# 1.什么是PEDoll

PeDoll是一款基于inline Hook的程序行为分析软件,主要包括以下功能

1.对关键API调用进行Hook生成报表,监视程序行为

2.运行时修改程序执行代码

3.程序的网络抓包,写入数据的Dump

4.软件实现的自旋锁断点,方便与[OllyDbg](https://link.zhihu.com/?target=https%3A//www.52pojie.cn/thread-350397-1-1.html" \t "_blank)联合调试

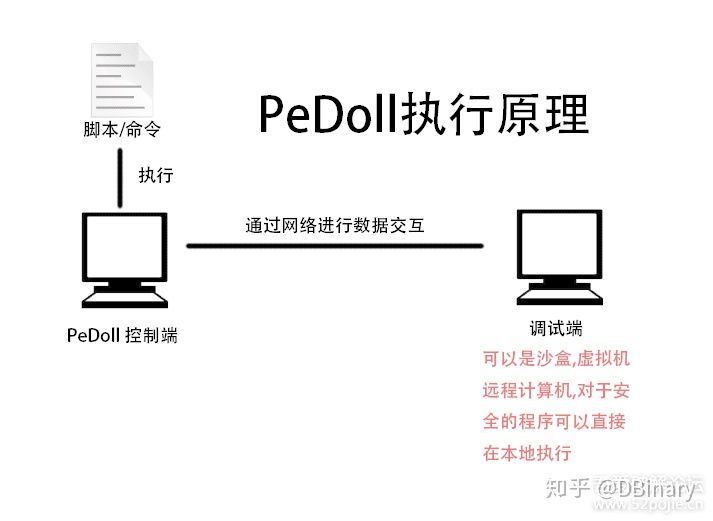
5.分析目标程序的内存,分析栈数据实现[破解](https://link.zhihu.com/?target=https%3A//www.52pojie.cn/" \t "_blank).

# 2.PeDoll的组成原理

PeDoll 主要面向逆向分析初学者或者是具有一定编程逆向基础的Cracker,旨在简化逆向分析工作,可以在一定程度上对一些具有反逆向功能的恶意程序(加壳,加花,反调试器)简化分析难度或实现自动化分析

PeDoll是基于简单脚本(命令)控制的行为分析软件,通过对不同的程序编写不同的脚本实现特定的分析,同时PeDoll是一款远程分析调试器,这也意味着在对恶意程序分析中控制端和调试端分开进行是被建议的

