第6章 网络威胁

罗文坚

主要内容

- 6.1 概述
- 6.2 计算机病毒
- 6.3 网络入侵
- 6.4 诱骗类威胁

概述

- 威胁：用威力逼迫恫吓使人屈服。
- 网络威胁：是网络安全受到威胁、存在着危险。

- 随着互联网的不断发展，网络安全威胁也呈现了一种新的趋势。
  - 最初，主要是计算机病毒，比如“CIH”、“大麻”等传统病毒。
  - 至今，已逐渐发展为包括特洛伊木马、后门程序、流氓软件、间谍软件、广告软件、网络钓鱼、垃圾邮件等等。
  - 目前的网络威胁往往是集多种特征于一体的混合型威胁。

网络威胁的三个阶段

- 第一阶段（1998年以前）：网络威胁主要来源于传统的计算机病毒，其特征是通过媒介复制进行传染，以攻击破坏个人电脑为目的。

- 第二阶段（大致在1998年以后）：网络威胁主要以蠕虫病毒和黑客攻击为主，其表现为蠕虫病毒通过网络大面积爆发、黑客攻击一些服务网站。

- 第三阶段（2005年以来）：网络威胁多样化，多数以偷窃资料、控制利用主机等手段谋取经济利益为目的。

网络威胁分类

- 从攻击发起者的角度来看：
  - 一类是主动攻击型威胁，如网络监听和黑客攻击等，这些威胁都是对方人为通过网络通信连接进行的；
  - 另一类就是被动型威胁，一般是用户通过某种途径访问了不当的信息而受到的攻击。例如，使用了带病毒的U盘，访问了带病毒、木马、恶意软件的网页、图片和邮件等。

- 依据攻击手段及破坏方式进行分类：
  - 第一类是以传统病毒、蠕虫、木马等为代表的计算机病毒；
  - 第二类是以黑客攻击为代表的网络入侵；
  - 第三类以间谍软件、广告软件、网络钓鱼软件为代表的欺骗类威胁。

主要内容

- 6.1 概述
- 6.2 计算机病毒
  - 6.2.1 病毒概述
  - 6.2.2 传统病毒
  - 6.2.3 蠕虫病毒
  - 6.2.4 木马
  - 6.2.5 病毒防治
- 6.3 网络入侵
- 6.4 诱骗类威胁

计算机病毒概述

- 1949年，约翰·冯·诺依曼的论文《自我繁衍的自动机理论》，从理论上论证了当今计算机病毒的存在。
- 20世纪60年代初，美国贝尔实验室的三位程序员编写了一个名为“磁芯大战”的游戏，游戏中程序通过复制自身来摆脱对方的控制。
- 1983年，美国南加州大学的弗雷德·科恩博士研制出一种在运行过程中可以复制自身的破坏性程序，第一次验证了计算机病毒的存在。
- 1984年，弗雷德·科恩发表论文《计算机病毒：原理和实验》。
- 1986年，Brain病毒，世界上流行的第一个病毒。
- 1988年，罗伯特·塔潘·莫里斯（美国前国家安全局首席科学家罗伯特·莫里斯的儿子）编写Morris蠕虫。

计算机病毒定义

- 《中华人民共和国计算机信息系统安全保护条例》中明确定义：
  - 病毒是指“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”。

- 计算机病毒特征
  1. 非授权性：在用户未知（未授权）的情况下执行。
  2. 寄生性：传统病毒特有；目前的网络病毒多是独立文件。
  3. 传染性：是否具有传染性是判断一个程序是否为计算机病毒的重要条件。
  4. 潜伏性：发作时间可能是预设的，不发作很难觉察出来。
  5. 破坏性：使正常程序无法运行；窃取资料；破坏文件等。
  6. 触发性：触发条件可能是时间、日期、文件类型等。

计算机病毒发展新的趋势

1. 无国界：过去，以磁盘等为媒介，从国外发现到国内流行，传播周期平均需要6-12个月；目前，Internet普及，几天甚至更短时间就传遍整个世界。

2. 多样化：引导型病毒、可执行文件型病毒、宏病毒和混合型病毒，利用Java、VB和ActiveX网页技术撰写病毒等。

3. 破坏性更强：修改文件（含注册表）、通信端口、用户密码，挤占内存，远程控制，等等。

4. 智能化：例如，超级病毒Verona，将病毒写入邮件原文。一旦用户用Outlook预览了该邮件，病毒就会发作。

5. 更加隐蔽化：主题随用户的传播改变；伪装成常用程序；病毒写入文件内部，而且文件长度不变；等等。

计算机病毒分类

- 计算机病毒可以根据其工作原理和传播方式划分成：

1. 传统病毒：寄生于宿主文件内，以可移动介质为传播途径的计算机病毒。

2. 蠕虫病毒：利用网络进行复制和传播，以独立智能程序形式存在的计算机病毒。

3. 木马：木马一般不会自我繁殖，也并不“刻意”去感染其他文件，而是通过伪装吸引用户下载并安装在用户的计算机内，向施种木马者提供打开的被种者计算机的门户，是施种者可以任意破坏、窃取被种者的文件，甚至远程操控被种者的计算机。

