典型病毒分析与处理

2010年10月

RISING 瑞星

计算机病毒基础

- 计算机病毒的定义、特征及其分类
- 计算机病毒的入侵方式及生命周期
- 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

计算机病毒的特征

非法性

隐藏性

潜伏性

可触发性

表现性

破坏性

传染性

针对性

变异性

不可预见性

计算机病毒的表现性体现：“中国黑客”病毒

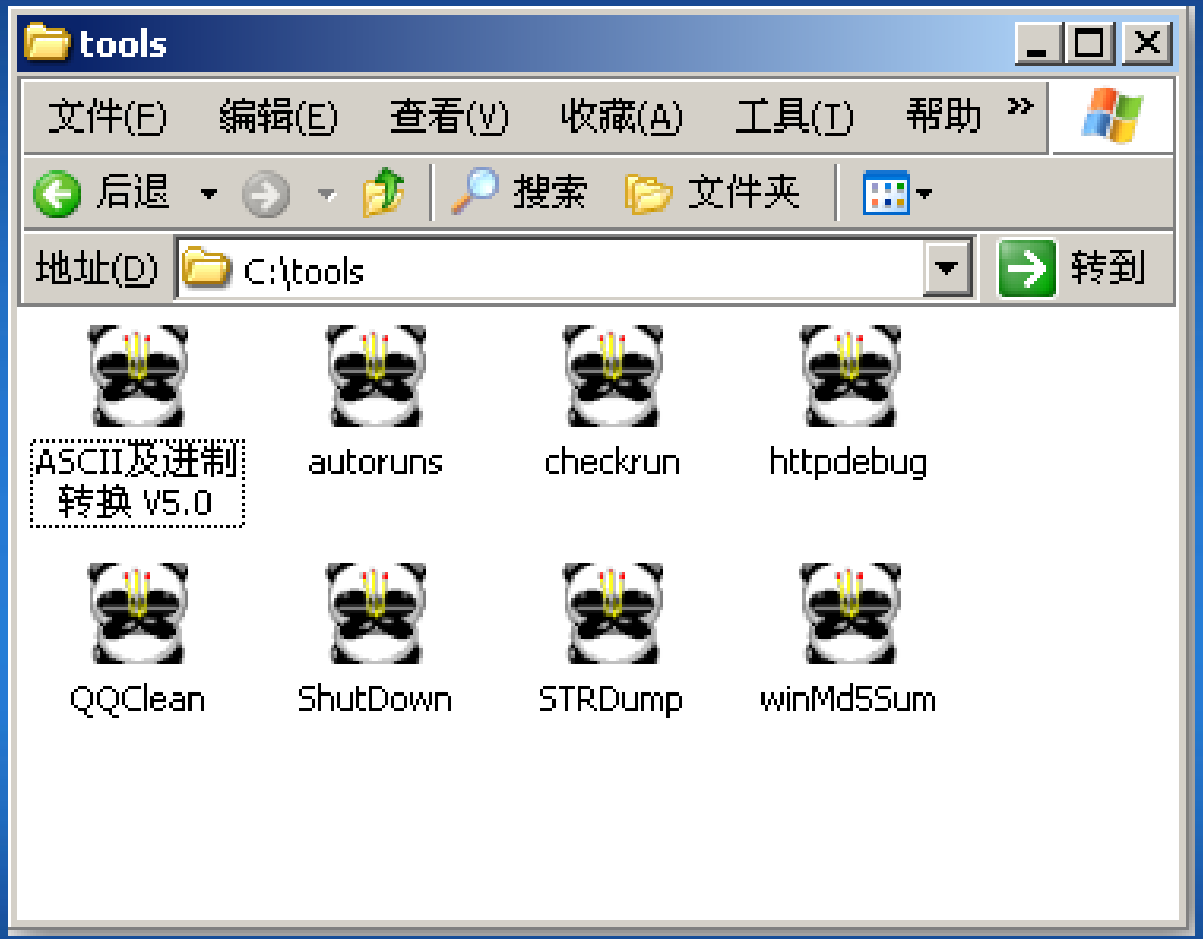
计算机病毒的表现性体现：“女鬼”病毒

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：“白雪公主”病毒

计算机病毒的表现性体现：“熊猫烧香”病毒



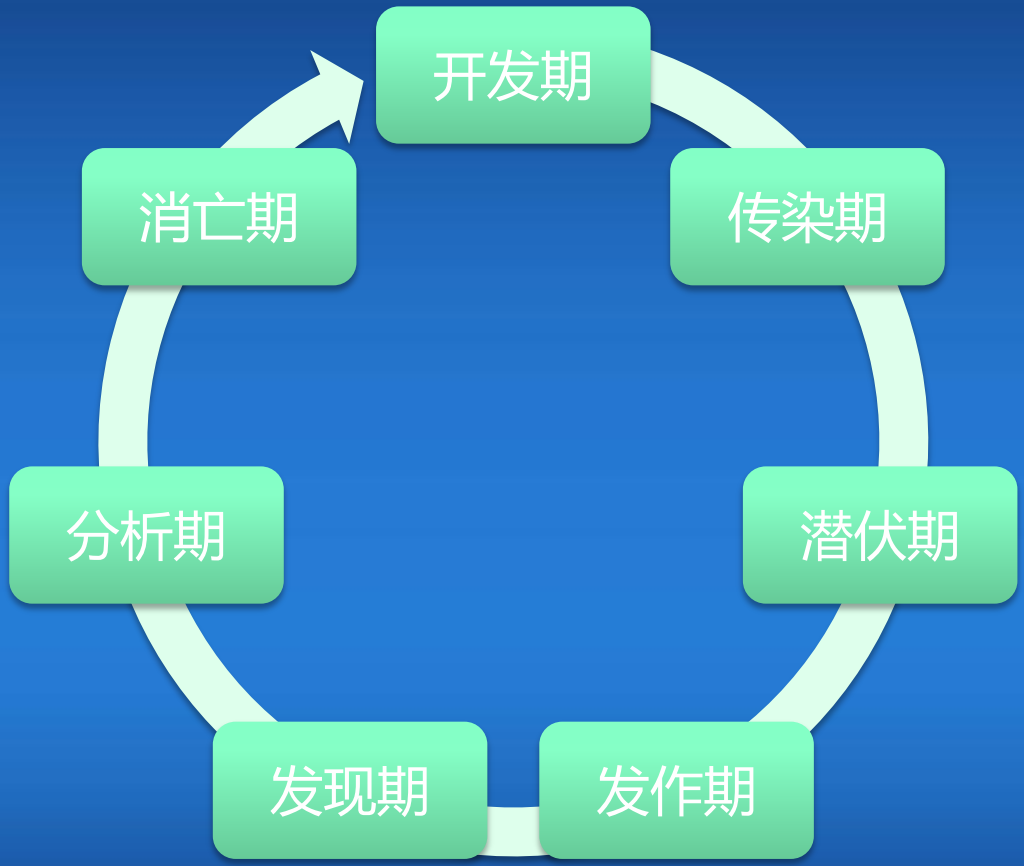
常见病毒分类

- 引导型病毒 - - MBR病毒、 BR病毒
  软（U)盘→硬盘→软（U)盘
- 文件型病毒
- 源码型病毒
- 嵌入型病毒
- 外壳型病毒
- 混合型病毒（又称复合型）

具有代表性的病毒类型

- 宏病毒：感染word、excel文件，驻留Normal模板
- 蠕虫病毒
- 特洛伊木马病毒
- 流氓软件

计算机病毒的生命周期



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

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。

Trojan 的子行为类型

- Spy
- PSW
- DL
- IMMSG
- MSNMSG
- QQMSG
- ICQMSG
- UCMSG
- Proxy
- Clicker
- Dialer

