TWCERT/CC 資安情資電子報

2020 年 12 月份

目錄

第 1 章、 封面故事

近五萬台 Fortinet VPN 登入資訊遭竊，全球多家金融機構與政府機關被駭

資安專家發現近五萬台 Fortinet FortiOS SSL VPN 裝置遭駭，受害者遍及全球，且多為政府機關、金融機構等重要單位。

專門觀測全球金融資安事件的研究單位 Bank Security，旗下資安專家日前透過推特發表資安通報，推文指出該單位發現近五萬台 Fortinet FortiOS SSL VPN 裝置遭駭，受害者遍及全球，且多為政府機關、金融機構等重要單位。

該篇推文自駭侵者論壇中擷取三張圖片，清楚顯示出多達 49,577 個 Fortinet SSL VPN 被駭裝置的 IP；Bank Security 透過 NSLOOKUP 調查這些 IP 對應到的網址，隨即發現這些網址大多屬於世界各國政府機構、銀行與金融服務廠商。

被駭侵者攻擊的 Fortinet SSL VPN 漏洞編號為 CVE-2018-13379，駭侵者可利用此漏洞存取 Fortinet VPN 中的 sslvpn_websession 檔案，進而竊得 VPN 網路的登入資訊，並且伺機發動後續的各種攻擊行動，例如駭入內網伺服器、竊取更多機敏資訊，甚至布署勒贖軟體等等。

CVE-2018-13379 這個漏洞，早在一年多以前就已經推出資安修復更新，然而這次仍有近五萬台 Fortinet VPN 裝置遭駭客透過此老舊漏洞攻破，顯示

各國政府與金融相關單位須更加重視並提升資安防護意識與能力。

Fortinet 說明，「客戶的安全是 Fortinet 的首要任務。在 2019 年 5 月，Fortinet 已發布解決相關 SSL 漏洞的 PSIRT 公告，同時已直接與客戶溝通，亦在 2019 年 8 月和 2020 年 7 月透過部落格發布相關訊息，強烈建議進行系統升級。雖然無法確認是否有攻擊已透過此漏洞進行，我們將持續與客戶溝通，但我們仍敦促客戶實施升級和緩解措施。如需要獲取更多資訊，請瀏覽我們最新的部落格，並參閱 2019 年 5 月的公告。」

Fortinet 在此建議：

1. 確實蒐集、統計目前組織單位中所使用的 Fortinet FortiGate 產品版本資訊。
2. 針對 FortiGate 產品於 2018 年被揭露的 SSL VPN 功能相關漏洞 (CVE-2018-13379) 進行更新 FortiOS 的動作。
3. 目前這些漏洞所影響的 FortiOS 版本為 6.0 系列(6.0.0-6.0.4)/5.6 系列(5.6.0-5.6.10)/5.4 系列(5.4.0-5.4.12)/5.2 系列(5.2.0-5.2.14)，為了避免再被此系列漏洞影響，如果您目前是使用以上 FortiOS 版本，且系統上開啟 SSL VPN 功能(tunnel mode or web mode)，請盡速更新系統至 5.6.13(5.6 系列)/6.0.11(6.0 系列)/6.2.6(6.2 系列)。
4. 請即訂閱 Fortinet FortiGuard PRIST advisories RSS feed，主動掌握所有最新產品漏洞資訊。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/hacker-posts-exploits-for-over-49-000-vulnerable-fortinet-vpns/
  2. https://securityaffairs.co/wordpress/111309/hacking/leak-vulnerable-fortinet-vpns.html

3. https://securityaffairs.co/wordpress/109897/cyber-warfare-2/fbi-cisa-joint-alert-energetic-bear.html
4. https://fortiguard.com/psirt/FG-IR-18-384
5. https://www.fortinet.com/blog/business-and-technology/fortios-ssl-vulnerability
6. https://www.fortinet.com/blog/business-and-technology/atp-29-targets-ssl-vpn-flaws
7. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379
8. https://www.fortiguard.com/rss-feeds

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、國內資訊產品代工大廠疑遭駭侵攻擊

台灣國際資訊產品代工大廠，疑似遭到勒贖軟體攻擊，造成部分電腦設備無法運作；該公司表示是辦公室自動化系統出現異常。

台灣國際資訊產品代工大廠，於 109 年 11 月初疑似遭到勒贖軟體攻擊，造成部分電腦設備無法運作；該公司對外否認遭到勒贖攻擊，並對媒體表示是辦公室自動化系統出現異常，可能是遭到駭客入侵攻擊所致。

據國際資安媒體 BleepingComuter 指出，根據該刊收集到的勒贖信件，該公司疑似是遭到一個名為 DoppelPaymer 的勒贖軟體攻擊。

據 BleepingComputer 揭露的勒贖信內容，駭侵者要求於期限內支付贖款，否則將於暗網上公布該駭侵組織取得的所有資料。BleepingComputer 根據暗網上 DoppelPaymer 在本次勒贖信中的連結，發現該組織要求支付高額枚比特幣的贖金。

DoppelPaymer 是專門攻擊企業的勒贖攻擊，主要是利用 Windows 內部網路的漏洞，取得管理權限後進行快速擴散；只要 DoppelPaymer 取得 Windows 網域控制器的控制權，就會感染整個區域網路內的所有 Windows 裝置。

曾遭 DoppelPaymer 攻擊的對象遍及公民營組織，民間企業如墨西哥石油、法國布列塔尼電信公司；公立機構如美國加州的托倫斯市、喬治亞州的新堡大學等。

- 建議採取資安強化措施
  1. 建議定期將所有軟體及作業系統進行安全性更新，以修補資安漏洞。
  2. VPN 使用多重驗證登入機制，以減少因遭網路釣魚攻擊導致帳密洩漏、密碼暴力破解，而被駭客登入之風險。
  3. 定期將檔案執行多重備份和異地備份，並檢視重要伺服器或電腦上是否有異常工作排程或異常檔案。
  4. 系統應嚴格區分使用者身份與權限，高權限之帳號應限縮登入來源及方式。
  5. 記錄遠端桌面服務登入所有重要主機之行為並留存，以利後續追蹤。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/laptop-maker-compal-hit-by-ransomware-17-million-demanded/
  2. https://www.zdnet.com/article/compal-the-second-largest-laptop-manufacturer-in-the-world-hit-by-ransomware/
  3. https://securityaffairs.co/wordpress/110638/malware/compal-ransomware-attack.html?utm_source=rss&utm_medium=rss&utm_campaign=compal-ransomware-attack

2.1.2、超過十萬台 Windows 電腦仍存有極嚴重的 SMBGhost 漏洞

資安廠商指出，雖然微軟早在三月就針對嚴重的 SMBGhost 漏洞發布修補軟體，但至今仍有超過十萬台的 Windows 10 電腦，尚未修補此一漏洞。

資安廠商 ESET 指出，雖然微軟早在三月間，就針對嚴重的 SMBGhost 漏洞發布修補軟體，但至今仍有超過十萬台的 Windows 10 電腦，尚未修補此一漏洞，曝露在嚴重的遠端駭入風險下。

