你真的了解計算機病毒嗎？內容很“幹”，記得喝水

原創 鴨血粉絲Tang Java極客技術 2021-12-10 07:30

每天早上七點三十，準時推送乾貨

計算機病毒與計算機相伴生的東西，它對計算機的安全構成一定的威脅，一旦病毒計算機遭到病毒入侵，輕則導致信息丟失，重則導致電腦癱瘓。因此，抵禦病毒入侵顯得十分重要。

想要抵禦病毒，你得先了解它們，知道它們長什麼樣子，是如何侵入計算機的才能很好的抵禦它們。

文章很長建議收藏，讀完這篇文章，給你的計算機一個安全的環境。

計算機病毒的特點

傳染性

這是病毒的基本特徵。計算機病毒會通過各種渠道從已被感染的計算機擴散到未被感染的計算機，造成被感染的計算機工作失常甚至癱瘓。是否具有感染性是判別一個程序是否為計算機病毒的重要條件。

隱蔽性

病毒通常附在正常程序中或磁盤較隱蔽的地方，也有的以隱含文件形式出現。如果不經過代碼分析，病毒程序與正常程序是不容易區分開來的。計算機病毒的源程序可以是一個獨立的程序體，源程序經過擴散生成的再生病毒一般採用附加和插入的方式隱藏在可執行程序和數據文件中，採取分散和多處隱藏的方式，當有病毒程序潛伏的程序被合法調用時，病毒程序也合法進入，並可將分散的程序部分在所非法佔用的存儲空間進行重新分配，構成一個完整的病毒體投入運行。

潛伏性

大部分病毒感染系統後，會長期隱藏在系統中，悄悄的繁殖和擴散而不被發覺，只有在滿足其特定條件的時候才啟動其表現（破壞）模塊。

破壞性

任何病毒只要入侵系統，就會對系統及應用程序產生程度不同的影響。輕則會降低計算機工作效率，佔用系統資源，重則可導致系統崩潰，根據病毒的這一特性可將病毒分為良性病毒和惡性病毒。良性病毒可能只顯示些畫面或無關緊要的語句，或者根本沒有任何破壞動作，但會佔用系統資源。惡性病毒具有明確的目的，或破壞數據、刪除文件，或加密磁盤、格式化磁盤，甚至造成不可挽回的損失。

不可預見性

從病毒的監測方面看，病毒還有不可預見性。計算機病毒常常被人們修改,致使許多病毒都生出不少變種、變體，而且病毒的製作技術也在不斷地深入性提高,病毒對反病毒軟件常常都是超前的,無法預測。

觸發性

病毒因某個事件或數值的出現，誘使病毒實施感染或進行進攻的特性稱為可觸發性。病毒既要隱蔽又要維持攻擊力，就必須有可觸發性。

病毒的觸發機制用於控制感染和破壞動作的頻率。計算機病毒一般都有一個觸發條件，它可以按照設計者的要求在某個點上激活並對系統發起攻擊。

針對性

有一定的環境要求，並不一定對任何系統都能感染。

寄生性

計算機病毒程序嵌入到宿主程序中，依賴於宿主程序的執行而生存，這就是計算機病毒的寄生性。

病毒程序在浸入到宿主程序後，一般會對宿主程序進行一定的修改，宿主程序一旦執行，病毒程序就被激活，從而進行自我複制。

通常認為，計算機病毒的主要特點是傳染性、隱蔽性、潛伏性、寄生性、破壞性。

病毒介紹

計算機病毒是人為製造的，有破壞性，又有傳染性和潛伏性的，對計算機信息或系統起破壞作用的程序。它不是獨立存在的，而是隱蔽在其他可執行的程序之中。計算機中病毒後，輕則影響機器運行速度，重則死機系統破壞；因此，病毒給用戶帶來很大的損失，通常情況下，我們稱這種具有破壞作用的程序為計算機病毒。

計算機病毒結構

一般由引導模塊、傳染模塊、表現模塊三部分組成。

引導模塊	引導代碼
傳染模塊	傳染條件判斷
	傳染代碼
表現模塊	表現及破壞條件判斷
	破壞代碼

病毒分類（按照宿主分類）

（1）引導型病毒
引導區型病毒侵染軟（硬、優）盤中的“主引導記錄”
（Master Boot Record，0柱面0磁頭1扇區）
解釋：引導型病毒是放在引導型扇區裡面，在計算機中都有個0柱面0磁頭1扇區特殊的記錄，是計算機開機的重要文件，病毒把Master Boot Record代碼修改之後，在計算機開機的時候可能就會先激活病毒。

