TWCERT/CC 資安情資電子報

2018 年 5 月份

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team/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電子報，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。

第 2 章、TWCERT/CC 近期動態

2.1、參與 Symantec 2018 年網路安全威脅研究報告(ISTR)發表會

4 月 18 日 Symantec 於慕軒飯店舉辦 2018 年網路安全威脅研究報告(Internet Security Threat Report, ISTR)發表會，TWCERT/C 主任陳永佳受邀參與，並分享 TWCERT/CC 於 106 年度資安事件通報分析，針對去年所觀察的通報狀況，提出企業較常遇到的幾項資安威脅，並給予相對應的防護建議。

2.2、協辦 2018 亞太資訊安全論壇

4 月 25 日至 27 日資安人媒體於南港展覽館五樓舉辦 2018 亞太資訊安全論壇，為期三天的研討會及資安展示會，TWCERT/CC 於此次研討會擔任協辦的角色，並有三天的攤位展示，進行 TWCERT/CC 業務及資安意識推廣，此外，於 4 月 27 日 TWCERT/CC 主任陳永佳受邀分享「企業發生資安事件怎麼辦-台灣民間資安協助窗口:TWCERT/CC」。

2.3、協辦 2018 駭客任務．資安戰役及 IRCON 2018 研討會

此次會議由國網中心及新竹科學工業園區於宜蘭老爺行旅合作舉辦，TWCERT/CC 協辦此次會議，設有連續兩天攤位展示，進行 TWCERT/CC 業務及資安意識推廣，TWCERT/CC 副主任吳專吉受邀於 5 月 3 日 IRCON 2018 分享「企業面臨的資安問題-如何利用有限的資源做好資安」。

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、辨識常見的駭客手法「變臉詐騙」

資安廠商趨勢科技日前公布 2017 年資安總評報告，除了勒索病毒，變臉詐騙(BEC)也對企業造成重大損失，是台灣企業 2017 年最需要提防的攻擊手法之一。

資料來源：

https://tw.appledaily.com/new/realtime/20180408/1330359/

https://www.bnext.com.tw/article/43602/business-email-compromise-billion-dollar-scam

https://www.informationsecurity.com.tw/article/article_print.aspx?aid=8530

3.1.2、行政院打造國際級資安研訓機構

行政院為延攬國際一流資安人才，提升台灣整體資安技術與能力，資通安全處規劃資安研訓機構今年九月開始運作，初期將在網路上成立虛擬機構，未來將視實際運作情況再決定是否設實體機構。

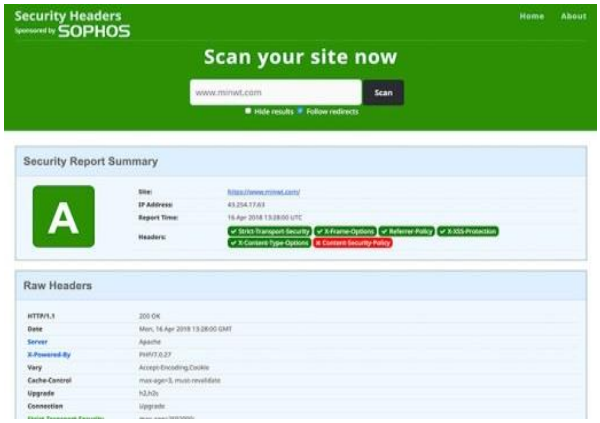
資料來源：

http://news.ltn.com.tw/news/politics/paper/1189990

https://www.nownews.com/news/20180405/2730362

3.1.3、HTTP Headers 設置，增加網站安全性

HTTP Headers 是超文字傳輸協定(HTTP)請求和回應訊息的核心，它承載了關於用戶端流覽器、請求頁面及伺服器等相關的資訊，而 HTTP Headers 設定得當，可以為網站增加安全性。



資料來源：

https://www.minwt.com/website/server/19863.html

https://yu-jack.github.io/2017/10/20/secure-header/

https://nkongkimo.wordpress.com/2010/04/28/http-header%25E5%2585%25A5%25E9%2596%2580/

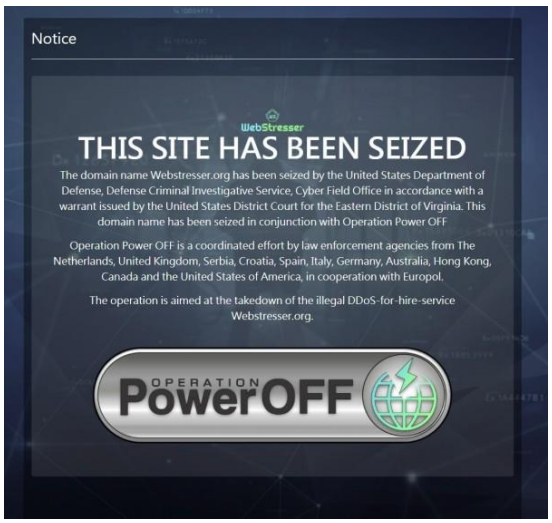
https://devco.re/blog/2014/03/10/security-issues-of-http-headers-1/

https://hzsh.xyz/877/%25E7%25B6%25B2%25E7%25AB%2599http-headers%25E9%2585%258D%25E7%25BD%25AE-%25E5%25BE%259E%25E8%25A8%25AA%25E5%25AE%25A2%25E7%25AB%25AF%25E6%258F%2590%25E5%258D%2587%25E7%25AB%2599%25E9%25BB%259E%25E5%25AE%2589%25E5%2585%25A8%25E6%2580%25A7

3.1.4、5 國聯手破獲全球最大非法 DDOS 販賣網站

英國國家打擊犯罪局表示，英國與荷蘭主導的行動已將一個與全

球逾 400 萬起網路攻擊有關的網站關閉，受害者包括一些大銀行。



資料來源：

http://www.cna.com.tw/news/ait/201804250416-1.aspx

http://news.ltn.com.tw/news/world/breakingnews/2406853

https://udn.com/news/story/6809/3107819

https://technews.tw/2018/04/26/cybercrime-website-behind-4-million-attacks-taken-down/

https://www.techbang.com/posts/58101-webstresserorg-the-worlds-largest-ddos-attack-service-market-has-led-4-million-cyber-attacks-smashed-by-europol

3.1.5、透過電子門卡安全漏洞可侵入飯店房間

芬蘭研究人員發現鎖具製造商亞薩合萊(Assa Abloy)的電子鎖系統有漏洞，駭客僅需隨便一張房卡，就能備份卡片內資料，製作一張通行所有房間的萬用卡片。

資料來源：

https://www.bnext.com.tw/article/48924/hotel-key-cards-even-invalid-ones-help-hackers-break-into-rooms

https://technews.tw/2018/04/27/hackers-find-devious-way-to-break-into-hotel-rooms/

https://news.mingpao.com/pns/dailynews/web_tc/article/20180427/s00014/1524767559770

https://www.ithome.com.tw/node/77526

https://www.ithome.com.tw/node/75122

3.2、駭客攻擊事件及手法

3.2.1、高雄果菜運銷公司遭駭，勒索比特幣約新台幣 7 萬多元

3 月中旬高雄十全果菜市場傳遭勒索軟體入侵，要求 48 小時內付款 0.3 比特幣(折合新台幣 7 萬多元)，否則將強行鎖住電腦，可能影響每日 2000 多萬交易量，經協商受害單位最後仍妥協白白損失 4 萬 3 千元支付的贖金。

