TWCERT/CC 資安情資電子報

2020 年 5 月份

目錄

第 1 章、 封面故事

微軟修復 Teams 重大資安漏洞：一張 GIF 圖檔可綁架整個單位的 Teams 帳號

資安廠商發現 Microsoft Teams 的資安漏洞，駭侵者可利用該漏洞傳送一張 GIF 圖檔，受害者讀取後便會遭駭；駭侵者甚至可藉以散布這種攻擊手法，取得整個單位的 Teams 帳號控制權限。

資安廠商 CyberArk 發現 Microsoft Teams 的一個資安漏洞，並發展出概念證實的攻擊手法，證明駭侵者可利用該漏洞傳送一張 GIF 圖檔來攻擊 Microsoft Teams。

該公司展示的攻擊方法，係利用 Microsoft Teams 的 DNS 組態設定漏洞；攻擊者只要先劫持兩個 Microsoft Teams 的子網域，取得兩個驗證用的 token，再傳送一張 GIF 圖檔給受害者，受害者讀取後便會遭駭。

受害者的 Microsoft Teams 被駭侵者接管後，駭侵者即可取得受害者帳號內的資訊和檔案，甚至可藉由呼叫 Teams API 進行各種操作，散布這種攻擊手法，最後取得整個單位的 Teams 帳號控制權限。

CyberArk 指出，駭侵者除了可以取得用戶在 Microsoft Teams 中的共享檔案外，也能取得成員間的對話記錄，甚至如登入資訊、機密檔案等資訊。

在 CyberArk 提出的報告中，包括一支示範影片，詳細說明整個漏洞機制與攻擊示範流程。

這個漏洞同時影響 Microsoft Teams 的網頁版與桌機版應用程式。

CyberArk 於三月將此一發現向微軟通報，微軟很快就修復了這兩個設定出現問題導致易受攻擊的子網域，並且在日前釋出修補程式，修復了這個資安漏洞。

- 資料來源：
  1. https://www.cyberark.com/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams/
  2. https://threatpost.com/single-malicious-gif-opened-microsoft-teams-to-nasty-attack/155155/
  3. https://www.zdnet.com/article/this-is-how-viewing-a-gif-in-microsoft-teams-triggers-account-hijacking-bug/

第 2 章、 遠距辦公資安專區

2.1、遠距辦公資安小錦囊

2.1.1、企業篇

近期因疫情影響，許多企業開始提出遠距辦公的因應措施，以下為企業應為員工遠距工作所需的準備：

1、使用高安全性的設備、系統與軟體

企業須選用安全之設備、系統與軟體，提供員工遠距作業使用，並留存日誌以檢核異常使用。使用安全的網路連線(ex:VPN)和安全的遠端會議系統進行討論，可避免機敏資訊外洩。

2、多重認證機制

建立多重認證，並要求員工在遠距工作時，透過多重身份認證後，方能操作企業內部系統。

3、定期審核授權狀況

企業需定期確認使用者帳號及其權限，避免有陌生帳號或不當被利用之帳號竊取內部資訊。

4、強化資安政策，提高資安警覺

強化企業既有的資安政策，設定資安問題處理流程以利快速處理各種突發的資安狀況，減低損害。且定期提醒員工在家工作資安相關注意事項，提升企業全體人員的資安警覺。

5、定期更新與備份

定期更新系統版本，以獲得最新資安防護，並需定期備份資料於安全設備中，減少資安事件發生時的損失。

2.1.2、個人篇

因疫情影響，企業開始實施或模擬在家辦公的應變措施，以下為員工在家遠距工作指南：

1、時時保持警覺

隨時對惡意郵件或軟體保持警覺心，看見有疑慮的郵件或連結，請勿點擊。如遇可能的資安問題即時警示相關人員進行確認與處理。

2、使用安全的網路設備

使用安全的家用網路以及無已知漏洞的網路連線設備。

3、避免被竊取資訊的可能

設定裝置閒置時鎖定並進行磁碟資訊加密，線上會議結束後，務必將相關設備關閉(ex:麥克風、視訊鏡頭)。

4、及時更新軟體避免漏洞

及時更新使用之系統與各應用軟體的版本。

5、使用強密碼

相關密碼設定使用強密碼，含英文大小寫數字，建議不使用生日、電話等易破解之資訊作為密碼。

遠距辦公資安小錦囊

個人篇

時時保持警覺

隨時對惡意郵件或軟體保持警覺心，看見有疑慮的郵件或連結，請勿點擊。如遇可能的資安問題即時警示相關人員進行確認與處理。

避免被竊取資訊的可能

設定裝置閒置時鎖定並進行磁碟資訊加密，線上會議結束後，務必將相關設備關閉(ex:麥克風、視訊鏡頭)。

及時更新軟體避免漏洞

及時更新使用之系統與各應用軟體的版本。

使用安全的網路設備

使用安全的家用網路以及無已知漏洞的網路連線設備。

使用強密碼

相關密碼設定使用強密碼，含英文大小寫數字，建議不使用生日、電話等易破解之資訊作為密碼。

官網：https://twcert.org.tw/
FB：台灣電腦網路危機處理暨協調中心 - TWCERT/CC
E-MAIL：twcert@cert.org.tw

2.1.3、遠距會議篇

越來越多企業單位讓員工遠距辦公，來因應企業可能遭遇之各種緊急事件。因此遠端視訊會議(video-teleconferencing,VTC)相關系統的使用量遽增，引發相關資安議題。身為遠端視訊會議的使用者，我們該如何做好資安防護呢？以下八點資安防護提醒：

1、選用無資通安全疑慮的視訊會議軟體

企業選用遠距會議軟體時，需考量其安全性，避免使用有資安漏洞和疑慮的軟體，落實資安防護。

2、選擇可信賴的下載軟體管道

在可信賴的官方網站或 app store 下載軟體，以避免安裝到含有惡意程式的偽冒軟體或 APP。

3、謹慎確認會議邀請與連結

來路不明的會議邀請或連結，極有可能是惡意連結，請勿點選避免受駭。

4、限制會議參與者

所有的會議建議設定密碼限制，並由會議發起人於會議開始前確認參與成員的身分。

5、避免在公開社群分享會議連結

請直接提供給與會者連結，如此可以最大限度地避免不相關的人員得知會議並混入會議中竊取商業機密。

6、謹慎使用螢幕共享的功能

會議中若使用螢幕共享的功能，需限制特殊指定人士才可使用並共享。

7、更新至最新的軟體版本

視訊會議軟體皆會因應各種資安漏洞進行修補更新，隨時更新到最新版本，可以確保使用上的安全。

8、確保使用設備的安全性

使用者參與線上視訊會議的資訊設備以及網路連線方式，皆需符合企業訂定之資安標準(ex: 限定使用資訊設備、不使用免費網路連線等)。

遠距辦公政策實施同時，企業與員工應積極做好資安準備，以避免發生資安事件，守護企業重要商業資產的安全性。

2.1.4、VPN 安全篇

越來越多企業單位讓員工遠距辦公，來因應企業可能遭遇之各種緊急事件。虛擬私人網路(Virtual Private Network, VPN) 可讓遠距工作者與企業之間建立專屬加密通道，以保障遠距存取企業內部網路的安全性。隨著 VPN 系統的使用量遽增，資安議題亦更為重要。

關於如何做好 VPN 的資安防護呢？以下六點資安防護提醒：

1、選擇信譽良好的 VPN 廠商

由於 VPN 系統可直接存取企業內部網路，因此若 VPN 廠商信譽不良，可能不當存取企業機敏資訊或日誌紀錄，導致機敏資訊洩漏。

2、具備完善的加密機制

選擇足夠安全加密機制，進行資訊的加密傳輸，如 RSA-2048 或 AES-256 等，以避免資料外洩。

3、建立多重認證機制

建立多重認證，並要求員工在遠距工作時，透過多重身份認證後，方能進行後續作業。

4、搭配防火牆或防護軟體

使用的 VPN 伺服器建議搭配相關防護措施，阻擋未經授權的連線，避免惡意程式流向主機。

5、監控 VPN 的使用狀況

監控並記錄 VPN 的使用狀況，定期檢核日誌以及早發現異常使用。

6、避免使用免費 VPN 服務

免費的 VPN 服務內含較多廣告，部分廣告有夾帶惡意程式的風險，亦有

個資外洩的疑慮。

遠距辦公政策實施同時，企業與員工應積極做好資安準備，以避免發生資安事件，守護企業重要商業資產的安全性。

2.2、COVID-19 進階持續威脅性組織，加劇遠距辦公資安威脅

COVID-19 網絡犯罪和進階持續威脅性組織，加劇遠距辦公資安威脅

（CISA 版權所有，授權 TWCERT/CC 翻譯）

一、摘要

美國國土安全部（DHS）網絡安全和基礎設施安全局（CISA）和英國國家網絡安全中心（NCSC）聯合針對：用目前 COVID-19(武漢肺炎) 網絡犯罪和進階持續威脅性組織（APT），進行網路攻擊提出警訊。

CISA 和 NCSC 注意到：駭客組織開始利用與 COVID-19 為主題的網路攻擊；同時，遠距辦公使得易受攻擊網路服務（如 VPN）的使用，加劇了對個人和組織的資安威脅。這些進階持續威脅性組織和網絡犯罪針對個人，中小企業和大型組織，利用 COVID-19 的相關主題，進行網路詐騙和釣魚電子郵件。本警訊解釋這些與 COVID-19 相關的惡意活動，並提供了一些個人和組織能遵循的實用建議，以減少受影響的風險。

由於攻擊的情況快速發展，該警訊未對所有的 COVID-19 相關惡意活動進行分類，個人和組織應採取積極性的措施來自我防護。

二、技術性細節

(一)、攻擊手法摘要

這些進階持續威脅性組織開始利用 COVID-19 疫情的大流行作為其主要攻擊手法的一部分，惡意人士通常會偽裝成可信任的單位，有時會偽裝成先前已被攻擊的單位，傳送以 COVID-19 為主題的釣魚訊息或惡意程式，犯罪者利用疫情來獲取商業利益並散布各種的勒索病毒和惡意軟體，以達到間諜活動、駭客活動、資訊竊取的長期目標。

接下來的數周或數月，進階持續威脅性組織可能繼續利用 COVID-19 的

大流行來從事活動。目前已觀察到的活動包括：

- 以 COVID-19 為誘餌的網路釣魚；
- 以 COVID-19 為誘餌的惡意軟體；
- 以 COVID-19 組成的網域名稱註冊；
- 針對遠端存取、遠端控制或遠端辦公基礎設施的攻擊。

惡意人士利用社交工程手法來誘導使用者進行特定操作，利用人性的弱點（例如好奇心和對疫情的恐懼）來誘使受害者從事以下操作：

- 開啟釣魚網站連結或下載內含釣魚連結的應用程式，或下載夾帶勒索軟體的惡意程式。例如：一個 Android 應用程式偽裝成疫情的最新資訊，試圖誘導使用者授權設備存取，以安裝名為「CovidLock」的勒索軟體。
- 開啟內含惡意軟體的檔案（附件）。例如以 COVID-19 為主題的內容，如：「武漢肺炎最新資訊」、「所在城市的最新疫情」、「緊急狀態」等。

