

专业特色选修课《网络信息安全》



计算机病毒和防病毒技术

Computer Viruses and Anti-Viruses

嵩 天

songtian@bit.edu.cn

北京理工大学计算机学院

本节大纲

- 计算机病毒概述
- 计算机病毒的种类
- 计算机病毒的原理
- 计算机病毒的防范
- 一些计算机病毒案例
- 本节总结

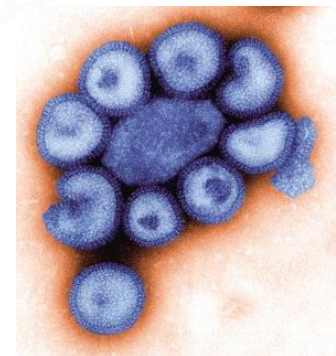
本节大纲

- 计算机病毒概述
- 计算机病毒的种类
- 计算机病毒的原理
- 计算机病毒的防范
- 一些计算机病毒案例
- 本节总结

计算机病毒的定义

- 病毒的定义

- 病毒是一种具有细胞感染性的亚显微粒子，可以利用宿主的细胞系统进行自我复制，但无法独立生长和复制
- 第一个已知的病毒是烟草花叶病毒，1899年发现



- 计算机病毒的定义

- 1994年《中华人民共和国计算机信息系统安全保护条例》第28条
- “破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码”。

计算机病毒的历史

- 1949年，冯诺依曼

- 《复杂自动机组织论》中提出了计算机程序能够在内存中自我复制
- 开创了计算机病毒的思想

- 约翰·冯·诺依曼（John von Neumann）

- 出生于匈牙利的美籍犹太人科学家，1903-1957
- 他在计算机科学、经济、物理学中的量子力学及几乎所有数学领域都作过重大贡献。
- 1926年，获得布达佩斯大学数学博士学位
- 1931年，获普林斯顿大学终身教授，与爱因斯坦一起工作



计算机病毒的历史

- 约翰·冯·诺依曼 - 计算机之父

- 量子力学领域：量子力学教科书《量子力学的数学基础》首次以数理分析清晰地提出了波函数的两类演化过程
- 计算机科学领域：1945年6月的“101页报告”是现代计算机科学发展里程碑式的文献，明确规定用二进制替代十进制，将计算机分成五大组件
- 经济学领域领域：1944年，冯·诺伊曼与人合作的巨作《博弈论与经济行为》出版，标志着现代系统博弈理论的初步形成，其思想影响了约翰纳什。



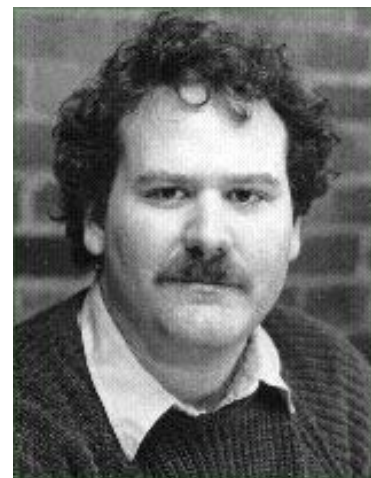
计算机病毒的历史

- 1960年，MIT

- MIT的一些青年研究者，利用业余时间玩儿游戏（开展竞赛），开发一段程序，销毁对方编写的程序

- 1983年，弗雷德·科恩博士（ Fred Cohen ）

- 在美国南加州大学攻读博士期间编写了一个可以“感染”电脑的小程序，该程序可以自我复制。
- 科恩在其博士论文给出了电脑病毒的第一个学术定义，这也是今天公认的标准。
- 计算机病毒之父



计算机病毒的历史

- 1986年，在巴基斯坦
 - 巴锡特和阿姆杰德两兄弟编写了Pakistan病毒，该病毒在一年内流传到了世界各地，针对IBM PC机
- 1988年，一种苹果机病毒发作
- 1988年，美国
 - 1988年11月3日，美国6千台计算机被病毒感染，造成Internet不能正常运行。这是一次非常典型计算机病毒入侵计算机网络的事件

