TWCERT/CC 資安情資電子報

2019 年 4 月份

目錄

第 1 章、 封面故事

華碩電腦 Live Update 遭駭，百萬使用者恐安裝惡意軟體

原本提供即時更新，保護使用者的資訊安全的華碩 Asus Live Update，近日被資安公司卡巴斯基公布，此更新機制遭受駭客攻擊利用，變成使用者安裝惡意軟體的一大捷徑。

為方便使用者，華碩(Asus)開發了一款自動、即時的軟體更新工具程式—Asus Live Update，附於華碩筆記型電腦內，當電腦開機時會自動開啟，連入華碩網站檢閱是否有華碩相關軟體更新版本，並進行自動更新。

此項方便的即時更新工具程式，卻在去年(2018)6 月至 11 月間，遭受有心人士透過未知管道獲得之合法華碩數位憑證，將後門或惡意程式植入被更新之軟體中，大量散播惡意軟體，此事件之攻擊手法被稱作「ShadowHammer」。

ShadowHammer 攻擊事件

今年(2019)1 月時，卡巴斯基公司應用了新的供應鏈攻擊(Supply Chain Attack)相關檢測技術，用以檢測合法程式中被隱藏的異常部分，因此發現華碩電腦可能遭駭並遭植入惡意軟體。在被發現之前，此攻擊可能已經持續了半年以上，影響範圍可能相當大。

Asus 目前表示已主動聯繫可能遭受攻擊之用戶，並且提供檢測以及更新之相關服務，也透過客服專員協助相關用戶解決問題，同時亦會持追蹤，確保使用者資訊安全無虞。

除了協助使用者，華碩已針對該軟體進行升級為全新多重驗證機制，針對此次事件的各種可能漏洞，強化其加密機制，確保事件不再發生。

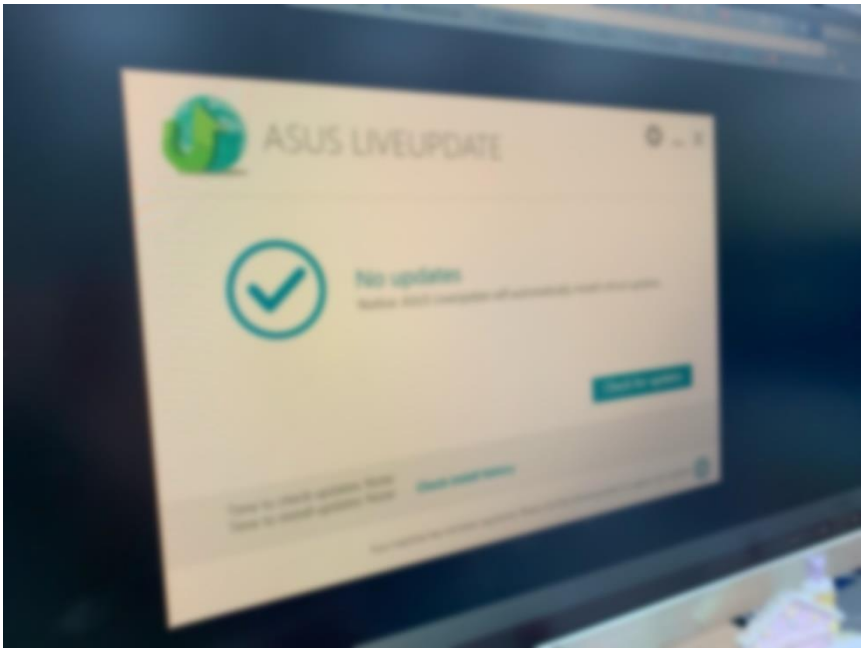
檢測及建議措施

在 ShadowHammer 攻擊中，目前已經在 200 支惡意程式樣本中，查

出約 600 個不同的 MAC 位址，未來將會對更多樣本進行檢測。卡巴斯基也提供擔心的使用者於其網站中(https://shadowhammer.kaspersky.com/)，查詢自己電腦是否有問題。同時，華碩已提供 ShadowHammer 的檢測工具 (https://dlcdnets.asus.com/pub/ASUS/nb/Apps_for_Win10/ASUSDiagnosticTool/ASDT_v1.0.1.0.zip?_ga=2.20570680.1823363715.1553584600-974246282.1552277686)，供擔心的民眾用以檢測電腦是否有被攻擊。

若民眾仍擔心安裝到惡意程式，建議可至「系統設定」視窗中，將「服務」和「啟動」標籤下的 Asus Live Update 選項取消，停止該程式的開機自動啟動。並且將 Asus Live Update 更新至最新 V3.6.8 或是更高的版本。且除非作業系統等較重要之升級，驅動程式不需持續更新，若真的需更新，使用者可直接於官網下載更新，不應透過其他軟體下載安裝，以避免遭植入惡意軟體。

- 資料來源：
  1. https://securelist.com/operation-shadowhammer/89992/
  2. https://www.kaspersky.com/blog/shadow-hammer-teaser/26149/
  3. https://www.asus.com/tw/News/IsyIB2Q5VN9N1Y3w



第 2 章、 資安宣導

請小心您收到的 Email，究竟是真是假？！

近期發現「竄改商務電子郵件」詐騙案例近期案例，臺中市某鞋品貿易公司遭詐騙集團鎖定，掌握林姓業務與國外合作公司(下稱 A 公司)有筆應付款項，仿照 A 公司業務的電子郵件帳號「xxxxxdaixx@163.com」，設立名稱相似的「xxxxxdeaixx@163.com」假帳號發信給該名林姓業務，謊稱原帳戶因稅務問題進行整併中，要求變更匯款帳戶至瑞典北歐斯安銀行之境外帳戶，林姓業務所屬公司因與 A 公司長期合作，遂不疑有他，直接以傳真銀行方式匯出臺幣數十萬元。孰料 5 天後，A 公司通知並未收到匯款，林姓業務連忙找出當初聯繫之電子郵件內容，發現假帳號竟多了 1 個 e 字母，「e」字之差使公司損失達數十萬元。

- 經分析是類詐騙手法略述如下：
  1. 詐騙集團攔截被害人公司交易信件，並申請與企業客戶電子郵件地址相似度極高的假郵件使之混淆(如前揭案例僅多一字母「e」，歹徒所設「xxxxxdeaixx@163.com」電子郵件與原本「xxxxxdaixx@163.com」極為相似)。
  2. 模仿原本往來郵件語氣發信給被駭企業之客戶，騙取企業或客戶變更匯款帳戶，藉機詐騙被害人將貨款匯至詐騙集團所預設帳戶。
  3. 取得企業客戶的信任而匯款，俟原受款客戶反映未收到貨款時，方知受騙。

第 3 章、 資安小知識—DNS (下)

網域名稱系統安全擴充(DNSSEC)

經歷上述的資安問題，為了解決使用者無法辨識收到的資訊是否有遭到竄改，因此，網際網路中，出現了「網域名稱系統安全擴充 (Domain Name System Security Extensions, DNSSEC)」。

在 DNSSEC 中，為了確保網路 DNS 的使用安全，使用了兩項相關技術：數位簽章以及 DNS 延伸安全協定 (Extension Mechanisms for DNS, EDNS)。

DNSSEC 與數位簽章

數位簽章

此協議主要是確保 DNS 權威主機中的資料都是未經有心人士竄改之資料。當 DNS 權威主機收到請求後，在回覆訊息中，會放入含憑證之 RRSIG。此時，DNSSEC 並不會直接傳遞明文之資訊，會透過加密密鑰對發送之 DNS 訊息透過雜湊函式(hash function)進行雜湊運算，經雜湊後之文件稱作「雜湊摘要 (Digest)」。並將此雜湊摘要(明文經雜湊後產生之雜湊值)，以 DNS 權威主機之金鑰進行加密，此時，權威主機將訊息明文及加密後之雜湊摘要同時傳給 DNS 伺服器。

DNS 伺服器收到後，會透過 DNS 權威主機金鑰(DNSKEY)進行解密。同時，為了確認該金鑰確實屬於此網域所有，因此將位於上一層之 DNS 權威主機中之 DS (Delegation Signer) 進行驗證，確保金鑰沒有被偽裝或竄改。

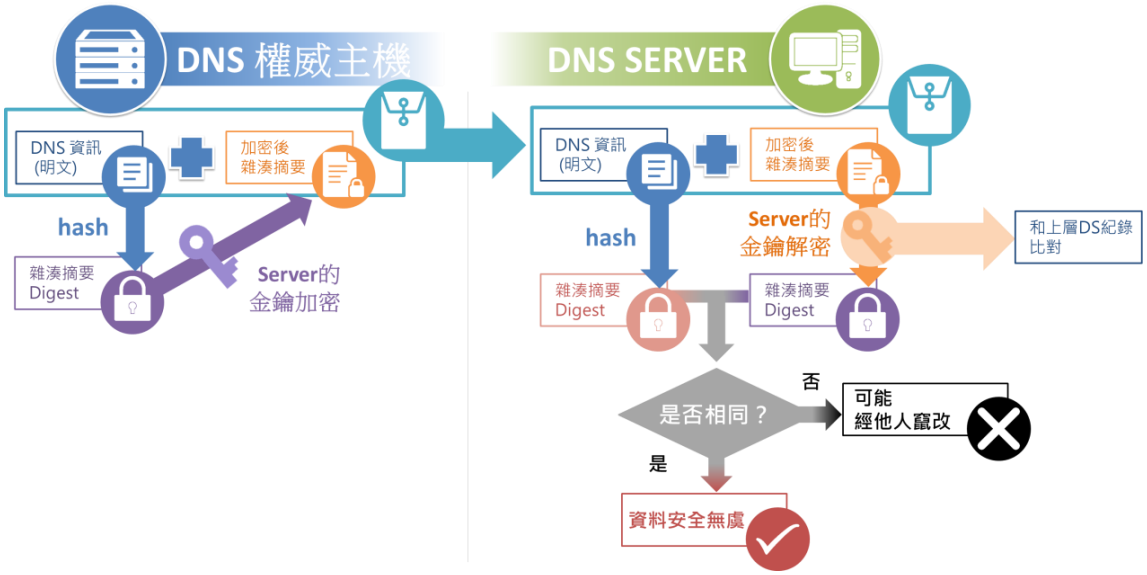
DNS 伺服器確認過後，將加密過之雜湊摘要以權威主機的金鑰解密，以取得完整雜湊摘要。此時若成功解

