TWCERT/CC 資安情資電子報

2018 年 9 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 1

第 2 章、 TWCERT/CC 近期動態 2

2.1、 TWCERT/CC 將於 10 月 3 日舉辦「2018 台灣資安通報應變年會-企業無可避免的資安管理責任」 2

2.2、 協辦 107 年度高中職資安種子教師研習營 3

2.3、 協辦 2018 神盾盃網路奪旗 CTF 競賽 4

第 3 章、 國內外重要資安新聞 5

3.1、 國內外資安政策、威脅與趨勢 5

3.1.1、 經濟部工業局提供資訊安全檢測診斷服務補助申請 5

3.1.2、 西澳政府進行內部稽核，發現弱密碼問題仍嚴重 6

3.1.3、 觀光業遭殭屍網路攻擊比例上升，身分資料被竊風險提高 7

3.1.4、 NCC 將公布物聯網資通安全檢測技術指引 8

3.1.5、 美國國土安全部將建立國家風險管理中心 8

3.1.6、 美國國土安全部和聯邦調查局聯合發表 HIDDEN COBRA 活動惡意軟體分析報告 9

3.1.7、 CyberSecurity Malaysia 建立 CyberSAFE 計畫，提升民眾資安意識 9

3.1.8、 Magniber 勒索軟體變種，目標鎖定臺灣等多個亞洲國家 10

3.2、 駭客攻擊事件及手法 11

3.2.1、 區塊鏈眾籌平台 KickICO 發現安全漏洞，KICK 虛擬代幣遭竊 11

3.2.2、 泰國兩銀行遭受駭客攻擊，導致客戶個資外洩 14

3.2.3、 Reddit 警告其用戶存在安全漏洞，駭客駭入平台系統並存取用戶資料 14

3.2.4、 香港衛生署半月內 3 起勒索軟體感染事件，所幸資料未外洩 .. 16
3.2.5、 台積電產線遭受病毒感染 18
3.2.6、 印度浦那 Cosmos Bank 遭駭，損失金額高達 94 億盧比 20
3.2.7、 中國華住連鎖酒店集團 1.3 億客戶資料遭暗網拍賣 22
3.3、 軟硬體漏洞資訊 24
3.3.1、 惠普噴墨印表機逾百款型號具 RCE 漏洞，宜速更新韌體 24
3.3.2、 編譯器 mingw-w64 產出執行檔具先天性缺陷，不受 ASLR 機制保護 25
3.3.3、 不可盡信 WhatsApp，留心虛構人士與偽冒訊息 26
3.3.4、 升級影音軟體工具 FFmpeg 避免 DoS & RCE 27
3.3.5、 網站開發應用框架 Django，恐遭受 Open Redirect 攻擊 27
3.3.6、 松鼠郵遞 SquirrelMail 用戶，慎防來信夾帶 XSS 陷阱 28
3.3.7、 華芸科技 ASUSTOR Data Master 預設帳密及 RCE 破綻 29
3.3.8、 新型釣魚術與 login 失敗正衝擊 Office 365 30
3.3.9、 攻擊 Samba 缺陷，駭客能製造 DoS 與不當存取 31
3.3.10、 飛利浦 PageWriter 系列心電圖儀器易受本機入侵 32
3.3.11、 編譯器 Ghostscript 嚴重弱點波及多種軟體與 OS 33
3.3.12、 慎防 Man-in-the-Disk 及 Triout 侵襲 Android 設備 34
3.3.13、 儘速更新各版 OpenSSH，解除 User Enumeration 瑕疵 35
3.3.14、 急報 Windows Task Scheduler 零時漏洞，恐釀本機擴權 36
3.3.15、 網站維護者宜升級 phpMyAdmin，免除 XSS 干擾 37
3.4、 資安研討會及活動 38
第 4 章、 2018 年 08 份事件通報統計 47

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、TWCERT/CC 將於 10 月 3 日舉辦「2018 台灣資安通報應變年會-企業無可避免的資安管理責任」

TWCERT/CC 將於 10 月 3 日集思台大會議中心舉辦「2018 台灣資安通報應變年會-企業無可避免的資安管理責任」，由行政院資通安全處指導，經濟部中小企業處、國家中山科學研究院、電子商務資安服務中心 EC-CERT 及國家中山科學研究院資訊通信研究所共同協辦此場會議。

隨著網際網路與物聯網蓬勃發展，企業所面臨的資安問題亦與日俱增，資安在當今的世代已愈來愈受重視，企業在經營時，需考量完善的資安防護，制定並落實資安政策及通報應變標準作業流程，才能即時應對席捲而來的資安威脅。

因此，有許多國家及企業為了能快速應對瞬息萬變的資安事件，紛紛自主成立資安事件應變團隊 (CERTs/CSIRTs)，但事實上很多時候，在事件發生時，仍然不清楚如何處理，或無法在第一時間應急救援，而造成資安事件應變團隊並沒有完全發揮或達到預期的效益。

此次亦特別邀請到 Adli Wahid 擔任 Keynote 演講者，Wahid 先生是國際上非常知名且資深的資安專家，目前服務於亞太網路資訊中心 (Asia Pacific Network Information Centre, APNIC)，並且有許多和 CERTs/CSIRTs 及執法組織合作的經驗，亦是國際安全組織「資安事件應變小組論壇 (Forum of Incident Response and Security Teams, FIRST)」委員會成員之一。

這次 Wahid 先生將基於國際資安合作經驗，分享自身在 APNIC 及 FIRST 協助各國家建置資安事件應變團隊的經驗，以及長期設法改善整體資訊安全時，所面臨的挑戰及關注。

這是一個非常難得的機會，在台灣就能聽到國際知名資安專家 Wahid 先生的演講，此外，參與此場會議，亦可了解以下幾項課題：

(1) 面臨資安管理法的因應之道。

(2) 電子商務資訊安全的重要性及相對應的解決策略。

(3) CERT/CSIRT 任務及服務內容，並了解如何自主建置 CSIRT。

(4) 資安通報的重要性及好處，提高企業資安通報意願。

會議全程皆為免費，歡迎大家共襄盛舉！

議程資訊及報名：https://www.informationsecurity.com.tw/edm/IS_EDM_181003/

2.2、協辦 107 年度高中職資安種子教師研習營

8 月 18 日至 19 日「教育部資訊安全人才培育計畫推動辦公室」，及「財團法人國家實驗研究院國家高速網路與計算中心」，共同主辦「107 年度高中職資安種子教師研習營」，此次研習營目的主要是協助培訓資安種子師資，促進資安扎根教育，TWCERT/CC 亦為此次研習營之協辦單位。8 月 19 日 TWCERT/CC 主任陳永佳受邀擔任講師，講題為：「網路安全威脅趨勢與實務案例分享」，針對近期或較常發生的資安事件進行案例探討與分享。

2.3、協辦 2018 神盾盃網路奪旗 CTF 競賽

國家中山科學研究院辦理「2018 神盾盃網路奪旗『CTF』競賽」，TWCERT/CC 協辦此場競賽，於 8 月 29 日上午 9 時假集思台大會議中心舉行頒獎典禮，由本院院長呆中興博士主持，除公開表揚「217」及「Taipei-Meow」等獲獎團隊外，同時也邀請國防大學理工學院陸儀斌教授以「網路奪旗競賽對國內資安發展之影響」為題進行講演，闡述資安產業發展之重要性。

神盾盃 CTF 競賽題型區分為「逆向工程」、「電腦鑑識」、「弱點分析」、「網頁安全」、「密碼學應用」及「其他類型」，此次競賽最終由國內外常勝軍「217」取得第一名，獲得新台幣 10 萬元獎金。

資訊與網路安全近年來已成為熱門議題，各國競相籌辦「網路奪旗競賽」，中科院自 105 年起，透過每年舉辦「神盾盃網路奪旗競賽」，發掘國內優秀資安人才，建立多方面的交流管道，以加速國內資安技術發展與突破，更希望藉此結合民間產業的力量，一同建構完整的國家資安防護體系。

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、經濟部工業局提供資訊安全檢測診斷服務補助申請

為協助產業資安防護能力提升，由經濟部工業局主辦、工業技術研究院協辦及中華民國資訊軟體協會執行，於 107 年「新興資安產業生態系推動計畫」，推動產業資訊安全檢測診斷服務，透過「資訊安全風險現況評估」，實施「伺服主機弱點掃描檢測」、「資訊設備組態基準檢測」及「網路封包側錄分析」檢測作業，以利受測企業掌握該組織之資安防護現況，並了解如何強化、改善及建立預防措施。

申請受測企業須為依我國公司法設立，並由中央主管機關核准登記之本國公司，並屬資通訊製造、雲端物聯網、金融服務及中小企業等營運項目者，而資訊安全檢測診斷服務費用由經濟部工業局部分補助，受測企業須交付自籌款。詳細申請規定請參考「經濟部工業局 107 年「新興資安產業生態系推動計畫」資訊安全檢測診斷服務申請須知」(下載連結：http://www.cisanet.org.tw/ReadFile/?p=Activity&n=e470e709-3ff6-41b3-8eea-f022528ad9ed.pdf)

資料來源：

http://www.cisanet.org.tw/News/activity_more?id=Mzgz

https://buzzorange.com/techorange/2018/08/23/cisa-08/

http://www.cisanet.org.tw/ReadFile/?p=Activity&n=e470e709-3ff6-41b3-8eea-f022528ad9ed.pdf

3.1.2、西澳政府進行內部稽核，發現弱密碼問題仍嚴重

西澳政府對內部進行稽核，發現仍有大量員工在系統中使用弱密碼，且有些弱密碼可以管理者權限存取含有重要資訊之系統，其中亦包含可由公開線上存取之系統。未確實施行組織內資安政策，或無良善管理機制，皆可能導致資安風險。

TWCERT/CC 建議，此些風險並非僅有政府機關需注意，一般企業應該也需注意，並定期稽核資安相關政策是否確實施行，以免企業遭駭或重要機敏資訊外洩。

No.	Password used	Accounts
1	Password123	1,464
2	Project10	994
3	support	866
4	password1	813
5	October2017	226
6	Monday01	225
7	Spring17	198
8	Sunday01	188
9	password	184
10	abcd1234	176

No.	Password used	Accounts
11	Spring2017	155
12	password2	142
13	August2017	141
14	sunday1	132
15	Welcome1	132
16	Password01	118
17	Summer01	102
18	Logitech1	98
19	support1	96
20	Summer17	96