至此，我们迎来了“计算机病毒”时代

计算机病毒概述

- 计算机病毒的法律制裁

- 1998年，陈盈豪

CIH病毒使全球6000万台计算机瘫痪，但他因为在被逮捕后无人起诉而免于法律制裁，如果被起诉，将获最高3年以下的有期徒刑

- 2007年，李俊等六人

熊猫烧香，出售木马程序，非法获利10万余元，中国内地地区100多万台计算机感染，李俊有期徒刑四年

计算机病毒概述

- 恶意软件和计算机病毒

- 恶意软件是介于计算机病毒和正常软件之间的一种软件
- 中国互联网协会的定义：

指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行，侵犯用户合法权益的软件，但已被我国现有法律法规规定的计算机病毒除外。

- 又叫“流氓软件”

计算机病毒的动机

- 恶作剧

- 以计算机爱好者为主，缺乏法制观念和社会责任感
- 炫耀自己的“高超技术”和智慧

- 报复心理

- 为了报复而编写电脑病毒程序，使憎恨对象遭受损害

- 军事目的

- 1990年5月8日纽约消息， 美国军队悬赏研制摧毁敌人电子系统的电脑病毒

计算机病毒的动机


- 政治目的
- 经济目的
 - 利用电脑病毒从事经济犯罪
 - 窃取竞争对手的电脑系统中的机密信息，或修改电脑中的数据
 - 挪用款项，或破坏竞争对手的电脑系统
 - 盗取他人的虚拟财产（Q币）

计算机病毒的发展趋势

- 计算机病毒种类越来越多？
- 计算机病毒感染率越来越高？

计算机病毒概述

- 计算机病毒的特点

- 传染性  传染性是病毒的基本特征

- 一但进入计算机系统并运行，就会搜寻其他符合其传播条件的程序或者存储介质，确定目标后，将其自身代码插入其中。

- 潜伏性

- 绝大多数计算机病毒感染系统后不会马上发作，黑色星期五

- 破坏性

- 降低计算机工作效率、占用系统资源、导致系统崩溃等

计算机病毒概述

- 计算机病毒的特点

- 隐藏性

最大的病毒程序不超过1MB，一般在1KB左右。病毒一般藏在用户不常去的系统文件中，或者和其他程序绑定到一起，实现隐藏。

- 可激发性

绝大多数计算机病毒具有发作的设置条件

- 未经授权而执行

病毒隐藏在正常程序中，当用户调用正常程序时窃取到系统的控制权，先于正常程序执行

本节大纲

- 计算机病毒概述
- 计算机病毒的种类
- 计算机病毒的原理
- 计算机病毒的防范
- 一些计算机病毒案例
- 本节总结

计算机病毒的种类

- 分类方法

- 根据操作系统分类
- 根据攻击的机型分类
- 根据破坏能力分类
- 根据病毒链接方式分类
- 根据传播媒介不同分类
- 根据算法不同分类
- 根据常规说法分类

