典型病毒分析与处理

——瑞星信息安全沙龙

2011年10月21日

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
- 常见反病毒工具

计算机病毒的定义

人为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被称为计算机病毒（Computer Virus）。

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

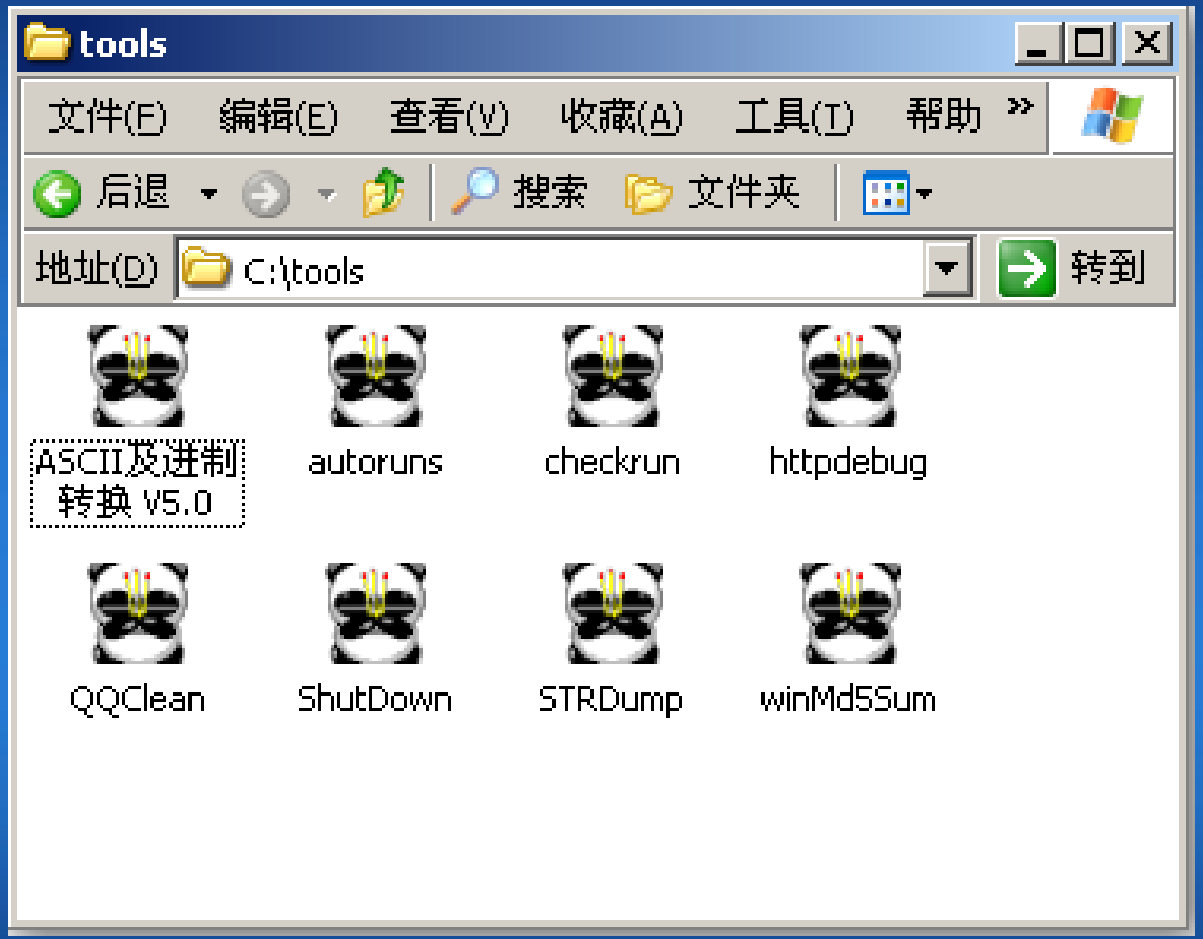
传染性

针对性

变异性

不可预见性

计算机病毒的表现性体现：“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

计算机病毒的入侵方式

- 源代码嵌入攻击
- 代码取代攻击
- 外壳寄生入侵
- 系统修改入侵

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

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。

Worm的子行为类型

Trojan 的子行为类型

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

Hack 的子行为类

- Exploit
- DDoser
- Flooder
- Spam
- Anti

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”。

版本信息

版本信息只允许为数字，对于版本信息不明确的不加版本信息。

主名称变种号

确为是同一家族病毒的条件:

病毒的主行为类型、行为类型、宿主文件类型、主名称均相同.

