TWCERT/CC 資安情資電子報

2019 年 7 月份

目錄

第 1 章、 封面故事

多支 Google Play 店中美肌相機 App 被發現會竊取用戶圖片，甚至導至釣魚網站

趨勢科技發現多支 Google Play 中的美肌相機類軟體，內藏惡意程式，不但會顯示詐騙廣告，將用戶導至釣魚網站，更利用各種刻意隱藏的手法，使用戶難以移除。

趨勢科技發表研究報告，指出在 Google Play 商店中上架的多支美肌相機類 Android App，內藏複雜的惡意軟體程式庫；用戶安裝使用後，會顯示全螢幕的詐騙廣告（例如假冒 Google 名義通知用戶抽中 iPhone X），甚至發送色情圖片，以拐騙用戶到釣魚網站留下個資。

這些 App 還會在安裝後，自己安裝程式清單中將自己隱藏起來，讓用戶難以移除，並且利用各種手段閃避惡意軟體或防毒程式的偵測。

這些 App 的下載用戶，主要以亞洲為最多，特別是印度；其中有三支 App 下載安裝次數超過一百萬次。在趨勢科技報告發表後，Google Play 已移除這一系列的惡意 App。

有鑑於這些 App 防不勝防，資安專家提出建議，用戶在安裝任何 App 前，應該先閱讀 Google Play 中的用戶評鑑，看看有沒有其他用戶反應 App 問題，以免受害。

- 資料來源：

1. https://blog.trendmicro.com/trendlabs-security-intelligence/various-google-play-beauty-camera-apps-sends-users-pornographic-content-redirects-them-to-phishing-websites-and-collects-their-pictures/

第 2 章、 資安小知識—惡意程式檢測 vs 防毒軟體 (下)

上期介紹了惡意程式、防毒軟體（靜態分析）以及病毒檢測（動態分析）。靜態分析是透過研究並分析程式碼內容，找出其中唯一的程式碼作為辨識特徵之病毒碼，搭配防毒軟體中之掃描功能，方能自遭受感染的電腦中，找出有問題的惡意程式。

相對於透過特徵值分析惡意程式的靜態分析方法，動態分析方法是將惡意程式放置於沙箱（SandBox）──一個幾乎與實體主機隔絕的環境──中，並於其中促使惡意程式實際執行，觀察該惡意程式的行為並記錄。動態分析本身是著重於惡意程式執行時的行為觀察，即便駭客將惡意程式的程式碼進行更動，則因其執行時仍然進行對受害電腦產生影響的惡意行為，因此不會被混淆分析，仍然可以判斷出該程式為惡意程式。

惡意程式 vs 靜態分析

在此方法中，研究者會先將惡意程式進行反編譯──亦即將惡意程式轉換回程式碼的樣態，並取得惡意程式可能執行的行為及命令等進行相關分析，研究人員會將其中特殊之程式碼片段，指定為特徵辨識用途之病毒碼，彙整之後放入防毒軟體資料庫中供使用者進行病毒防護。若電腦不幸接觸到該惡意程式，則防毒軟體在掃描到惡意程式後，會將其進行反編譯，將程式碼和資料庫中的病毒碼進行比對，若該程式擁有和病毒碼相同之程式片段，則防毒軟體會認定此為惡意程式，並且進行相關處置動作。在以上行為

中，研究人員僅是對於惡意程式中的程式碼進行「預測」，判斷此程式是否為惡意程式，因此並未真正執行惡意程式。

而惡意程式為了避免被反編譯、阻止反向工程，在其程式碼中，經常會包含「程式隱匿技術（Code Obfuscation technique）」，讓解析者無法知道該程式的運作流程和行為。程式隱匿技術原本的作用是用於一般合法軟體中，用來保護程式內容、智慧財產權等，避免軟體的商業機密被他人反編譯後，損害公司之商業利益，或是避免機密性質之內容遭到第三者的竊取和窺視。然而，此種技術卻經常被用於惡意程式中，將自身偽裝成一般正常之程式，規避防毒軟體的偵測。

除了程式隱匿技術之外，阻止軟體被反編譯的還有加殼（Packer）技術，也就是將程式碼用另一段正常的程式碼包裹，保護其中的程式碼不會輕易地被反編譯。在最初，加殼的目的主要是為防止檔案被破解，保護軟體的版權等，但是若此技術被應用於惡意程式中，便是一個防止惡意程式被破解及分析的便利工具。而這樣的加殼，會使得研究人員難以反編譯，進行近態分析動作。

除了以上兩種方法，還有一種透過加密技術(Crypter)，將程式碼進行加密，使得惡意程式難以被反編譯以及分析。在加密技術的運行下，會使得研究人員無法順利分析之外，也會因為程式碼經過加密，而規避了防毒軟體的偵測，導致電腦受到惡意程式的侵駭。

雖然靜態分析所需工具和資源較少，並且有一定的準確率，但由於靜態分析並沒有真正執行惡意程式，僅僅是分析程式碼的架構和行為，因此，只要將惡意程式中的惡意行為程式碼隱匿起來，靜態分析便難以準確偵測惡意程式。

惡意程式 vs 動態分析

相較於研究程式碼為主的靜態分析，動態分析是實際將程式在幾乎與實體主機隔絕的環境執行，並記錄該程式的行為，若有任何惡意之行為，便可以清楚判斷該程式為惡意程式，可抵禦靜態分析困難的隱匿技術、加殼及加密等，彌補靜態分析的缺陷。在動態分析方法中，多半是以建立沙箱的方式，將惡意程式在其中執行以取得更準確的惡意程式行為。然而，這種方法因需讓惡意程式實際執行，因此所需花費的時間較長，且建立沙箱以及運作所需要的資源和技術都較靜態分析高。此外，若惡意程式裡包含了偵測虛擬環境之功能，則可能被惡意程式偵測到本身處於虛擬環境中，進而不執行或不進行惡意行為以規避研究人員的分析。

為了規避動態分析，最為直接的方式便是偵測程式本身所在的環境是否為虛擬沙箱。由於虛擬化技術往往並非直接與硬體溝通，因此惡意程式便可監測到環境的行為，因而認為自己處於虛擬監測環境中，導致惡意程式停止運作或隱藏其惡意行為，待惡意程式入侵正常電腦後，方開始其惡意行為。

另一種迴避動態分析的方式，是拉長執行時間。有些惡意程式本身會有一定時間的潛伏期，例如電腦遭感染後數天才開始運作、進行惡意行為。由於無從得知、不固定的潛伏時間，即便研究人員將惡意程式放入沙箱中執行，也無法確定該程式是單純的程式或處於潛伏期，待條件滿足後，便會立刻進行竊取或破壞等惡意行為，因此，此種惡意程式對動態分析而言有一定之難度。

除上述兩種規避模式外，還有一種「無檔案攻擊」，顧名思義，這種攻擊一般無實際檔案或下載檔案，而是直接於受害電腦的記憶體中執行。由於此種攻擊無實際檔案，導致研究人員也無實際檔案可供分析，是反制動態分析的一種方式。在動態分析的過程中，一般沙箱會對內部檔案進行

