TWCERT/CC 資安情資電子報

2021 年 1 月份

目錄

=

第 1 章、 封面故事 1
駭侵者透過 Microsoft Teams 發動攻擊，某全球金融機構險遭攻陷 1
第 2 章、 國內外重要資安事件 3
2.1、 資安趨勢 3
2.1.1、 愈來愈多駭侵團體駭入 Web Mail，竄改郵件規則，進行 BEC 攻擊 3
2.1.2、 33 個開源 TCP/IP Stack 嚴重漏洞，IT、OT 及 IOT 設備面臨攻擊危機 . 5
2.1.3、 PLEASE_READ_ME 勒贖軟體，攻陷 83,000 個 MySQL 資料庫伺服器 . 8
2.1.4、 IBM 揭發針對 COVID-19 疫苗冷鏈發動的全球性釣魚攻擊活動 10
2.1.5、 微軟揭露在搜尋頁面安插蓋台廣告的惡意軟體 Adrozek 全球攻擊行動 . 12
2.2、 國際政府組織資安資訊 14
2.2.1、 美國國土安全部通令，政府單位應停用遭駭之 SolarWinds Orion 產品 14
2.2.2、 美國資安主管機關發出警訊，K-12 教育體系遭駭侵團體大規模攻擊 16
2.2.3、 駭侵團體藉 SolarWinds Orion 漏洞入侵美國政府，受害範圍持續擴大 18
2.2.4、 歐洲藥品管理局遭駭侵攻擊 20
2.2.5、 巴西衛生部官網原始碼內含資料庫登入資訊，導致巴西民眾個資曝光 .. 21
2.3、 行動裝置資安訊息 23
MobileIron 嚴重 RCE 資安漏洞，現遭 APT 駭侵團體大規模用於攻擊 23
2.4、 軟體系統資安議題 25
2.4.1、 Apple 推出 macOS、iOS、iPad OS、tvOS、watchOS 更新版 25
2.4.2、 APT 駭侵團體以最新 macOS 後門惡意軟體發動攻擊 27
2.4.3、 超過四萬筆 Amazon S3 的 public bucket URL 被公開 29
2.4.4、 Canon 遭到勒贖攻擊，部分企業資料遭竊 31
2.4.5、 資安廠商 FireEye 本身也遭駭侵攻擊，攻擊者疑有特定國家支持 33
2.4.6、 FireEye、微軟與 GoDaddy 合力對抗 SolarWinds 後門攻擊 35
2.4.7、 Spotify 再度發生資料外洩事件，部分用戶需更改密碼 37
2.4.8、 以色列大型保險公司 Shirbit 遭勒贖軟體攻擊 39
2.4.9、 韓國大型零售業者 E-Land 遭勒贖攻擊，200 萬張信用卡資料疑遭竊取 41

2.5、 軟硬體漏洞資訊 43
2.5.1、 資安專家發現 RTA 工業用網路卡存有嚴重資安漏洞 43
2.5.2、 Dell Wyse Thin Clients 的資安漏洞讓駭客擁有控制權..... 45
2.5.3、 PlayStation Now 的資安漏洞，讓駭侵者針對 Windows 玩家發動攻擊 . 47
2.5.4、 VMware 修復 Workspace One 與其他平台的 0-day 資安漏洞..... 49
第 3 章、 資安研討會及活動..... 51
第 4 章、 2020 年 12 月份資安情資分享概況..... 53

第 1 章、 封面故事

駭侵者透過 Microsoft Teams 發動攻擊，某全球金融機構險遭攻陷

資安廠商攔截到一起發生在某全球金融機構的攻擊事件，駭侵者透過該機構內部的 Microsoft Teams 帳號發動攻擊，險令該機構因而癱瘓。

資安廠商 Avanan 近期發表資安通報，指出該公司的防駭產品，攔截到一起發生在某全球金融機構的攻擊事件；駭侵者透過該機構內部的 Microsoft Teams 帳號發動攻擊，險令該機構因而癱瘓。

Avanan 說，這起事件發生在一家全球性的大型金融機構與其協力廠商。本案的駭侵者於一年多前先駭入了該協力廠商，接著以取得的 Microsoft Office 365 登入資訊潛入大型金融機構的 Microsoft Teams 溝通群組中，等候了近一年，都沒有發動任何攻擊。

在潛伏一年多後，駭侵者在某個群組內傳送檔案的對話中現身，提供了內含惡意軟體的檔案給群組成員；該檔案內含的惡意木馬軟體，可以監控受害者的螢幕，並且進行遠端遙控，控制受害者的桌面操作。

Avanan 說，這次攻擊事件的特殊之處，在於該木馬具有逃過 Microsoft Teams 偵測的能力，以致於在傳送惡意軟體的過程中，沒有被 Microsoft Teams 發現。

Avanan 指出，過去這類的駭侵攻擊行動，多半是透過 Email 進行，然而透過 Microsoft Teams 的攻擊，數量正在逐漸增加；隨著 Microsoft Teams 廣受採用，駭侵者只要取得 Office 365 的登入資訊，即可利用 Microsoft Teams 發動攻擊。

- 資料來源：
  1. https://www.avanan.com/blog/microsoft-teams-new-attack-form
  2. https://www.microsoft.com/en-us/microsoft-365/blog/2019/03/19/microsoft-teams-experiences-intelligent-workplace/

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、愈來愈多駭侵團體駭入 Web Mail，竄改郵件規則，進行 BEC 攻擊

FBI 日前發表資安通報，指出有愈來愈多駭侵團體，駭入 Web Mail 伺服器上的自動轉寄的郵件規則，以 BEC 攻擊手法盜領各種款項，造成極大損失。

美國聯邦調查局（FBI）日前發表資安通報，指出有愈來愈多駭侵團體，最近開始針對 Web Mail 服務自動轉寄的郵件規則發動 BEC（Business Email Compromise）攻擊，來盜領企業的各種帳款，造成極大損失。

FBI 指出，在疫情影響之下，愈來愈多中小企業採用遠距工作，並且更為依賴以網頁為基礎的 Web Mail 服務，較少使用本機的郵件軟體收發信件。

由於這類 Web Mail 服務的郵件規則，通常不會同步到本機端的郵件軟體，而是自成一格，因此給了駭侵者可乘之機：駭侵者可以先以社交工程或其他駭侵方式，先駭入員工的 Email 帳號，接下來駭侵者會竊取該員工的來往郵件內容，收集各種資訊後，接下來就利用這些資訊來偽裝成員工本人，向帳款支付者發送詐騙郵件，使其更改匯款帳戶為駭侵者控制的假帳號，藉以竊取企業的帳款。

駭侵者更會進一步修改 Web Mail 系統的郵件規則，將這類帳款相關郵件自動轉到其他 Email 信箱，進一步降低郵件內容被受害企業發現的機會。

由於這種做法，駭侵者發動惡意郵件攻擊造成的損失，正在快速擴大；根據 FBI 的報告指出，全球在 2019 年通報的企業惡意郵件攻擊，造成的損失高達 17 億美元。

FBI 說，如果企業的資訊與資安管理人員，未能經常檢視其 Web Mail 上的郵件規則與不明連線，就很容易受到這類攻擊而難以及時發現。

- 資料來源：
  1. https://image.communications.cyber.nj.gov/lib/fe3e15707564047c7c1270/m/2/FBI+PIN+-+11.25.2020.pdf
  2. https://www.securityweek.com/fbi-warns-auto-forwarding-email-rules-abused-bec-scams
  3. https://www.securityweek.com/bec-losses-surpassed-17-billion-2019-fbi

2.1.2、33 個開源 TCP/IP Stack 嚴重漏洞， IT、OT 及 IOT 設備面臨攻擊危機

33 個開源 TCP/IP Stack 嚴重漏洞，數以百萬計的 IT、OT 及 IOT 設備將面臨攻擊危機。

研究人員發現了 33 個 TCP/IP Stack 的漏洞存在於 4 個開源的 TCP / IP Stack 中，而今年六月底 JSOF 曾發布 TCP/IP 的 Ripple20 漏洞。由於這些漏洞會導致記憶體損毀或是記憶體存取的位置錯誤，這些情況可能造成資訊外洩、阻斷服務攻擊或遠端程式碼執行。

4 個受影響的開源 TCP / IP Stack 分別為 PicoTCP、FNET、Nut / Net 及 uIP，且分散在 DNS、IPv6、IPv4、TCP、ICMP、LLMNR 及 mDN 共七個 TCP/IP Stack 元件。這些漏洞將影響超過 150 間設備製造商，其中包括 Devolo、EMU Electronic A、FEIG、Genetec、Harting、Hensoldt、Microchip、Nanotec、NT-Ware、Tagmaster、Siemens、Uniflow、Yanzi Networks 的 IT、OT 及 IOT 的產品。

