西安电子科技大学 XIDIAN UNIVERSITY
计算机科学与技术学院 School of Computer Science and Technology
国家示范性软件学院 National Pilot School of Software Engineering

计算机安全导论

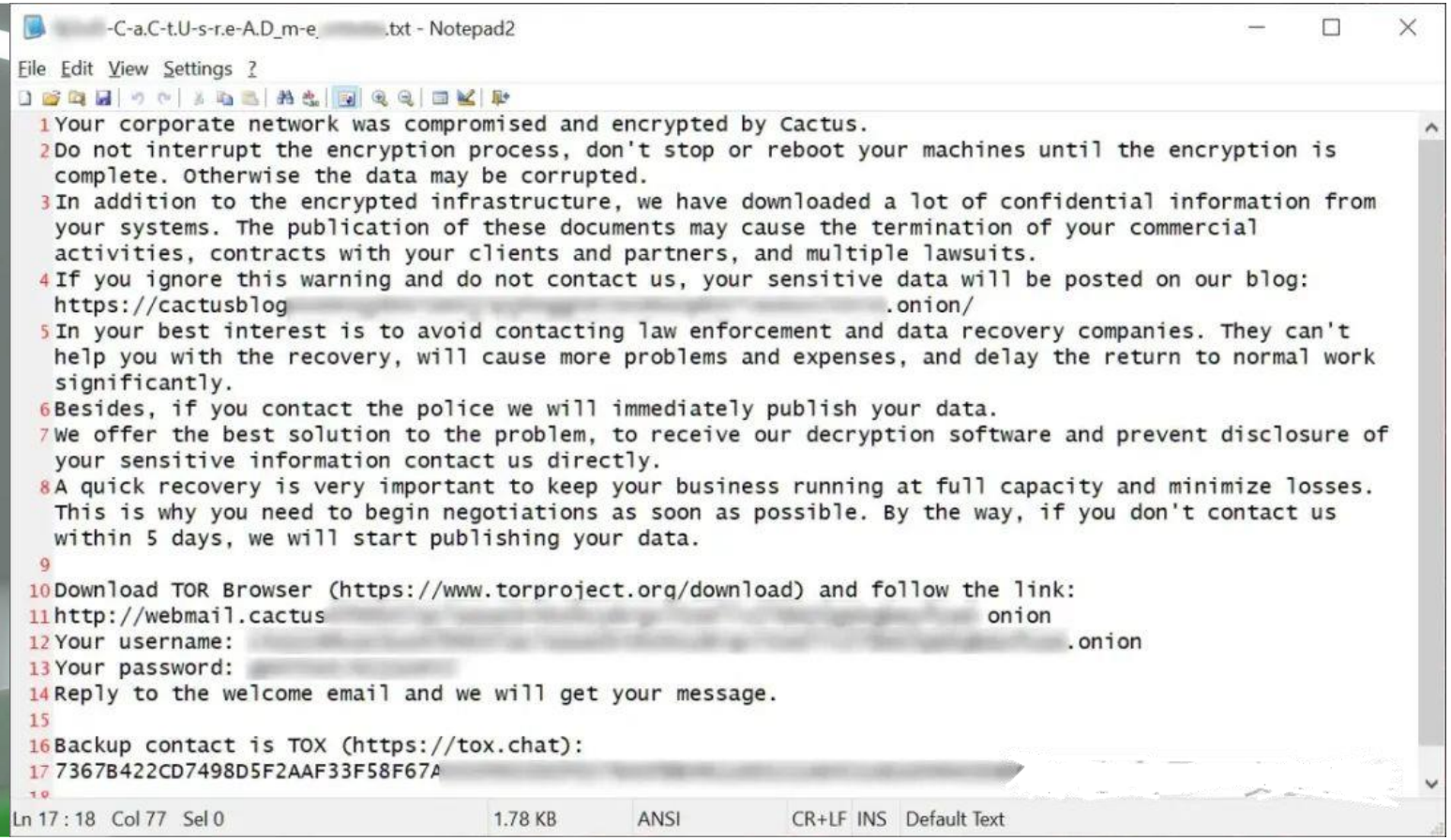
第5章
恶　意　软　件

主讲人：张志为

二〇二四年秋季学期

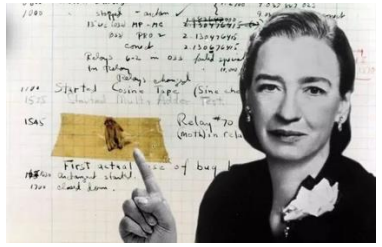
- 10月17日，全球电机制造巨头**尼得科(Nidec Corporation)** 证实今年8月遭受了勒索软件攻击，被窃取5万余份文件，包括商业合同、采购文件等内部文件，**在拒绝支付赎金后，勒索软件团伙公开了所窃取的数据信息**

- 11月4日，全球能源管理和自动化巨头**施耐德电气**证实遭遇网络攻击，此次事件中，黑客从服务器窃取了40GB的数据，包括内部开发人员的姓名、电子邮件地址、访问权限等敏感信息，**这已经是施耐德电气在2024年内第二次遭遇勒索攻击**



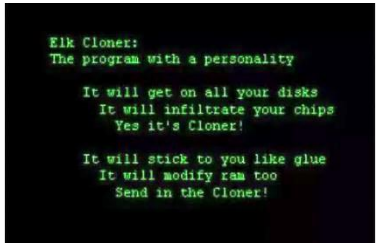
安全攻击威胁与防御的博弈

世界上第一个“Bug”
被Grace Hooper发现



1944年

世界上第一个计算机病毒
Elk Cloner引导区病毒



1981年

世界上第一个计算机木马
PC-Write木马

1986年

世界上第一个网络蠕虫
被Robert Morris意外制造

1988年

第三次工业革命

程序调试 减少软件设计与实现漏洞

病毒查杀 已知的恶意软件

防火墙 防御边界安全

入侵检测 关注来自系统内外部安全威胁

安全防御与攻击的持续较量

2020年代

网络信息系统安全深远影响民生与国际关系 2010年代

人类进入万物互联

万物智能新时代

2021年

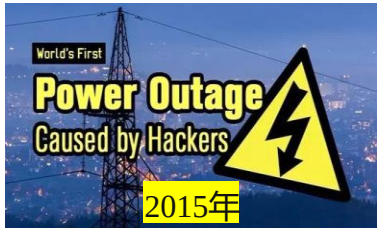
2020年

2017年

2013年

2022年

2019年



2015年

提纲

PART 1 内部攻击

PART 2 计算机病毒

PART 3 恶意软件攻击

PART 4 入侵隐私软件

PART 5 对策

提纲

PART 1 内部攻击

PART 2 计算机病毒

PART 3 恶意软件攻击

PART 4 入侵隐私软件

PART 5 对策

内部攻击Insider attack

- 内部攻击是指控制和保护资产的内部人员利用安全漏洞进行的攻击
- 在恶意软件Malware中，内部攻击是指由某位程序员在软件系统中创建的安全漏洞

后门Backdoor

- 后门是程序中隐藏的功能或命令，有时也称为活门，它允许用户执行一些操作，在正常情况下，这些操作是不允许用户执行的
- 当以正常方式使用时，程序能完全按预期和宣传的那样执行
- 但是，如果激活了隐藏的功能，程序会执行意想不到的操作，通常这些操作会违反安全策略，如执行特权升级
- 类型
  - 为调试插入的后门
  - 故意的后门
  - 复活节彩蛋(Easter Eggs)

逻辑炸弹Logic bomb

- 逻辑炸弹是一种程序，它根据一定的逻辑条件执行恶意操作
  - 逻辑炸弹的一个典型例子是程序员编写的工资管理系统软件，如果工资管理系统连续两次没有支付给他工资，他嵌入程序中的代码会使程序崩溃
  - 另一个典型的例子是逻辑炸弹与后门的结合，程序员在程序中放入了逻辑炸弹
  - 千年虫问题
  - Omega Engineering的逻辑炸弹