隨機掃描，但無檔案攻擊因不使用檔案，使得沙箱無法掃描含有惡意之檔案；並且，此種攻擊不似其餘惡意程式將本身包裝為應用程式，透過應用程式介面(API)進行溝通和惡意行為，無檔案攻擊多半躲藏於系統執行序中，即便沙箱攔截 API 的資訊，也無從取得惡意程式的訊息；無檔案攻擊通常也包含潛伏之功能，延後惡意行為的執行，招致沙箱有限的觀察時間中，無法順利觀察到惡意程式真正執行惡意行為；甚至此種攻擊往往會移除在記憶體內的感染痕跡，使得研究人員在事後要進行鑑識分析都有其難度。

靜態分析 & 動態分析

雖然目前分析技術及設備越來越完備，以及相關工具的進化，針對大部分的惡意程式已可以順利分析。但惡意程式隨著防護及鑑識工具的提升，也會為了避免被分析而增添更多的防護功能。若僅僅透過一種分析方式，難免會因其分析特性的弱點，而產生誤判或無法處理之狀況。因此，必須透過將兩種分析方式結合、互補，方能達到最好之惡意程式防護成效。

靜態分析可能因為隱匿技術而無法判斷，然而，若將該程式放入動態分析環境中，即便該惡意程式經過加殼方式而規避了靜態分析，但該程式要執行時，勢必得自行進行解殼並開始執行，此時，便可以透過動態分析對惡意程式進行分析和判斷，取得準確的判斷結果。

相反地，當惡意程式本身有潛伏期，需數天時間方進行惡意行為。此時，則可以將其程式碼直接進行反編譯，以靜態分析方式觀察並分析，取得其病毒碼，並以此作為判斷之特徵值。

透過靜態分析及動態分析的搭配，可以有效且正確地對惡意程式進行辨識以及後續處理。

靜態分析 & 動態分析

為了有效將靜態分析(防毒軟體)與動態分析(沙箱)結合，Virus Check 系統透過國家實驗研究院高速網路與計算中心的沙箱以及趨勢科技的防毒軟體，達到全面且完整地對檔案進行分析，減少惡意程式對使用者的威脅。

首先，此系統致力於保護檔案之機密性，由於國際上檢測系統多會將使用者所上傳之檔案分享給付費使用者，導致隱私和機密的流失。

收到檔案後，系統會以防毒軟體進行檢測，同時交予沙箱進行動態分析，將靜態以及動態分析同時且互補地檢驗，以達到最佳檢測成效。

待檢驗完畢後，系統會透過風險值告知使用者該檔案可能為惡意程式之風險為多少，並且附上完整檢測報告供使用者下載。

Virus Check 相較於僅進行靜態分析之國際檢測系統，更增添了動態分析之優勢，補足了防毒軟體的不足之處，以獲得完整之分析成果。除此之外，此系統可透過上傳之檔案，建構專屬於台灣之惡意程式資料庫，完整國家資安防線。

為了提高台灣整體資安防護能量、減少感染惡意程式之風險，除了不要下載來路不明之檔案，對於下載之檔案，最好透過檢測系統完整分析，避免電腦遭到惡意程式之威脅。台灣資安能量，需要大家共同參與和努力。

- 資料來源：

1. https://www.nccst.nat.gov.tw/ArticlesDetail?lang=zh&seq=1108
2. http://140.125.45.29/courses/files/network%20security/network%20security%20ch%2016.pdf
3. https://ithelp.ithome.com.tw/articles/10188209
4. https://www.itsfun.com.tw/加殼/wiki-9332436-9719216
5. https://www.itread01.com/content/1551727225.html
6. https://paper.seebug.org/222/#33
7. http://speed.cis.nctu.edu.tw/~ydlin/miscpub/indep_study_cywu.pdf
8. https://www.easyatm.com.tw/wiki/電腦病毒
9. https://blog.trendmicro.com.tw/?p=49025

第 3 章、 資安宣導

銓敘部個資外洩，轉傳個資恐觸法

銓敘部電腦疑遭入侵，59 萬筆公務人員個資外洩，相關單位已積極偵辦中。然而，此次個資外洩事件中，據傳有使用者透過 Line 群組或社群媒體轉傳外洩之個資資料。如此惡意傳遞遭外洩個資，恐觸犯個人資料保護法，請使用者務必小心以免觸法。

在 6 月 22 日，行政院收到來自美國、英國、加拿大、澳洲及紐西蘭所組成之五眼聯盟(Five Eyes)之通報，表示由銓敘部外洩高達 59 萬筆公務員個資，被公告在美國 RaidForums 網站中，供使用者瀏覽，目前國安局已緊急要求對方將外洩之個資進行下架。

此次外洩之個資，據傳是在 2012 年 6 月初即被竊取並外洩，目前個資竊取方式還未能確實掌握，有可能是透過維修人員流出、內鬼所為、甚至遭受駭客入侵等。除此之外，調查人員也發現張貼個資的貼文者，雖使用 Google 服務中的 gmail 信箱，但其申請之 IP 卻來自於中國。由於其中除了一般公務人員的個資外，更包含了情治系統人員的相關資訊，且現今仍有兩萬八千名人員仍在職，影響範圍令相關單位不敢輕忽。

然而，此次個資外洩事件卻引發出了案外案，據傳有使用者收到相關資訊後，將外洩的 59 萬筆個資透過 Line 群組等社群媒體進行轉傳，惡意分享個人資訊。實際上，如此傳遞他人個資，恐會觸犯個人資料保護法，即便是家庭或好友等不公開的群體，仍有觸法的疑慮。依照個人資料保護法中第 41 條，將他人個人資料搜集、處理、利用，意圖為自己或第三人之不法利益或損害他人利益者，恐處五年以下有期徒刑、得併科新台幣一百萬元以下罰金。

因此使用者即使透過管道取得相關個資，建議直接刪除，不可進行其他不法用途，甚至分享給他人，都是

觸法之行為。請使用者多加注意，以免在不知情的狀況下觸犯了法律。

第 4 章、 國內外重要資安事件

4.1、資安趨勢

4.1.1 Gmail、Google 日曆等服務，已成釣魚郵件與惡意軟體有效散布管道

卡巴斯基發表研究報告，指出用戶眾多的 Gmail 和 Google 日曆等 Google 雲端服務，現在也成為釣魚郵件與惡意軟體散布的有效管道。

資安公司卡巴斯基指出，用戶眾多，使用便利的 Google 各種雲端服務，目前成為駭侵團體發動釣魚郵件並散布惡意軟體的有效管道。

該公司近來發現，包括 Gmail、Google 日曆、Google 相簿、Google 線上表單、Google Drive 和儲存空間，甚至連網站分析工具 Google Analytics，都傳出駭客利用來散布釣魚垃圾信與惡意軟體的案例。

以 Google 日曆為例，駭客可以透過發送假的行程邀請給受害者，並在邀請中置入惡意軟體連結；通常用戶對於行程邀請的防備心較薄弱，再加上日曆服務不像 Email 一樣多半備有成熟且較精準的垃圾與病毒偵測機制，因此用戶中標比例更高。

