電腦病毒的基本觀念 – 個人電腦防毒篇（一）

資料整理自『PC 防毒/防駭 急救手冊 chap.1』學貫 鮑友仲著

一、什麼是電腦病毒?

有許多朋友都不清楚自己為什麼會中毒，甚至連病毒是什麼都不是很了解，只知道病毒會讓電腦受到很大的傷害。其實電腦病毒是一種電腦程式，它和你我平常所使用的 Internet Explorer、MS Word、Outlook 這些軟體一樣，都是屬於電腦程式的一種，只不過這種程式擁有如細菌般的「寄生」,「感染」,「繁殖」,「破壞」等特性，所以我們稱它為電腦病毒。

簡單來講，電腦病毒就是一段非常小的電腦程式(通常只有幾 KBytes 或幾百 KBytes)，它會不斷自我複製、隱藏、感染其它的軟體程式或電腦，然後伺機執行一些(破壞)動作。所以說它是一種簡潔具有破壞力的軟體。通常我們稱之為病毒的程式，便是因為執行它之後會影響使用者操作電腦，這包括嚴重的破壞資料、突然出現的畫面警式、喋喋不休的音樂干擾等等。只要是侵犯到使用者操作電腦的權利的話，基本上都可以說是病毒。

二、電腦病毒的起源

電腦病毒的起源最早在 1987 年，有一對巴基斯坦的兩兄弟，為自己創作的軟體而寫了一段保護程式，這段保護程式在發現有人盜拷軟體時，會自我複製到盜拷的磁片上，並將磁片的標籤名稱(VOLUME LABLE)改為「(C)BRAIN」，以警告使用者盜拷軟體。

三、電腦病毒的感染途徑

它們的感染途徑無非為下列兩種：

- 經由磁片或光碟片感染
  - ◎ 不小心使用中毒的開機磁片開機，你的電腦就感染了(開機型)電腦病毒。
  - ◎ 不小心執行磁片或光碟片裡而中毒的檔案，你的電腦就感染了(檔案型)電腦病毒。
  - ◎ 電腦系統已經感染電腦病毒，在你存取磁片或是將中毒檔案燒錄到光碟內時，這些病毒就趁機感染磁片與光碟媒介，然後再以前面一、二的方式傳染出去
- 經由網路感染

  這裡所謂的網路包括辦公室內的「區域網路」與大家常用的「網際網路」。當你從網路上取得一個中毒的檔案，或是收到的電子郵件裡的檔案中了電腦病毒，在不經意執行瀏覽或開啟它們之後，電腦病毒就會感染你的系統。

  不管是上述哪種感染途徑，這裡必須要澄清一點:「**電腦病毒一定**

要在電腦系統才能傳播」。

四、電腦病毒會造成哪些破壞

電腦病毒只會對電腦系統造成破壞，它不會影響人體的健康，依據電腦病毒的破壞程度，我們大致可以分成以下幾方面:

- 系統速度變慢與當機
- 不尋常的錯誤訊息出現。
- 程式載入時間比平常久。
- 可執行檔的大小改變系統。
- 記憶體容量忽然大量減少。
- 記憶體內增加來路不明的常駐程式。
- 磁碟壞軌突然增加。
- 硬碟容量變小
- 網路系統當機
- 資料毀損與電腦無法使用
- 檔案的內容多出了一些奇怪的資料。

五、電腦病毒的種類

- 檔案型電腦病毒

檔案型電腦病毒顧名思義就是病毒會寄生在可執行檔(副檔名為 .com 和 .exe 的檔案)內，而病毒寄生的方式，是把病毒程式碼放在原來檔案一開頭執行的地方，這樣當你在執行這個檔案時，就會先執行到電腦病毒程式，然後病毒就可以偷偷進入你的系統檔案型電腦病毒感染檔案的方式檔案型電腦病毒依傳染方式的不同，又分成「非常駐型」，「常駐型」、「千面人」和「隱形」四種類別：