美國國土安全部網路安全暨基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA)也針對此重大漏洞發出請提高警覺，並進行相關的建議措施與修補機制。

此 33 個漏洞因其攻擊記憶體的特性被稱為 AMNESIA:33，當中包含 3 個 CVSSv3 風險等級為 Critical，受影響的版本與相關 CVE 資訊如下：

TCP/IP Stack	受影響版本	解決方案
uIP	uIP (EOL), Version 1.0 and prior uIP-Contiki-NG, Version 4.5 and prior uIP-Contiki-OS (end-of-life [EOL]), Version 3.0 and prior	已終止更新，請參考防護建議措施
picoTCP	picoTCP -NG, Version 1.7.0 and prior picoTCP (EOL), Version 1.7.0 and prior	已終止更新，請參考防護建議措施
FNET	4.6.3	更新至 4.7.0 或更新版本
Nut/Net	5.1 and prior	更新至 5.2.4 或更新版本

CVE 編號	TCP/IP Stack	主旨	CVSS3.0
CVE-2020-24336	uIP	Remote Code Execution	9.8
CVE-2020-24338	picoTCP	Remote Code Execution	9.8
CVE-2020-25111	Nut/Net	Remote Code Execution	9.8
CVE-2020-13987	uIP	Denial of Service, Information Leak	8.2
CVE-2020-17437	uIP	Denial of Service	8.2
CVE-2020-24334	uIP	Denial of Service	8.2
CVE-2020-17443	picoTCP	Denial of Service	8.2
CVE-2020-24340	picoTCP	Denial of Service, Information Leak	8.2
CVE-2020-24341	picoTCP	Denial of Service, Information Leak	8.2
CVE-2020-17467	FNET	Information Leak	8.2
CVE-2020-25109	Nut/Net	Denial of Service	8.2
CVE-2020-25110	Nut/Net	Denial of Service	8.2
CVE-2020-17439	uIP	DNS Cache Poisoning	8.1
CVE-2020-25112	uIP	Remote Code Execution	8.1
CVE-2020-13984	uIP	Denial of Service	7.5
CVE-2020-13985	uIP	Denial of Service	7.5
CVE-2020-13986	uIP	Denial of Service	7.5
CVE-2020-13988	uIP	Denial of Service	7.5
CVE-2020-17440	uIP	Denial of Service	7.5
CVE-2020-24335	uIP	Denial of Service	7.5
CVE-2020-17441	picoTCP	Denial of Service, Information Leak	7.5
CVE-2020-17442	picoTCP	Denial of Service	7.5
CVE-2020-17444	picoTCP	Denial of Service	7.5
CVE-2020-17445	picoTCP	Denial of Service	7.5
CVE-2020-24337	picoTCP	Denial of Service	7.5
CVE-2020-24339	picoTCP	Denial of Service	7.5
CVE-2020-17468	FNET	Denial of Service	7.5
CVE-2020-25107	Nut/Net	Denial of Service	7.5
CVE-2020-25108	Nut/Net	Denial of Service	7.5
CVE-2020-17438	uIP	Denial of Service	7
CVE-2020-24383	FNET	Denial of Service, Information Leak	6.5
CVE-2020-17469	FNET	Denial of Service	5.9
CVE-2020-17470	FNET	DNS Cache Poisoning	4

- 建議防護措施

  1、根據 CVE 編號進行對應的漏洞修補。

  2、IOT 網路設備暴露於網路上，必要時以資安防護設備進行保護。

  3、使用內部 DNS 服務進行查詢。

  4、檢視網路設備記錄檔是否有異常流量。

  5、暫停非必要的網路服務。

- 資料來源：

  1. https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01

2.1.3、PLEASE_READ_ME 勒贖軟體，攻陷超過 83,000 個 MySQL 資料庫伺服器

資安專家發現暗網上有人標售大量自 MySQL 資料庫中駭侵竊取的資料，受害的伺服器總數高達 83,000 個以上，被標售的 MySQL 資料庫更多達 250,000 個以上。

資安廠商 Guardicore 近日公布研究報告，指出該公司旗下的資安專家，發現暗網上有人標售大量自 MySQL 資料庫中駭侵竊取的資料；受害的伺服器總數高達 85,000 個以上，被標售的 MySQL 資料庫更多達 250,000 個以上。

Guardicore 指出，用以發動攻擊的勒贖軟體，名為「PLEASE_READ_ME」，攻擊行動最早可追溯自 2020 年一月，攻擊方式就是針對曝露在 Internet 上的 MySQL 資料庫進行掃瞄，然後以暴力試誤法，找出其登入資訊，然後進行資料庫內容竊取、加密與勒贖攻擊。

駭侵者成功入侵 MySQL 資料庫後，會將其內容全部清空，並壓縮成 zip 檔，傳回攻擊者的伺服器；接著歹徒會在資料庫中新增一個稱為「警告」的表格，並在表格內放入勒贖恐嚇內容，並要求 0.08 個比特幣的贖金。

到目前為止，該公司一共截獲 92 起類似的攻擊行動；一開始攻擊行動集中於 2020 年第一季，自五月到十月初之間，攻擊頻率明顯減少，但到十月起攻擊活動又突然大量增加。

據 Guardicore 指出，駭客用以發動攻擊的 11 個 IP 位址，大多數位於英國與愛爾蘭；這些被竊的資料庫，旋即被放到暗網上拍賣，以每個資料庫 0.03 比特幣的「售價」起標。

Guardicore 說，全球估計約有近 500 萬個 MySQL 資料庫直接連上 Internet，都有可能成為這類勒贖攻擊的目標。

- 資料來源：
  1. https://www.guardicore.com/labs/please-read-me-opportunistic-ransomware-devastating-mysql-servers/
  2. https://www.bleepingcomputer.com/news/security/250-000-stolen-mysql-databases-for-sale-on-dark-web-auction-site/
  3. https://threatpost.com/please_read_me-ransomware-mysql-servers/162136/

2.1.4、IBM 揭發針對 COVID-19 疫苗冷鏈發動的全球性釣魚攻擊活動

IBM 旗下的資安研究團隊近期發現一起全球性的釣魚攻擊活動，目標鎖定 COVID-19 物流的冷鏈相關單位。

IBM 旗下的資安研究團隊 X-Force，近期發表研究報告；報告中指出該單位發現一起全球性的釣魚攻擊活動，目標鎖定 COVID-19 物流的冷鏈相關單位進行攻擊。

IBM X-Force 指出，這起攻擊事件涉及六個國家的疫苗冷鏈運輸相關單位，攻擊行動自 2020 年 9 月開始進行。攻擊者假冒為海爾生物醫療公司的員工，向參與疫苗冷鏈運送的合作單位發送釣魚信件，企圖騙取各種登入資訊，以便駭入其內部網路。

據 IBM X-Forece 的報告說，這些釣魚信的攻擊目標，包括歐盟稅收與關稅同盟總局（European Union Directorate-General for Taxation and Custom Union），以及能源、製造業、網站設計業、軟體業、網路資安業等，分布於德國、義大利、南韓、捷克、歐盟與台灣。

報告說，駭侵者以魚叉式釣魚攻擊，鎖定這些產業中的行銷、採購、資訊系統與財務相關主管人員，發送釣魚攻擊信件；另外也有一些攻擊行動係鎖定這些公司的支援體系。

IBM X-Force 指出，目前尚無明確證據，可以藉此找出發動這場攻擊的駭侵者身份，但由於此波攻擊行動沒有特定的金流情報，再加上駭侵攻擊本身的手法相當縝密，IBM 認為攻擊者幕後應有來自特定國家的支援。

- 資料來源：
  1. https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/
  2. https://us-cert.cisa.gov/ncas/current-activity/2020/12/03/ibm-releases-report-cyber-actors-targeting-covid-19-vaccine-supply
  3. https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/

2.1.5、微軟揭露在搜尋頁面安插蓋台廣告的惡意軟體 Adrozek 大規模全球攻擊行動

微軟指出一個名為 Adrozek 的惡意軟體，會在搜尋頁面中安插蓋台廣告，以賺取不法廣告分潤。

微軟旗下的資安研究單位 Microsoft 365 Defender Research Team，日前發表研究報告，指出該單位一個名為 Adrozek 的惡意軟體，會在搜尋頁面中安插蓋台廣告，以賺取不法廣告分潤。