同樣的，駭客也會透過共享 Google Photos 相片，來發送夾帶惡意連結的通知信；由於通知信是用 Google Photos 的系統發出，因此用戶不易起疑。

在卡巴斯基的報告中，分享了更多利用 Google 服務發送惡意連結的案

例，頗值參考；用戶在收到任何來自 Google 服務的通知或邀請時，也應該仔細檢視發送者，來自不明發送者的邀請不要點開，疑似詐騙或夾帶惡意連結的應立即檢舉。

- 資料來源：
  1. https://usa.kaspersky.com/blog/spam-through-google-services/17799/

4.1.2 資安研究單位指出，Email 仍是最主要的駭侵攻擊目標

多家資安研究單位共同指出，雖然現今各種駭侵方式日新月異，Email 仍然是最主要且最容易的駭侵管道。

綜合各家資安研究單位針對 Email 易遭攻擊的研究資料，有以下發現：

- Mimecast 指出，過去一年以來有高達 73% 的公私營單位曾遭假冒身分攻擊並造成損失；其中 55% 的攻擊是釣魚信件。
- Mimecast 又說，同時也有 53% 的公私營單位曾遭勒贖信件攻擊；一年前的比例是 26%。
- Proofpoint 表示，2019 年第一季觀察到的惡意檔案攻擊，有 61% 和 Emotet 有關；Emotet 是一個能發動各式攻擊的 botnet，會透過垃圾郵件等方式來夾帶惡意檔案。值得注意的是，在郵件中放置惡意檔案下載連結的攻擊方式，五倍於直接夾帶惡意軟體檔案。
- Proofpoint 也說，愈來愈多攻擊事件透過社交工程發動 Email 攻擊。

- 資料來源：
  1. https://usa.kaspersky.com/blog/spam-through-google-services/17799/

4.1.3 僵屍網路（Botnet）攻擊布署，由 Windows 轉向 Linux 與 IoT 設備

資安研究指出，駭侵團體布署僵屍網路（Botnet）的主要目標，已逐漸由傳統的 Windows 主機，轉移至 Linux 與 IoT 裝置上。

資安公司 NSFOCUS（北京綠盟科技）近日發表研究報告，指出以僵屍網路發動 DDoS 大規模攻擊的形態正在改變；駭侵團體布署大批僵屍網路的對象，正由過去的 Windows 電腦逐漸轉移到為數更多的 Linux 主機與 IoT 裝置。

NSFOCUS 的報告中含蓋該公司所監測到 2018 年的各種僵屍網路 DDoS 攻擊，並且羅列以下觀察統計數字：

- 去年該公司偵測到 111,472 次僵屍網路的攻擊指令，遭攻擊的目標共有 451,187 個，較 2017 年增加 66.4%；
- 美國（47.2%）和中國（39.78%）是僵屍網路 DDoS 攻擊的全球前兩大受害國；
- 最容易受到 DDoS 攻擊的網站是線上賭博和色情網站，共遭

到 29,161 次攻擊，平均每天被攻擊 79 次；

- 被植入惡意軟體發動 DDoS 攻擊的平台，由 Windows 快速轉移到 Linux 主機和各種 IoT 裝置。

- 資料來源：
  1. https://www.helpnetsecurity.com/2019/06/20/botnets-shift/
  2. https://finance.yahoo.com/news/nsfocus-shares-botnet-trends-2018-130000923.html

4.2、 國際政府組織資安資訊

4.2.1 Telegram 遭受來自中國的大規模 DDoS 攻擊

廣受用戶歡迎的全程加密通訊服務 Telegram，日前遭到來自中國的大規模 DDoS 攻擊；由於某抗議行動參與者大量使用 Telegram 進行溝通協調，資安專家懷疑此次攻擊可能和此相關。

Telegram 在抗議行動擴大時，於其官方 Twitter 上發出警示，表示正遭大規模強力 DDoS 攻擊，部分美洲和其他國家用戶可能會發生連線不穩狀況。

Telegram 也說，該次攻擊明顯是有人發動 Botnet 進行同時大量連線；當天的攻擊時間約持續一個多小時。

據 Telegram 執行長表示，這次攻擊幾乎所有來源 IP 都屬於中國所有，攻擊規模達到每秒 200~400 Gb。

據科技媒體 TechCrunch 表示，四年前當中國開始大規模搜捕人權律師時，Telegram 也曾同步遭到 DDoS 攻擊。

- 資料來源：
  1. https://twitter.com/telegram/status/1138768124914929664
  2. https://twitter.com/durov/status/1138942773430804480
  3. https://techcrunch.com/2019/06/12/telegram-faces-ddos-attack-in-china-again/

4.2.2 CloudFlare 多個代管網站因 BGP 路由洩露，一度無法連線

全球最大級的 CDN 服務商 CloudFlare，昨日因 BGP 洩露錯誤，導致多個知名大型網站的路由被錯誤導向，服務中斷長達近兩小時。

造成路由洩露錯誤的事主，是美國大型電信公司 Verizon；該公司在進行 BGP 設定時發生錯誤，導致 CloudFlare 代管的多個大型網站流量，被錯誤導向至美國賓州某家小公司的網站。

這個錯誤導致包括 Overcast、WP Engine、Sonassi、Discord 等知名網路公司的服務中斷長達近兩小時。

這次的 BGP 路由洩露錯誤可能屬於無心之過，但 BGP 可被有心人士用來當做攔截網路流量的攻擊武器。本月初就曾發生過歐洲的行動網路通信流量被錯誤導到中國電信的事件，而且時間也長達兩小時。

- 資料來源：
  1. https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today/
  2. https://www.datacenterdynamics.com/news/bgp-route-leak-causes-cloudflare-outages-aws-issues/
  3. https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/

4.2.3 美國太空總署遭駭，500MB 火星任務等計畫檔案被竊

NASA 內部調查報告指出，有 500MB 火星任務等內部資料，遭到駭客以一台 Rasberry Pi 電腦接入內網竊走。

根據 NASA 公開的調查資料指出，此起駭侵事件發生在去年四月間；駭客將一台 Rasberry Pi 微型電腦接到 NASA 噴射推進實驗室（JPL）的內部網路中，竊取了近 500MB 的內部資料。

被竊的資料，以火星相關任務的檔案資料為主，共有 23 個檔案。

報告指出，駭客除了取走資料外，同時也入侵了 NASA 所屬的衛星通訊網路；這個通訊網路係用來與 NASA 歷來發射的太空飛行器傳輸資料之用。

去年 12 月，美國司法部控告兩名和 APT10 有關的中國人，涉及駭入 NASA 和美國海軍使用的雲端服務商；資安媒體懷疑這次駭侵事件也和中國政府支持的 APT10 有關。

- 資料來源：
  1. https://www.zdnet.com/article/nasa-hacked-because-of-unauthorized-raspberry-pi-connected-to-its-network/
  2. https://www.digitaltrends.com/computing/hackers-steal-500-mb-nasa-data-raspberry-pi/