（2）文件型病毒
通常它感染各種可執行文件、有可解釋執行腳本的文件、可包含宏代碼的文件。每一次它們激活時，感染文件把病毒代碼自身複製到其他文件中。

（3）混合型病毒
混合型病毒通過技術手段把引導型病毒和文件型病毒組合成一體，使之具有引導型病毒和文件型病毒兩種特徵，以兩者相互促進的方式進行傳染。這種病毒既可以傳染引導區又可以傳染可執行文件，增加了病毒的傳染性以及生存率，使其傳播範圍更廣，更難於清除乾淨。

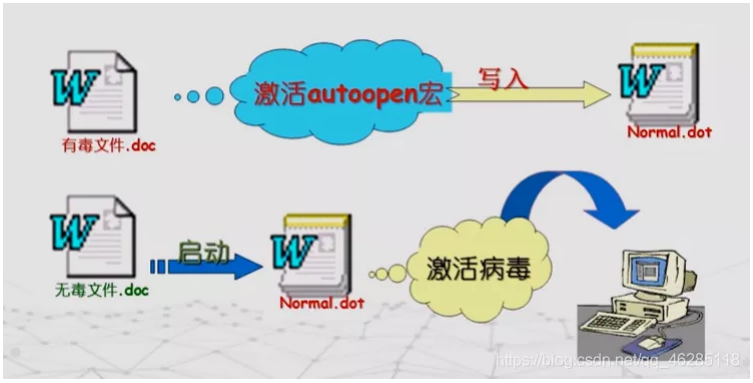
經典實例

宏病毒

1.病毒是一種使用宏編輯語言編寫的病毒，主要寄生於Word文檔或模板的宏中。一旦打開這樣的文檔，宏病毒就會被激活，進入計算機內存並駐留在Normal模板上，從而感染所有自動保存的文檔。如果網絡上其他用戶打開感染病毒的文檔，宏病毒就會轉移到他的計算機上。

宏病毒通常使用VB腳本，影響微軟的Office組建或類似的應用軟件，大多通過郵件傳播。
在我們計算機的Word文檔中就可以找到宏，

2.宏病毒的工作原理：



3.宏病毒的特點：
（1）感染數據文件。一般病毒只感染程序，而宏病毒專門感染數據文件。
（2）多平台交叉感染。當Word、Excel這類軟件在不同平台（如Windows、OS/2和MacinTosh）上運行時，會被宏病毒交叉感染。
（3）容易編寫。宏病毒以源代碼形式出現，所以編寫和修改宏病毒就更容易了。這也是宏病毒的數量居高不下的原因。
（4）容易傳播。只要打開帶有宏病毒的電子郵件，計算機就會被宏病毒感染。此後，打開或新建文件都會感染宏病毒。

4.宏病毒的預防
防治宏病毒的根本在於限制宏的執行。
（1）禁止所有宏的執行。在打開Word文檔時，按住Shift鍵，即可禁止自動宏，從而達到防治宏病毒的目的。

（2）檢查是否存在可疑的宏。若發現有一些奇怪名字的宏，肯定就是病毒無疑了，將它立即刪除即可。即便刪錯了也不會對Word文檔內容產生任何影響。具體做法是，選擇【工具】【| 宏】命令，打開【宏】對話框，選擇要刪除的宏，單擊【刪除】按鈕即可。

（3）按照自己的習慣設置。重新安裝Word後，建立一個新文檔，將Word的工作環境按照自己的使用習慣進行設置，並將需要使用的宏一次編制好，做完後保存新文檔。這時候的Normal.dot模板絕對沒有宏病毒，可將其備份起來。在遇到宏病毒時，用備份的Normal.dot模板覆蓋當前的模板，可以消除宏病毒。

（4）使用Windows自帶的寫字板。在使用可能有宏病毒的Word文檔時，先用Windows自帶的寫字板打開文檔，將其轉換為寫字板格式的文件保存後，再用Word調用。因為寫字板不調用、不保存宏，文檔經過這樣的轉換，所有附帶的宏（包括宏病毒）都將丟失。

（5）提示保存Normal模板。選擇【工具】【| 選項】命令，在【選項】對話框中打開【保存】選項卡，選中【提示保存Normal模板】複選框。一旦宏病毒感染了Word文檔，退出Word時，Word就會出現“更改的內容會影響到公用模板Normal，是否保存這些修改內容？”的提示信息，此時應選擇“否”，退出後進行殺毒。

（6）使用.rtf和.csv格式代替.doc和.xls。因為.rtf和.csv格式不支持宏功能，所以交換文件時候，用.rtf格式的文檔代替.doc格式，用.csv格式的電子表格代替.xls格式。這樣就可以避免宏病毒的傳播。

5.宏病毒的清除
（1）手工清除。選取【工具】【| 宏】命令，打開【宏】對話框，單擊【管理器】命令按鈕，打開【管理器】對話框，選擇【宏方案項】選項卡，在【宏方案項的有效範圍】下拉列表中選擇要檢查的文檔，將來源不明的宏刪除。退出Word，然後到C盤根目錄下查看有沒有Autoexec.dot文件，如果有這個文件就刪除，再找到Normal.dot文件，刪除它。Word會自動重新生成一個乾淨的Normal.dot文件。到目錄C:\Program Files\Microsoft Office\Office\Startup 下查看有沒有模板文件，如果有而且不是用戶自己建立的，則刪除它。重啟Word，這時Word已經恢復正常了。
（2）使用專業殺毒軟件。目前的專業殺毒軟件都具有清除宏病毒的能力。但是如果是新出現的病毒或者是病毒的變種則可能不能正常清除，此時需要手工清理.

