TWCERT/CC 資安情資電子報

2019 年 1 月份

目錄

第 1 章、 封面故事

台灣電腦網路危機處理暨協調中心(TWCERT/CC) 於 2019 年 1 月 1 日由台灣網路資訊中心(TWNIC)接力營運！

台灣電腦網路危機處理暨協調中心(TWCERT/CC)自 1998 年 9 月於國立中山大學成立；並於 2010 年 1 月由台灣網路資訊中心 (TWNIC) 接手維運；再於 2014 年 8 月起改由國家中山科學研究院承接。而今年(2019) 1 月 1 日起，為因應國家資安政策，將再次轉由 TWNIC 繼續推動 TWCERT/CC 的各項業務。

TWCERT/CC 承接過往情資交流、發布、資安事件處理、通報等之各種相關業務，同時也會持續發布資安新聞、駭侵事件、漏洞資訊，以及資安活動，供民眾參考並提高資安防範意識。

未來 TWCERT/CC 將會持續提高協調中心之任務和角色定位，收集國內外之資安事件，整合國內具協處資安事件之公私部門機關(構)，協助企業解決資安事件，以強化台灣資安防護能量。

● TWCERT/CC 服務項目：

1. 事件通報處理
2. 資源協調應變
3. 情資蒐整分享
4. 技術研究發展
5. 國際交流合作

● TWCERT/CC 資訊提供：

1. 資安新聞
2. 駭侵事件
3. 漏洞資訊
4. 資安活動

- 有任何資安事件發生，請放心通報我們！中心均簽署完整保密同意書，不會外洩任何一絲個人資訊。

- ✓ 官網：https://twcert.org.tw/
- ✓ Email：twcert@cert.org.tw
- ✓ 免付費電話：0800-885-066
- ✓ Facebook：台灣電腦網路危機處理暨協調中心-TWCERT/CC

- ✓ Instagram：twcertcc
- ✓ Twitter：@TWCERTCC

- TWCERT/CC 擁有 Root CVE 權限！若有任何系統漏洞，歡迎通報，TWCERT/CC 會進行處理、分析、通報，並發布其 CVE 編號。
  - ✓ 詳情請見：https://twcert.org.tw/subpages/ServeThePublic/public_document_details.aspx?id=65

- 歡迎所有有興趣合作之企業/單位和 TWCERT/CC 接洽。
  - ✓ 一般企業：和 TWCERT/CC 交換資安情資。本中心有任何最新威脅資訊會第一時間通知。同時企業若有任何資安問題，TWCERT/CC 會第一時間進行通報和合作之資安廠商轉介並處理。
  - ✓ 資安相關企業：和 TWCERT/CC 交換情資、合作建立資安資料庫，讓該資安企業之資安系統可經由彼此情資交流而更加完善。
  - ✓ CERT/CSIRT 組織或有意建立之企業：TWCERT/CC 歡迎各位企業/組織加入 CERT/CSIRT 聯盟。每半年進行一次聯盟會議，成員彼此交流 CERT/CSIRT 運作、處理經驗，共同提升 CERT/CSIRT 運作能量。

- 合作夥伴請見：https://twcert.org.tw/subpages/aboutus/partner.aspx

- 除一般情資交流合作，有興趣者歡迎和 TWCERT 簽署合作備忘錄 (MoU)，穩定彼此交流合作，加深資安防範能量。

第 2 章、 國內外重要資安新聞

2.1、國內外資安政策、威脅與趨勢

2.1.1 研究人員首次發現隱藏在 Windows UEFI 的 Rootkit 惡意軟體攻擊事件

長期追蹤各種攻擊事件的資安公司 ESET 指出，他們發現全球首個攻擊 Windows UEFI，隱藏在系統主機板 Flash 記憶體中的 Rootkit 型惡意程式。

該單位研究員 Fédréic Vachon 在於德國萊比錫舉辦的一場研討會上分享了這個案例。他指出，能夠隱藏在系統 Flash 中的 Rootkit 型惡意程式，近年來是大家的研究重點，但過去一直沒有掌握真實的攻擊事件。

這支被發現的 Rootkit 惡意程式名為 LoJax，是由惡意攻擊團體 Sednit 修改 Absolute Software 公司的產品 LoJack 而來；這個軟體的作用是幫助筆記型電腦用戶在自己的筆電被竊時，仍能從其他 PC 存取筆電上的資料。

Sednit 利用 LoJax 2009 版本的漏洞，將惡意程式透過釣魚郵件夾檔感染受害者的 Internet Explorer 瀏覽器，再將 LoJax 安裝到 UEFI 中。由於這個軟體隱藏在電腦的 UEFI 用以控制周邊設備的 SPI(Serial Peripheral Interface) Flash 記憶體之中，而且會在作業系統和防毒軟體啟動前先執行，因此即使電腦的硬碟遭到更換，該軟體仍然存在且可運作。

一旦感染，用戶除了清除整個 SPI Flash 記憶體或丟棄該主機板，無另外方法可移除。

ESET 在去年九月起開始偵測到透過 LoJax 發動的攻擊事件，主要的受害者是中歐及東歐各國政府單位的電腦主機。

Vachon 表示，用戶可以啟用 UEFI 中的 Secure Boot 功能，並且經常更新韌體，以避免這類惡意程式造成傷害。

圖片來源：https://threatpost.com/uefi-rootkit-sednit/140420/

- 資料來源：
  1. https://threatpost.com/uefi-rootkit-sednit/140420/
  2. https://github.com/eset/malware-ioc/blob/8864a5aa6c98b95d4fd9624b5f36c3dee65fdeba/sednit/README.adoc
  3. https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf

2.1.2 密碼安全公司 SplashData 公布 2018 年度最不安全密碼前 100 名

密碼安全公司 SplashData 在分析 2018 年外洩在網路上的 5 百萬筆密碼情資後，公布 2018 年度最不安全密碼前 100 名，並指出使用者依舊使用容易被猜到的簡單密碼，導致自身帳號安全暴露在風險之中。本年度中，「123456」仍蟬連最多人使用的弱密碼寶座，約有 3%的人使用此密碼；另約有 10%的人使用前 25 名的弱密碼。

前 25 名弱清單如下：

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou
11. princess
12. admin
13. welcome
14. 666666
15. abc123
16. football
17. 123123
18. monkey
19. 654321
20. !@#$%^&*
21. charlie
22. aa123456
23. donald
24. password1
25. qwerty123

完整清單請參考：https://www.teamsid.com/100-worst-passwords/

- TWCERT/CC 建議：
  1. 密碼建議使用 12 個字元以上且英文、數字、符號混合。
  2. 應避免多個服務使用同一組密碼，以免遭到撞庫攻擊。
  3. 定期更換各帳號密碼。

圖片來源：https://www.teamsid.com/100-worst-passwords/

- 資料來源：
  1. https://www.teamsid.com/100-worst-passwords/
  2. https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/

2.2、駭客攻擊事件及手法

2.2.1 萬豪集團遭駭，約 5 億喜達屋客戶資料外洩

萬豪國際集團(Marriott)是一家跨國酒店管理公司，曾收購喜達屋(Starwood)房產，其中包括以下酒店：喜達屋品牌(W 酒店、瑞吉酒店)、喜來登酒店及度假村、威斯汀酒店及度假村、Element 酒店，雅樂軒酒店，豪華精選酒店、Tribute Portfolio、艾美酒店及度假村、福朋喜來登酒店及參與喜達屋尊榮顧客（Starwood Preferred Guest, SPG）計劃的設計酒店。喜達屋品牌的分時度假酒店也包括在內。

該公司 11 月 30 日宣布，發現自 2014 年以來，有未經授權存取喜達屋酒店客戶預訂資料庫。目前尚不清楚系統是如何被攻擊，但約有多達 5 億客人受到影響。

該事件僅涉及喜達屋預訂資料，因為萬豪酒店擁有在不同網路上運行的獨立系統。會影響的是 9 月 10 日或之前在喜達屋酒店預訂的任何客戶。

攻擊者存取和複製的資訊包括訪客姓名及可能的實際地址和電子郵件地址。然而，對其中 3.27 億人，暴露的資料還包括護照號碼、喜達屋尊榮顧客（SPG）帳戶詳細資訊、出生日期、性別、到達和出發資訊，預訂日期和通訊喜好。

付款資訊(卡號和到期日)也存於資料庫中，雖使用 AES-128 算法加密，但萬豪尚未確定解密元素(密鑰和算法)是否被取得，若是將允許攻擊者獲得信用卡資訊。

對於那些受影響的人，萬豪為 WebWatcher 提供 1 年免費訂閱 WebWatcher 監控共享個人資訊的網站，並在檢測到客戶的資訊時通知客戶。此優惠僅適用於美國，加拿大和英國的會員。

該企業在 9 月 8 日其內部安全工具偵測到企圖存取該資料庫的行為而發出警報。因此通知資安專家確定通知的原因，調查顯示，自 2014 年以來，身份不明的一方未經授權存取喜達屋網路。

萬豪在此事件的資訊網站表示，發現未經授權的一方已經複製並已加密的資訊，即採取措施將其刪除。2018 年 11 月 19 日，萬豪成功將資料解密，並確定內容來自喜達屋客人預

訂資料庫。

該酒店公司設立了一支援中心，提供多種語言，每日供想要了解此事件的人士使用，並向受影響的客戶(電子郵件地址已被洩露)發送電子郵件。

萬豪警告，有心人士可能會試圖利用網路釣魚來誘騙人們提供機敏的資訊細節。出於這個原因，受影響的個人應該警覺，其資料外洩警報純粹僅提供資訊，不會有其他要求，其官方電子郵件地址為：starwoodhotels@email-marriott.com。

- TWCERT/CC 建議：
  客戶會員如接獲該公司電子郵件，應確認信件來源，並切勿任意點選信件附件或連結，任何操作應透過官方線上服務完成，以免遭有心人士利用。

