計算機病毒百題問答

王路敬 著

計算機病毒百題問答

王路敬 著

儒林圖書公司 印行

計算機病毒百題問答

著　　者：王 路 敬
出 版 者：儒林圖書有限公司
地　　址：台北市重慶南路一段111號
電　　話：3118971-3 • 3144000
郵政劃撥：0106792-1
吉豐印刷廠有限公司承印
板橋市三民路二段居仁巷一弄53號

行政院新聞局局版台業字第4336號
1991年10月初版
NT$ 130

前 言

自從美國首先發現電腦病毒以來，世界上許多國家和地區均出現了電腦病毒的干擾，而且正不斷蔓延，種類不斷增加。隨著微電腦的推廣和普及，各種版本 DOS 和應用軟體的廣泛交流，非法複製軟體的現象日益嚴重，加上機器管理缺乏嚴格的制度，據有關材料證實電腦病毒還在繼續蔓延。由於電腦病毒的存在，輕則使電腦降低執行速度，滋擾正常運轉，重則破壞資料，毀損儲存的訊息資源。若任其滋生、蔓延，嚴重後果自不待言。

本書採用了問題形式，而這些問題具有一定普遍性和針對性。因爲受電腦病毒困擾的使用者急需了解解除病毒威脅以及如何免除病毒再次攻擊的實用技術。所以從內容上儘量避免過多理論的論述，而著眼於要解決實際問題、能力和作業方法，因而有較強的實用性。本書共分四章：第一章電腦病毒概述。在明確什麼是電腦病毒的基礎上，進一步介紹有關電腦病毒分類、特徵、寄生模式、一般工作機理，最後落實到電腦病毒常用判別方法和處理的一般作業步驟。第二章檢測和防治微型電腦病毒的準備。該章的內容包括兩部分，其一微型電腦磁碟作業系統基本知識和磁碟空間的分配；其二檢測和消除病毒的必備工具 DEBUG 和 PCTOOLS 的使用。第三章微型電腦常見病毒的分析與消除。該章著重對圓點病毒、大麻病毒、Brain 病毒、黑色星期五病毒等流行最廣的幾種病毒進行了分析，提供預防和清除的具體作業

方法，對其他種類的病毒也作了簡單介紹。第四章常用檢測和解毒軟體使用簡介。全書共匯集了 111 個具有代表性的問題，逐一予以解答，奉獻給廣大讀者。

目　錄

第一章　電腦病毒概述

1．什麼是電腦病毒？

可以從不同角度給出電腦病毒的定義。一種定義是通過磁碟、磁帶和網路等作爲媒介傳播擴散，能"傳染"給其他程式的程式。另一種是能夠執行自身複製且借助一定的載體存在的具有潛伏性、傳染性和破壞性的程式。還有的定義是一種人爲製造的程式，它通過不同的途徑潛伏或寄生在儲存媒體（如磁碟、主記憶體）或程式裡。當某種條件或時機成熟時，它會自生複製並傳播，使電腦的資料受到不同程式的破壞等等，這些說法在某種意義上借用了生物學病毒的概念，電腦病毒同生物病毒所相似之處是能夠侵入電腦系統和網路，危害正常工作的"病原體"。它能夠對電腦系統進行各種破壞，同時能夠自我複製，具有傳染性。所以，電腦病毒就是能夠通過某種途徑潛伏在電腦儲存介質（或程式）裡，當達到某種條件時即被觸發的具有對電腦資料進行破壞作用的一組程式或指令集合。

與生物病毒不同的是幾乎所有的電腦病毒都是人爲地故意製造出來的，有時一旦擴散出來後連編者自己也無法控制，它已經不是一個簡單的純電腦學術問題，而是一個嚴重的社會問題了。

2. 電腦病毒是在什麼情況下出現的？

電腦病毒的產生是電腦技術和以電腦爲核心的社會訊息化過程發展到一定階段的必然產物。它產生的背景是：

(1) 電腦病毒是電腦犯罪的一種新的衍化形式。

電腦高技術犯罪，具有瞬時性、動態性和隨機性，不易取證，風險小破壞大，從而刺激了犯罪意識和犯罪活動，是某些人惡作劇和報復心態在電腦應用領域的表現。

(2) 電腦軟體產品的脆弱性是根本的技術原因。

電腦是電子產品，資料從輸入、儲存、處理、輸出等環節，易誤入、篡改、丟失、作假和破壞；程式易被刪除、改寫；電腦軟體設計的手工模式，效率低下生產週期長，人們至今沒有辦法事先了解一個程式有沒有錯誤，只能在執行中發現，修改錯誤，並不知道還有多少錯誤和缺陷隱藏在其中，這就爲病毒的侵入提供了方便。