報告中說，這個名為 Adrozek 的惡意軟體，會在各種瀏覽器中安裝外掛程式或延伸套件，修改瀏覽器的特定 DLL 檔案，並且竄改瀏覽器設定，以便在用戶以各種搜尋引擎搜尋所需資料時，在搜尋頁面上顯示 Adrozek 的蓋台廣告，蓋過搜尋引擎本身顯示的關鍵字廣告。

會遭到 Adrozek 攻擊的瀏覽器，主要是 Google Chrome、Microsoft Edge、Yandex Browser、Mozilla Firefox 等用戶相當多的主流瀏覽器。

雖然利用惡意瀏覽器外掛來顯示不當廣告不是新鮮事，但微軟指出 Adrozek 的攻擊範圍含蓋多種主流瀏覽器，同時具有強大的基礎架構，是相當罕見的；微軟觀察到共有 159 個不重覆的網域名稱與 Adrozek 有關，每個網域中平均有 17,300 個不重覆的 URL，每個 URL 觀察到超過 15,300 個惡意軟體樣本。

微軟資安團隊自今年（2020 年）五月起開始觀察到 Adrozek 的活動，在今年八月時達到高峰，一天有超過 30,000 台裝置遭到感染；感染的裝置遍及全球，最嚴重的地區包括歐洲、南亞與東南亞。

微軟說，以 Adrozek 仍在繼續擴大的攻擊範圍來看，Adrozek 的基礎架構仍在不斷擴張。

- 資料來源：
  1. https://www.microsoft.com/security/blog/2020/12/10/widespread-malware-campaign-seeks-to-silently-inject-ads-into-search-results-affects-multiple-browsers/
  2. https://siliconangle.com/2020/12/10/microsoft-warns-adrozek-malware-hijacking-advertising-search-results/
  3. https://threatpost.com/adrozek-malware-fake-ads-30k-devices/162217/

2.2、國際政府組織資安資訊

2.2.1、美國國土安全部通令，政府單位應立即停用遭駭之 SolarWinds Orion 產品

美國國土安全部資安中心日前發布通令，要求美國政府旗下所有單位，立即停用所有 SolarWinds Orion 產品，以避免發生更大規模透過該產品漏洞進行的駭侵攻擊。

美國國土安全部資安中心日前發布 21-01 號通令，要求美國政府旗下所有單位，立即停用所有使用中的 SolarWinds Orion IT 監管平台產品，以避免發生更大規模透過該產品漏洞進行的駭侵攻擊。

上周美國商務部與財政部驚傳遭到特定國家支持的駭侵攻擊事件，事件原因與其採用的 SolarWinds Orion Platform 遭到 APT 駭侵團體 Cozy Bear 滲透有關；APT 駭侵團體 Cozy Bear 於今年三月間在 SolarWinds Orion 的更新程式中植入木馬，取得遠端控制受駭系統的能力。

採用 SolarWinds Orion IT 管理平台的客戶，據估計有一萬八千個左右；而在經過調查之後發現，美國國土安全部本身的系統也遭到入侵；國土安全部旋即在 12 月 13 日發布通令，要求所有使用 SolarWinds Orion 系統的美國各級政府機構旗下的非軍事性質單位，應立即將所有執行 SolarWinds Orion 的電腦離線，甚至關閉其電源，以避免遭駭規模進一步擴大。

但資安專家指出，Cozy Bear 於三月起就成功於 SolarWinds Orion 中植入木馬，至今超過半年以上，很可能早已駭入並掌握重要機構的 SAML 或

Active Directory 主機，因此即使將執行 SolarWinds Orion 的主機斷網隔離，也無法有效防止駭侵者注入的其他惡意軟體在內網中傳散。

- 資料來源：
  1. https://cyber.dhs.gov/ed/21-01/
  2. https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network
  3. https://www.lawfareblog.com/solarwinds-breach-why-your-work-computers-are-down-today

2.2.2、美國資安主管機關發出警訊，K-12 教育體系遭駭侵團體大規模攻擊

美國政府多個單位，日前聯合發表資安警訊，指出有駭侵者正在針對美國的 K-12（幼兒園至中學）教育體系發動大規模攻擊，包括勒贖、資料竊取、干擾遠距教學等等。

包括聯邦調查局（Federal Bereau of Investigation, FBI）、網路安全暨基礎設施安全局（Cybersecurity & Infrastructure Security Agency, CISA）與跨州資訊共享分析中心（Multi-State Information Sharing and Analysis Center, MS-ISAC）等多個美國政府單位，日前聯合發表資安警訊；警訊中指出有駭侵者正在針對美國的 K-12（幼兒園至中學）教育體系發動大規模攻擊，包括勒贖攻擊、機敏資料竊取、干擾遠距教學等等。

聯合通報中指出，最近多個單位紛紛接獲大量來自 K-12 教育單位的勒贖攻擊通報；這些勒贖攻擊一如針對商業與其他公家單位的攻擊一樣，不但會竊取學生的各種個人機敏資訊並勒索贖金，同時也攻擊學校內的資訊裝置與遠距教學系統，造成學校運作的各種障礙。

通報也指出，近來針對 K-12 教育單位的勒贖攻擊，比例直線上升；在 2020 年一月到七月間，MS-ISAC 接獲的勒贖攻擊事件通報中，有 28% 係針對 K-12 教育單位；到了八月和九月，這個比例陡升至 57%。

通報說，用以攻擊 K-12 教育機構的勒贖軟體，種類相當多樣，最常見的五種分別是 Ryuk、Maze、Nefilim、AKO 與 Sodinokibi/REvil。

- 資料來源：
  1. https://us-cert.cisa.gov/sites/default/files/publications/AA20-345A_Joint_Cybersecurity_Advisory_Distance_Learning_S508C.pdf
  2. https://mashable.com/article/hackers-targeting-kindergartens-elementary-schools-warns-cisa/
  3. https://thecyberwire.com/newsletters/daily-briefing/9/238

2.2.3、駭侵團體藉 SolarWinds Orion 漏洞入侵美國政府事件，受害範圍持續擴大

近期爆出的美國多個政府單位，因 IT 設備監控軟體 SolarWinds Orion 漏洞而遭俄羅斯駭侵團體駭入的事件，受害單位與範圍持續擴大。

近期爆出的美國多個政府單位，包括美國財政部、商務部、國土安全部等重要政府單位，因 IT 設備監控軟體 SolarWinds Orion 漏洞，而遭俄羅斯 APT 駭侵團體 Cozy Bear 以木馬駭入的事件，目前受害單位與範圍仍在持續擴大。

據紐約時報於 12/15 的報導指出，美國國防部與美國國務院也在這波大規模駭侵攻擊行動中受到影響；受影響的單位包括部分軍事單位、情報單位，甚至還包括核能相關研究機構在內。

另外，包括美國疾病預防管制中心（ Centers for Disease Control and Prevention ）、美國司法部，以及多家製造業在內的公私單位，也都在這波遭 Cozy Bear 駭侵的名單之列。

負責主管美國資安事務的網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA），儘管一再對外呼籲資安防護的重要性，但該局也在這波針對 SolarWinds Orion 的駭侵攻擊中遭到入侵。

據先前 SolarWinds 提出的通報指出，這波受到 SolarWinds Orion 漏洞影響的該產品用戶多達 18,000 個單位以上，其中有很多客戶屬於美國政府與

名列財星 500 大名單之中的大型企業；可以預見隨著案情調查日漸明朗，受害單位範圍仍將不斷擴大。

目前這波駭侵行動造成的具體損失，包括受害政府或民間單位是否有資料外洩、哪些資料可能被竊、駭侵者在駭入各單位系統後，是否發動進一步攻擊等細節資訊，都還沒有對外公開。

- 資料來源：
  1. https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html?referringSource=articleShare
  2. https://www.reuters.com/article/us-usa-cyber-amazon-com-exclsuive-idUSKBN28N0PG
  3. https://nymag.com/intelligencer/2020/12/russian-spies-hacked-treasury-commerce-departments-report.html
  4. https://www.acw.org.tw/News/Detail.aspx?id=1164

2.2.4、歐洲藥品管理局遭駭侵攻擊

歐洲藥品管理局遭駭侵攻擊，COVID-19 疫苗相關資料遭非法存取。

歐洲藥品管理局（European Medicines Agency, EMA）於日前發出聲明，該機構證實遭受駭侵攻擊，駭客非法取閱了輝瑞藥廠與德國生技公司 BioNTech 提交給 EMA 並儲存於其伺服器的 COVID-19 疫苗候選株相關資料。兩間公司表示，與此事件有關的系統並無出現問題，也沒有任何參與研究的人員個資遭外洩。

