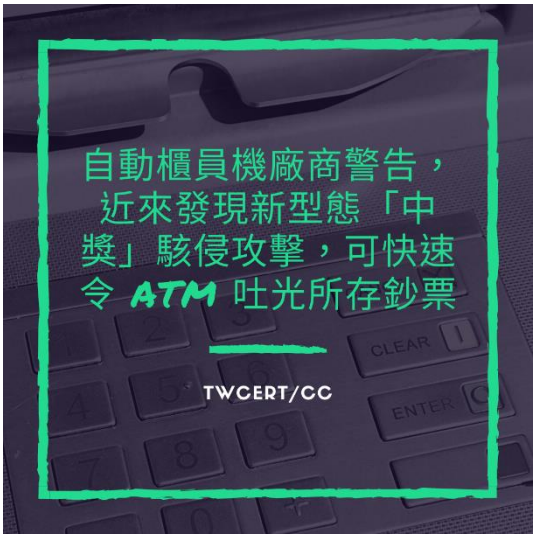
TWCERT/CC 資安情資電子報

2020 年 8 月份

目錄

第 1 章、 封面故事

自動櫃員機廠商警告，近來發現新型態「中獎」駭侵攻擊，可令 ATM 吐光所存鈔票



全球最大自動櫃員機（ATM）廠商發出警訊，指出最近出現新型態的「中獎」攻擊（Jackpotting）；駭侵者可讓 ATM 在極短時間內吐光機身存放的所有鈔票。

全球最大自動櫃員機（ATM）廠商 Diebold Nixdorf 日前發出警訊，指出最近出現新型態的「中獎」攻擊（Jackpotting）；駭侵者以實體入侵的方式，可讓 ATM 在極短時間內吐光機身存放的所有鈔票。

據廠商指出，這種新型態的中獎攻擊者，使用一種特製的入侵專用硬體，而且執行的軟體有一部分是該廠自己出的軟體工具；駭侵者以鑽洞破壞 ATM 機身或破壞機箱鎖的方式，將入侵裝置連上 ATM 後，即可命令 ATM 以極快的速度（每 23 秒送出 40 張鈔票）全數送出機身內存放的鈔票。

據廠商發出的通報指出，近期這類攻擊發半發生在歐洲國家，被攻擊的 ATM 機型多為 ProCast 終端機，其中大部分是 ProCast 2050xe USB。

過去的 Jackpotting 中獎攻擊，攻擊者使用的駭侵工具（俗稱「黑盒子」），內部的軟體多半是駭侵者自行開發的工具，用來模擬成 ATM 內部控制用的 PC 主機；除了竊取 ATM 內存放的鈔票之外，也會竊取金融卡或信用

卡資訊。

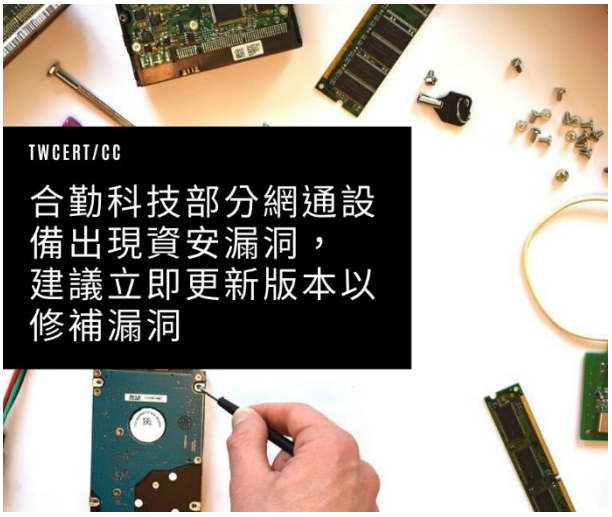
資安專家指出，以這次的新型態 Jackpotting 而言，雖然並不會竊取一般用戶的金融卡、信用卡資訊，但卻能取得並利用 ATM 製造商自己的軟體工具來製作黑盒子，可以說是個嚴重的警訊。

- 資料來源：
  1. https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/diebold-nixdorf-security-alert-2.pdf
  2. https://www.wired.com/story/thieves-are-emptying-atms-using-a-new-form-of-jackpotting/
  3. https://arstechnica.com/information-technology/2020/07/crooks-are-using-a-new-way-to-jackpot-atms-made-by-diebold/

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、合勤科技部分網通設備出現資安漏洞，建議立即更新版本以修補漏洞



合勤科技在 2020 年 2 月中接獲美國 CERT/CC 通報，其 NAS、防火牆（ATP/USG/VPN 系列）等網通設備，存在系統漏洞。

合勤科技在接獲通報後，即刻在五個工作天內完成內部清查、釋出修補韌體並發布安全性建議於合勤科技全球官網，以維護使用者安全。另也同步發布電子報給註冊用戶，主動告知風險，並呼籲使用者儘快進行更新。

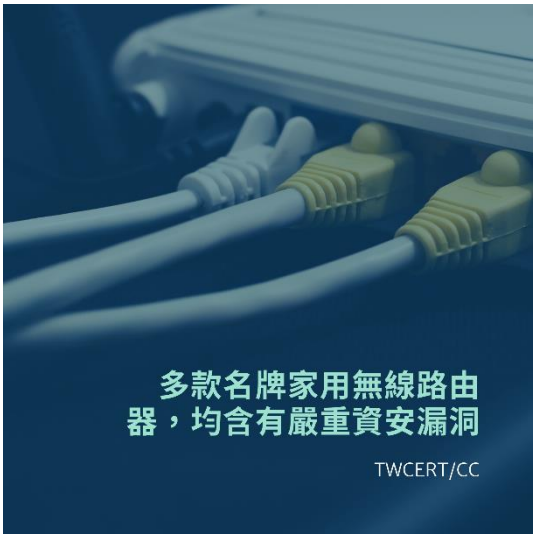
近期發現有攻擊者透過該漏洞進行駭侵攻擊，敬請尚未更新修補漏洞之用戶立即更新至最新版本，以確保網路使用安全。

受影響的 NAS 韌體版本為 5.21 或更早，防火牆（ATP/USG/VPN 系列）韌體版本為 ZLD V4.35（更早之前版本不受影響)。

詳細資訊請參閱合勤科技安全性建議。

- 資料來源：
  1. https://www.zyxel.com/tw/zh/support/remote-code-execution-vulnerability-of-NAS-products.shtml
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9054

2.1.2、多款名牌家用無線路由器，均含有嚴重資安漏洞



一份由德國智庫發表的研究報告指出，針對多款知名品牌家用路由器的資安檢測，發現多家大廠的暢銷產品，均含有嚴重資安漏洞，有些甚至無法透過韌體更新加以修補。

一份由德國智庫 Fraunhofer 發表的研究報告「2020 年家用路由器資安報告」指出，針對多款知名品牌家用路由器的資安檢測，發現 127 款來自多家大廠的暢銷產品，均含有一個以上的嚴重資安漏洞，有些甚至無法透過韌體更新加以修補。

這份報告檢測了來自七家知名大廠的 127 款家用無線路由器，以下為檢測結果：

* 127 款受測機種，沒有一台不存在資安漏洞；

* 其中有 46 款，在過去一年中沒有任何資安更新可供下載；

* 平均來說，一台路由器內含 53 個已知的嚴重資安漏洞；

* 其中漏洞最少、最安全的款式，含有 21 個嚴重資安漏洞；

* 許多路由器雖然經常更新，但這些更新並未將漏洞修補起來；

* 許多路由器的管理者密碼非常容易破解，並寫死（hard-coded）在系統中，用戶無法更改密碼；

研究報告還說，在這 127 款家用路由器中，有 91% 使用嵌入式 Linux 作業系統；雖然 Linux 本身的安全性還算不錯，但這些路由器採用的 Linux 版本都過於老舊，有不少機種的 Linux 核心，都還採用多年前便已停止維護的 Linux 2.6 版，而這就是這些路由器含有這麼多未修補漏洞的根本原因。

- 資料來源：
  1. https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf
  2. https://threatpost.com/report-most-popular-home-routers-have-critical-flaws/157346/