4.2.4 美國佛州小城為求解開被加密檔案，同意支付六十萬美元贖金

美國佛羅里達州的利維拉市，決定支付駭客六十萬美元贖金，以求解開被勒贖軟體加密的市政相關檔案。

佛州利維拉市約在三星期前遭到勒贖軟體攻擊，原因疑似為一名公務人員誤點釣魚郵件的連結，導致該市市政檔案遭到加密，更造成 Email 系統停擺、政府雇員薪資無法透過轉帳發放，僅能以手開支票支付；另外消防隊也無法透過電腦接聽報案來電。

據報導，利維拉市議會投票通過以比特幣支付六十萬美元贖金，是接受多家外部顧問公司的建議而行。另外議會也決議撥款一百萬美元，購置全新的電腦系統。

近來各公私單位遭勒贖軟體攻擊的案件日趨增加，雖然美國聯邦調查局（FBI）在其網頁呼籲不要繳付贖款，但不少受害單位別無選擇。

美國政府指出，去年有兩名伊朗人涉嫌發動超過二百起勒贖攻擊，造成至少三千萬美元的損失；歹徒不法獲利高達六百萬美元，而且至今依然逍遙法外。

- 資料來源：
  1. https://apnews.com/0762caec21874fc09741abbdec0f78ab
  2. https://www.techspot.com/news/80595-florida-city-agrees-pay-ransomware-hackers-600000-unlock.html

4.2.5 美國將惡意軟體植入俄羅斯電力網路，以在網路戰中先發制人

紐約時報報導，美國國防與情報單位已將惡意軟體植入俄羅斯電力網路之中，以便在網路戰中取得優勢地位。

紐約時報指出，該報掌握的資訊指出，美國為了防止俄羅斯透過網路進行滲透，或再次發生操弄選舉情形，已經在俄羅斯的電力網路中植入惡意軟體，必要時可先發制人發動攻擊。

紐約時報指出，有兩名美國情治單位官員證實這個消息，並且指出相關單位尚未向川普總統報告此事。

川普總統得知此事後，在推特上發文否認紐約時報的報導；俄羅斯政府發言人則表示該國一直在對抗類似的人侵行為，這類行為無法傷害俄國的經滴與關鍵產業。

- 資料來源：
  1. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
  2. https://edition.cnn.com/2019/06/15/politics/us-ramping-up-cyberattacks-russia/index.html

4.2.6 美軍網路作戰司令部對伊朗武器系統發動駭侵攻擊

華盛頓郵報報導，美國總統川普批准針對伊朗飛彈射控系統的駭侵攻擊行動，並在上周四發動攻擊。

據華郵報導指出，川普總統批准這項駭侵攻擊行動，名目上是為了報復上周伊朗在阿曼灣攻擊兩艘油輪，以及擊落美軍無人機的事件。

美軍的駭侵攻擊行動在上周四展開，由美國網路作戰司令部（US Cyber Command）執行目標是伊朗用以控制火箭與飛彈發射的射控系統，使之無法運作。

與傳統以火砲為主的攻擊不同，這場網路攻擊行動並沒有造成任何人員傷亡。

消息人士指出，美國網站司令部為這類攻擊行動已經籌畫了數周到數月之久，但美國官方並未證實確有這次攻擊行動。曾服務於川普政府的白宮前資深資安官員指出，這類攻擊對美國布署在荷姆茲海峽的海軍艦艇人員有防衛作用。

- 資料來源：
  1. https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html?utm_term=.cc6605f649eb
  2. https://www.bbc.com/news/world-us-canada-48735097

4.2.7 美國海關包商遭駭，旅客相片資料疑似外洩

美國海關暨邊境保衛局於本周一指出，與該局簽約的下包廠商疑似遭到駭侵，導致通關旅客的面部與車牌相片外洩。

美國海關暨邊境保衛局大量使用各種影像監控儀器，用於通關監視與邊防安檢之用；旅客的面孔與其車牌影像也被用於出入境監控確認之上。

該局表示這次遭竊的資料，主要是以汽車進行單次入出境的旅客面孔與車牌相片，受害旅客約有十萬名之多；雖然當局表示並未發現資料在暗網上求售的跡象，但英國科技媒體 The Register 報導卻說他們發現有疑似來自該外包商的大量個資在暗網供人自由下載。

該局表示，目前確認除了相片之外，旅客其他資訊，如姓名、護照號碼等個資並未外洩；目前該局正在進行進一步的調查，但沒有透露下包廠商的名稱。

- 資料來源：
  1. https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/?utm_term=.5aaca22277c1&wpisrc=nl_cybersecurity202&wpmm=1
  2. https://www.theregister.co.uk/2019/05/23/perceptics_hacked_license_plate_recognition/

4.2.8 美國各種公共事業遭高危險駭侵團體鎖定

資安研究單位指出，某些全球最危險的駭侵團體，顯已鎖定包括電力與石化產業在內的美國重要公用事業，列為駭侵攻擊目標。

資安公司 Dragos 的研究人員指出，一個稱為「Xenotime」的駭侵團體，自去年開始便鎖定美國的部分供電網路，伺機發動攻擊。

這個 Xenotime 駭侵團體，於兩年前曾針對沙烏地阿拉伯的石油化學工廠發動駭侵攻擊，成功破壞多個石油與瓦斯廠的運作。Dragos 指出，Xenotime 接下來的目標，極可能是美國與亞太地區的能源基礎設施。

資安專家指出，該駭侵團體可以用一個名為「Triton」的強大惡意軟體，入侵石油與電力公司的系統並造成破壞，而且不惜造成生命財產損失。這個惡意軟體係針對石油與電力公司使用的電腦系統進行客製。

- 資料來源：
  1. https://www.eenews.net/stories/1060575609
  2. https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html

4.2.9 美國情治單位成功測試利用 BlueKeep 漏洞，於目標電腦上執行任意程式碼

美國國土安全部的資安小組，已經發展出透過 WIndows 的 BlueKeep 漏洞遠端執行任意程式碼的模擬攻擊軟體，並且測試成功。

美國國土安全部表示，目前多個利用 BlueKeep 漏洞的惡意軟體，多半用以發動 DDoS 攻擊，意圖癱瘓被攻擊對象；但該部轄下的資安單位，已經成功發展出利用 BlueKeep 漏洞，以遠端執行程式碼的惡意軟體。

該單位在本周一發布公告，指出針對 Windows 2000 電腦的 BlueKeep 遠端程式執行模擬攻擊已告成功。Windows 2000 電腦並不在先前微軟發布 BlueKeep 修補程式的支援對象內。

資安專家指出，可進行遠端程式執行的 BlueKeep 惡意軟體，將有可能如同 2017 年的 WannaCry 勒贖攻擊一樣，引發全球性的資安危機。

美國國土安全部稍早也曾發布公告，強烈建議 Windows 各版本用戶盡速進行安全更新，以修補 BlueKeep 漏洞。

- 資料來源：
  1. https://www.us-cert.gov/ncas/alerts/AA19-168A
  2. https://techcrunch.com/2019/06/05/nsa-advisory-bluekeep-patch/
  3. https://techcrunch.com/2019/06/17/cisa-bluekeep-working-exploit/

