新世紀電腦殺手——電腦病毒（Computer Virus）

國中組應用科學科第一名

台北市和平國民中學

作　　者：林公立、董大偉
指導教師：王桂棹

一、研究動機

電腦病毒曾在世界各地引起一陣恐慌，隨著電腦的普遍，病毒到處感染，造成許多使用者憂心，因此引起我們對病毒的興趣，想了解到底什麼是病毒？而展開一連串的研究。

二、研究目的

我們試圖為病毒下一個完整定義，再對各種病毒做深入的研究，到底什麼是病毒，病毒如何侵入？如何進行破壞？甚至如何製造？都是我們想知道的，但是重點仍在探討病毒程式的構架，希望使用者能對病毒有深入的了解，進而防止病毒的破壞。

三、研究器材

1.PC/ XT/ AT

四、研究過程

我們在進行研究之前必須對電腦病毒有大概的了解，至少一些所能得到的資料要儘量研討，但我們發現台灣似乎連一本研究病毒的書也沒有，在缺乏資料的情形下，研究只好從基本做起。（可供參考的資料見附錄一）

1.開始研究：

我們一開始必須蒐集病毒，好對各種病毒都能詳細了解，我們在學校中蒐集了數種病毒，將這些受感染的程式和未受感染的程式做比較，發現受感染的程式較未受感染的程式大很多，可知多出的部分就是病毒的主體，像13號星期五就是這種，這種病毒可隨著程式執行時一起執行，因為他是附在原程式中的，使自己執行即可達到複製的效果。

2.侵入方法：

關於病毒的侵入方法，研究後我們得到一些較可能的方法：

2-1.由程式的拷貝，若拷貝到一個受感染的程式，一旦叫此程式，病毒就會一直擴散。

2-2.由已受感染的程式在電腦中執行，當病毒常駐記憶體後，將感染以後進入的任何程式。

2-3.在經過MODEM獲取一個新的程式時，若程式本身曾受病毒感染，一旦執行那也會使病毒擴散開來。

3.破壞方法

在受感染的程式執行時，病毒只做感染其他程式的工作，到一個特定情形病毒才發作，像特定日期、時間；破壞通常是刪除檔案或修改檔案一類的方法。

4.病毒本身

從表1中可發現，病毒分為：

⑴系統性病毒

⑵檔案性病毒

①一般檔案性病毒

②爆炸性病毒

③特洛伊式病毒（Trojan horse）

⑶混合性病毒

以下分別討論：

4-1系統性病毒

所謂系統性病毒是藉著磁碟機的BOOT或PARTITION來感染,也就是說病毒將磁片的BOOT SECTOR 或PARTITION部分改變為叫自己的程式，而進入記憶體後，最後再呼叫原BOOT，使使用者無法警覺，所以無論DOS讀進記憶體與否，病毒都早已侵入記憶體中，病毒修改磁碟的中斷向量，所以凡是一有磁碟運作，病毒就進入磁碟中，達到感染的效果；而一方面系統性病毒會縮小MEMORY SIZE，使用者所能用的SIZE也就縮小，縮小的部分即為病毒本身所放的記憶體位址，所以並不容易察覺。

4-2檔案性病毒

檔案性病毒是附加在檔案之中，隨著檔案執行而進行破壞，而方式相當多，以下討論檔案性病毒所衍生出的型態：

4-2-1一般檔案性病毒

一般檔案性病毒是寄生於使用者的程式中，而常駐於記憶體，並修改中斷向量，而到一特定的情況才發作，平時則進行感染。

4-2-2爆炸性病毒

此種病毒不常駐，不更改中斷向量，而在執行時就做感染其他程式的工作，感染完成後則判斷是否符合發作條件，是則破壞，否則執行使用者程式，此病毒可由檢查檔案大小發現。

4-2-3特洛伊式病毒（Trojan horse）

特洛伊是附於一個特定的軟體內，通常不主動感染其它程式，只藉拷貝傳播，此病毒多半為了懲治非法拷貝而用。

4-3混合性病毒

此病毒為最難防治的，包括了系統性病毒及檔案性病毒的特色，他們不經由BOOT感染，何時變為系統性及一般檔案性的時

間不定，使得防毒解毒，並不容易。

以上對表4所做的解說。

我們以最簡單的爆炸性病毒來討論病毒的工作：

病毒附加在未感染的程式之前成為受感染的程式，當受感程式執行時，病毒會測定現在是否遇上特定情況，若是則進行破壞，若不是則做感染的工作，之後在呼叫使用者所叫的程式，一切行為完全正確，使使用者無法察覺。