(3) 微電腦的普及應用是電腦病毒產生的必要環境。

1983年11月3日美國電腦專家首先提出了電腦病毒的概念並進行了驗證。幾年前電腦病毒就迅速蔓延，而這幾年正是微電腦普及應用熱潮，微電腦的廣泛普及，作業系統簡單明瞭，軟、硬體透明度高，基本上沒有什麼安全措施，能夠透徹了解它內部結構的使用者日益增多，對其存在的缺點和易攻擊處也了解的越來越清楚，不同的目的可以做出截然不同的選擇。目前，在 IBM PC 系列及其相容機上廣泛流行著各種病毒就很快說明這個問題。

3. 電腦病毒的來源有哪些？

(1) 搞電腦的人員和業餘愛好者的惡作劇尋開心製造出的病毒，

例如像圓點一類的良性病毒。

(2) 軟體公司及使用者爲保護自己的軟體被非法複製而採取的報復性懲罰措施。因爲他們發現對軟體上鎖，不如在其中藏有病毒對非法拷貝的打擊大，這更加助長了各種病毒的傳播。

(3) 旨在攻擊和摧毀電腦訊息系統和電腦系統而製造的病毒，就是蓄意進行破壞。例如1987年底出現的以色列耶路撒冷希伯萊大學的猶太人病毒，就是雇員在工作中受挫或被辭退時故意製造的，它針對性强，破壞性大，產生於內部，防不勝防。

(4) 用於研究或有益目的而設計的程式，由於某種原因失去控制或產生了意想不到的效果。

4. 電腦病毒是如何分類的？

電腦病毒可以從不同的角度分類。若按其表現性質可分爲良性和惡性的。良性的危害性小，不破壞系統和資料，但大量佔用系統開銷，將使機器無法正常工作陷於癱瘓。如圓點病毒就是良性的。惡性病毒可能會毀壞資料檔案，也可能使電腦停止工作。若按觸發的時間可分爲定時的和隨機的。定時病毒僅在某一特定時間才發作，而隨機病毒一般不是由時鐘來觸發的。若按其入侵模式可分作業系統型病毒，圓點病毒和大麻病毒是典型的作業系統病毒，這種病毒具有很强的破壞力（用它自己的程式意圖加入或取代部份作業系統進行工作），可以導致整個系統的癱瘓；原始程式碼病毒，在程式被編譯之前插入到FORTRAN、C 或 PASCAL 等語言撰寫的原始檔，完成這一工作的病毒程式一般是在語言處理程式或連接程式中；外殼病毒，常附在主程式的首尾，對原始檔不作修改，這種病毒較常見，易於編寫，也易於發現，一般測試可執行檔案的大小即可知；入侵病毒，侵入到主程式之中，並替代主程式中部份不常用到的功能模組或堆疊區，這種病毒一

般是針對某些特定程式而編寫的。若按其是否有傳染性可分爲不可傳染性和傳染性病毒。不可傳染性病毒有可能比傳染性的更具有危險性和難以預防。若按傳染模式可分磁碟引導區傳染的電腦病毒，作業系統傳染的電腦病毒和一般應用程式傳染的電腦病毒。若按其病毒攻擊的機種分類，攻擊微型電腦的，攻擊小型機的，攻擊工作站的，其中以攻擊微型電腦的病毒爲多，世界上出現的病毒幾乎90%是攻擊 IBM PC 機及其相容機。

當然，按照電腦病毒的特點及特性，電腦病毒的分類方法還有其他的分法，例如按攻擊的機種分，按寄生模式分等。因此，同一種病毒可以有不同的分法。

5. 電腦病毒一般具有哪些特點？

電腦病毒一般具有以下幾個特點：

(1) 破壞性：凡是由軟體手段能觸及到電腦資料的地方均可能受到電腦病毒的破壞。其表現：佔用 CPU 時間和主記憶體開銷，從而造成過程堵塞；對資料或檔案進行破壞；打亂螢幕的顯示等。

(2) 隱蔽性：病毒程式大多夾在正常程式之中，很難被發現。

(3) 潛伏性：病毒侵入後，一般不立即活動，需要等一段時間，條件成熟後才作用。

(4) 傳染性：對於絕大多數電腦病毒來講，傳染是它的一個重要特性，它通過修改別的程式，並把自身的拷貝包括進去，從而達到擴散的目的。

6. 微電腦病毒寄生的主要載體是什麼？

電腦病毒是一種可直接或間接執行的檔案，是依附於系統特點的檔案，是沒有檔名的秘密的程式，但它的存在卻不能以獨立檔案的形式存在，它必須是以現有的硬軟體檔資料而存在的。

