网络信息安全

第11讲 恶意代码及防护技术

杨 明

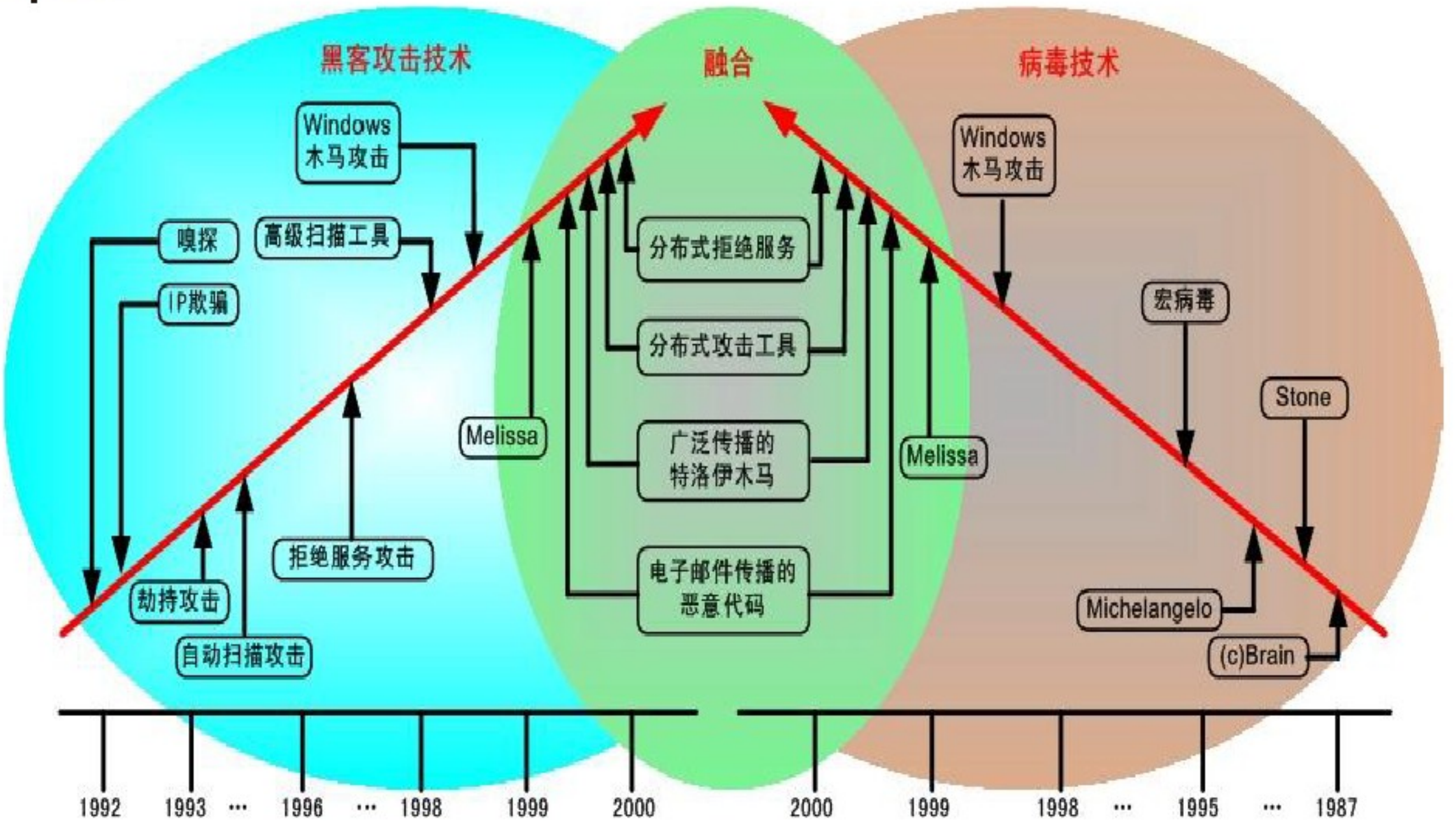
紫金学院计算机系

2016/3/5

内容

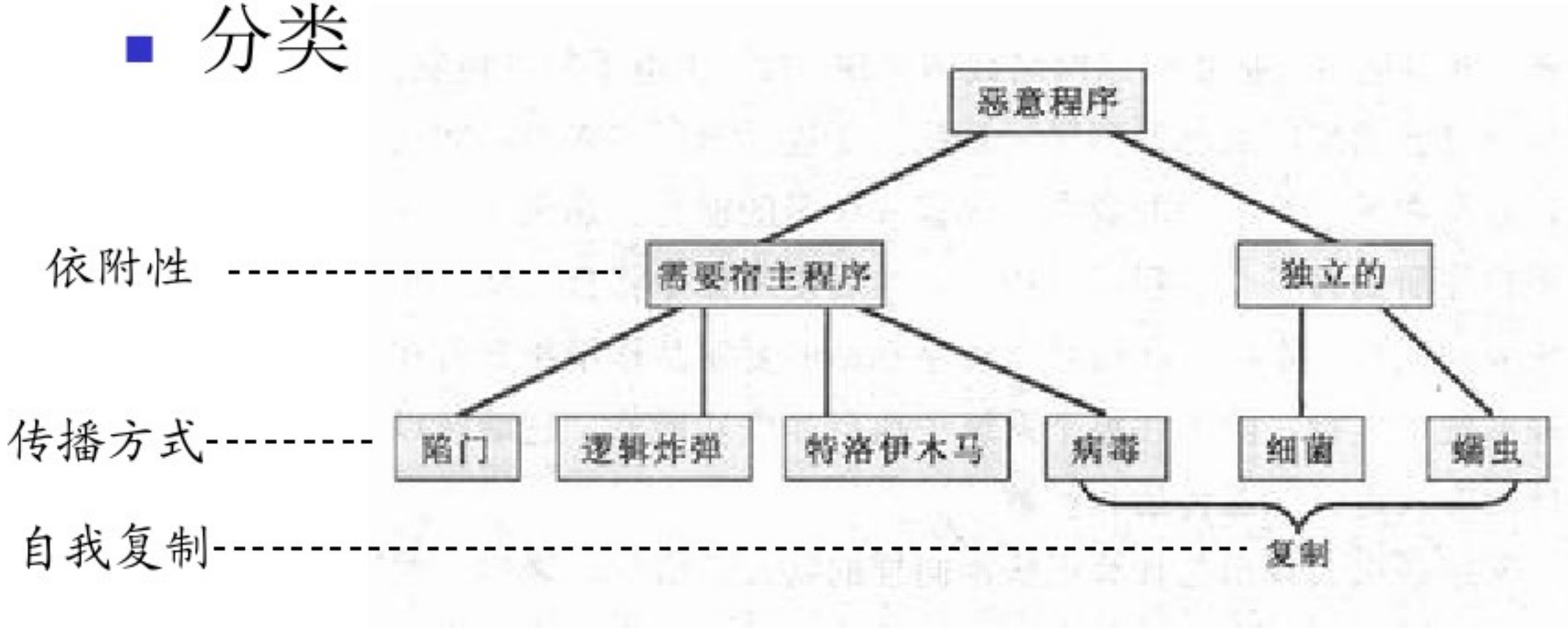
- 恶意代码的概念
- 计算机病毒
- 反病毒技术

网络攻击技术演变趋势图



恶意代码的概念

- 定义
  - 指以危害信息安全等不良意图为目的程序或代码
  - 潜伏在受害计算机系统中实施破坏或窃取信息
- 分类



恶意代码的主要功能

隐藏在主机上的所有活动

监视键盘

删除敏感信息

收集你的相关信息

窃取文件

诱骗访问恶意网站

开启后门（肉鸡）

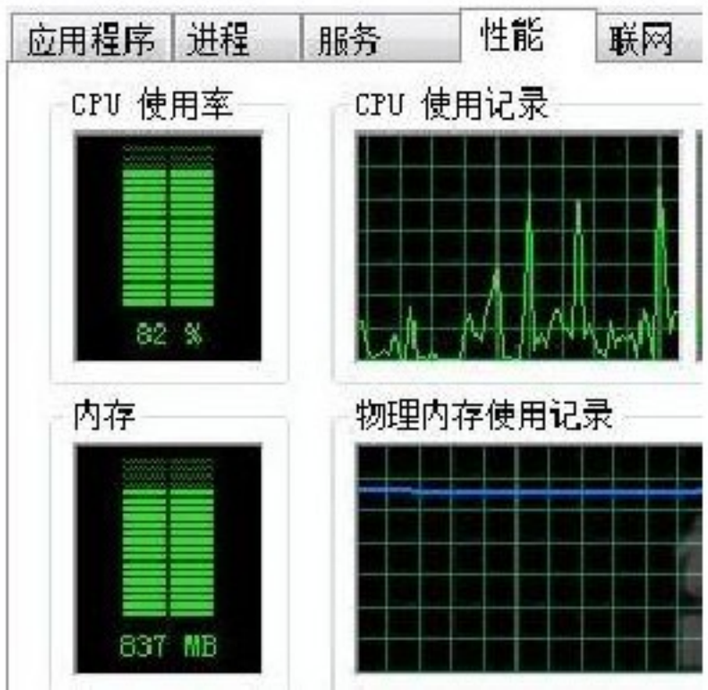