蠕蟲

1.定義：
蠕蟲（Worm）是一種通過網絡傳播的惡性病毒，通過分佈式網絡來擴散傳播特定的信息或錯誤，進而造成網絡服務遭到拒絕並發生死鎖。

2. 蠕蟲病毒的基本結構和傳播過程
蠕蟲的基本程序結構包括以下三個模塊
（1）傳播模塊：負責蠕蟲的傳播，傳播模塊又可分為三個基本模塊，即掃描模塊、攻擊模塊和復制模塊。
（2）隱藏模塊：浸入主機後，隱藏蠕蟲程序，防止被用戶發現。
（3）目的功能模塊：實現對計算機的控制、監視或破壞等功能。

蠕蟲程序的一般傳播過程為：

（1）掃描：由蠕蟲的掃描功能模塊負責探測存在漏洞的主機。當程序向某個主機發送探測漏洞的信息並收到成功的反饋信息後，就得到一個可傳播的對象。

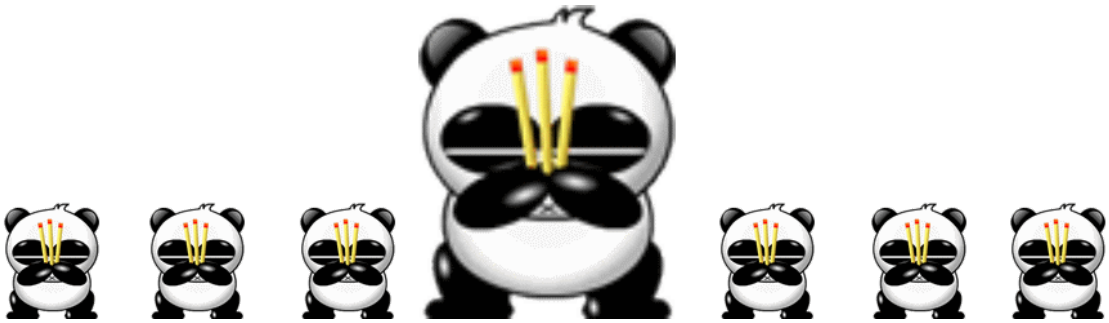
（2）攻擊：攻擊模塊按漏洞攻擊步驟自動攻擊步驟1中找到的對象，取得該主機的權限（一般為管理員權限），獲得一個shell。

（3）複製：複製模塊通過原主機和新主機的交互將蠕蟲程序複製到新主機並啟動。

由此可見，傳播模塊實現的實際上是自動入侵的功能，所以蠕蟲的傳播技術是蠕蟲技術的核心。

3.蠕蟲病毒實例——熊貓燒香

熊貓燒香是一個感染型的蠕蟲病毒，它能感染系統中exe，com，pif，src，html，asp等文件，它還能結束大量的反病毒軟件進程。



熊貓燒香是一種蠕蟲病毒的變種，經過多次變種而來，由於中毒電腦的可執行文件會出現“熊貓燒香”圖案，所以也被稱為“熊貓燒香”病毒。但原病毒只會對exe文件的圖標進行替換，並不會對系統本身進行破壞。而大多數是中等病毒變種，用戶電腦中毒後可能會出現藍屏、頻繁重啟以及系統硬盤中數據文件被破壞等現象。

同時，該病毒的某些變種可以通過局域網進行傳播，進而感染局域網內所有計算機系統，最終導致企業局域網癱瘓，無法正常使用，它能感染系統中exe，com，pif，src，html，asp等文件，它還能終止大量的反病毒軟件進程並且會刪除擴展名為gho的備份文件。被感染的用戶系統中所有.exe可執行文件全部被改成熊貓舉著三根香的模樣。

木馬

1.定義：

木馬全稱為特洛伊木馬（Trojan Horse,英文則簡稱Trojan），在計算機安全學中，特洛伊木馬是指一種計算機程序，表面上或實際上有某種有用的功能，同時又含有隱藏的可以控制用戶計算機系統、危害系統安全的功能，可能造成用戶資料的洩漏、破壞或整個系統的崩潰。在一定程度上，木馬也可以稱為計算機病毒。