碼，則代表此封包確實為該 DNS 權威主機所傳遞；否則若該封包非該權威主機傳遞，以該權威主機之金鑰無法解密。同時，再以同樣雜湊函式將明文進行雜湊運算，取得其雜湊摘要。最終，DNS 伺服器會將本身運算出之雜湊摘要，和收到的雜湊摘要進行比對，若經他人竄改，即便是肉眼難以辨別之空格，均會造成雜湊數值之大幅變動；若相同則代表未經他人竄改。

如此，DNS 伺服器便可透過以上動作確認：(1)該訊息確實為該 DNS 權威主機發送、(2)訊息未經他人竄改、(3)DNS 權威主機無法否認發送此封包。

目前，各大 DNS 廠商均開始進行 DNSSEC 之運作，以確保大眾使用之安全性。同時，網際網路名稱與數字位址分配機構(ICANN)也於本月發文公告，敦促全球網域相關產業全面採用 DNSSEC。DNSSEC 可以完全相容於舊有 DNS 架構，並且可以大幅避免 DNS 紀錄被竄改之問題。為了 DNS 的安全，ICANN 正努力進行推廣和執行，希望能及早促成 DNSSEC 之普及。

☞HINT：DNSSEC 可以看做寄送機密信件。傳送者為了保護手中機密文件，因此將內容以中英文鍵盤對照轉換的方法編撰成一般人看不懂的密碼，然後再用帶鎖的盒子鎖起來，和機密文件一起送出去。接收者會將從傳送者那收到的鑰匙將盒子解鎖，代表確實是傳送者所寄。接著將收到的機密信件透過同樣方式編撰成密碼，再和帶鎖盒子中加密文件比對，若相同則代表沒有被任何人修改其中文字。



NSEC

以舊有 DNS 而言，若使用者查詢之網址並不存在，DNS 權威主機僅會回覆使用者「不存在」之訊息。但未添加任何驗證訊息的「不存在」封包，很有可能會被有心人士擷取後，用以對一般使用者在查詢正常網域時，發送該網域不存在之訊息，導致使用者無法取得正確網域資訊及連接該網站。

因此，除了上述 DNS 訊息外，此機制會替此「不存在」之訊息進行簽章，以保障使用者取得「不存在」訊息，代表此網頁是確實不存在，而非他人偽造該訊息。回應並包含驗證之「不存在」之紀錄，稱作 NSEC。

NSEC，全名為 Next Secure，主要用以解決負面回應訊息(「不存在」訊息)之問題。此紀錄主要是將該網域下，所有的網域名稱進行排序，並透過兩者網域間之空隙，取得該被查詢網域之前後網域名稱做為紀錄並回傳。

這樣描述有些難以理解，因此舉例而言，若在 twcert.org.tw 網域下，有 a.twcert.org.tw、ma.twcert.org.tw、pop.twcert.org.tw、te.st.twcert.org.tw、let.twcert.org.tw、move.twcert.org.tw 等 6 筆網域名稱，則在該網域下，此些網域名稱會被排序為：

twcert.org.tw
a.twcert.org.tw
let.twcert.org.tw
ma.twcert.org.tw
move.twcert.org.tw
pop.twcert.org.tw
te.st.twcert.org.tw

此時，若使用者查詢 love.twcert.org.tw，則使用者會獲得理論上於該查詢網域的前一筆和後一筆，亦即前一筆 let.twcert.org.tw 以及後一筆之 ma.twcert.org.tw，代表兩者之間並無 love.twcert.org.tw 網域，因此驗證確實該網域並不存在。同時，若該訊息被有心人士擷取，由於有網域之驗證，此訊息也無法用於一般使用者查詢網域之偽造訊息，保障「不存在」之訊息正確性。

☞HINT：NSEC 可看作將號碼牌按照上面數字排放，例如已經排放了 1、2、3、5、6、7、8、10、12，若此時，有一位一號使用者來信要求取得 9 號號碼牌，負責人卻發覺並無 9 號號碼牌，因此回信給一號使用者說明

並無此號碼牌之狀況。若該信中僅說明沒有 9 號號碼牌，而無其他驗證資訊，則一號使用者可以在另外的二號使用者要求 10 號號碼牌時，將那封信偽造成負責人所寄，告訴二號使用者沒有 10 號號碼牌，導致二號使用者拿不到該號碼牌。而若當初負責人告之一號使用者的信中除了告知沒有 9 號號碼牌之外，同時也說明前面是 8 號、後面是 10 號，確定中間無任何號碼牌，則收到此封信的一號使用者，即便他想欺騙二號使用者，卻會因為裡面的驗證訊息(8 號和 10 號號碼牌資訊)而偽造不成，避免了一次詐騙。

DNSSEC 與 EDNS

EDNS，又稱為 EDNS0，全名為 Extension Mechanisms for DNS，譯為 DNS 延伸安全協定。是 DNSSEC 中的一項技術，主要用於提升 DNS 運作之安全性。

有鑒於 DNSSEC 的建立和發展，其所需之功能訊愈來愈多，若維持以往之 DNS 形式，所需的功能標示將難以以舊有格式完整表達。因此，在舊有的 DNS 封包中，延伸出更多的區段，

用以支持未來期望表達的特徵值。

例如當初的 DNS 封包是使用 UDP Port 53 封包進行傳輸，本身大小限制為 512 bytes。若以過往的 DNS 封包所應傳輸之內容而言是足夠的，但在 DNSSEC 中，由於增添了數位簽章的部分，其封包大小在包含數位簽章資料後已不足以負荷。而若此時使用 EDNS，可以將其封包大小上限大幅增加，可容納 4,096 bytes 的資料，如此，方可將 DNSSEC 所需資料內容完整地進行傳輸。

DNS 封包

在 DNS 所傳輸的封包中，分為許多欄位，例如表頭(Header)、查詢區域(Question Section)、回覆區域(Answer Section)、授權區域(Authority Section)以及額外紀錄區域(Additional Records Section)。

表頭主要標示此封包之編號、描述此訊息封包的功能，例如此封包為查詢或是回應用等、以及相關紀錄的數量。查詢區域，則是用以描述問題名稱、型態(是查詢 IP 位址、名稱伺服器.....等等)，以及問題類別(是否為 IP 位址格式)。

回覆區域則是記錄權威主機所回應之資料，例如資源名稱(針對哪一個問題進行回覆)、資源型態(對應查詢區域中的型態)、資源類別(對應查詢區域中的問題類別)、存活時間(封包傳送時存活的時間，若過久未到達目的地則會進行刪除)、資源資料長度(表示資源資料的長度)，以及資源資料(詢問回覆之答案)。

第三、授權區域，此區域並非使用者詢問問題之確切答案，而是在 DNS 詢問中，上層之其他 DNS 權威主機之資訊，引導 DNS 伺服器對上層之 DNS 權威主機進行詢問，直到得到答案為止。

最後，額外記錄區域則是當授權區域有除上述訊息外之額外訊息，方放入額外紀錄區域。

EDNS

對於 EDNS，DNS 伺服器不一定有支援 EDNS，因此，為了標示該伺服器是否有支援 EDNS，會在 Additional Records Section 中，加入一「opt」資訊。此時，若權威伺服器收到該封包，發覺額外紀錄區域有「opt」資訊，則可知使用者之 DNS 伺服器有支援 EDNS，並且於回覆時，也會於額外紀錄區域加上 opt 資訊進行回覆，代表此為 EDNS 封包。

但此封包為 EDNS 封包，卻不一定為 DNSSEC 封包，必須於 EDNS 訊息中的「do」區域被設定為 1 時，方為 DNSSEC 封包。

支援 EDNS 後，由於擴展了針對其他的 DNS 所需功能表達之特徵值欄位，並且亦擴增了封包大小限制，因此，除了 DNS 訊息傳遞時，可以包含數位簽章之資訊內容外，亦可以包含舊有 DNS 未能包含之特殊特徵值，讓 DNS 的運作更加安全。

由於意識到 EDNS 的重要性，在今年的二月一日，Clouflare、Google、IBM 等大型公共 DNS 業者進行了 EDNS 的符合性驗證。雖此次驗證僅有一天時間，但同時也是期盼未來 EDNS 發展的起點。

☞HINT：EDNS 就像是一小手拿包，雖然平常放錢包手機已經足夠，但是當外面天氣不好、下雨時，雨傘便放不進去；或者帶著讀到一半的書籍，想去舒適的咖啡廳閱讀，但是 A5 大小的書籍，一般小型手拿包亦放不下去。因此，可以拿一較大的包，將手拿包放入大包中，並且將雨傘、書籍都排放進去，如此一來，便可容納所需的大部分東西，甚至不需對手拿包進行改造便可。

DNSSEC

透過數位簽章及 EDNS 的運作，DNSSEC 額外確保三項資訊安全項目：

1. 資料完整性 (Data Integrity)：確保收到的資料是完整的，未經有心人士等第三者進行竄改。

2. 來源可驗證性 (Origin Authentication of DNS Data)：確保資訊的寄送者為正確之 DNS 權威主機/DNS 伺服器，而非收到有心人士偽造出之假資訊，被導入錯誤之釣魚網站。