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

病毒程序加载方式

- 程序的基本加载方式，病毒及正常的程序会用到此类方式进行加载，例如：MSN、QQ、声卡、显卡会使用此类方式加载其部分程序，但木马使用类加载方式会略少。对于计算机知识的普及对于MSCONFIG的编辑很多人已经熟悉。但是出现在“C:\Documents and Settings\All Users\「开始」菜单\程序\启动”中的程序加载方式我们需要引起重视。
- 通过Win.ini文件加载病毒程序，在WIN.INI文件中[Windows]域中的load和run项会在Windows启动时运行，在msconfig中也会看到此加载项。
- 在system.ini文件中，在[BOOT]下面有个“shell=文件名”。正确的文件名应该是“explorer.exe”，如果不是“explorer.exe”，而是“shell= explorer.exe xxx.exe”，那么“xxx.exe”程序就是异常程序。
- 通过注册表加载病毒，并保护其注册表项

  [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

  [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

  [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]

  病毒会利用此类注册表项加载木马程序，但是木马程序会将其键值进行保护。经常会发现在删除注册表项后会出现回写现象。原因是病毒会在文件中添加一个时间控件，在发现其需要保护的注册表项被改写后，会进行回写的操作从而起到保护的作用。

病毒程序加载方式

- 病毒利用注册表特性加载其病毒文件，并实现自杀释放病毒文件的方法
  [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
  [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
  此类注册表键值，会在计算机启动后被删除，病毒可以利用此类键值进行一次性破坏和启动释放其他程序的操作，也可利用此键值进行回写操作。在MSCONFIG中无法查到此类键值，但是可以利用卡卡上网安全助手及注册表编辑器修改并删除此键。
- 使用捆绑方式，达到病毒加载的方式。将病毒程序与正常的程序进行捆绑，在执行正常程序后病毒文件也将被执行。木马程序先获得控制权或另开一个线程以监视用户操作，截取密码等。
- 伪装其他文件欺骗用户，病毒文件名称会使用与常用软件相近或相同的文件名称蒙蔽用户。例如机器狗病毒，在替换系统文件后达到其自动加载的目的。
- 通常病毒程序会将自己和相应文件进行关联，这样当你打开一个文件时，木马也达到其运行的目的 。通过此方式加载的病毒程序，在处理时需要将注册表键值还原，并删除文件。例如：
  “HKEY_CLASSES_ROOT\exefile\shell\open\command”默认的字符串值为〔"%1" %*〕
  如果关联项已经被修改可以通过DOS命令行进行修复此问题：ftype 关联项（exefile）=字符串原值（“%1” %*）

病毒程序加载方式

- 通过系统加载规则进行加载，例如AUTORUN.INF此加载方式已经被病毒程序广为利用，以达到打开盘符时自动加载病毒文件的目的

  [autorun]

  open=shell\open=打开(&O)

  shell\open\Command=*****.exe

  shell\open\Default=1

  shell\explore=资源管理器(&X)

  shell\explore\Command=*****.exe

  由于已经将系统设备右键菜单进行了更改，无论是打开还是使用资源管理器均会启动病毒程序。顾处理以上AUTORUN.INF文件我们可以使用DOS命令进行处理。

病毒程序加载方式

- 引导区病毒此类病毒存放在软盘引导区、硬盘主引导区和引导区。由于病毒在宿主的操作系统启动前就加载到内存中，具有操作系统无关性，可以感染所有的X86类电脑。因此这类病毒将长期存在。病毒在ROM BIOS之后，系统引导时出现的病毒，它先于操作系统，依托的环境是BIOS中断服务程序。引导型病毒是利用操作系统的引导模块放在某个固定的位置，并且控制权的转交方式是以物理位置为依据，而不是以操作系统引导区的内容为依据，因而病毒占据该物理位置即可获得控制权，而将真正的引导区内容搬家转移或替换，待病毒程序执行后，将控制权交给真正的引导区内容，使得这个带病毒的系统看似正常运转，而病毒已隐藏在系统中并伺机传染、发作。