Source: OAG

資料來源：

https://audit.wa.gov.au/wp-content/uploads/2018/08/report2018_14-IS-GCC-App-Pass.pdf

https://www.washingtonpost.com/technology/2018/08/22/western-australian-government-officials-used-password-their-password-cool-cool/?noredirect=on&utm_term=.0194266293c3

3.1.3、觀光業遭殭屍網路攻擊比例上升，身分資料被竊風險提高

近期研究指出，觀光產業是目前最容易遭受網路攻擊的產業。這項研究分析從 2017 年 11 月到 2018 年 8 月的紀錄，並發現惡意假帳號透過傀儡殭屍網路攻擊飯店、航空公司、郵輪及旅行社的比例在部分國家有上升的趨勢。

資料來源：

https://blog.trendmicro.com.tw/?p=55990#more-55990

3.1.4、NCC 將公布物聯網資通安全檢測技術指引

因應物聯網帶來的資安挑戰，國家通訊傳播委員會參考國內、外相關資安防護指引及標準，將陸續制定公布無線 IP CAM、Wi-Fi AP、無線路由器等資通安全檢測技術指引，經由物聯網設備資安檢測之推廣，逐步健全我國資通安全環境，並促進物聯網各項創新應用服務之發展。

國家通訊傳播委員會
NATIONAL COMMUNICATIONS COMMISSION

資料來源：
https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&is_history=0&pages=0&sn_f=40217

3.1.5、美國國土安全部將建立國家風險管理中心

美國國土安全部 (Department of Homeland Security, DHS)在 7 月 31 日公布將建立一國家風險管理中心 (National Risk Management Center)，該中心為跨部門中心，以入口網站方式提供全方面資安資源，以協助私人關鍵基礎設施公司評估自身資安威脅及風險，以進行管理及減緩資安風險。

資料來源：

https://www.cyberscoop.com/dhs-risk-management-center/

https://www.darkreading.com/attacks-breaches/dhs-establishes-center-for-defense-of-critical-infrastructure-/d/d-id/1332442

https://www.securityweek.com/dhs-unveils-national-risk-management-center

3.1.6、美國國土安全部和聯邦調查局聯合發表 HIDDEN COBRA 活動惡意軟體分析報告

美國國土安全部 (DHS)和聯邦調查局 (FBI)發布朝鮮政府惡意軟體分析報告 (MAR)，確定了朝鮮政府使用的木馬惡意軟體變種 - 簡稱為 KEYMARBLE。此分析報告內容包括惡意軟體描述、應變作業和緩解技術的建議。企業組織或個人之用戶或管理員應注意與惡意軟體相關的活動並回報 TWCERT/CC 處置。

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

資料來源：

https://www.us-cert.gov/ncas/analysis-reports/AR18-221A

https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity

https://www.us-cert.gov/sites/default/files/publications/MAR-10135536.r17.v1.WHITE_stix.xml

3.1.7、CyberSecurity Malaysia 建立 CyberSAFE 計畫，提升民眾資安意識

馬來西亞網路安全機構 (CyberSecurity Malaysia, CSM)致力於提供廣泛的網路安全創新導引服務，以降低資訊系統的脆弱性，這有助於馬來西亞成為第三個致力於網路安全的國家。

CSM 提出 CyberSAFE 計畫，目的在提升人們對互聯網所面臨的

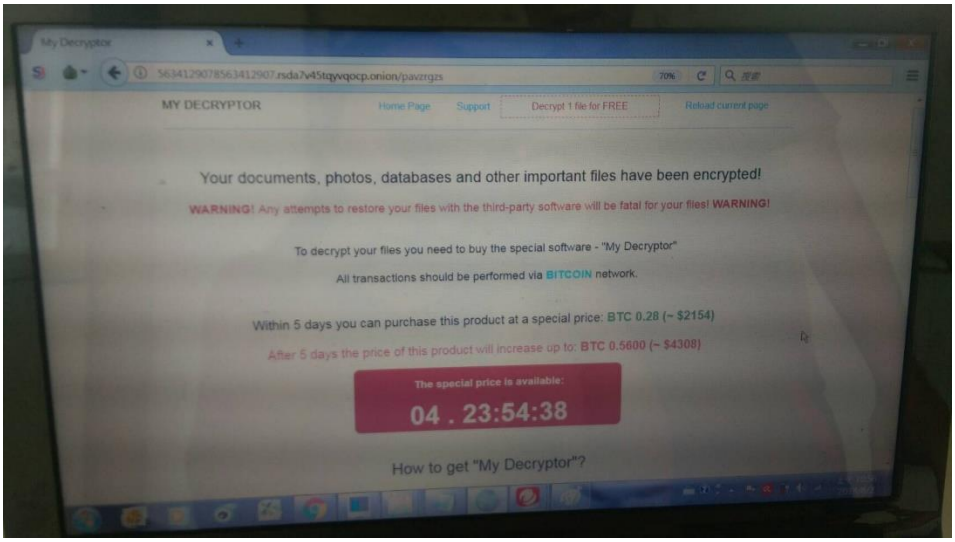
技術問題的敏感度，計畫實施對象包括學童、成人、在職成人甚至教師。該計畫取得了令人矚目的成功率，特別是教導最容易遭受網路攻擊的兒童，亦開設了相關課程來教育孩子和他們的學校老師，以確保他們不僅知道網路攻擊是什麼，也知道如何應對，而截至目前已經超過 230,100 名學生參加了 CyberSAFE 計畫。

由於 CyberSAFE 計畫是一項保護數位公民免受網路攻擊的預防措施，因此它必須具有趣味性和吸引力，以便人們持續傳授資訊安全認知，因此，CSM 正致力於達成此計畫效率，並繼續尋找使該計畫更加全面安全的方法，並以多種不同的方式進行，透過許多不同的平台來引發興趣並使其更具吸引力。

資料來源：
https://www.opengovasia.com/articles/cybersecurity-malaysias-astounding-achievements

3.1.8、Magniber 勒索軟體變種，目標鎖定臺灣等多個亞洲國家

勒索軟體爆發出來的事件與病毒種類不勝枚舉，TWCERT/CC 於 8 月獲報國內某單位遭「Magniber」勒索軟體攻擊，Magniber 通常使用漏洞利用工具 Magnitude，利用時下最新的軟體漏洞，如 Internet Explorer 中的 CVE-2016-0189 漏洞，各單位或個人應多加防範。



資料來源：

http://wubingdu.cn/magniber-%E5%8B%92%E7%B4%A2%E7%97%85%E6%AF%92/

https://www.ithome.com.tw/news/124669

https://www.ithome.com.tw/news/121296

https://www.ithome.com.tw/news/124904

https://www.ithome.com.tw/news/124747

https://www.ithome.com.tw/tech/119812

https://www.ithome.com.tw/voice/119800

https://www.informationsecurity.com.tw/article/article_detail.aspx?tv=13&aid=8479

3.2、駭客攻擊事件及手法

3.2.1、區塊鏈眾籌平台 KickICO 發現安全漏洞，KICK 虛擬代幣遭竊

KickICO 是一個基於以太坊區塊鏈的資金募集平台，7 月 29 日 KickICO 披露了一項安全漏洞，根據 KickICO 的官方公告，KickICO 遭黑客入侵存取其錢包並竊取超過 7000 萬 KICK 虛擬代幣 (Token)，換算約為 770 萬美元。

事件發生在 7 月 26 日，KickICO 執行長 Anti Danilevski 表示，

在接獲幾名受害者的投訴他們的錢包帳戶裡價值 80 萬美元的代幣不明原因消失後，該團隊隨即發現其安全漏洞，會導致攻擊者獲得 KICK 智慧合約 (Smart Contract)帳戶，從而控制 KickICO 代幣平台。

截至 7 月 29 日，該公司宣布災情得到控制，智慧合約已經恢復。KickICO 宣布將把所有被盜的 KICK 代幣歸還給他們的合法所有者，因此，受影響的用戶被要求發送電子郵件到 report@kickico.com，「以便將資金返還給錢包帳戶」。

該公司迅速開始對安全漏洞進行調查，內部員工發現攻擊者設法存取開發人員用來管理 KICK 虛擬代幣的智慧合約在 KickICO 平台的私鑰。

一旦獲得密鑰，攻擊者能夠透過存取控制 KickCoin 智慧合約的私鑰來進行攻擊，使用 KickCoin 智慧合約與 Bancor 網路整合的方法破壞了大約 40 個地址的代幣，並在相應數量的其他 40 個地址創建代幣，因此，KickCoins 的總數未受影響。

幸運的是，社群很快發現了安全漏洞並幫助平台緩解了這一漏洞。KickICO 透過將另一個離線儲存（或稱冷儲存, Cold Storage）的相關私鑰替換遭駭的私鑰，迅速做出反應並防止了進一步的損失。

曲速未來實驗室認為，目前市面上大部分的以太坊智慧合約，大多設立 Owner 特權角色。即使一份智慧合約沒有程式碼上的缺陷，也會有很大的風險，稱之為「單點威脅」，因為 Owner 特權角色在一定程度上可以影響該智慧合約的執行秩序，而並不能保證 Owner 自己不作惡又或是 Owner 特權不會被攻擊者竊取，而這次的 KickICO 盜幣事件就是由於 Owner 私鑰被竊取導致。

曲速未來實驗室表示，雖然 KickICO 重新控制了智慧合約，並且保證所有被盜的資金都將歸還到原錢包帳戶中。但目前大部分智慧合

約設立特權角色，雖然說從業務角度來說是可以理解的，但是這是與區塊鏈的核心思想相悖的，區塊鏈去中心化的目的之一就是消除單點威脅，而設立特權角色實際上是製造單點威脅。

曲速未來實驗室建議，面對「假去中心化」的專案，投資人需要謹慎以及提高警惕，因為特權帳戶隨時可能會監守自盜亦或是特權帳戶被竊取而產生大量經濟損失。

資料來源：

https://securityaffairs.co/wordpress/74910/hacking/kickico-hack.html

https://medium.com/@kickico/kickico-security-breach-issue-under-control-all-kickcoins-will-be-returned-ebe65a491dec

https://cryptovest.com/news/kickico-suffered-77m-hack-attack-says-will-return-stolen-kicko-tokens/

https://read01.com/ePG4407.html#.W2D_OqSFOUk

https://itw01.com/QVDXGEF.html

3.2.2、泰國兩銀行遭受駭客攻擊，導致客戶個資外洩

泰國開泰銀行 (Kasikorn Bank)及泰京銀行 (Krung Thai Bank)近日表示他們的系統遭駭，導致客戶資料外洩，但目前並無發現金錢損失。

泰京銀行線上貸款平台於 8 月遭駭，導致有將近 12 萬使用者的個資外洩，但並無導致金錢損失。

開泰銀行則在 7 月 25 日遭受攻擊，並導致有 3,000 名使用保函(Letter of Guarantee, L/G)服務的企業用戶資料疑似外洩，其中包含姓名及電話，但不含金融資訊，而銀行也立即加強資料防護。

