

公務機密維護宣導

我的電腦 被綁架了

◎魯明德

初為人父的小潘打算帶著剛加入家庭的新成員，去參加 2016 年的跨年活動及迎日出，正利用晚上小孩睡著安排行程之際，突然看到電腦螢幕上出現一個對話框，告訴他中獎了，可以獲得跨年免費住宿券，正在規劃跨年行程的小潘，心想剛好用得上，於是就點進去看看。



點進網頁之後，不幸的事情發生了，系統告訴他電腦已經被綁架，要付 500 美元的贖金才能獲釋，小潘不信邪地試著重開機，發現這一切都是無謂地掙扎，原來整個硬碟都已被加密鎖死了，必須要付贖金才能拿得到解密金鑰。本來他還慶幸有在網路空間

備份資料，沒想到連網路空間的資料也都一起被加密綁架了，事情演變至此，小潘頓時像是被五雷轟頂般，完全不知所措！

小潘於是請教司馬特老師，這時才發現很多人也有電腦被綁架之經驗，根據媒體報導，從 2015 年 9 月以來全臺已有上萬臺電腦受害，歹徒利用 2048 位元的 RSA 加密技術，將目標電腦的硬碟加密，如果沒有金鑰就無法破解。趨勢科技公司的 2016 年資安預測報告中指出：2016 年的網路勒索事件將更加頻繁，流動惡意程式的數量到 2016 年底將成長至 2 萬個，

隨著行動裝置的普及、物聯網應用的成熟，行動支付可能成為下一個被攻擊的目標。

一聽到行動裝置，小潘想到目前有很多人都是用手機或平板上網，公司好像也不反對員工用自己的筆記型電腦或行動裝置連網，當個人的電腦或行動裝置萬一被綁架，不就連累到公司的網路嗎？司馬特老師說現在幾乎人人手上都有智慧型手機或平板電腦，很多公司也都讓員工自己的設備連上公司的網路，這雖然可以提升員工的工作效率，但也增加資訊安全上的風險。

趨勢科技在 2015 年第二季的資安威脅報告中提到：在 Android 平臺上的惡意程式和高風險應用程式，到 2015 年 6 月已有 700 萬個，當公司只看到讓員工用自己的設備上班的便利性，及可減少公司採購設備的成本時，無形的資安風險也就隨之而起。



另有專家指出，企業資訊的數位化引起駭客的興趣，尤其是雲端、行動運算，甚至於物聯網的興起後，當企業選擇雲端方案後，無可避免就會面臨到資訊安全的問題，未來資訊安全面對的可能不再是單一駭客的侵犯，

而是一波波不同駭客團隊的攻擊，而且可能一年 365 天都會面臨網路攻擊的威脅。

企業在面對外部攻擊時，除了靠防毒軟體、防火牆這類軟體的防護外，其實內部的教育訓練及管理作為也是很重要的；在教育訓練上，要時時教育員工，不要隨便開啟來路不明的信件，也不要輕易相信網站給的訊息而開啟不明網站，以減少電腦被綁架的機會；其次，在企業內部資訊安全管理上，應該利用流量監控、大數據分析等方法，找出異常行為，提早發現可能的被攻擊點，及早做好防護，預防風險發生。系統中的資料除了每日備份外，最好還要做到異地備援，以防萬一本地機房淪陷時，還有另外的機房可以讓系統正常運作。網路跳出的網頁在不確定安全的狀況下，不要輕易點選，以免電腦再次遭到綁架。

(轉載自清流月刊 105 年 1 月版)

天下沒有白吃的午餐，網路跳出的網頁在不確定安全的狀況下，不要輕易點選，以免電腦遭到綁架。



【法務部廉政署】

檢舉電話：0800-286-586

檢舉傳真電話：02-25621156

電子信箱：gechief-p@mail.moj.gov.tw

【新竹區監理所政風室】

檢舉電話：03-5891935

檢舉傳真電話：03-5889820

電子信箱：schtru07@ms33.hinet.net

新竹區監理所政風室
關心您