這個漏洞的編號為 CVE-2020-0796，駭侵者只要針對未修補此漏洞電腦的 SMB 伺服器發送特製的攻擊封包，即可利用這個漏洞遠端執行任意程式碼。受此漏洞影響的 Windows 10 單機版與伺服器版本分別為 1903 與 1909。

據 ESET 估計，全球網路上約有 103,000 台 Windows 10 電腦曝露在此漏洞的攻擊風險之下，換算下來約等於全球網路上有開放 Port 445 電腦的 8% 左右。

這個漏洞的危險程度極高，其 CVSS 危險程度評分高達滿分 10 分。微軟甚至是在例行的每月 Patch Tuesday 之外，針對這個漏洞單獨發行修補程式；而美國國土安全部網路安全暨基礎設施安全局（US Cybersecurity & Infrastructure Security Agency, CISA）也針對此漏洞發表資安通報。

ESET 指出，鑒於本漏洞的高度危險性，尚未修補此漏洞的系統管理者，應立即安裝執行微軟提供的修補工具，或將 Windows 10 系統升級至最新版本，以防駭侵者利用此嚴重漏洞發動攻擊得逞。

- 資料來源：
  1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0796
  2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796
  3. https://us-cert.cisa.gov/ncas/current-activity/2020/06/05/unpatched-microsoft-systems-vulnerable-cve-2020-0796
  4. https://www.welivesecurity.com/2020/10/29/over-100000-machines-remain-vulnerable-smbghost-exploitation/

2.1.3、駭侵團體利用 Zerologon 漏洞攻擊日本汽車、製藥與機械工業全球據點

資安專家發現一波針對日本汽車、製藥與機械製造業者的大規模駭侵攻擊行動，利用近來發現的危險資安漏洞 Zerologon 進行。

資安廠商賽門鐵克旗下的資安研究人員，近來發現一波針對日本汽車、製藥與機械製造業者在全球各地分支機構的大規模駭侵攻擊行動，利用近來發現的危險資安漏洞 Zerologon 進行。

據賽門鐵克的研究報告指出，這波攻擊除了針對日本製造業在日本本土的工廠與辦公室外，也攻擊了這些企業在全球其他 16 個國家的分支機構，規模十分龐大。

除了日本之外，這 16 個被攻擊的國家包括美國、墨西哥、英國、法國、德國、比利時、阿聯、印度、中國、泰國、越南、香港、台灣、菲律賓、南韓、新加坡。

賽門鐵克說，該公司掌握了相當充分的證據，可證明這波攻擊的發動者，可能就是 APT 駭客組織 Cicada（又名 APT10、Stone Panda 或 Could Hopper）。

賽門鐵克指出，Cicada 在此波攻擊中，除了用上各種過去慣用的駭侵攻擊外，也加入了最近被發現的嚴重資安漏洞 Zerologon（CVE-2020-1472），能在極短時間內駭侵企業內網，立即掌握內網的 Active Directory 並取得控制

權。

除了 Zerologon 外，賽門鐵克也發現 Cicada 利用自製的 Backdoor.Hartip 惡意軟體，用以竊取企業機敏資訊，例如各種營業記錄文件、人力資源資料、會議記錄、收支記錄等等。

- 資料來源：
  1. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage
  2. https://www.zdnet.com/article/cicada-hacking-group-exploits-zerologon-launches-new-backdoor-in-automotive-industry-attack-wave/

2.1.4、資安廠商公布 2020 年最多人使用的前 200 組密碼

資安廠商公布 2020 年全球網友最常使用的 200 組密碼、這些密碼被洩漏的次數，以及駭侵者破解這類密碼所需的時間；同時呼籲大眾不要使用這些常見密碼。

資安廠商 NordPass 日前發表研究報告，公布該公司觀測到的 2020 年全球網友最常使用的 200 組密碼。報告中同時揭露了這些密碼被洩漏的次數，以及駭侵者破解這類密碼所需的時間。

根據這份報表，網友最常使用前十大密碼分別是：

1. 123456
2. 123456789
3. picture1
4. password
5. 12345678
6. 111111
7. 123123
8. 12345
9. 1234567890
10. senha（西班牙文的「密碼」）

NordPass 同時公布了駭侵者破解這些常用密碼通常所需要的時間；除了第三組需要三小時、第十組需要 10 秒外，其他八組常見密碼的破解所需時間，都在一秒以內。

在報告中，NordPass 也分析的這些常用密碼的類型，包括易記的數字組合、人名、常用裝置名稱、運動名稱、食物名稱、熱門遊戲或電影片名或主角名稱、勵志或罵人語句、鍵盤上字母與數字的排列順序，甚至就是「密碼」這個字的拼法等等。

NordPass 呼籲大眾，在設定新密碼時，除了避免使用這些常見密碼，並使用超過 12 個字元、混合使用大小寫字母、數字與特殊符號的強式密碼之外，為避免密碼不好記，也應使用密碼管理工具，並設定多階段登入驗證。

- 資料來源：
  1. https://solutionsreview.com/identity-management/nordpass-unveils-200-most-common-passwords-of-2020/
  2. https://nordpass.com/most-common-passwords-list/

2.1.4、Google Chrome 再次更新，但八成以上用戶尚未使用最新版本

資安專家指出，Google Chrome 雖然已更新到最新版，修補多個漏洞，但仍有八成以上用戶尚未更新，可能遭到攻擊。

資安專家指出，全球市場佔有率最高的 Google Chrome 瀏覽器，日前雖然已更新到最新版，修補多個漏洞，其中甚至包括多個 0-day 漏洞；但仍有八成以上用戶尚未更新，可能遭到駭侵者利用這些 0-day 漏洞發動攻擊。

在 11 月 17 日最新推出的 Chrome 87.0.4280.66 for Windows and Lunix、Chrome 87.0.4280.67 for Mac 中，一共修復多達 33 個資安漏洞，其中多達十個漏洞的危險程度評級達到「高度」等級，分別是 CVE-2020-16018、CVE-2020-16019、CVE-2020-16020、CVE-2020-16021、CVE-2020-16022、CVE-2020-16015、CVE-2020-16014、CVE-2020-16023、CVE-2020-16024、CVE-2020-16025 等。

雖然 Google Chrome 經常推出更新，但據資安公司 Menlo Labs 的研究報告指出，多數 Google Chrome 並未在第一時間就更新其 Chrome 瀏覽器。

據 Menlo Labs 在 11 月中進行的調查，該公司的客戶所使用的 Google Chrome，共有 49 個不同的版本；當時的調查資料顯示，僅有 61% 客戶使用當時最新的 Google Chrome 86 版，尚有 28% 還在使用前一版本的 Google Chrome。

甚至在已經執行當時最新的 86 版的客戶中，有高達 83% 的用戶仍在使用非最新版本，且含有多個 0-day 漏洞的 86.0.4240.198 之前版本；換言之，

