



牙醫師是社會的高級知識份子，對於資訊時代來臨，牙醫界自然不能置身於外。本專欄將以一系列漸進式的主題，來介紹如何入門駕馭電腦及如何遨遊網路的資訊世界以及一些與我們牙醫息息相關的電腦資訊，以期在不久的未來達成牙醫師人人上網，個個皆是電腦高手之目標。當然，如果您已是電腦高手，在此也誠摯地邀請您提供寶貴的學習經驗或獨到的資訊應用見解，多多投稿至本專欄，以饗大眾。

防毒篇



黃琮仁
北醫牙醫學系五年級

電腦病毒對大多數的電腦使用者而言應該是再耳熟能詳不過的名詞，有些人也許從來不曾真正碰到過電腦病毒，而吃過電腦病毒虧的人卻又聞毒色變，其實在個人電腦這麼普遍的今天，即使您不是一個電腦高手，也應該對電腦病毒有些基本的認識，就好比我們每天都會關心周遭所發生的人事物一樣，畢竟電腦病毒已經不再像過去是遙不可及的東西，自從 Internet 潮流席捲全球以來，電腦資訊以每秒千里的速度在傳送，我們每天可以透過 Internet 收到來自全球各地不同的消息，但在享受資訊便利的同時，電腦安全問題也就顯得格外重要了。

在幾年以前，電視新聞的氣象報告只是簡單的預報天氣狀況，不知道從什麼時候開始有了 3D 動態的衛星雲圖和氣象 Call-In 服務，這代表了氣象知識已經不再是一門專業知識，而逐漸成爲一種常識。電腦病毒也是如此，當它已經成爲工作中無法避免的一環時，我們就有必要真正的去面對它，瞭解它，而不再是頭痛醫頭，腳痛醫腳的到處求醫，雖然說久病也可以成良醫，可是若能不生病又可以替人治病不是更好嗎？在防毒基礎篇中，就是要從零開始的為大家介紹電腦病毒的基本觀念，希望有一天您也可以成爲一位真正的病毒醫生。

一、什麼是電腦病毒

▲ 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) 您的硬碟。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，您電腦效能將會變得比一般正常的電腦慢。這也是爲什麼不時就要做好防毒工作的主要原因了。

▲ 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。以 Java 病毒為例，Java 病毒它並不能破壞您硬碟上的資料，可是若您使用瀏覽器來瀏覽含有 Java 病毒的網頁，Java 病毒可以強迫您的 Windows 不斷的開啓新視窗，直到系統資源被吃光爲止，而您也只有

選擇重新開機一途了。所以在 Internet 革命以後，電腦病毒的定義就更改為只要是對使用者會造成不便的這些不懷好意的程式碼，就可以被歸類為病毒。

二、電腦病毒的生命週期

電腦病毒就好像細菌的生長一般，所以我們才將它稱做「病毒」。而電腦病毒的成長可以被歸納成下列幾個階段：

▲ 創造期：

當電腦駭客們花了數天或數週努力的研究出一些可以廣為散佈的程式碼，電腦病毒就這樣誕生了。當然，他們是不會這樣就算了的，他們通常都會設計一些破壞的行為在其中。

▲ 孕育期：

這些電腦駭客們會將這些含有電腦病毒的檔案放在一些容易散播的地方。如 BBS 站，Internet 的 FTP 站，甚至是公司或是學校的網路中等等。

▲ 潛伏期：

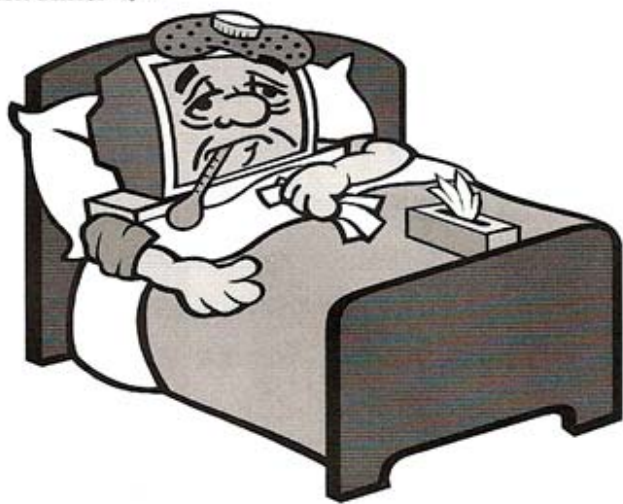
在潛伏期中，電腦病毒會不斷地繁殖與傳染。一個完美的病毒擁有很長的潛伏期，如此一來病毒就有更多的時間去傳染到更多的地方，更多的使用者，一旦發病將會造成更大的傷害。例如世界知名的米開朗基羅病毒，在每年三月六日發作前，有整整一年的潛伏期。