泰國銀行要求該兩間銀行應加強資安作為，且須為之後客戶的可能損失做好賠償準備。

資料來源：

https://www.reuters.com/article/us-krung-thai-bank-cyber/krung-thai-bank-kbank-increase-protective-measures-after-data-hack-idUSKBN1KL1RK

http://www.nationmultimedia.com/detail/Corporate/30351170

3.2.3、Reddit 警告其用戶存在安全漏洞，駭客駭入平台系統並存取用戶資料

Reddit 是一個娛樂、社交及新聞網站，註冊用戶可以將文字或

連結在網站上發布，基本上成為一個電子布告欄系統，目前是美國最大討論區，匯聚各國眾多鄉民的關注而成為重點情報聚集地，素有美國版 PTT 之稱。

2018 年 6 月 19 日 Reddit 發現資料洩露事件，根據 Reddit 的說法，在 2018 年 6 月 14 日至 18 日期間，駭客駭入 Reddit 的一些系統並設法存取了一些用戶資料、電子郵件地址和包含由平台管理的 Hash 密碼的 2007 年備份資料庫，攻擊者在公司雲和程式碼託管供應商中獲取了部分員工的帳戶。Reddit 表示對於包含備份資料、程式碼和其他日誌的 Reddit 系統，駭客並沒有獲得其寫入權限。

該公司表示擁有身分驗證要求雙因素身分驗證 (2FA)的機制，而 Reddit 帳戶雖受到基於 SMS 的雙因素身分驗證的保護，但這種情況也表明攻擊者可以攔截透過 SMS 發送的身分驗證代碼，Reddit 了解到基於 SMS 的身分驗證並不像期望的那樣安全，並且主要攻擊是透過 SMS 攔截。因此 Reddit 鼓勵應轉移到基於 token 的 2FA。

該公司已經向執法機構報告了安全漏洞，並通知受影響的人要求更改密碼，並採取措施鎖定和替換所有加密產生和 API 密鑰，以加強系統監控。

●TWCERT/CC 建議，自 2007 年以來仍在使用相同密碼的 Reddit 用戶必須立即更改其密碼，且若在其他網路服務使用相同登入帳密者也需一併修改。

資料來源： https://securityaffairs.co/wordpress/74982/data-

breach/reddit-data-breach.html
https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/
https://www.bleepingcomputer.com/news/security/reddit-announces-security-breach-after-hackers-bypassed-staffs-2fa/
https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/
https://www.csoonline.com/article/3293904/cloud-security/reddit-discloses-hack-says-sms-intercept-allowed-attackers-to-skirt-2fa-protections.html
https://www.cyberscoop.com/user-data-private-messages-exposed-reddit-breach/
https://www.darkreading.com/threat-intelligence/reddit-warns-users-of-data-breach/d/d-id/1332458
https://www.reuters.com/article/us-reddit-cyber/reddit-says-user-data-between-2005-and-2007-breached-idUSKBN1KM5WG?feedType=RSS&feedName=technologyNews
https://securityaffairs.co/wordpress/74982/data-breach/reddit-data-breach.html
https://www.theregister.co.uk/2018/08/01/reddit_hacked_sms_2fa/
https://www.tripwire.com/state-of-security/latest-security-news/reddit-says-some-user-data-accessed-in-security-incident
https://krebsonsecurity.com/2018/08/reddit-breach-highlights-limits-of-sms-based-authentication/

3.2.4、香港衞生署半月內 3 起勒索軟體感染事件，所幸資料未外洩

香港衞生署於 8 月 2 日證實過去約半個月內接連發生 3 宗電腦感染勒索軟體事件。

警方網路安全及科技罪案調查科正跟進調查衞生署轄下 3 個單位的電腦，警方表示分別於 7 月 16 日及 25 日接獲相關政府部門報案，暫時未有人被捕。

衞生署表示，轄下感染控制處、醫學遺傳服務及藥物辦公室，於7月15日起先後報告，部門共3台電腦被勒索軟體感染，署方已經匯報政府資訊保安事故應變辦事處，並向警方網路安全及科技罪案調查科報案，初步顯示受感染電腦無儲存機密個人資料或被駭客直接入侵，事件亦無引致資料外洩。

衞生署說，勒索軟體將電腦檔案加密，只留下聯絡電郵以取得解密鑰匙，但未提出勒索金額。香港衞生署並強調，該署平日有根據政府資訊科技總監辦公室提出的防禦勒索軟體建議，定期為電腦內的檔案作出備份，員工可從備份中取回檔案。署方也已提醒包括外判電腦服務供應商在內的所有員工，必須嚴格遵守資訊保安政策及指引，不應瀏覽不安全網站，或將未經電腦病毒掃描的隨身碟，連接署方電腦。

資料來源：

https://www.scmp.com/news/hong-kong/hong-kong-law-and-crime/article/2158023/after-singapore-medical-data-hack-hong-kongs

https://hk.news.appledaily.com/local/realtime/article/20180802/58513838

http://paper.wenweipo.com/2018/08/03/HK1808030017.htm

3.2.5、台積電產線遭受病毒感染

台灣知名積體電路製造龍頭 - 台積電，8 月 5 日發布聲明，表示該公司內部遭受病毒感染攻擊，並擴散至其他廠區產線。

台積電表示事件發生在 8 月 3 日傍晚受到電腦病毒感染，主因為新機台在安裝軟體的過程中操作失誤，因此病毒在新機台連接到公司內部電腦網路時發生病毒擴散的情況。

受影響範圍為台灣廠區部分電腦系統及廠房機台，受病毒感染的程度因工廠而異，台積電表示已經控制此病毒感染範圍，同時找到解決方案，至台灣時間下午兩點為止，約 80%受影響的機台已經恢復正常，台積公司預計在 8 月 6 日前，所有受影響機台皆能夠恢復正常，公司資料的完整性和機密資訊皆未受到影響，並已採取措施彌補此安全問題，同時將進一步加強資訊安全措施。

台積電向多數客戶通知相關事件，並個別溝通其晶圓交貨時程與細部資訊。並預估此次病毒感染事件確實將導致晶圓出貨延遲以及成本增加。

台積電於 8 月 6 日傍晚召開記者會，摘錄重點如下：

1. 目前確認感染之病毒為 WannaCry 變種，而此次受到影響之機台皆使用 Windows 7 作業系統，且未上 Patch。

2. 此次事件並非因為隨身碟造成的感染，該病毒是原本就存在於機台內，也並非人為加入所導致。

3. 感染原因為新機台在安裝軟體時，未於隔離環境先測試就接上內網。

4. 公司北、中、南生產系統網路是連接在一起的，所以竹科、中科、南科都一起受到感染，但海外廠沒有受到影響。

5. 後續台積電將於短時間內建立新機制，新機台若無安裝防護機制，內部將自動判斷並使該機台無法連上內部網路。

以下整理機台電腦常見之主要可能威脅：

· 產線大都隸屬於獨立網段，防毒軟體或作業系統更新不易

· 系統分散無法提供集中式安全管理政策

· 許多機台皆採用老舊系統

· 防毒軟體無法安裝或更新

· 作業系統漏洞微軟不再提供修補

· 隨身碟使用不慎，導致內藏病毒擴散

●TWCERT/CC 以下僅針對上述幾點可能之原因提供相關防護建議：

事前預防：

· 隨身碟由於輕便、容量大、隨插即用之功能，使其成為病毒傳播與侵犯的溫床。

企業如非使用隨身碟之必要，應實體與軟體方面封鎖關閉各電腦 USB 埠，並澈底嚴格管制隨身碟攜出入。

若有使用隨身碟之必要，應配發公司內部專用合法的隨身碟，才可以進行 USB 存取，並在隨身碟插入電腦前，應確認電腦是否安裝防毒軟體、病毒碼是否更新，以及作業系統漏洞是否修補，以確保使用環境的安全性；插入電腦後應隨即對隨身碟進行病毒掃描，以避免病毒於電腦間進行交叉感染。

· 平常應定時備份，並儲存於多個不同空間。

· 關閉作業系統中不須使用之通訊埠，關閉網路共用資料夾。

· 不要點擊來路不明的網站和檔案等。

· 隨時更新作業系統或軟體以修補已知漏洞。

· 利用白名單或帳號控管等權限限制以控制可存取名單。

事中處理：

若電腦出現疑似中毒異狀，如桌面檔案出現異常無法打開等，即刻拔除電源或關機 (使用筆電者請亦將筆電電池移除)，並確認電腦無

法連上網路，使用有線網路者拔除網路線，使用無線網路者亦須確保無法連上網路（例如關閉 Wifi 分享器電源或拔除 3/4G 無線網卡）。

事後處置：

· 系統恢復：將受駭電腦硬碟格式化後重灌至最新版官方作業系統。

· 資料恢復：將備份之資料還原至電腦中。

資料來源：

https://www.bleepingcomputer.com/news/security/hackers-exploiting-dlink-routers-to-redirect-users-to-fake-brazilian-banks/

https://blog.radware.com/security/2018/08/iot-hackers-trick-brazilian-bank-customers/

http://www.whatsmydnsserver.com/

3.2.6、印度浦那 Cosmos Bank 遭駭，損失金額高達 94 億盧比

總部位於印度浦那地區的該國第二大合作銀行 (Cosmos Cooperative Bank)成立於 1906 年，是該城市歷史最悠久的城市合作銀行之一，該銀行在印度國內的 7 個州有 140 個服務據點，實力雄厚業務廣泛。

據印度斯坦時報 8 月 14 日消息，該銀行伺服器曾在印度當地時

間 8 月 11 日和 13 日遭到駭客攻擊，幾小時內約有 9.4 億盧比（約台幣 4 億 1241 萬元）的資金被盜、數千名持卡人資訊洩露。

在 8 月 11 日下午 3 點到 10 點之間，身分不明的駭客共發起了超過 15000 次交易。其中有 8 億多盧比（約台幣 3 億 5000 萬元）透過 VISA 系統，分 14849 次轉入到國外銀行的簽帳卡中。

就在當地時間 8 月 13 日晚間 11 點 30 分，駭客又一次攻擊了該銀行，這次攻擊中駭客轉移走了至少 1.4 億盧比(約台幣 6142 萬元)。根據一位銀行官員的說法，初步調查顯示駭客活動似乎來自加拿大。這些被盜資金在全球 28 個國家的 ATM 中被提走，而這些交易都是用假簽帳卡進行的，其中 12,000 筆交易發生在印度國外。

