個人電腦防毒防駭實務

陳勇輝／國立海洋生物博物館科學教育組主任

周淑芬

一、前言

在網際網路發達的時代，隨時都有可能在無形中被有心人士以惡意程式如木馬程式等攻擊，無意中將個人隱私資料洩漏無遺，或被假冒名義散發色情廣告垃圾郵件，重創個人的聲譽。有些程式甚至會降低電腦效能，嚴重時造成電腦當機，這些情況往往造成個人及組織的重大損失。

最早的惡意程式源自於西方兩個通訊實驗室互相以程式攻擊對方，後來技術逐漸成熟，更被有心人士加以利用成為謀財的工具，像某些人利用遙控程式指揮對特定的組織植入木馬程式攻擊，癱瘓整體運作功能，有些竊取商業機密賣給敵對公司，造成公司巨大的商業利益損失。這些撰寫惡意程式的人就是駭客（Hacker），簡單說就是在網際網路上以電腦技術危害他人獲取不當利益的人。

目前常出現的惡意程式大略分為特洛依木馬程式（Trojan）、蠕蟲（worm）與病毒（Virus）程式三大類。木馬程式不會自我複製，也不會主動去感染其他檔案，它偽裝自己讓用戶下載執行，藉此使駭客可以毀壞、竊取被植入者的檔案，甚至遠端操控被植入者的電腦。蠕蟲（worm）可在電腦間自行大量複製本身程式，透過掌控電腦的傳輸檔案自動進行複製，例如以複本將程式傳給郵件通訊錄中的每一個人，透過網際網路的傳輸以驚人的速度擴展自己的感染範圍，因此讓網路的運作變得相當遲緩。病毒則為程式碼，雖不會如蠕蟲複製自身程式般的獨立運作，但會嘗試附加到被攻擊者使用的程式裏，可能會損壞硬體、軟體或資訊，主要散佈的方式是借助被攻擊者傳送電子郵件或檔案達成傳播的目的。

雖然政府大力推廣資訊安全的觀念與作法，但是普遍未受到重視，造成惡意程式四處流竄，讓人處於隨時隨地可能中毒的危機之中，然而防毒防駭的關鍵仍在使用者個人的習慣與作法，如何有正確的防毒觀念與作法，成為現代人必備的資訊修養之一。有鑑於此，本文將在觀念上與作法上說明個人防毒防駭的觀念與日常作法，以期達成人人都能落實有效的資安觀念與作法，讓病毒與惡意程式，處處碰壁，無法隨意肆虐傳播。

二、中毒現象

在使用電腦的過程中若發現電腦的效能明顯下降，硬碟在重複地讀寫，指示燈閃爍不定，電腦甚至自動重新開關機，鍵盤輸入無效，滑鼠也難以控制，正使用中的視窗突然被關閉，新的視窗莫名其妙地被打開，網路傳輸指示燈不停閃爍…等這些不正常現象，及出現沒見過的執行檔或是自動執行檔（autorun），這些就是中毒的病徵。此時應先進行隔離，最簡單的方式就是拔除網路線，並進行資安通報和尋求專業協助，進行掃毒的工作及早找出病源與種類。

三、基本資安觀念

（一）資安是每一個人責無旁貸的責任

在人人都可上網的時代，只要連上網路、瀏覽網站或是開啟分享檔案夾，就會有

中毒被駭的可能性。一旦病毒透過偽裝的方式，避過機關的防火牆偵測，進入個人電腦之中，在透過人的好奇心被開啟發病時，所有在同一網域中的電腦就會有中毒的機會。這好比是有人沒有公共衛生的觀念或警覺性太低，已感染具有高傳染力的病毒如流行性感冒時，仍然四處走動一般，讓週邊的人都有感染的危險。病毒的散佈策略無所不用其極，沒有日夜之分，個人若沒有小心防範的話，就有可能受到感染，危及週邊的電腦使用情形，因此唯有人人都具有資安的正確觀念與作法，才是阻隔駭客與預防病毒最佳的防線。

