电子科技大学
University of Electronic Science and Technology of China

网络安全攻防技术

电子科技大学 信息与软件工程学院

2020年11月5日

第九讲 网络攻击与防御（二）

恶意代码原理与防治

了解恶意代码的基本概念；理解不同类型恶意代码的原理和特点；掌握恶意代码防治技术在实际环境中的应用。

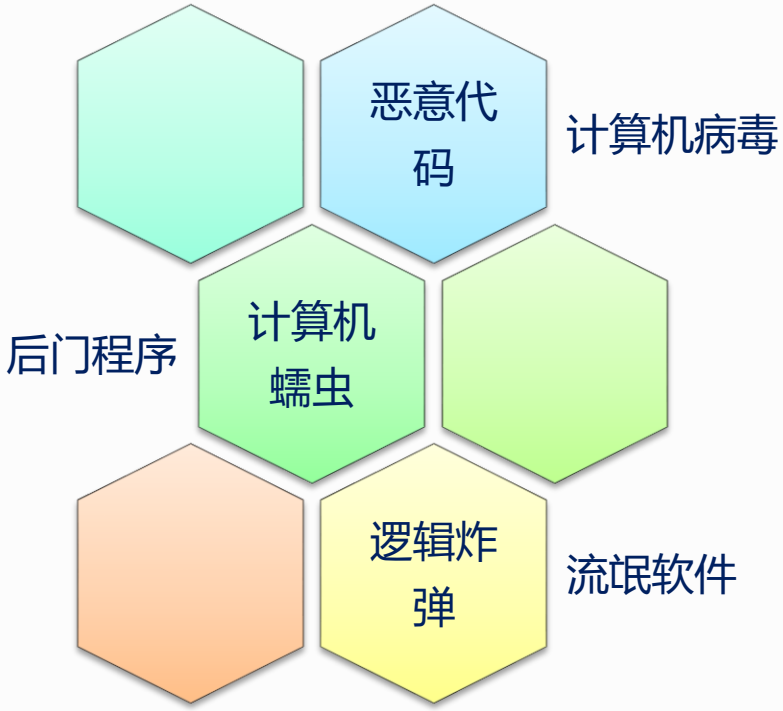
内容安排

网络攻击与防御（二）

- 恶意代码基本概念与技术原理
- 特洛伊木马技术原理
- 计算机蠕虫技术原理
- 恶意代码防治技术

引言

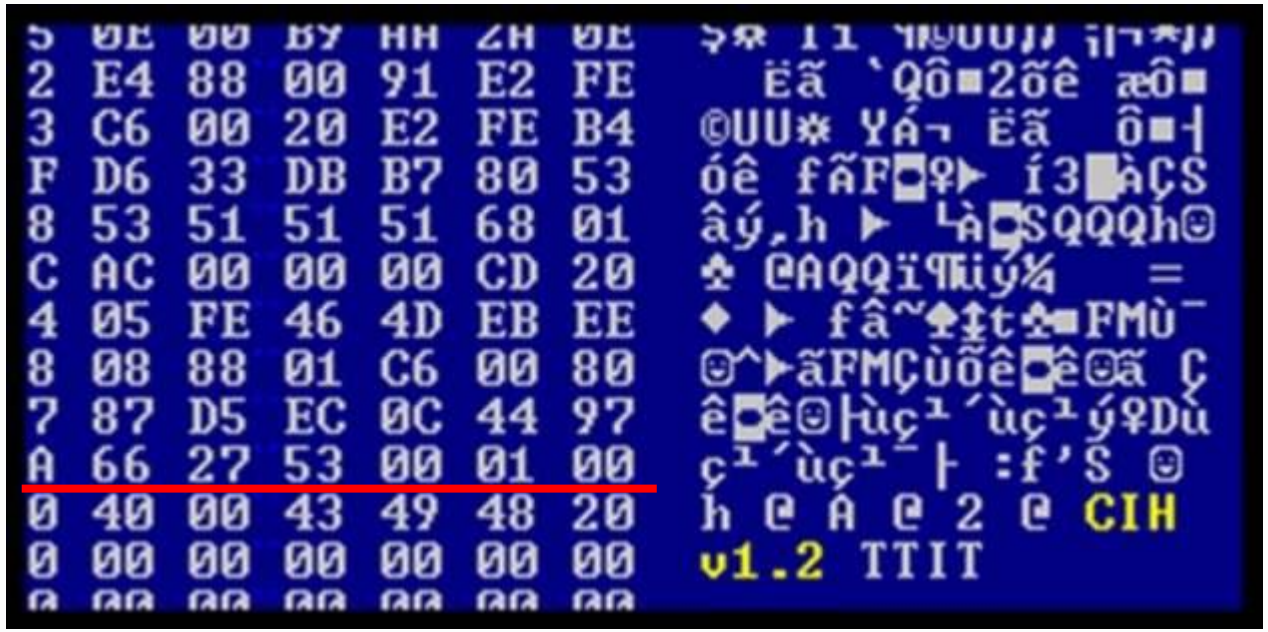
- 恶意代码（程序）是指故意编制或设置的、对网络或系统会产生威胁或潜在威胁的计算机代码。最常见的恶意代码有计算机病毒（简称病毒）、特洛伊木马（简称木马）、计算机蠕虫（简称蠕虫）、后门、逻辑炸弹等。



2019 年上半年，CNCERT 新增捕获计算机恶意程序样本数量约 3,200 万个，与 2018 年上半年基本持平，计算机恶意程序传播次数日均达约 998 万次。

一、恶意代码基本概念与技术原理

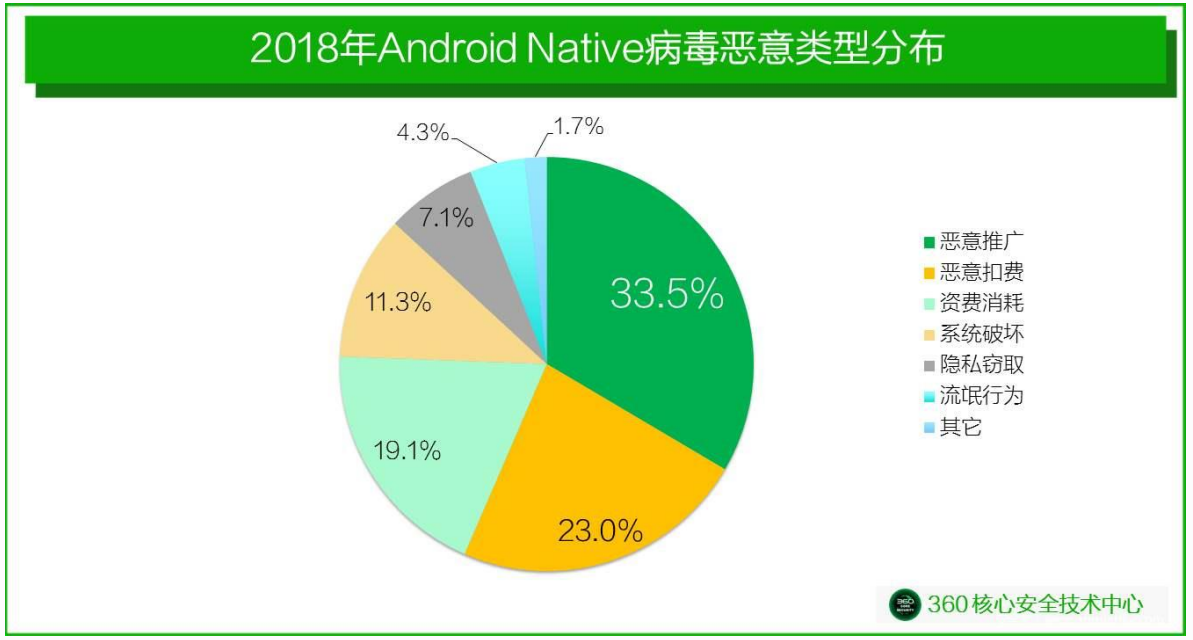
- 狭义的定义——计算机病毒
  - 是一种程序或代码片段，它用修改其它程序的方法将自身的精确拷贝或者可能演化的拷贝插入其它程序，从而感染其它程序。



一、恶意代码基本概念与技术原理

广义的定义

- 凡是人为编制的、干扰计算机正常运行并造成计算机软硬件故障，甚至破坏计算机数据的可自我复制的计算机程序或指令集合。



一、恶意代码基本概念与技术原理

- 起源
  - 冯.诺伊曼：1949年在论文《复杂自动装置的理论及组织的进行》里，已经勾勒出病毒程序的蓝图。他指出存在可以自我复制的程序。

理论基础

一、恶意代码基本概念与技术原理

◘ 起源

- 麦耀莱、维索斯基以及莫里斯：1966年，三个贝尔实验室的年轻技术人编制了一个被称做磁芯大战（Core War）的游戏，目标是通过覆盖对手的程序而将其“杀”掉。最初的游戏是在两个用一种被称作Redcode的汇编语言编写的程序之间展开的。

