TWCERT/CC 資安情資電子報

2020 年 10 月份

目錄

第 1 章、 封面故事

國內多家主機託管商遭疑似來自本土之 DVR 僵屍網路 DDoS 攻擊

國內多家知名主機託管廠商，近來連日遭到 DDoS 攻擊，許多託管網站因而連線受到影響。攻擊來源可能是來自國內大量遭駭入的 DVR 監控系統。

自九月下旬起，國內多家知名主機託管廠商，紛紛遭到來源不明的 DDoS 攻擊，造成眾多託管客戶的網站或部落格連線受到影響。

根據遭到攻擊的主機託管廠商公告，攻擊大量發生約在 9 月 20 日，一直到 9 月 22 日都沒有停止，因而造成許多託管於這些主機商的網站無法正常連線。

也有主機商在公告中指出，該公司遭到的 DDoS 攻擊，是以勒贖為目的而發動的，攻擊最大流量達到 15Gbps；目前有主機商已向 NCC 和調查局通報，並向刑事局報案。

另有主機商在其 Facebook 粉絲團中公告指出，該公司遭受的 DDoS 攻擊，根據 IP 分析，發現來源多半來自國內某家 DVR 廠商的監控產品；該公司認為很可能是這些 DVR 產品的 web 管理界面密碼過於簡單，用戶在使用時也沒有更換密碼，導致遭到駭侵者大規模入侵，並用以發動 DDoS 攻擊。

一些網管人員集中的討論區中，也提供了部分關於此次事件的相關研判與情報；有人分享可能是勒贖者的對話，要求受害者支付每月 100 美元的贖金，也有監控報告指出單一受駭 DVR 設備，同時對外連線數高達兩萬個以上，也有人提供了疑似用以發動攻擊的 IP 清單；但這些訊息都需要進一步查證。

建議所有使用各式 DVR 或 IoT 設備的用戶，一定要在啟用設備時，立即更改預設的管理界面登入帳密、隨時更新軟體或韌體；發現自己的網路有不正常的大量對外連線時，也要懷疑裝置是否遭到入侵，並即刻進行必要的離線或重置等手續。

- 資料來源：

1. https://host.com.tw/news/index/9 月 22 日 DDoS 攻擊狀況更新
2. https://hb.nss.com.tw/index.php?/news/view/1335/
3. https://www.facebook.com/pumonetwork/posts/4405247962850090

第 2 章、 國內外重要資安事件

2.1、資安趨勢

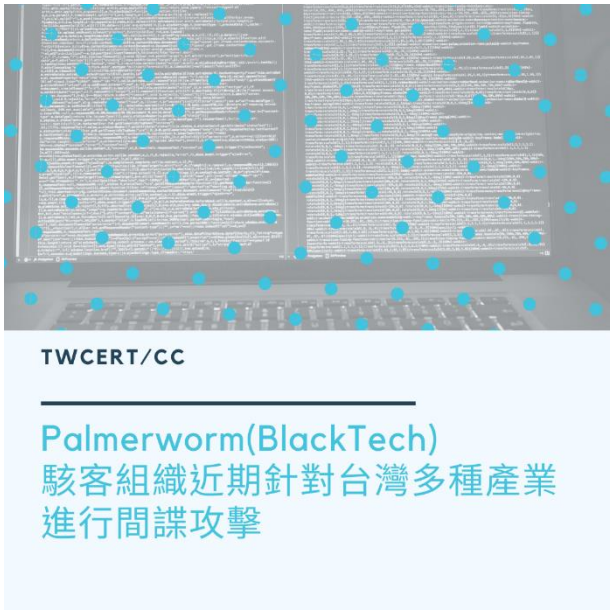
2.1.1、近日釣魚郵件資訊注意

TWCERT/CC 近日接獲多起釣魚信件通報，該信件標題採已匯款多少金額等引發收件者注意，並附上正確國內企業資訊之簽名檔等資訊，誘使使用者下載夾帶木馬病毒的附檔確認相關資訊。

經分析該惡意程式會紀錄鍵盤、麥克風及螢幕截圖並回傳至惡意中繼站。此惡意程式會偵測虛擬環境，若於虛擬環境則無動作進而躲避檢查。相關流程如圖示。據了解該釣魚郵件已行之有年，定期會寄送一波進行釣魚行動，請企業進行防範並同時向員工進行郵件的資安宣導避免誤載附檔，而受到監視，形成企業安全漏洞。

相關 IOC 資訊如欲索取，請用企業信箱寄信至 twcert@cert.org.tw 索取。

2.1.2、Palmerworm (BlackTech)駭客組織近期針對台灣多種產業進行間諜攻擊



TWCERT/CC 接獲國際情資，Palmerworm 駭客組織 (BlackTech)於 2019 年 8 月起，陸續利用新型客製化惡意程式，針對台灣建築、金融、電子與媒體業等諸多產業進行間諜攻擊。過去該駭客集團常用的惡意程式為 Backdoor.Kivars 和 Backdoor.Pled，但這次的攻擊採用新型的客製化惡意程式 Backdoor.Consock、Backdoor.Waship、Backdoor.Dalwit 和 Backdoor.Nomri，除了上述的四個後門外，亦會利用正常的軟體工具像是 Putty、PSExec、SNScan、WinRAR 進行攻擊行動；且會使用竊取的合法 code-signing 憑證來進行 payload 簽屬，藉以躲避安全軟體之偵測，請政府、企業單位注意並提供相關 IOC 資訊供防範。

相關 IOC 資訊如下：

DN
asiainfo.hpcloudnews.com
loop.microsoftmse.com

Hash
4c05ee584530fd9622b9e3be555c9132fad961848ea215ecb0dd9430df7e4ed8
50ba9a2235b9b67e16e6bd26ae042a958d065eb2c5273f07eee20ec86c58a653
5818bfe75d73a92eb775fae3b876086a9e70e1e677b7c162b49fb8c1cc996788
5a35672f293f8f586fa9cfac0b09c2c52a85d4e8bc77b1ed4d7c16c58fe97a81
69d60562a8d69500e8cb47a48293894385743716e2214fd4e81682ab6ed1c46b
6d40c289a154142cdd5298e345bcea30b13f26b9eddfe2d9634e71e1fb935fbe
6f97022782d63c6cea53ad151c5b7e764e62533d8257e439033c0307437bfb2a
73799d67d32a2b5554c39330e81e7c8069feaa56520e22a7fd0a52e8857c510c
81a4b84700b5f4770b11a5fe30a8df42e5579fd622fd54143b3d2578df4b559d
884cefccd5b3c3a219a176c0c614834b5b6676abbac1d1c98f39624fccc71bf9
8cd6dfffc251f9571f7a82cca2eca09914c950f3b96aaaeaeaaeeac342f9b550
8da532ea294cc2c99e02ce8513a15b108a7c49bd90f7001ce6148955304733cb
9c436db49b27bed20b42157b50d8bdad414b12f01e2127718250565017a08d84
9e3ecda0f8e23116e1e8f2853cf07837dd5bc0e2e4a70d927b37cfe4f6e69431
a7f3b8afb963528b4821b6151d259cf05ae970bc4400b805f7713bd8a0902a42
aa51b69d05741144d139b422c3b90fdf6d7d5a36dd6c7090c226a0fc155ada34
b32ab70f3f441a775771d6c824d4526715460c0fd72a1dfdec8cd531aef5fabd
d4d5c73c40f50cdef1500fca8329bc8f3f05f6e2ffda9c8feb9be1dcca6ccd31
eed2ab9f2c09e47c7689204ad7f91e5aef3cb25a41ea524004a48bb7dc59f969
f11e2146b4b7da69112f4681daca0c5ec18917acc4cf4f78d8bff7ac0b53e15c
f21601686a2af1a312e0f99effa2c2755f872b693534dbe14f034fa23587ac0b