（可供參考的資料附錄二）

由以上研究結果得知病毒至少須要具備幾種功能，才可稱為病毒，這些功能是：檢查特定情況，找尋目標、複製、感染、破壞，其餘還有些非必要的功能：檢查是否重覆感染、檢查是否被人發現，這些功能可使病毒更具效率。

5.受感染的程式及磁碟

受感染的程式最明顯的現象就是檔案迅速增大，執行速度極慢，而磁碟有不正常寫入或記憶體變小，就表示你的電腦危險了。

6.消毒方法

因為系統性病毒只感染磁碟的BOOT，所以解毒只須以DOS之SYS指令將未受感染的BOOT拷貝回去即可，若是檔案性病毒則要把受感染的部分除去，但、EXE檔還要改進入點之指標回原位。

7.病毒的正面功能：

病毒的正面功能可由多方面討論，較實際的用處是此時多了很多的程式設計師、學生開始研究相關軟體，使電腦界提昇了程度，而病毒有何開發價值呢？例如：自動化開發軟體、程式製造器、更正系統，有相當多的開發價值。

五、研究成果

這一次對病毒的研究，算是圓滿達成了，只是有許多相關層面，

礙於經費及傷害面積大，而無法一一研究，希望能有人繼續參與病毒的研究，若將以上之構想荒廢，實在甚為可惜。

六、結論

病毒的研究到此告一個段落，這次研究收穫最大的就是我們自己，對於我們想知道的也都得到了答案，對此研究也有很深的感想，電腦的貢獻是衆所皆知的，而任何事皆有正反兩面，為善作惡動念都在方寸之間，防毒、防拷的工作，只有好好從人心做起，否則是沒有用的。