3. 可驗證之不存在性(Authenticated Denial of Existence)：確保當使用者收到「該網址/位址不存在」訊息，可透過 NSEC 進行驗證，驗證該網域確實不存在，而非遭他人竄改。

為了彌補 DNS 亦遭受有心人士攻擊之問題，開啟了 DNSSEC 的技術。如此一來，可以大幅減少 DNS 相關駭侵攻擊，保障使用者的運作安全。在台灣，許多電信業者已紛紛跟進，根據台灣網路資訊中心(TWNIC)之註冊機構資訊，截至目前，中華電信、亞太電信、pchome、新世紀資通、台灣大哥大、Neustar、中華國際通訊網路、Gandi SAS、Key-Systems GmbH 等，均已註冊並使用 DNSSEC 服務。期盼未來有更多相關業者參與及使用 DNSSEC，令使用者擁有一個完整且安全的完善網路，不再被不法人士劫持，能真正自由安心地使用網路服務。

- 資料來源：

1. http://www.cc.ntu.edu.tw/chinese/epaper/0022/20120920_2206.html
2. http://www.myhome.net.tw/2011_03/p03.htm
3. https://www.lijyyh.com/2012/07/dnssec-introduction-to-dnssec.html
4. https://medium.com/@sj82516/dnssec-%E5%9F%BA%E6%9C%AC%E5%8E%9F%E7%90%86%E4%BB%8B%E7%B4%B9-65841439d0a5
5. https://blog.longwin.com.tw/2019/01/dnssec-dns-sign-edns-check-2019/
6. https://blog.twnic.net.tw/2019/01/23/2286/
7. https://blog.csdn.net/star_xiong/article/details/40429457
8. http://net.ndhu.edu.tw/~net/DL/20110330.pdf
9. https://en.wikipedia.org/wiki/Extension_mechanisms_for_DNS
10. http://dnssec.nctu.edu.tw/images/DNSSEC/DNSSECtech.pdf
11. http://www.myhome.net.tw/2011_07/p05.htm
12. https://www.twnic.net.tw/dnservice_company_intro.php

第 4 章、 資安活動紀事

參與賽門鐵克網路安全威脅報告(Internet Security Threat Report, ISTR)

台灣電腦網路危機處理暨協調中心(TWCERT/CC)及台灣網路資訊中心(TWNIC)副執行長丁綺萍，參與 ISTR-2019，講述對於我國資安趨勢的通報及相關研究結果。

台灣網路資訊中心於今年(2019 年) 1 月正式承接台灣電腦網路危機處理暨協調中心業務，並於 1 月至 2 月期間，處理了超過 10 萬筆之資安情資。在這些通報中，其受資安威脅的來源國家，中國佔了約 60%、第二則是佔了 9%的美國，再者為法國、香港、越南.....。若以資安威脅之類型而言，是以對外攻擊以及系統被入侵兩種類型為大宗，尤其對外攻擊更佔了所有資安通報數量 50%以上。其餘之殭屍電腦、可疑連線、惡意遠端操作、釣魚網頁、網頁木馬以及散播惡意程式，則相對少量。

在對外攻擊事件中，是針對本中心接獲之台灣 IP 資安通報，亦即台灣使用者透過台灣 IP 對其他系統或裝置進行攻擊。在這些對外攻擊之通報中，其中有部分之攻擊 IP，可能是被有心人士在不知情的狀況下，做為跳板來對其他系統/裝置進行攻擊的動作。但自接獲的通報中，本中心難以探查該攻擊 IP 是否是遭受他人利用，因此統一歸類於「對外攻擊」類型。

雖本中心會在接獲通報後，立即告知網路提供業者進行處理，但相關問題仍然層出不窮，希望能透過此些數據之分享，提高民眾對於裝置和網際網路的警覺，將資安事件的數量以及程度降到最低。


ymantec

第 5 章、 國內外重要資安事件

5.1、資安趨勢

5.1.1 去年第四季 DDoS 攻擊量體大減 85%

在 FBI 破獲並關閉 15 個「代客 DDoS」網站後，去年第四季全球 DDoS 攻擊量體大減 85%。

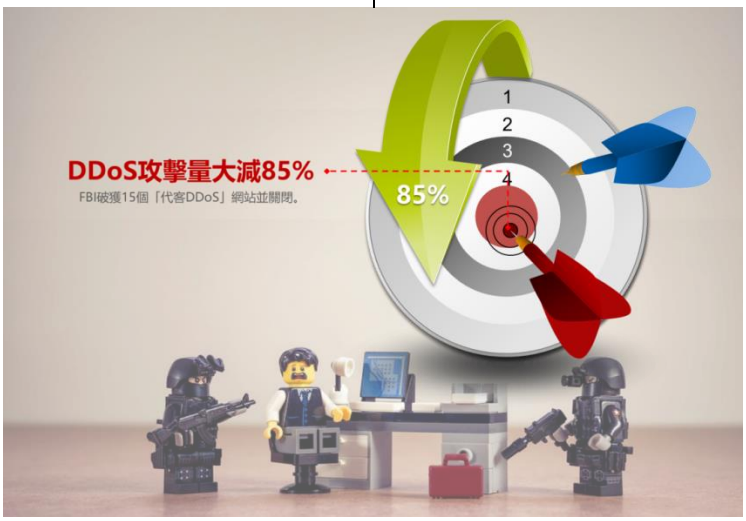
資安廠商 NexusGuard 發表研究報告，指出近期全球 DDoS 攻擊事件的量體，較過去大幅減少。

DDoS 減少的主因，是由於美國聯邦調查局在去年破獲了 15 個代客進行 DDoS 攻擊的網站，這些網站的網域也被美國司法部撤除。

研究報告指出，這些代客攻擊網站自 2014 年起，至少發動了二十萬起 DDoS 攻擊；而在 FBI 破獲這些網後，整體的 DDoS 攻擊事件，不論平均次數或最大攻擊量都大幅減少。

不過該單位也警告，雖然代客進行 DDoS 的攻擊減少了，但這只是 DDoS 攻擊形態的一種，透過 botnet 進行的 DDoS 攻擊仍十分常見，攻擊量體也未見降低。

- 資料來源：
  1. https://threatpost.com/threatlist-ddos-attack-sizes-drop-85-percent-post-fbi-crackdown/142907/
  2. https://www.nexusguard.com/threat-report-q4-2018



5.1.2 研究指出筆記型電腦 USB 插孔，比一般所知更易遭駭

英國劍橋大學與萊斯大學的最新研究指出，配備 USB C 連接埠的當代筆記型電腦，較一般認知更易遭到駭侵。

兩所大學的資安研究人員，日前在網路與分散式系統資安研究會上發表研究報告；報告指出目前用以保護筆記型電腦 USB 插孔的 IOMMU (輸出入記憶體管理單元)，並不足以完全發揮其應有的保護作用。

研究人員自製一稱為 Thunderclap 的測試工具，用以插入受測電腦 USB C 連接埠，觀察電腦反應；結果證實駭侵者能透過 USB 埠，順利取得受害電腦的控制權。可被駭入的系統包括 Windows、macOS、Linux 與 FreeBSD。

研究人員指出，許多透過 USB C 連接的裝置，都具有「直接記憶體存取」（DMA）能力，能夠跳過作業系統監控，存取電腦的主記憶體；IOMMU 的設計目的，就是要防止惡意裝置存取未經許可的記憶體內容，以免重要資料遭竊。然而該系統在許多電腦上是可以關閉的，甚至即使該系統開啟了，還是有被駭入的可能性。

研究人員建議用戶要經常更新作業系統，以取得最新漏洞修補；但更重要的是，要避免在自己的電腦上插入不明周邊裝置。

- 資料來源：
  1. https://www.cam.ac.uk/research/news/most-laptops-vulnerable-to-attack-via-peripheral-devices-say-researchers
  2. http://thunderclap.io/thunderclap-paper-ndss2019.pdf

5.2、 國際政府組織資安資訊

5.2.1 美國雲端企業服務大廠 Citrix 遭駭，6TB 文件恐遭伊朗駭客竊走

Iridium 駭客組織是使用一種稱為「密碼噴灑攻擊」(Password spraying attack) 的方式入侵 Citrix；這種方式是利用一些簡單的「萬用密碼」大量嘗試登入同一組織中的許多帳號，可以避免追蹤。

資安廠商 Resecurity 發表報告指出，該單位發現一名為「銥」(Iridium) 的伊朗駭侵團體，入侵了多個美國政府單位、承包商、瓦斯與石油公司，甚至包括企業雲端服務大廠 Citrix。

據報告指出，Citrix 是在去年耶誕假期間遭到 Iridium 駭入；除了這份報告外，FBI 也在今年三月六日前往 Citrix 進行相關調查。

據媒體報導，Citrix 共有多達 6TB 文件資料可能遭駭客竊取；至於文件含有哪些機密內容，目前仍在調查中。

由於 Citrix 提供許多美國政府單位和中大型企業的雲端服務，也包括遠端存取在內，所以這起駭侵事件中外流的機密資料可能牽連甚廣。

- 資料來源：
  1. https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network/
  2. https://resecurity.com/blog/supply-chain-the-major-target-of-cyberespionage-groups/
  3. https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

5.2.2 川金會進行時，北韓駭客持續攻擊美國與盟國單位

正當河內的川金會從籌備、兩人會面到破局，這段期間內北韓駭客依然沒有放鬆對美國及其歐洲盟友的網路攻擊力道。

紐約時報報導，近一年半來，北韓駭客不斷對美國、歐盟及其他盟邦的公家機關、私營企業等單位進行駭侵攻擊，甚至在川金會期間也不放鬆。

資安公司 McAfee 研究指出，自 2017 年以來，北韓駭侵團體不斷試圖駭入美國與其他盟國的銀行、公用事業、石油和瓦斯公司；不論雙方關係緊張還是和緩，攻擊行為都沒有減少。