作为网络传播的起点

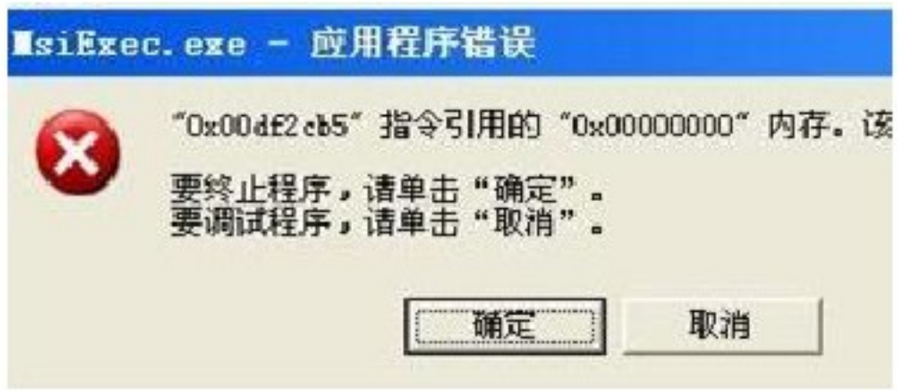
恶意代码的概念

恶意代码类型	主要特点		
计算机病毒	潜伏	传染	破坏
蠕虫	扫描	攻击	扩散
特洛伊木马	欺骗	隐藏	信息窃取
逻辑炸弹	潜伏	破坏	

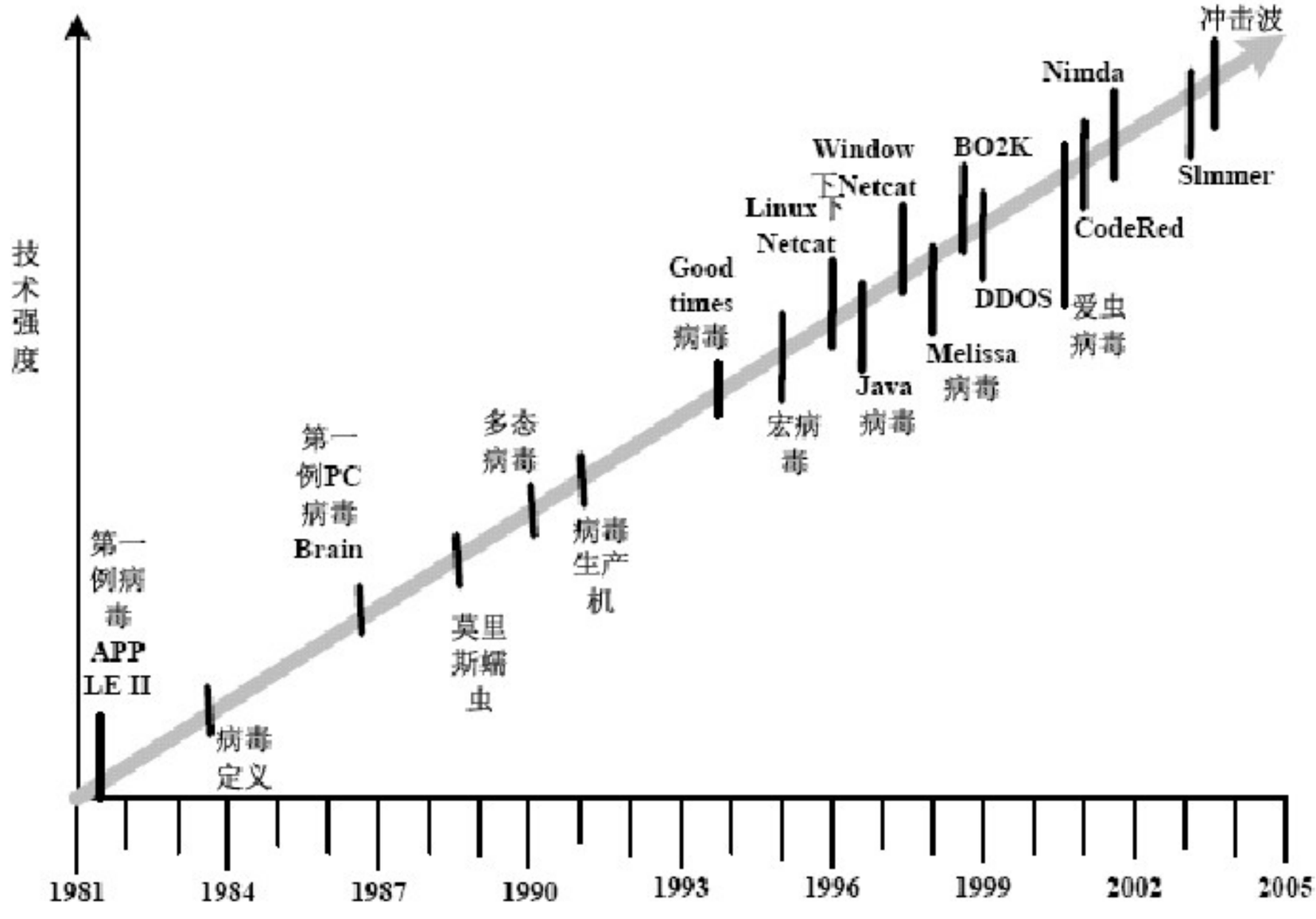
恶意代码的危害

- 攻击系统，造成系统瘫痪或操作异常；
- 危害数据文件的安全存储和使用；
- 泄露文件、配置或隐私信息；
- 肆意占用资源，影响系统或网络的性能；
- 攻击应用程序，如影响邮件的收发。





恶意代码的发展历史


技术强度
1981
1984
1987
1990
1993
1996
1999
