113年10月號

公務機密
資訊安全維護

林業及自然保育署
臺東分署

公務機密 資訊安全維護

目錄

7月資安通報創逾4年新高 數發部：擴大演練範圍所致

2024-09-01 08:29 中央社／ 台北1日電

資安月報顯示，7月資安事件通報數量共276件，較去年同期增加1.37倍，也是月報發布以來逾4年新高。數發部資安署表示，為協助更多機關找出系統存在的資安風險，今年實兵演練範圍擴大到全台各個公務機關，導致通報數增加。

根據數發部資安署最新資安月報，7月蒐整政府機關資安聯防情資共7萬6572件，創下2022年9月以來新高，年增27.1%。所謂資安聯防情資，就是機關透過系統偵測是否有壞人在門外徘徊，壞人可能嘗試開門，檢視門有無鎖好、伺機闖入，這些作法都可能留下異常紀錄。

資安署署長謝翠娟說明，與其實體攻擊，現在還不如透過網路攻擊更有效益，威脅情資變多，觀察可辨識的威脅種類，第1名為資訊蒐集類（43%），主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次是入侵攻擊類（22%），企圖得到系統權限；再來是入侵嘗試類（19%），可能是弱密碼狀態，外部嘗試入侵未經授權的主機。

資安署向中央社說明，每個機關都有設威脅偵測機制，監測外部有沒有探測、試圖闖關系統等行為，如果發現這類行為就會回報情資，但近期發現有些機關偵測辨識上沒那麼完整，因此加強輔導部分機關回傳情資的辨識品質，整體情資數量因此有所上升。

此外，資安署也彙整分析聯防情資資訊，發現近期駭客以「薪資評估通知」郵件主旨，搭配加薪訊息，寄送社交工程電子郵件攻擊政府機關。另外，也有駭客透過美國航空航天學會網站重新導向的漏洞，嵌入釣魚網址，企圖騙收件人點連結與提供敏感資訊，已提供各機關防護建議。

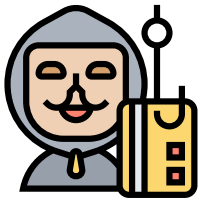
7月資安事件通報數量共276件，較去年同期增加1.37倍，也創下資安月報2020年6月開始對外發布以來逾4年新高。

資安通報創下歷年新高，是否代表公部門資安防護仍有不足，資安署指出，行政院國家資通安全會報每年都會辦理實兵演練，不定期、也不會事先通知機關，不然可能讓演練失真。資安署為協助更多機關找出系統存在的資安風險，今年擴大演練範圍到全台各個公務機關，並精進實兵演練技術，導致通報數量較過去增加。

資安署表示，7月實兵演練攻擊成功案件較多，其中件數較多的為無效的存取控制、危險或過舊的元件及加密機制失效為主，占通報件數61.59%，意味系統在權限管理、元件版本更新及機敏資料遮蔽上仍有加強空間。

資安署強調，通報發現問題後，除了通知機關立刻修補改善外，也持續透過滲透測試等手法，檢測公務機關對外資通系統的潛在脆弱點，提升機關資安防護、通報應變等能力。

研調：網路釣魚冒充科技品牌 微軟居榜首



2024/8/5 18:41

（中央社記者吳家豪台北5日電）資安業者Check Point Software今天發布「2024年第2季品牌網路釣魚報告」，揭露網路犯罪者企圖竊取個人資料或付款資料時最常冒充的品牌，結果顯示科技業為網路釣魚攻擊冒充首選，微軟高居榜首。

業者另公布數據顯示，2024年第2季全球各組織平均每週遭網路攻擊1636次，比去年同期增加30%；台灣各組織平均每週遭攻擊4061次，為全球平均近2.5倍。

Check Point發布新聞稿指出，微軟（Microsoft）仍是網路釣魚攻擊中最常被冒充的品牌，在所有攻擊中占比達57%。蘋果（Apple）占比10%，從今年第1季的第4名，躍升至第2季的第2名；領英（LinkedIn）仍位列第3，占比7%。

其他入列前10名的品牌包括谷歌（Google）、臉書（Facebook）、亞馬遜（Amazon）、DHL、愛迪達（adidas）、WhatsApp、Instagram。

資安業者分析，在品牌網路釣魚攻擊中，科技業是最常被冒充的產業，其次為社交網路和銀行業。由於科技公司通常掌握各種敏感資訊，包括個人資料、財務資訊及其他帳戶的存取權限，因此成為重要目標。

業者分析表示，網路釣魚攻擊仍是主要網路威脅之一，往往是更大規模供應鏈攻擊活動的起點。

為了防範網路釣魚攻擊，資安業者建議，使用者應始終驗證寄件者的電子郵件地址，切勿點擊來歷不明的連結，並在帳戶上啟用多重身分驗證。（編輯：張良知）

到全球知名暗網購買他人個資 台灣3電腦高手被起訴

呂志明 2024年8月28日
台灣3名電腦高手，到全球知名的網路犯罪市場、「創世紀市場」（Genesis Market）購買「權限蒐集資料庫機器人」，再利用這個機器人侵入相對應的網站瀏覽資訊，台北地檢署調查後，認為3人涉犯《個人資料保護法》、《刑法》妨害電腦使用罪，依法提起公訴。

