计算机病毒的分析与处理

2010年12月10日

计算机病毒基础

- 计算机病毒的定义、特征、结构及其分类
- 计算机病毒的入侵方式及生命周期
- 计算机病毒的传播途径
- 计算机病毒的命名规则
- 计算机病毒的加载方式

计算机病毒的定义

人为编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码被称为计算机病毒（Computer Virus）。

具有破坏性，复制性和传染性。

计算机病毒的特征

非法性

隐藏性

潜伏性

可触发性

表现性

破坏性

传染性

针对性

变异性

不可预见性

计算机病毒的结构

- 程序结构
- 存储结构

计算机病毒程序的组成部分

- 引导部分 - 将病毒主题加载到内存，为传染部分做准备。
- 传染部分 - 将病毒代码复制到传染目标。
- 表现部分
- 破坏部分

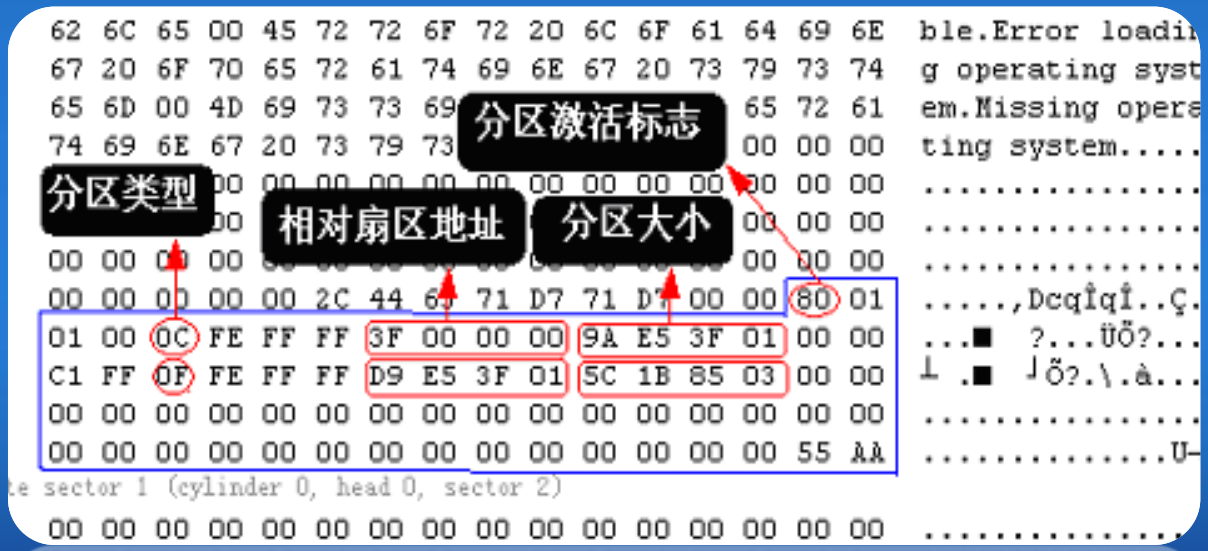
计算机病毒的存储结构

磁盘结构简介：

- MBR - 主引导记录（Main Boot Record）
- DBR - 系统引导记录（Dos Boot Record）
- FAT - 文件分配表（File Allocation Table）
- FDT - 文件目录表（File Directory Table）
- DATA