技术验证

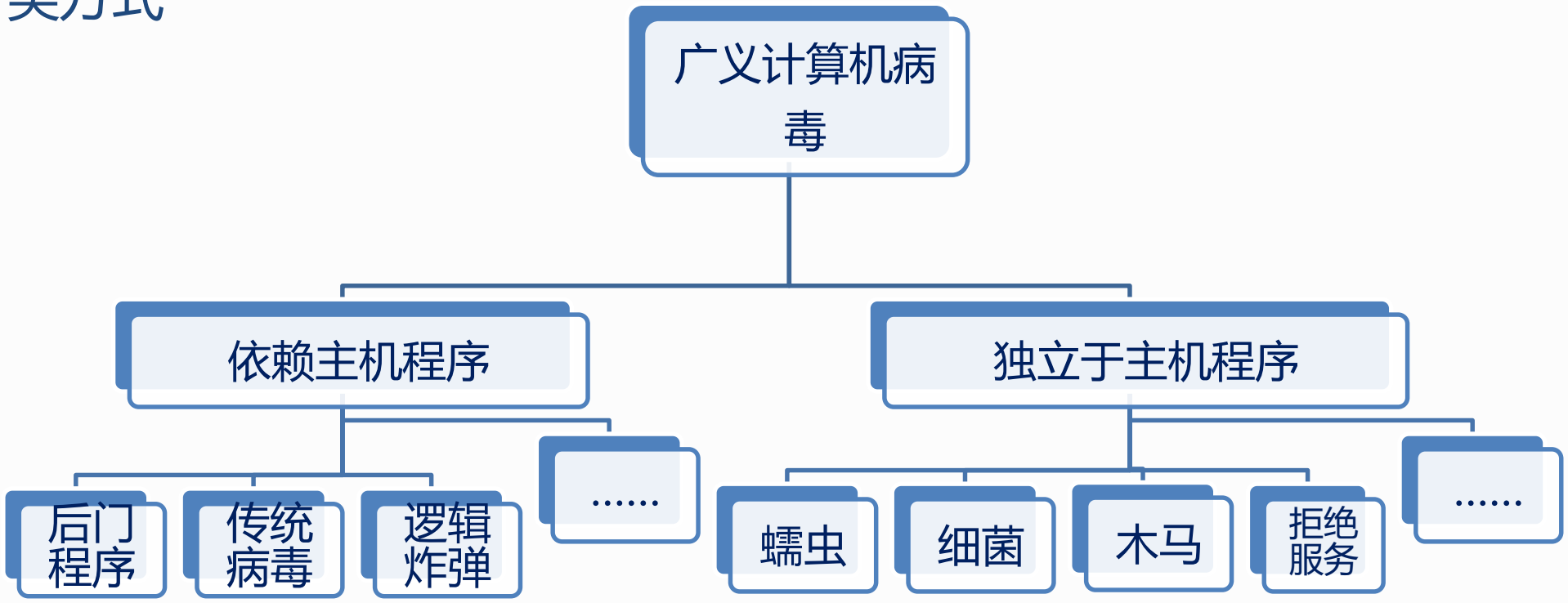
一、恶意代码基本概念与技术原理

- 起源
  - 弗雷德·科恩：1983年，弗雷德·科恩在南加州大学写出了第一个可自我复制并具有感染能力的程序。

工程实现

一、恶意代码基本概念与技术原理

- 分类方式

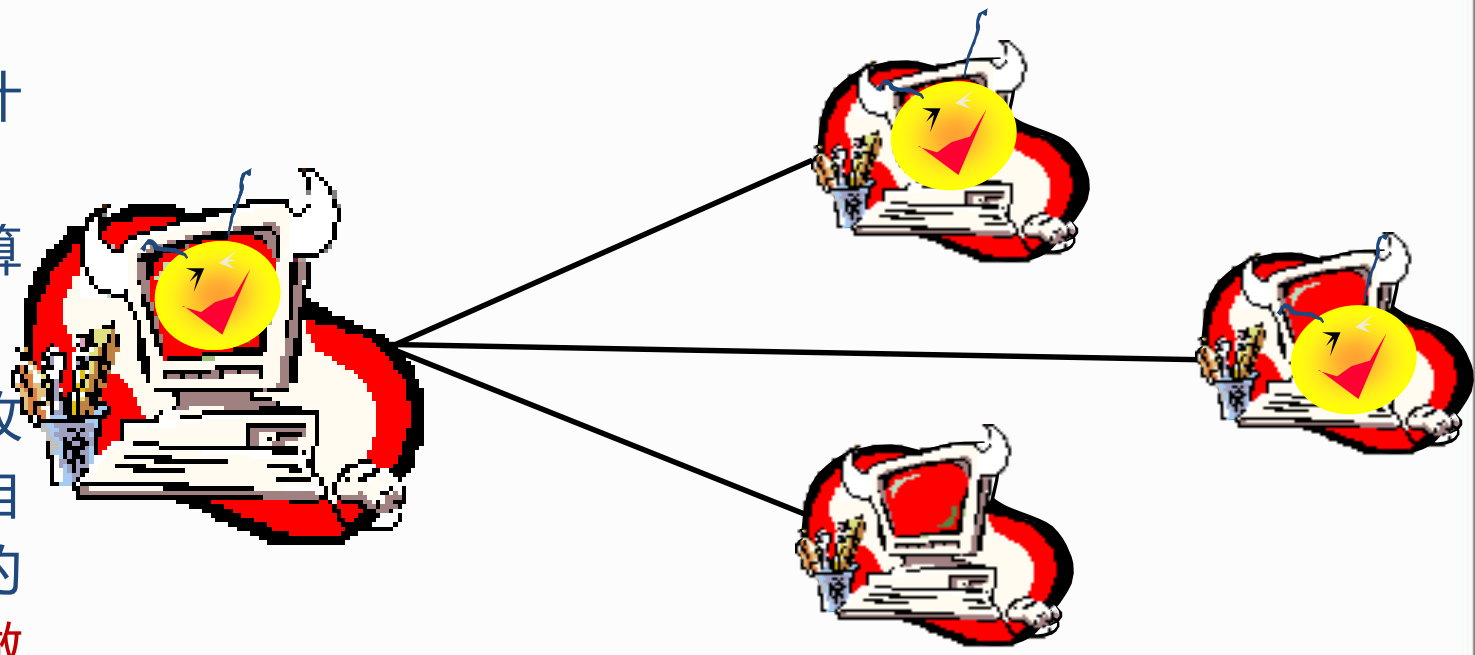


一、恶意代码基本概念与技术原理

- 传统计算机病毒（按传播方式分类）
  - 网络病毒：通过计算机网络传播感染网络中的可执行文件；
  - 文件病毒：感染计算机中的文件（如：ＣＯＭ，ＥＸＥ，ＤＯＣ等）；
  - 引导型病毒：感染软盘启动扇区（Boot）和硬盘的系统引导扇区（ＭＢＲ）；
  - 混合型病毒：是上述三种情况的混合。例如：多型病毒（文件和引导型）感染文件和引导扇区两种目标，这样的病毒通常都具有复杂的算法，它们使用非常规的办法侵入系统，同时使用了加密和变形算法。

一、恶意代码基本概念与技术原理

- 基本特征——传染性
  - 通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪；
  - 传统计算机病毒程序通过修改磁盘扇区信息或文件内容并把自身嵌入到其中的方法达到病毒的传染和扩散。被嵌入的程序叫做宿主程序。



一、恶意代码基本概念与技术原理

- 基本特征—潜伏性与可触发性
  - 第一表现：病毒程序需用专用检测程序才能检查出来
    - 可以躲在磁盘呆上几天，甚至几年；
    - 时机成熟，四处繁殖、扩散
  - 第二表现：病毒内部有一触发机制；
    - 不满足触发条件（时间、日期、文件类型或某些特定数据等），计算机病毒除了传染外不做什么破坏；
    - 满足触发条件，执行预设的破坏操作。

第九讲 网络攻击与防御——恶意代码防治

一、恶意代码基本概念与技术原理

- 基本特征——破坏性
  - 降低计算机系统的工作效率
  - 占用系统资源
  - 毁掉系统的部分数据
  - 破坏全部数据并使之无法恢复
  - 病毒交叉感染导致系统崩溃
  - ……
- 其他特征：不可预见性、衍生性、可执行性、主动性、欺骗性