宿主文件类型

JS	说明：JavaScript 脚本文件
VBS	说明：VBScript 脚本文件
HTML	说明：HTML 文件
Java	说明：Java 的 Class 文件
COM	说明：Dos 下的 Com 文件
EXE	说明：Dos 下的 Exe 文件
Boot	说明：硬盘或软盘引导区
Word	说明：MS 公司的 Word 文件
Excel	说明：MS 公司的 Excel 文件
PE	说明：PE 文件
WinREG	说明：注册表文件
Ruby	说明：一种脚本
Python	说明：一种脚本
BAT	BAT 脚本文件
IRC	说明：IRC 脚本

主名称

病毒的主名称是由分析员根据病毒体的特征字符串、特定行为或者所使用的编译平台来定的，如果无法确定则可以用字符串”Agent”来代替主名称，小于10k大小的文件可以命名为“Samll”。

举例说明

- Trojan.DL.VBS.Agent.cgk
- Trojan.PSW.ZhengTu.afl
- Worm.Mail.Bagle.ld
- Worm.MSN.Kelvir.i
- Backdoor.Agobot.ius
- Hack.DDoSer.Boxed.bc

瑞星每月(9月)病毒疫情排行榜：TOP 5排名趋势病毒名称百分比

- 01→Trojan.DL.Giframe.a
- 02→Trojan.DL.PicFrame.a
- 03↑Trojan.PSW.Win32.GameOL.yzx
- 04↑Trojan.DL.Script.VBS.Mnless.e
- 05↑Trojan.PSW.Win32.GameOL.yuc

计算机病毒分析与处理

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

典型病毒分析

- 橙色八月处理演示