篇名

電腦剋星——病毒與駭客

作者

王姿穎。私立曉明女中。二年丁班

電腦剋星——病毒與駭客

壹●前言

電腦是現代人無法缺少的工具之一，無論是打報告、記事、或者娛樂，都無法離開電腦。當我們正在使用電腦時，常常會出現「這個檔案有可能爲病毒潛在處，是否繼續開啓？」或是「爲了避免駭客入侵，建議您不要下載此檔案。」如果我們一不小心，當下次在開電腦時，資料突然被修改，更嚴重是不見，最後連主機都要重新換才行。是誰動了手腳呢？他們是怎麼進到我們的電腦呢？對於這些不速之客，我們又要怎麼預防，才不會受到傷害呢？這些問題值得我們現代人來思考。

貳●正文

一、電腦病毒

０１什麼是電腦病毒？

『電腦病毒是一段很小的電腦程式，是一種會不斷「自我複製」及「感染」的程式，會使檔案長度增加刪減、不尋常的錯誤訊息出現。

在傳統的 DOS 環境下，通常會存在可執行的檔案中，或者是軟硬碟的開機磁區啓動部份，隨著被感染程式由作業系統載入記憶體而同時執行，病毒因此獲得系統控制權；但在視窗系統中出現的文件巨集病毒則是附著在文件檔中，且其感染之對象亦限於文件檔。

電腦病毒分爲：

A.開機型病毒：是藏匿和感染磁碟片或硬碟的第一個磁區，即我們平常說的 Boot Sector。它藉由開機動作而侵入記憶體，若用已感染的磁片開機，那麼病毒將立即感染到硬碟。因 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 各類中斷得到完全控制，並且擁有更大的能力去進行傳染與破壞。

開機型病毒又可分爲：

- **a. 傳統開機型病毒：大多經磁碟傳染，進入電腦後再傳染到其他檔案。**

b. 隱型開機型病毒：感染的是硬碟的開機磁區，它僞造開機磁區的資料，使防毒軟件以爲系統正常。

c. 目錄型開機型病毒：只感染電腦的檔案配置表，一旦你的檔案配置表被破壞後，你的電腦檔案讀寫就會不正常，甚至失去檔案。

B.檔案型病毒：通常寄生在可執行檔中。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，又分成三種**:**

a. 非常駐型病毒：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。

b. 常駐型病毒：躲在記憶體中，行爲就像寄生在各類低階功能般，往往對磁碟造成更大的傷害。一旦進入記憶體中，只要執行檔被執行，它就對其進行感染動作，效果非常顯著。將它趕出記憶體的唯一方式就是完全關掉電源後再開機。

c. 隱形檔案型病毒：會把自己植入作業系統裡，當程式向作業系統要求中斷時，它就會感染提出要求的程式，而且看起來不像被感染的樣子。

C.複合型病毒：兼具開機型病毒和檔案型病毒的特性。可以傳染 ***.COM**、***.EXE** 檔及磁碟開機系統區。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！

D.千面人病毒：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。

E.巨集病毒：主要利用軟體本身提供的巨集能力來設計病毒，凡是有寫巨集能力的軟體都有巨集病毒存在的可能。

０２病毒是如何形成？

很多「病毒」不過是程式中的錯誤。當程式編寫員設計新程式時，都會注意不到其中的小問題或錯誤。就因爲這些小問題或錯誤，造成一些不必要的指令及影響。

０３病毒如何入侵？

電腦病毒一定要在電腦系統裏才能傳播。這提供很多途徑。它可以不需要人們介入就能由程式或系統傳播。

病毒第一件要做的事通常是複製。病毒會把附在一處可以有利於自己執行的系統裏。在運作電腦時，病毒可在短時間把自己複製多個。

病毒蔓延的主要方式是透過軟碟的分享。如果軟件是透過人手散佈出去的，病毒蔓延的速度會比 **BBS** 或國際網絡慢得多。由於文書處理系統及國際網絡十分受歡迎，所以電腦病毒容易在短日子裏傳播到無數用家的電腦系統。現在很多人都會用到文書處理器，並附在電子郵件中傳給其他人。如果這文件是帶有病毒，收件人亦會被傳染。現在很多電子郵件程式都會把接收到的郵件自動地放在文書處理器開啓，所以收件人是在沒有選擇的情況下被傳染病毒。

另一病毒傳播的途徑就是 CD。翻版 CD 很多都帶有病毒，但由於 CD 不能用來編寫，所以 CD 的病毒不能被清除。

０４病毒的影響

病毒可把電腦裏的程式或數據消失或改變。有些病毒被觸發時，會無條件把硬磁碟格式化及刪除磁碟上所有系統檔案；有些會感染主啓動記錄及 **DOS** 啓動磁區，之後它會降低記憶體及硬磁碟的效能，直至當我們的用電腦時螢光幕上顯示一些訊息或有其他損壞。』
（註一）

二、駭客

０１。什麼是駭客？

『駭客源於英語動詞 hack，意爲「劈、砍」，引申爲“做了一件非常完美的工作”。在早期麻省理工學院的校園俚語中，駭客則有“手法巧妙、技術高明的惡作劇”之意。在日本《新駭客詞典》中，駭客定義是“喜歡探索軟體程式奧秘，並從中增長了其個人才幹的人”。

０２。駭客如何入侵？

A.獲取密碼：有三種方法：一是通過網路監聽非法得到用戶密碼，這類方法有一定局限，但危害性極大，監聽者能夠獲得其所在網段的所有用戶帳號和密碼；二是在知道用戶的帳號後用一些專門軟體強行破解用戶密碼，這方法不受網段限制，但駭客要有足夠的耐心和時間；三是在獲得一個伺服器上的用戶密碼文件後，用暴力破解程式破解用戶密碼。此方法在所有方法中危害最大，它不需要像第二種方法那樣一遍一遍地嘗試登錄伺服器，而是在本地將加密後的密碼與