IP
103.40.112.228
172.104.92.110
45.76.218.116
45.77.181.203

- 資料來源：

1. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt

2.1.3、Ubike 幾年前當機事件，提醒務必加強防護意識以確保資訊安全

在 2016 年，公共自行車 YouBike (簡稱 Ubike)租賃系統無預警當機，導致全台兩萬多輛的 Ubike 無法租借使用。

在 2016 年，公共自行車 YouBike (簡稱 Ubike)租賃系統無預警當機，導致全台兩萬多輛的 Ubike 無法租借使用。經追查後發現，該租賃系統是遭到惡意程式攻擊，而當年負責 Ubike 租賃系統承包商中一位工程師因此遭到逮補。然而，在 4 年(2020 年)後的現在，此案經由法院判決該工程師無罪，主要原因為該系統一直使用共用帳號密碼，逾十位的工程師都可自由登入及修改內容，再加上攻擊者登入的 Log 紀錄都已遭到刪除，導致整體案件無法證實攻擊者究竟是否為該工程師，因此判工程師無罪。

對企業而言，系統通常會提供給數位、甚至所有員工使用，而為了方便登入，許多企業會建立共用帳號，提供給所有使用者登入後使用。然而，由於共用帳號無法區隔每一位使用者的身分，一旦系統發生問題或感染惡意程式，往往也難以追查究竟為哪一位使用者所為，甚至許多共用帳號使用簡易的帳號和低強度的密碼，例如常見的 password123、123456 或企業名稱等容易猜測的密碼，因此一旦有攻擊者欲入侵該系統，可透過簡單的暴力破解取得其密碼後入侵其中。

雖然此次事件被認為是相關工程師所為，但許多系統對使用者不設置太多限制，導致使用者可隨意下載檔案或應用程式，甚至存取不屬於該使用者

的機敏資訊。如此低限制的做法，可能導致惡意程式透過下載的檔案入侵主機，或使用者將機敏資訊存儲於個人裝置後，遭攻擊者入侵後竊取，使得企業資訊外洩。這些行為並非使用者有意而為之，但仍造成企業產生嚴重損失，因此除了員工本身的惡意行為外，也有可能在無意間讓第三者進行惡意行為而不自知。故企業對於系統的登入、存取、修正、新增、刪除等權限，都應進行嚴格管控，避免產生資料外洩的風險。

為避免類似事件發生，建議企業應採以下措施：

1. 避免建立共用密碼，要求每個使用者必須透過個人帳號登入。
2. 對系統每一個帳號的密碼要求一定之強度，避免攻擊者以暴力破解方式取得密碼。
3. 企業系統應要求使用者定期更新密碼，且避免使用與前三次相同之密碼。
4. 系統應嚴格區分使用者身份及權限，以權限最小化原則設定。
5. 應控管使用者於系統中的動作，包括檔案或應用程式的下載、增修等行為，都應予以限制。
6. 對於系統所記錄的 Log，應限制僅有極少數管理者能進行檢閱，避免內部人員隨意變更。

- 資料來源：
  1. https://news.ltn.com.tw/news/society/breakingnews/1904832

2.1.4、FBI 警告：勒贖為目的之 DDoS（RDDoS）攻擊，正威脅全球企業與組織

美國聯邦調查局日前發表資安通報，指出以勒贖為目的的 DDoS 攻擊，不但愈來愈頻繁，而且已經鎖定全球數千家企業與組織。

美國聯邦調查局（FBI）發表資安通報 MU-000132-DD，指出以勒贖為目的的分散式服務阻斷攻擊（DDoS），不但發生次數愈來愈頻繁，而且已經鎖定全球數千家企業與組織，隨時可能展開攻擊行動。

這類結合勒贖與 DDoS 的駭侵攻擊行動，稱為 RDDoS 或 RDoS，最近成為各個著名 APT 駭侵團體的新攻擊樣態。例如 Facny Bear、Cozy Bear、Lazarus Group、Armada Collective 等大型駭侵團體，最近都曾發動 RDDoS 攻擊。

駭侵團體發動 RDDoS 攻擊前，會先要求目標企業支付 10 到 20 枚比特幣的贖金（約為台幣 332 萬元到 664 萬元之間）；如果企業不從，就會遭到每秒流量高達 2Tbps 的大規模 DDoS 攻擊，造成企業內外網路癱瘓。

據資安媒體 BleepingComputer 揭露的勒贖信內容，這些駭侵團體不只會要求被攻擊的企業支付贖金，也會要求企業不得聲張；駭侵信中也威脅受害者若不支付贖金，遭到 DDoS 攻擊導致服務停擺後，將對該企業的信譽與形象造成嚴重傷害。

有時這些駭侵團體也會先以小規模 DDoS 攻擊，恫嚇受害企業支付贖金；資料中心業者 Akamai 指出這類小型攻擊的流量規模約在 200Gbps 左右；採用的攻擊手法相當多樣，包括 ARMS、DNS 洪水攻擊、GRE 協定洪水攻擊、SNMP 洪水攻擊、WSDIscovery 洪水攻擊等。

- 資料來源：
  1. https://www.documentcloud.org/documents/7070798-FLASH-MU-000132-DD.html
  2. https://www.bleepingcomputer.com/news/security/fbi-thousands-of-orgs-targeted-by-rdos-extortion-campaign/
  3. https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html

2.2、國際政府組織資安資訊

2.2.1、美國發出通報，指中國軍方旗下駭侵團體針對美國政府單位發動駭侵攻擊

美國資安與基礎建設安全局日前發表資安通報，指出中國軍方旗下駭侵團體，已針對美國政府單位發動駭侵攻擊；該資安通報也針對這些駭侵團體的常見攻擊手法提出分析。

隸屬美國國土安全部的資安與基礎建設安全局（Cyberserurity and Infrastructure Security Agency）日前發表資安通報 AA20-258A；報告指出中國軍方旗下多個駭侵團體，已針對美國政府單位發動駭侵攻擊；該資安通報也針對這些駭侵團體的常見攻擊手法提出分析。

報告說，中國軍方相關的駭侵組織，長年以使用各種公開資訊計畫並執行各種攻擊活動，而且有能力針對目標單位的內部網路快速發動攻擊。

CISA 長期以來透過美國國家資安保護計畫（National Cybersecurity Protection System）監控中國軍方相關駭侵團體的活動，發現這些團體鎖定包括美國政府機關、高科技製造業、醫療器材產業、土木工程、一般企業、教育、遊戲軟體、國防工業等進行駭侵活動長達十年。

CISA 利用 MITRE ATT&CK 分析架構，收集並分析中國軍方相關駭侵團體的活動，發現過去 12 個月以來，這些團體經常利用以下漏洞發動攻擊：

- CVE-2020-5902：F5 Big-IP 漏洞，可用以執行任意程式碼，並且隨意增刪、修改檔案內容；

- CVE-2019-19781：Citrix VPN 設備漏洞，可用於進行目錄遍歷攻擊（directory traversal attack）；
- CVE-2019-11510：Pulse 安全 VPN 伺服器漏洞：可讓攻擊者讀取任意檔案內容；
- CVE-2020-0688：Microsoft Exchange Server 漏洞，可用以遠端執行任意程式碼，並且竊取單位內部郵件。

CISA 和 FBI 建議所有可能受中國軍方相關駭侵攻擊的單位，均應提高警覺，除了立即修補以上常遭攻擊的漏洞外，也定期檢查設備與軟體的備置設定，確保定期更新且能抵禦外部攻擊，以提高駭侵攻擊得逞的難度並減輕損失。

- 資料來源：
  1. https://us-cert.cisa.gov/ncas/alerts/aa20-258a
  2. https://us-cert.cisa.gov/ncas/alerts/aa20-133a

2.2.2、美國政府所屬機構遭駭侵者利用已知 VPN 漏洞發動攻擊

美國資安主管機關日前發表資安通報，指出美國政府旗下某單位遭駭侵成功，內部資料可能也遭外洩。

美國資安主管機關「資安與基礎建設安全局」（Cybersecurity and Infrastructure Security Agency, CISA）日前發表資安通報，指出美國政府旗下某單位遭駭侵成功，且內部資料可能已經外洩。

CISA 於 9/24 發表該資安通報（AR20-268A）。通報中指出駭侵者成功取得該單位多名雇員的 Office 365 登入資訊，甚至包括網域管理員的登入資訊在內；並且使用該單位的私有 VPN 進行遠端登入，同時下載檔案。