這些用戶都處於可能被駭侵者透過未修補的 0-day 漏洞攻擊的風險之下。

- 資料來源：
  1. https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_17.html
  2. https://www.menlosecurity.com/blog/chrome-gets-patched-again-but-83-of-users-arent-running-the-latest-version

2.2、國際政府組織資安資訊

2.2.1、南韓發生供應鏈攻擊事件，北韓 APT 駭侵者竊取數位憑證、散布惡意軟體

資安專家發現北韓駭侵團體 Lazarus 在南韓發動供應鏈攻擊行動，企圖藉由在南韓有高安裝量的官方指定資安監控軟體，駭入受害者電腦並竊取機敏資訊。

斯洛伐克資安廠商 ESET 旗下的資安專家，日前發現北韓駭侵團體 Lazarus 在南韓發動供應鏈攻擊行動，企圖藉由在南韓有極高安裝量的官方指定資安監控軟體 WIZVERA VeraPort，駭入受害者電腦並竊取機敏資訊。

ESET 發表的研究報告指出，WIZVERA VeraPort 是南韓政府指定使用於存取政府與銀行網路服務時必須安裝的資安監控驗證軟體；VeraPort 會自動安裝各種政府與金融機構網站所需的系統元件和資安軟體，但 VeraPort 在驗證網站的數位憑證時，只會檢查數位簽章本身的真偽，不會檢查誰擁有這個數位簽章。

駭侵團體 Lazarus 利用此一漏洞，近期在南韓發動供應鏈供擊；據研究報告指出，Lazurus 的駭侵手法如下：首先駭入已獲得 VeraPort 認證，且擁有合法數位簽的網站，然後在其惡意軟體中加上合法的數位簽章，並植入遭駭的網站中。一旦安裝了 VeraPort 的受害者電腦連線到該網站，就會自動下載並安裝含有合法數位簽章的惡意軟體。

受害者電腦被安裝惡意軟體後，接著會下載 Dropper 惡意軟體，在受害電腦中開啟可遠端控制的後門，以進行後續的駭侵攻擊，包括檔案與資料竊取，或是做為跳板執行其他駭侵攻擊。

- 資料來源：
  1. https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/
  2. https://threatpost.com/hacked-software-south-korea-supply-chain-attack/161257/
  3. https://www.zdnet.com/article/lazarus-malware-strikes-south-korean-supply-chains/

2.2.2、美國政府資安單位指出，總統大選至今沒有因駭侵攻擊發生重大事故

美國主管資安事務的資安與基礎設施安全局局長 Krebs，在大選結束後發表談話，指出這次大選並未發生因駭侵攻擊造成的重大事故。

美國主管資安事務的資安與基礎設施安全局（Cybersecurity and Infrastructure Security Agency，CISA）局長 Christopher Krebs，在大選結束後發表談話，指出這次大選期間雖然不斷傳出各種駭侵事件，但最終的投票與計票工作，並未受到駭侵攻擊而造成重大事故。

Krebs 指出，過去四年以來，CISA 與美國各相關單位積極針對可能影響大選的資安攻擊進行準備，加強各種防禦措施，因此以目前觀察到的情報，整個投開票作業沒有因為資安事故而受到阻擾。

Krebs 說，由於全美各級政府，以及選舉相關的私部門通力合作，加強選舉相關系統的資安防護與復原能力，成功阻擋可能的惡意攻擊活動與駭侵團體，才獲致如此成績。

Krebs 表示，CISA 將會持續努力支援各州與地方選務單位的資安防護工作，直到所有選務工作告一段落為止。

由於美國大選仍有眾多州的計票工作尚在進行之中，Krebs 也表示，CISA 會持續監控所有外國駭侵團體的活動，防止這些駭侵攻擊影響最後計票與大選結果。

Krebs 也要求美國大眾保持冷靜，理性等待選舉結果出爐；不要輕信任何關於大選傳出的不實消息，僅只採信由政府選務機關發表的相關訊息。CISA 有一個專門用以澄清與選務資安工作相關謠言的網頁可供美國民眾參閱。

- 資料來源：
  1. https://www.cisa.gov/news/2020/11/04/statement-cisa-director-krebs-following-final-day-voting
  2. https://www.cisa.gov/rumorcontrol

2.2.3、美國網戰司令部指出，俄羅斯惡意軟體正攻擊外交、國會與使館機構

美國網戰司令部日前發表資安通報，指出該單位觀察到近來有俄羅斯駭侵團體，利用惡意軟體植入手法，攻擊外交、國會與使館所屬機構的電腦系統。

美國網戰司令部日前發表資安通報，指出該單位觀察到近來有一個名為 Turla 的俄羅斯 APT 駭侵團體，近來利用兩支惡意軟體，針對外交、國會與使館所屬機構的電腦系統發動植入攻擊。

資安媒體 BleepingComputer 指出，Turla 從 1996 年就開始活躍，過往曾有攻擊美軍總司令部、美國國防部與太空總署的記錄。

這兩支惡意軟體都是屬於後門攻擊型惡意軟體，其中一支名為 ComRAT。根據美國資安與基礎設施安全局的分析報告指出，ComRAT 會安裝一個 Windows PowerShell 指令檔，並載入一個含有惡意程式碼的 64 位元 DLL 檔，該檔即為 ComRAT 第四版。

ComRAT 接著會將一個通訊模組注入 Windows 系統預設的瀏覽器，並開始監聽並竊取受害電腦上的機敏資訊，並接受駭侵者的控制，以執行各種攻擊活動。

另一支在通報中提及的惡意軟體，稱為 Zebrocy，是兩段由 Golang 撰寫的 Windows 32 位元可執行檔；遭植入系統後，可供駭侵者遠端遙控，進行各種資料竊取或其他攻擊任務。

CISA 針對 ComRAT 與 Zebrocy 提供了完整的程式碼分析報告，並建議可能受攻擊的機構，務必使用最新版本的防毒防駭軟體、保持作業系統更新至最新版本、關閉檔案與印表機共享服務，或以密碼和其他措施加以保護，加強系統整體防護能力。

- 資料來源：
  1. https://us-cert.cisa.gov/ncas/current-activity/2020/10/29/cisa-fbi-and-cnmf-identify-new-malware-variant-comrat
  2. https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303a
  3. https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303b
  4. https://www.bleepingcomputer.com/news/security/us-shares-info-on-russian-malware-used-to-target-parliaments-embassies/

2.3、行動裝置資安訊息

2.3.1、Facebook 修復 Android 版 Messenger 的資安漏洞

Facebook 日前修復一個 Facebook Messenger for Android 的嚴重資安漏洞；該漏洞可讓駭客竊聽語音對話內容，甚至受害者身邊的聲音而不被發現。

發現這個漏洞的資安專家，是 Google 旗下資安研究團隊 Project Zero 的 Natalie Silvanovich；專家指出在一般情形下，Facebook Messenger 只會在受話者按下通話按鈕後，才開始傳送音訊資料，但這個漏洞讓駭侵者只要先登入 Facebook Messenger，並且在撥打電話給受害者時同時送出特製的訊息，即可在受害者尚未接起電話時，就啟用音訊資料傳輸；駭侵者將可以竊聽受害者身邊的所有聲音。