计算机病毒的种类

- 根据常规说法分类

- 系统病毒
- 蠕虫病毒
- 木马病毒
- 脚本病毒
- 宏病毒
- 后门病毒
- 病毒种植程序病毒
- 破坏性程序病毒
- 玩笑病毒
- 捆绑机病毒

计算机病毒的种类

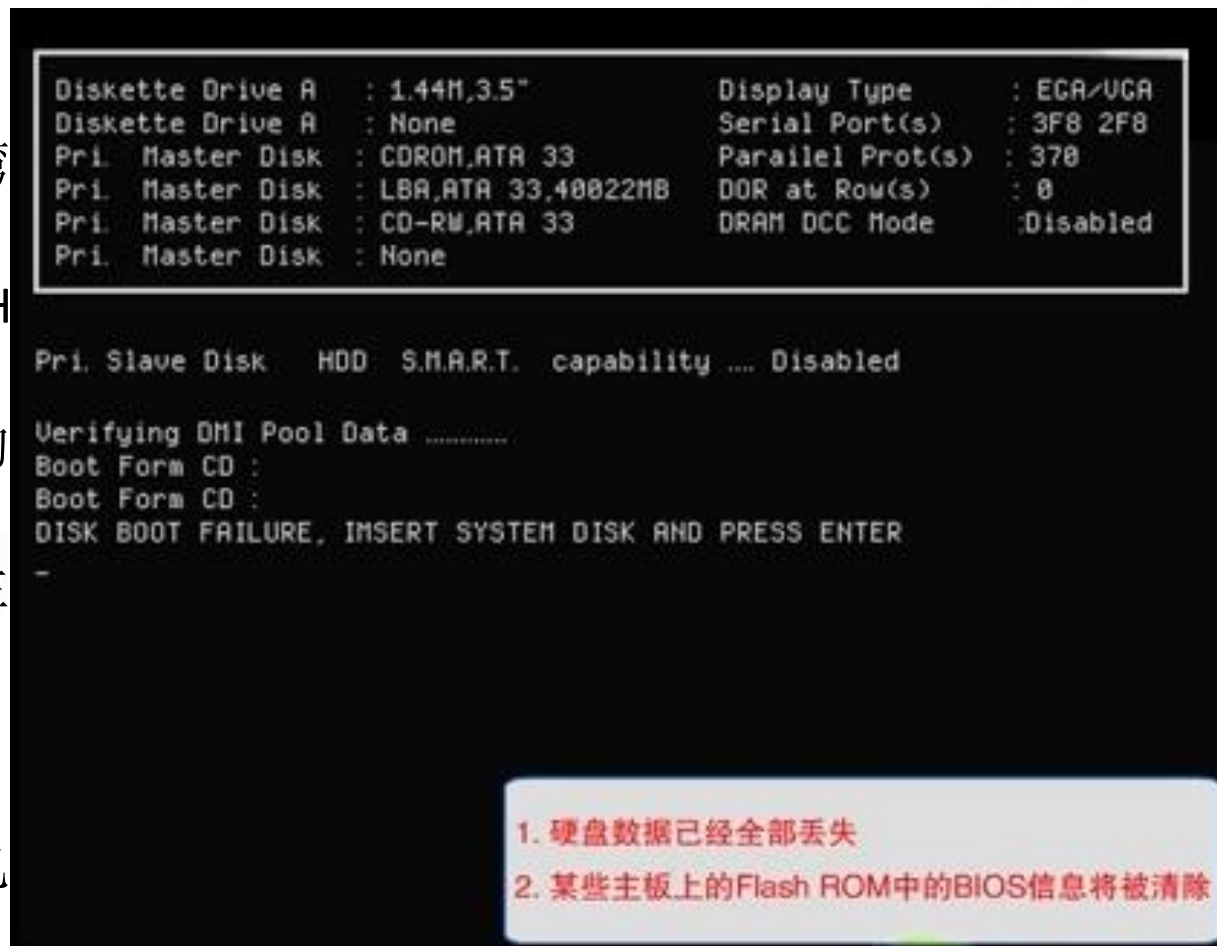
- 系统病毒

- 前缀为：Win32、PE、Win95、W32、W95等
- 共有的特性是可以感染windows操作系统的 *.exe 和 *.dll 文件，
并通过这些文件进行传播
- 例如：CIH病毒

计算机病毒

- CIH病毒

- 1998年6月，台湾
- 别名：Win95.CIH
- （1）清除全部的
- （2）清除某些主
- 每个月26日发作
- 全球损失超过5亿



计算机病毒的种类

- 蠕虫病毒

- 前缀为: Worm
- 共有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。
- 例如：冲击波（阻塞网络），小邮差（发带毒邮件） 等。

计算机病毒

- 冲击波病毒 (Worm. Blast)

- 2003年，明尼苏达州，19岁少年
- 运行时会不停地通过IP扫描寻找网络上系统为Win2K或XP的计算机
- 找到后利用DCOM RPC缓冲区漏洞攻击该系统，病毒体将会被传送到对方计算机中，使系统操作异常、不停重启、甚至导致系统崩溃。
- 还会对微软的一个升级网站进行拒绝服务攻击，导致该网站堵塞，使用户无法通过该网站升级系统。
- 造成了数百亿美元的损失。



计算机病毒的种类

- 木马病毒（特洛伊木马）

- 前缀为：Trojan
- 木马是一种特殊的程序，它们不感染文件，不自身复制和传播，甚至不破坏系统，是一个具有特定功能的可以里应外合的后门程序



计算机病毒的种类

- 脚本病毒

- 前缀为：Script、VBS、JS
- 共有特性是使用脚本语言编写，通过网页进行的传播的病毒
- 如：红色代码（Script.Redlof）、欢乐时光（VBS.Happytime）等
- 特点：跨平台、可以感染各类计算机系统