2002
2005
第一例病毒APP LE II
病毒定义
第一例PC病毒Brain
莫里斯蠕虫
多态病毒
病毒生产机
Good times病毒
宏病毒
Linux下Netcat
Window下Netcat
Java病毒
BO2K
Melissa病毒
DDOS
Nimda
CodeRed
爱虫病毒
Slmmer
冲击波

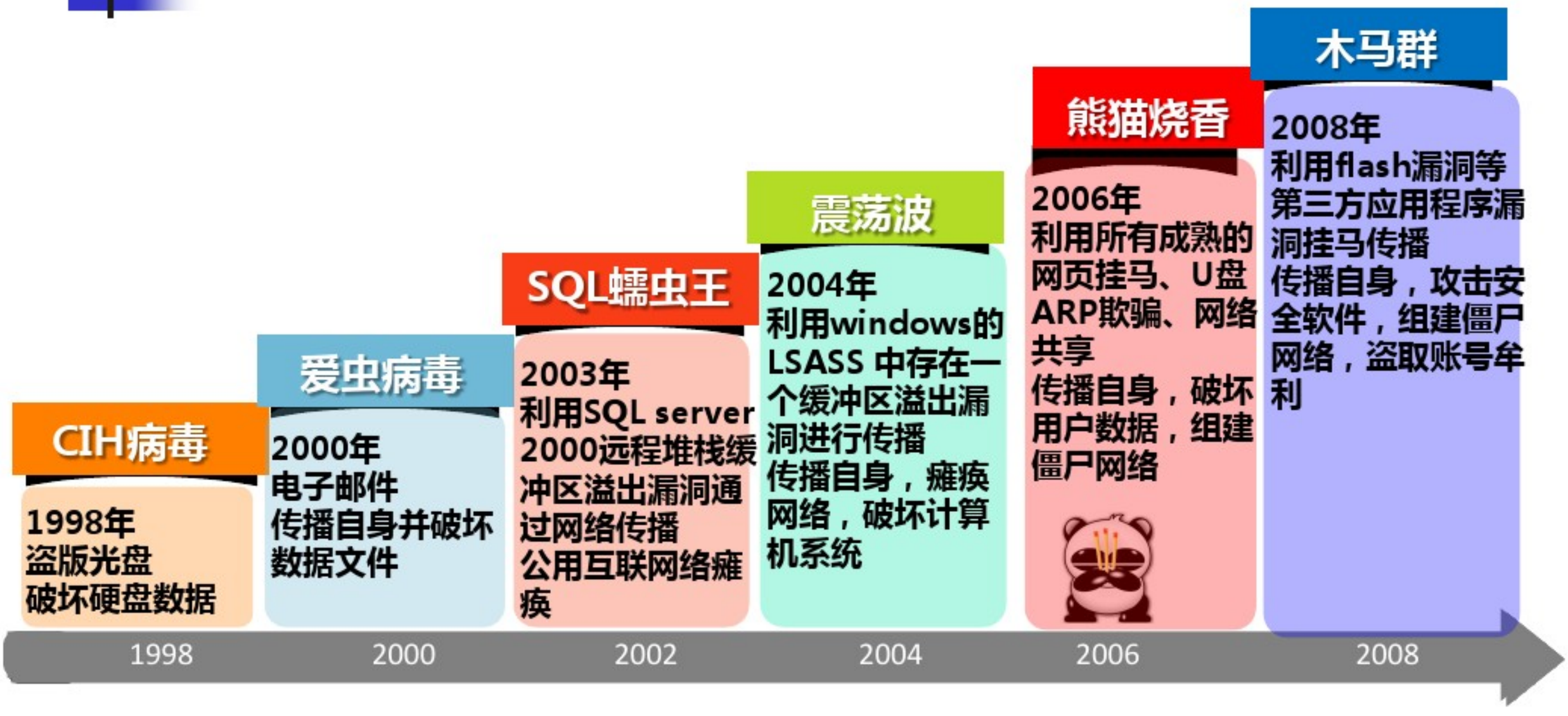
计算机病毒

- 定义
  - 计算机病毒能够寻找宿主对象，并且依附于宿主，是一类具有传染、隐蔽、破坏等能力的恶意代码。
- 产生的根源
  - 炫耀、玩笑、恶作剧或是报复
  - 各种矛盾激化、经济利益驱使
  - 计算机系统的复杂性和脆弱性
  - 网络战
    - “震网”病毒

