TWCERT/CC 資安情資電子報

2018 年 2 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 3
第 3 章、 國內外重要資安新聞 4
3.1、 國內外資安政策、威脅與趨勢 4
3.2、 駭客攻擊事件及手法 10
3.3、 軟硬體漏洞資訊 14
3.4、 資安研討會及活動 26
第 4 章、 2018 年 2 月份事件通報統計 27

第 1 章、摘要

為提升我國民眾資安意識，TWCERT/CC 於每月發布資安情資電子報，電子報中統整上月重要資安情資，包含 TWCERT/CC 近期動態、資安政策、威脅與趨勢、駭客攻擊事件、軟硬體漏洞、資安研討會活動及資安事件通報統計分析等資訊。

TWCERT/CC 近期動態，2018 年 2 月 7 日 TWCERT/CC 副主任吳專吉於「中華民國電腦稽核協會」台北月例會分享「企業資安聯防-事件通報與情資分享」。

在資安政策方面，台灣金融資安中心揭牌為強化防護能量；金管會公開示警銀行不得買賣比特幣；WIFI 聯盟推出具有新安全功能的 WPA3 協議；美國企業則建立網路安全防護網；川普欲將 5G 網路國有化以對抗中國網路威脅，美陸戰隊也擴編「網軍」徵募駭客。資安趨勢方面，日本引進深度學習 AI，防禦網路攻擊。在資安威脅方面，殭屍網路病毒 Mirai Okiru 針對 ARC 處理器攻擊；電商網站防護鬆散，易遭駭客盜取個資。

在駭客攻擊事件方面，新型鍵盤側錄程式注入攻擊導致超過 2000 個 WordPress 網站受害；物聯網設備存在弱密碼漏洞，進而被攻擊者利用插入惡意代碼。

在軟硬體漏洞方面，Samsung 瀏覽器迴避同源政策 SOP 恐使個資遭竊；全球 CPU 面臨 Spectre 與 Meltdown 旁道分析式漏洞威脅；防火牆系統 Sonicwall 介面無法過濾特定 payload；TP-Link 證實 command injection 漏洞影響卅餘型 WIFI 路由器；Transmission BitTorrent 設計缺陷，暗渡 PC 主控權；ISC 維護 DHCP 與 BIND 防止網路連線中斷；Foxit 閱讀軟體功能瑕疵易肇生 RCE、訊息外洩；義籍駭客破解 Master IPCAM01 並取得 root 密碼；殭屍軟體 Zyklon

復出，刻正威脅微軟 Office 用戶；聯想察覺 Lenovo 及 IBM 系列交換器內 HP 後門隱藏 14 年之久；Symantec 多款產品恐洩漏 Diffie-Hellman 密鑰及避開 TLS 協定；Seagate 家用雲端裝置 Personal cloud 測出漏洞，恐遭遠距執行系統指令。

在資安研討會方面，2018 年 3 月 13 日至 15 日 iThome 於台北國際會議中心(TICC)中舉辦「2018 臺灣資安大會」。

在 2018 年 2 月事件通報統計方面，分別說明通報來源統計圖、攻擊來源統計圖及攻擊類型統計圖等統計數據，經分析後，該月以「一頁式廣告詐騙網頁」屬特殊案件。

第 2 章、TWCERT/CC 近期動態

2.1、2018 年 2 月 7 日 TWCERT/CC 副主任吳專吉於中華民國電腦稽核協會台北月例會分享「企業資安聯防-事件通報與情資分享」

2018 年 2 月 7 日 TWCERT/CC 副主任吳專吉於「中華民國電腦稽核協會」台北月例會分享「企業資安聯防-事件通報與情資分享」，分享大綱如下：

1. 企業資安危機通報站 - TWCERT/CC
2. 企業通報應變機制之建立
3. 事件應變作業與威脅分析實務

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、金管會公開示警 銀行不得買賣比特幣

金管會公開示警，「比特幣」屬於高度投機性的數位「虛擬商品」，社會大眾務必注意有關收受、交易或持有比特幣所衍生的相關風險；金管會更要求銀行，「不得參與或提供比特幣交易」。

資料來源：

http://news.ltn.com.tw/news/business/paper/1161740

3.1.2、強化防護能量，金融資安中心揭牌

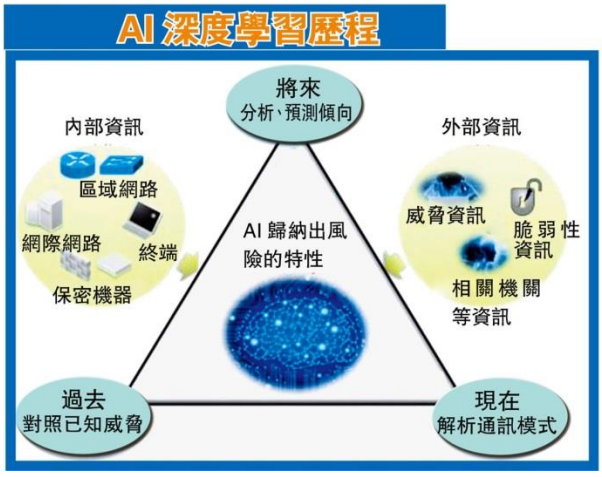
台灣第一個針對金融業所設立的金融資安資訊分享與分析中心（F-ISAC），於 2017 年 12 月 22 日正式掛牌成立，未來將協同全台超過 200 多家的銀行、保險及證券期貨等業者，共同來打造金融圈的資安情資聯防網路。