這個漏洞出現在 Facebook Messenger 在實作 WebRTC 網路影音傳輸協定時發生的錯誤，受此漏洞影響的 Facebook Messenger for Android 版本為 284.0.0.16.119 與較舊的所有版本。

Natalie Silvanovich 在提報給 Facebook 的資安漏洞通報中，也提供了重現此漏洞的詳細操作步驟。值得注意的是，欲利用這個漏洞進行攻擊的駭侵者，必須擁有和受害者透過 Facebook Messenger 通話的權限，也就是說必須是受害者的朋友，或經受害者同意透過 Facebook Messenger 通話。

Facebook 於 10 月 6 日時接獲 Natalie Silvanovich 的資安漏洞通報，隨即於 11 月 17 日推出修復此漏洞的更新版本；所有在 Android 裝置上使用 Facebook Messenger 的用戶，應即更新至最新版本，以避免遭此漏洞攻擊。

- 影響產品/版本：Facebook Messenger for Android 284.0.0.16.119 與較舊版本
- 解決方案：升級至 Facebook Messenger for Android 最新版本

- 資料來源：
  1. https://bugs.chromium.org/p/project-zero/issues/detail?id=2098
  2. https://threatpost.com/facebook-messenger-bug-spying-android/161435/
  3. https://thehackernews.com/2020/11/facebook-messenger-bug-lets-hackers.html

2.4、軟體系統資安議題

2.4.1、資安專家發現 Linux 弱點，導致 DNS 快取污染攻擊再度成為可行

美國與中國資安專家日前聯合發表研究報告，指出一種新式攻擊手法，可利用 Linux 存在的弱點發動 DNS 快取污染攻擊。

美國加州大學與中國北京清大的資安專家，日前聯合發表研究報告；研究人員發現一種新式攻擊手法，可利用 Linux 存在的弱點發動 DNS 快取污染攻擊。

DNS 快取污染攻擊係透過大量發送偽造的 DNS 查詢交易 ID，來將受害者的網路連線導向至偽造的網站伺服器；一般認為已於 2008 年透過隨機連接埠技術解決，也就是 DNS 查詢接收使用的連接埠不再固定使用 port 53，而會隨機使用 port 0 到 port 65535。即使攻擊者猜中了查詢者使用的交易 ID，也很難猜中查詢封包使用哪一個連接埠來傳送。

隨機連接埠技術看似解決了 DNS 快取污染的問題，但兩所大學的研究人員近來發現，可以利用「旁路攻擊」的技術來找出 DNS 用戶端查詢時使用的連接埠，從而使隨機連接埠的防護技術失效。

研究報告指出，由於 Linux 核心在處理 ICMP 查詢時，雖然會限制每個用戶一秒只能查詢一千次，但這個限制只針對單一用戶端使用的連接埠；換言之，攻擊者可以同時利用一千個不同的連接埠來發送 DNS 查詢要求，就能

根據 Server 的回應，找出可供使用的連接埠號，從而大大提高猜中 DNS 查詢使用連接埠號的機率，進而發動 DNS 快取污染攻擊。

Linux 的這個漏洞已在日前編為 CVE-2020-25705，其 CVSS 危險程度評分達 7.3 分；已在 5.10 版的 Linux 核心版本中得到修補。

- 資料來源：
  1. https://dl.acm.org/doi/pdf/10.1145/3372297.3417280
  2. https://www.bleepingcomputer.com/news/security/dns-cache-poisoning-attacks-return-due-to-linux-weakness/
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25705
  4. https://access.redhat.com/security/cve/cve-2020-25705

2.4.2、新發現 Linux 系統蠕蟲 Gitpaste-12，將惡意程式碼托管於 Github 與 Pastebin

資安專家發現新種蠕蟲，專門攻擊 x86 Linux 伺服器與 Linux IoT 裝置；該蠕蟲可載入 12 種以上不同的攻擊模組，更把其攻擊程式碼托管於 Github 與 Pastebin。

網通大廠 Juniper 旗下的資安研究團隊 Juniper Threat Labs 日前發表研究報告，指出該單位的資安專家於十月中旬發現新種蠕蟲，專門攻擊 x86 Linux 伺服器，以及以 ARM 和 MIPS 處理器為基礎的 Linux IoT 裝置；該蠕蟲因可載入 12 種以上不同的攻擊模組，所以被稱為「Gitpaste-12」。

資安專家更發現，Gitpaste-12 把其攻擊模組的程式碼，托管於 Github 與 Pastebin；在感染初期，主要會利用過去已知的 11 種資安漏洞，如 Apache Struts 的 CVE-2017-5638、Asus 路由器的 CVE-2013-5948、Opendreambox Webadmin 擴充套件的 CVE-2017-14135 與 Tenda 路由器的 CVE-2929-10987 等漏洞，利用密碼暴力試誤法等方式入侵系統後，再利用其主要的 shell script 載入並執行後續需要的攻擊用模組。

接著 Gitpaste-12 會先從 Pastebin 下載一段程式碼，設定一個每分鐘執行一次的 cron job，用以進行自我更新；然後 Gitpaste-12 會再從 Github 下載執行攻擊用的程式碼，這段程式碼中包含阻擋系統防毒防駭功能的指令，包括關閉防火牆規則、selinux、apparmor 等防護功能，而且這段程式碼中還包括許多以簡體中文撰寫的程式註解。

資安專家也說，這段程式碼還有不少專門用以阻擋阿里雲、騰訊雲資安防護功能的指令，顯然其攻擊是針對這些雲端服務上的目標而設定。

- 資料來源：
  1. https://blogs.juniper.net/en-us/threat-research/gitpaste-12
  2. https://threatpost.com/gitpaste-12-worm-linux-servers-iot-devices/161016/

2.4.3、Microsoft Teams 用戶遭假冒更新檔案進行攻擊

微軟公司針對 Microsoft Teams 用戶示警，指出有駭侵者利用偽造的 Microsoft Teams 更新發動攻擊，試圖安裝惡意軟體。

微軟公司日前針對 Microsoft Teams 用戶發出警示訊息，指出有駭侵者透過 Cobalt Strike 利用偽造的 Microsoft Teams 更新發動攻擊，試圖在整個內網的所有 Windows 電腦中安裝惡意軟體。

微軟說，駭侵者對受害對象發送偽造的系統更新通知，誘騙用戶安裝內含惡意軟體的 Cobalt Strike 程式，利用 Zerologon 漏洞感染內網所有 Windows 裝置，並且入侵 Windows AD 伺服器並取得控制權。

據指出，這波攻擊的受害者，主要是小學與學前教育機構；這些機構由於受到 Covid-19 影響，必須透過諸如 Microsoft Teams 之類的解決方案，來進行遠距教學。

