幻影殺手——電腦病毒

國中組應用科學科第三名

臺北縣立江翠國民中學

作　　者：顏正昇、吳協恩
指導教師：翁志誠、黃山港

一、研究動機

隨著科技的進步，資訊的發達，電腦這一種新時代的產物，漸漸地成為這新時代的新寵兒，雖然電腦的速度快，功能強，但是對於外來的入侵者——「病毒」（Virus），却沒有半點的防衛能力，不禁令人驚奇，到底這小小的病毒如何侵入、繁殖、和進行可怕的破壞行動？

二、研究目的

本實驗在探討國內常見的電腦病毒，了解它們的特性及行動，讓大家了解電腦病毒的真象，進而撰寫一套防毒程式來抑制電腦病毒。（註：本實驗在探討電腦病毒的一切行動，將會牽涉到電腦病毒的程式碼，為了免除引起另一場病毒之風，所以本實驗所反組譯並加註解的電腦病毒的程式碼，將不對外公布。）

三、研究設備器材

㈠個人電腦。
㈡作業系統：MS-DOS。
㈢工具程式：Turbo Assembler。
　　Symbolic Debug。

Person Editor Ⅱ。

㈣病毒標本。

四、研究過程或方法

㈠收集電腦病毒。

㈡利用Symbolic Debug將電腦病毒的程式反組譯後，將病毒的程式印下來，並加註解和作病毒程式的分析。

㈢將病毒釋放到系統中，利用磁碟片或事先寫出的程式來被病毒感染，觀察病毒如何傳染和破壞。

㈣將病毒的特性，如標記、特徵、發作等測式的結果紀錄下來。

五、實驗結果

本實驗研究的對象有大腦病毒（（c）Brain）、黑色星期五（Black Friday）、兩隻老虎（Two Tigers）、快樂星期天（Happy Sunday）、程式殺手（Programs Killer）、維也納病毒（Vienna）、晴天炸彈（Sunny）、1701等八種病毒，底下將為您細說電腦病毒的真像。

㈠大腦病毒（（c）Brain）

1.啟動感染型（TSR）

2.標記：病毒將啟動磁區（BOOT）的第5及第6位元組改為（1234_{16}），以供病毒自己判斷此碟片是否中毒。

3.特徵：此病毒只感染360K的磁碟片，1.2M的磁碟片及其他形式的磁碟皆不感染，而受感染的磁碟片標記會被改為（c）Brain，如果磁碟片沒有三個連續的磁區的話，將不會遭到毒手。它會在啟動磁區裡留下一些訊息。

4.發作：這一隻電腦病毒並沒有任何的破壞行動。

5.相關資料：此一病毒原為巴基斯坦的兩個兄弟有感於非法拷

貝的風氣太盛，為了警告非法拷貝的人，所以在他們所賣出的非法軟體中加入了（c）Brain這一隻病毒。

㈡黑色星期五（Black Friday）

1.檔案感染型（TSR）

2.標記：將檔案最後加上MsDos五個位元組，以供病毒判別之用。

3.特徵：受此電腦病毒感染的可執行檔的檔案長度會加長，*.COM檔會加長1813bytes, *.EXE檔會加長1808～1823bytes，而且會不斷的長大，而在它侵入系統後約30分鐘後，螢幕的一部分會無故上捲，然後整個主機的速度會變得很慢。

4.發作：到了13號星期五的話，也就是西方人所忌諱的日子，如果記憶體中有病毒侵入的話，只要執行任一可執行檔，都會遭到刪除。

5.相關資料：此病毒又叫耶路撒冷病毒，以它為藍本的病毒不勝枚舉如兩隻兩虎（Two Tigers）、快樂星期天（Happy Sunday）、程式殺手（Programs Killer）……等。

㈢兩隻老虎：（Two tigers）

1.檔案感染型（TSR）

2.它將檔案最後加上$9EE97299_{16}$以供病毒判別之用。

3.特徵：受此電腦病毒感染的可執行檔的檔案長度會加長，*.COM檔會加長1813 bytes, *.EXE會加長1808～1823 bytes，而且會不斷的長大，如果系統時間為13號或星期五時，就會唱出世界名曲一「兩隻兩虎」，而且每10秒就唱一次，不過歌曲有些變調，十分地惹人厭。

4.發作：這隻病毒並沒有破壞資料的行為，它只是純粹為了搗

蛋而改出的病毒。

5.相關資料：此病毒是由國內玩家修改黑色星期五的程式而產生的，在國內十分地普遍。

㈣快樂星期天（Happy Sunday）

1.檔案感染型（TSR）

2.標記：它將受感染的檔案最後加上Hwang用來判斷檔案是否中毒，不再重覆感染。

3.特徵：它將＊.COM檔加長1636 bytes，而＊.EXE檔加長1636～1651 bytes，都只長大一次，而當系統時間為星期天時，每隔10秒就會在螢幕上顯示：

Today is Sunday ! Why do you work so hard ?

All work and no play make you a dull boy !

Come on ! Let′ s go out and have some fun !