McAfee 研究人員透過駭入北韓駭客使用的伺服器，直接即時目擊北韓駭客攻擊美國與世界其他國家公司行號的行為，受駭公司多達一百家以上。

駭客利用與北韓友好的納米比亞網路當做跳板，對各國重要公司的內部網路進行攻擊；攻擊目標主要分布在美國紐約、休士頓，以及主要盟邦重要城市的公司，如倫敦、馬德里、東京、特拉維夫、羅馬、曼谷、台北、首爾、東京、香港；甚至連俄羅斯和中國的城市也包括在內。

北韓駭客駭入這些公司的目的尚不明確，但遭攻擊的，多是公司的工程技術人員或高階主管，因為這些人能存取該公司機密資訊或智慧財產。

- 資料來源：
  1. https://www.nytimes.com/2019/03/03/technology/north-korea-hackers-trump.html
  2. https://www.thesun.co.uk/news/8555223/north-korean-hackers-hit-us-european-banks-trump/

5.2.3 亞洲多款遊戲於開發階段再遭中國駭侵團體「供應鏈攻擊」植入後門

多款亞洲遊戲與平台，遭中國駭侵團體之「供應鏈攻擊」（Supply-chain attack），於遊戲開發時便遭植入後門。

資安廠商 ESET 發表研究報告指出，亞洲的遊戲產業再次出現多起「供應鏈攻擊」案例，至少有兩款遊戲、一個遊戲平台，於開發過程中就遭駭客植入惡意程式。

ESET 指出，三個遭到駭入的遊戲產品或平台，雖然各自使用不同的植入手法，但都用了同一個後門。

使用同一後門、相同手法，同樣針對遊戲開發者的攻擊事件，在 2011 年也發生過；由 Kaspersy 在 2013 年揭發，並稱該組織為「Winnti」。ESET 認為這次事件同樣也和 Winnti 組織有關。

目前確認遭到攻擊的遊戲產品，有兩個已經移除其中的惡意軟體；但還有一個始終沒有處理。

- 資料來源：
  1. https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/
  2. https://securelist.com/winnti-more-than-just-a-game/37029/
  3. https://docs.microsoft.com/zh-tw/windows/security/threat-protection/intelligence/supply-chain-malware

5.2.4 中國新駭侵團體 APT40 鎖定海軍科技進行網路間諜活動

資安廠商 FireEye 發表報告，詳細描述中國新駭侵團體 APT40 的駭侵行為分析，結果發現該團體主要目標是取得海軍相關機密科技。

FireEye 在報告中指出，APT40 主要的攻擊目標，包括工程、運輸、國防工業和大學研究單位，目的在取得這些單位和海軍科技相關的機密資料。

研究也指出，受到攻擊的單位及其所屬國家，多半都和「一帶一路」有關，包括柬埔寨、比利時、德國、香港、菲律賓、馬來西亞、挪威、沙烏地阿拉伯、瑞士、美國、英國等。

報告也指出，APT40 除了以駭侵行動竊取重要技術機密資料，也意圖影響「一帶一路」相關國家選舉結果。

在 FireEye 的研究報告中，還分析了 APT40 使用的多種攻擊手法。

- 資料來源：
  1. https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html
  2. https://www.infosecurity-magazine.com/news/chinas-apt40-group-stole-navy-1-1/

5.2.5 印尼選委會指控中俄駭客意圖擾亂總統大選，憑空多出一千七百多萬幽靈選民

印尼選委會高官指出，該國總統大選的選民資料庫，刻正遭到來自中國與俄國的駭侵攻擊。

根據彭博新聞報導，即將在 4 月 17 日舉行總統大選的印尼，其選民資料庫遭到來自中國與俄羅斯的駭侵。

印尼選委會主席阿里夫．布迪曼指出，這些駭侵行動試圖操弄或竄改資料庫內的資料內容，像是大量產生幽靈人口或虛假的投票人身分。

布迪曼說，這些駭侵行動「不只天天發生，而且每個小時都在發生」；而目前他也無法確定這些行為的目的，是要阻擾總統大選順利進行，還是要扶植特定候選人。

印尼選委會目前正在積極調查整起事件，目前估計在選民資料庫中憑空出現一千七百五十萬個幽靈選民；去年的一場選舉也憑空出現了七十萬選民。不過印尼選委會也表示，這些駭侵行動將無法擾亂大選進行。

中國外交部否認印尼選委會的指控，稱該國一向不干擾他國內政，而且反對任何形式的駭侵行為；俄國當局也予以否認，克里姆林官發言人並且說這項指控是「沒有根據的」。

- 資料來源：
  1. https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers
  2. https://www.reuters.com/article/us-indonesia-election-idUSKBN1QU135

5.2.6 巴基斯坦政府網站遭駭客植入按鍵記錄軟體

巴基斯坦政府機關網站日前被發現遭駭客植入按鍵記錄軟體，可能已有數百人受害。

新加坡電信旗下的資安廠商 Trustwave 日前發表研究報告指出，該公司發現巴基斯坦主管移民與護照發放事務的政府官方網站，遭到駭客植入按鍵記錄軟體。

報告指出該網站被植入的是 Scanbox，用戶一旦在受感染的網站上登入，Scanbox 的 Javascript 程式就會收集用戶的各種資訊，包括使用的電腦和所有按鍵。Scanbox 是許多「先進長期威脅」（Advanced Persistent Threat）駭侵組織常用的惡意軟體。

該網站的功能主要供巴基斯坦護照申請者追蹤申請進度，Trustwave 是在三月二日首次發現該站遭植入 Scanbox，光是當天就有至少七十人被 Scanbox 竊取資料，其中三分之二還輸入了登入資訊。

Trustwave 指出，雖然他們立即通報巴基斯坦當局，但並沒有收到回應，而該網站內的 Scanbox 也尚未移除。二月底時孟加拉駐開羅大使館網站也遭到同類攻擊。

- 資料來源：
  1. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/attacker-tracking-users-seeking-pakistani-passport/
  2. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/bangladesh-embassy-website-in-cairo-compromised/

5.2.7 全球級鋁業公司 Norsk Hydro 遭勒贖軟體癱瘓，被迫切回手動生產

全球規模數一數二的鋁業公司挪威海德魯，於 19 日遭猛烈的勒贖軟體駭侵攻擊，數個鋁品生產線被迫切回手動操作模式。

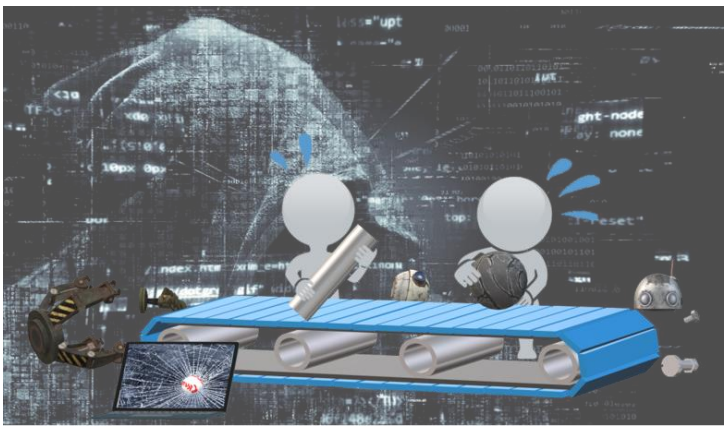
全球規模數一數二的鋁業公司挪威海德魯(Norsk Hydro)，於本周二(19日)遭到猛烈的勒贖軟體駭侵攻擊；目前該公司各種資訊設備均被迫離線，數個鋁品生產線被迫切回手動操作模式，連官方網站也無法正常運作。

挪威國安局表示，攻擊 Norsk Hydro 的惡意軟體名為 LockerGoga，是一種新出現的勒贖軟體；一旦中毒，電腦裡的檔案會被加密，歹徒藉此要脅支付高額贖款。

LockerGoga 對 Norsk Hydro 造成的影響十分巨大，除了位在挪威本土和美國的數個工廠無法以電腦運作之外，該公司的內部網路和資訊系統也無法使用，員工被迫使用電話、手機或平板透過外部服務繼續工作。

Norsk Hydro 沒有透露歹徒要求的贖金數額，也未公開因此受到的損害估計；該公司也表示不打算支付贖款。他們擁有完善的備份，目前正在逐步從備份檔回復系統和資料。

- 資料來源：
  1. https://www.zdnet.com/article/aluminium-producer-switches-to-manual-operations-after-extensive-cyber-attack/
  2. https://www.reuters.com/article/us-norsk-hydro-cyber/aluminum-producer-hydro-hit-by-cyber-attack-shuts-some-plants-idUSKCN1R00NJ
  3. https://www.bbc.com/news/technology-47624207



5.2.8 上周遭勒贖軟體癱瘓的挪威海德魯鋁業公司，部分業務已逐漸復原

挪威海德魯(Norsk Hydro)鋁業公司，在歷經嚴重的勒贖軟體 LockertGoga 攻擊，導致生產和各項業務近乎癱瘓後，目前已經大部分恢復正常作業。

根據挪威海德魯公司發表的消息，該公司在歷經一星期的備份復原和搶修工作後，大部分業務已經恢復正常運作。

受影響最嚴重的鋁擠型生產部門，目前的稼動率約達正常水準的八成左右；但仍有部份事業單位的運作陷於停頓，也還有不少單位仍需仰賴手動操作。

該公司並未對後續可能的攻擊掉以輕心。該公司警告所有合作伙伴和客戶，小心任何看似來自該公司寄出的不明信件；若有疑問應先與該公司連絡，確認信件真偽。

據 ZDNet 報導，挪威海德魯鋁業因這次勒贖攻擊的所有損失，估計超過四千萬美元；其中包括因生產受阻而未能實現的營收。這部分的損失是否能得到保險賠償，目前仍有待觀察。