微軟表示，駭侵者購買搜尋引擎關於 Microsoft Teams 的關鍵字廣告，誘騙用戶點擊偽造的升級連結，並把用戶導向內含惡意軟體連結的假網站；用戶一旦點擊並安裝假的升級檔案，惡意軟體就會安裝真正的 Microsoft Teams 升級軟體，以降低用戶戒心，但會同時執行一段 PowerShell 程式碼，下載安裝更多惡意軟體。

微軟說，第一次安裝到用戶上的惡意軟體，以竊取資訊為主，包括受害者的登入資訊、瀏覽器資料、付款資訊等；接續載入的惡意軟體，就會包括 Cobalt Strike 的 beacon，可以讓攻擊者用來定位受害者並發動後續攻擊，包括勒贖攻擊等。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/
  2. https://threatpost.com/microsoft-teams-fakeupdates-malware/161071/

2.4.4、勒贖軟體 Maze 幕後駭侵組織宣布停止運作

惡名昭彰的勒贖攻擊軟體 Maze，其幕後組織宣布停止運作；但資安專家仍表懷疑。

曾發動多次勒贖攻擊，同時威脅受害者，若不支付贖金即公開竊得資料，造成重大損失的惡意軟體 Maze，其幕後駭侵組織發表公告，宣布即日起停止該軟體運作；但資安專家仍表懷疑，並呼籲各界不可掉以輕心。

該組織的公告發布於暗網上，指出該組織即日起停止運作；任何以 Maze 或該組織為名的攻擊行動，均與該團體無關。

在公告中，該組織也宣稱未與任何其他單位合作，也沒有後續接手 Maze 的組織；該組織的駭侵專家也沒有進行其他駭侵軟體的專案，因此不可能有後續者。

但資安專家並不輕信該組織的說法；有資安專家指出，該組織的人員很可能只是為了暫避風頭而發出此聲明，實際上可能會轉移到其他惡意軟體計畫；也有資安專家指出，目前的勒贖「市場」非常擁擠，競逐者眾；很可能是 Maze 透過勒贖攻擊能夠取得的贖金開始下降，駭侵者於是轉移陣地，另起爐灶。

Maze 組織在公開信中也提到該組織發展 Maze 的理由，是希望提醒世人資安防護的重要性；也有資安專家認為該團體將受害者都稱為「客戶」，可能希望受害者以非正式的方式僱用其為資安防護服務提供者；其贖金則是支

付給該單位的服務費用。

資安專家也提醒，犯人極少突然幡然悔悟，改過向善；很可能只是放棄舊工具，換個名字重操舊業而已，大家仍應提高警覺，做好應做的資安防護工作，不要輕信這類的說法。

- 資料來源：
  1. https://twitter.com/inderbarara/status/1323249010749046788/photo/1
  2. https://siliconangle.com/2020/11/02/infamous-maze-ransomware-group-announces-shutting/
  3. https://techcrunch.com/2020/11/02/maze-ransomware-group-shutting-down/

2.4.5、Apple 推出 macOS Big Sur 11.0.1，修復 60 個資安漏洞

Apple 公司日前推出 macOS Big Sur 11.0.1，一口氣修復了 60 個資安漏洞；其中有些漏洞已經被廣為用於駭侵攻擊之用。

Apple 公司日前推出 macOS Big Sur 的第一個升級版本 11.0.1，一口氣修復了高達 60 個資安漏洞；其中有些漏洞已經被廣為用於駭侵攻擊之用。

於今年 11 月 12 日首次推出的 macOS 11.0 Big Sur，於推出數日之後立即就推出了小升級版，除了解決一些作業系統本身的錯誤外，最重要的是內含多達 60 個資安漏洞的修補。

值得注意的是，在這批得到修補的資安漏洞中，有一個發生在字型子系統的 CVE-2020-27930，先前已經遭到駭侵者大規模使用；駭侵者可以使用特製的字型檔案，引發系統記憶體崩潰，從而利用這個漏洞來遠端執行任意程式碼，或是竊取系統上的機敏資訊。

在 macOS Big Sur 11.0.1 中修補，可能導致駭侵者遠端執行任意程式碼的其他資安漏洞，還包括 CVE-2020-27910、CVE-2020-27916、CVE-2020-10017、CVE-2020-9949、CVE-2020-9883、CVE-2020-9999、CVE-2020-9965 等，一共有高達 21 個 RCE 漏洞都得到修補。

已經將 Mac 電腦系統升級至 macOS Big Sur 的各款 Mac 電腦用戶，應儘速透過系統更新，將電腦的作業系統更新至最新的 macOS 11.0.1，以降低遭

駭侵者利用這些漏洞發動攻擊的風險。

- 資料來源：
  1. https://support.apple.com/en-us/HT211931
  2. https://www.securityweek.com/macos-big-sur-1101-patches-60-vulnerabilities
  3. https://www.securityweek.com/apple-patches-three-actively-exploited-vulnerabilities

2.5、軟硬體漏洞資訊

2.5.1、Oracle WebLogic 伺服器嚴重漏洞，已遭駭侵團體大規模惡意濫用

發生在 Oracle WebLogic 伺服器上的嚴重漏洞 CVE-2020-14882，近來傳出已遭駭侵團體大規模濫用，用於資料竊取、植入惡意程式碼等攻擊活動。

CVE-2020-14882 是存於 Oracle Fusion Middleware 旗下 Oracle WebLogic 伺服器控制台模組的嚴重資安漏洞，可讓未經授權的駭侵者，利用簡單的 HTTP Get 請求指令，輕易取得伺服器控制權限；且其 CVSS 危險程度評分高達接近十分滿分的 9.8 分。

雖然 Oracle 已於十月底推出資安修補程式，解決了此一漏洞，但仍有許多 Oracle WebLogic 伺服器尚未更新；資安專家最近觀察到許多試圖利用此漏洞的攻擊活動，甚至已有駭侵團體，利用 Cobalt Strike 這個原本用於找出漏洞加以修復的系統入侵工具，來進行此一漏洞的攻擊活動。

資安專家指出，他們觀察到近期有近 66% 的勒贖攻擊，沒有採用過去常用的各種市售公版駭侵工具，而是改以 Cobalt Strike 工具來發動攻擊；而除了攻擊 CVE-2020-14882 漏洞之外，駭侵者也會同時攻擊另一個存於 Oracle WebLogic 伺服器漏洞 CVE-2020-14750；這個漏洞同樣也能讓未經授權的攻擊者，取得伺服器的控制權限。

Oracle 已於十月底推出這兩個漏洞的更新修補程式，美國資安與基礎建設安全局（CISA）也強烈敦促 Oracle WebLogic 伺服器的管理者，應儘速更新修補這兩個漏洞，以降低遭鎖定攻擊的資安風險。

- CVE 編號：CVE-2020-14882
- 影響產品/版本：Oracle WebLogic Server 10.3.6.0.0、12.1.3.0.0、12.2.1.3.0、12.2.1.4.0、14.1.1.0
- 解決方案： 儘速更新到最新版本，或安裝資安修補程式

