第三节 计算机病毒和木马的基本知识和预防

本节内容

一．计算机病毒的基本知识

二．计算机病毒的主要特征

三．计算机病毒常见的表现现象

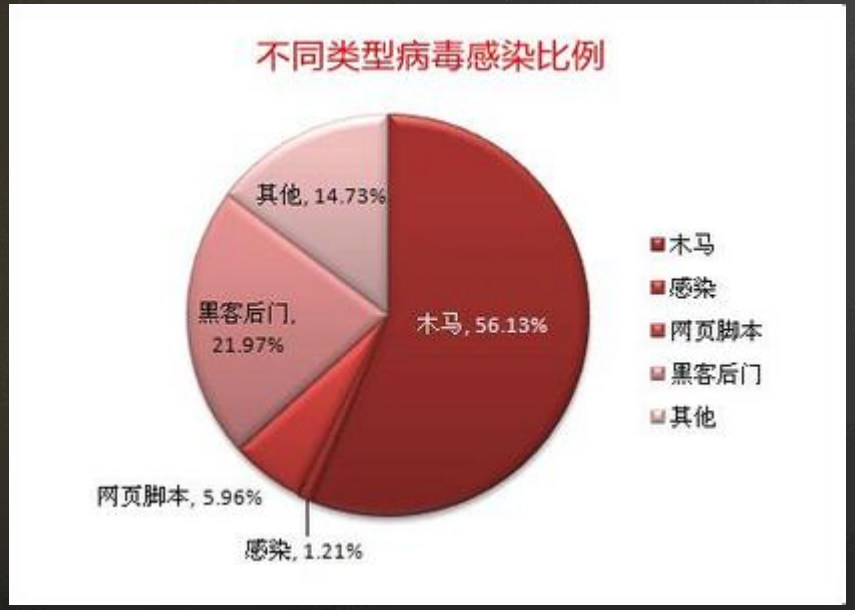
四．计算机病毒和木马的区别

五．计算机病毒、木马的预防方法

六．360安全卫士的功能和使用方法

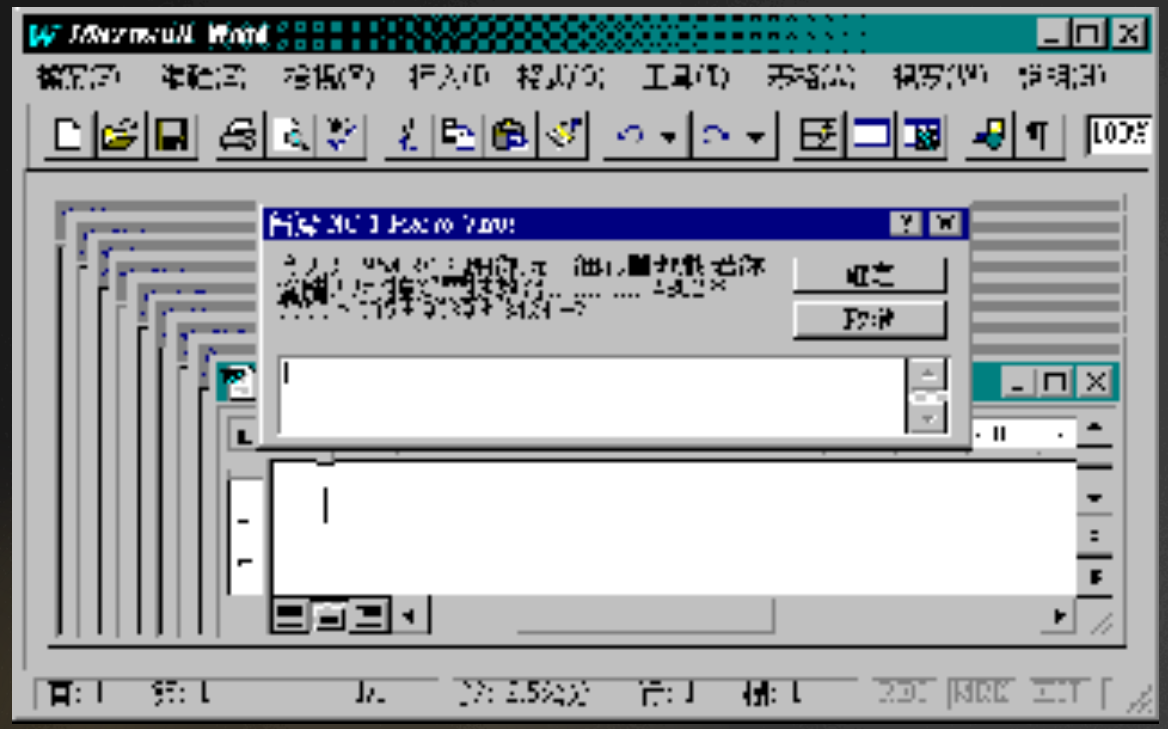
一、计算机病毒的概念

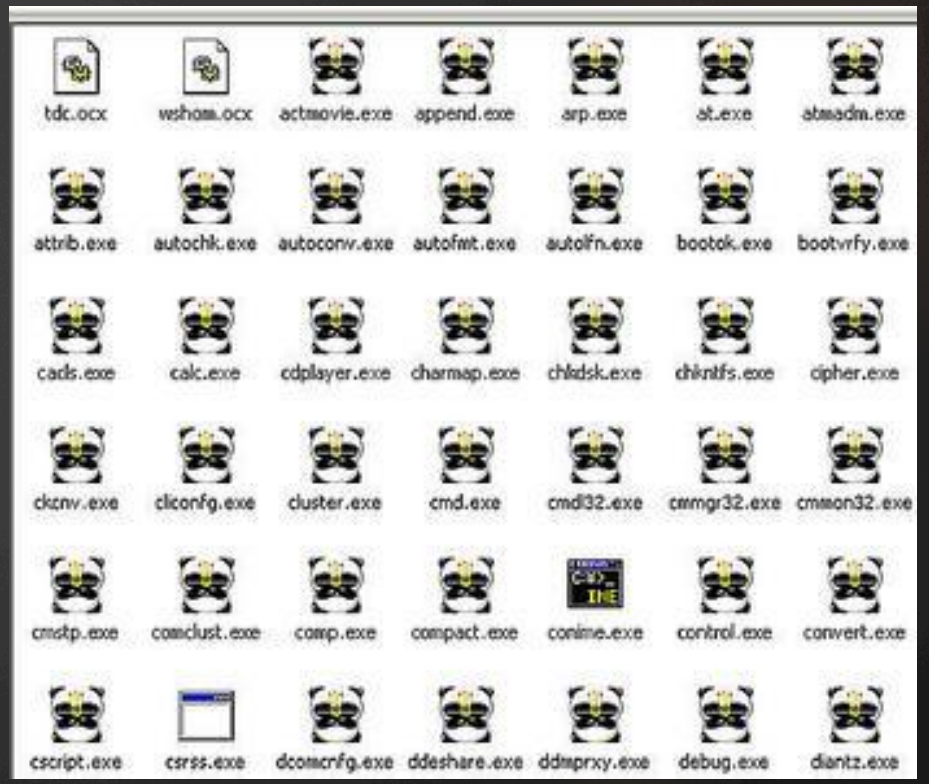
- 计算机病毒是指编制成单独的或者附着在其他计算机程序上用以破坏或降低计算机功能或者毁坏数据，影响计算机使用，并能够自我复制的一组计算机指令或程序代码。



二、计算机病毒的特征

- 可执行性：计算机病毒是一段可执行的指令代码。
- 寄生性：大多数病毒将自身附着在已存在的程序上，并将其代码插入该程序，当该程序执行时，该病毒也被执行。
- 传染性：所有的计算机病毒都能传染给其他未感染该类计算机病毒的计算机。
- 破坏性：计算机病毒或多或少地都对计算机有一定的破坏作用。




tdc.ocx
wshom.ocx
actmovie.exe
append.exe
arp.exe
at.exe
atmadm.exe
attrib.exe
autochk.exe
autoconv.exe
autofmt.exe
autolfn.exe
bootok.exe
bootvrfy.exe
cacls.exe
calc.exe
cdplayer.exe
charmap.exe
chkdsk.exe
chkntfs.exe
cipher.exe
ckcnv.exe
cliconfg.exe
cluster.exe
cmd.exe
cmd32.exe
cmmgr32.exe
cmmon32.exe
cmstp.exe
comclust.exe
comp.exe
compact.exe
conime.exe
control.exe
convert.exe
cscript.exe
csrss.exe
dcomcnfg.exe
ddeshare.exe
ddmprxy.exe
debug.exe
diantz.exe