- 資料來源：
  1. https://twitter.com/NorskHydroASA/status/1110521624703524864
  2. https://www.hydro.com/nl-nl/media/news/2019/update-on-cyber-attack-march-26/
  3. https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week/

5.2.9 英國國安單位：華為整體資安架構存有嚴重的系統化弊病

英國國安單位發表調查報告，指出雖然沒有直接證據證明華為資安問題和中國政府監控有關，但華為的資安架構存有明顯的技術問題；一但採用華為設備，可能對英國的通訊網路安全造成威脅。

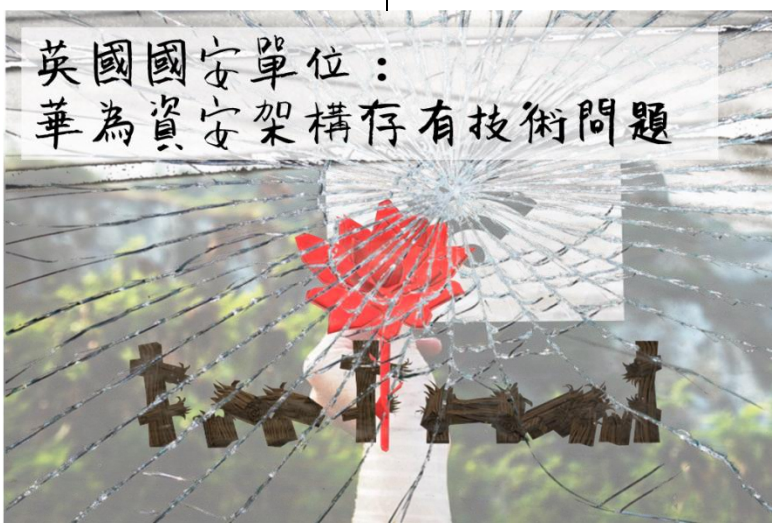
英國國家安全委員會(National Security Advisor)於日前發表針對華為網通產品與其企業資安風險的調查報告。報告中指責華為公司在軟體開發和資安防護能力上「存有嚴重且系統化的弊病」。

報告指出，調查發現華為公司的軟體開發流程存有許多基本上無法容忍的疏漏，這些都可能提供駭侵團體可乘之機；而該公司的整體資安意識也十分薄弱。

報告也說，如果華為沒有改善其軟體開發和公司治理的資安強度，未來英國境內的電信網路若是採用華為設備，針對未來的資安危機風險管理將會十分困難。

華為公司針對此事表示，該公司已經初步投入二十億美元，用以加強華為產品的軟體開發流程的資安防護。

- 資料來源：
  1. https://techcrunch.com/2019/03/28/uk-report-blasts-huawei-for-network-security-incompetence/
  2. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf



5.3、 社群媒體資安近況

5.3.1 Facebook 承認用明碼文字檔儲存數億用戶密碼

Facebook 被踢爆多年來一直以未加密的明碼純文字檔儲存數億用戶密碼，而且任何 Facebook 企業內的人均可存取。

資安廠商 KrebsOnSecurity 發表新聞稿，指出自 2012 年以來，Facebook 便以未加密的明碼純文字檔儲存數億用戶密碼於公司內部的伺服器上；稍後 Facebook 也承認該報導。

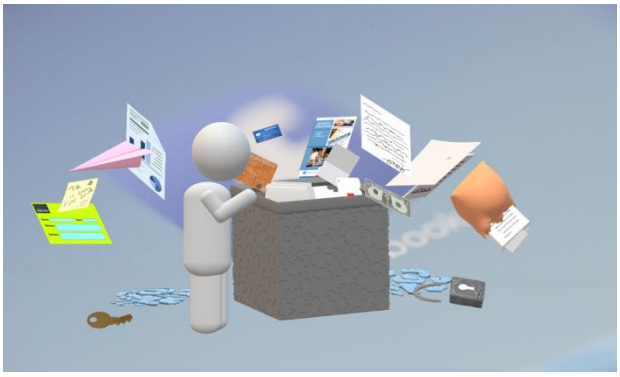
Facebook 在稍晚發表的說明中指出，約有二億到六億 Facebook 用戶的密碼以明碼儲存，而且 Facebook 二萬名員工均可存取。不過 Facebook 認為這些密碼不曾向外流出。

KrebsOnSecurity 的報告也指出，根據匿名 Facebook 工程師查閱存取記錄，發現這些年來約有二千名臉書工程師或開發者存取過這些密碼檔，存取次數則達到九百萬次。

Facebook 表示，近期將會通知數億名 Facebook Lite 與數萬名 Instagram 用戶關於密碼存放風險的問題與指南。

同樣的問題不只發生在 Facebook，Twitter 和 Github 也承認過去曾以明碼存放用戶密碼。

- 資料來源：
  1. https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years/
  2. https://arstechnica.com/information-technology/2019/03/facebook-developers-wrote-apps-that-stored-users-passwords-in-plaintext/
  3. https://newsroom.fb.com/news/2019/03/keeping-passwords-secure/



5.3.2 新發現透過 GitHub 和 Slack 進行的定位攻擊事件

資安廠商趨勢科技發表報告指出，該公司研究人員發現一種全新、針對特定人員攻擊方式，特色在於利用 GitHub 和 Slack 進行誘騙駭侵。

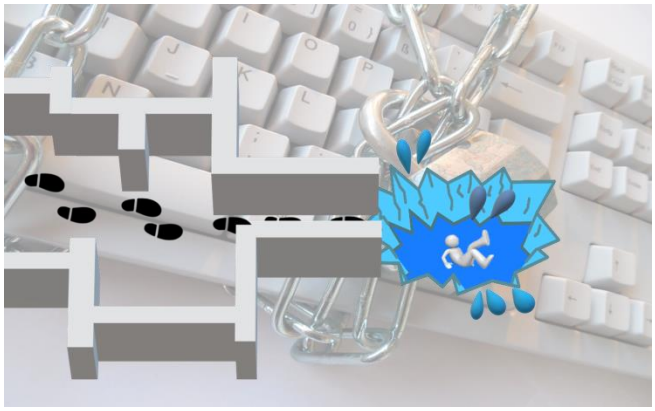
據趨勢科技指出，該攻擊事件是一種典型的「水坑攻擊」，也就是誘導特定受害者進入某個遭到植入惡意軟體的網站，而該網站是這些受害者可能想要造訪的目標。

以這次攻擊事件來說，駭侵者是利用 Windows 系統中一個已知的安全漏洞 CVE-2018-8174，讓受害電腦下載具備後門的惡意程式，從而竊取用戶的敏感資訊，特別是和受害者個人相關的各種資訊。

值得注意的是，由於駭侵者透過程式設計師常用的程式碼發布平台 GitHub 和即時溝通平台 Slack 引人入坑，因此針對特定身分人士進行駭侵的意圖極為明顯。這也是趨勢科技首次發現用這種管道散布的攻擊手法。

在趨勢科技通報後，Slack 表示已經立即移除相關惡意檔案，並且關閉駭侵者使用的 Slack workplace。Slack 本身的系統並未遭到入侵。 GitHub 也立即進行了相應的處理，移除駭侵者存放的相關檔案。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/new-slub-backdoor-uses-slack-github-as-communication-channels/
  2. https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/



5.4、軟體系統資安議題

5.4.1 再也不用記密碼了！
W3C 正式批准全新網頁安全登入協定 WebAuthn

全球網頁標準協會 W3C 昨天宣布批准一項全新的網頁安全登入協定 WebAuthn，最大的好處就是支援多種用戶端的安全登入方式，而且不再於伺服器端儲存登入帳號與密碼。

新的 WebAuthn 是一組公開的 API，支援該技術的網站可讓用戶透過各種生物特徵（如指紋、面孔辨識）、行動裝置或 FIDO 安全鎖等登入網站，無需輸入帳號密碼。

支援 WebAuthn 的網站，將不再需要儲存用戶的帳號和密碼，因此駭客無法透過攻擊網站伺服器取得帳密的方式，偽裝成用戶本人登入；用戶也不再需要記憶又臭又長的密碼，或使用密碼管理工具。

目前 Android 和 Windows 10 已經內建 WebAuthn 支援，Google Chrome、Mozilla Firefox 和 Microsoft Edge 也在正式版中支援 WebAuthn，Apple Safari 目前則是在去年 12 月起的測試版本中支援了 WebAuthn。

- 資料來源：
  1. https://venturebeat.com/2019/03/04/w3c-approves-webauthn-as-the-web-standard-for-password-free-logins/
  2. https://www.w3.org/TR/webauthn/

