淺談電腦病毒及其防治方法

水產養殖系　林志遠

一、前言

電腦尤其在微電腦科技方面的進步，不僅已深入社會各層面，其未來雄厚之潛力更是不容忽視，舉凡圖形、影像、聲音、文字處理、統計計算、繪圖、排版、動畫簡報、自動監測控制、資訊數位化之功能等等，在各界之應用極多。對於研究者而言，如能善用電腦之協助，則不僅能大爲節省文稿之重覆繕打、資料建立與計算及圖表製作之時間，更能提昇個人在上述三項工作上之品質，甚至可利用電腦快速及大量記憶之功能，經由資料庫管理、線性規劃及模擬軟體來事先評估試驗研究之可行性、流程設計及預期結果等。也因此個人電腦在本所之成長極爲驚人，大量使用之結果，確實提昇了本所之研究環境。但近年來猖獗之電腦病毒實是最頭痛的問題，若稍有不察，不僅個人辛苦建立之資料毀於一旦，且許多關聯使用者之資料恐也不保。筆者在總所常見有許多位同仁蒙受電腦病毒之苦，但由於大多缺乏基本電腦操作能力及關於此方面之觀念，即使一再遭受電腦病毒之禍害，仍然不知如何以對。因此，作者便整理出一些工作經驗及參考許多刊物有關電腦病毒的專欄，擇其重點略作介紹。

二、何謂電腦病毒

對於電腦而言，所謂的電腦病毒就是一組程式碼，能夠將自己感染在其他的程式中，並且不斷的藉機會來傳染給其他更多的程式並伺機破壞程式及資料。目前幾乎每一個電腦使用者都免不了會遭遇電腦病毒之問題，因此，如何去預防病毒的感染以及如何去解救中毒的電腦，也就成爲大家所關注的重點。

大體上說來，對電腦病毒的防治可以分爲三個階段：一爲『預防』，二爲『偵測』，三爲『解毒』。由於電腦病毒種類實在太多，如果僅希望依靠解毒軟體來清除病毒的話，那是永遠也無法解決的，因爲目前的解毒軟體都是針對已知之病毒特性來進行掃毒，對於新的病毒則需發展新的解毒程式。因此，較好的方式是在『預防』和『偵測』兩方面上下工夫，特別是『預防』工作，例如可採用一些綜合性的防禦軟體，但最重要的還是自己平常養成使用電腦之良好習慣，如此才能夠應付日新月異的各種病毒。

三、常見之電腦病毒種類及徵狀

(一)依傳染途徑區分

病毒若以傳染途徑來區分的話，最主要可以分爲『系統性病毒』及『檔案性病毒』兩種。系統性病毒通常存於作業系統裡面，例如磁片的 boot 磁區。只要您使用感染過的磁片開機，則您所得到的作業環境就是潛伏有病毒的作業系統了。在這種情形下，無論您使用任何的 DOS 指令 (如 DIR,TYPE) 都有可能將病毒感染到其他磁片上！檔案型態的病毒顧名思義是潛伏在您的執行檔中 (如.EXE,.COM)，一旦您執行了含有病毒的檔案時，此型病毒就開始工作了！至於病毒病發的結果，輕則常駐在記憶體中伺機感染其他檔案，重則毀掉所有的資料。一般而言，檔案型態的病毒並不會去感染系統，而系統型態的病毒並不會去感染檔案。但是最近已經有『混合型』的病毒被發現，此型的病毒感染能力強，破壞力大，令人防不勝防。

(二)依傳染方式區分

病毒的傳染方式有很多，但最常見的方式就是『常駐式』。也就是說當執行了一個含有病毒的程式時，病毒本身就常駐在記憶體中，當再執行其他的程式時，病毒便藉由這個機會傳染過去。另外一類的病毒則並不常駐在記憶體中，而僅在含毒的程式被執行時順便感染磁碟機中的其他檔案。

(三)依病毒毒性區分

病毒感染的目的，通常就在於『發作』的時刻。當然也有一些例外的情形。最常見的『爆發』情形就是洗掉磁碟機中所有的資料，有些病毒會將硬式磁碟機改寫成只能存取而不能開機，也有一些病毒會在一定的時間發出音樂

或訊息干擾您的工作，另有一些病毒會把您磁片的册標(Volumn label)都改成固定的文字，更有一些病毒會去塗寫主機CMOS的資料，使您的電腦速度降到最慢或無法開機或硬碟無法進入等。

目前在美國一地所流傳的PC及相容電腦病毒估計有數百種之多，並且正以每個月 3～10種的『產量』在快速增加。近半數都曾經在台灣出現過了。表一列出常見之病毒名稱、傳染情形及其破壞力等資料。