圖片來源：
https://www.bleepingcomputer.com/news/security/marriott-data-breach-affects-500-million-starwood-guests/

- 資料來源：

1. http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/
2. https://krebsonsecurity.com/2018/11/marriott-data-on-500-million-guests-stolen-in-4-year-breach/
3. https://krebsonsecurity.com/2018/12/what-the-marriott-breach-says-about-security/
4. https://www.bleepingcomputer.com/news/security/marriott-data-breach-affects-500-million-starwood-guests/
5. https://www.bankinfosecurity.com/starwood-a-11751
6. https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html
7. https://www.cyberscoop.com/marriott-data-breach-starwood-hotels-gdpr/
8. https://www.darkreading.com/attacks-breaches/massive-starwood-hotels-breach-hits-500-million-guests/d/d-id/1333379
9. https://www.hackread.com/marriott-hotel-data-breach-500m-guests-data-stolen/
10. https://www.helpnetsecurity.com/2018/11/30/marriott-data-breach-reactions/
11. https://www.infosecurity-magazine.com/news/marriot-starwood-hack-500-million/
12. https://www.itnews.com.au/news/marriotts-starwood-hack-hits-up-to-500m-guests-516350
13. https://blog.malwarebytes.com/101/2018/11/marriott-breach-impacts-500-million-customers-heres-what-to-do-about-it/
14. https://motherboard.vice.com/en_us/article/kzvgbm/marriott-hotels-500-million-data-breach-hack
15. https://nakedsecurity.sophos.com/2018/11/30/huge-marriott-breach-puts-500-million-victims-at-risk/
16. https://www.reuters.com/article/legal-us-marriott-intnl-cyber/marriotts-starwood-database-hacked-500-million-may-be-affected-idUSKCN1O02VH
17. https://arstechnica.com/information-technology/2018/11/marriott-breach-leaves-500-million-exposed-with-passport-card-numbers-stolen/
18. https://securityaffairs.co/wordpress/

78578/data-breach/marriot-starwood-data-breach.html
19. https://www.securityweek.com/marriott-hit-massive-data-breach-500-million-starwood-customers-impacted
20. https://thehackernews.com/2018/11/marriott-starwood-data-breach.html
21. https://www.theregister.co.uk/2018/11/30/marriott_starwood_hotels_500m_customer_records_hacked/
22. https://www.tripwire.com/state-of-security/security-data-protection/marr iott-reveals-security-incident-involving - starwood-reservation-database/
23. https://www.welivesecurity.com/2018/11/30/marriott-starwood-data-breach-response/
24. https://www.zdnet.com/article/marriott-announces-data-breach-affecting-500-million-hotel-guests/
25. https://techcrunch.com/2018/11/30/starwood-hotels-says-500-million-guest-records-stolen-in-massive-data-breach/
26. https://answers.kroll.com/zh/index.html

2.2.2 BeatStars 音樂平台遭網頁置換攻擊，官方表示無資料外洩

BeatStars 是家社交化音樂市場和經銷企業。平台上有超過 35 萬音樂製作人和唱片藝術家合作項目，同時向全球銷售、分享自己的音樂作品。

107 年 12 月 5 日，BeatStars 披露一起安全性漏洞。其 CEO，Abe Batshon 在 Twitter 上的 Periscope 直播節目中透露，該網站週一停機的神秘原因是未經授權存取其伺服器。

Batshon 表示，在 12 月 4 日星期二晚上，發現極不尋常的行為，有人試圖進入他們的伺服器，企圖存取資料庫以及運行代碼。

震驚之餘，其工程團隊 24 小時內不間斷地調查，試圖釐清情況與原因，並通知相關部門，承諾提供駭客存取的最新資訊。

目前，根據網上分享的 BeatStars 網站截圖，這一事件導致該網站遭到大規模網頁置換攻擊，Batshon 在直播過程中證實該網站遭攻擊，表示清楚這次襲擊的動機，且能猜測關於駭客可能身分。

Batshon 表示，攻擊者試圖大規模刪除更改系統內容和資料庫。攻擊發生後，沒有使用者內容丟失，財務資料也沒有被洩露，因該網站沒有存儲支付細節。目前尚不清楚駭客是否存取了使用者的個人記錄。

圖片來源：
https://www.zdnet.com/article/beatstars-discloses-security-breach-in-twitter-live-stream/

● 資料來源：
1. https://www.zdnet.com/article/beatstars-discloses-security-breach-in-twitter-live-stream/
2. https://twitter.com/BeatStars/status/1069803712800010240
3. https://twitter.com/AyeNuWAV/status/1070016705781481472
4. https://twitter.com/bogbeatz/status/1070018118150316032
5. https://twitter.com/YDMGProd/status/1070028480388235264

2.2.3 知名問答網站 Quora 遭駭，約 1 億用戶資料外洩

Quora 是廣受歡迎的問答型社群網路服務網站，由 Facebook 前僱員查理·切沃(Charlie Cheever)和亞當·安捷羅(Adam D' Angelo)於 2009 年 6 月創辦。在 2009 年 12 月推出測試版，隨後在 2010 年 6 月 21 日向公眾開放。

2018 年 12 月 3 日，Quora 遭遇重大資料洩露，未知的駭客入侵其系統，遭竊取之用戶資料多達 1 億。

該公司向受影響的用戶通報此事件，並重置他們的密碼作為預防措施，同時也向執法部門報案，並聘請資安鑑識公司協助調查。

Quora 調查其安全性漏洞，發現 11 月 30 日惡意第三方未經授權存取某系統，部分用戶資料遭竊。

外洩的資料包括姓名、電子郵件、雜湊密碼、從連結網路導入的資料、對外發布的內容和網路行為 (例如問題、答案、評論和投票) 以及不公開的內容和網路操作 (例如應答請求、降低投票和直接消息)。

Quora 表示，雖密碼是加密的(每個使用者的雜湊值使用不一樣的 salt)，但盡量不要多個服務使用相同密碼，並建議用戶更改密碼。

屬於匿名發佈使用者的資料和財務資料和社保號碼沒有外洩問題，因為 Quora 平臺沒有使用這些資料。

Quora 表示已查明外洩的原因，並已採取解決措施，但無透露技術細節，該公司聲明將努力降低事件的影響，避免未來出現安全性漏洞。

圖片來源：https://www.quora.com/

● 資料來源：
1. https://www.bleepingcomputer.com/news/security/quora-hacked-100-million-users-data-exposed/
2. https://blog.quora.com/Quora-Security-Update
3. https://help.quora.com/hc/en-us/articles/360020212652
4. https://www.bankinfosecurity.com/b

logs/question-did-quora-hack-expose-100-million-users-data-p-2690
5. https://www.nytimes.com/2018/12/04/technology/quora-hack-data-breach.html
6. https://www.cbsnews.com/news/quora-data-breach-exposes-100-million-users-personal-info-2018-12-04/
7. https://www.cyberscoop.com/quora-hacked-100-million-users/
8. https://www.darkreading.com/threat-intelligence/quora-breach-exposes-information-of-100-million-users/d/d-id/1333397
9. https://www.hackread.com/quora-hacked-data-of-100-million-users-stolen/
10. https://www.helpnetsecurity.com/2018/12/04/quora-data-breach/
11. https://www.infosecurity-magazine.com/news/quora-breach-hits-100-million/
12. https://www.itnews.com.au/news/quora-hacked-about-100-million-user-accounts-leaked-516470
13. https://motherboard.vice.com/en_us/article/d3b43x/quora-data-breach-hackers-100-million-users
14. https://securityaffairs.co/wordpress/78657/data-breach/quora-data-breach.html
15. https://www.securityweek.com/quora-data-breach-hits-100-million-users
16. https://news.softpedia.com/news/quora-suffers-data-breach-users-names-emails-encrypted-passwords-exposed-524084.shtml
17. https://thehackernews.com/2018/12/quora-hack.html
18. https://www.theregister.co.uk/2018/12/04/100_million_quora_passwords/
19. https://www.tripwire.com/state-of-security/security-data-protection/security-incident-potentially-exposed-100-million-quora-users-personal-data/
20. https://www.zdnet.com/article/quora-discloses-mega-breach-impacting-100-million-users/

2.2.4 美國太空總署員工資料遭不明存取，影響範圍與數量正在調查中

繼 2011 年和 2016 年曾遭遇安全漏洞事件，美國國家航空暨太空總署（NASA）於 2018 年 12 月 19 日承認今年早些時候遭駭客入侵。

在發給所有員工的內部備忘錄中，該機構表示，一名未知的入侵者可能存取其中一台存儲當前和前任員工個人資料的伺服器。 NASA 表示，社會安全號碼也受到了損害。

該機構表示，近兩個月前的 10 月 23 日發現駭客行為。目前尚不清楚為什麼該機構等待近兩個月方通知員工，但美國執法部門通常會要求被駭客入侵的組織在調查事件時推遲通知受影響的受害者。

美國國家航空暨太空總署證實，現正與聯邦網路安全合作夥伴協同檢查伺服器，以確定潛在資料洩漏的範圍，並識別可能受影響的人，但不認為其他任務都受到駭客攻擊。

該機構仍然不知道駭侵的範圍和受影響員工數量。美國國家航空暨太

空總署表示，正通知所有員工，以便可以針對可能的欺詐採取對策，作為預防措施。

NASA 助理署長 Bob Gibbs 在備忘錄中表示，從 2006 年 7 月到 2018 年 10 月，那些在中心之間加入、與該機構分離和/或在中心之間轉移的 NASA 公務員可能受到影響。

並補充表示，一旦確定，NASA 將向過去和現在的個人識別資訊 (Personally Identifiable Information, PII) 受影響的員工提供具體的後續資訊，包括提供身份保護服務和相關資源，而對駭客的調查則「需要時間」。