CISA 指出，駭侵者可能是透過 Pulse Secure VPN 的已知漏洞 CVE-2019-11510 入侵該單位並取得單位雇員的登入資訊。該漏洞的修補程式，早在 2019 年四月便已釋出，美國國土安全部更在稍早針對此漏洞發表資安通報，要求美國政府各單位提高警覺並儘速修補；但 CISA 仍觀察到多起利用此漏洞針對美國政府各單位發動駭侵攻擊的案例。

CISA 在通報中指出，駭侵者先以某雇員的 Office 365 帳號，向該單位的 IT 支援系統取得 VPN 的連線方式與使用密碼，然後再查出其內網 Active Directory 與群組原則金鑰，之後再利用一些常用的 Windows 指令連上 VPS，

並連上控制伺器，下載並在內網中執行惡意軟體。

- 資料來源：
  1. https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a
  2. https://www.tenable.com/blog/cve-2019-11510-critical-pulse-connect-secure-vulnerability-used-in-sodinokibi-ransomware
  3. https://threatpost.com/feds-cyberattack-data-stolen/159541/

2.2.3、美國發布通報，要求大選相關單位嚴防透過 Email 進行的駭侵攻擊

主管美國資安事務的資安暨基礎建設安全局（CISA），日前發表資安通報，警告和即將舉行的美國總統大選活動有關的各單位，均應嚴防透過 Email 進行的駭侵攻擊。

主管美國資安事務的資安暨基礎建設安全局（Cybersecurity & Infrastructure Security Agency, CISA），日前發表資安通報，警告和即將舉行的美國總統大選活動有關的各單位，均應嚴防透過 Email 進行的各式駭侵攻擊。

CISA 在通報中指出，與大選相關的各種單位，包括政黨、競選活動、智庫、公民團體和相關個人等，過去一直都是駭侵團體鎖定的對象；最近的研究報告顯示，有 32% 的駭侵事件始於釣魚郵件攻擊，更有 78% 的間諜資料竊取透過釣魚攻擊展開。

CISA 要求使用雲端 Email 服務的個人或團體，必須使用由服務提供者指定的各種保護措施，包括：

○ 所有的郵件帳號均須設定多次登入認證，包括使用符合 FIDO2 標準的硬體隨機密碼產生器、使用 TOTP 演算法的軟體隨機密碼產生 App 等。

○ 除非只有簡訊或 EMail 驗證方式可用，否則儘可能不要使用簡訊或 Email 傳送的登入驗證碼，因為很容易在中途遭到攔截。

○ 最好將所有 Email 用戶升級到更進階的帳號防護方案；包括 Google、Microsoft 等雲端服務大廠，均提供這類服務。

另外，針對身分地位較敏感的個人，或是保護程度要求較高的重要單位，CISA 也要求採行以下方式保護其資安：

● 採用密碼管理工具，並要求所有組織成員使用；因為密碼管理工具在遇到詐騙網站時，不會自動輸入帳密。

● 減少要求用戶更換密碼，也不要規定太複雜的密碼規則：最近的研究指出，太複雜的密碼規則要求與過度頻繁的密碼更換規定，會提升用戶的使用困難，反而降低保護程度；可以依據美國國家標準局提出的規範，以長但是好記的密碼、多詞組成的密碼為原則。

- 資料來源：
  1. https://www.cisa.gov/sites/default/files/publications/CISA_Insights_Actions_to_Counter_Email-Based_Attacks_on_Election-Related_S508C.pdf
  2. https://pages.nist.gov/800-63-3/sp800-63b.html#memsecretver
  3. https://www.tripwire.com/state-of-security/security-data-protection/cisa-warns-election-related-entities-to-be-on-watch-for-phishing-attacks/。

2.2.4、紐西蘭證交所連四天遭 DDoS 攻擊，當局展開調查

紐西蘭證交所連續四天遭境外 DDoS 攻擊，造成股市交易嚴重受阻；紐西蘭當局認為情形嚴重，已訓令該國資安與情治單位展開調查行動。

自 8 月 25 日起，紐西蘭證交所已經連續四天遭境外 DDoS 攻擊，造成股市交易嚴重受阻；紐西蘭當局認為情形嚴重，已訓令該國資安與情治單位立即展開調查行動。

紐西蘭證交所自 8 月 25 日起，每天都遭到來自不明境外駭侵攻擊；攻擊者以分散式服務阻斷攻擊（Distributed Denial of Service，DDoS），造成證交所官網與交易系統癱瘓而無法運作。

8 月 28 日的攻擊是連續第四天發生，造成紐西蘭股市無法準時於上午十時開始交易；整個交易開始時間延後了三個小時，一直到下午一點才開盤。

紐西蘭財政部和政府通訊安全局（Government Comunications Security Bureau）已針對本案，會同紐西蘭情治單位成立專案小組，對本案進行調查。紐國財政府長 Grant Robertson 說，基於調查所需，無法透露詳細調查細節，但紐國政府認為這一系列駭侵攻擊行為十分嚴重。

紐西蘭與美國、英國、加拿大、澳大利亞等英語系國家，同為情報交換組織「五眼聯盟」的一員，另外紐西蘭也在去年與其他 27 個國家簽署資安情報共享互助協定，以聯合對抗俄羅斯、北韓與中國等國的駭侵攻擊威脅。

- 資料來源：
  1. https://finance.yahoo.com/news/cyber-attacks-halt-zealand-stock-223847466.html
  2. https://edition.cnn.com/2020/08/27/investing/new-zealand-stock-exchange-cyber-attack/index.html
  3. https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/

2.3、行動裝置資安訊息

2.3.1、Google Play Store 移除 17 個內含 Joker 惡意軟體的 App

Google Play Store 日前移除多達 17 支內含惡意軟體 Joker 的 App，下載次數總和高達 120,000 次。

Google Play Store 日前移除多達 17 支內含惡意軟體 Joker 的 App，這 17 支 App 的下載次數總和高達 120,000 次，內含的 Joker 惡意程式除了會竊取用戶機敏資訊外，更會擅自幫訂戶訂閱多種要價昂貴的線上服務。

資安廠商 ZScaler 於 9 月 24 日發表研究報告，指出有 17 支 Google Play Store 中的熱門軟體，內部含有變種的 Joker 惡意軟體；一旦用戶安裝這些 App，Joker 就會竊取手機中的簡訊內容、通訊錄、手機軟硬體資訊等機敏資料，更會擅自為用戶訂閱高價的線上服務，造成用戶通訊費用帳單金額暴增。

Google 除了在 Play Store 中下架這些惡意軟體 App 外，也透過機制，讓已安裝在用戶手機上的這些 App 無法啟動；但用戶仍需在自己的手機上手動移除這些 App。

這 17 支 App 如下：

- All Good PDF Scanner
- Mint Leaf Message-Your Private Message

- Unique Keyboard - Fancy Fonts and Free Emoticons
- Tangram App Lock
- Direct Messenger
- Private SMS
- One Sentence Translator - Multifunctional Translator
- Style Photo Collage
- Meticulous Scanner
- Desire Translate
- Talent Photo Editor - Blur focus
- Care Message
- Part Message
- Paper Doc Scanner
- Blue Scanner
- Hummingbird PDF Converter - Photo to PDF
- All Good PDF Scanner

這已是 Google 近半年來第三次大規模自 Play Store 中下架內含 Joker 惡意軟體的 App；先前在七月和九月初也有多個內含 Joker 惡意軟體的 App 遭下架。這些 App 在上架時都是不含惡意程式碼的，直到用戶下載並使用一段時間後，才將惡意程式碼下載安裝進 App 中，因此往往能躲過 Play Store 的偵測機制。

- 資料來源：
  1. https://www.zscaler.com/blogs/security-research/joker-playing-hide-and-seek-google-play
  2. https://www.zdnet.com/article/google-removes-17-android-apps-doing-wap-billing-fraud-from-the-play-store/
  3. https://arstechnica.com/information-technology/2020/09/joker-the-malware-that-signs-you-up-for-pricey-services-floods-android-markets/