- **非常駐型**：非常駐叫病毒會在你執行中毒的程式時，馬上去搜尋磁碟內其它的檔案，然後立刻傳染給它。
- **常駐型病毒**：常駐型病毒會躲在系統記憶體中，只要執行任何可執行檔，它就會進行感染動作，散播效果比非常駐型還要顯著。
- **千面人病毒**：實千面人病毒也是常駐型病毒的一種，不過它運用特殊的程式寫作技巧，使得它再次感染別的檔案之後都會換一個面貌，就好像有成千種面具一樣。之所以這樣做的目的就是要干擾防毒程式檢查病毒的能力，以增加病毒的散播力。
- **隱形檔案型病毒**：隱形檔案型病毒卻是讓感染後的檔案看起來和沒感染一樣。基本上隱形檔案型病毒所需使用的技巧比千面人病毒更高，而且隱形檔案型病毒躲過防毒程式檢查的能力更強。在前幾年引起轟動的 CIH 電腦病毒，其實就是隱形檔案型病毒的一種，所以

才能在常時躲過成堆防毒軟體的偵測，散播到全世界造成非常大的災害。

- 開機型電腦病毒

開機型電腦病毒就是一種寄生在硬碟或磁片開機啟動部位的病毒。一般說來，硬碟的開機啟動部位分為「**硬碟分割表**」與「**啟動磁區**」兩個部分，電腦病毒入侵之後會把原先的硬碟分割表挪到後面位置，這樣在開機的時候便會先執行病毒程式。

- 混合型電腦病毒

混合型電腦病毒就是同時兼具有「檔案型」與「開機型」電腦病毒的特色於一身，也就是混合型電腦病毒會同時寄生、感染你系統的可執行檔與開機區域。由於混合型病毒的雙重感染特性，所以這種病毒具有相當大的傳染力，例如早期台灣曾經流行的大榔頭病毒(Hammer)，就是混合型病毒的代表作。

- 巨集病毒

巨集病毒又名為「文件病毒」，因為它是伴隨文件檔一起散播的。最有名的巨集病毒，就是前一陣子的瑪俐莎病毒，它造成許多公司內部網路系統當機。巨集病毒是目前最熱門的話題，因為它跟大家常用的 MS Office 軟體息息相關，主要是利用軟體本身所提供的巨集能力來設計病毒，所以凡是具有寫巨集能力的軟體都有巨集病毒存在的可能，如 MS Word、Excel、Power Point 都相繼出現它們的巨集病毒。

- 特洛依(Trojan)木馬程式

特洛依木馬(Trojan Horse)程式其實嚴格來說不應該算是電腦病毒，因為它沒有病毒「複製」、「感染」的特性，不過因為這類程式通常都含有破壞力在裡面，所以現在也漸漸把它歸類為電腦病毒的一種。

日前特洛依木馬程式最常被電腦駭客廣泛用來入侵電腦系統。當駭客在你的電腦系統放入特洛依木馬程式之後，它便可以透過網際網路竊取你電腦裡面的資料，而在今日網際網路如此普及的情形下，特洛依木馬程式對使用者的威脅，已經攀升到病肖威脅排行榜的第二位。

- 蠕蟲病毒/電腦病蟲(Worm)

蠕蟲病毒(Worm)對使用者來說，該算是近來病毒威脅排行榜的第一位，你應該聽過娜妲病毒 Nimda、思坎病毒 Sircam、聖誕節病毒 MALDAL、璩美鳳事件的「如果偷怕光碟出 DVD 版」的「蘇活族」病毒 SHOHO、賓拉登病毒-這些名字吧!這些都是屬於蠕蟲病毒。蠕蟲病毒可說是完全因應網際網路而誕生的，它會利用網路上其它各種管道(主

要是利用「電子郵件」)，自動將病蟲本體擴散出去。

- 第二代電腦病毒

第二代電腦病毒，基本上完全是屬於網際網路下的產物，所謂的第二代電腦病毒就是指用 Java Applet 或 ActiveX Control 所設計的惡意程式，這類程式在你用瀏覽器瀏覽它們的網頁時，會讓 Java Applet 或 ActiveX Control 程式耗用你電腦的資源，使得你的系統因為資源不足而當機，並且常常會在視窗旁邊跑出一些奇怪的畫面，破壞你電腦的運作。

除此之外，有些惡意的 Java Applet 和 ActiveX Control，還會利用某些系統上的漏洞來暗地進行破壞動作，這些惡意程式可能會摧毀資料、竊取你的密碼、資料等等，所以大家逐漸把這類程式也列為電腦病毒的一種。