圖片來源：
https://www.zdnet.com/article/nasa-discloses-data-breach/

- 資料來源：
  1. https://www.zdnet.com/article/nasa-discloses-data-breach/
  2. http://spaceref.com/news/viewsr.html?pid=52074

2.2.5 知名咖啡連鎖店 POS 系統發現異常活動，客戶信用卡資訊可能外洩

美國咖啡連鎖店 Caribou Coffee 在發現未經授權訪問其 POS 系統後宣布其駭侵事件。

該公司在其總共 603 個點中列出受影響的 239 家商店，這些商店大約佔其所有站點的 40%。

影響範圍包括在 2018 年 8 月 28 日和 2018 年 12 月 3 日間，在受影響的商店中使用信用卡或簽帳金融卡的所有客戶。

受影響客戶應顧慮其卡片詳細資訊可能遭洩露並採取預防措施，例如要求更換卡、查看信用卡報告，以及參加身份保護計劃。

Caribou Coffee 官方表示，他們在 10 月發現一些錯誤，當時其 IT 員工透過其安全監控流程被警告其網路上有「異常活動」。

該公司表示，在與專家調查資料洩露的網路安全公司 Mandiant 的專家合作的兩天後，Mandiant 告知 Caribou Coffee，發現了公司 POS 系統的未經授權訪問。

這也暴露了一些咖啡店的客戶資料，Caribou Coffee 表示，入侵者可能已經暴露並收集了姓名、卡號、有效

期和卡安全碼。

Caribou Coffee 官方表示，透過公司網站進行的信用卡支付不會受到影響，因為此支付系統與店內 POS 系統是分開的，並相信這次駭侵行為已得到控制。

該公司表示正與信用卡公司定期溝通，並向他們提供必要的資訊，以通知可能已發行受影響信用卡的銀行，用戶可以透過其主頁上公佈的公司資料洩露通知查閱受影響商店列表。

圖片來源：https://www.zdnet.com/article/caribou-coffee-chain-announces-card-breach-impacting-239-stores/?fbclid=IwAR2tIebt9eTiF0CipuN7Ha2d29H66xWDScoRp9-JlFzT1rL7OpBRad9zrTE

- 資料來源：
  1. https://www.zdnet.com/article/caribou-coffee-chain-announces-card-breach-impacting-239-stores/?fbclid=IwAR2tIebt9eTiF0CipuN7Ha2d29H66xWDScoRp9-JlFzT1rL7OpBRad9zrTE
  2. https://assets.coffeeandbagels-static.com/cariboucoffee/Data-Security-Notice.pdf?fbclid=IwAR1xXlHCdm3WEFD9bAKINc0fTPiZyobP8wKNEnDKW0YU0_k-N-UN0Rbpqjk

2.3、軟硬體漏洞資訊

2.3.1 高階腳本語言 Perl 測出多種 overflow 觸發情境

Perl 是高階、通用、直譯、動態的腳本程式語言，師法眾多語言特性(C、sed、awk、shell)，廣泛應用於各領域，經分析數個原始程式，察覺因輸入值安全過濾欠周，易肇生 segmentation fault，如 Perl_my_setenv( )函數若遭遇本機輸入鉅量字串，將觸發整數溢位而破壞記憶體配置精確性；而遠端攻擊者經由變造之正規表示式語法，可衍生 heap-buffer-overflow，迫使 S_grok_bslash_N( )將機敏資訊寫入 stderr 位置，可越界讀取而獲悉重要設計關鍵，另惡意正規表示式亦可導致 S_regatom( )函數溢位後，發動 RCE 攻擊，新版 Perl 已釋出並修補缺陷。

圖片來源：https://hsto.org/getpro/habr/post_images/707/723/436/70772343650f66c353ad80a06d5272ca.jpg

- 影響產品：
  perl 5.29.1、5.28.0、5.26.2.以前版本
- 解決辦法：
  下載 perl 5.28.1，請參考 https://www.perl.org/get.html。
- 資料來源：
  1. https://metacpan.org/changes/release/SHAY/perl-5.26.3
  2. https://rt.perl.org/Public/Bug/Display.html?id=133204
  3. https://rt.perl.org/Public/Bug/Display.html?id=133423
  4. https://rt.perl.org/Public/Bug/Display.html?id=133192
  5. https://rt.perl.org/Public/Bug/Display.html?id=131649
  6. https://securitytracker.com/id/1042181
  7. http://tech.mozilla.com.tw/posts/4282/address-sanitizerasan-%25E4%25B8%2580%25E5%2580%258B-cc-%25E8%25A8%2598%25E6%2586%25B6%25E9%25AB%2594%25E5%2581%25B5%25E9%258C%25AF%25E7%259A%2584%25E5%25B7%25A5%25E5%2585%25B7
  8. https://www.perl.org/get.html

2.3.2 鼎陽 SDS 1202X-E 示波器易遭入侵竄改測試數據

電子訊號示波器，是實驗室常見儀器，研製設備時不可或缺，經資安業者 SEC-Consult 分析對岸業者 SIGLENT 出廠 SDS 1202X-E 型數位示波器，發覺使用過時軟體部件，如 BusyBox 1.20.1 (2012)、GNU glibc 2.13 (2011)、Linux kernel 3.19.0 (2015) 等，顯見未落實更新服務，此外尚有其他破綻，如兩組後門帳號 root、siglent 儲存在唯獨 cramfs 檔案系統中 shadow 檔案，令一般使用者難以更換密碼，反而攻擊者能輕易地從 port 23 採 telnet 登入，管理 SDS 1202X-E 示波器；而透過 EasyScopeX 波形分析工具，無須身分驗證，能逕調示波器參數設定，且 EasyScopeX 所產生流量均為明文封包，在 port 5024、5025 可竊聽其內容，因鼎陽科技對上述瑕疵無回應，亦無修補，建議持有該設備之學校、企業，儘量於可靠封閉網路環境操作，關閉 port 23，並採取硬體電路介面 UART(通用非同步收發傳輸器：Universal Asynchronous Receiver/ Transmitter)，維護作業安全性。

圖片來源：
https://mediacdn.eu/mage/media/catalog/product/cache/11/image/800x/040ec09b1e35df139433887a97daa66f/s/d/sds1202x-e-side.png

- 影響產品：
  韌體 5.1.3.13
- 解決辦法：
  暫無。
- 資料來源：
  1. https://www.sec-consult.com/en/blog/advisories/multiple-vulnerabilities-in-siglent-technologies-sds-1202x-e-digital-oscilloscope/
  2. https://www.bleepingcomputer.com/news/security/digital-oscilloscope-comes-with-backdoor-accounts-old-software-components/
  3. https://zh.wikipedia.org/wiki/Cramfs
  4. https://blog.gtwang.org/linux/linux-etc-shadow-file-format/
  5. https://zh.wikipedia.org/wiki/UART
  6. http://www.siglent.com/ens/
  7. http://www.siglent.com/about.aspx?id=549

2.3.3 儘速更新 Zoom！避免駭客亂入視訊會議

雲端視訊會議室 Zoom，可跨平台支援桌機、行動裝置多方開會，提供會中提問、螢幕共享、文字聊天、錄影等功能，經 Tenable 公司研究，其 3 款桌機版 Zoom client(macOS、Windows、Linux)之訊息泵浦函式，囿於欠缺輸入字串檢驗，攻擊者僅須掌握與會者 IP、port、ID 等資訊，可偽造 UDP 訊息，送出惡意命令，入侵後能劫持操縱受害者桌面、鍵盤、滑鼠；或者假冒與會者發表意見；甚至比照主席，將某人踢出會議並封鎖開會邀請，駭客身分可以是與會人員、區域網路用戶，理論上攻擊行動可跨網域實施，損及用戶商譽，Zoom Video Communications 已釋出升級版修補該弱點，據悉全球企業用戶達 75 萬，經查國內 Zoom 使用機關、業者有新北市消防局、交通大學、台北市電腦公會、全球人壽、富邦證券、中華電信、中華航空等，建議相關單位儘速部署安全 Zoom 版本。

圖片來源：https://news.it.ufl.edu/wp-content/uploads/2018/09/Zoom_Featured_Image_250_250.png

- 影響產品：
  - Zoom client for macOS 4.1.33259.0925 前版本
  - Zoom client for Windows 4.1.33259.0925 前版本
  - Zoom client for Linux 2.4.129780.0915 前版本

- 解決辦法：
  - 下載 Zoom for macOS 4.1.34801.1116，請參考 https://support.zoom.us/hc/en-us/articles/ 201361963-New-Updates-for-Mac-OS。
  - 下載 Zoom for Windows 4.1.34814.1119，請參考 https://support.zoom.us/hc/en-us/articles/ 201361953-New-Updates-for-Windows。
  - 下載 Zoom for Linux 2.6.146750.1204，請參考 https://support.zoom.us/hc/en-us/articles/205759689-New-Updates-for-Linux。

- 資料來源：
  1. https://www.tenable.com/blog/tenable-research-advisory-zoom-unauthorized-command-execution-cve-2018-15715
  2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15715
  3. https://support.zoom.us/hc/en-us/sections/201214205-Release-Notes
  4. https://www.tenable.com/security/research/tra-2018-40
  5. https://github.com/tenable/poc/tree/master/Zoom
  6. https://zoomnow.net/
  7. https://zoomnow.net/zntw_zoom_FAQ.php
  8. https://zoom.us/zoomisbetter
  9. https://zoomnow.net/zntw_about_zoom.php
  10. https://support.zoom.us/hc/en-us/articles/201361963-New-Updates-for-Mac-OS
  11. https://support.zoom.us/hc/en-us/articles/201361953-New-Updates-for-Windows
  12. https://support.zoom.us/hc/en-us/articles/205759689-New-Updates-for-Linux