目前 EMA、執法機構與其他有關單位正密切合作，展開了全面性的調查。提醒國內與 COVID-19 疫苗相關廠商、研究單位及供應鏈廠商密切注意資安防護及相關資安訊息，避免遭受駭客攻擊。

- 資料來源：
  1. https://investors.biontech.de/news-releases/news-release-details/statement-regarding-cyber-attack-european-medicines-agency
  2. https://www.ema.europa.eu/en/news/cyberattack-european-medicines-agency

2.2.5、巴西衛生部官網原始碼內含資料庫登入資訊，導致巴西民眾個資曝光

媒體發現巴西衛生部官方網站，將一個重要政府資料庫的登入資訊寫在網站程式碼中，導致超過 2 億 4300 萬名巴西民眾的個資對外曝光。

巴西一家名為 Estadao 的報社，日前發現巴西衛生部官方網站直接將一個重要政府資料庫的登入資訊，以極易破解的編碼方式寫在網站程式碼中；導致超過 2 億 4300 萬名巴西民眾的個資對外曝光超過半年以上。

Estadao 記者是在讀到一篇由巴西的非政府組織「巴西開放知識」（Open Knowledge Brasil, OKBR）的報告後決定開啟調查，該報告指出某個巴西政府單位的官方網站，也將某個政府資料庫的登入資訊，直接寫在網站程式碼內。

Estadao 調查巴西政府所屬的各個部門官方網站，確認是否也有類似錯誤發生時，發現巴西衛生部的官網，竟然也犯了相同的錯誤，將該部門所屬巴西公民健康資料庫的登入資訊，以非常容易還原的 Base64 編碼，直接寫在網站程式碼中，導致任何人都能登入該資料庫並存取資訊。

該資料庫內含 1989 年以來總供 2 億 4300 萬名已經逝世與仍然存活巴西民眾的個人資料，資料欄位包括完整姓名、住家地址、電話號碼與個人健康與就診記錄等。

目前巴西衛生部已經將官網內的登入資訊加以移除，但無法確認這個資料庫在過去是否曾遭不當存取；要是確認資料已遭不肖人士竊取，這起事故將會是嚴重的資安事件。

- 資料來源：
  1. https://www.zdnet.com/article/data-of-243-million-brazilians-exposed-online-via-website-source-code/
  2. https://saude.estadao.com.br/noticias/geral,nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes,70003536340
  3. https://en.wikipedia.org/wiki/Sistema_Único_de_Saúde

2.3、行動裝置資安訊息

MobileIron 嚴重 RCE 資安漏洞，現遭 APT 駭侵團體大規模用於攻擊

廣受採用的行動裝置布署服務平台 MobileIron，於六月被台灣資安廠商發現的嚴重漏洞，證實已遭 APT 駭侵團體大規模用於攻擊行動。

廣為全球各大政府單位與企業採用，用於布署並管理員工持有行動裝置的服務平台 MobileIron，於六月被台灣資安廠商 Devcore 發現的嚴重漏洞，證實已遭 APT 駭侵團體大規模用於攻擊行動。

英國國家資安中心（National Cyber Security Centre）於十一月下旬發表資安通報，指出 MobileIron 的這個嚴重資安漏洞，確定已遭多個背後有國家勢力支持的 APT 駭侵團體大規模利用，用於攻擊英國公私營單位所屬的網路。

據資安媒體 ThreatPost 報導指出，受到此波攻擊的單位，可能包括但不限於醫療機構、地方政府組織、物流業者、司法單位等。

遭 APT 駭侵團體利用的漏洞，其 CVE 編號為 CVE-2020-15505，其 CVSS 危險程度評分高達 9.8 分（滿分為 10 分），屬於嚴重等級的資安漏洞；駭侵者可利用這個漏洞遠端執行任意程式碼，在受害者的內部網路中竊取機敏資訊。

更有甚者，美國資安與基礎設施安全局（Cybersecurity & Infrastructure Security Agency）也指出有 APT 駭侵團體整合此漏洞與 ZeroLogon 微軟伺服器漏洞，發動猛烈攻擊。

MobileIron 這個漏洞早在今年六月由台灣資安廠商 Devocre 發現並提報後，當月就已經推出修正工具；然而現在卻還發生駭侵事件，MobileIron 企業用戶應儘速更新系統，以避免駭侵攻擊持續造成破壞。

- 資料來源：
  1. https://www.ncsc.gov.uk/news/alert-multiple-actors-attempt-exploit-mobileiron-vulnerability
  2. https://us-cert.cisa.gov/ncas/alerts/aa20-283a
  3. https://threatpost.com/critical-mobileiron-rce-flaw-attack/161600/

2.4、軟體系統資安議題

2.4.1、Apple 推出 macOS、iOS、iPad OS、tvOS、watchOS 更新版

Apple 推出的 macOS 更新版，修復多達 59 個軟體漏洞，其中更包括 30 個遠端執行任意程式碼的漏洞。其他裝置也同時推出更新版。

Apple 推出 macOS Big Sur 11.1 更新版，新版修復多達 59 個軟體漏洞；其中更包括 30 個可能導致駭侵者遠端執行任意程式碼（RCE）的嚴重漏洞；Mac 電腦系統用戶，均應立即更新至最新版本。

同時推出的更新版本，還包括 macOS Catalina 與 macOS Mojave 兩個較舊主要版本 macOS 的更新，同樣也修復了多個已知漏洞。

在這些獲得修復的漏洞中，比較嚴重的遠端任意程式碼執行漏洞包括：

1. CVE-2020-27941：發生於 AppleGraphicsControl 子系統，駭侵者可取得核心執行權限；

2. CVE-2020-27910、CVE-2020-27916：發生於 macOS Mojave 與 Catalina 的 Audio 子系統，駭侵者可利用特製聲音檔案取得 RCE 權限。

3. CVE-2020-9960、CVE-2020-27980、CVE-20200-27948：發生於 CoreAudio 子系統中，駭侵者可利用特製聲音檔誘發越界讀寫錯誤，藉以取得 RCE 權

限。

4. CVE-2020-27922：發生於 CoreText，駭侵者可利用特製字型檔案，藉以取得 RCE 權限。

除了 macOS 外，Apple 也同步推出 tvOS 與 watchOS 新版，分別解決了 AppleTV 9 個漏洞、Apple Watch 的 10 個漏洞；iOS 與 iPad OS 也同時推出 14.3 新版，一個修復 11 個資安漏洞，其中包括兩個嚴重漏洞 CVE-2020-27943 和 CVE-2020-27944。

所有上述產品的用戶，應立即透過軟體更新功能，將裝置的作業系統更新至最新版本，以避免遭到駭侵者利用已知漏洞發動攻擊。

- 資料來源：
  1. https://support.apple.com/en-gb/HT212011
  2. https://support.apple.com/en-us/HT212003
  3. https://www.securityweek.com/apple-patches-tens-code-execution-vulnerabilities-macos

2.4.2、APT 駭侵團體以最新 macOS 後門惡意軟體發動攻擊

資安廠商發現一起與 APT 駭侵團體有關的後門惡意軟體攻擊行動，利用偽裝的 Word 檔案夾帶指令檔，欺騙 macOS 用戶安裝後門惡意軟體並竊取機敏資訊。

資安廠商趨勢科技，日前發現一起與 APT 駭侵團體有關的後門惡意軟體攻擊行動；駭侵者利用偽裝的 Word 檔案夾帶指令檔，意圖欺騙 macOS 用戶安裝後門惡意軟體，竊取機敏資訊並發動後續攻擊行動。

趨勢科技的資安研究人員在報告中指出，該公司截獲的惡意軟體取樣，會偽裝成一個 Microsoft Word 檔案，但事實上是一個經由 zip 壓縮的程式碼安裝包；這個安裝包的檔名中含有一些特殊字元，以逃避某些防毒防駭軟體的偵測。

用戶如果點擊這個偽裝的 Word 檔，實際上會執行一段 shell script 指令碼；這段指令碼會下載後續的惡意軟體，並且更改檔案屬性，並試圖自我刪除以隱匿蹤跡；最後會在用戶的 macOS 系統中安裝後門惡意軟體，將各種系統配置資訊上傳到駭侵者布署的控制伺服器，同時接受指令，發動進一步的駭侵攻擊。

趨勢科技說，根據其惡意軟體使用的程式碼片段，以及檔案中使用越南文來看，該惡意攻擊可能與著名的 APT 駭侵團體 APT32（又名 OceanLotus）有關；該團體於 2020 年曾被發現試圖竊取中國的 Covid-19

