誤疏失，暫時或永久取得使用者的身份資訊。

至於第三名的敏感資料外洩（Sensitive Data Exposure），主要是因為不少網路應用程式對於金融資訊、健康資料及個人資料的保護不足，若遭當駭客取得，就可以進行信用卡詐欺、身份竊取或是其他的犯罪行為等。因此，針對敏感性資料去需要做額外的保護措施，例如不使用或傳送時的資料必須加密，或者是瀏覽器瀏覽時，也必須要特別注意。

在 2013 年版排名中有兩個容易混淆的風險項目，是 Insecure Direct Object References 和 Missing Function Level Access Control，因此，在這次新版排名中，就合併成第五名的「無效的存取控管」(Broken Access Control)，希望藉由嚴格的存取控管，降低駭客利用這些漏洞去存取沒有經過授權的功能或察看敏感資料、修改使用者數據、更改訪問權限等。

第六名則是強調設定必須注意安全的「不安全的組態設定」（Security Misconfiguration），經常是使用不安全的預設值，或者是錯誤配置像是 HTTP 標頭或者是系統顯示的錯誤資訊已經包含敏感性個資所造成的，除了要安全設定所有作業系統、框架、函示庫以及應用程式外，更必須做到系統更新與升級，以確保系統安全與時並進。

第七名是常見的跨站攻擊(Cross-Site Scripting ,XSS)，主要就是發生在，當應用程式缺乏適當的驗證，如允許網頁可出現不可信任的資訊時，或者是允許在使用者瀏覽器中執行腳本程式，恐導致有心人士劫持使用者 Session、網頁置換或者是轉址到其他惡意網站等。XSS 風險排名可以從 2013 年排名第三名降到 2017 年第七名，主要跟很多自動化的掃描工具，都已經內建可以掃 XSS 的風險，也加快相關的漏洞修補速度，使得整體 XSS 漏洞數量看起來比以往少，但「風險」卻沒有因此減少。

第九名就是使用已有漏洞的元件（Using Components with Known Vulnerabilities），這些元件包括函示庫、框架以及其他的軟體模組，而元件會和應用程式以相同的權限執行。如果有一個容易受到攻擊的元件被駭客利用，就可能會導致嚴重的資料儀式或者伺服器被駭客接收，而使用有漏洞元件的應用程式或者是 API，都會破壞應用程式的防護並啟用各種攻擊形式，這也意味著，許多開發者在洗用套件、框架的習慣不好，除了會帶來嚴重的資料遺失外，也表示用這個框架的人，並沒有即時升級或更新到最新版。

由於臺灣有許多資安檢測都會將 OWAPS Top 10 的風險列為必檢查的項目之一，不過，OWASP 臺灣分會研發長胡辰澔提醒，這十大風險其實是一種風險框架，會因應技術發展而持續變動，若企業和組織將這 10 項視為內部唯一要解決的資安風險議題，或直接作為稽核或法遵的檢核表的檢查項目，甚至是，作為內部執行滲透測試時要解決的資安風險時，反而，會讓企業資安風險的因應範圍，限縮到這十個層面，「但，這不是 OWASP Top 10 期待的目的。」他說。

舉例而言，像是 2013 年十大資安風險，就算今年沒入榜，也仍是企業必須關注的風險，如 2013 年排名第八名的偽造跨站請求（Cross-Site Request Forgery，CSRF），就算許多開發框架多已內建 CSRF 風險防禦機制，今年也沒有進入前十大風險而名列第十三名，但胡辰澔表示，這依舊是不可掉以輕心的重要風險之一。

- https://ithome.com.tw/news/118411

（資料來源：臺灣 iThome）

3.1.4、US-CERT 警告 WINDOWS 的 ASLR 含有可接管系統的臭蟲

美國電腦緊急應變中心（US-CERT）上周警告，Windows 8、Windows 8.1 與 Windows 10 的「位址空間配置隨機載入」（Address Space Layout Randomization，ASLR）含有一臭蟲，將允許遠端駭客掌控受駭系統。

ASLR 於虛擬位址空間中隨機配置應用程式的程式碼與資料，以提高駭客的攻擊門檻，主要預防基於記憶體的程式執行攻擊，為許多作業系統的預設安全機制，涵蓋 Windows、macOS、Linux、Android 與 iOS。

微軟是在 2006 年發表 Windows Vista 時開始導入 ASLR，卻是在 2012 年的 Windows 8 出了差錯。發現該臭蟲的 US-CERT 漏洞分析師 Will Dormann 表示，若使用者是利用 Enhanced Mitigation Experience Toolkit（EMET）或 Windows Defender Exploit Guard 啟用 ASLR 時，Windows 8 及之後的 Windows 版本將無法妥善地隨機配置每個應用程式，在特定狀況下即會出現瑕疵。

相關瑕疵可能造成應用程式被重新配置到可預測的位置，失去

ASLR 應有的保護能力，而讓駭客有機可趁。

微軟則說這並非安全漏洞，因為該問題並不會影響採用預設配置的 Windows 作業系統，而只會影響那些透過 EMET 或 Windows Defender Exploit Guard 啟用 ASLR 的系統，打算在完成調查後釋出解決方案。

Vulnerability Note VU#817544

Windows 8 and later fail to properly randomize every application if system-wide mandatory ASLR is enabled via EMET or Windows Defender Exploit Guard

Original Release date: 17 11月 2017 | Last revised: 19 11月 2017

Print Tweet Send Share

Overview

Microsoft Windows 8 introduced a change in how system-wide mandatory ASLR is implemented. This change requires system-wide bottom-up ASLR to be enabled for mandatory ASLR to receive entropy. Tools that enable system-wide ASLR without also setting bottom-up ASLR will fail to properly randomize executables that do not opt in to ASLR.

