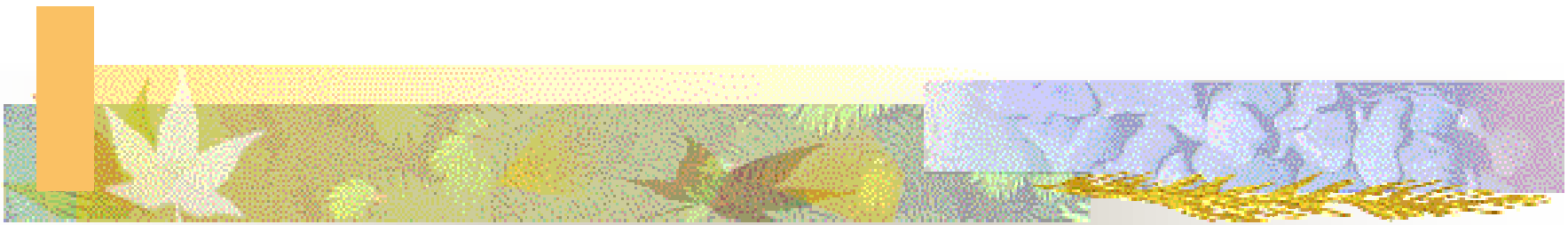
電腦病毒
Computer Virus



中正電機所
古忠平

大綱

- 簡介
- 定義
- 病毒的產生
- 病毒的影響
- 病毒的類別
- 傳播
- 預防
- 介紹病毒

簡介

- 簡單的說，電腦病毒只是一個電腦程式。它與你常用的文書處理軟體、你常玩的電腦遊戲，都一樣 ，都是電腦程式罷了。只不過電腦遊戲可以讓你享受聲光的刺激，文書處理軟體是設計來讓你打字排 版列印出來，而電腦病毒是設計來破壞電腦裡的軟體，讓你的工作不能正常進行。

- 什麼是病毒碼(Virus Pattern)??

  病毒程式中擷取一小段獨一無二且足以代表這之病毒的二進位（Binary Code）程式碼，作爲掃毒程式辨認此病毒的依據。這段獨一無二的二進位程式碼就是所謂的病毒碼。

第一支電腦病毒程式

- 1987年的C-Brain大腦病毒
- 作者：巴基斯坦兄弟
- 目的：防止他人盜拷他們的軟體
- 病毒發作：吃掉盜拷者的硬碟空間
  (給盜拷者一點小小的教訓)

定義

- 電腦病毒是一段很小的電腦程式，它是一種會不斷「自我複製」及「感染」的程式，在傳統的DOS環境下，通常它會寄存在可執行的檔案之中，或者是軟、硬碟的開機磁區啓動部份，隨著被感染程式由作業系統載入記憶體而同時執行，病毒因此獲得系統控制權；但在視窗系統中出現的文件巨集病毒則是附著在文件檔中，且其感染之對象亦限於文件檔。
- 簡單來說，會使檔案長度增加刪減、不尋常的錯誤訊息出現, 而且可以不斷的去感染其它程式的程式，我們都可以通稱它爲電腦毒。
- 根據病毒創造者的動機，這些指令可以做出任何事，其中包括顯示一段訊息、刪除檔案或精細地改變數據。有些情況下，電腦病毒並沒有破壞指令的企圖。但取而代之就是毒病佔據磁碟空間，中央處理器時間或網絡的連接。

病毒的產生

- 電腦病毒被製造有很多不同的原因。例如：病毒是由僱員故意製造用來向 公司報復，表示自己的不滿；有些就是用來慶祝某些節日；甚至有些是由宗教狂、政治狂製造的 ，目的就是想從這途徑發表自己的聲音。有些程式編寫員製造電腦病毒的目的是爲了表現自己的 能力或挑戰自己或別人，他們只是想看看病毒會帶來甚麼後果或者看看是否有人能夠把病毒清除 ，其實這種做法是錯誤運用自己的能力。
- 其實很多〝病毒〞只不過是程式中的錯誤。當一個程式 編寫員設計一個新程式時，很多時都會注要不到其中的小問題或錯誤(bugs)。
- 其實大部的〝錯誤〞病毒都沒有破壞性，所以正確來說這些錯誤病毒應該被定義爲〝錯誤(bug)〞而不是〝病毒〞 。