據報導，高雄十全果菜市場的果菜運銷公司於 3 月 19 日當天上午 8 點許，果菜市場總經理辦公室祕書交易電腦接獲駭客寄發以中東及羅馬拼音的勒索信函，指稱已在 3 部電腦植入「比特幣病毒」，要求以 0.3 比特幣，轉入指定帳號才能解鎖以拿回電腦主導權，否則強行鎖住電腦。

果菜公司私下尋求電腦廠商仍無法處理，隔天開市作業即受到影

響，包括經銷商、帳目等資料被鎖，狀況混亂，果菜市場隔天 20 日報警請刑大科偵隊協助，經確認是國際常見的比特幣勒索事件。

果菜公司因每日交易量 2000 多萬元，果菜公司為免市場受動盪，不斷派員議價，幾經斡旋議價付贖獲得折半贖金，最後付贖 4.3 萬元到指定帳戶，21 日上午 11 點許透過駭客電郵寄送解密檔解鎖，方得以恢復經銷商及帳目交易秩序。

高雄市警局民族派出所副所長傅水利表示，經高市刑大科偵隊以及委外工程人員協助調查，勒索病毒類似上一波「WannaCry」手法，且發現業者電腦防禦機制薄弱，幾乎不設防，相關設備主機未裝設防毒軟體且授權委外廠商遠端登入，連備份資料都未存放，資安防護出現嚴重漏洞，全案依妨害電腦使用罪受理偵辦。

果菜公司不具名經理坦言有此事，但案情細節不願多談。只透露雖然電腦遭駭無法作業，但最終以人工方式解決，雖然作業流程冗長、繁複，但並未影響這兩天市場交易，未來將請電腦公司協助加強防火牆及資安管控。

警方表示，駭客入侵時有所聞，不少政府部門或民間企業都難逃毒手，只要被駭，幾乎無解，只有付錢一途，業者唯有事前加密，定時更換密碼，做好防範措施才是自保之道。

●TWCERT/CC 建議採取以下方法來避免受勒索軟體影響 ：

1. 定期備份並遵循 3-2-1 規則來備份檔案：建立三份副本，使用兩種不同媒體，一份副本要存放在不同的地方，此外至少有一個系統備份是處於實體隔離的網路環境。

2. 刪除收到的可疑電子郵件，尤其是包含連結或附件的。

3. 確保電腦上的防毒軟體版本及病毒碼更新至最新。

4. 保持作業系統及其他軟體及應用程式為最新版本以及修補。

5. 部分微軟 Office 檔案會要求用戶啟動巨集以觀看其內容，對此類電子郵件附件務必提高警覺。

6. 一旦受到感染，馬上將受感染電腦從網路上及外接儲存裝置隔離。在清除惡意軟體前不要開啟任何檔案。

7. 確實做好實體網路隔離機制，重要電腦非必要儘可能不要隨時保持對外連線，並強化防火牆及其他防護措施。

8. 如果可以，儘可能不要支付贖金，因為除了不能保證可以得到解鎖，卻相反等於告知歹徒他的病毒與獲利作法可行，進而擴大或深入駭侵惡行。

資料來源：

https://tw.appledaily.com/new/realtime/20180331/1325591/

https://tw.news.yahoo.com/果菜市場遭駭客勒索-付贖 4-3 萬解救-215009365.html

http://news.ltn.com.tw/news/society/breakingnews/2382335

http://www.chinatimes.com/newspapers/20180401000502-260107

3.2.2、伊朗遭受全球性的網路攻擊，螢幕被顯示美國國旗

近期駭客發動全國性網路攻擊，包含伊朗的數據中心。伊朗資訊科技部表示，駭客在畫面上留下美國國旗圖片和一段警告：「別來擾亂我們的選舉。」(Don’ t mess with our elections)。

伊朗聲明表示這起攻擊影響全球 20 萬台路由交換器，其中伊朗有 3500 台。Cisco 也曾發布路由器弱點警告並附上修復程式，然時逢伊朗新年假期，因此部分公司並未完成安裝修復程式。

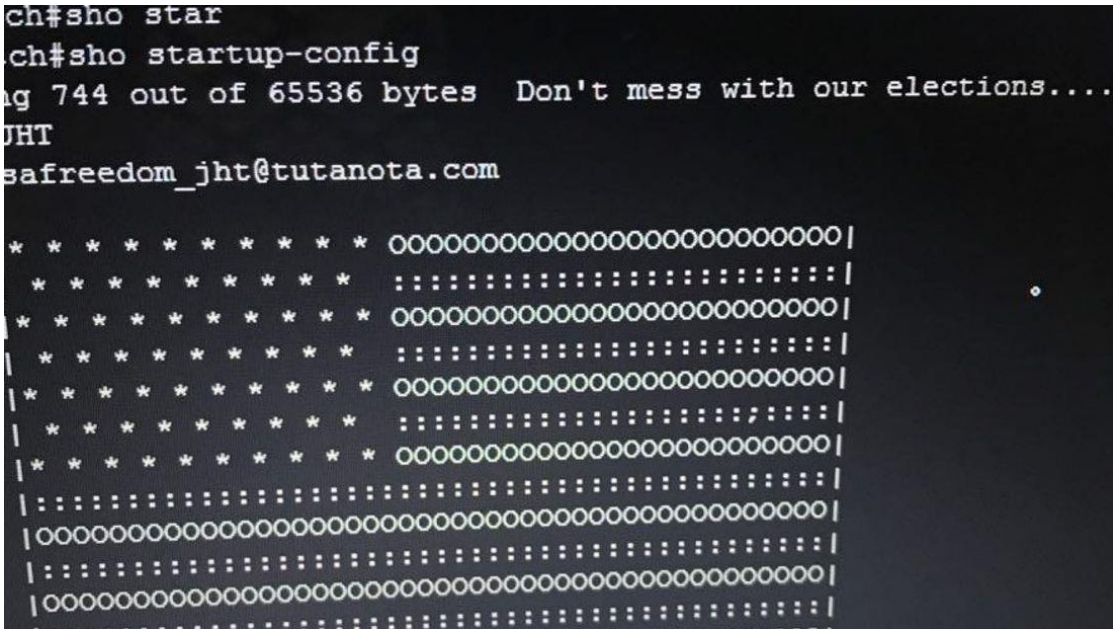
伊朗當局在聲明中表示，這起駭客事件利用 Cisco 路由器的弱點，攻擊各網路供應商，並中斷用戶的網路存取，而 Cisco 尚未立即對此回覆置評。

伊朗資訊科技部部長於推文發布留有美國國旗圖片和訊息的電腦畫面，但目前不清楚攻擊來源。

伊朗官方電視台報導，這起攻擊主要影響歐洲、印度和美國。美國有 5 萬 5000 台裝置遭殃，中國則有 1 萬 4000 台，在所有受影響裝置中，伊朗的數量占 2%。

伊朗電腦危機應變組織 MAHER 在襲擊事件發生後也展示曾向受影響的公司提供弱點方面的資訊。

伊朗國營資訊技術組織的副主管表示，這次攻擊在數小時內就被減緩影響，沒有任何資料流失。



資料來源：

https://tw.news.yahoo.com/駭客入侵全球 20 萬台路由器-伊朗網路出現美國旗-051023675.html

https://www.reuters.com/article/iran-cyber-hackers/iran-hit-by-global-cyber-attack-that-left-u-s-flag-on-screens-idUSL5N1RK0DQ?rpc=401

https://securityaffairs.co/wordpress/71181/hacking/cve-2018-0171-russia-iran-attacks.html

https://www.theguardian.com/world/2018/apr/08/hackers-warn-iran-dont-mess-with-us-elections