六、防毒應有的觀念

培養防毒的觀念，以降低感染電腦病毒的機率，加上電腦有安裝使用一些不錯的防毒軟體，可使一般人達到「百毒難侵」的境界，因此，建立防毒應有的觀念，是非常必要的基礎。

- 為何會感染到電腦病毒

看過前幾節的介紹之後，應該知道電腦病毒其實只是個「電腦程式」，而我們都知道程式必須要「執行」之後才會有所動作，就好像你要使用 Microsoft Word 文書軟體，首先必須要「執行」它然後才可以使用它工作一樣。既然所有電腦程式都必須要「執行」之後才會動作，當然電腦病毒也不例外。

所以，為什麼會感染到電腦病毒，答案其實很簡單，就是「你執行到一個含有電腦病毒程式的檔案」。舉例來說，當你從網路上或是從學校、朋友那邊拷貝了一個檔案回來，如果這個檔案裡面被感染病毒，在不知情的狀況下「執行」這個檔案，就等於是間接執行到病毒程式一樣，既然執行到病毒程式，當然病毒就會被啟動，所以就中了電腦病毒;簡言之，電腦會中毒絕對是因為你執行到了被感染病毒的檔案或磁片 。

依據目前電腦媒介的使用狀況，我把中毒的原因簡化成五種情形，分別是：

- ■執行到網路上中毒的檔案:從網路下載回來的檔案裡面已經被感染病毒，執行它之後，你的電腦就會中毒。
- ■執行到磁片 、光碟內中毒的檔案:毒，執行它之後，你的電腦就會中毒。
- ■使用中毒的磁片開機:磁片的啟動磁區(boot sector)已經中毒，你

使用中毒的磁區開機，你的電腦就會中毒。

■開啟中毒的巨集文件:巨集文件裡面已經被感染病毒，開啟它 之後就會執行裡面的巨集病毒程式，所以你的電腦就會中毒。(註:所謂巨集文件就是如 word、Excel 等等之類，支援巨集功能的文件。)

■ 收到的電子郵件含有病毒行它之後，你的電腦就會中毒。

■ 收到的電子郵件含有病毒:電子郵件含有的附檔已經被病毒感染，執 行它之後，你的電腦就會中毒。

■ 娜妲 Nimda 病毒變相的第六種感染途徑其實除了上述五種感染途徑以外，前一陣子造成大災難的娜妲 Nimda 病毒，它創造了第六種的變相感染途徑，那就是**利用微軟 Windows 作業系統的系統漏洞**，來修改網站 htm，.html 及.asp 等檔案為病毒格式，使得你瀏覽到這些病毒網頁時，系統就會中毒。不過嚴格來說，娜妲 Nimda 第六穫利用系統漏洞的感染方式，只能算是「執行到網路上中毒的檔案」途徑的變相而已，所以我沒把它列為第六種感染途徑。

七、預防中毒的基本觀念

知道為什麼中毒的原因，我們就可以針對這些情形，盡量避免去執行一些動作，以降低中毒的機率。以下我列舉一些預防中毒的基本觀念，提供大家參考。

■ 不要隨便執行、開啟電子郵件內的檔案

電子郵件自從有了夾帶附檔的功能之後，幾乎已經變成病毒傳播媒介的第一名，第一個利用電子郵件傳播而聲名大噪最有名的例子當屬「瑪俐莎」(Melissa)病毒莫屬。還記得常時短短不到一個小時的時間,「瑪俐莎」病毒就藉由電子郵件散撥五萬封病毒郵件出去，造成當時全球許多公司的網路系統癱瘓，由此可見電子郵件的傳染威力。

自從瑪俐莎病毒的「成功案例」之後，目前幾乎所有新款的電腦病毒，不論是思坎 Sircam、尼姆達 Nimda、求職信、Gone・・・等等，幾乎都利用電子郵件列為病毒傳播散發的基本途徑，別因為一時好奇打開含有病毒的郵件附檔，不良的習慣會讓你的電腦常被病毒入侵。