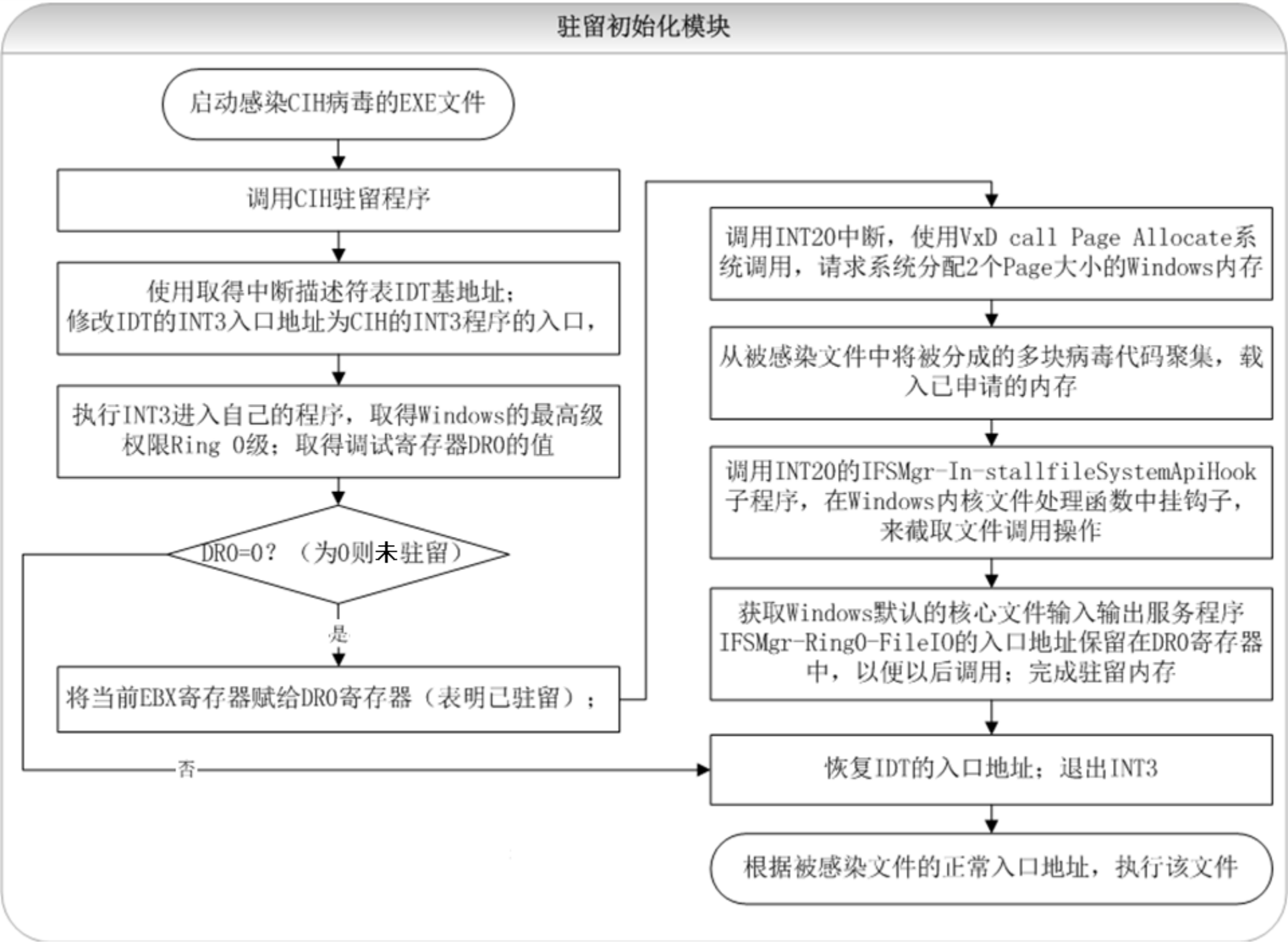
主要内容

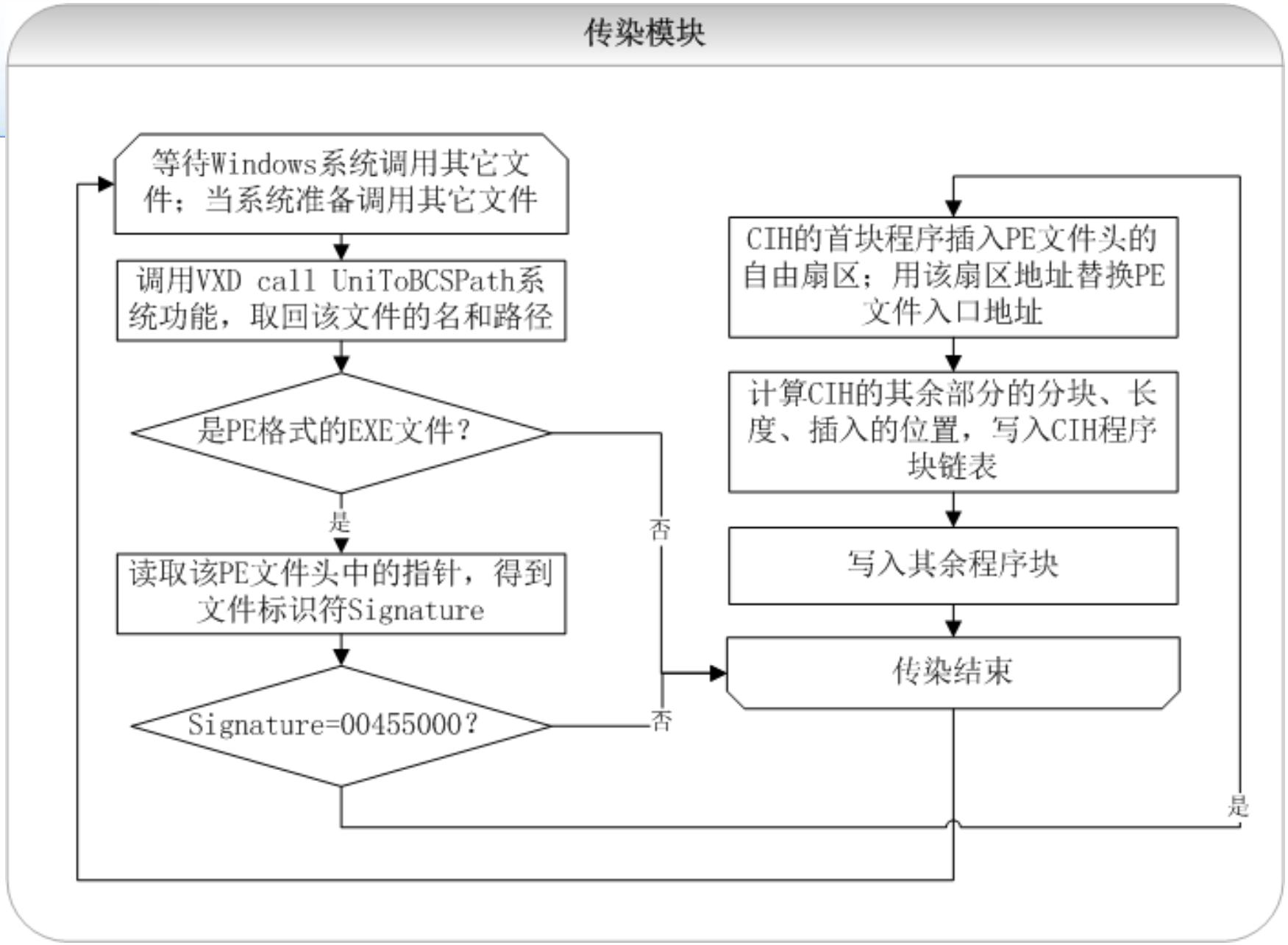
- 6.1 概述
- 6.2 计算机病毒
  - 6.2.1 病毒概述
  - 6.2.2 传统病毒
  - 6.2.3 蠕虫病毒
  - 6.2.4 木马
  - 6.2.5 病毒防治
- 6.3 网络入侵
- 6.4 诱骗类威胁