Description

- https://www.ithome.com.tw/news/118467

（資料來源：臺灣 iThome）

3.1.5、US-CERT 與 FBI 警告：小心四處流竄的北韓駭客工具 FALLCHILL

美國國土安全部旗下的電腦緊急應變小組（US-CERT）與 FBI 於 11 月 14 日聯手提出警告，揭露了北韓政府所使用的遠端控制工具（Remote administration tool，RAT）—Fallchill，並公布 90 個涉及散布 Fallchill 的網址。

根據 US-CERT 與 FBI 的調查，由北韓政府所支持的 Hidden Cobra 駭客行動自 2009 年起曾陸續發動分散式阻斷服務（DDoS）攻擊、植入 Volgmer 木馬，以及散布 Fallchill 惡意程式。

Fallchill 自 2016 年起便鎖定航太、電信與金融產業展開攻擊，它是個具備完整功能的 RAT，通常是藉由偷渡式下載植入受害者電腦，

駭客再藉由層層的代理伺服器發送各種指令到被感染的系統上。

Fallchill 會蒐集被駭系統上的作業系統、處理器、IP 位址及 MAC 等資訊，而且內建眾多惡意功能，包括可取得硬碟資訊、建立或終止程序、搜尋/讀取/執行檔案、變更檔案或目錄時間戳、變更檔案目錄，或是刪除惡意程式及相關檔案等。

US-CERT 表示，Hidden Cobra 行動還利用其他工具以建立基於 Fallchill 的惡意程式即服務（Malware-as-a-service），還能遞送其他的惡意程式到受害電腦上。


Alert (TA17-318A)

HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL

More

Original release date: November 14, 2017

Print Tweet Send Share

Systems Affected

Network systems

Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FB Working with U.S. government partners, DHS and FBI identified Internet Protocol (IP) addresses and other indicators of compromise (IOCs) associated with a remote administration tool (RAT) used by the North Korean government—commonly known as FALLCHILL. The U.S. Government refers to malicious cyber ac by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit https://www.us-cert.gov/hiddencobra.

FBI has high confidence that HIDDEN COBRA actors are using the IP addresses—listed in this report's IOC files—to maintain a presence on victims' networks to further network exploitation. DHS and FBI are distributing these IP addresses to enable network defense and reduce exposure to any North Korean governr malicious cyber activity.

- https://www.ithome.com.tw/news/118271

（資料來源：臺灣 iThome）

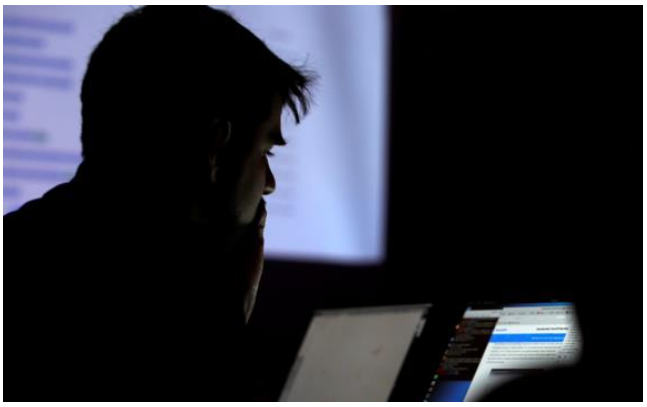
3.1.6、防駭客 星、臺 9 國簽訂資安聯防

駭客跨國攻擊時有所聞，包括臺灣、新加坡、澳大利亞、紐西蘭在內的 9 個亞太國家、49 家金融機構，於 11 月 14 日由新加坡金融管理局（MAS）與 FS-ISAC 全球金融服務資訊共享與分析中心主導啟動新加坡亞太區分析中心辦公室，希望透過跨國資訊共享防制網路犯罪、聯手防堵駭客攻擊。

全球成員達 7,000 名的 FS-ISAC，主要是機構法人和技術開發者，此次參與合作計畫的 9 個國家有澳大利亞、印度，日本，馬來西亞，

紐西蘭，新加坡，韓國，臺灣和泰國。

FS-ISAC 總裁兼執行長 Bill Nelson 表示，虛擬世界日愈複雜，網路攻擊愈見頻繁，與其一再強化防堵強度，更重要是各國與業界保持友好關係，事前做好資訊情報分享，才有更好的網絡應變能力，尤其加強在亞太區的情報共享影響力，有助於增強全球整體金融服務業的適應能力。



- https://ctee.com.tw/News/ViewCateNews.aspx?newsid=167146&cateid=jrdc

（資料來源：臺灣工商時報）

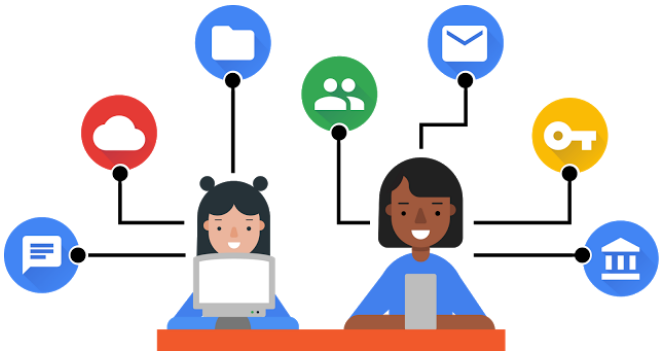
3.1.7、GOOGLE 公布常見帳號竊取手法，網路釣魚比駭客入侵更嚴重

我們很常聽到某某駭客組織入侵了某某公司的伺服器，盜取了多少多少的帳號資訊，特別是信用卡資料。聽起來這些大廠們好像永遠都可能被駭客攻破，並且害大家的資料被盜取，信用卡被盜刷，但是根據 Google 的說法，他們統計了一年份的帳號被盜資訊，發現大多數帳號被盜用的原因主要還是以網路釣魚攻擊為主，反倒是常聽到的鍵盤側錄（keylogging）或是主機被攻破的損失還沒有網路釣魚來得大。

Google 與加州大學合作，分析了數個案例，研究駭客如何入侵

別人的帳號，從 2016 年 3 月到 2017 年 3 月之間，統計了相當多資料，統整出一些重要的發現。據統計，駭客通常會竊取相當龐大的帳號量，但有許多是無效的帳號，成功率大約 7%，而網路釣魚與鍵盤側錄得來的資料則準確的多，有 12 至 25%的成功率。

Google 指出越來越多工具可進行包含用戶密碼的資料竊取，在它們檢驗的釣魚與鍵盤紀錄程式中，分別有 82%及 74%具有收集用戶 IP 位址的能力，並且多能獲取電話號碼及裝置型號等，駭客就是利用這些弱點偷走用戶的寶貴資訊。



- https://security.googleblog.com/2017/11/new-research-understanding-root-cause.html

（資料來源：美國 Google Security Blog）

3.1.8、十多款防毒軟體隔離恐失效，AVGATER 漏洞能縱放被封鎖的惡意程式

澳洲資安業者 Kapsch 近日指出，坊間的十多款防毒軟體都含有 AVGater 漏洞，這是個權限擴張漏洞，將允許駭客釋放與執行遭到防毒軟體隔離的惡意程式，目前包括趨勢科技（Trend Micro）、卡巴斯基實驗室（Kaspersky Lab）與 Emsisoft 等 6 家業者皆已修補該漏洞，Kapsch 並未列出其他尚未修補的業者名單。