為了營造真實感，惡意人士會在電子郵件中偽造發信者的資訊，讓其看上去是來自從可信賴的來源，例如「世界衛生組織（WHO）」或「譚德賽」。在幾個案例中，惡意人士發送釣魚郵件，並包含偽冒的登入頁面，其他的案例包含偽裝人資部門並要求員工開啟郵件附件。這些附件可能以武漢肺炎或 COVID-19 為檔名，例如「總統與內閣通過由於武漢肺炎導致的預算刪減」。

(二)、網路釣魚

CISA 和 NCSC 皆觀察到大量利用上述社交工程技術的網路釣魚活動。其所使用的主旨包括：

- 2020 冠狀病毒最新資訊；

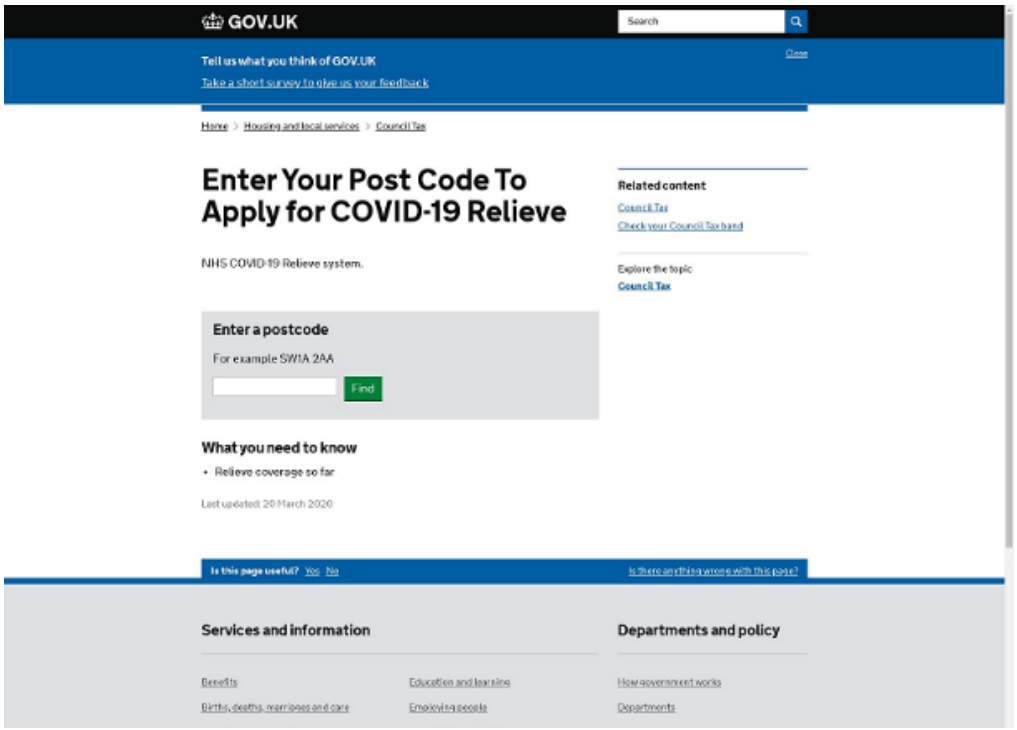
- 冠狀病毒最新資訊；
- 2019-nCov：所在城市的最新確診病例；
- 2019-nCov：所在城市疫情爆發（緊急）。

這些電子郵件可能要求從事行動，鼓勵受害者開啟惡意人士所架設的網站並提供有價值的資料（如使用者名稱和密碼、信用卡資訊和其他個人資料）。

(三)、簡訊釣魚

儘管大多數的網路釣魚皆透過電子郵件，NCSC 以察覺到一些嘗試其他手段來進行（例如手機簡訊）來進行的網路釣魚。

從前，這些釣魚簡訊通常使用財務上的誘因（例如政府補助或退稅）來做為誘餌。COVID-19 相關的釣魚活動則延伸自財務上的內容，特別是流行性疾病對財務的影響，以及政府在就業或經濟上的支援計畫。例如：有一系列的簡訊偽裝成英國政府，藉此收集關於電子郵件、地址、姓名、銀行帳戶等資訊，這些簡訊號稱來自 UKGOV 或與 COVID 相關，並包含了釣魚網站的連結。



如同上述示例，惡意訊息可能透過電子郵件以外的方式散布，除了簡訊，可能的方式包含 WhatsApp 和其他通訊服務。惡意人士可能繼續示財務相關內容來從事釣魚活動，具體而言，政府的新措施可能成為新的釣魚手段。

(四)、利用釣魚竊取登入資訊

許多惡意人士使用與 COVID-19 相關的網路釣魚來竊取使用者的登入資訊，這些電子郵件透過上述的社交工程手段，有時並輔與緊急用語來增加說服力。

如果使用者開啟網站，便會顯示一個包含密碼輸入欄位的詐欺網站，其可能與各種線上服務相關，包含 Google 和微軟的電子郵件服務，或是政府服務的登入頁面。

為了更進一步說服受害者，這些網站通常在網址中會包含與 COVID-19 相關的措辭，例如「corona-virus-business-update」、「covid19-advisory」、「cov19esupport」等，這些偽冒的網址使其看起來合法或類似知名網站，辨識惡意偽冒網站的唯一方法是檢查網站的網址。在某些情況下，惡意人士會

根據受害者來修飾這些偽冒的登入頁面。

倘若受害者在這些偽冒的頁面上輸入個人密碼或登入資訊，攻擊者便能存取受害者的網路帳戶，例如電子郵件，並獲得權限來存取個人的敏感資訊，或使用受害者的通訊錄來進一步散布釣魚郵件。

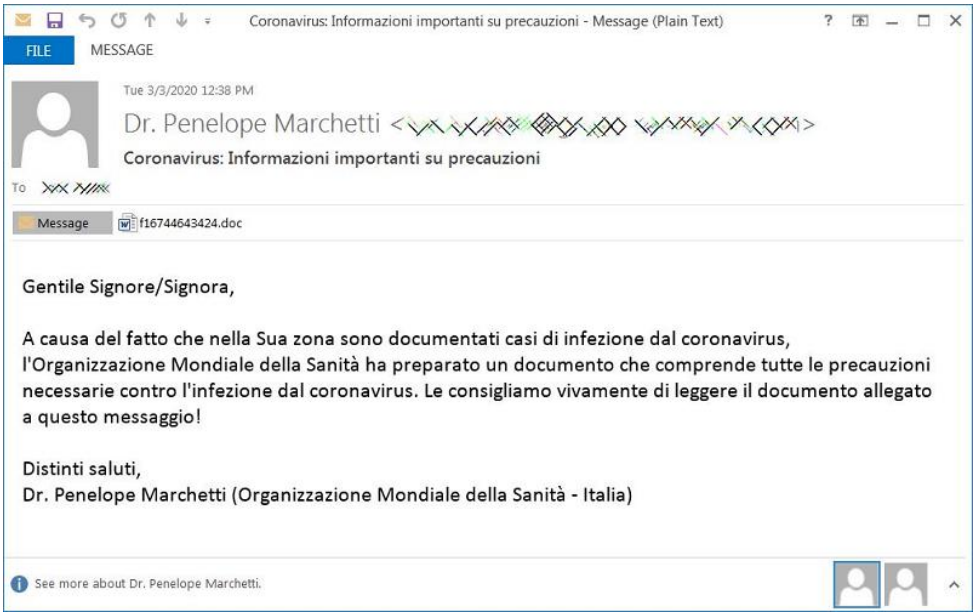
(五)、利用網路釣魚散布惡意程式

許多惡意人士使用 COVID-19 相關的網路釣魚來散布惡意程式。大多數的情況下，惡意人士會傳送電子郵件，便誘導受害者開啟附件或從網站連結下載檔案。當受害者打開連結時，將執行惡意程式，從而危害使用者設備。

NCSC 發現一個名為「Agent Tesla」的鍵盤輸入記錄程式，透過各種不同的電子郵件來散布。該電子郵件偽冒世界衛生組織秘書長譚得賽．阿德諾姆．格布瑞索斯博士的名義傳送，這個電子郵件的惡意活動開始於 2020 年 3 月 19 日。另一個類似的案例宣稱將提供溫度計和口罩以防範疫情，該郵件宣稱附加了這些用品的圖片，但實則夾帶了「Agent Tesla」惡意程式。

在其他案例中，郵件會包含 Excel 試算表附件，或包含網頁頁面連結下載試算表檔案，在這兩種情況底下，該試算表中皆包含巨集程式，如果使用者啟動了巨集，將執行嵌入式動態鏈接庫（DLL）並安裝「Get2 loader」惡意程式。「Get2 loader」已被發現內含「GraceWire」木馬程式。

另一個被稱為「TrickBot」的惡意程式也被發現。在一個案例中，一封針對義大利使用者的電子郵件宣稱為 COVID-19 的相關訊息，其附件檔案帶有一個內含惡意程序的巨集，一但巨集執行，JavaScript 將被啟動並在系統中執行名為「TrickBot」的惡意檔案。



在許多案例中，木馬程式（如 Trickbot 和 GraceWire）將下載其他惡意檔案，如遠端存取的木馬程式或桌面分享軟體、勒索軟體。為了最大化的提升受害者付款可能，犯罪人士通常會在一個機構承受更大的壓力時實施攻擊，在美國、西班牙和歐洲各地都有醫院或衛生組織收到勒索軟體影響。

個人和機構都應注意這些持續發展的釣魚活動，CISA 和 NCSC 都提供了能緩解惡意軟體和勒索軟體攻擊的指導方針。

(六)、危害遠距辦公的設備

許多組織已快速的建立了新的網路，包含 VPN 和相關的 IT 基礎設施。惡意人士會利用 VPN 和其他遠距辦公軟體中已知的漏洞。

在案例中，CISA 和 NCSC 發現有惡意人士掃描 Citrix 系統的已知漏洞，自 2020 年 1 月開始，CVE-2019-19781 已經被大範圍報導，CISA 和 NCSC 都提供了該漏洞的指導方針，並將繼續調查此漏洞。

已知的漏洞也影響許多 VPN 產品，如 Pulse Secure、Fortinet 和 Palo Alto。CISA 提供有關 Pulse Secure 漏洞的指導方針，而 NCSC 提供有關 Pulse Secure、Fortinet、Palo Alto 中的漏洞指南。

惡意人士嘗試利用使用量爆增的通訊平台，如 Zoom 和微軟 Teams，透過釣魚電子郵件，並夾帶如「zoom-us-zoom _ ##########.exe」、「microsoft