Omega Engineering的逻辑炸弹

- 一个真正触发了逻辑炸弹并造成损害的例子是程序员Tim Lloyd对他的前雇主Omega Engineering公司使用了逻辑炸弹，之后被定罪。在1996年7月31日，Omega Engineering公司的生产操作服务器上的逻辑炸弹被触发，他造成了公司数百万美元的损失，并导致公司大规模裁员。
- Omega Engineering炸弹背后的逻辑，包含以下字符串：
  - 7/30/96
    - 触发炸弹的时间（日期）
  - F:
    - 此后续命令重点运行在F卷，改卷包含服务器的重要文件
  - F:\LOGIN\LOGIN 12345
    - 登录一个虚构用户，12345(后门)，该用户12345使用管理权限运行后续命令
  - CD\PUBLIC
    - 移动到程序的公用文件夹
  - FIX.EXE/Y F:*.*
    - 运行程序FIX.EXE，删除所有文件
  - PURGE F:\\ALL
    - 阻止删除文件的恢复

内部攻击的防御

- 避免单点故障
- 使用代码走查
- 使用归档和报告工具
- 限制授权和权限
- 重要系统的物理安全
- 监控员工行为
- 控制软件的安装

提纲

PART 1 内部攻击

PART 2 计算机病毒

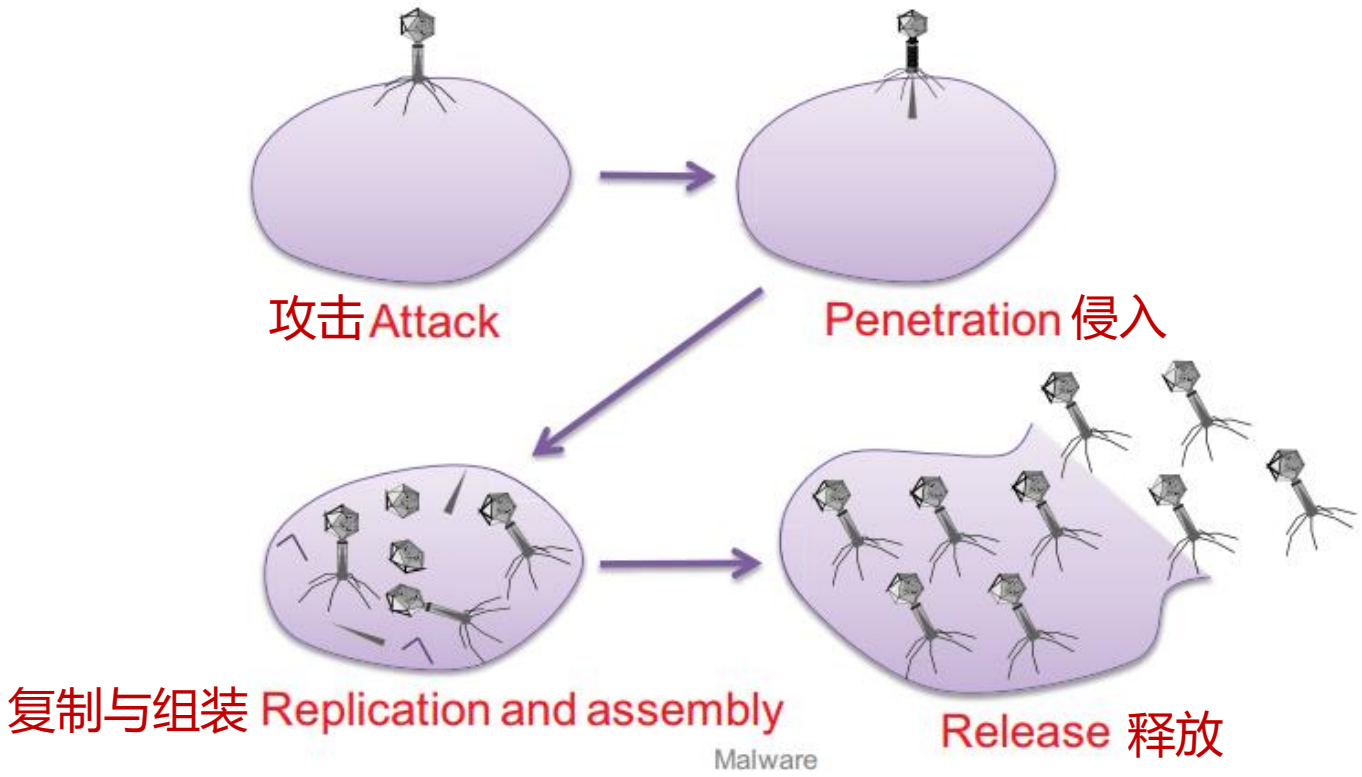
PART 3 恶意软件攻击

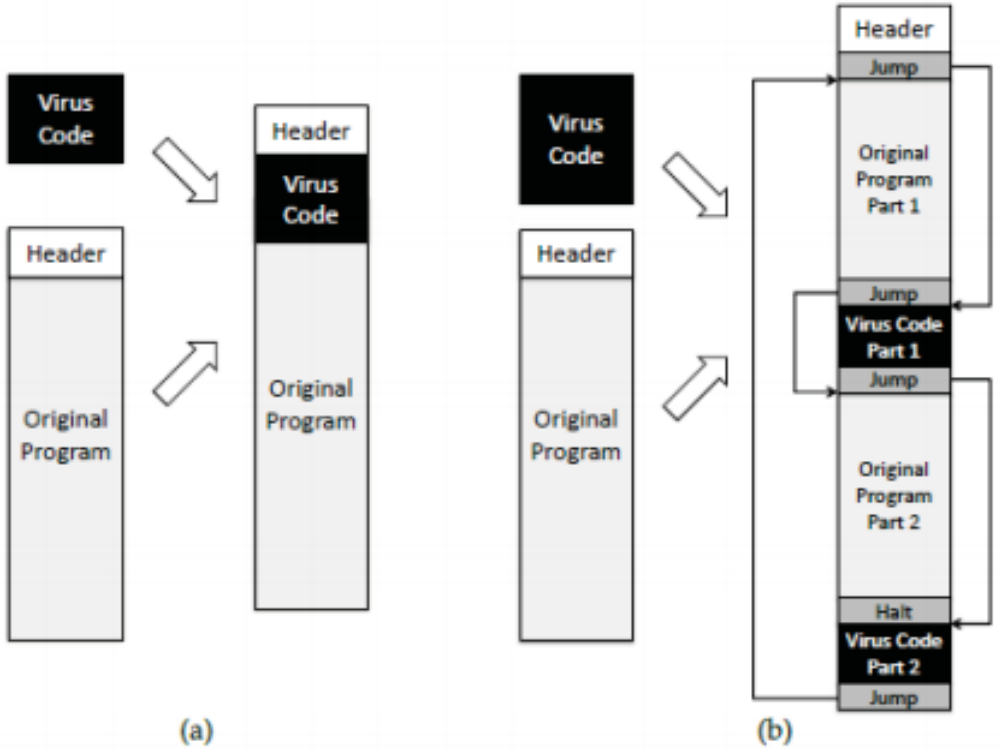
PART 4 入侵隐私软件

PART 5 对策

计算机病毒

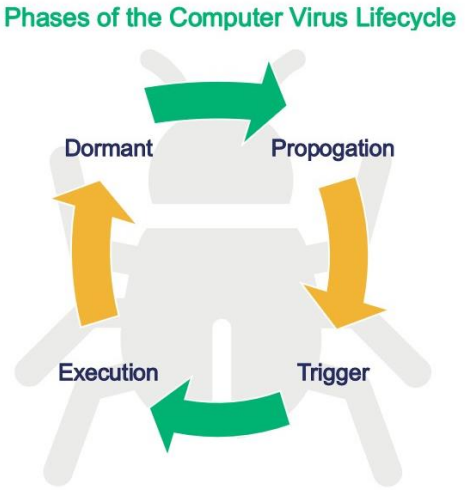
- 计算机病毒是一种能自我复制的计算机指令或程序代码，它通过修改其他文件与程序来插入代码，且能进一步自我复制， 这种自我复制的特性是计算机病毒与其它类型恶意软件（如逻辑炸弹）的不同之处
- 病毒的另一个特性是其复制需要某种类型的用户协助，如打开电子邮件附件或共享USB驱动器





