Chinese病毒分析报告

本次样本为Synaptics挖矿木马

样本行为：

运行程序后，创建可执行文件Synaptics.exe，并在后台保持运行，修改注册表完成自启动等，获取路径系统信息，修改ini文件，截取屏幕，创建许多dll，并不断写入占用主机资源，并且会与外界主机进行通信，并且会感染同一网段中的所有主机

预防及修复措施

1、对所有涉毒服务器进行全面病毒查杀或重新安装操作系统；

2. 对临时接入终端进行准入控制，强制安装杀毒软件，并对存储介质进行病毒查杀；

急救措施：任务管理器结束Synaptics，删除开机自启，删除C:\Documents and Settings\Administrator\Local Settings\Temp和C:\WINDOWS\system32\Synaptics文件夹下新增文件。断开网络通信。

# 1.上传漏洞平台检测

<https://s.threatbook.cn/report/file/419ec2d834566eba595076e10c2c86643b19d96d5f67adc96f2c7b096479a3dc/?env=win7_sp1_enx64_office2013>

**特征值：**

文件名称：chinese.exe

MD5:439d072028f855710d8537ba8ce2f544

SHA1:100bcf72961b7fe5eb4b5deec47d3957a73f2735

**·行为签名**

一、高危行为（3）

1.持久化

·设置注册表实现自启动(reg\_key:HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Synaptics Pointing Device Driver

reg\_value:C:\ProgramData\Synaptics\Synaptics.exe)

2.一般行为

·释放了一个二进制文件并执行(C:\tmppjmeo7\.\_cache\_chinese.exe)

3.系统敏感操作

·将文件属性设置为隐藏(API:SetFileAttributesW)

1. 可疑行为（9）

1.反逆向工程

·尝试拖慢分析任务的进度

2.信息搜集

·获取按键信息(API:GetKeyState)

·安装消息钩子(API:SetWindowsHookExA)

3.一般行为

·通过COM组件访问音频的硬件信息

·创建新的文档类文件（C:\Users\vbccsb\AppData\Local\Temp\WZSE0.TMP\Chinese\Data\Manual.pdf)

4.静态文件特征

·命中了yara规则(strings ["ZItk","ZKEw"])

5.系统敏感操作

·修改网络代理设置(API:RegDeleteValueW)

·将自身拷贝到其他目录下(API:CopyFileA)

·程序出现错误时，将错误返回给调用者(API:SetErrorMode)

·修改网络代理设置(API:RegDeleteValueW)

三、低危行为（6）

1.系统环境探测

·获取系统信息(API:GetSystemInfo)

2.一般行为

·读写ini文件(C:\Windows\win.ini)

·在临时目录中创建文件(API:NtCreateFile)

·搜索并加载模块资源(API:LoadResource)

·样本从自身读取所需要的信息(API:NtReadFile)

3.系统敏感操作

·在文件系统上创建可执行文件(C:\Users\vbccsb\AppData\Local\Temp\WZSE0.TMP\Chinese\Setup.exe

,C:\tmppjmeo7\.\_cache\_chinese.exe)