另外其中1名被告林逸松的辯護律師杜佳燕，涉嫌利用陪偵機會，將偵查內容洩漏給同案被告，同時林逸松還另涉犯個資法的部分，檢察官則另行簽分偵辦。

創世紀市場是非法販賣網站帳號權限的網站市場，民眾在註冊成為該網站的用戶後，可以用虛擬資產交易所錢包或非託管錢包轉出比特幣或萊特幣等虛擬資產支付，以購買機器人，再以機器人存有遭駭客竊取的網路使用者外洩的登錄資訊，包括密碼及網路「數位指紋」、瀏覽器歷使紀錄、COOKIE、自嬌填充表單數據、IP位址和位置等資訊。

購買者利用這些資訊可以冒充合法用戶，登錄受害者的網路銀行、電子郵件、購物平台、社群媒體等帳戶個人資訊，甚至可以更改合法用戶的密碼。而這些機器人不僅存有合法用戶的相關登入資訊，還包括我國國人的國民身分證統一編號、手機號碼及各大網站登入帳號密碼等個人資訊，甚至包括我國政府機關系統存取權限，這些全都可以提供給買家直接使用。

由於長久以來，暗網市場一直扮演網路犯罪分子從事不法交易的市場，而號稱全球最上暗網市場之一「創世紀市場」，也成為網路犯罪者在此交易購買受害者資料的地方，去年4月間，美國聯邦調查局和澳大利亞、加拿大、德國、波蘭、瑞典和歐盟的執法機構，查封創世紀市場域名並對網站總部實施司法制裁。

去年6月間，調查局接獲美國聯邦調查局情資，「創世紀市場」網站非法販售國人個資，調查局資安工作站接獲線索後，深入追查發現該網站註冊用戶除以網路匿蹤技術隱匿真實身分，並透過虛擬貨幣匿蹤技術等方式製造金流斷點。

經過蒐證、交叉比對後，掌握台灣電腦犯罪高手林逸松及陳姓、虞姓男子，在創世紀市場購買多筆國人使用的社群平台或蝦皮、露天等商用平台的帳號密碼、手機號碼及身分證統一編號等網站權限，因此報請台北地檢署由檢肅黑金專組檢察官羅韋淵指揮偵辦。

檢調查出，台灣電腦高手林逸松在創世紀市場購買11個權限蒐集資料庫機器人、陳韋志購買18個、虞修志購買29個，3人利用機器人登入相對應的網站瀏覽資訊，造成被侵入的政府機關、學校、購物平台用戶的損害。

今年4月18日、7月2日，檢察官指揮新北市調查處、台北市調查處及花蓮縣調查站，分二波發動搜索，查扣涉案人相關主機及電磁紀錄等證物，同時約談林逸松、陳韋志、虞修志等3人到案。

台北地檢署調查後認為3人涉犯《個人資料保護法》、《刑法》妨害電腦使用罪，依法提起公訴。

每月一常識

新版個人資料保護法與過去有很大的不同，新法進一步擴大了個人資料的保護範圍，並且讓所有產業一體適用；新法甚至首度增加團體訴訟，而且違法的罰則也加重了，企業老闆要負更大的責任。接下來，我們以60個Q&A，快速帶你認識新版個人資料保護法

Q6 哪些個人資料是被個資法保護？

A 個資法所定義的個人資料，是指自然人的姓名、出生年月日、國民身分證統一編碼、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動，以及其他得以間接或直接識別該個人的資料。

文/iThome

公共Wi-Fi 免費無線網路暗藏個資外洩危機！掌握4招確保上網安全

（圖／歐新社）

2024/06/24 12:50文／記者劉惠琴

外出或出國旅遊時，不論是在任一家咖啡廳、購物中心、機場或車站等公共場所，許多人都會透過該場所所提供的免費Wi-Fi無線網路，來讓手機、平板或電腦裝置上網。這些標榜Wi-Fi Free 免費無線上網的服務，由於任何人都能同時跟你處在同一個無線網域進行Wi-Fi連線上網，難保不會有網路駭客或不肖網路犯罪份子潛藏其中趁機暗地植入惡意程式進而竊取裝置個人資料，相對地也成為使用公共網路上網環境的安全威脅風險因素。

對此，外媒ZDNET 報導指出，若處於需使用公共Wi-Fi 無線上網，在使用前、使用時與使用後的過程之中，為確保裝置連線上網的資訊安全性，建議謹慎掌握四個要點來做檢視。首先，就是在連線公共網路時，務必先檢視核對裝置透過WiFi連線的場所名稱是否正確，以防誤陷偽裝名稱的無線網路環境。

第二，在連上公共WiFi網路，上網瀏覽網頁或應用程式的過程中，要避免輸入任何有關個人的機敏資料，如網路銀行帳號密碼、或信用卡號，並避免查看銀行帳號等動作。此外，若連上公用WiFi時，跳出要求需要提供個人Email電子郵件資訊，建議可申請一個特定的新Email帳號，作為登入連線公用WiFi所專用（跟平常個人電子郵件區隔），以避免輸入電子郵件帳號資訊，恐遭有心人士存取日後進行惡意寄送垃圾信箱或釣魚惡意詐騙等行為。

第三，使用公共WiFi網路時，建議可為裝置另外安裝下載需付費使用的VPN私人虛擬網路，可為裝置上網時的IP位址增添一層安全加密防護並可加密上網數據流量，亦能防止個人機敏資料遭不當竊取的資安風險。

第四，每當使用公共WiFi網路之後，務必定期清除手機、平板或電腦裝置上的上網搜尋與瀏覽紀錄與網路連線相關設定。以避免下此在造訪該場所時，所使用的手機裝置在你不知情的狀況下，透過自動連線功能WiFi上網，恐不慎遭有心人士竊資的安全風險。