典型病毒分析与反病毒技术

主讲人：黄伟烽

计算机病毒基础

- 计算机病毒的定义、特征、结构及其分类
- 计算机病毒的传播途径
- 计算机病毒的命名规则
- 计算机病毒的加载方式
- 反病毒技术介绍
- 手动分析与处理

计算机病毒的定义

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以自我复制的计算机程序或者指令集合都是计算机病毒。

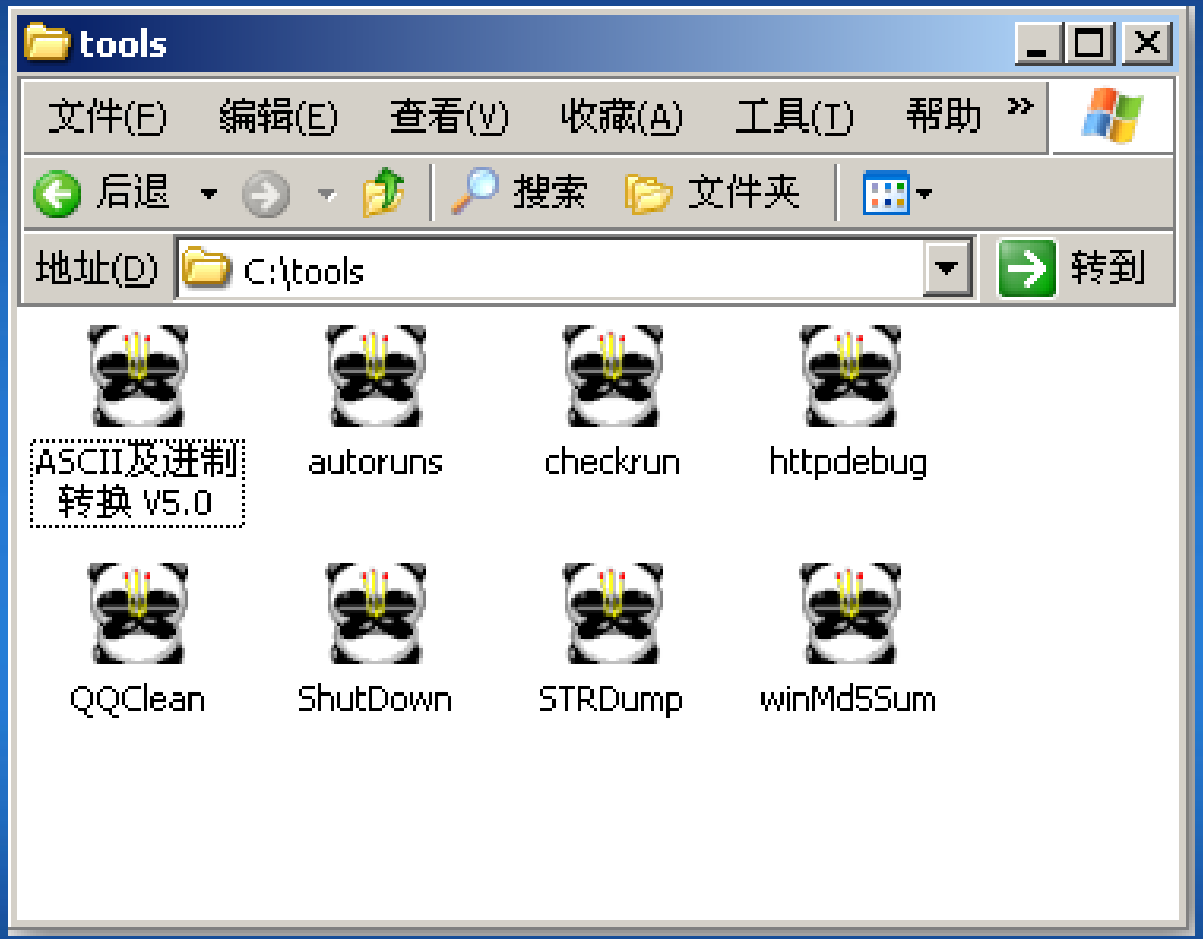
计算机病毒的特征

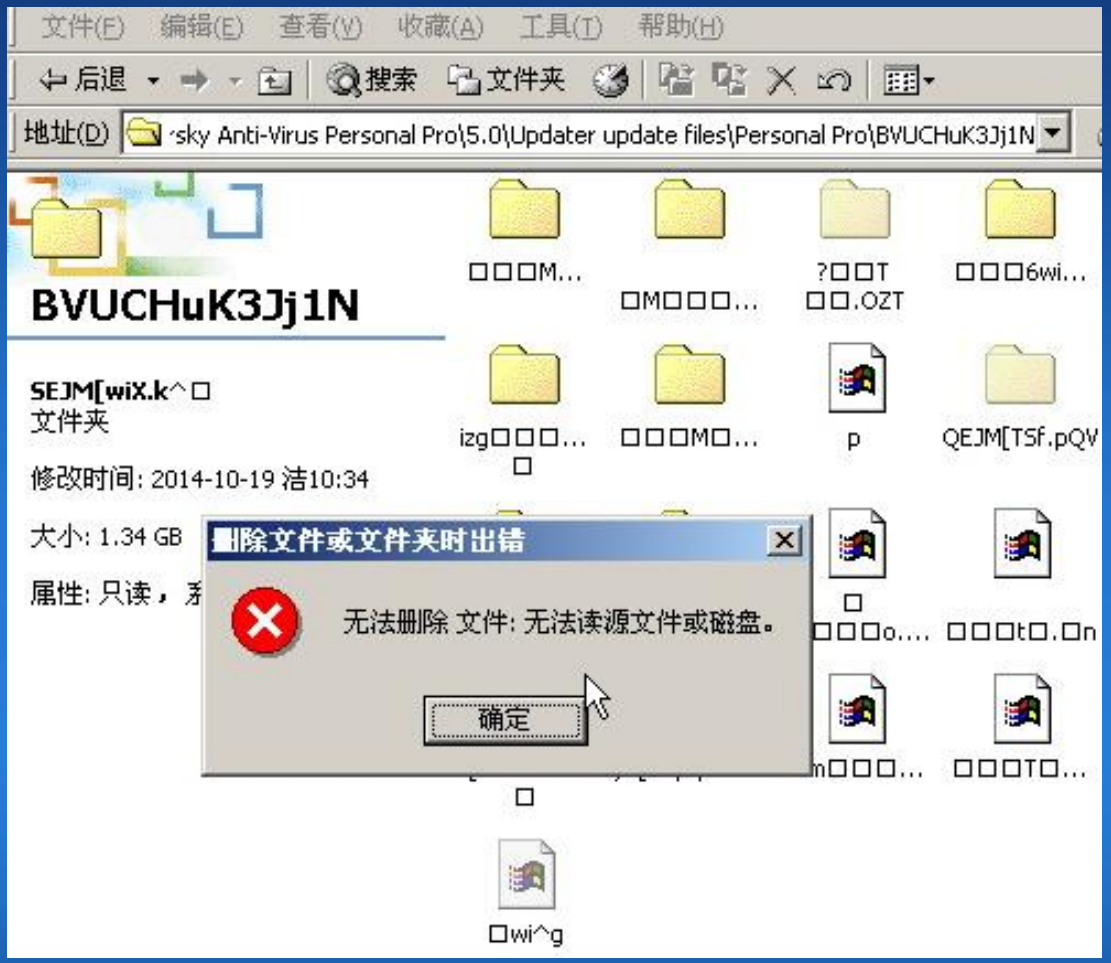
计算机病毒的表现性体现：“女鬼”病毒

我是个美食家，喜欢吃各种各样的美味
我可以毫不皱眉的津津有味的咀嚼别人不敢吃的东西
一天，有人对我说：
“你有一样东西肯定没尝过，也不敢尝
我不服气的说：“什么东西我不敢吃？快说”
“人肉！你尝过吗？”
我无话可说了，因为我确实没有吃过，也不知哪里能够尝到
晚上，我在玩电脑，我的妻子依偎我的身边，
我发觉我的妻子的皮肤是那么的光洁，那么的嫩滑，
我问妻子想不想玩一会儿电脑？
妻子柔顺的说好的
当妻子沉迷于电脑之中时，我猛的拿起鼠标线……
然后，我任凭她死命的挣扎……
大约二十分钟过后，我的妻子不动了，我开始……
……
……
……
……
虽然了了心愿，但我每次睡觉时总梦见她……

RISING 瑞星

计算机病毒的表现性体现：“熊猫烧香”病毒




文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) ·sky Anti-Virus Personal Pro\5.0\Updater update files\Personal Pro\BVUCHuK3Jj1N
BVUCHuK3Jj1N
SEJM[wiX.k^□
文件夹
修改时间: 2014-10-19 洁10:34
大小: 1.34 GB
属性: 只读，
□□□M...
□M□□□...
?□□T
□□.OZT
□□□6wi...
izg□□□...
□
□□□M□...
p
QEJM[TSf.pQV
□
□□□o....
□□□t□.□n
m□□□...
□□□T□...
□
□wi^g
删除文件或文件夹时出错
无法删除 文件: 无法读源文件或磁盘。
确定

