蠕虫病毒

6.1 蠕虫的基本概念

- 1988年
  - 美国CORNELL大学研究生莫里斯编写的蠕虫病毒蔓延造成了数千台计算机停机，蠕虫病毒开始现身网络
- 后来的红色代码，尼姆达病毒的疯狂
  - 造成几十亿美元的损失
- 2003年1月26日，“2003蠕虫王”
  - 迅速传播并袭击了全球，致使互联网网路严重堵塞
  - 作为互联网主要基础的域名服务器（DNS）的瘫痪造成网民浏览互联网网页及收发电子邮件的速度大幅减缓
  - 银行自动提款机的运作中断，机票等网络预订系统的运作中断，信用卡等收付款系统出现故障
  - 造成的直接经济损失至少在12亿美元以上

Morris

- 90行程序代码
- 2小时：
  - 6000台电脑（互联网的十分之一）瘫痪
  - 1500万美元的损失
  - 3年缓刑/1万罚金/400小时的社区义务劳动
- 病毒的萌芽：

  没有企图用蠕虫去破坏数据或文件，但他企图让蠕虫广泛传播

6.1 蠕虫的基本概念

蠕虫病毒造成的损失

病毒名称	持续时间	造成损失
莫里斯蠕虫	1988年	6000多台计算机停机，直接经济损失达9600万美元!
美丽杀手	1999年	政府部门和一些大公司紧急关闭了网络服务器，经济损失超过12亿美元!
爱虫病毒	2000年5月至今	众多用户电脑被感染，损失超过100亿美元以上
红色代码	2001年7月	网络瘫痪，直接经济损失超过26亿美元
求职信	2001年12月至今	大量病毒邮件堵塞服务器，损失达数百亿美元
Sq蠕虫王	2003年1月	网络大面积瘫痪，银行自动提款机运做中断，直接经济损失超过26亿美元

6.1 蠕虫的基本概念

- 1982年，Shock和Hupp
  - 根据《The Shockwave Rider》一书中的概念提出了一种“蠕虫Worm”程序的思想
- 蠕虫病毒是一种常见的计算机病毒
- 利用网络进行复制和传播
  - 传播通常不需要所谓的激活
  - 通过分布式网络来散播特定的信息或错误，进而造成网络服务遭到拒绝并发生死锁
    - 通过网络
    - 电子邮件

6.1 蠕虫的基本概念

- 蠕虫是一种通过网络传播的恶性病毒
  - 具有病毒的共性
    - 传播性、隐蔽性和破坏性等
  - 自己特有的特性
    - 不利用文件寄生（有的只存在于内存中），对网络造成拒绝服务，以及和黑客技术相结合等
- 在破坏程度上高于普通病毒
  - 在短短数小时内蔓延至整个因特网，并造成网络瘫痪

6.1 蠕虫的基本概念

- 根据攻击对象不同
  - 面向企业用户和局域网
    - 利用系统漏洞，主动进行攻击，可以使整个因特网瘫痪
    - “红色代码”、“尼姆达”、“SQL蠕虫王”
    - 具有很大的主动攻击性，爆发也具有一定的突然性
    - 相对来说查杀较容易
  - 针对个人用户
    - 通过网络（主要是电子邮件、恶意网页）迅速传播
    - “爱虫”、“求职信”
    - 传播方式比较复杂和多样，少数利用了微软的应用程序的漏洞，更多的利用社会工程学对用户进行欺骗和诱使
    - 造成的损失非常大，同时很难根除

6.2 蠕虫和其他病毒的关系

- 不采取利用PE格式插入文件的方法
  - 蠕虫复制自身并在因特网中进行传播
- 普通病毒的传染主要针对计算机内的文件系统
  - 蠕虫传染目标是因特网内所有计算机
    - 局域网条件下的共享文件夹、电子邮件、网络中的恶意网页、大量存在着漏洞的服务器

蠕虫病毒和普通病毒的区别

比较项目	普通病毒	蠕虫病毒
存在形式	寄存文件	独立程序
传染机制	宿主程序文件	主动攻击
传染目标	本地文件	网络计算机

6.2 蠕虫和其他病毒的关系

- 蠕虫与木马
  - 共性
    - 自我传播，不感染其他文件
  - 传播特性上有微小差别
    - 木马需要用户上当受骗来进行传播
    - 蠕虫包含自我复制程序，利用所在系统进行传播
  - 破坏目的不同
    - 蠕虫的破坏目的是纯粹的破坏
      耗费网络资源、删除用户数据
    - 木马的破坏目的是窃取用户的信息

6.3 蠕虫病毒的特性

- 蠕虫病毒具有自我复制能力
- 蠕虫病毒具有很强的传播性
- 蠕虫病毒具有一定的潜伏性
- 蠕虫病毒具有特定的触发性
- 蠕虫病毒具有很大的破坏性

6.3 蠕虫病毒的特性

■ 蠕虫病毒的特点

- **传染方式多**
  - 蠕虫入侵网络的主要途径是通过工作站传播到服务器硬盘中，再由服务器的共享目录传播到其他的工作站
  - 但蠕虫病毒的传染方式比较复杂
- **传播速度快**
  - 在单机上，病毒只能通过软盘从一台计算机传染到另一台计算机
  - 在网络中则可以通过网络通信机制，借助高速电缆进行迅速扩散

6.3 蠕虫病毒的特性

蠕虫病毒的特点

- **清除难度大**
  - 单机病毒可通过删除带毒文件、低级格式化硬盘等措施清除
  - 而网络中只要有一台工作站未能杀毒干净就可能使整个网络重新全部被病毒感染，甚至刚刚完成杀毒工作的一台工作站马上就能被网上另一台工作站的带毒程序所传染
  - 仅对工作站进行病毒杀除不能彻底解决网络蠕虫病毒的问题
- **破坏性强**
  - 网络中蠕虫病毒将直接影响网络的工作状态
  - 轻则降低速度，影响工作效率
  - 重则造成网络系统的瘫痪，破坏服务器系统资源，使多年的工作毁于一旦