5.4.2 微軟大量釋出三月份重大更新檔案

三月的微軟周二更新日，微軟再度釋出多個重大更新。

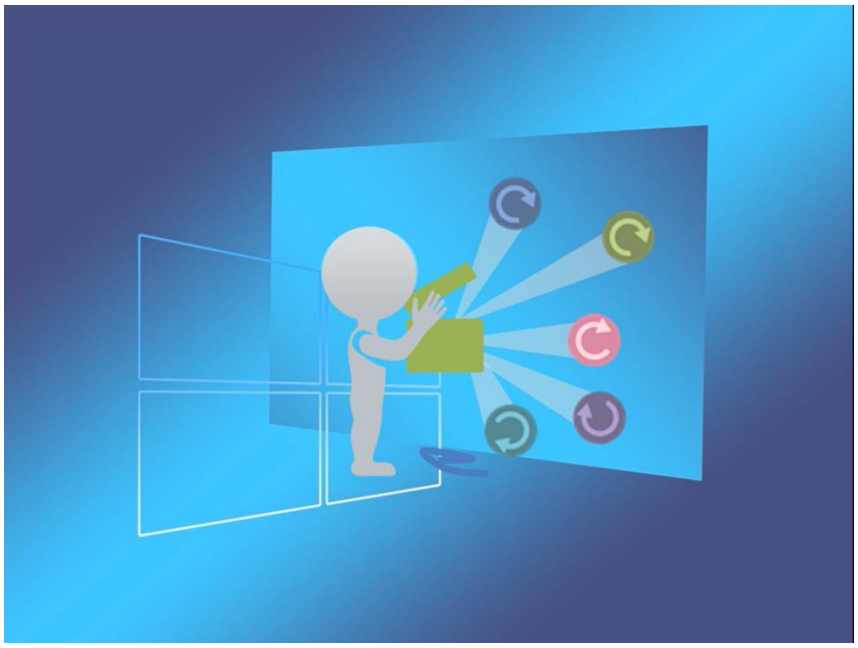
這次微軟一共釋出多達 64 個軟體更新，其中包括 17 個嚴重（Critical）等級的更新，以及 2 個針對零日漏洞的更新。

在獲得修補的漏洞中，有多個屬於可供駭侵者遠端執行程式碼的嚴重漏洞。

這批更新檔修補的產品，包括 Adobe Flash Player、IE 瀏覽器、MS Edge 瀏覽器、MS Windows 作業系統、MS Office 與 SharePoint、ChakraCore、Team Foundation Server、企業用 Skype、Visual Studio 及 NuGet。

建議所有 Windows 和 Office 用戶，立即透過 Windows Update 等官方管道安裝更新檔。

- 資料來源：
  1. https://www.ghacks.net/2019/03/12/microsoft-windows-security-updates-march-2019-overview/
  2. https://www.us-cert.gov/ncas/current-activity/2019/03/12/Microsoft-Releases-March-2019-Security-Updates
  3. https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/ac45e477-1019-e911-a98b-000d3a33a34d
  4. https://portal.msrc.microsoft.com/en-us/security-guidance



5.4.3 偽造的瀏覽器更新通知再度泛濫，可能導致電腦遭勒贖

資安研究單位發現偽造瀏覽器更新通知的惡意活動再度增加，會在用戶電腦或手機中安裝勒贖軟體。

資安研究網站 Security Boulevard 指出，最近該站發現偽造瀏覽器更新通知的惡意活動再度增加；當受害者誤判而安裝了「更新軟體」時，實際上可能被安裝勒贖軟體或會入侵網銀的惡意軟體。

Security Boulevard 指出，受害者在瀏覽含惡意軟體的網站時，會看到偽造的「更新中心」彈跳視窗，指出「瀏覽器發生嚴重錯誤 (Critical error)，需立即更新，否則可能造成資料損壞、個資外流等問題」；當用戶按下更新按鈕後，實際上下載的是惡意軟體。

該報導指出，下載的惡意軟體會偽裝成 JPG 檔案，除了 Windows 電腦易受攻擊外，甚至還有 Android 版本。許多以 WordPress 網站都遭到感染，駭客多半是將惡意程式碼塞在 footer.php 這支 WordPress 系統程式中。

常見的掃毒軟體大多可成功發現並提出警告，該報告也建議網站經營者也應在伺服器端安裝掃毒軟體，避免自己的網站被駭客注入惡意程式碼。

- 資料來源：
  1. https://securityboulevard.com/2019/02/fake-browser-updates-push-ransomware-and-bank-malware/

5.4.4 WinRAR 先前修補好的長年漏洞，已用於多起 APT 攻擊事件

先前被發現且存在長達十餘年的 WinRAR 漏洞，雖然已經修復，但仍遭多個駭侵組織用於攻擊事件。

先前本中心報導過的 WinRAR 安全漏洞，雖已在日前修復，但資安研究單位仍發現多個駭侵組織利用此漏洞發動攻擊，其中甚至包括多個 APT 駭侵組織在內。

WinRAR 的漏洞 CVE-2018-20250 主要是用以解壓 ACE 檔案的程式庫久未更新所致；而當資安公司 Check Point 公布該漏洞數日後，就出現利用該漏洞進行的攻擊事件。McAfee 更指出，漏洞公布後一周內，該公司就偵測到超過百起基於該漏洞的駭侵事件。

該漏洞的問題在於駭侵者可將惡意檔案置於用戶電腦的開機啟動目錄，因此能夠感染用戶電腦。McAfee 指出，典型的攻擊手法是將檔案偽裝成用戶可能感興趣的相簿檔；當用戶解壓縮時，會解出一些 MP3 檔案，但其開機啟動目錄內也會被塞入惡意軟體，而用戶對此將一無所知。

南韓和中國資安廠商也都偵測到類似的攻擊事件，其中某些事件疑為 APT 駭侵團體所為。

建議 Windows 電腦用戶如有安裝 WinRAR，應立即更新至最新版本。

- 資料來源：
  1. https://www.twcert.org.tw/subpages/securityInfo/securitypolicy_details.aspx?id=810
  2. https://www.securityweek.com/recently-patched-winrar-flaw-exploited-apt-attacks
  3. https://www.securityweek.com/winrar-vulnerability-exposes-millions-users-attacks
  4. https://twitter.com/WinRAR_RARLAB/status/1100358049993240577

5.4.5 含有八億有效用戶資料的龐大資料庫，全無保護，任人存取

資安研究人員發現一個內含近八億一千萬個 Email 帳號與各種個資的資料庫，竟然未有任何保護措施，放在網上任人存取。

上周資安研究人員 Bob Diachenko 和 Vinny Troia 發現，在網址 Verifications.io 之下，存有一個檔案大小達 150GB，內含超過八億筆用戶資料的 MongoDB 資料庫，沒有任何保護措施，任何人皆可存取。

這家 Verification.io 公司，本身並不是 Email 行銷業者；其主要業務是透過各種方法確認 Email 為有效信箱，因此資料庫中 Email 真實比率相當高。

除 Email 地址外，資料庫還包含許多重要行銷用資料，包括姓名、Email 地址、電話號碼、實體地址、性別、生日、個人貸款額、利率、社群平台帳號、信用評等、公司名稱、年營收額、傳真號碼、公司網址、公司分類等等。

目前尚不清楚除研究者之外，是否還有人存取過這一大筆資料；Verification.io 也已將資料庫撤下網路。

- 資料來源：
  1. https://securitydiscovery.com/800-million-emails-leaked-online-by-email-verification-service/
  2. https://www.wired.com/story/email-marketing-company-809-million-records-exposed-online/

5.5、軟硬體漏洞資訊

5.5.1 研究人員再次發現 Intel 處理器安全漏洞，且修補不易

英國 IT 媒體 The Register 報導，Intel 處理器再次被研究人員發現嚴重資安漏洞，惡意軟體可以利用該漏洞取得權限，任意存取記憶體內的所有資料。

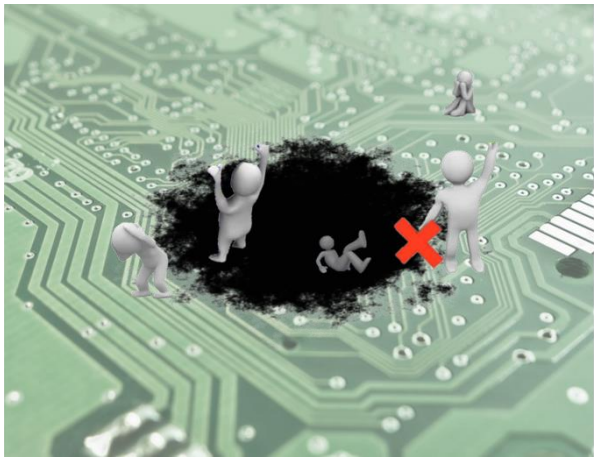
美國伍斯特理工學院(Wocester Polytechnic Institute)與德國呂貝克大學(Universität zu Lübeck)資安研究人員發表研究報告指出，這稱為「The Spoiler」的資安漏洞，和一年多前被爆出的 Intel 「Spectre」漏洞一樣，都源於處理器為加快計算效能所需「預執行」(Speculative Execution)功能。

透過這個漏洞，惡意程式可直接取得記憶體內的資料；而且只要在瀏覽器內執行特定的 Javascript 即可做到。

研究人員同時指出，這個漏洞屬於硬體的問題，而且從 Intel Core 一代處理器以來就存在；由於修正硬體錯誤極為困難耗時，因此可能要用好幾年的時間才能在新世代處理器中與以更正。同樣的錯誤則並未出現在 AMD 處理器上。

- 影響產品：
  Intel Core 架構所有處理器
- 解決辦法：
  目前尚無解決方案。

- 資料來源：
  1. https://arxiv.org/pdf/1903.00446.pdf
  2. https://www.theregister.co.uk/2019/03/05/spoiler_intel_processor_flaw/



5.5.2 Windows 10 與 Windows Server 2019 DHCP 存有可遠端執行程式碼的漏洞

資安廠商 Positive Technologies 指出，在 Windows 10 與 Windows Server 2019 發現 DHCP 漏洞，可讓入侵者遠端執行程式碼；建議用戶儘速透過 Windows Update 更新系統以修補漏洞。

該報告指出，駭侵者可以利用自己的電腦設定 DHCP 伺服器，當收到要求協助設定網路的 DHCP 要求時，該伺服器會送出變造的封包；以 Windows 10 電腦為例，每隔數小時就會發出 DHCP 要求並更新網路租約，攻擊者可利用此漏洞在受害電腦上執行任意程式碼。

