免費防毒軟體比較

白河商工　胡洲遠

壹、前言

因為電腦病毒及系統本身漏洞的關係，個人電腦常會遭受各種入侵或攻擊，所以電腦除了安裝作業系統與所需的應用軟體外，也有必要安裝防毒軟體。病毒的產生及變形極為快速，單單更新病毒碼並不足以保護電腦系統，但是每年都購買新版防毒軟體對於經費有限的學校、師生或一般家庭來說，都是一項負擔。

若使用網路上的破解版，除了有木馬的疑慮，基本上也違反了智慧財產權。故本篇文章將針對網路上評價較高或較有名氣的一些免費防毒軟體做比較與介紹，提供可不用付費、評價又不錯的防毒軟體，免除大家金錢上之困擾，亦可提供對電腦病毒與防毒軟體不甚瞭解者，做為參考依據。

貳、何謂電腦病毒

一、電腦病毒的定義：

1、過去式：所謂電腦病毒在技術上來說，是一種會自我複製的可執行程式。在真實的世界中，大部份的電腦病毒都會有一個共通的特性—它們通常都會發病。當病毒發病時，它很可能會破壞硬碟中的重要資料，有些病毒則會重新格式化(Format)硬碟。就算病毒尚未發病，它也會帶來不少麻煩。首先病毒可能會佔據一些系統的記憶空間，並尋找機會自行繁殖複製，電腦效能將會變得比一般正常的電腦慢。

2、現在式：自從 Internet 盛行以來，Java 和 ActiveX 的網頁技術逐漸被廣泛使用，一些有心人士於是利用 Java 和 ActiveX 的特性來撰寫病毒。而且木馬程式還會利用 Internet 的特性，竊取使用者資料，亦有像電腦蠕蟲會利用電子郵件來散播病毒。

二、電腦病毒的種類：

1、巨集病毒(MacroVirus)：

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 TaiwanNO.1Word 巨集病毒。

2、開機型病毒(BootStrapSectorVirus)：

開機型病毒是藏匿在磁碟片或硬碟的第一個磁區。因為 DOS 的架構設計，使得病毒可以於每次開機時，在作業系統還沒被載入之前就被載入到記

憶體中，這個特性使得病毒可以針對 DOS 的各類中斷(Interrupt)得到完全的控制，並且擁有更大的能力去進行傳染與破壞。

3、檔案型病毒(FileInfectorVirus)：

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。檔案型的病毒依傳染方式的不同，又分成非常駐型以及常駐型兩種：

(1)非常駐型病毒(Non-memoryResidentVirus)：

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。

(2)常駐型病毒(MemoryResidentVirus)：

常駐型病毒躲在記憶體中，其行為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)。

4、複合型病毒(Multi-PartiteVirus)：

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(BootSector)。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。

5、隱型飛機式病毒(StealthVirus)：

隱型飛機式病毒又稱作中斷截取者(InterruptInterceptors)。顧名思義，它藉由控制 DOS 的中斷向量來讓 DOS 以及防毒軟體認為所有的檔案都是乾淨的。

6、千面人病毒(Polymorphic/MutationVirus)：

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 2byte 的共同病毒碼（好像戴面具只剩兩個眼睛露出來）。

7、網頁惡意程式：

為了讓網頁看起來更生動，更漂亮，許多語言也紛紛出籠，其中最有名的就屬 JAVA 和 ActiveX 了，不幸的是，這兩個語言都相繼地成為第二代病毒的溫床。JAVA 和 ActiveX 的執行方式，是把程式碼寫在網頁上，當你連上這個網站時，瀏覽器就把這些程式碼抓下來，然後用使用者自己系統裡的資源

去執行它。可是如此一來，使用者就會在神不知鬼不覺的狀態下，執行了一些來路不明的程式。

8、特洛伊木馬程式：

通常會假裝是破解版軟體、遊戲等，吸引使用者下載執行，若被此種病毒入侵，病毒撰寫者便可竊取使用者資料，如 Back Orifice。故下載應在原公司或有信譽網站，而不明網站的檔案不要亂下載。

9、電腦蠕蟲：

會不斷繁殖，並利用電子郵件散播給通訊錄內的成員，常見的有 Melissa、I Love You。

10、隨身碟病毒：

感染的途徑是利用隨身碟，常見的有 Kavo。預防此種病毒，須養成正確使用方法，為近來流行的病毒，變形極快，掃毒軟體不見得能抓到新型的病毒，故此病毒的預防辦法獨立說明見第 5 頁「陸、預防隨身碟的方法」。