2.3.2、哥倫比亞大學研究：多個熱門 Android App 未遵守基本資料加密原則

哥倫比亞大學的一組資安研究團隊指出，該團隊分析了 1,780 個不同的 Android 熱門行動應用程式，發現其中多個 App 並未遵守一些最基本的資料加密原則，而且未修復。

哥倫比亞大學的一組資安研究團隊，近日在 IEEE 計算計科學會刊上發表研究報告，指出該團隊利用自行開發的分析工具，分析了 1,780 個不同的 Android 熱門行動應用程式，發現其中多個 App 並未遵守一些最基本的資料加密原則，而且從未修復。

該團隊開發的分析工具稱為 CRYLOGGER，會檢查 26 種基本的資料加密原則；在該工具分析的 1,780 個 Android 熱門 App 中，有 1,775 個使用不安全的 PRNG 亂數產生器；1,764 個使用了較弱的雜湊演算法（如 SHA1、MD2、MD5 等）；另外有 1,076 個 App 使用較弱的區塊加密法工作模式。

研究報告指出，大多數受檢的 Android App 都沒有遵守這 26 種最基本的資料加密原則，而被點名的 306 個 App 的情況尤其嚴重到已經成為資安漏洞等級。

這批 306 個 App 均屬 Google Play Store 上的熱門 App，下載安裝次數由數十萬次到超過一億次不等。研究團隊向這 306 個熱門 App 的開發者發出資安通報，說明檢測出的問題；但只有 18 個開發者回覆，其中有 8 個開發者後續與研究團隊進行連繫。

研究團隊也說，有部分加密問題是來自 App 程式碼呼叫的 Java 程式庫；該團隊也向其中六個熱門程式庫的開發者發出通報。

- 資料來源：
  1. https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/1mbmHwIxTb2/pdf
  2. https://www.zdnet.com/article/academics-find-crypto-bugs-in-306-popular-android-apps-none-get-patched/

2.4、軟體系統資安議題

2.4.1、美國網路行銷業者洩露近 3,900 萬筆美國人個資記錄

資安媒體研究團隊發現一家美國網路行銷公司，有一個內含 3,900 萬筆美國人客戶資料的資料庫外洩。

資安媒體 Cybernews 的研究團隊，日前發現一家美國網路行銷公司 Voew Media，有一個內含 3,900 萬筆美國人客戶資料的資料庫發生外洩事件。

這個龐大的資料庫被放置在 Amazon Web Services 雲端伺服器上，未加任何保護，所以只要知道資料庫網址的人，即可存取並下載所有資料。

這個資料庫中共有 5,302 個檔案，內含 700 個用來進行精準行銷的 PDF 文件檔，以及 59 個 CSV 與 XLS 檔案；這 59 個資料檔中內含美國國內客戶的近 3,900 萬筆資料，而有 2,351 餘萬筆資料是不重覆的個資。其他檔案大多都是用以進行行銷活動的素材或製作物檔案。

這些個資的欄位，則包括用戶的全名、Email 地址、實體地址、電話號碼與郵遞區號；資料收集期間則在 2018 到 2019 年間，算是相當新的資料。

Cybernews 在發現這個大型資料庫後，已於七月底進行通報；Amazon 隨即關閉了這個資料庫的存取權限，目前已經無法自由存取這個資料庫。

這次洩露事件是 Cybernews 在今年夏季發現的第二件；在八月初 Cybernews 也曾揭露另一起資料庫外洩事件，當時有個資料庫，內含近三億五千萬個不重覆的 Email 地址，同樣未經保護，被置於 Amazon Web Services 伺服器上，存取不受任何限制。

- 資料來源：
  1. https://cybernews.com/security/online-marketing-company-exposes-data-of-millions-americans/
  2. https://cybernews.com/security/350-million-email-addresses-left-exposed-on-an-unsecured-server/

2.4.2、華納音樂集團旗下多個線上商店遭駭，用戶資料恐遭竊

華納音樂集團所屬的多個位於美國的線上商店，今年四月開始遭到駭侵攻擊，顧客個資可能已遭駭侵者竊得。

全球第三大音樂品牌華納音樂集團，旗下所屬的多個位於美國的線上商店，於今年四月起遭到多波駭侵攻擊；華納音樂近日發表聲明證實遭駭，並指出其顧客個資可能已遭駭侵者竊得。

華納音樂集團日前對可能遭駭的顧客發出資安通報，指出該公司旗下有多個託管於第三方電商開店服務的網路商店，從今年 4 月 25 日到 8 月 5 日之間，遭到多次未經授權的存取；顧客在網站上填寫的各項資料可能已經遭到駭侵者不法取得。

華納音樂說，可能遭竊的用戶個資項目，包括姓名、Email 地址、電話號碼、帳單寄送地址、送資地址、信用卡或金融卡的卡號、到期日與安全碼等；但影響僅限直接刷卡消費的顧客，透過 PayPal 消費的用戶不受影響。

華納表示，將會免費提供個資可能遭竊的顧客為期一年的免費卡片異常交易監控服務；顧客如果發現信用卡或金融卡出現不明交易或盜刷，就會收到警訊，應即刻向發卡單位通報，避免進一步的損失。

目前華納音樂已開始進行調查，暫時沒有發現外洩資料遭濫用的情形，但用戶仍應提高警覺，注意自己的信用卡是否出現異常交易。

資安專家指出，儘管華納音樂沒有透露這幾波攻擊的技術細節，但以目前資訊研判，很可能是遭到典型的 MageCart 攻擊；駭侵者在電商平台的結帳頁面植入惡意程式碼，用以竊取交易過程中用戶輸入的各種資訊。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/warner-music-group-finds-hackers-compromised-its-online-stores/
  2. https://www.documentcloud.org/documents/7201631-Warner-Music-Group-Breach-Letter-BC.html

2.4.3、微軟推出九月 Patch Tuesday 每月資安修補包，修復 129 個資安漏洞

微軟推出九月例行資安修補包，此次一共修復 129 個資安漏洞；建議微軟各產品用戶都能儘速安裝更新，以降低資安風險。

微軟於 9 月 8 日推出九月份例行資安修補包 Patch Tuesday；此次一共修復 129 個已知資安漏洞；其中有 23 個屬於危險程度較高的資安漏洞，105 個屬於重要等級的資安漏洞。

這 129 個漏洞分別屬於 Microsoft Windows、Edge（舊版與以 Chromium 為基礎的新版）、ChakraCore、Internet Explorer、SQL Server、Office 相關產品、Visual Studio、Exchange Server、ASP.NET、OneDrive 與 Azure DevOps 等。

其中比較重要，資安危害程度較高的漏洞更新如下：

CVE-2020-16875：這個漏洞是本月修補包中最為嚴重的漏洞，CVSS 嚴重程度評分高達 8.4 分；該漏洞發生原因為 Microsoft Exchange Server 的記憶體崩潰錯誤，駭侵者可以利用特製的 Email 信件，透過此漏洞遠端執行任意程式碼；任何使用 Exchange Server 的用戶，應即刻修補此一漏洞。

CVE-2020-1129：這個漏洞發生在 Windows Codec 程式庫，駭侵者可利用特製的影像檔，透過這個漏洞遠端執行任意程式碼。

CVE-2020-0922：這個漏洞發生在 Microsoft COM for Windows，駭侵者可將受害者導向含有特製 Javascript 程式碼的惡意網站，入侵用戶系統並遠端執行任意程式碼。

在九月的 Patch Tuesday 發表後，2020 年已得到修補的微軟產品各項資安漏洞，總數已經破千；建議微軟各產品用戶都能儘速安裝更新每月資安修補包，以降低資安風險。

- 資料來源：
  1. https://www.thezdi.com/blog/2020/9/8/the-september-2020-security-update-review
  2. https://krebsonsecurity.com/2020/09/microsoft-patch-tuesday-sept-2020-edition/
  3. https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Sep

2.4.4、特斯拉證實，俄籍駭客試圖買通員工植入惡意軟體

特斯拉對外證實，日前遭到逮捕的俄羅斯駭客，試圖買通該公司員工，在系統中植入惡意軟體，以竊取公司機敏資訊。

全球電動車龍頭大廠特斯拉對外證實，遭到美國司法部逮捕的俄羅斯駭客，試圖重金買通公司員工，以便在特斯拉汽車工廠的電腦系統中植入惡意軟體，竊取該公司機敏資訊。

遭到逮捕的俄羅斯籍駭客為 Egor Igorevich Kriuchkov，年僅 27 歲。美國情治單位認為他屬於一個大型犯罪集團，試圖以惡意軟體收集特斯拉等大型製造業者的各種機敏資訊，包括產品設計資料等，藉以勒贖高額金錢。