4.發作：它的發作時間是星期天，到了星期天，執行任何程式均都會被它刪除。

5.相關資料：本病毒是由一位名叫Y.W.Hwang 的人修改黑色星期五而成的。

㈤程式殺手（Programs Killer）

1.檔案感染型（TSR）

2.標記：同上

3.特徵：它將＊.COM檔加上1733 bytes，而＊.EXE檔加長1733～1748 bytes，只長大一次，而在病毒侵入30分鐘後，螢幕的左上角會不斷的以反白加閃爍的效果顯示Ha ! Ha ! 。

4.發作：當系統中有此病毒時，執行LOTUS.COM、CWI.EXE、ETBASIC.EXE、BASICA.COM、123.EXE、DBASE.EXE、BASIC.COM都將被它刪除。

5.相關資料：同上。

㈥維也納病毒（Vienna）

1.檔案感染型（每次攻擊一個程式，非TSR）

2.標記：它把受感染的檔案時間改成62秒，可說是一種十分巧妙的設計，因為時間不可能為62秒，所以它可以不必開檔即能作判別。

3.特徵：它並沒有任何的特徵，除了＊.COM檔加長648 bytes，而如果檔案小於10或大於64000 bytes，就不會遭到它的感染或破壞。

4.發作：當它獲得控制權時，會把系統時間取出，和7作AND的邏輯運算，是零的話（也就是說時間為16秒，32秒或48秒），就會改寫程式的第一行指令，使程式一執行就會重開機。

5.相關資料：此電腦病毒原為一奧地利人所寫出的，原來是做一示範病毒，但倒也成了一隻真正的電腦病毒。

㈦晴天炸彈（Sunny）

1.檔案感染型（每次攻擊三個程式，非TSR）

2.標記：同上

3.特徵：它把＊.COM檔加長，可是並不是加長一定的長度，如果檔案小於743bytes，則加長到1486 bytes，如果大於743 bytes，則加長743 bytes，而當它獲得控制權時，便先尋找硬碟下手、此病毒可說是十分地惡毒。

4.發作：當它獲得控制權時，會檢查系統時間是否為8秒，如果是的話，它就會把目前的工作磁碟片的前160個磁區毀壞，也就是說，那磁碟必須重新格式化了，然後，它會在螢幕上寫下：

Greetings from National Central University !
Is today sunny ?

5.相關資料：這一隻病毒的威力十分地恐怖，可以媲美硬碟殺

手（Disk Killer），而市面上的偵測程式都拿它束手無策，依上面的文字看來此一病毒是從中央大學出來的，而最近又有一隻名叫DOOM-2的病毒，它已俱有AI的能力，當有程式在追踪它時，它便重開機以免被追踪，而此病毒也是從中央大學出來的。

(八)1701

1.檔案感染型（TSR）

2.標記：此電腦病毒可以說是這八隻病毒裏最高明的，它常駐的方式十分特別，而在它常駐後，用檢查常駐程式的程式去檢查，並不能發覺到它，只要有程式載入，它就會去檢查程式的前三個bytes，看是不是JMP到倒數1701 bytes，這就是它的判別方式，可說是一隻十分高明的電腦病毒。

3.特徵：除了＊.COM檔加長1701 bytes外，沒有其他的相關資料。

4.發作：它的發作日期是1988年的10月到12月間，發作時，整個螢幕的文字會像下雨一般掉下，十分的奇妙。

5.相關資料：此電腦病毒它只感染和IBM相容的電腦，並不感染IBM的原廠電腦，十分地令人不解，而寫此病毒的人的程式能力高深莫測，他對電腦的MCB、BIOS的資訊區、PSP、Vedio I/ O……都十分地了解

六、結論

事實上，「電腦病毒」和一般的生物病毒是截然不同的兩種東西，「電腦病毒」是由一行一行的機械指令組合而成的，而生物病毒是由核醣核酸和蛋白質所組成的，而電腦病毒的行為和生物病毒十分地相似，所以就稱這些會自我繁殖和破壞磁碟資料的程式為「病毒」——

（Virus）

根據上面所研究的病毒，我們發展出一套防毒的程式，底下就說明其功能及使用方法。

㈠DISKPRO.COM（Disk Proector）

功能：將磁碟貼上「防寫標籤」，而原本硬碟並無防寫標籤，而此程式利用的原理是在軟體和硬體之間作一道檢查，每當有寫入動作時，都必先被此程式檢查，而達到防寫的目的。

使用方法：執行DISKPRO則啟動本程式，而鍵入DISKPRO—，則將此程式從記憶體中移除，本程式提供了所謂熱鍵（Hot Key）的功能，在任何時候鍵入Ctrl F11，就可保護軟式磁碟（Floppy Disk）,Alt F11則相反；而鍵入Ctrl F12，就可保護硬式磁碟（Hard Disk），Alt F12則相反。

㈡CHKMEM.COM（Memory Checker）

功能：此程式是針對本實驗所研究的TSR型病毒寫出，如果記憶體中有病毒存在，就將它所攔截的中斷向量歸還，並把病毒從記憶體中移除。

使用方法：鍵入CHKMEM即可。

㈢CHKTSR.COM（TSR Checker）

功能：此程式是針對TSR病毒所寫出的，此程式會常駐在記憶體中，一有常駐程式要常駐時，它們會問：

Are you sure it is a TSR program ?

（Y/ N）

此程式是為了預防TSR型病毒所寫的，防止TSR型病毒侵入。

使用方法：鍵入CHKTSR即可執行，而鍵入CHKTSR—，就可把程式釋放。

（註：以上三個程式為了不使自己遭受病毒的攻擊，所以都附加有自我治療的功能，安全上沒有問題。）

七、參考資料

熱訊
倚天雜誌
淺談電腦病毒
透析電腦病毒

評語

本作品對電腦病毒有相當程度之了解，因之對電腦操作系中，開機程式，中斷處理等等皆有超出國中程度之表現，針對現有病毒擬防預之道，亦表現甚佳，這是一件很好的工程創作。若作者能在理論上多加注意，追求些相關的學養，當可使作品更成熟。