參、防毒軟體的病毒碼與掃瞄引擎

一、什麼是病毒碼(VirusPattern)：

所謂的病毒碼其實可以想像成是犯人的指紋，當防毒軟體公司收集到一隻新的病毒時，他們就會從這個病毒程式中截取一小段獨一無二而且足以表示這隻病毒的二進位程式碼(BinaryCode)，來當做掃毒程式辨認此病毒的依據，而這段獨一無二的二進位程式碼就是所謂的病毒碼。在防毒軟體公司中都會有一組電腦功力高強的人，專門在為各種不類型的檔案或病毒抓病毒碼，可是當病毒愈來愈多，要找出每一隻病毒都獨一無二的病毒碼可能就不太容易，有時後甚至這些病毒碼還會誤判到一些不是病毒的正常檔案，所以通常防毒軟體公司在將病毒碼送給客戶前都必須先經過一番嚴格的測試，比方說拿這些病毒碼去掃描前 100 大(Top100)軟體都不會造成任何誤判現象，而且都能偵測到所有的病毒才能出貨，經過這些手續之後一個病毒碼定義檔才算是真正完成，可放在 Internet 或 BBS 上供使用者自由 Download。

二、何謂掃瞄引擎(ScanEngine)：

掃瞄引擎可以說是防毒軟體中最精華的部份。當您使用一套防毒軟體時，不論它的畫面是否精美，操作是否簡便，功能是否完善，這些其實都還不足以證明一套防毒軟體的好壞，事實上，當您操作防毒軟體去掃描某一個磁碟機或目錄時，它其實是把這個磁碟機或目錄下的檔案一一送進掃瞄引擎來進行掃描，也就是說您所看到的漂亮畫面其實只是一個使用者介面(UI，UserInterface)，真正影響掃描速度及

偵測率的因素就是掃毒引擎，掃毒引擎是一個沒有畫面，沒有包裝的核心程式，它被放在防毒軟體所安裝的目錄之下，就好像汽車引擎平常是無法直接看見的，可是它卻是影響汽車性能最主要的關鍵。有了病毒碼，有了掃毒引擎，再配合一個精美的操作畫面，就成了市面上您所看到的防毒軟體。

三、為什麼要更新掃瞄引擎和病毒碼：

在一開始提到過絕大多數的人都以為安裝了一套防毒軟體之後，就可以從此高枕無憂，這是一個絕對錯誤的觀念，因為病毒的種類及型態一直在改變，新病毒也每天不斷的被產生，如果不經常更換最新的病毒碼以及掃毒引擎，再強悍的防毒軟體也會有失靈的一天。舉個最明顯的例子來說，在還沒有出現巨集病毒以前，全世界沒有任何一家防毒軟體廠商支援巨集病毒掃描能力，當然如果您還在沿用數年前的防毒軟體，就無法偵測到巨集病毒了。

肆、四套免費防毒軟體介紹

一、Avast (www.avast.com):

1、評價：依獨立實驗室 AV-Comparatives 去年的總報名，avast!在偵查率上有了極大的提高（特別是在 2009 下半年），同時減少了誤報數量。其按需掃描速度更是名列前三。最近 avast!釋出了新版本 V5，有了很大的提升（如全新的圖形用戶介面）和新的防護功能。

2、軟體版本：最新版 V5

3、軟體語言：V5 繁體中文（有多國語言版）

4、說明：直接在線上下載軟體安裝後，尚需申請序號便可免費用一年，過了一年再註冊即可。

二、AVG（www.avg.com）:

1、評價：依獨立實驗室 AV-Comparatives 去年的總報名，儘管 AVG 今年的表現尚好，但成績仍不如預期。希望明年能看到 AVG 的進步。AVG 的所有產品，包括 AVG LinkScanner，都能保證用戶只訪問安全的網站。AVG 的反病毒免費版本為家庭用戶提供基本的安全防護（但沒有網路防護和 rootkit 高級防護等功能）。

2、軟體版本：9.0

3、軟體語言：繁體中文（內建多國語系）

4、說明：內建防毒、防間諜軟體功能，可偵測大部分病毒、蠕蟲與木馬程式，免費版沒有防火牆功能與垃圾信 SPAM 阻擋功能，但可即時監控檔案存取並提供網頁防護功能。

三、AVIRA（www.avira.com）:

1、評價：依獨立實驗室 AV-Comparatives 去年的總報名，AVIRA 是 2008 年的年度最佳防毒軟體。2009 年 AVIRA 同樣有著出色的惡意軟體偵查率和前攝性偵查率，但誤報數量也較大。正是 AVIRA 的高偵查率和網路防護功能，使得其在缺少行為防護等功能的情況下仍可以在全功能動態測試中顯示出優秀的防護能力。AVIRA 對系統性能的影響非常小。2010 年，AVIRA 將推出其含有行為防護功能的新版本。