據報導指出，Kriuchkov 於 2020 年 7 月中透過 WhatsApp 與特斯拉內華達工廠的俄裔員工，以高達五十萬美元的重金，要求該員工在特斯拉公司系統中安裝惡意軟體，以便進行 DDoS 攻擊。

該名特斯拉員工立即秘密向特斯拉與 FBI 提出檢舉，FBI 便開始追蹤 Kriuchkov，並透過該名特斯拉員工與 Kriuchkov 談判並拖延時間，以獲取更多關於該犯罪組織的情報；期間 Kriuchkov 表示該組織曾成功買通其他兩家大廠員工，獲取的贖金高達四百萬美元。

特斯拉員工在與 Kriuchkov 談判過程中，一度將佣金提高到一百萬美元，但在 2020 年 8 月 21 日時，Kriuchkov 表示要暫停此計畫，因為該組織正

在全力攻擊另一家公司，需要集中資源；最後 FBI 決定收網，於 2020 年 8 月 22 日在洛杉磯成功逮捕 Kriuchkov 歸案，而特斯拉則在稍後證實該事件。

- 建議採取資安強化措施

1、 建議企業定期將重要資料及系統進行備份，藉由備份於不同儲存媒體、異地備援等方式，降低遭受資安事件之風險。

2、 建議加強員工資安意識，遇到可疑的事件或不明來源的電子郵件時務必進行通報，並落實對員工之資安宣導，定期進行社交工程演練。

3、 建議企業將內部網路進行分段隔離，避免橫向感染其他主機與系統，並進行使用者權限控管，依業務需求分割網路，以減少遭受資安攻擊之損害。

- 資料來源：

1. http://www.documentcloud.org/documents/7044253-Egor-Igorevich-Kriuchkov-criminal-complaint.html
2. https://www.zdnet.com/article/russian-arrested-for-trying-to-recruit-an-insider-and-hack-a-nevada-company/
3. https://www.zdnet.com/article/elon-musk-confirms-russian-hacking-plot-targeted-tesla-factory/

2.4.5、多家俄國企業遭到 OldGremlin 鎖定發動勒贖攻擊

資安廠商觀測指出，一個全新的駭侵團體 OldGremlin 開始針對俄國企業，發動勒贖駭侵攻擊，受害者包括金融服務業、製造業和醫療保健業等。

資安廠商 Group-IB 發表研究報告指出，一個全新的駭侵團體 OldGremlin，近來開始針對俄國企業，發動勒贖駭侵攻擊；受害者包括金融服務業、製造業和醫療保健業等。

這個名為 OldGremlin 的全新駭侵團體，典型的攻擊手法是透透 Email 發動魚叉式釣魚攻擊，以和肺炎疫情或媒體採訪邀請有關的主題，誘使受害者開啟含有惡意程式碼或連結的信件，再以自製的 TinyPosh 和 TinyNode 後門程式進行駭侵攻擊。

研究人員發現 OldGremlin 自今年七月起發動第一次攻擊動，對某家俄國醫療業者發動勒贖攻擊，該公司內部網路的資料全遭加密；駭侵者要求五萬美元贖金以解鎖檔案。

到目前為止，Group-IB 至少觀察到 OldGremlin 發動七次釣魚攻擊；該團體時而假冒為自治團體、俄國冶金公司、白俄羅斯曳引機工廠、牙醫診所、媒體等不同身分，向目標發送主題諸如「即將到期帳單」之類的郵件，並夾帶含有 TinyPosh 或 TinyNode 惡意軟體的檔案。

Group-IB 指出，該團體使用的惡意軟體開始執行後的 20 秒左右，就會觸發 Windows Defender 的反應，並且自動刪除惡意軟體；但這 20 秒已經足夠讓惡意程式碼常駐在系統中，並且下載其他惡意軟體，用戶反而因為這樣而不會意識到電腦遭駭。

- 資料來源：
  1. https://www.group-ib.com/blog/oldgremlin
  2. https://threatpost.com/oldgremlin-russian-ransomware/159479/

2.4.6、智利大型銀行遭勒贖攻擊，所有分行均無法正常營業

一家智利大型銀行於 9 月 7 日遭到勒贖攻擊，導致全國各地分行均無法正常營業。

一家智利大型銀行 Banco Estado 於 9 月第一周的周末遭到猛烈的勒贖駭侵攻擊，導致該銀行在智利全國各地的分行，在 9 月 7 日周一開市時均無法正常營業。

Banco Estado 是智利最大的三家銀行之一，也是唯一的公營銀行。該行於 9 月 7 日緊急發布資安通報，表示該行於周末遭到駭侵攻擊，被迫於周一關閉所有分行。

據了解，由於該行員工開啟的 Email 中含有惡意程式碼的 Office 夾檔，導致銀行的內部網路遭到入侵；調查人員認為駭侵者在上周末透過惡意程式碼開啟的後門，在 Banco Estado 的內部網路中執行了勒贖軟體。

資安媒體 ZDNet 獲得的情報指出，造成 Banco Estado 駭侵事件的勒贖軟體，稱為 REvil，又名 Sodinokibi 或 Sodin，會加密系統內的所有檔案，但不會將這些檔案全部清除。

在 Banco Estado 向智利警方提出資安通報案件後，智利政府隨即對全國各公私營單位發布警訊，警告可能遭到大規模的勒贖攻擊，要各單位提高警覺。

在損害方面，由於 Banco Estado 很快就採取了妥善的斷網隔離措施，因此僅有部分檔案遭到加密；用戶存款目前也沒有受到影響。該銀行的官網、ATM、手機 App 目前仍可正常操作，未受波及。

- 資料來源：
  1. https://twitter.com/BancoEstado/status/1302941450695573504/photo/1
  2. https://www.zdnet.com/article/chilean-bank-shuts-down-all-branches-following-ransomware-attack/
  3. https://cointelegraph.com/news/major-chilean-bank-shuts-down-all-branches-following-ransomware-attack

2.4.7、德國醫院遭勒贖攻擊，導致重症病人無法就近接受急診

德國杜塞道夫大學醫院於 9 月 10 日遭勒贖攻擊，導致醫院部份設備停擺，急症服務也無法正常運作；一名重症病患被迫轉至較遠的其他醫院，不幸因就診延誤而過世。

德國杜塞道夫大學醫院於 9 月 10 日遭勒贖攻擊，導致醫院部份設備停擺，急症服務也無法正常運作；一名重症病患被迫轉至 32 公里之外的其他醫院，不幸因就診延誤一小時以上而過世。

根據德國主管資安事務的聯邦資訊科技安全局（Bundesamt für Sicherheit in der Informationstechnik，BSI）指出，杜塞道夫大學醫院係遭駭侵者利用 Citrix VPN 裝置的已知漏洞 CVE-2019-19781 進行攻擊，侵入其內部網路，造成該院多項醫療服務無法正常運作。

CVE-2019-19781 是在去年（2019）十二月時發現的漏洞，在今年一月時提供資安修補程式，BSI 也曾在當時發布資安通報，要求使用 Citrix VPN 設備的德國各公私單位立即更新；然而包括受害的杜塞道夫醫院許多單位，並未按照公告要求即時更新，導致今日的悲劇。