计算机病毒的种类

- 宏病毒

- 前缀为: Macro
- 是脚本病毒的一种, 感染Word、Word97、Excel、Excel97等软件
- 宏: Word、Excel等Office工具中提供的一个功能
- 特点: 由于word、excel等文件交流频繁, 病毒的传播广泛

计算机病毒的种类

- 病毒种植程序病毒

- 前缀为: Dropper
- 共有特性是运行时会从程序内释放出一个或几个新的病毒到系统目录下, 由释放出来的新病毒产生破坏
- 例如: 冰河播种者 (Dropper.BingHe2.2C)

计算机病毒的种类

- 捆绑机病毒

- 前缀为: Binder
- 共有特性是病毒作者会使用特定的捆绑程序将病毒与一些应用程序如QQ、IE捆绑起来，表面上看是一个正常的文件，当用户运行这些捆绑病毒时，会表面上运行这些应用程序，然后隐藏运行捆绑在一起的病毒，从而给用户造成危害。
- 例如：捆绑QQ（Binder.QQPass.QQBin）等。

本节大纲

- 计算机病毒概述
- 计算机病毒的种类
- 计算机病毒的原理
- 计算机病毒的防范
- 一些计算机病毒案例
- 本节总结

计算机病毒的原理

- 计算机病毒的结构

- 病毒的逻辑结构
- 病毒的磁盘存储结构
- 病毒的内存驻留结构

关键：理解PE (Portable Executable) 格式

计算机病毒的原理

- 计算机病毒的逻辑结构

- 病毒的引导模块；
- 病毒的传染模块；
- 病毒的发作（表现和破坏）模块。

引导模块
传染条件判断模块 实施传染模块
触发条件判断模块 实施表现或破坏模块

计算机病毒的原理

- 计算机病毒的存储结构

- 经过格式化后的磁盘应包括：

- (1) 主引导记录区（硬盘）

- (2) 引导记录区

- (3) 文件分配表（FAT）

- (4) 目录区

- (5) 数据区

计算机病毒的原理

- 计算机病毒的内存驻留结构

- 系统型病毒的内存驻留结构

系统型病毒是在系统启动时被装入的

病毒程序将自身移动到适当的内存高端

采用修改内存向量描述字的方法隐藏自己

有些病毒也利用小块没有使用的低端内存系统

计算机病毒的原理

- 计算机病毒的内存驻留结构

- 文件型病毒的内存驻留结构

病毒程序是在运行其宿主程序时被装入内存，可以驻留在内存中操作系统允许的任何位置

计算机病毒的原理

- 计算机病毒的作用机制

- (1) 引导机制

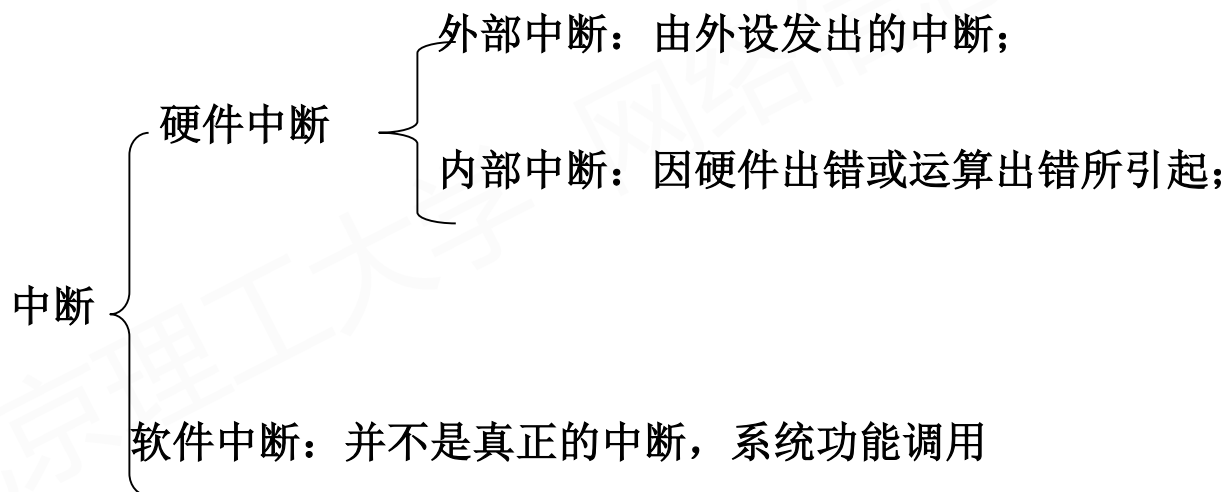
- (2) 传染机制