- 資料來源：
  1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14882
  2. https://www.bleepingcomputer.com/news/security/critical-bug-actively-used-to-deploy-cobalt-strike-on-oracle-servers/
  3. https://www.bleepingcomputer.com/news/security/critical-oracle-weblogic-flaw-actively-targeted-in-attacks/
  4. https://www.oracle.com/security-alerts/cpuoct2020.html

2.5.2、VMware 揭露 Workspace One 的嚴重 0-day 資安漏洞

VMware 揭露 Workspace One 的嚴重 0-day 資安漏洞，可用以遠端執行任意程式碼。

虛擬技術大廠 VMware 近日發表資安通報，指出旗下 VMware Workspace One 的某些版本，存有嚴重的 0-day 資安漏洞，可能導致駭侵者用以提升執行權限，進而遠端執行任意程式碼。

這個漏洞的 CVE 編號為 CVE-2020-4006，是一種指令注入錯誤，存於 VMware Workspace One 的某些 Windows 與 Linux 版本；駭侵者只要能夠取得管理者密碼，並且可透過連接埠號 8443 連線，即可以不受限的使用者身分執行任意程式碼。

受到該漏洞影響的 VMware Workspace One 版本，包括 VMware Workspace One Access Linux 版 20.10 與 20.01、VMware Identity Manager Linux 版 3.3.1 至 3.3.3、VMware Identity Manager Connector Linux 版 3.3.1 與 3.3.2、VMware Identity Manager Connector Windows 版 3.3.1 到 3.3.3。

這個漏洞的 CVSS 危險程度評分高達 9.1 分（滿分為 10 分）；目前 VMware 提供暫時解決方案，已經遭此漏洞攻擊的系統管理員，可以依照暫時解決方案提供的步驟，把相關的系統設定選項鎖定住；但如果要更動系統設定，則必須反向操作才能更改。

- CVE 編號：CVE-2020-4006
- 影響產品/版本：

  VMware Workspace One Access Linux 版 20.10 與 20.01

  VMware Identity Manager Linux 版 3.3.1 至 3.3.3

  VMware Identity Manager Connector Linux 版 3.3.1 與 3.3.2

  VMware Identity Manager Connector Windows 版 3.3.1 到 3.3.3

- 解決方案：依照暫時解決方案提供的步驟處理

- 資料來源：
  1. https://www.vmware.com/security/advisories/VMSA-2020-0027.html
  2. https://kb.vmware.com/s/article/81731
  3. https://www.bleepingcomputer.com/news/security/vmware-discloses-critical-zero-day-vulnerability-in-workspace-one/

2.5.3、WordPress 擴充套件 Ultimate Member 最新嚴重資安漏洞

資安防護廠商 Wordfence 日前發表研究報告，指出一個廣為安裝的 WordPress 擴充套件 Ultimate Members 存有一個嚴重資安漏洞，可導致駭侵者提升自身執行權限，並且奪取 WordPress 網站的控制權。

Ultimate Members 是用來強化 WordPress 使用者權限管理的擴充套件，安裝次數超過十萬次以上；Wordfence 的資安專家，發現 Ultimate Member 在處理使用者註冊表單時存有漏洞，駭侵者可以透過直接更新用戶 meta data 的方式提升新註冊帳號的權限，進而輕易取得系統管理員身分，進行任何未經授權的操作。

這個漏洞目前尚無 CVE 編號，但其 CVSS 危險程度評分高達滿分十分；版本號碼在 2.1.11 之前（含 2.1.11）的 Ultimate Member 都存有此一漏洞。

Wordfence 於 10 月 23 日通報 Ultimate Member 的開發者，並待其推出修正版本後，於日前公開此一漏洞；所有在其 WordPress 系統內安裝有 Ultimate Member 擴充套件的用戶，均應立即更新至 2.1.12 與後續版本，以降低駭侵者利用此漏洞發動攻擊的風險。

- 影響產品/版本：Ultimate Member 2.1.11 與所有較舊版本
- 解決方案：升級至 Ultimate Member 2.1.12 與其後續版本

- 資料來源：
  1. https://www.wordfence.com/blog/2020/11/critical-privilege-escalation-vulnerabilities-affect-100k-sites-using-ultimate-member-plugin/
  2. https://www.bleepingcomputer.com/news/security/wordpress-plugin-bugs-can-let-attackers-hijack-up-to-100k-sites/

2.5.4、WordPress 擴充套件 wp-file-manager 漏洞，遭大規模用於駭侵攻擊

WordPress 上廣為使用的檔案管理擴充套件 wp-file-manager，日前遭發現一個嚴重資安漏洞，可能遭駭侵者用以遠端執行任意程式碼。

該漏洞已遭駭侵者用以大規模發動攻擊，使用此擴充套件的 WordPress 管理者，應儘速更新以避免遭此漏洞影響。

這個漏洞出現在 The File Manager 處理檔案上傳使用的 connetor.mininal.php 程式碼中，這段程式碼可在未經授權的情形下存取，駭侵者因此可以上傳任意檔案到 WordPress 伺服器，遠端執行任意程式碼。

這個漏洞編號為 CVE-2020-25213，其 CVSS 危險程度評分高達 9.8 分。據資安專家指出，該漏洞在八月底開始遭到駭侵者用以攻擊 WordPress 伺服器，在八月最後一周，每天偵測到的攻擊次數超過 15,000 次。

存有此漏洞的 wp-file-manager 版本分別為：

1. File Manager Plugin for WordPress 6.0 至 6.8
2. File Manager Pro Plugin for WordPress 7.6 至 7.8

The File Manager 總下載次數超過 600,000 次，其開發者已於九月初提供升級版本供用戶下載，解決了這個嚴重漏洞。任何 The File Manager 用戶均應盡速下載更新至最新版本（目前為 6.9 版），以避免此漏洞帶來的資安風

險。

- CVE 編號：CVE-2020-25213
- 影響產品/版本：File Manger 6.0~6.8、File Manager Pro 7.6~7.8
- 解決方案：升級至最新版本

- 資料來源：
  1. https://securitynews.sonicwall.com/xmlpost/cve-2020-25213-wordpress-plugin-wp-file-manager-actively-being-exploited-in-the-wild/
  2. https://medium.com/bugbountywriteup/exploiting-cve-2020-25213-wp-file-manager-wordpress-plugin-6-9-3f79241f0cd8
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25213
  4. https://nvd.nist.gov/vuln/detail/CVE-2020-25213

2.5.5、Apple 發表 iOS、iPad OS 14.2 與 watchOS 7.1，修補 3 個 0-day 漏洞

Apple 於 11 月 5 日發表發表最新版本的 iOS、iPad OS 14.2 與 watch OS 7.1，除例行的新增功能與錯誤修復外，更解決了三個可讓駭侵者遠端執行任意程式碼的嚴重 0-day 漏洞。

