使用Stu\_pe 入口点 rva 入口点原生 映像基址 映像大小 区块对齐大小

总区块数 文件头大小 校验和 引擎014C 子系统0002

区块每块都要对齐，以1000为单位，少了要补到1000

数据目录 导入表 rva 大小 raw raw是指文件中的地址或长度

导入系统中的函数 dll kernel.dll gdi32.dll user32.dll

资源：位图，图标对话框 regis about

Ith和vnr的原理，应该是hook了api 拦截文本显示过程

特殊码原理

Sfx真正的入口点

日文编码一般高位是80

调试选项的配置很重要，并不是功能越多越好，有些功能开了反而被利用

F12停止程序 黑箱子测试

字符串:文件名

API 消息 代码还原 结构识别 错误处理 壳 常见反调试手段

系统中各种结构，表，信息 pe的各种地址 函数dll地址

学会自己正向研究

现在开始，进行完整的研究，对每个例子都进行详细的研究，从pe到函数还原

OD各项功能的仔细研究

查询十进制 ? 在modify里可以查

下面任务栏可以查asciii码

修改寄存器modify eip可以直接跳转 修改内存数据和指令

修改指令 撤销指令

交换xchg

数学指令 有符号乘法

条件 显示跳转方向

字符串操作指令 movs movs [] [] rep重复 movs

映像基址

日志 可执行模块（入口，大小） 调用堆栈 资源 cpu run trace

查找函数

Hit跟踪 run跟踪 查看调用树 查找:模块中的名字 所有参考字符串 数字 当前模块

所有分支 所有模块间调用

分析代码