计算机病毒的特征

- 主要特征
  - 宿主性：依附在另一个程序上
  - 隐蔽性：长期隐藏，条件触发
  - 传染性：自我复制，感染其他程序
  - 破坏性：执行恶意的破坏或恶作剧、消耗资源
  - 变异性：逃避反病毒程序的检查

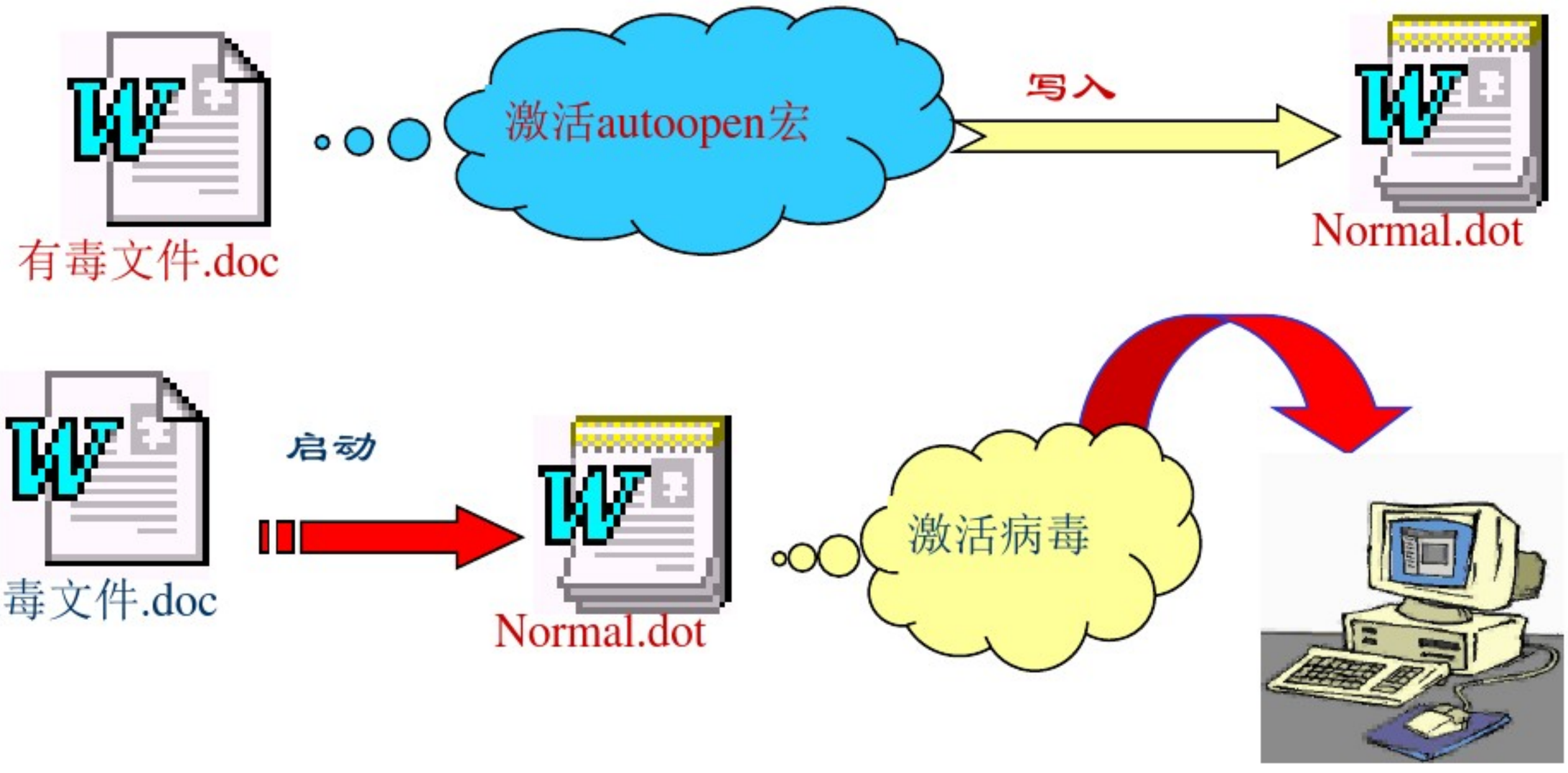
计算机病毒的发展简史


CIH病毒
1998年
盗版光盘
破坏硬盘数据
爱虫病毒
2000年
电子邮件
传播自身并破坏
数据文件
SQL蠕虫王
2003年
利用SQL server
2000远程堆栈缓
冲区溢出漏洞通
过网络传播
公用互联网络瘫
痪
震荡波
2004年
利用windows的
LSASS 中存在一
个缓冲区溢出漏
洞进行传播
传播自身，瘫痪
网络，破坏计算
机系统
熊猫烧香
2006年
利用所有成熟的
网页挂马、U盘
ARP欺骗、网络
共享
传播自身，破坏
用户数据，组建
僵尸网络
木马群
2008年
利用flash漏洞等
第三方应用程序漏
洞挂马传播
传播自身，攻击安
全软件，组建僵尸
网络，盗取账号牟
利
1998
2000
2002
2004
2006
2008