該報告亦指出，某些網路上，攻擊者可透過手機或平板發動此類攻擊。

- CVE 編號：
  - CVE-2019-0697
  - CVE-2019-0726

- 影響產品：
  - Windows 10 各平台版本
  - WIndows Server 2019 各平台版本

- 解決辦法：
  透過 Windows Update 安裝微軟 2019 年三月更新修補程式。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0697
  2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0726
  3. https://www.techrepublic.com/article/windows-10-dhcp-vulnerability-allows-for-remote-code-execution/

5.5.3 Google Chrome 瀏覽器存在安全漏洞，允許攻擊者遠端執行任意程式碼，請儘速確認並進行修正

Google 安全研究團隊發現，Google Chrome 瀏覽器存在使用釋放後記憶體(use-after-free)漏洞，攻擊者可藉由誘騙使用者點擊含有惡意程式碼的連結，導致遠端執行任意程式碼。

- CVE 編號：
  - CVE-2019-5786
- 影響產品：
  Google Chrome 72.0.3626.119(含)以前版本
- 解決辦法：
  請更新 Google Chrome 瀏覽器至 72.0.3626.121 後版本，更新方式如下：
  1. 開啟瀏覽器，於網址列輸入 chrome://settings/help，瀏覽器將執行版本檢查與自動更新
  2. 點擊「重新啟動」完成更新
- 資料來源：
  1. https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop.html
  2. https://thehackernews.com/2019/03/update-google-chrome-hack.html
  3. https://www.ithome.com.tw/news/129152

5.5.4 Mozilla Firefox 瀏覽器存在安全漏洞，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

根據 Mozilla 發布的安全性公告顯示，Mozilla Firefox 瀏覽器由於別名資訊不正確或類型混淆等原因，導致存在可繞過邊界檢查(Bounds check)而產生緩衝區溢位問題，及可對記憶體任意進行讀取與寫入之漏洞(CVE-2019-

9810 與 CVE-2019-9813)。攻擊者可藉由誘騙使用者點擊含有惡意程式碼的連結，導致遠端執行任意程式碼。

- CVE 編號：
  - CVE-2019-9810
  - CVE-2019-9813
- 影響產品：
  - Mozilla Firefox 66.0(含)以前版本
  - Mozilla Firefox ESR 60.6.0(含)以前版本
- 解決辦法：
  1. 請確認瀏覽器版本，點擊瀏覽器選單按鈕，點選「說明」→「關於 Firefox」，可查看當前使用的 Mozilla Firefox 瀏覽器是否為受影響之版本。
  2. 更新方式如下：
     (1) 開啟瀏覽器，點擊選單按鈕，點選「說明」→「關於 Firefox」，瀏覽器將執行版本檢查與更新。
     (2) 點擊「重新啟動以更新 Firefox」完成更新。
  3. 保持良好使用習慣，請勿點擊來路不明的網址連結。
- 資料來源：
  1. https://www.mozilla.org/en-US/security/advisories/mfsa2019-09/
  2. https://www.tenable.com/plugins/nessus/123012
  3. https://www.ghacks.net/2019/03/23/mozilla-releases-security-updates-firefox-66-0-1-and-60-6-1-esr/

5.5.5 Apache Solr 存在安全漏洞，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

Apache Solr 是開放原始碼的全文檢索伺服器，以 Lucene 程式庫為核心，進行全文資料的解析、索引及搜尋。

研究人員發現，Solr 的 ConfigAPI 允許攻擊者透過 HTTP POST 請求修改 jmx.serviceUrl 內容，將 JMX 伺服

器指向惡意 RMI/LDAP 伺服器，再運用 Solr 不安全的反序列化功能(ObjectInputStream)，進而導致遠端執行任意程式碼。

- CVE 編號：
  - CVE-2019-0192
- 影響產品：
  - Apache Solr 5.0.0 至 5.5.5 版本
  - Apache Solr 6.0.0 至 6.6.5 版本
- 解決辦法：

  目前 Apache 官方已針對此弱點釋出修復版本，可聯絡系統維護廠商或參考以下建議進行：

  1. 更新時，建議進行測試後再安裝更新。
  2. 可於系統輸入指令「solr version」確認目前使用的版本。若為上述受影響版本，可採取下列措施：

     (1). 更新 Apache Solr 至 7.0 以後版本。

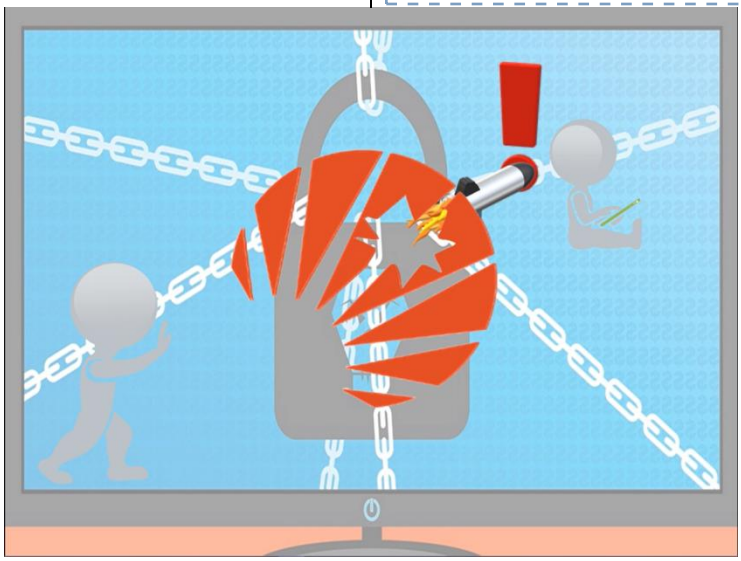
     (2). 若無法立即更新 Solr 版本，可進行下列替代措施：

     a. 停用 ConfigAPI：請執行 Solr 並開啟系統屬性，將 disable.configEdit 設置為 true

     b. 下載 SOLR-13301.patch 並且重新編譯 Solr，下載連結網址如下：https://issues.apache.org/jira/secure/attachment/12961503/12961503_SOLR-13301.patch

     c. 只允許受信任的來源電腦存取 Solr 伺服器

- 資料來源：
  1. https://issues.apache.org/jira/browse/SOLR-13301
  2. https://vulmon.com/vulnerabilitydetails?qid=CVE-2019-0192
  3. http://mail-archives.us.apache.org/mod_mbox/www-announce/201903.mbox/%3CCAECwjAV1buZwg%2BMcV9EAQ19MeAWztPVJYD4zGK8kQdADFYij1w%40mail.gmail.com%3E



5.5.6 Cisco 三款 VPN 路由器產品存在安全漏洞，允許遠端攻擊者執行任意程式碼，請儘速確認並進行修正

研究團隊發現 Cisco RV110W、RV130W 及 RV215W 三款 VPN 路由器產品存在安全性漏洞，肇因於此三款產品之網頁管理介面程式未完整驗證用戶提交的資料，導致未經授權的遠端攻擊者可針對目標設備發送特製的 HTTP 請求，進而造成遠端攻擊者可以管理員權限執行任意程式碼。

- CVE 編號：
  - CVE-2019-1663
- 影響產品：
  - RV110W Wireless-N VPN Firewall：韌體版本 1.2.2.1 以前的所有版本
  - RV130W Wireless-N Multifunction VPN Router：韌體版本 1.0.3.45 前的所有版本
  - RV215W Wireless-N VPN Router：韌體版本 1.3.1.1 前的所有版本
- 解決辦法：

  目前 Cisco 官方已針對此弱點釋出修復版本，可聯絡設備維護廠商或參考以下建議進行更新：

  1. 連線至網址：https://software.cisco.com/download/home，點擊「Browse All」按鈕。
  2. 按照型號下載更新檔：
     (1). RV110W Wireless-N VPN Firewall：

     點擊「Routers > Small Business Routers > Small Business RV Series Routers > RV110W Wireless-N VPN Firewall > Wireless Router Firmware」選擇 1.2.2.1 或後續版本進行下載。

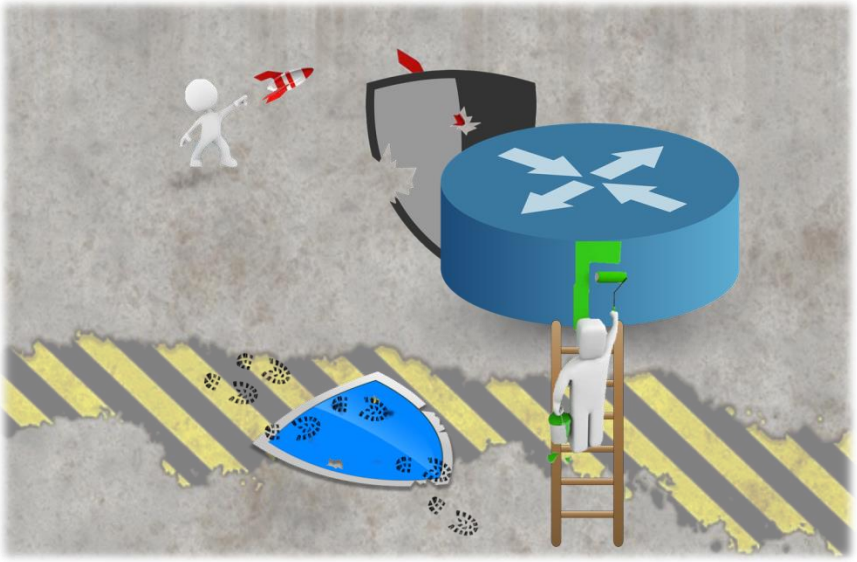
     (2). RV130W Wireless-N Multifunction VPN Router：

     點擊「Routers > Small Business Routers > Small Business RV Series Routers > RV130W Wireless-N Multifunction VPN Router > Small Business Router Firmware」選擇 1.0.3.45 或後續版本進行下載。