**·释放文件**

一、低危文件（3）

1.RCX1D08.tmp

文件大小:744.00KB

文件路径:C:\ProgramData\Synaptics\RCX1D08.tmp

2.Chinese.lang

文件大小:561.94KB

文件路径:C:\Users\vbccsb\AppData\Local\Temp\WZSE0.TMP\Chinese\Data\Chinese.lang

3..\_cache\_chinese.exe

文件大小:3.74MB

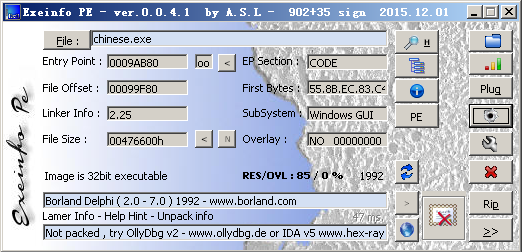
文件路径:C:\tmppjmeo7\.\_cache\_chinese.exe

1. 静态分析

**·文件类型**

Windows PE样本

**·壳检测**



入口：0009AB80

无壳

delphi语言

无随机地址

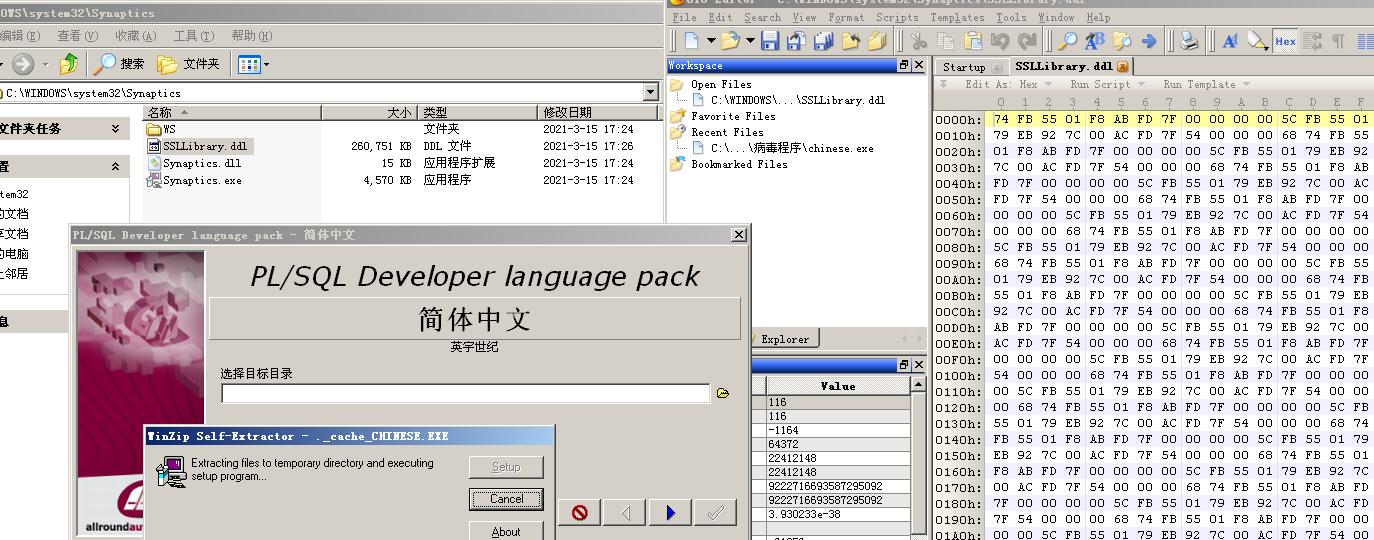
**·dependency walker分析**

程序运行后

·在成功挂接PSAPI.DLL后在当前目录创建文件.\_cache\_CHINESE.EXE

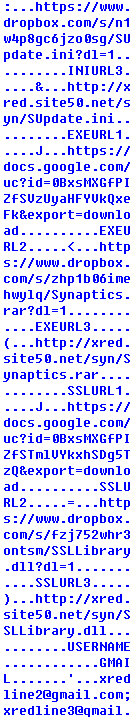


·在windows/system32/synaptics下创建synaptics.exe文件，该程序启动不断在SSLLibrary.ddl文件中写入内容74FBA901F8ABFD7F000000005CDBA90179EB927C00ACFD7F5400000068，还会创建文件夹和synaptics.dll



**·Ida-pro分析**

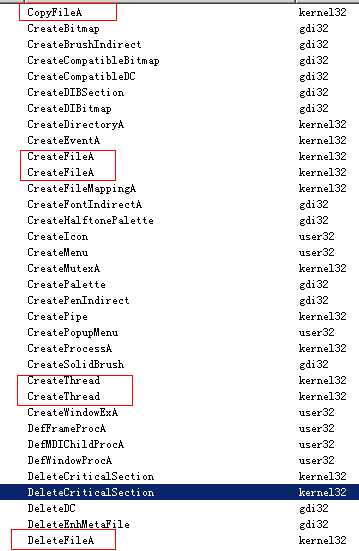
一、尝试连接外网地址并下载文件



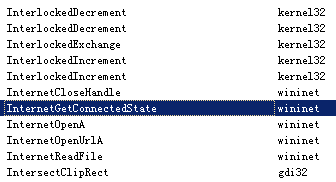
二、检测键盘输入



三、创建、复制、删除文件操作，可能存在修改、删除、复制系统关键信息的行为；



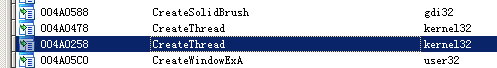
四、打开并读取某个网页操作，可能存在打开一个网络里面的URL然后在读取一些东西下来本地行为；