一、恶意代码基本概念与技术原理

◘ 基本结构

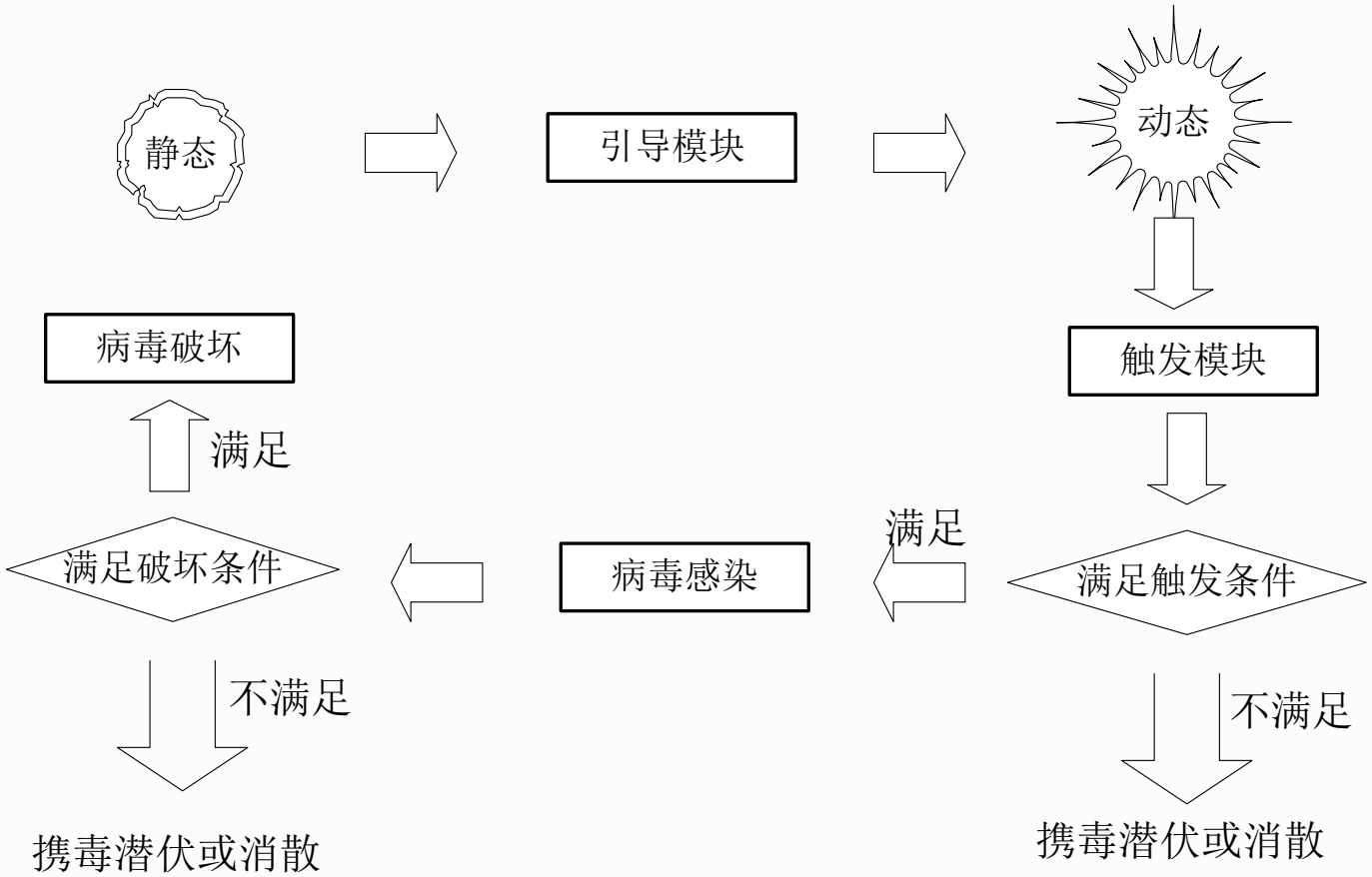
一、恶意代码基本概念与技术原理

◘ 控制逻辑

```
main()
{调用引导功能模块;
A：do
  {寻找传染对象;
  if(传染条件不满足)
      goto A；}
  while(满足传染条件);
  调用传染功能模块;
while(满足破坏条件)
      {激活病毒程序;
      调用破坏功能模块；}
  运行宿主源程序;
  if  不关机
      goto A;
  关机;
}
```

一、恶意代码基本概念与技术原理

工作机制



一、恶意代码基本概念与技术原理

- 引导型病毒——引导模块
  - 磁盘引导区结构
    - 在其盘片的每一面上，以转动轴为轴心、以一定的磁密度为间隔的若干同心圆就被划分成磁道(Track)，每个磁道又被划分为若干个扇区(Sector)，数据就按扇区存放在硬盘上。
    - 记录着磁盘的一些最基本的信息，磁盘的第一个扇区被保留为主引导扇区，它位于整个硬盘的0磁道0柱面1扇区，包括硬盘主引导记录MBR(Main Boot Record)和分区表DPT(Disk Partition Table)以及磁盘的有效标志。

一、恶意代码基本概念与技术原理

◘引导型病毒——引导模块

- 标准的主引导扇区
  - 主引导记录MBR(Main Boot Record)：就是检查分区表是否正确以及确定哪个分区为引导分区，并在程序结束时把该分区的启动程序(也就是操作系统引导扇区)调入内存加以执行。
  - 512字节的主引导扇区里MBR占446个字节（偏移0--偏移1BDH），DPT占64个字节（偏移1BEH--偏移1FDH），最后两个字节“55AA”（偏移1FEH--偏移1FFH）是硬盘有效标志。

一、恶意代码基本概念与技术原理

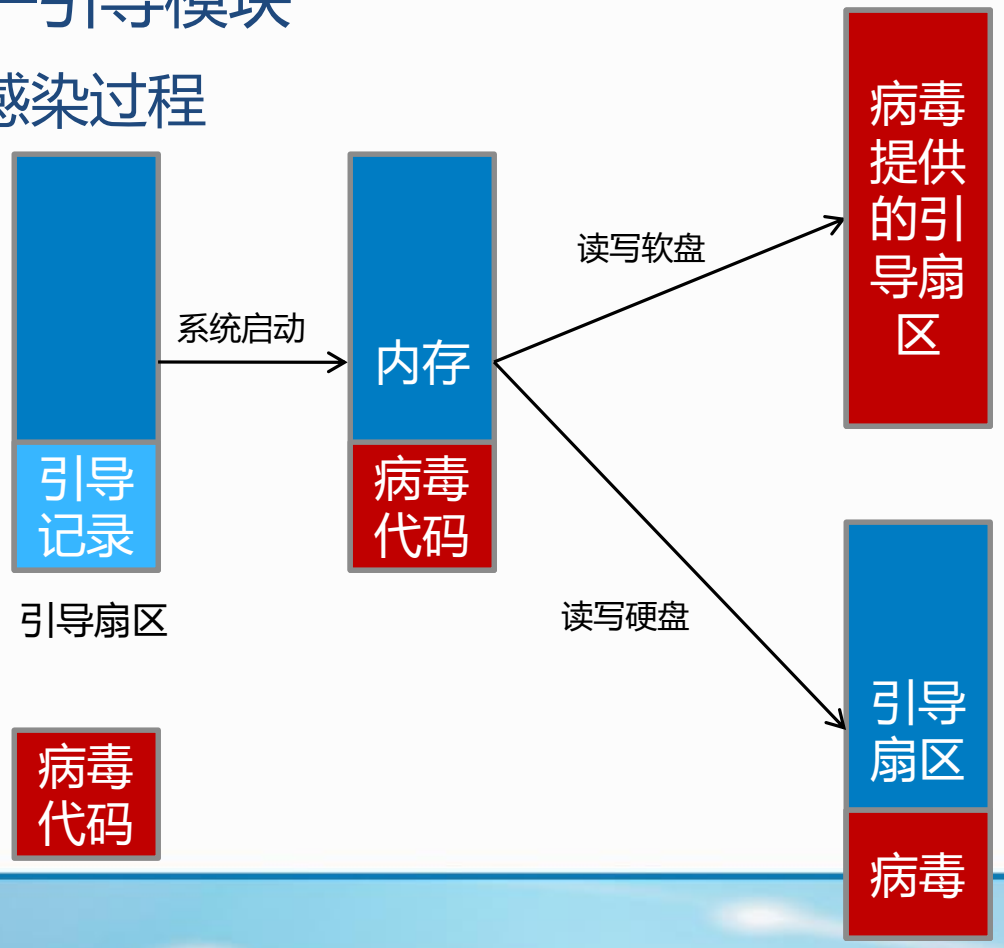
◘引导型病毒——引导模块

- 系统引导过程
  - BIOS 程序首先将存储设备的MBR载入内存，并执行引导记录中的引导程序；
  - 引导程序会将存储设备中的操作系统内核载入内存，进入内核的入口点开始执行；
  - 操作系统内核完成系统的初始化，并允许用户与操作系统进行交互

一、恶意代码基本概念与技术原理

◘引导型病毒——引导模块

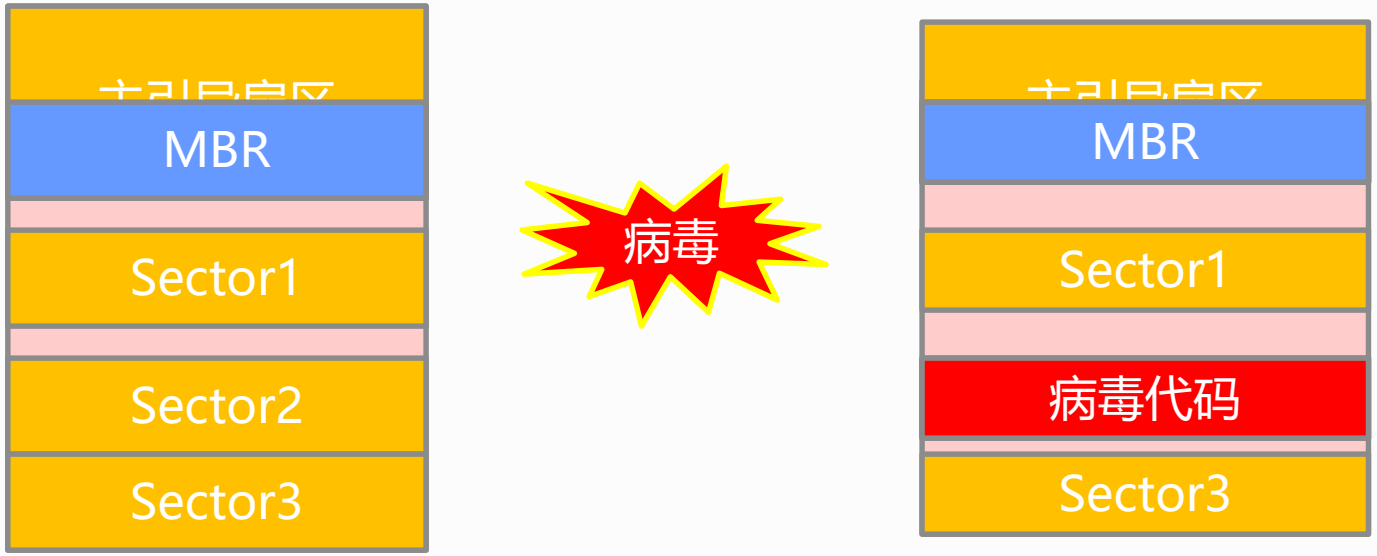
➢ 引导型病毒感染过程



一、恶意代码基本概念与技术原理

◘引导型病毒——引导模块

- 感染后的结果



硬盘

被病毒感染后的硬盘

一、恶意代码基本概念与技术原理

- 引导型病毒——引导模块
  - “石头”病毒：把自己放在主引导记录和第一个引导扇区之间，这中间很多扇区是没有被使用的；
  - “大脑”和“乒乓”病毒：可以分析文件分配表的结构，发现没有被使用的扇区之后，将扇区的标志设置为“坏”，然后将病毒代码放在这些所谓的坏扇区中；
  - 其它病毒：通常将自己放在硬盘的最后一个扇区上（由于现代的硬盘是非常大，最后一个扇区被使用的可能性是非常小的，但是如果在硬盘上同时安装了OS/2操作系统，这些病毒会损坏OS/2操作系统的文件，因为OS/2操作系统会使用这个扇区存放一些系统数据）。现在这种病毒已经比较少。