BSI 指出，德國聯邦政府準備通過新法，要求政府撥付給醫療院所的預算中，至少要有 15% 以上用於改善資安防護能力。

德國媒體報導說，在駭侵者留下的勒贖訊息中，被勒贖的對象並非杜塞道夫大學醫院，而是海因里希．海涅大學；警方告知駭侵者，其攻擊對象是

醫院，且已造成不幸之後，駭侵者隨即撤回勒贖要求，並且提供解鎖密鑰。

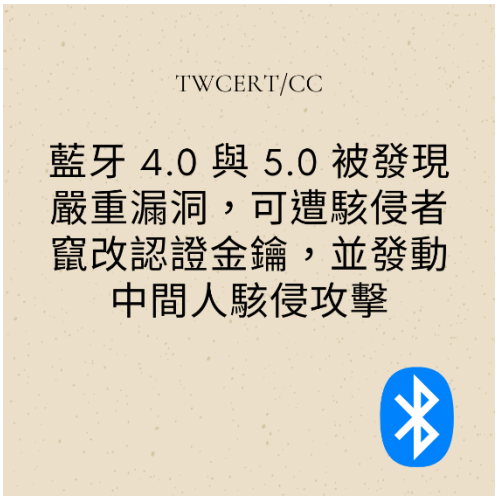
杜塞道夫大學醫院取得解鎖密鑰後，目前各系統的運作已逐漸恢復正常；調查後也發現並未外洩任何資料。

資安媒體 BleepingComputer 試圖連絡各駭侵團體，多數駭侵團體都表示不會攻擊醫院；如果發生誤攻擊事件，也會立即免費提供解鎖金鑰；但各醫療院所遭到勒贖駭侵的事件，仍在不斷發生之中。

- 資料來源：
  1. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html
  2. https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/krankenhaus-derzeit-nur-sehr-eingeschraenkt-erreichbar-patientenversorgung-eingeschraenkt
  3. https://www.n-tv.de/panorama/IT-Ausfall-in-Duesseldorf-war-Hackerangriff-article22042665.html
  4. https://www.bleepingcomputer.com/news/security/ransomware-attack-at-german-hospital-leads-to-death-of-patient/

2.5、軟硬體漏洞資訊

2.5.1、藍牙 4.0 與 5.0 被發現嚴重漏洞



藍牙 4.0 與 5.0 被發現嚴重漏洞，可遭駭侵者竄改認證金鑰，並發動中間人駭侵攻擊。

推動藍牙無線通訊技術發展的 Bluetooth Special Interest Group（SIG）與卡內基美隆大學資安事件通報處理中心，日前聯合發布資安通報，指出一個存在於 Bluetooth 4.0 與 5.0 版本的資安漏洞，將可導致駭侵者竊改藍牙裝置配對時使用的認證金鑰，並且強迫使用較弱的加密傳輸協定。

這個漏洞被稱為「BLURtooth」，存在於藍牙通訊協定中的「跨傳輸埠金鑰產生」(Cross-Transport Key Derivation, CTKD)，是兩個藍牙裝置進行配對時產生加密金鑰並相互認證時進行的程序；駭侵者可利用 CTKD 的漏洞，竄改其中一台配對裝置的加密金鑰，讓駭侵者持有的藍牙裝置可與對象裝置連線，藉以進行中間人攻擊。

SIG 說，這個漏洞是由瑞士洛桑聯邦理工學院與美國普度大學的資安研究團隊各自獨立發現。

據 SIG 指出，所有支援藍牙 4.0 和 5.0 的裝置，都存有此一漏洞；支援藍牙 5.1 的裝置，則可啟用某些防護功能，因此可以避開 BLURtooth 攻擊。

SIG 表示，目前暫時無法針對既有的藍牙產品提供修補程式；用戶必須主動提防來自不明裝置的藍牙配對要求，只和自己信任的裝置進行配對連線。未來當這些裝置得到軟體或韌體更新時，視原廠安排將會修補這個漏洞。

- CVE 編號：CVE-2020-15802
- 影響產品/版本：所有支援藍牙 4.0 和 5.0 的裝置
- 解決方案：待原廠推出軟體或韌體更新

- 資料來源：
  1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15802
  2. https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/bluetooth-security/blurtooth/
  3. https://kb.cert.org/vuls/id/589825
  4. https://www.zdnet.com/article/blurtooth-vulnerability-lets-attackers-overwrite-bluetooth-authentication-keys/

2.5.2、藍牙協定再次遭發現嚴重資安漏洞 BLESA，數十億台低功率藍牙裝置曝險

廣為全球數十億台裝置使用的藍牙通訊協定，再遭發現嚴重資安漏洞，而且難以全面修補。

這個漏洞稱為 BLESA（Bluetooth Low Energy Spoofing Attack），顧名思義，發生在低功率藍牙通訊協定上；該漏洞存在於低功率藍牙裝置配對後重新連接的過程。

發現這個漏洞的美國普渡大學資安研究團隊指出，在兩台低功率藍牙設備完成配對，常因距離過遠而暫時失去連線；在距離再次接近後的重新連線過程中，理論上應該再次檢查並確認兩者的加密金鑰與先前配對時一致，接下來才能恢復連線並開始傳輸資料。

研究團隊指出，在低功率藍牙的官方規格中，重新連線的標準中並不包括足夠安全的確認機制；首先，在重新連線時，再次驗證金鑰正確性的流程是非必要的，可以跳過；再者也有方法可以規避金鑰再次驗證的過程；這就是 BLESA 的攻擊破口。

攻擊者可以利用 DoS 攻擊迫使目標裝置的藍牙連線中斷，並啟動重新連線機制，並在重新連線時發動 BLESA 攻擊。

BLESA 攻擊主要透過軟體堆疊來進行，據普渡大學研究團隊的報告，多個作業系統平台的藍牙堆疊程式庫都無法抵擋 BLESA 攻擊，包括 Linux 使用的 BlueZ、Android 使用的 Fluoride 與 iOS 的 BLE 堆疊；但是 BLESA 攻擊對

Windows 使用的 BLE 堆疊是無效的。

報告指出，Apple 已經在今年六月提報這個漏洞（編號為 CVE-2020-9770），並且已於六月修復；但在研究團隊測試的 Android 裝置（例如執行 Android 10 的 Google Pixel XL）則尚未修復此漏洞。

由於使用低功率藍牙協定的裝置數量太過龐大，涉及眾多品牌，而且絕大部分產品甚至無法更新，因此這個漏洞難完全修復。

- CVE 編號：CVE-2020-9770
- 影響產品/版本：所有支援 BLE（Bluetooth Low Energy）通訊協定的產品；但 Windows BLE Stack 除外
- 解決方案：iOS 裝置可升級至最新版本作業系統，其餘裝置需待原廠提供資安修補軟體

- 資料來源：
  1. https://friends.cs.purdue.edu/pubs/WOOT20.pdf
  2. https://threatpost.com/bluetooth-spoofing-bug-iot-devices/159291/
  3. https://www.zdnet.com/article/billions-of-devices-vulnerable-to-new-blesa-bluetooth-security-flaw/

2.5.3、Thunderbolt 界面遭發現多個資安漏洞，讓駭侵者連上電腦系統 PCIe 匯流排

近來廣為各種電腦系統採用的高速傳輸界面 Thunderbolt，遭資安研究人員發現多個漏洞，最終可讓駭侵者直接存取電腦的 PCIe 高速匯流排，並發動各種攻擊。

近來廣為各種電腦系統採用的高速傳輸界面 Thunderbolt，遭資安研究人員發現多個資安漏洞；最終可讓駭侵者直接存取電腦的 PCIe 高速匯流排，並發動各種攻擊。

這些漏洞是由就讀於荷蘭安荷芬科技大學的 Björn Ruytenberg 於 Black Hat USA 2020 資安研討會上發表。Ruytenberg 以名為 Thunderspy 的模擬攻擊器，能夠成功攻擊 Thunderbolt 1、2、3，亦即 Thunderbolt 至今推出的所有版本。

Ruytenberg 在報告中一共揭露七個 Thunderbolt 的資安漏洞，包括不適當的韌體驗證機制、脆弱的裝置驗證機制、可使用未經驗證的裝置 metadata、利用舊版相容性發動的攻擊等等。

Ruytenberg 也模擬了九種不同的攻擊手法，包括駭侵者可以憑空偽造不存在的 Thunderbolt 裝置身分、複製使用者驗證過的 Thunderbolt 裝置，最後甚至可以直接存取受害系統的 PCIe 匯流排，以進行 DMA 攻擊。

