TWCERT/CC 資安情資電子報

2020 年 3 月份

目錄

第 1 章、 封面故事

知名 YouTube 電玩直播頻道被盜，用以進行加密貨幣詐騙

一個擁有 188 萬訂戶的大型 YouTube 電玩直播頻道被盜，之後被用來進行比特幣詐騙活動。

擁有 188 萬名訂戶的大型 YouTube 電玩直播頻道 Neebs Gaming 被駭侵者挾持；隨後該頻道便假冒全球最大加密貨幣交易平台 Coinbase 之名，進行比特幣詐騙活動。

在該 YouTube 帳號被盜後，其帳號名稱就被改為 Coinbase Pro，原本的影片內容也全遭刪除。

據媒體報導指出，詐騙活動是假冒 Coinbase CEO Brian Armstrong 之名進行的；影片中宣稱 Coinbase 正在進行史上最大比特幣空投活動，總獎額高達一萬枚比特幣；參加者只要將自己手上的比特幣轉帳到某個加密錢包網址中，就可以獲得最多十倍的獎金。

該詐騙直播還盜用了 Brian Armstrong 在其他場合的演說影片，加以移花接木以取信於人。一共有 95,000 觀看了詐騙直播影片。

影片中提到的比特幣轉帳用錢包，在詐騙影片播出後收到了二十筆轉帳，轉帳總額達到 2.465 枚比特幣，相當於美金 24,000 元。

Neebs Gaming 在 YouTube 頻道被盜後，立刻向 YouTube 平台反應。

先前 YouTube 上也發生過類似的加密貨幣詐騙事件。2018 年時有詐騙者誘使用戶點擊下載惡意軟體，以盜取用戶的電腦計算資源進行挖礦運算，替詐騙者賺取 Minero 幣；上個月也有一個擁有八十多萬訂戶的 YouTube 頻道被盜，竊盜者運用該頻道進行以太幣詐騙活動。

- 資料來源：
  1. https://twitter.com/NeebsOfficial/status/1228723251863486465
  2. https://www.reddit.com/r/CryptoCurrency/comments/f4u6tl/beware_of_the_scam_that_is_live_now_on_youtube/
  3. https://www.hackread.com/popular-youtube-gaming-channel-hacked-crypto-scam/

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、APT 駭侵組織假冒知名媒體記者名義，對重要人士發動釣魚攻擊

資安專家指出，有伊朗 APT 駭侵組織針對重要人士發動釣魚郵件攻擊，手法是假冒知名媒體記者的名義進行約訪。

資安廠商 Certfa Lab 的研究人員於本周三發表調查報告，指出該公司發現由伊朗支持的 APT 駭侵團體「Charming Kitten（迷人小貓）」，最近針對政治人物或人權運動家進行 Email 駭侵與監聽攻擊；而攻擊的手法，是透過假冒為華爾街日報或紐約時報的記者，對目標對象發出訪問邀約，進而對目標發動釣魚郵件攻擊。

這波釣魚郵件攻擊的目的，在於取得重要政治人物或人權運動家的 Email 往來內容、通訊錄名單，甚至 Email 的帳號密碼。

這些用來進行釣魚攻擊的郵件，會在郵件中放入看起來極像來自華爾街日報或紐約時報的真實網址，但實際上卻會導向惡意軟體頁面；一旦受害者點擊，即有可能洩露部分基本資訊，例如使用裝置名稱、作業系統名稱與版本、IP 位址等訊息。

然後受害者會收到一個假冒為訪問題綱的連結，並且會連到一個放在 Google Sites 的網頁；如果用戶不疑有他，繼續點頁面中的連結，就會被導到一個假

冒的登入頁面，可能被騙走重要的帳號和密碼。

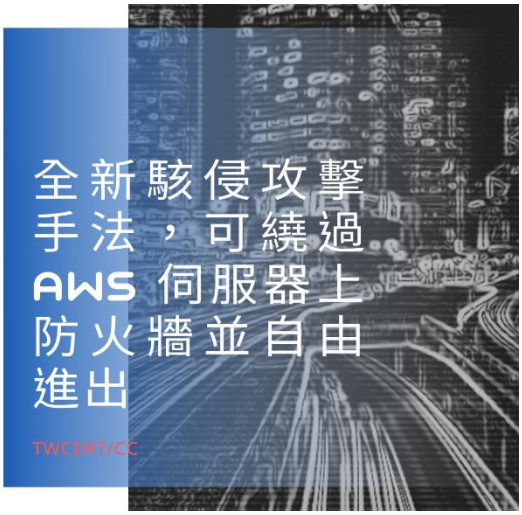
Certfa 的專家自 2018 年開始監控 Charming Kitten，並指出該駭侵團體曾經自行開發利用 Windows 資安漏洞的惡意軟體，進行駭侵攻擊的工具。

Certfa 在報告中指出，Charming Kitten 長期鎖定的駭侵對象包括美國、英國、沙烏地阿拉伯與多個歐洲國家的政府單位、智庫、學術單位，試圖竊取這些單位內部的機敏資訊，或鎖定重要人士進行駭侵攻擊。

微軟和另一家資安公司 ClearSky 的資安研究人員，則指出該駭侵團體曾試圖駭入美國總統川普連任競選活動使用的 Email 帳號。

- 資料來源：
  1. https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/
  2. https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/
  3. https://threatpost.com/charming-kitten-uses-fake-interview-requests-to-target-public-figures/152628/

2.1.2、全新駭侵攻擊手法，可繞過 AWS 伺服器上防火牆並自由進出



一種全新的駭侵攻擊手法，可利用植入系統的 Rootkit 避開 AWS 的防火牆設定進行資料竊取或其他攻擊。

資安廠商 Sophos 發表研究報告，指出發現一種全新且複雜成熟的駭侵攻擊手法，可以繞過 Amazon Web Service 內建的資安防護機制，進行資料竊取或其他形式的攻擊。

這種攻擊手法稱為「Could Snooper」，原理是設法將一個 Rootkit 低階後門惡意軟體植入 AWS 中的 Linux 伺服器，成功感染伺服器之後，該 Rootkit 便會透過變造的網路封包，以「尾隨」正常封包的手法，光明正大地通過防火牆所允許的傳入通訊埠，將內部的機敏資訊傳到外部，甚至從外部進行遙控，形成後門。