3.2.3、索迪斯 Filmology 資料外洩 - 用戶需要取消其信用卡

索迪斯集團(Sodexo)是一家總部位於法國從事餐飲服務及綜合後勤管理的知名大型跨國企業，近期索迪斯向部分客戶通報稱遭受針對其電影券平台 Filmology 的針對性攻擊，並敦促他們取消其信用卡。

該服務為透過打折的電影票提供英國員工獎勵，該企業針對此事件為保護消費者及其資料以及「消除任何進一步的潛在風險」，已將該服務網站撤下，索迪斯 Filmology 在向資訊專員辦公室回報後，並聘請專業的鑑識調查小組。

Sodexo Filmology 公司發布的資料洩露通告表示，建議所有在 4 月 19 日至 3 月 3 日之間使用過該網站的員工取消他們的信用卡並檢查他們的信用卡帳單。並表示這起事件是由於該企業用於託管 Cinema Benefits 平台的系統遭受到有針對性的攻擊所引起，儘管已經採用了經 CREST 認可的安全專家所制定的預防措施。

透過網路搜索可以發現此攻擊已持續數月，因為在 2 月份的 Money Saving Expert 論壇上可以找到數名員工在上面發表遭盜用的事件。有員工表示在與 Filmology 確認事件細節後，被告知在付款頁面被竊取銀行資料，付款頁面的駭侵已進行了 2 個多月，涉及許多帳戶。

資料來源：

https://securityaffairs.co/wordpress/71211/data-breach/sodexo-filmology-data-breach.html

http://forums.moneysavingexpert.com/showthread.php?t=5801854

3.2.4、研究發現，超過 2000 萬個 Chrome 用戶安裝了惡意偽冒廣告攔截器(Ad blocker)

瀏覽器外掛中，廣告攔截程式(Ad blocker)在幫助用戶安全瀏覽網路發揮重要的作用，同時不會因為在關閉彈出式廣告而被重導向到用垃圾郵件轟炸用戶的詐騙網站。

目前在桌上型電腦和移動設備上有超過 10 億人正在使用的 Chrome 瀏覽器，在資安公司研究報告中揭露，Chrome 瀏覽器就像

是大量偽冒外掛程式的集散地，尤其是惡意的廣告攔截器，根據說法，由於 Chrome 網路商店的安全性管控不佳，目前有超過 2000 萬的 Chrome 用戶在其瀏覽器上安裝了偽造的廣告攔截器外掛程式。

這些偽冒外掛程式的主要例子之一就是擁有超過 1000 萬用戶的 Google Chrome 瀏覽器外掛「AdRemover」。在進一步的檢查中，Adguard 研究人員發現了兩個包含混淆腳本的.txt 檔案，可以追蹤由受害者瀏覽器發出的每個 request。

研究人員將其標記為一個由數百萬個受感染瀏覽器所組成的「natural botnet」，它可以或已經被用來竊取 Chrome 用戶的個人資料，並將其發送到疑似命令與控制伺服器(C&C)。

這個隱藏的腳本除監聽瀏覽器發出的請求外，並以 MD5(url +" %Ujy%BNY0O")比較從 coupons.txt 加載的簽名列表。當所述簽名被命中時，便從 domaing.qyz.sx 加載一個 iframe，傳遞被訪問頁面的相關資訊，然後重新初始化該外掛。例如，其中一個簽名與 https://www.google.com/相對應。

此外，Chrome 網路商店上還有其他四款假廣告攔截器遵循與 AdRemover 外掛程式相同的模式。偽冒的惡意 Adblockers 列表如下：

Webutation(目前由超過 30,000 名用戶安裝)

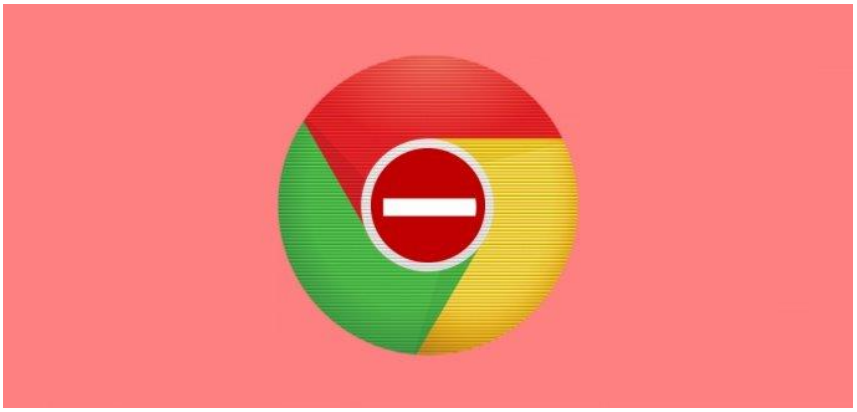
HD for YouTube(目前由超過 40 萬用戶安裝)

Adblock Pro(目前由超過 200 萬用戶安裝)

uBlock Plus(目前由超過 800 萬用戶安裝)

Google Chrome 的 AdRemover(目前由超過 1000 萬用戶安裝)

該資安公司已經向 Google 通知 Chrome 網路商店上存在惡意 Adblockers 的情況，但是在發布時，所有上述外掛程式仍可安裝使用。因此，如果用戶正在使用這些 Adblocker 中的任何之一，建議立即移除以免遭駭客利用。



資料來源：

https://www.hackread.com/20-million-chrome-users-have-installed-fake-malicious-ad-blockers/

https://blog.adguard.com/en/over-20-000-000-of-chrome-users-are-victims-of-fake-ad-blockers/

3.2.5、停止下載「skin」，50,000 個 Minecraft 用戶感染抹除硬碟資料的惡意軟體

據研究人員表示，發現近 50,000 名 Minecraft 用戶感染惡意軟體，該惡意軟體會重新格式化硬碟，並清除目標系統中的備份資料以及刪除其他重要檔案。Avast 研究人員發現針對 Minecraft 玩家的惡意軟體，其主要目標是那些下載用以改變 Minecraft 中角色預設外觀的 PNG 檔案格式「skin」的 Minecraft 用戶。

這些惡意「skin」包含一個惡意的 Powershell 腳本，觸發惡意軟體刪除用戶資料並重新格式化系統的硬碟。感染惡意軟體還會啟動 tourstart.exe 迴圈，從而影響目標系統的性能。

此外，受害者的 Minecraft 帳戶收件箱中還會收到的無聊訊息，表明整起活動都是為了愚弄用戶。以下為 Avast 研究人員分享的訊息原文：「"You Are Nailed, Buy A New Computer This Is A Piece Of Sh*t" "You have maxed your internet usage for a lifetime" "Your a** got glued."」

然而，研究人員在最近 10 天內阻止了 14,500 次針對 Minecraft

用戶的感染企圖，這表示用戶始終有高度感染此惡意軟體的風險。根據 Avast 的惡意軟體分析師 Alexej Savcin 的說法，惡意程式碼在很大程度上並不起眼，可以在提供關於如何使用記事本製作病毒的逐步說明的網站上找到。

持平而言，儘管主嫌並不是專業的網路犯罪分子，但更重要的是為什麼感染的「skin」可以合法地上傳到 Minecraft 網站。由於惡意軟體的網域是來自 Minecraft 官方，任何觸發的檢測都可能被用戶誤解為誤報。

Minecraft 在全球擁有超過 7400 萬玩家，使其成為惡意駭客和網路犯罪分子的利潤目標。這次只是一個會刪除用戶資料惱人的惡意軟體，改天可能就是一個會接管系統的勒索軟體，並迫使受害者支付贖金。

Avast 已經通知 Minecraft 在 Mojang 的開發人員，希望該公司很快就會提出解決方案。同時，建議用戶避免在系統上安裝 Minecraft「skin」，直到問題得到解決。