4.3、 社群媒體資安近況

4.3.1 Facebook 開發的兩支 WordPress 插件程式，遭爆內含資安漏洞

資安研究人員發現 Facebook 為 WordPress 開發的兩支插件擴充程式，內含 0-Day 漏洞，無法阻擋 CSRF/XSRF 攻擊。

據該研究人員通報，出現漏洞的兩支由 Facebook 開發的 WordPress 插件程式，一支是 Messenger Customer Chat，另一支是 Facebook for WooCommerce，各有二十萬和二萬個安裝次數。

這兩支插件程式的漏洞在於未能檢測並阻擋跨站請求偽造攻擊（Cross-Site Request Forgery, CSRF/XSRF），讓不同網站可以偽裝成用戶本人以進行各種操作。

目前 Facebook 已經修復這兩支插件，但由於發表這兩個漏洞的資安研究者並沒有依照慣例，搶在修補程式發布前就公告漏洞資訊，因此也引起資安與開發社群的批判。

- 資料來源：
  1. https://threatpost.com/irked-researcher-discloses-facebook-wordpress-plugin-flaws/145771/
  2. https://www.pluginvulnerabilities.com/2019/06/17/automattic-is-having-woocommerce-install-by-default-an-insecure-plugin-by-facebook/
  3. https://www.pluginvulnerabilities.com/2019/06/17/facebooks-wordpress-plugin-messenger-customer-chat-contains-an-authenticated-settings-change-vulnerability/

4.3.2 新型釣魚詐騙活動，以加密訊息為由，騙取用戶帳號密碼

資安專家發現網路上出現新型態釣魚詐騙活動，以解開加密訊息為由，騙取用戶的帳號與密碼等登入資訊。

資安專家 Lawrence Abrams 指出，最近發現一種新型態的網路約魚詐騙；受害者會收到偽裝成系統通知信件的釣魚郵件，偽稱有一封加密的訊息寄送給你，需要登入才能讀取內容。

用戶一旦上當，點按登入按鈕後，就會被導向到假的 Microsoft One Drive 登入頁面；用戶輸入的帳號與密碼等登入資訊，就會遭駭客取得。

資安專家提醒用戶，注意不明的系統通知信，如果發現寄送地址有問題，就應提高警覺，不要任意輸入登入資訊；另外儘可能啟用二階段登入驗證，以確保安全。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/phishing-scam-asks-you-to-login-to-read-encrypted-message/

4.4、 軟體系統資安議題

4.4.1 全球電信業者疑遭駭侵團體滲透，長期竊取通聯資料

資安專家指出，全球超過十家大型電信業者疑遭駭侵團體 APT10 長期滲透，大量通聯資料已遭竊。

資安研究單位 Cybereason 日前發布研究報告，指出全球至少有十家以上電信業者，長期遭到 APT10 駭侵團體攻擊，竊取大量通聯資料。

據報告指出，在這個稱為「Operation Softcell」的長期攻擊行動中，遭竊的資料以對話的 Metadata 為主，包括每通電話的來電時間、持續時間、日期、手機所在基站的位置等等，但不包含對話內容。

報告也指出，駭侵行動的攻擊非常深入，駭客有能力在任何時間直接癱瘓受害電信業者的行動電話服務；但攻擊的主要目的在於監聽並竊取資料，而非阻斷服務。

報告沒有點名受害的十家電信業者，但這些業者遍及歐洲、亞洲、非洲與中東地區；北美電信業者尚未受害。

Operation Softcell 攻擊行動使用的手法十分純熟先進，透過技術比對，Cybereason 懷疑這次攻擊行動係由與中國政府關係密切的 APT10 駭侵團體所為。

- 資料來源：
  1. https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-

campaign-agahttps://techcrunch.com/2019/06/24/hackers-cell-networks-call-records-theft/inst-telecommunications-providers
2. https://techcrunch.com/2019/06/24/hackers-cell-networks-call-records-theft/
3. https://www.theverge.com/2019/6/25/18744020/operation-softcell-hack-call-detail-records-apt10-cybersecurity-cell-network-providers

4.4.2 Linux 主機新威脅：HiddenWasp

資安研究單位發現一個專門攻擊 Linux 主機的新惡意軟體 HiddenWasp，幾乎可以躲過所有防毒系統偵測，造成極大威脅。

資安公司 Intezer 發表研究報告指出，該公司的研究團隊發現一隻前所未見的新型惡意軟體，專門攻擊 Linux 主機，而且現今所有防毒軟體均無法偵測。

這隻被取名為 HiddenWasp 的惡意軟體，並不像最近常見的惡意軟體一樣著重在虛擬貨幣挖礦或 DDoS，而是用來進行遠端遙控。

根據分析結果，研究人員認為 HiddenWasp 使用許多已經開源的惡意軟體程式碼，和許多源自中國的惡意軟體也有相當類似的特徵。

Intezer 的報告中詳述了 HiddenWasp 的感染途徑與運作方式，提供資安人員參考防範。

- 資料來源：

1. https://www.intezer.com/blog-hiddenwasp-malware-targeting-linux-systems/
2. https://www.securityweek.com/sophisticated-hiddenwasp-malware-targets-linux

4.4.3 Netflix 發現 FreeBSD 和 Linux 的 TCP 安全漏洞

Netflix 的研究人員發表研究報告，指出多個 FreeBSD 與 Linux 核心的 TCP 安全漏洞。

Netflix 的報告指出，新發現的 TCP 安全漏洞與「最大分段大小」（Maximum Segment Size, MSS）與「TCP 選擇確認」（Selective Acknoledgement, SACK）功能有關。

其中最嚴重的安全漏洞，稱為「SACKPanic」，係透過操弄一連串的 SACK 指令，引發整數溢位錯誤，最後導至 Linux 發生核心錯誤（kernel panic）。

Netflix 在 GitHub 中發表的公告，內含各個安全漏洞的修補指南或暫時性解決方案，請使用 Linux 或 FreeBSD 主機的管理員注意並安裝更新。

- 資料來源：
  1. https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md
  2. https://www.computing.co.uk/ctg/news/3077598/netflix-warns-of-several-new-tcp-networking-vulnerabilities

4.4.4 MacOS 0-Day 漏洞：駭客執行惡意程式碼並假造滑鼠點擊

資安專家發現 MacOS Mojave 最新 0-Day 漏洞，駭客可製造假的滑鼠點擊，讓作業系統以為惡意軟體取得用戶授權執行。

資安專家表示，這個新發現的 MacOS Mojave 0-Day 漏洞，是用來跳過作業系統對來源不明軟體的安裝限制之用。

在用戶安裝不明來源的軟體時，MacOS 會跳出視窗，要求用戶授權系統執行該軟體，但遇到 Apple 認證開發者發行的軟體時，就沒有這個步驟。

研究者利用這個特性，成功把受信任軟體改寫成惡意軟體，以跳過授權畫面；並且利用該程式進行各種惡意操作；例如偷偷打開麥克風進行竊聽；而為了避免用戶查覺畫面上出現的麥克風啟動訊息，該惡意軟體可透過假造滑鼠點擊來啟動休眠模式。