Sophos 說，該公司發現一些 AWS 伺服器的防火牆雖然只開放了 Web 通訊所需的通訊埠 80 和 443，但仍偵測到通訊埠 2080 和 2053 有不正常的 TCP 封包傳輸，因而發現這個攻擊手法。

Sophos 表示，這個後門 Rootkit 係基於 Gh0st RAT 惡意軟體的程式碼，該公司也已經偵測到 AWS 中的 Linux 和 Windows 伺服器都遭到類似 Rootkit 的攻擊；鑑於該手法的複雜度，有理由相信這類攻擊和 APT 駭侵團體有關，但尚無直接證據可歸因於特定的 APT 駭侵團體。

- 資料來源：
  1. https://news.sophos.com/wp-content/uploads/2020/02/CloudSnooper_report.pdf
  2. https://news.sophos.com/en-us/2020/02/25/cloud-snooper-attack-bypasses-firewall-security-measures/

2.1.3、新形態勒贖攻擊：以大量假點擊致使受害者 Google AdSense 遭停權

針對網站擁有者發動的新型態勒贖攻擊，威脅將以大量無效廣告點擊攻擊受害者的網站，致使其 Google AdSense 營利資格遭停權。

資安公司 KrebsOnSecurity 近日發表研究報告，指出他們接獲用戶通報，一種新形態的勒贖攻擊正在擴散，目標是所有透過 Google AdSense 廣告聯播網獲取廣告營收的網站擁有者。

報告指出，用戶會收到來自攻擊者的勒贖信件，信中要求受害者以比特幣支付約 5,000 美元的贖款，否則就將以大量機器人攻擊受害者擁有的網站，製造大量無效廣告點擊，包括點了廣告就離站的 100% 跳出率攻擊、多個 IP 輪流點擊等。

由於 Google AdSense 對這類詐騙點擊有很強大的偵測機制，意圖製造假點擊的 AdSense 用戶經常會遭到停權處分，而且被停權的網站很難再次加入 Google AdSsense 計畫，所以這個勒贖攻擊即利用此一弱點，以大量假點擊造成受害者的 Google AdSense 被 Google 停權。

KrebsOnSecurity 也在報告中說，據通報者提供的網站流量分析，確實在收到勒贖信件後，他的 Google AdSense 流量與營收報告中也出現了明顯過高的無效廣告點擊流量。

攻擊者也表示，被攻擊的網站在一開始很可能會得到較平常更高的廣告點擊營收，但很快 Google 系統便會偵測到異常流量，然後把超額的廣告刊登費用自受害者處扣除，歸還給廣告刊登者，這就會造成受害者的廣告營收損失。

Google 表示已經注意到這波勒贖攻擊，將會強化其異常廣告點擊的偵測能力，但該公司也說，目前這類因勒贖攻擊而產生的異常點擊案例仍然不多。

- 資料來源：
  1. https://krebsonsecurity.com/2020/02/pay-up-or-well-make-google-ban-your-ads/
  2. https://threatpost.com/hacker-scheme-threatens-adsense-customers-with-account-suspension/152943/
  3. https://www.searchenginejournal.com/google-adsense-crackdown/322123/

2.1.4、新發現：惡意軟體 Emotet 可透過駭侵鄰近無線網路進行擴散

資安專家發現最新 Emotet 變種，擁有透過駭侵鄰近不安全的無線網路，進行自我擴散的能力。

資安廠商 Binary Defense 的專家日前發表研究報告，指出該公司最近發現了新型 Emotet 惡意軟體的變種，可以從已感染的裝置，駭入鄰近未經加密的無線網路，並且進行自我擴散。

報告中描述了變種 Emotet 如何透過無線網路擴散：當某個裝置首先被感染時，會有兩個可執行檔 worm.exe 和 service.exe 從自我解壓縮的 RAR 檔中解開，同時自動執行 worm.exe。

接著 worm.exe 會開始掃瞄附近可駭侵的不安全的無線網路，並利用網路上可取得的各種預設密碼檔進行暴力嘗試，並開始進行駭侵攻擊。

專家指出，一旦 Emotet 能夠成功透過無線網路擴大駭侵範圍，就可能造成大量感染；由於 Emotet 透過社交工程和釣魚郵件造成的災情原本就肆虐甚廣，專家擔憂這種新的擴散方式，將會造成更大規模的資安災情。

專家也表示在一月份偵測到的無線擴散版 Emotet 惡意程式碼，其執行檔的日期標籤標為 2018 年四月份，這表示這個版本的 Emotet 可能兩年前就開始駭侵活動。

由於 Emotet 可做為載體承載多種駭侵攻擊工具，如資料竊取、Email 通訊錄搜刮、自我擴散，甚至是勒贖軟體等，因此威脅甚大。

不過目前發現的無線擴散版 Emotet 還不會進行加密通訊，因此資安專家建議資安管理人員可透過其封包特徵碼加以阻擋預防。

- 資料來源：
  1. https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/
  2. https://threatpost.com/emotet-now-hacks-nearby-wi-fi-networks-to-spread-like-a-worm/152725/

2.1.5、駭侵者利用武漢肺炎病毒為主題，針對和運輸有關的各行業發動攻擊

資安專家發現愈來愈多駭侵攻擊以武漢肺炎為名，針對製造業與運輸業等各行業進行 Email 攻擊。

資安廠商 Proofpoint 的研究人員發現，近來出現愈來愈多以武漢肺炎為名的 Email 惡意攻擊事件，針對和運輸相關的各個產業發動攻擊。

據資安專家指出，遭到攻擊的行業包括製造業、工業、金融、運輸、製藥與化粧品等行業。Email 內容詐稱提供武漢肺炎對全球流通業的影響分析，企圖誤導受害者開啟 Email 中的惡意夾檔。

在這波攻擊中，駭侵者利用的是夾帶惡意程式碼的 Microsoft Word 檔案。這個檔案中夾帶的惡意軟體名為 AZORult，透過一個兩年半之前就已發現的方程式編輯器資安漏洞（CVE-2017-11882）發動攻擊。

過去有相當多惡意軟體都利用這個資安漏洞進行駭侵攻擊；受害者如果誤開這個 Word 檔，AZORult 即會進行安裝並竊取電腦內的資訊；資安專家也說，由於 AZORult 具備相當的調整彈性，未來也很可能被用來安裝勒贖軟體。