資料來源：
https://www.hackread.com/50000-minecraft-users-infected-with-hard-drive-wiping-malware/

https://blog.avast.com/minecraft-players-exposed-to-malicious-code-in-modified-skins

3.3、軟硬體漏洞資訊

3.3.1、一打弱點波及 Trend Micro 郵件加密閘道，包括 XSS、RCE、SQL injection

以 Linux 為基礎的趨勢郵件加密閘道 Trend Micro Email Encryption Gateway(TMEEG)，功能係於企業閘道位置，按照收、寄件信箱及關鍵字等預設規則，對郵件自動化加解密，TMEEG 被分析出 12 項弱點，其 RPM 新流程 HTTP 連線未加密，更新檔亦無驗證，受中間人攻擊或 CSRF，則檔案明文訊息及更新檔易遭竄改，導致 RCE；日誌儲存路徑被惡意控制恐釀 root 身分遭濫用；最為嚴重瑕疵乃系統級程式 registration 無前置身分驗證，若管理者帳密等組態被竄改，則所有電郵皆不保；configuration.jsp 遇 XML external entity，可能暴露本該保護之組態腳本資料；另 keymanserverconfig.jsp、mimebuilderconfig.jsp、editPolicy.jsp 所轄參數均有 XSS 缺點，參數過濾為周，故無法防止非預期函數執行；至於 SQL injection 發生在 policies.jsp、editPolicy.jsp、emailSearch.jsp 等腳本，同樣是參數無檢驗機制，然引發不當 SQL 語法，恐遭駭客刪除重要資料表，或者越權查詢內容，甚至獲得全數郵件，趨勢公司已大部修補並公開下載，然 2 項漏洞涉及軟體工程複雜性，建議採白名單式網管，縮減受威脅程度。

資料來源：

https://success.trendmicro.com/solution/1119349#

https://www.coresecurity.com/advisories/trend-micro-email-encryption-gateway-multiple-vulnerabilities

3.3.2、友訊 DIR-850L 無線路由器 0-day 漏洞遭披露，入口網頁不設防

資安分析師 Gem George 研究發現，D-Link DIR-850L 無線路由設備因設計瑕疵，其入口網頁 SharePort Web Access 雖有帳密驗證介面，然僅需於網址列後貼上 category_view.php 或 folder_view.php，可逕自規避驗證而瀏覽設備資訊，操作過程皆免身分權限過濾，尤其 folder_view.php 具有增刪資料夾功能，此 0-day 漏洞事件極易探勘，技術門檻幾近於零，實作影片於 youtobe 撥放，點閱率逾 200，自弱點發現迄今約一週，D-Link 尚無回應，亦未供應修補檔，建議使用者限制連線存取對象 IP，先期備份重要檔案，避免成為攻擊標靶。

資料來源：

https://www.youtube.com/watch?v=Wmm4p8znS3s

https://exploit.kitploit.com/2018/03/d-link-dir-850l-wireless-ac1200-dual.html

3.3.3、CA 公布 Workload Automation AE、Workload Control Center、API Developer 產品瑕疵，企業客戶請關注修補進度

CA Technologies 前身為組合國際電腦股份有限公司(Computer Associates Inc)，就大型機(mainframe)、分散式、虛擬化、雲端運算等異質 IT 環境，研發管理和保護技術方案，供應自動化及負載平衡相關服務，經分析特定軟體，計有 5 項缺陷恐受遠端攻擊，Workload Automation AE 將引發 SQL injection；Workload Control Center 之 Apache MyFaces 元件衍生 RCE；另 API Developer 內 profile picture、widgetID 變數、apiExplorer 於運算過程皆有觸發 Cross-Site Scripting 之風險，CA 公司已釋出對應修補方式，使用上述產品之企業宜檢視安裝版本及修補進度。

資料來源：

https://support.ca.com/us/product-content/recommended-reading/security-notices/ca20180329-01--security-notice-for-ca-workload-automation-ae.html

https://support.ca.com/us/product-content/recommended-reading/security-notices/ca20180328-01--security-notice-for-ca-api-developer-portal.html

3.3.4、惡意播放清單將觸發 DVD X Player 緩衝區溢位與例外處理脫序

知名播放軟體 DVD X Player 標準版，系統需求低(CPU 350 MHz 以上)，適用於 Windows 98、2000、XP、Vista、7 等歷代作業系統，特點是無區碼限制，提供桌上劇院愛好者便利性，自 2011 年 DVD X Player Standard 5.5.0 發行迄今，升級版號歷經更迭，現行 DVD X Player Standard 5.5.3.9 經駭客 Prasenjit Kanti Paul 測試，若本機接收處理畸形播放清單檔(PLF)，將引發 buffer overflow，被迫導入結構化例外處理(Structured Exception Handling)之探勘攻擊，結合 pop pop ret 技術促使控制權交付特定 shellcode，可能憑藉高階權限執行非預期程式，該瑕疵列高危險性，惟須注意其測試環境乃 Windows XP SP3 x86，然未知程式漏洞於 Windows 7 奏效與否，Aviosoft 公司(前身 DVD X Studios)迄今尚無公開對策。

資料來源：

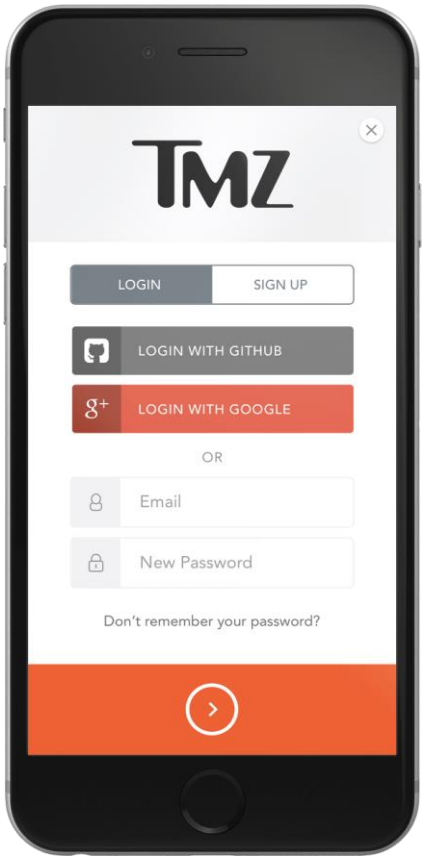
https://0day4u.wordpress.com/2018/03/30/buffer-overflow-on-dvd-x-player-standard-5-5-3-9/

https://vuldb.com//?id.115494

http://www.cnblogs.com/Wrong-Side/p/4456268.html

3.3.5、身分驗證整合平台 Auth0 修補 token 參數核驗破綻與 CSRF 瑕疵

為整合平台間複雜的身分驗證，大型 'Identity-as-a-service' 供應商 Auth0 扮演代理人角色，幫助開發人員連通自家系統和第三方，融合現行主流 authentication(認證)和 authorization(授權)協定，當第三方登入之際，Auth0 的 API 封裝授權協議，提供統一介面，完成用戶認證流程，再回應系統是否認證成功，經 Cinta Infinita 研究員滲透測試，查 Auth0 authentication 出現嚴重安全破綻，藉由 token-based 認證，駭客得以繞過 JSON Web Token(JWT)之 audience 參數檢查，將 token 移花接木假冒他人，越權獲得暨控制資料；另啟動 Legacy Lock API 旗標之租戶，恐在驗證帳密後，HTML 表單遭截獲，令受害者連線被非法帳號頂替，行動遭駭客一覽無遺，綜合前述弱點，攻擊者循不同社交軟體媒介，可接觸目標系統之入口並實施攻擊，估計全球逾 2000 企業以日均 4200 萬次登入量，依賴 Auth0 服務平台，漏洞影響幅員頗鉅，所幸 Auth0 於獲報 4 小時內補強 JWT audience 參數檢查功能，另宣布將於今年 7 月 16 日強制停用 Legacy Lock API。