電腦病毒的影響

- 有些電腦病毒例如 Format C (macro virus)及Stoned Daniela， 當它們被觸發時，會無條件地把硬磁碟格式化及刪除磁碟上所有系統檔案。

- 有些病毒， 如Monkey(Stoned. Empire. Monkey)及AntiEXE，會感染主啓動記錄(Master Boot Record MBR)及DOS啓動磁區(Dos Boot Sector)，之後它會降低記憶體及硬磁碟的效能，直至當我們的用電腦時螢光幕上顯示一些訊息 或有其他損壞。

病毒的類別

- 開機型病毒（Boot Strap Sector Virus)
- 檔案型病毒 (File Infector Virus)
- 複合型病毒 (Multi-Partite Virus)
- 千面人病毒 (Polymorphic/Mutation Virus)
- 巨集病毒 (Macro Virus)

開機型病毒

- 開機型病毒是藏匿和感染磁碟片或硬碟的第一個磁區，即我們平常所說的Boot Sector。開機型病毒藉由開機動作而侵入記憶體，若你用已感染的磁片開機，那麼病毒將立即感染到你的硬碟。
- 開機型病毒又可以分爲：

a. 傳統開機型病毒。傳統開機型病毒大多經由磁碟傳染，進入電腦後再伺機傳染其他檔案，最有名的例子是米開朗基羅病毒。

b. 隱型開機型病毒。隱型開機型病毒感染的是硬碟的開機磁區，它僞造開機磁區的資料，使防毒軟件以爲系是正常的。

c. 目錄型開機型病毒。它只感染電腦的檔案配置表(FAT)，一但你的檔案配置表被破壞後，你的電腦檔案讀寫就會不正常，甚至失去檔案。

檔案型病毒

- 檔案型病毒通常寄生在可執行檔(如 *.COM, *.EXE等)中。當這些檔案被執行時, 病毒的程式就跟著被執行。我們常見的檔案型病毒有Connie系到病毒與耶路撒冷(Jerusalem)系列病毒等等。檔案型的病毒依傳染方式的不同, 又分成非常駐型、常駐型和隱形三種:

a. 非常駐型病毒(Non-memory Resident Virus) : 非常駐型病毒將自己寄生在 *.COM, *.EXE或是 *.SYS的檔案中。當這些中毒的程式被執行時，就會嘗試地去傳染給另一個或多個檔案。
常駐型病毒(Memory Resident Virus) :常駐型病毒躲在記憶體中，其行爲就好像是寄生在各類的低階功能一般(如 Interrupts)，由於這個原因, 常駐型病毒往往對磁碟造成更大的傷害。一旦常駐型病毒進入了記憶體中, 只要執行檔被執行, 它就對其進行感染的動作, 其效果非常顯著。將它趕出記憶體的唯一方式就是冷開機(完全關掉電源之後再開機)。

b. 隱形檔案型病毒：它會把自己植入作業系統裡面，當程式向作業系統要求中斷服務時，它就會感染那個提出要的程式，而且看起來不像被感染的樣子。

複合型病毒&千面人病毒&巨集病毒

- 複合型病毒兼具開機型病毒以及檔案型病毒的特性。它們可以傳染 *.COM, *.EXE 檔，也可以傳染磁碟的開機系統區(Boot Sector)。由於這個特性，使得這種病毒具有相當程度的傳染力。一旦發病，其破壞的程度將會非常可觀！例如：台灣曾經流行的大榔頭(Hammer)，歐洲流行的Flip翻轉病毒皆是。
- 千面人病毒可怕的地方，在於每當它們繁殖一次，就會以不同的病毒碼傳染到別的地方去。每一個中毒的檔案中，所含的病毒碼都不一樣，對於掃描固定病毒碼的防毒軟體來說，無疑是一個嚴重的考驗！如Whale病毒依附於.COM檔時，幾乎無法找到相同的病毒碼，而Flip病毒則只有2 byte的共同病毒碼（好像戴面具只剩兩個眼睛露出來）。
- 巨集病毒是目前最熱門的話題，它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Word、Excel、AmiPro都相繼傳出巨集病毒危害的事件,在台灣最著名的例子正是Taiwan NO.1 Word巨集病毒。