資安專家表示，這波攻擊的來源來自某些東歐國家，然而目前尚無任何 APT 駭侵團體與此案有關的證據。

不久前才出現一波以日本為主要攻擊對象，提供虛假防疫訊息的惡意攻擊；資安專家指出，隨著武漢肺炎影響日漸擴大，可能會有愈來愈多這類假借疫情之名的惡意攻擊。

- 資料來源：
  1. https://www.proofpoint.com/us/corporate-blog/post/coronavirus-themed-attacks-target-global-shipping-concerns
  2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

2.1.6、澳洲多家銀行與金融單位接獲 DDoS 攻擊威脅

近來澳洲多家銀行與金融機構收到恐嚇信件，揚言將發動一連串強力的 DDoS 駭侵攻擊。

據澳洲媒體報導，該國多家銀行與金融機構，最近都收到來自某一駭侵團體的恐嚇信件，指稱如不支付相當數額的贖金，將對這些機構發動強力 DDoS 服務阻斷攻擊。

歹徒要求這些贖金必須以加密貨幣 Monero（XMR）來支付，但詳細的贖金金額細節並未公開。

澳洲資安中心（Australian Cyber Security Centre）在日前針對這波攻擊威脅也發出警訊，但據該中心表示，目前尚未觀察到任何針對目標金融單位發動的 DDoS 攻擊行為。

據 ZDNet 指出，澳洲最近的這波金融機構駭侵勒贖威脅，其實是自 2019 年十月起全球阻斷攻擊勒贖威脅（RDoS，Ramson Denial of Service）的一部分。這類勒贖威脅一開始都先以金融業為目標，但很快就會擴及製造業和其他行

業。

過去新加坡和南非的銀行接獲類似勒贖威脅後，同樣的勒贖威脅就轉移到土耳其的電信業者與南非的網路服務接取業者。

ZDNet 報導中認為發動這些攻擊的駭侵團體，有可能是惡名昭彰的 APT 組織 Fancy Bear 或 Cozy Bear。

- 資料來源：
  1. https://www.zdnet.com/article/australian-banks-targeted-by-ddos-extortionists/
  2. https://www.zdnet.com/article/a-ddos-gang-is-extorting-businesses-posing-as-russian-government-hackers/

2.1.7、便宜的資料竊取軟體服務大為流行，可竊取 60 多種應用軟體的資料

一個名為「浣熊」（Racoon）的惡意軟體服務，在駭侵相關論壇中大為流行，可從 60 多種常用軟體中竊取個資，而且使用費並不貴。

資安公司 CyberArk 發表研究報告，指出一個名為「浣熊」（Racoon）的惡意軟體服務（Malware-as-a-service），最近在英語系駭侵論壇上大為流行；即使不具備太多駭侵專業知識，有意進行駭侵攻擊者，也可以相當便宜的代價，透過這個惡意軟體服務發動資料竊取攻擊。

報告指出，這個惡意軟體服務係以 C++ 撰寫，技術上來說並不非常強大，但足夠有用，植入受害者系統後，可以攻擊六十多種常見應用軟體並取得資料；包括各種常見瀏覽器、Email、加密貨幣錢包、FTP 連線程式等都在範圍內；另外這個惡意軟體也會收集各種系統資訊。

這個惡意軟體服務的收費非常平易近人，一星期的服務費為 75 美元，一個月則為 200 美元；用戶可以透過集中化的管理工具來調整惡意軟體的設定值，並且存取竊得的各種資料，同時下載惡意軟體的執行檔。

一開始這個惡意軟體僅在俄語駭侵論壇中流傳，但去年四月起出現英文版後，即在英語系的駭侵論壇逐漸流行起來；由於價格便宜，使用門檻又低，全球已有數十萬台電腦遭其攻擊。

- 資料來源：
  1. https://www.cyberark.com/threat-research-blog/raccoon-the-story-of-a-typical-infostealer/
  2. https://www.bleepingcomputer.com/news/security/racoon-malware-steals-your-data-from-nearly-60-apps/

2.2、國際政府組織資安資訊

2.2.1、美國聯邦檢查官正式起訴涉嫌 Equifax 駭侵案人員

美國聯邦檢查官正式起訴某國軍方人員涉及美國史上最大的 Equifax 駭侵案，竊取多達一億五千萬名美國人的消費金融資料。

美國聯邦檢查官於本周一正式起訴四名某國軍方人員，指這四人涉及美國史上最大的 Equifax 駭侵案，竊取多達一億五千萬名美國人的消費金融資料。

檢查官說，這四人涉及指使駭侵團體 APT10 竊取大量美國民眾個資，不僅用於情報活動，同時也用以協助該國企業取得更多情報。

聯邦總檢查長 William Barr 在記者會中指出，該單位掌握多項對美國人民個資的長期駭侵攻擊行為，這些資料被用以協助發展人工智慧技術，也用於進一步的智慧化駭侵攻擊。

這四人一共被控九項罪名，包括詐騙監聽、經濟間諜活動、進行各種電腦詐騙等犯罪活動。

Eqifax 是美國最大的信用卡消費記錄業者，2017 年該公司發生的大規模駭侵事件，造成一億五千萬美國人的消費金融個資外洩，是史上最大的資料外洩事件；兩年來該公司在各種調查與司法控訴要求下，需支付高達六億五千萬美金的賠償金。

據美國媒體指出，駭侵者是在 2017 年 5 月開始駭入 Eqifax 的主機，利用名為 Apache Struts 的資安漏洞，竊得該公司多個系統的登入權限，並開始大量竊取個資。

被竊走的美國用戶個資，除了消費金融記錄外，還有包括社會福利編號和護照相片等敏感資訊，可用於製作進一步的詐騙攻擊之用。

- 資料來源：
  1. https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking
  2. https://www.politico.com/news/2020/02/10/us-charges-chinese-spies-with-massive-equifax-hack-113129
  3. https://www.washingtonpost.com/national-security/justice-dept-charges-four-members-of-chinese-military-in-connection-with-2017-hack-at-equifax/2020/02/10/07a1f7be-4c13-11ea-bf44-f5043eb3918a_story.html
  4. https://techcrunch.com/2020/02/10/justice-department-breach-equifax/