對此該銀行已經對這名尚未查明的駭客和幾個涉案公司提起了訴訟。其中提到此次攻擊是針對 ATM 伺服器，這些伺服器都位於海外，也就是資金流入的地區。

合作銀行董事 Krishnakumar Goyal 表示，駭客為印度國家支付公司 (NPCI)系統設計了一個「並行系統」並自行批准了這些交易。也正因如此駭客可以獲得銀行系統許可，從而繞過嚴格的網路安全措施盜走巨額資金。

該銀行已關閉該伺服器，並對其線上銀行交易設置限制機制。警方宣稱此案還在繼續調查之中。Cosmos Bank 稱客戶的資金是安全的，並未受到波及。

巧合的是，美國聯邦調查局才在 8 月 10 日發出警告，稱駭客可能利用一種惡意軟體操控 ATM，進而提取大量現金，引發全球 ATM 系統的危機，但目前尚未能得知此次印度銀行資金被盜，與這類軟體是否有關係。

資料來源：

https://timesofindia.indiatimes.com/business/india-business/pune-based-cosmos-bank-loses-rs-94-crore-in-cyber-hack/articleshow/65399204.cms

http://www.dnaindia.com/india/report-hackers-swindle-rs-94-crore-from-pune-s-cosmos-bank-2649650

https://www.finextra.com/newsarticle/32520/indias-cosmos-bank-falls-victim-to-global-atm-cash-out-fraud

https://new.qq.com/omn/20180815/20180815A01SD3.html

https://krebsonsecurity.com/2018/08/fbi-warns-of-unlimited-atm-cashout-blitz/

3.2.7、中國華住連鎖酒店集團 1.3 億客戶資料遭暗網拍賣

中國最大的連鎖酒店之一華住酒店集團有限公司在中國 1,119 個城市的 5,162 家酒店中經營 13 個酒店品牌。

幾家網路安全公司在中國暗網論壇發現一名駭客以 8 個比特幣（56,000 美元）的價格出售超過 1.3 億筆酒店客人的個人詳細資訊。

根據駭客線上發布的描述，他從華住酒店公司盜取的資料量為 141.5GB，包含 2.4 億筆訂房紀錄，其中包括大約 1.3 億筆是入住客人的登記資訊。

被線上銷售的資料包含官方網站註冊資訊 (身分證號碼、手機號碼、電子郵件地址、登錄密碼)、登記入住資訊 (客戶姓名、身分證號碼、家庭住址、生日) 及訂房資訊 (姓名、卡號、手機號碼、入住時間、退房時間、酒店 ID 號碼、房間號碼)。

涉及酒店包括漢庭酒店、美爵、禧玥、諾富特、美居、CitiGO、桔子、全季、星程、宜必思尚品、宜必思、怡萊及海友。

華住連鎖酒店在中國社交網路微博上發表聲明表示，仍在調查情況，並已通知當局。

中國網路安全公司紫豹告訴當地一家新聞媒體，他們表示已驗證這些資料是真實的。該公司亦表示，這次的原因似乎是華住開發團隊在 GitHub 帳戶上傳資料庫的副本所致。

資料來源：

https://www.bleepingcomputer.com/news/security/data-of-130-million-chinese-hotel-chain-guests-sold-on-dark-web-forum/

http://www.epochtimes.com/b5/18/8/28/n10673338.htm

https://china.hket.com/article/2148659/%E8%8F%AF%E4%BD%8F%E6%97%97%E4%B8%8B%E9%85%92%E5%BA%97%E4%BD%8F%E5%AE%A2%E8%B3%87%E6%96%99%E7%96%91%E5%A4%96%E6%B4%A9%20%E6%B6%891.3%E5%84%84%E4%BA%BA%E7%A7%81%E9%9A%B1

3.3、軟硬體漏洞資訊

3.3.1、惠普噴墨印表機逾百款型號具 RCE 漏洞，宜速更新韌體

3C 大廠美國惠普 (Hewlett-Packard Company)，自從印表機產品弱點抓漏獎勵專案啟動後，徵求白帽駭客為其測試商品，近日獲致成效，HP 公開 2 項韌體瑕疵，CVSS 3.0 計分高達 9.8，具高度危險性，影響 166 種噴墨印表機型號，涵蓋旗下 PageWide、DesignJet、Officejet、Deskjet、Envy 及 Photosmart 六系列，若駭客成功探勘，可輸入特製檔案，觸發 Buffer Overflow，再擴權後執行任意程式碼，對設備危害頗鉅，目前尚無入侵案例，惠普已公告相關韌體更新版本，使用者應儘快安裝，此事件儼然對企業形成新挑戰，畢竟資安長通常不參與會商印表機購案，未來導入新設備可能會經歷更嚴謹的審查。

資料來源：

https://sensorstechforum.com/cve-2018-5924-hp-printers-firmware/

https://support.hp.com/us-en/document/c06097712

3.3.2、編譯器 mingw-w64 產出執行檔具先天性缺陷，不受 ASLR 機制保護

據美國 CERT/CC 官方研究指出，因 mingw-w64 編譯器預設不產生重定位表 (Relocations Table)，而 Relocations Table 恰巧是結合位址空間隨機化配置 (ASLR)之必要條件，故近五年內以 mingw-w64 製造之執行檔，載入到記憶體後，無法重新標定在記憶體內正確新址，亦失去 ASLR 保護作用，無法阻撓駭客預測記憶體位址，顯露出緩衝區溢位弱點，面對攻擊者實施返回導向設計 (Return-Oriented Programming, ROP)，此種進階堆疊溢位攻擊，能控制堆疊呼叫以劫持程式控制流程，並執行機器語言指令。權宜之計就是開發中程式，以主程式前加底線方式 (例：__declspec (dllexport))，強制產生檔案包含 Relocations Table，然對於已運用軟體成品，目前暫無解決方案，已確認受該漏洞影響之環境為 Arch Linux、CentOS、Debian GNU/Linux、Fedora Project、Gentoo Linux、Red Hat, Inc.、SUSE Linux、Ubuntu 及 VideoLAN，上述作業系統皆完成更新。

資料來源：

https://www.zdnet.com/article/windows-apps-made-on-linux-hit-by-security-fail/

https://www.kb.cert.org/vuls/id/307144

3.3.3、不可盡信 WhatsApp，留心虛構人士與偽冒訊息

WhatsApp Messenger 目前在全球約 15 億用戶，每日多達 650 億訊息量，使用 Protobuf2 協定進行點對點加密，能在智慧型手機跨平台傳送簡訊、檔案、圖片、影音，經以色列 Check Point 軟體技術公司研究指出其程式瑕疵，因 WhatsApp 產生 QR code 前會先製作公、私對鑰，攻擊者運用 Burp Suite 等工具，修改特定參數，可發動三類攻擊模式：一是模擬真實群組成員，甚至創建不存在的身分，搭配假訊息，引述轉發給他人誤導大眾；二是寄出文字給自己，攔截加密流量後，解密並竄改，最後接收狀態呈現出某人所發消息，實際上是駭客自導自演；三是變更 msgstore.db 資料庫，刻意在群組內發送私訊給受害者，只有受害者得見，其餘人皆無法接收，造成訊息落差；上述手法皆可能引發群體對立糾紛。

對此 Facebook 聲明，WhatsApp 基本功能為點對點加密傳輸，上述弱點不妨礙運作，所涉攻擊手法屬個案，且用戶訊息均未存於 WhatsApp 伺服器中，故此時無修補計畫，依賴 WhatsApp 做日常通訊之使用者，應考慮重要資料是否更換交流管道。

資料來源：

https://www.youtube.com/watch?v=rtSFaHPA0C4&feature=youtu.be

https://research.checkpoint.com/fakesapp-a-vulnerability-in-whatsapp/

3.3.4、升級影音軟體工具 FFmpeg 避免 DoS & RCE

FFmpeg team 以 C 語言開發的 FFmpeg (Fast Forward mpeg)，是個可執行多種格式音訊、視訊錄影轉檔之自由軟體，支援各類函式庫與參數，跨 Linux、Mac OS X、Windows 環境皆適用，而部分格式轉換功能出現漏洞，無法避免惡意檔案所衍生之異常結果，如轉換成 MOV 可能引發 Divide-by-Zero 錯誤而當機；轉換 AVI 至 MPEG4 時，若變數 MQUANT 呈現負值，則陣列資料存取失誤，導致 DoS；另 Demuxer 處理 ASF 檔案影像信號，將連鎖觸發緩衝區溢位及 RCE 事件，相關瑕疵已於目前版本修補完成，且每隔一季釋出新版，升級軟體用途。

資料來源：

https://security-tracker.debian.org/tracker/CVE-2018-14395

https://nvd.nist.gov/vuln/detail/CVE-2018-13305#vulnCurrentDescriptionTitle

3.3.5、網站開發應用框架 Django，恐遭受 Open Redirect 攻擊

由 Python 寫成的 Django，是開放原始碼的網頁應用框架，採用了 MVT (Model、View、Template)軟體設計模式，其核心框架包括網頁伺服器、內建分發系統、表單序列化及驗證系統，並支援中介軟體，因為每個網站總有同質性基本需求，如：用戶註冊、後台、表

單等，憑藉 Django，開發者毋須重複製造相同模組，僅需專注設計專屬程式，經測試得知，Django 在 APPEND_SLASH 參數與 django.middleware.common.CommonMiddleware 元件同步運行時，預設作用可將 Request 內 URL 字串自動轉向末尾附加斜線號 / 之網址，攻擊者利用該普遍特性，以社交工程伎倆誘騙受害者誤點惡意鏈結，而惡意 URL 未被攔截，將導向駭客控制網站，遂行釣魚或詐騙，Django 軟體基金會已公告各版本修補檔及升級軟體。

資料來源：

https://appuals.com/django-vulnerable-to-open-redirects-in-commonmiddleware-paving-way-for-phishing-attacks/

https://www.djangoproject.com/weblog/2018/aug/01/security-releases/

3.3.6、松鼠郵遞 SquirrelMail 用戶，慎防來信夾帶 XSS 陷阱

松鼠郵遞為開源免費軟體，早期以 PHP 開發電子郵件客戶端，本身即完整郵件系統，輔以 200 餘種外掛彈性搭配，後以 C 語言設計 IMAP proxy server，兼能跨 OS 平台支援 SMTP、IMAP，因無須結合 SQL Server 且相容於主流瀏覽器、標準郵件伺服器，重視維管便利性者，易傾向安裝之，前印度總理辦公室曾因安全顧慮而淘汰