新版本作業系統解決的問題，包括在字體處理模組 FontParser 與核心的錯誤；這些錯誤可導致駭侵者以核心等級權限遠端執行任意程式碼。

根據 Apple 的更新說說明文件指出，這三個 0-day 漏洞分別如下：

1. CVE-2020-27930：存於 FontParser 的記憶體崩潰錯誤，駭侵者可以用特製的字型檔引發此錯誤，進而遠端執行惡意程式碼；
2. CVE-2020-27932：記憶體啟始過程中發生的錯誤，可讓駭侵者以核心等級權限執行任意程式碼；
3. CVE-2020-27950：程式碼型別的錯誤，惡意程式可利用此錯誤竊取核心記憶體內容。

這三個錯誤是由 Google 旗下的資安團隊 Project Zero 於今年十月下旬發現，並向 Apple 通報；受影響的裝置包括 iPhone 5s 與後續版本、iPod Touch 第六代與第七代、iPad Air、iPad mini 2 與後續版本、Apple Watch 所有版本；上述 Apple 裝置與產品之用戶，應立即使用內建的軟體更新功能，更新至最新版本作業系統，以降低遭駭侵者利用這批漏洞發動攻擊的資安風險。

- CVE 編號：CVE-2020-27930、CVE-2020-27932、CVE-2020-27950
- 影響產品/版本：iPhone 5s 與後續版本、iPod Touch 第六代與第七代、iPad Air、iPad mini 2 與後續版本、Apple Watch 所有版本。
- 解決方案：使用內建的軟體更新功能，更新至最新版本作業系統。

- 資料來源：
  1. https://support.apple.com/en-us/HT201222
  2. https://support.apple.com/en-us/HT211929
  3. https://thehackernews.com/2020/11/update-your-ios-devices-now-3-actively.html

2.5.6、視訊會議服務 Webex 漏洞，可能遭駭侵者潛入會議

廣為使用的 Cisco Webex 視訊會議服務，近來資安專家發現一個資安漏洞；駭侵者可利用此漏洞隱身於視訊會議之中，進而竊聽會議中的機敏資訊。

這個漏洞的編號為 CVE-2020-3419，由 IBM 旗下的資安研究專家發現。漏洞的成因在於 Webex 在處理認證 token 時的錯誤，駭侵者可以藉由特製的會議連線要求來誘發此漏洞。

利用此一漏洞進入視訊會議的駭侵者，將不會出現在視訊會議與會人清單之上，因此不但與會者無法發現，連視訊會議的發起人也無法把隱身的駭侵者移出。

Cisco 指出，雖然此一漏洞會讓駭侵者潛入會議而不被發現，然而駭侵者必須先擁有會議的加入連結與密碼，才能利用此漏洞發動攻擊；因此這個漏洞的 CVSS 危險程度評分僅達 6.5 分（滿分為 10 分）。

Cisco 也表示，由於這個漏洞係發生在該公司的雲端伺服器上，因此該公司可直接修補漏洞，Webex 用戶不需採取任何行動；該漏洞也已經在日前修補完成。

Cisco 說，目前還沒有觀察到這個漏洞遭到駭侵者大規模濫用的跡象，不過由於近日全球各地的疫情再度趨於嚴重，用戶對視訊會議的依賴程度將再度提高；資安專家呼籲各種視訊會議平台的用戶，都必須正視愈來愈高的駭

侵風險，提高警覺。

- CVE 編號：CVE-2020-3419
- 影響產品/版本：Cisco Webex 雲端服務（2020.11.17 前）
- 解決方案：雲端伺服器已更新，用戶無需採取任何行動

- 資料來源：
  1. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-auth-token-3vg57A5r
  2. https://securityintelligence.com/posts/ibm-works-with-cisco-exorcise-ghosts-webex-meetings/
  3. https://threatpost.com/cisco-webex-flaw-snooping/161355/

2.5.7、資安專家發現新方式，可在數分鐘內竊走 Tesla Model X

比利時 KU Leuven 大學的資安研究人員 Lennert Wouters，日前發表研究報告，指出 Tesla Model X 與其無線鑰匙的兩個資安漏洞，加以結合後，即可讓有心人士在數分鐘內竊走受害者的 Model X 電動車。

Lennert Wouters 指出，他發展出的攻擊竊車方式，是針對 Tesla Model X 無線鑰匙的安全漏洞；該無線鑰匙以低功率藍牙連線到汽車，且可以透過其藍牙連線更新無線鑰匙內晶片中執行的軟體；然而其更新機制並未受到足夠的保護。

Wouters 及其研究團隊找到的方法，是先利用修改過的 Model X ECU（電子控制單元）強制將無線鑰匙視為一般的可連線藍牙裝置，接下來利用其韌體更新機制，將含有惡意程式碼的韌體更新到無線鑰匙上，研究人員即可取得汽車和鑰匙之間溝通使用的加密資訊，並且開啟車門鎖。

解開車門鎖後，研究人員即可像汽車修護技師一樣，直接連線到 Model X 的診斷維護界面，將破解過後的車鑰與汽車進行配對，這樣就能開走 Model X。

研究人員指出，整個駭入 Model X 所需的工具，只需一組 ECU、一台

Raspberry Pi 微型電腦、一個無線車鑰、一台 CAN Shield 電路板，以及一顆電池；全部加起來不到 200 美元。

Tesla 於今年八月接獲研究人員通報後，已於新版 Tesla 軟體 2020.48 中修復這個漏洞，車主應在每次原廠推出無線軟體更新（Over-the-air）時盡速更新至最新版本，以防有人利用此漏洞竊走愛車。

- 影響產品/版本：Tesla Model X 軟體版本 2020.48 之前版本
- 解決方案：更新至 Tesla Model X 軟體版本 2020.48 與後續版本

- 資料來源：
  1. https://www.securityweek.com/researchers-show-tesla-model-x-can-be-stolen-minutes
  2. https://www.wired.com/story/tesla-model-x-hack-bluetooth/

第 3 章、 資安研討會及活動

Progress MOVEit 安全檔案分享與傳檔自動化 六大活用術	
活動時間	**12/16 14:35~15:15**
活動地點	**線上講座**
活動網站	**https://webinar.ithome.com.tw/**
活動概要	 **主辦單位：iThome** 數位轉型浪潮遠距辦公，對許多高科技產業或是金融業而言，資料檔案在各使用者、地點、合作夥伴以及客戶之間的移動過程至關重要，影響企業營運。然而，檔案傳輸需求卻會因為企業性質而有所不同，有的偶爾傳送普通資料即可，有時卻需要大量交換機密或管制資訊。如何在企業內部或是外部雲端安全的分享檔案，保護個資與公司重要數位資產，事關重大，不可輕忽。 Progress MOVEit 檔案傳輸管理（MFT）系統無論安全性、掌控能力還是自動化程度都更為優異，非常符合重要營運流程和法規上的要求。一般機構如果擔心和遠端機房、客戶、合作廠商、服務業者以及雲端應用程式交換檔案的安全問題，檔案傳輸管理（Managed File Transfe）產品的完整稽核功能就是最佳選擇。 本活動將告訴您 Progress MOVEit 檔案傳輸管理（MFT）六大活用術，解決您所有的安全檔案分享與自動化傳檔所遇到的問題，內容精采可期，名額有限，僅快報名喔!!