传统病毒

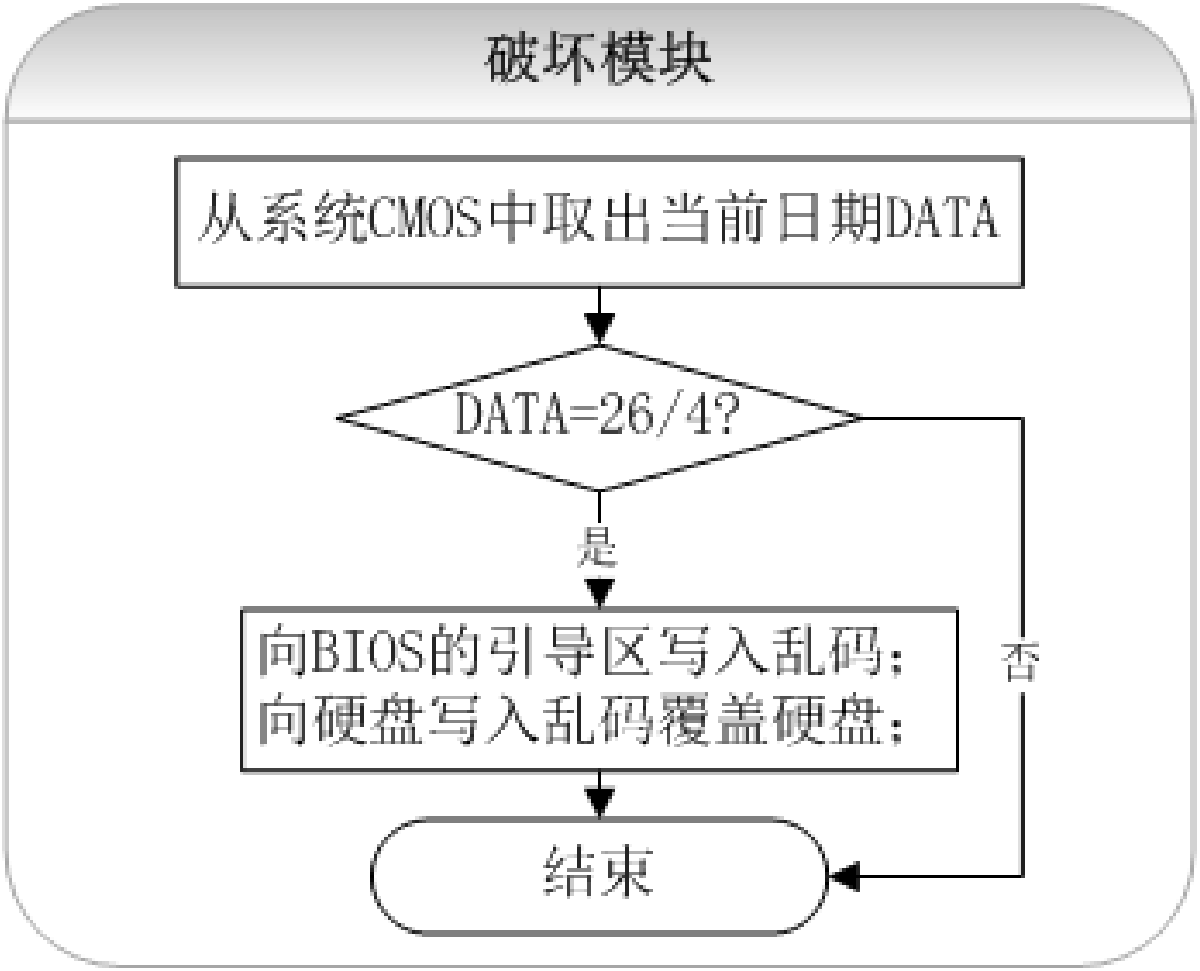
- 传统病毒的代表
  - 巴基斯坦智囊（Brain）、大麻、磁盘杀手（DISK KILLER）、CIH等。
- 传统病毒一般有三个主要模块组成，包括启动模块、传染模块和破坏模块。

- CIH病毒
  - 感染Windows 95/98环境下PE格式的EXE文件（第一例）。
  - 病毒发作时直接攻击和破坏计算机硬件系统。
  - 该病毒通过文件复制进行传播。
  - 计算机开机后，运行了带病毒的文件，其病毒就驻留在Wnidows核心内存里。
  - 由初始化驻留模块、传染模块和破坏模块组成。


驻留初始化模块
启动感染CIH病毒的EXE文件
调用CIH驻留程序
使用取得中断描述符表IDT基地址；
修改IDT的INT3入口地址为CIH的INT3程序的入口，
执行INT3进入自己的程序，取得Windows的最高级权限Ring 0级；取得调试寄存器DR0的值
DR0=0？（为0则未驻留）
是
否
将当前EBX寄存器赋给DR0寄存器（表明已驻留）；
调用INT20中断，使用VxD call Page Allocate系统调用，请求系统分配2个Page大小的Windows内存
从被感染文件中将被分成的多块病毒代码聚集，载入已申请的内存
调用INT20的IFSMgr-In-stallfileSystemApiHook子程序，在Windows内核文件处理函数中挂钩子，来截取文件调用操作
获取Windows默认的核心文件输入输出服务程序IFSMgr-Ring0-FileIO的入口地址保留在DR0寄存器中，以便以后调用；完成驻留内存
恢复IDT的入口地址；退出INT3
根据被感染文件的正常入口地址，执行该文件