資料來源：

http://www.cna.com.tw/news/afe/201712220109-1.aspx

3.1.3、日本引進深度學習 AI，防禦網路攻擊

日本「產經新聞」報導，防衛省計畫 2021 年引進人工智慧(AI)系統，強化因應網路攻擊的能力，未來希望能讓日本政府全體機構都在網路安全領域活用此一利器。



資料來源：

http://www.ydn.com.tw/News/272466

3.1.4、WIFI 聯盟推出具有新安全功能的 WPA3 協議

日前 WIFI 聯盟終於宣布了期待已久的下一代無線安全協議 WPA3。由於 WPA3 可能無法透過韌體更新，讓現有路由器直接支援新的加密協定，今年要買到具有 WPA3 的設備，可能還是需要等等。

資料來源：

https://thehackernews.com/2018/01/wpa3-wifi-security.html

3.1.5、一種針對 ARC 處理器攻擊的殭屍網路病毒 Mirai Okiru

ARC(Argonaut RISC Core)嵌入式處理器是全球第二大最受歡迎的 CPU，使用的範圍包括相機、手機、電錶、電視機、隨身碟、汽車和物聯網。然而一種針對 ARC 處理器攻擊的殭屍網路病毒 Mirai Okiru，它的影響範圍有可能在 2018 年呈現指數級增長。

資料來源：

https://thehackernews.com/2018/01/mirai-okiru-arc-botnet.html

3.1.6、電商網站防護鬆散，易遭駭客盜取個資

民眾上網購物日益頻繁，但部分電商對消費者個人資料保護出現漏洞，讓買家個資成為詐騙集團行騙資料。警政署 165 反詐騙專線統計 2017 年讓消費者個資外洩造成的詐騙案高達 2182 件，前五大高風險網路賣場依序是：ez 訂、金石堂、DEVILCASE、蝦皮拍賣和 OB 嚴選。

資料來源：

https://money.udn.com/money/story/5648/2941367

3.1.7、美國企業建立網路安全防護網

駭客入侵企業網路不但重創公司聲譽，更要花上千萬美元來修復網路漏洞和賠償客戶損失。由於代價慘重，部分企業的董事會愈來愈關注網路安全，並著重如何分配董事之間的職責。一些企業董事會則加強與內部負責網路安全的主管溝通。

資料來源：

http://www.chinatimes.com/newspapers/20180122000883-260203

3.1.8、美陸戰隊擴編「網軍」徵募駭客

美國陸戰隊在 2018 財政年度《國防授權法案》(NDAA)中，編列增募 1000 名專精網路、電戰通訊等專長士兵的預算。美國陸戰隊積極展現強化網路能力的企圖心，認為在未來複合戰爭型態中，網路干擾可能比火砲威力更重要。

資料來源：

https://www.ydn.com.tw/News/274486

3.1.9、川普欲將 5G 網路國有化以對抗中國網路威脅

美國總統川普目前要求透過聯邦政府建立覆蓋全美的高速 5G 無線網路，並將 5G 網路國有化，以保障網路安全並對抗包括中國在內的外來網路威脅。

資料來源：

http://www.chinatimes.com/realtimenews/20180129004196-260408

3.2、駭客攻擊事件及手法

3.2.1、你的物聯網設備密碼改了嗎？小心，隱私被看光光

近年來，物聯網設備越來越多，並逐漸滲透到我們生活的各個角落。 依據 Gartner 發布的報告顯示，2020 年全球物聯網設備數量約達到 240 億，而全球目前有 75 億人口，已超過全球人口數的 3 倍。隨著物聯網的發展，安全問題也隨之而來，其重要性也越來越引人關注。

物聯網漏洞不是在這一兩年來才出現的新鮮事。早在 2014 年，便有研究人員發現，中國某知名廠商所生產的數位視訊錄影機(DVR)因弱密碼感染了病毒，被駭客用來挖礦和發動網路攻擊；同時，駭客也在網路上公布了全球好幾萬台的攝影機鏡頭，將個人日常私生活畫面在網路上公開直播。在網路中，我們可以找到許多物聯網設備並容易的入侵破壞，如攝影鏡頭、智能家電、工控設備等。

根據駭客在網路實測的結果，如果你使用預設的帳號密碼，就能很容易登入 IOT 設備，一旦控制了這些設備，後果將不堪設想。你的隱私跟安全將面臨嚴重的威脅。

此外，駭客還可以利用被控制的設備組成疆屍網路，著名的案例為 2016 年 10 月 21 日，美國 DNS Sever Dyn Inc.遭到了大規模的分散式阻斷服務服務攻擊(DDoS)，這是史上最嚴重的 DDoS 攻擊，它導致 Twitter、亞馬遜、Shopify、Airbnb、PayPal 等數百家知名網站無法訪問。這次攻擊的來源主要是物聯網設備，這些設備存在弱密碼漏洞，進而被攻擊者利用插入惡意代碼，引發了這場美國網路中斷事件。綜上分析，可歸結出三個原因：

