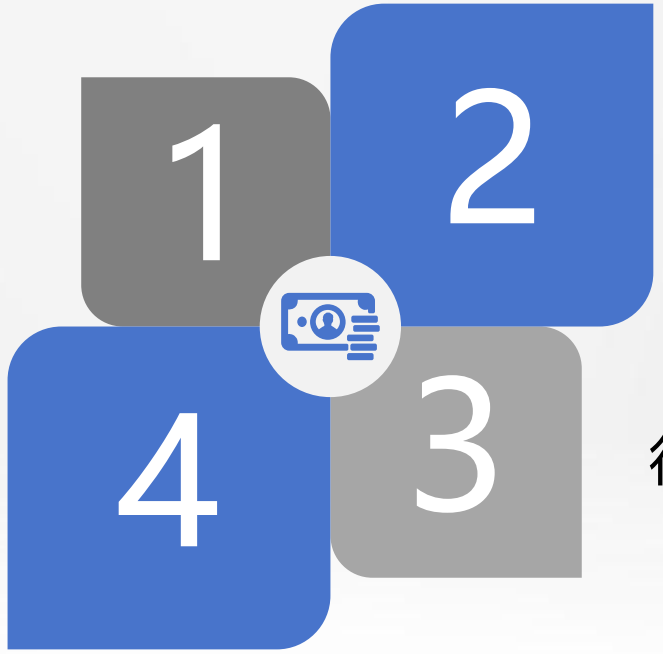
第3章 计算机病毒

3.4 反病毒技术简述

计算机病毒诊断技术

特征代码法

校验和法



软件模拟法

行为监测法

3.4 反病毒技术简述

01 特征代码法

采集已知病毒样本

打开被检测文件，在文件中搜索，检查文件中是否含有病毒数据库中的病毒特征代码（唯一性）。

优点

检测准确快速、可识别病毒的名称、误报警率低、依据检测结果，可做杀毒处理。

缺点

不能检测未知病毒；开销大、效率低

3.4 反病毒技术简述

02 校验和法

将正常文件的内容，计算其校验和，将该校验和写入文件中或写入别的文件中保存。针对多态病毒。

特点

能发现已知病毒，也能发现未知病毒，但是，它不能识别病毒类型和名称。误报率高。

03 行为监测法

利用病毒的特有行为特征性来监测病毒的方法。

行为特征

- 占有内存特殊位置
- 改DOS系统为数据区的内存总量
- 对COM、EXE文件做写入动作
- 病毒程序与宿主程序的切换

特点

- 可发现未知病毒、可相当准确地预报未知的多数病毒。
- 可能误报警、不能识别病毒名称、实现时有一定难度。

3.4 反病毒技术简述

04 软件模拟法

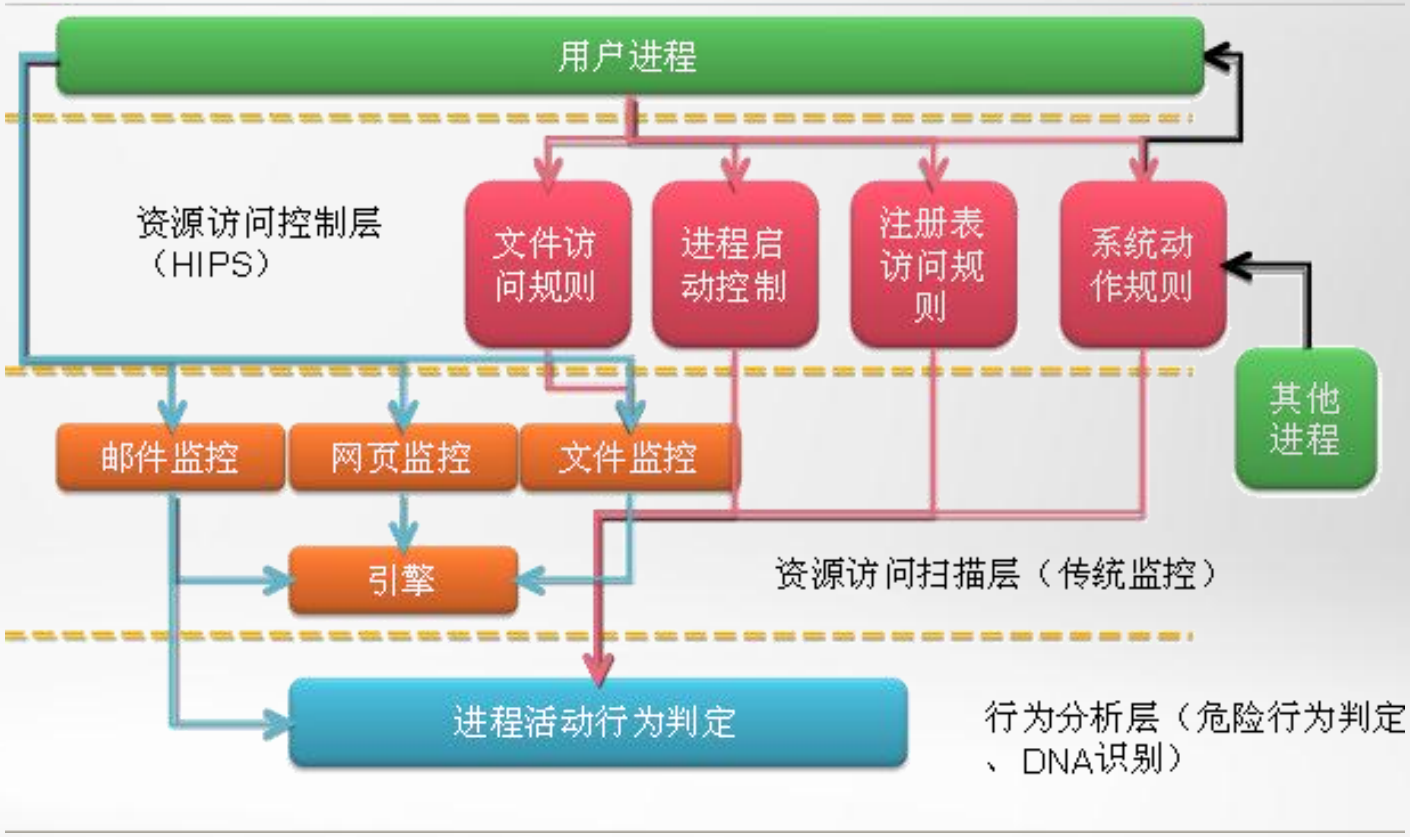