病毒的傳播

- 蔓延的主要方式：透過軟件的分享
- 利用網路：電子郵件(附加檔案的方式)
- 翻版CD :如果用家用的是正版軟件，病毒就不會發作；相反如果用的是反翻軟件，病毒程式就會執行〔破壞系統〕。

我中毒了嗎？

- 若電腦常會當機, 但用掃毒軟體又掃不出有病毒存在, 該怎麼辦?
  - 若經掃毒程式掃描後未發現病毒存在而仍會經常當機,有可能是硬體不穩所造成的,不一定是病毒所造成的現象, 建議您先檢查是做什麼動作而造成當機, 再請電腦工程師檢查造成當機的原因是硬碟或軟體方面。

我中毒了嗎？

- 發現電腦用DOS開機磁片開機後,主記憶體爲何不到640kb,是不是病毒?
  - 如果使用無病毒感染之開機磁片開機後,主記憶體仍不到640k,應該是硬體部分使用了這些記憶體,而非程式或病毒導致.

我中毒了嗎？

- 有何簡易的方法，判斷電腦是否中毒？
  - 其實電腦少根筋時，是有跡可尋的，由於電腦病毒會影響電腦系統, 所以, 當使用者發現使用的電腦有下列狀況時，應該要考慮是否有病毒感染的問題：

- 檔案長度、日期改變
- 系統執行速度下降
- 檔案無故消失、I/O 動作改變
- 奇怪的錯誤訊息、演奏美妙音樂
- 系統經常無故當機

預防

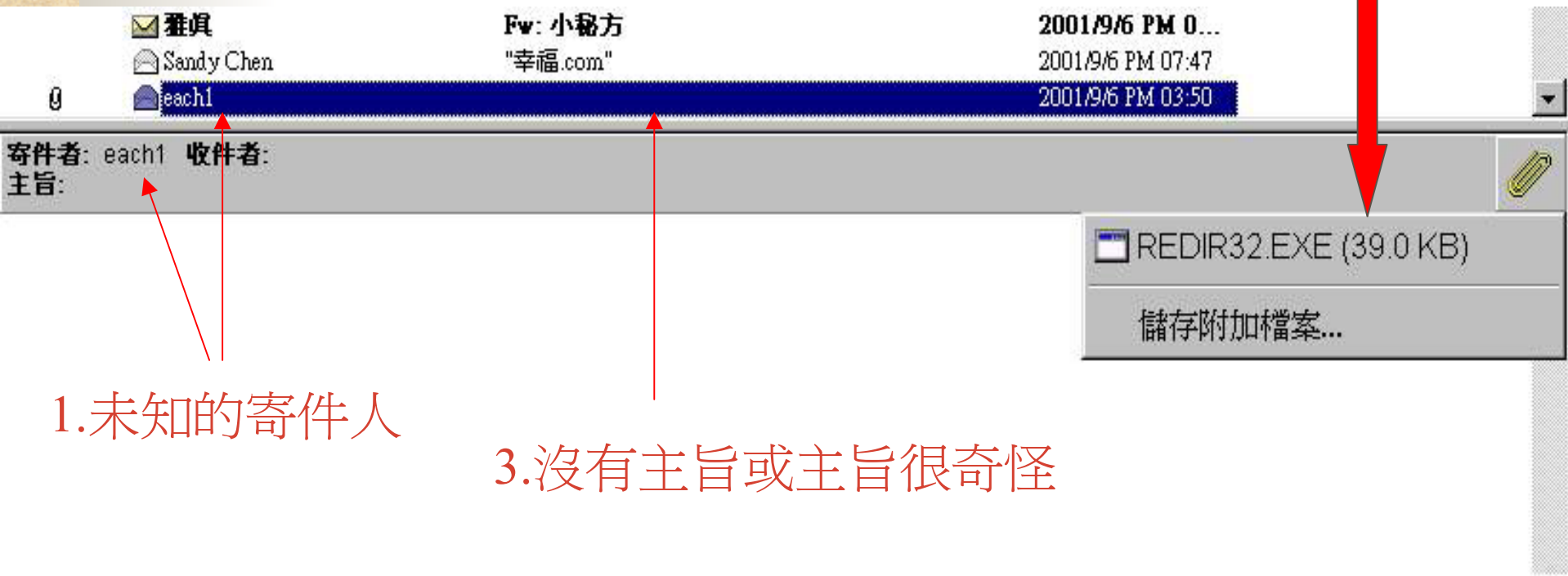
- 電腦病毒的防治包括了兩方面，一是預防，二是治毒。古人有云，預防勝於治療，所以預防電腦病毒對保護你的電腦系統免受病毒破壞是非常重要的。但是，亡羊補牢，爲時未晚也，治毒和預防都不可忽視。