-teams_V#mu#D_##########.exe」的惡意檔案，CISA 和 NCSC 也發現到知名通訊平台網站的仿冒。此外，攻擊者也能劫持未建立安全措示（如密碼保護）或舊版未更新軟體的線上會議或線上課程。

遠距辦公的興起也到導致了微軟遠端桌面連線（RDP）的使用量增加，對於不安全的 RDP 終端從事的攻擊活動已被大量回報，近期的分析報告了不安全的 RDP 終端增加了 127%，RDP 使用的增加可能使未建立適當安全措施的 IT 系統更容易遭受攻擊。

三、緩解措施

(一)、針對個人的網路釣魚指導方針

NCSC 提供了幾個主要的技巧來辨識網路釣魚電子郵件：

- 權威性：寄件人是否宣稱為官方人士（例如銀行、醫院、律師或政府機關），犯罪者通常會假裝是重要人物或組織來誘導受害者從事特定行為。
- 急迫性：其是否告知回復的期限有限（要求 24 小時或立即回覆），犯罪者通常以罰款或其他負面的後果來威脅受害者。
- 情緒性：訊息是否令人恐慌、害怕、希望或好奇，惡意人士經常使用具威脅性的語言，尋求支持或嘗試令受害者主動了解更多。
- 稀有性：該訊息是否提供一些稀有的資源（如演唱會門票、錢財、醫療用品），害怕錯過一個好的交易或機會可能令受害者更快的回應。

(二)、針對組織或網路安全專業人士的網路釣魚指導方針

組織對網絡釣魚的防禦通常取決於使用者是否能夠發現網絡釣魚電子郵件。但是，能擴大防禦範圍並採用更多技術措施的組織可以提升對於網路釣魚攻擊的抵禦能力。

除了對於使用者的教育訓練，組織亦應考慮 NCSC 的指導方針。該指導

方針將措施分為四個階層，在階層上建立防禦措施：

1. 令攻擊者更難接觸使用者
2. 幫助使用者辨識並通報可疑的網路釣魚電子郵件
3. 保護組織以避免受到未偵測到之釣魚郵件影響
4. 快速處理事件

CISA 和 NCSC 也建議有時可以讓組織中部份的釣魚攻擊成功執行，這能幫助最小化事件的損害。

(三)、針對組織或個人使用通訊平台的指導方針

由於 COVID-19 疫情，越來越多的私人或組織開始使用通訊平台（例如 Zoom 和微軟 Teams）進行線上會議，惡意人士也在入侵未受密碼保護或未安裝修復的軟體和會議。

避免線上會議受到劫持的技巧：

- 不進行公開會議，要求輸入會議密碼或使用等候功能並控制使用者的進入。
- 不要在未受限制的公開社交媒體分享會議連結，應直接向特定人員提供會議連結。
- 管理螢幕分享選項。將螢幕分享更改為「僅限主機」。
- 確保使用的遠距軟體的最新版本。
- 確保遠距辦公政策滿足實體和資訊安全要求

四、版權聲明

第 3 章、 國內外重要資安事件

3.1、資安趨勢

3.1.1、口罩實名制 2.0 預購踴躍，注意防範詐騙簡訊

網路購物與跨國網購的盛行，詐騙集團也將其詐騙手法運用於網購。

通常商品到貨後會寄送簡訊通知顧客領取，於是詐騙集團利用此模式，發送「包裹已派發，請您及時查收」或是「快遞已郵寄請您及時查收」簡訊，並附上短網址，假冒快遞送貨以及包裹到貨通知，誘使民眾點擊網址以竊取財物、個資或植入惡意程式。

近期由於口罩實名制 2.0 線上預購踴躍，此種釣魚簡訊詐騙的模式又開始盛行，詐騙集團利用民眾擔心疫情想快點取得口罩的心情，誘導民眾點擊簡訊上的短網址查看物流進度。網址為詐騙集團製作的假網站，若民眾沒注意

是假網站並輸入個資或信用卡資訊，詐騙集團就會收到填寫的個資與信用卡資訊，導致民眾的信用卡被盜刷或是手機預設的小額付費功能遭盜用。甚至有網友點擊短網址後，手機被用來傳送大量簡訊，並且收到簡訊費用。如果民眾剛好有網購訂購商品，就更容易掉入詐騙集團設下的陷阱。

口罩實名制 2.0 線上預購口罩成功之後，民眾信箱會收到衛福部寄送的口罩預購成功通知信，信件中提醒民眾，政府「不會以簡訊或其他方式通知您繳費」，只會在到貨時收到簡訊取貨通知及序號，若要查詢繳費及取貨資訊，請至口罩預購系統查詢。

若民眾手機預設小額付款功能遭盜用，建議聯繫電信公司客服，關閉手機小額付款功能；若有輸入信用卡資訊、遭盜刷或是發現非本人刷卡的紀錄，應立即向信用卡公司反映並停用信用卡，以免造成金錢損失。建議民眾發現不明簡訊不要因為好奇心，點擊來路不明的網址或連結，若想查詢商品資訊，建議直接到購物網站查詢。進入可疑網站不輸入帳密、個資與金融資訊，務必確認網址及網站的真實性，以防進入駭客利用相似字組成與官方網站極為相似的假網站。建議民眾謹慎處理任何與金錢或個資相關的資訊以避免遭詐騙或撥打 165 反詐騙專線求證。

- 資料來源：
  1. https://agirls.aotter.net/post/57092
  2. https://news.ltn.com.tw/news/society/breakingnews/2868959
  3. https://udn.com/news/story/7320/4450386。

3.1.2、台灣情治單位協同微軟，破獲位在某公立圖書館內的僵屍網路攻擊跳板

國內情治單位與微軟合作，聯手打擊 Necurs 全球僵屍網路攻擊行動，發現某公立圖書館的 LED 燈具控制器之 IP 成為攻擊跳板。

國內情治單位於去年年中與微軟數位犯罪防範中心（Digital Crime Unit）合作，共同聯手打擊 Necurs 全球僵屍網路攻擊行動，並且發現國內某公立圖書館的 LED 燈具控制器之 IP 位址，竟成為攻擊跳板。

據台灣法務部調查局指出，這個 LED 燈具控制器本身並未遭駭，被駭侵者利用的弱點在於管理該控制器的外包廠商，並未正確設定管理用的 VPN，使該公立圖書館的 IP 被駭客用來當成跳板，發動各種駭侵攻擊。

這次在台灣查獲僵屍網路跳板的資安查緝行動，是微軟全球網路犯罪防治活動的一環；微軟指出，這個全球 Necures 打擊活動，在去年鎖定了四十萬個可疑的 IP 位址，監測其活動後，將鎖定範圍縮小到 90 個最可疑的 IP，確認駭侵者以僵屍網路透過這些 IP 發動各種攻擊活動。

微軟說，這些攻擊活動類型包括釣魚郵件、惡意軟體擴散、勒贖軟體遞送，以及發動分散式服務阻斷攻擊（DDoS）等。

根據微軟的統計數字，遭到 Necures 感染的某一裝置，在 58 天的觀察期間內，對外就發送了高達 3800 萬封垃圾郵件，寄給超過 4000 萬個潛在受害者。

今年三月初，美國微軟也宣布成功奪得 Necures 僵屍網路在美國本土的基礎設施控制權，阻止駭侵者進一步的攻擊活動。

- 資料來源：
  1. https://news.microsoft.com/apac/features/law-enforcement-and-microsoft-come-together-to-bust-a-major-malware-attack-in-taiwan/
  2. https://www.bleepingcomputer.com/news/security/microsoft-helped-stop-a-botnet-controlled-via-an-led-light-console/
  3. https://www.bleepingcomputer.com/news/security/microsoft-takes-control-of-necurs-us-based-infrastructure/

3.1.3、駭客散布勒索恐嚇郵件詐騙使用者

本中心近期接獲多起民眾收到勒索恐嚇郵件的通報。

該郵件宣稱已掌握收件人過去 180 天在電腦網路上的所有活動，如瀏覽過成人網站等，並已植入惡意軟體，來控制收件人的電腦鏡頭拍攝其私密影片。

若不想私密影片外流必須於開啟郵件的 24 小時內支付特定數量比特幣(千元美金以上)，否則將會隨機轉發給收件人的親朋好友。提醒民眾收到此類勒索恐嚇的詐騙郵件，請勿匯款。

郵件特徵：

1、郵件開頭為 Your password is XXXX.或是 I am aware, XXXX, is your password.可能隨機更換。

2、郵件內容表示對方已掌握帳號密碼、FB 和手機通訊錄，以及所有在電腦網路上的活動。

3、郵件內表明因為瀏覽成人網站，因此遭植入惡意軟體，駭客可以藉此控制電腦鏡頭拍攝不雅影片。

4、要求 24 小時內支付特定數量比特幣(數千美金以上)至指定的帳戶。

5、威脅若不支付就會將影片外流。

圖 1、詐騙郵件部分內容

I am aware, XXXXX, is your password.
I require your 100% attention for the next 24 hours, or I will ertainly make sure you that you live out of shame for the rest of your existence.
Hi, you don't know me. Yet I know just about everything concerning you. Your personal facebook contact list, phone contacts along with all the digital activity on your computer from past XXX days. Including, your self pleasure video footage, which brings me to the main reason why I'm composing this specific e-mail to you.
Well the last time you went to see the adult porn web sites, my spyware was activated in your computer which ended up shooting a eye-catching footage of your self pleasure play by triggering your cam.
(you got a exceptionally odd preference btw haha)
I own the full recording. If perhaps you think I am messing around, simply reply proof and I will be fonwarding the recording randomly to XX people you're friends with. It could be your friends, co workers, boss, mother and father (I don't know! My software program will randomly

TWCERT/CC 提供以下防護建議：

1、建議立即將有使用郵件中提到密碼的系統進行密碼更改，並且定期更換密碼。

2、建議使用 12 個字元以上且英文、數字與符號混合之密碼，應避免多個服務使用同一組密碼。

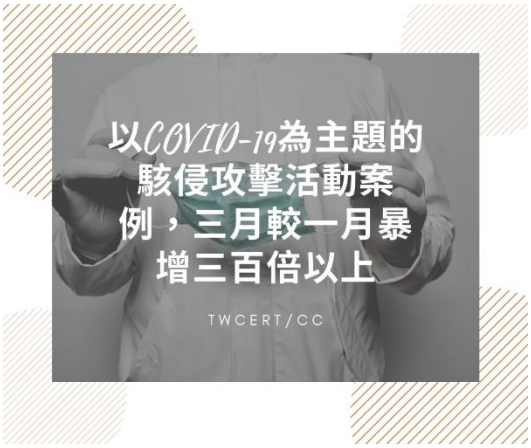
3、不隨意開啟不明身分寄件人的郵件，不點擊信件中的任意連結、附件或檔案，以避免遭植入惡意軟體。