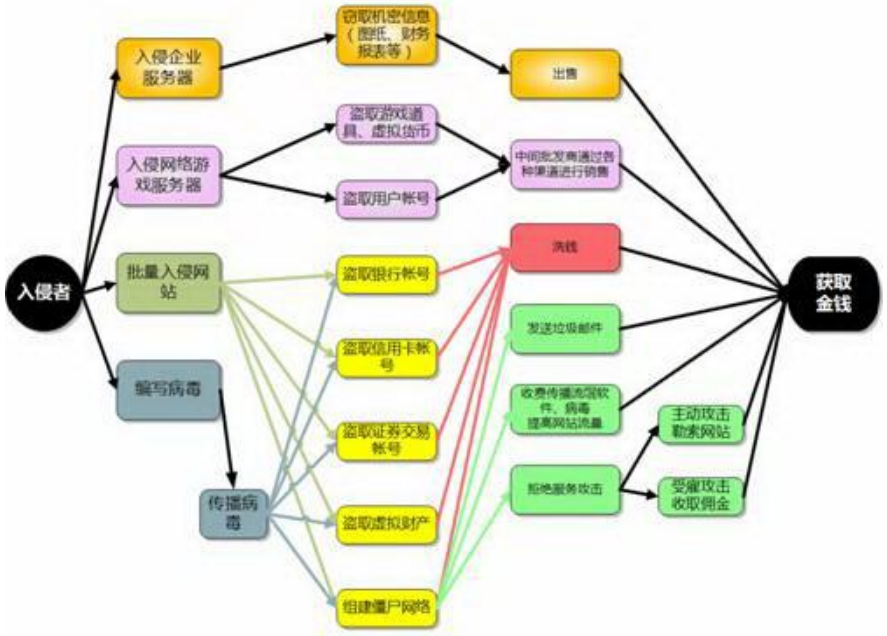
计算机病毒

- 潜伏阶段
  - 病毒只是存在——病毒很低调并避免被检测到
- 繁殖阶段
  - 病毒进行自我赋值，感染新系统中的新文件
- 触发阶段
  - 一些逻辑条件导致病毒从潜伏或繁殖阶段转换为执行病毒预定的操作
- 行动阶段
  - 病毒会执行恶意的操作，这些执行是早已设计好的，成为有效载荷
  - 这些操作可以包括一些貌似无辜的行为，如在计算机屏幕上显示很滑稽的图片；还包括一些恶意的行为：如删除硬盘上所有的重要文件



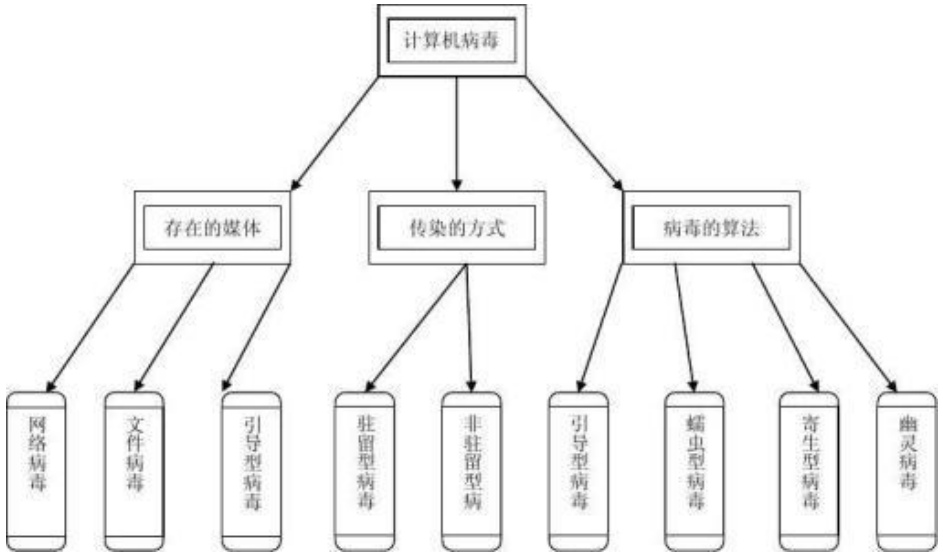
黑客/病毒产业链示意图

资料来源：瑞星反病毒中心



病毒的分类

- 程序病毒/文件病毒
  - 感染计算机中的文件（如：COM，EXE，DOC等）
- 宏病毒/文档病毒
  - 打开文档时，启动病毒，并搜索其它要感染的文件
- 引导型病毒
  - 感染启动扇区（Boot）和硬盘的系统引导扇区（MBR）
- 混合型病毒
  - 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
- 网络病毒
  - 通过计算机网络传播感染网络中的可执行文件
- ……



病毒隐藏/欺骗方式

- **加密病毒**
  - 解密引擎+加密病毒代码的主体
  - 随机生成加密密钥
  - 通过查找解密引擎进行检测
- **多态病毒**
  - 具有随机变体的解密引擎的加密病毒（例如，填充代码）
  - 使用CPU仿真器进行检测
- **变形病毒**
  - 不同的病毒体
  - 方法包括代码排列和指令替换
  - 具有挑战性的检测

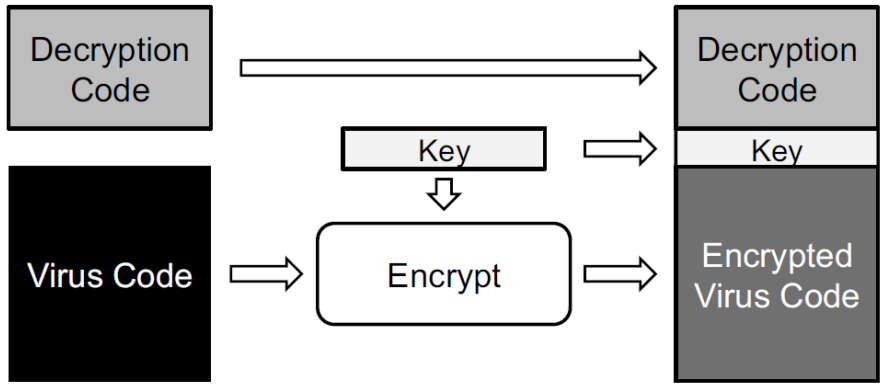
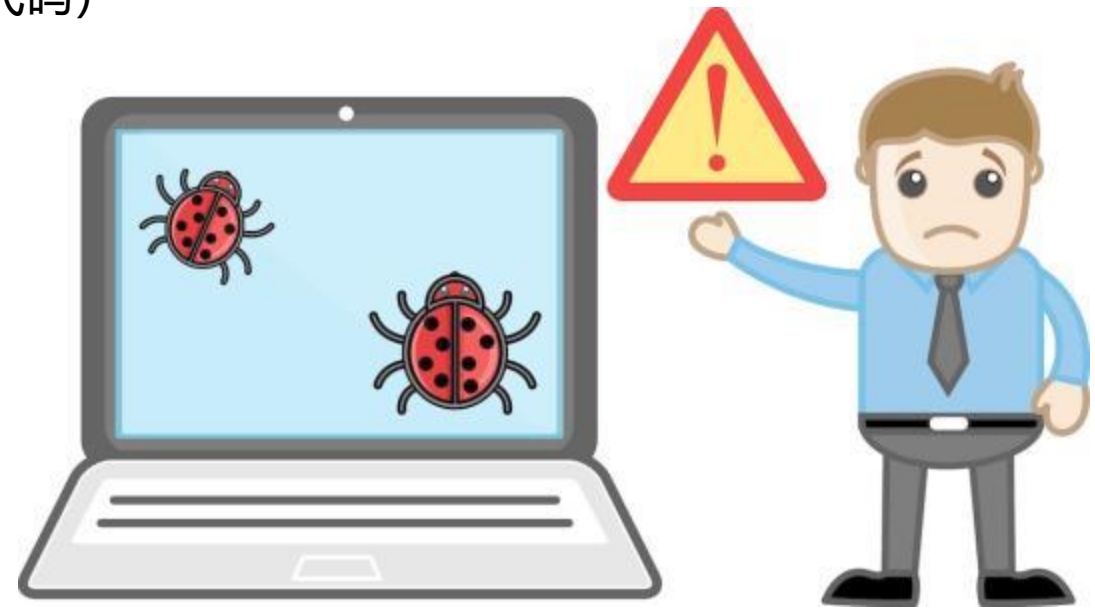