1. 提倡尊重知識產權的觀念，支持使用合法原版的軟件，拒絕使用翻版軟件，只有這樣才能夠確實降低使用者電腦發生中毒的機會。
2. 平常就要將重要的資料備份起來，畢竟解毒軟體不能完全還原中毒的資料，只有靠自己的備份才是最重要的。
3. 建立一張緊急救援磁片，而且是乾淨可開機，DOS的版本與硬碟相同，同時裡面還要有以下程式：FDISK.EXE、FORMAT.COM、UNFORMAT.COM、SYS.COM、UNDELETE.EXE、SCANDISK.EXE、掃毒軟體所備份的啓動磁區及硬碟分割表檔案。如果你有PCTOOLS或Norton Utility等軟體，用它們來幫助你做一張緊急救援磁片，它們甚至可以還原CMOS資料，或是災後重建資料。(別忘了貼上防寫標籤。)
4. 不要隨便使用來路不明的檔案或磁碟，就算要使用，先用掃毒軟體掃一掃再用。

5. 隨時注意特殊的檔案(如COMMAND.COM、EMM386.EXE、WIN.COM、SMARTDRV.COM等)的長度與日期，以及記憶體使用的情形。利用MEM.EXE或MEMMAKER等來檢查傳統記憶體(Conventional Memory)有否640K(655360Bytes)？一般來說， 假如您的 BIOS 沒有挪做其它用途的話， 那您的電腦八成是中毒了！
6. 避免用軟碟開機，甚且是別人的磁片。
7. 準備一些好的防毒、掃毒、解毒軟體，並且定期使用。
8. 建立正確病毒基本觀念，瞭解病毒感染、發作的原理，以提高自己的警覺心。
9. 學習災後重建資料的技巧，別以爲DIR看到一堆亂碼就救不回來了，其實有很多軟體修復資料的功能很強大，學會使用它們是很有幫助的。

判斷可疑的電子郵件

2.附加檔案小於100kB



1.未知的寄件人

3.沒有主旨或主旨很奇怪

防止您個人的Outlook Express電子郵件帳戶散發病毒

- 請在您的通訊錄上新增一個『！０００００』，請注意，這個新聯絡人除姓名外不要再輸入任何資料．這個聯絡人會出現在您通訊錄中的第一筆，若是病毒企圖由您的通訊錄中大量的自動傳 送email，您的電腦會給您一個錯誤的訊息如下：

  “這個訊息無法傳送．一或多個收件者沒有電子郵件帳號．請確認您的通訊錄並確認所有的收件者的電子郵件帳號．”
- 你可以按下OK鍵讓這個訊息(病毒)不要送出．當然因爲無法自動送出，所有的信件會存在您的”草稿或是”寄件匣”中．立即把所有存在”草稿或是”寄件匣”中的信件刪除即可解決這個問題，同時不會繼續散播病毒．請現在就這麼做，並告訴您所有通訊錄中的人．

中毒了怎麼辦

請熟記以下的六字口訣：

1. 關(Step 1；關閉電源)
2. 開(Step 2；以乾淨磁片開機)
3. 掃(Step 3；用防毒軟體掃瞄病毒)
4. 除(Step 4；若偵測到病毒，則刪除之)
5. 救(Step 5；若偵測到的是硬碟分割區或啓動區病毒時，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爲中毒磁碟)以救回資料；若不行就只有重新格式化硬碟了
6. 防(Step 6；好了！您的電腦安全了。不過爲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)

如何知道電腦受到病毒感染?