Outlook Express，替之以 SquirrelMail，如今更迭遲緩而光輝不再。經分析指出存在多項 XSS 破綻，因 magicHTML 函數原始設計未納入 HTML 標籤語法過濾功能，遠端駭客可在郵件安排<svg>、<form action>、<math>等指令，利用表單動作屬性、可縮放向量圖屬性，實行跨站台腳本攻擊，待收件人點擊閱覽新郵件頁面，旋即在受害者瀏覽器執行惡意腳本，可能偷取 Cookie 等憑證資料，由於 SquirrelMail 遍及 50 餘種語系地區，且其財務吃緊，維護應處能力已不復存，相關弱點列為高度危險，建議使用者升級至 1.4.23-svn 版並搭配 Hanno Böck 自行編撰修補檔，或許支持者可考量替代軟體。

資料來源：

https://sourceforge.net/p/squirrelmail/bugs/2831/

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=905023

3.3.7、華芸科技 ASUSTOR Data Master 預設帳密及 RCE 破綻

華芸科技 (ASUSTOR Inc.)是華碩子公司，自有品牌 ASUSTOR 意即 ASUS Storage，研發 NAS 及相關韌、硬體、應用程式，其中 ASUSTOR Data Master (ADM)係專屬 NAS 作業系統，呈現類平板圖形化介面，經研究員 Kyle Lovett 和 Matthew Fulton 連袂分析，發覺 ADM 存在多組預設帳密 (root/admin)，駭客能直接操作 phpmyadmin、virtualbox 等網頁；另因欠缺輸入字串檢查，腳本參數被注入 OS 命令後，移至 aggrecate_js.cgi 呼叫執行；而常見的 SQL Injection，亦影響 Photo Gallery 圖庫樹狀清單介面，亦用參數

album_id 或 scope，可製造隱碼攻擊，研究者已通知華芸上揭漏洞，然未獲回應，迄今官網亦無相關處置聲明，僅釋出新版 ADM 3.1.3.RHU2 修補單項 RCE 弱點。

資料來源：

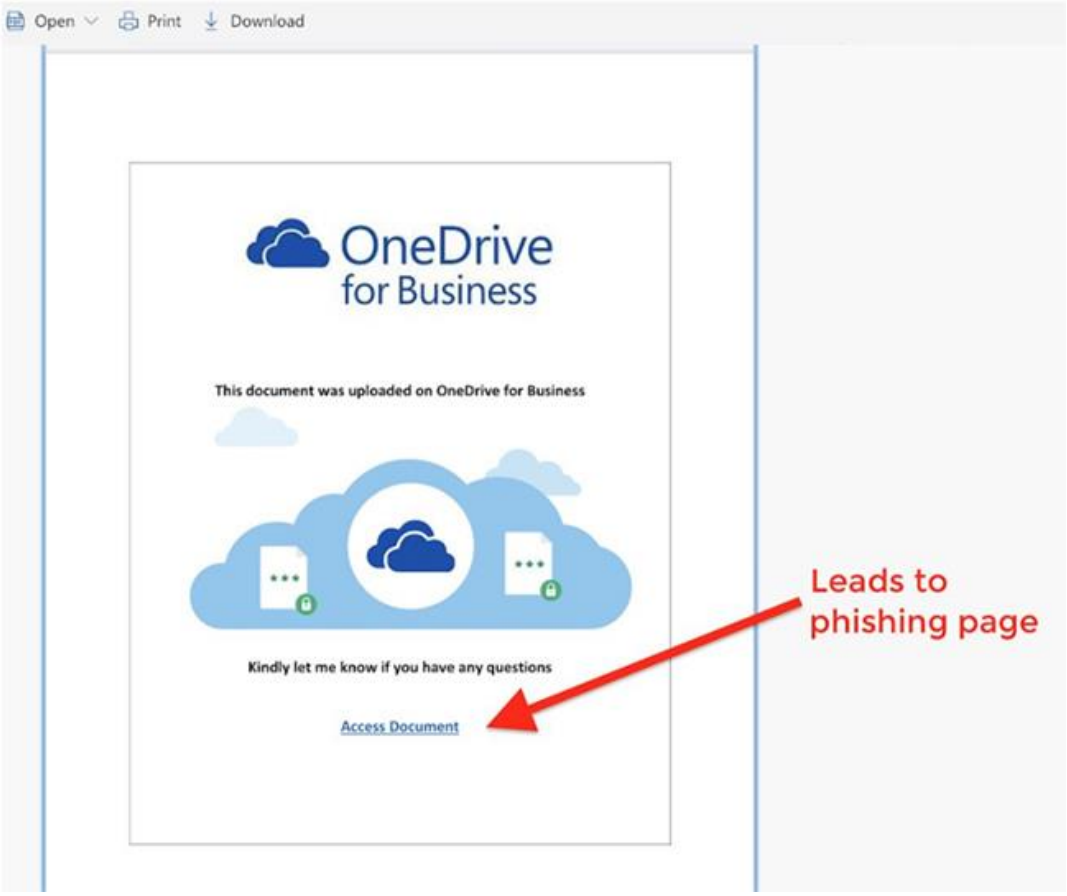
https://exploit.kitploit.com/2018/08/asustor-adm-310rfq3-remote-command.html

https://github.com/mefulton/CVE-2018-11510/blob/master/admex.py

3.3.8、新型釣魚術與 login 失敗正衝擊 Office 365

微軟主打的 Office 365，除傳統 Office 套裝以外，尚有 Exchange、SharePoint、Lync 等線上服務，並建置機器學習與 AI 安全保護，掃描電子郵件中來自惡意網域之 link，繼 5 月份 baseStriker 之後，再度陷於風險。雲端資安公司 Avanan 根據在野攻擊案例，研究新型釣魚攻擊模式，利用 Microsoft 安全機制不偵測自家商品的特性，將惡意鏈結置入 SharePoint 檔案，受害者透過 SharePoint 邀請函開啟時，導向逼真的 Office 365 登入畫面，所鍵入私人帳密直接奉送駭客。理想作法可採用 2FA 或多元認證，讓駭客手中帳密難以運用，但 Office 365 最新認證功能啟用狀態時，將導致訂購者登入錯誤，微軟

仍未解決登入問題，故眼下暫無妥善反制釣魚能力，評估過去半個月，全球約有 10% Office 365 用戶受衝擊，而目前無法有效阻擋此釣魚手段，僅得依賴人工檢測可疑之處，辨識網址真偽。



資料來源：

https://www.helpnetsecurity.com/2018/08/15/office-365-phishing-sharepoint/

https://www.bleepingcomputer.com/news/microsoft/microsoft-office-365-having-login-and-activation-issues/

3.3.9、攻擊 Samba 缺陷，駭客能製造 DoS 與不當存取

考量同網段上相異作業系統 (Windows、Linux、UNIX、IBM System 390)資源共享便利性，便催生 open-source 的 Samba，Samba 建基於 NetBIOS (Network Basic Input/Output System)通訊協定，可連接 Windows 的 SMB (Server Message Block)與 CIFS

(Common Internet File System)，讓 PC 間破除 OS 的隔閡，分享資料夾及印表機。分析指出，其 libsmbclient 函式庫未稽核目錄清單內容，極長檔名字串恐覆蓋記憶體配置區域；而 Samba 擔任 AD DC 時，因 null pointer 造成反參照錯誤，若接收惡意 RPC 請求，易導致 DRSUAPI server 內 DsCrackNames 呼叫程序或 DNS、LDAP 服務毀損;輕型目錄存取協議對於使用者控制檢查未臻完善，透過 LDAP 搜尋語法表示式，可獲得機密系統參數;另 Samba 改版時重編程式，造成較弱 NTLMv1 身分驗證方式回歸，使駭客得以避開嚴謹規範，進行未授權存取，發動進階攻擊，Samba Team 已公布修補檔，並升級相關軟體版本。

資料來源：

https://www.samba.org/samba/history/security.html

https://agenparl.eu/samba-releases-security-updates/

3.3.10、飛利浦 PageWriter 系列心電圖儀器易受本機入侵

荷蘭飛利浦 Philips 公司，通報旗下醫療產品出現錯誤，PageWriter Cardiograph 心電圖偵測儀能產生 Electrocardiography (ECG)圖表，輔助醫師診斷，此類設備涉及醫療安全，其資料處理過程不容有失，然因內建寫死 Superuser 密碼，知情者得以全面調整設備功能；另囿於記憶體邊界控管瑕疵，若本機駭客送入特製字串，可能觸發緩衝區溢位或格式化字串攻擊 (Format String Attack)，衍生越界讀寫記憶體事件；上述軟體缺陷均打破安全

藩籬，使攻擊者有權變更組態設定，影響診斷資料精密性及完整性，危及療程，弱點型號為 PageWriter TC10、TC20、TC30、TC50、TC70 Cardiograph 系列醫材，Philips 預計 2019 年夏著手更新，系統缺失修正前，宜詳加規範設備使用人，確保惡意攻擊者無法實機操作。

資料來源：

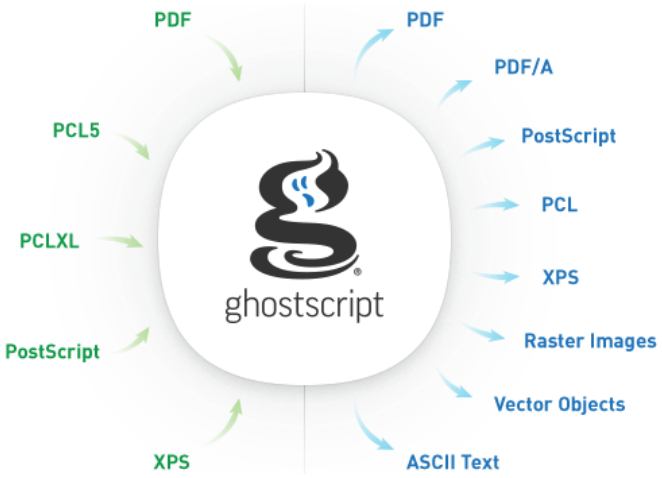
https://appuals.com/philips-to-look-into-pagewriter-cardiograph-device-vulnerabilities-mid-2019/

https://www.cybersecurity-help.cz/vdb/SB2018082016?affChecked=1

3.3.11、編譯器 Ghostscript 嚴重弱點波及多種軟體與 OS

基於 Adobe PostScript 及 PDF 的頁面描述語言需求，Artifex Software 以 C 語言開發 Ghostscript 編譯器，現今適用 Linux、Unix、mac OS X、VMS、Windows、OS/2，並被 ImageMagick、Evince、GIMP 等編輯工具納為基本功能，影響力遍及上百款套裝軟體及函式庫，經 Google Project Zero 研究員 Tavis Ormandy 長期分析，指出 Ghostscript 內建-dSAFER 選項，本是防止惡意行為的沙箱保護機制，但竟包含嚴重破綻，駭客製作各類惡意檔案 (PDF、PS、EPS、XPS)，交給 Ghostscript 解析，可能執行任意指令或造成資料類型混淆，甚至可開啟受限制檔案，於隨機目錄恣意生成檔案，鑒於