（1）節省成本，使用未經安全檢測的設備。

（2）使用者缺乏安全意識，設備缺乏安全更新機制。

（3）設備間身分授權及驗證機制薄弱。

根據上述的威脅，TWCERT/CC 提出以下幾點建議：

（1）使用經過安全檢測的互聯網設備。

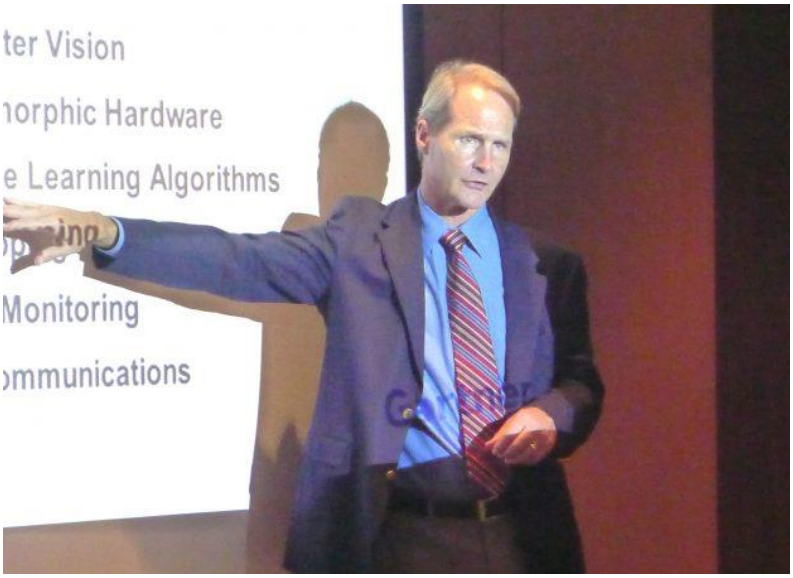
（2）安裝設備後，立即修改密碼並符合複雜性原則。

（3）不要將設備暴露在公開的網路上。

（4）定期實施設備的安全性更新。

（5）如設備未使用，儘量關閉電源。

（6）使用互聯網設備應注意個人隱私保護。



資料來源：

https://technews.tw/2016/09/20/gartner-the-units-of-internet-of-things-unit-will-less-and-cheap/

3.2.2、又有新的鍵盤側錄程式注入攻擊，超過 2000 個 WordPress 網站受害

繼 2017 年 12 月，超過 5,000 個網站遭感染挖礦與鍵盤側錄的惡意程式後，資安研究人員再次警告，又發現超過 2000 個運行於開源 WordPress 內容管理系統的網站遭注入新的惡意程式。

該惡意程式同樣會記錄包括密碼以及管理員或訪問者的任何其他輸入資料，也安裝了瀏覽器中的數位貨幣挖礦器，導致站點訪問者電腦運行 Coinhive 的 JavaScript，從而無需警告即可挖掘數位貨幣 Monero。

網站搜索服務 PublicWWW 所提供的資料顯示，截至 2018 年 1 月 29 日下午，該軟體包在 2,092 個站點中運行。

網站安全公司 Sucuri 表示，這與 12 月份在近 5,500 個 WordPress 網站上運行並被清除的惡意代碼相似，而新的感染則在以下三個新的網站，msdns[.]online、cdns[.]ws 和 cdjs[.]online。

攻擊者將 cdjs[.]online 腳本注入到網站的 WordPress 數據庫(wp_posts 表)或 WordPress 主題的 function.php 中的 cdns[.] ws 和 msdns[.]online 腳本。

注入鍵盤側錄程式的行為與之前的活動相同，腳本通過 WebSocket 協議將每個網站表單(包括登錄表單)輸入的數據發送給駭客。

注入的腳本包括：

hxxps://cdjs[.]online/lib.js

hxxps://cdjs[.]online/lib.js?ver=...

hxxps://cdns[.]ws/lib/googleanalytics.js?ver=...

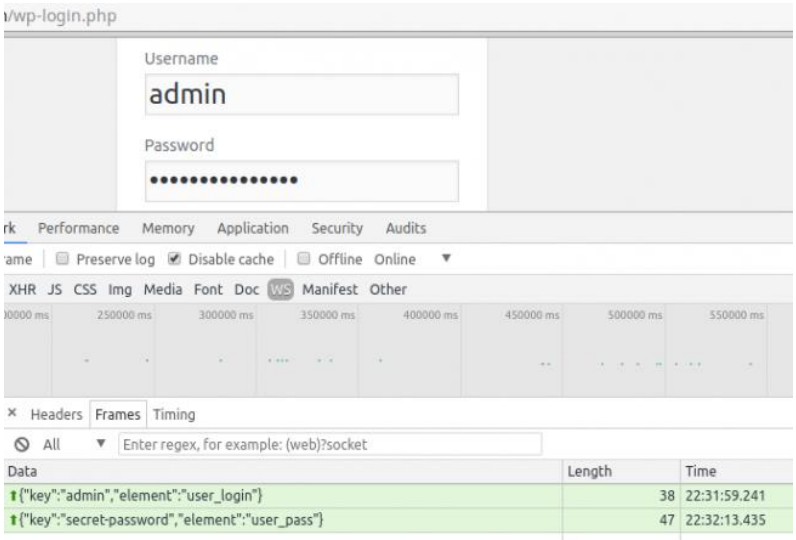
hxxps://msdns[.]online/lib/mnngldr.js?ver=...

hxxps://msdns[.]online/lib/klldr.js

Sucuri 並沒有明確地說出網站是如何被感染的。攻擊者極有可能利用網站使用未安全更新的軟體而導致的安全弱點。

雖然沒有上次近 5,500 個網站受害規模大，但再次感染顯示仍然有很多網站在原始感染後未能妥善進行自我防護措施，有些網站可能甚至沒有注意到原來的感染。

由於這些腳本讓攻擊者可以存取所有舊密碼，TWCERT/CC 建議受害網站維運者應即更改所有網站密碼，想要清理受感染站點的人員應按照以下第一個連結所提供之步驟操作。