表一　常見之電腦病毒名稱、傳染情形及其破壞力

病毒名稱	感染範圍 1	2	3	4	5	6	7	8	損害能力
DOOM II	▲	▲	▲	▲	△	▲	▲	▲	O,P,F,L
Hammer	▲	△	▲	▲	△	△	▲	△	O,P,F,L
New Jerusalem	▲	△	▲	▲	▲	△	△	△	O,P
Sunny(1-5)	△	△	▲	△	△	△	△	△	P
Virus-101	▲	▲	▲	▲	▲	▲	△	△	P
Taiwan	△	△	▲	△	△	△	△	△	P
Sunday	▲	△	▲	▲	▲	△	△	△	O,P
AIDS	△	△	▲	△	△	△	△	△	P
Disk Killer	▲	△	△	△	△	▲	▲	△	B,O,P,D,F
Jerusalem	▲	△	▲	▲	▲	△	△	△	O,P
Stoned/Marijuana	▲	△	△	△	△	▲	△	▲	O,B,L
Jerusalem-B	▲	△	▲	▲	▲	△	△	△	O,P
Friday 13th COM	△	△	▲	△	△	△	△	△	P

『感染範圍』：
1 是否會常駐在記憶體中
2 是否感染 COMMAND.COM 檔
3 是否感染 .COM 檔
4 是否感染 .EXE 檔
5 是否感染 Overlay 檔
6 是否感染軟碟 Boot 磁區
7 是否感染硬碟 Boot 磁區
8 是否感染硬碟 Partition Table

『損害能力』：
O 影響系統程式的執行
P 破壞執行檔或 Overlay 檔
F 洗掉磁碟機（全部或一部份）
L 直接或間接的破壞檔案的連結
B 破壞或洗掉 Boot 磁區
D 破壞資料檔
▲：有感染
△：未感染

四、如何預防電腦病毒感染

(一)一般方法

由於本所大部份之個人電腦多爲個人所使用，其操作環境單純，因此只要保持良好的使用習慣，幾乎就可以得到相當高的安全性，以下提出幾種應保持之習慣來預防電腦病毒的感染：

1、重要資料應備份，並存放不同地點。
2、不使用外來的作業系統磁片開機。
3、隨時保留一片 DOS作業系統磁片，並貼上防寫貼紙。
4、儘量不使用來路不明的應用軟體。
5、使用新軟體時，應隔離測試，並先以掃毒程式檢查。
6、常用的工具及病毒防禦軟體應另外做磁片備份並貼上防寫貼紙。
7、硬碟要經常做 MIRROR (PC-TOOLS 程式之一)，並將MIRROR檔存放於軟碟中，並習慣配合使用PCFORMAT(同前)來格式化磁片。

(二)使用病毒預防軟體

病毒預防軟體通常是整套防禦系統的第一線。其任務在於如何使病毒無法進行感染、破壞的工作。一般而言，這類的預防軟體通常有下列 4大類之各別或混合功能：

1、監視程式常駐：

大多數的檔案型態病毒幾乎都以常駐的型式來伺機感染，因此只要有效的防止程式常駐就可以應付大多數的病毒。由於平常使用到的軟體亦可能是常駐程式，因此這一類的防毒程式通常都允許使用者定義『允許常駐』的名單以避免誤判。

2、防止程式直接寫入磁區：

對於爆炸性或系統性的病毒而言，其感染的動作都必需經由磁區的絕對讀寫來達成。因此如果能夠有效的阻止程式直接寫入磁區，即可防止大多數的爆炸性病毒之破壞。

3、防止執行檔被改寫：

一般檔案型態的病毒在感染時，一定要將檔案加以改寫。因此若能阻止程式去更動EXE/COM 檔的內容，則大多數的檔案型態病毒都無法感染，方法是將檔案屬性設定

爲 read only。

4、禁止硬碟被寫入：

此類程式執行後可以讓硬碟有類似貼上防寫貼紙的功能。在測試某些不需寫入任何檔案的程式時，以此種程式加以防護最爲安全。

五、潛伏電腦病毒之偵測、解毒法

(一)病毒偵測軟體

病毒偵測軟體主要用於檢查系統的檔案及作業系統是否已經感染了病毒，對於防止病毒的蔓延具有相當的實效。此外對於來源不確定的軟體亦可以先用偵測軟體做預先檢查，以收預警的效果。此類的軟體功能也分爲 4項：

1、對檔案做核對：

在系統沒有病毒侵入時，將完整的檔案的 CRC 或 CHECK-SUM 值保存起來。如果檔案遭到病毒侵入的話，則檢查時就會發現到錯誤。基本上這個檢查的方法相當的確實有效，但仍需小心留意確定原始檔案是無毒的，免得白忙一場。

2、掃描系統區：

這類的軟體通常會去核驗系統的 BOOT 區，如果發現有系統性病毒時就會提醒您來注意。

3、掃描執行檔：

此類的軟體會掃描可執行檔，並且會將『病毒標本』的數值來和所掃描的程式做比對，一旦發現您的程式是含有病毒的話就會提出警告。

4、掃描記憶體：

此類軟體會掃描記憶體中是否已經有『登記在案』的病毒常駐著，如果有的話就提出警告、或逕行銷毀病毒。

有許多病毒之預防、偵測常駐型程式，爲避免佔用太多主記憶體空間，因此常縮短各種病毒之採樣比對碼，雖然達到其小型化的目的，但對於偵測病毒之正確性就相對降低，可能造成一無毒軟體因被誤判有毒而無法執行的情況（此類程式如TRACER, GILLETTE,VB3等都曾被發現過誤判，但所佔比例極低）。而使用者在遇到此類程式發出之警告聲時也常手忙腳亂、不知眞假，此時應以非常駐型之完整病毒偵測程式加以確認，若確定是爲誤判，則必須移去該病毒偵防程式，才能執行欲執行之應用或工具軟體。