Figure 5: How an encrypted virus is structured.



病毒防御

病毒特征码

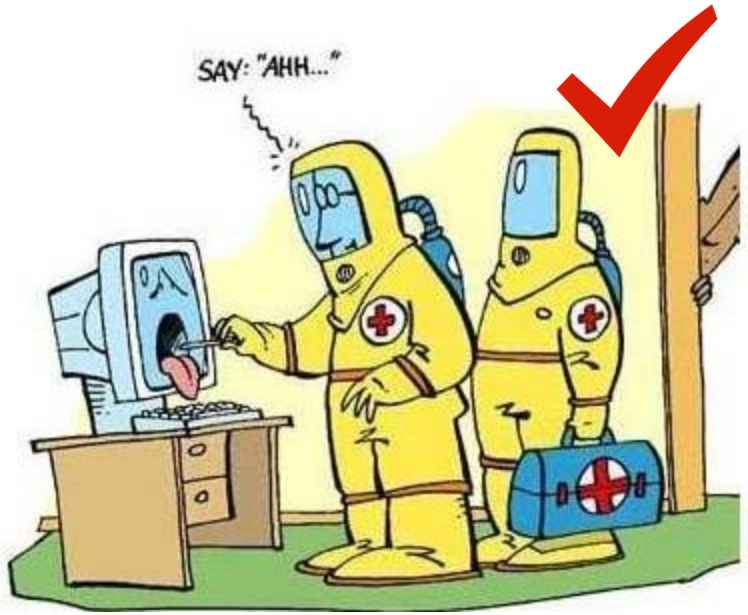
- 专家通过研究被感染文件，找到具体计算机病毒的特征代码段，之后创建唯一标识这类病毒的特征字符串
- 一般将特征字符串称为病毒的特征码，它是病毒的一种数字指纹
- 检测文件中病毒特征码的存在是模式匹配问题的一个实例

病毒的检测与隔离

- 检测文件是否感染病毒有两种方式: 1.定期扫描整个文件系统; 2.实时分析每个新创建的文件、每个修改的文件、收到的每封电子邮件附件（后一种更有效）
- 隔离：只要有一部分包含与病毒特征匹配的代码，就会被放入受保护的存储区，之后对隔离的程序进一步分析

安全实践

- 安全意识、规范操作、防护体系



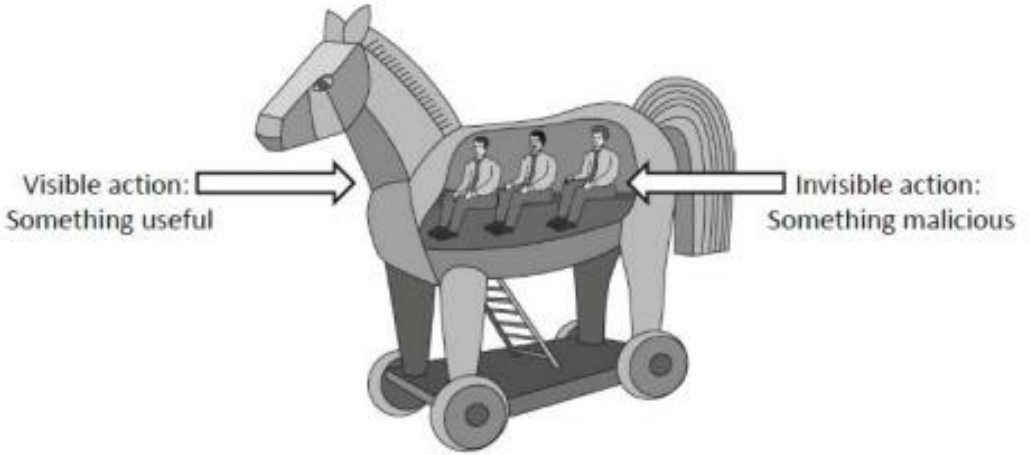
提纲

特洛伊木马Trojan Horse

- 特洛伊木马(简称木马)是隐藏在系统中的用以完成未授权功能的非法程序，是黑客常用的一种攻击工具，它伪装成合法程序，植入系统，对计算机网络安全构成严重威胁。区别于其他恶意代码，木马不以感染其它程序为目的，一般也不使用网络进行主动复制传播

- 特洛伊木马是基于C/S(客户/服务器)结构的远程控制程序，是一类隐藏在合法程序中的恶意代码，这些代码或者执行恶意行为，或者为非授权访问系统的特权功能而提供后门。

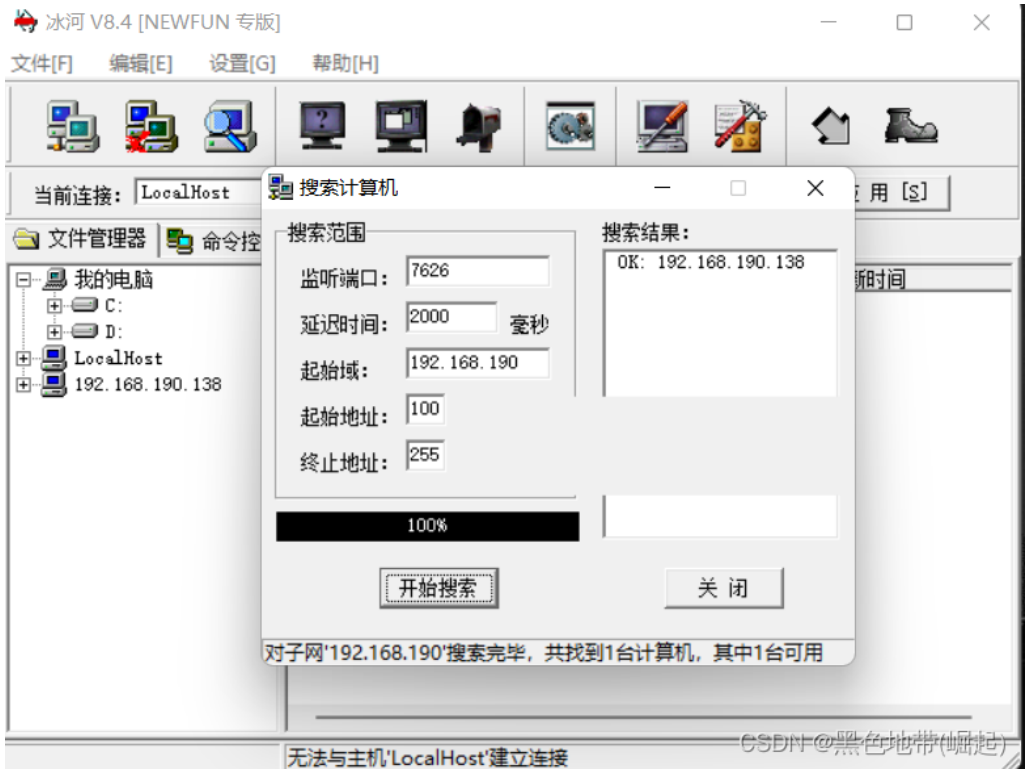
- 通常，使用木马的过程大致分两步首先，把木马的服务器端程序通过网络远程植入受控机器，然后通过安装程序或者启动机制使术马程序在受控的机器内运行。一旦木马成功植入，就形成了基于C/S结构的控制架构体系，服务端程序位于受控机器端，客户端程序位于控制机器端