2.木馬病毒工作原理

一個完整的特洛伊木馬套裝程序含了兩部分：服務端（服務器部分）和客戶端（控制器部分）。植入對方電腦的是服務端，而黑客正是利用客戶端進入運行了服務端的電腦。運行了木馬程序的服務端以後，會產生一個有著容易迷惑用戶的名稱的進程，暗中打開端口，向指定地點發送數據（如網絡遊戲的密碼，即時通信軟件密碼和用戶上網密碼等），黑客甚至可以利用這些打開的端口進入電腦系統。

3.木馬病毒的檢測

查看system.ini、win.ini、啟動組中的啟動項目。在【開始】【| 運行】命令，輸入msconfig，運行Windows自帶的“系統配置實用程序”。選中system.ini標籤，展開【boot】目錄，查看“shell=”這行，正常“shell=Explorer.exe”，如果不是，就有可能中了木馬病毒。選中win.ini標籤，展開【windows】目錄項，查看“run=”和“load=”行，等號後面應該為空。再看看有沒有非正常啟動項目，要是有類似netbus、netspy、bo等關鍵詞，就極有可能是中了木馬。

其他的一些方法，例如在正常操作計算機時，發現計算機的處理速度明顯變慢、硬盤不停讀寫、鼠標不聽使喚、鍵槃無效、一些窗口自動關閉或打開……這一切都表明可能是木馬客戶端在遠程控制計算機。

4.木馬病毒實例

Internet上每天都有新的木馬出現，所採取的隱蔽措施也是五花八門。下面介紹幾種常見的木馬病毒的清除方法。

1）冰河 v1.1 v2.2
冰河是最好的国产木马。
清除木马 v1.1
打开注册表 Regedit，点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 查找以下的两个路径，并删除
" C:\windows\system\ kernel32.exe"
" C:\windows\system\ sysexplr.exe"
关闭 Regedit
重新启动到 MSDOS 方式
删除 C:\windows\system\ kernel32.exe 和 C:\windows\system\ sysexplr.exe 木马程序，重新启动。
清除木马 v2.2
服务器程序、路径用户是可以随意定义的，写入注册表的键名也可以自己定义。
因此，不能明确说明。
你可以察看注册表，把可疑的文件路径删除。
重新启动到 MSDOS 方式
删除于注册表相对应的木马程序
重新启动 Windows，清除完毕。
2）Acid Battery v1.0
清除木马的步骤：
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
删除右边的 Explorer ="C:\WINDOWS\expiorer.exe"
关闭 Regedit
重新启动到 MSDOS 方式
删除 c:\windows\expiorer.exe 木马程序
注意：不要删除正确的 ExpLorer.exe 程序，它们之间只有 i 与 L 的差别。
重新启动，清除完毕。
3）AttackFTP
清除木马的步骤：
打开 win.ini 文件
在【WINDOWS】下面有 load=wscan.exe
删除 wscan.exe ，正确是 load=
保存退出 win.ini。
打开注册表 Regedit
点击目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
删除右边的 Reminder="wscan.exe /s"
关闭 Regedit，重新启动到 MSDOS 系统中
删除 C:\windows\system\ wscan.exe
清除完毕。

預防病毒

病毒預防

1.對病毒的預防在病毒防治工作中起主導作用，是病毒防治的重點，主要針對病毒可能入侵的系統薄弱環節加以保護和監控。預防計算機病毒要從以下幾個方面著手。

（1）檢查外來文件。對於網絡上下載的或者外部存儲器中的程序和文檔，在執行或打開文檔之前，一定要檢查是否有病毒。
（2）局域網預防。盡可能選擇無盤工作站。限制用戶對服務器上可執行文件的操作。使用抗病毒軟件動態檢查使用中的文件。
（3）使用確認和數據完整性工具。
（4）週期性備份工作文件。

2.網絡病毒的防治相對單機病毒的防治具有更大的難度。目前，網絡大都採用Client/Server（客戶機/服務器）的工作模式。防治網絡病毒需要從服務器和工作站兩個主要方面並結合網絡管理著手解決。
（1）在網絡管理方面進行防治
——制定嚴格的工作站安全操作規程。
——建立完整的網絡軟件和硬件的維護製度，定期對各工作站進行維護。
——建立網絡系統軟件的安全管理制度。
——設置正確的訪問權限和文件屬性

（2）基於工作站的防治方法

工作站是網絡的門，只要將這扇門關好，就能有效地防治病毒入侵。可以使用單機反病毒軟件、防病毒卡以及工作站防病毒

芯片。

（3）基於服務器的防治方法

服務器是網絡的核心，一旦服務器被病毒感染，就會使整個網絡陷於癱瘓。目前，基於服務器的防治病毒方法一般採用NLM

（Netware Loadable Module）技術進行程序設計，以服務器為基礎，提供實時掃描病毒能力。其優點主要表現在不佔用工作站的內存，可以集中掃毒，能實現實時掃描功能，以及軟件安裝和升級都很方便等方面。