Ghostscript 應用面廣泛，其 RCE 效果危及者眾多，且官方暫無正式修補，目前權宜之計，僅能從政策參數停用相關編碼功能，避免成為入侵對象。



資料來源：

https://cxsecurity.com/issue/WLB-2018080153

https://www.bleepingcomputer.com/news/security/no-patch-available-yet-for-new-major-vulnerability-in-ghostscript-interpreter/

3.3.12、慎防 Man-in-the-Disk 及 Triout 侵襲 Android 設備

由於全球 Android 商品普及，針對性的攻擊技術與日俱增，以色列 Check Point 資安公司發現手機新弱點 Man-in-the-Disk (MitD)，因外部儲存器 (External Storage)為共享硬體資源，且不受沙箱保護，儲存資料易遭竄改，而導致 APP 觸發 DoS 或者更新流程被劫持，以惡意程式覆蓋自動更新執行檔，Google 翻譯、Google 語音助理、俄羅斯 Yandex 搜尋引擎、Yandex 翻譯、小米瀏覽器均具 MitD 漏洞。另羅馬尼亞 BitDefende 公司找出新型態間諜軟體 framework，命名 Triout，能建立強大監視力並隱藏在貌似合法的 APP 內，Triout 可蒐集電話錄音、簡訊、通聯紀錄、錄影拍照檔案、GPS 座標，送回 C&C 伺服器，惟 Triout 作者身分、散播途徑、危害次數均不詳。結合 MitD 入侵途徑與 Triout 監視技術，對設備持有者

隱私形成威脅，儘管 Google 已對旗下 APP 完成修補，而小米沒打算理會這問題，想當然耳，仍有諸多軟體難以倖免。

資料來源：

https://www.youtube.com/watch?v=M3rQ_J8rS7c&feature=youtu.be
https://labs.bitdefender.com/2018/08/triout-spyware-framework-for-android-with-extensive-surveillance-capabilities/

3.3.13、儘速更新各版 OpenSSH，解除 User Enumeration 瑕疵

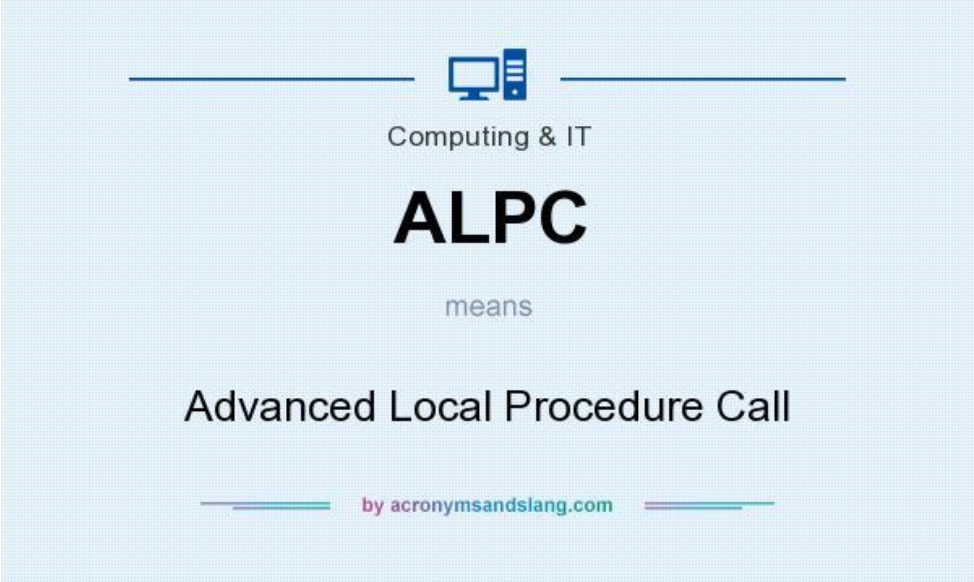
自 1999 年發展迄今的 OpenSSH (OpenBSD Secure Shell)，係開放原始碼，以 C 語言撰寫之跨平台加密通訊軟體，據 Qualys 研究員分析，得知 OpenSSH 自開創迄今，全數版本皆存在姓名列舉(User Enumeration)弱點，在 auth2-gss.c、auth2-hostbased.c、and auth2-pubkey.c 原始碼內，凡涉及 userauth_pubkey()函數區段均有設計瑕疵，故對於無效使用者登入，未待完整解析封包內所有 Request，迅速回應錯誤訊息，毫不延遲的時間差距，則透露出帳號不存在的事實，反之若使用者有效時，伺服器逕中斷與攻擊者的連線，駭客以惡意封包探勘，結合時序攻擊 (Timing Attack)與暴力破解方式，極易分別輸入帳號是否正確，從而獲得真實用戶帳號。基於 OpenSSH 廣泛運用，探勘實務亦公開披露，大量設備已受威脅，儘

管公布修補方式，且 OpenBSD 已升級至最新版，然龐大的終端修補量可能耗時數月，目前 OpenSSH 官網連線失敗，網站似遭連線超載拖垮，建議使用者近日可隨機測試是否回復營運，儘快下載新版。

資料來源：
https://blog.nviso.be/2018/08/21/openssh-user-enumeration-vulnerability-a-close-look/
https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0

3.3.14、急報 Windows Task Scheduler 零時漏洞，恐釀本機擴權

化名 SandboxEscaper 的研究員，近日在 Twitter 發布微軟既有的未知零時漏洞，經證實在 64 位元 Windows 10 及 Windows Server 2016，自動排程 Task Scheduler 運作時使用進階本地程序呼叫(Advanced Local Procedure Call)介面，以建立用戶模式下跨程序之高速資料傳送途徑，但本機駭客可對 C:\Windows\Tasks 路徑內*.job 檔案產生 Hard Link，再呼叫_SchRpcSetSecurity()函數，惡意覆寫原始 job 檔案，利用 Task Scheduler 系統權限執行週期任務時機，成為攻擊者幫兇，由於 Hard Link 效果僅限於相同硬碟分割區，故攻擊手段有所限制，但對同機多用戶仍有威脅，微軟預計 9 月份更新一併解決，眼下暫無修補。



資料來源：

https://thehackernews.com/2018/08/windows-zero-day-exploit.htm

https://twitter.com/SandboxEscaper/status/1034125195148255235

3.3.15、網站維護者宜升級 phpMyAdmin，免除 XSS 干擾

以 PHP 開發之免費軟體工具 phpMyAdmin，支援在網頁伺服器管理 MySQL 資料庫，其優勢為鉅量資料的匯入匯出，能產出 HTML 頁面俾供操作。經分析 Sql.php、import.php 程式碼察覺 XSS 破綻，因 phpMyAdmin 匯入檔案作業欠缺資料檢核機制，在惡意檔案內埋藏特殊指令 SIGNAL SQLSTATE 語法或其他腳本碼，可將攻擊型 payload 送入，輾轉經由 getWarnings()、getWarningMessagesArray()、addHTML()等函數加以運算執行，最終觸發指令生效，此類 Cross-Site Scripting 行為若結合系統級權限，恐危害網站資料庫完整性，The phpMyAdmin Project 已於 8 月 21 日完成修補並釋出升級版。

資料來源：

https://www.phpmyadmin.net/security/PMASA-2018-5/

https://blue-bird1.github.io/2018/08/25/CVE-2018-15605/

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
2018/10/03	2018 台灣資安通報應變年會-企業無可避免的資安管理責任	【資安研討會】2018 台灣資安通報應變年會-企業無可避免的資安管理責任 日期：2018 年 10 月 3 日 (三) 地點：集思台大會議中心 (台北市羅斯福路 4 段 85 號 B1) 參與對象：中小企業組織及團體 主辦單位：台灣電腦網路危機處理暨協調中心 (TWCERT/CC) 報名費用：全程免費 議程資訊及報名： https://www.informationsecurity.com.tw/edm/IS_EDM_181003/ 參與此場會議，可了解以下幾項課題： 1.面臨資安管理法之因應之道。 2.電子商務資訊安全的重要性及相對應的解決策略。 3.CERT/CSIRT 任務及服務內容，並了解如何自主建置 CSIRT。

時間	研討會/課程名稱	研討會相關資料
		4.資安通報的重要性及好處，提高企業資安通報意願。 活動概要： 隨著網際網路與物聯網蓬勃發展，不僅給人們帶來便利的生活，也衍伸出許多資安問題，例如電商業者網站資訊安全防護未完善，而造成客戶資料外洩，引發大量的詐騙事件；或讓有心人士成功入侵電商網站，修改商品價格，而造成電商業者財務重大損失等問題，然而電子商務之資安風險，不再僅僅是客戶資料外洩或財務損失，在新版個資法上線後，將可能影響企業商譽及巨額財務損失。 企業除了面臨上述的資安問題外，另外還有網路攝影機監控畫面外洩、勒索軟體攻擊事件、DDoS 攻擊事件、挖礦程式盛行等，亦是企業頻繁遭遇的資安問題，因此資安在當今的世代已愈來愈受重視，企業在經營時，需考量完善的資安防護，制定並落實資安政策及通報應變標準作業流程，才能即時應對席捲而來的資安威脅。
2018/09/15、2018/09/22	工業局補助資安課程-新興安全威脅《wifi 無線網路與物聯安全實作》	【資安訓練課程】工業局補助資安課程-新興安全威脅《wifi 無線網路與物聯安全實作》 日期：2018 年 9 月 15 日 (六)、2018 年 9 月 22 日(六) 每日 09:10 ~ 16:20 共 12 小時 活動地點：新北市板橋區民族路 168 號 主辦單位：中華電信學院 課程資訊及報名： https://www.accupass.com/event/1807250208111459278143 課程費用：付費 課程簡介： 在行動裝置普及率持續上升的狀況之下，有線網路持續遭到取代，新型態的裝置多以無線網路取代有線網路，

