TWCERT/CC 資安情資電子報

2019 年 10 月份

目錄

第 1 章、 封面故事

YouTube 大量用戶帳號遭劫持，創作者哀鴻遍野

近日大量 YouTube 影音創作者帳號被劫，尤以汽車評鑑或汽車改裝類頻道為甚；其他類型 YouTube 帳號亦傳大量被盜。

據 ZDNet 報導，這次大量帳號被盜事件，集可能是預謀已久的協同攻擊行為；被盜的帳戶有許多都是訂閱破數十萬的人氣 YouTuber，在 Twitter 上和 YouTube 支援論壇中可以看到大量相關抱怨和討論。

整個攻擊手法以釣魚郵件開始，攻擊者以釣魚郵件，誘騙帳號持有人登入假的 Google 登入頁面，取得用戶的 Google 登入帳密後，立即將用戶的 YouTube 頻道管理權限轉移給攻擊者自己的其他帳號，同時修改 YouTube 頻道原本使用的自定網址，讓循此網址進來的觀眾看到錯誤訊息，誤以為該頻道已關閉。

更有受害者指出，這些攻擊者有能力通過二階段登入驗證，因為攻擊者很可能也同時攔截了受害者應該要收到的驗證密碼簡訊。

目前 Google 尚未針對此事發表任何評論。

- 攻擊手法：釣魚郵件
- 關鍵字：YouTube, Phising, 2FA
- 資料來源：
  1. https://www.zdnet.com/article/massive-wave-of-account-hijacks-hits-youtube-creators/

第 2 章、 國內外重要資安事件

2.1、國際政府組織資安資訊

2.1.1 美軍駭入伊朗革命衛隊系統，摧毀其恐怖攻擊資料庫

美軍網路作戰司令部（US Cyber Command）證實，曾在六月時針對伊朗革命衛隊的資料庫發動網路攻擊，將其摧毀，以防行駛於波斯灣的各國油輪與貨輪再次遭該組織襲擊。

美國官員指出，這場攻擊行動是在美軍無人機遭擊落後的報復行動，且由川普總統批准執行。

美國網路作戰司令部拒絕透露行動細節，但這樣的網路軍事攻擊行動，足以顯示網路作戰已經正式成為美軍整體戰力的重要一環。

- 攻擊手法：不明
- 資料來源：
  1. https://www.stripes.com/news/us/us-military-carried-out-secret-cyberstrike-on-iran-to-prevent-it-from-interfering-with-shipping-officials-say-1.596335
  2. https://www.stripes.com/news/middle-east/with-trump-s-approval-pentagon-launched-cyber-strikes-against-iran-1.587171

2.1.2 以 Deepfake 技術偽造 CEO 來電，歹徒「命令」子公司匯款詐騙成功

可以偽造人臉表情或聲音的 Deepfake 技術，又出現新的受害案例。歹徒偽造母公司 CEO 來電指示子公司進行匯款，成功得手 24 萬餘美元。

這個發生在今年三月的案件，受害者是家德商所屬的英國能源公司。

歹徒使用市售可用來合成逼真語音的 AI 輔助軟體，假扮母公司的德籍 CEO，去電英國子公司總經理，要求緊急匯款到某設籍於匈牙利的公司。

由於來電者的語音模仿德籍 CEO 十分逼真，連其德國口音都唯妙唯肖，英籍總經理不疑有他，遵示辦理，匯了 243,000 美元；日後才發現這是詐騙。

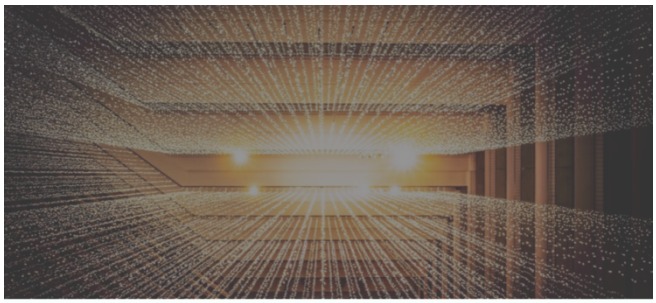
歹徒甚至在日後又撥了假電話，要求第二筆匯款；但這次英籍總經理沒有上當。

警方追查該筆匯款流向，發現這筆匯到匈牙利的款項，被轉匯到墨西哥等多個不同國家，顯然是為了逃避查緝的洗錢行為。

這家受騙公司的名稱目前並未透露，詐騙金額則由保險公司全數理賠；但各國資安情報組織先前即曾指出，類似利用 AI 的 deepfake 詐騙案會逐漸增加，且更加難以分辨真偽。

- 資料來源：
  1. https://thenextweb.com/security/2019/09/02/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000/
  2. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