相關資訊。

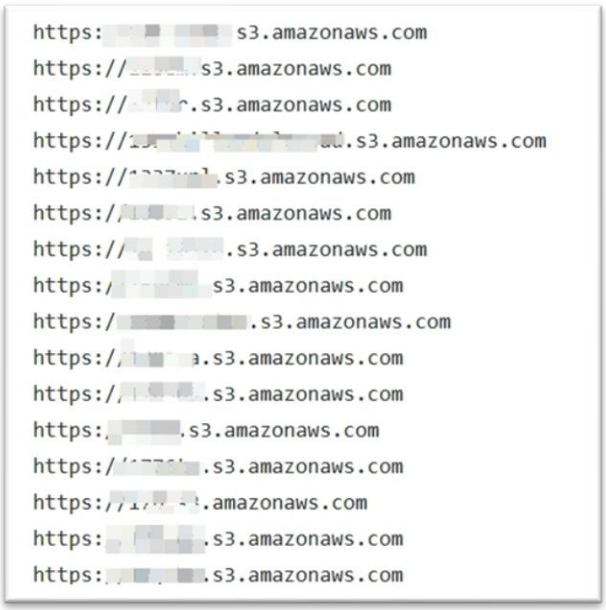
趨勢科技呼籲所有使用者，不要開啟可疑對象寄送的任何檔案，特別是公私機構常常是這類駭侵者的攻擊目標，應加強內部的資安教育訓練，隨時更新軟硬體系統，並且加強資安防護能力。

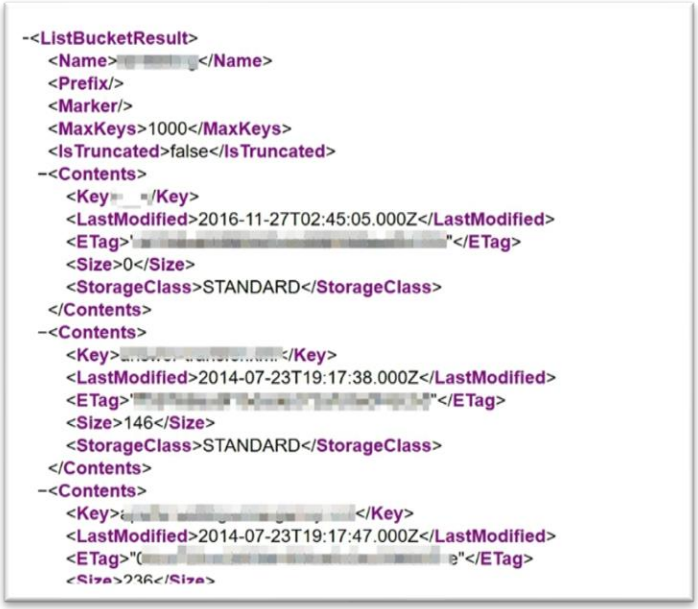
- 資料來源：
  1. https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html
  2. https://www.securityweek.com/vietnam-linked-cyberspies-use-new-macos-backdoor-attacks

2.4.3、超過四萬筆 Amazon S3 的 public bucket URL 被公開

TWCERT/CC 近日接獲情資，超過四萬筆 Amazon Simple Storage Service(Amazon S3)的 public bucket URL 已被公開於 GitHub。

Amazon S3 是一種雲端儲存服務，通常拿來備份伺服器、日誌及檔案。Amazon S3 雖然設定 public bucket，但還是需要知道 URL 才能下載。本次情資的揭露可能讓有心人士透過 URL 下載檔案，甚至包括帶有敏感的個人隱私資料。其手法可透過 http://[bucket_name].s3.amazonaws.com/<Key>對檔名為 Key 的檔案進行下載。





- 建議措施：

1.修改 AWS Identity and Access Management（IAM）Policy 來限制訪問的對象。

2.修改設定以禁止 Amazon S3 公用存取。

- 資料來源：

1. https://aws.amazon.com/tw/s3/faqs/
2. https://aws.amazon.com/tw/premiumsupport/knowledge-center/secure-s3-resources/

2.4.4、Canon 遭到勒贖攻擊，部分企業資料遭竊

Canon 在美國的分公司，於今年年中遭到勒贖攻擊，且有部分企業資料遭竊。

全球光學暨影像產品大廠 Canon，其美國分公司於今年年中遭到勒贖攻擊，且有部分企業資料遭竊。

Canon 在聲明稿中表示，該公司的內部網路與資料伺服器，於今年 7 月 20 日至 8 月 6 日之間，遭到未經授權的不當存取；Canon 於今年 11 月展開內部調查，發現該公司自 2005 到 2020 年間的員工資料遭竊。

被竊的員工資料中，包含多項個資欄位，例如姓名、社會安全碼、駕照號碼、身分證字號、金融開戶帳號、數位化的簽名，以及生日等。

該資料不只包括 Canon 員工，也包括員工家屬和相關受益人的資料在內。

雖然 Canon 並未在其聲明中透露攻擊相關的細節，以及誰是可能的攻擊者，但目前已停止運作的 Maze 駭侵團體，曾在今年 8 月時宣稱已經駭入 Canon 公司，並且在暗網上公布了約 2.5GB 的部分竊得檔案樣本；這批樣本據稱是總竊得資料量的 5%。

在 8 月 Canon 遭到攻擊時，Canon 的部分對外網站曾經停止服務達數日之久，當時有部分客戶存於該公司雲端服務的影像檔遭到波及而損毀，但並未外洩。

Canon 在日前發出的聲明中指出，駭客可能會利用這批竊得的員工個資，進行多種詐騙，例如偽裝成公務或司法機關，利用這些資料，要求個別員工提供更多個資、或是製作假證件或開立人頭戶，導致受害者遭到調查或原有帳戶被凍結等。

- 資料來源：
  1. https://www.usa.canon.com/internet/portal/us/home/explore/securityincident
  2. https://www.bankinfosecurity.com/canon-ransomware-attack-exposed-employee-data-a-15476
  3. https://www.databreachtoday.com/maze-reportedly-posts-exfiltrated-canon-usa-data-a-14813?

2.4.5、資安廠商 FireEye 本身也遭駭侵攻擊，攻擊者疑有特定國家支持

全球知名資安大廠 FireEye 也遭駭侵團體攻擊，該公司認為攻擊者可能由特定國家的支持。

全球知名資安大廠 FireEye，近日發表資安通報，指出該公司近期也遭駭侵團體攻擊；由於攻擊手法的縝密與技術力，該公司認為攻擊者極可能由特定國家的支持。

FireEye 於報告中指出，該公司發現遭到某駭侵團體入侵，目標是該公司內部用以模擬駭侵攻擊的「紅隊」用以發動模擬攻擊，並且評估客戶資安防護能力使用的內部工具；FireEye 指出目前沒有觀察到這些工具被用以發動其他駭侵攻擊的跡象。

這次針對 FireEye 的攻擊，同時還針對 FireEye 內部的各種系統發動攻擊，試圖取得存取權限，並且試圖收集 FireEye 承包的美國政府資安專案相關資訊；FireEye 指出，目前沒有觀察到這些資料遭竊的現象；一些該公司的資安防護相關 metadata 資訊與客戶相關資料，也並未在這波攻擊中遭到竊取。

FireEye 董事長兼執行長 Kevin Mandia 在向美國證管會提出的報告中說，該公司發現這次攻擊使用的手法十分成熟，而且經過充分準備與嚴格執行紀律，具有世界級的水準；該公司因此認為攻擊者背後必然有特定國家勢

力的支援。

目前 FireEye 正在與美國聯邦調查局、微軟公司合作調查整起攻擊事件。

- 資料來源：
  1. https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html
  2. https://www.sec.gov/ix?doc=/Archives/edgar/data/1370880/000137088020000037/feye-20201208.htm
  3. https://www.bleepingcomputer.com/news/security/fireeye-reveals-that-it-was-hacked-by-a-nation-state-apt-group/

2.4.6、FireEye、微軟與 GoDaddy 合力對抗 SolarWinds 後門攻擊

為對抗近來造成嚴重衝擊的 SolarWinds 後門攻擊行動，FireEye、微軟與 GoDaddy 聯合起來，共同對抗該攻擊行動，避免其惡意軟體持續蔓延。

為對抗近來造成嚴重衝擊的 SolarWinds 後門攻擊行動「Sunburst」，FireEye、微軟與 GoDaddy 共同成立聯合行動組織，依各公司的不同專長，一同對抗該攻擊行動，避免其惡意軟體持續蔓延。

據專業資安媒體 BleepingComputer 報導指出，FireEye 在日前公布了一份關於 Sunburst 攻擊行動的分析報告，報告中明確列出 Sunburst 如何利用供應鏈攻擊手法進行惡意軟體的植入，以及其後門的運作方式；報告並指出 Sunburst 成立了一台控制伺服器，用以接受駭侵團體的指令，並控制受到木馬植入的受害設備。