（二）隨時更新作業系統的安全漏洞

目前個人電腦所使用的作業系統以微軟作業系統最為普遍，然而隨著功能的增加，系統程式的複雜性也隨之增加，這也意味著系統所出現安全漏洞的機會大幅增加，也許系統主要功能並未受到影響，讓人誤以為這樣就已經安全無虞了。其實不然，任何嚴密的防護都會有漏洞，程式設計師本身因為當局者迷，往往在設計時並無法看出有任何盲點，可是對於有經驗的行家，或是有心人士就可以找出系統的安全漏洞，並加以攻擊，造成系統無法正常運作，這就是微軟公司為何要常常發佈系統修護的更新程式，讓使用者能修補系統的缺失，減少被攻擊的機會，因此當收到更新的訊息時，雖然可以選擇不去更新與安全無關的功能，但對於系統安全的更新，則是必需要去落實的事。

（三）隨時更新防毒程式的病毒碼

中毒、被駭與收到垃圾郵件是資訊時代必然的現象，就像在醫學發達的現代，並沒有人從未生過病，換句話說，人人或多或少都會生病，只是程度與頻率上的差異而已。任何防毒防駭程式都不是無懈可擊的，任何一種新鎖的發明，就會有一種鑰匙的出現，換句話說，雖然市面上販售防毒軟體公司信誓旦旦推銷該公司產品防毒功能如何強大，仍無法保證完全不中毒，誠如動物病毒為適應環境會不斷地演化出新的變種，全世界的駭客們也極力開發新的電腦病毒，因此要打破「只要有防毒程式，就百毒不侵」的迷思，因為如果真如此有效，哪還需要去防毒？所以應該是大幅降低中毒的風險與機率，萬一真的不幸中毒也是容易清除的小病毒，而不是無可救藥，最後只能重灌整個作業系統的嚴重病毒。而使用掃毒程式時若能在斷線或在安全模式下，則效果會事半功倍。因此，隨時更新防毒程式的病毒碼是維護資安必須養成的好習慣。

（四）定期更換個人密碼

個人密碼的定期更換是必需做的，而且最好選擇包括文字或英文、數字或符號等至少6個字元以上的密碼；密碼的設定也應該避免使用自己的生日或是常用號碼如手機號碼，當密碼字元愈高愈沒有規則性的時候，越難解碼，密碼難解度提高會降低被駭客破解的可能性。此外不將自己的帳號密碼交予他人使用，也不要與他人共用同一個帳號密碼，也是避免資料外洩的方法。瀏覽不同網站時不要採用同一組帳號密碼，以免網站被駭，帳戶、密碼被破解後，自己所有相關資料的大門都將大開，將自己赤裸裸地暴露任人宰割。且至少每三個月至半年就應該更換密碼，增高破解密碼的困難度。暫時離開電腦時，可用螢幕保護程式將電腦鎖住，以防止資料外漏。簡單來說，就是採用動態密碼的策略，讓每次的破解都需要重頭開始，利用重重困難迫使駭客知難而退。

（五）不輕易執行檔案副檔名為.exe與.com檔案

檔案的名稱由兩個部份所組成檔案名與副檔名，前者為檔案的名字，附檔名則表示檔案本身的性質，如.doc，就是WORD的文字處理檔，而.exe或是.com，則是應用程式

的執行檔，電腦病毒的檔案在未被執行之前，是不會發生感染的作用，只有在執行的時候才會有作用，一般病毒的檔案副檔名都為.exe或.com，表示這些檔案都是執行檔，需點選執行之後，病毒才會產生感染作用，因此若發現有不名檔案名稱的檔案，且副檔名為.exe或.com時，都需要經過掃毒與安全性的仔細確認後，再執行檔案以免中毒。

（六）清理垃圾文件

有些病毒留在電腦的暫存檔之中，其中以瀏覽網路時系統所產生的暫存檔最為明顯，將這些垃圾文件刪除，有助於清除附生在暫存檔上的病毒。網路上有免費軟體如CCleaner等可以自行下載使用，清除不需要的垃圾文件，除了可以防毒之外，也可以增加電腦效能。