- **Signature=”00455000”表明该文件是PE格式的可执行文件，且尚未感染。**


破坏模块
从系统CMOS中取出当前日期DATA
DATA=26/4?
是
否
向BIOS的引导区写入乱码；
向硬盘写入乱码覆盖硬盘；
结束

主要内容

- 6.1 概述
- 6.2 计算机病毒
  - 6.2.1 病毒概述
  - 6.2.2 传统病毒
  - 6.2.3 蠕虫病毒
  - 6.2.4 木马
  - 6.2.5 病毒防治
- 6.3 网络入侵
- 6.4 诱骗类威胁

蠕虫病毒

- 蠕虫病毒产生于20世纪80年代后期，鼎盛时期却是从20世纪90年代末开始的，而且迅速成为计算机病毒的主流。

- 蠕虫病毒的代表包括：
  - Morris蠕虫，1988年
  - 红色代码（Code Red），2001年
  - 尼姆达（Nimda），2001年
  - 求职信，2002年
  - SQL蠕虫王，2003
  - 熊猫烧香，2006年底-2007年初，中国警方破获的首例计算机病毒大案

蠕虫病毒

- 蠕虫与传统病毒的区别：
  - 传统病毒是需要“寄生”，通过感染其它文件进行传播。
  - 蠕虫病毒一般不需要寄生在宿主文件中，传播途径主要包括局域网内的共享文件夹、电子邮件、网络中的恶意网页和大量存在着漏洞的服务器等。
  - 可以说，蠕虫病毒是以计算机为载体，以网络为攻击对象。

- 蠕虫病毒与普通病毒的另一个不同是，蠕虫病毒往往能够利用漏洞。

- 漏洞分为软件漏洞和人为缺陷。

蠕虫病毒

- 软件漏洞主要指程序员由于习惯不规范、错误理解或想当然，在软件中留下存在安全隐患的代码。
  - 例如，缓冲区溢出漏洞、微软IE和Outlook的自动执行漏洞等。

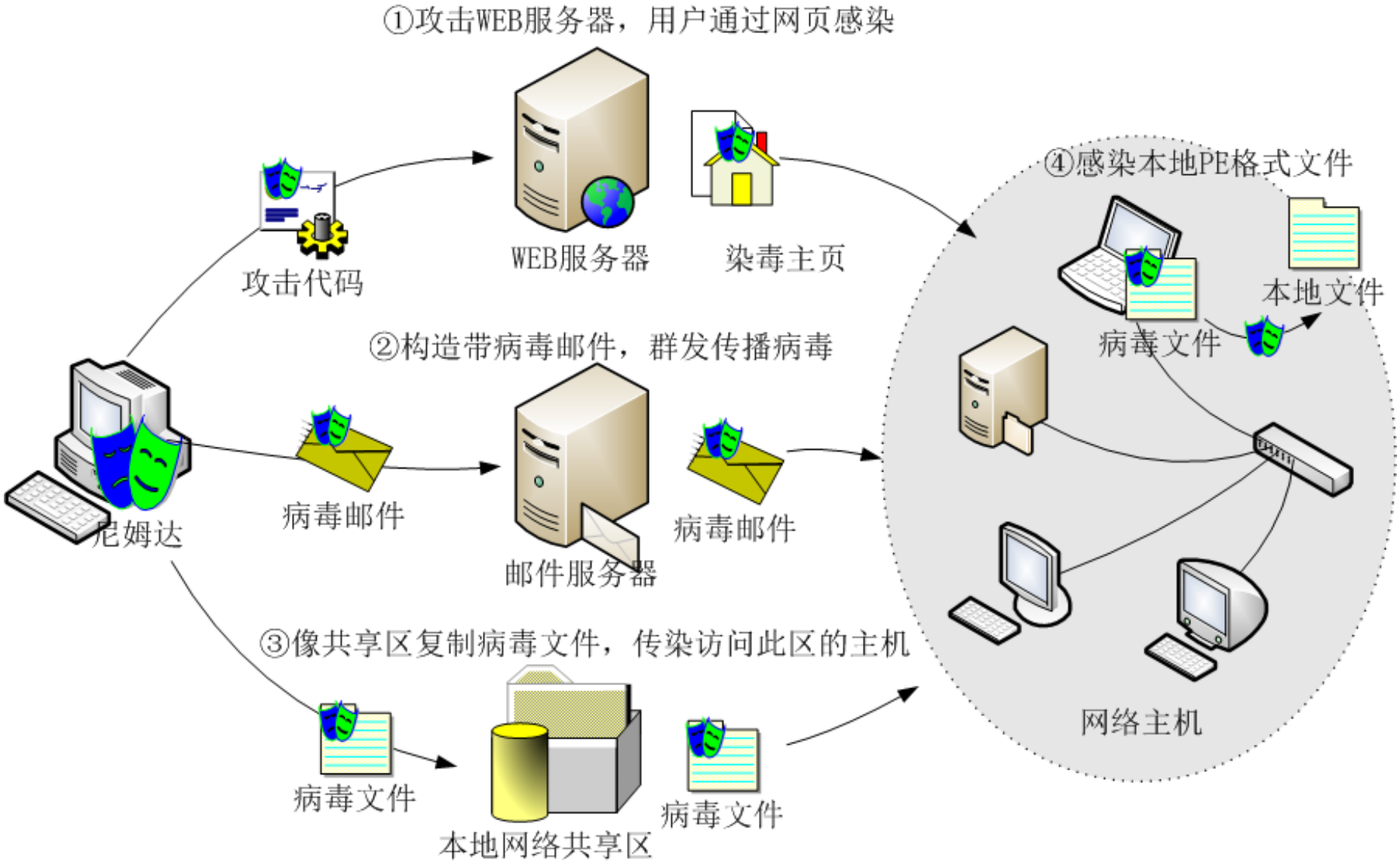
- 人为缺陷主要指的是计算机用户的疏忽，这就是所谓的社会工程学（Social Engineering）问题。
  - 例如，当收到标题为求职信息的邮件时，大多数人都会抱着好奇的心理去点击它，则求职信病毒将顺利侵入。