微電腦系統在目前來說永久性儲存設備即輔助記憶體主要是磁碟。磁碟包括硬碟和軟碟。從儲存容量角度來講，硬碟容量是一般軟碟容量的幾十至幾百倍、並且硬碟容量越來越大，軟碟分一般密度 320KB 或 360KB，中等密度 720KB 和高密度 1.2MB 等。微型電腦系統所使用的檔案存放於磁碟之中，所以微型電腦的病毒是以磁碟爲主要載體的。

7. 電腦病毒在磁碟中儲存有哪幾種情況？

從目前發現的電腦病毒來分析，病毒在磁碟中的儲存位置有兩種：

(1) 儲存於磁碟的引導磁區，對軟碟來說只有一個引導磁區，而對硬碟來說有些病毒則可能儲存在主引導磁區，例如大麻病毒。

(2) 磁碟的使用者空間中。例如黑色星期五病毒，專門感染.COM和.EXE 可執行檔案，將自身作爲正常程式的一部份和正常程式連接在一起駐留在磁碟使用者空間中。

8. 電腦病毒寄生模式有哪幾種？

(1) 寄生在磁碟引導磁區中：任何作業系統都有個靴帶式啓動過程，例如DOS在啓動時，首先由系統讀入引導磁區記錄並執行

它，將 DOS 讀入主記憶體。病毒程式就是利用了這一點，自身佔據了引導磁區而將原來的引導磁區內容及其病毒的其他部份放到磁碟的其他空間，並將這些磁區標上損壞磁簇的旗標。這樣，系統的一次初始化，病毒就被激活了。它首先將自身拷貝到主記憶體的高端並佔據該範圍，然後設置觸發條件如 INT 13H 中斷（磁碟讀寫中斷）向量的修改，設置內部時鐘的某一值爲條件等，最後引入正常的作業系統。這時一旦觸發條件成熟，如一個磁碟讀或寫的請求，病毒就被觸發。如果磁碟沒有被感染（通過識別旗標）則進行傳染。

(2) 寄生在可執行程式中：這種病毒寄生在正常的可執行程式中，一旦程式執行病毒就被激活，於是病毒程式首先被執行，它將自身常駐主記憶體，然後設置觸發條件，也可能立即進行傳染，但一般不作表現。做完這些工作後，開始執行正常的程式，病毒程式也可能在執行正常程式之後再設置觸發條件等工作。病毒可以寄生在原始檔的前端也可以寄生在尾部，但都要修改原始檔的長度和一些控制訊息，以保證病毒成爲原始檔的一部分，並在執行時首先執行它。這種病毒傳染性比較强。

(3) 寄生在硬碟的主引導磁區中：例如大麻病毒感染硬碟的主引導磁區，該磁區與 DOS 無關。

9. 目前電腦病毒的破壞作用表現在哪些方面？

不管是良性病毒還是惡性病毒，對使用者都會造成一定的破壞性。目前侵入電腦病毒的破壞情況，主要表現在以下諸方面：

(1) 破壞檔案配置表 FAT，使使用者在磁碟上的訊息丟失。

(2) 刪除軟碟上或者硬碟上的可執行檔案或資料檔案。如果刪除的檔案是系統檔案，則會導致這片磁碟不能引導系統。例如黑色星期五病毒當某月13日又爲星期五時，執行.COM 或.EXE檔案將會刪除該檔案。90年4月15是北京晚報報導大陸有些地方的電腦在4月13日激發了感染上的"十三號星期五"病毒，電腦工作效率或程式受到不同程度的破壞。

(3) 修改或破壞檔案中的資料。

(4) 改變磁碟分配，造成資料寫入錯誤。

(5) 影響主記憶體常駐程式的正常執行。

(6) 在磁碟上產生壞的磁區，使磁碟可用空間減小。

(7) 更改或重寫磁碟的卷冊標記。

(8) 使主記憶體可用的空間因病毒程式自身在系統中的多次複製而減小，使得正常的資料或檔案不能儲存。

(9) 對整個磁碟或磁碟的特定磁道或磁區進行格式化。

(10) 在系統中產生新檔案。

(11) 改變系統的正常執行過程。

10. 電腦病毒的工作過程應包括哪些環節？

電腦病毒的完整工作過程應包括以下幾個環節：

(1) 傳染源：病毒總是依附於某些儲存介質，例如軟碟、硬碟等構成傳染源。

(2) 傳染媒介：病毒傳染的媒介由工作的環境來定，可能是電腦網路病毒，也可能是可移動的儲存介質，例如磁碟等。

(3) 病毒激活：是指將病毒載入主記憶體，並設置觸發條件，一旦觸發條件成熟，病毒就開始作用——自我複製到傳染對象