2.1.3 巴爾的摩市府證實，勒贖攻擊造成市政資料損毀



TWCERT/CC

巴爾的摩市府證實，勒贖攻擊造成市政資料損毀

巴爾的摩市府審計單位證實，在數個月前針對該市的勒贖攻擊，確實造成部分市政資料永久損毀，無法復原。

美國巴爾的摩市審計員指出，該市資訊部門的部分資料，確定在先前該市遭受的勒贖攻擊中受損。

受損的資料是關於該市資訊部門的人員績效考核資料；這些資料都存在電腦系統的本地端，沒有其他備份；目前確認這些資料已經永久損毀。

巴爾的摩市於今年五月遭到勒贖攻擊，多個市政系統資料遭到加密，該市市政陷入癱瘓；該市隨後支付六百萬美元贖款，但遭到攻擊的市政系統與資料尚未全面復原。

巴爾的摩市先前任命的資訊部門主管，也因為此次攻擊事件而飽受責難；目前暫時處於停職狀態。

- 資料來源：
  1. https://www.baltimoresun.com/politics/bs-md-ci-data-lost-20190911-i6feniyk5nd3pereznpdxwsf7a-story.html
  2. https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html
  3. https://www.baltimoresun.com/politics/bs-md-ci-frank-johnson-leave-20190910-waliphukdbcg3evzylbrjfefui-story.html

2.2、社群媒體資安近況

2.2.1 Facebook 近四億二千萬筆用戶個資外洩，資料庫被公開在網路上

資安研究人員在網路上發現多個含 Facebook 用戶大量個資的超大型資料庫檔案，未經任何保護，可自由存取；總資料筆數高達四億一千九百萬筆；資料含臉書用戶 ID、手機號碼等個資。

資安研究單位 GDI 基金會研究人員，日前發現數個資料庫，內含近四億二千萬筆 Facebook 用戶個資。

這些資料中有一億三千多萬筆資料屬於美國的 Facebook 用戶，一千八百萬筆屬於英國，也有五千萬筆以上來自臉書的越南用戶。

外洩個資欄位包括用戶在臉書的 User ID、姓名、電話、生日、國家、性別、所在地、資料更新日期等。

資安人員指出，這些含超多內容的資料庫檔案，未經任何密碼保護，知道網址的人皆可任意存取。

駭客可經由這個資料庫輕易取得臉書用戶的手機號碼，發送垃圾簡訊或詐騙電話，甚至發動 SIM 卡置換攻擊，或是利用這個電話號碼來竊取用戶在其他網路服務的登入資訊。

Facebook 對此表示，這批資料是在 Facebook 去年取消用戶透過電話查詢其他用戶前流出的，內容十分老舊，且 Facebook 很早以前就限制開發者取得用戶電話；目前沒證據指出資料由 Facebook 內部直接外洩。

- 資料來源：
  1. https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/

2. https://www.theguardian.com/technology/2019/sep/04/facebook-users-phone-numbers-privacy-lapse

2.2.2 大量 Instagram 釣魚郵件，藉侵權為由騙取帳號控制權

資安單位發現大量假冒 Instagram 發送的詐騙釣魚信件，意在竊取帳號控制權，用戶須提高警覺，避免點擊假連結。

據資安公司 Sophos 發布的消息指出，近來有大量假冒熱門相片影片分享社群平台 Instagram 的釣魚信件，在網路上流傳，意圖騙取受害者的帳號控制權。

這波釣魚信件假裝是由 Instagram 平台發出的警告信，指稱用戶分享侵害著作權的內容，如果不按下信件中的申訴按鈕，帳號可能會在 24 小時內遭停權。

用戶如果受騙而按下連結，就會被導向到一個假網站，並要求輸入 Instagram 帳號與密碼；歹徒就可取得用戶的 Instagram 控制權。

由於很多用戶會將同樣的帳號密碼使用在不同服務上，所以歹徒還可能進一步入侵受害者在其他服務上的帳號。

事實上，Instagram 對於侵權內容的處理，並不會在事前通知用戶，

而是會先下架內容才通知用戶，所以流程是不一樣的。Instagram 用戶如果收到不明的通知信，一定要提高警覺。

- 資料來源：

1. https://nakedsecurity.sophos.com/2019/09/24/instagram-phish-poses-as-copyright-infringement-warning-dont-click/
2. https://help.instagram.com/1445818549016877

2.3、行動裝置資安訊息

2.3.1 Google 資安研究團隊揭發史上最大 iPhone 駭侵事件

Google 資安研究團隊 Project Zero 揭發史上為期最長、受害範圍最大的 iPhone 駭侵事件；駭侵行動長達兩年時間，受害人數難以估計。

駭侵者係利用 iOS 長期未被發現的 0-day 漏洞，在數個網站中放置惡意程式碼；只要以 iPhone 瀏覽這些網站，就會被植入惡意軟體；用戶在 iPhone 上進行的通訊活動，以及行事曆、相片、密碼、手機所在位置的即時座標等個資都會遭竊。

據 Google 指出，這些被置入惡意程式的網站，每周都有數千訪客。雖然 Google 未指出哪些網站放置惡意程式，也沒指名駭侵者或目標，但據 TechCrunch 報導，熟知內情人士認為這是中國支持的駭侵團體，以維吾爾穆斯林人士為目標的駭侵行動。