4、建議個人及企業都應定期將系統進行更新，安裝防毒軟體與防火牆，確保系統、設備與軟體處於最新版本，避免受到攻擊而造成損失。

5、至 TWCERT/CC 官網 https://www.twcert.org.tw/tw/mp-1.html 進行資安通報。

- 資料來源：
  1. https://malwaretips.com/resources/we-have-installed-one-rat-software-into-your-device-blackmail-scam.352/
  2. https://www.facebook.com/twcertcc/posts/2253444848218581/

3.1.4、以 COVID-19 為主題的駭侵攻擊活動案例，三月較一月增三百倍以上



資安廠商指出，以 COVID-19(新冠肺炎、武漢肺炎)為主題的駭侵攻擊案例數量，今年三月份較一月份增加了三百倍之多。

資安廠商 ZSCALER 發表研究報告指出，該公司觀察到以 COVID-19 為主題的駭侵攻擊案例數量，今年三月份較一月份增加了三百倍之多。

該公司說，一月時該公司觀察到的這類攻擊，為數僅有 1,200 次；到了三月份則暴增到 380,000 次。

報告指出，各類駭侵團體非常喜歡搭上各種全球熱議話題的便車，以引誘受害者上勾；而在現今全球受到肺炎疫情嚴重衝擊的情況下，以肺炎疫情為主題的駭侵攻擊，數量增多也是可預期之事。

報告進一步分析指出，自從全球疫情爆發以來，首先觀察到的現象，就是肺炎相關新網域名稱登錄數量大量增加；其中疑似用以發動駭侵攻擊的可疑新域名，數量高達 130,000 個以上；光是三月份增加了近十萬個。

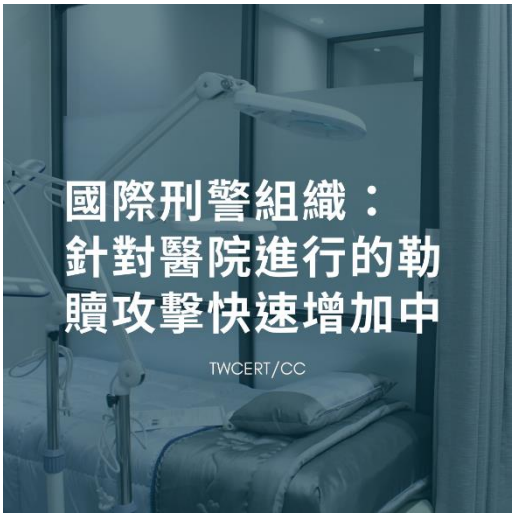
報告也列舉一些代表性的肺炎駭侵攻擊案例，包括針對企業受害者的釣魚信件，經常會假冒企業內的 IT 單位，發送 VPN 或測試主機連結給在家工作的員工，但實際上導向的是惡意網站，企圖騙取員工用以登入公司各系統的資訊。

針對個人的駭侵行動，則常會假冒政府防疫單位或公益團體，要求用戶登入並且捐款，實際上是在騙取用戶的各種金融服務相關機敏資訊。

在巴西則有一種透過惡意 PowerPoint 簡報檔進行攻擊的手法。檔案偽稱內含遭肺炎病毒汙染的旅館清單，誘使用戶開啟檔案，同時植入惡意軟體，竊取用戶鍵盤輸入內容或電腦內的檔案。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/researchers-30-000-percent-increase-in-pandemic-related-threats/
  2. https://www.zscaler.com/blogs/research/30000-percent-increase-covid-19-themed-attacks

3.1.5、國際刑警組織：針對醫院進行的勒贖攻擊快速增加中



國際刑警組織指出，儘管全球COVID-19(新冠肺炎、武漢肺炎)疫情持續爆發，但試圖在醫院關鍵系統中植入惡意勒贖軟體的攻擊行動，最近仍然大量增加。

國際刑警組織發出警告，指出儘管全球 COVID-19 疫情持續爆發，各國醫院收治大量肺炎患者，即將不堪負荷，但試圖在醫院關鍵系統中植入惡意勒贖軟體的攻擊行動，仍然大量增加。

一個名為 Maze 的勒贖軟體，公開了從某一家藥品試驗公司取得並加密的資料，在暗網中叫賣；另一個知名勒贖軟體 Ryuk 則是每天都傳出醫療院所遭其攻擊的消息。

雖然有部分「業者」宣稱不會針對醫療體系進行資安駭侵攻擊，但事實上針對醫療院所和相關產業的攻擊活動，還是不斷升高。

媒體也報導說，一個俄語的駭侵組織，上周勒贖攻擊了兩家歐洲醫療產業公司，其中一家是藥廠，另一家是醫材製造商。

有鑑於這類針對醫療體系的駭侵攻擊，在疫情持續擴大之際仍大加肆虐，國際刑警組織也對其 194 個會員國發出紫色警示，要各國對可能的勒贖攻擊提高警覺，嚴加防範。

國際刑警組織指出，近來的勒贖攻擊樣態，多是透過假冒國際或各國政府單位的公文或指示，假稱含有疫情相關重要資訊，誘使相關人員誤開，進

而植入惡意軟體。

國際刑警組織建議各國的衛生單位，應提升資安防護意識與防護等級，勤於升級其轄下的軟硬體設備，取得並安裝最新資安修補軟體，同時對不明郵件和文件檔案提高警覺，並加強資料離線備份工作，確保即使遭到攻擊也能迅速回復正常運作。

- 資料來源：
  1. https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware
  2. https://twitter.com/INTERPOL_HQ/status/1246376755985694720?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1246376755985694720&ref_url=https%3A%2F%2Fwww.bleepingcomputer.com%2Fnews%2Fsecurity%2Finterpol-ransomware-attacks-on-hospitals-are-increasing%2F
  3. https://www.bleepingcomputer.com/news/security/interpol-ransomware-attacks-on-hospitals-are-increasing/

3.1.6、美國多家大型航太製造業者遭勒贖攻擊，拒付贖款後機密內容遭曝光

多家美國航太製造業者內部重要資料，在遭駭但拒付贖款後被公布在網路上。

多家美國航太製造業者，包括波音、洛克希德馬丁、SpaceX 等公司，其內部多種重要資料，在遭到駭侵攻擊但拒付贖款之後，資料被公布在網路上。

公布資料的駭侵者據說是在幕後操作 DoppelPaymer 的 Windows 勒贖軟體的駭侵組織；由於上述幾家公司在遭勒贖軟體入侵攻擊後拒付贖金，資料就被公布在網路上。

這批機密度極高的資料中，包括由洛克希德馬丁公司設計製造的軍用裝置的細節，包括反飛彈系統中天線元件的設計規格等。

外洩資料還包括這些公司的各種內部文件，例如支付單據、分析報表、法律文書等，甚至還包括 SpaceX 提供給外包生產廠商的各種資料。

這些資料是駭侵團體攻擊一家名為 Visser Precision 公司所取得的；這家公司是上述幾家大廠的外包廠商。駭侵者駭入 Visser Precision 的電腦，將這批重要檔案加密，並要求數千萬美元的贖金，但遭到拒付。駭侵者便將部分資料公開在網路上作為報復手段。

這並非 DoppelPaymer 駭侵組織第一次公布受害者的資料，該駭侵組織網

站，經常貼出許多拒付贖款者所屬的資料，做為恫嚇其他受害者的手段；在駭侵者威脅公開資料時是否支付贖金，即使在資安專家之間，也有各種不同意見。有人認為無論如何都不該助長勒贖攻擊，有些人則認為如果資料過於敏感，支付贖金也是可以考慮的選項。

但無論如何，製造業者都應加強資安防護強度，並提高從業人員的資安意識，才能從根本避免愈來愈猖獗的勒贖攻擊事件。

建議採取的資安強化措施：

1、建議定期將重要資料進行備份。

2、不隨意開啟不明寄件人寄送的郵件，在未確認寄件人身分或是針對標題及內容可疑的信件，不隨意點擊或下載任何信件中的連結與夾帶附件。不進入可疑或不安全的網站，必須確認網址的正確性，可使用網址識別套件或直接手動鍵入網址，以防止遭駭客入侵，被植入惡意軟體而造成損失。

3、應定期更新作業系統版本以及軟體或應用程式版本，安裝防毒軟體與防火牆，確保設備軟體處於最新版本。

4、建議企業進行內部教育訓練，加強資安宣導，提升員工資安意識。

5、及時發現中了勒索軟體的當下，建議立即將電腦關機，中斷網路連線、拔除實體網路線及 USB 裝置，將受害主機進行隔離。

6、參考 TWCERT/CC 官網(https://www.twcert.org.tw/tw/lp-22-1-2-20.html)提供之勒索病毒解鎖服務，參考已被解鎖勒索軟體之解鎖工具。

- 資料來源：
  1. https://www.theregister.co.uk/2020/04/10/lockheed_martin_spacex_ransomware_leak/
  2. https://malware.wikia.org/wiki/DoppelPaymer
  3. https://www.malwarebytes.com/ransomware/

4. https://www.ithome.com.tw/tech/101366

5. https://blog.trendmicro.com.tw/?p=18070。

3.1.7、四十萬筆卡片消費記錄，於暗網上以 200 萬美金出售

資安公司發現一大批卡片消費資料在暗網上待價而沽，總筆數高達四十萬筆，受害者主要來自南韓與美國的銀行等金融業者。

設立於新加坡的資安公司 Group-IB 發表研究報告指出，該公司發現一大批卡片消費資料在暗網上待價而沽，總筆數高達四十萬筆；受害者主要來自南韓與美國銀行等金融業者。

這筆在暗網上的資料是由不明身分者於四月九日上傳，要價高達兩百萬美元，一筆資料相當於五美元；出售者還說這些資料有 30%~40% 的正確性。

在這批資料中，有近一半（49.9%）來自南韓的銀行與金融機構，另外 49.3% 則來自美國的銀行與金融機構。Group-IB 指出，在暗網上很少看到來自南韓的資料，所以相當罕見。

這些外洩的資料，主要以記錄在信用卡磁條上的資訊（Track 2）為主，包括銀行識別碼（BIN）、卡號或帳號、有效日期等，有些還包括三位數安全碼（CVV）。該公司說，這些資訊通常都是從被惡意軟體植入的 POS 終端機或 ATM 刷卡機洩漏的，不過在這個案例中未能確認資料來源。

Group-IB 公司表示，自 2019 年起，愈來愈多亞太國家的各種刷卡資料，被盜取出售的案例愈來愈頻繁。在 2019 年十月，來自印度的刷卡資料就有一百三十萬筆，2019 年二月和 2018 年十一月也有兩批巴基斯坦的大量刷卡記

錄在暗網上求售。

- 資料來源：
  1. https://www.group-ib.com/media/south-korean-and-us-banks-cards/
  2. https://www.hackread.com/dark-web-hackers-sell-south-korea-us-card-data/
  3. https://www.group-ib.com/media/biggest-card-database-ever/

