计算机病毒

- 链接方式分类
  - 源码型
  - 嵌入型
  - 外壳型
  - 操作系统型
- 传播途径
  - 电子邮件
  - 外部介质
  - 复制
  - 下载
  - 浏览网页
- 交叉感染
  - 多个病毒感染同一个文件
- 与病毒类似的软件故障
  - 某些软件无法运行
  - 网络连接数过多导致无法上网
  - 防火墙配置不当导致无法上网
- 组成模块
  - 感染模块
    - 寻找一个可执行文件
    - 检测该文件是否有感染标记
    - 如果没有，进行感染，将代码放入宿主程序
  - 触发模块
    - 检查预定触发条件是否满足
    - 如果满足返回真值
    - 不满足返回假
  - 破坏模块
  - 主控模块
    - 调用感染模式，进行感染
    - 调用触发模块，接受返回值
    - 真，执行破坏模块
    - 否，执行后续程序
- 破坏性
  - 破坏系统数据
  - 破坏目录文件
  - 修改内存
  - 干扰系统运行
  - 效率降低
  - 破坏显示
  - 干扰键盘操作
  - 制造噪音
  - 修改CMOS参数
  - 影响打印机
- 一种程序
  - 他用修改其他程序的方法将自己的精确拷贝或者可能深化的形式放入其他程序中
- 新动向
  - 变种繁多，烟花目趋完善
  - 混合通用性病毒
  - 隐藏性病毒
  - 多态型病毒
  - 病毒的自动化生产
- 异常状况
  - 运行速度降低
  - 容易死机
  - 文件改变
  - 磁盘可用空间减少
  - 系统参数被修改
  - 文件被破坏
  - 频繁产生错误信息
  - 系统异常频繁重启
  - Office宏病毒提示
- 寄生感染
  - 放入宿主程序的头部、中部或者尾部
  - 插入感染
    - 拦腰斩断宿主，病毒插入宿主程序中部
  - 反插入感染
    - 把宿主程序放在病毒中部。
  - 没有入口点的感染
    - 修改跳转指令，使跳转到病毒
  - 零长度感染
    - 将恶意代码放入空洞中，不修改宿主的文件大小
    - 空洞是指只够长度全部为零的程序数据区或堆栈区
- 典型的计算机病毒
  - DOS病毒
    - 引导型病毒传播机制
      - 感染磁盘引导扇区和硬盘主引导扇区的计算机病毒程序
        - 1. 将系统正常的引导信息，转移到空闲位置保存起来，用病毒替换正常的。这样就可以先运行病毒再运行引导
        - 2. 将自身代码写入引导扇区
    - 文件型病毒传播机制
      - 利用系统上的文件进行传染
  - WIN32 PE病毒
    - 隐藏技术
      - 反跟踪技术
      - 避开修改中断向量
      - 请求在内存中的合法身份
      - 维持宿舍程序的外部特征
      - 不适用明显的感染标志
    - 花指令
      - 加入一些没有意义的代码
    - 简单加密
      - 对主体代码采用固定的秘钥进行加密
      - 通常采用 XOR OR SUB ADD
    - 多态
      - 多态引擎组成
        - 指令位置变化模块
        - 寄存器变换模块
        - 指令扩展模块
        - 指令收缩模块
        - 等价指令替换模块
        - 无用指令随机插入
        - 垃圾指令插入
    - 代码的优化
      - 所占空间优化
      - 运行时间优化
    - 线程技术
      - 远程线程，远程开启一个线程去运行病毒
    - 进程/线程之间的相互保护
      - 只要进程不被终结，线程会一直存在
  - 宏病毒
    - 二进制
    - 汇编语言写的
  - 脚本病毒
    - 编写简单
    - 破坏力大
    - 感染力强，病毒变种多
  - HTML病毒
    - ActiveX
    - 修改注册表
    - 拒绝服务供给
    - 破坏系统
    - 窃取硬盘文件
    - 非法下载文件到用户计算机上
    - 设置硬盘共享