受這個 0-day 漏洞影響的 iOS 版本，自 iOS 10 一直到 iOS 12；Google 於二月通報 Apple 這個發現，Apple 隨即在二月發行的 iOS 12.1.4 更新中修補了這個嚴重漏洞。

富比士雜誌也指出，這些網站不只攻擊 iPhone，也存有針對 Android 和 Windows 系統的惡意程式碼。

- 攻擊手法：於網站中安插攻擊用的惡意程式碼。
- 資料來源：
  1. https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html
  2. https://techcrunch.com/2019/08/31/china-google-iphone-uyghur/
  3. https://www.forbes.com/sites/thomasbrewster/2019/09/01/iphone-hackers-caught-by-google-also-targeted-android-and-microsoft-windows-say-sources/#2adac7224adf

2.3.2 新發現 Android 木馬，不但竊取用戶個資，還會暗中訂閱付費服務

資安研究單位發現一個名為「小丑」（Joker）的 Android 木馬，除了會竊取用戶個資、製造廣告假點閱外，甚至還會暗中訂閱付費服務。

資安公司 CSIS 日前發表研究報告，指出該公司發現一個全新的 Android 木馬程式，稱為「小丑」（Joker），且已經大量透過 Google Play 官方軟體下載中心散布。

這個惡意程式不但會竊取用戶手機中的通訊錄、裝置資訊和簡訊通訊內容，也會製造廣告假點擊，浪費用戶頻寬並詐取廣告分潤；更嚴重的是會自動幫用戶訂閱付費服務，造成更大的損失。

目前 CSIS 觀測到 Joker 已藏身在 24 支於 Google Play 上架的 App 之中，總安裝次數接近五十萬次。受害者多分布於歐洲和亞洲各國，但也觀測到當用戶身處美國和加拿大時，該木馬便會自動停止執行。

CSIS 的報告中有詳細的惡意軟體行為分析可供參考。

- 資料來源：
  1. https://medium.com/csis-techblog/analysis-of-joker-a-spy-premium-subscription-bot-on-googleplay-9ad24f044451

2.3.3 Android 全新 0-Day 漏洞，可導致駭侵者取得更高操作權限

趨勢科技旗下的資安研究單位 ZDI 發表研究報告指出，該單位發現一個嚴重的 Android 0-Day 漏洞；駭侵者可藉此取得更高的作業系統操作權限。。

ZDI 指出，這個漏洞出現在 Android 的繪圖相關子系統驅動程式 V4l2（Video4Linux 2）中； 駭侵者只要先取得較低的執行權限，接著利用這個漏洞，就可以獲得更高權限，進而控制整個裝置。

這個 0-Day 漏洞的 CVSS 嚴重程度分數達到 7.8，算是相當嚴重的安全漏洞；ZDI 於今年三月通報 Google，但目前針對該漏洞的修補程式，尚未出現在 Google 九月的系統更新之中。

- 影響產品(版本) ：Android 各版本
- 解決方案：尚無。
- CVE 編號：暫無

- 資料來源：
  1. https://www.zerodayinitiative.com/advisories/ZDI-19-780/
  2. https://threatpost.com/android-zero-day-bug-opens-door-to-privilege-escalation-attack-researchers-warn/148014/

2.3.4 蘋果澄清 Google 發表 iOS 安全漏洞報告的若干疑點

日前 Google 發表關於 iOS 的重大安全漏洞消息，造成用戶震撼；蘋果針對其內容發表澄清聲明。

日前 Google 的資安研究團隊 Project Zero 發表重大資安公告，指稱蘋果的 iOS 作業系統存有嚴重資安漏洞，導致駭侵團體長年利用該漏洞竊取用戶敏感資訊；消息傳開後造成媒體大量報導，並造成用戶震撼。

蘋果針對該報告中的問題，於日前發表聲明，澄清下列疑慮：首先，駭侵團體的攻擊目標是針對特定對象，也就是維吾爾人社群，而非針對一般大眾。其次，蘋果強調在 Google 發出公告前六個月，蘋果即已修復該漏洞。

蘋果也說，透過特定網站發動駭侵攻擊的時間，並非如 Google 所說的長達兩年，而是約兩個月。蘋果也在內部發現此一漏洞的十天內就修補了該漏洞。

- 資料來源：
  1. https://www.apple.com/newsroom/2019/09/a-message-about-ios-security/

2.3.5 名為「Checkm8」的漏洞，能破解自 iPhone 4s 到 iPhone X 的所有先前 iPhone 機種

駭客發表一個存在於 iPhone 硬體的漏洞破解方法，能夠暫時性地破解 iOS；為近年來影響範圍最大的 iPhone 漏洞。

這個稱為「Checkm8」（將軍）的漏洞，能在從 iPhone 4s 到 iPhone X 的各種舊款 iPhone 上執行，破解作業系統的執行權限限制，一度引起 iPhone 用戶群的緊張。