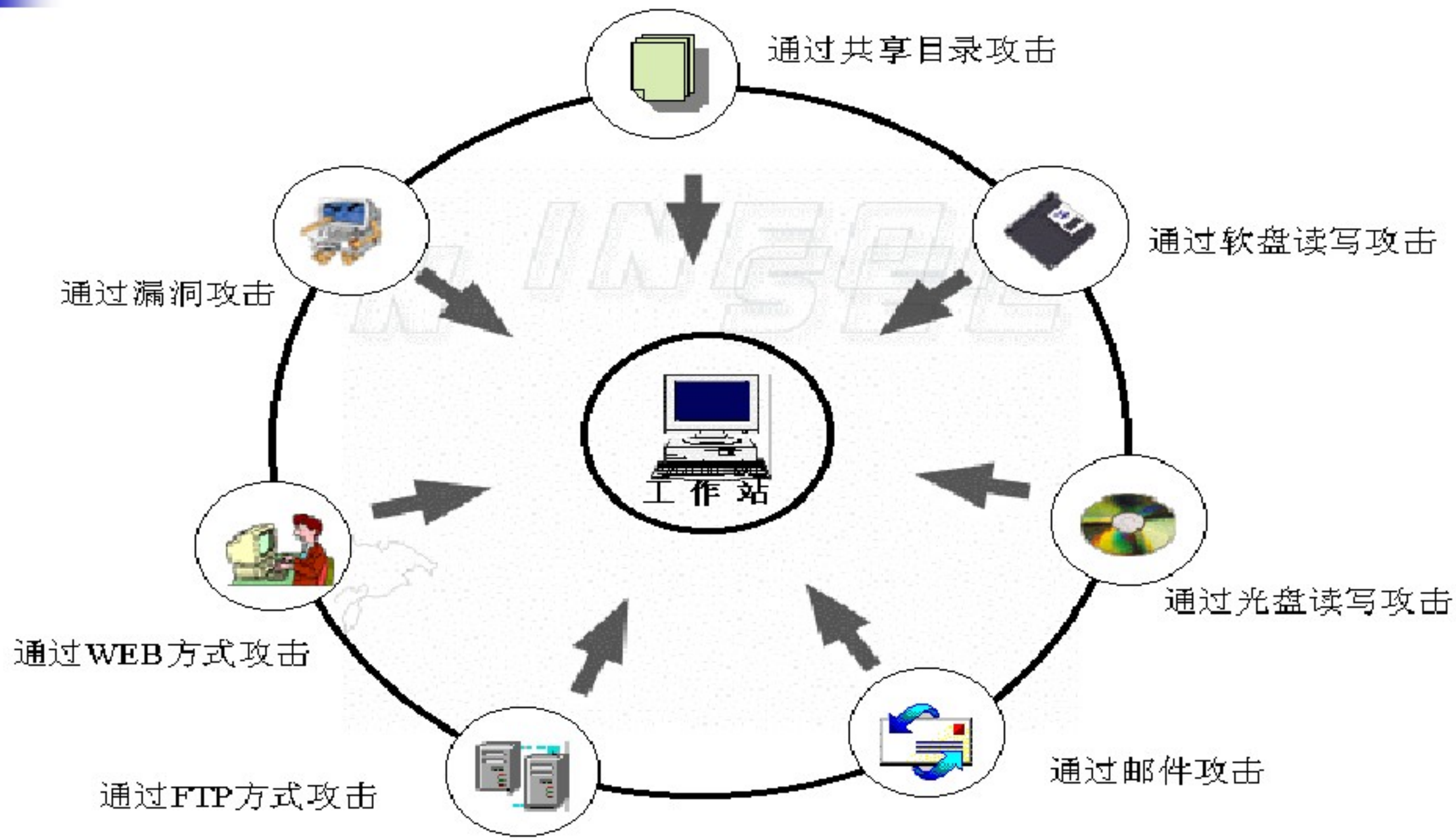
宏病毒

- 特点
  - 利用word中的“宏”繁殖传染
    - 宏是嵌入到字处理文档中的一段可执行程序
  - 宏病毒感染文档，而不是可执行代码
  - 宏病毒是平台无关的
  - 宏病毒容易传染
    - 电子邮件
  - 不同类型的宏
    - 自动执行：normal.dot，启动
    - 自动宏：打开/关闭文档、创建、退出
    - 宏命令