(二)病毒解毒軟體

通常病毒偵測軟體皆有其相對之解毒軟體配合，以便消滅前者所偵知之病毒種類，例如SCAN與CLEAN,TRACER與HACKER,SCANVIR與HUNT VIR 等。首先解毒程式會先清除記憶體中之病毒，而後對於檔案型病毒，掃除多餘之病毒碼而恢復原程式檔案長度，對於系統型病毒則清除boot磁區中之病毒碼，並可能重建 FAT表及硬碟分割表，以求完全根除。一些解毒程式在病毒消滅後，甚至可使磁碟具有免疫能力，其方法爲在適當磁碟位置，寫入可讓外來病毒偵測其已存在之識別碼來騙過電腦病毒，以免感染眞正之病毒碼。

六、電腦病毒破壞後之資料補救

檔案型病毒由於祇破壞某些特定檔案且大多爲執行檔，祇要不是使用原版磁片，通常也容易被重新恢復，雖然可以用 PCTOOLS查看有那些檔案被刪掉，甚至恢復，但因檔案多已被感染，故還是應重新拷貝一份爲妥。

破壞力大之系統型病毒是比較棘手的，除了平常應進行例行備份工作外，資料之補救有幾個方法可姑且一試，但並不保證一定有效，端視電腦病毒之殺傷程度而定。

1、使用 DOS 之 RECOVER 程式

2、使用Norton Utility之NDD(Disk Doctor)程式

3、使用 PCTOOLS 之 REBUILD 程式

前兩種方法較適用於軟碟磁片，補救回來之檔案不論是完整的或破碎的（視病毒種類），其檔名僅爲一代表序號，可在查看內容後更改檔名。第三種方法軟硬碟皆適用，且最佳狀況可使被毀滅的磁碟恢復破壞前舊觀，但相對地有許多限制且事前工作也不可或缺。REBUILD程式必須與其他PCTOOLS程式如MIRROR,PCFORMAT合用，每日關機前必須執行MIRROR，在磁碟被病毒破壞後，則可以REBUILD 恢復，若破壞嚴重者則可先以PCFORMAT程式（注意不可用其他format程式）格式化磁碟，再執行REBUILD 。其他各程式之操作細節請自行參考有關手冊。

七、結語

電腦病毒的橫行，除造成使用者困擾外，也常引起電腦廠商與購買者間之糾紛，許多電腦販售廠常以電腦病毒來作爲其電腦品質低劣

及維護服務欠佳的推托之辭，可能因一部低品質硬碟而指責使用者使用不當或感染病毒，然後便可讓其爲所欲爲、動不動就重新format硬碟，使你未備份的寶貴的資料毀於一旦，而且這種情形經常循環發生，造成莫大損失，不得不愼；但反過來說，使用者也可能因經常感染電腦病毒而指責廠商，使其疲於奔命。另一種比較嚴重的情形是由於使用者之種種使用不當，不知反省錯誤，卻怪罪於電腦病毒，或可稱之爲「恐電腦病毒徵候羣」，在此列述一簡單且正確之方法如下：

(一)當硬體無法正常運作時（指開機後到可鍵入指令前之間）

1、檢查電源、排線、開關是否正常。

2、硬碟無法進入時，檢查bios設定。以 DOS 磁片開機再檢查硬碟，若出現HDD control error 或 HDD failure，可能導因於磁碟控制卡，除非老手可自行拆機外，應尋求電腦廠商之協助。

(二)當軟體無法正常運作時

對於常使用之軟體突然變得不正常，先以病毒偵測程式掃瞄，再確定檔案之完整性，必要時重新安裝。

(三)鄭重推薦使用病毒預防軟體（如前述）。

由於病毒實在是太多且解不勝解，因此必須強調『預防重於解毒』的重要性！目前所流行的病毒不外乎是破壞您整台硬碟的資料，或是感染可執行的檔案而已，對於有良好備份（Back-Up)習慣的使用者來說威脅並不大。在國外有一些非常可怕的病毒，他們可能會將您的會計或文書資料任意改一兩個數字、文字而不動聲色，也可能把一長篇大論的報表在印出時填入幾個錯字，當您發現了這個病毒存在的時候，往往已經有幾個月的錯帳及資料整理不出來，而這種病毒未來也可能發生在您身上。

備註：

有許多病毒預防、偵測、掃除之電腦病毒公益軟體(Pubilc Domain, PD) 將存放於本所連線電腦之 C:\VIRUS 目錄下，並附有各程式簡易說明檔.DOC，有機會連線請自行取用，其他未盡事項請連絡資訊系。