- 欺骗性：有些计算机病毒能隐藏它对计算机的文件或引导扇区的修改，当程序读这些文件或扇区时，这些文件或扇区表现的是未被修改的原貌，其目的是欺骗反病毒程序，使其认为这些文件或扇区并未被修改。
- 隐藏性和潜伏性：计算机病毒都能利用操作系统的弱点将自己隐藏起来，使用常规方法难以查出；计算机病毒并不是随时都在运行，而是有一定的激发条件，当条件不满足时，它潜伏在计算机的外存中并不执行。
- 衍生性：有一部分病毒具有多态性，它每感染一个EXE文件就会演变成另一种病毒。

3、计算机病毒的表现形式

1）在特定情况下屏幕上出现某些异常字符或特定画面；

2）文件长度异常增减或莫名产生新文件；

3）一些文件打开异常或突然丢失；

4）系统无故进行大量磁盘读写或未经用户允许进行格式化操作；

5）可用的内存或硬盘空间变小；

6）系统出现异常的重启现象，经常死机，或者蓝屏无法进入系统；

7）打印机等外部设备出现工作异常；

8）在汉字库正常的情况下，无法调用和打印汉字或汉字库无故损坏；

9）磁盘上无故出现扇区损坏；

10）程序或数据神秘地消失了，文件名不能辨认等。

4、木马

- “木马”程序是目前比较流行的病毒文件，与一般的病毒不同，它不具备破坏性和主动传播性。
- 它的基本原理是：通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种主机的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种主机。

- “木马”与计算机网络中常常要用到的远程控制软件有些相似，但由于远程控制软件是“善意”的控制，因此通常不具有隐蔽性；“木马”则完全相反，木马要达到的是“偷窃”性的远程控制，如果没有很强的隐蔽性的话，那就是“毫无价值”的。
- 与病毒的区别：

① 木马不主动传播，不破坏，而是窃听

② 计算机病毒式是主动攻击，而木马是被动攻击，所以更难预防

木 马 计

5、计算机病毒和木马的预防

一般来说，计算机病毒的预防分为两种：管理方法上的预防和技术上的预防，而在一定的程度上，这两种方法是相辅相成的。

（1）用管理手段预防的方法

- 系统启动盘要专用，并且要加上写保护，以防止病毒侵入。
- 尽量不使用来历不明的软盘或U盘，除非经过彻底检查。
- 尽量不使用非法复制或解密的软件。
- 不要轻易让他人使用自己的系统，如果无法做到这点，至少不能让他们自己带程序盘来使用。

- 对于重要的系统盘、数据盘及硬盘上的重要文件内容要经常备份，以保证系统或数据遭到破坏后能及时得到恢复。
- 经常利用各种病毒检测软件对硬盘进行相应的检查，以便及时发现和消除病毒。
- 对于网络上的计算机用户，要遵守网络软件的使用规定，不要随意使用网络上外来的软件，尤其是当从电子邮件或从互联网上下载文件时，在打开这些文件前，应用反病毒工具扫描该文件。

（2）用技术手段预防的方法

采用一定的技术措施，如防病毒软件、防火墙软件等，预防计算机病毒对系统的入侵，或发现病毒欲传染时，向用户发出警报。

- 瑞星
- 360安全卫士
- 木马克星
- 金山毒霸
- 诺顿防病毒软件

6、病毒的清除注意事项

- 注意文件提前备份
- 断开网络连接进行查杀
- 当无法再Windows下进行查杀时，可以提前该制作一张DOS环境下的杀毒软盘，作为应对措施，进行杀毒。
- 及时安装补丁
- 及时更新病毒库

7、360安全卫士软件的介绍（实操部分讲解）

- 软件的下载、安装、功能了解
- 具体操作：电脑体检、查杀木马、清理插件、修复漏洞、系统修复、软件管家、木马防火墙等