Ruytenberg 的模擬攻擊程序，也能成功地在未經授權的情況下，直接調降 Thunderbolt 的資安防護設定值，甚至直接關閉所有安全設定，並且阻斷未

來所有的韌體更新。

報告指出，所有在 2011 年至 2020 年間發售的 Thunderbolt 裝置，都存有以上漏洞，而且無法以軟體更新方式修復；這些漏洞甚至還會影響 Thunderbolt 4 與 USB 4 預定推出的時間，因為硬體晶片必須重新設計。

- 建議採取資安強化措施

1. 建議用戶勿將自己具有 Thunderbolt 的設備處於無人看管之情況，避免讓未經授權的人存取，並只使用信任的周邊設備連接電腦。

2. Intel 尚未提供修補 Thunderspy 漏洞之安全性公告，並且因該漏洞無法以軟體更新方式修復，故硬體晶片需要變更設計。

- 資料來源：

1. https://blackhat.com/us-20/briefings/schedule/#when-lightning-strikes-thrice-breaking-thunderbolt--security-20628
2. https://i.blackhat.com/USA-20/Thursday/us-20-Ruytenberg-When-Lightning-Strikes-Thrice-Breaking-Thunderbolt-3-Security-wp.pdf

2.5.4、微軟發現利用 Zerologon 漏洞的攻擊行動開始出現

微軟最近開始觀測到利用 Zerologon 漏洞的攻擊行動，且有逐漸增加的趨勢；由於這個漏洞可能引來嚴重駭侵攻擊，美國政府已要求各單位應在三天內修補此漏洞。

微軟最近開始觀測到利用 Zerologon 漏洞的攻擊行動，且有逐漸增加的趨勢。

Zerologon 這個漏洞的 CVE 編號為 CVE-2020-1472，在九月初由荷蘭的資安研究團隊發現；這個漏洞的 CVSS 嚴重程度評分高達滿分的 10 分，屬於極嚴重資安漏洞。

Zerologon 漏洞發生在微軟 Netlogon 協定中的身分認證過程中，駭侵者可用以假冒任何內部網路中的電腦身分、關閉 Netlogon 身分認證中要求的各種資安選項，甚至更改 Active Directory 中任何一台電腦的登入密碼。

透過 Zerologon 的攻擊過程非常快速，幾秒內就可以完成，而且能夠立即掌握整個遭到入侵的企業內部網路，比傳統駭侵手法要快速簡便地多。

也因為這個原因，資安專家在發現此漏洞時，便預測很快就會有駭侵團體利用此漏洞發展出新的駭侵工具並發動攻擊；不出半個月，微軟便已偵測到愈來愈的 Zerologon 攻擊。

自 Windows 2008 至今的各版本 Windows Server，都含有 CVE-2020-1472 Zerologon 漏洞；微軟已經緊急推出兩個修補方法，暫時可以阻擋利用

Zerologon 的攻擊行動。

由於這個漏洞可能造成的嚴重後果，美國政府已要求各單位應在三天內修補此漏洞，否則就應將伺服器自聯邦政府網路離線。

- CVE 編號：CVE-2020-1472
- 解決方案：微軟推出的暫時阻擋利用 Zerologon 攻擊行動的兩個修補方法

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
  2. https://www.zdnet.com/article/zerologon-attack-lets-hackers-take-over-enterprise-networks/
  3. https://www.zdnet.com/article/microsoft-says-it-detected-active-attacks-leveraging-zerologon-vulnerability/
  4. https://cyber.dhs.gov/ed/20-04/

2.5.5、WordPress File Manager 擴充套件含有嚴重 0-day 資安漏洞

資安廠商 Wordfence 於日前發表研究報告，指出一個使用相當廣泛的 WordPress 擴充套件「File Manager」，含有一個嚴重的 0-day 資安漏洞

資安廠商 Wordfence 於日前發表研究報告，指出一個使用相當廣泛的 WordPress 擴充套件「File Manager」，含有一個嚴重的 0-day 資安漏洞；駭侵者可透過此漏洞遠端執行任意程式碼。

File Manager 是個可讓 WordPress 管理者更方便地管理網站內檔案的擴充套件；為達到此一目的，File Manager 使用了一個叫做 elFinder 的程式庫，該漏洞就發生在 File Manager 為了直接執行 php 程式碼而修改了 elFinder 中的 connector.minimal.php.dist 檔名為 connector.minimal.php，而這個檔案實際上並無作用，而且也未設有任何存取限制，導致駭侵者可以利用這個漏洞植入惡意程式碼。

據 Wordfence 的報告指出，這個 0-day 漏洞主要影響的 File Manager 版本為 6.0 到 6.8，其 CVSS 危險評分高達滿分的 10.0 分。

據估計，安裝了 File Manager 的 WordPress 網站約有七十萬個；File Manager 的開發者也已釋出資安修補更新版本；用戶只要將 File Manager 擴充套件升級到 6.9 版即可。

- 影響產品/版本：File Manager 6.0 到 6.8
- 解決方案：升級至 File Manager 6.9 以上版本

- 資料來源：
  1. https://wordpress.org/plugins/wp-file-manager/
  2. https://www.wordfence.com/blog/2020/09/700000-wordpress-users-affected-by-zero-day-vulnerability-in-file-manager-plugin/

2.5.6、PAN-OS 存有緩衝區溢位漏洞(CVE-2020-2040)，請盡速更新

PAN-OS 為運行於 Palo Alto Networks 新世代防火牆之作業系統，研究人員發現 PAN-OS 之 Captive Portal 或多因素驗證(Multi-Factor Authentication, MFA)介面存在緩衝區溢位漏洞(CVE-2020-2040)，未經身分驗證的攻擊者可藉由發送惡意請求，利用此漏洞進而以 root 權限執行任意程式碼。

目前 Palo Alto Networks 官方已針對此漏洞釋出更新程式，請參考以下建議盡速進行更新：

1. 請登入設備並檢視 Dashboard 資訊，或於指令介面輸入「show system info」指令，確認當前使用之 PAN-OS 版本，並於 Web 介面中確認是否啟用 Captive Portal 或多因素驗證功能。

2. 如使用受影響之 PAN-OS 版本，且啟用 Captive Portal 或多因素驗證功能，請瀏覽官方公告網頁(https://security.paloaltonetworks.com/CVE-2020-2040)進行 PAN-OS 版本更新。

- 影響產品/版本：PAN-OS 9.1.3 以前版本、PAN-OS 9.0.9 以前版本、PAN-OS 8.1.15 以前版本、PAN-OS 8.0：所有版本

- 參考資料：
  1. https://security.paloaltonetworks.com/CVE-2020-2040
  2. https://nvd.nist.gov/vuln/detail/CVE-2020-2040

2.5.7、Facebook 修復 Instagram 嚴重漏洞，可導致駭客遠端執行任意程式碼

Facebook 近日針對於四月初發現的 Instagram 嚴重資安漏洞發表修補新版。

Facebook 近日針對於四月初發現的 Instagram 嚴重資安漏洞發表修補新版；這個漏洞可導致用戶的手機遭駭侵者遠端執行任意程式碼，並且挾持手機中的相機、麥克風等裝置。

資安廠商 Check Point 是在今年四月初時發現這個漏洞，並提報給 Facebook；該漏洞編號為 CVE-2020-1895，主要發生於 Instagram 進行影像處理時的錯誤。駭侵者可以利用一張特製的影像檔案，透過簡訊、WhatsApp 或其他任何方法傳給受害者，當受害者收到這張影像檔案並儲存於手機後，再開啟 Instagram，就能執行惡意程式碼。

Check Point 指出，這個漏洞出在 Instagram 使用的第三方影像處理程式庫 Mozjpeg，這是一個由 Mozilla 開發的開源 JPEG 解碼器；由於 Instagram 使用這個程式庫的方法不當，造成駭侵者可使用特製影像檔案，直接利用 Instagram 向使用者要求的多種系統權限，包括存取用戶手機上的通訊錄、GPS 座標資訊、攝影機與本機檔案系統等；駭侵者也能讀取用戶透過 Instagram 傳送的私訊，並且擅自張貼或刪除貼文，甚至竄改系統設定。