2.1.3、美國法院判決微軟取得以疫情為由之詐騙網域

美國法院判決，微軟可以取得六個專門以肺炎疫情為由，用來竊取 Office 365 用戶權限的詐騙網域所有權。

美國聯邦東維吉尼亞地區法院最近判決，微軟可以取得六個專門以肺炎疫情為由，用來竊取 Office 365 用戶權限的詐騙網域所有權，以防止駭侵團體繼續其惡行。

擁有這六個網域的駭侵團體，鎖定 Office 365 的企業使用者發動所謂「BEC」攻擊（Business Email Compromise）；假冒企業內部同事或客戶，以肺炎疫情為名寄送釣魚信件，企圖詐騙目標企業員工。

但和一般釣魚信件攻擊不同的是，這波攻擊不會把受害者導向到假網站騙取用戶的登入資訊，而是在信件中附加一個惡意 Office 文件檔，在受害者系統上安裝假冒的 Office 365 應用程式。

用戶一旦執行這個假冒的 Office 365 應用程式，該應用程式會要求用戶給予其 Office 365 的存取權限，因此駭侵者可以透過 OAuth 2 來竊得用戶的 Office 365 權限與所有內容，不需要實際騙取登入資訊。

微軟認為至少有兩名駭侵者涉及這波釣魚信件攻擊活動，而根據 FBI 的統計指出，BEC 詐騙佔 2019 年向 FBI 網路詐欺申訴中心(IC3)報告之網路犯罪損失的一半。這類 BEC 攻擊事件是現今最嚴重的網路犯罪樣態；在 2019

年造成所有企業超過 17.7 億美元的損失，平均一起攻擊事件的損失就高達 7.5 萬美元。

- 資料來源：
  1. http://www.documentcloud.org/documents/6982601-Microsoft-civil-complaint-against-COVID-19.html
  2. https://www.zdnet.com/article/microsoft-seizes-six-domains-used-in-covid-19-phishing-operations/

2.1.4、美國資安單位警告：製造業應嚴防針對 Triconex 資安漏洞進行的駭侵攻擊

美國國家安全局（NSA）與資安暨基礎設施安全局（CISA）日前發布警訊，指出美國製造業廣泛使用的 Triconex TriStation 等安控設備，含有嚴重的資安漏洞。

美國國家安全局（National Secutiry Agency, NSA）與資安暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）日前聯合發布警訊，指出美國製造業廣泛使用的 Triconex TriStation、Tricon 通訊模組等安控設備，因含有一個嚴重的資安漏洞，很可能被美國敵對勢力旗下的駭侵團體鎖定，用以發動大規模駭侵攻擊。

根據 CIS-CERT 發布的漏洞通報，由 Schneider Electric 製造生產的 Triconex TriStation 和 Tricon 通訊模組，含有一個 CVSS 分數高達滿分十分的嚴重資安漏洞；成功利用這個漏洞入侵的駭侵者，將可能竊取內部網路上所有未加密的通訊內容、發動 DDoS 攻擊，甚至不當存取企業內部各種資源。

出現漏洞的 Schneider Triconex TriStation 和 Tricon 通訊模組，是用來進行製造流程安全控製的組件；當發生嚴重事故如火災或爆炸時，可用來緊急中斷工廠的製造流程，避免損害擴大。

Schneider 這套系統廣泛用在美國各地的核能發電廠、煉油廠、石化工業、礦業、淨水廠等重要設施；NSA/CISA 的聯合警告中指出，像這類用在製造業的營運系統（oprational systems, OT），特別是關鍵基礎設施中的連網

OT，近日已發生多起遭到駭侵者攻擊的案例；NSA/CISA 認為這類 OT 系統的漏洞之所以變成外國敵對勢力的目標，是因為只要成功入侵，就能大大影響美國國家安全和社會穩定。

- 資料來源：
  1. https://us-cert.cisa.gov/ics/advisories/icsa-20-205-01
  2. https://us-cert.cisa.gov/ncas/alerts/aa20-205a
  3. https://threatpost.com/nsa-urgent-warning-industrial-cyberattacks-triconex/157723/

2.1.5、英國三十八萬 BMW 車主個資遭置於暗網販售

資安廠商發現，多達三十八萬名英國 BMW 車主資料，被某個駭侵團體置於暗網上求售。

設立於以色列特拉維夫的資安廠商 KELA 近來發現，有多達三十八萬名英國 BMW 車主，其資料被某個名為 KelvinSecurity Team 的駭侵團體置於暗網上求售。

據 KELA 指出，這披遭駭的 BMW 車主資料，受害者人數多達 384,319 名；資料欄位則包括車主的姓氏、名字、Email 地址、住家地址、車輛序號、經銷商名稱等多種個人可辨識資訊。

KELA 表示，駭侵者宣稱這批 BMW 車主的資料是來自一家服務多家車廠的電話行銷公司；而除了 BMW 之外，還有 Mercedes Benz、SEAT、Honda、Hyundai 等多家車廠的五十萬名以上顧客資料亦遭待價而沽。

KELA 說，KelvinSecurity Team 求售的這些資料，係由駭入一家美國企管顧問公司 Frost & Sullivan 而取得的。

KELA 也指出，這個名為 KelvinSecurity Team 的駭侵團體，在暗網上十分活躍，經常把駭侵取得的資料庫放上暗網出售；光是今年六月，就有取自各公私營單位的 16 個資料庫被拿出來賣，受害者甚至包括美國政府各標案的外包廠商，以及俄羅斯軍方的武器開發相關單位。

KelvinSecurity Team 過去也曾把自墨西哥、伊朗、美國、澳大利亞、瑞

典、法國、印尼等國各公私單位的 28 個資料庫放上暗網，而且供人免費下載取用。

- 資料來源：
  1. https://www.technadu.com/details-384319-bmw-owners-for-sale-dark-web/112982/amp/
  2. https://www.scmagazine.com/home/security-news/bmw-customer-database-for-sale-on-dark-web/
  3. https://www.tomsguide.com/news/bmw-call-centre-data-breach

2.2、國際政府組織資安資訊

2.2.1、美英資安機關警告，全球約 6 萬餘台 NAS 遭感染，QNAP 提醒用戶須回復出廠預設再更新

美國 CISA、英國 NCSC 近日共同發表資安警訊，指出至 2020 年 6 月中旬為止，全球約有 62,000 台 QNAP NAS 設備遭到 QSnatch 惡意軟體駭入。。

美國資安與基礎設施安全局（Cybersecurity and Infrastructure Securoty Agency, CISA）與英國國家資安中心（National Cyber Security Centre, NCSC），近日共同發表資安警訊，指出至 2020 年 6 月中旬為止，全球約有高達 62,000 台 QNAP NAS 設備，遭到一個名為 QSnatch 的惡意軟體駭入。

報告中指出，這個惡意軟體的第一波攻擊遠從 2014 年就已啟動，第二波攻擊則起始於 2018 年末；到今年六月中旬為止的感染台數已經達到 62,000 台。

被感染的 QNAP NAS 約有 7,600 台位於美國境內，約 3,900 台位於英國。

報告說，QSnatch 植入後，會設定一個詐騙的 Web 管理界面登入畫面，竊取登入用的管理帳號和密碼，也會開啟 SSH 後門，並且安裝一個 Webshell，讓駭侵者遠端操控，更會將系統設定檔與 log 檔透過 https 傳回到駭侵者處。

QSnatch 入侵後還會竄改系統更新機制，防止取得弱點修補後的更新套件，藉以在系統中持續寄生，導致病毒難以清除；CISA 建議已感染用戶，在更新之前必須完全將裝置重置為出廠預設狀態，再來更新韌體。原廠 QNAP 也提供了避免再次遭到 QSnatch 感染的建議，包括變更管理者密碼、取消 SSH 和 Telnet 服務、關閉連接埠 22、443、80、8080、8081。

QNAP 同時也建議使用者安裝或更新 Malware Remover 套件至最新版本，Malware Remover 套件可對 NAS 進行掃描確認有無感染 QSnatch，若確認感染將會主動將惡意軟體加以清除。

- 資料來源：
  1. https://www.ncsc.gov.uk/news/legacy-risk-malware-targeting-qnap-nas-devices
  2. https://us-cert.cisa.gov/ncas/alerts/aa20-209a
  3. https://www.qnap.com/en/security-advisory/nas-201911-01