該研究者已經將此漏洞向 Apple 通報。

- 資料來源：
  1. https://threatpost.com/macos-zero-day-malicious-code/145259/
  2. https://www.wired.com/story/apple-macos-bug-synthetic-clicks/

4.4.5 微軟發出警訊：現正發生利用 Office 漏洞的大規模垃圾郵件攻擊

微軟資安專家發出警訊，指出目前正有一場大規模垃圾郵件攻擊事件，會夾帶內含惡意程式碼的 RTF 檔案。

微軟資安專家指出，這些垃圾郵件中夾帶的 RTF 檔，內含多種不同語言的程式碼；一但用戶開啟 RTF 檔，程式碼就會在用戶無法查覺的情形下自動執行。

惡意程式碼執行後，會安裝一個後門木馬程式，導致用戶的資料外流，甚至遭遠端遙控。目前受攻擊的以歐洲用戶為主。

微軟指出，這波垃圾信攻擊使用的 Office 漏洞編號為 CVE-2017-11992，是屬於比較老舊的漏洞；雖然微軟已在 2017 年十一月發行的安全更新修補此一漏洞，但據信仍有許多用戶並未安裝更新程式。

據卡巴斯基發表的報告指出，這個 CVE-2017-11992 漏洞仍然高居 2018 年惡意軟體利用率的榜首。

- 資料來源：
  1. https://twitter.com/MsftSecIntel/status/1137118977983897600
  2. https://www.zdnet.com/article/microsoft-warns-about-email-spam-campaign-abusing-office-vulnerability/

4.4.6 駭侵團體開始大規模網路掃瞄仍有 BlueKeep 漏洞的 Windows 電腦

資安公司發現已有駭侵團體開始大規模進行網路掃瞄，試圖找出仍未更新修補 BlueKeep 漏洞的 Windows 電腦。

微軟在兩星期前破天荒針對 Windows XP、WIndows Vista、Windows 7 等早已停止支援的作業系統，提供 BlueKeep 漏洞的安全修補更新；這是因為 BlueKeep 漏洞可能造成嚴重的感染，駭客不但能遠端遙控受害電腦，更能進行大量感染。

雖然微軟和眾多資安單位大力宣傳，希望用戶都能安裝修補程式，但仍有不少電腦未能更新；資安公司 Panda 更發現已有駭侵組織開始在網路上大規模掃瞄電腦，試圖找出尚未更新的攻擊對象。

Panda 指出至少有六個駭侵團體已經發展出利用 BlueKeep 漏洞的惡意軟體，而且至少有兩個已被資安研究單位進行徹底剖析；Panda 表示雖然目前只偵測到掃瞄行為，但該漏洞被駭侵團體用來大舉攻擊，也只是時間早晚的問題。

- 資料來源：
  1. https://www.pandasecurity.com/mediacenter/security/bluekeep-windows-vulnerability-scan/
  2. https://www.zdnet.com/article/intense-scanning-activity-detected-for-bluekeep-rdp-flaw/

4.4.7 又出現針對 Windows RDP 發動暴力嘗試攻擊的 Botnet

資安公司再度發現一個針對啟用 RDP（遠端桌面遙控）服務的 Windows 主機進行暴力嘗試法進行攻擊的 Botnet，稱為 GoldBrute。

這個名為 GoldBrute 的惡意軟體，針對網路上 150 萬台保護薄弱的 Windows RDP 主機進行暴力嘗試攻擊。

資安公司 Morphus Labs 的專家分析 GoldBrute 指出，這個惡意軟體會掃瞄網路上的 Windows RDP 主機，並且回報攻擊報告；然後該惡意軟體會挑出攻擊清單，發動 Botnet 從多個不同 IP 進行攻擊，每次攻擊僅使用一組帳號密碼，試圖登入目標主機。

研究人員修改該惡意軟體的程式碼，找出 GoldBrute 主要發動攻擊來源的分布地圖；地圖顯示被用以攻擊的 IP 來源，來自中國的最多，也有不少來自南韓、台灣、美國、英國和法國。

- 資料來源：
  1. https://morphuslabs.com/goldbrute-botnet-brute-forcing-1-5-million-rdp-servers-371f219ec37d
  2. https://www.bleepingcomputer.com/news/security/new-goldbrute-botnet-is-trying-to-hack-15-million-rdp-servers/

第 5 章、 資安研討會及活動

TANET 2019 - 臺灣網際網路研討會 資訊展望 X 5 新啟航	
活動時間	2019/9/25 – 2019/9/27
活動地點	高雄國際會議中心
活動網站	https://tanet2019.nsysu.edu.tw/index.php
活動概要	TANET2019 臺灣網際網路研討會以「資訊展望、5 新起航」為主題。因科技的日新月異，使物聯網絡擴大成熟，經濟和生活將迎來重大變革，同時影響智慧校園的發展，也為教學形式上碰撞出新的火花。本次大會圍繞著五大主軸「物聯新通訊、智慧新生活、雲端新服務、資安新防護、軟體新應用」擴展，全方面探討物聯網絡時代帶來的關鍵課題。 5 新議題延伸的子議題涵蓋 5G 網路通訊、人工智慧及其應用、前瞻資安研發、網路規劃建置、物聯網(IOT)、深度學習、網際網路技術、區塊鏈、軟體工程等多達 55 個領域，將徵求各方資訊從業人員於本次大會發表優質論文，進行深度探索，交流切磋。大會也將邀請產、官、學界資深專家進行精彩的專題演講，以及各類議題討論、論壇分享、資安體驗營、戶外參訪等活動，藉由不同交流形式，共覽學術面及實務面的最新技術發展，使與會者從 5 新啟航，激發創意思維，共同展望智能時代的美麗新境界。


TANET 2019
TANET2019
臺灣網際網路研討會
Taiwan Academic Network Conference
暨資訊工程X智慧計算學門成果發表會
資訊展望、5新啟航
會議日期：2019/9/25-27
會議地點：高雄國際會議中心ICCK
TANET2019臺灣網際網路研討會以「資訊展望、5新起航」為主題。因科技的日新月異，使物聯網絡擴大成熟，經濟和生活將迎來重大變革，同時影響智慧校園的發展，也為教學形式上碰撞出新的火花。本次大會圍繞著五大主軸「物聯新通訊、智慧新生活、雲端新服務、資安新防護、軟體新應用」擴展，全方位探討物聯網絡時代帶來的關鍵課題。
5新議題延伸的子議題涵蓋5G網路通訊、人工智慧及其應用、前瞻資安研發、網路規劃建置、物聯網(IOT)、深度學習、網際網路技術、區塊鏈、軟體工程等多達55個領域，將徵求各方資訊從業人員於本次大會發表優質論文，進行深度探索，交流切磋。大會也將邀請產、官、學界資深專家進行精彩的專題演講，以及各類議題討論、論壇分享、資安體驗營、戶外參訪等活動，藉由不同交流形式，共覽學術面及實務面的最新技術發展，使與會者從5新啟航，激發創意思維，共同展望智能時代的美麗新境界。
活動網站：
https://tanet2019.nsysu.edu.tw
指導單位：教育部、科技部
主辦單位：國立中山大學
協辦單位：財團法人臺灣網路資訊中心
國家高速網路與計算中心
中華民國資訊安全學會
科技部工程司工程科技推展中心