時間	研討會/課程名稱	研討會相關資料
		在此趨勢之下政府機關與企業也只好擁抱原本認為不夠安全的無線網路，透過了解無線網路所面臨的資安危脅，進一步強化無線網路管理的安全。另一方面，在物聯網來臨的時代，廣義上的物聯網裝置包含網路攝影機、無線基地台....等等，這些都有可能受到駭客的攻擊，過去大家只認為伺服器與電腦才會受駭的時代已經過去，如何有效解決物聯網時代面臨的威脅便是本課程最重要的目標。
2018/09/29	ISDA 教育訓練 Burpsuite 實戰百分百	【資安訓練課程】ISDA 教育訓練 Burpsuite 實戰百分百 日期：2018 年 09 月 29 日 (六) 13:00-17:30 地點：台北市中正區重慶南路一段 77 號 3-4 樓 線上報名連結： https://reg.isda.org.tw/info.php?no=36 報名費用：學生 NT$1,800、社會人士 NT$3,000 報名注意事項： 活動滿 10 人開班，確認開班後，將有專人通知付款方式，若活動當天不克前來，將無法退費，但可自行轉讓他人，以上需知無法同意者，請勿報名。 活動議程： 13:00~13:30 入場 13:30~14:30 burpsuite 只有高手們才會的技巧 14:30~15:30 如何自幹更強大的 burpsite 外掛 15:30~17:00 專業 burpsuite 技巧初體驗 17:00~17:30 FAQ 活動概要： 本次活動為「ISDA 教育訓練 - Burpsuite 實戰百分百」，適合進階學員參加。沒有最專業，只有更專業，如何更上一層樓，快來一探駭客高手們的秘密。
2018/09/19-20 2018/09/	107 年度新興資安產業生態系推動計	【資安訓練課程】107 年度新興資安產業生態系推動計畫 - 資安專業人才培育委外人才培訓 - 資安事故處理課程（第二梯）

時間	研討會/課程名稱	研討會相關資料
26-27	畫 - 資安專業人才培育委外人才培訓 - 資安事故處理課程(第二梯)	課程時間：2018 年 09 月 19 日（三） - 09 月 20 日（四）/2018 年 09 月 26 日（三） - 09 月 27 日（四） 受訓地點：臺北巨匠電腦 - 電腦教室（臺北市公園路 30 號 3 樓） 主辦單位：經濟部工業局 線上報名連結： http://www.cisanet.org.tw/News/activity_more?id=MzQ0 課程簡介： 課程設計除透過瞭解資安事故處理生命週期，藉以學習當資安事故發生時如何進行資安事故處理程序之外，並由資安事故處理以及數位鑑識處理之實務操作，讓結業學員學習到包含數位證據保全有效性之資安事故處理實務，俾利資訊安全產業與相關企業對於資安事故處理人才之運用。本課程邀請業界致力於資安事故處理與數位鑑識等專家共同指導，讓學員透過講師自身處理過的案例經驗中，了解各項資安事故發生後的處置手段，並接由數位鑑識相關專業講師教導如何保全事故後的數位跡證，透過理論與實務相輔佐的方式，讓學員能夠制定一套適用於各公司的資安事故緊急應變 SOP，往後遭遇資安事故時，便能即時應對處變，更甚而從源頭進行預防。 課程大綱： 1.資安事故處理實務 2.數位鑑識處理實務
2018/09/29	The Dungeons of Hackers Conference 2018 - 駭客的地下城	【資安研討會】The Dungeons of Hackers Conference 2018 - 駭客的地下城 日期：2018 年 09 月 29 日（六） 地點：高雄蓮潭國際會館 Gardenvilla 會議中心 2F & 3F（高雄市左營區崇德路 801 號） 主辦單位：TDOHakcer

時間	研討會/課程名稱	研討會相關資料
		線上報名連結： https://tdohackerparty.kktix.cc/events/tdoh-conf-2018 活動概要： 除邀請國內知名資安講者與優秀學生外，今年更邀請了香港與日韓之優秀講者一同共襄盛舉。本屆講者陣容包含數位國際級講者（曾於 DEFCON /Black Hat... 等國際資安研討會發表過之講者）。 傳統的邊際安全性產品不僅在 DDoS 的因應對策方面顯得相對薄弱，亦因其狀態表 (Stateful)結構而無法阻擋狀態耗盡攻擊，尤其現在直播和串流視訊或是遊戲，這些服務往往是 TCP 和 UDP 混合使用，在防護上將變得越來越有挑戰性。本工作坊將會現場架設一個測試環境，並且將防禦設備（價值 1400 萬）真實架設在前端，讓各位有機會和企業 DDoS 解決方案現場交手一番。
2018/09/29	數位鑑識概念與實作	【資安訓練課程】數位鑑識概念與實作 日期：2018 年 9 月 29 日（六） 09：30-16：30（12：30-13：30 休息） 共 6 小時 活動地點：國立交通大學 台北校區 主辦單位：亥客書院 課程資訊及報名： https://hackercollege.nctu.edu.tw/?p=594 課程費用：每人$8000 含教材。若報名人數不足，將不予開辦。多人報名或一人同時報名多門課程均有優惠，請洽「蔡小姐 (03)5731762 E-mail: wltt@nctu.edu.tw」。 課程大綱： 〇數位鑑識簡介 〇現場數位證據取證流程及工具 〇儲存媒體鑑識 〇行動裝置鑑識

時間	研討會/課程名稱	研討會相關資料
		○鑑識軟體設備 課程簡介： 本課程將包含數位鑑識簡介、現場數位證據取證種類及蒐證 SOP、現場工具介紹、Autopsy 工具介紹等實作、鑑識軟體設備等主題。
2018/10/06	流量分析	【資安訓練課程】流量分析 日期：2018 年 10 月 6 日（六）09：30-16：30（12：30-13：30 休息） 共 6 小時 活動地點：國立交通大學 台北校區 主辦單位：亥客書院 課程資訊及報名： https://hackercollege.nctu.edu.tw/?p=891 課程費用：每人$8000 含教材。若報名人數不足，將不予開辦。多人報名或一人同時報名多門課程均有優惠，請洽「蔡小姐 (03)5731762 E-mail: wltt@nctu.edu.tw」。 課程大綱： ○網路模型概論 ○DoS 攻擊技術介紹 ○流量分析工具介紹與操作 ○惡意流量分析實作 課程簡介： 網路流量攻擊為企業最常遭受到的資安威脅之一，但網路環境的複雜，使得 這類攻擊不易被偵測或阻擋，在事件發生後的分析與檢測顯得格外重要。本課程將介紹網路流量攻擊的基礎原理，並帶出對應的檢測方式及工具操作演練。
2018/10/27	惡意程式檢測實務	【資安訓練課程】惡意程式檢測實務 日期：2018 年 10 月 27 日（六）09：30-16：30（12：30-13：30 休息） 共 6 小時 活動地點：國立交通大學 台北校區 主辦單位：亥客書院

時間	研討會/課程名稱	研討會相關資料
		課程資訊及報名： https://hackercollege.nctu.edu.tw/?p=885 課程費用：每人$7000 含教材。若報名人數不足，將不予開辦。多人報名或一人同時報名多門課程均有優惠，請洽「蔡小姐 (03)5731762 E-mail: wltt@nctu.edu.tw」。 課程大綱： 〇惡意程式簡介與分類 〇惡意程式分析技術概述 〇系統鑑識工具與實做 〇逆向工程工具與實做 課程簡介： 惡意程式一向為嚴重的資安威脅，從一般的殭屍網路、勒索軟體到精密的 APT 攻擊，惡意程式都扮演重要的攻擊媒介。因此檢測系統中的惡意程式，為相當重要的資安議題。本課程從惡意程式的介紹出發，全面理解各種惡意程式的生態，再進一步探討分析惡意程式的手法。分析惡意程式的部分，先以系統鑑識的角度，說明如何用各種工具從系統中檢測出惡意程式。而後再進一步以逆向工程的方式，了解惡意程式的行為。藉此從多種不同的面相，了解惡意程式。
2018/10/27 2018/11/3	白帽菁英萌芽計畫〈入門一〉ISDA 白帽駭客巡迴(南開科技大學)	【資安訓練課程】白帽菁英萌芽計畫〈入門一〉ISDA 白帽駭客巡迴 巡迴第 7 站：南開科技大學 日期：2018 年 10 月 27 日 (六) 13:00-18:00 地點：南開科技大學 線上報名連結： https://reg.isda.org.tw/info.php?no=27 報名時間：2018 年 9 月 22 日至 10 月 22 日 ----------我是分隔線---------- 巡迴第 8 站：國立東華大學 日期：2018 年 1 1 月 3 日 (六) 13:00-18:00

時間	研討會/課程名稱	研討會相關資料
		地點：國立東華大學 線上報名連結： https://reg.isda.org.tw/info.php?no=28 報名時間：2018 年 9 月 29 日至 10 月 29 日 ----------我是分隔線---------- 報名注意事項： 活動對象為各大專院校與高中職等在學之學生，學生名額優先，學生家長與教育人士請出示證件。 活動議程： 13:00~13:30 活動簡介 13:30~14:20 WarGame#1 LV1 14:30~15:20 WarGame#1 LV2 15:30~16:20 WarGame#1 LV3 16:30~17:00 FAQ 活動概要： 只要有心，人人都可以成為白帽駭客，ISDA 團隊將帶領各位學員來挑戰極限！ 在這個萬物皆可駭的年代，該學習什麼樣的技能，與培養正確的觀念，來成為『白帽菁英』的一員。本次活動中，ISDA 的專業資安教育訓練團隊，將透過 WarGame 實作教學，傳授您擁有基本的白帽駭客技能，取得進入資安界與駭客圈的入場券。 白帽菁英萌芽計畫，將舉辦於全台灣八個縣市，落實推廣全台灣的資安教育活動。
2018/11/10-2018/11/18	認證系統安全從業人員 SSCP 輔導班	【資安訓練課程】認證系統安全從業人員 SSCP 輔導班 日期：2018 年 11 月 10 日至 11 月 18 日（假日班） 活動地點：台北市復興南路一段 390 號 2 樓 主辦單位：財團法人資訊工業策進會 數位教育研究所數位人才培育中心

時間	研討會/課程名稱	研討會相關資料
		課程資訊及報名： http://taipei.iiiedu.org.tw/course/security/187-asq902.html 課程費用：28 小時 / 40000 元，優惠價 25000 元 承辦人：羅小姐　電話：(02)66316586 E-Mail：showyann@iii.org.tw 課程簡介： 培養學員具通過 SSCP 認證考試之實力。 培養學員具實務從事資安工作之知識與能力 培養學員具備網路通訊安全、封包分析、監控與惡意程式碼防治、風險處理、災害復原等實用知識與應用