2.2.2、美國國防部所屬單位遭駭，相關人員之個人資訊被竊

美國國防部所屬單位日前遭駭侵攻擊，相關人員的多項可辨識身分之個資遭竊。

發生個資被竊案件的單位，是從屬於美國國防部的防衛資訊系統局（Defense Information System Agency, DISA），其職能包括對作戰任務提供 IT 後勤支援服務，同時負責白宮重要高官的通訊安全等事宜。

美國國防部發言人在上周四證實，發現 DISA 的部分系統遭到駭侵，與該單位有業務關係的所屬人員的資料遭到竊取；被竊的資料屬於可辨識個人身分的資訊，例如姓名、社會安全碼等多項個資。

據路透社報導指出，這起駭侵事件可能發生在 2019 年的五月到七月之間，但是美國國防部沒有透露駭侵事件的細節，例如駭侵手法、受影響程度、可能的駭侵者是誰、個資被竊的人數等資訊，僅表示目前正在進行調查工作，也已針對 DISA 的各項系統進行資安防護強化工作。

所有個資可能被竊的受害者，在二月 11 日時均收到 DISA 資訊長署名的一封信，信中除了通知個資可能遭竊之外，也表示 DISA 將會免費提供信用監控服務，一旦受害者的信用卡或銀行帳戶出現不明異動，即可立刻收到警示。

據 DISA 網站上的資訊，該單位的軍職和文職僱員約有八千人。

- 資料來源：
  1. https://www.reuters.com/article/us-usa-defense-breach/u-s-agency-responsible-for-trumps-secure-communication-suffered-data-breach-letter-idUSKBN20E27A?utm_medium=Social&utm_source=twitter
  2. https://www.cnet.com/news/data-breach-hits-us-defense-agency-responsible-for-securing-combat-it/

2.2.3、聯合國人權辦公室駭侵事件，源於微軟 SharePoint 已公開的資安漏洞

聯合國人權辦公室去年七月的遭駭事件，來自未被修補的微軟 SharePoint 伺服器漏洞。

據專業資安媒體 Threatpost 報導指出，去年七月發生於聯合國人權辦公室的嚴重駭侵事件，源自於微軟 SharePoint 伺服器一個未被適當修補的資安漏洞，因而造成多達 400GB 機敏資料外洩。

據上周被人權媒體 The New Humanitarian 公開的聯合國機密文件指出，一共有至少 42 台聯合國布署在日內瓦和維也納三個不同辦公室的伺服器遭到駭侵，可能洩漏的資料，包括聯合國至少 1600 名內部職員的個人資料，以及和聯合國進行合作的組織相關機密文件。

據美聯社指出，駭侵團體係利用微軟 SharePoint 伺服器一個已知的資安漏洞（CVE-2019-0604），植入可用以遠端執行任意程式碼的惡意軟體。

這個漏洞早在去年二月就已被發現，微軟也在四月就推出資安修補軟體供用戶更新。

以這個漏洞來說，像這類有更新卻未套用而造成的駭侵事件，在去年五月也發生在沙烏地阿拉伯和加拿大；兩國的資安主管機關都曾發布警訊，指有駭侵團體利用此漏洞進行攻擊。

據 Threatpost 指出，這次駭侵事件是有史以來聯合國遭遇的最大規模資安攻擊事件。雖然聯合國官員說駭侵團體並未取得任何密碼和主機存取權，但資安專家認為聯合國的資安防護能力仍然過於薄弱。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0604
  2. https://threatpost.com/un-hack-microsoft-sharepoint-flaw/152378/
  3. https://www.darkreading.com/threat-intelligence/united-nations-data-breach-started-with-microsoft-sharepoint-bug/d/d-id/1336926

2.2.4、丹麥政府稅務軟體錯誤，造成 126 萬人個資外洩

由於稅務入口的軟體錯誤，多達 126 萬名丹麥國民的個資遭到外洩。

丹麥日前驚傳由政府造成的大規模個資外洩事件，一共有 126 萬名丹麥國民的個資，因為丹麥政府財政部的稅務入口網站程式錯誤而外洩。

受到影響的人數多達丹麥總人口的五分之一，可說是丹麥歷史上最嚴重的資安事故。

這個軟體錯誤存在的時間長達五年，自 2015 年 2 月就開始造成影響，但一直到 2020 年 1 月丹麥政府進行內部稽核時才被發現。

發生這起資安事故的網站，是丹麥政府的稅務入口網站，可供居民進行稅務申報與繳納之用；每當居民申報稅務資訊時，申報人的身分證字號就會出現在網頁的 URL 中；有心人士可以利用 Google 或 Adobe 的網頁流量分析服務，來分析並收集 URL 中的身分證字號。

丹麥的身分證字號格式共有十碼，前六碼是持有者的出生年月日，最後一碼的奇偶數則代表性別，因此只要身分證字號外洩，個人的生日和性別的資料也等同外洩。

丹麥政府在獲知此事時，並未在第一時間公開此一外洩事件；因為丹麥政府認為只有 Google 和 Adobe 這兩家大公司的分析工具可以取得 URL 中的個資，影響不會太大。

然而丹麥當地的資安業者與專家並不認同這種做法，他們還要求政府應該公開財稅入口網站的程式碼，以檢視並發現是否存有其他資安風險。

- 資料來源：
  1. https://www.ufst.dk/nyheder/kammeradvokaten-vurderer-ansvar-i-utilsigtet-afsendelse-af-cpr-numre-ingen-risiko-for-misbrug-for-borgere/
  2. https://www.zdnet.com/article/software-error-exposes-the-id-numbers-for-1-26-million-danish-citizens/

2.2.5、波多黎各政府遭釣魚攻擊，損失達 400 萬美元

波多黎各政府日前遭大規模釣魚郵件駭侵攻擊，財損高達 400 萬美元以上。

這場嚴重的駭侵攻擊源於去年 12 月，受害者為波多黎各政府的財政部門。一名任職於波多黎各公務人員退休系統的公務人員，其 Email 被駭客攻破，接著許多政府單位都收到假冒該名公務員的釣魚與詐騙匯款要求 Email。

在這波攻擊中損失最慘重的兩個單位，分別是波多黎各政府所屬的工業發展公司與旅遊公司；前者甚至被騙兩次，分別匯給歹徒 6.3 萬美元與 260 萬美元，而後者也匯給歹徒 150 萬美元巨款。