所以要預防中毒，絕對不要隨便執行、開啟電子郵件內的檔案，尤其是你不認識的人所寄來的檔案。不要因為一時好奇心作祟，就打開陌生郵件的廣告文件或免費軟體，有很多中毒的例子都是利用這樣感染的。如果是熟人所寄來的資料檔案，使用之前也請先用掃毒軟體檢查，更保險的做法是你先發一封確認信給對方，請他回函究竟有沒有寄檔案給你，因為現在很多病毒都會自動竊取使用者電腦通訊錄的資料，然後

假冒名字寄病毒信給感染者的朋友，而收信者心想是熟人寄來的檔案應該沒有問題，就開啟文件被感染到病毒。因此，當初「瑪俐莎」病毒就類似這樣「老鼠會」的傳播方式，短短時間就席捲全球，造成許多網路系統的癱瘓。

謹守絕對不隨便執行、開啟電子郵件內夾帶的檔案，就可以降低出電子郵件感染到電腦病毒的威脅，而如果你可以杜絕從電子郵件中感染到病毒，軌可以減少 60%以上感染到病毒的機率，這點大家千萬要牢記。(其實筆者有一個習慣，只要看到郵件附檔是執行檔，我就一律不開啟此封郵件，因為寧可少玩軟體、也不感染病毒是我的信條，提供各位參考。)

■ 不要隨便下載不知名網站內的檔案

如果要大家都不要從網路下載檔案的話，我想你會說乾脆不要使用網際網路好了．…當然我也不會要大家這樣做，而是要大家不要下載「不知名」網站內的檔案。同樣一套微軟的 Internet Explorer 瀏覽器，可能在網路上有成千上萬的網站可以供你下載，但是如果我問你，從 Hinet 下載放心，還是從另一個「HaHa 阿沙不魯」網站下載，哪一個網站取得的檔案你比較放心?

答案當然是從 Hinet 取得放心，因為你知道 Hinet 這種知名的網站，絕對不會故意放一個有毒的檔案讓你下載，他們一定會在放入網站前先掃描過這個檔案有沒有感染到病毒，確定無毒後才放上網去。所以要預防中毒的第二個觀念:不要隨便下載不知名網站內的檔案，如果你可以在比較知名的網站取得的話，盡量去這些地方下載，迫不得已只有這些「HaHa 阿沙不魯」網站有提供的話，下載回來請先用掃毒軟體檢查一遍。之前大家聞之色變的 CIH 病毒，就有人將它假冒為 Windows98 Service Pack 及 ICQ 中文化程式．…．等等名稱，供人下載。結果下載回來的人都完全以為檔案沒問題，於是執行後就感染到 CIH 病毒，在該月 26 日病毒發作時把硬碟資料損毀。大家對於下載回來的檔案可要提高警覺。

■ 不要隨便使用來源不明的軟體與文件

學生最常犯的一個毛病，就是喜歡把學校電腦裡面的軟體拷貝回家使用。住在我樓上鄰居的小孩，電腦因為中 CIH 病毒被毀，他跑來問我說「我都沒有使用網路啊!為什麼還會中毒呢?」

結果我用掃毒軟體幫他檢查的結果，是他從學校拷貝的遊戲軟體感染了 CIH 病毒，導致牠的電腦被毀。所以防毒的第三個觀念:不要隨便使用來源不明的軟體與文件，雖然使用原版軟體不一定就 100%一定不會中毒，但是使用原版軟體中毒的機率絕對在 5%以下。如果你一定無法、不可避免要拷貝軟體回來使用的話，也請你確定檔案來源是無毒的，拷貝前最好先用掃毒軟體檢查一遍。另外，你可能會帶作業去學校

寫，在學校儲存的文件檔案，回家後要開啟前，請先用掃毒軟體檢查一遍。

千萬要記住，常你在公眾地方所使用的電腦系統，是很難保證在你使用前、或使用後不會感染到電腦病毒，建議你避免使用這些電腦所取得到的檔案與文件。

■ 絕對不要用外來的磁片開機，並將 BIOS 開機順序設定為 C:優先

除了你電腦自己製作的開機片，或是原版軟體裡面所附的開機片之外，其它任何外來，不管是學校、公司或任何地方取得的磁片，絕對不要用它們來開機。開機型病毒的破壞力通常都比其它類型的病毒來得大，甚至不小心用中毒的磁片開機後，你的硬碟資料或 windows 系統就毀了，讓你連後悔或解毒的機會都沒有。所以，絕對不要用外來的磁片開機，除非你能 100%確定這外來磁片無毒。