病毒的入侵必將對系統資源構成威脅，即使良性病毒也要侵吞系統的寶貴資源，所以防治病毒入侵遠比病毒入侵後再加以清除更為重要。抗病毒技術必須建立“預防為主，消滅結合”的基本觀念。

檢測病毒

檢測計算機上是否被病毒感染，通常可以採用手工檢測和自動檢測。

——手工檢測是指通過一些工具軟件（比如Debug.com、Pctools.exe等），對易遭病毒攻擊和修改的內存及磁盤的相關部分進行檢測，通過與正常狀態進行對比來判斷是否被病毒感染。雖然該方法操作複雜，易出錯且效率低，但是該方法可以檢測和識別未知病毒，以及檢測一些自動檢測工具不能識別的新病毒。

——自動檢測是指通過一些診斷軟件和殺毒軟件，來判斷一個系統或磁盤是否有病毒，如使用瑞星、金山毒霸等軟件。雖然該方法可以方便檢測大量病毒且操作簡單，但是自動檢測工具只能識別已知的病毒，而且它的發展總是滯後於病毒的發展。對病毒進行檢測可以採用手工方法和自動方法相結合的方式。檢測病毒的技術和方法主要有以下幾種。

比較法

比較法是將原始備份與被檢測的引導扇區或被檢測的文件進行比較。該方法的優點是簡單、方便，不需要專用軟件。缺點是無法確認計算機病毒的種類和名稱。由於要進行比較，保存好原始備份就非常重要了，製作備份時必須在無計算機病毒的環境下進行，製作好的備份必須妥善保管，貼上標籤，並加上寫保護。