2.2.2、美英等國資安機關警告，俄羅斯駭侵團體針對肺炎疫苗研發單位發動攻擊

美國、英國、加拿大三國的情治與資安主管機關，日前發表聯合聲明，指出某些來自俄羅斯的駭侵團體，正在針對全球關於 Covid-19 的研究與疫苗開發單位進行攻擊。

包括美國國家安全局、國防部所屬的資安與基礎設施安全局、英國國家資安中心、加拿大通訊安全局與基礎設施安全局等三國情治與資安主管機關，於 7 月 16 日發表聯合聲明，指出某些來自俄羅斯的駭侵團體 Cozy Bear（APT29），正在針對全球關於 Covid-19 的研究與疫苗開發單位進行攻擊。

聲明中指出，Cozy Bear 利用一種特製的 WellMail 惡意軟體，鎖定和 Covid-19 相關的全球研究機構和疫苗開發單位進行駭侵攻擊。

聲明說，在最近幾次針對這些單位的攻擊中，發現駭侵者會先掃瞄目標對象使用的外部與內部 IP，試圖尋找弱點加以攻擊；發現弱點後即會布署相關攻擊工具進行攻擊，以竊取這些單位的研究資料和成果。

Cozy Bear 的攻擊行動，主要鎖定這些研究單位使用的雲端工具或軟體的已知資安漏洞，如 Citrix 的 CVE-2019-19781、Pulse Secure 的 CVE-2019-11510、FortGate 的 CVE-2018-13379、Zimbra 的 CVE-2019-9670。

美國的資安主管機關 CISA 先前就曾發出警告，指出針對 Covid-19 研究單位，或單純假藉疫情相關主題為名的駭侵活動，自今年三月起就不斷增加。

- 資料來源：

1. https://media.defense.gov/2020/Jul/16/2002457639/-1/-1/0/NCSC_APT29_ADVISORY-QUAD-OFFICIAL-20200709-1810.PDF
2. https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development
3. https://www.nsa.gov/news-features/press-room/Article/2275378/nsa-teams-with-ncsc-cse-dhs-cisa-to-expose-russian-intelligence-services-target/
4. https://www.meritalk.com/articles/u-s-uk-canada-warn-against-russian-led-covid-rd-vaccine-attacks/

2.2.3、美國資安主管機關要求 24 小時內修補 Windows DNS 嚴重漏洞

美國資安與基礎設施安全局日前下令，所有美國聯邦機關與附屬單位，需在 24 小時內修補某個 Windows DNS 嚴重資安漏洞。

美國資安與基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）日前下令，所有美國聯邦機關與附屬單位，需在 24 小時內修補某個 Windows DNS 嚴重資安漏洞。

這個漏洞的 CVE 編號是 CVE-2020-1350，發生在 Windows DNS Server，稱為「SIGRed」，可讓駭侵者遠端執行任意程式碼。

這個漏洞發生在 Windows Server 2003 到 2019 版本，其 CVSS 危險評分高達滿分的 10 分。

資安廠商 Check Point 發現這個漏洞的存在；藉由發送一個大於 64 KB 的 SIG 記錄檔，可以在 Windows DNS Server 引發一個緩衝區溢位錯誤，進而用以入侵這台 DNS Server 並執行任意程式碼。

Check Point 指出，任何出現在 DNS Server 的嚴重漏洞都非常危險，因為駭侵者極易透過 DNS Server 染指整個單位的所有設備。這類漏洞十分罕見，但 SIGRed 漏洞存在竟然長達 17 年才被發現。微軟已於日前發布這個漏洞的修補程式。

鑑於此一漏洞的嚴重性，CISA 除通令美國聯邦政府旗下各單位應於 24 小時內修補漏洞外，還要求任何無法在七個工作天內解決此一問題單位，應即移除單位內的所有 Windows 伺服器系統。

- 資料來源：
  1. https://www.cisa.gov/blog/2020/07/16/emergency-directive-ed-20-03-windows-dns-server-vulnerability
  2. https://cyber.dhs.gov/ed/20-03/
  3. https://www.bleepingcomputer.com/news/security/microsoft-patches-critical-wormable-sigred-bug-in-windows-dns-server/。

2.2.4、以色列供水系統，遭到兩次駭侵攻擊

以色列官員表示，該國供水系統近來連續遭到兩次駭侵攻擊，所幸並未造成太大的損失。

以色列主管全國供水事務的官員上周表示，該國供水系統近來連續遭到兩次駭侵攻擊，所幸並未造成太大的損失。

以色列官員說。兩次針對供水系統的攻擊都發生在六月，第一起攻擊位於上加利利（Upper Galilee）農業用水的供水加壓系統，第二起則發生在以色列中部的馬特耶胡達地區，同樣也是針對供水加壓系統發動攻擊。

官員指出，這些被攻擊的系統，都是針對農業灌概用的微型澆灌系統，在案發當時已經直接由當地的系統管理人員修復完成，沒有造成實質損失。

不過根據英國金融時報的報導指出，同樣在六月時，西方國家的情報單位掌握具體情資，指出以色列的淨水系統也曾遭到駭侵者成功控制；駭侵者更試圖竄改淨水用氯消毒劑的投入比例，幸好並未成功。

一旦駭侵者成功更改氯消毒劑的投入比例，很可能造成淨水場供水區域人口的大規模中毒事件。

以色列國家資安主管機關 Israel National Cyber-Directorate 和供水主管機關，在事件後也要求所有淨水廠的連網電腦設備，必須變更登入密碼；特別是和加氯消毒相關的電腦設備，更應提高警覺。

四月時以色列的供水系統亦曾遭到攻擊，以色列官員當時沒有提供可疑駭侵者的資訊。

- 資料來源：
  1. https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/
  2. https://www.ft.com/content/3ea57426-40e2-42da-9e2c-97b0e39dd967
  3. https://www.ynet.co.il/article/rJrCqmAkw
  4. https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html

2.3、社群媒體資安近況

2.3.1、Twitter 遭大規模駭侵攻擊，多個認證名人、品牌帳號被用以發送詐騙訊息

Twitter 日前發生重大資安事故，多個經官方認證的名人、品牌帳號，被駭侵者挾持並用以發送比特幣詐騙貼文。

Twitter 發生重大資安事故，包括美國民主黨總統候選人拜登（Joe Biden）、Tesla 與 SpaceX 創辦人 Elon Musk、美國前總統歐巴馬、亞馬遜創辦人 Jeff Bezos、微軟創辦人 Bill Gates、知名投資大師華倫巴菲特、前紐約市長麥可彭博、以及知名品牌如 Apple、Uber、CashApp 等的官方 Twitter 帳號，都遭到駭侵者挾持，用以發送比特幣詐騙貼文。

詐騙貼文假藉這些名人或品牌的名義，詐稱舉辦限時半小時的比特幣大放送活動；只要把相當於 1000 美元的比特幣匯入某數位錢包，該名人或品牌就會匯回 2000 美元。

雖然大部分人都能立即判斷出這是詐騙訊息，但仍有人不疑有他，真的匯了比特幣到該數位錢包位址；7 月 15 日當天該錢包的交易筆數高達 383 筆，收到了 13 枚比特幣匯入款，相當於美金 117,000 元左右。

Twitter 在事發當時立即暫停所有認證帳號的推文權限，刪除遭挾持帳號發送的詐騙推文，並且進行調查；事後 Twitter 發表聲明，指出該公司認為是內部員工遭到駭侵者以社交工程騙取管理系統權限，駭侵者取得權限後，除

了假冒這些帳號發出詐騙推文外，還改掉了這些帳號連結的 Email 地址，以增加帳號合法擁有者取回帳號控制權的難度。

Twitter 指出，該公司目前沒有查出內部員工和駭侵者勾結犯案的證據，但目前有跡象顯示發動本次攻擊的駭侵者，與先前透過 SIM-Swap 方式竊得 Twitter CEO Jack Dorsey 帳號的駭侵者有關。目前 FBI 也已介入調查本案。

- 資料來源：
  1. https://techcrunch.com/2020/07/15/twitter-accounts-hacked-crypto-scam/
  2. https://krebsonsecurity.com/2020/07/whos-behind-wednesdays-epic-twitter-hack/
  3. https://techcrunch.com/2020/07/16/daily-crunch-twitter-hacked-in-crypto-scam/
  4. https://twitter.com/TwitterSupport/status/1283518038445223936