3.1.8、針對電視串流廣告的詐騙攻擊，假冒超過 200 萬台裝置觀看廣告

資安廠商發現史上最大的智慧連網電視廣告詐騙點閱攻擊，遭假冒的裝置多達兩百萬台以上，且詐騙流量佔正常廣告流量比例最高達 50%。

資安廠商 WhiteOps 發表研究報告指出，該公司的研究人員發現史上最大的智慧連網電視廣告詐騙攻擊行動；遭僵屍網路假冒的電視、機上盒、手機等裝置，多達兩百萬台以上，分布於三十個以上國家；而詐騙廣告流量最高時達整體廣告流量的 50%。

WhiteOps 發表的報告中稱這次攻擊行動為 ICEBUCKET，主要的攻擊方式為假冒各種連網電視或影片觀看裝置以播放由 SSAI（Server-Side Ad Insertion，伺服器端廣告置入）播送的廣告，以假冒且無效的廣告觀看來詐取廣告分潤獎金。

ICEBUCKET 會透過僵屍網路，將受害裝置向 SSAI 偽稱為可以播放廣告的裝置，誘騙 SSAI 伺服器對其播送廣告；為成功騙取 SSAI 伺服器，ICEBUCKET 偽裝成超過 1000 種不同的 User-agent、300 種以上不同的 appID、使用來自三十國至少兩百萬個不同的 IP 位址，向在 9 國境內約 1700 台 SSAI 伺服器發動假冒廣告攻擊。

根據 WhiteOps 的統計，這波攻擊行動假冒的裝置，有 46% 是扮成 Roku 品牌的各型網路影音機上盒，26.8% 偽裝為採用 Tizen 作業系統的三星電視、20.7% 偽裝為 Google TV 機上盒，還有 6.1% 是 Android 行動裝置。

目前還不清楚這波 ICEBUCKET 的幕後有哪些駭侵團體，也不清楚整體廣告產業損失的金額有多大，但 WhiteOps 預期這類的假冒廣告詐騙攻擊將會愈來愈多。

- 資料來源：
  1. https://www.whiteops.com/blog/giving-fraudsters-the-cold-shoulder-inside-the-largest-connected-tv-bot-attack
  2. https://www.zdnet.com/article/icebucket-group-mimicked-smart-tvs-to-steal-ad-money/
  3. https://threatpost.com/icebucket-streaming-tv-fraudsters-steal-ad-dollars/154852/

3.2、國際政府組織資安資訊

澳洲政府公布借 COVID-19 疫情為名進行駭侵攻擊的多種樣態

澳洲資安主管機關發布新聞，公開多種該單位監測到的假借 COVID-19(新冠肺炎、武漢肺炎)疫情進行的駭侵攻擊樣態。

澳洲資安主管機關澳洲資安中心（ Austrilian Cyber Security Centre，ACSC）發布新聞，公開了多種該單位監測到的假借 COVID-19 疫情進行的駭侵攻擊樣態，並呼籲各界應該特別提高警覺，以降低受到駭侵攻擊的風險。

ACSC 指出，該單位在疫情升高期間，觀測到比平時更為活躍的駭侵攻擊，而且許多駭侵活動都假借 COVID-19，意圖誘使個人或組織羊入虎口；ACSC 也預期在接下來數周，這類駭侵活動不論在頻率、攻擊範圍或影響程度都有增無減。

ACSC 觀察指出，數周以來肺炎相關新網站的域名註冊量數以千計，雖然其中不乏正規可信賴的網站，但也有不少是和駭侵攻擊相關。

ACSC 觀測到的這類肺炎攻擊樣態，在釣魚攻擊方面有五種，分別是透過簡訊或即時通訊進行釣魚並散布惡意軟體、假冒澳洲郵政單位的個資釣魚信件攻擊、假冒國際衛生防疫單位寄送的釣魚信、以抗疫為名夾帶惡意檔案的郵件攻擊、以及假冒防疫單位募捐的詐騙匯款攻擊等。

ACSC 同時也發現數種針對在家工作者進行的駭侵攻擊，其中之一是假冒國際防疫單位，要求在家工作者加入成為募款志工，實際上卻變成詐騙匯款車手；另一種是假冒抽獎活動，要求受害者匯一小筆款項以換取大額現金中獎機會的詐騙，或是以一些蠅頭小利要求受害者協助匯款，實際上進行國際洗錢活動。

- 資料來源：

1. https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity
2. https://www.zdnet.com/article/acsc-issues-warning-around-coronavirus-themed-malicious-cyber-activity/
3. https://techwireasia.com/2020/03/covid-19-phishing-and-email-scams-surge-in-australia/

3.3、社群媒體資安近況

兩億六千七百萬組 Facebook 用戶資訊，在暗網上待價而沽

資安專家發現有駭侵者在暗網上出售一批含有大量 Facebook 用戶個資的資料庫，受害者多達兩億六千七百萬名用戶。

著名的獨立資安研究者 Bob Doachenko 日前發表研究報告指出，他發現有駭侵者在暗網上出售一批含有大量 Facebook 用戶個資的資料庫，受害者多達兩億六千七百萬名用戶。

Bob Diachenko 是在網路上發現這個 Elasticsearch 資料庫，內含的 Facebook 用戶個資欄位相當多元，包括用戶的全名、電話號碼、Facebook 用戶 ID 等，可供駭侵者用來當成發動各種駭侵攻擊的素材。

代管這個資料庫的 ISP，在 Bob Diachenko 向其通報後，立即撤下了這個資料庫。

當原本的資料庫遭撤下後，沒過多久，Bob Diachenko 又在另一台伺服器上發現另一個資料庫，除了原本的內容外，又多加了四千兩百萬筆資料；而且這個資料庫馬上遭到不明駭侵者攻擊，在資料庫上留下訊息，要擁有者加強其伺服器的資安防護工作。

而在新增的資料中，還多了包括用戶 Email、生日、性別等個資欄位。Diachenko 認為這些資料是在 Facebook 尚未關閉其 Social graph 相關 API 前，透

過程式搜刮取得的。

這批外洩的 Facebook 用戶個資，以美國的 Facebook 用戶為主；讀者如果擔心自己的 Facebook 帳號是否也遭洩露，可以到 https://amibreached.com/ 搜尋。

- 資料來源：
  1. https://threatpost.com/267m-facebook-phone-numbers-exposed-online/151327/
  2. https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/
  3. https://www.windowscentral.com/massive-data-breach-leaves-267-million-facebook-users-data-exposed

3.4、行動裝置資安訊息

3.4.1、難移除的 Android 惡意軟體，透過非官方 App Store 大量擴散

資安廠商指出，一支極難移除的 Android 惡意軟體 xHelper，目前正透過非官方的 App Store 大量擴散。

資安廠商卡巴斯基（Kaspersky）日前發表研究報告，指出有一支極難移除的 Android 惡意軟體 xHelper，目前正透過非官方的 App Store 大量擴散，受害者日漸增加中。

這支 xHelper 和一般惡意軟體相同的地方，是偽裝成系統清理工具軟體，誘使用戶安裝；一旦受害者下載安裝之後，它就會開始收集用戶手機上的各種機敏資訊，同時下載更多的惡意軟體，甚至取得手機的 root 權限。

但 xHelper 與眾不同的特色，在於會建立極深的巢狀目錄，使得真正的系統工具很難將之完全清除；它甚至會利用其 root 權限開啟 Android 系統目錄的寫入權限，把自己掛載到系統目錄中。

xHelper 甚至還會改寫 mount() 函數，以防用戶和防毒軟體進入系統目錄內將之刪除；這也能確保每次手機重開機後，都會自動執行 xHelper 與其他的惡意軟體；甚至在重新安裝手機系統時，也無法清除惡意軟體程式碼。

據卡巴斯基的研究人員表示，這種作法確實非常厲害，即使用戶將手機清空至出廠預設狀態，xHelper 仍然不動如山，極難移除。

目前 xHelper 主要的受害者分布在俄羅斯、歐洲和東南亞，主要攻擊對象為仍然使用舊版 Android 6、7 的 Android 手機；這些尚未或無法升級作業系統的手機，仍然佔 Android 整體市場的 15%。

卡巴斯基說，要徹底移除 xHelper，只有一個方法：除了進行手機還原至出廠預設值外，也要把整個 Flash 記憶體完全清空；如果手機支援 Android Recovery 模式，還要手動將 libe.so 檔案從原始韌體檔案中取出，再替換到手機內，再清除整個系統分割區才行。

- 資料來源：
  1. https://securelist.com/unkillable-xhelper-and-a-trojan-matryoshka/96487/
  2. https://www.theregister.co.uk/2020/04/08/xhelper_android_malware/

3.4.2、超過一億巴基斯坦手機用戶，個資遭駭侵者於暗網出售

巴基斯坦資安廠商指出，該公司發現有一批該國手機用戶的個資於暗網上待價而沽，受害人數高達一億一千五百萬人。

巴基斯坦資安廠商 rewterz 發表研究報告，指出該公司發現有一批該國手機用戶的個資，於暗網上待價而沽；據統計這個案件的受害人數，高達一億一千五百萬人。

Rewterz 說，駭侵者在暗網上出售這批個資，要價高達 210 萬美元。該公司從樣品檔中發現這批個資包括受害者的個人姓名、完整住址、手機號碼、身分證字號與稅務編號等個人可識別資訊。

Rewterz 表示，這批個資的銷售對象，是暗網中的 VIP 進階用戶；整個資料庫中的個資相當新，是不久前才從一系列駭侵行動中取得的，而且仍在持續更新中。

Rewterz 的研究人員說，這一批個資檔案，以嚴整的 CSV 整理得有條不紊，對有需要的人來說可謂非常好用。

Rewterz 從資料的來源，推測這可能是多次駭侵行動匯整起來的資料，但也不排除是一次大規模駭侵就取得如此多的個資。目前也無法確認到底是巴基斯坦哪一家電信業者的用戶遭駭，也有可能是所有業者的用戶都遭到攻擊了。

然而在這則消息曝光後，有一些懷疑論開始質疑這則訊息的正確性，甚至質疑資安公司公布這類駭侵訊息的動機；為此 Rewterz 也發表了另一篇聲明，解釋暗網的運作規則與一般「明網」不同，以公開各種資安事件，對公眾資安認知的重要性。

- 資料來源：
  1. http://www.rewterz.com/articles/115-million-pakistani-mobile-users-data-go-on-sale-on-dark-web
  2. http://www.rewterz.com/articles/rewterz-official-statement-on-the-reported-data-breach-of-115m-pakistani-mobile-users
  3. https://www.brecorder.com/2020/04/10/588270/personal-data-of-115mn-pakistani-mobile-users-go-on-sale-on-dark-web/

3.4.3、數位錢包 App Key Ring 雲端設定錯誤，導致四千四百萬筆用戶個資外洩

擁有一千四百萬用戶的數位錢包服務 Key Ring，日前傳出因為雲端資料庫設定錯誤，造成四千四百萬筆各種用戶個資在網路上曝光。

資安廠商 vpnMentor 發表研究報告，指出在北美極受歡迎，擁有一千四百萬用戶的數位錢包服務 Key Ring，因為其 AWS 雲端資料庫安全設定有誤，造成四千四百萬筆各種用戶個資在網路上曝光。