Shadow 文件中的密碼相比較就能非常容易地破獲用戶口令，尤其對那些密碼安全系數極低的用戶，更是在短短的一兩分鐘內，甚至幾十秒內就可以將其破解。

B.放置特洛伊木馬程式：此程式可直接侵入用戶的電腦進行破壞，它常僞裝成工具程式或遊戲，誘使用戶打開有特洛伊木馬程式的郵件附件或從網上直接下載，一旦用戶打開了這些郵件附件或者執行這些程式後，它們就會像古特洛伊人在敵人城外留下的藏滿士兵的木馬一樣留在自己的電腦中，並在自己的電腦系統中隱藏個可以在 **windows** 啓動時執行的程式。當您連接到網上時，這個程式就會通知駭客，來報告您的 **IP** 地址和預先設定的端口。駭客收到這些資訊後，再利用這個潛伏在其中的程式，任意修改您電腦的參數設定、窺視你整個硬碟中的內容。

C.電子郵件攻擊：主要表現兩種方式：一是電子郵件轟炸，就是通常所說的郵件炸彈，是用僞造的 **IP** 地址和電子郵件地址向同一信箱發送數以無窮多次的內容相同的垃圾郵件，致使受害人郵箱被“炸”，嚴重者可能會給電子郵件伺服器作業系統帶來危險和癱瘓；二是電子郵件欺騙，攻擊者佯稱自己爲系統管理員，給用戶發送郵件要求用戶修改密碼或在貌似正常的附件中載入病毒或其他木馬程式，這類欺騙只要用戶提高警惕，危害性不大。

D.通過一個節點來攻擊其他節點：駭客在突破一台主機後，往往以此主機作爲根據地，攻擊其他主機。他們可用網路監聽方法，嘗試攻破同一網路內的其他主機；也可以通過 **IP** 欺騙和主機信任關係，攻擊其他主機。這類攻擊很狡猾，但由於某些技術很難掌握，因此較少被駭客使用。

E.網路監聽：這是主機的一種工作模式，在模式下，主機可以接受到本網段在同一條物理通道上傳輸的所有資訊，不管這些資訊的發送方和接受方是誰。此時，如果兩台主機進行通信的資訊沒有加密，只要使用某些網路監聽工具就可以輕而易舉地截取包括密碼帳號在內的資料。雖然網路監聽獲得的具有一定的局限，但監聽者往往能夠獲得其所在網段的所有用戶帳號及密碼。

F.尋找系統漏洞：許多系統都有安全漏洞，其中某些是作業系統或應用軟體本身具有的，這些漏洞在補丁未被開發出來之前一般很難防禦駭客的破壞，除非你將網線拔掉；還有一些漏洞是由於系統管理員配置錯誤引起的，如在網路文件系統中，將目錄和文件以可寫的方式調出，將未加 **Shadow** 的用戶文件以明碼方式存放在某一目錄下，這都會給駭客帶來可乘之機。

G.利用帳號進行攻擊：有的駭客會利用作業系統提供的預設帳戶和口令進行攻擊。駭客用 **Unix** 作業系統提供的命令收集資訊，不斷提高自己的攻擊能力。這類攻擊只要系統管理員提高警惕，將系統提供的預設帳戶關掉或提醒無密碼用戶

增加密碼一般都能克服。

H.偷取特權：利用各種特洛伊木馬程式、後門程式和駭客自己編寫的導致緩衝區溢出的程式進行攻擊，前者可使駭客非法獲得對用戶機器的完全控制權，後者可使駭客獲得用戶許可權，而擁有對整個網路的絕對控制權。這手段一旦奏效，危害性極大。』（註二）

０３駭客的影響

『許多駭客會藉由網際網路的方式進入您的主機，然後駭客可做到很多事情，您可能不會受到什麼影響，但是您也可能因此而導致重大的損失，甚至能破壞社會金融秩序，危害國家安全。』（註三）

參●結論

現在的科技發達，往往會出現一些漏洞，病毒和駭客也隨機而來，但這些不法的傷害行爲，爲什麼還會有人冒著危險，走在法律危險區呢？

除了有報復之心的人外，**『有些程式編寫員製造電腦病毒的目的是爲了表現自己的能力或挑戰自己或別人，他們只是想看看病毒會帶來甚麼後果或者看看是否有人能把病毒清除』**(註一)。駭客也是一樣，雖然喜歡在網路上入侵他人電腦，破解密碼，但其目的只不過是想證明自己的功力，他們不更動主機上的任何資料，頂多留下「到此一遊」的訊息。其實這種做法是錯誤運用自己的能力。他們證明自己「我很強」，但他們的所作所爲可能都會造成別人的不便，甚至使對方有財務上的損失，無論他們如何炫耀，這些行爲都是不被讚許的。

我們除了拒絕成爲這樣的人，也要做好防備。你可以從小事如不下載網路遊戲做起，或者可以選購正版的防毒軟體。平時的小心謹慎，才不會喪失自己的財產。

肆●引註資料

註一、電腦病毒 http://www.ied.edu.hk/has/comp/compviru/index.htm(檢索日期：96 年 7 月 15 日)
註二、鄭文哲，麥惠東。駭客。(台灣：松崗，民 89)。頁 72-74。
註三、GateLock 專區－教育專區－認識駭客
http://www.trend.com.tw/gatelock/edu/hacker.asp(檢索日期：96 年 7 月 15 日)