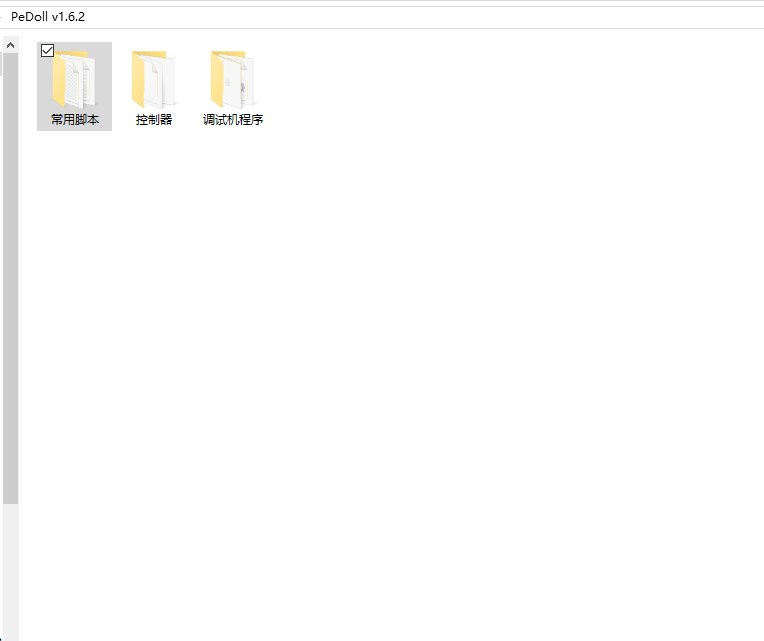
其运行原理如下所示



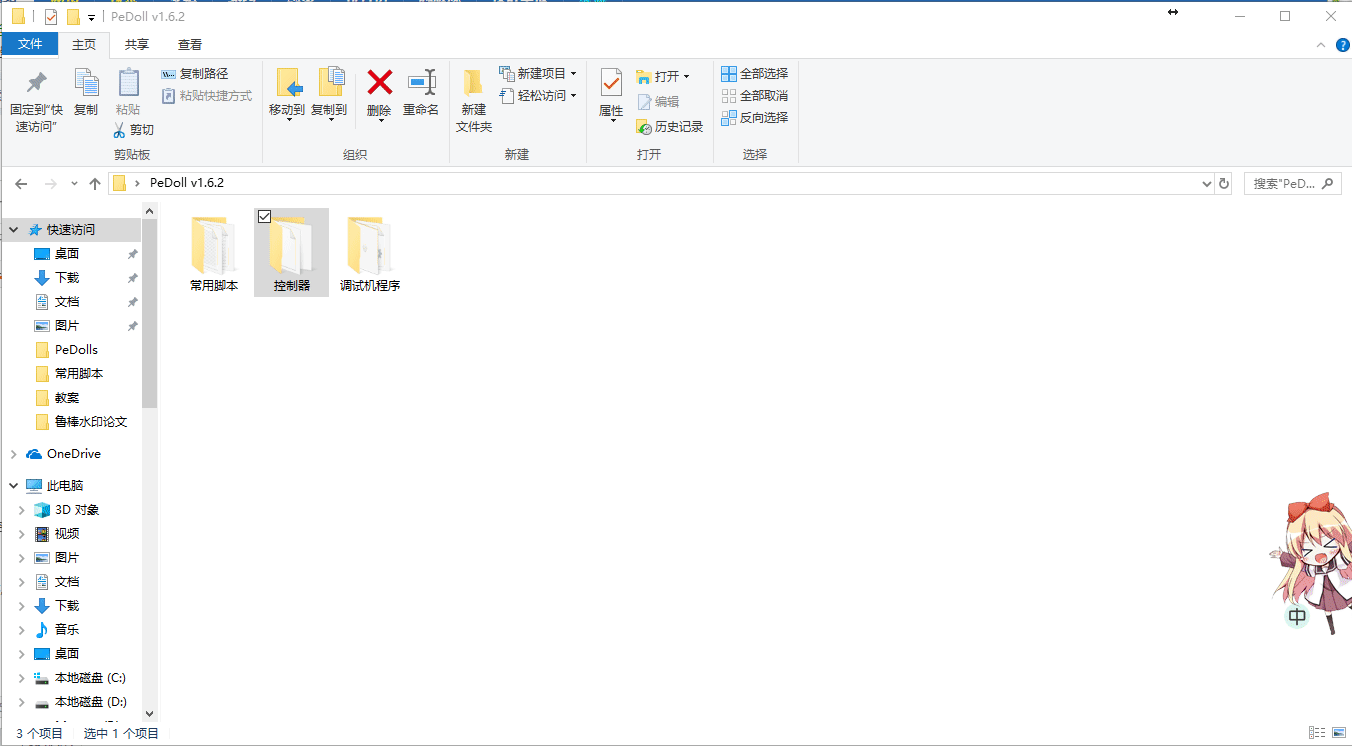
PeDoll包含三个文件夹



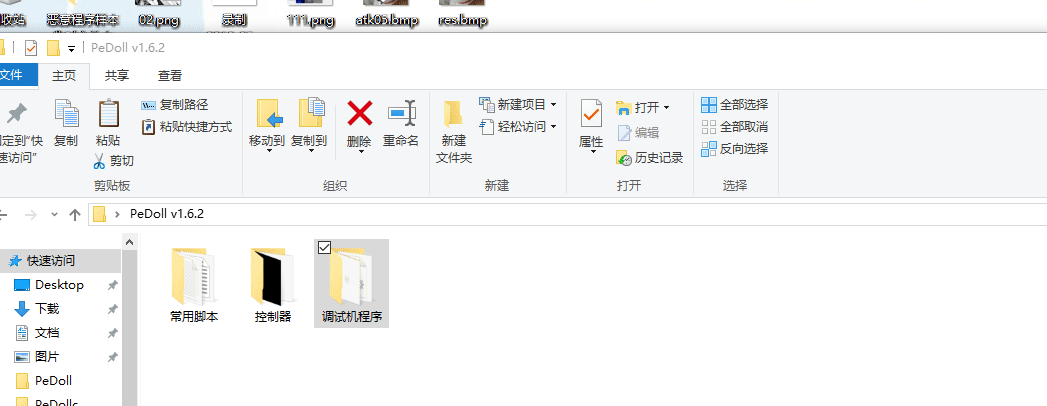
1.常用脚本,包括一系列已经编写好的常用脚本,包括一些常用的对MBR勒索病毒,用户锁勒索病毒,易语言注册码破解,网络抓包分析,远程注入代码分析.....等常用脚本



2.控制器,在控制端执行的程序