- (3) 破坏机制

计算机病毒的引导机制

- 中断和计算机病毒

- 中断是CPU处理外部突发事件的一个重要技术，包括：



计算机病毒的引导机制

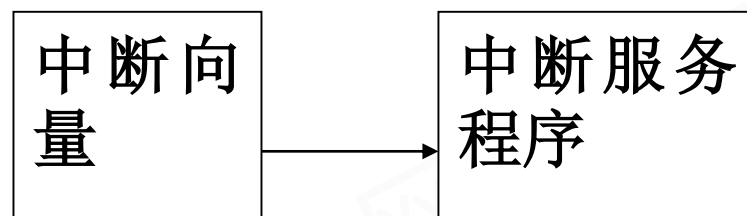
- 计算机病毒常用中断

- INT 08H和INT 1CH的定时中断，病毒用来判断激发条件；
- INT 09H键盘输入中断，病毒用于监视用户击键情况；
- INT 10H屏幕输入输出，一些病毒用于在屏幕上显示信息来表现自己；
- INT 13H磁盘输入输出中断，引导型病毒用于传染病毒和格式化磁盘；
- INT 21H DOS功能调用，绝大多数文件型病毒修改该中断。

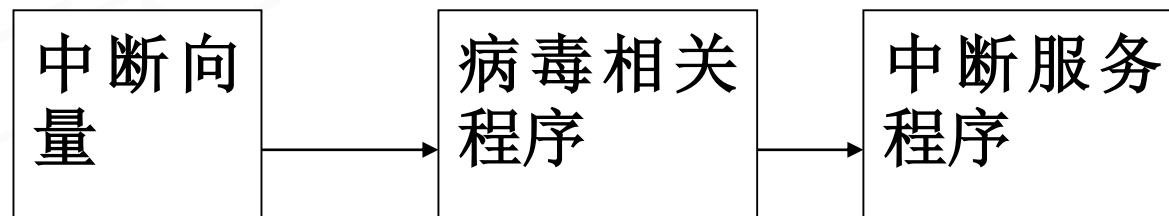
计算机病毒的引导机制

- 计算机病毒对中断的使用

盗用前:



盗用后:



Windows下的钩子函数 (Hook)

计算机病毒的传染机制

- 传染是指计算机病毒由一个载体传播到另一载体，由一个系统进入另一个系统的过程。
- 计算机病毒的传染方式主要有：
 - 病毒程序利用操作系统的引导机制或加载机制进入内存；
 - 从内存的病毒传染新的存储介质或程序文件，利用操作系统的读写磁盘的中断或加载机制来实现。

计算机病毒的传染机制

- 利用可执行文件.COM或.EXE传染病毒
 - 病毒程序通过.COM或者.EXE文件的执行驻入内存
 - 一旦进入内存, 便开始监视系统的运行
 - 当它发现被传染的目标时, 进行如下操作:
 - (1) 首先对运行的可执行文件特定地址的标识位信息进行判断是否已感染了病毒;
 - (2) 当条件满足, 解析PE格式将病毒链接到可执行文件的首部或尾部或中间, 并存入磁盘中;
 - (3) 完成传染后, 继续监视系统的运行, 试图寻找新的攻击目标。

计算机病毒的破坏机制

- 利用中断向量

在设计原则、工作原理上与传染机制基体相同，通过修改某一中断向量入口地址，使其指向病毒程序的破坏模块。

- 利用系统函数

采用高级语言开发，利用DOS命令、系统函数等实现破坏。

本节大纲

- 计算机病毒概述
- 计算机病毒的种类
- 计算机病毒的原理
- 计算机病毒的防范
- 一些计算机病毒案例
- 本节总结

计算机病毒的检测方法

- 特征代码法

- 利用已知病毒的特征代码来检测病毒
- 检测已知病毒的最简单、开销最小的方法
- 特征代码法的特点：
 - 速度慢
 - 误报警率低
 - 不能检查多形性病毒
 - 不能对付隐蔽性病毒