- 应用程序劫持ImageFileExecutionOptions项
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ImageFileExecutionOptions下的注册表项，这个是针对系统可以设置每个程序指定的纠错程序来实现的。
- 灰鸽子是通过添加服务项来实现自启动的，会在[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runservices]下生成键值，并在[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\]下创建可疑主键。

计算机病毒分析与处理

常用病毒分析方法

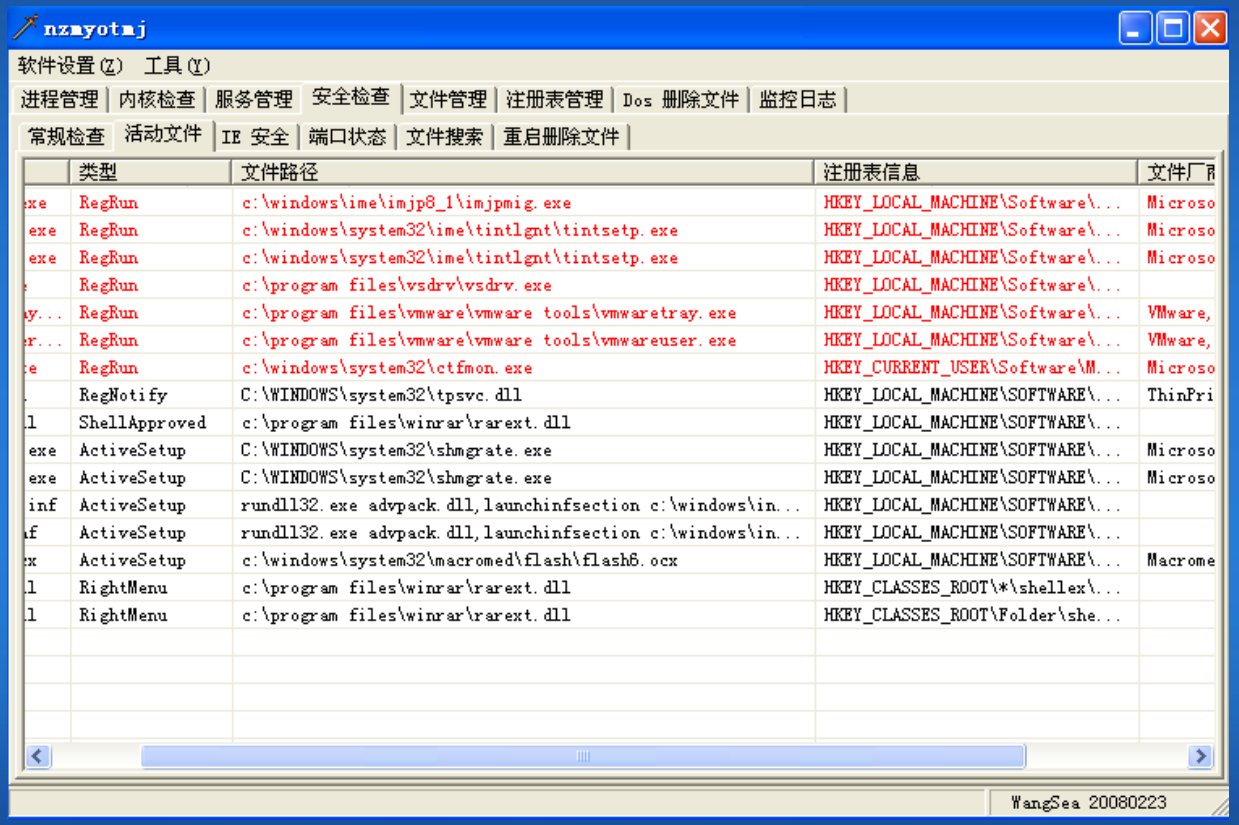
1. 进程和常规启动项
2. 服务项和驱动项
3. 查看劫持项和钩子，开机引导等
4. 实时分析和抓包