- 蠕虫病毒的攻击和传播主要就是利用漏洞。

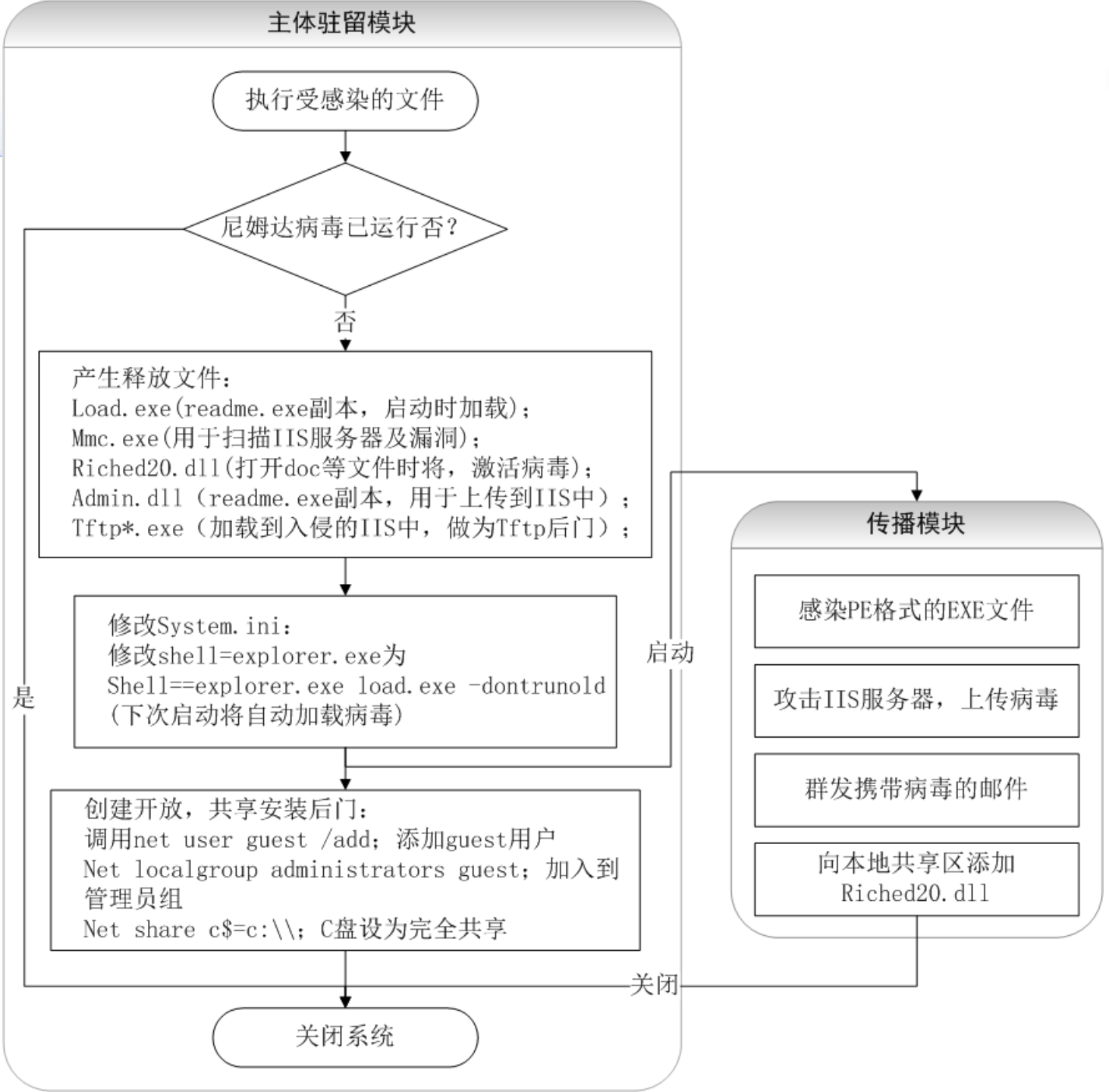
尼姆达蠕虫Worms.Nimda

- 2001年9月18日，尼姆达病毒在全球蔓延，它能够通过多种传播渠道进行传播，传染性极强，同时破坏力也极大。
  - 尼姆达病毒是一个精心设计的蠕虫病毒，其结构复杂堪称历年来之最。
  - 尼姆达病毒激活后，使用其副本替换系统文件；将系统的各驱动器设为开放共享，降低系统安全性；创建Guest账号并将其加入到管理员组中，安装Guest用户后门。
  - 由于尼姆达病毒通过网络大量传播，产生大量异常的网络流量和大量的垃圾邮件，网络性能势必受到严重影响。

Nimda传播途径


①攻击WEB服务器，用户通过网页感染
攻击代码
WEB服务器
染毒主页
④感染本地PE格式文件
本地文件
病毒文件
②构造带病毒邮件，群发传播病毒
尼姆达
病毒邮件
邮件服务器
病毒邮件
③像共享区复制病毒文件，传染访问此区的主机
病毒文件
本地网络共享区
病毒文件
网络主机

尼姆达病毒程序


主体驻留模块
执行受感染的文件
尼姆达病毒已运行否?
是
否
产生释放文件:
Load.exe(readme.exe副本，启动时加载);
Mmc.exe(用于扫描IIS服务器及漏洞);
Riched20.dll(打开doc等文件时将，激活病毒);
Admin.dll（readme.exe副本，用于上传到IIS中）;
Tftp*.exe（加载到入侵的IIS中，做为Tftp后门）;
修改System.ini:
修改shell=explorer.exe为
Shell==explorer.exe load.exe -dontrunold
(下次启动将自动加载病毒)
启动
创建开放，共享安装后门:
调用net user guest /add；添加guest用户
Net localgroup administrators guest；加入到管理员组
Net share c$=c:\\；C盘设为完全共享
关闭
关闭系统
传播模块
感染PE格式的EXE文件
攻击IIS服务器，上传病毒
群发携带病毒的邮件
向本地共享区添加Riched20.dll