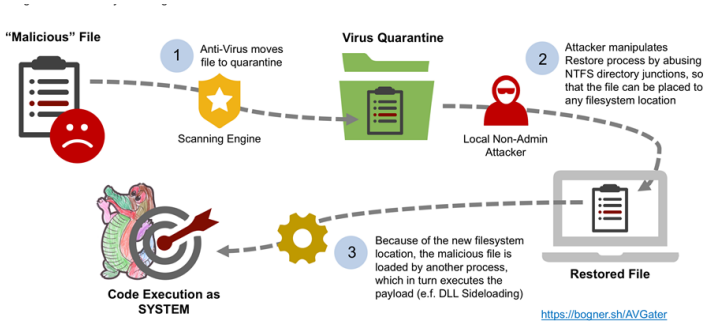
簡單地說，AVGater 漏洞利用了 NTFS 的目錄連結（directory junctions）功能，來操弄防毒軟體的隔離還原程序，以將原本被隔

離的檔案移到任意的檔案系統中。

根據 Kapsch 所描述的攻擊場景，當防毒軟體將惡意程式移到隔離區之後，駭客可利用目錄連結功能將原始路徑改至位於 C:\Program Files 或 C:\Windows 中的文件夾；繼之執行還原功能，讓具備系統權限的防毒軟體將檔案送至駭客所指定的目的地。

由於許多 Windows 服務或核心程序會載入與執行儲存於特定 Windows 目錄中的所有 DLL，因此當使用者重新啟動電腦之後，這些原本被隔離的惡意程式就會隨之被執行。

相關攻擊最大的限制是駭客必須實際存取目標對象的電腦，同時 Kapsch 也建議企業最好封鎖一般員工執行還原隔離的能力。



- https://www.ithome.com.tw/news/118213

（資料來源：臺灣 iThome）

3.1.9、空白 WORD 暗藏木馬，俄國駭客組織用微軟 DDE 協定攻擊散佈惡意程式

安全研究人員發現的俄國駭客組織 Fancy Bear 最近發動網釣攻擊，其中利用微軟 Windows 中的動態資料交換（Dynamic Data Exchange，DDE）協定，使 Word 文件不用巨集也可感染用戶 PC。

Fancy Bear 又名 APT28，是極為活躍的俄國駭客組織，曾經先後入侵美國民主黨代表大會及世界反禁藥組織竊取資料。近日安全公

司趨勢科技雙雙發現，Fancy Bear 最近散佈了一份宣稱要發動紐約市恐怖攻擊的 Word 文件 IsisAttackInNewYork.docx，利用 Microsoft 動態資料交換（Dynamic Data Exchange, DDE）協定來感染用戶 PC。

用戶如果在誘使下打開這份 Word 檔案會發現內文是空的。但檔案一經開啟，Office 產品中的 DDE 功能即呼叫 PowerShell 執行指令，連上外部 C&C 伺服器，載入名為 Seduploader 的惡意程式。該程式會蒐集受害電腦的主機資訊回傳給攻擊者。如果該機器是攻擊者有興趣的目標，即會執行第二道 PowerShell 指令，安裝 X-Agent 或 Sedreco 等後門程式。

趨勢科技研究人員 Ryan Sherstobitoff 及 Michael Rea 表示，使用 Office DDE 攻擊時，不論巨集是否啟動，攻擊者都能在受害系統中執行任意程式碼，這也是 Fancy Bear/APT 28 首次被發現使用到這種過去較不為人知的攻擊手法。

但這並不是 DDE 第一次遭到駭客濫用。上個月思科（Cisco）旗下的資安團隊 Talos 也發現一則假冒美國證券交易委員會（SEC）的網釣郵件中，駭客也是利用 DDE 協定來散布惡意程式。同月 Word DDE 協定攻擊也被發現用來散佈 Locky 勒索軟體。

- https://www.ithome.com.tw/news/118203

（資料來源：臺灣 iThome）

3.1.10、4 成公司查不到攻擊的駭客　金融業最常被盯上

近幾年來駭客攻擊金融業盜轉、盜領帳戶獲利情形時有耳聞。根據資誠（PwC）調查，當網路攻擊發生，約 4 成的受害企業表示他們無法清楚辨識罪魁禍首是誰，等於束手無策。資誠企管顧問執行董事張晉瑞表示，近幾年來駭客時常鎖定金融業做特定病毒攻擊各公司，金融業花千萬元維護資安只是基本的、要做到完備至少得破費億元。

去年第一銀行發生駭客盜領 ATM 鈔票案，損失上千萬元；而今年也同樣有遠東銀行國際匯款系統 SWIFT（環球銀行間金融電訊網路）發生了交易異常，遭駭客盜轉了 18 億元匯款到海外。

張晉瑞表示，國內企業對資安防護觀念不足，中小型金融機構因既有資源匱乏無法進行軟硬體設備升級，反而更容易被駭客盯上，他也呼籲業者不要掉以輕心。他強調，國外已有調查確認駭客所做的產業行為已創造「黑色經濟」，據傳其獲利比賣毒品還高，且有專門的產業鏈運作，「防駭已不能用傳統思維，花千萬元維護資安只是基本配套、要做到好至少上億元。」

由於 4G、5G 網路逐漸普及，近年來民眾消費型態已轉為電子交易模式。張晉瑞指出，各銀行因此不斷投入防駭資金，但國內防範機制仍有所不足。他也分析，現在駭客犯罪分 2 種，第 1 種為企業化經營，從發病毒到取款車手都是自己人；第 2 則是專賣病毒碼，讓有心人士以黑市交易、並用比特幣完成付款，因為其區塊鏈技術難以追查，因此源頭掌控不易。

張晉瑞也表示，今年以來金融業者遭駭客攻擊主要有 4 大類型，如遠銀 SWIFT 盜領案與去年一銀 ATM 盜領案都是電子郵件釣魚方式做為斷點駭入企業系統；而台新證等多家券商遭 DDoS（分散式阻斷服務攻擊），另有勒索病毒如 WannaCry 和 Petya，前者為專門綁架