2.3.2、假扮成 TikTok 替代程式的惡意軟體，在印度藉由 WhatsApp 等管道肆虐

資安廠商發現，在印度境內有假扮成 TikTok 替代程式的惡意軟體，正在透過 WhatsApp、手機簡訊等管道大肆擴散。

資安廠商卡巴斯基發現，在印度境內有假扮成 TikTok 替代程式的惡意軟體，正在透過 WhatsApp、手機簡訊等管道大肆擴散；受害者一旦安裝惡意軟體，該軟體會竊取用戶手機內的各項資訊，並且自動轉寄下載連結給受害者通訊錄內的所有人。

卡巴斯基的資安研究人員指出，假冒 TikTok 的這支惡意 App，外部的名稱叫做「TikTok Pro」，詐騙用戶的文案訊息，以「讓你重新觀看 TikTok 上的影片，並且製作創意影音」。

卡巴斯基說，先前印度政府下令禁止 59 支中國製作的 App 在印度境內發行；除了假冒 TikTok 外，還有很多假冒其他被禁熱門 App 的惡意軟體，同樣也用這種方式吸引受害者安裝。

報告也指出，這批惡意軟體雖然不會竊取用戶機敏資訊回傳，但會要求用戶輸入自己的 TikTok 登入資訊，然後點按廣告或下載廣告軟體，駭侵者可藉以賺取不法廣告收益。

卡巴斯基的研究人員說，現在的駭侵者手段十分靈活，會利用當下的話題來吸引用戶上勾；卡巴斯基建議用戶不要因為認識的人傳來連結，就不疑

有他；下載任何軟體時，都應透過官方 App Store 管道，並且確認安裝時這支 App 沒有要求授予不必要的存取權限。

- 資料來源：

1. https://www.firstpost.com/tech/news-analysis/malware-disguised-as-tiktok-alternative-app-is-being-circulated-via-whatsapp-sms-by-cybercriminals-report-8632871.html
2. https://www.digit.in/press-release/general/kaspersky-discovers-malware-disguised-as-tiktok-app-alternative-55615.html
3. http://surl.twcert.org.tw/FfEbk

2.4、行動裝置資安訊息

2.4.1、Apple 發布 iOS、iPadOS 13.6 更新，一次修復 29 個資安漏洞

Apple 日前發表 iOS、iPadOS 13.6，除了新增功能之外，同時修復 29 個資安漏洞；建議所有 iPhone 和 iPad 用戶，應立即更新系統。

Apple 日前發表 iOS、iPadOS 13.6，除了新增功能之外，同時一口氣修補了 29 個資安漏洞；其中有 10 個漏洞可導致駭侵者遠端執行任意程式碼（RCE）。

首先，有四個 RCE 漏洞（CVE-2020-9888、CVE-2020-9889、CVE-2020-9890、CVE-2020-9891）發生在聲音子系統中；只要播放一個特製的損壞聲音檔案，駭侵者便可用以執行任意程式碼。

另外有三個 RCE 漏洞發生在 WebKit 瀏覽器引擎中：CVE-2020-9894、CVE-2020-9893、CVE-2020-9895；利用特製的網頁來進行遠端執行程式碼。駭侵者經常會把這類攻擊工具偽裝成「越獄」破解工具，誘使想越獄的用戶瀏覽，繞過防範較為嚴密的官方 App Store，以入侵受害者的系統。

除了 iOS 和 iPadOS 外，Apple 也同時發布了 macOS、tvOS、WatchOS 的新版本，以 macOS Catalina 10.15.6 的更新程式為例，也一口氣修補了近 20 個嚴重程度不一的資安漏洞。

Apple Watch 的作業系統更新 WatchOS 6.2.8 則更新了 18 個資安漏洞、tvOS 13.4.8 則更新了 20 個資安漏洞。

由於這波更新幾乎含蓋所有 Apple 硬體產品，建議所有 iPhone、iPad、Mac、Apple Watch 和 Apple TV 用戶，應立即透過系統更新功能修復這些資安漏洞，以降低遭駭侵者利用這些已知漏洞發動攻擊的風險。

- 資料來源：
  1. https://support.apple.com/en-us/HT211288
  2. https://support.apple.com/en-us/HT211289
  3. https://support.apple.com/en-us/HT211291
  4. https://support.apple.com/en-us/HT211290
  5. https://www.theregister.com/2020/07/16/apple_july_updates/。

2.4.2、駭客利用 BadPower 漏洞，鎖定快速充電器進行攻擊

資安廠商發現專門鎖定快速充電器的攻擊手法，可能會造成設備起火事故。

國外的資安研究團隊發現，部分快速充電器產品存在安全問題 BadPower。利用此資安漏洞，駭客能鎖定各種電子設備的快速充電器進行攻擊，可能會造成設備中的零組件燒燬，甚至引起火災事故。

一般來說，市售的快速充電器，和一般充電器看起來差別不大，主要差別在於控制充電速度與電量的韌體程式；設備韌體會和被充電裝置進行溝通，以決定要以多大的電壓或電流進行充電。

利用 BadPower 漏洞的攻擊手法，會提供超過充電裝置額定電壓電流的供電，導致被充電設備的損壞、高溫，甚至發生火災事故。

該資安團隊在報告中指出，某些廠商之產品在資料通道中設有可讀寫充電器韌體程式碼的進入點，要存取這些進入點時，卻沒有足夠安全的認證程序，或是其快充通訊協定內存有可破壞韌體程式碼的漏洞，駭客便是利用這些漏洞進行攻擊。

該資安團隊針對市售 35 款快充設備進行測試，發現 8 個品牌的產品，共 18 款設備存有 BadPower 漏洞問題；針對快速充電器控制晶片廠商調查，發現在 34 家晶片廠中，有 18 家的快充晶片產品可透過各種方式更新韌體；廠

商如果沒有做好相關資安防護，其充電器就可能存有 BadPower 漏洞，並遭到駭客攻擊。

- 建議採取資安強化措施

1、 根據廠商發布之安全性更新，將充電設備的韌體更新至最新版本。

2、 建議用戶不要使用 Type-C 轉接其他 USB 傳輸線為不支援快速充電的設備充電，也不建議將快速充電器借給他人使用，以免發生電力過載造成設備損壞。

3、 建議廠商針對充電器韌體之程式碼進行安全性檢查，並將透過 USB 更新韌體的方式進行嚴格的驗證，防止駭客利用資安漏洞進行攻擊。

- 資料來源：

1. https://xlab.tencent.com/cn/2020/07/16/badpower/
2. https://www.zdnet.com/article/badpower-attack-corrupts-fast-chargers-to-melt-or-set-your-device-on-fire/

2.4.3、多達 14.8% Android 裝置用戶，感染無法移除的惡意軟體

資安廠商指出，高達 14.8% 的 Android 用戶，其裝置在去年曾經感染無法移除的惡意軟體或廣告軟體。

資安廠商 Kaspersky 旗下的資安研究專家指出，高達 14.8% 的 Android 用戶，其裝置在去年曾經感染無法移除的惡意軟體或廣告軟體。

卡巴斯基在最近發表的一份研究報告中指出，該公司接到愈來愈多客戶反映，手機被安裝了不明來源，而且無法移除的廣告軟體；以 Android 用戶的總數量來看，受此攻擊困擾的用戶比例高達 14.8%。

報告指出，這類無法移除的廣告軟體或惡意軟體，主要透過兩種手法植入裝置：先取得裝置的 root 權限，然後在裝置的系統分割區內安裝惡意軟體，接著把用以顯示擾人廣告的程式碼寫入手機韌體內。這樣即使用戶將手機清除並恢復原廠設定值，也無法移除被植入的惡意程式碼。

用戶雖然在手機上安裝各種防毒軟體，但這些防毒軟體如果和一般正常軟體相同，沒有取得 root 權限，就無法進入系統分割區刪除惡意程式，使得這些防毒軟體無法發揮應有的功用。

這類無法移除的惡意軟體，在平價 Android 手機的盛行率，較一般價位的手機高出許多。據 Kaspersky 統計，高達 27% 的 Android 手機受害。

以國家來區分，這類無法移除的惡意 Android 軟體，受害率最高的國家分別有美國、中國、阿爾及利亞、委內瑞拉、奈及利亞、肯亞、印尼、菲律賓、印度、俄羅斯、埃及、烏克蘭、孟加拉、巴基斯坦、伊朗、哈薩克斯坦、南非、阿根廷等國。