新加坡資安市場解密講座: 台灣資安浴血東南亞叢林戰鬥之起點	
活動時間	2019/7/26
活動地點	臺北市大安區和平東路二段 106 號 11 樓
活動網站	https://ievents.iii.org.tw/eventS.aspx?t=0&id=547
活動概要	● **台灣資安浴血東南亞叢林戰鬥之起點**

	獅城新加坡，2005 年即開始推動資安政策，2015 年成立隸總理辦公室的網路安全局，宣示網路安全是國家推動的政策方針之一，須從防護、創新以及夥伴關係三方面著手。新加坡也將扮演東協網路安全的促進者，推動打造東協與新加坡網路安全卓越中心。 基於新加坡的關鍵定位，本會特別邀請 Accrete Innovation 創辦人 Edmas Neo 先生來台傳授心法，協助國內資安業者爭取國際資金投資，提昇其接軌國際市場之能量。 Edmas Neo 先生擁有超過 20 年的產業經驗，橫跨私人公司與政府部門，擔任科技、創新、創業、及策略顧問，他曾在 IBM 擔任資安顧問 (Certified Solution Expert)，負責金融、醫療及政府客戶。之後加入政府 IDA(Infocomm Development Authority)以及 Infocomm Investments，投入各種加速器計劃，包括 SEA Anchor 和 TAGPASS 等，有效推動新加坡、韓國和台灣 100 多個創業團隊在國際市場上的拓展。並且在他擔任 創業行動社群 Action Community for Entrepreneurship (ACE) 執行長的期間，ACE 國際中心成功將其足跡擴展到曼谷和中國。吸引來自 16 個城市的合作夥伴，創建了一個超過 25,000 家創業公司的網絡，為區域生態體系帶來了巨大的價值。

New Attacks against Blockchain and 5G Networks	
活動時間	2019/7/29
活動地點	台北市松山區民生東路四段 133 號科技服務大樓 1 樓 101 會議室
活動網站	https://ievents.iii.org.tw/eventS.aspx?t=0&id=585
活動概要	● **資安 Rank-One 研討會常客講師** ■ 國立新加坡大學 Min Suk Kang 助理教授 ■ Main Research： Internet denial-of-service problems, cellular network security, and Internet privacy.

	■ Recent Publications： 2019“ Practical Verifiable In-network Filtering for DDoS Defense” 2019“SurFi: Detecting Surveillance Camera Looping Attacks with Wi-Fi Channel State Information” ● **國際最新攻擊技術分享：** 5G 與區塊鏈最新型態攻擊，與可行解決方案建議 ● **國內無線射頻資安需求交流：** 邀請對無線射頻資安有興趣的產學研究對象，一同探討 5G 世代下的射頻安全訊息 

DEF CON 27	
活動時間	2019/8/8 – 8/11
活動地點	Paris Las Vegas Las Vegas, NV 89109, US
活動網站	https://www.defcon.org/
活動概要	● **The DEF CON 27 Theme: 'Technology's Promise'：** DEF CON 26 was about the inflection point between disorder and dystopia - the moment before the point of no return. The DEF CON 27 theme, in a way, responds to '1983' with new questions. What does it look like when we make the better choice? What kind of world do we hack together in the sunniest timeline? How does our real best-case scenario compare to the future we've been dreaming

of for generations?

Extra consideration will be granted for submissions that tie into this year's theme. We want you to hear about your hacks and research, and how will it relate to the discussions below.

1) **Cypherpunk and "engineering out of the problem".**：

Tim May was once quoted saying anonymity online would "alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret." At the time his manifesto was for "both a social and economic revolution" and so began the newly formed "Cypherpunks". Cypherpunks invented cryptography with the aim of abolishing big brother, but 30 years later we have big corporations in their place. Large corporations have insured that the 21st century hasn't come without compromises.

Crypto-anarchism is still alive and well today in well known examples like Tor, Freenet, cryptocurrencies, etc. Tell us what you're doing now to circumvent the future we're living in? Corporations are developing advanced facial recognition and becoming "the new big brother". Social media is exchanging a false sense of freedom at the expense of a total removal of anonymity. The Cypherpunk ethos will have to adapt now that we have merged the "instagram-able" life, biometrics, ML, IOT, and micro-targeting. To build a future that doesn't limit our love of modern technology and socialization at the expense of freedom will require decentralization and anonymity technology breakthroughs. What are you doing to engineer your way out of these problems?

2) **"Keep InfoSec out of Hacking"**：

DEF CON wants to support the culture of hacking. Between the TV interviews and the assessments we are still the same people with funny names threading the eye of the needle to make the next breakthrough. Hackers have become mainstream, seemingly to leave the underground to make a "legitimate" living. The industry has developed policies for ethical hacking, multimillion dollar pentesting orgs, bug bounty programs, and set the foundations of security for behemoth corporations. Being paid for hacking was the dream, but now it is an industry unto itself that focuses predominantly on enterprise.

DEF CON is a hacker con, not an InfoSec conference. Hackers are more focused on the joy of discovery, irreverence, novel if impractical approaches. InfoSec is more focused on enterprise, frameworks, and protecting the interests of share holders. There is great value in both types of content, but our con is a hacker con by design.

Activities that enable the hacker mindset and demonstrate how to master a certain technique are always going to be selected over a great enterprise InfoSec talk. DEF CON has always tried to provide a way to amplify the work of hackers, to create a venue for research that allows for others to

	grow. The idea that technology should be free was written into the subtext of "The Hacker Manifesto" and is just as valid today as it was 33 years ago. 3) **We want the computer from Star Trek, what we're getting is HAL 9000.**： At DEF CON 24 we hosted DARPA's Grand Cyber Challenge, a challenge to the innovation community with a $2M prize to build a computer that can hack and patch software with no one at the keyboard. This was a lot of fun, and yet there were whispers among us of a future where artificial intelligence will render some human jobs irrelevant. We can see ourselves approaching an event horizon of automation. This technology is not without a price, but how do we get to the utopian world where we ask a computer to make us a cup of earl grey without landing ourselves in a black mirror dystopia? Engineers are developing smart home devices with disembodied voices, while hackers are quick to shout tropes of "NSA listening devices". Is the reckless misuse of technology leading us to a dark future? What can hackers do to help achieve the sunniest timeline? Above are some suggested topics that loosely align with the theme, we consider all talk subjects. If your talk doesn't fit in one of these topics don't worry, the suggested themes are just a starting point. We've dozens of speaking slots, the tracks will be filled with a clustering of subjects; hardware hacking, lock picking, mobile hacking, reverse engineering, legalities of hacking, and more.