2.3.4 爆發今年第三波 Flash player 0-day 攻擊，"毒針行動"隨俄烏衝突竄起

回顧今年 3 次 Flash player 0-day 攻擊，均伴隨區域衝突發生，2 月於朝鮮半島，6 月在中東(卡達交惡四鄰)，11 月底烏克蘭與俄羅斯海軍衝突後，旋即爆發 Operation Poison Needles(毒針行動)，據信烏克蘭駭客利用 Flash 的 use-after-free 漏洞，採取一系列連鎖攻擊，以社交工程誘騙莫斯科 Polyclinic No.2 醫院職員，開啟 office 文件(22.docx)後直接觸發弱點，嵌入的惡意 Flash 物件在受害主機上執行程式碼，獲得管理權並操作 command line，解壓縮偽裝之 scan042.jpg，再解壓後門程式 backup.exe，擁有與 NVIDIA 顯示卡 Control Panel 程式一致特徵，相當逼真，且 backup.exe 能常駐作業系統，蒐集受害主機軟硬體資訊，監控鍵盤滑鼠活動，偵測防毒軟體，苗頭不對還能啟動自毀滅跡，Adobe 已迅速反應，於 12 月 5 日升級新版，並順帶修補 DLL hijacking 缺失。儘管該事件影響對像為俄籍人士，然該入侵技術能適用新舊版 Windows，且不分與 32、64 位元，若惡意組織針對 Flash player 的探勘途徑，加以武裝化，仍形成嚴重威脅，敦請金融、醫療、公務機關火速更新。

圖片來源：
https://www.sensorstechforum.com/wp-content/uploads/2014/11/Adobe-Issues-and-Emergency-Flash-Player-Update.jpg

- 影響產品：
  Flash Player 31.0.0.153 前版本

- 解決辦法：
  - 取得 Flash Player 32.0.0.101，啟動 Adobe Flash Player 自動更新，或於官網下載升級版，連結為 https://get.adobe.com/flashplayer/。
  - 對無法判別真偽之 Office 檔案，以「受保護的檢視」進行唯讀開啟模式。

- 資料來源：
1. https://atr-blog.gigamon.com/wp-content/uploads/2018/12/Untitled-6.gif
2. https://www.securityweek.com/russian-hospital-targeted-flash-zero-day-after-kerch-incident
3. https://www.youtube.com/watch?v=4OYQyLSVDlU&feature=youtu.be
4. https://atr-blog.gigamon.com/2018/12/05/adobe-flash-zero-day-exploited-in-the-wild/
5. https://thehackernews.com/2018/12/flash-player-vulnerability.html
6. https://www.sensorstechforum.com/cve-2018-15982-adobe-flash/
7. http://blogs.360.cn/post/PoisonNeedles_CVE-2018-15982_EN
8. https://helpx.adobe.com/security/products/flash-player/apsb18-42.html
9. https://www.theregister.co.uk/2018/12/05/flash_zeroday_adobe/
10. https://zh.wikipedia.org/wiki/VirusTotal
11. https://hk.saowen.com/a/7d832c24cdaf856d87876941f8cf854d8739c048aec6c8d16f6667e05a493031
12. http://www.p2f.ru/
13. https://www.infobyip.com/ipbulklookup.php
14. https://securityaffairs.co/wordpress/78712/hacking/cve-2018-15982-flash-zero-day.html
15. http://blogs.360.cn/post/PoisonNeedles_CVE-2018-15982.html
16. https://get.adobe.com/flashplayer/

2.3.5 檔案同步工具 Qsync 測出 XSS 瑕疵，宜安裝 QNAP 更新版本

威聯通以 Linux 為基礎，研發專屬 Turbo NAS 作業系統 QTS，並搭配 Qsync 檔案同步工具，Qsync Client 操作者將檔案拖至 Qsync 資料夾後，NAS 端 Qsync Central Station 會讓其他連線中 Client(桌機或行動裝置)同步更新檔案，經研究員 Marcin Zieba 分析，指出一項高危險程度的跨站台腳本漏

洞，恐讓攻擊者遠端注入惡意 JavaScript 碼，干擾數版 Qsync Central 在不同 QTS 環境上作業安全性，據 11 月 29 日 QNAP Systems 官方公告，已升級相關 Qsync Central，可按本文所述步驟執行更新。

圖片來源：https://www.qnap.com/zh-tw/utilities/essentials

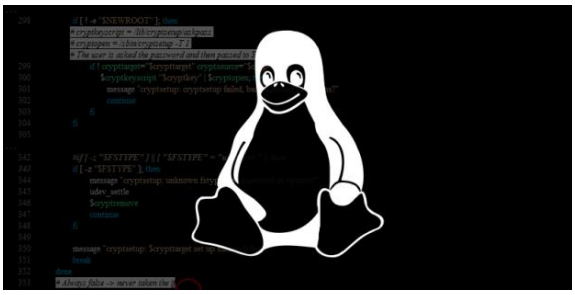
- 影響產品：
  - QTS 4.2.6 build 20180711 前版本
  - Qsync Central 3.0.2 前版本
  - Qsync Central 3.0.3 前版本
  - Qsync Central 3.0.4 前版本

- 解決辦法：
  - 更新 QTS 4.2.6 步驟：瀏覽控制台→系統→韌體更新，按下檢查更新，自動執行後續下載&安裝。
  - 更新 Qsync Central 3.0.2.01、3.0.3.01、3.0.4.01 步驟：管理者開啟 App Center→搜尋 Qsync Central→搜尋清單顯示最新版號→確認更新。

- 資料來源：
  1. https://www.qnap.com/zh-tw/security-advisory/nas-201811-29
  2. https://nvd.nist.gov/vuln/detail/CVE-2018-0716
  3. https://www.qnap.com/zh-tw/utilities/essentials
  4. https://docs.qnap.com/nas/4.2/SMB/tc/index.html?qsync.htm

2.3.6 警告！Linux 用戶憑藉高 UID 值可逕執行 systemctl 系統命令

據數位鑑識專家 Rich Mirch 分析，多數流行 Linux 發行版，如 Red Hat、Debian、Ubuntu、CentOS，皆有共同漏洞，讓未授權用戶得以執行系統指令，癥結在於應用工具組 PolicyKit，儘管 PolicyKit 目的在於控制權限分配，但遇到特別的帳號，其 UID 大於 INT_MAX (21474836 47)，亦即變數儲存上限值(0x7FFFFFFF)，則該帳號擺脫授權驗證機制，若某新建帳號 UID 為 3000000000，則用戶搖身一變為管理者，能執行 systemctl 指令，搭配各種參數，控制 OS 各項背景程式、工具、函式庫，決定全部 service 啟動與否，目前僅 Debian 系列已釋出 policy kit-1 改良版，餘尚未獲得全面修補方案，系統管理者請檢查可疑帳號 UID，並關注更新進度。



圖片來源：
https://www.securitynewspaper.com/snews-up/2017/03/Linux.png

- 影響產品：
  PolicyKit 0.115
- 解決辦法：
  - 系統管理者檢查帳號，毋使 UID 超過 2147483646 者啟用。
  - Debian Linux 用戶可參考 https://sources.debian.org/src/policykit-1/，取得 policykit-1 0.105-18+deb9u1 或較新版本。
- 資料來源：
  1. https://www.youtube.com/watch?v=GTIwS9zzuhk
  2. https://www.securitynewspaper.com/2018/12/08/linux-users-with-limited-privileges-could-execute-any-command/
  3. https://thehackernews.com/2018/12/linux-user-privilege-policykit.html
  4. https://packetstormsecurity.com/files/150686/Debian-Security-Advisory-4350-1.html
  5. https://security-tracker.debian.org/tracker/DSA-4350-1
  6. https://security-tracker.debian.org/tracker/CVE-2018-19788
  7. https://www.debian.org/security/2018/dsa-4350
  8. https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=915332
  9. https://people.canonical.com/~ubuntu-security/cve/2018/CVE-2018-19788.html
  10. https://gitlab.freedesktop.org/polkit/polkit/issues/74
  11. https://github.com/systemd/systemd/issues/11026
  12. https://github.com/mirchr/security-research/blob/master/vulnerabilities/CVE-2018-19788.sh
  13. http://cve.mitre.org/cgi-bin/cvename. cgi?name=CVE-2018-19788
  14. https://linux.cn/article-5926-1.html
  15. http://linux.vbird.org/linux_basic/0560daemons.php#systemctl_cmd
  16. http://man.linuxde.net/systemctl
  17. https://www.anquanke.com/vul/id/1419341
  18. https://sources.debian.org/src/policykit-1/

2.3.7 容器管理系統 Kubernetes(K8S)存弱點，入侵者可擴權操作

開源工具 K8S 初始由 Google 設計，乃是容器叢集管理系統，Kubernetes 本意係舵手(希臘語)，能管理 Docker 等建置的容器，經 Darren Shepherd 分析指出，其 Kubernetes API server 因權限配置瑕疵，處理惡意 proxy request 時，留下 TCP 連線，無論入侵者是否通過身分驗證，皆能利用既有 TLS 憑

證作掩護，經由該連線接觸後台 server，且隨意發送 request，即使匿名人士也可擴權操作，達到顯示 pod 清單、執行指令、取得輸出結果等目的，本項漏洞之 CVSS 評分 9.8，屬嚴重等級，不容輕忽。Linux Foundation 已就各版 Kubernetes 公布升級軟體，唯 Kubernetes 1.0.x-1.9.x 系列舊版不在維護範圍，須規劃安裝新版，若作業環境無法立即更新，可調整設定，停止「群集 API 使用權、匿名帳號請求」等危險授權項目。

圖片來源：https://codingcompiler.com/wp-content/uploads/2018/01/kubernetes-tutorials.png

- 影響產品：
  - Kubernetes 1.0.x-1.9.x
  - Kubernetes 1.10.0-1.10.10
  - Kubernetes 1.11.0-1.11.4
  - Kubernetes 1.12.0-1.12.2