MBR

MBR称为硬盘主引导记录，它是由FDISK建立在柱面0、磁头0，扇区1的磁盘引导记录数据区。



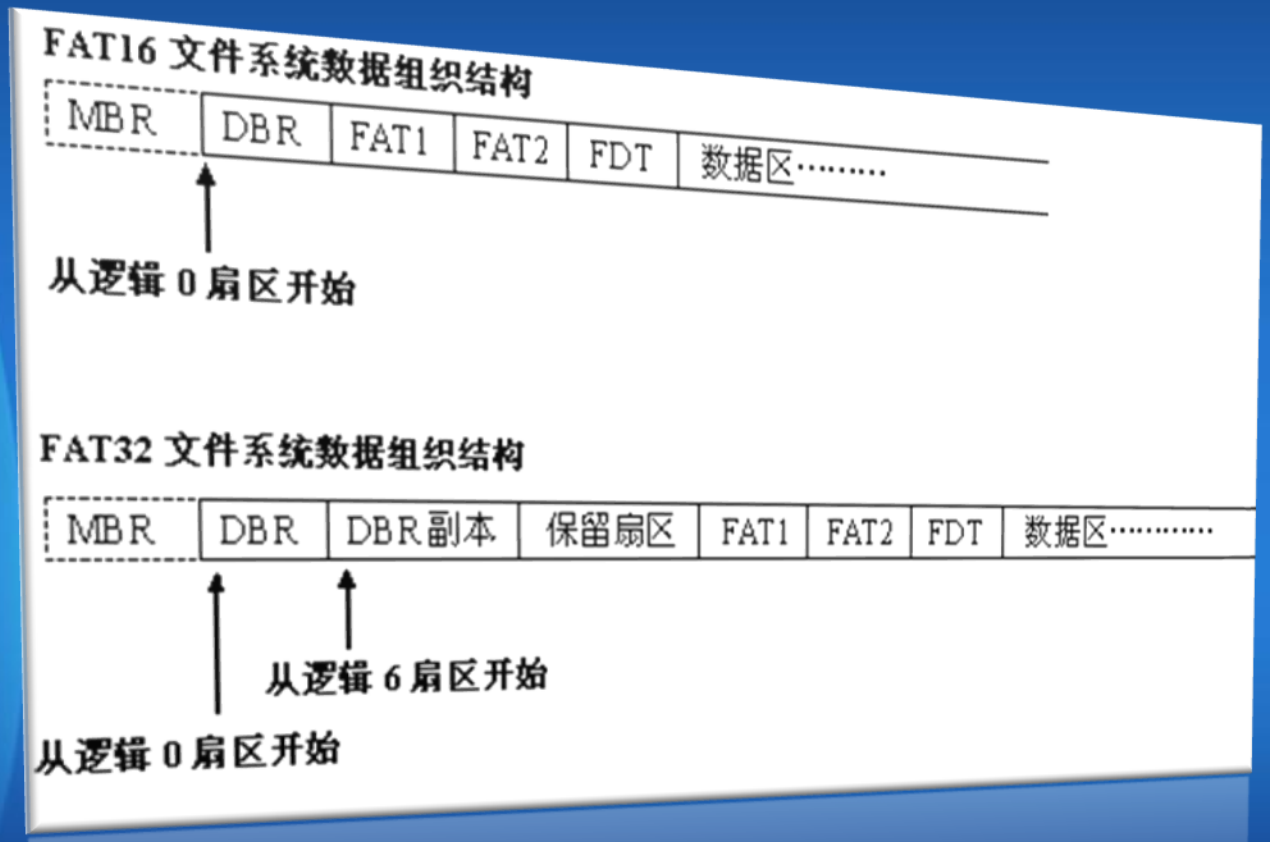
DBR

DBR是经由FORMAT高级格式化写到磁盘逻辑0扇区上的，主要功能是完成DOS系统的自举。

FDT表和FAT表

FDT表和FAT表是FAT文件系统组织结构的两个组成部分，FDT中记录了文件的名字、起始地址等信息，FAT记录了文件在磁盘上的具体位置。

硬盘分区总体结构示意图

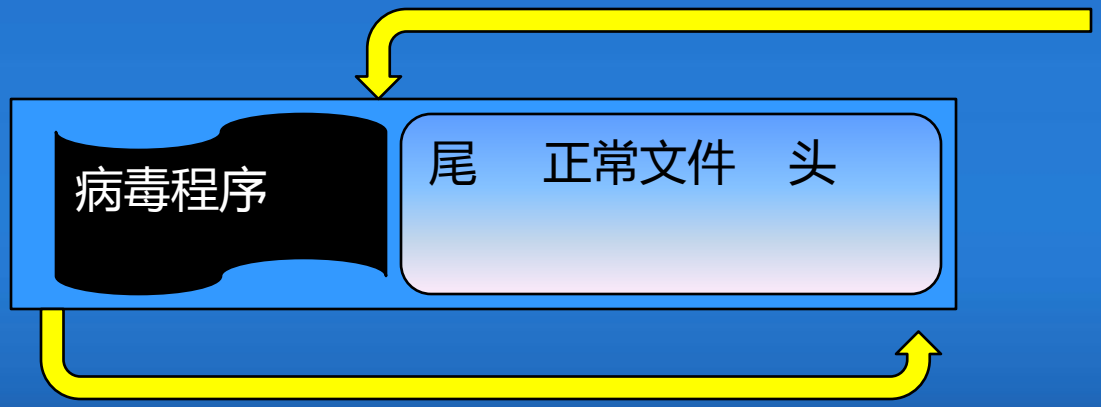


系统型病毒的磁盘存储结构

- 指传染硬盘主引导区或DOS引导扇区的病毒
- 病毒程序被划分为两个部分，第一部分存放在磁盘引导区，第二部分存放在磁盘的其它扇区中并标记为坏簇（簇号存放在磁盘的偏移地址01F9处）。

