3.1 计算机病毒概述

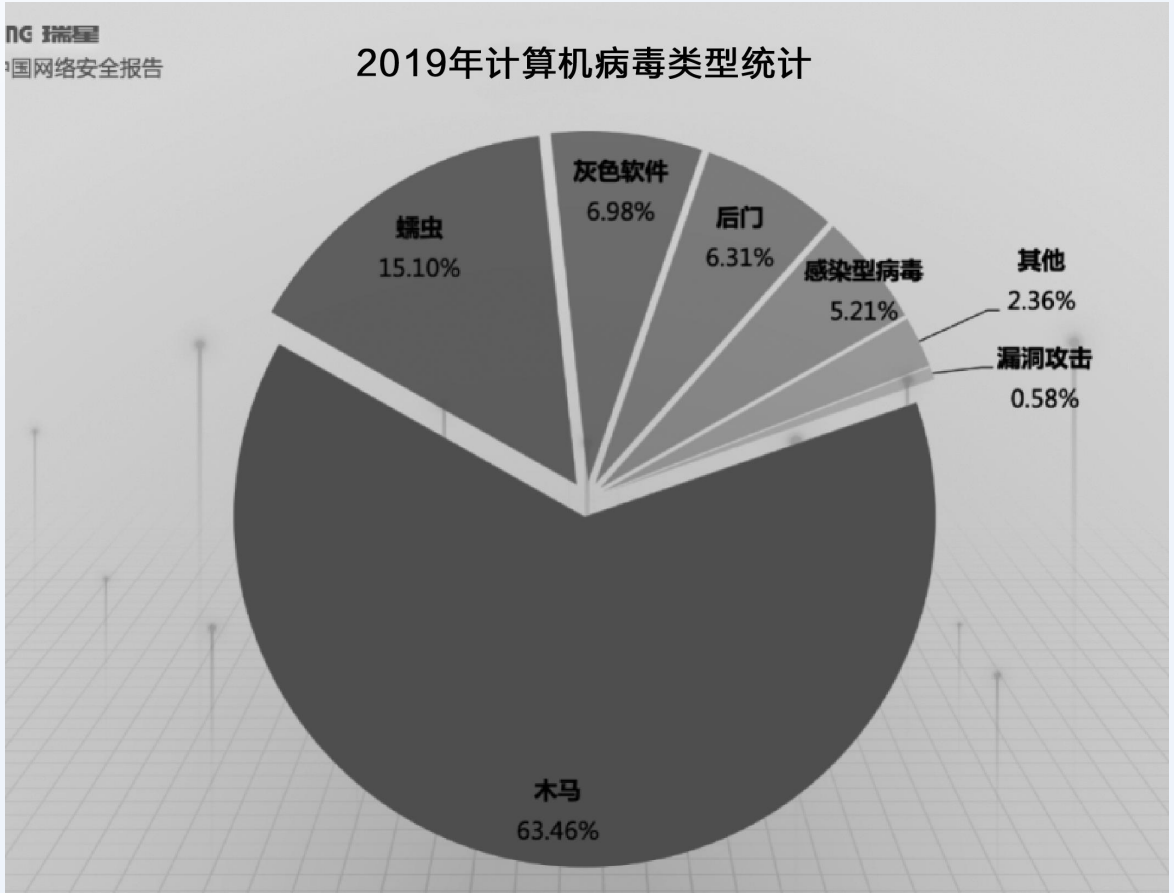
计算机病毒的定义

1994年2月18日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》，在《条例》第二十八条中明确指出：“计算机病毒，指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 ”。