但這個漏洞的破解有諸多限制：必須以實體 USB 連接電腦和 iPhone，進入 DFU 模式後，在電腦上執行破解程式才行；而且只要 iPhone 重新開機，破解就失效，必須重覆上述步驟。

此外，除了 iPhone 4s、iPhone 5 和 iPhone 5c 等沒有 Secure Enclave 晶片的機種之外，其他所有 iPhone 機種的資料，都無法透過這個破解取得並解密。

由於是硬體漏洞所致，所以這個漏洞無法修復；不過專家評估這個漏洞並不會造成研重的攻擊事件，用戶只要不讓手機與解鎖密碼落入他人手中，就不必過於擔憂。

- 資料來源：
  1. https://appleinsider.com/articles/19/09/28/the-checkm8-exploit-isnt-a-big-deal-to-iphone-or-ipad-users-and-heres-why
  2. https://www.theregister.co.uk/2019/09/27/unpatchable_exploit_for_ios/

2.4、軟體系統資安議題

2.4.1Windows Defender 防毒軟體於近期更新後無法運作

內建於多個 Windows 版本中的防毒軟體 Windows Defender，在最近一次更新之後出現問題，無法順利掃毒。

在套用微軟於 2019 年七月發行的每月更新包後，內建於多種 Windows 版本中的掃毒軟體 Windows Defender 出現問題；不論是快速或完整掃毒，在掃瞄約 40 個檔案後，Windows Defender 便會出現「沒有發現威脅」的訊息，然後停止掃毒。

出問題的 Windows Defender 版本是 4.18.1908.7；針對這個錯誤，微軟也推出新版 Windows Defender 加以解決。

如果你還沒有升級到新版，也可以使用「自定掃瞄」來避開這個錯誤。

- 資料來源：
  1. https://wccftech.com/microsoft-fixes-windows-defender-scans-broke/

2.4.2 惡意活動邀請造成十億 Google 日曆用戶嚴重資安威脅

近來許多 Google 日曆用戶頻繁收到內含惡意連結的活動邀請，造成嚴重資安威脅。Google 已著手處理此一問題。

近來眾多 Google 日曆用戶發現，自己的行事曆中出現奇怪的活動邀請；這些活動邀請往往以贈獎或其他吸引人點擊的文案，以類似釣魚郵件的手法，誘使用戶點擊惡意連結，填寫個資、信用卡資訊。

某些連結甚至直接夾帶惡意軟體，用戶只要一點擊，就有被駭侵的可能。

雖然早在數年前就有資安專家提出類似警告，但 Google 一直到日前才正式承諾，已經認知到該問題，並已著手處理。但 Google 認定這些惡意邀請的出現，並不是產品本身有錯誤或漏洞，而是一種濫用行為。

Google 也呼籲用戶小心處理日曆中出現的不明邀請，若認為該活動邀請有問題，可以提出檢舉並予以刪除。

- 資料來源：
  1. https://support.google.com/calendar/thread/13429505?hl=en
  2. https://support.google.com/calendar/answer/6110973?hl=en&ref_topic=3418057#report_spam
  3. https://www.forbes.com/sites/daveywinder/2019/09/09/google-finally-confirms-security-problem-for-15-billion-gmail-and-calendar-users/#72c55416279f

2.4.3 Google Play 商店中再次發現兩個自拍 App，會一直顯示蓋版廣告

資安研究人員在 Google Play 商店中再度發現兩個自拍美顏 App，不但會持續顯示蓋版廣告，而且難以移除。

資安公司 Wandera 的研究人員指出，他們在 Google Play 商店中發現兩個新的惡意廣告 App，都是頗受歡迎的自拍美顏軟體。

這兩個軟體，一個叫做 Sun Pro Beauty Camera，已有一百萬次下載；另一個叫做 DUnny Sweet Beauty Selfie Camera，約有五十萬次下載。

這兩個 App 都藏有用戶不知情的惡意廣告機制，安裝之後用戶的手機就會不停跳出蓋版廣告，即使用戶在執行其他軟體，廣告仍會不斷跳出；不但干擾用戶操作，更會快速消耗手機資量傳輸量與電力。

這兩支 App 還會在第一次使用後，把自己從應用程式列表中隱藏起來，讓用戶難以移除；即使移除手機桌面的捷徑，App 仍會在背景持續執行。

研究人員也發現這兩個 App，都使用來自中國的 APK 包裝機制 Ijiami（愛加密），以避免程式碼被解開檢視。

Google 已將這兩支 App 自 Google Play 商店中下架。

- 資料來源：
  1. https://www.wandera.com/mobile-security/google-play-adware/
  2. https://www.zdnet.com/article/two-android-adware-apps-with-1-5-million-downloads-removed-from-google-play-store/

2.4.4 Google Chrome 應用程式商店中出現假冒廣告阻擋外掛，用以詐騙電商銷售分潤

兩支假冒知名網頁廣告阻擋器的假冒外掛程式，於 Google Chrome 應用程式商店中被發現；估計每月詐得的電商購物分潤，高達數百萬美元。

這兩支假冒外掛程式是「AdBlock by AdBlock Inc.」及「uBlock by Charlie Lee」，分別假冒 AdBlock 和 uBlock 這兩個廣受歡迎的廣告阻擋軟體。