文件型病毒的磁盘存储结构

依附于宿主文件的首部、尾部、中部或“空闲”部位，病毒程序没有独立占用磁盘上的空白簇。



计算机病毒的分类

- 根据感染方式类型划分
- 根据病毒攻击的操作系统划分
- 根据病毒的链接方式划分
- 根据病毒的破坏情况划分
- 根据与被感染对象的关系分类

根据感染方式类型划分

- 引导型病毒 - - MBR病毒、 BR病毒
- 文件型病毒
- 源码型病毒
- 嵌入型病毒
- 外壳型病毒
- 混合型病毒（又称复合型）

根据病毒攻击的操作系统划分

- DOS - - 早期盛行
- WINDOWS
- UNIX
- OS/2

根据病毒的链接方式划分

- 源码型病毒
- 嵌入型病毒
- 外壳型病毒
- 操作系统型病毒

根据病毒的破坏情况划分

- 良性病毒
- 恶性病毒

根据与被感染对象的关系分类

- 寄生病毒
- 伴随型病毒
- 独立型病毒

计算机病毒的入侵方式

- 源代码嵌入攻击
- 代码取代攻击
- 外壳寄生入侵
- 系统修改入侵

计算机病毒的生命周期

计算机病毒的命名

- 组成病毒名称的六个字段：
- 主行为类型.子行为类型.宿主文件类型.主名称.版本信息.主名称变种号

病毒的主/子行为类型及其对应关系

- Backdoor
- Worm
- Trojan
- Virus
- Harm
- Dropper
- Hack
- Binder

病毒名称	病毒中文名称	病毒介绍
Backdoor	后门	指在不知道也不允许的情况下，在被感染的系统上以隐蔽的方式运行。可以对被感染的系统进行远程控制，而且无法通过正常的方法禁止其运行。“后门”其实是木马的一种特例，它们之间的区别在于“后门”可以对被感染的系统进行远程控制（如：文件管理、进程控制等）。
Worm	蠕虫	指利用系统的漏洞、外发邮件、共享目录、可传输文件的软件（如：MSN、OICQ、IRC等）、可移动存储介质（如：U盘、软盘），这些方式传播自己的病毒。这种类型的病毒其子型行为类型用于表示病毒所使用的传播方式。
Trojan	木马	指在不知道也不允许的情况下，在被感染的系统上以隐蔽的方式运行，而且无法通过正常的方法禁止其运行。这种病毒通常都有利益目的，它的利益目的也就是这种病毒的子行为。
Virus	感染型病毒	指将病毒代码附加到被感染的宿主文件（如：PE文件、DOS下的COM文件、VBS文件、具有可运行宏的文件）中，使病毒代码在被感染宿主文件运行时取得运行权的病毒。
Harm	破坏性程序	指那些不会传播也不感染，运行后直接破坏本地计算机（如：格式化硬盘、大量删除文件等）导致本地计算机无法正常使用的程序。
Dropper	释放病毒的程序	指不属于正常的安装或自解压程序，并且运行后释放病毒并将它们运行。
Hack	黑客工具	指可以在本地计算机通过网络攻击其他计算机的工具。
Binder	捆绑病毒的工具	
Constructor	病毒生成器	指可以生成不同功能的病毒的程序。
Joke	玩笑程序	指运行后不会对系统造成破坏，但是会对用户造成心理恐慌的程序。