为了检测多态性病毒，可应用软件模拟法。它是一种软件分析器，用软件方法来模拟和分析程序的运行。

沙盘（沙盒）-Sandboxie

3.4 反病毒技术简述

主动防御（瑞星 ）

主动防御是一种阻止恶意程序执行的技术。可以在病毒发作时进行主动而有效的全面防范，从技术层面上有效应对未知病毒的传播。



3.4 反病毒技术简述

- 杀毒软件中的“主动防御功能”

	功能列表	瑞星
资源访问规则控制（HIPS）	系统动作	●
	注册表	●
	关键进程保护	●
	系统文件保护	●
	限制启动子程序	●
	限制全局钩子	●
	限制加载驱动	●
	防DLL注入	●
	防写内存	●
	防止启动远程线程	●
	防止终止进程	●
	防止模拟发送消息	●
	防止模拟按键	●
资源访问扫描（传统监控）	文件监控	●
	邮件监控	●
	网页监控	●
智能分析		●

3.5 防病毒软件


360杀毒
日志 设置 反馈
360杀毒正在保护您的系统!
已检测活跃文件: 0
已保护您的系统
0001 天
全盘扫描
快速扫描
功能大全
已隔离威胁对象: 16
查看隔离文件
多引擎保护中:
自定义扫描
宏病毒扫描
弹窗过滤
软件管家
程序版本 5.0.0.8170(64位)
检查更新
消息中心: 360为什么能保持免费?