2、軟體版本：10

3、軟體語言：英文（第 9 版以前有繁體中文，目前最新的的第 10 版，2010/03/22 推出，則尚未有中文版）

4、說明：註冊商標是一把「小紅傘」。免費版比付費版本少了 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。以前的小紅傘因為沒有繁體中文介面，所以對英文比較感冒的使用者就轉而選擇

Avast! 或是 AVG 等其它有中文介面的免費防毒軟體。第 9 版不久前完成了免費個人版的中文化，並在 2010/01/05 開始提供免費中文版的下載，但更新速度極快，目前已出第 10 版，然尚未中文化。

四、Microsoft (www.microsoft.com/security_essentials):

1、評價：依獨立實驗室 AV-Comparatives 去年的總報名，Microsoft 顯示了出色的前攝性偵查率，較低的誤報數量和優秀的惡意軟體清除能力。Microsoft 在 2009 年發布了免費的 Microsoft Security Essentials 防病毒軟體。其用戶介面簡明，Security Essentials 目標是為那些無經濟能力或無意購買完整收費安全軟體的用戶提供基本的防護。

2、軟體版本：1.0

3、軟體語言：繁體中文

4、說明：2009 年 10 月推出，安裝過程會驗證 Windows 是否為正版。系統所佔資源不高(大概是因為沒有複雜的功能)，在掃描速度上不算快但也還可以接受。

伍、四套免費防毒軟體得獎比較

依獨立實驗室 AV-Comparatives 2009 年對眾多防毒軟體所做的評比中，以上四套軟體所獲得的獎項如下表：

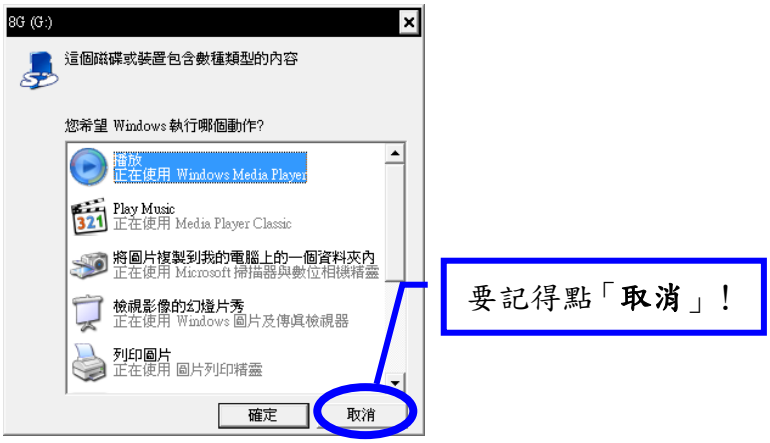
公司名稱	防毒軟體名稱	2009 所獲獎項名稱	備註
Avast	avast! Home Edition	掃描速度測試「銅獎」	
AVG	AVG 防毒軟體免費版	無	
AVIRA	Avira AntiVir Personal - FREE Antivirus	1. 整體性能測試(低系統影響)「金獎」 2. PUA(潛在有害程式)偵查測試「銀獎」 3. 全功能動態保護測試「銅獎」	1. 2008 年度最佳防病毒軟體
Microsoft	Microsoft Security Essentials	1. 前攝性偵查測試「金獎」 2. 低誤報率測試「金獎」 3. 整體性能測試(低系統影響)「銀獎」 4. 惡意軟體清除測試「銅獎」	