資料來源：

https://sucuri.net/guides/how-to-clean-hacked-wordpress

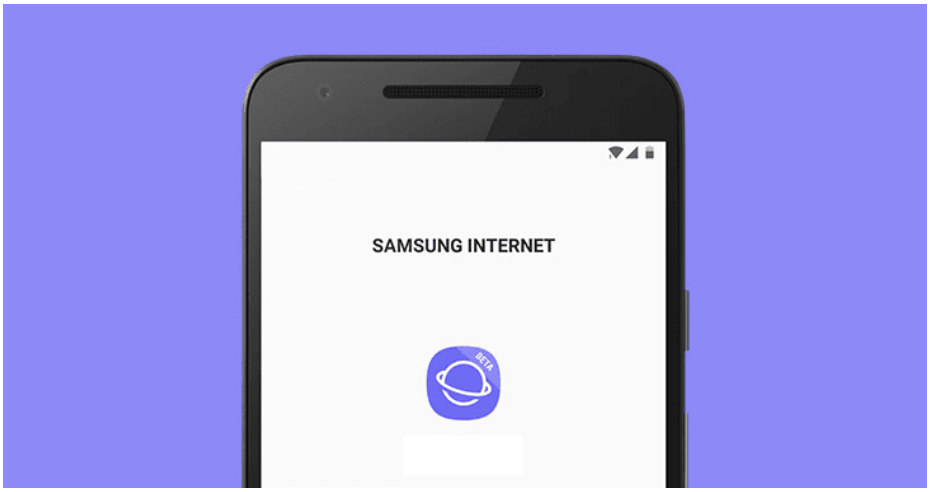
https://arstechnica.com/information-technology/2018/01/more-than-20

00-wordpress-websites-are-infected-with-a-keylogger/

3.3、軟硬體漏洞資訊

3.3.1、Samsung 瀏覽器迴避同源政策 SOP 恐使個資遭竊

普及率高的 Samsung Android 瀏覽器出現嚴重缺失，javascript 竟能違背 Same Origin Policy 而跨站台行動，已知二種可略過同源政策之弱點，均能導致機敏個資外洩，Internet Browser 5.4.02.3 以前舊版，因攻擊程式碼架構已公開，使用者開啟新頁籤時可能面臨廣泛威脅；至於最新版 6.2.01.12 則因 IFRAME Handler 元件瑕疵，易受 Cross site Scripting 攻擊，使瀏覽器被移花接木，網址列 URL 與頁面內容來源相異，該公司已修補部分軟體漏洞。



資料來源：

http://securityaffairs.co/wordpress/67235/hacking/samsung-sop-bypass-issue.html

3.3.2、全球 CPU 面臨 Spectre 與 Meltdown 漏洞威脅

全球只要使用 CPU 的資訊產品，無論行動裝置或個人電腦，幾乎都難免有鬼魅(Spectre)和熔毀(Meltdown)兩類漏洞，基於 CPU 架構體系，對間接分支(indirect branch)指令有 speculatively execute

相關設計，讓有益數據在用到前先完成運算，並儲存結果於 cache，但經由研究人員分析，此機制可讓低權限的操作者，能接觸本機其他 AP 與 OS 所占用記憶體，破解記憶體區間該有之保護，從而獲得密碼等隱私資料，部分 CPU 製造商已公布修補方式，軟體開發商亦研製相應產品更新，陸續釋放給底層用戶，但改善 kernel page-table isolation 技術後，CPU 效能最多降低 30%。

資料來源：

https://meltdownattack.com/

https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

http://www.kb.cert.org/vuls/id/584653

3.3.3、防火牆系統 Sonicwall 介面無法過濾特定 payload

SonicOS 是 Sonicwall 網路安全設備專屬作業系統管理介面，經

測試新舊版 SonicOS 均發生多項共同輸入驗證缺失且導致過濾機制遭略過，在用戶設定組態 SSO 下層模組三個輸入欄〔Host Name / IP Address〕、〔Client Name/IP Address〕、〔Proxy Forward To〕未受嚴謹稽核，另〔CFS Custom Category〕與〔Cloud AV DB Exclusion Settings〕模組僅於 Add 功能正常過濾 Name 欄位，然 Update 功能竟讓惡意程式碼假冒網域名偷渡，上述弱點使駭客趁定義客製化過濾內容同時，反而將內含惡意請求語法字串送進明細表資料庫，負責過濾網路流量的防火牆竟未篩選管理介面獲得參數，恐肇生 session 劫持、導向釣魚網頁、操弄模組功能，Dell 尚未公開正式修補方案。

資料來源：

https://cxsecurity.com/issue/WLB-2018010066

https://packetstormsecurity.com/files/145725/SonicWall-SonicOS-NSA-Web-Firewall-Cross-Site-Scripting.html

https://packetstormsecurity.com/files/145689/SonicWall-SonicOS-NSA-Filter-Bypass.html

3.3.4、TP-Link 證實 command injection 漏洞影響卅餘型 WIFI 路由器

普聯公司專營網路通訊設備，其家用型無線路由器，特別是 WVR、WAR、ER 系列型號測試出類似弱點，具備管理者身分人士可遠端注入任意 command，無論 LAN 和 WAN 都可能發生入侵事件，該等設備介面皆以 Lua 語言開發，究其原因係多個腳本內變數接收外部字串輸入後，未經過濾即視作正常值納入運算處理，TP-Link 尚未公布修補方式，然謹慎保存管理者帳密便可降低風險。

資料來源：

https://packetstormsecurity.com/files/145823/TP-Link-Remote-Command-Injection.html

http://www.tp-link.com/tw/download-center.html

3.3.5、小心 Transmission BitTorrent 設計缺陷，暗渡 PC 主控權

Transmission Project 採用 peer-to-peer 的 BitTorrent 協定，以 C 語言開發自由工具軟體，經測試 Transmission client 全體版本搭配相異 OS 與 browser，皆無法避免「domain name system 重