- 資料來源：
  1. https://securelist.com/pig-in-a-poke-smartphone-adware/97607/
  2. https://threatpost.com/android-users-undeletable-adware/157189/

2.4.4、Joker Android 惡意軟體再出新招，跳過 Google Play Store 惡意軟體偵測機制

資安廠商指出，一個名為 Joker 的 Android 惡意程式，最近發展出能逃過 Google Play Store 惡意軟體偵測機制的方法，藏身在至少 11 支 Android App 中。

資安廠商 Check Point 的資安研究人員，日前發表研究報告指出，一個名為 Joker 的 Android 惡意程式，最近發展出能逃過 Google Play Store 惡意軟體偵測機制的方法，並且藏身在至少 11 支 Android App 中。

Joker 這支 Android 惡意軟體，自 2017 年開始就有藏身在 Android App 中的記錄；當時主要的駭侵手法是竊取用戶的簡訊內容；最新版本的 Joker 則轉而進行訂閱詐騙，在用戶不知情的情形下訂閱或購買十分昂貴的 app 或內容，從中賺取不法分潤。

新版 Joker 把惡意軟體程式碼的酬載部分，以 Base64 編碼藏在 App 內的 dex 檔案中，這種做法就無需連線到外部的駭侵控制伺服器，以下載惡意程式碼，更能躲過 Android Play Store 的惡意軟體偵測機制。

雖然 Google Play Store 曾於今年一月時，大舉下架近 1700 支內藏 Joker 惡意軟體的 Android App，但 Check Point 指出，他們在 11 支仍在架上的 Android App 中發現了新版 Joker，而且還發現每周都有新的 Joker 惡意 App 上架到 Google Play Store 中。顯然 Google Play Store 的審核機制無法發現 Joker 惡意軟體的存在。

Check Point 指出，用戶如果發現自己的手機帳單或信用卡費用無故暴增，或是訂閱了自己根本沒訂的 App 或服務，很可能就是誤遭 Joker 等惡意軟體之害，應立即移除可疑的 App。

- 資料來源：

1. https://research.checkpoint.com/2020/new-joker-variant-hits-google-play-with-an-old-trick/
2. https://www.bleepingcomputer.com/news/security/joker-android-malware-keeps-evading-google-play-store-defenses/
3. https://www.forbes.com/sites/zakdoffman/2020/07/09/ldangerous-android-malware-warning-google-play-store-security/#4f0a14f11f9e

2.4.5、資安廠商發現 DJI 無人機 app，其系統設計可能導致用戶資訊外洩

法國、美國資安廠商近日發表研究報告指出，DJI 無人機的 Android 控制 app，不僅可能導致用戶手機內的資訊外洩，更可能讓用戶的手機遭駭侵者控制。

法國資安廠商 Synacktiv 和美國資安廠商 GRIMM 日前發表研究報告，指出全球市佔最高的無人機大廠 DJI，其 Android 版本無人機控制 app DJI GO 4 的一些功能設計，可能導致用戶手機內的資訊外洩，甚至讓用戶的手機遭駭侵者控制。

這兩家廠商的資安專家發現，DJI GO 4 app 在進行軟體更新時，不會經由 Google Play Store 進行，而是逕行更新 App 程式碼；除了違反 Google Play Store 的使用規範，更可能導致 DJI 與任何第三方公司，可直接取得這支 App 執行時要求的權限，包括讀取用戶的通訊錄、存取麥克風、手機鏡頭與地理座標等資訊。

GRIMM 發表的報告也指出，這支 App 使用了「微博軟體開發套件」（Weibo software development kit），除了再次繞過 Google Play Store 的機制、讓微博取得用戶資訊外，也可能透過該 SDK 直接在用戶手機上安裝任意程式碼。

報告也指出，DJI GO 4 收集許多和無人機操作無關的用戶機敏資訊，例如手機的 IMSI、IMEI 以及 SIM 卡編號等；另外 Synaktiv 也指出，DJI GO 4 a

pp 即使被用戶關閉，還是能在背景進行資料傳輸。

Synaktiv 和 GRIMM 的報告中對這支 App 進行了詳細的技術分析，甚至還發現這支 App 內有反制分析的功能存在；在使用相同 SDK 的其他 App 中，沒有看到這樣的設計。

DJI 被懷疑有資安風險不是第一次，三年前美國陸軍和海軍就因資安風險疑慮，全面禁用 DJI 無人機產品。

- 資料來源：
  1. https://www.synacktiv.com/en/publications/dji-android-go-4-application-security-analysis.html
  2. https://blog.grimm-co.com/2020/07/dji-privacy-analysis-validation.html
  3. https://www.cyberscoop.com/dji-drones-china-android-application/

2.5、軟體系統資安議題

2.5.1、全新 Mac 勒贖軟體 EvilQuest 透過盜版軟體包散布

資安專家發現一個全新的 Mac 平台勒贖軟體 EvilQuest，利用盜版軟體包大肆擴散。

資安研究者 Dinesh Devadoss 近日發現一個全新的 Mac 平台勒贖軟體 Evil Quest，會利用盜版軟體包大肆擴散。這個勒贖軟體不但會將系統上的檔案加密以進行勒贖，甚至還內含鍵盤記錄器，還會竊取受害用戶電腦中的加密貨幣錢包。

專家在多個透過 BitTorrent 散布的 Mac 盜版軟體包中發現 EvilQuest；雖然這種傳播感染方式沒有複雜的技術，但很多 macOS 平台上的惡意軟體，都是以這種方式散布的。

另外也有數名資安防護專家，也在不同的盜版軟體包中發現 EvilQuest 的存在；有些偽裝成 Google 軟體更新包，有些則被包在一個稱為 Little Snitch 的 Mac 防火牆軟體的安裝程式內，透過一個俄羅斯的盜版軟體討論區分享的 BItTorrent 連結散布。

一旦用戶不幸安裝了藏有 EvilQuest 的盜版軟體，就會看到一個「檔案已遭加密」的跳出視窗，被加密的檔案除了用戶在系統上的一些設定檔和資料檔外，連專門儲存系統服務和外部網站登入資訊的 Keychain 資料檔也會被加密，導致系統運作出現錯誤。

資安專家呼籲 Mac 用戶，絕對不要下載來路不明或非法的盜版、破解版軟體，以免因小失大。

- 資料來源：
  1. https://twitter.com/dineshdina04/status/1277668001538433025
  2. https://threatpost.com/evilquest-mac-ransomware-keylogger-crypto-wallet-stealing/157034/

2.5.2、美國某媒體集團旗下三十家新聞媒體，遭 WastedLocker 勒贖軟體攻擊

資安廠商發現近來有某個美國大型媒體集團，旗下三十家以上的新聞媒體，遭到一個名為 WastedLocker 的勒贖軟體攻擊。

資安廠商 Symantec 發現，近來有某個美國大型媒體集團，旗下共有三十家以上的新聞媒體，遭到一個名為 WastedLocker 的勒贖軟體攻擊；該惡意軟體甚至還利用這些媒體網站來散播惡意軟體，導致更多大型企業的電腦遭駭。

這個惡意軟體採用一個稱為「SocGholish」的 JavaScript 架構，會偽裝成某種軟體更新程式，以騙取受害者信任。這波攻擊目前有多達 11 家大型企業受害，其中有 8 個名列財星五百大企業名單之內，更有多家受害者屬於製造業。

除製造業以為，多家分屬金融服務、醫療、能源與大眾運輸產業的知名公司，也在受害名單之列。

Symantec 指出，這波攻擊行動與俄羅斯的 Evil Corp. 有關，之前也曾透過其他勒贖軟體多次發動駭侵攻擊，總共造成數億美元的損失。美國聯邦法院曾對其中兩名駭侵分子發出通緝令，其中一名嫌疑人的懸賞金額高達五萬美元，但至今這兩人仍舊逍遙法外。

據 Symantec 的報告指出，在這波攻擊中，有至少 150 個正常的網站遭到植入 WastedLocker 勒贖軟體；當用戶瀏覽這些網站時，就會下載 ScoGolish 惡意指令到電腦中。

另一家資安廠商 NCC Group 則指出，該公司在今年五月起開始觀測到 WastedLocker 的攻擊活動。

- 資料來源：
  1. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us
  2. https://www.bleepingcomputer.com/news/security/dozens-of-us-news-sites-hacked-in-wastedlocker-ransomware-attacks/
  3. https://www.darkreading.com/attacks-breaches/attackers-compromised-dozens-of-news-websites-as-part-of-ransomware-campaign/d/d-id/1338265