病毒：Virus

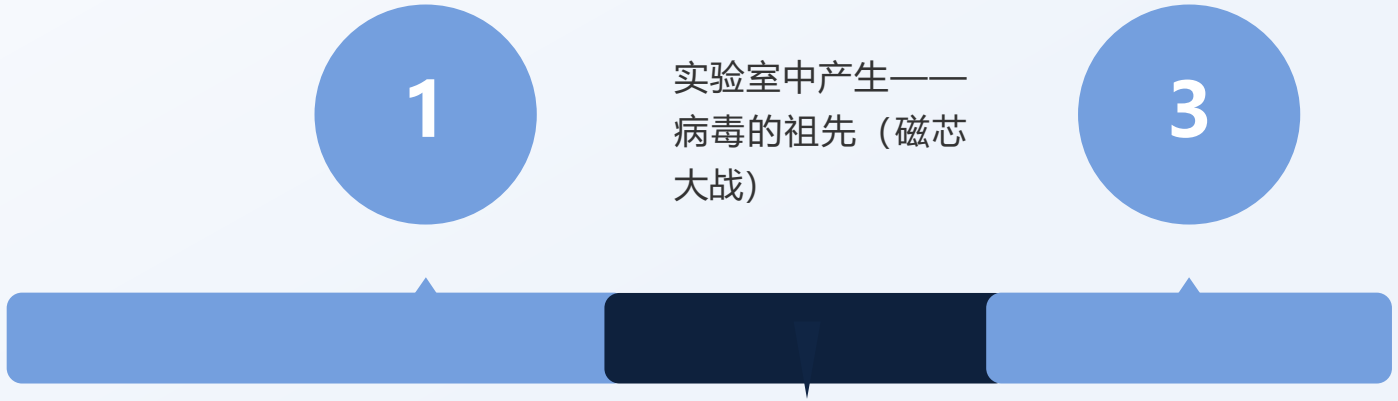
计算机病毒的基本概念

国家信息中心联合瑞星公司发布的《2019年中国网络安全报告》中，“云安全”系统共截获计算机病毒样本1.03亿个，计算机病毒感染次数4.38亿次，计算机病毒总体数量比2018年同期增加32.69%。报告显示,新增木马病毒6557万个,是第一大种类病毒,占到总体数量的63.46%;排名第二的为蠕虫病毒，数量为1560万个，占总体数量的15.10%，如图3-1所示。



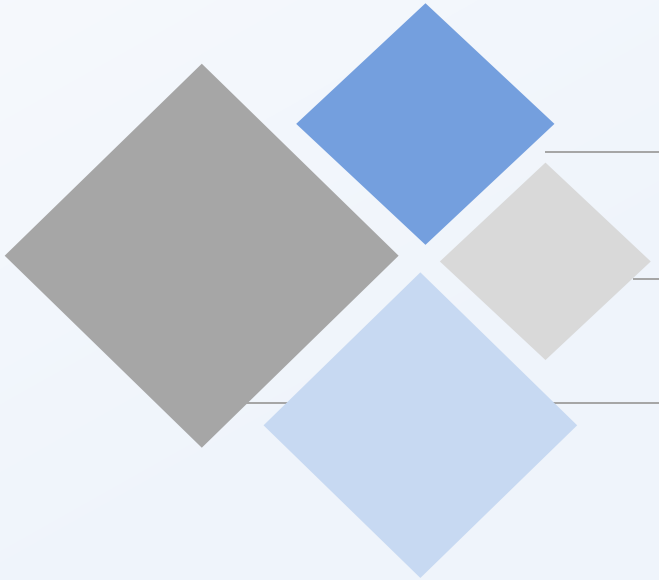
3.1 计算机病毒概述

02 OPTION 计算机病毒的发展史



3.1 计算机病毒概述

03 病毒的产生原因



编制人员出于一种炫耀和显示自己能力的目的

某些软件作者出于版权保护的目的而编制

出于某种报复目的或恶作剧而编写病毒

出于政治、战争的需要

3.1 计算机病毒概述

计算机病毒的发展历程

- DOS引导阶段
- DOS可执行阶段
- 伴随阶段
- 多形阶段
- 生成器、变体机阶段
- 网络、蠕虫阶段
- 视窗阶段
- 宏病毒阶段
- 邮件病毒阶段
- 移动设备病毒阶段

013.1 计算机病毒概述

时间（年）	名称	
1987	黑色星期五	病毒第一次大
1988	蠕虫病毒	罗伯特·莫里斯
1990	4096	第一个隐蔽型病毒
1991	米开朗基罗	第一个格式化硬盘的
1996	Nuclear	基于Microsoft Office
1998	CIH	第一个破坏硬件的病毒
1999	Mellisa、happy99	邮件病毒
2000	VBS.Timofonica	第一个手机病毒
2001	Nimda	集中了当时所有蠕虫传播途径，成为当
2003	冲击波	通过微软的RPC缓冲区溢出漏洞进行传播的
2006	熊猫烧香	破坏多种文件的蠕虫病毒
2008	磁碟机病毒	其破坏、自我保护和反杀毒软件能力均10倍于“熊猫烧香”
2014	苹果大盗病毒	爆发在“越狱”的iPhone手机上，目的是盗取Apple ID和密码
2017	WannaCry勒索病毒	至少150个国家的30万名用户中招，造成损失达80亿美元
2018	GandCrab勒索病毒	勒索病毒依然是2018年影响最大的病毒

