談電腦中毒與防毒

張真誠　　李維斌
中正大學資工系教授　　逢甲大學資工系助理教授

看過「網路上身」這部電影嗎？片中一連串令人生畏的陰謀是如何輕易地架構起來的呢？「ID4」這部電影是否耳熟能詳呢？還記得片中擊敗外星人的秘密武器嗎？你知道答案嗎？沒錯！就是電腦病毒。在電影劇情中，不論電腦病毒是陰謀分子的武器或是拯救世界的大功臣，都顯示出電腦病毒對電腦系統所造成的威脅與傷害，也因為這個特性使得「電腦病毒」成為一個令眾多電腦使用者揮之不去的夢魘。人人一聽到「電腦病毒」這四字便心驚膽跳，心中也掀起一連串的問號：病毒何時會發作？病毒會造成什麼破壞？我的電腦為什麼會中毒呢？要解答這些問題必須先對「電腦病毒」做一些觀念的介紹，而這也是本文的主要目的，本文將採不同於坊間常見的角度來介紹病毒，希望能藉此解答大多數人心中的疑惑與恐懼。

電腦病毒說穿了只是一串不懷好意的程式指令，因此我們以這個角度切入電腦病毒的世界，將使觀念變得容易些。底下的病毒樣本碼取材自 [Cohen, F. “A Short Course on Computer Viruses,” New York: Wiley 1994]。我們將以此為樣本做為貫穿本文的中心觀念。

```
Program V :=
{ goto main;
        1234567;

        subroutine infect-exectuable :=
          {  loop:
             file := get-random-executable-file;
             if (first-line-of-file = 1234567)
                  then goto loop
                  else prepend V to file; }
        subroutine do-damage :=
             { whatever damage is to be done }
        subroutine trigger-pulled :=
             { return true if some condition holds }
main:   main-program :=
             { infect-exetutable;
               if trigger-pulled then do-damage;
               goto next; }
next;
}
```

由以上的病毒樣本程式不難看出病毒運作的邏輯。首先病毒會去尋找未被感染的目標，目的是能廣為流傳。至於尋找寄宿主的方式則有常駐型，躲在記憶體中被動地等待獵物；或是直接感染，當病毒被啟動時立即尋找下一個目標。因為病毒都想要躲久一點，以便感染更多的檔案並增加其破壞力，因而牠不會一取得控制權就發作，通常病毒的身上都會設定一個發作的條件，而病毒程式碼會不斷地去檢查發作的條件是否成立？在取得控制權且尚未滿足發作條件的時期，病毒只會悄悄地感染其他未被感染的檔案，這段時期就是所謂的潛伏期，一旦發作條件成立，病毒就會毫不留情地進行預設的破壞工作。當然病毒在做這些事之前的先決條件是牠必須先被執行以取得控制權才能進一步做自己想做的事，否則一切免談。

接下來，我們將以此病毒模型解釋電腦病毒何時會發作？常常有人問病毒何時會發作？其實這個問題的意義不大，因為沒有人可以預期病毒設計者會在 trigger-pulled 這個部分設定何種發作條件，因此發作的日期可以是任何一天，甚至病毒作者可以設計一個計數器來控制發作的時機。至於第二個問題，病毒會對電腦做出什麼破壞？這個問題與前一個問題一樣無法有肯定的答案，因為它可能只是嚇嚇你但不作任何破壞，也可能讓你的系統回天乏術。這個問題與 do-damage 這個副程式的設計有關。其實當你對某種破壞行為質疑時，會設計程式的讀者不妨思考一下你能否寫出這種程式？沒有程式概念的人則可參考現有的軟體以進一步了解目前的軟體是否有能力執行該種迫害工作。舉例來說，是否有電腦病毒會破壞 BIOS 內的資料？這個答案是可能的，因為現在的電腦可藉由修改 BIOS 的內容以達到升級的目的，而這個動作是由軟體所執行的，因此破壞 BIOS 內容的病毒是存在的

至於為何會中毒呢？因為病毒是一段可執行的程式碼或指令，因此一隻病毒如果不去執行它的話，基本上牠是無害的。因此你會直覺的想到我會笨到去執行一隻病毒嗎？當然你不會，病毒也知道這一點，所以牠會隱藏自己的身分以欺騙你去執行它。接著問題來了，牠會隱身在哪裡呢？這個問題其實很簡單，因要病毒要活動的先決條件是要取得電腦的控制權，因此任何可能被執行的地方都是藏身的好地方。很顯然地.EXE 及.COM 就是兩個大目標，此外藏在啟動磁區(Boot)的小程式也是一個吸引病毒的好目標，當電腦開機時會自動讀取在啟動磁區中的小程式並執行它以便載入作業系統，因此當這個小程式被病毒取代後其影響自不在話下。此外，隨著電腦檔案的日益複雜，越來越多的檔案格式出現了，也給了病毒更多的藏身機會。例如.DLL 檔、ActiveX 及存在於 MS Office Word 或 Excel 等檔案中的巨集程式，都成為病毒的新樂園。由電腦軟體的趨勢來看，新的檔案格式伴隨著新型態病毒的出現已是不可遏止的歪風了。到此讀者應不難想像目前正炙手可熱的 PDA，因為可以執行一些應用程式，因此會遭受電腦病毒的攻擊也不是什麼稀奇的事了。到此為止，有興趣的讀者應有能力思索出還有哪些檔案或系統會引起病毒的興趣，當你發現時，請小心病毒可能已經在等你了。

除了隱身在可執行的檔案中外，還必須要有誘發使用者執行的慾望才行。這一點在微軟作業系統中特別容易，因為一般人的檔案瀏覽器會將已知的副檔名隱藏起來，也就是說 beauty.jpg.exe 在螢幕上所顯示的是 beauty.jpg，在誤以為是美女圖的情況下你會不會想看一下呢？此外藏身電子郵件之中則是最近最紅的病毒傳播方式，因為對親朋好友的信任，我們可能會毫不猶豫地走出錯誤的第一步，因此拜網際網路之賜，病毒可輕易地透過這個通路來遨遊全世界。

在如此險惡的環境中如何預防心愛的電腦中毒及解毒？很顯然地成為現在電腦族應具備的功夫之一。以下為一些老生常談的注意事項，希望各位讀者能因為本文的介紹而更能體認這些原則背後的理由：

- 不使用來路不明的軟體。
- 準備一張乾淨的開機片，以備不時之需。
- 不要使用盜版軟體。目前沒有百分之百的防毒方式，因此如果原版軟體含有病毒，至少可向原公司索賠，但如果是非法軟體，就毫無保障可言了。
- 定期使用掃毒軟體檢查電腦，並更新掃毒軟體的版本以因應接踵而來的新病毒。
- 盡量使用硬碟開機。因為磁片的流通性很大，所以很難確保它的啟動磁區是否無毒。

- 備份資料。不論是否是因為電腦病毒的考量，備份資料都是相當必要且重要的工作。
- 不要隨意在網路下傳軟體回來使用，要用的話也須先經過測試。
- 收到內含附加檔案的電子郵件時，可以先另存新檔，在經過測試之後才開啟它。