該報告同時也列出了多個 IP 位址，一旦控制伺服器發現有來自這些 IP 的回傳資訊，就會立即停止來自這批 IP 裝置中惡意軟體的運作。

在 12 月 15 日，在域名商 GoDaddy 的協助下，該控制伺服器使用的網域名稱控制權被微軟取得，同時將其對應 IP 轉移到微軟控制的 IP；這使得微軟得以掌握控制伺服器與惡意軟體間的通訊，並且進行進一步的分析，同時阻止該惡意軟體的進一步感染。

不過 FireEye 也表示，此波攻擊行動幕後的 APT 駭侵團體 Cozy Bear，也很快針對防制行動做出因應，正在積極建置新的攻擊網路基礎建設，以繼續控制遭到植入木馬的受害系統。

- 資料來源：

1. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
2. https://krebsonsecurity.com/2020/12/malicious-domain-in-solarwinds-hack-turned-into-killswitch/
3. https://www.bleepingcomputer.com/news/security/fireeye-microsoft-create-kill-switch-for-solarwinds-backdoor/

2.4.7、Spotify 再度發生資料外洩事件，部分用戶需更改密碼

串流音樂服務大廠 Spotify 日前通知部分用戶，其原本使用的密碼被重置，應重新設定新密碼；原因是該公司再度發生資料外洩事件。

串流音樂服務大廠 Spotify 日前發送通知給部分用戶，告知其原本使用的密碼被重置，應重新設定新密碼；原因是該公司再度發生資料外洩事件。

Spotify 在寄給受影響用戶的 Email 中指出，該公司儲存的部分用戶資料，被外洩給該公司的某個合作伙伴；遭到外洩的資料欄位，包括登入用的 Email、密碼、用戶設定的顯示名稱、性別、出生日期等個人資訊。

Spotify 指出，在 11 月 12 日時，該公司發現其系統中的某個漏洞，造成部分用戶的帳號註冊資訊曝露給該公司的某個第三方合作伙伴；該公司推測整個漏洞的影響時間，自今年 4 月 9 日起，到發現問題的 11 月 12 日止，長達七個月以上。

Spotify 說，該公司已經修正這個系統錯誤，而且這些洩露給第三方合作伙伴的資料也沒有外流；然而 Spotify 除了要求被重置密碼的用戶更換密碼外，也建議用戶如果將同樣的登入資訊（登入用的 Email 與密碼）使用在其他網路服務時，也應一併更新密碼，以降低登入資訊外洩可能造成的資安風險。

事實上，Spotfy 近來屢次遭到駭侵攻擊；就在 Spotify 對外發布這波資料外洩事件的數日前，才發生過一個名為「Daniel」的駭侵者竊走 Spotify 站內最熱門歌手專頁的事件。數月前也發生過駭侵者利用在別處取得的其他服務用戶登入資訊，用以登入並竊取用戶帳號控制權的事件。

- 資料來源：
  1. https://oag.ca.gov/system/files/Copy%20of%20Spotify%20Breach%20Notice%20Letter%20%28CALIFORNIA%29.DOCX_.pdf
  2. https://threatpost.com/spotify-changes-passwords-data-breach/162256/
  3. https://portswigger.net/daily-swig/spotify-security-vulnerability-exposed-personal-data-to-business-partners

2.4.8、以色列大型保險公司 Shirbit 遭勒贖軟體攻擊

以色列大型保險公司 Shirbit 於本月初遭駭侵團體發動勒贖攻擊，要求贖款高達 200 枚比特幣。

以色列大型保險公司 Shirbit 於本月初遭駭侵團體「黑影」（Black Shadow）發動勒贖攻擊，要求贖款高達 200 枚比特幣。

據耶路撒冷當地媒體 The Jerusalem Post 報導，Black Shadow 一開始開價為 50 枚比特幣，但 Shirbit 沒有在駭客限定的時間之內支付贖款，Black Shadow 便在其「官方」Telegram 頻道中宣布，將贖款調漲四倍，同時公布部分該駭侵團體竊得的資料。

在 Shirbit 被公開的部分資料中，包括許多該公司員工與顧客的機敏資訊；駭侵者威脅如果 Shirbit 不支付贖金，這些資料將會逐步對外公開。

據當地媒體 Channel 12 Israel 指出，負責調查整起事故的政府單位，認為這起事件是由以色列境內的駭侵者所為，暫時沒有外國勢力支持的駭侵團體涉入的跡象；不過調查單位也證實，被洩露的資料確實是來自 Shirbit。

Shirbit 公司在對外界的聲明中，沒有提到任何這起攻擊事件的細節，僅表示被竊取的資料並不損及該公司顧客的權益；該公司也有完整的資料備份，目前也積極配合調查單位進行後續處理。

- 資料來源：
  1. https://www.jpost.com/israel-news/shirbit-hackers-demand-almost-1-million-in-ransom-money-to-stop-leaks-650995
  2. https://mundo.sputniknews.com/seguridad/202012041093722764-hackers-publican-informacion-personal-de-asegurados-israelies-tras-impago-de-rescate/
  3. https://news.bitcoin.com/black-shadow-hackers-demand-200-btc-ransom-from-israeli-insurance-giant-shirbit/

2.4.9、韓國大型零售業者 E-Land 遭勒贖攻擊，200 萬張信用卡資料疑遭竊取

韓國大型百貨零售業者 E-Land 長期遭勒贖軟體駭侵攻擊，駭侵者表示已自該公司竊得 200 萬張信用卡資訊。

韓國大型百貨零售業者 E-Land，自去年起長期遭勒贖軟體 Clop 發動勒贖攻擊；雖然該公司宣稱並無顧客資料流失，但駭侵者表示已自該公司竊得 200 萬張信用卡資訊。

E-Land 是韓國最大百貨零售業者之一，旗下擁有多家連鎖服飾店、家居用品賣場、百貨公司與折扣商場；然而自去年以來，該公司一直遭受勒贖攻擊之苦，2020 年 11 月更是因此關閉 23 家 NC Department Store 百貨門市與其他品牌店面。

該公司執行長徐昌賢於新聞稿中宣稱，勒贖攻擊並未造成客戶資料的損失，因為客戶資料與其他該公司的機敏資料，均加密儲存於其他未受攻擊的獨立伺服器內；然而根據 BleepingComputer 自 Clop 駭侵團體取得的資訊指出，該團體在駭入 E-Land 的一年多期間，透過植入於 POS 系統的惡意軟體，已經取得超過 200 萬張信用卡 Track 2 的卡片資訊。

Clop 駭侵團體植入在 E-Land POS 系統的惡意軟體，會在顧客刷卡時自 POS 中竊取卡片資訊，並傳輸到駭侵者架設的控制伺服器中；Clop 取得的 Track 2 信用卡資訊，其中包括信用卡卡號、信用卡到期日，但不包括信用卡

CVV 安全碼，因此僅能用於製造偽卡，在實體店面盜刷。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/ransomware-gang-says-they-stole-2-million-credit-cards-from-e-land/
  2. https://www.bleepingcomputer.com/news/security/ransomware-forces-e-land-south-korean-retail-giant-to-close-stores/
  3. https://www.elandretail.com/service/customer_center_03.do?bbsID=380002&boardID=BID00000000000000377

2.5、軟硬體漏洞資訊

2.5.1、資安專家發現 RTA 工業用網路卡存有嚴重資安漏洞

資安專家發現 RTA 工業用網路卡其控制軟體存有嚴重資安漏洞，可導致駭侵者攻擊工業製造控制系統。

資安廠商 Claroty 旗下的資安研究人員，日前發表研究報告，指出美國工業用網通設備大廠 Real-Time Automation 製造的工業用乙太網路卡 499ES，其控制軟體存有一個嚴重的資安漏洞，將可導致駭侵者遠端攻擊使用此設備的工業製造控制系統。

RTA 499ES 網路卡廣泛使用於各種工廠的自動化生產設備之中，Claroty 的報告指出，該漏洞可使駭侵者發動 DoS 攻擊，甚至在某些情形下可以遠端執行任意程式碼。

這個漏洞的 CVE 編號為 CVE-2020-25159，其 CVSS 危險程度評分高達 9.8 分（滿分為 10 分），所有在 2020 年 11 月 21 日之前發行的 RTA 499ES EtherNet/IP 網路卡源碼堆疊版本 2.28 前的舊版本，都存有這個嚴重漏洞。