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

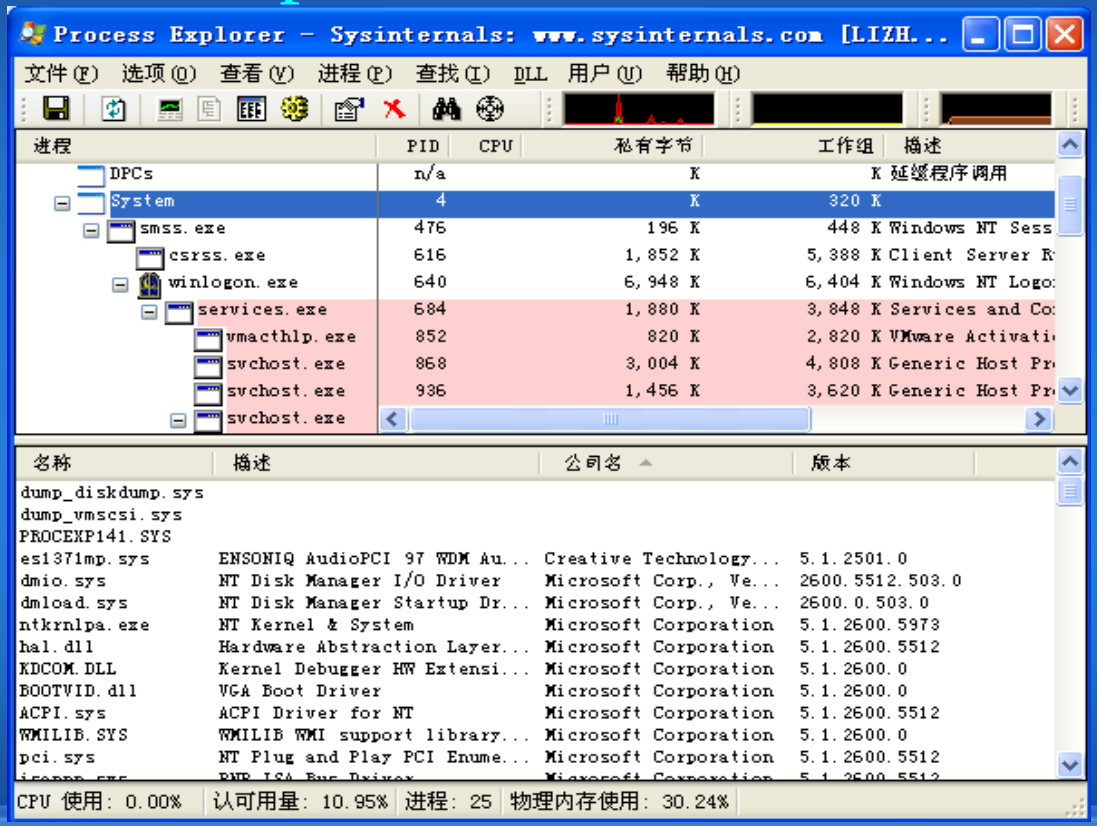
常见反病毒工具

- Wsyscheck



常见反病毒工具

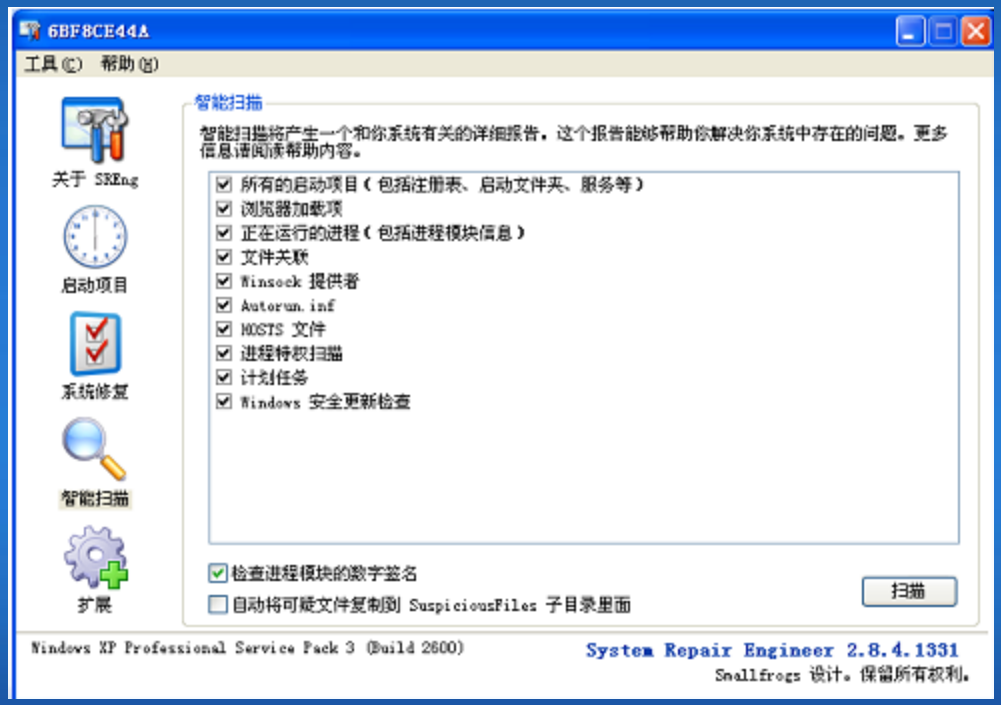