Key Ring App 提供的服務，主要是讓用戶掃描拍攝各種會員卡或點數卡，存放在手機上，免去攜帶多張實體卡片的麻煩；很多用戶因為這個 App 的便利性，也會將存有各種敏感個資的其他政府核發身分證明卡片、就醫卡等卡片掃描上傳。

據 vpnMentor 指出，Key Ring 在 AWS 上共有五個設定錯誤的 S3 雲端資料庫，而且全都沒有使用密碼保護；只要知道網址，任何人都能隨意存取資料庫內的大量個資。

據 vpnMentor 統計指出，在這五個資料庫中至少有四千四百萬筆各式資料，包括政府核發的身分識別資訊（包括姓名、生日、性別等）、各式會員卡、點數卡、美國步槍協會會員卡、藥用大麻使用執照、醫保卡等，甚至連信用卡的卡號、用戶姓名、到期日、安全檢查碼等大量個人身分可辨識資訊都包括在內。

vpnMentor 甚至還找到屬於 Key Ring 的其他雲端檔案，包括上述資料庫的快照備份檔案，以及 Key Ring 公司內部資料庫，記錄了用戶姓名、Email、家戶住址、使用裝置名稱、IP 位址、加密的密碼資訊等。

vpnMentor 在發現這批資料的二月中旬，就通報 Key Ring 公司。

- 資料來源：
  1. https://www.vpnmentor.com/blog/report-keyring-leak/
  2. https://threatpost.com/44m-digital-wallet-key-ring-cloud-misconfig/154260/

3.5、軟體系統資安議題

3.5.1、Cisco WebEx 視訊會議用戶，近來遭到詐騙更新訊息攻擊

資安廠商指出，近來針對 Cisco WebEx 視訊會議軟體用戶發動的詐騙更新攻擊，正在大量增加，目的在於竊取登入視訊會議用的資訊。

資安廠商 Cofense 的研究人員日前發表研究報告，指出近來由於 COVID-19(新冠肺炎、武漢肺炎)疫情擴散影響，大量人員在家遠距工作，視訊會議系統使用量大增；該公司觀察到近期有駭侵者針對 Cisco WebEx 視訊會議軟體用戶發動詐騙更新攻擊，且攻擊次數正在大量增加。

這波針對 Cisco WebEx 的釣魚信件攻擊，其訊息內容偽裝成由 Cisco 公司發送的緊急資安修補更新，透過假造的 meetings@webex[.]com 地址寄送，主旨例如「Critical Update」或「Alert!」等，目的在於誘使用戶點擊信件中的惡意連結，以竊取用戶登入視訊會議用的資訊。

詐騙信件內容則是回收使用一封由 Cisco 在 2016 年 12 月發出的真實更新訊息，更新的對象是編號 CVE-2016-9223 的資安漏洞；雖然這個漏洞早在 2016 年底就已經修補完成，但現在卻被駭客用來當作取信於受害者的詐騙訊息。

信件最後邀請用戶加入自動更新方案，但在「加入」按鈕中埋入釣魚網頁的 URL；用戶點按後就會進到一個假的登入頁面，要求輸入用戶在 WebEx

用來登入的帳號與密碼。

這個詐騙網頁為了取信於受害者，其詐騙網址甚至還有 SSL 憑證；資安公司建議用戶，在當下疫情快速擴散，人心惶惶的時刻，收到各種可疑信件時，必須更加提高警覺，以免受害。

- 資料來源：
  1. https://cofense.com/new-phishing-campaign-spoofs-webex-target-remote-workers/
  2. https://threatpost.com/cisco-critical-update-phishing-webex/154585/

3.5.2、Zoom 等著名視訊會議軟體成為眾多駭侵者假冒對象

全球肺炎疫情日益擴大，遠距工作者人增，社會對 Zoom 之類的視訊會議軟體需求大增；資安廠商指出，假冒或針對 Zoom 等知名視訊會議服務的駭侵攻擊活動也大為增加。

肺炎疫情日益擴大，世界各國均有大量工作者採行遠距上班方式，對 Zoom 之類的視訊會議軟體需求大增；然而據資安廠商 CheckPoint 指出，該公司觀察到許多假冒或針對 Zoom 視訊會議的駭侵攻擊活動。

CheckPoint 指出，該公司觀察到近來域名中含有「Zoom」的新域名註冊量大幅增加；一月初每天約有十到二十個，到了三月中旨之後暴增到每日一百個以上；自 2020 年至今累計新增 1700 個含有「Zoom」的域名，但其中有四分之一以上，是在上個星期才註冊的。

更值得注意的是，在這些含有 Zoom 的新網域中，有約 4% 的域名內含有特殊字元，明顯是駭侵者打算用來混淆一般大眾視聽，造成誤判之用。

除了 Zoom 之外，最近大幅用於遠距教學的 Google Hangout Meet，也遭駭侵者假冒其名義註冊惡意網域；CheckPoint 發現有兩個域名「googloclassroom\.com」和「googieclassroom\.com」，試圖假冒官方的 classroom.google.com 網站進行惡意詐騙。

另外，這些駭侵者也會透過各種方式，誘使受害者安裝執行假冒的 Zoom 或其他協作軟體的連線程式；CheckPoint 就觀察到名為「Zoom-us-zoom-########.exe」或「microsoft-teams_V#mu#D_#########.exe」的惡意軟體執行檔；受害者一旦執行這些檔案，惡意軟體 InstallCore PUA 就會安裝至電腦系統中，可能導致更多其他惡意軟體也入侵系統。

- 資料來源：
  1. https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/
  2. https://www.hackread.com/hackers-can-drop-malware-with-fake-zoom-apps/

3.5.3、Intel 發表四月平台資安更新，修復多個嚴重資安漏洞

Intel 最新發表四月份的「平台資安更新」（Platform Update），其中包括六個漏洞更新，採用各種 Intel 解決方案的用戶，應立即注意更新。

Intel 最新發表四月份的「平台資安更新」（Platform Update），其中包括六個資安漏洞更新。在這六個獲得更新的資安漏洞中，有 2 個屬於高度危險等級，另外 4 個為中度危險等級。

第一個高度危險的資安漏洞為 CVE-2020-0600，CVSS 危險程度評分為 7.8，發生在 Intel NUC 超迷你電腦主機平台不正確的緩衝區存取限制；駭侵者可透過此漏洞提升自身的執行權限等級，進而進行駭侵操作。

第二個高度危險的資安漏洞為 CVE-2020-0578，CVSS 危險程度評分為 4.3 到 7.1，發生在 Intel Modular Server MSF2600KISPP 計算模組不正確的狀況檢查機制，同樣可讓駭侵者提升執行權限。

其他四個中等程度的資安漏洞，其 CVSS 危險程度評分自 4.3 到 6.7 之間，分別發生在多種不同的 Intel 平台或模組，在 Intel 發表的資安修補通報中有詳細的描述。

Intel 建議所有使用 Intel 各項解決方案的用戶，應檢視自己的設備，是否為此次資安修補更新的目標對象；Intel 也發表了使用這些模組的下游製造商支援清單，用戶可依據各自設備所屬廠牌，在這份列表中取得支援服務與軟

體更新下載點。

- 資料來源：
  1. https://www.intel.com/content/www/us/en/security-center/default.html
  2. https://www.intel.com/content/www/us/en/support/topics/oems.html
  3. https://www.bleepingcomputer.com/news/security/intel-april-platform-update-fixes-high-severity-security-issues/

3.5.4、微軟發表四月「Patch Tuesday」資安修補包，共修復 113 個資安漏洞

微軟推出四月分的「Patch Tuesday」資安漏洞修補包，一共修復多達 113 個資安漏洞，其中有 3 個 0-day 漏洞、15 個嚴重漏洞。

微軟於日前推出 2020 年四月分的「Patch Tuesday」資安漏洞修補包。這個月的修補包一共修復多達 113 個資安漏洞；其中有 3 個是 0-day 漏洞、15 個嚴重漏洞、93 個重要等級漏洞、3 個一般等級漏洞、2 個低危險等級漏洞。

在最危險的 3 個 0-day 漏洞中，其中有兩個已經公開，分別是 CVE-2020-0935、CVE-2020-1020；前者問題出在 One Drive for Windows，駭侵者可透過此漏洞提升執行權限，後者則是出自 Adobe 字體管理程式庫，可讓駭侵者遠端執行任意程式碼。

另外，在這三個 0-day 漏洞中，也有兩個 0-day 漏洞已被駭侵者用以進行攻擊活動，分別是 CVE-2020-0938、CVE-2020-1020，兩者都是出自 Adobe 字體管理程式庫，可讓駭侵者遠端執行任意程式碼。

其他被標示為嚴重等級且於此次獲得修補的漏洞，部分摘錄如下：

- CVE-2020-1022：Dynamic Business Central，可讓駭侵者遠端執行任意程式碼。
- CVE-2020-0687：Microsoft Graphics，可讓駭侵者遠端執行任意程式

碼。

- CVE-2020-0907：Microsoft Graphics Components，可讓駭侵者遠端執行任意程式碼。
- CVE-2020-0931：Microsoft SharePoint，可讓駭侵者遠端執行任意程式碼。
- CVE-2020-0927：MIcrosoft SharePoint，可讓駭侵者進行 XSS 攻擊。
- CVE-2020-0932：Microsoft SharePoint，可讓駭侵者遠端執行任意程式碼。
- CVE-2020-0929：Microsoft SharePoint，可讓駭侵者遠端執行任意程式碼。
- CVE-2020-0974：Microsoft SharePoint，可讓駭侵者遠端執行任意程式碼。
- CVE-2020-0969：Chakra Scripting Engine，記憶體崩潰漏洞。
- CVE-2020-0970：Scripting Engine 記憶體崩潰漏洞。
- CVE-2020-0965：Microsoft Windows Codecs Library，可讓駭侵者遠端執行任意程式碼。

建議所有微軟產品用戶，應盡速安裝本月的資安修補包，以避免遭駭。

- 資料來源：

1. https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Apr
2. https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2020-patch-tuesday-fixes-3-zero-days-15-critical-flaws/
3. https://threatpost.com/april-patch-tuesday-microsoft-active-exploit/154794/

3.5.5、任天堂表示近 16 萬個 Nintendo Network ID 遭到不當登入

任天堂日前發表聲明，指出約有十六萬個 Nintendo Network 帳號遭到入侵；部分與帳號連動的信用卡遭到盜刷購買遊戲虛疑貨幣或其他遊戲。

日本任天堂本社於日前發表聲明，指出約有 160,000 個 Nintendo Network ID 遭到不當登入使用，部分與帳號連動的信用卡，甚至遭到歹徒盜刷，用以購買「堡壘英雄」（Fortnite）遊戲中的虛擬貨幣或其他遊戲。