這個漏洞的 CVSS 危險程度評分高達 7.8 分，屬於高危險程度。

Check Point 發現此漏洞後，隨即秘密向 Facebook 提報；Facebook 於日前修復並發行更新版本；Facebook 也表示並未發現這個漏洞被濫用的跡象。用戶只要將 Instagram 更新至 128.0.0.26.128 後版本即可。

- CVE 編號：CVE-2020-1895
- 影響產品/版本：Instagram 128.0.0.26.128 之前版本
- 解決方案：將 Instagram App 更新至 128.0.0.26.128 之後版本

- 參考資料：
  1. https://research.checkpoint.com/2020/instagram_rce-code-execution-vulnerability-in-instagram-app-for-android-and-ios/
  2. https://m.facebook.com/security/advisories/cve-2020-1895
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1895
  4. https://nvd.nist.gov/vuln/detail/CVE-2020-1895

第 3 章、 資安研討會及活動

[台灣網路講堂]言論自由與內容審查： 失控的使用者 PO 文誰負責？	
活動時間	**2020 年 10 月 12 日（一）14:00-16:00**
活動地點	**IEAT 會議中心 10F 第 3 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/ihub20201012**
活動概要	 **主辦單位：TWNIC、TWIGF、NII** 臺灣已經連續多年成為「遭國外假訊息攻擊」最嚴重國家，且國內民眾散播各種假訊息或發表仇恨言論的案例亦層出不窮。因此，究竟使用者 PO 文該由誰負責管理（審查）與負責，以及如何兼顧保障言論自由等問題值得探討。

2020 台灣資安通報應變年會	
活動時間	**2020 年 10 月 27 日(星期二) 8:30-17:00**
活動地點	**台北市中正區徐州路 2 號 台大醫院國際會議中心**
活動網站	**https://www.informationsecurity.com.tw/Seminar/ISevent20201027/**
活動概要	 **主辦單位：TWNIC、TWCERT/CC** 隨著全球資訊環境的瞬息萬變，在物聯網、AI、5G 技術快速發展下，資訊安全議題已成為數位經濟下重要顯學。資安情資及資安事件應變備受企業對重視，如何以國際思維掌握資安先機，運用國內外資安情資進行事前防禦，並鼓勵建立資安事件通報及諮詢管道，以利因應資安事件，減低企業駭侵之衝擊及損害，為本次活動之核心。最後分享我國企業如何建立產品資安事件應變小組(PSIRT)經驗，讓企業產品受到國際肯定提升企業品牌形象。誠摯邀請產官學研各單位參與交流，一起超前部署，掌握資安聯防與應變先機，提升我國企業資安防護能量，達到資安聯防目標。 ★本會議報名截止日為 2020 年 10 月 23 日(五) 16:00。主辦單位將視報名狀況提前或延後線上報名時間。若報名者不克參加，可指派其他人選參加，並告知主辦單位。 ★本活動可以向 TWCERT/CC 申請出席證明，歡迎踴躍參加! 活動洽詢 02-8729-1099 分機 649 /李小姐

InfoSec Taiwan 2020 - Workshop 實作課程	
活動時間	**2020/11/02(一) 09:00~17:00**
活動地點	**台北文創大樓(台北市信義區菸廠路 88 號)**
活動網站	**https://event.twcsa.org/site/course/7y4p3J0m_oL6h-WZ9XNXcQ..**
活動概要	 **主辦單位：台灣數位安全聯盟** 報名時間：2020-10-01 ~ 2020-10-31 InfoSec Taiwan 2020 規劃了資安實務課程，透過深入淺出的實務教學，讓學員實際學習資安工作與建置技術，結合台灣數位安全聯盟專業講師，提供符合產業需求的資安技術!

InfoSec Taiwan 2020 - Briefing 年會	
活動時間	**2020/11/03(二)~2020/11/04(三) 09:00~17:00**
活動地點	**台北文創大樓 6 樓(台北市信義區菸廠路 88 號)**
活動網站	**https://event.twcsa.org/site/course/5t2kIENz-rXMDMsfG5FgQA..**
活動概要	 **主辦單位：台灣數位安全聯盟** 報名時間：2020-09-21 ~ 2020-10-25 智慧聯網的時代來臨，許多應用都與資訊安全相關，資訊安全的議題早已跨越了國境的邊界，近來幾次大型網路攻擊事件，不論國內外都引起了許多人的憂心，不論是近來經常發生的勒索攻擊威脅，或是網站遭到資料的竊取，這些都已成為全球性的資安問題，如何因應新興的資安問題所帶來的資安風險，成為我們所關注的話題。 國際資安大會，由台灣數位安全聯盟主辦，同步接軌 Cloud Security Alliance、The Honeynet Project 與 OWASP 等國際資訊安全組織最新研究成果，提供與會人員掌握全球資訊安全發展脈動與趨勢，會議內容涵蓋雲端服務安全、誘捕資安技術、網站應用程式安全、事件掌握與應變等議題，接軌國際資安社群有助於掌握全球發展趨勢。

第 4 章、 2020 年 09 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。

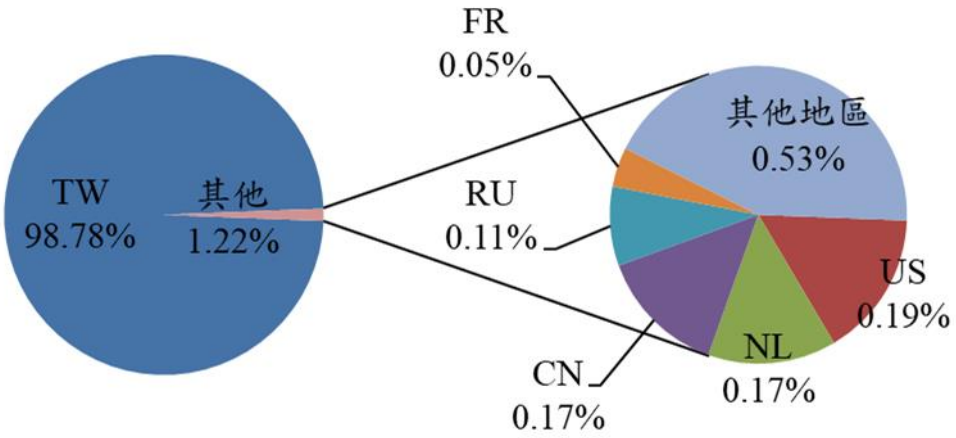


圖 1、分享地區統計圖

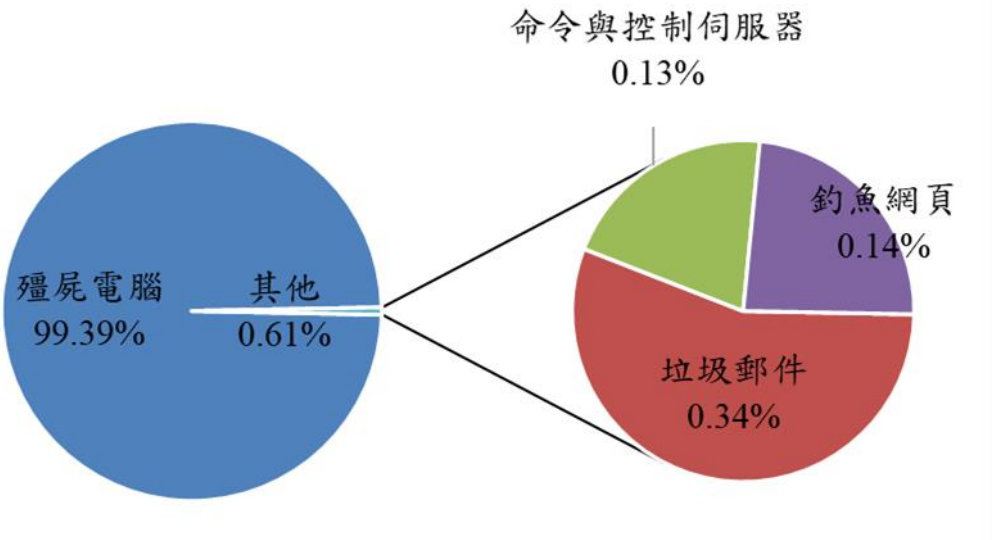


圖 2、分享類型統計圖

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 10 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**