綁定」攻擊，這弱點肇因於 Transmission 背景服務處理 RPC session-id 之機制有破綻，駭客得以竄改 Transmission 用戶 DNS 名稱，將 HTTP POST 命令趁機寫入表頭資訊 X-Transmission-Session-Id，後續則能執行受害主機任何程式，開啟任何檔案，此途徑的確有效，但探勘門檻極高，此為 Torrent 軟體界首例 RCE 攻擊態樣，目前相關修補程式已提供下載。

資料來源：

https://github.com/transmission/transmission/pull/468

https://thehackernews.com/2018/01/bittorent-transmission-hacking.html

3.3.6、ISC 維護 DHCP 與 BIND 防止網路連線中斷

非營利的網路系統協會（Internet Systems Consortium,ISC），發展了幾項關鍵技術，如 BIND、ISC DHCP 及 Kea，兼具全球 13 個 DNS root server 其中之 F-root 營運者身分。始於 1980 年代於加州柏克萊大學發展的 Berkeley Internet Name Domai(簡稱 BIND)，處理遞迴的 fetch()清除過程觸發 Use-after-free，引發 assertion failure 及域名伺服器 named 元件崩毀;另 Dynamic Host Configuration Protocol 網路服務，同樣地清理 OMAPI 連線程序失敗，過度消耗 DHCP server 可用 socket，用戶將無法申請 IP 租約，

DHCP、BIND 兩者漏洞均屬遠端觸發型 DoS，ISC 僅就 BIND 提供安全更新，至於 DHCP 則因危害有限，可逕從組態設定著手，尚未規劃修補。

資料來源：

https://kb.isc.org/article/AA-01541

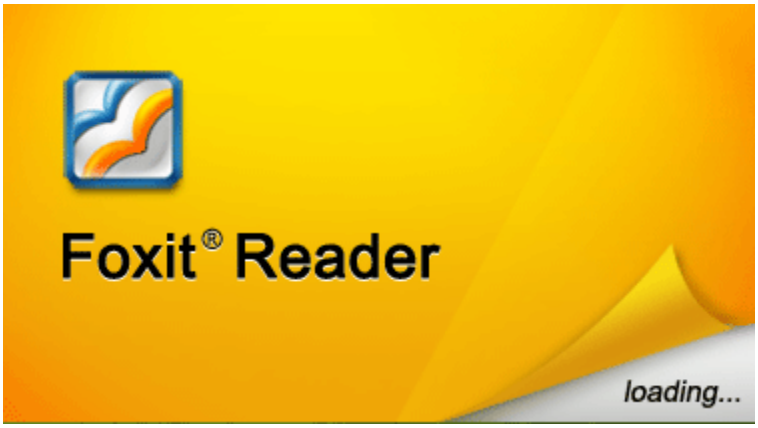
https://kb.isc.org/article/AA-01542

https://www.isc.org/downloads/bind/

3.3.7、Foxit 閱讀軟體功能瑕疵易肇生 RCE、訊息外洩

福昕軟體公司研發數款 PDF 閱讀工具，其特色在體積小、速度快，經測弱點在 Android 平台之 MobilePDF 與 Windows 平台 5 之 PhantomPDF、Reader，用智慧機閱讀 PDF 須注意，內含跳離字元的 URI 未完整檢驗，即使手動關閉 MobilePDF，WIFI 仍繼續傳輸而使資料被讀取。至於桌機使用 PhantomPDF 或 Reader 則意外較多，多種涉及 XML Forms Architecture 的 Type confusion 與 use-after-free 狀況，恐衍生 Remote Code Execution；而 single instance 模式以滑鼠雙擊開啟惡意 PDF，可能因錯置 Address

control 碼而當機；開啟 EPUB 檔案若碰巧其 ZIP 壓縮之檔名長度超限，則觸發 buffer overflow；無論是否採安全模式閱讀，皆有數種函數及參數運用時觸發 out-of-bounds read，造成隨機檔案、異常 PDF 被開啟，Foxit 就相關版本軟體進行升級並公告。



資料來源：

http://www.foxitsoftware.com/support/security-bulletins.php#content-2017

https://www.foxitsoftware.com/support/security-bulletins.php#content-2018

3.3.8、義籍駭客破解 Master IPCAM01 並取得 root 密碼

近期義大利駭客頗為活躍，除了間諜軟體 skygofree 喧騰一時，自稱 Raffaele Sabato 的駭客亦破解該國 Barni Carlo spa 公司出廠的網路攝影機，型號 Master IPCAM01，相關漏洞若組合運用，駭客可無拘無束地下載組態備份 config_backup.bin，變造 webserver.conf 再送回設備端，即可遍覽路徑，取得 root 密碼 hash 值並破解，另外循 HTTP request 途徑則能獲得 IP camara 管理性資

料並變更 web server 通信埠，等同接管全機。目前尚未獲悉修補訊息，然須注意所有探勘行動皆發生於輸入預設帳密之後，鑒於眾多網路攝影機預設密碼業已披露，故修改實為保全 IoT 之根本要務。