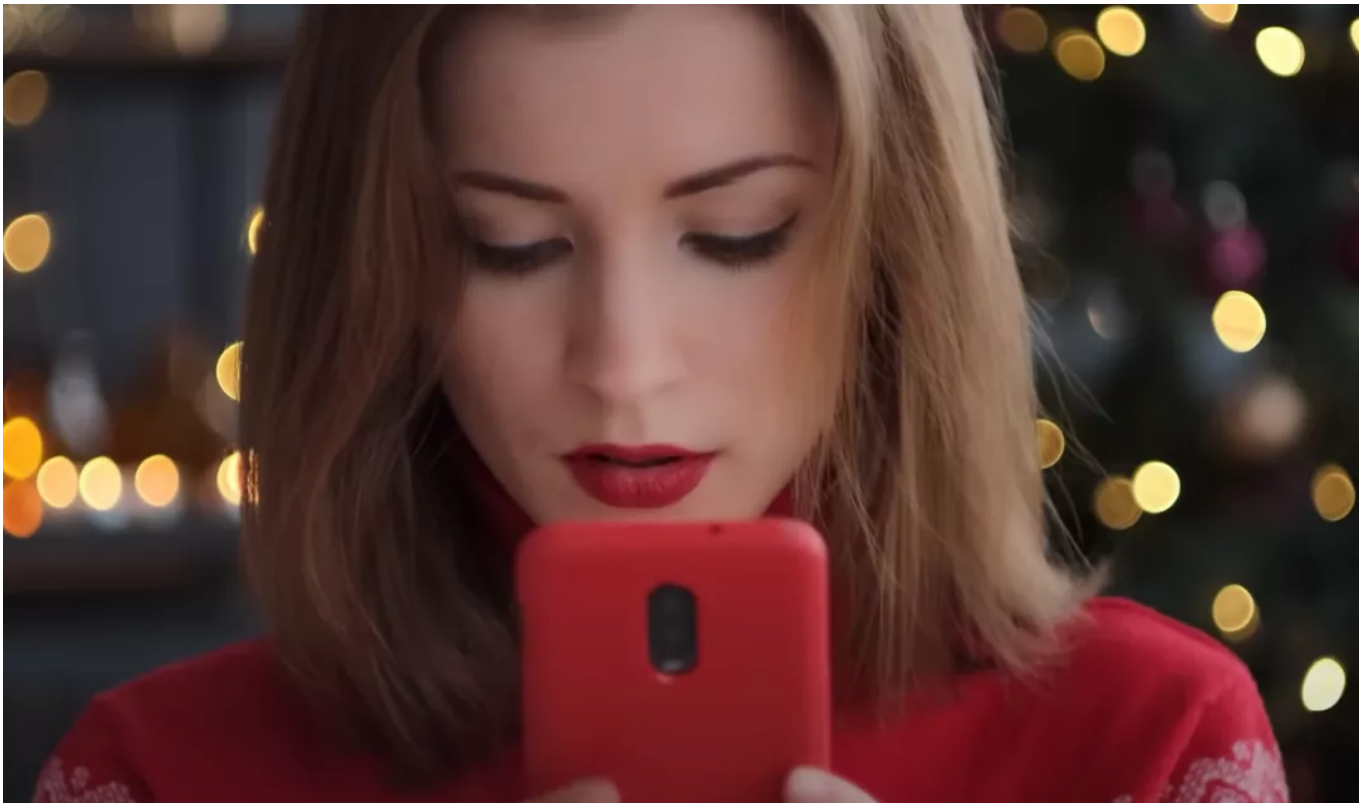
特征代碼法

特征代碼法是用每一種計算機病毒體含有的特定字符串對被檢測的對象進行掃描。如果被檢測對象內部發現了某一種特定字符串，就表明發現了該字符串所代表的的計算機病毒，這種計算機病毒掃描軟件稱之為Virus Scanner。該方法優點是檢測準確快速、可識別病毒的名稱、誤報警率低，依

據檢測結果可做解毒處理。缺點是不能檢測未知病毒，且蒐集已知病毒的特征代碼費用開銷大，在網絡上效率低。

分析法

分析法是防殺計算機病毒不可缺少的重要技術，該方法要求具有比較全面的有關計算機、DOS、Windows、網絡等的結構和功能調用，以及與計算機病毒相關的各種知識。除此之外，還需要反彙編工具、二進製文件編輯器等用於分析的工具程序和專用的實驗計算機。分析的步驟分為靜態分析和動態分析兩種。靜態分析是指利用反彙編工具將計算機病毒代碼打印成反彙編指令程序清單後進行分析，了解計算機病毒分成哪些模塊，使用了哪些系統調用，採用了哪些技巧，並將計算機病毒感染文件的過程翻轉為清除計算機病毒、修復文件的過程。動態分析是指，利用DEBUG等調試工具在內存帶毒的情況下，對計算機病毒做動態跟踪，觀察計算機病毒的具體工作過程，以進一步在靜態分析的基礎上理解計算機病毒的工作原理。



校驗和法

計算正常文件的校驗和，並將結果寫入此文件或其他文件中保存。在文件使用過程中或使用之前，定期檢查文件的校驗和與原來保存的校驗和是否一致，從而可以發現文件是否被感染，這種方法稱為校驗和。該方法優點是方法簡單，能發現未知病毒，也能發現被檢查文件的細微變化。缺點是會誤報警，不能識別病毒名稱，不能對付隱蔽型病毒。

行為監測法

行為監測法是利用病毒的特有行為特徵性來監測病毒的方法。監測病毒的行為特徵如下。

——佔有INT 13H所有的引導型病毒，都攻擊Boot扇區或主引導扇區。
——修改DOS系統數據區的內存總量。
——對.com、.exe文件進行寫入操作。
——病毒程序與宿主程序進行切換。

行為監測法的優點是可發現未知病毒，能夠相當準確地預報未知的多數病毒。行為監測法的缺點是會誤報警，不能識別病毒
名稱，實現時有一定難度。

軟件仿真掃描法

該技術專門用於對付多態性計算機病毒，能夠仿真CPU執行，在DOS虛擬機下偽執行計算機病毒程序，安全地將其解密，然後再進行掃描。

先知掃描法

先知掃描技術就是將專業人員用來判斷程序是否存在計算機病毒代碼的方法，分析歸納成專家系統和知識庫，再利用軟件仿
真技術偽執行新的計算機病毒，超前分析出新計算機病毒代碼，用於對付以後的計算機病毒。

人工智能陷阱技術和宏病毒陷阱技術

人工智能陷阱技術是一種監測計算機行為的常駐式掃描技術。其優點是執行速度快、操作簡便，且可以檢測到各種計算機病
毒；缺點是程序設計難度大，且不容易考慮周全。
宏病毒陷阱技術則是結合了特征代碼法和人工智能陷阱技術，根據行為模式來檢測已知及未知的宏病毒。