據美國媒體指出，不少用戶於上個月開始在社群平台上貼文指出，他們雖然用了高強度密碼，但其 Nintendo Network ID 仍被不明駭侵者入侵。Nintendo Network ID 是任天堂提供給老舊遊戲平台如 Wii U、Nintendo 3DS 的網路服務帳號系統。

任天堂在調查後指出，並非 Nintendo Network ID 本身遭到駭侵攻擊，而是與其整合連動的其他服務遭駭，導致駭侵者可以取得與 NNID 連動的用戶「任天堂 Account」profile 相關資料遭外洩。

任天堂說，外洩的資訊包括用戶使用的暱稱、出生年月日、所在國家或地區、Email 地址等，但不包括信用卡資料。由於有些用戶將其 NIntendo Account 與其 PayPal 帳號連動，因此讓歹徒成功利用其 PayPal 帳號盜刷購買。

目前仍不清楚駭侵者的身分，目前任天堂已經取消用戶透過 NNID 登入其任天堂帳號的功能；任天堂也已重置遭駭 NNID 用戶的原有密碼，並發信

要求潛在受害者盡快變更密碼。

- 資料來源：
  1. https://www.nintendo.co.jp/support/information/2020/0424.html
  2. https://www.zdnet.com/article/nintendo-says-160000-users-impacted-in-recent-account-hacks/
  3. https://techcrunch.com/2020/04/24/after-160000-accounts-are-compromised-nintendo-shuts-down-nnid-logins/

3.6、軟硬體漏洞資訊

3.6.1、Google 修復 Chrome 多個嚴重資安漏洞

資安組織 Center of Internet Security 日前發表研究報告，指出 Google Chrome 有八個嚴重資安漏洞，最嚴重者可導致駭侵者用以遠端執行任意程式碼。

Google 隨即發表這些漏洞的修補程式，並將在近期向用戶推送更新。

在這八個得到修補的資安洞中，有三個比較嚴重的資安漏洞。其中 CVE-2020-6450 和 CVE-2020-6451 的問題出在 Chrome 的 WebAudio 組件，用以處理 web 應用中的聲音合成；這兩個漏洞都屬於「use-after-free」錯誤，也就是試圖存取已釋放記憶體時發生的錯誤。駭侵者可以利用這個錯誤造成程式停止執行，甚至執行任意程式碼。

另一個嚴重錯誤出在 Chrome 的 Media 組件，用以在瀏覽器中呈現畫面與聲音；這個錯誤為記憶體緩衝區溢位錯誤，造成駭侵者的可乘之機，用以竄改資料或進行其他攻擊。

這些錯誤發生在 Google Chrome 80.0.3987.162 先前的各平台版本，包括 Windows、macOS、Linux 等；目前尚未傳出有駭侵者利用這批漏洞進行大規模駭侵攻擊。一般用戶請注意近日的 Chrome 更新訊息，以更新至最新版本，杜絕這批資安漏洞帶來的駭侵風險。

- CVE 編號：CVE-2020-6450、CVE-2020-6451、CVE-2020-6452 等
- 影響版本：Google Chrome 80.0.3987.162 先前所有版本
- 解決方案：更新至最新版本

- 資料來源：
  1. https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2020-044/
  2. https://chromereleases.googleblog.com/2020/03/stable-channel-update-for-desktop_31.html
  3. https://threatpost.com/google-squashes-high-severity-flaws-in-chrome-browser/154424/

3.6.2、iOS 13 郵件軟體遭發現 2 個嚴重 0-day 漏洞，駭侵者可遠端執行任意程式碼

資安廠商 ZecOps 發表重量級研究報告指出，該公司發現 iOS 13 的內建郵件軟體 Mail.app 有兩個相當嚴重的 0-day 漏洞，可能已經遭駭侵者用以發動攻擊。

這兩個 0-day 漏洞之所以嚴重，在於其中有一個屬於無需用戶操作（0-click）類型，駭侵者只需寄送含有特製內容的 Email 給用戶，無需用戶打開 Email 進行操作，即可透過此一漏洞植入用戶的 iOS 裝置並開始執行。

ZecOps 指出，該公司已經發現這兩個漏洞有遭駭侵者大規模濫用的跡象，目標對象包括某些重要人士、各行各業的高階主，以及大公司的員工等等。

ZecOps 也說，在該公司觀察到的受害案例中，他們發現駭侵者一旦發現已成功透過 Email 駭入受害者手時，就會立即將該封惡意郵件自郵件伺服器與用戶的手機中刪除，以避免遭到追蹤。

ZecOps 說，他們認為發動這些攻擊的駭侵團體，很可能背後有某些國家勢力的支持，或是有專門僱用駭侵者的團體給予資助。

另一家資安公司 Trail of Bits 表示，透過這個漏洞發動駭侵攻擊用的惡意軟體，可能是在時間壓力下匆忙開發出來的初期版本，因為還必須寄送檔案體積很大的惡意郵件才可能感染 iOS 裝置；這種信件很容易被 GMail、Outlook 之類的郵件服務偵測並擋掉。

蘋果公司表示，已經在測試版的 iOS 13.4.5 Beta 中解決這兩個 0-day 漏洞，正式版也即將推送上線。待正式版上線後，用戶應立即更新其 iOS 裝置。

- 影響版本：iOS 13.5 先前各版本
- 解決方案：待 iOS 13.5.4 正式版推出後立即進行更新
- 資料來源：
  1. https://blog.zecops.com/vulnerabilities/youve-got-0-click-mail/
  2. https://9to5mac.com/2020/04/22/report-iphone-mail-app-zero-day-exploits-found-in-the-wild-apple-has-fix-coming-in-next-public-ios-release/
  3. https://www.vice.com/en_us/article/pken5n/iphone-email-zero-day-hack-in-the-wild

3.6.3、Mozilla Firefox 修復可能遭遠端執行任意程式碼之 0-day 漏洞

開放源碼瀏覽器 Mozilla Firefox，其開發維護單位 Mozilla Foundation 於日前宣布，修復兩個可能讓駭侵者得以遠端執行任意程式碼的嚴重等級 0-day 資安漏洞。

Mozilla 表示，這兩個漏洞都是屬於「use-after-free」漏洞，而且可能已經大量遭到駭侵者用以發動攻擊。

其中 CVE-2020-6819 這個漏洞和 Firefox 瀏覽器中的「nsDocShell destructor」組件相關，瀏覽器用以讀取 HTTP 檔頭資訊；這裡的程式錯誤可導致駭侵者藉以執行任意程式碼。

另一個漏洞編號為 CVE-2020-6820，問題出在 StreamsAPI 中的 Readable Stream 組件；駭侵者同樣也可利用這個錯誤來遠端執行任意程式碼。

所有受到影響的 Firefox 版本，包括 Firefox 74.0.1 先前所有版本，以及企業用戶的 Firefox Extended Support Release 68.6.1 先前所有版本，作業系統平台包括 Windows、macOS、Linux。

Mozilla 指出，由於已經傳出有駭侵者利用這兩個 0-day 漏洞發動攻擊，因此強烈建議所有 Firefox 用戶立即更新到最新版本，以修補這兩個漏洞。

- CVE 編號：CVE-2020-6819、CVE-2020-6820
- 影響版本：Firefox 74.0.1 先前所有版本、Firefox ESR 68.6.1 先前所有版本
- 解決方案：更新至最新版本

- 資料來源：
  1. https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/
  2. https://threatpost.com/firefox-zero-day-flaws-exploited-in-the-wild-get-patched/154466/
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6819
  4. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6820

3.6.4、VMware 修復 vCenter Server 的嚴重漏洞，用戶請盡速更新

虛擬計算環境大廠 VMware 日前公布最新資安修補資訊，指出該公司已針對 CVE-2020-3952 這個嚴重的資安漏洞，發表專屬修補程式。

請目前所有使用 vCenter Server 產品的用戶，立即更新以避免資安風險。

據 VMware 發表的資安通報指出，這個 CVE-2020-3952 的資安漏洞， 在某些特定情形之下，會造成 VMware vCenter Server 內嵌或外部的「平台服務控制單元」（Paltform Services Controller）發生錯誤，進而讓駭侵者於 VMware Directory Service 中取得受害者的各種機敏資料，並進而取得 VMWare vCenter Server 或其他 VMware 產品的控制權。

在 CVSSv3 評級標準下，這個極嚴重資安漏洞的危險評分高達滿分的 10.0 分。

受到這個資安漏洞影響的 VMware 產品，主要是於 Windows Server 或虛擬環境下執行的 vCenter Server 6.7，而且必須是自先前的 6.0 或 6.5 升級上來的版本，因為這兩個版本的 vmdir 布署流程容易受到駭侵者的攻擊。

VMware 建議用戶或系統管理者，應立即檢查自己的 VMware vCenter Server 版本，若為上述的易受攻擊版本，應立即按照 VMware 提供的原廠指示，將其升級至 6.7u3f 或 7.0 版本。

VMware 是在接獲不明來源的密報後知悉此漏洞的存在，並且很快地推出修補程式。

- CVE 編號：CVE-2020-3952
- 影響版本：自 VMware vCenter Server 6.0 或 6.5 升級的版本 6.7
- 解決方案：升級至 6.7u3f 或 7.0

- 資料來源：
  1. https://www.vmware.com/security/advisories/VMSA-2020-0006.html
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3952
  3. https://www.helpnetsecurity.com/2020/04/14/cve-2020-3952/

第 4 章、 資安研討會及活動

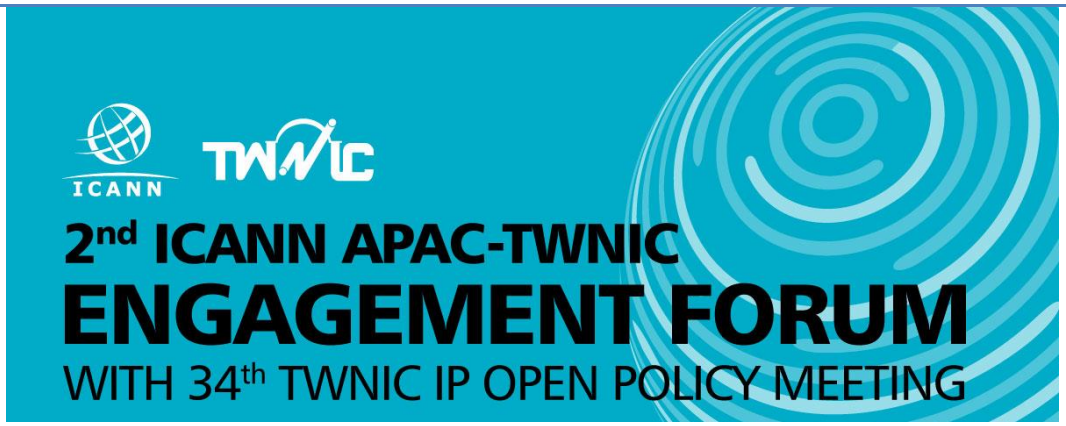
「ISACA 第三方風險管理白皮書」研討會	
活動時間	**2020-05-27 13:30 ~ 16:40**
活動地點	**台大醫院國際會議中心 4 樓 402 室 (台北市中正區徐州路 2 號 4 樓)**
活動網站	**https://www.caa.org.tw/coursedetail-3339.html**
活動概要	中華民國電腦稽核協會 Computer Audit Association 主辦單位：中華民國電腦稽核協會、ISACA Taiwan Chapter 報名時間:2020-04-24~2020-05-26 報名費用：本會會員(含團體會員公司同仁)免費，非會員 500 元 報名名額：限額 90 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 一場突如其來的疫情打亂了世界的運作步調，更擴及到全面性的經濟危機；尤其是與第三方廠商高度關聯的供應斷鏈議題，相信會影響日後所有企業的產業佈局與風險評估方法。但不變的是，今後每個企業仍需藉由第三方廠商的輔助，以達成產品和服務的交付。無論這些第三方廠商是實際做出貢獻，或僅是從旁輔助，他們都是企業的延伸，也有伴隨的風險。因此，第三方廠商亦應屬於企業風險管理的範疇，同時對董事會、企業領導者和 IT 從業者的重要性與日俱增。