個人用戶資料、後者是透過企業區網綁架企業全部資料。他也呼籲金融業應再加強資安防範。

- https://www.ettoday.net/news/20171108/1048316.htm?t=%E5%AD%98%E6%AC%BE%E5%AE%89%E5%85%A8%E5%97%8E%EF%BC%9F4%E6%88%90%E5%85%AC%E5%8F%B8%E6%9F%A5%E4%B8%8D%E5%88%B0%E6%94%BB%E6%93%8A%E7%9A%84%E9%A7%AD%E5%AE%A2%E3%80%80%E9%87%91%E8%9E%8D%E6%A5%AD%E6%9C%80%E5%B8%B8%E8%A2%AB%E7%9B%AF%E4%B8%8A

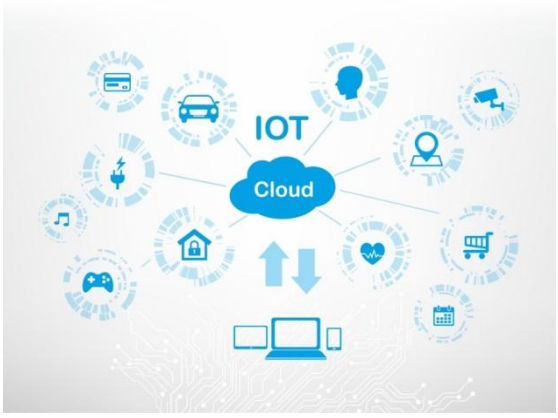
（資料來源：臺灣 ETtoday 新聞雲）

3.1.11、物聯網資安漏洞 行政院擬訂標準防堵

行政院長賴清德 11 月 2 日上午在行政院會聽取行政院資通安全處報告「當前資安情勢分析」，並在會中表示，台灣關鍵資訊基礎設施的資安威脅日增，特別是金融、資通信，以及水力、電力等設施，請資安處持續與各主管部會加強聯繫，完備各關鍵資訊基礎設施的資安防護機制。近期所發生大型分散式阻斷服務（DDoS）攻擊案例，發動來源皆以物聯網（IoT）設備為主，請相關部會在推動數位經濟產業（包含人工智慧、物聯網等）的同時，也要擴大培育包含資安人才在內的數位科技人才，並重視部會內部資安人力的安排。

行政院資通安全處處長簡宏偉出席院會後記者會時表示，政府機

關資安人才缺口約 500 人，目前措施是跟教育部合作，從學校教育培育人才，也跟國家發展委員會、經濟部合作，增進公務員資安職能培育。物聯網部分，將協調經濟部跟國家通訊傳播委員會，針對物聯網設備訂定相關資安標準，預定年底就會推出，例如現在被駭客攻擊最嚴重的是網路攝影機（IP CAM）；他指出，網路攝影機有如一台小電腦，但很多使用者都只用預設密碼，未來將規定首次啟動強制密碼更新、提高密碼複雜度等。



- https://udn.com/news/story/7240/2793830

（資料來源：臺灣聯合新聞網）

3.1.12、醫療領域 IOT 應用帶來安全新隱憂

據 IoT Tech News 報導，物聯網可說妙用無窮，包括從遠端查看家裡的情況、追蹤健身目標的進度，在開車中途改變路線以避開塞車等。但其實生活各方面不見得都要連網，畢竟裝置本身及其儲存、收集的數據就容易遭受攻擊，有被駭客竊取的風險。

隨著物聯網逐漸滲透進醫療業，可能出現不少問題。首先，醫療物聯網雖然極為便利，卻存在安全隱患。醫療設備管理患者的治療和用藥、監測和報告/傳輸有關其生命體徵或症狀的資訊，甚至管理病歷資料庫。這些資訊若遭駭客竊取，後果不堪設想。

病歷不僅包含患者健康相關資訊，還有個人身分等敏感資料，理所當然成為網路犯罪分子優先鎖定的目標。許多醫院和醫療機構負責管理大量患者的電子病歷，有些更已將網路虛擬化作為管理網路的方式。這麼多數據由須完美協調存取憑證的程式來管理，可想而知，這種管理方法絕非萬無一失。

更致命的可能性是，駭客可能會干擾由連網醫療設備收發的患者狀況相關資訊。這些設備中若有任何一個遭入侵，如病房中常見用於傳送患者生命體徵相關資訊的設備，則依賴此訊息來替患者進行必要護理的醫生和護士，在患者需要照護時就會無所適從。

另外，管理藥物的設備亦可能被網路犯罪分子劫持和操縱。因此，醫療物聯網在廣泛實施之前，須審慎考慮所有重要因素，尤其是連網設備如何防止駭客入侵，以及用戶的安全。

- https://www.digitimes.com.tw/iot/article.asp?cat=158&id=0000516173_YF22G10466LFXW4BVW627

（資料來源：臺灣 DIGITIMES）

3.2、駭客攻擊事件及手法

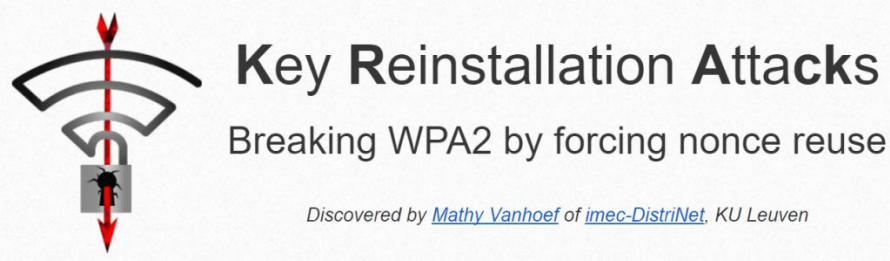
3.2.1、KRACK Detector 偵測工具，可用來避免有心人士利用 WPA2 弱點進行 KRACK 攻擊

WPA2 無線通訊協定存在弱點，駭客能操縱 KRACKS 攔截竄改 WI-FI 傳輸資料，而該弱點在於 WPA2 無線通訊協定本身，非僅涉及特定作業系統或裝備，駭客可藉此新招取得控制權及機敏資料，甚而假手受害者實行網路犯罪，其影響不容小覷，各原廠業者已陸續提供安全更新。

KRACK Detector 是一個 Python 腳本，用於檢測網路上客戶端設備的可能的 KRACK 攻擊。該腳本旨在運行在 access point(AP,一般來說即為無線網路基地台等)而不是客戶端設備上。它會監聽 Wi-Fi 介面並等待訊號交握過程中（4-way Handshake）有無重複的訊息 3(即惡意訊息)，如果有這樣的情況發生，KRACK Detector 將會阻斷該可疑的設備，阻止它發送更多的敏感資訊到 AP。