實時I/O掃描

實時I/O掃描的目的在於即時對計算機上的輸入/輸出數據作病毒碼比對，希望能夠在病毒尚未被執行前，將病毒防禦於門外。

網絡病毒檢測技術

網絡監測法是一種檢查、發現網絡病毒的方法。網絡病毒的特點是通過網絡進行傳播，如果在服務器、網絡接入端和網站設置病毒防火牆，可以起到大規模防止病毒擴散的目的。

殺毒技術

將染毒文件的病毒代碼摘除，使之恢復為可正常運行的文件，稱為病毒的清除。清除病毒所採用的技術稱為殺毒技術。

引導型病毒的清除

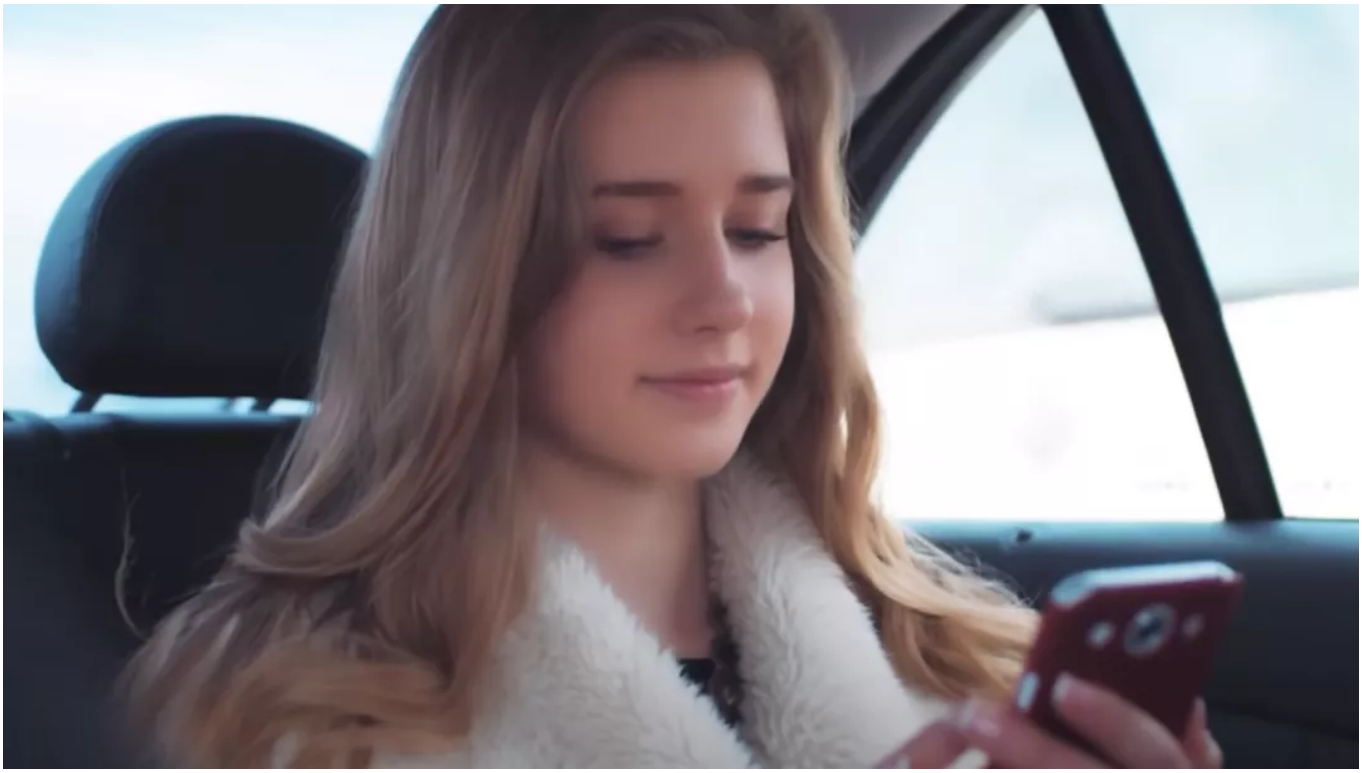
引導型病毒感染時一般攻擊硬盤主引導區以及硬盤或移動存儲介質的Boot扇區。一般使用FDISK/MBR可以清除大多數引導型病毒。

宏病毒的清除

為了恢復宏病毒，須用非文檔格式保存足夠的信息。RTF（Rich Text Format）適合保留原始文檔的足夠信息而不包含宏。然後退出文檔編輯器，刪除已感染的文檔文件以及Normal.dot和start-up目錄下的文件。

文件型病毒的清除

一般文件型病毒的染毒文件可以修復。當恢復受感染文件需要考慮下列因素。
——不管文件的屬性，測試和恢復所有目錄下的可執行文件。
——希望確保文件的屬性和最近修改時間不改變。
——一定考慮一個文件多重感染的情況。