（七）備份自己的資料

除了將自己的資料與系統放置在不同的硬碟如D碟之外，應該再定期備份自己的資料，備份後的資料應採用異碟備份的方式保存，而不是將備份資料放置在相同實體硬碟中所分割的虛擬硬碟之中，只進行檔案壓縮，節省儲藏空間而已。若可能的話，更應該採取異地備份的方式，將檔案備份在不同地點的儲備裝置上如大型隨身硬碟中或將檔案燒錄至高容量光碟中保存。

四、電子郵件

（一）個人電子郵件分級分類

由於目前各入口網站上皆可申請免費的電子郵件，甚至個人服務的單位也會提供電子郵件，以符合公務上的需求，所以個人可能同時有好幾個電子郵件，但是不是都做了分類使用則因人而異。筆者認為目前個人的電子郵件至少需分級成三類，首先為公務需求的電子郵件，如xxx@nmmba.gov.tw，主要功能用於工作業務上的來往，對外聯絡的代表；其次為個人瀏覽網路之用的電子郵件，這類的郵件筆者建議使用入口網站如Yahoo、Google等的免費電子郵件如xxx@yahoo.com.tw，主要使用於個人一般商務方面，如網路購物或是參加網路活動，可減少個人隱私資料外洩。最後就是個人私用的電子郵件，使用付費或是免費的電子郵件都可以，但只限於個人親朋好友的通信用或是重要通信如與銀行來往的資料，也就是說不隨意讓不相關的人知道，也決不用於一般網購的登錄信箱之用或認證之用。有人認為應該使用網路郵件的方式開啟，也可以降低中毒的機率，或是以純文字檔開啟郵件，都是可以採用的防毒技巧。

（二）使用垃圾郵件處理功能，建立郵件中黑名單與安全白名單

垃圾郵件是病毒的溫床與傳播的媒介，表面上看似沒有危害，但是卻暗藏危機，目前許多機構都有防堵垃圾郵件的機制，但是垃圾郵件種類繁多，內容千奇百怪且數量驚人，雖然大多數的垃圾郵件都會被防堵在防火牆外，但有時防堵機制也會誤將正式郵件阻擋在外，有些垃圾郵件卻堂堂溜進信箱中，因此建立收件的黑名單，讓已偷渡的垃圾郵件在下一次會受到阻隔，而有意義的信件則能順利進入收件信箱之中。依筆者使用習慣對首次寄電子郵件給筆者的對方，筆者通常都會請他使用純文字檔的方式寄來，收信之後再將他列入安全名單（白名單）中，避免被垃圾郵件防堵機制阻擋在外。

（三）看到垃圾郵件，絕不因好奇開啟

許多垃圾郵件內容多為色情與商品廣告，既然收到垃圾郵件是無法避免的事，那麼如何有效的防堵是刻不容緩的事。而垃圾郵件在未被開啟之前，可以由幾點特徵看出其端倪。首先在開啟郵件之前，可以先從郵件主旨窺視信件大概的內容，若有懷疑則立即採用永久刪除的方式即同時按下Shift與Delete鍵將其刪除；近年來駭客更利用人的

好奇心，使用被入侵帳戶發信給通訊錄中的親朋好友散播病毒，內容如我要與你道歉，或提醒小人在附近的警訊信件，或告發有些商品可能致癌的謠言等引誘人開啟，所以對於某些主旨不明的友人郵件或是發信的主旨內容與你認識的人平常作為不符合者最好也加以刪除。除了主旨之外，檢查郵件發信時間也可以看出些端倪，有些發信時間為三更半夜或凌晨，可能與發信人的生活習慣不符合者也不要開啟，利用多重觀點的反覆檢驗，就可以明顯揭發假冒信，換句話說，如果親朋好友的信箱已經被冒用，散佈不實的內容，當然也是垃圾郵件，一旦開啟之後可能就會中毒。

（四）不使用自動閱讀信件內容的功能

信件即使隱藏病毒只要信件未被開啟，病毒也就無法發生任何作用。有些應用軟體有自動閱讀信件內容的功能，這個功能往往被駭客用為啟動病毒的引線，因此收信時，寧可先閱讀主旨確認安全之後在開啟內容。