宏病毒的基本机制


有毒文件.doc
激活autoopen宏
写入
Normal.dot
无毒文件.doc
启动
Normal.dot
激活病毒

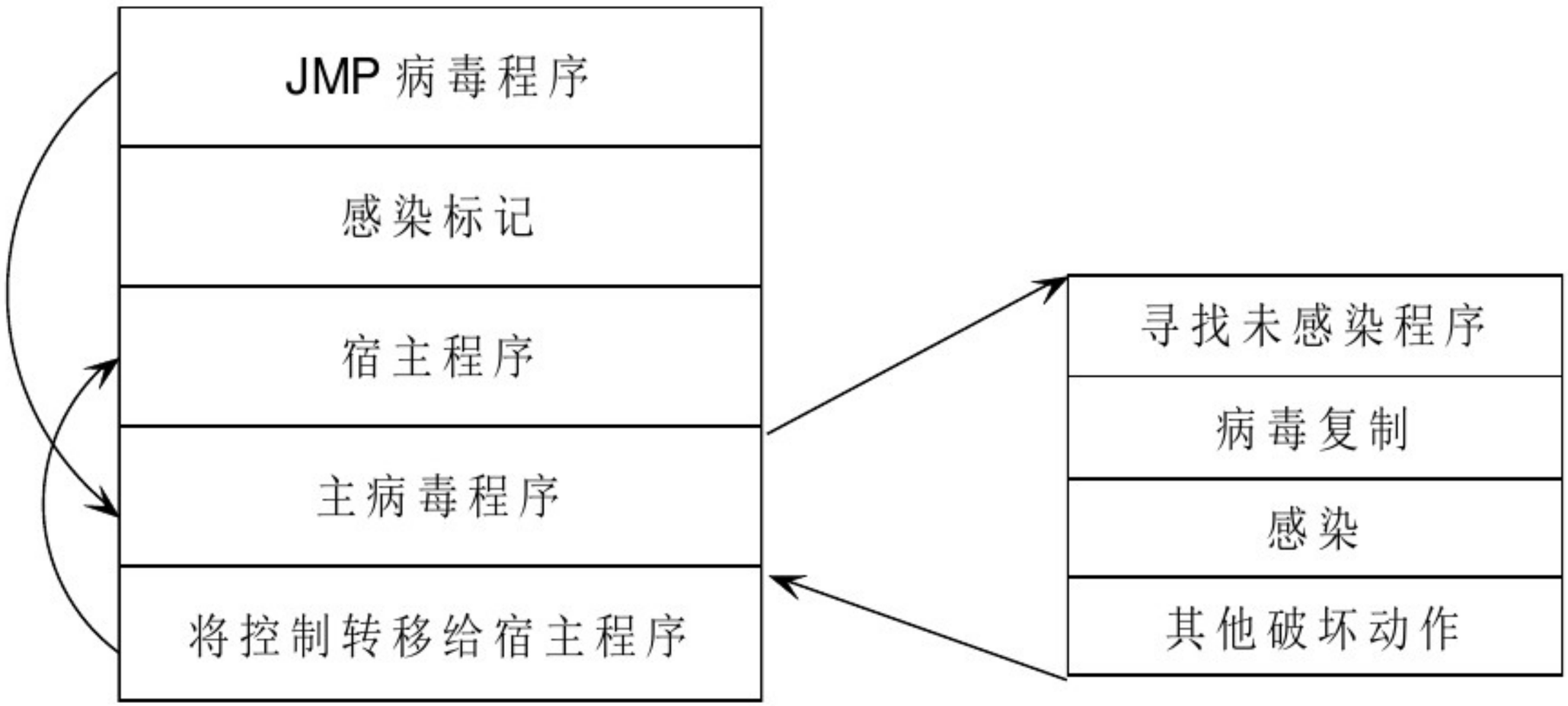
病毒的传播途径


通过共享目录攻击
通过软盘读写攻击
通过漏洞攻击
工作站
通过光盘读写攻击
通过WEB方式攻击
通过邮件攻击
通过FTP方式攻击

计算机病毒的工作原理

- 计算机病毒的结构
  - 引导模块
    - 设法获得被执行的机会，获取系统的控制权以引导其他模块进行工作。
  - 传染模块
    - 完成计算机病毒的繁殖和传播
  - 触发模块
    - 是毒破坏行动是否执行的决定者
  - 破坏模块
    - 具体负责破坏活动的执行