「SAP ERP 稽核實務」例會專題演講	
活動時間	**2020/5/28(四)，下午 2:00～5:00**
活動地點	**國立中正大學創新大樓管理學院 383 教室 (嘉義縣民雄鄉大學路 168 號)**
活動網站	**https://www.caa.org.tw/coursedetail-3340.html**
活動概要	中華民國電腦稽核協會 Computer Audit Association 主辦單位：中正大學會計與資訊科技學系、中華民國電腦稽核協會南區分會、ISACA Taiwan Chapter 報名時間:2020-04-27~2020-05-27 報名費用：本會會員(含團體會員公司同仁)及合辦學校教職員免費，非會員 500 元 報名名額：限額 40 名，額滿為止，請儘速報名！ 活動洽詢：南區分會 蕭又菁 秘書，電話：0912-328-818 《例會專題演講》 演講大綱： 1.課程目標 2.SAP 簡介 3.SAP 權限架構簡介 4.SAP 特權帳號管理 5.SAP 程式安全管理 6.SAP 資料表管理 7.SAP 變更管理

榮耀資戰	
活動時間	**初賽：線上進行(2020/5/30)**
活動地點	**台北市信義區菸廠路 88 號(**決賽 2020/7/24、7/25)
活動網站	**https://cyberthrones.zyxel.com/**
活動概要	 主辦單位：財團法人合勤基金會、財團法人國家實驗研究院國家高速網路與計算中心 初賽：線上進行(2020/5/30) 決賽：臺北文創大樓(松山文創園區)6 樓多功能會議廳 / 110 台北市信義區菸廠路 88 號 (2020/7/24、7/25) 不斷進化的資安威脅，等著你來挑戰破解！ 首屆合勤資安大賽『榮耀資戰』廣邀台灣優秀學子來挑戰 你是 CTF 好手卻找不到發揮的場子嗎？ 你是 KOTH 達人想挑戰自我極限嗎？ 你是被疫情影響只能窩在家的資安高手嗎？ 長期致力網通資安發展的合勤控集團 首度在台灣舉辦大型資安競賽『榮耀資戰』 快來累積實戰演練的經驗值 和對手切磋攻防強化資安技能、發掘無窮潛能！ 沒錯，就是你！馬上揪團報名！ 與合勤聯手抵禦資安威脅，成為新世代的資安悍將！

第 19 屆亞太資訊安全論壇暨展會	
活動時間	**6/9 (二) – 6/10 (三) 09:00 ~ 17:00**
活動地點	**台北市敦化南路一段 108 號 B2F**
活動網站	**https://www.informationsecurity.com.tw/event/event_info.aspx?eid=1498**
活動概要	 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。 活動洽詢: 02-8729-1042 潘小姐 / Iris.Pan@newera.messefrankfurt.com 主辦單位: 資安人

CYBERSEC 2020 臺灣資安大會	
活動時間	**8/12(二) – 8/14(四) 08:30 ~ 17:00**
活動地點	**台北市南港區經貿二路 2 號 (南港展覽二館)**
活動網站	https://r.itho.me/sec2020
活動概要	 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 8/12-8/14 於南港展覽二館盛大登場！ 匯聚世界級資安大神、國內資安頂尖高手，從提供超過 200 堂資安面向的議程、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 家以上全球與國內知名標竿資安品牌，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，與來自臺灣與亞太地區超過 8,000 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。 主辦單位：iThome 了解更多大會資訊：https://r.itho.me/sec2020

第二屆 ICANN APAC-TWNIC Engagement Forum 與第 34 屆 TWNIC IP 政策資源管理會議	
活動時間	**2020 年 11 月 12、13 日**
活動地點	**台北市仁愛路三段 160 號**
活動網站	**https://forum.twnic.tw/2020/registration.htm**
活動概要	 網際網路名稱與數字位址分配機構（ICANN）及財團法人台灣網路資訊中心（TWNIC）共同舉辦合作交流論壇 (ICANN APNIC-TWNIC Engagement Forum)，集合了網路相關利害關係人與國際相關網路社群，針對域名、IP 位址及網路安全等主題，進行深入議題探討，這將是台灣與國際網路利害關係人共同面對面討論全球網路議題的最佳機會。 第 34 屆 TWNIC IP 政策資源管理會議希望促進網際網路相關產業發展為目標之會議，提供各界有關網路技術研究、產業發展之溝通交流平台，彙集臺灣地區各 ISP 業者之意見提供相關 IP 政策及管理機制。 本次論壇邀請喬治亞科技大學公共政策學院的 Milton Mueller 教授擔任專題演講主講人，他的主要研究領域為網路的政經發展，主題涵蓋網路所有權、運作機制及資通訊產業的全球治理。他是網路治理計畫的創立者之一，在 ICANN 及 OECD 的公民社群中具有領導地位。曾經參與建立非商業使用者選舉人並當選兩次主席、擔任 GNSO 議會委員；並於多個 ICANN 工作小組中服務，曾擔任 PIR(.org)之諮詢議會委員。參與網路治理經驗豐富，演講內容精彩可期。

	ICANN 及 TWNIC 建立論壇平台，讓地區內之網路相關利害關係人，可以藉由合作交流論壇從區域及台灣的角度探索政策、科技與協作等不同面向中各方利害關係人的觀點。

第 5 章、 2020 年 04 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。

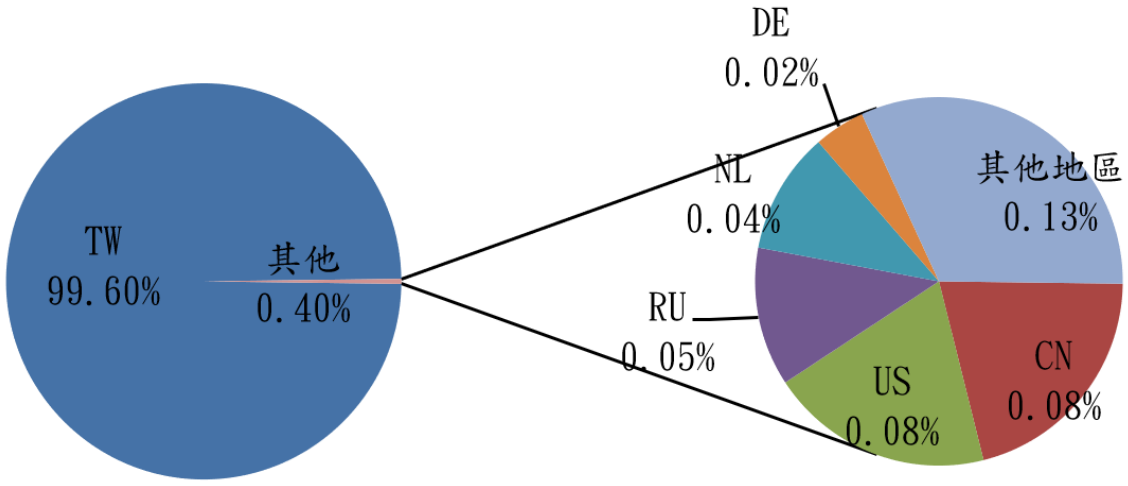


圖 1、分享地區統計圖

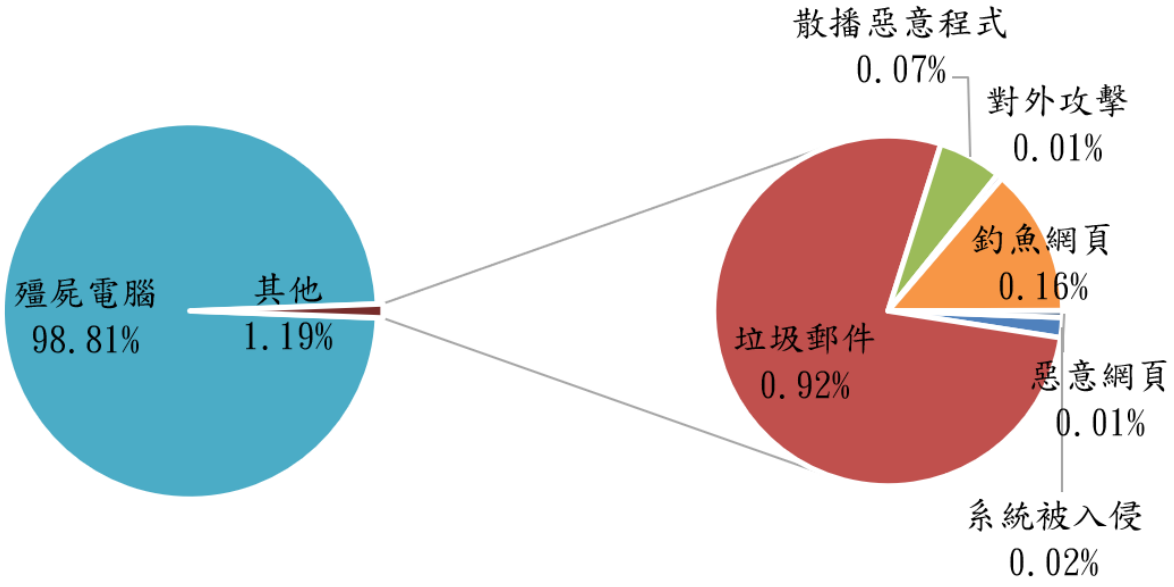

殭屍電腦
98.81%
其他
1.19%
散播惡意程式
0.07%
對外攻擊
0.01%
釣魚網頁
0.16%
垃圾郵件
0.92%
惡意網頁
0.01%
系統被入侵
0.02%

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 5 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**