資料來源：

https://thehackernews.com/2018/04/auth0-authentication-bypass.html

https://auth0.com/docs/security/bulletins/cve-2018-6873

https://auth0.com/docs/security/bulletins/cve-2018-6874

3.3.6、惡意物件恐釀 Password Vault 密碼金庫 RCE 危機，企業速取得 CyberArk 釋出版本

資安公司 CyberArk 宗旨，在保護企業 IT 資產免於內外部攻擊，對層峰帳密提供稽核管控之系統化服務，旗下產品 Enterprise Password Vault(EPV)，設計如保險庫般存放重要密碼，對 OS、應用程式、database、網路設備、腳本之重要密碼集中管理，按照組織政策，設定排程、對象設備(系統)、複雜性等參數，能定期偵測 IT 資產密碼狀況，自動化模擬使用者輪流登入設備，變更密碼及測試，並

能監控、隔離、記錄高階帳密連線活動，據悉客戶遍及全球 65 國 3000 家企業，經德國 RedTeam 資安測試團隊研究發掘嚴重漏洞，EPV 無法檢驗序列化 .NET 物件 CyberArk.Services.Web.SessionIdentifiers 之完整性，接收假造物件時，連帶影響對 HTTP 認證請求內授權 header 之處理結果，讓未獲授權之攻擊者，竟仗系統服務權限發動 RCE 攻擊，恐有機會開啟 Password Vault 後門，危及關鍵帳密，CyberArk 已修補升級各版 Password Vault。

資料來源：

https://www.redteam-pentesting.de/en/advisories/rt-sa-2017-014/-cyberark-password-vault-web-access-remote-code-execution

https://thehackernews.com/2018/04/enterprise-password-vault.html

3.3.7、使用 Outlook 預覽 RTF 信件，用戶隱私將外流

Microsoft 郵件軟體 Outlook，可閱讀 Rich Text Format 與 HTML 格式郵件，據資安分析員 Dormann 調查，若駭客利用 Outlook 運作方式破綻，寄送惡意 RTF 信件且內含 OLE(Object Linking and

Embedding)物件，Outlook 將自動單一登入(SSO)，與遠端 SMB 伺服器啟始驗證，SMB 連線過程送出 IP、帳號、hostname、密碼 hash 值等系統資訊，自動化連線至攻擊方設備頗具當機風險，涉及 DoS 之瑕疵現已修補；儘管 2018 年 4 月份安全更新已公布，禁止自動化 SMB 連線，然無法阻絕因社交工程而誘導鏈結至惡意 UNC 路徑，仍有機會手動觸發 SMB 連線，導致機敏資料外流，若原始密碼複雜度過低，雜湊值易遭短期內暴力破解，除例行更新外，尚須阻擋專用 port(445/tcp、137/tcp、139/tcp、137/udp、139/udp)與停用 NTLM SSO 認證方式，方得保系統無虞。

資料來源：

https://insights.sei.cmu.edu/cert/2018/04/automatically-stealing-password-hashes-with-microsoft-outlook-and-ole.html

https://thehackernews.com/2018/04/outlook-smb-vulnerability.html

3.3.8、排版軟體 Adobe InDesign 受偽冒檔案衝擊，衍生 memory corruption 及惡意函數執行

Adobe 所開發 desktop publishing 軟體 InDesign，具有靈活圖文排版能力，與 Photoshop、Illustrator、Acrobat 高度相容，可於桌機環境製作海報傳單、雜誌書冊等文宣品，亦可生產電子書，其成品均適用平板展示。經 FortiGuard Labs 分析，無論在 Windows 或 Mac 平台上操作 InDesign，囿於其安裝工具無法辨識搜尋路徑可

靠性，可能載入惡意 DLL，以系統權限執行非預期函數；另特製 inx 交換格式檔案開啟過程，因解析肇生記憶體越界錯誤，易引發程式 crash 或任意代碼執行，Adobe 已公告更新版本。

資料來源：

https://helpx.adobe.com/security/products/indesign/apsb18-11.html

https://www.cybersecurity-help.cz/vdb/SB2018041014?affChecked=1

3.3.9、安裝音樂後製軟體 SoundEngine，留神危險 DLL 來源路徑

日本 Coderium 公司製作音樂編輯軟體 SoundEngine，適用 Windows Vista 以後平台，具音源錄播、波形剪貼、格式轉換等編輯功能，SoundEngine 分 free 與 professional 兩系列，經分析弱點存在於 SoundEngine Free 5.21 以前版本，囿於 Dynamic Link Library 實作方式之先天缺陷，在 Windows Vista & 7 環境，經身分驗證之駭客，於本機探勘 Search Path 漏洞，劫持 DLL 並以木馬頂替，SoundEngine Free 安裝工具搜尋到不可靠路徑後，安裝過程載入惡意 DLL，恐令攻擊者接管 OS 管理權，該弱點影響僅止於 SoundEngine Free 安裝階段，無損音樂後製功能，目前 Coderium

已修補相關瑕疵，最新釋出版 SoundEngine Free 5.23 可供下載。

資料來源：

https://soundengine.jp/wordpress/penguin_press/press_release/4187/

http://jvn.jp/en/jp/JVN85056623/index.html

3.3.10、注意 LG NAS 無法抵禦 command injection，用戶資料悉數外流

VPNMentor 係研究員與駭客組成之團隊，本月中測試 LG 出廠 network attached storage，察覺 Pre-Authentication 之遠端命令注入漏洞，破綻在於 LG NAS 遠端管理登入介面，對「password」參數缺乏合宜過濾，成為駭客攻擊點，搭配 Burp Suite 工具，經由特製 PHP shell 將 payload 傳入 LG NAS 介面，可竊取資料庫內全數帳密、email、MD5 hash 值，並能新增專用帳密，從此駭客成為授權用戶，得隨意窺探設備內任何資料，目前 LG Electronics 尚無修補方案，建議管理者定期檢查有無異常帳號，並建構防火牆確保連線 IP 來源可靠。

資料來源：

https://youtu.be/7RgCq5d13qk

https://www.vpnmentor.com/blog/critical-vulnerability-found-majority-lg-nas-devices/

3.3.11、執行 7-Zip 毋用記憶體分頁選項，以保護 Windows 平台

知名壓縮軟體 7-Zip 以 C、C++開發，係遍及 86 個語系地區的開放原始碼軟體，搭配 Windows 及 Unix-like 作業系統，提供圖形介面與自行開發的 7z 格式，有別其他壓縮軟體，7-Zip 支援 Large memory page 選項，經在 Windows 10 平台測試 7-Zip，察覺其特點反成弱點，因對大型運用權無安全限制，一旦用戶經 7-Zip 之 Large memory pages 選項呼叫 LsaAddAccountRights 函數，可直接被賦予 SeLockMemoryPrivilege 權力，即使在沙箱環境亦然，若用戶蓄意為之，可憑藉 SeLockMemoryPrivilege 特權操縱任何程式，對作業系統形成威脅，7-Zip 暫無更新公告。