資料來源：

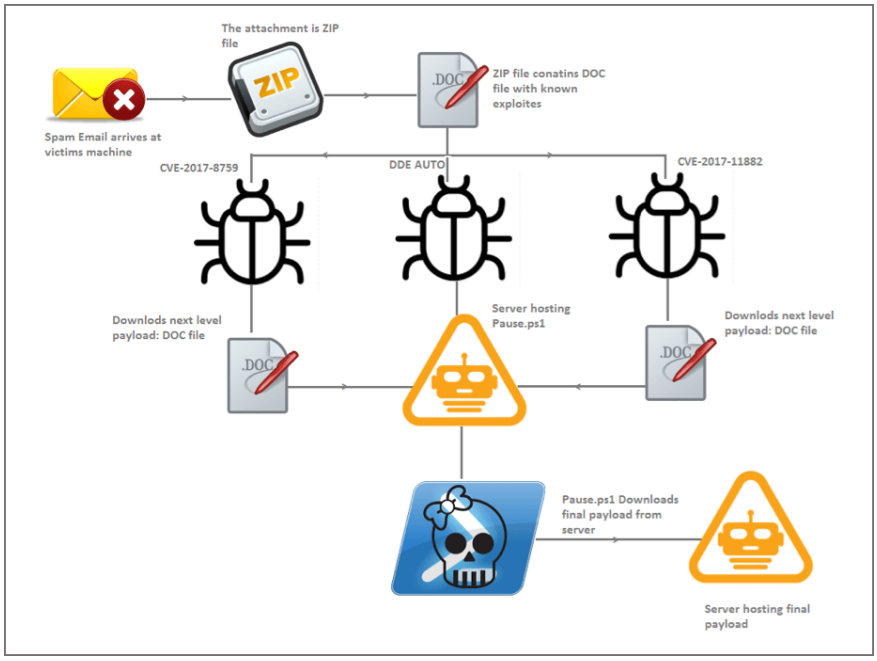
http://syrion.me/blog/master-ipcam/

https://www.hkvstar.com/technology-news/ip-camera-default-user-name-and-password.html

3.3.9、殭屍軟體氣旋 Zyklon 復出，刻正威脅微軟 Office 用戶

早在 2016 年初，Zyklon 如同氣旋般橫掃網路，該 botnet 惡意程式透過 HTTP 竊取受害者之鍵盤紀錄、密碼等隱私，如今新一波駭客行動挾 Zyklon 復出，藉由 Office 三個已知漏洞散播，恐鎖定癱瘓

電信、保險及金融相關產業，經分析氣旋探勘漏洞技術，基礎在於去年公開的.NET Framework、DDE protocol、Office 方程式編輯器漏洞，故氣旋透過嵌入 DDE 協定的 Word 文件，配賦十進位 dotless IP 為 URL，偷渡回連 C&C 伺服器，以 PowerShell script 進行幕後多階段感染；另利用 Equation Editor 元件本身為 out-of-process COM server 屬性，規避 Data Execution Prevention 和 Address space layout randomization 保護機制；同時具備 FinSpy 間諜軟體特徵，能側錄受害主機並偷渡資料，此外還能使役受害 PC 挖礦，順帶布署 DDoS 網路攻擊；當然 Zyklon 感染途徑也不脫 email 等社交工程，儘管微軟 2017 年已提供安全更新，惟對欠缺資安意識者，漠視例行修補與郵件警覺，必然形成危害。

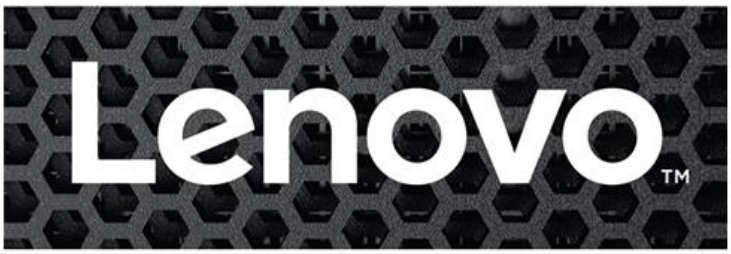


資料來源：

https://thehackernews.com/2018/01/microsoft-office-malware.html

3.3.10、聯想察覺 Lenovo 及 IBM 系列交換器內 HP backdoor 隱藏 14 年之久

14 年前被埋入 Enterprise Networking Operating System 的後門 HP backdoor，隨著二度企業併購，影響到既有 Lenovo 和 IBM 廠牌多型號網路設備，若未使用 LDAP、RADIUS、TACAS+等遠端驗證功能，或者啟動 Backdoor 與 Secure Backdoor 相關設定，則成立特殊後門條件，讓攻擊者能經由 serial console、Telnet、SSH、Web 等一般介面，略過身分驗證而獲得高階權限，恐干擾交換器出入流量且形成當機，聯想已就各款設備提供韌體更新。



資料來源：

https://support.lenovo.com/tw/zh/product_security/len-16095

http://securityaffairs.co/wordpress/67729/hacking/lenovo-backdoor-net

working-switches.html

3.3.11、Symantec 多款產品恐洩漏 Diffie-Hellman 密鑰及避開 TLS 協定

Symantec 公告 9 類網路安全軟體涉及相同資料外洩弱點，其實並非 Symantec 原始設計缺乏安全意識，而是採用 OpenSSL 函式庫

套件開發所致，儘管 OpenSSL 1.0.2 系列已有升級解決方案，然開發完成品繼承 2 項既定漏洞，使駭客可藉 rsaz_1024_mul_avx2()之蒙哥馬利乘法程序觸發 overflow，獲得 Diffie-Hellman 密鑰資訊；另經由製造 handshake 錯誤狀態，引發 OpenSSL 1.0.2b 後續版本 handshake 函數，SSL_read()和 SSL_write()被不當呼叫，使明文資料繞開傳輸層安全性(TLS)加解保護，結果反而違悖 OpenSSL 避免竊聽的本意，Symantec 表示本次不提供修補檔，於下次軟體升級一併處理。

