防疫與防駭－資安新思維

近期【新型冠狀病毒】肆虐，引發全球大流行，進而影響民眾生命安全。我國因已有對抗 SARS 經驗，超前部署提前啟動登機檢疫等措施，民眾亦能主動配合政府各項防疫政策，因此得以有效控制疫情。但是民眾在面對【電腦病毒】時，卻未必能瞭解及重視相關防駭措施，導致企業運作、民眾個人資料及自身財產安全遭受重大影響與損失。

經分析近日發生之數起重大資安事件，發現駭客主要是透過釣魚信件、釣魚網站或是勒索病毒等方式進行攻擊。尤其駭客常利用社交工程方式，寄發偽冒來源的釣魚信件或夾藏惡意程式的附件，誘騙點擊釣魚網站連結或開啟附件，藉以騙取個資、帳號密碼或植入惡意程式。此外駭客也常利用勒索病毒將受害者電腦內的所有資料加密，藉此勒索贖金。

常見的釣魚信件、釣魚網站及勒索病毒，可能觸犯詐欺、恐嚇及妨害電腦使用等罪，經統計近 3 年與電腦犯罪相關的案件數量，107 年計有 5,863 件，財物損失達新臺幣 4 億 3,310 萬 4,904 元；108 年計有 5,587 件，財物損失達新臺幣 5 億 7,122 萬 3,914 元，雖然發生件數減少，惟單一案件之平均財損金額卻呈現大幅增加情形。另外統計 109 年 1 至 4 月與電腦相關犯罪案件財物損失達新臺幣 2 億 486 萬 5,913 元，相較 108 年同期財損（新臺幣 1 億 6353 萬 5113 元）增加 25.27%，另與 107 年同期（新臺幣 1 億 708 萬 9904 元）比較增幅則達 91.3%，顯見近 2 年電腦犯罪案件之財物損失金額有逐年增加的趨勢。

新冠肺炎疫情期間，本局也發現有駭客集團假借防疫名義架設釣魚網站，企圖誘騙民眾點擊，並竊取個人資料及郵件帳號密碼。經偵查分析，駭客集團係透過不知情民眾及企業的無線分享器連網裝置作為跳板連線，由於該無線分享器存在漏洞（CVE-2019-19822 及 CVE-2019-19823），導致駭客可以取得管理者密碼並設定 VPN 作為跳板。該連網裝置使用者多為一般民眾及中小企業，若未立即修補更新恐造成資安缺口，故本局立即函請設備廠商改善修補漏洞問題，該廠商接獲本局通報後，已於 109 年 4 月份發布修補更新程式，並關閉遠端管理漏洞。

防疫是全民共識，為了身體健康，大家都能保持警覺並配合各項防疫措施，而【電腦病毒】如同此次疫情的【新型冠狀病毒】，都是肉眼無法看見，一旦使用者沒有做好自身防護與保持警覺，就可能遭受駭客入侵，造成嚴重損失。本局借鏡此次防疫作為，並結合資安防護的觀點，提供幾項資安防護建議：

1. 安裝防毒軟體並更新病毒碼。
2. 勿點擊不明來源的網址及安裝程式。
3. 定期依照密碼複雜度規則更新密碼。
4. 企業及機關應落實內外網區隔及防護。
5. 資安人員應阻絕釣魚網站並禁止電腦連結。
6. 受駭電腦應阻斷網路避免病毒橫向擴散。

本案來源台灣電腦網路危機處理暨協調中心網站