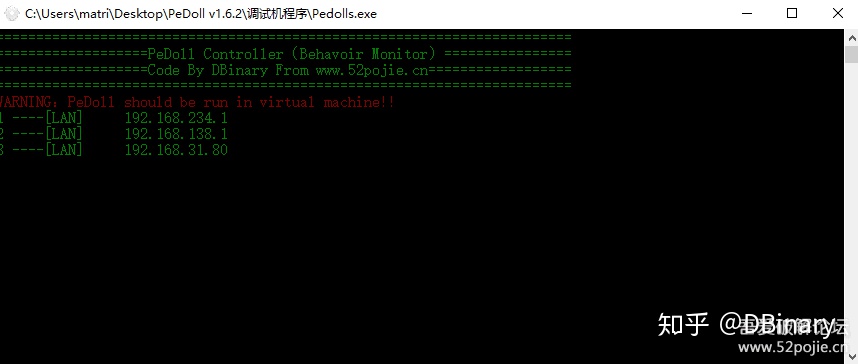
3.调试机程序,需要拷贝到调试机或其他安全环境中执行的程序(可信程序可以直接在本机执行)



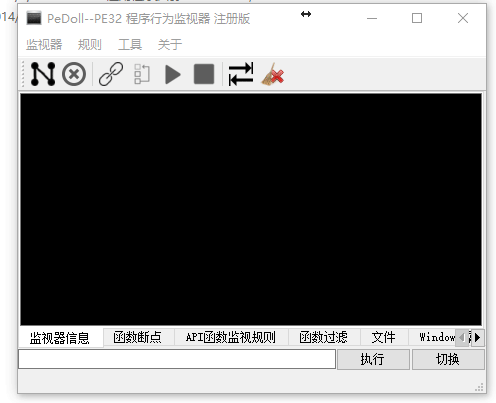
PS:其中PE.dll是PEDoll完成DLL注入的并执行inline hook的文件,PeDolls.exe用于执行注入,执行可执行文件与控制端进行交互等操作,PeDolls.exe可以在注入成功后关闭不影响调试

# 3.部署PeDoll调试环境

记录调试机上的IP地址(假设调试机和控制机在同一内网中)