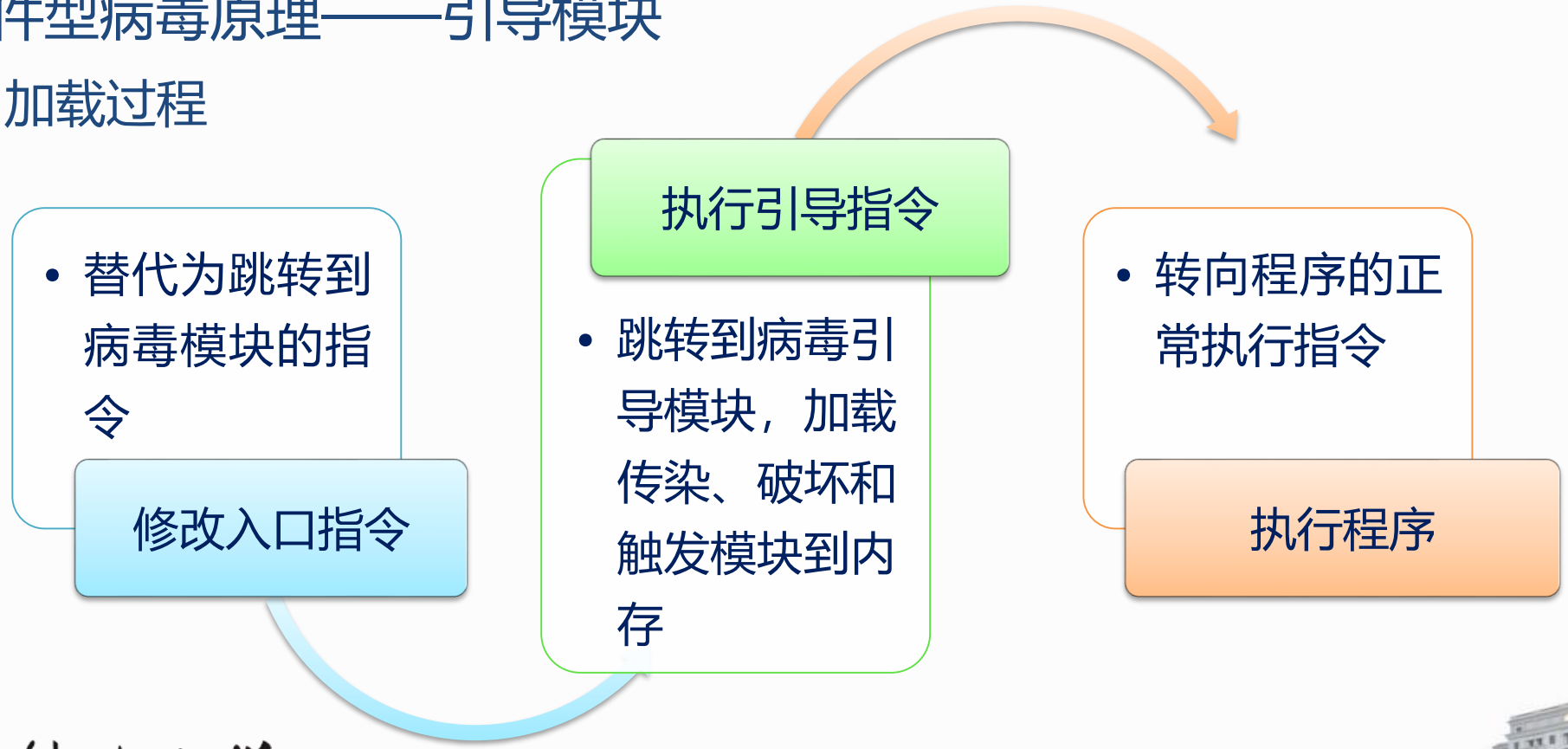
一、恶意代码基本概念与技术原理

- 文件型病毒——引导模块
  - 将代码片段植入可执行文件中，在文件被执行时被装入内存并得到被执行的机会
  - WindowsPE格式可执行文件的执行过程
    - ①Shell（Explorer.exe ）调用CreateProcess函数激活exe程序；②系统创建一个进程内核对象，引用计数置为1；③系统为进程创建一个4GB的进程虚拟地址空间；④PE装载器把exe的代码映射到地址空间，并查找ImportTable引入相关的动态链接库（DLLs ）；⑤系统为进程创建一个主线程，线程得到CPU后，把CS:IP指向.text节中的程序进入点（OEP），此处是一条JMP指令，它跳到XXXCRTStartup函数处执行。

一、恶意代码基本概念与技术原理

文件型病毒原理——引导模块

- 加载过程



一、恶意代码基本概念与技术原理

- 计算机病毒——感染模块
  - 被动传染（静态时）
    - 用户在进行拷贝磁盘或文件时，把一个病毒由一个载体复制到另一个载体上。或者是通过网络上的信息传递，把一个病毒程序从一方传递到另一方。这种传染方式叫做计算机病毒的被动传染。
  - 主动传染（动态时）
    - 以计算机系统的运行以及病毒程序处于激活状态为先决条件。在病毒处于激活的状态下，只要传染条件满足，病毒程序能主动地把病毒自身传染给另一个载体或另一个系统。这种传染方式叫做计算机病毒的主动传染。

一、恶意代码基本概念与技术原理

- 计算机病毒——感染模块
  - 传染过程
    - 系统（程序）运行-〉各种模块进入内存-〉按多种传染方式传染
  - 传染方式
    - 立即传染，即病毒在被执行的瞬间，抢在宿主程序开始执行前，立即感染磁盘上的其他程序，然后再执行宿主程序。
    - 驻留内存并伺机传染，驻留在系统内存中的病毒程序在宿主程序运行结束后，仍可活动，直至关闭计算机。

一、恶意代码基本概念与技术原理

- 计算机病毒——感染模块
  - 传染机理（文件型病毒）
    - 首先根据病毒自己的特定标识来判断该文件是否已感染了该病毒；
    - 当条件满足时，将病毒链接到文件的特定部位，并存入磁盘中；
    - 完成传染后，继续监视系统的运行，试图寻找新的攻击目标。
  - 传染条件（文件型病毒）
    - 加载执行文件
    - 浏览目录过程
    - 创建文件过程

一、恶意代码基本概念与技术原理

- 计算机病毒——破坏模块
  - 破坏对象
    - 系统数据区、文件、内存、系统运行速度、磁盘、CMOS、主板和网络等。
  - 破坏的程度
    - 良性
    - 恶性

一、恶意代码基本概念与技术原理

- 计算机病毒——破坏模块
  - 触发条件
    - 计算机病毒在传染和发作之前，往往要判断某些特定条件是否满足，满足则传染或发作，否则不传染或不发作或只传染不发作，这个条件就是计算机病毒的触发条件。
  - 触发模块的目的：调节病毒的攻击性和潜伏性之间的平衡
    - 大范围的感染行为、频繁的破坏行为可能给用户以重创，但是，它们总是使系统或多或少地出现异常，容易使病毒暴露。
    - 可触发性是病毒的攻击性和潜伏性之间的调整杠杆，可以控制病毒感染和破坏的频度，兼顾杀伤力和潜伏性。

一、恶意代码基本概念与技术原理

- 计算机病毒——破坏模块
  - 常见触发条件
    - 日期触发：黑色星期五、米开朗基罗、切尔洛贝利……
    - 时间触发
    - 键盘触发
    - 感染触发：例如，运行感染文件个数触发、感染序数触发、感染磁盘数触发、感染失败触发等。
    - 启动触发
    - 访问磁盘次数触发
    - CPU型号/主板型号触发

一、恶意代码基本概念与技术原理

- 计算机病毒——传播渠道
  - 电子邮件
    - 例如梅丽莎病毒，第一个通过电子邮件传播的病毒网络共享
  - P2P共享软件
    - 例如WORM_LIRVA.C病毒可以通过Kazaa点对点文件共享软件传即
  - 即时通信软件
    - 例如MSN、QQ病毒
  - 系统中程序的漏洞缺陷
    - 例如震荡波病毒、勒索病毒
  - 未来，物联网，云计算？……

一、恶意代码基本概念与技术原理

- 计算机病毒——传播渠道
  - 电子邮件
    - html格式的信件正文可以嵌入病毒脚本
    - 邮件附件更是可以附带各种不同类型的病毒文件
  - 特点：
    - 利用社会工程学，发信人的地址也许是熟识的；邮件的内容带有欺骗性、诱惑性；
    - 此类病毒的代表有WORM_NETSKY、WORM_BAGLE、WORM_MYDOOM系列等

一、恶意代码基本概念与技术原理

- 计算机病毒——传播渠道
  - 电子邮件传播实例——WORM_MYDOOM.A
    - 发送的邮件所使用的地址为从被感染的系统中收集
    - 默认的Windows地址簿（WAB）
    - WAB，ADB，TBB，DBX，ASP，PHP，SHT，HTM，TXT等类型的文件
  - 使用自身的SMTP引擎发送邮件
    - 从收集到电子邮件地址中提取SMTP服务器名称
    - 例如收集到的邮件地址为 user@sample.com
      - » WORM_MYDOOM.A从邮件地址中提取出域名的部分，然后加上一些前缀（如mx.，mail.，smtp.，mx1.，mxs.，mail1.，relay.，ns.，gate.等）尝试作为邮件的发送服务器地址