陸、預防隨身碟的方法

一、插入隨身碟時按住鍵盤“左邊”的「Shift」，或不要開啟出現的對話方塊：

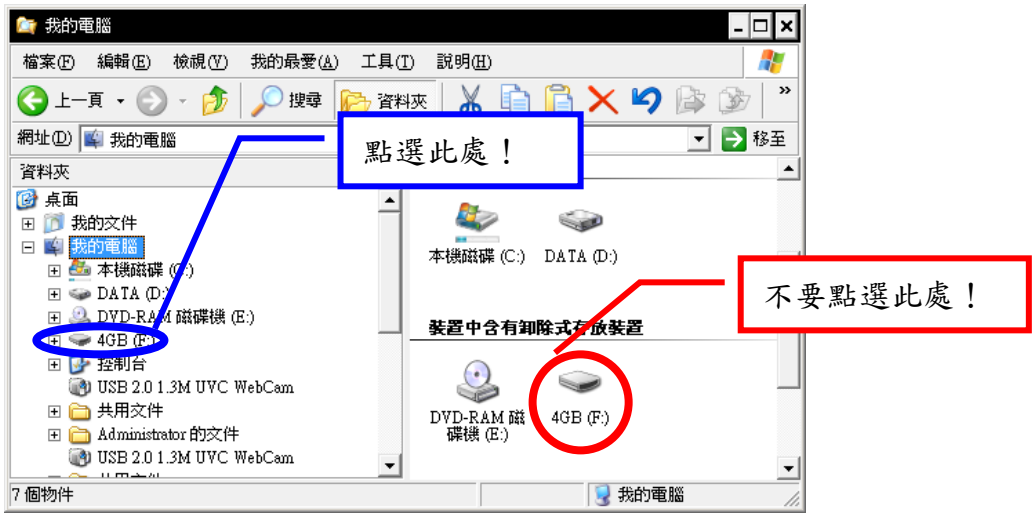
因為插入隨身碟時按住鍵盤“左邊”的「Shift」大約 10 秒，便不會出現右圖的對話方塊;若忘記按而出現下圖的對話方塊時，也要按「取消」，再用「檔案總管」開啟。

這樣若隨身碟已中病毒，可以避免去執行「auturun.inf」自動執行檔，而感染電腦。

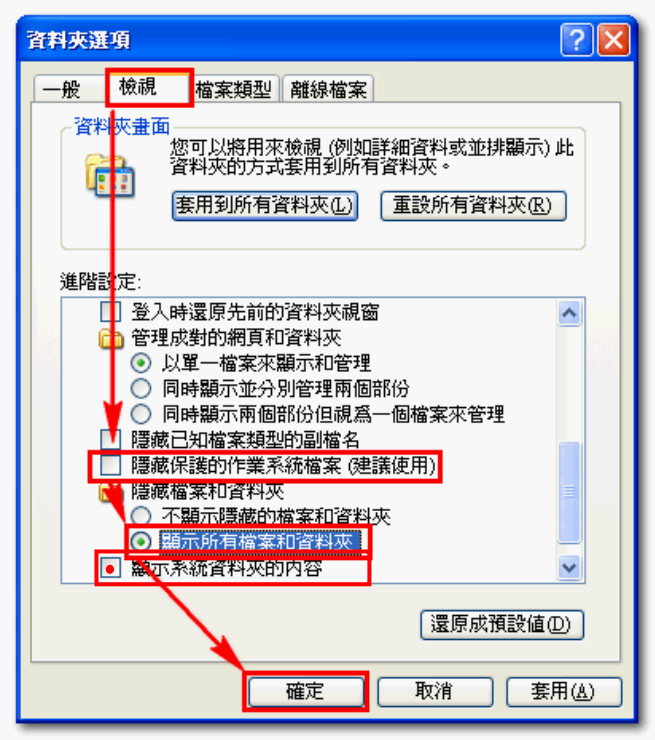


二、用「檔案總管」開啟檔案取代用「我的電腦」：

見下圖，用「檔案總管」左邊的磁碟代號來開啟隨身碟（一樣為避免去執行「auturun.inf」的自動執行檔），而不要使用右邊紅色處框起來的代號。



且可將檔案的副檔名、隱藏檔、系統檔等設定開啟，如此便能發現隱藏的病毒及做刪除的動作，設定步驟點選功能表【工具／資料夾選項】，開啟資料夾選項的視窗，如下方之二圖：



隨身碟內奇怪的檔案便可刪除！(但 C 磁碟等非隨身碟，內有重要程式及系統檔，則不可亂刪)

柒、結論

除「AVG」公司的防毒軟體較無突出之表現外，其餘三套防毒軟體都有其特色與過人之處。依具權威的全球獨立實驗室 AV-Comparatives 報告評價來看，幾個月前才正式推出防毒軟體的 Microsoft，後起之秀似乎有較佳的表現，不過，如果使用的 Windows 作業系統不是正版的，安裝上也會碰到一點麻煩。

如果不是使用正版 Windows 作業系統的使用者，或是不愛 Microsoft 的使用者，則可以考慮使用 AVIRA 的小紅傘防毒軟體。以往 AVIRA（小紅傘）沒有中文介面，即便知道它是「2008 年度最佳防病毒軟體」，很多人也望而怯步不敢使用，但目前第 10 版的中文化介面未推出，若英文不夠好的人，可以先安裝之前的第 9 版，或是先安裝 Avast 應急，等 AVIRA（小紅傘）第 10 版中文版本推出後再更新，因為 AVIRA（小紅傘）在 2009 年的總體表現也多項名列前矛，因此也很推薦一般不想付費的使用者來安裝使用。

捌、參考資料

1、趨勢科技，http://www.trend.com.tw/

2、Anti-Virus Comparative，Summary Report 2009