Nimda病毒的防范及清除

- 感染的用户应重新安装系统，以便彻底清除其它潜在的后门。

- 如不能立刻重装系统，可参考下列步骤来清除蠕虫或者防止被蠕虫攻击：
  ① 下载IE和IIS的补丁程序到受影响的主机上；
  ② 安装杀毒软件和微软的CodeRedII清除程序；
  ③ 备份重要数据；
  ④ 断开网络连接（例如，拔掉网线）；
  ⑤ 执行杀毒工作，清除CodeRedII蠕虫留下的后门；
  ⑥ 安装IE和IIS的补丁；
  ⑦ 重启系统，再次运行杀毒软件以确保完全清除蠕虫。

主要内容

- 6.1 概述
- 6.2 计算机病毒
  - 6.2.1 病毒概述
  - 6.2.2 传统病毒
  - 6.2.3 蠕虫病毒
  - 6.2.4 木马
  - 6.2.5 病毒防治
- 6.3 网络入侵
- 6.4 诱骗类威胁

木马

- 木马病毒，“木马计”，伪装潜伏的网络病毒。

- 1986年的PC-Write木马是世界上第一个计算机木马。
  - PC-Write木马伪装成共享软件PC-Write的2.72版本。
  - 事实上，编写PC-Write的Quicksoft公司从未发行过2.72版本。
  - 一旦用户信以为真，运行该木马程序，那么他的下场就是硬盘被格式化。

- 随着Internet的普及，木马逐渐形成了独特的伪装和传播两种特征，作为黑客窃取信息的工具四处泛滥。

木马

- 木马是有隐藏性的、传播性的可被用来进行恶意行为的程序。因此，也被看作是一种计算机病毒。
  - 木马一般不会直接对电脑产生危害，以控制电脑为目的。当然，电脑一旦被木马所控制，后果不堪设想。

- 木马的传播（种木马或植入木马）方式：
  - 主要通过电子邮件附件、被挂载木马的网页以及捆绑了木马程序的应用软件。
  - 木马被下载安装后完成修改注册表、驻留内存、安装后门程序、设置开机加载等，甚至能够使杀毒程序、个人防火墙等防范软件失效。

- 木马病毒的分类：盗号类木马、网页点击类木马、下载类木马 、代理类木马。

木马病毒的分类

1. 盗号类木马
   - 通常采用记录用户键盘输入、Hook应用程序进程等方法获取用户的密码和账号。
   - 窃取到的信息一般通过发送电子邮件或向远程控制程序直接提交的方式发送给木马作者。
   - 盗号木马的目标一般为游戏软件、即时通讯软件以及网上交易系统。

2. 网页点击类木马
   - 模拟用户点击广告等动作，短时间内产生大量的点击量。
   - 目的一般是为了赚取高额的广告推广费用。

木马病毒的分类

3. 下载类木马
   - 体积小，功能是从网络上下载其他病毒程序或安装广告软件。
   - 因为体积很小，下载类木马更容易传播，传播速度也更快。
   - 通常，功能强大、体积也很大的后门类病毒，如“灰鸽子”、“黑洞”等，传播时都单独编写一个小巧的下载型木马，用户中毒后会把后门主程序下载到本机运行。

4. 代理类木马
   - 用户感染代理类木马后，会在本机开启HTTP、SOCKS等代理服务功能。
   - 黑客将受感染的计算机作为跳板，以被感染用户的身份进行黑客活动，达到隐藏自己的目的。