波多黎各政府直到該名被冒名的公務員表示沒有收到任何匯款，才發現這是一起網路詐騙案件。

波多黎各政府已向美國聯邦調查局報告本案，並已展開調查行動。

無獨有偶，在波多黎各發生這起釣魚詐騙案的同時，美國德州和喬治亞州也分別發生類似的釣魚詐騙案，合計損失高達三百萬美金以上。

去年發生在美國本土的釣魚詐騙案，受害者超過兩萬三千家公司，總損失金額高達 17 億美元；估計這樣的釣魚詐騙案在今年還會更為嚴重。

- 資料來源：
  1. https://www.nbcnews.com/news/latino/puerto-rico-says-it-was-scammed-out-2-6-million-n1136191
  2. https://apnews.com/e03bea7e491b9c95350887880376562f

2.3、行動裝置資安訊息

2.3.1、多個 Android 平台 VPN App 可能帶來嚴重資安風險

多個在 Android 平台上的 VPN App 內含嚴重資安漏洞，可能導致中間人駭侵攻擊。

VPN 專業媒體 VPN Pro 發表報告指出，在 Android 平台上有多個下載量相當大、廣受歡迎的 VPN app，內含嚴重資安風險，可能導致用戶在使用其 VPN 服務時遭到駭侵攻擊。

根據該媒體的統計，這些危險的 VPN 服務至少影響一億兩千萬用戶。

該報導列出了多個在 Google Play Store 中廣受歡迎的危險 VPN App：

- SuperVPN Free VPN Client（一億次下載安裝）
- TapVPN Free VPN（一千萬次下載安裝）
- Best Ultimate VPN - Fastest Secure Ulimited VPN（五百萬次下載安裝）
- Korea VPN - Plugin for OpenVPN（一百萬次下載安裝）

- Wuma VPN-PRO(Fast & Unlimited & Security)（已自 Google Play Store 中移除）
- VPN Unblocker Free unlimited Best Anonymous Secure（一百萬次下載安裝）
- VPN Download: Top, Quick & Unblock Sites（已自 Google Play Store 中移除）
- Super VPN 2019 USA - Free VPN, Unblock Proxy VPN（五萬次下載安裝）
- Secure VPN - Fast VPN Free & Unlimited VPN（已自 Google Play Store 中移除）
- Power VPN Free VPN（已自 Google Play Store 中移除）

VPN Pro 在 2019 年一月以中間人攻擊測試這些在 Google Play Store 中廣受歡迎的一系列 VPN App，發現這些 VPN App 存有兩種主要的資安漏洞，一是將加密金鑰寫死（hard coded）在其程式碼中，駭侵者可以輕易據以解開加密通訊；二是未將各種機敏資訊予以加密。其中甚至有一個 VPN App 早就因被認定為惡意軟體而遭 Google Play Store 移除。

其中最多人下載的 SuperVPN 早在 2016 年就被一位澳洲資安研究者列為惡意軟體，但至今該 App 仍未被下架。

- 資料來源：
  1. https://vpnpro.com/blog/major-vulnerabilities-found-in-top-free-vpn-apps/
  2. https://research.csiro.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf

2.3.2、Google 表示正在努力加強 Android App 和 Google Play Store 的安全性

Google 表示持續加強 Android App，特別是 Google Play Store 中 App 的安全性，目前已見成效。

Android 裝置使用的 App 有許多惡意軟體混雜其中，過去經常傳出大規模感染和駭侵事件，甚至連 Google 官方直營的 Google Play Store 都經常有惡意 App 夾藏其中。

對此 Google 表示多年來一直在設法加強 Android App 與 Google Play Store 的安全性，而目前已經有一些成果可以分享。

Google 負責 Google Play Store 與 Android App 安全性的主管，日前在 Google 官方部落格發表專文，指出光是去年一年就從 Google Play Store 上下架了超過 79 萬個違反 Google App 上架規範的 App。

而在上個月，Google 也從 Play Store 中移了一萬七千個內含 Joker（或稱 Bread）惡意軟體的 App，其中有不少被移除的 App 使用各種技巧隱藏其中的惡意程式碼，但還是被 Google 偵測到。

不過即使如此，資安公司 Check Point 仍然指出在 Play Store 中還有為數破百的 Android App 內含嚴重資安漏洞；即時用戶正常定期更新，仍可導致用戶的 Android 裝置遭駭侵攻擊，遠端執行任意程式碼。

Google 表示將會繼續努力提升 Android App 的整體安全性，例如要求 App 不得在沒有必要的情形下要求過多權限，否則就違反 Play Store 的上架規範。

- 資料來源：
  1. https://android-developers.googleblog.com/2020/02/how-we-fought-bad-apps-and-malicious.html
  2. https://threatpost.com/google-efforts-against-bad-android-apps-work/152851/
  3. https://threatpost.com/popular-apps-on-google-play-store-remain-unpatched/150502/

2.3.3、Google 開始限制 Android App 於背景追蹤用戶所在地資訊

Google 將自八月起開始限制 Android App，若需在背景追蹤用戶所在地資訊，需通過程式審核。

Google 在一篇針對 Android 開發者的網誌貼文中指出，將自今年八月起從嚴審核會在背景追蹤用戶所在地的新 App；既有此類 App 也將在十一月起需要進行審核。

Google 在網誌文章中說，許多用戶表示對於 App 追蹤用戶地點造成的隱私問題表示關切，而 Google 在檢視眾多要求位置資訊權限的 App 後，發現有許多 App 的核心功能，並不需要用戶的所在地資訊，或是只需要在 App 執行期間追蹤用戶。

因此 Google Play Store 將修改 App 上架規範，如果 App 要在背景追蹤用戶資訊，則必須符合四個條件：追蹤用戶資訊的功能對用戶是確切有用的、用戶

可預期自己的位置會被追蹤、追蹤用戶是該 App 的核心必要功能，而且開啟背景追蹤有其必要；不然就會被拒絕上架。

iOS 很早就開始規定 App 在追蹤用戶時，必須透過系統服務通知用戶，並且讓用戶選擇是否同意 App 進行追蹤；Android 此時宣布跟進，對所有行動用戶是有益的。不過 iOS 對於背景追蹤的的規定，並不包括 Apple 自己開發的 App 在內，這點曾受部分開發者的批評。