计算机病毒的检测方法

- 特征代码法

- 特征代码法的获得：

- 选取病毒中最具代表性的程序片段
 - 通常采用16进制表示
 - 例如：ClamAV中的一条病毒

b44ccd21b430cd21b8acaccd213dcaca7403eb

计算机病毒的检测方法

- 校验和法

- 将正常文件的内容，计算其校验和（或对其进行认证）
- 在文件使用过程中，定期地或每次使用文件前，检查文件现在内容算出的校验和与原来保存的校验和是否一致
- 可以发现文件是否被感染

计算机病毒的检测方法

- 行为监测法

- 利用病毒的特有行为特征来监测病毒的方法，称为行为监测法。
- 例如：占有INT 13H、修改注册表
- 优点：可发现未知病毒、可相当准确地预报未知的多数病毒。
- 缺点：可能误报警、不能识别病毒名称、实现时有一定难度。

计算机病毒的防御方法

- 杀毒引擎

- 病毒集合A，特征码集合B，如果按照某种对应法则 f ，对于集合A中的病毒，在集合B中有特征码和它对应，法则 f 即为杀毒引擎。
- 对杀毒引擎的评价指标：
 - A中病毒是否命中
 - 特征码冗余度
 - 速度

计算机病毒的防御方法

- 主动防御 – 利用行为监测法
 - 可以防御未知病毒、未知威胁、ZeroDay攻击等
 - 所谓“主动防御”其实是针对传统的“特征码技术”而言。
 - 创立动态仿真反病毒专家系统：
 - 自动准确判定新病毒
 - 程序行为监控并举
 - 自动提取特征值实现多重防护

计算机病毒的防御方法

- 云计算杀毒（云安全）

- 云计算（cloud computing），一种分布式计算技术
- 实例：360杀毒
- 从个别机器上发现病毒的行为或特征，防范所有云安全终端
- 云计算杀毒的实质是：杀毒软件的互联网化

本节大纲

- 计算机病毒概述
- 计算机病毒的种类
- 计算机病毒的原理
- 计算机病毒的防范
- 一些计算机病毒案例
- 本节总结

计算机病毒案例

- 爱虫病毒

- 2000年
- 通过Outlook电子邮件系统传播，邮件主题为“I Love You”，包含附件“Love-Letter-for-you.txt.vbs”
- 打开病毒附件后，该病毒会自动向通讯簿中的所有电子邮件地址发送病毒邮件副本，阻塞邮件服务器，还感染扩展名VBS、HTA、JPG和MP3等十二种数据文件
- 损失估计：全球超过100亿美元