附錄一、病毒附加在程式中的情形（針對十三號星期五）

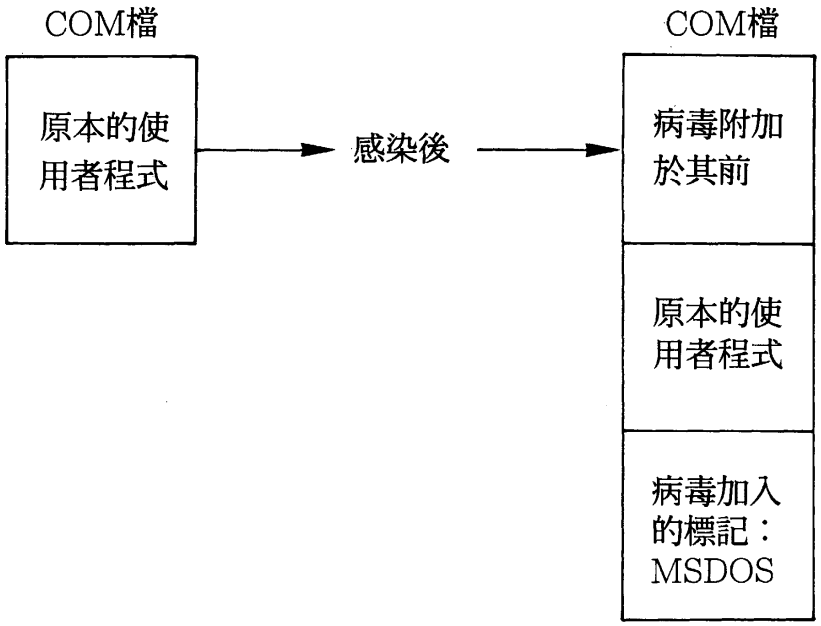
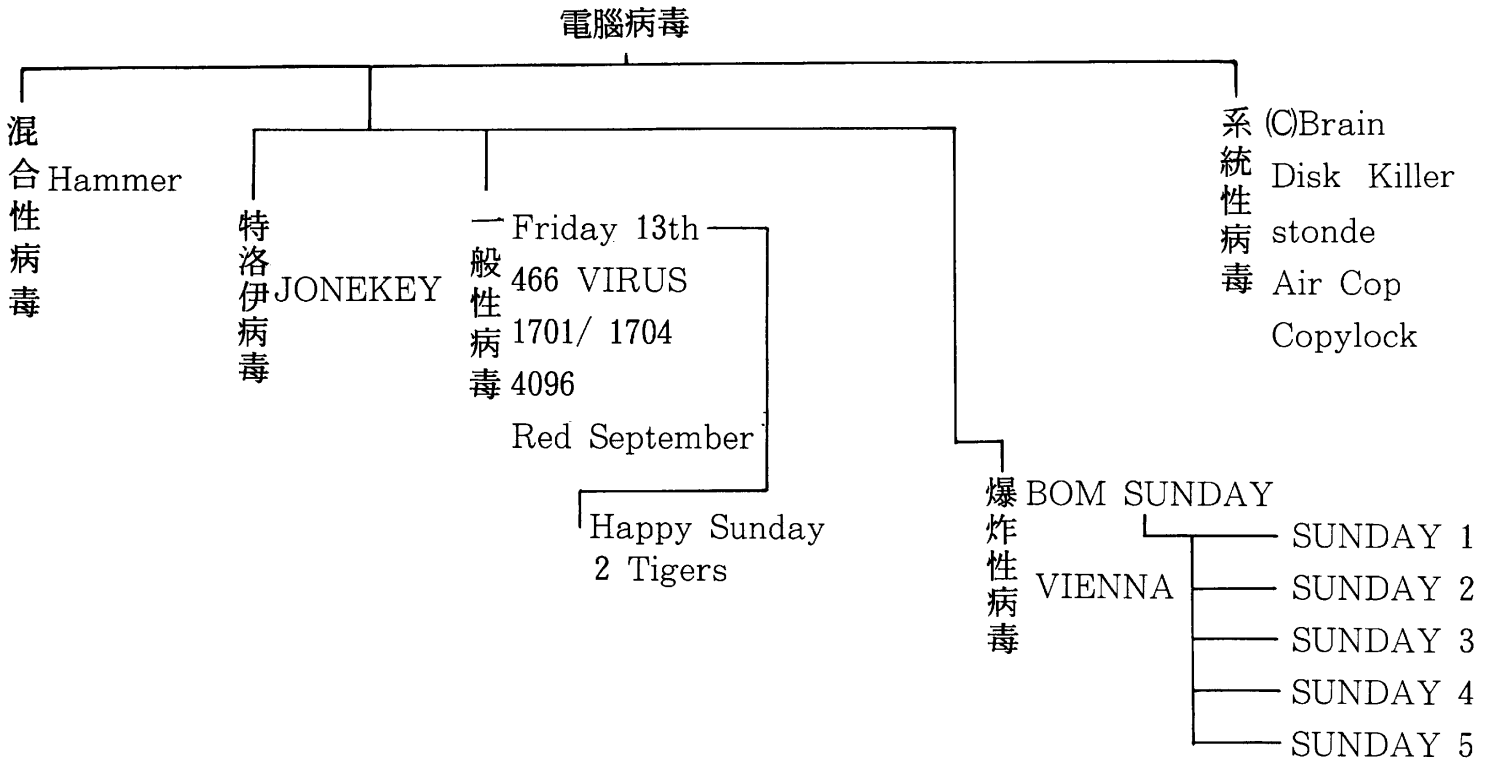


表 4. 電 腦 病 毒 分 類 表
(英 文 部 份 為 具 代 表 性 的 病 毒)



附錄二.病毒虛擬碼及流程（爆炸性病毒病毒虛擬碼）

```
check-system-date                    ；查閱日期
 {
  call int 21h ah=1ah
  if month=day+4--> return （0）
  else return(1)
 }
 kill-disk                           ；破壞磁碟
 {
  call 13h ah=03h
  write ′ h′  to file allocation table and file directory
 }
  find -file                         ；找尋可侵入的檔案
 {
  call int 21h ah=11h
  find *.exe or *.com
  return ( file name )
 }
 check-file-mark ( file name )  ；檢驗病毒標記
{
 open file
 read mark word
 if mark=abc -->return ( 0 )
 else return(1)
 }
attack-program ( file name )        ；感染
{
 open file
 append virus code
 write virus mark -->abc
```

```
  }
main-program                          ;主程式
{
  return-number=check-system-date
  if return-number=0 goto kill
  :again
  find-file
  return-number=check-file-mark
  if return-number=0 goto again
  attack-program
  goto end
  :kill
  kill-disk
  :end
}
```

1.各程序功用：

check-system-date：由int 21h 檢查現在日期，若月數＝日數＋4則傳回0－>符合

kill-disk　　：破壞FAT及 ROOT，將前12個磁區填入h蓋過FAT及ROOT.