在 Google 的宣布中則將 Google 自行開發的 App 也納入此一規範，並且提供了一些審核可能通過的案例，供開發者參考。

- 資料來源：
  1. https://android-developers.googleblog.com/2020/02/safer-location-access.html
  2. https://www.theverge.com/2020/2/21/21146834/google-play-store-background-location-tracking-review-process-android-11

2.4、軟體系統資安議題

2.4.1、Google 移除 500 個以上 Chrome 的惡意延伸套件

TWCERT/CC
Google 移除 500 個以上
Chrome 的惡意延伸套件

Google 近期針對 Chrome 瀏覽器上的惡意延伸套件（Extensions）進行了為期兩個多月的調查後，自 Chrome Web Store 中移除了超過 500 種內含惡意程式碼的延伸套件。

據 ZDNet 指出，被移除的延伸套件，多半是因為內含惡意廣告程式碼，會在用戶瀏覽網頁時進行各種和廣告有關的詐騙。

舉例來說，有些惡意延伸套件會顯示大量廣告，或是顯示聯盟行銷的購物連結，單純賺取佣金；但有些則會把用戶導向到看似真實電商網站的假冒頁面，甚至是惡意軟體下載或個資釣魚頁面。

根據資安廠商 Duo 的報告指出，有一些 Chrome 惡意延伸套件肆虐期間超過兩年以上，受害者人更高達一百七十萬人。

資安專家透過特製的 Chrome 延伸套件掃瞄工具，發現有許多不同的 Chrome 惡意延伸套件，內含相同或近似的惡意程式碼，但以不同的名目包裝，企圖混淆用戶視聽。

Google 表示，所有被認定為惡意的 Chrome 延伸套件，不但已從 Google Chrome Web Store 中移除，用戶先前安裝的這些套件也會被自動停用。

- 資料來源：
  1. https://www.zdnet.com/article/google-removes-500-malicious-chrome-extensions-from-the-web-store/
  2. https://duo.com/labs/research/crxcavator-malvertising-2020

2.4.2、微軟推出 2020 年二月 Patch Tuesday 資安修補包

微軟推出每月例行性的「Patch Tuesday」軟體資安漏洞修補包，近 100 個資安漏洞得到修補。

微軟於日前推出 2020 年二月的「Patch Tuesday」例行軟體資安修補包，一共補上了近百個先前發現的多種軟體資安漏洞。

在這些被修補的資安漏洞中，比較重要的包括舊版 Internet Explorer 網路瀏覽器的一個 0-day 漏洞（CVE-2020-0674）；未修補的用戶只要逛到某些藏有惡意程式碼的網頁，連點擊都不需要，就會被安裝惡意軟體。

這個修補包同時也修補了一個存在於 Windows 8、Windows 10 和 Windows Server 2008 到 2012 的嚴重漏洞 CVE-2020-0729，這個漏洞發生在 Windows 對 .LNK 檔的處理不當，以致可被攻擊者用以遠端執行任意程式碼。

另外，發生在 Microsoft Exchange 2010 到 2019 各版本的一個漏洞 CVE-2020-0688，同樣也能讓駭侵者遠端執行任意程式碼；這個漏洞本次也得以修補完成。

長期以來，有許多駭侵攻擊都是針對已知的微軟軟體資安漏洞進行攻擊，有些漏洞甚至是非常老舊的漏洞，但仍然會有為數眾多的系統遭駭，這表示許多用戶並未養成自動安裝或定期更新的習慣，因而將自身曝露在駭侵風險之

下。

微軟每月都會定期針對已發現的資安漏洞推出例行修補包，建議所有用戶不論是否已經發現系統弱點，都能定期安裝這些修補軟體，以減低遭到駭侵攻擊得逞的機會。

- 資料來源：
  1. https://krebsonsecurity.com/2020/02/microsoft-patch-tuesday-february-2020-edition/
  2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0729
  3. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0674
  4. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1280

2.4.3、NEC 承認遭駭，兩萬多個國防相關檔案遭竊

日本最大製造業者 NEC 承認遭駭侵，大量國防相關檔案被竊。

日本最大電氣相關產品製造業與 IT 業者日本電氣（NEC），日前公開遭嚴重駭侵的始末。

NEC 承認的駭侵事件發生於 2016 年 12 月，距今已有三年之久。

據報，目前由 NEC 確認遭駭的檔案數量非常多，高達 27,455 個，全部都是和日本防衛省相關的業務往來文件；但 NEC 強調這些文件內並不包含日本國防機密或相關人員的個人資料在內。

針對日本大型製造業的駭侵活動正在日益升高，事實上這是一個多月來傳出的第二起類似駭侵事件。上個月，另一家日本超大型製造業者三菱電機也曾傳出大規模駭侵事件，同樣也有和日本國防相關的檔案被竊。

日本防衛省表示，該單位掌握到的情報指出，除了三菱電機和 NEC 外，另外還有兩家與日本防衛省進行業務合作的公司也遭駭侵；但日本防衛省並沒有透露這兩家公司的確實名稱。

目前還沒有充分證據指出 NEC 駭侵事件的幕後主要攻擊者，但日本媒體和資安專家都認為和針對三菱電機發動攻擊的駭侵組織可能有關。

- 資料來源：
  1. https://english.kyodonews.net/news/2020/01/ffddb0eb9728-nec-receives-major-cyberattacks-defense-data-theft-suspected.html
  2. https://www.asahi.com/articles/ASN1005YHN1ZULFA044.html
  3. https://latesthackingnews.com/2020/02/03/japanese-firm-nec-electronics-confirm-security-breach/
  4. https://www.zdnet.com/article/japanese-company-nec-confirms-2016-security-breach/

2.4.4、廠商釋出 DVR 新版 firmware，以對應先前針對資安漏洞的駭侵攻擊

國內爆發近年來最大規模的網路監視系統駭侵事件，多家品牌網路監視器 DVR 主機遭駭侵並且植入惡意軟體，業者已於日前釋出新版韌體，以修補漏洞。

2020 年一月，國內爆發近年來最大規模的網路監視系統駭侵事件，多家品牌網路監視器 DVR 主機遭駭侵並且植入惡意軟體；據非正式估計，受害主機多達十萬台到二十萬台之譜。

這波攻擊的典型症狀，是 DVR 資安漏洞遭鎖定並植入 DDoS 惡意軟體，並由 DVR 主機發出大量網路攻擊封包，除了攻擊其他對象外，還會造成用戶主機所在區域網路被塞爆，內網各項網路連線均告受阻。