發現這兩支假冒外掛的，是另一家知名廣告阻擋軟體開發者 AdGuard；AdGuard 在其官方部落格中發文指出，這兩支假冒外掛合計已有 160 萬用戶。

報告進一步分析假冒外掛後，發現這兩支外掛都會進行「cookie stuffing」詐騙，也就是在用戶瀏覽器中偷偷塞入不相干的第三方 cookie；當用戶於某些電商網站購物時，就可以透過該 cookie 進行不實推薦認證，詐取分潤傭金。

AdGuard 發現這兩支假冒外掛的詐騙 cookie，詐騙的目標包括 Alexa 前一萬名中的三百個大型網站，每個月可詐得的傭金，估計高達數百萬美元。

在這個消息公開後，Google 已將這兩支假冒外掛下架，但由於 Google 對 Chrome Store 外掛程式上架的審核非常鬆散，資安專家建議用戶在安裝任何瀏覽器外掛時，最好三思，是否真的需要這個外掛，也不要輕信外掛的說明文字、評價和用戶留言。

- 資料來源：
  1. https://adguard.com/en/blog/fake-ad-blockers-part-2.html
  2. https://www.zdnet.com/article/google-removes-two-chrome-ad-blocker-extensions-caught-cookie-stuffing/

3. https://www.tomshardware.com/news/adblock-ublock-fake-google-chrome-browser-extensions,40422.html

2.4.5 維基百科遭 DDoS 攻擊，一度無法存取

負責維運維基百科的維基媒體（Wikimedia）德國分部，日前指出該單位的多台伺服器遭到「分散式服務阻斷攻擊」（DDoS），導致美國、英國、歐洲和中東地區的用戶，無法連線到維基百科存取其內容。

根據專門監測網路故障事件的非政府組織 NetBlocks 指出，這次攻擊事件造成的維基百科服務中斷，約持續九小時；駭侵者主要攻擊美國和歐洲境內的維基媒體伺服器。

英國國家網路安全中心（NCSC）在這次事件後也發表聲明，呼籲各公私組織應該發展更有效的因應對策，以防制日趨頻繁且嚴重的此類服務阻斷攻擊。

- 攻擊手法：分散式服務阻斷攻擊（DDoS）
- 關鍵字：Wikipedia, Wikimedia, NCSC
- 資料來源：
  1. https://twitter.com/WikimediaDE/status/1170077481447186432
  2. https://twitter.com/netblocks/status/1170174414840901632
  3. https://www.bleepingcomputer.com/news/security/wikipedia-ddos-attacks-prompt-ncsc-to-remind-of-dos-mitigation/

2.4.6 汽車行銷業者資料庫未加任何保護，近兩億車主資料曝光

資安研究人員發現一個含有近兩億名車主個資的巨大資料庫公開在網路上，未經任何保護。

資安廠商 SecurityDoscovery 的研究人員 Jeremiah Fowler 日前在網路上發現一個巨大 ElasticSearch 資料庫，內含近兩億名美國車主的多項個資，且未加上任何保護措施，可任人自由存取。

該資料庫的檔案大小高達 413 GB，資料欄位包括車主姓名、Email 地址、電話號碼、居住地址等個資，而且均以明碼儲存。

研究人員追蹤該資料庫的擁有者，發現資料庫屬於一家美國汽車行銷公司 dealerleads.com。這家公司的業務，以汽車的網路行銷與市場調查為主。

研究人員指出，這類資料庫外洩的資安事件，多半肇因於錯誤的資料庫參數設定； delaerleads.com 在得知此事後，已將資料庫設定為外界無法存取，但是否有車主因此受到影響，目前仍不得而知。

- 資料來源：
  1. https://securitydiscovery.com/dealer-leads/
  2. https://www.infosecurity-magazine.com/news/marketer-exposes-198-million-car/

2.4.7 美國再傳智慧家居裝置疑遭駭入事件

美國威斯康辛一戶人家指出，他們使用的智慧家居裝置疑似遭駭；歹徒不但控制其空調溫度控制器、播放低俗音樂，還透過監視鏡頭與其對話。

智慧家居裝置的安全性，再度引發大眾關注。住在美國威斯康辛某處的一戶人家，日前疑似遭到駭客入侵其智慧家居裝置，使得他們十分驚恐。

據媒體報導指出，歹徒不僅控制該戶的 Google Nest 空調恆溫控制器，將溫度設定到華氏 90 度（攝氏 32.2 度）的高溫，還透過設在廚房的 Google Nest 監視鏡頭播放低俗音樂，並且與受害者對話。

受害者懷疑他們家中的無線路由器遭到駭入，因此歹徒才能取得智慧家居裝置的控制權。

Google 表示在這起事件中，該公司的產品並未遭到入侵，而是用戶使用已遭破解的；Google 呼籲用戶應盡可能使用二階段驗證登入，以加強戶內各種資訊裝置的安全性。