find-file　　：找尋＊.exe或＊.com檔

check-file-mark　：檢查是否已感染，標記為abc

attack-program　：感染程式

main-program　　：主程式，分別呼叫以上各程序。

2.程式流程

程式由main-program進入，先檢查系統時間是否符合條件，若符合則進行破壞，就是將FAT及ROOT蓋過去，否則尋找可侵入的檔案侵入並寫下標記，就完成工作。

中斷函數及功能

中斷號碼	輸入參數	功能	傳回值
以下配合5-1系統性病毒 為何更改磁碟中斷向量？ 因INT 13H管磁碟的各項動作，更改後磁碟動作即可被發現 ，因此一執行磁碟指令極有可能被病毒感染			
13H	（AH＝00H）	重設磁碟	
	（AH＝01H）	讀取目前磁碟狀態	AL
	（AH＝02H） DL磁碟 DH磁頭 CH磁軌 CL磁區 AL數目 ES:BS	讀取特定磁區資料	AH：磁碟狀態 CF＝0成功 CF＝1失敗
	（AH＝03H） DL,DH CH,CL AL同上 ES:BS 緩衝區	寫入特定磁區資料	AH：磁碟狀態 CF＝0成功 CF＝1失敗
	（AH＝04H） 其餘同上	驗證磁區	AH：磁碟狀態
	（AH＝05H） DL磁碟 DH磁面 CH磁軌	FORMAT磁區	AH：磁碟狀態

	BS:BX C,R,H,N		
	AH＝08H （AH＝09H） （AH＝0AH） （AH＝0BH） （AH＝0CH） （AH＝0DH） （AH＝10H） （AH＝11H） （AH＝12H） （AH＝13H） （AH＝14H） （AH＝15H） （AH＝16H） （AH＝17H）	硬碟功能常式	AH：磁碟狀態 其餘略
	（AH＝4EH） CX＝屬性 DS:DX＝ 路徑名稱 所在位置	找名稱相符檔案	磁碟傳送區 BYTE 0-20 預留給函數4FH 用 BYTE 0-20 屬性 BYTE 0-20 最後更改時間 BYTE 0-20 最後更改日期 BYTE 0-20 檔案長度低位元組 BYTE 0-20 檔案長度高位元組 BYTE 0-20 檔案名稱及延伸檔名

以下配合5.病毒本身檢查特定情況等			
21H	(AH=2AH)	取得日期	CX: year DH: month DL: day AL: 星期
	(AH=2CH)	取得時間	CH: 時 CL: 分 DH: 秒 DL: 秒/ 100
	(AH=4EH) CX=屬性 DS:DX= 路徑名稱 所在位置	找名稱相符檔案	磁碟傳送區 BYTE 0-20 預留給函數4FH用 BYTE 0-20 屬性 BYTE 0-20 最後更改時間 BYTE 0-20 最後更改日期 BYTE 0-20 檔案長度低位元組 BYTE 0-20 檔案長度高位元組 BYTE 0-20檔案名稱及延伸檔名

被病毒感染後增大的byte數

No	英文名稱	中文名稱	感染後增加的byte數
系統性病毒			
1.	©Brain	大腦病毒	磁片中多三個bad Clusterr記憶體減少七個64K=448KB
2.	STONED	石頭病毒	感染 BOOT 佔 0.5 KB

3.	Air cop	空中警探	感染 BOOT 佔 0.5 KB
4.	CopyLock	防拷病毒	感染 BOOT 佔 0.5 KB
系統性病毒			
5.	FRIDAY 13TH	十三號星期五	COM檔案增加 1813 BYTES EXE 檔案每次執行增加 1808 BYTE 原因：EXE檔不做5 BYTES的 ′ MSDOS′ 標記因此少 5 BYTES
6.	2 TIGERS	兩隻老虎	檔案增加1808 BYTES
7.	HAPPY SUNDAY	快樂星期日	檔案增加 1631 BYTES
8.	1701/ 1704	落淚病毒	檔案增加1701-1074 BYTES
9.	Progkiller	程式殺手	檔案增加1728-1733 BYTES
10	VIENNA	維也納病毒	COM檔案增加 1813 BYTES
11	DISK KILL 2	磁碟殺手	COM檔案增加708-743 BYTES

PS.本資料部份由DEBUG及PC TOOLS實驗獲得部份經由各雜誌獲得，由於手中尚缺部份病毒程式，有些無法實地核對，於結稿（79.3.7）後將繼續設法獲得其餘病毒，將於科展當天提供最新資料。

評語

本作品對目前流行的電腦病毒了解相當深入，對於預防之道亦十分中肯，基於預防而作的研究，應有正面價值。然而對國中程度而言

，此研究終究命題過於複雜而難以週延。希望作者多注意基本學術知識，以期更上層樓。