木马病毒程序的组成

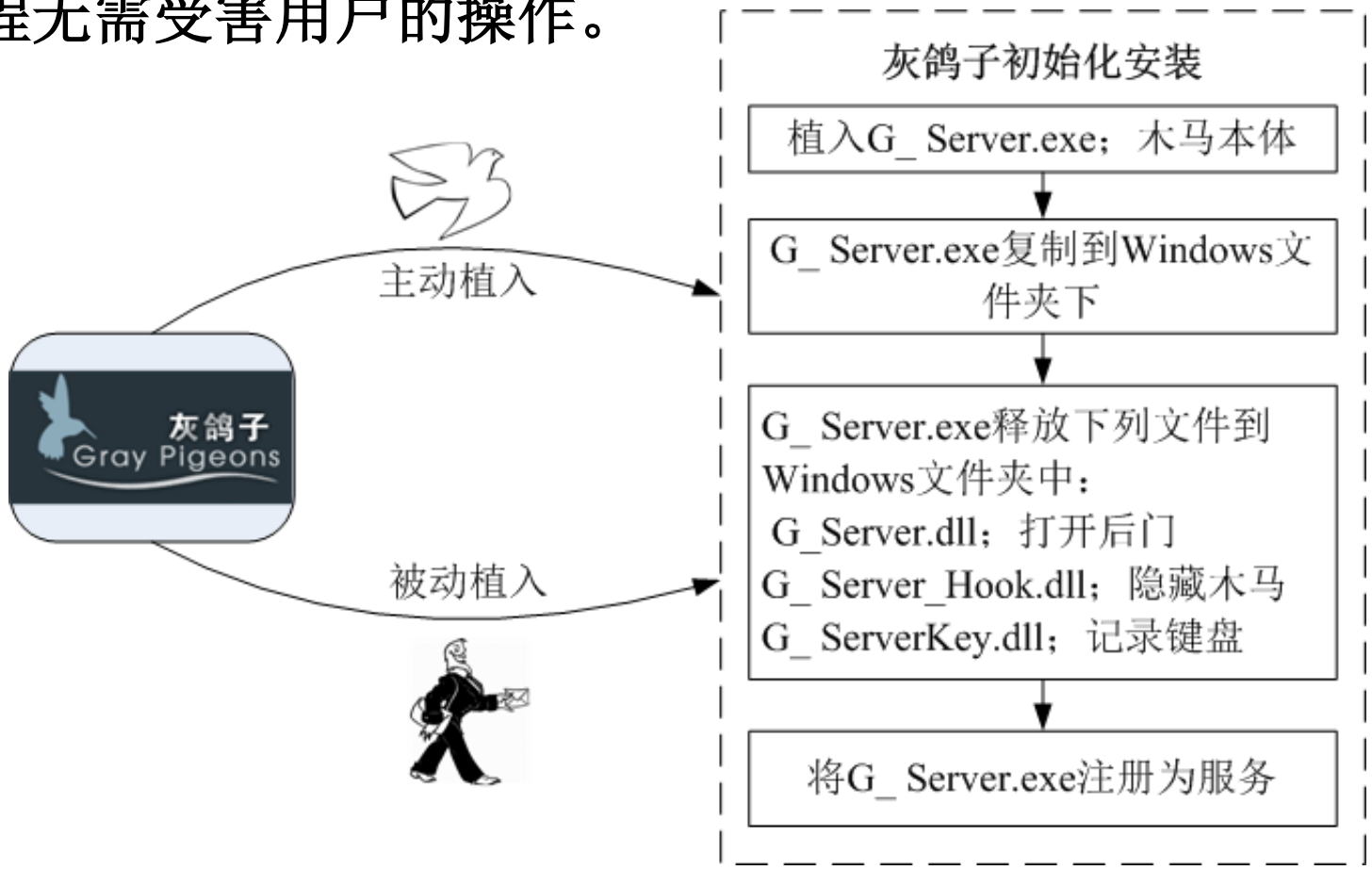
1. 控制端程序（客户端）
   - 是黑客用来控制远程计算机中的木马的程序。

2. 木马程序（服务器端）
   - 是木马病毒的核心，是潜入被感染的计算机内部、获取其操作权限的程序。

3. 木马配置程序
   - 通过修改木马名称、图标等来伪装、隐藏木马程序，并配置端口号、回送地址等信息确定反馈信息的传输路径。

灰鸽子的植入方法

- 被动植入是指植入过程必须依赖受害用户的手工操作。一般是伪装成合法程序，以降低用户的警觉性并诱骗用户。
- 主动植入是将灰鸽子程序通过程序自动安装到目标系统，植入过程无需受害用户的操作。



灰鸽子的初始化安装

- 木马程序G_Server.exe运行后，将自己复制到Windows文件夹内，并释放G_Server.dll和G_Server_Hook.dll。
  - G_Server.dll：实现后门功能，与控制客户端通信。
  - G_Server_Hook.dll：隐藏木马，包括隐藏文件、隐藏进程和隐藏通信。
  - G_Server.exe、G_Server.dll和G_Server_Hook.dll组成了灰鸽子的服务端。
  - 有的灰鸽子会多释放一个G_ServerKey.dll文件，用于记录键盘操作。

- G_Server.exe将自己注册成服务，以便每次开机都自动运行，在加载G_Server.dll、G_Server_Hook.dll和G_ServerKey.dll后自动退出。 G_Server.exe这个名字并不是固定的，是可以定制的。

灰鸽子的隐藏技术

- 隐藏文件
  - 灰鸽子拦截了对API函数的调用，隐藏了木马程序和它注册的服务项。
  - 即使设置了“显示所有隐藏文件”，也看不到它们。

- 隐藏进程
  - 修改列举进程API函数的入口地址，在别的程序在调用这些函数的时候，首先转向木马程序。木马程序中需要做的工作就是在列表中将自己的进程信息去掉，从而实现进程的隐藏。

灰鸽子的隐藏技术

- 隐藏通讯
  - 采用通信端口复用技术和反弹端口技术。
  - 通讯端口复用技术是指将自己的通讯直接绑定到正常用户进程的端口，接收数据后，根据包格式判断是不是自己的，如果是它的，自己处理，否则通过127.0.0.1的地址交给真正的服务器应用进行处理。
  - 反弹端口技术是指木马程序启动后主动连接客户，为了隐蔽起见，控制端的被动端口一般设置为80端口。
    - 对内部网络到外部网络的访问请求，防火墙一般不进行过于严格的检查，加之其连接请求有可能伪造成对外部资源的正常访问，因此容易通过防火墙。

灰鸽子的客户端程序

- 客户端程序主要包括两个功能：
  1. 定制生成服务器端程序。
  2. 控制远程的服务器端。

- 定制生成服务器端程序：
  - 首先，利用客户端程序配置生成一个服务器端程序文件，服务器端文件的名字默认为G_ Server.exe，然后开始在网络中传播植入这个程序。
  - 木马植入成功后，系统启动时，木马就会加载运行，然后通过反弹端口技术主动连接客户控制端。

灰鸽子的客户端程序

- 客户控制端程序的功能：
  - 对远程计算机文件管理：模仿Windows资源管理器，可以对文件进行复制、粘贴、删除、重命名、远程执行等，可以上传下载文件或文件夹，操作简单易用。
  - 远程控制命令：查看远程系统信息、查看剪贴板、进程管理、窗口管理、插件功能、服务管理、共享管理、代理服务、MS-DOS模拟、关机、重启。
  - 捕获屏幕，实时控制：可以连续地捕获远程计算机屏幕，并把本地的鼠标及键盘操作传送到远程被控制端，实现实时控制功能。
  - 注册表模拟器：远程操作注册表就像操作本地注册表一样方便。
- 入侵者满足私欲后，可以自行删除灰鸽子文件，这一过程用户根本无法觉察。任何悲惨的事情都有可能发生。

主要内容

- 6.1 概述
- 6.2 计算机病毒
  - 6.2.1 病毒概述
  - 6.2.2 传统病毒
  - 6.2.3 蠕虫病毒
  - 6.2.4 木马
  - 6.2.5 病毒防治
- 6.3 网络入侵
- 6.4 诱骗类威胁

病毒防治

- 病毒防治技术略滞后于病毒技术。

- 对于大多数计算机用户来说，防治病毒首先需要选择一个有效的防病毒产品，并及时进行产品升级。

- 计算机病毒防治技术主要包括:
  - 检测、清除、预防和免疫。

  - 检测和清除是根治病毒的有力手段。
  - 预防和免疫也是保证计算机系统安全的重要措施。

检测

- 病毒检测方法主要包括：特征代码法、校验和法、行为监测法以及软件模拟法等。

- 特征代码法
  - 特征代码查毒就是检查文件中是否含有病毒数据库中的病毒特征代码。
  - 检测已知病毒的最简单、开销最小的方法。
  - 检测工具必须不断更新版本，无法检测从未见过的新病毒。