一月時，國內多家公司已在官網或經銷商網站、粉絲頁中證實遭到攻擊，並提供緊急處理步驟，包括新版韌體下載、維修服務資源等等。

而在二月時，廠商在官網釋出新版的 DVR 主機韌體，供用戶更新並修補漏洞。

在韌體更新網頁中，提供了多款機種的新版韌體；在頁面中也強烈建議用戶在更新韌體之後，務必更改預設的管理者帳號與密碼，並使用混合複雜字母、數字與特殊符號的高強度密碼，以免再次發生使用預設帳號密碼，而遭攻擊者輕易進入管理界面的問題。

去年在網路上曾有監視錄音工程公司發表一篇文章，直接公開各廠 DVR 主機的預設登入用帳號密碼或所謂「萬用工程登入密碼」。

除了更改管理者登入帳密外，資安單位也建議用戶修改 DVR 管理界面預設使用的網路埠號，並且在防火牆設定更強大的防護措施。

- 資料來源：
  1. https://www.twcert.org.tw/tw/cp-104-3259-932ae-1.html

2.5、軟硬體漏洞資訊

2.5.1、WordPress 重要擴充套件內含資安漏洞，70 萬個網站曝險

一個廣受歡迎的 WordPress 擴充套件 GDPR Cookie Consent 內含嚴重資安漏洞，可能導致 70 萬個使用該套件的 WordPress 架設網站曝險。

這個 WordPress 擴充套件的功能，是讓以 WordPress 架設的網站，能夠自動顯示一條 Banner，告知訪客該站使用 Cookie 並符合歐盟一般資料保護法規（GDPR）。

這個資安漏洞存在於該擴充套件在處理 AJAX 特效時的疏失，可能導致駭侵者取得 WordPress 的更高權限，例如變更 WordPress 網站的內容、或是任何內容下線或上線。

目前這個資安漏洞已有 CVSS 危險性評級；其評級為「嚴重級」的 9.0 分。

資安公司 Wordfence 在發現此漏洞時，已在第一時間通報該擴充套件的開發者和 WordPress 的開發公司 Automattic，很快的該擴充套件就暫時從 WordPress.org 的擴充套件目錄中下架。

在新版 GDPR Cookie Consent 解決此漏洞後，該擴充套件又再度上架到 WordPress.org 擴充套件目錄了。

有此資安漏洞的舊版本為 1.8.2 之前的舊版，更新至 2 月 11 日推出的 1.8.3 新版即可修復此一漏洞。

WordFence 的事件報告中，詳列了這個資安漏洞的細節，包括錯誤內容與如何利用此漏洞攻擊 WordPress 主程式。

- 影響版本：GDPR Cookie Consent 1.8.2 之前版本
- 解決方案：升級至 1.8.3 之後版本
- 資料來源：
  1. https://www.wordfence.com/blog/2020/02/improper-access-controls-in-gdpr-cookie-consent-plugin/
  2. https://threatpost.com/critical-wordpress-plugin-bug-afflicts-700k-sites/152871/

2.5.2、WordPress 擴充套件的 0-day 漏洞，可用以新增管理者帳號

一個名為 ThemeRex 的 WordPress 擴充套件，被發現內含一個嚴重的 0-day 資安漏洞，不但可被駭侵者用以遠端執行任意程式碼，更可用來新增管理者帳號。

據資安廠商 Wordfence 的報告指出，估計約有 44,000 個 WordPress 網站使用該擴充套件，也已偵測到利用此 0-day 漏洞進行的駭侵攻擊。

這個漏洞來自於 WordPress REST API，該套件沒有先檢查用戶是否具有管理者權限，就能執行任何 php 函式；結果就是駭侵者可透過這個漏洞，遠端執行任意程式碼，並且在網站系統中新增具備管理者權限的帳號。

這個 0-day 漏洞的 CVSS 評分高達 9.8 分，屬於極度嚴重等級的資安漏洞。

目前發行 ThemeRex 的公司尚未推出更新程式，資安媒體 The Bleeping Computer 也連絡該公司進行詢問。

Wordfence 的資安專家表示，鑑於已經出現攻擊此漏洞的案例，安裝了這個擴充套件的 WordPress 用戶，最好暫時移除套件，直到新版推出為止。

- 影響版本：ThemeRex 1.6.50 後版本
- 資料來源：
  1. https://www.wordfence.com/blog/2020/02/zero-day-vulnerability-in-themerex-addons-plugin-exploited-in-the-wild/

2. https://www.bleepingcomputer.com/news/security/zero-day-in-wordpress-plugin-exploited-to-create-admin-accounts/

2.5.3、WhatsApp 爆重大安全漏洞，用戶私人檔案可能遭竊

Facebook 臉書旗下著名通訊軟體 WhatsApp，被發現有重大安全漏洞，可能讓用戶私人檔案被有心人士竊取，並陷入網路釣魚的風險。

國外 IT 資訊網站 The Hacker News 報導，PerimeterX 公司的研究員 Gal Weizman 在 2 月 4 日公布了多項來自通訊軟體 WhatsApp 的重大安全漏洞。幾乎所有平台之版本受影響，包括 WhatsApp 的 Windows、Mac 以及 iOS、Android 版本。

根據 Gal Weizman 最近於部落格公開的內容，攻擊者可將 WhatsApp 所傳送網頁連結的預覽內容，替換為知名網站之圖示，誘使使用者點擊。

當使用者點擊惡意連結時，將開啟惡意網頁並繞過 WhatsApp 的網頁內容安全原則（Content Security Policy, CSP），執行惡意程式碼，進行跨站腳本攻擊（Cross-Site Scripting, XSS），以竊取使用者的網頁快取資料（Cookie）。在 Windows 和 Mac 版本之 WhatsApp，也會受到 XSS 攻擊，並竊取電腦中的用戶文件和檔案等，此安全漏洞甚至能讓駭客進一步進行遠端程式碼執行（Remote Code Execution, RCE）。

Gal Weizman 指出，WhatsApp 在編寫用戶端軟體時，使用了未更新的內核版本（Chromium/69），由於舊版的 Chromium 允許惡意的 XSS 程式碼在用戶端被執行，即使用戶使用最新版的 WhatsApp 版本，電腦也可能被攻擊。