一、恶意代码基本概念与技术原理

- 计算机病毒——传播渠道
  - 通过搜索局域网中所有具有写权限的网络共享
  - 将自身进行复制进行传播
  - 可自带口令猜测的字典来破解薄弱用户口令

sharing

一、恶意代码基本概念与技术原理

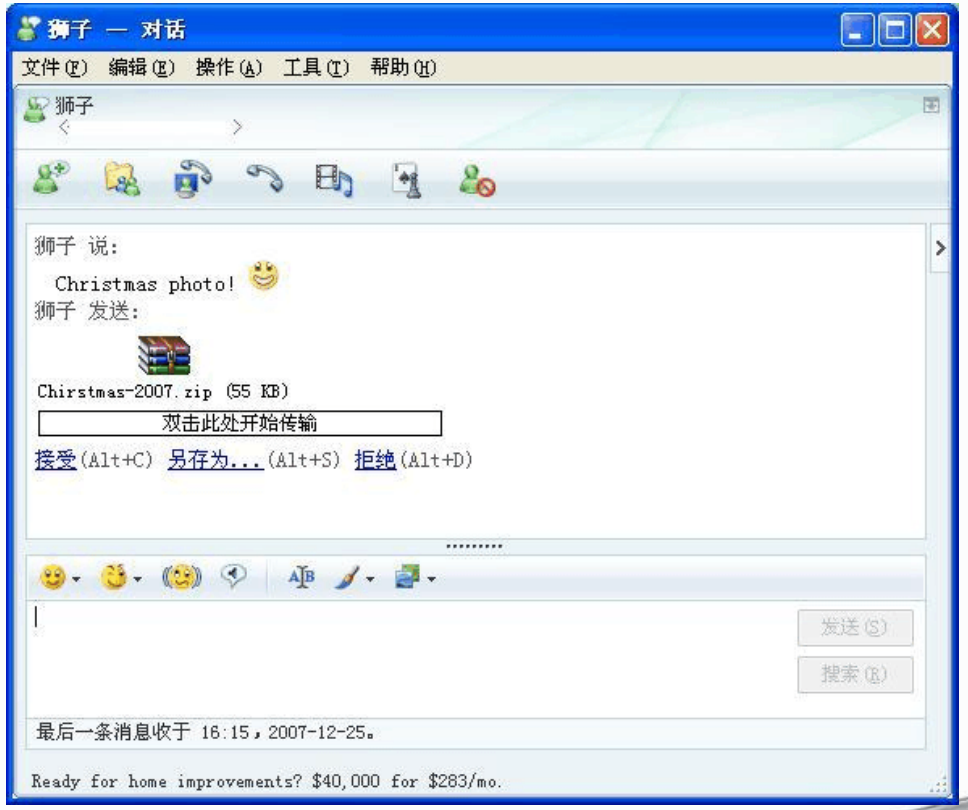
- 计算机病毒——传播渠道
  - 系统漏洞传播方式
    - 利用漏洞，即操作系统的一些缺陷，执行任意的代码
    - 病毒通过对某个存在漏洞的操作系统进行漏洞的利用，达到传播的目的

一、恶意代码基本概念与技术原理

- 计算机病毒——传播渠道
  - P2P共享软件传播方式
    - 生成自身拷贝时使用一些吸引人或是容易被人搜索到的名称，以获得被他人下载的机会
    - 例如WORM_MYDOOM.A生成如下的文件名称就很具有欺骗性： nuke2004，office_crack， rootkitXP， strip-girl-2.0bdcom_patchers， activation_crack，icq2004-final，winamp5

一、恶意代码基本概念与技术原理

- 计算机病毒——传播渠道
  - 即时通信软件传播方式
    - 将自身快速地在即时通信软件之间快速传送
    - 病毒也会同时发送一些欺骗性的文字，使得接收方确信是发送方发送的文件，从而接收并打开



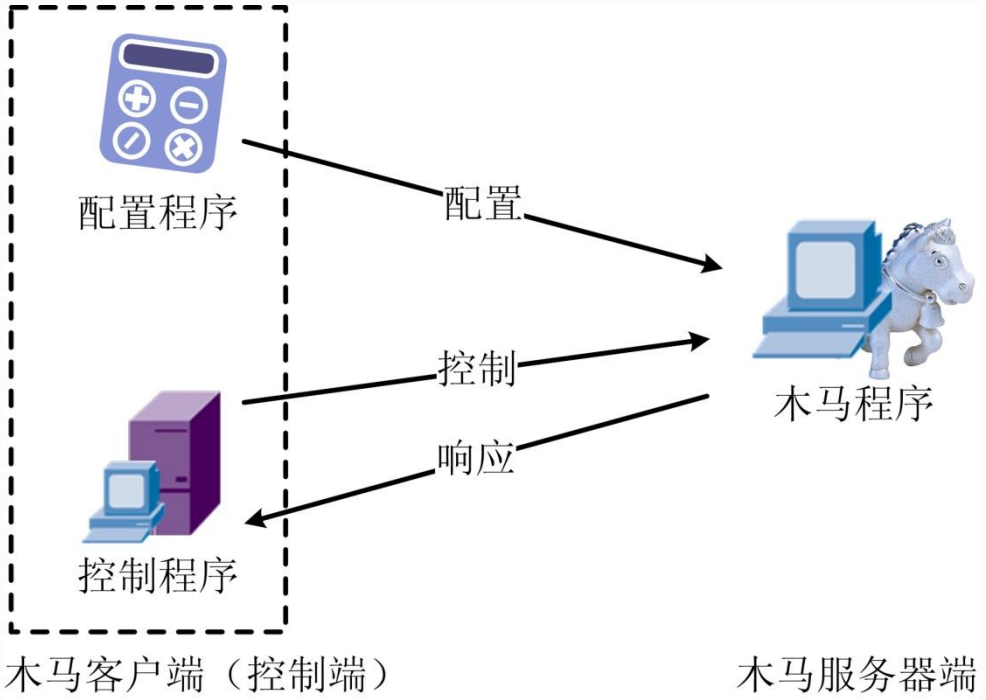
二、特洛伊木马技术原理

- 定义
  - 特洛伊木马(Trojan Horse)，是一种恶意程序，是一种基于远程控制的黑客工具
- 特点
  - 一旦侵入用户的计算机，就悄悄地在宿主计算机上运行，在用户毫无察觉的情况下，让攻击者获得远程访问和控制系统的权限；
  - 进而在用户的计算机中修改文件、修改注册表、控制鼠标、监视/控制键盘，或窃取用户信息

二、特洛伊木马技术原理

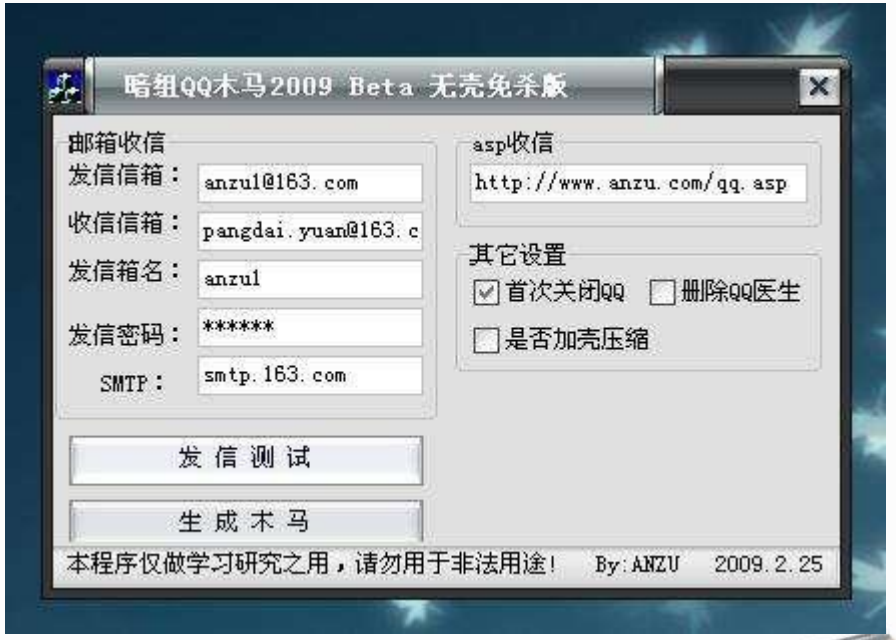
结构

- 木马系统软件一般由木马配置程序、控制程序和木马程序(服务器程序)三部分组成。



二、特洛伊木马技术原理

- 入侵过程
  - 步骤一：配置木马
    - 木马伪装，即让木马在服务端尽可能隐藏得更隐蔽
    - 信息反馈，即设置信息反馈的方式或地址，如设置信息反馈的邮件地址、QQ号、MSN号等
  - 在释放木马之前可以配置木马，释放之后也可远程配置木马



二、特洛伊木马技术原理

- 入侵过程
  - 步骤二：传播木马
    - 以邮件附件的形式传播。控制端将木马伪装之后添加到附件中，发送给收件人
    - 通过MSN、QQ等聊天工具软件传播。在进行聊天时，利用文件传送功能发送伪装过的木马程序给对方
    - 通过提供软件下载的网站(Web/FTP/BBS)传播
    - 通过带木马的磁盘和光盘进行传播
    - 木马可以通过Script、ActiveX及Asp、CGI交互脚本的方式植入
    - 木马可以利用系统的一些漏洞进行植入
    - 通过其他的病毒或蠕虫传播