- 校验和法
  - 对正常状态下的重要文件进行计算，取得其校验和，以后定期检查这些文件的校验和与原来保存的校验和是否一致。
  - 既可检测已知病毒，又可发现未知病毒。
  - 因为文件内容的改变有可能是正常程序引起的，所以校验和法使用不当可能会引起误报。

检测

- 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。当一个可疑程序运行时，监视其行为，如果发现了病毒行为，立即报警。
  - 可以发现未知病毒，但容易引起误报。
- 软件模拟法
  - 软件模拟法是为了对付多态型病毒。
  - 多态病毒：每次感染时，采用随机方法对病毒主体进行加密，放入宿主程序的代码互不相同，特征代码法无法检测。
  - 通过模拟病毒的执行环境，为其构造虚拟机，在虚拟机中执行病毒引擎解码程序，安全地将多态型病毒解开并还原其本来面目，再加以扫描。
  - 软件模拟法的优点是可识别未知病毒、病毒定位准确、误报率低；缺点是检测速度受到一定影响、消耗系统资源较高。

计算机中毒的常见症状

- 系统运行速度减慢；
- 系统经常无故发生死机；
- 文件长度发生变化；
- 存储的容量异常减少；
- 丢失文件或文件损坏；
- 屏幕上出现异常显示；
- 系统的蜂鸣器出现异常声响；
- 磁盘卷标发生变化；
- 系统不识别硬盘；
- 对存储系统异常访问；
- 键盘输入异常；
- 文件的日期、时间、属性等发生变化；
- 文件无法正确读取、复制或打开；
- 命令执行出现错误；
- WINDOWS操作系统无故频繁出现错误；
- 系统异常重新启动；
- 一些外部设备工作异常；
- 出现异常的程序驻留内存

清除

- 清除病毒主要分为使用防病毒软件和手工清除病毒两种方法。
  - 防病毒软件由安全厂商精心研制，可以有效查杀绝大多数计算机病毒，多数用户应采用防病毒软件来清除病毒。
    - 防病毒软件对检测到的病毒一般采取三种处理方案，分别是清除、隔离和删除。
    - 清除是指在发现文件被感染病毒时，采取的清除病毒并保留文件的动作。
    - 隔离是指在发现病毒后，无法确认清除动作会带来什么后果，又不想直接删除文件，故采取监视病毒并阻止病毒运行的方法。
  - 如果某类病毒清除失败、删除失败、隔离失败，对个人用户来讲，格式化硬盘、重建系统可能就是最后的有效选择。

蠕虫或木马等病毒的清除

- 目前，Windows操作系统下的病毒大多是蠕虫病毒或木马等网络病毒，对于这类病毒，其手工清除过程大致如下。

1. 结束所有可疑进程
   - 运行中的病毒，会因为文件正在使用而无法被删除，因此在清除病毒之前必须终止病毒的运行。
   - 断开网络，关闭所有应用程序。
   - 使用netstat -an分析机器上是否有后门程序在运行。
   - 使用tasklist/m 来查看当前运行的进程（所有exe和dll），使用tasklist/v查看进程对应的程序是否真实。病毒通常会使用一个和系统程序相似或相同的名称。
   - 有的病毒不止一个进程，相互守护，或者它以dll注入形式存在，可以使用ntsd -c q -p PID杀死进程，PID为进程标识符。

蠕虫或木马等病毒的清除

2. 删除病毒文件并恢复注册表
   - 在安全模式下，删除病毒文件，恢复注册表。

3. 内核级后门的清除
   - 感染了这类病毒后，即使有的应用程序并没有感染病毒，但它们的输出依然被病毒控制，用户可能得到虚假的文件列表、服务列表、进程列表和注册表键值。整个系统将是不可信任的。重装系统！

4. 重启后扫描
   - 完成了上述三步，随后需要重新启动系统，并使用带有最新病毒库的防病毒软件对全盘进行扫描（这一步非常重要，做不好的话前功尽弃）。

预防

1. 安装防毒软件
   – 打开你的防毒软件的自动升级服务，定期扫描计算机。
2. 注意U盘、光盘等存储媒介
   – 在使用软盘、光盘、U盘或活动硬盘前，进行病毒扫描。
3. 关注下载安全
   – 下载要从比较可靠的站点进行，下载后做病毒扫描。
4. 关注电子邮件安全
   – 来历不明的邮件决不要打开，决不要轻易运行附件。
5. 使用基于客户端的防火墙
   – 可以增强抵御黑客和恶意代码攻击的能力。
6. 警惕欺骗性的病毒
   – 警惕欺骗型病毒。天下没有免费的午餐。
7. 备份

免疫

- 计算机病毒免疫：提高计算机系统对计算机病毒的抵抗力，从而达到防止病毒侵害的目的，包括两个方面：
  1. 提高计算机系统的健壮性
  2. 给计算机注射“病毒疫苗”。

- 提高系统健壮性的主要途径包括以下内容：
  - 及时升级操作系统，保证系统安装最新的补丁；
  - 安装防病毒软件，及时升级病毒定义文件和防病毒引擎；
  - 定期扫描系统和磁盘文件；
  - 打开个人防火墙；
  - 使用软盘或U盘写保护；
  - 重要的数据信息写入只读光盘。

注射“病毒疫苗”

- 实施免疫，伪装系统或软件已被某病毒感染，主要方法包括：
  - 感染标识免疫：人为地为正常对象中加上病毒感染标识，使计算机病毒误以为已经感染，从而达到免疫的目的。
  - 文件扩展名免疫：将扩展名改为非COM、EXE、SYS、BAT等形式，防止以扩展名为传染条件的文件型病毒的侵入。
    - 将系统默认的可执行文件的后缀名改为非COM、EXE、SYS、BAT等形式，以便用户使用。
  - 外部加密免疫：在文件的存取权限和存取路径上进行加密保护，以防止文件被非法阅读和修改。
  - 内部加密免疫：对文件内容加密变换后进行存储，使用时再进行解密。

作业

1. 习题2（1）：传统病毒与蠕虫有什么区别？
2. 习题2（2）：木马的传播途径有哪些？