病毒的去激活

清除內存中的病毒是指把RAM中的病毒進入非激活狀態。這需要操作系統和彙編語言的知識。

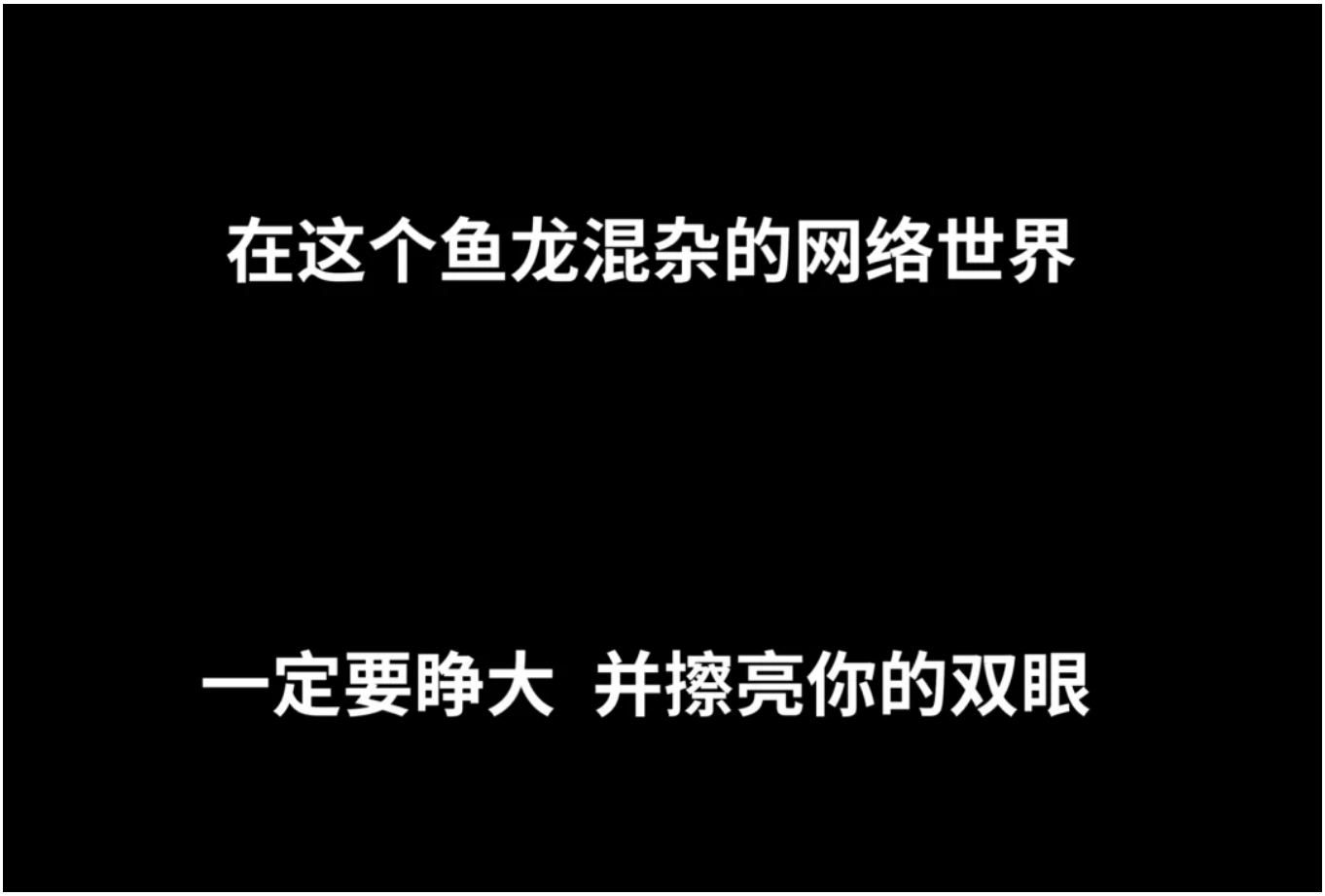
使用殺病毒軟件清除病毒

計算機一旦感染病毒，一般用戶首選是使用殺病毒軟件來清除病毒。其優點是使用方便、技術要求不高，不需要具有太多的計算機知識。缺點是有時會刪除帶毒文件，可能導致系統不能正常運行，同時需要經常升級病毒代碼庫。

結語

在因特網技術以及計算機技術不斷發展的形勢下，我國已經完全進入信息化時代，信息化時代的到來，使得人們的生活以及工作都得到了極大地方便，但是，在為人們提供錄入巨大方便的同時，網絡同樣也存在著一定的安全隱患。

因此，我們對於一些開放型的信息必須要加大其控制的力度，嚴防黑客以及破壞分子的不法行為。這是一場無形的戰鬥，在這場鬥爭中，安全技術是最為關鍵的方面，提高安全防禦技術，是提高我國計算機網絡安全的根本所在。



號外！號外！

Java 極客技術微信群中有很多優秀的小伙伴在討論技術，偶爾還有不定期的資料分享和紅包發放！如果你想提升自己，並且想和優秀的人一起進步，請添加下方微信，阿粉會迅速拉你進群。

注意：添加好友時，備註【加群】可以更快的拉你進群哦！

喜歡就分享

認同就點贊

支持就在看

一鍵四連，你的offer也四連

喜歡此內容的人還喜歡

工業控制系統中的蓋茨木馬應急響應

SupCERT

記一次Kubernetes 集群被入侵，服務器變礦機

湃森信息科技