該工具目前僅支援 Linux 版本，工具使用方式可參考以下連結 2，TWCERT/CC 提醒使用者可使用該工具檢測是否遭到 KRACK 攻擊。此外仍建議用戶密切注意所屬設備之原廠官網有無更新訊息，微軟已於 10 月 10 日安全更新解決此事。未獲更新前，若處公共 Wi-Fi 環境，儘量以 HTTPS 方式 (未必無虞) 上網，最好採 VPN 保護傳輸。

- http://securityaffairs.co/wordpress/65229/hacking/krack-detector.html



3.2.2、「加入 LINE@會員、分享好友， 即可獲得折價券」，勿貪小便宜，避免個資遭竊

近日 LINE 通訊軟體流傳「台鐵 130 周年活動」，聲稱加入好友可「免費搭乘普悠瑪」或「免費領取台鐵便當」; 也有流傳版本稱高鐵歡慶 10 周年，若將訊息分享到 10 人以上群組 3 次，或分享給 20 位好友，將送雙鐵搭乘旅遊 5 日券或 7-11 百元禮券。

台鐵局及台灣高鐵公司昨雙雙發聲明澄清，從未成立任何 LINE 官方帳號，亦無舉辦相關活動，呼籲民眾不要輕信來源不明帳號或點選不明連結，若因參加此類活動而衍生任何問題或糾紛，台鐵及高鐵均無法負責。

近期常見 LINE@詐騙方式如下：

（1）轉發訊息送 1000 元家樂福禮券。

（2）加入好友送中油、7-11 折價金。

（3）加好友送 e-tag 儲值金。

●TWCERT/CC 提醒您，遇來路不明的 LINE 官方帳號，可先透過業者官網、客服等正式管道求證，不要輕易在聊天室中回覆 LINE ID、手機號碼等個資，避免個資遭竊。

- https://tw.appledaily.com/headline/daily/20171109/37840370

3.2.3、美國服飾商 Forever 21 顧客信用卡資料外洩

美國服飾商 Forever 21 在禮拜二發表聲明，他們發現有未經授權的連線從商店存取信用卡資料，一間洛杉磯未具名的資安公司正在協助調查此次事件，調查重點為 2017 年 3 月至 10 月間，但目前尚未提供進一步調查結果。

Forever 21 發言人指出，他們自 2015 年為系統引進加密機制，而此次的事件是由於部分商店的系統加密機制未正常運作而造成的。

Forever 21 建議顧客若最近接獲異常刷卡訊息，請提高警覺，以免信用卡遭盜刷。

●TWCERT/CC 提醒您，應僅在有安全連線的狀況下使用信用卡交易，

且平時應注意異常刷卡通知，以免遭盜刷。

●https://www.cyberscoop.com/forever-21-data-breach/

3.2.4、英國典當業之電商購物網站客戶資料遭駭

英國的一間典當公司 Cash Converters 表示該企業在 2017 年 9 月期間發現其購物網站遭駭客入侵，其客戶資料遭竊，遭非法存取的資料包含個人資料、密碼、歷史購物資訊。該企業已向英國及澳大利亞當局通報此事件，並呼籲用戶若有在該平台購物，應更換其密碼。

●TWCERT/CC 提醒台灣用戶，台灣許多小型零售業亦提供網路購物平台供消費者線上消費，建議用戶在選擇購物網站時

(1)選擇有提供 https 加密傳輸購物網站，且平時應注意異常刷卡通知，以免遭盜刷。

(2)用戶的帳號及密碼勿同一組在多平台使用，並且使用 20 位以

上英文數字符號混用的強密碼

(3)企業提供電商平台有義務保護其客戶資料，強化網站的資訊安全，以免觸犯個人資料保護法

- http://securityaffairs.co/wordpress/65750/data-breach/cash-converters-data-breach.html

3.2.5、Uber 證實遭駭，5700 萬筆資料外洩

根據 Bloomberg 報導，Uber 在 2016 年 10 月發生重大資安事件，導致 5000 萬名乘客姓名、電子郵件、手機號碼外洩，此外有 700 萬名 Uber 駕駛的個資遭竊(包括 60 萬美國駕駛的駕照)。經外部鑑識專家的鑑定，行程地點紀錄、信用卡卡號、銀行帳號、社會安全碼和

出生日期等資料未遭外洩。

Uber 認為，乘客方面無須採取任何動作，因為未發現任何證據顯示有與此事件相關的詐騙或濫用行為發生。Uber 會持續監控受影響的帳戶，並標示相關帳戶提供進一步的詐騙防護。

- http://www.cna.com.tw/news/firstnews/201711220026-1.as

3.3、軟硬體漏洞資訊

3.3.1、Oracle 緊急釋出更新修復 Identity Manager 漏洞

Oracle Identity Manager(OIM)產品存在極嚴重弱點，CVSS 評分為 10，據判 OIM 預設帳號密碼應屬 hard coded 或者根本沒有，故駭客無須身分驗證即可輕鬆取得遠端系統控制權，危及企業整體個資，Oracle 就各版本軟體提供對應之安全更新。

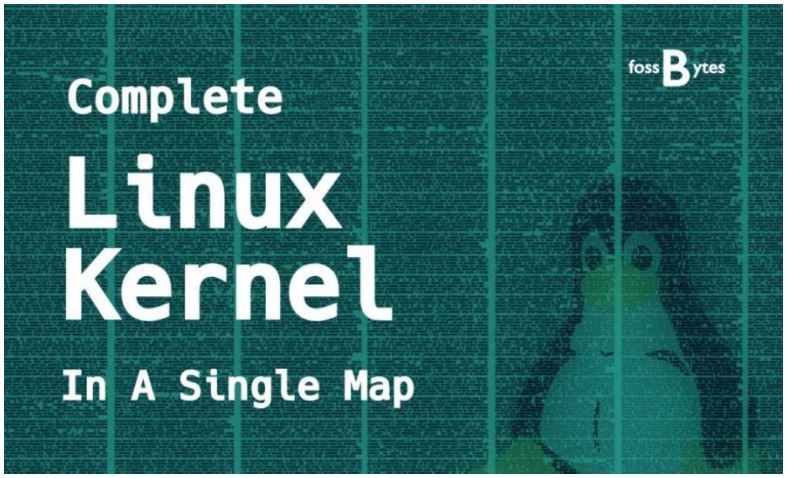
3.3.2、Oracle Tuxedo 軟體平臺存在嚴重漏洞 JoltandBleed