資料來源：

https://www.symantec.com/security-center/network-protection-security-advisories/SA159

https://www.hkcert.org/my_url/zh/alert/18011801

3.3.12、Seagate 家用雲端裝置 Personal cloud 測出漏洞，恐遭遠距執行系統 command

硬碟大廠 Seagate 推出網路儲存裝置 Personal cloud，用於架設私人專屬雲端，達到異地備份與遠距存取之目的，近日獨立研究員 Yorick Koster 測試出該設備漏洞，由於 uploadTelemetry 及

getLogs 兩副程式原始設計所運用之 csrf_exempt decorator，會停用 Cross-Site Request Forgery 防護，允許駭客藉此於 URL 內注入惡意指令，透過 GET 參數回傳給 fastcgi.server 元件，以 root 權限執行，等同接管整機設備，而 Seagate 自 2017 年 10 月獲告產品瑕疵，迄今尚未公告修補事宜，讓「輕鬆存取」的產品形象又多了一層意義。

資料來源：

https://blogs.securiteam.com/index.php/archives/3548

https://www.exploit-db.com/exploits/43659/

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
2018/03/13– 03/15	2018 臺灣資安大會	【資安研討會】2018 臺灣資安大會 主辦單位：iThome 日期：2018 年 3 月 13 日至 15 日 地點：台北國際會議中心 TICC (台北市信義路五段 1 號) 線上報名連結： https://signuptcss.ithome.com.tw/2018/signup?utm_source=tcss_website&utm_medium=link&utm_campaign=tcss2018&utm_content=navi_shortcut 資料來源：https://cyber.ithome.com.tw/ 活動概要： 今年主題聚焦「Cyber First Cyber Taiwan 建構資安優先意識、看見臺灣的資安動能」，三天會期總計超過 140 場議程，涵蓋高達 60 種熱門資安議題與技術面向，更從新興科技、典範轉移，以及軟體開發與硬體設計等面向深入資安死角，全方位關照資安。 現場更囊括 700 種以上主流資安產品與解決方案一次看盡，無論你對資安的了解或多或少，來到現場都能找到下一步對策，再造企業核心競爭力！ ● Keynote 國內外資安專家齊聚演講 ● Cyber First 熱門資安議題技術論壇 ● Cyber LAB 史上最強攻防實機體驗 ● Cyber Taiwan 臺灣資安館聚焦自主研發 ● Cyber Security Expo 百大資安展遍覽知名廠牌 ● CIO/CISO 資安長專屬前瞻策略會議

第 4 章、2018 年 2 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 1 月收到通報計 527 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。