- 資料來源：
  1. https://fox6now.com/2019/09/22/felt-so-violated-milwaukee-couple-warns-hackers-are-outsmarting-smart-homes/
  2. https://www.businessinsider.com/hacker-breaks-into-smart-home-google-nest-devices-terrorizes-couple-2019-9

2.4.8 假冒微軟 Office 365 的釣魚郵件，利用 Google 搜尋轉址功能行騙

資安研究人員發現全新釣魚郵件攻擊行動，除了假冒微軟 Office 365 登入畫面以騙取帳密之外，還透過 Google 搜尋轉址功能來隱藏行蹤。

資安公司 COdense Phshing Defense Center 的研究人員，近來發現一批全新釣魚郵件攻擊行動，會利用 Google 轉址功能隱藏詐騙登入頁面的網址。

這種手法是利用一種叫做 Percent 編碼的技巧，把非拉丁字母的網址字元轉換成以百分比符號加上兩個十六進位數字，讓瀏覽器能夠處理非英數字元的多國語言網址。

歹徒利用 Google 的轉址服務，隱藏詐騙頁面的實際網址；這樣不但能騙過郵件服務的惡意信件掃瞄器，也能讓用戶誤以為網址是來自 Google，所以不用擔心。

有些釣魚郵件業者，甚至會利用 CAPTCHA 機制，防止郵件服務的掃瞄分析機制進一步追蹤信件中的釣魚連結。

- 資料來源：
  1. https://cofense.com/threat-actors-use-percentage-based-url-encoding-bypass-email-gateways/
  2. https://www.bleepingcomputer.com/news/security/microsoft-phishing-attack-uses-google-redirects-to-evade-detection/

2.5、軟硬體漏洞資訊

2.5.1 微軟緊急修補兩個已遭大規模濫用的 0-day 漏洞

微軟日前發出緊急修補更新程式，用以更新兩個新近被發現，而且已遭駭侵者大規模濫用的 Internet Explorer 和 Microsoft Defender 中的 0-day 漏洞（CVE-2019-1366、CVE-2019-1255）。

這兩個漏洞，前者存於 IE 之中，可讓駭侵者取得系統控制權，並且執行任意程式碼，後者則存於 Microsoft Defender 中，可用來發動 DDoS 攻擊。

由於這兩個 0-day 漏洞已遭駭侵者大規模濫用，因此微軟來不及等到下個月的 Patch Tuesday 例行更新，直接針對這兩個漏洞發布修補更新。

- CVE 編號：CVE-2019-1367、CVE-2019-1255
- 影響產品(版本)：IE 9, 10, 11、Microsoft Defender 1.1.16300.1 之前版本
- 解決方案：安裝微軟最新推出的安全更新程式
- 資料來源：
  1. https://www.us-cert.gov/ncas/current-activity/2019/09/23/microsoft-releases-out-band-security-updates
  2. https://support.microsoft.com/en-us/help/4522007/cumulative-security-update-for-internet-explorer
  3. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367

3.5.2 phpMyAdmin 被發現 0-day 漏洞

資安研究人員在使用率極高的開源 MySQL 網頁管理界面 phpMyAdmin 中，發現一個中等嚴重程度的 0-day 資安濡洞，駭侵者可用以刪除受害用戶的網頁伺服器。

研究報告指出，這個 0-day 漏洞屬於典型的 CSRF 漏洞，駭侵者可以藉由發送某個特別設計的 URL 給具有管理權限，且已登入其 phpMyAdmin 系統的用戶，受者者點按該連結後，即可在受害者不知情的情形下，刪除利用 phpMyAdmin 設定的 MySQL 資料庫。

這個 0-day 漏洞雖然會刪除網頁伺服器，但並不會刪除資料庫本身或任何資料庫中的表格。

此外資安研究人員在今年六月發現此一漏洞時，立即通報給 phpMyAdmin 的維護團隊，但該團隊未能在九十天內修復此漏洞；目前該漏洞亦尚未修復。

- CVE 編號：CVE-2019-12922
- 影響產品：phpMyAdmin 4.9.0.1 在內的各已推出版本
- 解決方案：尚無，資料庫管理者應避免點按可疑連結
- 資料來源：
  1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12922
  2. https://seclists.org/fulldisclosure/2019/Sep/23
  3. https://thehackernews.com/2019/09/phpmyadmin-csrf-exploit.html?m=1