Rootkit	越权执行	设法让自己达到和内核一样的运行级别，甚至进入内核空间，这样它就拥有了和内核一样的访问权限，因而可以对内核指令进行修改。
Packer		加了某类专门针对杀毒软件免杀的壳的文件。这种壳专门针对杀毒软件作变形免杀，逃避查杀。

Worm的子行为类型

Trojan 的子行为类型

- Spy
- PSW
- DL
- IMMSG
- MSNMSG
- QQMSG
- ICQMSG
- UCMSG
- Proxy
- Clicker
- Dialer

Hack 的子行为类

宿主文件类型

JS	说明：JavaScript 脚本文件
VBS	说明：VBScript 脚本文件
HTML	说明：HTML 文件
Java	说明：Java 的 Class 文件
COM	说明：Dos 下的 Com 文件
EXE	说明：Dos 下的 Exe 文件
Boot	说明：硬盘或软盘引导区
Word	说明：MS 公司的 Word 文件
Excel	说明：MS 公司的 Excel 文件
PE	说明：PE 文件
WinREG	说明：注册表文件
Ruby	说明：一种脚本
Python	说明：一种脚本
BAT	BAT 脚本文件
IRC	说明：IRC 脚本

主名称

病毒的主名称是由分析员根据病毒体的特征字符串、特定行为或者所使用的编译平台来定的，如果无法确定则可以用字符串”Agent”来代替主名称，小于10k大小的文件可以命名为“Samll”。

主名称变种号

确为是同一家族病毒的条件:

病毒的主行为类型、行为类型、宿主文件类型、主名称均相同.

举例说明

- Trojan.DL.VBS.Agent.cgk
- Trojan.PSW.ZhengTu.afl
- Worm.Mail.Bagle.ld
- Worm.MSN.Kelvir.i
- Backdoor.Agobot.ius
- Hack.DDoSer.Boxed.bc

病毒加载方式

方法	简单描述	例子
修改注册表	通过修改注册表实现开机自启动或者特定情况下启动。	开机启动相关注册表键参考程序AUTORUN（RUN，RUNCONCE，服务，BHO，DEBUG IMAGE HELP，WINLOGON NOTIFY），文件关联
修改相关INI/BAT文件	通过修改INI文件实现开机自启动	Win.ini,system.ini, Autoexec.bat, Config.sys
替换系统文件	通过替换系统文件实现开机启动或者特定情况下启动。	替换explorer.exe实现开机启动。
利用系统特性优先加载	通常为恶意DLL文件，利用WINDOWS系统优先加载当前目录下的DLL特性	在IE所在的目录下增加伪造的ws2_32.dll,使IE启动时加载这个伪造的dll
小段感染代码	感染目标可以为PE文件，HTML文件中的脚本或纯脚本文件，功能仅为简单的加载病毒体	磁碟机
其他	无	自动播放（autorun.inf）

计算机病毒的传播途径

- 网络
- 移动存储介质
- 硬盘
- 光盘
- 点对点通信系统和无线通道

典型病毒分析

- U盘病毒处理演示