- 解決辦法：
  - Kubernetes 1.10.11，由 https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG-1.10.md/#v11011 下載。
  - Kubernetes 1.11.5，由 https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG-1.11.md/#v1115 下載。
  - Kubernetes 1.12.3，由 https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG-1.12.md/#v1123 下載。
  - Kubernetes 1.13.0-rc.1，由 https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG-1.13.md/#v1130-rc1 下載。
  - 因 Kubernetes 1.0.x-1.9.x 不再後續維護，請考慮其它版本。

- 資料來源：

1. https://asciinema.org/a/kubSrehAf14K7MQ9aZw2RpCYd
2. https://meterpreter.org/kubernetes-were-patched-to-fix-the-privilege-escalation-vulnerability/?cn-reloaded=1
3. https://github.com/kubernetes/kubernetes/issues/71411
4. https://groups.google.com/forum/#
5. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1002105
6. https://asciinema.org/a/TjbO5p1JJN0dnNSSWhrcopn9e
7. https://github.com/evict/poc_CVE-2018-1002105
8. https://access.redhat.com/errata/RHSA-2018:3754
9. https://zh.wikipedia.org/wiki/Kubernetes
10. https://www.mile.cloud/zh-hant/cloudmilexgcpug-kubernetes/
11. https://medium.com/@evenchange4/%25E4%25BA%2594%25E5%2588%2586%25E9%2590%2598-kubernetes-%25E6%259C%2589%25E6%2584%259F-e51f093cb10b
12. https://kknews.cc/zh-tw/tech/59a95b6.html
13. https://kubernetes.io/
14. https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG-1.10.md/#v11011
15. https://github.com/kubernetes/kuber

netes/blob/master/CHANGELOG-1.10.md/#v1115
16. https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG-1.10.md/#v1123
17. https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG-1.10.md/#v1130-rc1

2.3.8 喬安 JA-Q1H Wi-Fi 攝影機恐有停機之虞

大陸安防監控業者喬安科技，旗下 JA-Q1H Wi-Fi 攝影機因韌體設計缺失，遵守 Open Network Video Interface Forum(ONVIF)標準之函數 GetStreamUri method( )、GetVideoEncoderConfigurationOptions( )無法處理空字串之例外狀況；另 CreateUsers( )、SetImagingSettings( )、GetStreamUri( )函數對輸入值包含 '>' 符號亦無法正確處理，攻擊者可遠距造成設備停機或重啟，目前暫無修補聲明。

圖片來源：
https://img10.joybuy.com/N0/s800x800_jfs/t15694/327/2534250173/127870/98f4023/5ab1c999Nd25505c7.jpg.dpg

- 影響產品：
  firmware 21.0.0.91
- 解決辦法：
  暫無。
- 資料來源：

1. https://www.secnews24.com/2018/12/10/cve-2018-20050-mishandling-of-an-empty-string-on-the-jooan-ja-q1h-wi-fi-camera-with-firmware-21-0-0-91-al/
2. https://www.secnews24.com/2018/12/10/cve-2018-20051-mishandling-of-on-the-jooan-ja-q1h-wi-fi-camera-with-firmware-21-0-0-91-allows-remo/
3. http://www.qacctv.com/
4. https://github.com/iamweifan/jooan/blob/master/ss_poc.py
5. https://github.com/iamweifan/jooan/blob/master/es_poc.py
6. https://www.itri.org.tw/chi/Content/techTransfer/tech_tran_cont.aspx?&SiteID=1&MmmID=620622511005426631&Keyword=&MSid=4402
7. https://kknews.cc/zh-tw/tech/p4g4nej.html
8. https://www.hanmin.com.tw/onvif%25E6%2598%25AF%25E4%25BB%2580%25E9%25BA%25BC/

2.3.9 慎防滑鼠鍵盤應用程式 Logitech Options，暗開 Windows 後門

滑鼠發展先驅羅技公司，其高階輸入介面裝置包含 WIFI 滑鼠、鍵盤，並開發 Logitech Options(適用 Mac、Windows)軟體輔助用戶，定義客製化輸入功能，據 Google Project Zero 研究員 Tavis Ormandy 測試，Logitech Options 會在 Windows 寫入登錄值成為常駐程式，並開啟無線鍵盤"Craft"上 websocket server 與 port 10134，但未曾設計類型檢查和來源辯證機制，若參數 tool_options 接收錯誤資料型態則發生當機，而攻擊者可無限嘗試猜測 process ID，直到 bruteforce 成功，進而接管鈕控制器"crown"，取代真正用戶發送 keystroke 訊號，接手操作，上述 2 項安全缺失影響 Windows7、8、10，儘管 Logitech 於 12 月 13 日釋出 Options 7.00.564，並於官網支援網頁(英語系)註明「Fixes Origin checks and type checking bugs」，然在中文網頁卻無此文字，復經其他研究員測試新版 Logitech Options 仍可被入侵，相關報告已公開，建議使用者以白名單防止外部惡意連線至 port 10134，並關注更新訊息。

圖片來源：https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTlcqLoW0udfD2sO8L93Gb9F7QIeJK7xbOQ--uyv-6g0nLG-3Cr

- 影響產品：
  Options 7.00.564(for Windows)前版本
- 解決辦法：
  - 設定白名單，阻絕可疑連線通過 port 10134。
  - 檢查系統檔案或登錄值，是否出現與 Logitech Options 無關之軟體安裝跡象
- 資料來源：
  1. https://bugs.chromium.org/p/project-zero/issues/detail?id=1663
  2. https://github.com/Logitech/logi_craft_sdk
  3. https://www.logitech.com/en-us/product/options
  4. https://support.logitech.com/en_us/software/options
  5. https://support.logitech.com/zh_tw/downloads
  6. https://www.logitech.com/zh-tw/about/logitech-story
  7. https://www.logitech.com/zh-tw/product/options/page/flow-multi-device-control

2.3.10 急訊！SQLite DB 嚴重漏洞"麥哲倫"，波及全球 IT 環境

關聯式資料庫引擎 SQLite，係 C 語言開發，為輕量級嵌入式資料庫，可整合在用戶程式中，非常見主從式架構，經騰訊刀鋒安全團隊 (Tencent Blade security Team)研究，SQLite 存在嚴重 RCE，攻擊者可從遠距或本機，循 Web SQL API 介面注入程式碼字串後，被視作 SQL 語法執行，衍生資料外洩、服務停止等後果。因 SQLite 蹤跡遍及全球各類硬體、OS、應用程式，特別是採用 Chromium 開源技術之瀏覽器(Google Chrome、Vivaldi、Opera、Brave)，影響範圍之廣無法估計，該漏洞命名為'Magellan'，取麥哲倫航海環繞地球之意，儘管 SQLite Team 已改善，且暫無在野攻擊事件，然囿於全面修補工程浩大，及官方修補釋出後必遭逆向工程研究其探勘原理，"麥哲倫"仍將威脅軟體生態數年，確定安全無虞者為 Firefox、Edge、Safari、Chrome 71.0.3578.80 後版本。

圖片來源：
https://upload.wikimedia.org/wikipedia/commons/thumb/3/38/SQLite370.svg/199px-SQLite370.svg.png

- 影響產品：
  SQLite 3.26.0 之前版本
- 解決辦法：
  下載 SQLite 3.26.0 壓縮檔，參考 https://www.sqlite.org/download.html 。
- 資料來源：
  1. https://blade.tencent.com/magellan/index_en.html
  2. https://www.zdnet.com/article/sqlite-bug-impacts-thousands-of-apps-including-all-chromium-based-browsers/
  3. https://news.ycombinator.com/item?id=18685296
  4. https://securityaffairs.co/wordpress/78920/hacking/magellan-rce-flaw-in-sqlite-potentially-affects-billions-of-apps.html
  5. https://worthdoingbadly.com/sqlitebug/
  6. https://thehackernews.com/2018/12/sqlite-vulnerability.html
  7. https://developers.google.com/web/tools/lighthouse/audits/web-sql
  8. https://www.sqlite.org/releaselog/3_26_0.html
  9. https://www.sqlite.org/about.html
  10. https://www.sqlite.org/prosupport.html
  11. https://blade.tencent.com/magellan/index.html
  12. https://github.com/zhuowei/worthdoingbadly.com/blob/master/_posts/2018-12-14-sqlitebug.html
  13. https://chromium.googlesource.com/chromium/src/+/c368e30ae55600a1c3c9cb1710a54f9c55de786e
  14. https://zh.wikipedia.org/wiki/SQLite
  15. https://www.sqlite.org/download.html

2.3.11 三星官網介面出現 CSRF，險成會員帳號劫持途徑

Samsung 手機用戶，可於雲端設定個人化服務，自然不免身分驗證程序，然經烏克蘭軟體抓漏好手 Artem Moskowsky 測試，發覺三星官網入口，囿於辨識用戶請求時，安全性過低，存在不同程度之跨站台請求偽造漏洞，且實際探勘這 3 項 CSRF 均可奏效，能窺伺、竄改用戶個資；停用 2-factor authentication 身分驗證；甚至強行置換安全提問與答案，重設密碼後假冒受害者身分，三星獲報後已修正 web 安全性設計，並餽贈獎金$13300。

圖片來源：https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQMAEUUYg7cAN7HjQOhDojWiOX-EXKhlSke1WvU1ap5m7-HaTWD3w

- 影響產品：
  Samsung 帳號管理系統
- 解決辦法：
  三星已更正 web 入口網站安全性設計。
- 資料來源：
  1. https://nakedsecurity.sophos.com/2018/12/12/samsung-fixes-flaws-that-could-have-let-attackers-hijack-your-account/
  2. https://www.theregister.co.uk/2018/12/10/samsung_patches_accountstealing_hole/
  3. https://www.technadu.com/samsung-fixes-three-critical-bugs-reported-ukrainian-bug-bounty-hunter/51192/
  4. https://www.zdnet.com/article/bug-allowed-full-takeover-of-samsung-user-accounts/
  5. http://www.kb-iot.com/post/730.html
  6. https://medium.com/@moskowsky
  7. https://account.samsung.com/membership/intro