第 3 章、 資安研討會及活動

2019 CYBERSEC 101	
活動時間	2019/9/6(五)、9/20(五)、10/25(五)、11/8(五)、11/29(五)
活動地點	台北市松山區敦化南路一段 108 號 B2
活動網站	https://cybersec101.ithome.com.tw/
活動概要	 CYBERSEC 101 為全新系列研討會，藉由定期舉辦，持續對資安實務做更全面更深入的探討與交流，期能擴大 IT 與資安人員的資安視野，精進資安防禦技能，持續提升企業組織的資安防禦水平。 2019 年 CYBERSEC 101 資安實務研討會的第一場次，將以當前全球最受企業與政府矚目的「NIST Cybersecurity Framework」為主題，透過此一完整涵蓋企業五大防禦構面的資安藍圖，由資安專家帶領 IT 與資安人員，以每個月一個子題的節奏，依序探討 NIST Cybersecurity Framework 的五大資安防禦功能（Identify、Protect、Detect、Respond、Recover），完整檢視企業資安防禦的全貌，為企業資安防禦奠定持續改善的基礎。

CDX2.0 推廣活動	
活動時間	2019/09/10(二) 13:00~16:00
活動地點	臺北市和平東路二段 106 號 4 樓
活動網站	https://nchc-cdx.kktix.cc/events/cdxactivity-0910
活動概要	 雲端資安攻防平台（Cyber Defense Exercise，CDX）為科技部指導國家高速網路與計算中心（國網中心）執行「資訊安全開放資料平台研發與惡意程式知識庫維運（II）」計畫之一，平台採用雲端服務的架構進行規劃與設計，主要用以改善傳統攻防平台受限於軟硬體限制、管理與使用不易等問題，以虛擬化的架構實現攻防演練場景快速部署的可行性，提供多人多場景同時進行攻防演練之環境，並可提供模擬真實的網路環境用於攻防技術相關研究，讓參與者能夠熟悉與掌握以往曾經發生過的資訊安全事件，並從中學習資訊安全的檢測與分析技巧。

Cyber Attack Taipei Series 2019	
活動時間	2019/09/17 (二) 8:00~17:00
活動地點	台北市中山區中山北路二段 39 巷 3 號
活動網站	https://www.eventbrite.com/e/cyber-attack-taipei-series-2019-tickets-68951581035

活動概要	 **Threat Intelligence, Cybersecurity, Digital Investigation, Cyber Forensics, Artificial Intelligence, IoT, Machine Learning, BigData, Fintech** **About this Event** WHO SHOULD ATTEND • Administrators • Chief Information Security Officers (CISO) • Chief Information Officers (CIO) • Chief Technology Officers (CTO) • IT Directors • Cyber Security Heads • Senior Executives in Security • Technology and Risk Officers • Network and Information Profiles

9 月台北例會-物聯網時代的資安與隱私風險管理	
活動時間	2019/09/24 (二) 14:30~16:30
活動地點	台北市信義區基隆路一段 143 號 3 樓
活動網站	https://www.caa.org.tw/newsdetail-15994.html
活動概要	中華民國電腦稽核協會 Computer Audit Association **1.物聯網產品資安與隱私風險管理框架介紹** **2.組織採用物聯網設備之風險與管理措施** **3.組織物聯網設備管理成熟度評鑑方法介紹**

	主講講師： 姓名：李冠樟 機構：安侯企業管理股份有限公司 單位：資訊科技諮詢服務 職稱：經理 證照：CISA、CISM、CEH、ISO 27001 LA、BS 10012 LA、ISO 20000 LA、ISO 22301 LA、ITIL Foundation 專長：資訊安全管理、資訊系統稽核、個人資料與隱私保護、資訊服務管理、營業秘密保護

9 月新竹例會-機敏資料管理實務講座	
活動時間	2019/09/25 (三) 09:30~12:30
活動地點	新竹市光復路二段 153 號 2 樓
活動網站	https://www.caa.org.tw/newsdetail-15990.html
活動概要	中華民國電腦稽核協會 Computer Audit Association **1.營業秘密與智慧財產的法制要件** **2.新版營業秘密法對企業之影響** **3.營業秘密的侵害與救濟** **4.案例說明與企業應有之防護佈局** **講師：** 張紹斌 中華民國電腦稽核協會理事長/合盛法律事務所主持律師 證照 - 中華民國律師、司法官、BS 10012

第 4 章、 2019 年 9 月份事件通報概況

本中心每日透過官方網站、電郵、電話等方式接收資安情資通報，以下為各項統計數據，分別為通報地區統計圖及通報類型統計圖。

通報地區統計圖為本中心所接獲之通報中，針對通報事件責任所屬地區之通報次數比率，如圖 1 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比率，如圖 2 所示。