（五）不點選電子郵件或即時通軟體中的網址

有些垃圾郵件採用純文字的方式躲過防火牆的偵測，進入收件信箱中，但是在內容中有連接的網址，透過文字吸引閱讀者點選上網，一旦連上網站，就形成一條安全無阻的通道，輕易地讓木馬程式或病毒程式偷渡進入個人電腦中蟄伏，伺機而動進行不正當的破壞電腦行為。

（六）轉寄信件前，請先將發信者的電子郵件地址刪除

利用電子郵件轉寄好文章與親朋好友分享時，往往將最初發件人或其他已收件人的電子郵件地址也隨著文章的分享而四處轉寄，這些有效的電子郵件很容易就成為廣告郵件公司發送郵件的目標，因此分享郵件時，請先將信件內的電子信箱刪除。若主動分享好文章給親朋好友時，也應採用密件附件的方式寄出，那麼收件人就看不到已被保密的電子郵件名單，降低好友的電子郵件地址外洩的可能性。

（七）在個人的通訊目錄的第一個名單上寫入假名，阻隔通訊錄被盜用

在個人通訊錄的第一位名單中製造假的、無意義的電子信箱，如姓名欄寫入“! Auto Sending Stop !”；電子郵件地址欄寫入bbb@bbb.com.jp製造假的電子信箱，以防自己的信箱不小心被植入任何惡意程式時，可以讓惡意程式以為是無效的郵件信箱的假象，防止通訊錄中好友的電子郵件被盜錄。

五、硬體隔絕

（一）需要使用網路時，才連上網路

目前在辦公室內使用個人電腦都是隨時保持連上網路的狀態，這種狀況猶如將所有的雞蛋放在同一籃子的危險；為何辦公室內一個電腦中毒之後，其他在相同網域上的電腦也會瞬間中毒？那是因為病毒往往就是透過網路分享方式迅速感染同一網域的其他電腦，這種情形最容易發生在同一機構中，造成公司整體運作的癱瘓。若仔細分析個人使用電腦的時間，會發現並非所有時間都需要連上網路，有時撰寫文件、計算成績或設計圖案時；甚至閱讀網路上的文章，都是可以在離線狀態下進行，並不需要一直保持網路連線，不需要使用網路時，可以採用網路停用功能，使自己暫時離開連線狀態，或多或少可以避免被駭客一網打盡的風險，同時也可以降低網路伺服器的負擔或是上網的費用。

（二）使用個人硬體防火牆，避免受到直接的攻擊

採用防毒軟體在執行時會佔用中央處理器的效能與記憶體空間，當電腦受到惡意程式的大量攻擊時，幾乎所有的工作效能都轉移去防堵病毒的攻擊，而使電腦效能大幅降低，甚至會造成電腦動不動就當機的現象，

讓使用者備感不便。使用硬體防火牆的好處在於它是獨立運作的裝置，遇到惡意程式攻擊入侵時可以獨立與惡意程式相抗衡，無需使用個人電腦的效能；猶如公司中董事長的特助，可以過濾分擔董事長的庶務，讓董事長可以不受干擾專心處理關鍵的事務，硬體防火牆也有相同的功效。

六、網際網路

（一）不瀏覽不知名的網站

上網就會中毒的情況常發生在瀏覽一些不知名的網站時，尤其是色情、賭博或是網購商品的網站。甚至連已經投入大量經費防堵任何惡意程式侵入的入口網站業者也在前些時候發現，只要使用者使用入口網站就會中毒的情況，這些惡意程式的入侵就連世界知名的網站都無法避免，而那些只圖商業利益的網站，是不可能投資保護其瀏覽者的權益。

（二）避免由線上直接安裝任何程式

有些系統可以由線上直接安裝程式，雖然方便也易有中毒的風險，寧可下載進行掃毒確認安全無虞之後再進行安裝。安裝過程中，也只選擇必要的項目進行安裝，不需要的附加項目則寧可捨棄不要安裝，除了可以節省硬碟空間外，也可降低被惡意程式植入的風險。