Oracle 旗下 Tuxedo(Transactions for Unix, Extended for Distributed Operations)係一高端中介軟體平臺，提供異質運算服務，也是應用軟體伺服器(application server)的核心，若無 Tuxedo，用戶僅能透過 sql 聯繫資料庫，而 Tuxedo 和 jolt server 須安裝於同一設備作為 application server，Tuxedo 有 5 項漏洞均與 jolt 協定有關，駭客可藉 memory leak 接管 PeopleSoft 個資異動權限；暴力破解 DomainPWD 密碼；利用堆疊溢位接觸關鍵或完整資料及導致 DoS，Oracle 就相關版本提供安全更新。

3.3.3、Linux Kernel 內 ALSA 定序介面、waitid()系統呼叫存在弱點導致系統權限遭剽竊

Linux Kernel 2 項弱點，發生於 ALSA(Advanced Linux Sound Architecture) 定序介面、waitid()系統呼叫，駭客加工 ioctl call 夾

在惡意程式中，觸發多個 procedure 搶著無規律輸出，形成競爭狀態並導致 ALSA 記憶體 Use After Free；waitid()回傳 child procedure 識別碼(PID)與結束狀態值(status)出錯，觸發記憶體崩潰，本機駭客可藉此提升至系統管理者，執行任意程式，官方就相關版本軟體提供對應之安全更新。

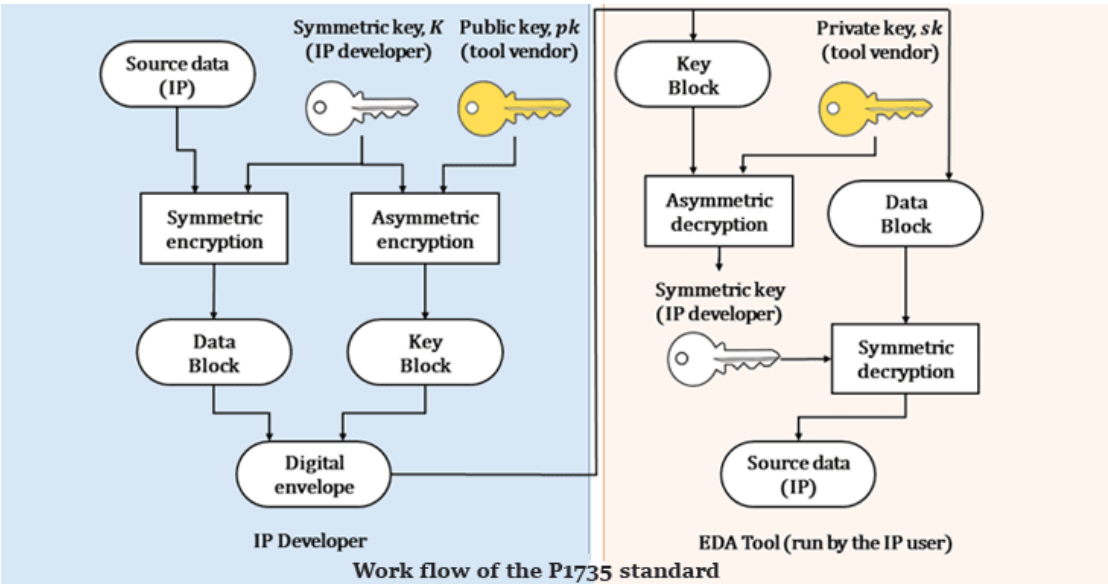


3.3.4、Linux kernel 經檢測 USB 驅動程式漏洞多達數十項

經 Google 安全專家實測，找出 Linux 核心 USB 次系統驅動程式漏洞多達 79 個(本文摘列)，幾乎都能導致服務中斷，亦可能使駭客插入惡意腳本或提升權限，唯必需透過 USB 裝置直接觸發，相關漏洞未悉數配賦 CVE 編號，亦無安全更新。

3.3.5、IEEE P1735 規範之加密流程出現 7 漏洞，將危及電子設計智財權

研究報告 Standardizing Bad Cryptographic Practice 指出，IEEE P1735 標準之加密流程，重機密性而忽略完整性，因而存在弱點，駭客可藉此盜竊智慧財產權、竄改原創設計、插入硬體木馬，影響遍及多數半導體產業，恐損及業者收益與商譽，各廠安全更新仍處發展階段，基於資安顧慮，漏洞細節未公開。



Work flow of the P1735 standard

3.3.6、OpenSSL 釋出新版修補資料外洩漏洞

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 協定以避免竊聽，現存在 2 項弱點，bn_sqrx8x_internal()函式及 X.509 IPAddressFamily 憑證皆有可能洩漏系統資訊，遭致駭客遠端截收，OpenSSL 就相關版本軟體提供對應之安全更新。

3.3.7、LibreOffice 釋出新版修補記憶體寫入錯誤

免費開放辦公室套裝軟體 LibreOffice，系列產品 Impress 及 Writer 存在 out-of-bounds memory write 瑕疵，駭客可藉此變造惡意檔案格式，造成服務阻斷及冒用身分執行任意程式，LibreOffice 提供修補後軟體版本。

3.3.8、Apache 釋出 OpenOffice4.1.4 版修補漏洞

開放源碼的辦公室軟體 Apache OpenOffice(AOO)，其 Impress 及 Writer 存在 out-of-bounds memory write 瑕疵，駭客可藉此變造惡意檔案格式，造成服務阻斷及冒用身分執行任意程式，Apache 提供升級版本修補之。