病毒的基本工作机制

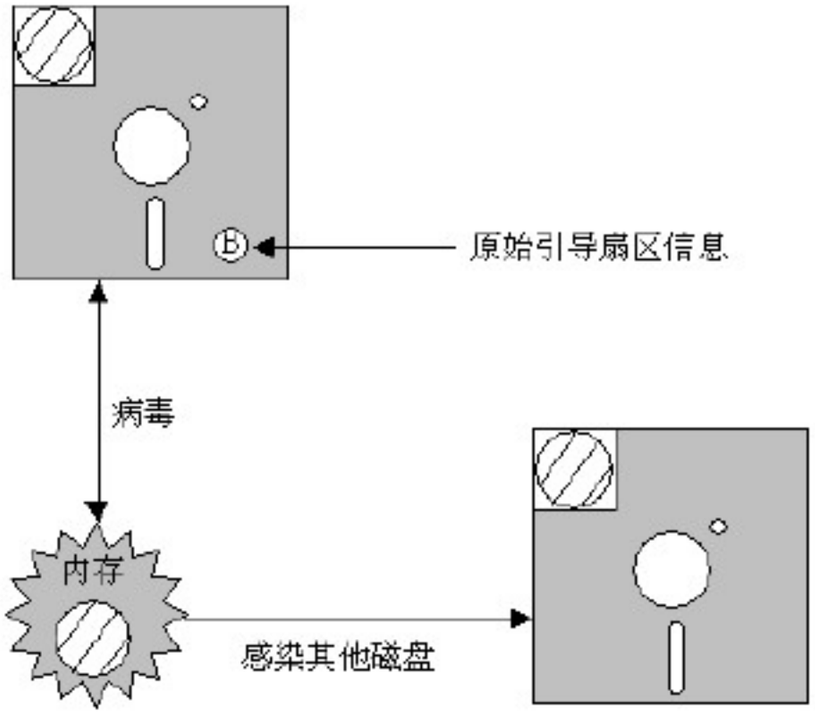

JMP 病毒程序
感染标记
宿主程序
主病毒程序
将控制转移给宿主程序
寻找未感染程序
病毒复制
感染
其他破坏动作
被感染程序执行

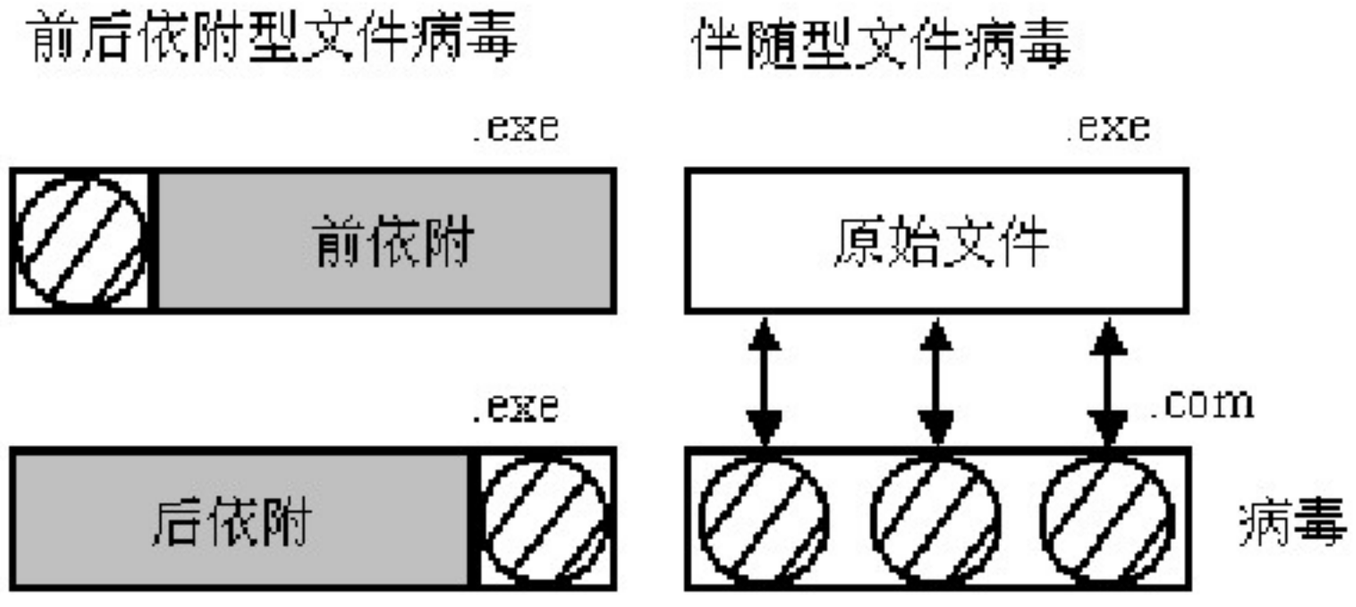
计算机病毒的引导机制

- 基本方法
  - 主动型（也称为隐蔽型或技术型）
  - 被动型（也称为公开型或欺骗型）
- 计算机病毒的引导过程
  - 驻留内存：病毒若要发挥其破坏作用，一般要驻留内存。有的病毒不驻留内存。
  - 窃取系统控制权：病毒驻留内存后，必须取代或扩充系统的原有功能，并窃取系统的控制权。
  - 隐蔽等待触发：此后病毒隐蔽自己，等待时机，在条件成熟时，再进行传染和破坏。

计算机病毒的寄生对象

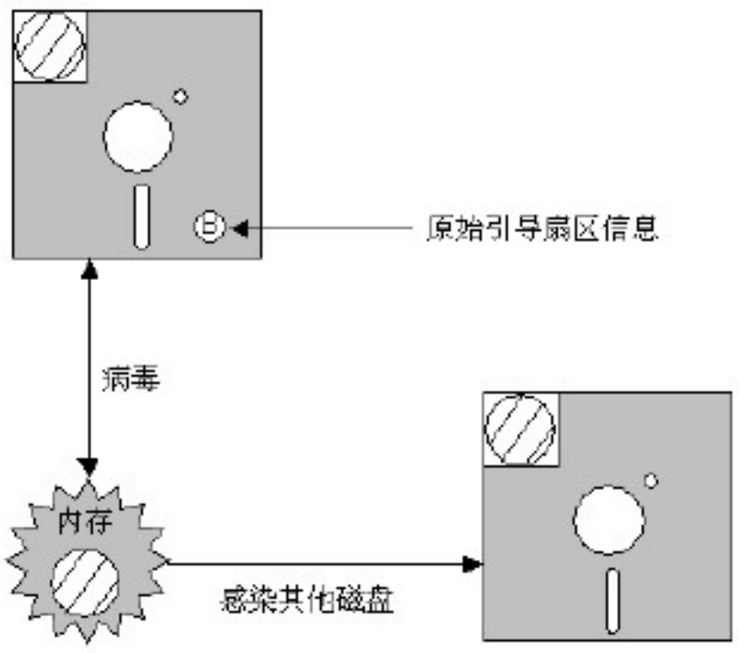
- 计算机病毒的寄生对象
  - 磁盘的引导扇区和特定文件（**EXE**、**COM**等可执行程序
  - **DLL**、**DOC**、**HTML**等经常使用的文件中

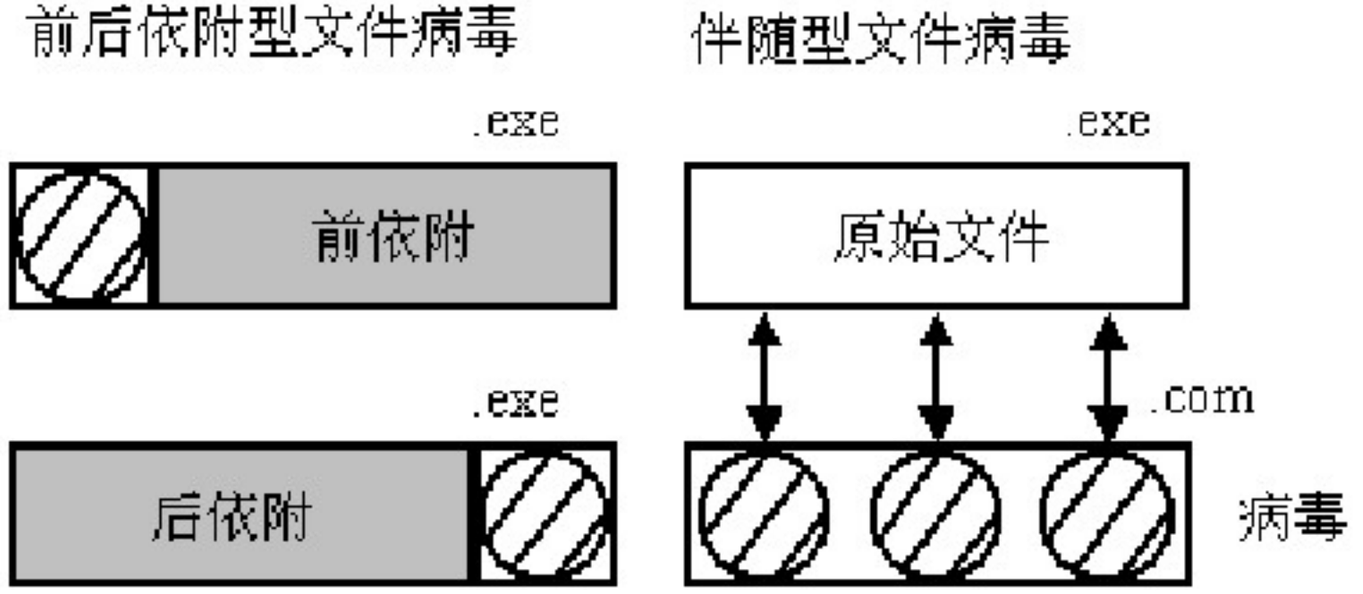




常用的寄生方式

- 替代法
  - 病毒程序用自己的部分或全部代码指令**直接替换**掉磁盘引导扇区或者文件中的原有内容。
- 链接法
  - 病毒程序将自身**插入**到原有内容的**首部**、**尾部**或者**中间**，和原有内容链接为一个整体。





病毒的活动过程

- 潜伏阶段
  - 病毒是空闲的
- 触发阶段
  - 病毒被某个事件激活
  - 包括日期、某个程序运行、中断调用、启动次数等
- 繁殖阶段
  - 复制病毒、传染其他程序
- 执行阶段
  - 执行某种有害或无害的功能
  - 盗窃、破坏数据信息、破坏硬件设备、耗费系统资源、产生视觉/听觉效果等