2.5.3、遠距會議服務 Zoom 修復 Windows 版的遠端執行任意程式碼 0-day 漏洞

資安廠商日前發現 Zoom 含有一個可讓駭侵者遠端執行任意程式碼的 0-day 漏洞；而 Zoom 已經在更新版中修補此一問題。

資安廠商 0patch 日前發表研究報告指出，有一名不願透露姓名的獨立資安研究人員，向該公司通報，他發現 Zoom 含有一個可讓駭侵者遠端執行任意程式碼的 0-day 漏洞；而 Zoom 已經在更新版中修補此一問題。

0patch 說，這個漏洞發生在 Zoom 的 Windows 版本應用程式；駭侵者只要讓受害者下載並開啟一個含有惡意程式碼的檔案，就可以利用此漏洞，在受害者的 Windows 系統中遠端執行任意程式碼。

不過值得注意的是，這個 0-day 漏洞只會發生在 Windows 7 或更舊的 Windows 版本，以及 Windows Server 2008 或更舊的版本。

這位獨立資安研究人員，沒有直接向 Zoom 通報該漏洞，而是選擇將資訊提交給 0patch；而 0patch 在研究確認該漏洞真實存在後，於 7 月 9 日發表了漏洞報告，還提供了該公司自行研發的修補程式，但沒有透露任何關於該 0-day 漏洞的技術細節。

隨後，原廠 Zoom 公司也在 7 月 13 日推出了更新版 Windows 軟體，修補了這個漏洞；0patch 也確認了該修補程式確實可以解決原先的 0-day RCE 漏洞。

建議所有仍在舊版 Windows 上執行 Zoom 的用戶，都能盡快將 Zoom 升級至最新版本，或是將 Windows 系統更新為 Windows 10，以避免受到這個 0-day 漏洞的影響。

- 資料來源：
  1. https://blog.0patch.com/2020/07/remote-code-execution-vulnerability-in.html
  2. https://www.bleepingcomputer.com/news/security/zoom-fixes-zero-day-rce-bug-affecting-windows-7-more-updates-soon/
  3. https://support.zoom.us/hc/en-us/articles/360046081271-New-updates-for-July-10-2020

2.5.4、多達一千三百種以上釣魚詐騙攻擊工具，可在駭侵論壇中買到

資安媒體報導指出，在某個駭侵論壇上有人出售多達一千三百種以上的釣魚詐騙攻擊工具，攻擊對象包括大型網站、銀行、金融組織等。

資安媒體 Bleeping Computer 日前報導指出，在某個駭侵論壇上，有人出售多達一千三百種以上的釣魚詐騙攻擊工具，供有心人士購買使用。

這批為數龐大的釣魚攻擊工具，全部包在一起的售價為 32,500 美元，總大小達到 3.3GB；如果單獨購買，每個釣魚攻擊工具售價僅 25 美元。

Bleeping Computer 分析指出，這批釣魚攻擊工具，鎖定攻擊對象包括大型網站、銀行、金融組織等，例如 PayPal、Dropbox、Amazon、OneDrive、Office 365、Outlook、Gmail、Spotify、Netflix、美國銀行、大通銀行、富國銀行、美國第一銀行、Apple、Facebook、LinkedIn 等對象。

在這些攻擊工具中，有些甚至還提供多國語言的支援服務；另外大多數 Webmail 的服務也都在攻擊對象之列。這些攻擊工具可以攻擊所有版本的 CPanel、Zimbra、Microsoft Outlook OVA。

Bleeping Coumputer 指出，從每支釣魚攻擊工具只賣 25 美元來看，這組攻擊工具的品質可能不如以往；在 2019 年時，釣魚攻擊工具的平均賣價是 304 美元，最便宜的是 20 美元，最貴的是 880 美元。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/over-1-300-phishing-kits-for-sale-on-hacker-forum/
  2. https://twitter.com/Bank_Security/status/1281210258715807746

2.6、軟硬體漏洞資訊

2.6.1、國內門禁設備商修復產品資安漏洞，請立即更新韌體

國內門禁設備商奇偶科技(GeoVision)門禁設備，近日針對部分門禁控制器型號的資安漏洞(CVE-2020-3928、CVE-2020-3929、CVE-2020-3930、CVE-2020-3931)進行修復並發布韌體更新，請相關用戶立即更新至最新版本。

GeoVision 於 7 月 8 日發布相關產品資安公告，表示已修補 CVE-2020-3928、CVE-2020-3929、CVE-2020-3930 以及 CVE-2020-3931 等四個 CVE 編號之漏洞，資安漏洞包含：移除內含工程模式使用的帳號密碼；修正誤用同一組金鑰，導致有機會受中間人攻擊解析流量之問題；修正系統日誌未有良好的權限控管；以及因應緩衝區溢位狀況強化防護未經授權的網路惡意攻擊。建議相關用戶盡速更新設備韌體版本，避免因資安漏洞而遭受駭侵。

此外，若用戶於更新新版韌體上有任何問題或疑慮，可聯繫 GeoVision 的產品資安團隊協助處理：security@geovision.com.tw

最新韌體版本下載路徑：https://s3.amazonaws.com/geovision_downloads/Manual/e-letter/cybersecurity/0708/Cybersecurity_Upgrade-notice_ASController_TW.pdf

詳細韌體更新步驟，請參閱奇偶科技提供之韌體更新步驟：

1、GV-GF192x 韌體更新步驟 https://s3.amazonaws.com/geovision_downloads/Manual/Access-Control/TechnicalNotice/Firmware_Upgrade_Instructions_GF192x-TW.pdf

2、GV-AS Controller 韌體更新步驟 https://s3.amazonaws.com/geovision_downloads/Manual/Access-Control/TechnicalNotice/Firmware_Upgrade_Instructions_ASController-TW.pdf

3、GV-AS1010 韌體更新步驟 https://s3.amazonaws.com/geovision_downloads/Manual/Access-Control/TechnicalNotice/Firmware_Upgrade_Instructions_GV-AS1010-TW.pdf

- CVE 編號：CVE-2020-3928、CVE-2020-3929、CVE-2020-3930 、CVE-2020-3931
- 影響版本：

  GV-AS210 型號 v2.21 之前版本

  GV-AS410 型號 v2.21 之前版本

  GV-AS810 型號 v2.21 之前版本

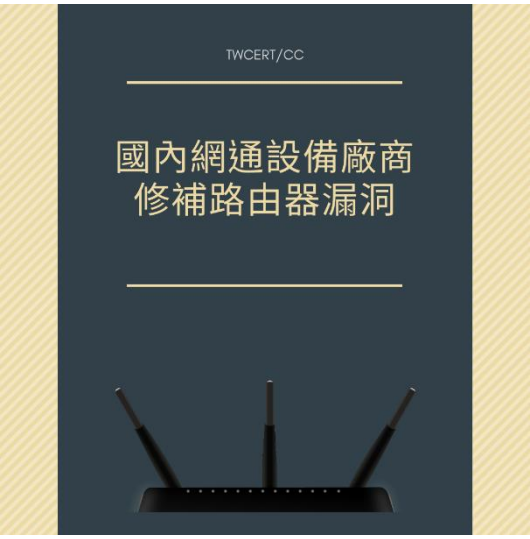
  GV-GF192x 型號 v1.10 之前版本

  GV-AS1010 型號 v1.32 之前版本

- 解決方案：請立即更新到最新版本的韌體

- 資料來源：
  1. https://www.twcert.org.tw/tw/lp-132-1-1-20.html
  2. https://s3.amazonaws.com/geovision_downloads/Manual/e-letter/cybersecurity/0708/Cybersecurity_Upgrade-notice_ASController_TW.pdf

2.6.2、國內網通設備廠商修補路由器漏洞



國內網通設備廠商最近更新其路由器產品 RT-AC1900P 的兩個資安漏洞；這兩個資安漏洞編號分別是 CVE-2020-15498 、 CVE-2020-15499。