3.3.9、Microsoft 釋出 11 月安全更新修補 53 項漏洞

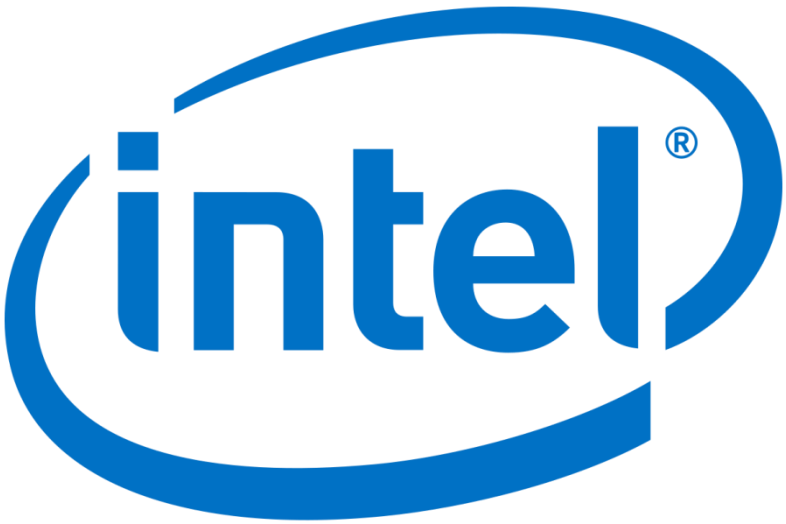
Microsoft 多項產品存在弱點，包含存在 Equation Editor 元件長達 17 年之 stack buffer overflow 漏洞，歸類於 out-of-process COM server，不受 DEP 保護，駭客可藉此攻擊作業系統、瀏覽器、OFFICE，製造惡意檔案、request、網頁、URL，能觸發記憶體錯誤，繞過安全檢查機制，挖掘機密資料，執行惡意代碼並造成服務中斷，官方就相關版本軟體提供對應之安全更新。

3.3.10、EMC 修補 ScaleIO 與 RSA® Authentication Manager 數個漏洞

EMC 旗下 2 款產品存在弱點，其一是軟體定義式儲存(SDS)的 ScaleIO，亦屬企業級 Server SAN(Storage Area Network)系統，其暫存 log 易暴露機敏個資、解析器錯誤導致 DoS、尚有 Buffer Overflow 衍生擴權執行命令之事件；另有 RSA Authentication Manager 出現瑕疵，駭客可藉此執行 Cross-Site Scripting 程式碼，取得受害者資料並竄改，EMC 提供相關升級版本軟體。

3.3.11、特定 Intel 處理器技術多組漏洞導致代碼執行或提權事件

Intel 管理引擎(Management Engine，ME)、受信任的執行引擎(Trusted Execution Engine，TXE)及伺服器平台服務(Server Platform Services，SPS)存在多個安全漏洞，部分允許攻擊者於本地用戶的目標系統進行提權與執行任意程式碼。



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
2017/12/21、2017/12/28	白帽駭客認知班	【資安訓練課程】白帽駭客認知班 主辦單位：中國文化大學進修推廣部、NTC.im 人才培訓中心 日期:2017 年 12 月 21 日 (四) 、2017 年 12 月 28 日 (四) 地點：台北市建國南路二段 231 號 (中國文化大學進修推廣部) 線上報名連結： http://my.sce.pccu.edu.tw/MS/Detail.aspx?ProdId=8OM4_A6121&Source=Search&SourceKey=250799&CataId=0407 資料來源： https://www.accupass.com/event/1712031734497 05

時間	研討會/課程名稱	研討會相關資料
		9050030 活動概要： 有感覺自己使用的桌電、筆電突然間變的很慢？或是在開機沒使用的狀況下感覺（或聽到）硬碟瘋狂的運轉嗎？有時一個人時，感覺不是背後有人，而是電腦很像在自己工作中…。事實上在少部分的情況下，你的電腦是安全的。這些情況是公司資訊部門的資訊安全防護，而你又從來不安裝來路不明的非授權軟體，或是有資安敏感度，從不點擊或開啟美圖、影片、音樂、網站等…。好了，所以如果你已經感覺到不安，如果你想要知道更多不安全的可能，那我們從駭客的視角學習，相信是開啟認知的第一步。 這門課是大數據技能養成系列的課程，我們將以白帽駭客的工具做教學，使用 2.5 小時的快講，讓參與者可以從不知道到有認知能力，在我們準備好的環境下，逐步的操作駭客工具，知道駭客如何下手及如何防禦，適合完全沒有駭客經驗的人學習。 關於本認知班的教學，出發點是養成學員對於安全的認知，而不是養成一個駭客，如並非期望增進資安認知的學員，不適合參與這門課程。
2017/12/19	2018 資安趨勢論壇	【資安研討會】2018 資安趨勢論壇 主辦單位：資安人 日期：2017 年 12 月 19 日(二) 09：00~12：30 地點：台北文創大樓 6 樓會議室 線上報名連結： https://www.informationsecurity.com.tw/seminar/isevent20171219/register.aspx 資料來源： https://www.informationsecurity.com.tw/Seminar/ISevent20171219/index.htm 活動概要： 資安趨勢論壇將分享從資安立法的角度、資訊長的角色扮演、銳不可抵的金融科技、全球網際威脅的整體作戰必要

時間	研討會/課程名稱	研討會相關資料
		的防禦，歡迎您們再度參與。
2017/12/12-12/15	2017 Taiwan Internet Forum-與你我有關的資訊安全	【資安研討會】2017 Taiwan Internet Forum-與你我有關的資訊安全 主辦單位：TWNIC 財團法人台灣網路資訊中心 日期:2017 年 12 月 12 日 (二) ~ 2017 年 12 月 15 日 (五) 地點：台大醫院國際會議中心 線上報名連結： https://opm.twnic.net.tw/summit2017/online.html 資料來源： http://www.ipv6.org.tw/summit2017/index.html 活動概要： 網際網路的快速發展，不僅造就新一波的產業革命，更在不斷推陳出新的應用服務下，引領現代生活的改變與革新。在近來的網路發展趨勢中，新一代的 IPv6 網路位址帶來了新的應用與發展的契機，更創造了無限商機。當全球網路使用者已超過 31 億使用人口，而台灣更已高達 1 千 9 百萬使用人口的整體網路環境下，與網路相關的經濟活動更與網路建立了高度的依存關係；網路已經成為生活當中的一部份，網路也消弭了彼此溝通的界線，站在全球網路發展的重要轉變時刻，台灣如何與世界協同合作並掌握發展趨勢，「2017 Taiwan Internet Forum」敬邀我國網路產官學共同參與討論。

第 4 章、本月份事件通報統計

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，本月共收到通報共 544 筆，以下為本中心所蒐整之各項統計數據，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。