将它填写在控制端中,并点击连接按钮



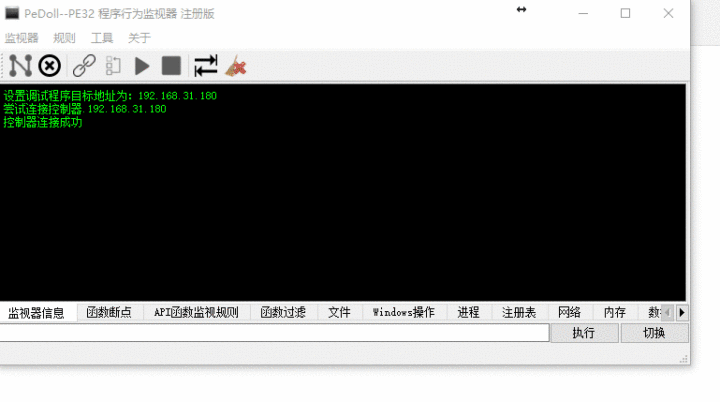
至此完成PeDoll的部署

# 4.范例1 使用PeDoll分析Net user勒索程序

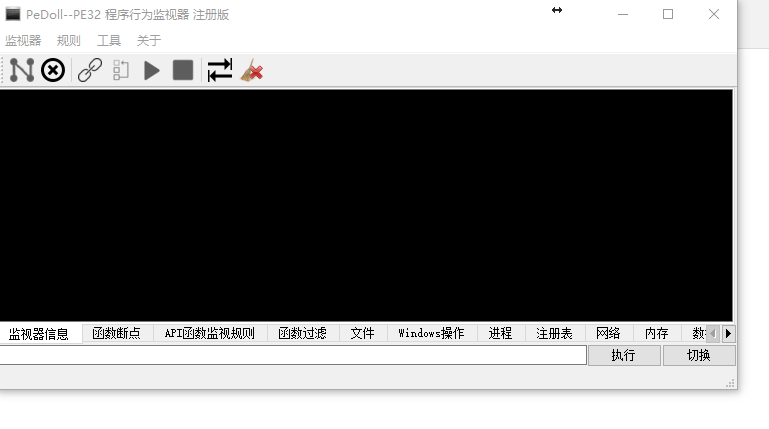
step1.将样本拷贝到调试机中,这里命名为Sample1.exe



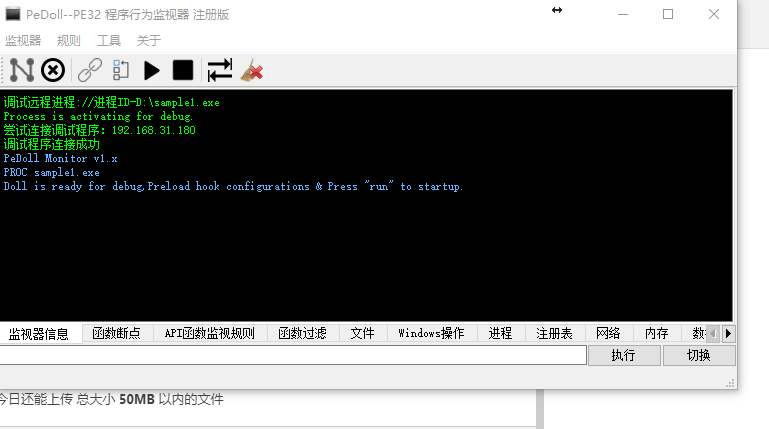
step2.加载分析脚本



step3.挂载目标程序,输入命令 doll db <D:\Sample1.exe>,回车,然后连接

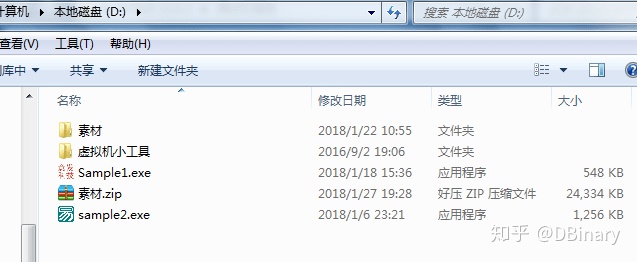