由於採用這款工業用網卡的廠商眾多，美國資安與基礎設施安全局（Cybersecurity and Infrastructure Security Agency）也特別發布資安通告，敦促所有採用此款設備的廠商，應盡速將 499ES 的控制軟體升級至最新

版本，同時盡可能避免使用此網路設備的製造系統直接連上網路，最好將整套系統與外部網路完全隔離，以避免駭侵者透過外部網路發動攻擊。

- CVE 編號：CVE-2020-25159
- 影響產品/版本：所有在 2020 年 11 月 21 日之前發行的 RTA 499ES EtherNet/IP 網路卡源碼堆疊版本 2.28 前的舊版本
- 解決方案：
  1. 建議設備相關用戶立即將 RTA 499ES 網路卡的控制軟體升級到最新版本 2.28。
  2. 建議將系統與外部網路隔離，避免使用此網路設備的製造系統直接連上網路。

- 資料來源：
  1. https://www.claroty.com/2020/11/17/blog-research-rta-enip-stack-vulnerability/
  2. https://us-cert.cisa.gov/ics/advisories/icsa-20-324-03
  3. https://securityaffairs.co/wordpress/111646/ics-scada/automation-systems-opens-flaw.html

2.5.2、Dell Wyse Thin Clients 的資安漏洞讓駭客擁有控制權

Dell 近期修補了兩個關於 Dell Wyse Thin Clients 的資安漏洞。Dell Wyse Thin Clients 是一種適合用來連接遠端桌面的小型設備。資安廠商 CyberMDX 表示，這些漏洞使得攻擊者可遠端執行任意程式碼、存取設備上所有文件與憑證。

這兩個漏洞的 CVSS 漏洞嚴重性得分均為 10 (滿分 10 分)。

第一個漏洞 (CVE-2020-29491) 是 Wyse Thin Clients 設備對 FTP 伺服器進行連線時，並未進行身分驗證，使攻擊者可以存取其他設備的組態設定。

CyberMDX 表示，藉由這個漏洞發起攻擊非常容易，攻擊者僅須透過 FTP 將更改後的組態設定檔上傳到 FTP 伺服器。唯一可能阻擋攻擊的方法是通過身分驗證才能透過 FTP 上傳檔案，但預設情況下，身分驗證功能是被關閉的。

第二個漏洞 (CVE-2020-29492) ，則是儲存這些組態設定的 FTP 伺服器預設是允許任何人可以對組態設定進行讀取與寫入，攻擊者可透過該漏洞，讀取和寫入設備的組態設定。

Wyse Thin Clients 設備會透過組態設定的.ini 檔案中的系統相關參數，進行相關的系統配置，攻擊者可建立.ini 檔案或修改系統相關參數，進一步發起其他攻擊，例如啟用遠端操作軟體（Virtual Network Computing, VNC）以進行遠端控制、竊取遠端桌面憑證等。

所有使用 ThinOS 8.x 及更低版本的 Wyse Thin Clients 均會受到影響。Dell 已進行修補，使用者應盡速更新 ThinOS 至版本 9.x 以上。如果設備無法更新 ThinOS 至版本 9.x，建議關閉 FTP 伺服器，並採用其他遠端管理方式。

- CVE 編號：CVE-2020-29491、CVE-2020-29492
- 影響產品/版本：使用 ThinOS 8.x 及更低版本的 Wyse Thin Clients。
- 解決方案：更新至最新版本。

- 資料來源：
  1. https://www.cybermdx.com/vulnerability-research-disclosures/dell-wyse-thin-client-vulnerability
  2. https://threatpost.com/critical-bugs-dell-wyse-thin-clients/162452/

2.5.3、PlayStation Now 的資安漏洞，可讓駭侵者針對 Windows 玩家發動攻擊

全球玩家多達 220 萬的 PlayStation Now 遊戲服務，其所屬 Windows 應用程式遭資安專家發現一個漏洞；該漏洞可導致駭侵者藉以駭入玩家電腦，遠端執行任意程式碼。

發現此漏洞的資安專家 Parsia Hakimian 於今年五月發現這個漏洞；這個漏洞可讓未經授權的駭侵者發動程式碼注入攻擊。

PlayStation Now 安裝在 Windows 電腦中的 psnowlauncher.exe 在執行後，會透過 AGL Electron 應用程式，於本機連接埠 1235 啟動的 WebSocket 伺服器；駭侵者可利用 AGL 連上存有惡意軟體的網站，載入任意的惡意 JavaScript 程式碼，因為 AGL 不會針對連線 URL 進行必要的檢查。

Hakimian 說，駭侵者可以利用多種方法誘使用戶點按惡意連結，例如透過釣魚郵件、遊戲社群或聊天室來散布惡意網站的 URL。這個漏洞會影響的 PS Now 版本為所有執行在 Windows 7.1 SP1 與後續 Windows 版本的 PS Now 11.0.2 與較舊版本。

Hakimian 在今年五月透過 HackerOne 的漏洞有獎徵答比賽，將這個漏洞回報給 Sony 公司；Sony 隨即在六月底就解決了這個漏洞。

- 影響產品/版本：執行於 Windows 7.1 SP1 與後續 Windows 版本的 PS Now 11.0.2 與較舊版本
- 解決方案：更新至最新版本 PS Now

- 資料來源：
  1. https://hackerone.com/reports/873614
  2. https://twitter.com/CryptoGangsta/status/1334944816375812096
  3. https://www.bleepingcomputer.com/news/security/playstation-now-bugs-let-sites-run-malicious-code-on-windows-pcs/

2.5.4、VMware 修復 Workspace One 與其他平台的 0-day 資安漏洞

VMware 日前針對旗下 Workspace One 與其他平台產品被發現的 0-day 資安漏洞，推出修補程式；相關產品用戶應儘速加以更新。

獲得修補的 0-day 漏洞，其 CVE 編號為 CVE-2020-4006，駭侵者只要取得能夠存取內網的 port 8443，即可利用此漏洞注入指令，不但能提升自身執行權限，更可遠端執行任意程式碼。

此一漏洞在發現初期的 CVSS 危險程度評分高達 9.1 分（滿分為 10 分），被評為「危險」等級；然而在後續的研究中調降其評分至 7.2 分，等級亦降為「重要」等級，原因在於後續研究指出，駭侵者必須先取得系統管理密碼，才能利用此漏洞，大大提高駭侵者利用此漏洞發動攻擊的難度，因而調降其評分。

不過，駭侵者若能利用暴力試誤法或社交攻擊方式，設法取得密碼，未曾更新 VMware 相關產品平台的用戶，就仍然存有高度被攻擊的風險。

受此漏洞影響的產品包括 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，用戶應立即下載安裝 VMware 提供的官方資安修補工具，以修補此一漏洞，降低遭駭侵者用以

攻擊的可能。

- 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

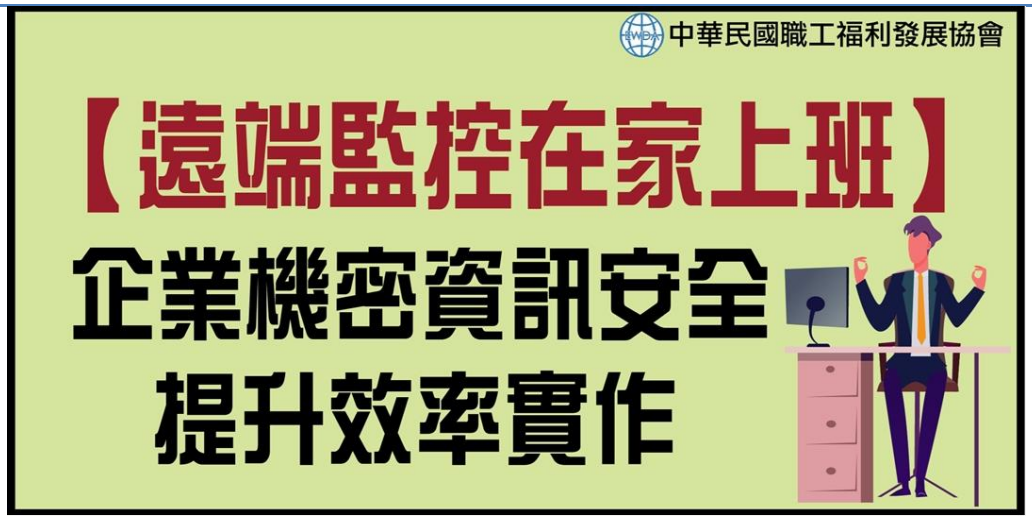
  VMware Identity Manager Connector Linux 版 3.3.1 與 3.3.2