▲ 發病期：

當一切條件形成之後，病毒於是就開始破壞的動作。有些病毒會在某些特定的日期發病，有些則自己有個倒數計時裝置來決定發病的時間。雖然有些病毒並沒有發病時的破壞動作，但是它們仍然會佔據一些系統資源，而降低系統運作的效率。

▲ 根除期：

如果有夠多的防毒軟體能夠偵測及控制這些病毒，並且有夠多的使用者購買了防毒軟體，那麼這些病毒就有機會被連根撲滅。雖然到現在為止，並沒有人敢宣稱某一隻病毒完全絕跡，但是有些病毒已經很明顯的被完全制止了 - 如早期的 Disk Killer 等。



三、電腦病毒的種類

▲ 巨集病毒 (Macro Virus):

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。

▲ 開機型病毒 (Boot Sector Virus):

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。



▲檔案型病毒 (File Infector Virus):

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。

▲複合型病毒 (Multi-Partite Virus):

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強的傳染力。

▲隱型飛機式病毒 (Stealth Virus):

隱型飛機式病毒又稱作中斷截取者(Interrupt Interceptors)。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。

四、第二代病毒是什麼碗糕?

第一代病毒(傳統型病毒)的共同特色,就是有一定有一個「寄主」程式,所謂寄主程式就是指那些讓病毒窩藏的地方。最常見的就是一些可執行檔,像是副檔名為.EXE及.COM的檔案。但是由於微軟的WORD愈來愈流行,且WORD所提供的巨集功能又很強,使用WORD巨集寫出來的病毒也愈來愈多,也因此副檔名為.DOC的也會成為寄主程式。尤其是這一年來,巨集病毒可真的算是紅上半邊天,只要提到Taiwan NO.1,那可說是無人不知,無人不曉。也許你覺得像WORD這種文件檔都可以中毒,真是一件不可思議的事,那麼,第二代病毒的特性更會讓你合不攏嘴!相對於第一代病毒,第二代病毒完全不需要寄主的程式,如果硬要說它寄生在哪裡,或許只能說它是寄生在「Internet」上吧。

回歸到第一代病毒來看,病毒是寄生在「可執行的」程式碼中,伺機對系統進行破壞,因為病毒本身也就是一段「可執行的」程式碼而已。也

因此,在以往病毒都是存在於「可執行檔」中,因為具有「可執行的」程式碼的檔案,就只有「可執行檔」。但是,文件病毒的流行,讓人對這個定義有了疑問,而其實並不違背。因為所謂的文件病毒,也只是利用文件中巨集寫成的,而巨集本身也是「可執行的」程式碼,當然也能成為病毒的溫床囉!現在再來看看所謂的第二代病毒,它就是利用網頁編寫所用的JAVA或ActiveX這些語言。由這些語言可以寫出一些「可執行的」程式碼,而在使用者瀏覽網頁時,一併下載下來在系統裡執行。既然JAVA或ActiveX可寫成一些「可執行的」程式碼,那就沒什麼理由不能讓病毒藏身其中。

結論

在讀完了這篇文章後,您是不是對電腦病毒有了清楚的概念,許多人以為買了一套防毒軟體之後就可以永遠高枕無憂,但事實卻不竟然,由於病毒不斷翻新,防毒軟體勢必緊追猛打,創新偵測引擎,更新病毒碼,才能對時下流行的病毒一一反擊!!

以下所列的是常用軟體的網址,可以參考看看!!

趨勢科技	http://www.trend.com.tw
金帥資訊	http://www.ggreat.com.tw ; http://w5.dj.net.tw/~ggreat
正點資訊	http://www.goodpoint.com.tw
Dr Solomon's	http://www.drsolomon.com
ThunderBYTE	http://www.thunderbyte.nl
F-PROT	http://www.commandcom.com
EliaShim	http://www.eliashim.com
IBM AV	http://www.av.ibm.com/ current/FrontPage
McAfee	http://www.mcafee.com
Symantec	http://www.symantec.com/avcenter