資料來源：

https://sourceforge.net/p/sevenzip/discussion/45797/thread/e730c709/?limit=25&page=1#b240

https://tools.cisco.com/security/center/viewAlert.x?alertId=57517

3.3.12、ASUS 更新韌體設計，消彌旗下 14 型路由器 RCE 及 buffer overflow 危機

資訊產品大廠華碩，公告 14 款路由器及專配 4 種版本韌體，具數類瑕疵，最為嚴重者影響全數軟硬體，係變造資料輸入後，將擴權執行代碼；原始碼 httpd.c 內函數 handle_request( )設計不當，身分認證失敗仍可處理 POST 請求；web.c 內 do_vpnupload_post( )及 ej_update_variables( )函數，對身分驗證狀態邏輯判斷失常，可放行無授權之 NVRAM 組態更新，且未過濾輸入字串長度，導致更新設定時引發 stack buffer overflow；駭客亦可藉惡意 DNS 和 DHCPv6 封包、IPv6 RA 訊號，取得遠端系統控制權，造成溢位、DoS，並竊取機敏資料，ASUS 發布最新韌體以解決安全問題，目前已有用戶反映設備遭遇不明設定異動情事，建議儘速下載安裝官方程式。

資料來源：

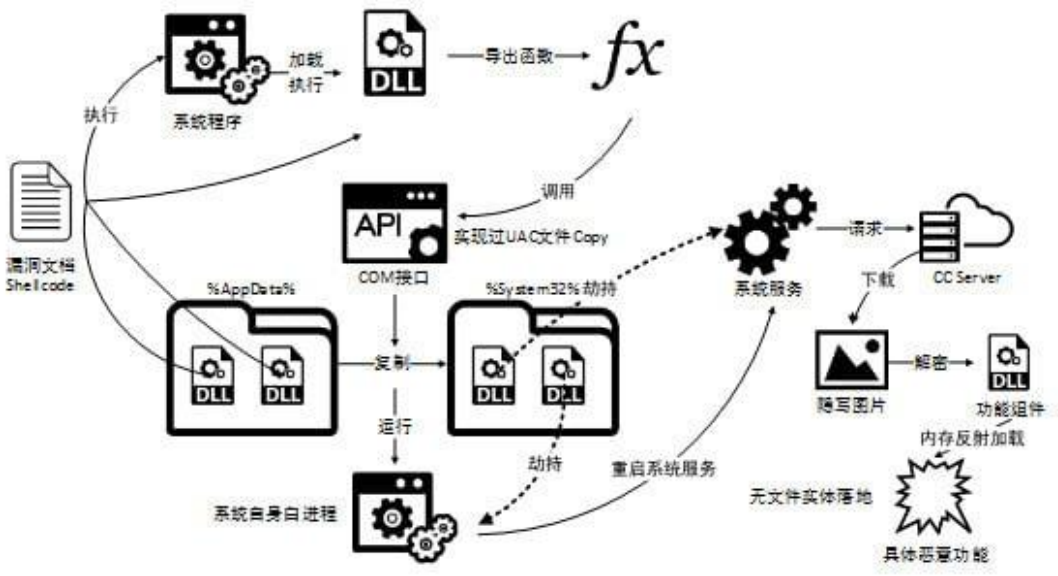
https://www.w0lfzhang.com/2018/01/17/ASUS-router-stack-overflow-in-http-server/

https://www.exploit-db.com/exploits/43881/

3.3.13、微軟用戶慎防「double kill」，全球首例 APT 正藉 Office 瞄準 IE kernel 破綻

本月份微軟產品再度面臨威脅，據中國大陸資安研究單位 Qihoo 360 Core 指出，喚作「雙殺」的 APT(advanced persistent threat)，刻正藉由 Office 檔案掩護，攻陷 Internet Explorer 之 0-day 漏洞，因 IE 瀏覽器引擎可被其他程式呼叫，內嵌惡意網頁的 Office 檔一旦被使用者開啟，則於背景遂行複雜攻擊流程，前期從遠端載入 code 或 payload，伺機植入木馬，後續採用 UAC bypass、資訊藏密相關技術，躲避流量監測與防毒軟體偵測，鑒於 Office 高市佔率，該漏洞危及用戶甚廣，然微軟態度如同過年前遭遇 Skype DLL 劫持事件，一貫地冷處理，僅回應每月提供更新解決安全問題，意即在理想狀況下，母親節前可完成安全更新部署，殊值注意者，此 APT 顯然鎖定 Windows 使用者，故請收斂好奇心，莫開啟來路不明的檔案(不限

Office 格式)，直到 5 月份順利修補。



資料來源：

https://www.bleepingcomputer.com/news/security/internet-explorer-zero-day-exploited-in-the-wild-by-apt-group/

https://news.softpedia.com/news/zero-day-flaw-in-internet-explorer-allows-hackers-to-infect-windows-pcs-520804.shtml

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
2018/05/15	2018 Explore Next Cyber Taiwan-國際資安新創交流活動	【資安研討會】2018 Explore Next Cyber Taiwan-國際資安新創交流活動 日期：2018 年 05 月 15 日(二) 地點:南港展覽館 504 會議室 (台北市南港區經貿二路 1 號 5 樓) 主辦單位：經濟部工業局、經濟部國際合作處 活動網址： http://pr.ithome.com.tw/2007/20180419-itri/1111.htm

時間	研討會/課程名稱	研討會相關資料
		活動概要： 臺灣政經情勢特殊，經常面對嚴峻的網路攻擊，我們必須用更高的標準看待資訊安全並加以觀察與思考。基於化危機為轉機並符合現今產業與國際趨勢， 「2018Explore Next Cyber Taiwan-國際資安新創交流活動」，透過邀請國際專家剖析美洲、歐洲、亞洲之資安市場及趨勢。上午場邀請美國、以色列、荷蘭、韓國之新創成功業者進行交流與分享，下午場以國際觀點探討資安關鍵技術應用與趨勢，期望透過本次活動提昇臺灣資安產業接軌國際市場之能量。
2018/05/20-07/12	2018AppHackathon	【資安競賽】2018AppHackathon 主辦單位：台灣雲端安全聯盟 日期：2018 年 05 月 20 日(日) - 2018 年 07 月 12 日(四) 地點：集思台大會議中心(台北市 106 大安區羅斯福路四段 85 號 B1) 線上報名連結： https://csa.kktix.cc/events/2018apphack 活動概要： 智慧型手機已成為現代人必備的設備，同時 App 使用也成為最貼近人類生活的一種通訊模式。但要如何提供具有安全性的 App 服務，已成為各行各業所注意的焦點。此外，要如何檢測一個具有安全性的 App 服務程式，也是 App 產業非常重視的課題。 因此，資安學會特別舉辦此次 App 自動化檢測工具競賽活動，其的目的是在培養未來各產業需求的自動化檢測平台之開發人才，以提升相關資訊素養能力。也就是，希望從競賽當中，互相觀摩學習，激盪出創意的火花，發掘賦有各式創新檢測想法與測試模式。