step4.执行程序,得出结果

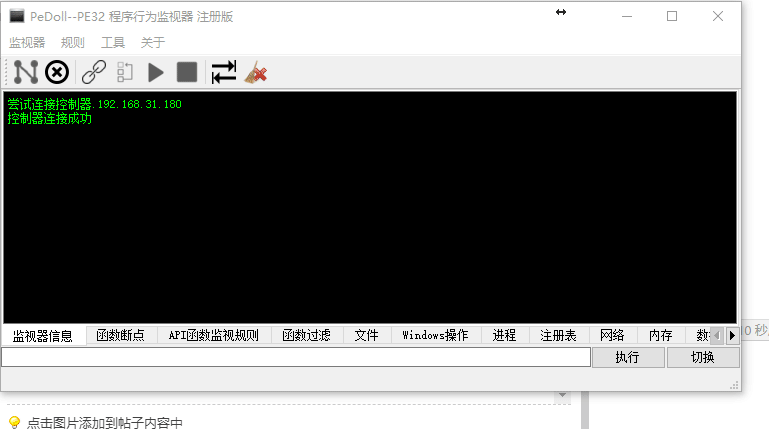


# 4.范例2 使用PeDoll使用API断点分析MBR勒索程序

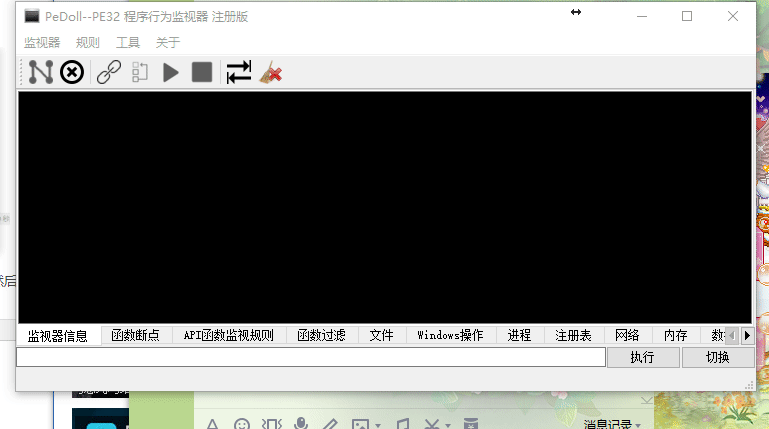
step1.重复第三节的内容,将样本拷贝到调试机中,这里为sample2.exe



step2.清理之前加载的脚本,重新挂载MBR勒索病毒脚本



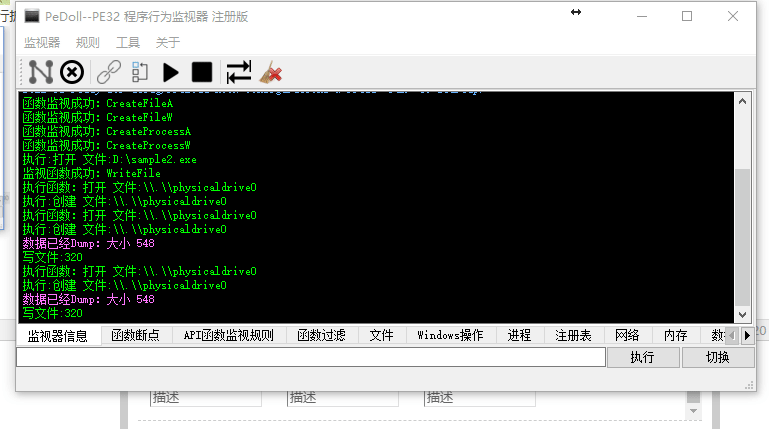
step3.挂载目标程序,输入命令 doll db <D:\Sample2.exe>,回车,然后连接,执行,触发断点