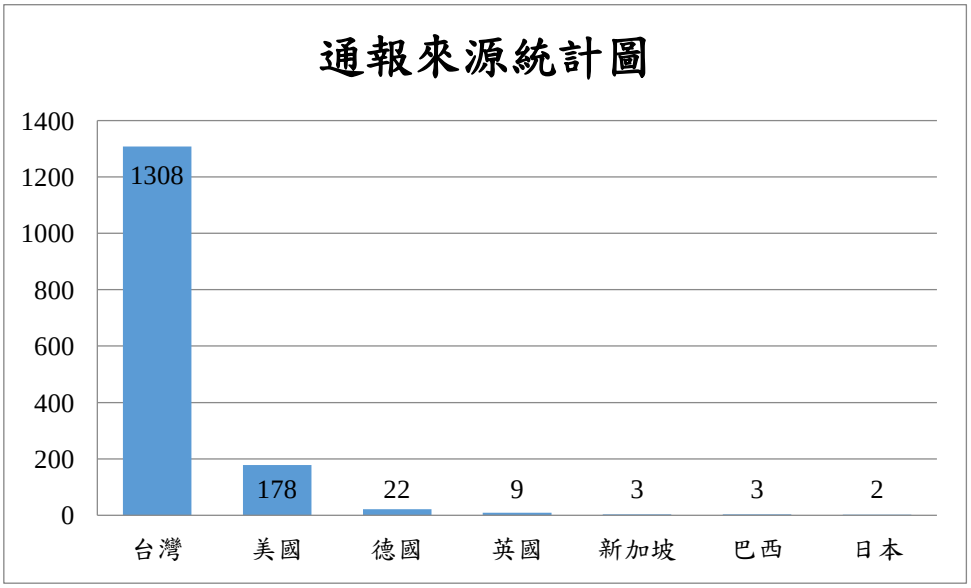


圖 1、通報來源統計圖

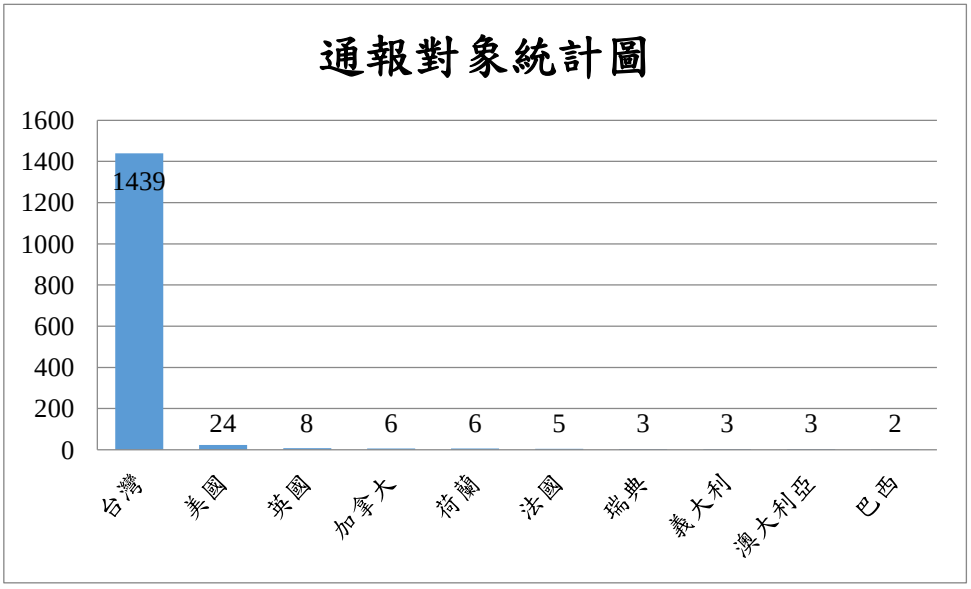


圖 2、通報對象統計圖

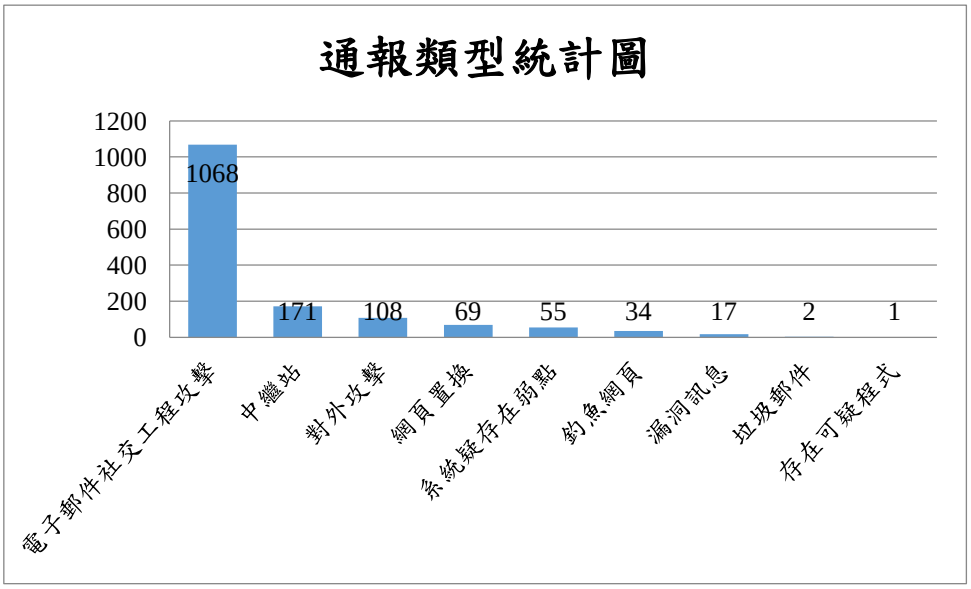


圖 3、通報類型統計圖

本月通報主要來源來自國外固定合作資安夥伴提供之情資，本中心接獲大量疑因遭駭客以電子郵件社交工程攻擊方式所獲之電子郵件帳號及密碼外洩清單，立即分析清單內電郵網域屬「.tw」之單位，逐一透過查找之聯絡方式聯繫通報權責單位，提醒務必將通報之電郵

帳號密碼更新。

電子郵件社交工程攻擊即為透過傳送電子郵件，假冒親友或公司主管客戶等相關寄件者，以聳動或針對收信者業務之偽冒標題及信件內容，吸引誘騙收件者好奇或信任，開啟郵件進行非法攻擊行為。TWCERT/CC 建議，切勿輕易打開可疑或不明電子郵件、點選郵件內的連結、下載附件檔案，或回傳個人或公司資訊、資料等，並即使來自可信任之寄件者亦應與對方確認，以免遭駭客利用。

除通報至 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 66%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

資料日期：106 年 12 月 10 日

編　　輯：曾佩雅

服務電話：03-4115387

市話免付費電話：0800-885-066

電子郵件：twcert@cert.org.tw

網　　址：https://www.twcert.org.tw/

Facebook：https://www.facebook.com/twcertcc

若有任何問題或建議，請通知我們，也歡迎您的不吝指教。