CLOUDSEC 企業資安高峰論壇 2019	
活動時間	2019/8/21
活動地點	台北國際會議中心 (TICC)
活動網站	https://www.cloudsec.com/tw/
活動概要	CLOUDSEC2019 **PICTURE THIS! See. Secure. Go Further.** **擘畫企業安全藍圖，帶您看更廣，走更遠**

	期許每天都能機敏地運用日益複雜和不斷移轉的 IT 環境，提升生產力... 期望企業能掌握威脅、抵禦攻擊，即使面對事件也能迅速恢復到日常... 形塑網路安全為一個戰略，運籌帷幄，敏銳地管理不斷變化的威脅和風險... 這一切令人嚮往，而您的企業，是否已具備如此能力？ 「CLOUDSEC 企業資安高峰論壇 2019」將帶您在混亂的世代中看得更清楚， 掌握多樣化的技術和洞悉複雜的ＩＴ架構，從不同的角度、不同產業案例，看到更多事件的蛛絲馬跡；即使面對挑戰也能從容以對。 CLOUDSEC 企業資安高峰論壇，是趨勢科技發表最新資安趨勢、技術和願景的時刻，如果您曾經參與，2019 更不能錯過。

第 6 章、 2019 年 6 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。

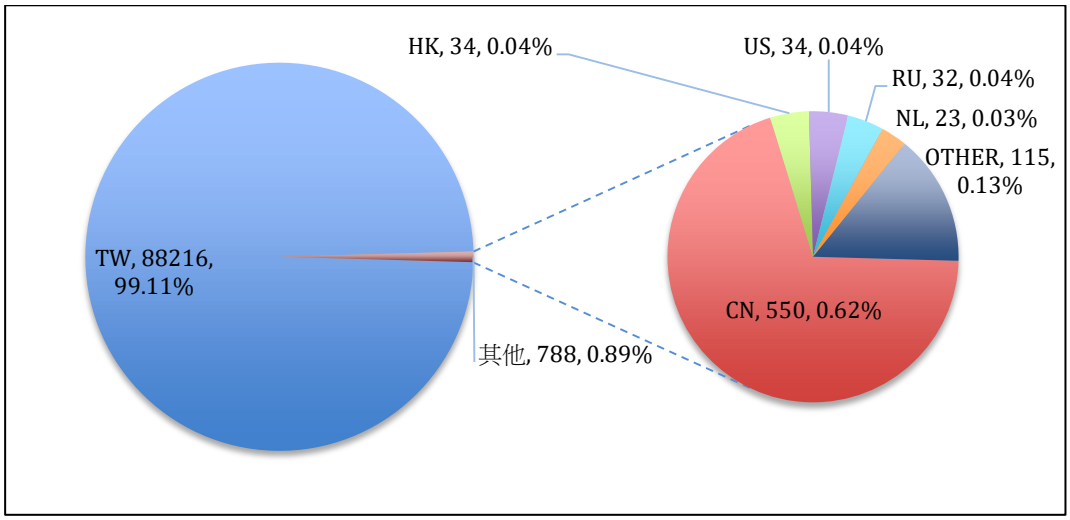

圖 1、通報地區統計圖

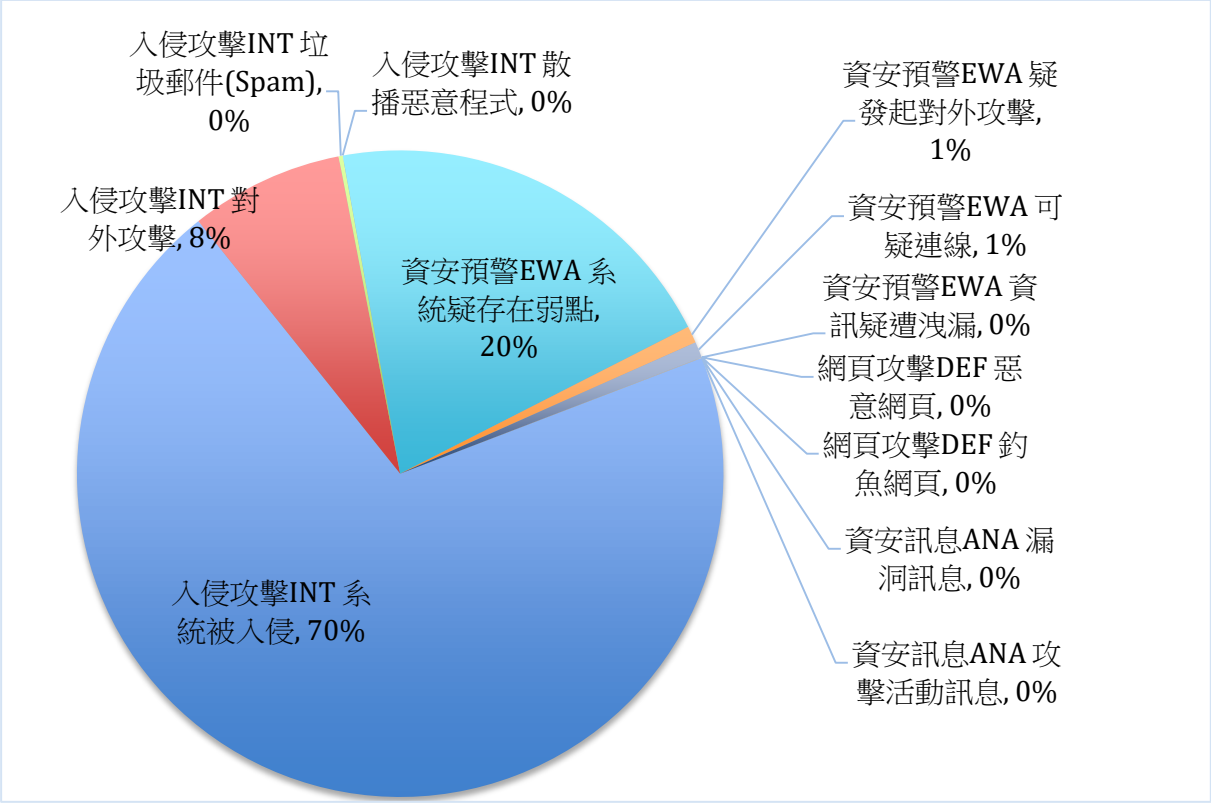
入侵攻擊INT 垃圾郵件(Spam), 0%
入侵攻擊INT 散播惡意程式, 0%
資安預警EWA 疑發起對外攻擊, 1%
入侵攻擊INT 對外攻擊, 8%
資安預警EWA 可疑連線, 1%
資安預警EWA 系統疑存在弱點, 20%
資安預警EWA 資訊疑遭洩漏, 0%
網頁攻擊DEF 惡意網頁, 0%
網頁攻擊DEF 釣魚網頁, 0%
資安訊息ANA 漏洞訊息, 0%
入侵攻擊INT 系統被入侵, 70%
資安訊息ANA 攻擊活動訊息, 0%

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 7 月 12 日

編輯：林克容、黃耀輝、江奕昉

服務電話：0800-885-066

電子郵件：twcert@cert.org.tw

官網：https://twcert.org.tw/

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

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

Twitter：@TWCERTCC

電子報線上閱覽：https://blog.twnic.net.tw/