二、特洛伊木马技术原理

- 入侵过程
  - 步骤三：启用木马
    - 服务器端的用户运行木马或捆绑木马的程序后，木马就会自动进行安装和隐藏；
    - 在注册表、启动组等位置设置木马的触发启动条件，完成木马服务器的安装；
    - 附加或者捆绑在系统程序或者其它应用程序上，或者干脆替代它们运行这些系统程序的时候就会激活木马（比如修改系统文件explorer.exe在其中加入木马）；
    - 木马程序被激活后，进入内存，开启并监听预先定义的木马端口，准备与控制端建立连接。

二、特洛伊木马技术原理

- 入侵过程
  - 步骤四：信息反馈
    - 设计成熟的木马都有一个信息反馈机制；
    - 信息反馈机制是指木马成功安装后会收集一些服务端的软硬件信息，并通过E-MAIL，IRC等方式告知控制端攻击者；
    - 从反馈信息中控制端可以知道使用的操作系统，系统目录，硬盘分区情况，系统口令等，在这些信息中，最重要的是服务端IP。

二、特洛伊木马技术原理

◘ 入侵过程

➢步骤五：建立连接

– 控制端要与服务端建立连接必须知道服务端的木马端口和IP地址

– 由于木马端口是事先设定的，为已知项，所以最重要的是如何获得服务端的IP地址

– 获得服务端的IP地址的方法主要有两种：信息反馈和IP扫描。

拓展学习

- 了解冰河木马的工作原理和过程。（不需要提交作业，第四次实验内容为mini木马程序的编制）

三、计算机蠕虫技术原理

定义

- 蠕虫是一种通过网络自动传播它自身功能的拷贝或它的某些部分到其他的计算机系统中的恶意代码。

特点

- 可利用系统缺陷进行自动传播
- 不需要宿主

三、计算机蠕虫技术原理

◘ 功能结构

- 主程序+引导程序
  - 主程序的主要功能是搜索和扫描，这个程序能够读取系统的公共配置文件，获得与本机联网的客户端信息，检测到网络中的哪台机器没有被占用，从而通过系统的漏洞，将引导程序建立到远程计算机上
  - 引导程序实际上是蠕虫病毒主程序（或一个程序段）自身的一个副本

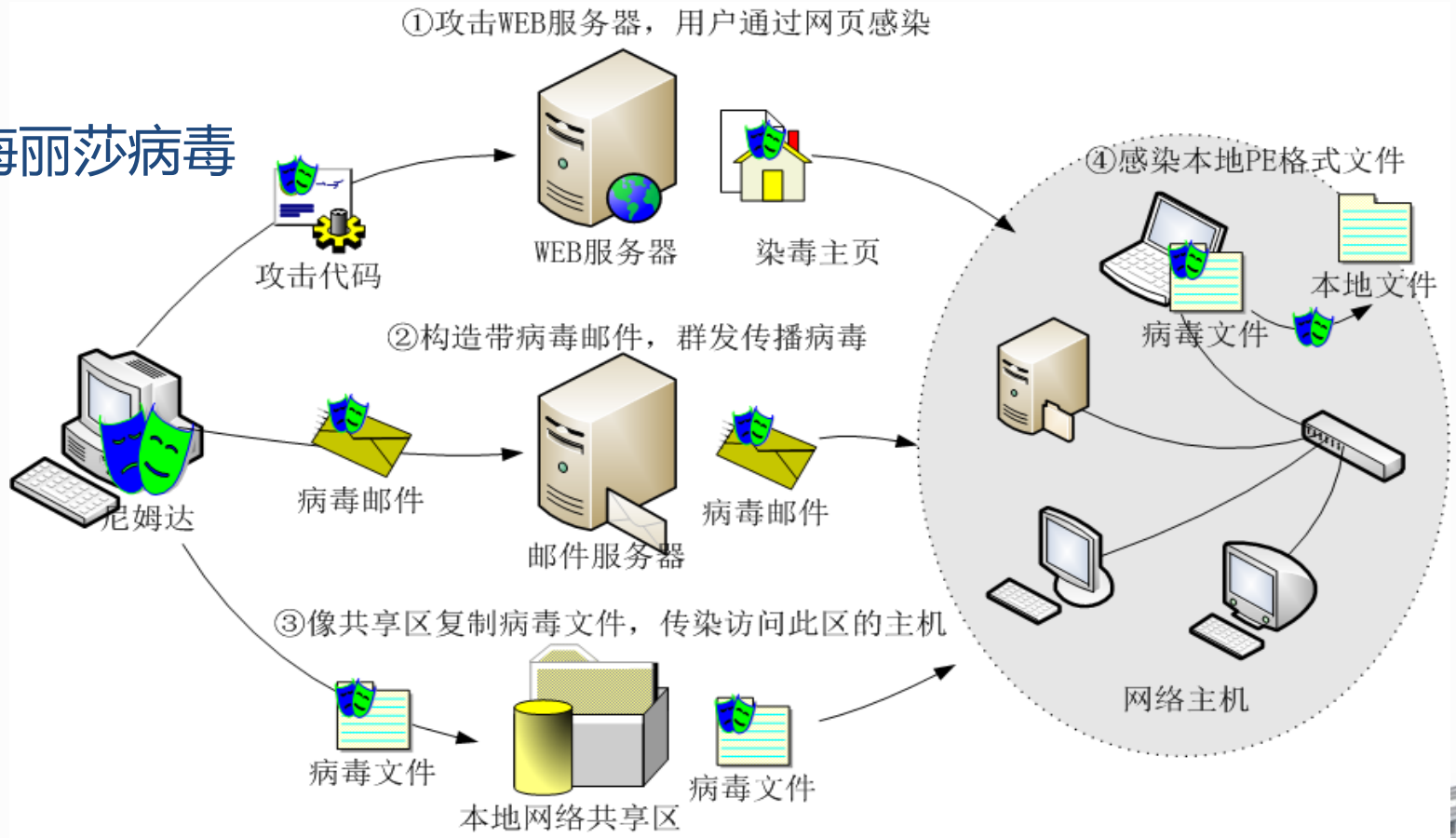
三、计算机蠕虫技术原理

工作模式

- 传播策略
  - 传播目标：现在流行的蠕虫采用的传播技术目标，一般是尽快地传播到尽量多的计算机中；
  - 传播手段：随机选取某一段IP地址，然后对这一地址段上的主机进行扫描，发现活跃主机并尝试利用漏洞传输；
- 没有优化的扫描程序可能会不断重复上面这一过程，大量蠕虫程序的扫描引起严重的网络拥塞

三、计算机蠕虫技术原理

- 工作模式
  - 实例——梅丽莎病毒



三、计算机蠕虫技术原理

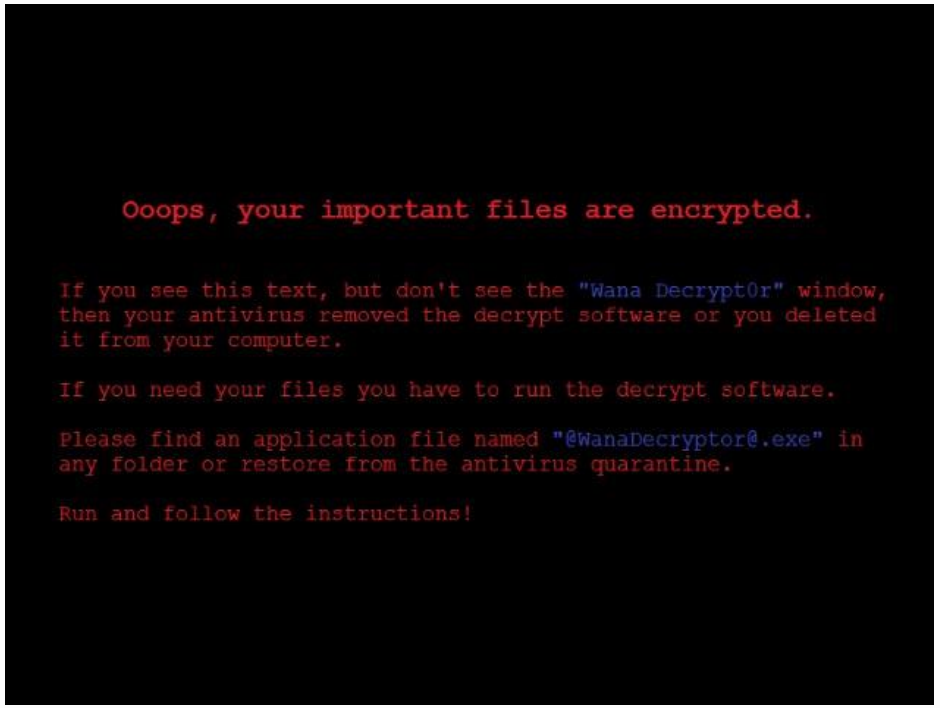
□ 计算机蠕虫与传统病毒对比

	病　　毒	蠕　　虫
存在形式	寄生	独立个体
复制机制	插入到宿主程序(文件)中	自身的拷贝
传染机制	宿主程序运行	系统存在漏洞(Vulnerability)
搜索机制(传染目标)	主要是针对本地文件	主要针对网络上的其它计算机
触发传染	计算机\使用者	程序自身
影响重点	文件系统	网络性能、系统性能
防治措施	从宿主程序中摘除	漏洞补丁

蠕虫的定义中强调了自身副本的完整性和独立性，这也是区分蠕虫和病毒的重要因素。可以通过简单的观察攻击程序是否存在载体来区分蠕虫与病毒。

三、计算机蠕虫技术原理

- 典型恶意代码实例分析——勒索病毒WannaCry



病毒名称：Trojan-Ransom.Win32.Wanna.m

所属家族：木马/勒索/蠕虫

MD5: DB349B97C37D22F5EA1D1841E3C89EB4

SHA1:

E889544AFF85FFAF8B0D0DA705105DEE7C97FE26

CRC32: 9FBB1227

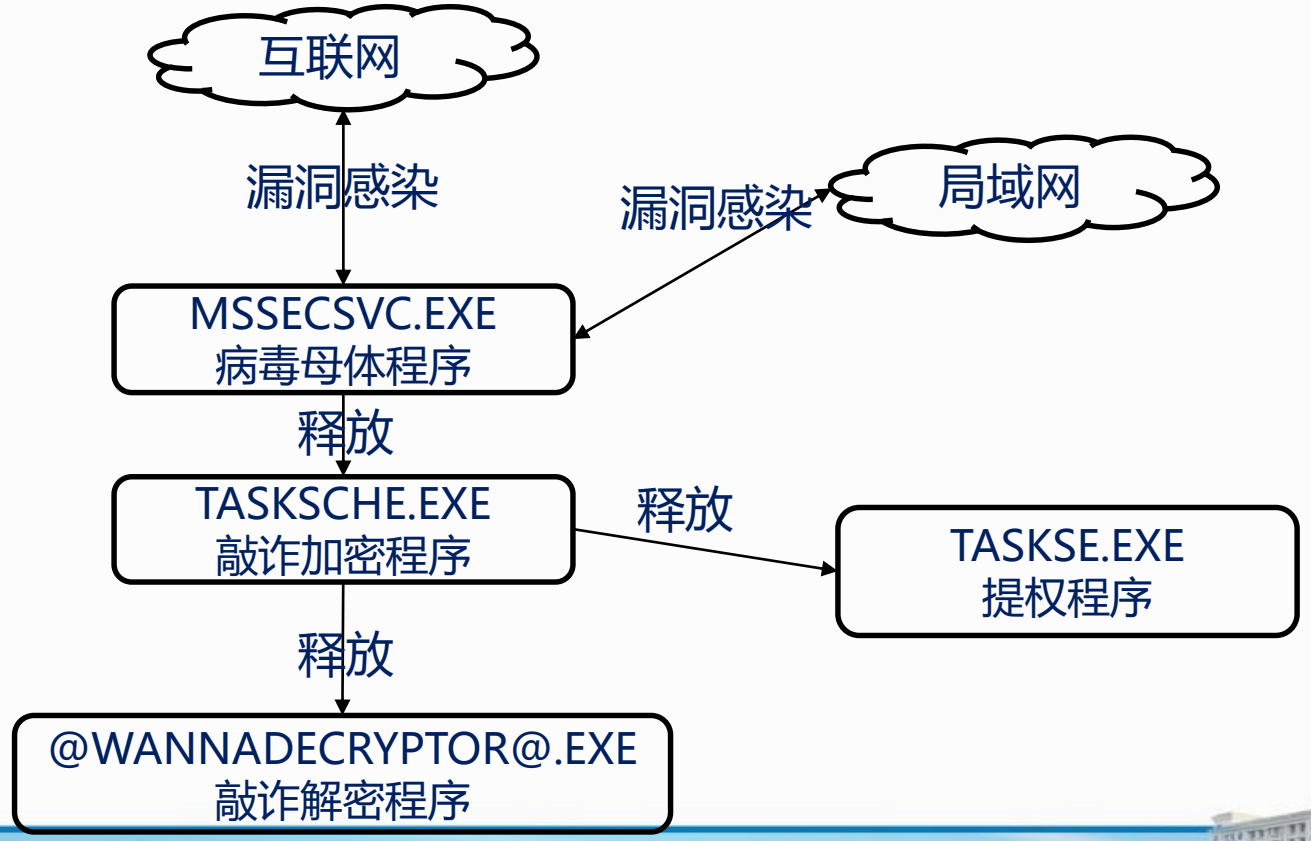
三、计算机蠕虫技术原理

- 典型恶意代码实例分析——勒索病毒WannaCry
  - 病毒主要行为
    - 扫描局域网和公网，寻找存在MS17-010漏洞的主机进行传播；
    - 释放主程序文件，包括加解密器、说明文件、语言文件等；
    - 在内存中加载加密器模块，加密执行类型文件，加密完成后启动解密模块；
    - 解密模块启动后，设置桌面背景显示勒索信息，并定期弹出窗口显示付款账号等信息。

被加密文件后缀为.WNCRY

三、计算机蠕虫技术原理

- 典型恶意代码实例分析——勒索病毒WannaCry
  - 工作逻辑



三、计算机蠕虫技术原理

□ 典型恶意代码实例分析——勒索病毒WannaCry

➢ 执行过程：①尝试连接 http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

```
15  qmemcpy(&szUrl, aHttpWww_iuqerf, 0x39u);      // http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
16  v8 = 0;
17  v9 = 0;
18  v10 = 0;
19  v11 = 0;
20  v12 = 0;
21  v13 = 0;
22  v14 = 0;
23  v4 = InternetOpenA(0, 1u, 0, 0, 0);
24  v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// 尝试连接
25  if ( v5 )
26  {
27    InternetCloseHandle(v4);                    // 连接成功什么也不做，返回0
28    InternetCloseHandle(v5);
29    result = 0;
30  }
31  else
32  {
33    InternetCloseHandle(v4);                    // 连接失败
34    InternetCloseHandle(0);
35    startAddr();                                // 入口
36    result = 0;
37  }
38  return result;
```

传播控制开关

三、计算机蠕虫技术原理

- 典型恶意代码实例分析——勒索病毒WannaCry
  - 执行过程：②创建服务启动,每次开机都会自启动

```
11  ServiceStatus.dwWaitHint = 0;
12  result = RegisterServiceCtrlHandlerA(ServiceName, HandlerProc);// "mssecsvc2.0"
13  hServiceStatus = result;
14  if ( result )
15  {
16    ServiceStatus.dwCurrentState = 4;
17    ServiceStatus.dwCheckPoint = 0;
18    ServiceStatus.dwWaitHint = 0;
19    SetServiceStatus(result, &ServiceStatus);
20    start_worm();                          // 创建服务运行 执行蠕虫行为
21    Sleep(86400000u);
22    ExitProcess(1u);
23  }
24  return result;
25}
```

设置开机启动

三、计算机蠕虫技术原理

◘ 典型恶意代码实例分析——勒索病毒WannaCry

➢ 执行过程：③从内存中读取MS17_010漏洞利用代码,payload分为x86和x64两个版本

```
{
  v1 = 0;
  do
  {
    payload = &payload_x86;                    // 读取MS17_010利用漏洞
    if ( v1 )
      payload = &payload_x64;
    v3 = *(DWORD **)&FileName[4 * v1 + 260];
    (&v11)[v1] = v3;
    qmemcpy(v3, payload, v1 != 0 ? 0xC8A4 : 0x4060);
    (&v11)[v1] = (DWORD *)((char *)(&v11)[v1] + (v1 != 0 ? 0xC8A4 : 0x4060));
    ++v1;
  }
  while ( v1 < 2 );
```

读取攻击载荷

EternalBlue(MS17-010)是在Windows的SMB服务处理SMB v1请求时发生的缓冲区溢出漏洞，这个漏洞导致攻击者在目标系统上可以执行任意代码。

三、计算机蠕虫技术原理

◘ 典型恶意代码实例分析——勒索病毒WannaCry

➢ 执行过程：④分别创建两个线程，扫描内网和外网，进行蠕虫传播感染

```
void *v3; // eax@5

result = sub_407B90();                          // 初始化网络，获取payload
if ( result )
{
  v1 = (void *)beginthreadex(0, 0, infect_lan, 0, 0, 0);// 内网
  if ( v1 )
    CloseHandle(v1);
  v2 = 0;
  do
  {
    v3 = (void *)beginthreadex(0, 0, infect_wan, v2, 0, 0);// 外网
    if ( v3 )
      CloseHandle(v3);
    Sleep(2000u);
    ++v2;
  }
  while ( v2 < 128 );
  result = 0;
}
return result;
}
```

自动传播

三、计算机蠕虫技术原理

□ 典型恶意代码实例分析——勒索病毒WannaCry

- 执行过程：⑤对于内网,则直接扫描当前计算机所在的网段进行感染

```
47  SizePointer = 0;
48  if ( GetAdaptersInfo(0, &SizePointer) != 111 )
49    return 0;
50  if ( !SizePointer )
51    return 0;
52  v2 = LocalAlloc(0, SizePointer);
53  v3 = v2;
54  hMem = v2;
55  if ( !v2 )
56    return 0;
57  if ( GetAdaptersInfo((PIP_ADAPTER_INFO)v2, &SizePointer) )
58  {
59    LocalFree(v3);
60    return 0;
```

内网传播

三、计算机蠕虫技术原理

□ 典型恶意代码实例分析——勒索病毒WannaCry

- ➢ 执行过程：⑥对于外网，随机生成公网IP，尝试连接445端口，成功，则对该地址进行漏洞攻击

```
.text:004076B0          push    esi             ; name
.text:004076B1          mov     esi, [esp+4+s]
.text:004076B5          push    esi             ; s
.text:004076B6          call    connect_445     ; 如果有开放445端口
.text:004076BB          add     esp, 4
.text:004076BE          test    eax, eax
.text:004076C0          jle     short loc_407702
.text:004076C2          push    0
.text:004076C4          push    0
.text:004076C6          push    esi
.text:004076C7          push    offset ms17_010_attack ; 如果445端口连接成功，则对该地址进行漏洞攻击
.text:004076CC          push    0
.text:004076CE          push    0
.text:004076D0          call    ds:_beginthreadex
.text:004076D6          mov     esi, eax
.text:004076D8          add     esp, 18h
.text:004076DB          test    esi, esi
.text:004076DD          jz      short loc_407702
.text:004076DF          push    927C0h          ; dwMilliseconds
```