     (3). RV215W Wireless-N VPN Router：

     點擊「Routers > Small Business Routers > Small Business RV Series Routers > RV215W Wireless-N VPN Router > Wireless Router Firmware」選擇 1.3.1.1 或後續版本進行下載。
  3. 使用設備之管理頁面功能進行韌體更新。

- 資料來源：
  1. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-rmi-cmd-ex
  2. https://www.ithome.com.tw/news/129047



第 6 章、 資安研討會及活動

ICANN APAC-TWNIC Engagement Forum	
活動時間	2019/4/16 – 4/17
活動地點	臺大醫院國際會議中心
活動網站	https://forum.twnic.net.tw/2019/
活動概要	 ICANN 及 TWNIC 共同舉辦合作交流論壇 (ICANN APAC-TWNIC Engagement Forum)，集合了網路相關利害關係人與國際相關網路社群，針對域名、IP 位址及網路安全等主題，進行深入議題探討，這將是台灣與國際網路利害關係人共同面對面討論全球網路議題的最佳機會。 ICANN 及 TWNIC 建立論壇平台的目的，是讓地區內之網路相關利害關係人，可在「一個世界、一個網路」的目標下，以合作交流論壇建立一個共同合作、討論與鏈結的全球網路社群。 我們需要您的參與，為「一個世界、一個網路」共同發聲！ The ICANN APAC-TWNIC Engagement Forum is a joint effort of the two Internet organizations to bring the stakeholders of the Internet together with the local and international communities to share and discuss the latest topics on Internet policies, domain name, IP address allocation, and cybersecurity. It is the best chance to meet, discuss and share your opinions on the latest issues and know the stakeholders in Taiwan. It is also our goal to establish a platform for the communities to ignite the discussions from a variety of aspects of stakeholders and to keep pace with dynamic technologies and rapid innovation. With our goal "One World. One Internet.", facilitating we work together, discuss together, connect together under the global community as One.

	We need you to participate and voice out for the One Internet!

2019 年資訊安全列車系列-政府暨教育界資訊安全研討會	
活動時間	2019/4/23、2019/4/25、2019/4/26
活動地點	台北場—集思台大國際會議中心蘇格里底廳 台中場—順天經貿廣場 高雄場—國立科學工藝館 S105 階梯教室
活動網站	http://www.software.acer.net/webc/html/activity/show.aspx?num=283&page=1
活動概要	● 指導單位：行政院人事行政總處 ● 主辦單位：中華民國資訊安全學會 ● 協辦廠商：宏碁資訊服務(股)商用軟體事業單位公營業務處 ● 演講主題： ✓ 資安專題演講/台北場：區塊鏈應用之限制與安全性考量 ✓ 資安專題演講/台中高雄場：區塊鏈在數據分析與保全的應用 ✓ 機關資安實務分享：公務機關落實資安法的挑戰 ✓ 基礎建設的資安防禦 ✓ 政府暨企業進階管理與安全防護：以 windows 10 為例 ✓ 全方位公務機關辦公環境：資安/效率/維護

2019 亞太資訊安全論壇暨展會	
活動時間	2019/5/8 – 5/10
活動地點	台北世貿南港展覽館
活動網站	https://secutechinfosecurity.tw.messefrankfurt.com/taipei/zh-tw/visitors/welcome.html
活動概要	2019 年第十八屆(年) 亞太資訊安全論壇暨展會，《資安人》媒體，將於三天展覽會會場上，從四個主軸出發深入探討資訊安全議題: 觀念：與法規同步，與協同合作夥伴共同推動資安關鍵角色的重要性。 ● 組織：企業組織設立專職單位與專職資訊安全人員。 ● 管理：採用工具的評估讓觀念具體呈現其效力。 ● 技術：新型態網路部署規劃，建置。

	3 天論壇，10 個關鍵資安主題，50 場演講 + 攤位展示。 ● 資安議題方向： ✓ 資安管理與法規 (Security Management and Compliance) ✓ 網際威脅 (Cybersecurity) ✓ 雲端與行動安全 (Cloud & Mobile Info Security) ● 資安與監控安防聯網 ✓ 資安議題：Infra Security、Endpoint、Application Security、Wireless、Cloud、Mobile Security、SIEM、Incident Response、Identity Management ..... 歡迎各界、資安領域廠商們參與，展現您們的優秀產品與高品質的服務。

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.

第 7 章、 2019 年 3 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。

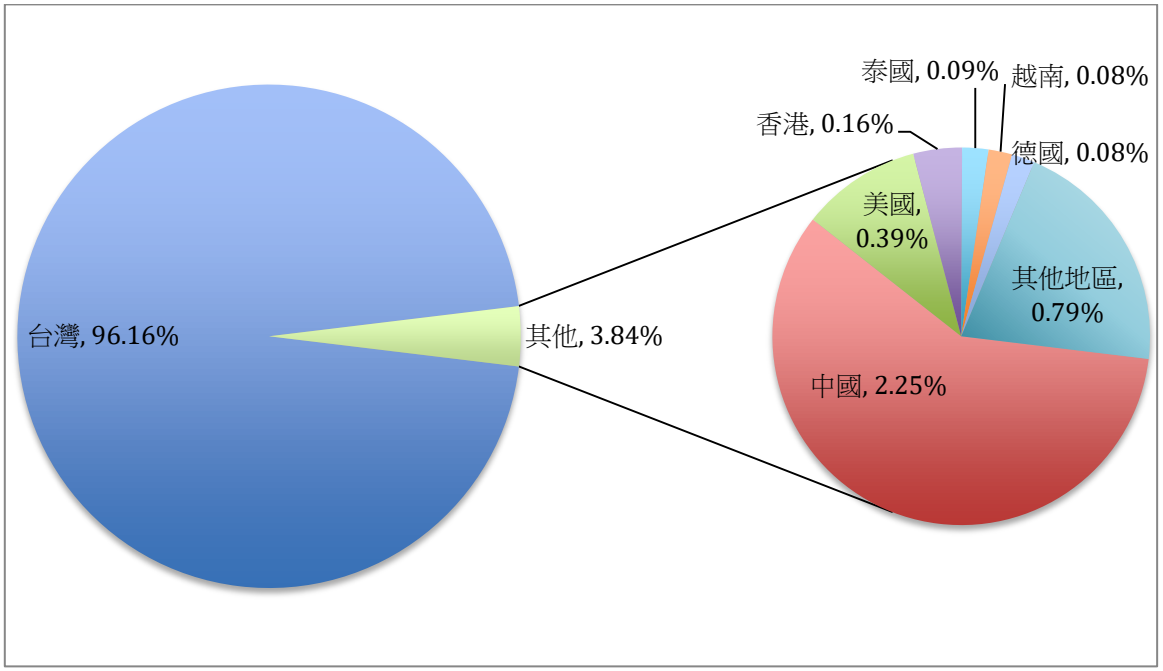


圖 1、通報地區統計圖

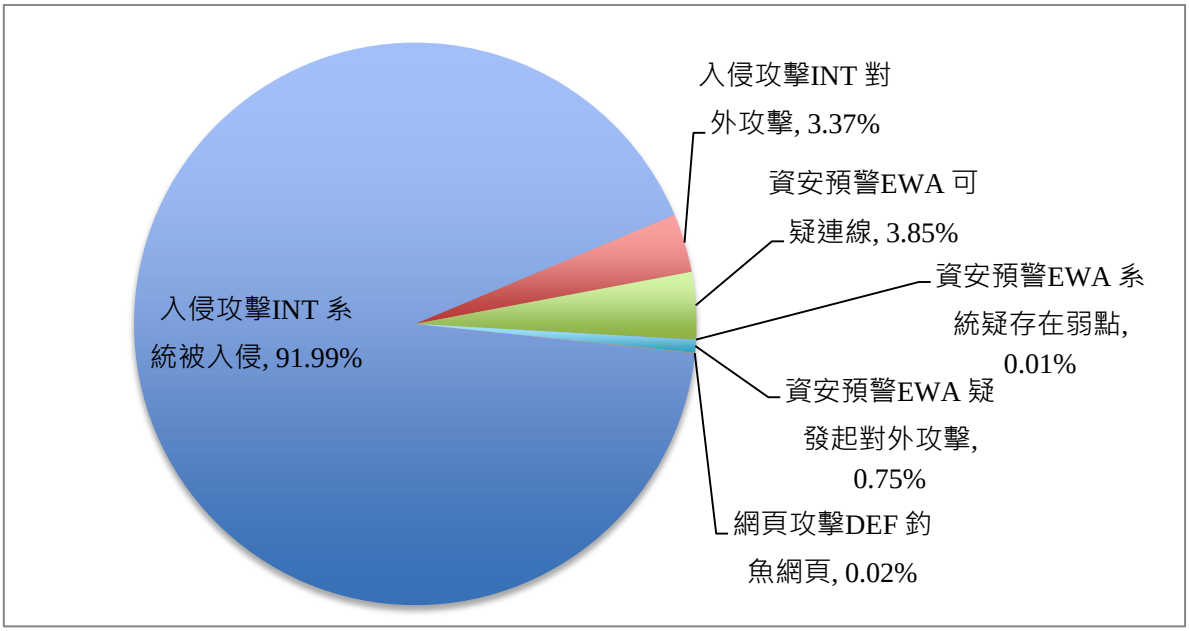

入侵攻擊INT 對外攻擊, 3.37%
資安預警EWA 可疑連線, 3.85%
資安預警EWA 系統疑存在弱點, 0.01%
資安預警EWA 疑發起對外攻擊, 0.75%
網頁攻擊DEF 釣魚網頁, 0.02%
入侵攻擊INT 系統被入侵, 91.99%

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 4 月 10 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/

電子報線上閱覽：https://blog.twnic.net.tw/