平常將 BIOS 開機順序設定為 C:優先

■ 不要隨便開啟 office 的巨集功能

微軟的 office 套裝軟體在巨集病毒出現之後，就開始加入巨集病毒的預防措施，每次在文件開啟時都會問你是否要執行巨集功能。舉例來說，圖???是一個巨集病毒的樣本。

假如你不知道這個 Word 文件含有病毒，不小心將它打開的話，微軟的 Office 軟體(從 Office97 之後)會出現一個視窗跟你說文件包含有巨集，問你是否要開啟，這時請選擇「關閉巨集」按鈕，千萬不要隨意啟動 Office 的巨集功能，因為很可能該巨集就包含有病毒程式碼在裡面。

■ **勇於修正系統漏洞**

類似的 Worm 所攻擊的系統漏洞，其發明者都是根據已經被公開的系統漏洞設計，並沒有所謂新鮮的花樣。像 Nimda 攻擊的漏洞之一還是在 Nimda 出現前半年就已經被公佈與修正的 IIS 問題。這些 Worm 的出現只是在驗收網管人員平時辛苦的成績。

八、使用防毒軟體就再也不會感染病毒了嗎?

了解了預防中毒的基本觀念，可能有讀者心裡會想:「這麼麻煩幹嘛?買套防毒軟體不就得了?安裝它之後就可以不怕病毒的入侵！」基本上有許多電腦使用者都有類似的錯誤觀念，以為自己電腦裝了防毒軟體以後就可以百毒不侵，從此不會被病毒感染，可以肆無忌憚的隨便使用網路上下載的檔案，或是任意拿不知何處取得的軟體回家使用。防毒軟體是可以讓你不受病

毒入侵沒錯，不過它是讓你不被「**已知的病毒**」入侵，也就是說，防毒軟體它可以檢查檔案是否中了「目前已經知道的電腦病毒」，然後避免你不小心執行到這些中毒檔案而感染到系統。

以目前世界上每天平均 6 隻以上新病毒誕生的機率來看，防毒軟體其質是沒有能力讓你絕對不會感染病毒的(新病毒防毒軟體就無法預防)因此裝了防毒軟體之後，你的電腦還是有可能會中毒。所以使用防毒軟體的目的是讓我們不被過去的病毒侵害，建立基本應有預防中毒的觀念是降低你感染病毒的機率，兩者是相輔相成，不是互相排擠。以筆者為例，我每天幾乎都必須從網路上取得資訊或下載檔案，好幾年沒中過毒，不是我的防毒軟體多先進，而是我本身有建立基本的防毒觀念，與養成時時更新防毒軟體的病毒碼檔案。(所謂的病毒碼就是防毒軟體的病毒資料庫，它是用來讓防毒軟體比對檔案或磁碟是否有感染病毒的重要資訊。)

所以千萬不要以為裝了防毒軟體就不怕病毒入侵，也不要以為自己絕對不會感染病毒就不裝防毒軟體，因為根據我的經驗，通常上述這兩種人反而被病毒感染的機會是最大的」！

九、中毒了怎麼辦？

請熟記以下的六字口訣：

關(Step 1；關閉電源)

開(Step 2；以乾淨磁片開機)

掃(Step 3；用防毒軟體掃瞄病毒)

除(Step 4；若偵測到病毒，則刪除之)

救(Step 5；若偵測到的是硬碟分割區或啟動區病毒時，可用"硬碟緊急救援磁片"救回資料，或用乾淨 DOS 磁片中的 FDISK 指令，執行 FDISK/MBR 以救回硬碟分割區資料；另可在 A 槽中執行 A>SYS C:(C 為中毒磁碟)以救回資料；若不行就只有重新格式化硬碟了

防(Step 6；好了！您的電腦安全了。不過為了預防未來不再受到病毒之侵害，建議您經常更新你的防毒軟件，以建立完善且堅固的病毒防疫系統)