  VMware Identity Manager Connector Windows 版 3.3.1 到 3.3.3
- 解決方案：下載安裝 VMware 提供的官方資安修補工具

- 資料來源：
  1. https://kb.vmware.com/s/article/81754
  2. https://www.vmware.com/security/advisories/VMSA-2020-0027.html
  3. https://threatpost.com/vmware-fix-critical-zero-day-bug/161896/

第 3 章、 資安研討會及活動

1 月例會_物聯網應用與資訊安全	
活動時間	**2021/1/29(五)，下午 2:00～5:00**
活動地點	**宏電科技-ATEN CIC Room 互動應用展示中心** **地址：台北市信義區基隆路一段 143 號 3 樓**
活動網站	**https://www.caa.org.tw/coursedetail-3447.html**
活動概要	**主辦單位：中華民國電腦稽核協會、ISACA Taiwan Chapter** 報名時間:2020-12-07~2021-01-28 演講大綱：1.物聯網發展與應用 2.資訊安全近期因應 3.未來挑戰與建議 主講講師：余啟民 東吳大學 法學院暨法律學系 副教授/科技暨智慧財產權法律研究中心 主任 證照：BS 10012 專長：數位資訊法律、國際商事法律、英美契約法 適合對象：本協會之會員、稽核人員、資訊安全人員、IT、MIS 部門等或對此相關議題有興趣者 報名費用：本會會員(含團體會員公司同仁)免費，非會員 500 元 報名名額：限額 50 名，額滿為止，請儘速報名！ 參加本活動可獲得 3 小時 CISA、CISM、CGEIT、CRISC、CIA 等進修時數

【遠端監控在家上班】企業機密資訊安全及提升效率實作	
活動時間	**2021-02-19(五) 09:30 ~ 16:30**
活動地點	**台北市中正區懷寧街 43 號 5 樓**
活動網站	**https://www.accupass.com/event/2008260330053701468420**
活動概要	 **主辦單位：中華民國職工福利發展協會** 透過此獨家課程，您也將實際操作一系列高效應用工具，全方位的學習防止內外威脅，管控內外資安，並了解如何全面建立"密碼管理"、"加密安全文檔"避免被外部盜取機密，阻止勒索程式，根除遠端威脅，增加生產力。 ※本實作課程，授課現場將由老師帶領實操，請學員務必自備可無線上網的智慧型手機及筆電(平版)： 1.不需要事先註冊軟體，不需寫程式 2.手機(必備) 預載 LINE。 3.筆電(必備) 預載 Google chrome 瀏覽器 【課程效益】 本課程將針對企業機密資訊安全的操作進行深入的解說，包括資安監控工具前後台操作程序、法律須知。課程結束後，學員將對於防止內外威脅，管控內外資安，並了解如何全面合法員工監控，建立「密碼管理」、「加密安全文檔」 避免被盜取機密，有深刻的了解，並有能力自行操作！

第 4 章、 2020 年 12 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。

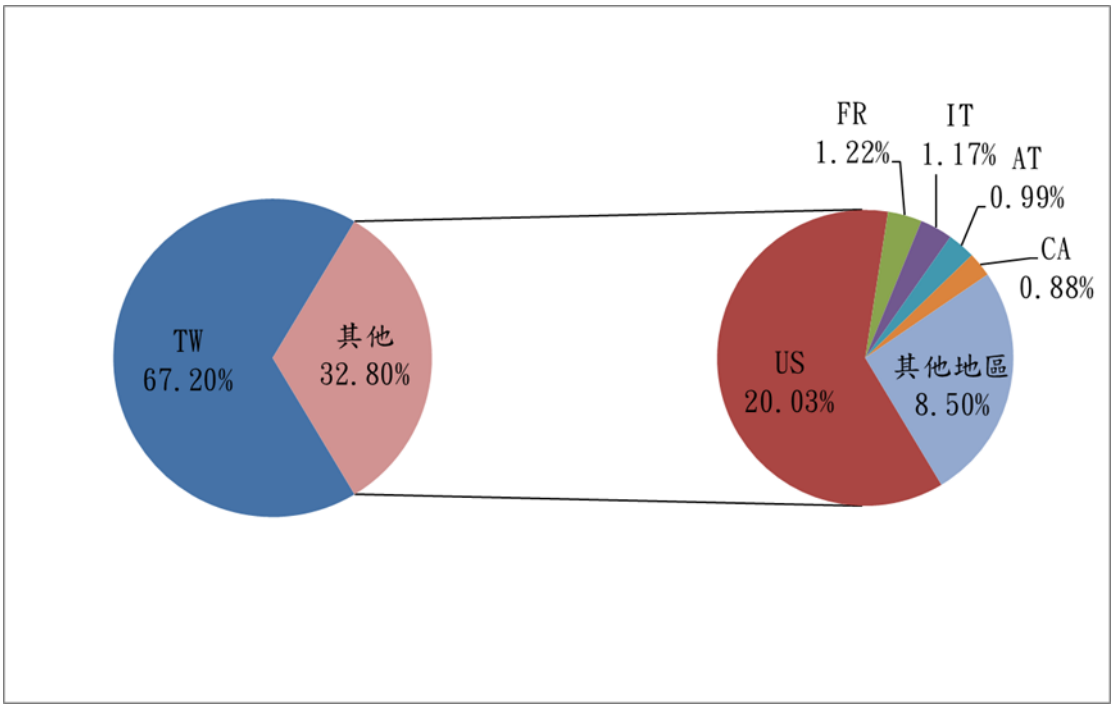


圖 1、分享地區統計圖

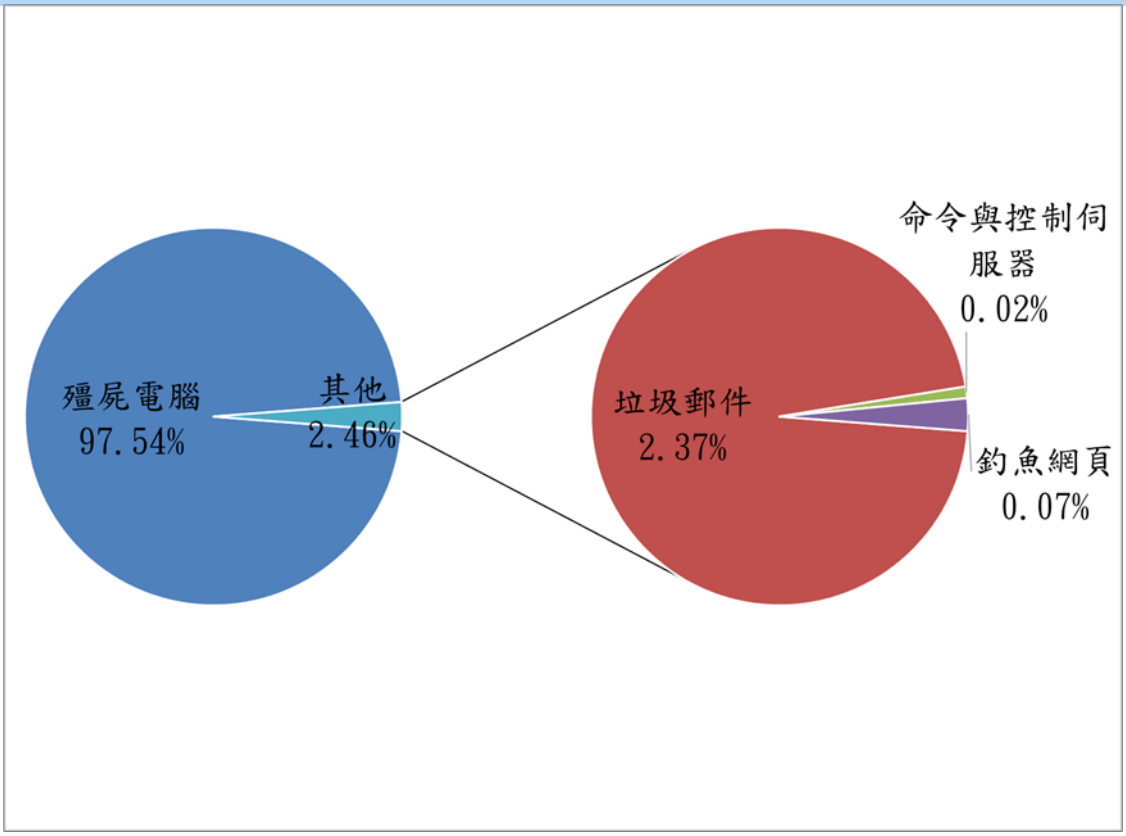


圖 2、分享類型統計圖

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：**2021 年 1 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**