3.2 计算机病毒分类

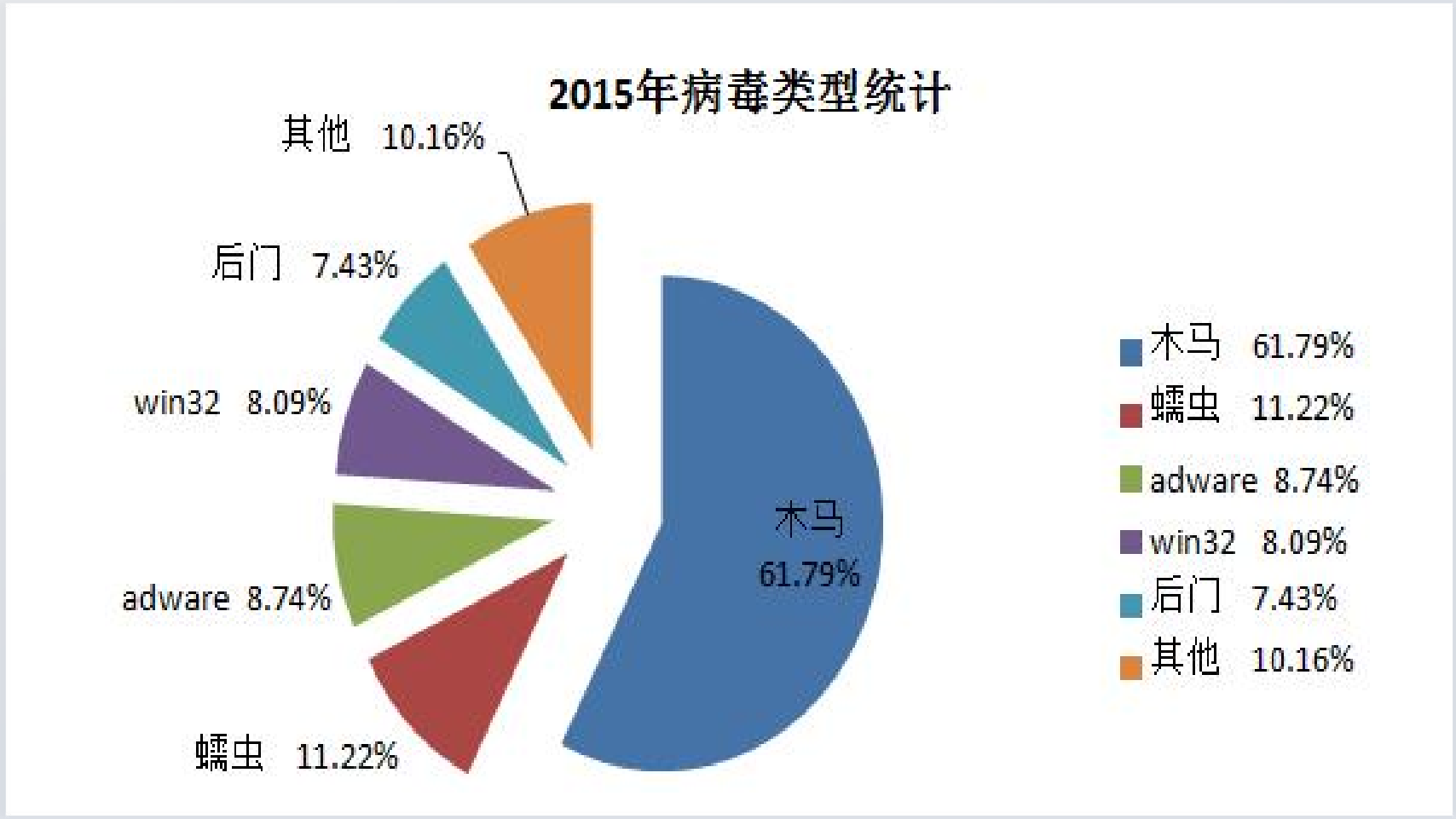
根据病毒的传染途径

根据病毒依附的操作系统

依据不同的分类标准，计算机病毒可以做不同的归类。常见的分类标准有：

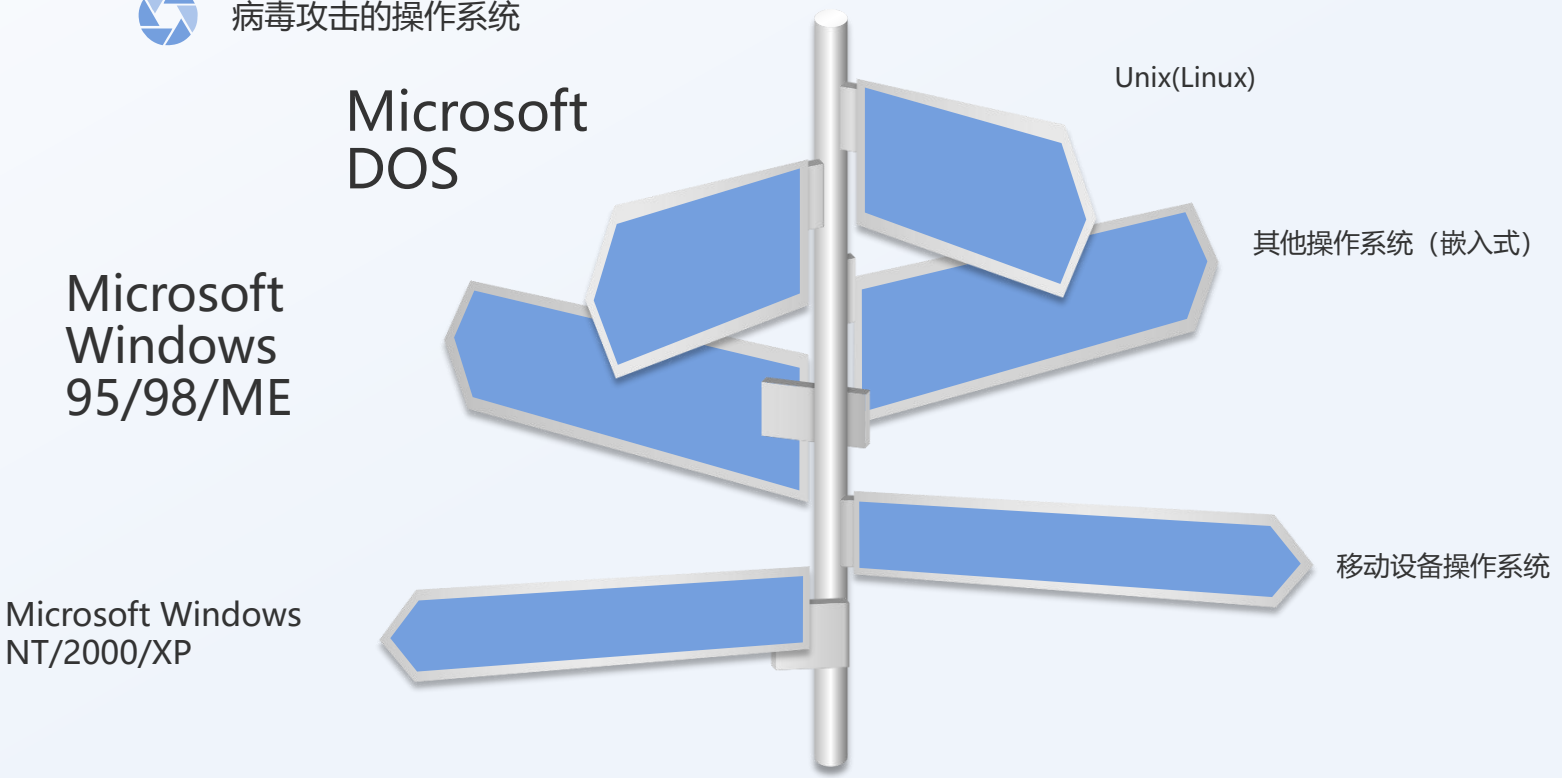
根据病毒的传播媒介

3.2 计算机病毒分类


2015年病毒类型统计
其他 10.16%
后门 7.43%
win32 8.09%
adware 8.74%
蠕虫 11.22%
木马 61.79%
木马 61.79%
蠕虫 11.22%
adware 8.74%
win32 8.09%
后门 7.43%
其他 10.16%