计算机病毒案例

- 红色代码病毒

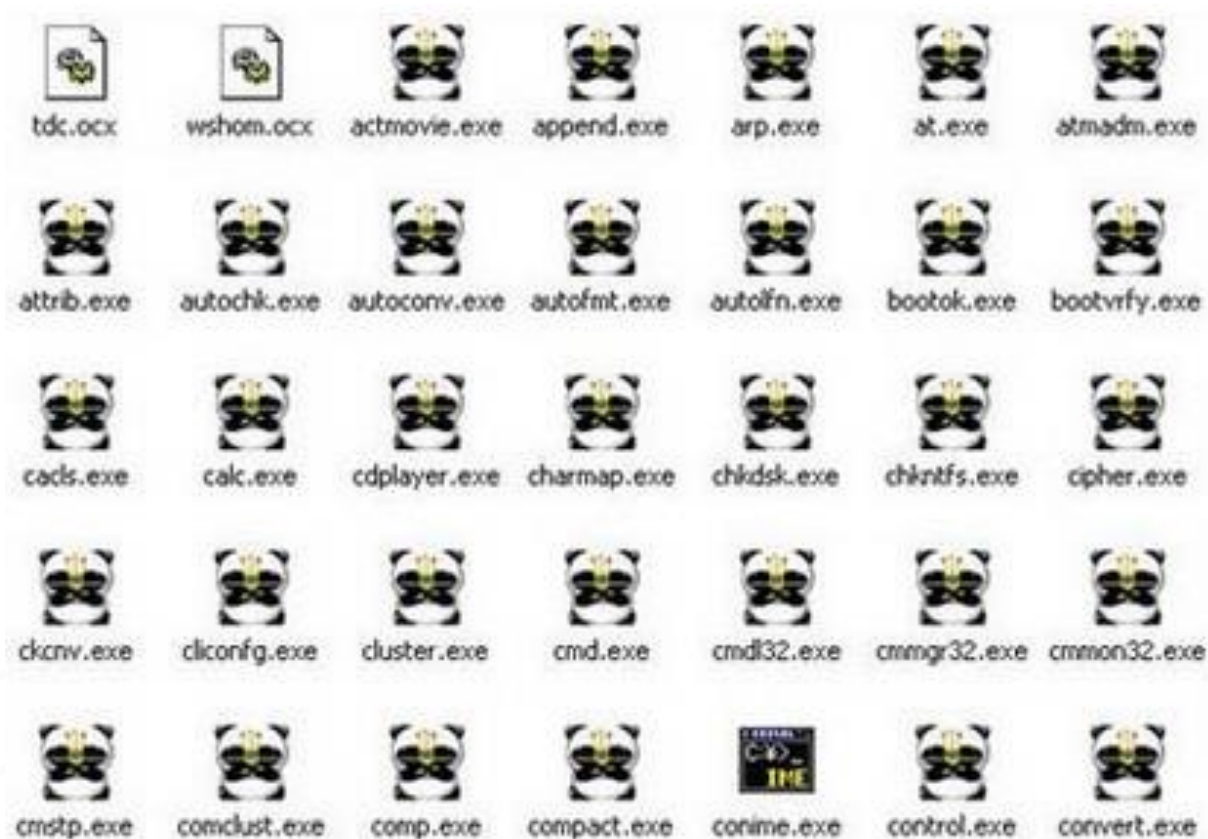
- 2001年7月，计算机蠕虫病毒
- 通过网络服务器和互联网进行传播，专门针对运行微软互联网信息服务软件（IIS）的网络服务器来进行攻击。极具讽刺意味的是，在此之前，微软曾经发布了一个补丁，来修补这个漏洞。
- 被它感染后，会在网络站点上会显示：“你好！欢迎光临www.worm.com！”，随后病毒便会主动寻找其他易受攻击的主机，这个行为持续大约20天
- 对某些特定IP地址发起拒绝服务(DoS)攻击
- 1周内感染40万台计算机，全球损失超过26亿美元

计算机病毒案例

- MyDoom病毒（世界末日）

- 2004年1月，最快散播速度的邮件病毒记录
- 它会自动生成病毒文件，修改注册表，通过电子邮件进行传播，会尝试从多个URL下载并执行一个后门程序，保存在Windows文件夹，名称为winvpn32.exe，允许恶意用户远程访问被感染的计算机。
- 病毒使用自身的SMTP引擎向外发送带毒电子邮件，进行传播。
- 全球损失超过100亿美元

计算机病毒案例



计算机病毒案例

- 熊猫烧香

- 2006年底，由Delphi工具编写
- 能够终止大量的反病毒软件和防火墙软件进程
- 会删除扩展名为gho的文件，使用户无法使用ghost恢复操作系统
- 感染系统的*.exe、*.com、*.pif、*.src、*.html、*.asp文件，导致用户打开这些网页文件时IE自动连接到指定网址中下载病毒
- 可以修改注册表启动项，被感染的文件图标变成“熊猫烧香”的图案。病毒还可以通过共享文件夹、系统弱口令等多种方式进行传播
- 全球损失超过无法估计
- 李俊等六人被判处最多有期徒刑四年（破坏计算机系统罪）