- 電腦執行速度比平常緩慢。
- 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。
- 磁碟可利用的空間突然減少。
- 檔案名稱、副檔名、日期、屬性被更改過。
- 檔案的內容多出了一些奇怪的資料。

病毒的生命週期

1. 創造期
2. 孕育期
3. 潛伏感染期
4. 發病期
5. 根除期

防毒公司

- 賽門鐵克　　上網瀏覽一下吧！！

  http://www.symantec.com/region/tw/
- 趨勢科技

  http://www.trend.com.tw/

電算中心積極爭取防毒軟體經費與趨勢科技股份有限公司簽定OfficeScan防毒軟體全校授權一年，安裝 Windows 3.X/ 95/ 98/ ME/ 2000 等作業系統都可經由瀏覽器連結至 **http://antivirus.ccu.edu.tw**，下載最新版OfficeScan用戶端防毒軟體。安裝OfficeScan可以避免病毒散播，減少個人電腦資料毀損的機率，且可隨時更新病毒碼，多一份防護少一份損失。

病毒介紹

I Love You病毒

- I LOVE YOU是一隻只會影響微軟系統的MICROSOFT OUTLOOK與OUTLOOK EXPRESS的電腦病毒，它是不會影響使用MACINTOSH或LINOX操作系統的電腦。如果是使用後者電腦，打開I LOVE YO U的電子信是沒有問題的，但不要打開它附帶的檔案。

  “I LOVE YOU”電腦病毒是滲透一位電腦用戶的地址薄，自發地向遇襲者的聯絡人發出這封信，這項病毒也可以使用即時語言與網絡交談系統作祟，如ICQ系統等。所以不要接受清談室的檔案

Black Firday (黑色星期五)

- 這隻病毒於1987年在以色列希伯萊大學(Hebrew University) 電腦中心出現，並於１９８９年１月１３日星期五在英國及世界各地爆發，這病毒會在每月的13號並且該日是星期五的日子才會發作。當這病毒出現後，很多人士便以這病毒爲藍圖，並製造出很多很出品的病毒，如Jerusalem, New Jerusalem, Payday。

介紹最新病毒

Code Red紅色警戒 (別名：TROJ_BADY.A)

- 數十萬台電腦成爲駭客攻擊跳板，(別名：TROJ_BADY.A)爆全球駭客危機
- Code Red紅色密碼只針對安裝微軟IIS網頁伺服器的作業系統進行感染，包括：Windows NT Server、Windows 2000 Server
- 特性：第一，當電腦系統日期爲：20~28之間時，該蠕蟲會自動執行，對美國政府網站(www1.whitehouse.gov)發動阻絕式服務攻擊；第二，當電腦系統日期小於20，此蠕蟲會任意產生IP位址，並透過80 PORT 來散播和複製自己，微軟IIS的使用者需至微軟網站下載修復程式。

紅色警戒變種病蟲 CodeRed.v3(CodeRed.C)

病蟲特徵：

1. 攻擊架在Microsoft NT 上的IIS 4.0、IIS 5.0 及Windows NT，Windows 2000作業系統。
2. 建立超過300個步驟去尋找有弱點的主機，並且自行複製。

病蟲造成的影響：

1. 進行阻絕服務-（Denial of Service）攻擊
2. 駭客能完全地遠程遙控受感染電腦主機

狡猾善變的Sircam思坎病毒

- 病毒風險級數：中度風險
- 破壞力持續上昇趨
- 主要藉由電子郵件進行散播，電腦族一旦執行電子郵件夾帶的附加檔案，電腦將遭病毒感染。之後，病毒會尋找通訊錄中的名單，自動發送病毒郵件。
- 此病毒最爲狡猾之處爲，郵件主旨及附加檔案名稱並不固定

總結

- 防毒軟體（定期更新病毒碼）
- 小心電子郵件（100KB）
- 定期備份資料