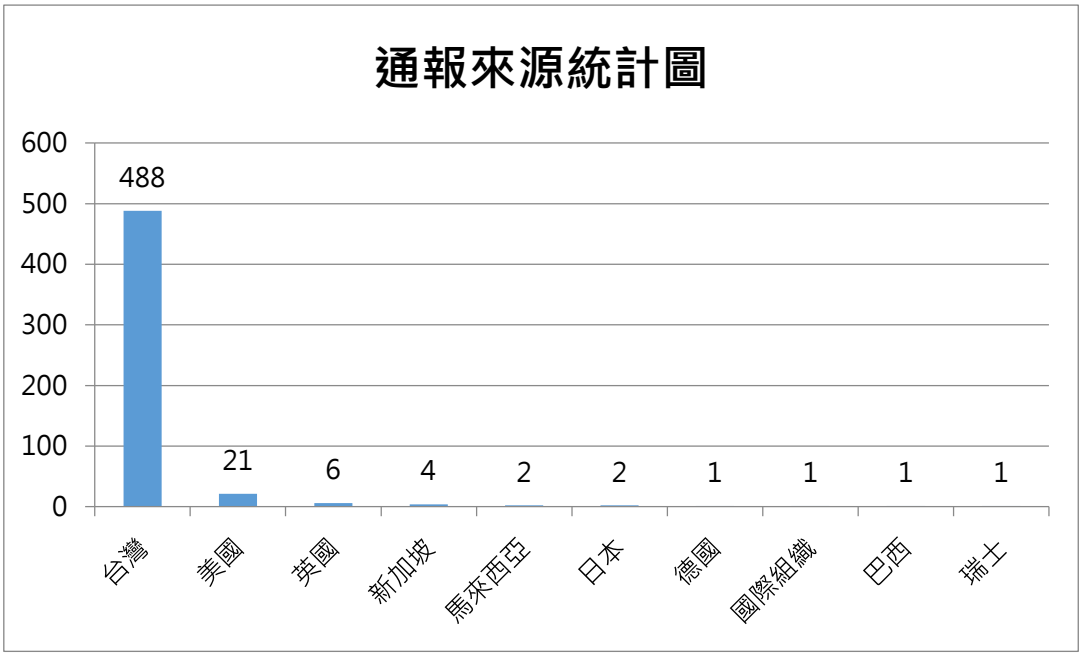


圖 1、通報來源統計圖

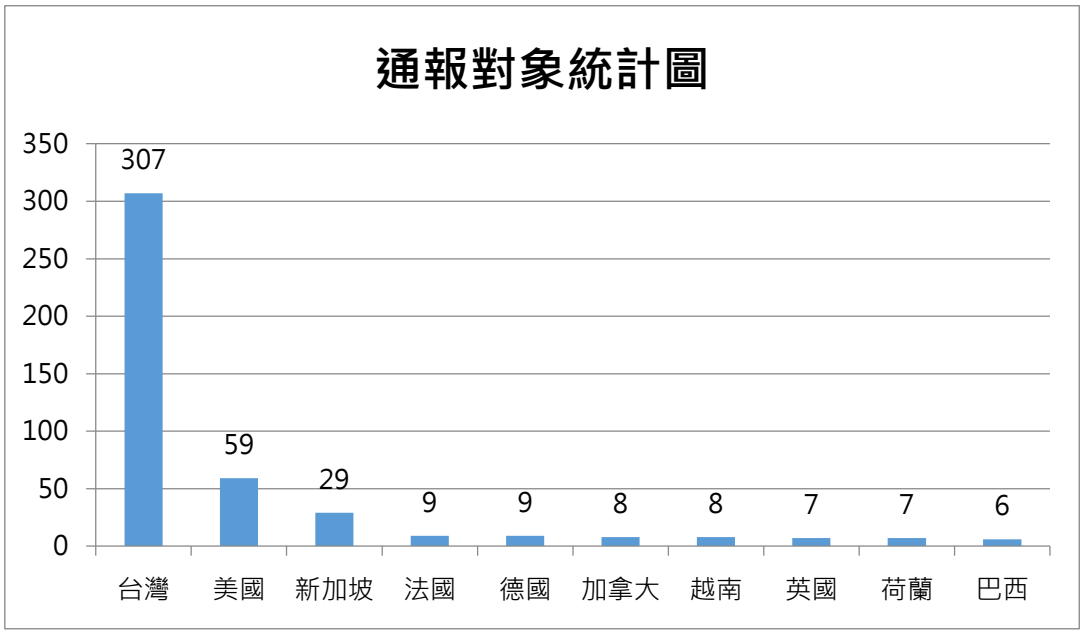


圖 2、通報對象統計圖

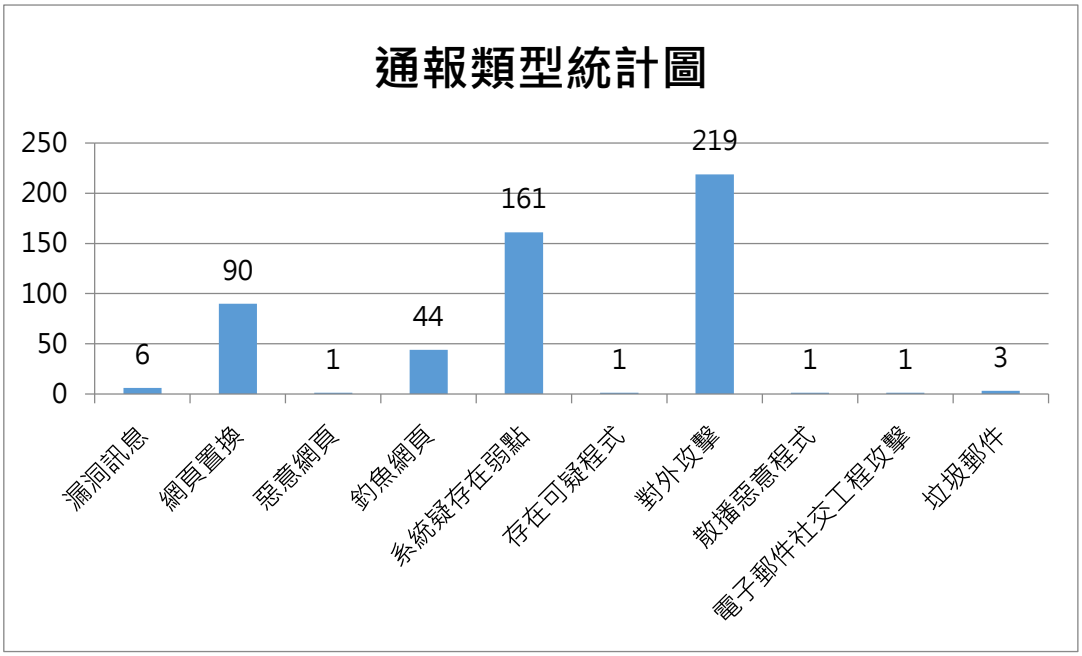


圖 3、通報類型統計圖

本月以「一頁式廣告詐騙網頁」屬特殊案件，近來臉書購物成為民眾線上購物新管道，而相關詐騙案例也隨之頻傳，且受害者除遭受詐騙外，個人資料也可能因此遭有心人士收集利用。

消保處副處長吳政學亦表示，今年臉書詐騙案例特別多，受害人大多是點擊臉書廣告後連到一頁式購物網。

這類一頁式廣告資訊精簡，甚至沒有聯絡人，商品價格也明顯低於市場行情，且永遠有拍賣倒數，更宣稱免運貨到付款、7 天鑑賞期無條件退貨等利多條件誘導民眾受騙。

警政署刑事警察局 165 反詐騙與「Whoscall 網路購物詐騙回報系統」合作，2017 年開始架設假廣告網頁通報平台「http://cybercrime.whoscall.com/」，提供民眾上傳相關資料，再由刑事局人員進行進一步審核。

並現與 TWCERT/CC 合作，透過通報系統移除相關詐騙偽冒網頁，以減少受害情形，避免災害擴大。

TWCERT/CC 提醒網路購物民眾，網路購物務必尋找可信賴的台灣業者，避免透過一頁式廣告資訊進行交易，以免受害，並可透過假廣告網頁通報平台「http://cybercrime.whoscall.com/」回報可疑網頁，由刑事人員以及 TWCERT/CC 人員處理，減少詐騙情事。

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 2 月 15 日

編　　輯：曾佩雅

服務電話：03-4115387

市話免付費服務電話：0800-885-066

電子郵件：twcert@cert.org.tw

官　　網：https://www.twcert.org.tw/

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

資安電子報訂閱：http://i-to.cc/S5HzJ

如有任何疑問或建議，歡迎您不吝指教。