冰河——2001年中美黑客大战中的主力“兵器”

- 黄鑫毕业于**西安电子科技大学**，职业是网络安全网站“安全焦点”冰河木马软件的创作者，他没入侵过任何一部机器，没黑过任何一个网站，但不妨碍黄鑫成为中国黑客江湖旗帜性人物之一，他创造的冰河可令原本无缚鸡之力的老百姓顷刻变成一个极具攻击力的黑客，黄鑫也因此被冠予**木马教父**之名
- **冰河木马**名为**冰河远程监控软件**，在推出伊始便饱受追捧，作为一款强大的远程监控软件，它具有非常丰富的监控功能，包括：自动跟踪目标屏幕变化、记录各种口令信息、获取系统信息、限制系统功能、远程文件操作、注册表操作、点对点通讯等

扩展阅读：【人物】铁马冰河，侠骨黄鑫 - 知乎



计算机蠕虫

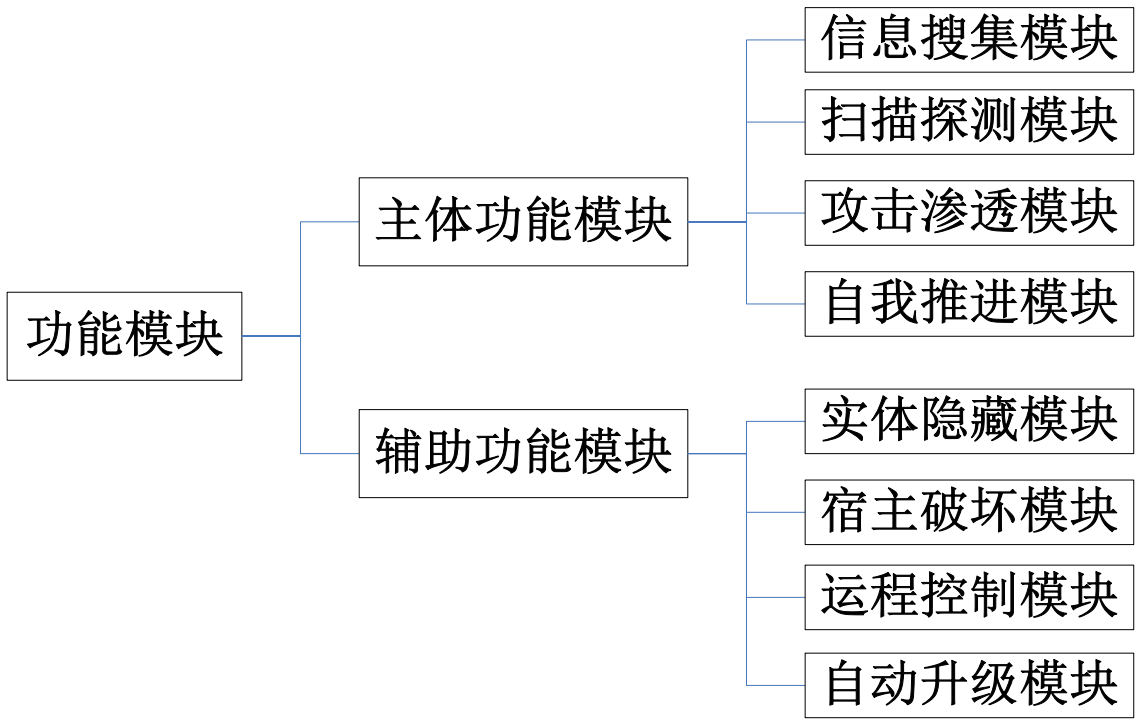
- **计算机蠕虫**是一种恶意程序，不需要将自己注入其它程序就能传播自己的副本，并且不需要与人交互。因此，从技术角度而言，计算机蠕虫不是计算机病毒（因为他们不会感染其它程序)
- 但有些人对此术语感到迷惑，因为两者都是通过自我复制传播，在大多数情况下，计算机蠕虫会携带恶意的有效载荷，如删除文件或安装后门

勒索病毒?
勒索蠕虫?

挖矿病毒?
挖矿木马?

计算机蠕虫

蠕虫的功能结构



检测蠕虫

- 与病毒扫描技术类似，使用基于特征码的文件扫描技术执行蠕虫检测
- 在网络层的扫描和过滤，会在把数据包发送给其他主机之前，分析数据包中的内容，实时检测蠕虫，阻止其进一步传播

Rootkits

- Rootkit 是一种特殊类型的 恶意软件。Rootkits最早是一组用于UNIX操作系统的工具集，黑客使用它们隐藏入侵活动的痕迹，它能在操作系统中隐藏恶意程序。这些程序在植入系统后，Rootkits 会将它们 隐藏起来，它能隐藏任何恶意程序过程、文件夹、注册码
- 找出 Rootkit 十分困难。有一些软件包可以检测 Rootkit。这些软件包可划分为以下两类
  - 基于签名的检查程序和基于行为的检查程序。基于签名（特征码）的检查程序，例如大多数病毒扫描程序，会检查二进制文件是否为已知的 Rootkit
  - 基于行为的检查程序试图通过查找一些代表 Rootkit 主要行为的隐藏元素来找出 Rootkit
- 一个流行的基于行为的 Rootkit 检查程序是 Rootkit Revealer，在发现系统中存在 Rootkit 之后，能够采取的补救措施也较为有限。由于 Rootkit 可以将自身隐藏起来，所以可能无法知道它们已经在系统中存在了多长的时间。而且也不知道 Rootkit 已经对哪些信息造成了损害。对于找出的 Rootkit，最好的应对方法便是格式化硬盘并且重新安装操作系统，这是得到证明的唯一可以彻底删除 Rootkit 的方法
- 防止 Rootkit 进入系统是能够使用的最佳办法。防卫的要素包括：病毒扫描程序、定期更新软件、在主机和网络上安装防火墙，以及强密码策略

