新竹市立內湖國民中學110年校內人員資通安全教育宣導(三)

110.11.19

新型冠狀病毒與電腦病毒的合力出擊

資料來源：資安知安報你知 （2020-001）

作者：中華電信數據通信分公司_陳昭全 / ACW小編整理

新型冠狀病毒(COVID-19)疫情肆虐全球，人們的生活習慣與工作型態逐漸被改變。乘著肺炎疫情所帶來的轉變，駭客組織或是有心人士利用相關內容，不斷發出病毒攻擊，試圖從中謀取利益。駭客製作出適用全球各地社交攻擊信件，因此在短短幾個月內網路上充斥著各式有關新冠肺炎的攻擊信件。根據Google表示，新冠肺炎疫情帶來新的資安風險，**每天就可攔下1800萬則與疫情相關的惡意程式和網路釣魚郵件，以及超過2.4億與疫情相關的垃圾郵件，呈現數字令人吃驚**。

因應疫情遠距辦公需求上升，所衍生資訊安全問題也逐一浮現。其中，雲端視訊通訊軟體Zoom不斷爆出資安疑慮，包括干擾會議、加密僅限於文字而不包含音訊與視訊等問題，隨後行政院、教育部也明定公務機關及特定非公務機關還有轄下的教育單位，禁止使用有資安疑慮的產品進行遠端會議。但實務上仍有不少使用者僅追求使用便利而沒有資安的考量，如果是公務上需求，仍避免使用具有疑慮的軟體產品，軟體的操作是可被教育訓練，惟不應本末倒置忽略真正的問題。

其次是線上影音平台的需求大增，根據Kantar調研機構統計由於疫情影響，使正版及盜版線上串流影音平台流量暴增，也引來駭客覬覦。**國內外的資安研究團隊皆發現，愈來愈多駭客正利用這股趨勢，透過盜版的影片串流網站或種子檔案入侵受害者的電腦，不少挖礦病毒與後門程式隨著影片散播至世界各地的電腦，一旦受害者下載後，就會啟動用戶電腦的記憶體資源用來挖礦，替駭客賺取虛擬貨幣**。

由上述例子可知，駭客攻擊主要目標其實是人，使用者因素一直以來是整個資訊系統裡不確定性高且脆弱的一環，因此提升全民資安素養至為關鍵。不管郵件社交標題再聳動，都能保持警覺心，不隨意瀏覽可疑網站、下載或開啟來路不明的檔案。根據不同情境在安全性與便利性的取捨上做出良好的判斷，就可避免不少資安事件發生。面對資安威脅，企業與個人都應有良好的資安習慣，定期實施資訊安全教育訓練、宣導資安政策、資安意識從小扎根，落實與持續是重要關鍵。

除人員的訓練外，設備系統更新是另一大重點，從過往的資安事件中發現，許多企業過於依賴防護設備的阻擋，內部的資安防護其實不足，一旦病毒進入到企業內部往往都會導致重大災情。在提升內部資安防護能量上，定期更新作業系統安全性是最基本的項目，病毒若沒可利用的弱點，自然就無法擴散，影響到其它電腦系統。如有無法更新的機台或設備，應優先考慮逐步淘汰，或者優先做好實體隔離以降低資安風險。如還有餘力可以建立備份機制甚至是備援系統，如此一來，安全保障更多一層。

不論駭客利用新冠肺炎議題或其它熱門議題進行攻擊，透過教育訓練提升人員資安觀念、定期更新系統防護能量，善用備份功能讓資料多份保障，是提升資安防護能量的不二法門。

❖資安詞彙集錦❖

1、網路釣魚(Phishing)

透過電子郵件、通訊軟體獲取個人資訊，竊取身份認證。通常在訊息中會夾帶惡意連結，引導收件者連至真假難辨的網站，要求提供帳號密碼等資訊。

2、種子檔案(Torrent File)

係指可以儲存一組檔案的中介資料。這種格式的檔案被 BitTorrent 協定所定義。目前於網頁上大部分使用瀏覽器下載檔案，但有時下載下來的非檔案本體，而是副檔名為「.torrent」的檔案，在 Torrent 檔裡通常記錄了伺服器的地址，以及要下載文件的一些資訊。

3、挖礦病毒(Crypto-Currency Mining)

係指一段代碼或一個軟體，可在用戶的個人電腦或智慧型手機上悄悄運行挖礦程序。攻擊者利用受害者不知情的狀況下，入侵使用者裝置和行動設備來挖掘加密貨幣。

4、後門程式(Back Door)

係指竊取電腦使用者的密碼或個人資料，甚至可以操控被竊者的螢幕資訊，後門程式通常會利用惡意電子郵件、惡意網頁、部份共享軟體的傳播方式來達到散佈的目的。

5、虛擬貨幣(Virtual Currency)

指在虛擬空間中特定社群內可以購買商品和服務的貨幣，它具有交易媒介和記帳單位的貨幣功能。