3.2 计算机病毒分类

病毒攻击的操作系统

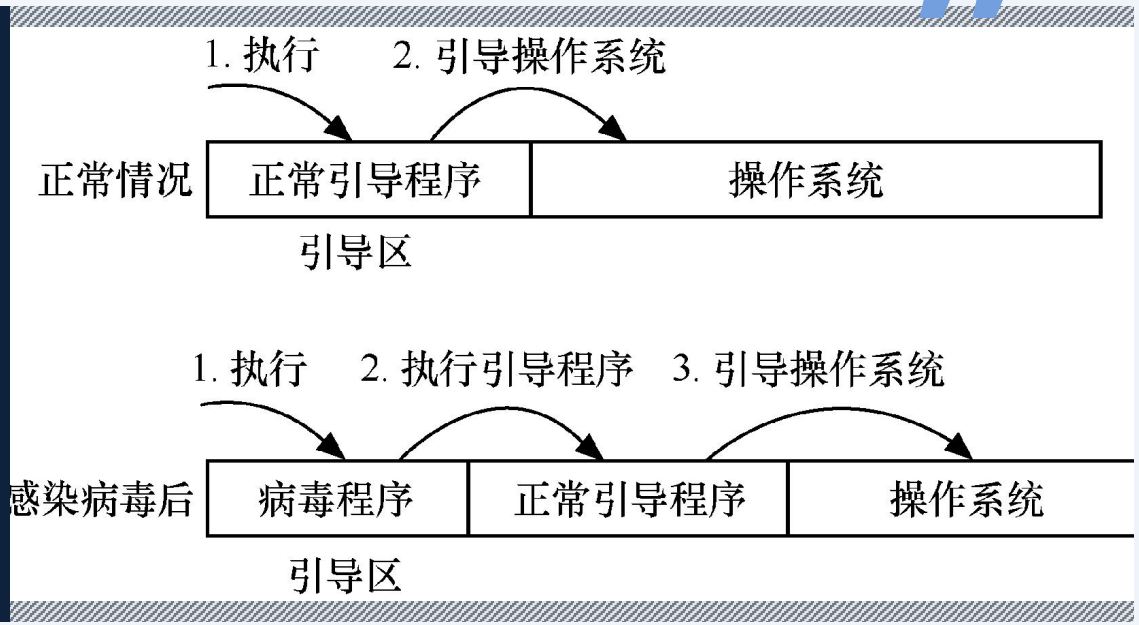


3.2 计算机病毒分类

按照计算机病毒的
宿主分类

3.2 计算机病毒分类

引导型病毒



3.2 计算机病毒分类

蠕虫病毒

蠕虫（Worm）病毒是自包含的程序（或是一套程序），能传播自身功能的副本或自身某些部分到其他的计算机系统中（通常是经过网络连接）。与一般计算机病毒不同，蠕虫病毒不需要将其自身附着到宿主程序中。

传统病毒与蠕虫病毒的比较

比较项目	病毒类型	
	传统病毒	蠕虫病毒
存在形式	寄存文件	独立存在
传染机制	宿主文件运行	主动攻击
传染目标	文件	网络

计算机病毒的分类

3.2.1 按照计算机病毒依附的操作系统分类

1、基于DOS操作系统的病毒

2、基于Windows操作系统的病毒

3、基于UNIX/Linux操作系统的病毒

4、基于嵌入式操作系统的病毒

3.2.2 按照计算机病毒的宿主分类

1、引导型病毒

2、文件型病毒

3、宏病毒

3.2.1 按照计算机病毒依附的操作系统分类

1、基于DOS操作系统的病毒

基于 DOS 操作系统的病毒是一种只能在DOS 环境下运行、传染的计算机病毒，是最早出现的计算机病毒。例如，“米开朗基罗”病毒、“黑色星期五”病毒等均属于此类病毒。
DOS 下的病毒一般又分为引导型病毒、文件型病毒、混合型病毒等。

2、基于Windows操作系统的病毒

目前，Windows 操作系统是市场占有率最高的操作系统，大部分病毒基于此操作系统， Windows 操作系统中即便是安全性最高的Windows10也存在漏洞，而且该漏洞已经被黑客利用，制作了能感染Windows10操作系统的“威金”病毒、盗号木马等。