第 4 章、2018 年 08 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 8 月收到通報計 1619 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。

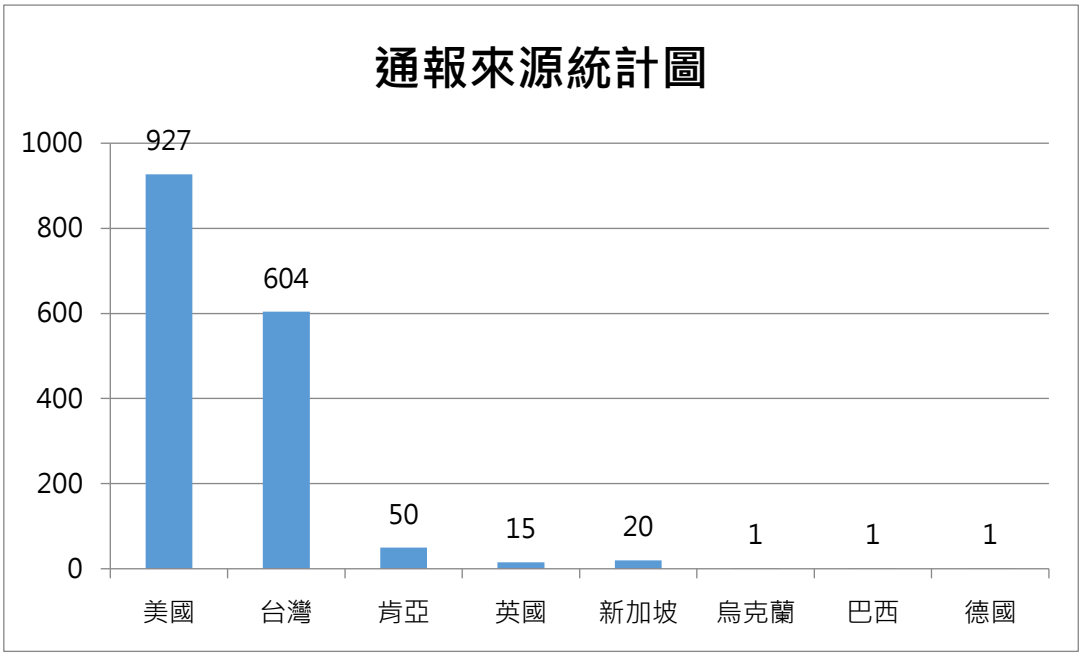


圖 1、通報來源統計圖

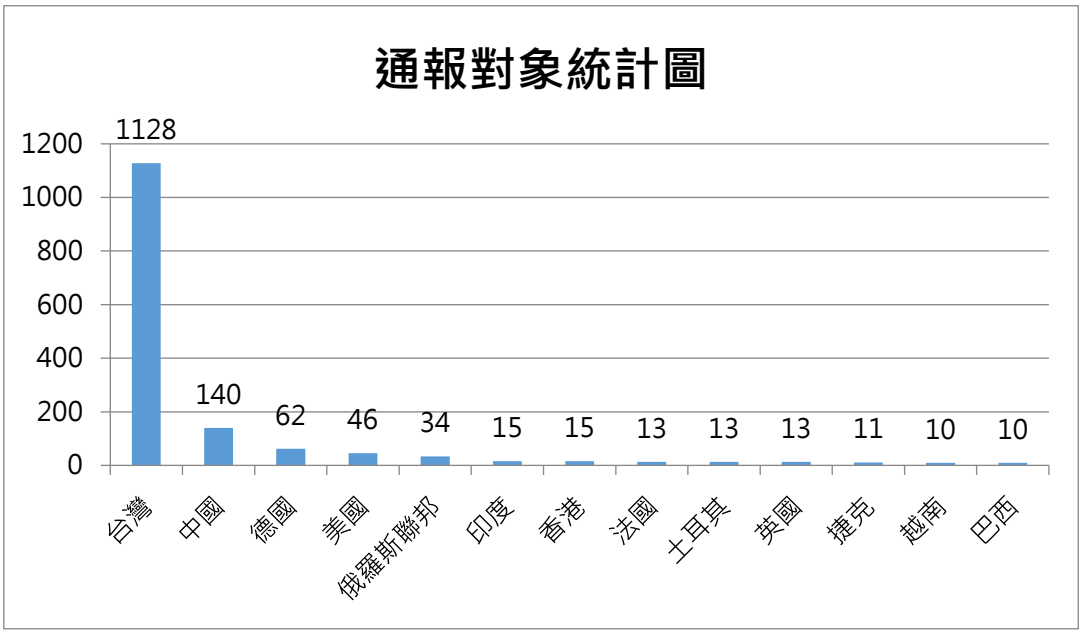


圖 2、通報對象統計圖

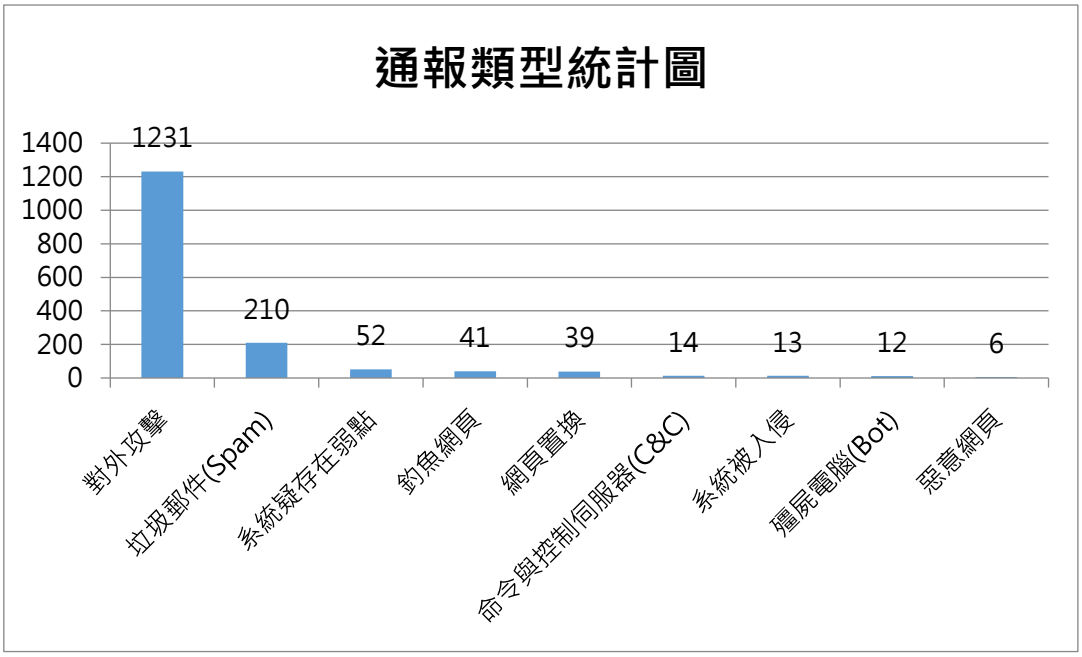


圖 3、通報類型統計圖

本月接獲國外 CERT/CC 通報案件中以疑似散布「Satori 殭屍網路 (Mirai 變種)」事件屬特殊案件。Satori 原意為日本禪宗「開悟」，然在此情境則無禪意，由於華為家庭路由器韌體設計存在弱點，駭客

可注入 shell meta 字元“$()”，構成有效之惡意 request，通過 port 37215 及 UPnP 設計所形成之漏洞，針對 HG532 觸發其更新行為，趁機引發 RCE 攻擊，目前已影響數十萬設備，儘管華為提供安全性建議，惟 Mirai 原始碼已公諸於世，仍應擔心其他變種 IoT 殭屍網路竄起。

●編註：

過往 Mirai 僵屍網路曾造成美國東部大斷網，目前出現進化變種 Okiru，亦稱 Satori，它利用新發現 Zero-Day 漏洞控制數十萬家庭路由器，據紀錄可於 12 小時內感染 20 萬以上設備，肆虐範圍涵蓋阿根廷、美、義、德、埃及、土耳其、烏克蘭、委內瑞拉和秘魯等國。

能蔓延如此神速，在於 Satori 乃針對華為 HG532 而創造，利用嵌入式漏洞，以蠕蟲形式自行傳播到開放 port 37215 之設備，至於漏洞原理，則在 HG532 之韌體設計，由於該 router 使用 TR-064 技術報告標準開發，提供通用隨插即用 (UPnP)功能，便於將嵌入式 UPnP 設備加入加到 LAN，HG532 韌體原始碼內部分指令 (/ctrlt/DeviceUpgrade_1)，支援 DeviceUpgrade 的服務類型，執行更新牽涉到二段指令，<NewStatusURL> 和 <NewDownloadURL>，後者原文為<NewDownloadURL>$(echo HUAWEIUPNP) </NewDownloadURL>，取得管理權限的駭客經由 port 37215 送出加工之 request，注入 shell meta 字元“$()”到 NewStatusURL 及 NewDownloadURL，返回預設 HUAWEIUPNP 訊息，就能在 DeviceUpgrade 程序運行中執行任意碼。

因 Mirai 原始碼早已公開，故改造 Mirai 以創建變體並非難事，況且攻擊者身分隱秘，即便 Satori 被壓制，恐仍有後續家族，繼續打

擊其他物聯網受害目標。

●解決方案：

(1)設定裝備內建防火牆功能

(2)修改預設密碼

(3)電信商部署防火牆

●參考連結：

[1] https://twcert.org.tw/subpages/securityInfo/securitypolicy_details.aspx?id=761

[2] https://twcert.org.tw/subpages/securityInfo/loophole_details.aspx?id=4848

[3] https://research.checkpoint.com/good-zero-day-skiddie/

[4] https://thehackernews.com/2017/12/satori-mirai-iot-botnet.html

[5] http://www.seckurity.com/2017/12/24/satori-iot-botnet-exploits-zero-day-to-zombify-huawei-brand-routers/

[6] http://securityaffairs.co/wordpress/67040/malware/satori-botnet-mirai-variant.html

[7] https://4.bp.blogspot.com/-Rn_wpJ8eB2M/Wj4Or4ez7sI/AAAAAAAAvUE/dgpqf5cFD8c-IIb5zpHJd3VLdlNIxCVbQCLcBGAs/s1600/Satori-Okiku-Mirai-IoT-Botnet-Malware.png

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 9 月 15 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。