step4.命令输入hook WriteFile,监视MBR锁写入数据,然后点击执行抓取数据

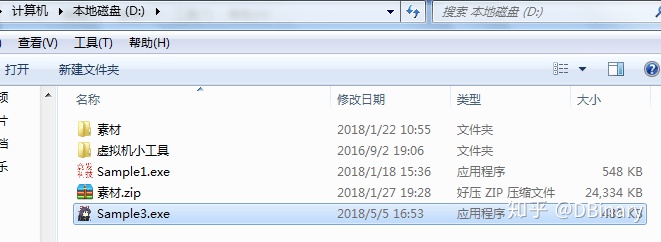


step5.在数据中查看MBR锁密码

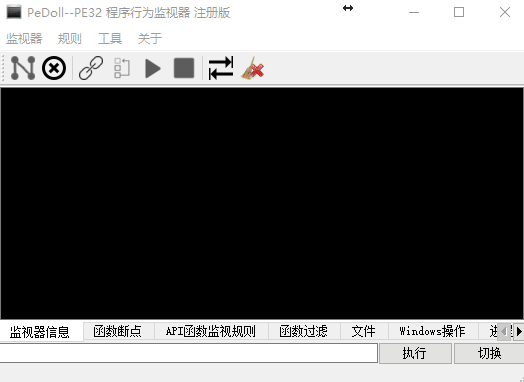


# 5.范例3 使用PeDoll binary hook分析易语言的注册码/密码

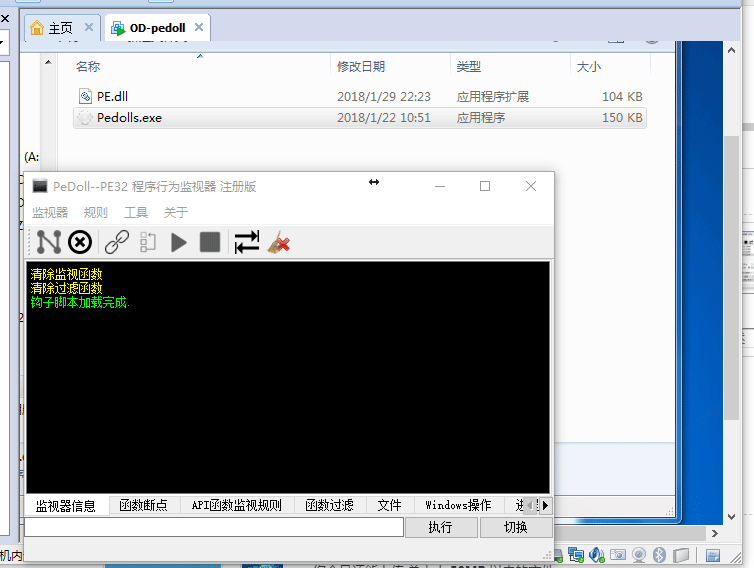
将样本拷贝到调试机中,命名为Sample3.exe



step2.清理之前加载的脚本,重新挂载易语言密码破解脚本



step3.输入命令doll db <Sample3.exe>执行程序



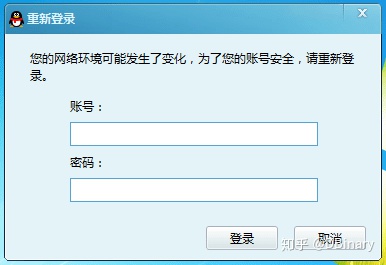
step4.执行Hook,在界面上输入任意文本密码,得出该程序的正确密码



# 6.范例4 使用PeDoll 远程注入完成对钓鱼程序的网络抓包功能

将样本拷贝到调试机中,执行

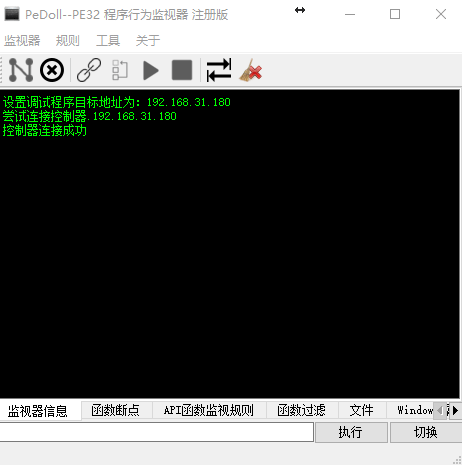
些许弹出钓鱼界面



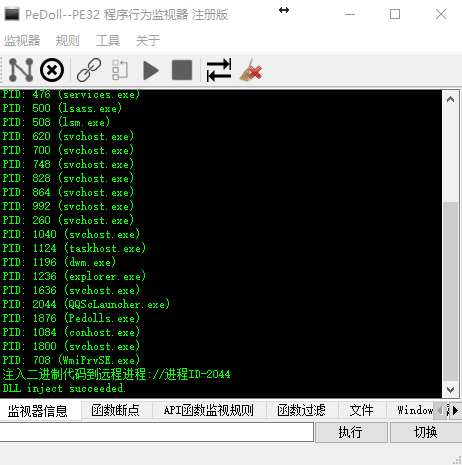
通过分析,该程序为

QQScLauncher.exe

step1.转到PeDoll控制端,输入enumprocess枚举进程,输入 doll di <PID>并注入



step2.考虑到该钓鱼样本应该为邮箱钓鱼,挂载TCP连接分析脚本



step3.点击运行,然后随便在钓鱼界面数据输入数据,等待抓包



step4.切换到数据,分析smtp数据包(钓鱼作者的邮箱账号密码都在那,BASE64解码一下大家都懂得)