3、基于UNIX/Linux操作系统的病毒

现在UNIX/Linux操作系统应用非常广泛，许多大型服务器均采用UNIX/Linux操作系统，或者基于UNIX/Linux开发的操作系统。例如，Solaris是Sun公司开发和发布的操作系统，是UNIX操作系统的一个重要分支，而2008年4月出现的“Turkey”新蠕虫专门攻击Solaris操作系统。

4、基于嵌入式操作系统的病毒

嵌入式操作系统是一种用途广泛的系统，过去主要应用于工业控制和国防系统领域。随着Internet技术的发展，以及嵌入式操作系统的微型化和专业化，嵌入式操作系统的应用越来越广泛，如应用到手机操作系统中。现在，Android、iOS是主要的手机操作系统。目前发现了多种手机病毒，手机病毒也是一种计算机程序，和其他计算机病毒(程序)一样具有传染性、破坏性。手机病毒可通过发送短信、彩信，发送电子邮件，浏览网站，下载铃声等方式进行传播。手机病毒可能会导致用户手机死机、关机、数据被破坏、向外发送垃圾邮件、拨打电话等，甚至会损毁SIM卡、芯片等硬件。

3.2.2 按照计算机病毒的宿主分类

1、引导型病毒

引导扇区是大部分系统启动或引导指令所保存的地方，对所有的磁盘来讲，不管是否可以引导，其都有一个引导扇区。引导型病毒感染的主要方式是通过已被感染的引导盘进行引导。

引导型病毒隐藏在ROM基本输入/输出系统(Basic Input/Output System，BIOS)之中，先于操作系统，依托的环境是BIOS 中断服务程序。引导型病毒利用操作系统的引导模块放在某个固定的位置，并且控制权的转交方式以物理地址为依据，而不是以操作系统引导区的内容为依据。因此，病毒占据该物理位置即可获得控制权，而对真正的引导区内容进行转移或替换，待病毒程序被执行后，将控制权交给真正的引导区内容，使这个带病毒的系统看似正常运转，病毒却已隐藏在系统中伺机传染、发作，如图3-2所示。

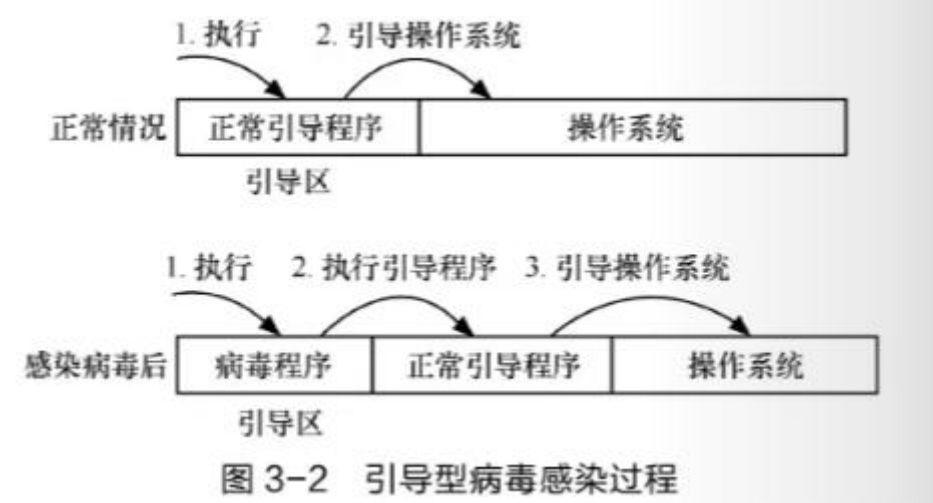


图 3-2　引导型病毒感染过程

引导型病毒按其所在的引导区不同又可分为两类，即MBR(主引导区)病毒、BR(引导区)病毒。MBR病毒寄生在硬盘分区主引导程序所占据的硬盘0头0柱面第1个扇区中，典型的病毒有“大麻(Stoned)”“2708”等;BR病毒寄生在硬盘逻辑0扇区或软盘逻辑0扇区(即0面0道第1个扇区)中，典型的病毒有“Brain”“小球”等。

引导型病毒几乎都会常驻在内存中，差别是在内存中的位置不同。所谓“常驻”，是指应用程序把要执行的部分在内存中驻留一份，这样就不必在每次要执行时都到硬盘中搜寻，可以提高效率。