該安全漏洞在 2019 年 10 月被 WhatsApp 之母公司 Facebook 證實，此重大安全漏洞也被臉書公司發布 CVE 漏洞（CVE-2019-18426）近年來，WhatsApp 接連爆出多項重大的資安缺失。光是在 2019 年間，便有 8 項重大安全漏洞被公開。

WhatsApp 表示，包括電腦及行動版本的應用程式，該項安全漏洞已於 2019 年 12 月被修復。建議使用者可以於官網或 App 商店下載最新版的應用程式以修復該漏洞。

- CVE 編號：CVE-2019-18426
- 影響版本：桌面版版本 0.3.9309 以前、手機 APP 版本 2.20.10 以前
- 解決方案：更新該軟體所發布之最新版本
- 資料來源：
  1. https://thehackernews.com/2020/02/hack-whatsapp-web.html
  2. https://www.techradar.com/news/whatsapp-desktop-has-a-worrying-security-flaw
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18426
  4. https://www.perimeterx.com/tech-blog/2020/whatsapp-fs-read-vuln-disclosure/

第 3 章、 資安研討會及活動

第 19 屆亞太資訊安全論壇暨展會	
活動時間	**6/9 (二) – 6/10 (三) 09:00 ~ 17:00**
活動地點	**台北市敦化南路一段 108 號 B2F**
活動網站	**https://www.informationsecurity.com.tw/event/event_info.aspx?eid=1498**
活動概要	 參加對象: 政府、金融、醫院、高科技製造業等產業資安、網管、IT、程式等人員 。 參加方式: 全程免費參加 / 報名請務必留下公司 email 及電話。 同期展出: 政府論壇、關鍵資訊基礎、金融論壇、製造業論壇、醫療論壇等專屬研討會。 參加提醒: 請務必攜帶任職公司的個人職務名片前來報到換取會議入場證。 注意事項: 主辦單位享有審核參與人員之權力，同時本活動因須審核產業屬性，恕不接受現場報名。 活動洽詢: 02-8729-1042 潘小姐 / Iris.Pan@newera.messefrankfurt.com 主辦單位: 資安人

CYBERSEC 2020 臺灣資安大會	
活動時間	**8/12(二) – 8/14(四) 08:30 ~ 17:00**
活動地點	**台北市南港區經貿二路 2 號 (南港展覽二館)**
活動網站	https://r.itho.me/sec2020
活動概要	 國際級資安大會 X 超規格資安大展【CYBERSEC 2020 臺灣資安大會】，即將在 8/12-8/14 於南港展覽二館盛大登場！ 匯聚世界級資安大神、國內資安頂尖高手，從提供超過 200 堂資安面向的議程、量身打造最扎實的 CyberLab 實戰演練課程，探討國際最新、最熱門且最全面的資安議題與技術，讓您全方面迎戰資安風險。即刻提升實戰能力。 現場網羅超過 250 家以上全球與國內知名標竿資安品牌，展示 1000+業界最新、最適切的資安產品與服務。平日難以跟進的所有資安產品資訊、市場與發展，都可以在此一次獲得！ 邀請您與我們一同參與這年度資安盛會，與來自臺灣與亞太地區超過 8,000 位菁英進行交流，從技術層面與策略層面，探討資安百種面向、交流技術與知識，讓資安戰場更加壯大，得以更快速地反應、更快速地處理，形成足以跟攻擊者匹敵的更強力防禦。 了解更多大會資訊：https://r.itho.me/sec2020

第 4 章、 2020 年 02 月份資安情資分享概況

本中心每日透過官方網站、電郵、電話等方式接收資安情資，以下為各項統計數據，分別為對外資安情資分享地區統計圖及資安情資分享類型統計圖。

分享地區統計圖為本中心所接獲之資安情資分享中，針對資安情資所屬地區之分享比率，如圖 1 所示；分享類型統計圖則為本中心所接獲的資安情資分享中，各項攻擊類型之比率，如圖 2 所示。

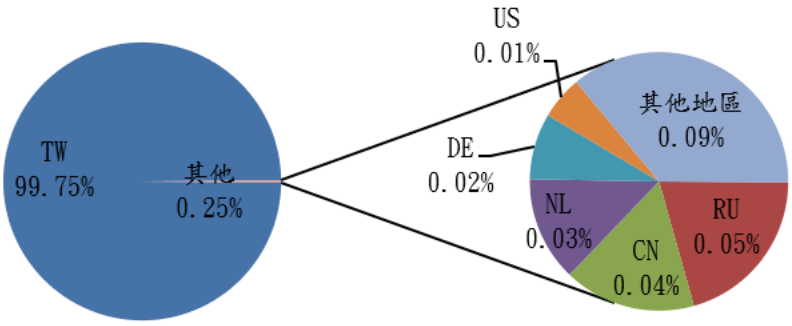


圖 1、分享地區統計圖

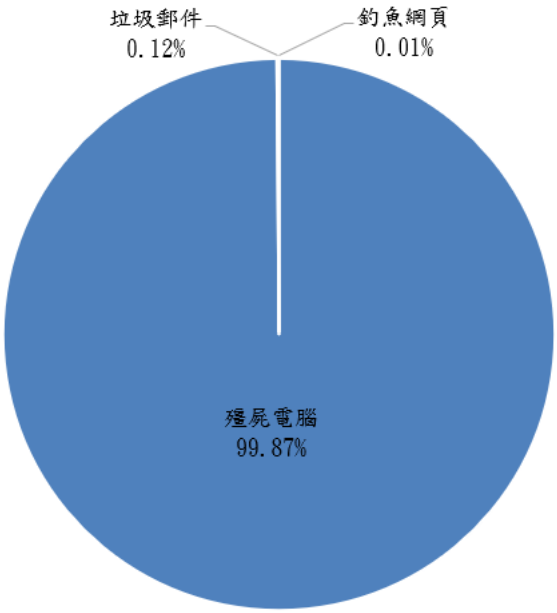


圖 2、分享類型統計圖

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：**2020 年 3 月 10 日**

編輯：**林克容、江奕昉、洪彩馨**

服務電話：**0800-885-066**

電子郵件：**twcert@cert.org.tw**

官網：**https://twcert.org.tw/**

痞客邦：**http://twcert.pixnet.net/blog**

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

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

Twitter：**@TWCERTCC**