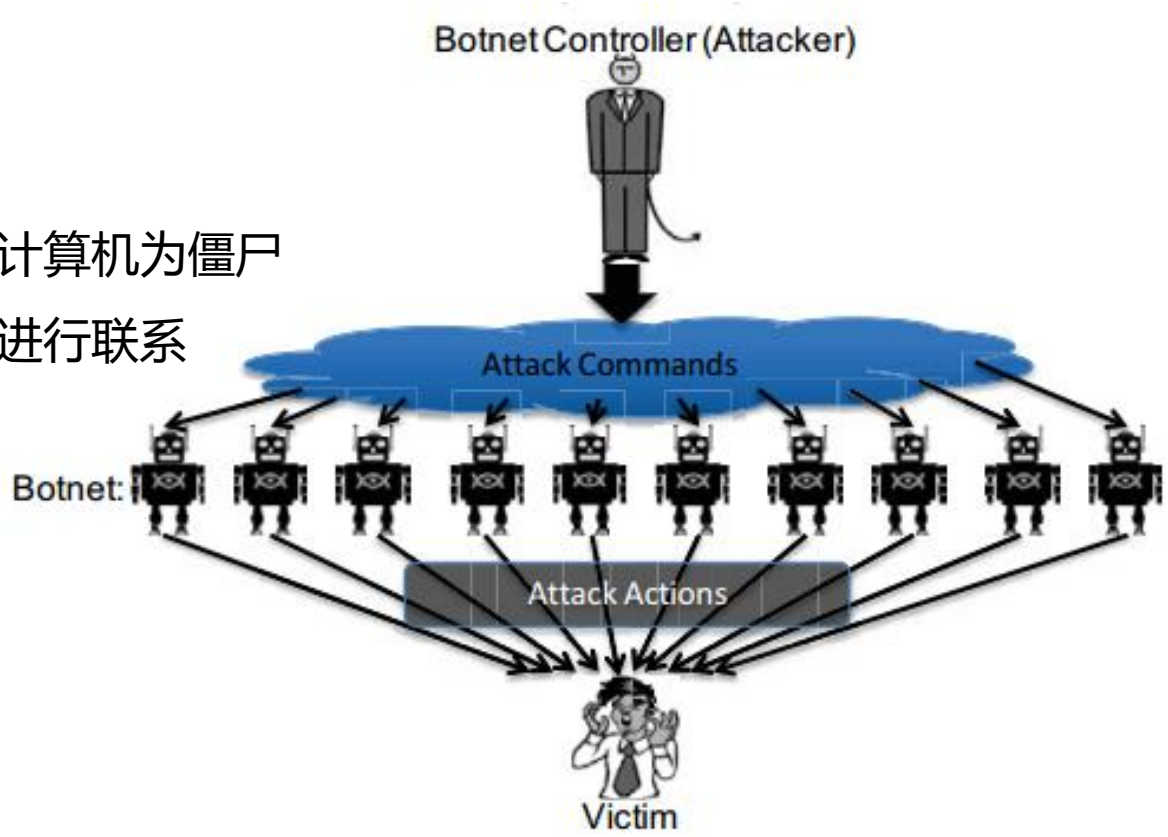
零日攻击0day

- 0day最早成立的初衷是推行互联网共享，中国网民最早接触的最多的就是软件破解和盗版影片的部分
- 最早的破解是专门针对软件的，后来发展到游戏，音乐，影视等其它内容
- 0day中的0表示zero，可叫zero day，早期的0day表示在软件发行后的24小时内就出现破解版本，现在已经引申了这个含义，只要是发布后，在最短时间内出现相关破解的，都可以叫0day
- 如果一个漏洞被发现后,当天或更准确的定义是在24小时内，立即被恶意利用，出现对该漏洞的攻击方法或出现攻击行为，那么该漏洞被称为零日漏洞，该攻击被称为零日攻击
- 没有漏洞的产品是不可能的，防范零日攻击最好的解决方法就是“免疫”。所谓免疫，是指存在一种方法或系统，能够把漏洞保护起来，能够抵御基于该漏洞的攻击，消除该漏洞存在的风险将来的情况可能是“有漏洞，没风险”

僵尸网络

- 僵尸网络 Botnet 是指采用一种或多种传播手段，将大量主机感染bot程序（僵尸程序）病毒，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络

- **创建和控制**
  - 中央的命令和控制机制
  - 一旦被感染的计算机上安装了僵尸软件，则此计算机为僵尸计算机，其会发送请求命令与中央控制服务器进行联系
- **使用**
  - 一旦僵尸网络已经集成，它的拥有者会利用它执行非法活动，例如获取信用卡号码、银行帐户凭证、海量的其他个人信息
  - 可针对大型网站、甚至小型政府基础设施发动分布式拒绝服务攻击