引导区感染了病毒后，使用格式化程序可清除病毒;如果主引导区感染了病毒，则使用格式化程序是不能清除该病毒的，可以使用

2、文件型病毒

文件型病毒主要以可执行程序为宿主，一般感染文件扩展名为“.com”“.exe”“.bat”等的可执行程序。文件型病毒通常隐藏在宿主程序中，执行宿主程序时，将会先执行病毒程序再执行宿主程序，看起来并无异常。此后，病毒会驻留在内存中，伺机或直接传染其他文件。

文件型病毒的特点是附着于正常程序文件，成为程序文件的一个外壳或部件。文件型病毒的安装必须借助于病毒的载体程序，即要运行病毒的载体程序，才能引入内存。“CIH”就是典型的文件型病毒。根据文件型病毒寄生在文件中的方式不同，可以分为覆盖型文件病毒、依附型文件病毒、伴随型文件病毒，如图3-3所示。

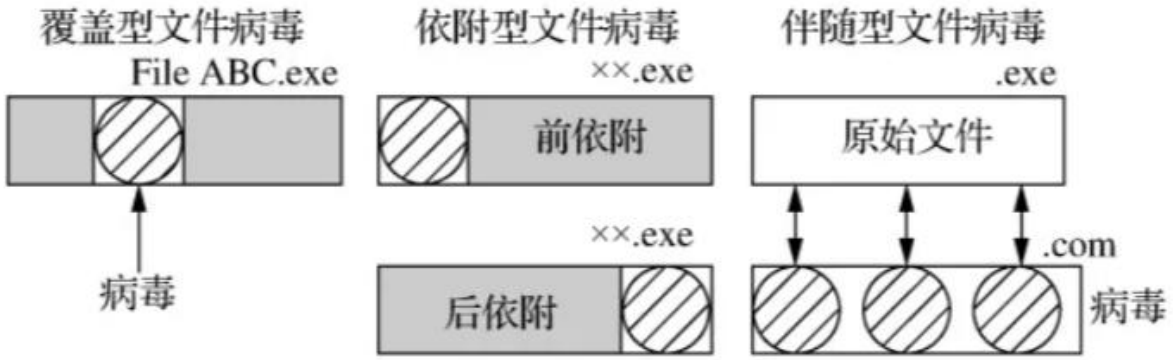


图 3-3　文件型病毒的分类

(1)覆盖型文件病毒:此类计算机病毒的特征是覆盖所感染文件中的数据。也就是说，一旦某个文件感染了此类计算机病毒，即使将带毒文件中的恶意代码清除，文件中被其覆盖的那部分内容也无法恢复。对于被覆盖的文件，只能将其彻底删除。

(2)依附型文件病毒:依附型文件病毒会把自己的代码复制到宿主文件的开头或结尾处，并不改变其攻击目标(即该病毒的宿主程序)，相当于给宿主程序加了一个“外壳”。此后，依附病毒常常会移动文件指针到文件末尾，写入病毒体，并将文件的前3字节修改为一个跳转语句(JMP/EB)，略过源文件代码而跳到病毒体。病毒体尾部保存了原文件前3字节的数据，于是病毒执行完毕之后会恢复数据并把控制权交回给原文件。

(3)伴随型文件病毒:伴随型文件病毒并不改变文件本身，而是根据算法产生EXE文件的伴随体，具有同样的名称和不同的扩展名。例如，xcopy.exe的伴随体是xcopy.com，其把自身写入 COM文件并不改变EXE文件，当DOS加载文件时，伴随体优先被执行，再由伴随体加载并执行原来的EXE 文件。

3、宏病毒

宏是Microsoft 公司为其Office软件包设计的一个特殊功能,是软件设计者为了让人们在使用软件进行工作时避免重复相同的动作而设计出来的一种工具。其利用简单的语法将常用的动作写成宏，在工作时，可以直接利用事先编好的宏自动运行，完成某项特定的任务，而不必再重复相同的动作，目的是让用户文档中的一些任务自动化。

宏病毒主要以Microsoft Office的“宏”为宿主，寄生在文档或模板的宏中。一旦打开这样的文档，其中的宏就会被执行，宏病毒就会被激活，并能通过DOC文档及DOT 模板进行自我复制及传播。