360杀毒 - 设置
常规设置
升级设置
多引擎设置
病毒扫描设置
实时防护设置
文件白名单
免打扰设置
异常提醒
系统白名单
多引擎设置
360杀毒内含多个领先的查杀引擎，已经默认为您选择了最佳组合。您也可以根据自己的电脑配置及查杀需求对其进行调整。
引擎
病毒查杀
实时防护
云查杀引擎
QVM II 人工智能引擎
系统修复引擎
Avira(小红伞)常规查杀引擎
删除引擎（可释放200MB磁盘空间）
BitDefender常规查杀引擎
删除引擎（可释放600MB磁盘空间）
当360杀毒所在磁盘空间不足时，可以对Avira（小红伞）及BitDefender常规查杀引擎文件进行选择性删除，释放磁盘空间。
恢复默认设置
确定
取消

3.5 防病毒软件


360杀毒 - 设置
常规设置
升级设置
多引擎设置
病毒扫描设置
实时防护设置
文件白名单
免打扰设置
异常提醒
系统白名单
设置文件及目录白名单
加入白名单的文件及目录在病毒扫描和实时防护时将被跳过。
如果在加入白名单后文件的大小或日期发生改变，该条目将会失效。
文件
状态
E:\360Downloads\附件3：两村住房信息登记表及个人政...
有效
G:\ss\2\无忧截图.exe
有效
添加文件
添加目录
删除
全选
设置文件扩展名白名单
带有白名单扩展名的文件在病毒扫描和实时防护时将被跳过。
扩展名
添加
删除
定期扫描白名单中具有极强传播性及感染性的文件。
恢复默认设置
确定
取消


系统安全
自定义扫描
宏病毒扫描
人工服务
安全沙箱
防黑加固
手机助手
网购先赔
系统优化
弹窗拦截
软件净化
上网加速
文件堡垒
文件粉碎机
垃圾清理
进程追踪器
杀毒擦家
系统急救
杀毒急救盘
系统急救箱
断网急救箱
备份助手
系统重装
修复杀毒
自定义扫描
宏病毒扫描
弹窗拦截
软件净化

3.5 防病毒软件


系统安全
自定义扫描
宏病毒扫描
人工服务
安全沙箱
系统优化
弹窗过滤
软件管家
上网加速
文件堡垒
系统急救
杀毒急救盘
系统急救箱
断网急救箱
备份助手
自定义扫描
宏病毒扫
360隔离沙箱
功能介绍
360隔离沙箱集合智能识别与轻量的虚拟化技术。
自动识别特定软件进入沙箱，不留痕迹，让您用的省心更安心。
360隔离沙箱
状态设置
文件列表
程序列表
例外列表
高级设置
沙箱虚拟环境:已开启
隔离沙箱 - 虚拟环境已经建立，放心使用有风险软件，一切不留痕迹。
已开启
安全视频搜索
运行指定程序
清理沙箱文件
创建"隔离沙箱"桌面图标
360隔离沙箱将自动识别有风险的播放器、电子书程序，并弹窗提示您隔离运行。
当前沙箱占用空间：小于1MB
版本：3.5.0.1033

3.5 防病毒软件


打开(O)
用360压缩打开(W)
解压到(Z)...
解压到当前文件夹(G)
解压到 电子书\ (F)
打开方式(H)
使用 360解除占用
使用 360强力删除
在360隔离沙箱中运行


360隔离沙箱
功能介绍
高级设置 - 提供可选项功能设置。
您可以根据您的需求来设置这些功能。
360 隔离沙箱
状态设置
文件列表
程序列表
例外列表
高级设置
创建"隔离沙箱"桌面图标
沙箱提示设置
在系统右键菜单中增加“文件在沙箱中运行”的功能
网络连接异常时，u盘内可疑程序入沙箱运行
标示在沙箱内运行的程序
沙箱内发现木马时，立即提示拦截（建议开启）
禁止沙箱中运行的程序访问网络
64位操作系统下，强力加固模式 (实验性质功能，重启后生效)
关机清理沙箱设置
关机时自动清理沙箱内所有文件与注册表
关机时不清理沙箱，保留所有文件与注册表不被清除
关机时不清理沙箱，沙箱空间不足时自动清理，保留以下勾选的文件不清理：
百度影音、快播的缓存文件
办公文档(Office文档、PDF文档、记事本文档)
图片文件(jpg/bmp/png等常见图片格式)
音乐、视频文件(如mp3/wma/rmvb/avi等)
压缩包文件(如zip/rar/7z等)
可执行文件(exe/dll)
版本：3.5.0.1025

3.5 防病毒软件

网络病毒的体系结构