- Procesxp



RISING 瑞星

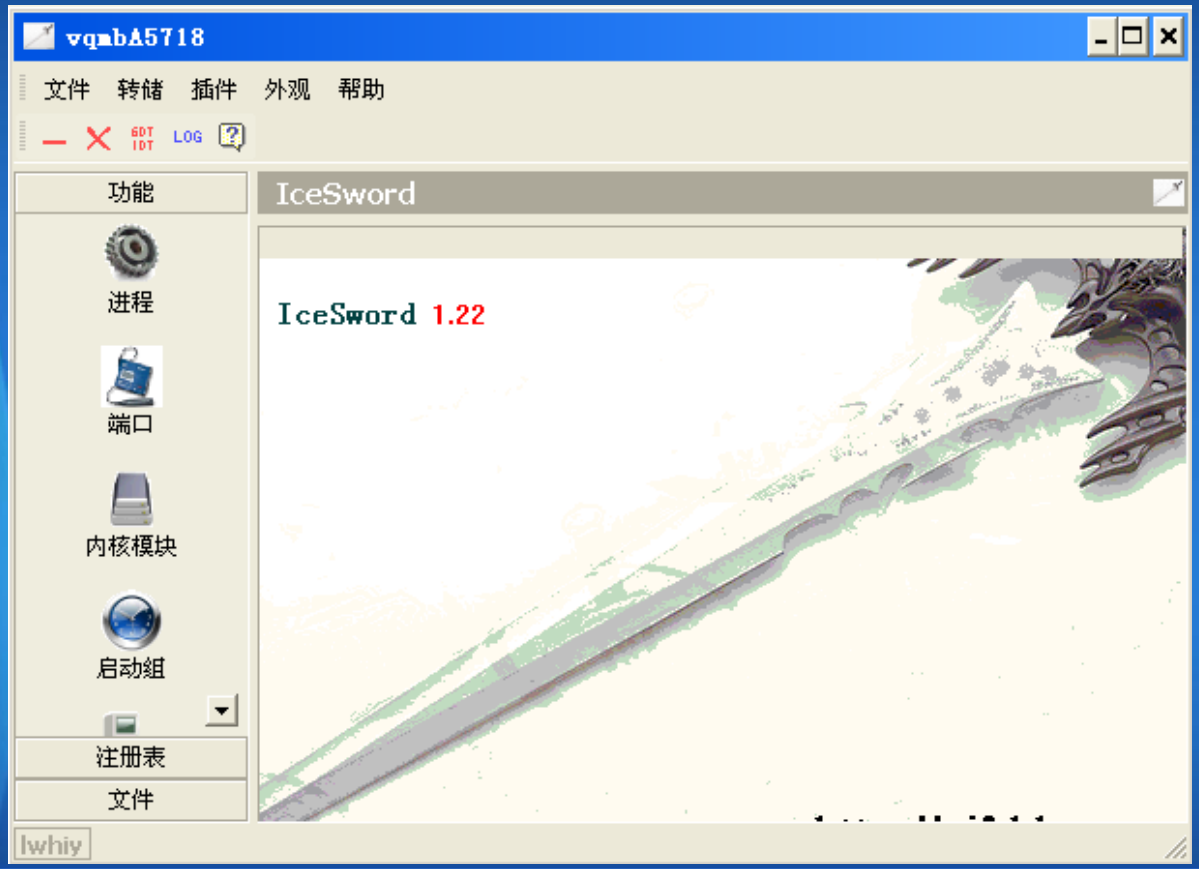
常见反病毒工具

- SReng(与PLA一起使用)



常见反病毒工具

- Icesword



典型病毒处理演示

- 虚拟机处理演示


信息安全　源自瑞星
谢谢大家!