時間	研討會/課程名稱	研討會相關資料
		最後希望透過此次的競賽活動，能匯集各界菁英智慧，進而發揮創意，開發自動化檢測平台，作為選擇檢測 App 方案之參考，以紓解 App 資安漏洞問題暨改善 App 開發之安全品質。
2018/05/24-05/25	第二十八屆全國資訊安全會議暨資安產業技術研討會	【資安研討會】第二十八屆全國資訊安全會議暨資安產業技術研討會 日期:2018 年 05 月 24 日(四) - 2018 年 05 月 25 日(五) 地點：國立臺灣科技大學國際大樓一樓會議廳(台北市大安區基隆路四段 43 號) 主辦單位：中華民國資訊安全學會、國立臺灣科技大學 活動網址：https://twisc.kktix.cc/events/39966ee4 活動概要： 「第二十八屆全國資訊安全會議暨資安產業技術研討會」即將於臺灣科技大學國際大樓一樓會議廳舉行，會場設有贊助廠商攤位並提供產業技術研討會之機會向來賓展示相關技術與產品解決方案。此次會議有為數眾多的資訊安全研究成果發表，屆時預期將會有非常多來自產、官、學界的各界先進蒞臨。為了讓蒞臨嘉賓能夠更輕鬆的吸收相關的業界新知，我們今年將準備精彩的內容，包含了各類資訊安全相關議題，我們將邀請業界、學界專家到場進行 Keynote 演講。「 資安產業技術研討會」 也開放給一般民眾入場，無需註冊及報名費用。另外會場備有精緻的茶點，我們也將準備精美的小禮物贈送給各位蒞臨嘉賓。歡迎蒞臨現場和我們一起參與這場一年一度的資安盛宴，更多詳情請至會議網站查詢。
2018/05/26	基礎網頁安全與滲透測試	【資安訓練課程】基礎網頁安全與滲透測試 課程時間：2018 年 05 月 26 日(六) 受訓地點：國立交通大學 台北校區 (台北市中正區忠孝西路一段 118 號) 主辦單位：亥客書院 線上報名連結：

時間	研討會/課程名稱	研討會相關資料
		https://hackercollege.nctu.edu.tw/?p=302 課程簡介： 滲透測試是一種檢驗系統安全強度的技術，透過各種專家知識和最佳法則(best practices)所研擬的流程方法，由一組安全技術團隊，以探察、分析、驗證到記錄的流程，模擬駭客的行為找出系統上邏輯性錯誤或更深層次的漏洞。 目前企業對外聯通管道主要以網頁與電子郵件為主，因此本課程將先說明基本滲透測試的知識與技能，了解目前國內外常見的網頁弱點，並實際操作具有弱點的虛擬網站，探討實務上的測試方式，了解潛在的安全威脅與問題。 課程大綱： 基礎網頁安全(上午) 1.Web 應用程式安全趨勢 2.網頁安全常見威脅 3.OWASP Top 10 4.CWE/SANS Top 25 5.CVSS 與常見網頁攻擊手法 基礎網頁滲透測試(下午) 1.滲透測試簡介 2.常用之滲透測試方法論 3.網頁滲透測試框架 4.網頁滲透測試流程與細節 5.網站應用程式弱點實作 ★ 本學院課程提供務實的技術演練，課程中將進行虛擬軟體模擬演練，教導學員安裝軟體及實務案例操演，使學員於課後能夠持續使用與練習。 ★ 本課程提供一人一機筆記型電腦上課使用。如欲自備自備筆記型電腦，電腦軟硬體需求: i3 以上 CPU、4G 以上記憶體、40G 可用硬碟空間、安裝 64-bits 作業系

時間	研討會/課程名稱	研討會相關資料
		統、VirtualBox 5.1.10 以上版本。
2018/06/01	舞弊稽核與數位鑑識系列_事件應變第一線人員之數位證據保全實作	【資安訓練課程】舞弊稽核與數位鑑識系列_事件應變第一線人員之數位證據保全實作 主辦單位：中華民國電腦稽核協會 課程時間：2018 年 06 月 01 日(五) 受訓地點：電腦稽核協會訓練教室(台北市信義區基隆路 1 段 143 號 2 樓之 2) 線上報名連結： http://bit.ly/2Ey4rOK 課程簡介： 對於個人電腦或伺服器進行數位鑑識蒐證前之準備工作說明，及現場數位證據保全程序說明，現場蒐證工具說明及操作現場數位證據保全工具。 課程大綱： 1.數位證據特性及保全要點 2.ISO/IEC 27037 介紹 3.數位證據保全建議程序 4.第一線工具適用時機及功能簡介 5.實務操作
2018/07/10-12	2018 國際資安組織台灣高峰會	【資安研討會】2018 國際資訊安全組織台灣高峰會 主辦單位：CSA Taiwan Chapter、The Honeynet Project Taiwan Chapter、OWASP Taiwan Chapter Workshop 日期：2018 年 07 月 10 日(二) 研討會日期 : 2018 年 07 月 11 日(三) ~ 2018 年 07 月 12 日(四) 地點：集思台大會議中心(台北市大安區羅斯福路四段 85 號 B1) 線上報名連結：http://2018.twcsa.org/ 活動概要： 今年的國際資訊安全組織台灣高峰會，由 Cloud Security Alliance 台灣分會、The Honeynet Project

時間	研討會/課程名稱	研討會相關資料
		台灣分會以及 OWASP 台灣分會共同主辦，同步接軌 Cloud Security Alliance、The Honeynet Project 與 OWASP 等國際資訊安全組織最新研究成果，有來自國內外的專業講師帶來的精彩分享，提供與會人員掌握全球資訊安全發展脈動與趨勢，會議內容涵蓋雲端服務安全、誘捕資安技術、網站應用程式安全、事件掌握與應變等議題，接軌國際資安社群有助於掌握全球發展趨勢。
2018/07/27-28	HITCON Community 2018	【資安研討會】HITCON Community 2018 主辦單位：HITCON GIRLS、社團法人台灣駭客協會 Association of Hackers in Taiwan、CHROOT Security Group 會議日期：2018 年 07 月 27 日(五) ~ 2018 年 07 月 28 日(六) 會議地點 : 台北南港展覽館一館 5 樓(台北市南港區經貿二路 1 號五樓) 報名日期 ： ■ 第一階段 售票日期：2018/05/05 20:00 - 2018/06/02 12:00 ■ 第二階段 售票日期：2018/06/16 20:00 - 2018/07/07 12:00 會眾票： ■ 一般票票價：新台幣 3,500 元 ■ 學生票票價：新台幣 1,500 元 ■ 此票價包含 HITCON Community 2018 會眾 Badge 乙張、迎賓袋乙份及 HITCON Community 2018 限量 T-Shirt 乙件 升級票： 今年提供一個精美設計且和主題搭配的電路板，歡迎選擇「升級」票種，你將會拿到 HITCON 獨家的特製電路板！(市價約二千元，還有玩不完的多樣功能！)

時間	研討會/課程名稱	研討會相關資料
		■ 一般票票價：新台幣 5,000 元 ■ 學生票票價：新台幣 3,000 元 ■ 此票價享會眾票所屬福利，並另包含 HITCON Community 2018 專屬電路板，電路板詳細規格將於日後公布 VIP 票 ■ 票價：新台幣 10,000 元 ■ 此票價享會眾票所屬福利，並另包含 HITCON Communtiy 2018 會議廳快速通關、HITCON Community 2018 貴賓室通行權、專屬 VIP 晚宴與高科技電路板，HITCON Community 2018 專屬電路板詳細規格將於日後公布 ■ VIP 晚宴時間：2018 / 07 / 27(五)18 : 00，地點將個別公布 報名網址： https://hitcon.kktix.cc/events/hitcon-cmt-2018 活動概要： 今年的 HITCON Community 以區塊鏈(Blockchain) 作為主題，不只是因為區塊鏈技術中數據的儲存、驗證、傳遞與資安息息相關，更因為分散式節點的去中心化，正是反對權威、支持資訊自由交流的駭客精神。

第 4 章、2018 年 04 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，2018 年 4 月收到通報計 5662 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。