计算机病毒的传播途径

- 网络
- 移动存储介质
- 硬盘
- 光盘
- 点对点通信系统和无线通道

计算机病毒的命名

组成病毒名称的六个字段:

主行为类型.子行为类型.宿主文件类型.
主名称.版本信息.主名称变种号

病毒的主/子行为类型及其对应关系

- Backdoor
- Worm
- Trojan
- Virus
- Harm
- Dropper
- Hack
- Binder

病毒名称	病毒中文名称	病毒介绍
Backdoor	后门	指在不知道也不允许的情况下，在被感染的系统上以隐蔽的方式运行。可以对被感染的系统进行远程控制，而且无法通过正常的方法禁止其运行。“后门”其实是木马的一种特例，它们之间的区别在于“后门”可以对被感染的系统进行远程控制（如：文件管理、进程控制等）。
Worm	蠕虫	指利用系统的漏洞、外发邮件、共享目录、可传输文件的软件（如：MSN、OICQ、IRC等）、可移动存储介质（如：U盘、软盘），这些方式传播自己的病毒。这种类型的病毒其子型行为类型用于表示病毒所使用的传播方式。
Trojan	木马	指在不知道也不允许的情况下，在被感染的系统上以隐蔽的方式运行，而且无法通过正常的方法禁止其运行。这种病毒通常都有利益目的，它的利益目的也就是这种病毒的子行为。
Virus	感染型病毒	指将病毒代码附加到被感染的宿主文件（如：PE文件、DOS下的COM文件、VBS文件、具有可运行宏的文件）中，使病毒代码在被感染宿主文件运行时取得运行权的病毒。
Harm	破坏性程序	指那些不会传播也不感染，运行后直接破坏本地计算机（如：格式化硬盘、大量删除文件等）导致本地计算机无法正常使用的程序。
Dropper	释放病毒的程序	指不属于正常的安装或自解压程序，并且运行后释放病毒并将它们运行。
Hack	黑客工具	指可以在本地计算机通过网络攻击其他计算机的工具。
Binder	捆绑病毒的工具	
Constructor	病毒生成器	指可以生成不同功能的病毒的程序。
Joke	玩笑程序	指运行后不会对系统造成破坏，但是会对用户造成心理恐慌的程序。
Rootkit	越权执行	设法让自己达到和内核一样的运行级别，甚至进入内核空间，这样它就拥有了和内核一样的访问权限，因而可以对内核指令进行修改。
Packer		加了某类专门针对杀毒软件免杀的壳的文件。这种壳专门针对杀毒软件作变形免杀，逃避查杀。

瑞星每月(10月)病毒疫情排行榜
TOP 5

- Hack.Exploit.Script.JS.Agent.ju
- Trojan.DL.PicFrame.a
- Trojan.DL.Giframe.a
- Trojan.Win32.FakeKsUsr.a
- Trojan.PSW.Win32.GameOL.yuc

反病毒技术特点

传统的“特征码技术”为主

- 启发式查毒技术—“经典指令集”技术

新的反病毒技术为辅

- 行为查杀病毒技术—“指令虚拟”技术

广泛应用的反病毒技术

➢1、特征码扫描法

特征码扫描法是分析出病毒的特征病毒码并集中存放于病毒代码库文件中，在扫描时将扫描对象与特征代码库比较，如有吻合则判断为染上病毒。

该技术实现简单有效，安全彻底。但查杀病毒滞后，并且庞大的特征码库会造成查毒速度下降。

广泛应用的反病毒技术

➢2、虚拟执行技术

该技术通过虚拟执行方法查杀病毒，可以对付加密、变形、异型及病毒生产机生产的病毒，具有如下特点：

- 在查杀病毒时，在机器虚拟内存中模拟出一个“指令执行虚拟机器”。
- 在虚拟机环境中虚拟执行（不会被实际执行）可疑带毒文件。
- 在执行过程中，从虚拟机环境内截获文件数据，如果含有可疑病毒代码，则杀毒后将其还原到原文件中，从而实现对各类可执行文件内病毒的查杀。