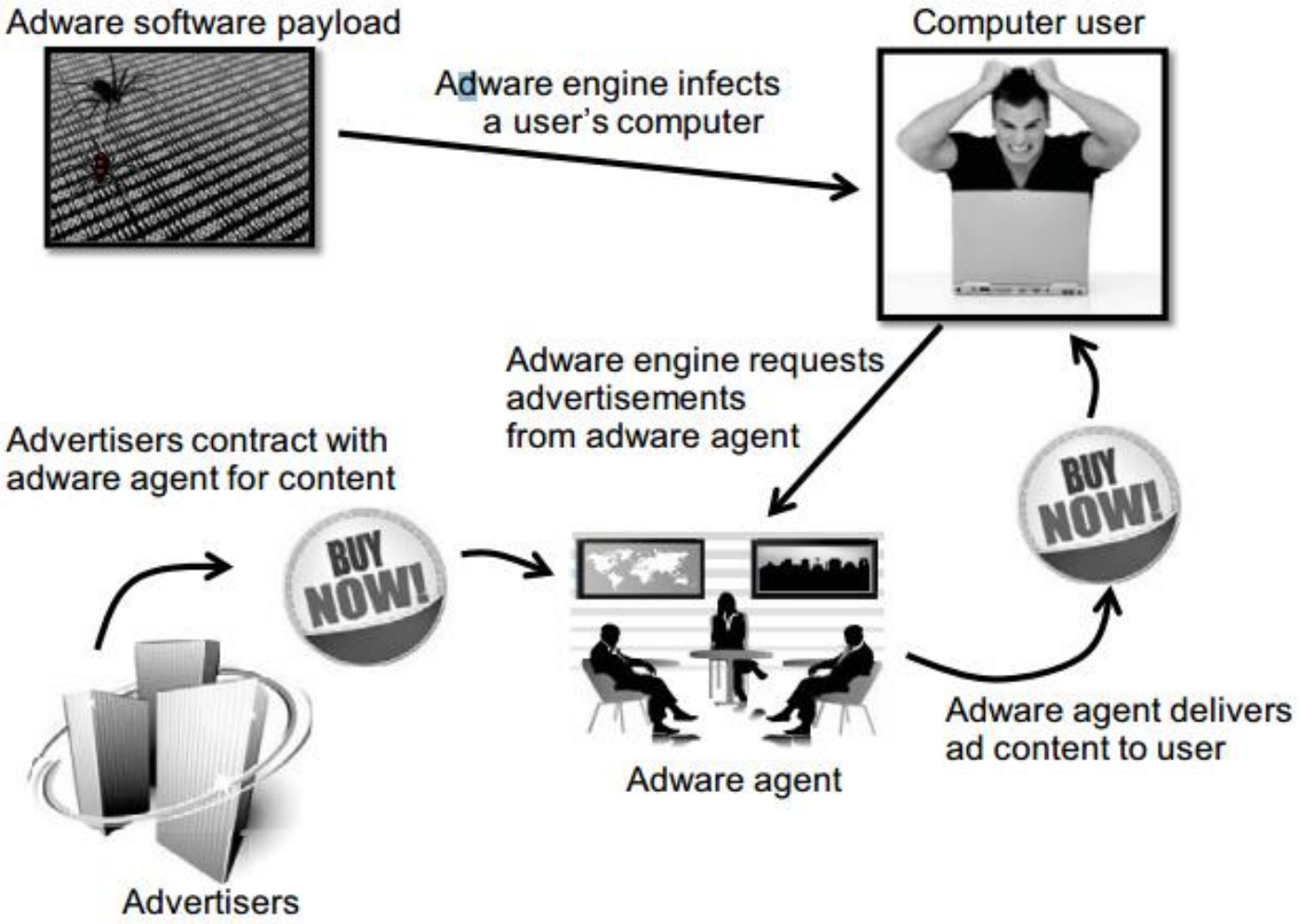


提纲

入侵隐私软件

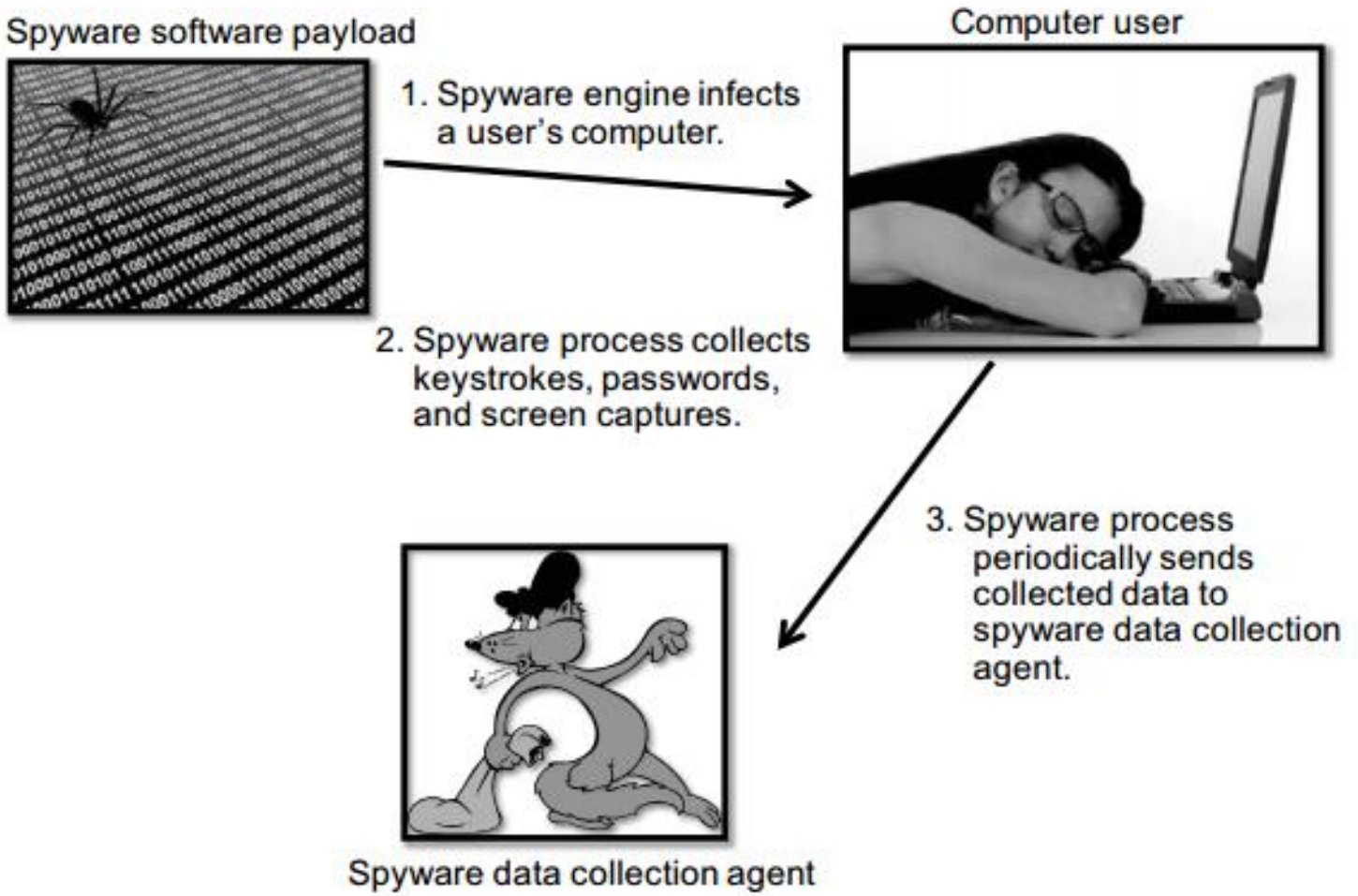
- 另一种类型的恶意软件是入侵隐私软件（Privacy-invasive software），其目标是用户隐私或用户认为敏感或有价值的信息
- 入侵隐私软件背后的意图通常具有商业性，在任何情况下，执行这类入侵隐私软件极少是出于好奇或故意破坏

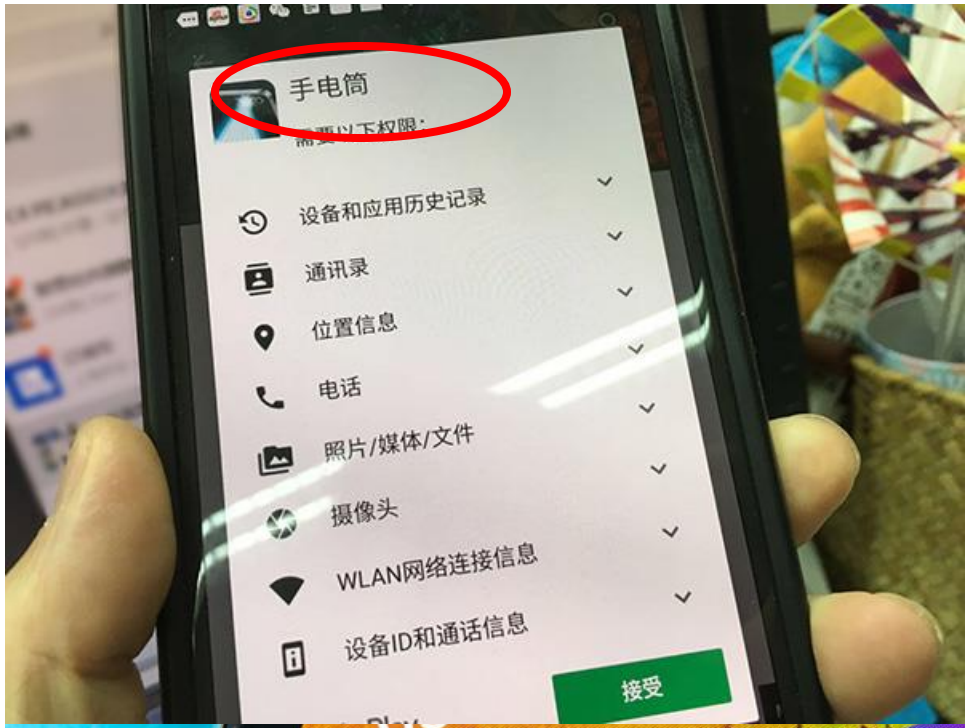
广告软件


Adware software payload
Computer user
Adware engine infects
a user's computer
Adware engine requests
advertisements
from adware agent
Advertisers contract with
adware agent for content
BUY
NOW!
BUY
NOW!
Adware agent delivers
ad content to user
Adware agent
Advertisers


联想电脑管家 - 弹窗拦截
自动拦截以下弹窗，拒绝骚扰
累计拦截 221 次
弹窗来源
拦截时间
拦截次数
搜狗今日新词
22:09
119次
搜狗输入法弹窗
11:19
15次
WinRAR广告
2020.10.09
85次
今日资讯
2020.08.03
1次
今日资讯
2020.07.30
1次

间谍软件





键盘记录、屏幕截图、追踪Cookie、数据收获……

流氓软件


360


嘟嘟安装解压向导
欢迎
所需空间：约20M
恢复默认路径
解压路径：
C:\DuDu\
更改
创建快捷方式
星月天气
帮我买
傲游浏览器
360安全浏览器
360安全套装
视频影音
UC浏览器
立即安装
我已经阅读并同意《许可协议》
360安全导航
<默认