（三）線上系統的登出習慣

登入任何線上系統時，寧可以選擇以手動方式輸入帳號密碼，絶不使用複製與剪貼的方式進行，可避免遺留任何蛛絲馬跡，受惡意程式所利用。另外也不要選擇讓系統紀錄任何登錄的資料，以免帳號密碼遭竊，個人資料外洩而渾然不知；登錄任何系統時如報名系統或部落格等，也宜採用手動輸入的方式。使用任何需要登錄的系統完畢後，不要直接關閉網頁，而是要先點選登出後再關閉網頁，如此系統才會真正的關閉網路通道，因為有些系統在使用者網頁關閉或斷線之後，並不會馬上自動關閉系統，而是留有緩衝時間，過了緩衝時間後，系統發現使用者沒有任何的動作，才會自動關閉網路通道，而這段系統半放開放的空窗期，駭客就有機會入侵影響系統的作業，就像警衛暫時離開崗位去化粧室的空檔，已在旁伺機而動的小偷就會趁隙而入的狀況。因為在網際網路的世界中，駭客從未休息過也從未放棄任何微小的漏洞與機會。

（四）下載任何檔案之前請先進行掃毒

即時通軟體的方便性在於隨時可以傳輸檔案，因此受到許多網路族的青睞，然而這些進入個人電腦的檔案往往未經過掃毒檢驗，其中是否含有隱藏病毒並未知曉，另外由於是從親朋好友的帳戶傳輸過來，因此常使人疏於防備，往往在開啟檔案的一霎那，隱藏病毒就立刻發生效應，藉此侵入個人帳號，再由新的寄主擴大感染的範圍。筆者一次慘痛的疏忽經驗，差點影響整個機構的運作，幸好及時發現情況不對，經過查證確認是病毒後，立即透過電子郵件發佈警訊並採取清除措施，而後立即升級即時通的版本，並設定任何下載前的掃毒措施，以免重蹈覆徹。

除非必要否則不要任意下載網站的檔案，尤其是遊戲類的小程式，這些表面看似無害有趣的小程式往往暗藏著木馬程式，可以透過網路竊取個人電腦資料或是取得電腦的控制權，成為犯罪的工具，最近美國查獲一名使用網路犯罪的駭客，乃是利用木馬程式侵入他人電腦後，以借刀殺人的手法發動惡意攻擊，使特定對象的資訊系統癱瘓，藉此收取錢財，而被植入木馬程式的電腦則在使用者毫無知覺下成為犯罪的工具。

（五）使用兩種防木馬程式

誠如上述所言，病毒種類千變萬化，單一的防毒程式並無法保障個人電腦不被植入

木馬程式，且單一公司的防毒程式也無法完全阻隔不同種類的木馬程式，因此使用兩種不同公司的防毒產品可以截長補短，共同防禦摒除木馬程式。目前網路上大都推薦自由軟體Ad-ware 2007與Spybot-spy & destroy兩種。

七、結語

其實個人的生活素養與資安素養才是最重要的資安關鍵，無論任何的防毒程式，都無法阻擋因個人的惡習所造成的衝擊。個人若沒有正確的防毒觀念，不採用任防毒防駭措施，心術不正，常下載非法軟體，瀏覽色情網站，就像明末吳三桂打開山海關的大門，讓清兵長驅直入中原，造成明朝的滅亡慘劇，因此若個人不落實執行資安的防範於日常工作中，而是四處招惹病毒讓病毒長驅直入，那再好的防毒軟體終將無用武之地，最後落得個人資料外洩，或引起廣泛地中毒，是必然會發生的慘劇。總而言之，防毒防駭成功的關鍵不在於外在軟硬體的優劣，因為這些防毒措施是否發揮效果在於使用者的觀念與作法，而非軟硬體本身，唯有使用者的正確觀念與落實的作法，才能達到打擊防範病毒的散佈，與阻斷惡意程式的攻擊，最終達成零中毒與資料安全不洩漏的最佳狀態。