企業資安防護及案例分享研討會(台中場)	
活動時間	**12/18(五) 14:00-16:30**
活動地點	**經濟部加工出口區管理處臺中分處後棟 3 樓康樂室** **(臺中市潭子區建國路 1 號)**
活動網站	**https://docs.google.com/forms/d/e/1FAIpQLScjYXvEmzSWPmh0gCSeF2mXw_Quuqv46JHPeTLfDg3IgboyBg/viewform**
活動概要	 **主辦單位： TWNIC、TWCERT/CC** 2020 資安大調查-資訊安全最脆弱的環節居然是員工! 暨於現代網際網路的發展與依賴相對面臨到資訊安全的擔憂，從資安攻擊源頭來看，6 成資安事件的來源是駭客（60.3%），但也有 3 成多資安事件的觸發來源是內部員工（35.7%），近半數企業已經意識到員工資安知識可以大幅減低企業資安破口問題，54.7%企業每年資安演練至少 1 次，來強化員工意識。 本次活動將介紹台灣電腦網路危機處理暨協調中心(TWCERT/CC)之服務內容，希望企業能充分利用政府相關資源推動企業資安事件通報、產品資安漏洞通報、惡意檔案檢測服務等，另邀請中華電信林經理探討「企業因應勒索軟體的資安策略」，透過強健的員工資訊安全培訓，企業可以降低員工為駭客開啟大門的風險，提升企業資安意識。本活動名額有限，敬邀各單位與先進報名與會。 聯絡方式：04-2242-1717#242 黃小姐 eva@tcca.org.tw

WEA x BSI 資安風險趨勢講座	
活動時間	**12.28 (一) 13:30 ~ 16:30**
活動地點	**柯達大飯店 台北長安(台北市中山區松江路 61-1 號)**
活動網站	**https://www.wea4risk.com/index/apply.php**
活動概要	 **主辦單位：崴亞風險咨詢顧問股份有限公司** 在疫情衝擊、5G 時代來臨等情況下，企業不得不面臨數位轉型壓力。但轉型伴隨而來的許多新風險，包含跨國經營可能面對的歐洲 GDPR 法規、企業內部人員疏失、資安防護不周等。 「資安就是國安」更是台灣近年來推動的施政重點，而在這波浪潮中，企業該如何因應？ 數位方便了民眾的生活，也增加了企業對資安人才的需求，對於資安長（CSO、CISO）的需求更是與日俱增。有感於此，WEA 提早佈局決定開辦面向資安人員、資安主管的免費講座，提早展望高階管理層該具有的專業知識層級，了解企業培養資安長、資訊長的必備知識！ 為你的升職之路添磚加瓦。 適合對象：資安專業、管理人員、公司治理主管、各金融機構資安部門、對資安風險有興趣的各方專業人士 報名時間：~ 109.12.21 止

第 4 章、 2020 年 11 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。

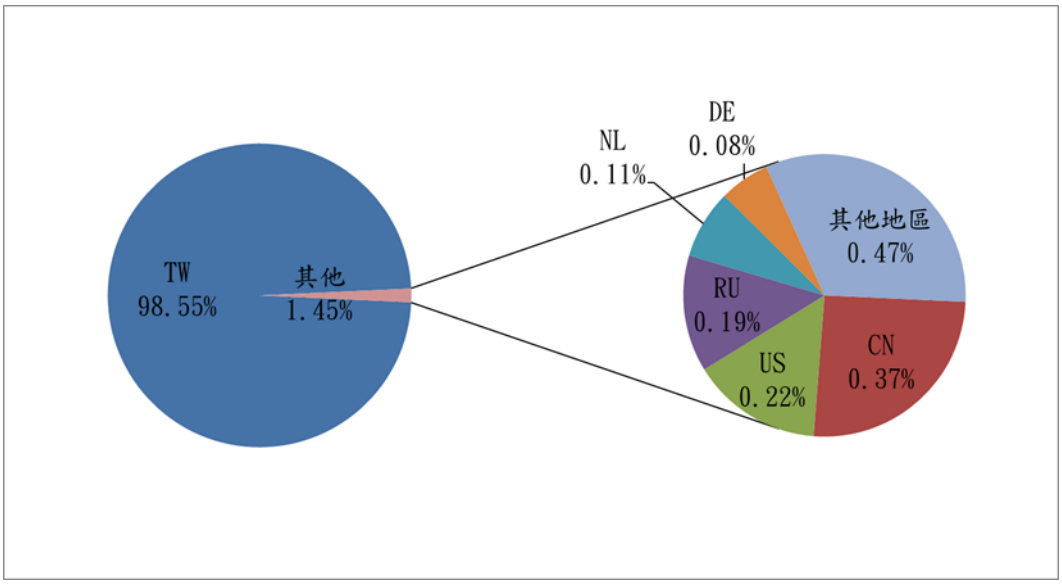

圖 1、分享地區統計圖

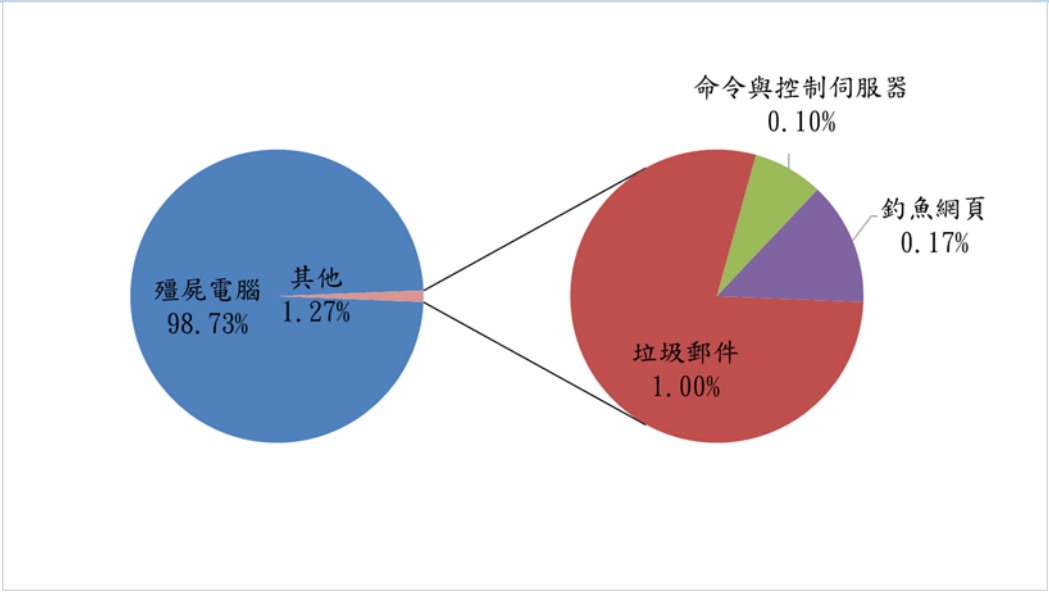

圖 2、分享類型統計圖

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 12 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**