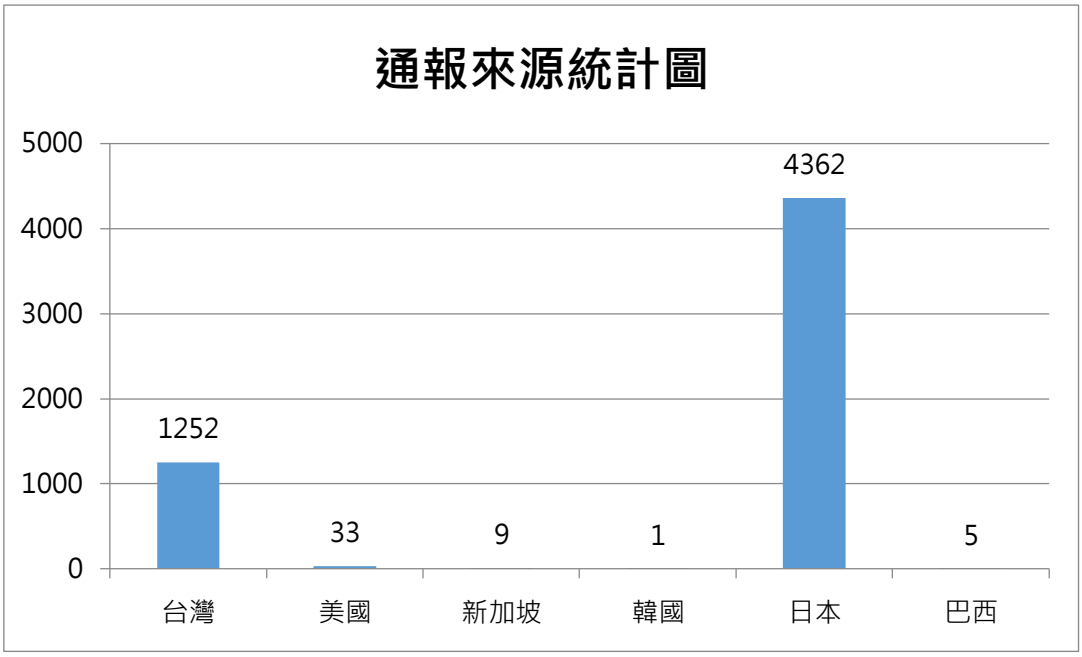


圖 1、通報來源統計圖

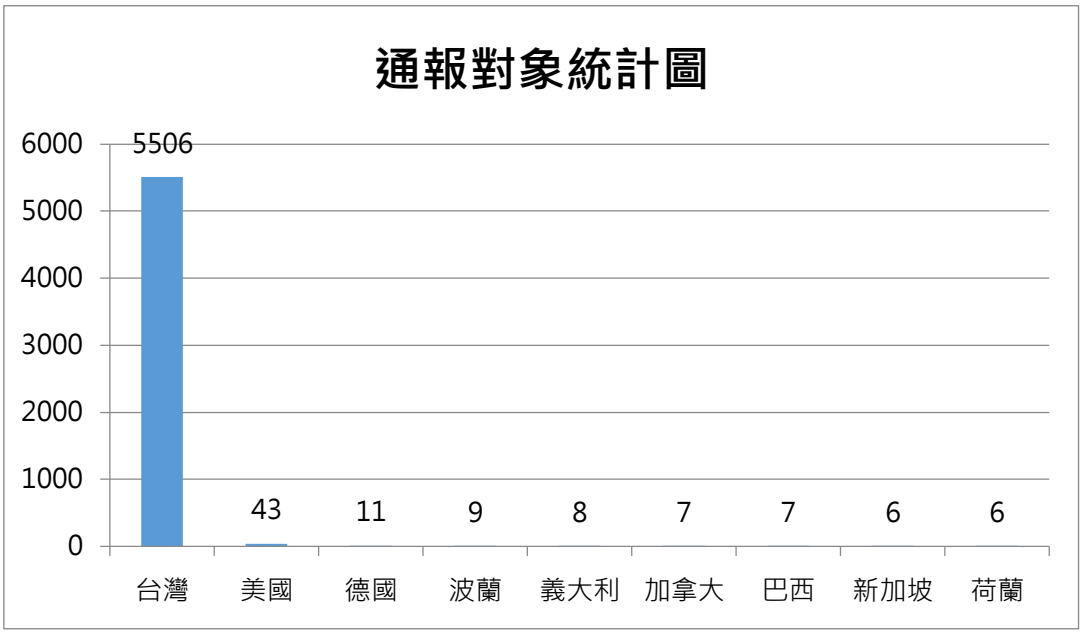


圖 2、通報對象統計圖

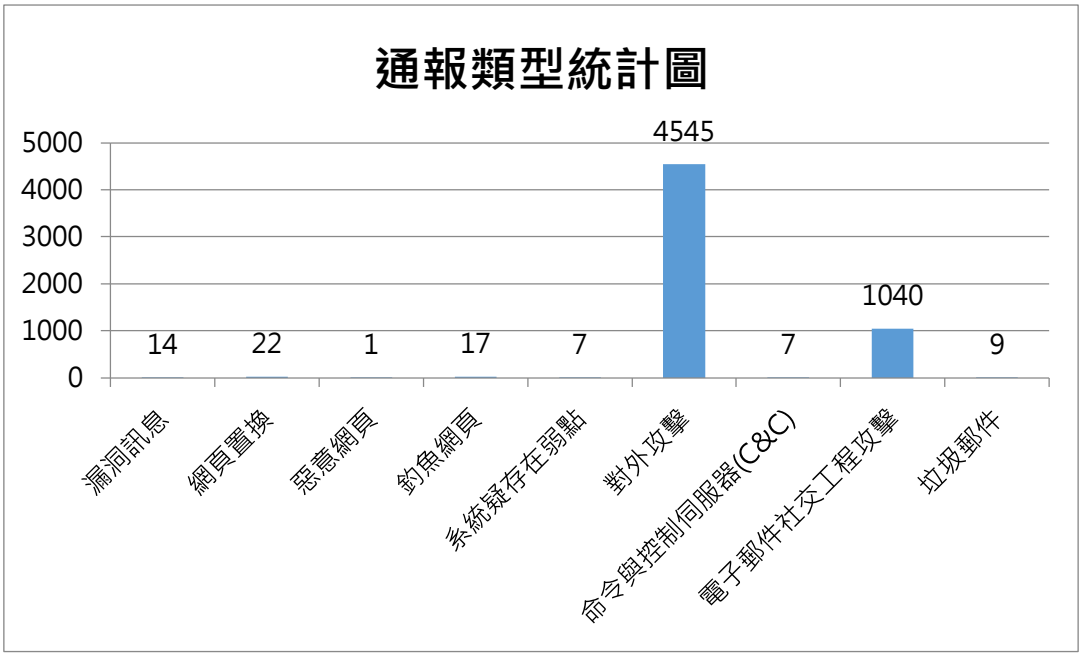


圖 3、通報類型統計圖

本月多筆通報為網頁的「資料庫注入攻擊(SQL Injection)漏洞」，可經由該漏洞取得後端資料庫權限及完整資料(包含大量使用者個資或敏感性資料)，同時也有機會對資料進行破壞或修改。

建議網頁過濾 SQL 語法常用之關鍵字，如：user、select 及 from 等關鍵字，及注釋符號與特殊規則，如：單引號(')等符號；利用正規表示式檢查網頁所傳入參數之型態，若參數型態不符時便導回原頁面或網站首頁。利用專業弱點掃描程式進行系統弱點掃描，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 5 月 9 日

編　　輯：羅文翎

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/

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

資安電子報訂閱：http://i-to.cc/S5HzJ

線上電子報閱覽：https://twcertcc.blogspot.tw/

如有任何疑問或建議，歡迎您不吝指教。