2.3.12 微軟緊急修補 JSsript 引擎，抑制 IE 0-day 在野攻擊

微軟所開發動態 script 語言 Jscript，為 Internet Explorer 內含之腳本碼引擎，據 Google 威脅分析師 Clement Lecigne 指出，因 Jscript9.dll 處理記憶體內物件的方式存在瑕疵，易遭觸發 memory corruption 並衍生 RCE 攻擊，駭客可經由魚叉式釣魚誘騙受害者瀏覽惡意網站，或者寄送各種可嵌入 Jscript 之特製文件，如 HTML、Office 檔案、PDF，成功探勘即可執行任何程式，危害程度與受害者權限成正比，然漏洞發生條件端賴各版 IE 與 OS 搭配組合，如 IE 9 配 Server 2008、IE 10 配 Server 2012，而 IE 11 受攻擊面最廣，在 Windows7、8.1、10 與 Server 2008、2012、2019、2019 皆無從倖免，由於刻正發生在野攻擊，12 月 19 日微軟緊急公告非常態更新，若作業環境不宜(不敢)立即安裝，建議嘗試官方 cacls 指令教學，先行限制 JScript.dll 存取，降低 IE 慣用者風險，最好是換瀏覽器，完全杜絕此項 0-day 漏洞。

圖片來源：https://krebsonsecurity.com/wp-content/uploads/2018/12/iexploder.jpg

- 影響產品：
  - Internet Explorer 9
  - Internet Explorer 10
  - Internet Explorer 10
- 解決辦法：
  - 執行命令列 cacls 指令，停用 JScript.dll。
  - 參考 https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8653，就所屬環境下載更新。
- 資料來源：
  1. https://www.zdnet.com/article/microsoft-releases-security-update-for-new-ie-zero-day/
  2. https://www.tenable.com/blog/microsoft-releases-out-of-band-patch-for-internet-explorer-remote-code-execution-vulnerability
  3. https://kb.cert.org/vuls/id/573168/
  4. https://www.bleepingcomputer.com/news/security/microsoft-releases-out-of-band-security-update-for-internet-explorer-rce-zero-day/
  5. https://krebsonsecurity.com/2018/12/microsoft-issues-emergency-fix-for-ie-zero-day/#more-46087
  6. https://en.wikipedia.org/wiki/JScript
  7. https://zh.wikipedia.org/wiki/JScript
  8. https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2018-8653
  9. https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8653

2.3.13 烏賊快取 Squid Cache 錯誤訊息網頁成 XSS 媒介

以 C++開發之 Squid Cache 係開源的 HTTP 代理伺服器，可當快取伺服器並過濾流量，支援 Unix、mac OS X、Linux、Windows 等平台，運行 HTTP、HTTPS、FTP 等主流協定，應用於多種防火牆及影音串流服務，經德國研究員 Nikolas Lohmann 分析，Squid 之錯誤訊息樣本網頁 ERR_SECURE_CONNECT _FAIL，因特定變數處理不當，無法辨識 http 程式轉意字元，若接收到惡意 X.509 憑證內容，將遭注入任意 html code，所產生之警告網頁在受害瀏覽器發動 Cross-Site Scripting，相當諷刺，攻擊者竟可藉由啟動 TLS/SSL 安全設定，找到滲透入口，反而取消"--enable-ssl" 或"--with-openssl"能避免生成夾帶 XSS 的官方訊息，Squid project 已釋出更新版本，舊版修補方式亦同步公告。

圖片來源：
https://upload.wikimedia.org/wikipedia/zh/thumb/b/b7/Squid-cache_logo.jpg/200px-Squid-cache_logo.jpg

- 影響產品：
  - Squid 3.1.12.1 ~ 3.1.23
  - Squid 3.2.0.4 ~ 3.5.28
  - Squid 4.0 ~ 4.3
- 解決辦法：
  - 下載 Squid 4.4，請參考 http://www.squid-cache.org/Versions/v4/
  - 修補 Squid 3.5，請參考 http://www.squid-cache.org/Versions/v3/3.5/changesets/squid-3.5-f1657a9decc820f748fa3aff68168d314 5258031.patch
  - 修補 Squid 4，請參考 http://www.squid-cache.org/Versions/v4/changesets/squid-4-828245b90206602014ce057c3db39fb80fcc4b08.patch
- 資料來源：
  1. http://www.squid-cache.org/Advisories/SQUID-2018_4.txt
  2. https://github.com/squid-cache/squid/pull/306
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19131
  4. http://www.squid-cache.org/Versions/v5/changesets/squid-5-6feeb15ff312f3e145763adf8d234ed6a0b3f11d.patch
  5. https://zh.wikipedia.org/wiki/Squid_
  6. http://www.squid-cache.org/
  7. http://www.squid-cache.org/Intro/
  8. http://www.squid-cache.org/Intro/who.html
  9. http://www.squid-cache.org/Versions/v4/

10. http://www.squid-cache.org/Versions/v3/3.5/changesets/squid-3.5-f1657a9decc820f748fa3aff68168d3145258031.patch
11. http://www.squid-cache.org/Versions/v4/changesets/squid-4-828245b90206602014ce057c3db39fb80fcc4b08.patch

2.3.14 研華改善遠端監控軟體 WebAccess HMI/SCADA 高風險 Buffer Overflow

國內研華科技(Advantech)生產工業自動化、IoT 商品，旗下 Advantech WebAccess 軟體為跨平台、瀏覽器之人機介面，屬資料採集與監控系統(supervisory control and data acquisition：SCADA)，適用於自動化設備動態圖形顯示和即時資料掌控，經 Tenable 研究員 Jacob Baines 查測，具高危險程度 stack buffer overflow，CVSS v3 評分 7.3，攻擊者送出帶運算碼 70022 的 DCERPC 訊息，將觸發 BwPAlarm.dll 溢位，極可能引發 DoSc 或 RCE，已確定在 Windows 2008 R2 SP1 平台上 WebAccess/ SCADA 8.3.2 有此漏洞，針對上述重要安全事件，研華公司已升級軟體版本並公告。

圖片來源：
https://www.taiwanexcellence.org/upload/product/old/104153BA-A020_L.jpg

- 影響產品：
  WebAccess 8.3.2 以前版本
- 解決辦法：
  取得 WebAccess 8.3.3，請參考 https://support.advantech.com/support/DownloadSRDetail_New.aspx?SR_ID=1-MS9MJV&Doc_Source=Download 。
- 資料來源：
  1. https://www.tenable.com/security/research/tra-2018-45
  2. https://ics-cert.us-cert.gov/advisories/ICSA-18-352-02
  3. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18999
  4. https://www.securityfocus.com/bid/106245/references
  5. http://www.nsfocus.net/vulndb/42291
  6. https://support.advantech.com/support/DownloadSRDetail_New.aspx?SR_ID=1-MS9MJV&Doc_Source=Download

2.3.15 公布 Pulse Secure 二安全產品弱點

Pulse Secure, LLC 過往隸屬 Juniper Networks 的 Junos Pulse 產品線，後由 Siris Capital 收購，專職開發 SSL VPN 遠端存取服務，近期外部研究者 Rafael Pedrero、Ekzhin Ear 檢測出 Pulse Secure 產品瑕疵，其 Secure Access SSL VPN 軟體 SA-4000 因 update.cgi 權限控管欠佳，恐遭低權限人員竄改參數，然 SA-4000 已逾官方維護生命週期；另虛擬流量管理器 Virtual Traffic Manager (vTM)之 XSS，讓遠端攻擊者能注入腳本程式語言，以及避開授權查驗，探勘後果為外流受害者活動歷史、帳密等隱私資料。

圖片來源：
https://www.accyotta.com/pulsesecure/virtual-traffic-manager

- 影響產品：
  - Secure Access SSL VPN SA-4000 5.1R5 (build 9627) 4.2 Release (build 7631)
  - Virtual Traffic Manager 9.9r2 之前版本、10.4r1
- 解決辦法：
  連結 https://my.pulsesecure.net/members/redirect/?application=licensinganddownloadcenter，登入會員帳密，下載更新。
- 資料來源：
  1. https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA43730
  2. https://seclists.org/fulldisclosure/2018/Dec/37
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20306
  4. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20307
  5. https://vuldb.com//?id.128289
  6. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20193
  7. https://www.pulsesecure.net/vtm/tech-info/
  8. https://my.pulsesecure.net/members/redirect/?application=licensinganddownloadcenter

2.3.16 留意行動版 FB 瑕疵，垃圾廣告正蔓延

波蘭籍資安鑑識分析好手 Lasq，部落格甫開張就揭 Facebook 的瘡疤，上週 Lasq 意識到，有個在臉書散布垃圾廣告的組織行動，藉由分享趣味圖案，吸引人按下滑鼠，彈出對話框詢問是否年逾 16，再按鍵則挑出一堆廣告，而 FB 出現期望中的內容，賡續追查發現，該行動鎖定法國人，還避開來自波蘭的轉址流量，此資安事件無法以 X-Frame-Options=DENY 方式阻絕，因攻擊者係利用 Facebook 行動版網頁分享對話方塊功能，當 mobile_iframe=true，能操控受害者後續瀏覽之 URL，危險之處在於 FB 朋友之間信任，無防備狀態下被誘導至釣魚網頁而交出個資，下載惡意程式，甚可能變更受害者隱私選項，刪除 account，然 FB 官方認為此為功能非漏洞，並宣稱已改善 Clickjacking 偵測系統，足以防止攻擊，但 Lasq 實測後仍可得手，並提供探勘工具 (https://malfind.com/test/poc.html)，惟須注意試驗 poc.html 時請調整為隱私，莫影響社交關係。

圖片來源：https://zdnet4.cbsistatic.com/hub/i/2018/09/28/ff0fec41-7365-4f02-8017-ac1a566d9a6d/5288580bd98cc107d7efcbb59303a6ce/facebook-icon.jpg