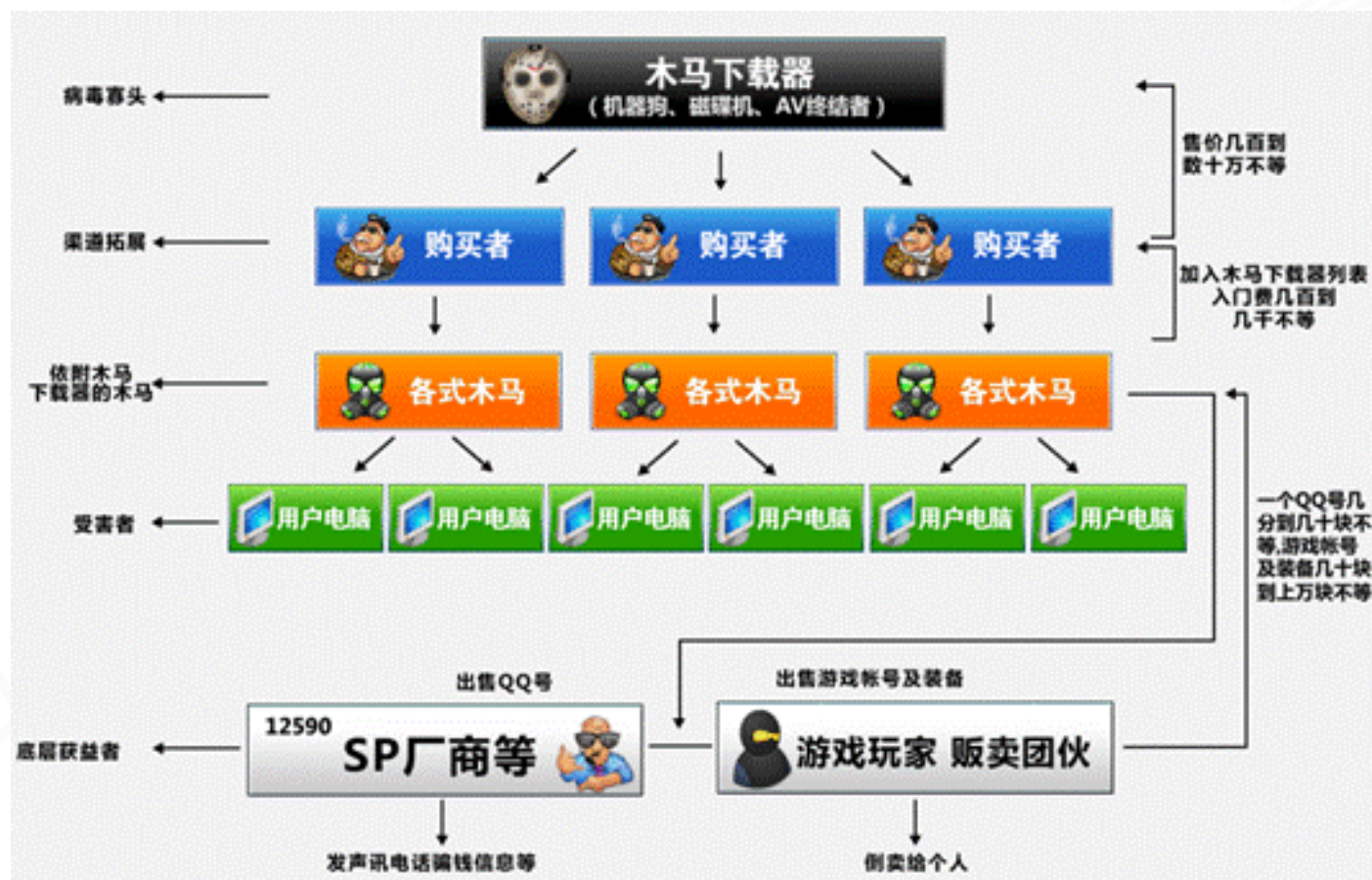
计算机病毒案例

- 网游大盗

- 2007年底, Trojan/PSW.GamePass.jws
- 专门盗取网络游戏帐号和密码的病毒
- 采用VisualC++编写, 并经过加壳处理
- 该病毒会盗取包括“魔兽世界”、“完美世界”、“征途”、等多款网游玩家的帐户和密码, 并且会下载其它病毒到本地运行。玩家计算机一旦中毒, 就可能导致游戏帐号、装备等丢失。在07年轰动一时, 网游玩家提心吊胆。
- 估计损失: 几千万美元
- 贺斌等4人被判处有期徒刑4年 (盗窃罪)

计算机病毒案例

- 病毒产业链



计算机病毒案例

- 手机病毒

- 针对智能手机（2.5G/3G）

- Timofonica

给地址簿中的邮箱发送带毒邮件，还能通过短信服务器中转向手机发送大量短信。

- Hack.mobile.smsdos

会让手机死机或自动关机。

思考

今天，我们如何看待计算机病毒？

本节总结

- 经过本节的学习，我们知道
 - 计算机病毒的历史和特点
 - 木马、蠕虫、后门、系统病毒等类型
 - 病毒的原理
 - 常见病毒和病毒产业链