广泛应用的反病毒技术

➢ 3、实时监控技术

通过利用操作系统底层接口技术，对系统中的所有类型文件或定类型的文件进行实时的行为监控。

一旦有病毒传染或发作时就及时报警，从而实现了对病毒的实时、永久、自动监控。

这种技术能够有效控制病毒的传播途径，但是这种技术的实现难度
较大，系统资源的占用率也会有所降低。

广泛应用的反病毒技术

- **4、智能引擎技术**

智能引擎技术发展了特征码扫描法的优点，改进了其弊端，使得病毒扫描速度不随病毒库的增大而减慢。

早在瑞星杀毒软件即采用了此项技术，使病毒扫描速度提高了一倍之多。

广泛应用的反病毒技术

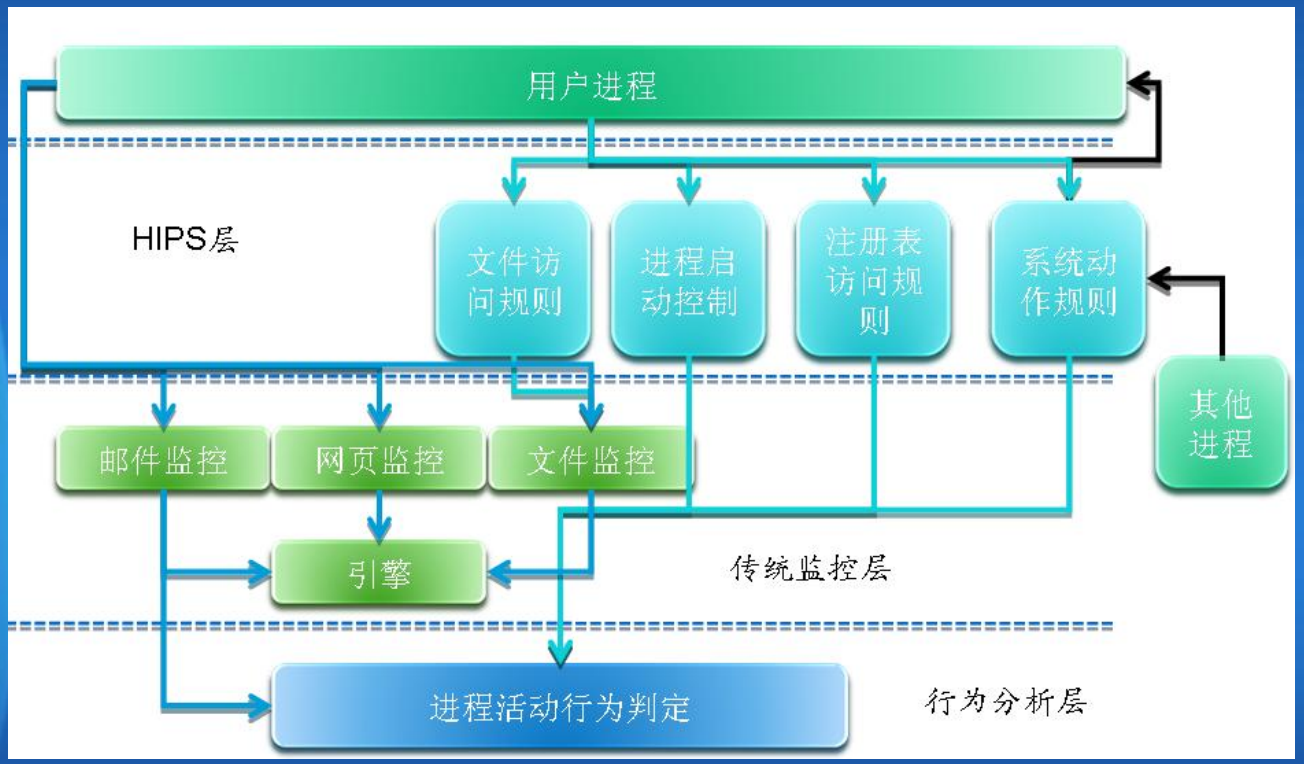
- **5、嵌入式杀毒技术**

嵌入式杀毒技术是对病毒经常攻击的应用程序或对象提供重点保护的技术，它利用操作系统或应用程序提供的内部接口来实现。

它对使用频度高、使用范围广的主要的应用软件提供被动式的防护。如对Office、Outlook、IE、Winzip、NetAnt等应用软件进行被动式杀毒。

广泛应用的反病毒技术

- **6、主动防御技术**



计算机病毒简单分析与处理

常用病毒分析方法

1. 进程和常规启动项
2. 服务项和驱动项
3. 查看劫持项和钩子，开机引导等
4. 实时分析和抓包

计算机病毒处理

1. 清理内存中的病毒
2. 清理启动项、服务项、驱动项等
3. 重启，后处理
4. 使用杀毒引擎遍历全盘

典型病毒ati2avxx.exe处理演示

- 虚拟机处理演示

信息安全　源自瑞星

谢谢大家!