- 影響產品：
  Facebook
- 解決辦法：
  暫無。

- 資料來源：
  1. https://malfind.com/index.php/2018/12/21/how-i-accidentaly-found-clickjacking-in-facebook/
  2. https://www.bleepingcomputer.com/news/security/the-clickjacking-bug-that-facebook-wont-fix/
  3. https://www.zdnet.com/article/researcher-publishes-proof-of-concept-code-for-creating-facebook-worm/
  4. https://twitter.com/lasq88
  5. https://developers.facebook.com/docs/sharing/reference/share-dialog
  6. https://zh.wikipedia.org/wiki/Facebook
  7. https://zh.wikipedia.org/wiki/%25E7%2582%25B9%25E5%2587%25BB%25E5%258A%25AB%25E6%258C%2581
  8. https://blog.m157q.tw/posts/2018/07/23/clickjacking-frame-attack-defense/
  9. https://www.qa-knowhow.com/?p=2944

2.3.17 驚爆！多款 D-Link 路由器竟存三種帳密外洩途徑

研究員 Tyler Cui 測試多型 D-Link 路由器，查覺 atbox.htm、spaces.htm、dirary0.js 三網頁分別以不同指令句，記錄明文密碼，任何人無須權限，即可閱讀獲知帳密，關於上述缺陷，至少涉及 DSL-2770L、DIR-140L、DIR-640L、DWR-116、DWR-512、DWR-555、DWR-921 等 7 種型號，而官方均回應韌體修補仍開發中，用戶請建置其他防禦措施。

圖片來源:https://images.yaoota.com/_XzHd-gXZA1VZWt6aqRYtjs_PfA=/trim/yaootaweb-production/media/crawledproductimages/ed5ee30fb9a6940b6c16460baa1f2a0a.jpg

- 影響產品：
  韌體 ME_1.01、ME_1.02、AU_1.06、1.00、1.01RU、1.02、1.03、1.05、2.01、2.02
- 解決辦法：
  暫無。
- 資料來源：
  1. https://seclists.org/fulldisclosure/2018/Dec/46
  2. https://seclists.org/fulldisclosure/2018/Dec/45
  3. https://seclists.org/fulldisclosure/2018/Dec/38

2.3.18 趨勢修補 OfficeScan XG 權限控管雙缺陷

據 Abdullah H. AlJaber 分析，Trend Micro 中控式防毒軟體 OfficeScan XG，出現二項權限控管瑕疵，將導致重要檔案被攻擊者擴權存取變更，由於實際探勘手段須實體接觸設備始得成功，故其 CVSS 3.0

Score 為 5.9，列中級威脅，趨勢已公布修補程式。

圖片來源：https://static.spiceworks.com/images/products/0009/9347/Thumbnails_Trend-Micro_OfficeScan-XG_Q1-2017_profile.jpg

- 影響產品：
  OfficeScan XG

- 解決辦法：
  循 http://files.trendmicro.com/products/officescan/XG/SP1/osce_xg_sp1_win_en_criticalpatch_5261.exe 獲得修補程式。

- 資料來源：
  1. https://success.trendmicro.com/solution/1121674#
  2. https://www.securityfocus.com/bid/106305
  3. https://vuldb.com//?id.128284
  4. https://vuldb.com//?id.128283
  5. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18332
  6. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18331

2.4、資安研討會及活動

2019 臺灣資安大會	
活動時間	2019/3/19 – 3/21
活動地點	臺北國際會議中心 & 世貿一館 2 樓
活動網站	https://cyber.ithome.com.tw/
活動概要	2019 臺灣資安大會邀請您與我們一起參與臺灣年度資安盛事，為期一週的 2019 臺灣資安大會 (CYBERSEC 2019) 在此集結 180 家以上的國際及臺灣在地知名資安夥伴，展示最新與最適切的資安產品與服務，提供超過 180 堂資安全面向的議程，探討 80 種以上最熱與最廣泛的資安議題與技術。除了豐富的資安對策，更可與來自臺灣與亞太地區的 6,000 位與會者進行交流，拓展專業人脈成為未來工作的助力。 現今面對的攻擊已非單一人、單一部門乃至於單一企業可以有效防守，孤軍奮戰難以抗衡全球日漸壯大且有組織的縝密攻擊。不論您來自業界、專家學者、法務人士、公部門或企業用戶等，都歡迎與我們一同在此從技術層面與策略層面，探討資安百種面向、交流技術與知識。期許大家除了將資安意識與知識帶回組織中，從上至下凝聚共識與成長，並與資安產業的夥伴們偕同防禦，共同在資安戰場更加壯大，得以更快速地反應、更快速地處理，形成足以跟攻擊者匹敵的更強力防禦。 ● 2019 臺灣資安大會特色： ✓ 臺灣最大規模資安會議 ✓ 技術研討、主題論壇、實機操作、攻防演練一應俱全 ✓ 從技術到策略、從最新趨勢到日常營運 ✓ 產官學研齊聚一堂共商資安對策 ✓ 實戰演練資安攻防，提升實務防禦與鑑識能力 ✓ 最大規模的資安展覽，有效找到最適資安產品與服務 ✓ 凝聚共識與成長，偕同資安夥伴建構更強力防禦

Black hat 2019 年亞洲大會	
活動時間	2019/3/26 – 3/29
活動地點	新加坡濱海灣金沙會展中心
活動網站	https://ubm.io/2zZu87q
活動概要	**blackhat ASIA –針對亞洲社群資安發展需求，發表產業最新資安訊息與因應技術** ● blackhat Asia 為網路安全(Cyber Security)專業會議暨展會，提供最新資安教育訓練、產業趨勢簡報會暨產品展示，吸引多國政府機構、企業資安人員、系統整合代理商、經銷商等專業人員與會。 ✓ 為亞洲資安發展量身訂做專業議題，邀集「亞洲區資安委員會」，收集最新議題技術 ✓ 新加坡為國際政治中立國家，順利邀集歐、美、中東、亞太等重要講者。 ✓ 亞洲市場資安需求量逐漸上升，亞太企業開始重視人員培訓與資安環境建置。 **趨勢簡報會議(Briefings)–匯集全球資安專家談亞太資安議題與解決方案** ● 趨勢簡報會：為各行業從事資安相關人員提供一個學習亞太地區網路安全風險與趨勢的平台；邀請資安行業中頂尖人士主講，熱門議題包含：IOS & Andorid、車控系統、物聯網、虛擬貨幣、支付系統、加密系統運用、企業軟體漏洞、國際資安政策等漏洞攻防主題； ● 2019 年講師與簡報主題詳請請見：https://ubm.io/2rN2NRq (完整議題預計於 2019 年 2 月公布) ● 2019 年趨勢簡報會主題範疇：應用程式安全、密碼學、數據鑑識/事件應變、企業、資安漏洞發展、硬體/內嵌、網路防禦、人為因素、物聯網、惡意軟體、平台安全、資安開發週期、逆向工程、政策 **商業大會(Business Hall) - 全球資安產品品牌拓展亞太市場的國際平台** ● 2019 年指標展廠： Infoblox CONTROL YOUR NETWORK　QUALYS ON DEMAND SECURITY　POLYSWARM　ANOMALI　hackerone efficient iP DEFINING SMART DDI　Lockpath　eLearnSecurity Forging security professionals　wolfSSL　CASHSHIELD

	2018 會議與展會規模 ● 來自 60 個國家，超過 2,200 名專業人士與會，亞太區 88%、美國 6%、歐洲 3%、中東 3%。 ● 邀集 57 名資安權威，舉辦 33 場專業簡報、10 場教育訓練與 30 場產品展示，18 家國際媒體出席。 **匯聚 60 國，跨越醫療、軍警、金融、電信、資安的產官學決策代表與會** ● 系統整合商： M Tech!、Netpoleon、Westcon Comstor、Pacific Tech、Quantiq International ● 醫療保健：IHis、MSD International Gmbh、新加坡保健集團、陳篤生醫院 ● 金融服務：2C2P Pte Ltd、Allianz Asia Pacific、FinIQ Consulting Pte Ltd、歐力士亞洲有限公司 ● 電信服務：CommzGate、Ericsson Telecommunications、華為技術有限公司、LGA Telecom Pte Ltd ● 資訊服務：CTC Global Pte Ltd、Deskera Singapore、ITOCHU Techo-solutions、NCS Pte Ltd ● 政府單位：新加坡中央公積金、香港警務處、新加坡資訊通信媒體發展局、新加坡內政部 ● 電腦製造商：Garhi Japan、三菱電機公司、三星公司、索尼電子公司 ● 公民與軍事防衛：DSTA、Jupiter Protection Pte.Ltd、MINDEF、S-fifteen Space Systems ● 資訊安全:Attila CybertechPte Ltd、CDNetworks Singapore、Horangi、VenusTech

2019 亞太資訊安全論壇暨展會	
活動時間	2019/5/8 – 5/10
活動地點	台北世貿南港展覽館
活動網站	https://secutechinfosecurity.tw.messefrankfurt.com/taipei/zh-tw/visitors/welcome.html
活動概要	2019 年第十八屆(年) 亞太資訊安全論壇暨展會，《資安人》媒體，將於三天展覽會會場上，從四個主軸出發深入探討資訊安全議題: 觀念：與法規同步，與協同合作夥伴共同推動資安關鍵角色的重要性。 ● 組織：企業組織設立專職單位與專職資訊安全人員。 ● 管理：採用工具的評估讓觀念具體呈現其效力。 ● 技術：新型態網路部署規劃，建置。

	3 天論壇，10 個關鍵資安主題，50 場演講 + 攤位展示。 ● 資安議題方向： ✓ 資安管理與法規 (Security Management and Compliance) ✓ 網際威脅 (Cybersecurity) ✓ 雲端與行動安全 (Cloud & Mobile Info Security) ● 資安與監控安防聯網 ✓ 資安議題：Infra Security、Endpoint、Application Security、Wireless、Cloud、Mobile Security、SIEM、Incident Response、Identity Management ..... 歡迎各界、資安領域廠商們參與，展現您們的優秀產品與高品質的服務。

