網路資訊安全防身術

劉耀權

現今網際網路連線已不像數年前那麼簡單與安全，網路因駭客及病毒入侵而肆虐成災，電腦不斷地被駭客嘗試入侵，這樣的問題每天不斷地重覆，而且可能已經悄悄地發生在您的電腦中。這種情況好比當您在家中看電視時，陌生人明目張膽地闖進家裡，並將值錢的家當搬得一乾二淨，但您仍渾然不覺，直到您在電視新聞中看到家裡被竊的消息，才驚覺到家裡早被洗劫一空了！我們來看看到底駭客及病毒會在電腦中造成多大的災害：

一、個人資料及重要文件均可能被竊取或破壞，包括您的銀行帳戶、密碼、研究紀錄、機密文件、個人的E-mail等，可能會造成金錢上的損失或被冒認身分。

二、若被駭客安裝後門程式，會導致電腦不明原因當機，開機及處理效能變慢，影響日常的工作業務。

三、若被網路型病毒感染，則會發送龐大的網路訊息，佔用大量網路頻寬，使網路連線速度變慢，甚至會造成電腦自動關機，無法正常使用電腦等情況。

四、電腦被入侵後，駭客會把該電腦當成入侵下一臺電腦之跳板，「跳板電腦」之原使用者可能被懷疑為駭客而遭檢調單位調查，徒增生活上的困擾。

五、被當成轉信站，轉寄大量垃圾郵件，結果IP位址被限制連線，而無法使用網路，造成資訊交流的不便。

如何為您的電腦建構基本的防護措施，減低被駭客及病毒入侵的機會呢？下列數點建議可供參考：

一、保持電腦中的作業系統及應用軟體沒有任何漏洞

（一）每月連線至www.windowsupdate.com及www.officeupdate.com查看微軟是否已發布最新漏洞的修正檔，如有重大漏洞的修正檔，應立即更新。

（二）注意學術網路工作小組不定時以網頁及電子郵件發布微軟漏洞的公告，公告後應儘速下載及安裝修正檔。

二、安裝防毒軟體

（一）不管任何廠牌的防毒軟體，請設定每天自動更新病毒碼至少一次，這樣才能確保防毒軟體有能力防範最新型的病毒。

（二）若不想設定自動更新，請留意學術網路工作小組每星期透過電子郵件發布的最新病毒碼公告，下載及安裝最新的病毒碼。

三、安裝防火牆軟體

（一）防火牆除了可以阻檔大部分的網路攻擊及不當連線外，亦會記錄入侵者的來源IP位址及其攻擊模式，產生詳細的連線紀錄證明，以便使用者更進一步的處理。

（二）防火牆之安裝及設定其實非常簡單，其中一個較普及的防火牆軟體，已置於學術網路工作小組網頁（http://net.mc.ntu.edu.tw/download/download.htm），提供有需要之同仁下載安裝。

四、請更改Windows作業系統之管理者帳號名稱及密碼

（一）“Administrator”帳號是Windows NT/2000/XP/2003安裝完成後，作業系統預設擁有最高權限的管理者帳號名稱，這個帳號必須設定密碼，且密碼設定不能太過簡單（如1234、abcd、aaaa等），網路上很多駭客及病毒專門入侵這些密碼設定過於簡單的電

腦。

（二）一般來說，網路駭客要入侵一臺電腦時，其中一種手法是利用各種帳號與密碼的配對，產生不同的排列組合，不斷嘗試登入網路中的電腦，如果使用者保留“Administrator”這個帳號名稱，無形中減低了駭客入侵的困難度，因為駭客已不需再猜測帳號，只需要猜測密碼就可以進行入侵，所以請將“Administrator”更改成其他名稱。

五、請勿開啟或預覽任何來歷不明及主旨語意不清的電子郵件及其附件檔案

（一）來歷不明之電子郵件內容，可能隱藏惡意的程式碼，開啟或預覽這類電子郵件，會自動連結到有問題的網頁，自動安裝後門程式或被病毒感染。

（二）不要開啟檔案名稱不詳及目的不明確的電子郵件附檔，這些附件檔案通常夾帶了病毒及後門程式。

六、請勿使用網路芳鄰共享資料夾

（一）病毒會利用網路芳鄰作散播的途徑，感染其他電腦共享資料夾中的檔案。

（二）Windows NT/2000/XP安裝完成後，預設會將電腦中全部資料分享於網路上，造成資料被竊取及破壞。若要檢查電腦目前已分享了哪些資料夾，請在Windows的「開始」→「執行」→輸入“cmd”，再輸入“net share”即可。

七、關閉作業系統內不需要之服務項目

Windows NT/2000/XP安裝完成後，作業系統預設會啟動多項內建的服務，例如“IIS”及“WWW”服務等，請關閉不使用的服務項目，作業系統所執行的服務愈多，被駭客入侵的成功機會愈高。

八、請勿隨意安裝軟體

請儘量不要安裝網路上下載或別人提供的不明軟體，因軟體內同樣可能隱藏了間碟程式或後門程式。

九、請勿隨意點選網址

不要點選不確定的HTTP連結，若連線到有問題的網站，可能會被該網頁之程式碼操控，自動下載及安裝後門程式到您的電腦中。

資料外洩的嚴重性日漸受到關注，請勿忽略網路安全的重要性，此乃網路使用者共同的責任，您的網路資訊安全就是大家的網路資訊安全，讓我們共同來打造一個安全的網路使用環境！