# 7.如何编写PeDoll脚本

## 一.API hook

     在常用脚本的脚本编写手册中,包含了PeDoll所有支持hook 的API

     如果想要监视某一个API函数,只需要编写

     hook + 该API的函数名(大小写敏感)

     例如,我们想知道这个程序是否对文件进行的操作(假设不考虑更底层API调用),只需要对CreateFileA CreateFileW进行监视就可以了

     脚本代码如下

    hook CreateFileA

    hook CreateFileW

## 二.binary hook

     PeDoll 支持对二进制代码的直接hook,这对于一些自定义函数的hook尤为有效,注意,在进行binary hook你必须使用其他工具知晓该处代码的栈结构并且你需要在脚本中去平衡堆栈

     其代码格式为

    binary 需要hook的二进制代码16进制序列 执行完成后出栈字节数 ESP或EBP的解释方式 执行结束后EAX的值

    例如我们知道易语言字符串比较函数的特征为8B5424048B4C240885D2750D,因为是调用者清理堆栈(cdecl call)所以其出栈字节数为0

    在ESP+4和ESP+8偏移处是字符串指针 当执行结束后EAX为0是表示比对匹配,因此其代码可以写为

    binary 8B5424048B4C240885D2750D 0 S4S8 0

   其中S4表示String at ESP+4, 其中S8表示String at ESP+8

   当然,假如要解释为数字,就可以写为D4D8 表示Decimal at ESP+4, 其中S8表示Decimal at ESP+8

   同理

   B4表示String at EBP+4, 其中B8表示String at EBP+8

   E4 表示Decimal at EBP+4, 其中E8表示Decimal at EBP+8

## 三.API过滤及断点

    以CreateFileA为例,查看脚本编写手册如下说明

    API:      CreateFileA       Regular:      1.       CREATEFILEA      2.       <UNKNOW|CREATE|OPEN|RESET >      3.     <var lpFileName>

   其中1表示这个函数名,注意它是大写的

   2.表示它的三个参数,UNKNOW表示未知操作,CREATE表示创建,OPEN表示打开,RESET表示复位

   3.表示这个函数将操作的文件

   如果我们需要对这个函数进行监视,当他"打开一个"名叫123.txt时进行断点,那么代码可以这样写

  hook CreateFileA

  FILTER\_START    <---过滤器开始,如果需要设置断点,这个代码一定要先写

  CREATEFILEA <OPEN> <123.txt> QUERY SHOW

  其中,QUERY表示断点询问,当然QUERY还可以写成REJECT表示直接拒绝该函数操作,或者 TERMINATE 表示直接结束程序,如果不写或写为PASS表示默认放行

其中,参数中还支持其它比较运算符,包括(+ 包含,=全等,>大于,<小于,&与,!非)

例如

   CREATEFILEA <OPEN> <\*> QUERY SHOW 表示打开任意文件时下断点

   CREATEFILEA <OPEN> <\*123> QUERY SHOW 表示打开的文件包含123字符时断点

   CONNECT <192.168.1.1> <>1000> QUERY SHOW 表示当客户端连接192.168.1.1的端口大于1000时断点

   CONNECT <192.168.1.1> <!1000> QUERY SHOW 示当客户端连接192.168.1.1的端口不等于1000时断点

...以此类推

# 8.如何获得PeDoll

  Release 1.6.1版本-----https://pan.baidu.com/s/189\_m79g2-K0QVwkhxxSpBw

  Github 完整源代码----https://github.com/matrixcascade/PeDoll

# 9.其它

  1.PeDoll 只是简化破解的一些流程,仅仅只是挂载脚本并不能让你学会破解.

  2.pedoll logo源代码都为本人原创,允许任意修改,但在其派生及二次开发版本请注明原作者的版权信息

  3.编译环境为VisualStudio 2010 + Qt 4.8.6 Framework

  4.其它问题直接github上留言