计算机病毒的过去与现在

目的	从炫技、恶作剧、仇视破坏到贪婪	→	依托互联网，集团化运作，以经济利益作为唯一目标 
技术	自我复制和传播，破坏电脑功能和数据，甚至破坏硬件，影响电脑正常使用	→	病毒技术本身没有突破，和以前的病毒没有本质区别
传播途径	通过磁盘、光盘、电子邮件、网络共享等方式传播 危害的表象：一个电脑病毒感染数千万台电脑，横行全球，破坏用户系统 (CIH、梅丽莎、冲击波、尼姆达等等)	→	生产、传播、破坏的流程完全互联网化，组成分工明确、日趋成熟的病毒产业链；各种基础互联网应用都成为病毒入侵通道，其中“网页挂马”最常见，占总量90%以上。

计算机病毒的防护

- 病毒的预防
- 病毒的检测
- 病毒的清除

病毒的防范

- 病毒的防范
  - 预防为主、治疗为辅
- 防范措施
  - 安装真正有效的防杀计算机病毒软件
  - 不要随便直接运行或直接打开电子函件中夹带的附件文件
  - 安装网络服务器时应保证没有计算机病毒存在
  - 一定要用硬盘启动网络服务器

病毒的防范

- 注意病毒传入途径
  - 终端漏洞导致病毒传播
  - 邮件接收导致病毒传播
  - 外部带有病毒的介质直接接入网络导致病毒传播
  - 内部用户绕过边界防护措施，直接接入因特网导致病毒被引入
  - 网页中的恶意代码传入

反病毒技术

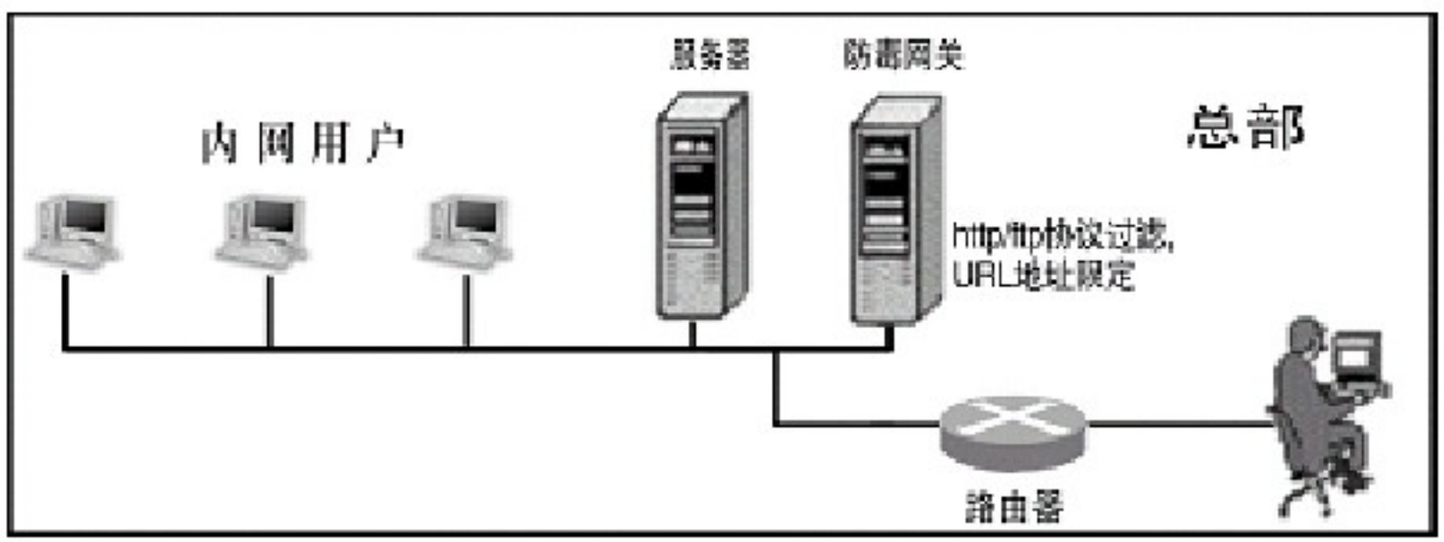
- 特征扫描的方法
  - 根据提取的病毒特征，查找计算机中是否有文件存在相同的感染特征。
- 内存扫描程序
  - 尽管病毒可以毫无觉察的把自己隐藏在程序和文件中，但病毒不能在内存中隐藏自己。
  - 内存扫描程序可以直接搜索内存，查找病毒代码。
- 完整性检查器
  - 记录计算机在未感染状态可执行文件和引导记录的信息指纹，将这一信息存放在硬盘的数据库中，并根据需要进行匹配测试，判断文件是否被病毒感染。

反病毒技术

- 行为监视器
  - 行为监视器又叫行为监视程序，它是内存驻留程序，这种程序静静地在后台工作，等待病毒或其他有恶意的损害活动。
  - 如果行为监视程序检测到这类活动，它就会通知用户，并且让用户决定这一类活动是否继续。
- CPU仿真器或虚拟机
  - 一个可执行文件中的指令先由仿真器来解释，而不是直接由底层的处理器解释。
  - 使用虚拟机技术，是目前较为前沿的一种反病毒技术。
  - 以程序在执行过程是否具有感染行为作为依据来判断该程序是否是病毒，查毒准确率几乎可达100％。

防病毒软件

- 防病毒软件
  - 瑞星、 360安全卫士 、趋势、卡巴斯基、MCAFEE、SYMANTEC、江民科技、金山
- 防病毒网关
  - 保护网络入口的防病毒网关
  - 保护邮件器的防病毒网关



反病毒产品发展

5 2008年以后，出现基于云计算的云杀毒服务

4 2003年左右，出现具备防毒功能的硬件网关设备

3 2000年前后，出现集中控制分布处理的网络杀毒软件

2 90s中杀防集成化，90s末出现实时防毒的反病毒软件

1 80s末—90s初，病毒数量激增，硬件防病毒卡出现

小结

- 恶意代码的概念
  - 定义和分类
- 计算机病毒
  - 定义与特征
  - 结构与工作原理
- 反病毒技术
  - 病毒的检测
  - 反病毒软件