  - 蠕虫
    - 主动传染性
    - 功能模型
      - 基本功能模块
        - 搜索模块
        - 攻击模块
        - 传输模块
        - 信息搜索模块
        - 繁殖模块
      - 扩展功能模块
        - 通信模块
        - 隐藏模块
        - 破坏模块
        - 控制模块
    - 工作流程
      - 随机生成IP地址
      - 探测地址
        - 主机是否存在
        - 漏洞是否存在
          - 攻击、传染和处理
    - 行为特征
      - 自我繁殖
      - 利用软件漏洞
      - 造成网络拥塞
      - 消耗系统资源
      - 留下安全隐患
- 手机病毒
  - 特性
    - 传染性
    - 破坏性
    - 寄生性
    - 隐藏性
    - 程序性
    - 潜伏性
    - 可触发性
    - 衍生性
    - 欺骗性
    - 不可预见性
- 感染目标
  - 主引导扇区
  - 硬盘BOOT扇区
  - 软盘BOOT扇区
  - EXE文件
  - COM文件
  - COMMAND文件
  - IBMBIOS文件、IBMDOS文件
  - eml、doc、dot、bvs、bat、pl、html、flash、dll、sys、asp等
- 机制
  - 传播机制
  - 触发机制
  - 破坏机制
- 破坏情况分类
  - 良性病毒
  - 恶性病毒
- 特征
  - 隐藏性
  - 传染性
  - 潜伏性
  - 破坏性
- 按攻击目标分类
  - 攻击微型计算机病毒
  - 攻击小型计算机病毒
  - 攻击工作站的病毒
- 宿主程序
  - 操作系统
  - 应用程序
- 与病毒类似的硬件故障
  - 系统的硬件配置
    - 软件无法运行
  - 电源电压不稳定
    - 磁盘文件丢失
  - 插件接触不良
    - 设备时好时坏
  - 软驱故障
    - 读坏磁盘
- 防病毒软件分类
  - 病毒扫描软件
  - 完整性检查软件
  - 行为封锁软件
- 生命周期
  - 感染
    - 自我复制传播给目标系统
  - 潜伏
    - 逃避用户和防病毒软件的监视而隐藏自身行踪的行为
  - 繁殖
    - 不断潜入当前主机的其他程序，进行传播，每个被感染的程序成为新的病毒源
  - 发作
    - 实施各种破坏行为
- 寄生方式和传播途径分类
  - 引导型
  - 文件型
  - 混合型
- 病毒之最
  - 最具杀伤力的病毒
    - CIH
  - 最浪漫
    - I LOVE U
  - 最漂亮
    - 图片病毒
  - 最虔诚
    - 熊猫烧香
  - 最烦人
    - 即时在线聊天病毒
  - 最佳创意
    - AV终结者
  - 最流氓
    - 灰鸽子
  - 最坚强
    - 网页病毒
  - 最牛
    - 未来
- 广义上的病毒
  - 一切恶意程序的统称
- 按平台分类
  - 攻击DOS系统的病毒
  - 攻击Windows系统的病毒
  - 攻击Unix系统的病毒
  - 攻击OS/2系统的病毒
  - 其他操作系统
    - 手机病毒等
- 命名
  - 病毒名前缀.病毒名.病毒后缀
    - 前缀指病毒的分类
    - 后缀指病毒的变种特征
- 入侵的方式
  - 替代方式
  - 链接方式
- 触发机制
  - 日期和时间触发
  - 键盘触发
  - 感染触发
  - 启动触发
  - 磁盘访问触发中断访问触发
  - 其他机制出触发
- 防御基本策略
  - 安装至少一种防病毒软件
  - 定期升级你的防病毒软件
  - 不要随便打开邮件附件
  - 尽量减少授权使用你计算机的人呢
  - 及时为计算机安装最新的安全补丁
  - 从外部获取数据前先检查
  - 安装完整性检查软件
  - 定期备份你的文件
  - 建立一个系统恢复盘
- 传播媒介分类
  - 单机病毒
  - 网络病毒