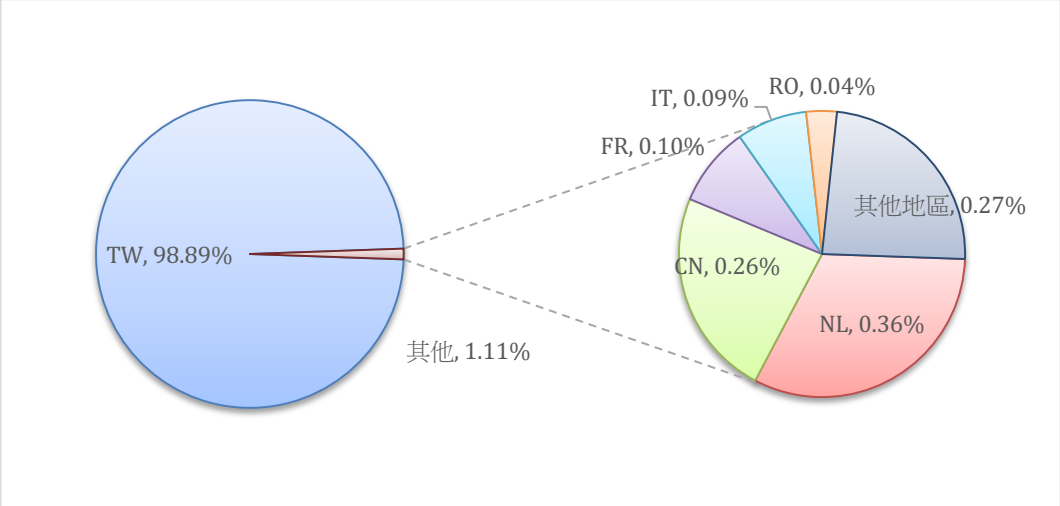


圖 1、通報地區統計圖

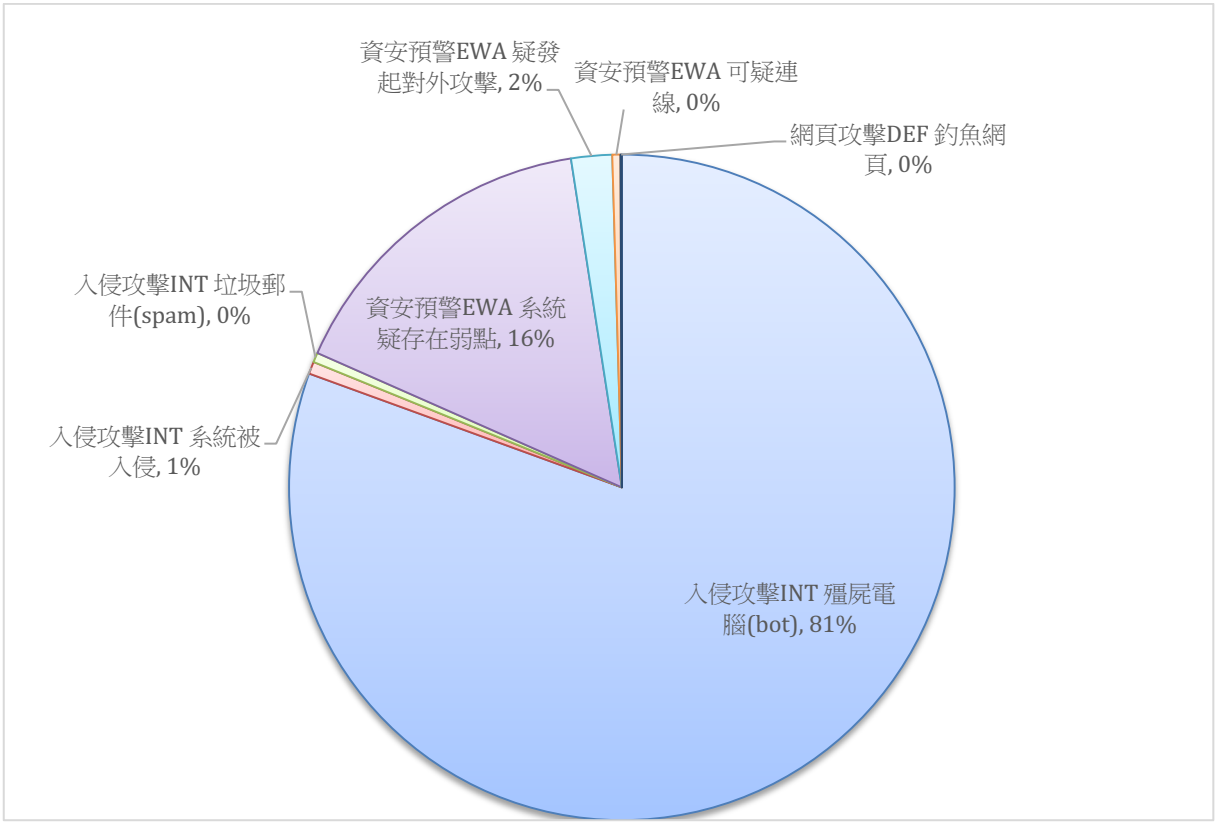

資安預警EWA 疑發起對外攻擊, 2%
資安預警EWA 可疑連線, 0%
網頁攻擊DEF 釣魚網頁, 0%
入侵攻擊INT 垃圾郵件(spam), 0%
資安預警EWA 系統疑存在弱點, 16%
入侵攻擊INT 系統被入侵, 1%
入侵攻擊INT 殭屍電腦(bot), 81%

圖 2、通報類型統計圖

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 10 月 23 日

編輯：林克容、江奕昉、張洛瑀

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/

Instagram：https://www.instagram.com/twcertcc/

Twitter：@TWCERTCC