CVE-2020-15498 這個漏洞發生在該款路由器的 wget 程式，在連線到伺服器下載韌體更新程式時，會接受偽造的數位安全認證簽章。

駭侵者可以利用這個漏洞發動中間人攻擊，最終可以竊聽路由器的所有網路流量；新版韌體取消使用 wget 下載更新程式碼的做法，避免中間人攻擊手法。

CVE-2020-15499 這個漏洞則發生在該款路由器的 web 管理界面的「更新說明」(release notes) 頁面；這個頁面因為內容處理的疏漏，可能造成駭侵者發動跨站指令碼攻擊（XSS）。

廠商已針對這兩個漏洞推出新版韌體，建議路由器 RT-AC1900P 版本號碼為 3.0.0.4.385_10000-gd8ccd3d 的用戶，應即更新至 3.0.0.4.385_20253 以上版本，即可修復這兩個漏洞。

- CVE 編號：CVE-2020-15498、CVE-2020-15499
- 影響版本：RT-AC1900P，版本號碼 3.0.0.4.385_10000-gd8ccd3d

- 解決方案：更新至 3.0.0.4.385_20253 以上版本

- 資料來源：
  1. https://www.trustwave.com/en-us/resources/security-resources/security-advisories/?fid=27440
  2. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/asus-router-vulnerable-to-fake-updates-and-xss-cve-2020-15498-and-cve-2020-15499/。

2.6.3、全球知名網路設備廠商修復重大資安漏洞

全球知名網路設備廠商修復重大資安漏洞

知名網路和網安設備廠商 F5，發布針對 BIG-IP 應用傳遞控制器上重大漏洞的說明以及修復更新，呼籲使用該設備（服務）的企業和組織盡速更新設備軟體至最新版本，以避免受到惡意攻擊。

安全技術服務公司 POSITIVE TECHNOLOGIES 的資安專家發現，網路設備商 F5 所生產的 BIG-IP 應用傳遞控制器（ADC, Application Delivery Controller），存在嚴重資安漏洞，漏洞的 CVE ID 分別為：

CVE-2020-5902：遠端程式碼執行（RCE）

CVE-2020-5903：跨站腳本攻擊（XSS）

兩個漏洞的 CVSS 3.1 危險程度評級分別高達 10 分和 7.5 分，係屬危害程度嚴重之漏洞。

CVE-2020-5902 存在於 BIG-IP 系列產品的 TMUI（Traffic Management User Interface，流量管理介面）當中，攻擊者首先需向設備傳送特製的 HTTP 請求，藉此訪問設備的管理介面。在未經授權的情況下，該管理介面允許攻擊者遠端執行任意指令與執行任意 JAVA 程式碼、遠端操縱設備並修改網路設定、危害關鍵資料，在更嚴重的情況下，攻擊者能損壞機構內部網路，並透過設備發動對外攻擊或散布勒索軟體。

CVE-2020-5903 駭客可透過已登入的使用者權限執行 JavaScript，進行跨站腳本攻擊（XSS）。若使用者具備可執行 Bash 之管理員權限，則可進行遠

端任意指令執行。

由於漏洞存在於軟體層面，因此除了 BIG-IP 硬體設備，架設在 AWS、Azure 或阿里雲等企業雲端服務的 BIG-IP 版本亦會受到漏洞的威脅。

POSITIVE TECHNOLOGIES 的新聞稿中指出，全球潛在風險的主機，40%位於美國境內，16%位於中國，而有 3%的設備位於我國境內。分析結果顯示，我國使用 F5 BIG-IP 網路設備的組織，包含多所大學與國家級研究機構等。

F5 公司於第一時間接獲通報並釋出更新，提供受影響機構進行漏洞修補。

- 建議採取資安強化措施

使用 F5 BIG-IP 設備的機構或企業，應檢查目前所安裝之軟體版本，是否受到漏洞影響，並根據 F5 所提供的解決方式，安裝更新軟體以修補漏洞。由於部分受影響版本的修復更新尚未釋出，機構應參考 F5 公司提供的修復指南來修補漏洞影響。

- CVE 編號：CVE-2020-5902、CVE-2020-5903
- 影響版本：BIG-IP 軟體版本 11.x、12.x、13.x、14.x、15.x
- 解決方案：使用廠商提供的部分更新版程式進行漏洞修復，或是參考廠商之漏洞修復指南。

- 資料來源：

1. https://www.ptsecurity.com/ww-en/about/news/f5-fixes-critical-vulnerability-discovered-by-positive-technologies-in-big-ip-application-delivery-controller/
2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5902
3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5903
4. https://support.f5.com/csp/article/K52145254

2.6.4、SAP 修復 NetWeaver AS JAVA 應用伺服器重大資安漏洞

SAP 發布安全性更新，修補該公司之 SAP NetWeaver AS JAVA 應用伺服器的資安漏洞，請用戶立即進行更新。

SAP 針對 NetWeaver 平台版本 7.3-7.5 的資安漏洞進行修補。該漏洞可使駭侵者無須經過認證即可透過 HTTP 控制 SAP 應用程式，並可以 SAP service user account 權限執行任意系統命令、存取 SAP 資料庫、甚至進行如關機等行為。此漏洞可影響 SAP 應用伺服器的資料與服務之機密性、完整性與可使用性。

SAP 已釋出更新檔，建議相關用戶立即更新修補漏洞。

漏洞相關細節請點此(需登入) https://launchpad.support.sap.com/#/notes/2934135，漏洞修補請點此(需登入)https://launchpad.support.sap.com/。

- 建議措施：
  1. 確認存在已知 SAP 系統漏洞之設備並進行相關更新。
  2. 監控設備上之可疑使用者行為並進行相關處理。
  3. 如無法進行更新，建議將受影響設備解除網路連線。
  4. 請參閱 SAP 官方釋出之更新檔進行更新

- CVE 編號：CVE-2020-6287、CVE-2020-6286
- 影響版本：NetWeaver 平台版本 7.3~7.5
- 解決方案：查看可能受影響之 SAP 應用程式請點此 https://us-cert.cisa.gov/ncas/alerts/aa20-195a

- 資料來源：
  1. https://us-cert.cisa.gov/ncas/alerts/aa20-195a
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6287
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6286

2.6.5、微軟發布兩個 Windows 重大漏洞通報

七月一日，微軟公司發布兩個 Windows 重大資安漏洞，分別是 CVE-2020-1425、CVE-2020-1457。

這兩個漏洞都發生在 Windows 用以處理多媒體檔案壓縮、解壓縮與播放工作的 Windows Codecs 程式庫；其中 CVE-2020-1425 漏洞的問題出在 Windows Codecs 程式庫在記憶體管理上的錯誤，導致駭侵者可用特製的影像檔案突破此漏洞，取得重要系統資訊，進而遠端執行任意程式碼。

CVE-2020-1457 的錯誤也和 CVE-2020-1425 類似，同樣是 Windows Codecs 程式庫的記憶體管理問題，也同樣能讓駭侵者利用特製影像檔案突破漏洞，遠端執行任意程式碼。

這兩個漏洞的 CVSS 3.0 嚴重程度分數都是 7.7 分，受到影響的 Windows 系統版本如下：

Windows 10 version 1709、1803、1809、1903、1909、2004 的 32 位元、ARM 64 位元、x64 各平台版本；

Windows Server 2019 Server Core 安裝版；

Windows Server version 1709、1803、1903、1909、2004 Server Core 安裝版。

目前微軟並未針對這兩個嚴重漏洞單獨推出修補程式，而是表示在接下來的每月定期資安更新周期中，會推出修補軟體；屆時用戶再安裝修補程式即可。

- CVE 編號：CVE-2020-1425、CVE-2020-1457
- 影響版本：Windows 10 version 1709、1803、1809、1903、1909、2004 的 32 位元、ARM 64 位元、x64 各平台版本；Windows Server 2019 Server Core 安裝版；Windows Server version 1709、1803、1903、1909、2004 Server Core 安裝版。
- 解決方案：安裝微軟定期推出的資安修補包

- 資料來源：
  1. https://www.jpcert.or.jp/english/at/2020/at200027.html
  2. https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1425
  3. https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1457

2.6.6、Microsoft .NET Framework, SharePoint Server 和 Visual Studio 存在資安漏洞

Microsoft .NET Framework, SharePoint Server 和 Visual Studio 存在遠端執行任意程式碼（RCE）資安漏洞(CVE-2020-1147)。