骚扰电话/电信诈骗


卖房
开发票
房贷
诈骗
贷款


打 / 击 / 电 / 信 / 诈 / 骗 · 提 / 高 / 防 / 范 / 能 / 力
PREVENTION OF TELECOM FRAUD
预防
打击犯罪·提高意识·自我保护
电信诈骗
诈骗识别公式
"十个凡是"防电信诈骗
谨记“三不一及时”
人 物
无法准确
确认其身份
+
沟通工具
电话短信网络等
见不到本人
+
要 求
汇款、转账
= 诈骗
随便贷
航班取消
退税
恭喜您中头等奖
来我办公室
防范诈骗擦亮眼 不信不睬不给钱

提纲

PART 1 内部攻击

PART 2 计算机病毒

PART 3 恶意软件攻击

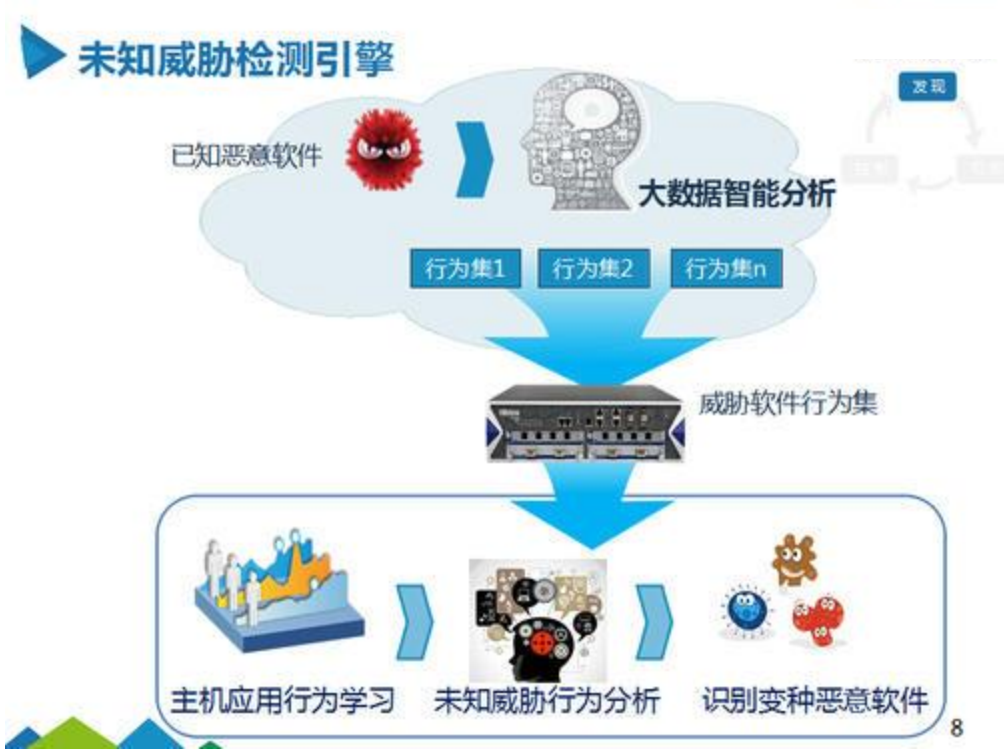
PART 4 入侵隐私软件

PART 5 对策

最佳实践

- 采用的系统尽可能具有多样性
- 尝试限制来自受信源对系统进行软件安装
- 关闭自动执行
- 对敏感系统和数据的路径采用最小特权原则
- 避免使用无法证明可靠来源的免费软件和共享软件
- 避免使用P2P等共享网络的音乐、视频资源
- 安装网络监控
- 安装网络防火墙
- 提高多因素身份验证
- 保持软件更新
- 避免使用弱密钥
- 使用恶意软件检测和清除软件

基于行为的恶意软件检测



检测所有恶意软件的不可能性

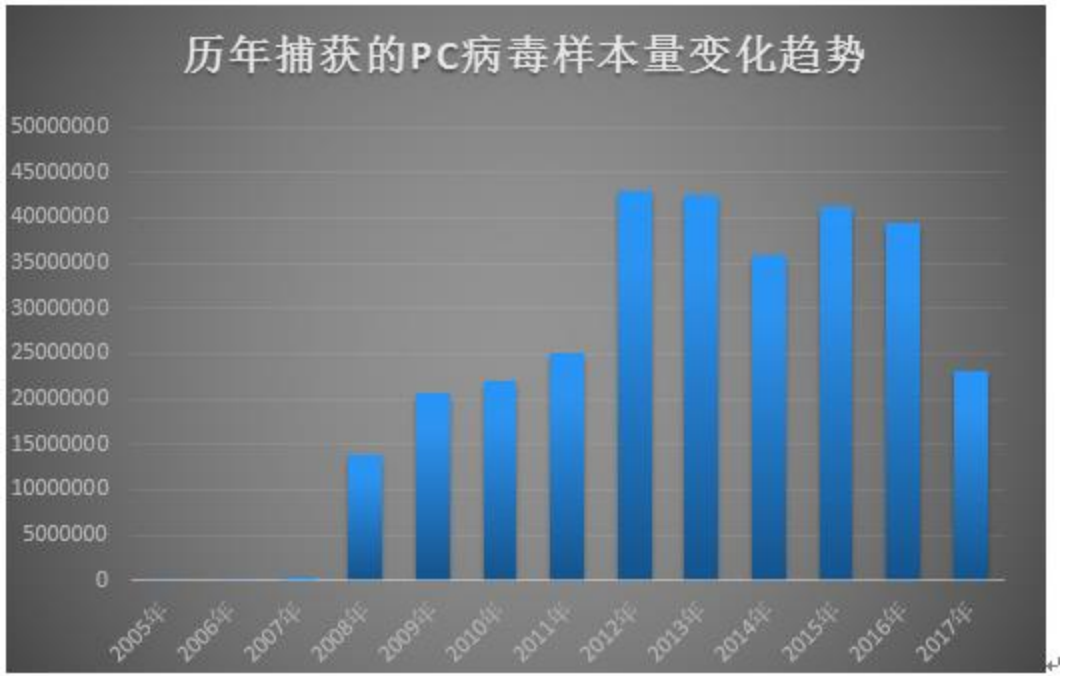
```
UltraWorm():
    if (SuperKiller(UltraWorm) = true) then
        Terminate execution.
    else
        Output UltraWorm.
        Do something malicious.
        Terminate execution.
```

- 如果 SuperKiller 认为 UltraWorm 是恶意的，但是现实中它不是
- 如果 SuperKiller 认为 UltraWorm 不是恶意的，但是现实中它却是
- **完美的恶意软件检测器是不存在的**

恶意软件检测的军备竞赛

- 计算机病毒和病毒检测程序的军备竞赛持续进行

电脑病毒越来越少了吗?



RISING 瑞星杀毒软件

金山毒霸

360 www.360.cn

腾讯电脑管家 玩得酷 靠得住

JIANGMIN 江民科技

火绒安全

恶意软件的经济

IDC
ANALYZE THE FUTURE

来源：IDC中国，2020

练习题

思考题

- 什么是高级可持续攻击（APT）？
- 蠕虫病毒和传统病毒的主要区别是什么?
- 无恶意攻击行为的恶意软件对信息安全构成威胁吗?
- 下列哪些不是病毒特征

  A 传染性　B 隐蔽性　C 多态性　D 潜伏性　E 可用性
- 下面恶意代码不需要宿主程序的有____

  A 蠕虫　B 限门　C 木马　D 病毒

习题

- R-4.5、R-4.9
- C-4.6、C-4.8

本章结束

~End~

是什麼讓火焰燃燒，是叢柴之間的空隙，它們靠此呼吸。

What makes a fire burn is space between the logs, a breathing space.