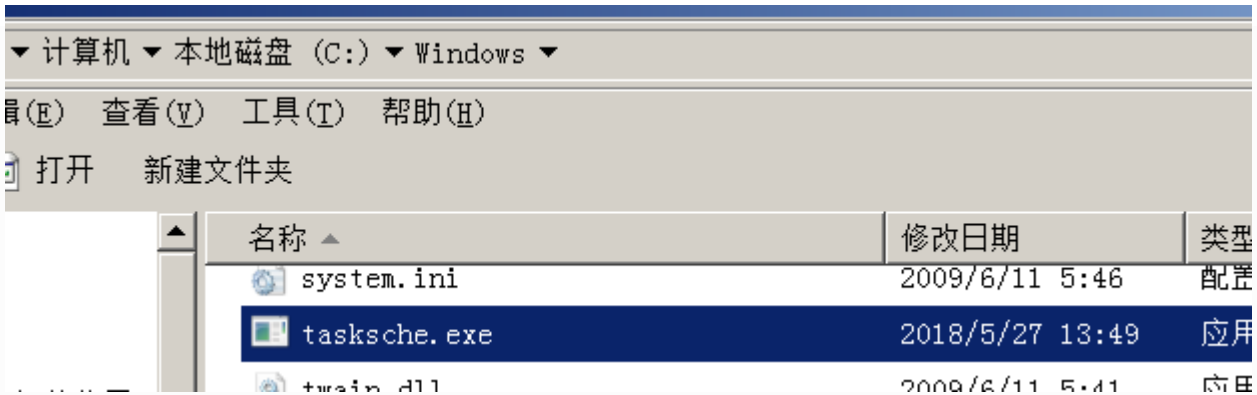
外网传播

三、计算机蠕虫技术原理

◘ 典型恶意代码实例分析——勒索病毒WannaCry

➢ 执行过程：⑦写入“C:\windows\tasksche.exe”并执行。

```
v16 = 129;
if ( CreateProcessA(0, &Dest, 0, 0, 0, 0x8000000, 0, 0, &v14, &v10) )// 创建进程
{
  CloseHandle(v11);
  CloseHandle(v10);
}
}
```



权限提升

三、计算机蠕虫技术原理

- 典型恶意代码实例分析——勒索病毒WannaCry
  - 执行过程：⑧加载 t.wncy 文件, 并执行t.wncy的 TaskStart函数。

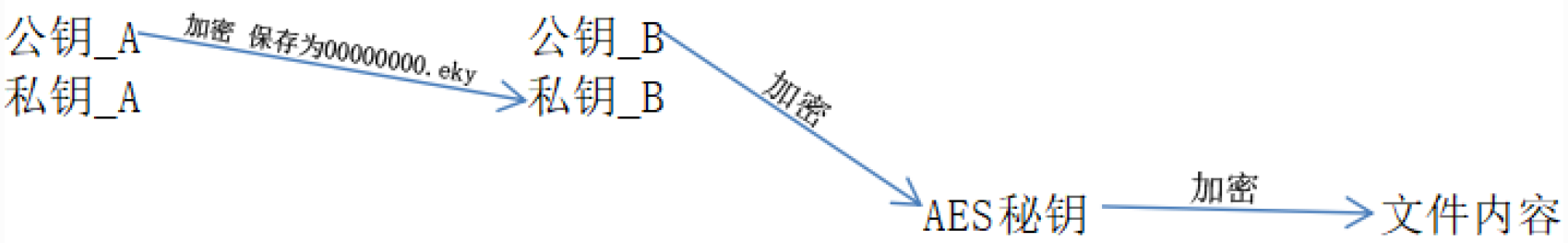
```
v6 = (void *)sub_4014A6(&v10, aT_wnry, (int)&v15);
if ( v6 )
{
  v7 = sub_4021BD(v6, v15);
  if ( v7 )
  {
    TaskStart = (void (__stdcall *)(_DWORD, _DWORD))sub_402924(v7, asc_40F4E8);
    if ( TaskStart )
      TaskStart(0, 0);
  }
}
}
```

启动加密

三、计算机蠕虫技术原理

□ 典型恶意代码实例分析——勒索病毒WannaCry

- 执行过程：⑧判断文件类型，创建AES密钥加密文件。



加密过程

加密文件的算法是AES， 而AES秘钥被RSA公钥_B加密， 私钥_B 被RSA公钥A 加密，而私钥_A在攻击者手里。

四、恶意代码防治技术

- 技术的发展过程
  - 第一代反病毒技术
    - 采用单纯的病毒特征代码分析，清除染毒文件中的病毒
  - 第二代反病毒技术
    - 采用静态广谱特征扫描技术检测病毒，可以检测变形病毒，但是误报率高

四、恶意代码防治技术

◘ 技术的发展过程

- ➢第三代反病毒技术
  - 将静态扫描技术和动态仿真跟踪技术结合起来，将查找病毒和清除病毒合二为一。
- ➢第四代反病毒技术
  - 基于病毒家族体系的命名规则、基于多位CRC校验和扫描机理、启发式智能代码分析模块、动态数据还原模块(能查出隐蔽性极强的压缩加密文件中的病毒)、内存解毒模块、自身免疫模块等先进的解毒技术

目前杀毒软件仍然是以特征检测杀毒为主，行为启发式扫描检测技术为辅

四、恶意代码防治技术

- 技术分类
  - 病毒预防技术
  - 病毒检测技术
  - 病毒消除技术
  - 病毒免疫技术

四、恶意代码防治技术

- 病毒检测技术
  - 手工检测
    - 利用IDA、OllyDBGDebug、PCTools、SysInfo、WinHex等工具软件进行病毒的检测，这种方法比较复杂，费时费力
    - 可以剖析病毒、可以检测一些自动检测工具不能识别的新病毒

最为可靠

四、恶意代码防治技术

◘ 病毒检测技术

- ➢ 自动检测
  - – 利用一些专业诊断软件来判断引导扇区、磁盘文件是否有毒的方法
  - – 自动检测比较简单，一般用户都可以进行，但需要较好的诊断软件
  - – 可方便地检测大量的病毒，自动检测工具的发展总是滞后于病毒的发展

便捷高效

四、恶意代码防治技术

病毒检测技术

- 自动检测技术实例——特征值检测
  - 一些常见的病毒具有很明显的特征，即病毒中含有特殊的字符串。用抗病毒软件检查文件中是否存在这些特征，从而判定是否发生感染
  - 计算机病毒的特征值有别于病毒标识，特征值是指一种病毒有别于另一种病毒的字符串，有时简称特征串。

setup.exe

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00001A00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	07	00	
00001A10	03	00	00	00	48	00	00	80	04	00	00	00	78	00	00	80	H € x €
00001A20	05	00	00	00	90	00	00	80	06	00	00	00	A8	00	00	80	€ ¨ €
00001A30	09	00	00	00	C0	00	00	80	0E	00	00	00	D8	00	00	80	À € Ø €
00001A40	18	00	00	00	F8	00	00	80	00	00	00	00	00	00	00	00	ø €
00001A50	00	00	00	00	00	00	04	00	01	00	00	00	10	01	00	80	€
00001A60	02	00	00	00	28	01	00	80	03	00	00	00	40	01	00	80	(€ @ €
00001A70	04	00	00	00	58	01	00	80	00	00	00	00	00	00	00	00	X €
00001A80	00	00	00	00	00	00	01	00	6D	00	00	00	70	01	00	80	m p €
00001A90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	
00001AA0	67	00	00	00	88	01	00	80	00	00	00	00	00	00	00	00	g ˆ €
00001AB0	00	00	00	00	00	00	01	00	07	00	00	00	A0	01	00	80	€
00001AC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	
00001AD0	6D	00	00	00	B8	01	00	80	00	00	00	00	00	00	00	00	m ¸ €
00001AE0	00	00	00	00	00	00	02	00	6B	00	00	00	D0	01	00	80	k Ð €

局限性?

四、恶意代码防治技术

◘ 病毒检测技术

- ➢ 自动检测技术实例——校验和检测技术
  - – 根据正常文件的信息(包括文件名称、大小、时间、日期及内容)，计算其校验和
  - – 定期地或每次使用文件前，检查文件现有信息算出的校验和与原来保存的校验和是否一致

局限性?

四、恶意代码防治技术

- 病毒检测技术
  - 自动检测技术实例——行为监测法检测技术
    - 利用病毒的特有行为特性监测病毒的方法，称为行为监测法，也称为人工智能陷阱法
    - 通过对病毒多年的观察、研究，人们发现病毒有一些行为，是病毒的共同行为，而且比较特殊，在正常程序中，这些行为比较罕见。
  - 常见的病毒行为特性
    - 占用INT 13H，对可执行文件做写入动作，病毒程序与宿主程序的切换，搜索API函数地址

四、恶意代码防治技术

◘ 病毒检测技术

- ➢ 启发式代码扫描技术
  - – 源于人工智能技术，是基于给定的判断规则和定义的扫描技术
  - – 若发现被扫描程序中存在可疑的程序功能指令，则作出存在病毒的预警或判断
- ➢ 启发式扫描类型
  - – 静态启发式
  - – 动态启发式

四、恶意代码防治技术

- 病毒检测技术
  - 启发式代码扫描技术——实例
    - 文件是否加密？1.5分
      - » 加密的文件往往很可疑，但别忘了一些正常软件防盗版措施也会进行加密
    - 是否打开一个端口并监听？2分
      - » 这类行为可能比加密更可疑（需注意这里的分值只是一个例子用来展示打分的概念）
    - 是否对一个已经存在的文件进行写入操作？3分
      - » 根据写入对象的不同这个分值也可能不同
    - 是否有写入注册表行为？1分
    - ……

结束语

感 谢 聆 听!

特别说明：PPT中所有来自于网络的图片和素材仅用于教学，并保证在未经原作者同意的情况下，不用于任何商业目的。