此為當軟體於反序列化 XML 過程時，無法檢查所輸入 XML 檔案的來源標記之漏洞。攻擊者可上傳一特製文件至利用上述軟體來處理內容的伺服器上，既可觸發該漏洞進行任意程式碼執行。

- CVE 編號：CVE-2020-1147
- 影響版本：
  1. .NET Core 2.1,
  2. .NET Framework 2.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 and 4.8 (depending on the Windows version),
  3. SharePoint Enterprise Server 2013 Service Pack 1, SharePoint Enterprise Server 2016, SharePoint Server 2010 Service Pack 2, SharePoint Server 2019,
  4. Visual Studio 2017 version 15.9, and Visual Studio 2019 versions 16.0, 16.4 and 16.6
- 解決方案：微軟已釋出相關安全公告，但尚未提供更新與防護措施建議。建議個人與機構組織關注微軟發布之 CVE-2020-1147 安全性公告，並優先進行軟體更新。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1147

第 3 章、 資安研討會及活動

企業智慧轉型 趨勢高峰論壇-數據驅動，商業再進化	
活動時間	**2020-08-11(二) 13:00 ~ 16:30**
活動地點	**台中市西屯區文心路二段 107 號 4 樓**
活動網站	**https://edm.bnext.com.tw/2020CHT-bigdata/**
活動概要	 **詳細活動議程及報名方式，請參閱活動網站。** 【 8/11 台中場 】企業智慧轉型 趨勢高峰論壇-數據驅動，商業再進化 活動時間：2020-08-11(二) 13:00 ~ 16:30 活動地點： 台灣台中市西屯區文心路二段 107 號 4 樓 集思台中文心會議中心

CYBERSEC 2020 臺灣資安大會 8/11-12 重磅回歸！	
活動時間	**2020 年 8 月 11-12 日**
活動地點	**南港展覽二館（臺北市南港區經貿二路 2 號）**
活動網站	https://r.itho.me/sec2020
活動概要	 **詳細活動報名及議程請見官方網站。** **主辦單位：iThome** 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 8/11-8/12 於南港展覽二館盛大登場！ 匯聚超頂尖資安高手現身說法，提供超過 180 堂資安跨領域、多面向的議程、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 家以上業界知名標竿資安品牌，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，與超過 5,000 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。 日期：2020 年 8 月 11-12 日 地點：南港展覽二館（臺北市南港區經貿二路 2 號） 了解更多大會資訊：https://r.itho.me/sec2020 活動全程免費，請立即報名↘ https://r.itho.me/2020_singup

(台灣網路講堂)發動網路攻擊算挑起戰爭嗎?	
活動時間	**2020 年 8 月 19 日（三）13:30 – 16:40**
活動地點	**IEAT 會議中心 8F 綜合教室** **（臺北市中山區松江路 350 號,台北市進出口商業同業公會）**
活動網站	https://www.ihub.tw/Calendar/ihub-20200819
活動概要	 **詳細活動報名與議程，請參閱活動網站。** 本場次特別邀請國際法專家及網路安全技術專家，分別就跨國界的網路衝突情境如何適用於國際法， 以及攻擊國歸因的技術挑戰進行專題演講，在網路戰爭攻擊或防衛成為各國發展重心的趨勢下，作 為國內進一步思考臺灣的機會與挑戰的開端。 活動議程 13:30 - 14:00 活動報到 14:00 - 14:10 開場與致詞 / 主持人：NII 產業發展協進會 陳文生 顧問 14:10 – 15:00 專題演講 1：從國際法分析網路攻擊 / 講者：國防大學法律系 田力品 系主任 15:00 - 15:50 專題演講 2：網路攻擊事件歸因的技術挑戰 / 講者：奧義智慧科技 吳明蔚博士 15:50 - 16:40 專題演講 3：中國對台的灰色地帶行動 / 講者：前戰爭學院榮譽講座 廖宏祥老師

第 19 屆暨展會亞太資訊安全論壇	
活動時間	**2020 年 9 月 1 日 (二)、9 月 2 日 (三)**
活動地點	**台北市信義區菸廠路 88 號**
活動網站	https://www.informationsecurity.com.tw/event/event_info.aspx?eid=1498
活動概要	 **詳細活動報名及議程請見官方網站。** **主辦單位: 資安人媒體** 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。 交通路線: 於捷運板南線國父紀念館站 5 號出口，自光復南路右轉菸廠路，步行約 500 公尺。 活動洽詢: 02-8729-1042 潘小姐 / Iris.Pan@newera.messefrankfurt.com

第 4 章、 2020 年 07 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。

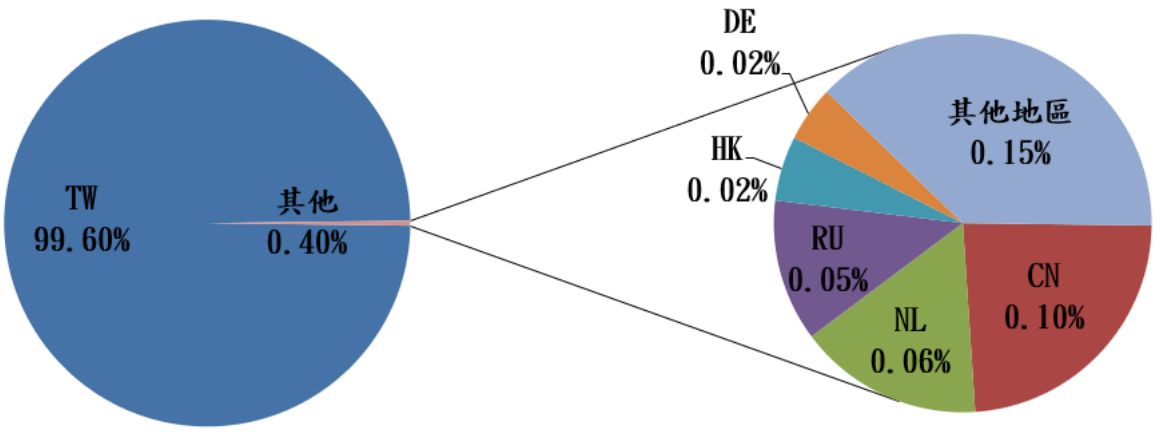


圖 1、分享地區統計圖

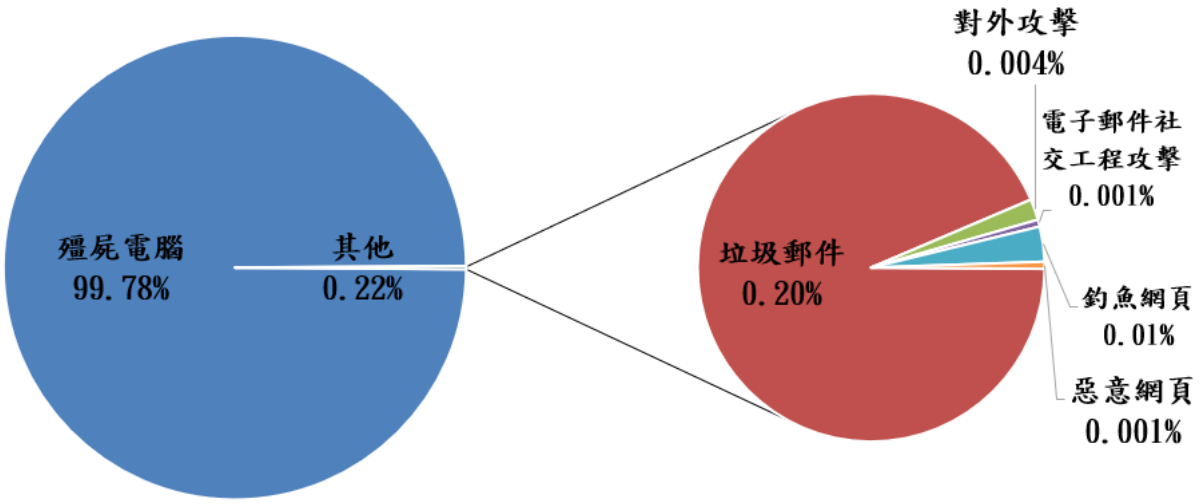

殭屍電腦
99.78%
其他
0.22%
垃圾郵件
0.20%
對外攻擊
0.004%
電子郵件社
交工程攻擊
0.001%
釣魚網頁
0.01%
惡意網頁
0.001%

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 8 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**