第 3 章、 2018 年 12 月份事件通報統計

本中心每日透過官方網站、電郵、電話等方式接收資安事件通報，2018 年 12 月通報總計 919 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事件，屬於我國疑似遭利用發起攻擊或被攻擊之 IP，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。

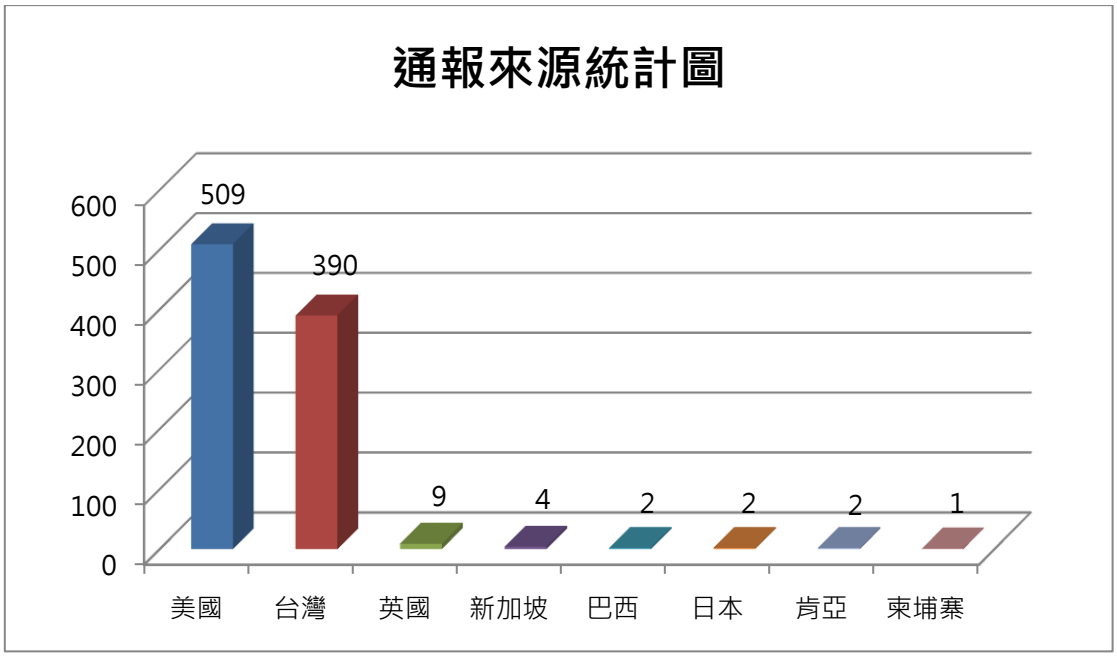


圖 1、通報來源統計圖

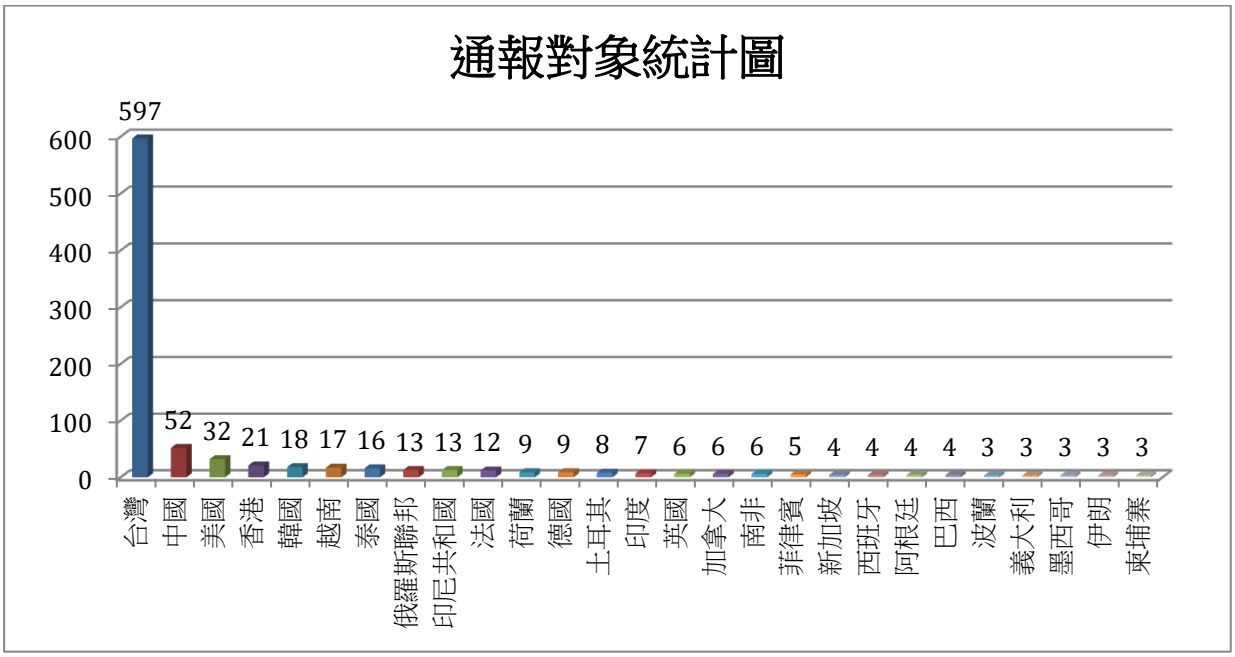


圖 2、通報對象統計圖

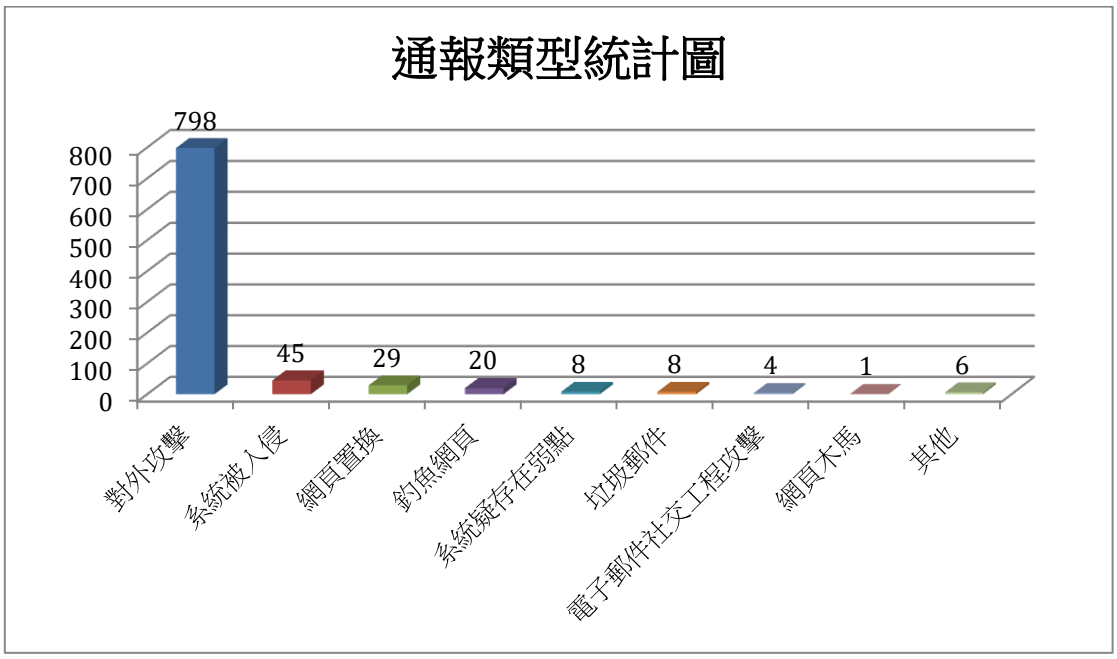


圖 3、通報類型統計圖

本中心近期接獲通報，有民眾表示因感染勒索病毒，重要檔案被有心人士進行加密，並收到一組連結以支付贖金。

由於勒索病毒種類繁多，且可透過比特幣(Bitcoin)等虛擬貨幣支付，不須透過實體貨幣進行交易，以匿名方式之虛擬貨幣令有心人士更加隱匿，因此雖勒索病毒自 1980 年代已然存在，卻因其不斷更新、改版，因此造成勒索病毒的持續猖狂。

目前之勒索病毒，僅有部分有出現解藥，新型病毒則須待相關資安公司或單位進行分析後方能得其解藥。由於其加密之金鑰透過病毒之更新越發加長，因此一般解碼軟體通常需要極長時間方能解開，少則數月、多則數年，因此不建議一般民眾如此嘗試。

一般民眾若真的不幸遭受勒索病毒攻擊，建議先將尚未中毒之資料備份，並尋求資安廠商之協助，嘗試是否有所解藥，且同時提供資安廠商訊息，製作病毒資料庫以及相關解藥。

- TWCERT/CC 提供以下防護建議：
  - 不點不明連結、不下載不明軟體/檔案。
  - 定期備份資料於其他磁碟/裝置中。
  - 確實持續更新電腦的作業系統、Office 應用程式等至最新版本。
  - 更新電腦防毒軟體病毒碼。

- 參考連結：
  1. https://id-ransomware.malware hunterteam.com/
  2. https://www.nomoreransom.org/
  3. https://www.trendmicro.com/zh_tw/forHome.html

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：2019 年 1 月 17 日

編輯：林克容、江奕昉

服務電話：0800-885-066

電子郵件：twcert@cert.org.tw

官網：https://twcert.org.tw/

Facebook 粉絲專頁：https://www.facebook.com/twcertcc/

電子報線上閱覽：https://blog.twnic.net.tw/