五、获取一个行输入，一般出现这个函数，很大程度上可能是一个后门程序；



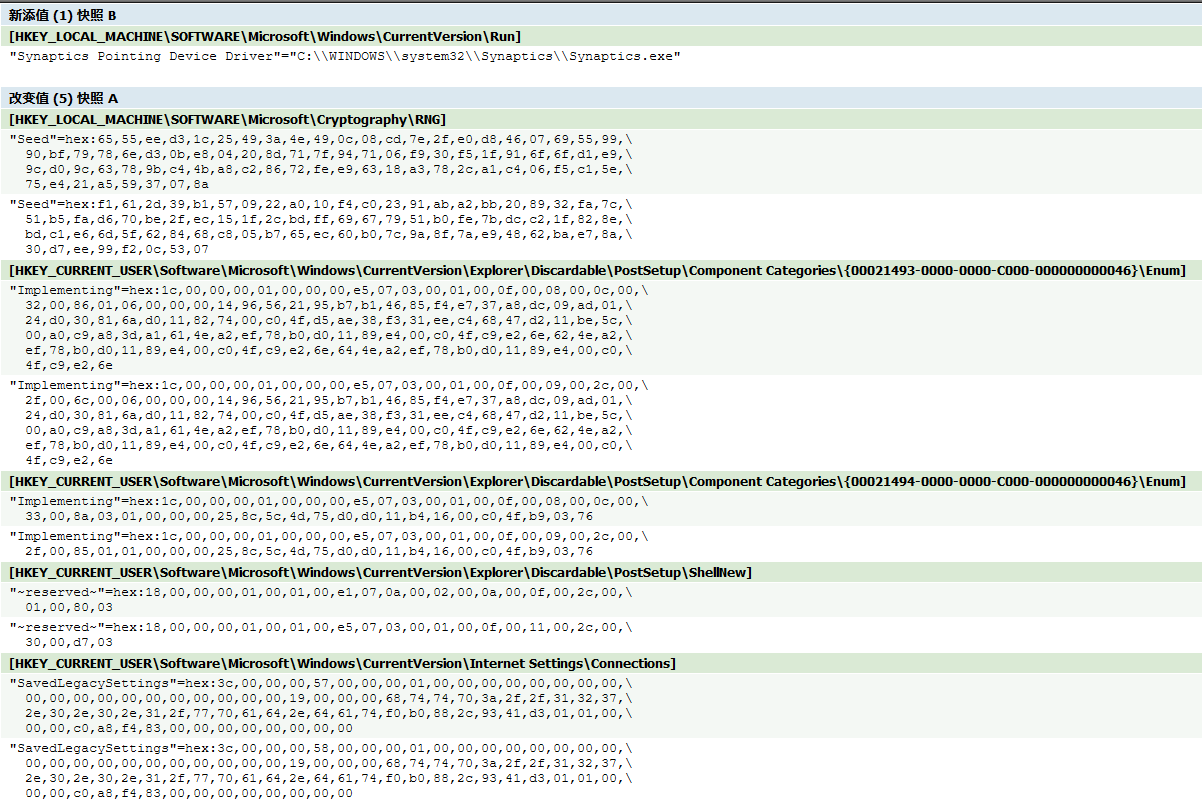
六、创建一个线程，可能存在恶意程序相互捆绑的行为；

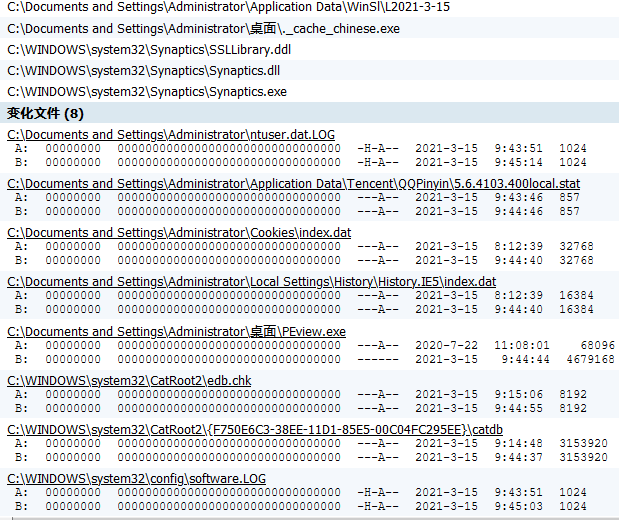


1. 动态分析

**·注册表检测**

一、注册表活动，快照b为打开病毒程序后，病毒修改自己的注册表



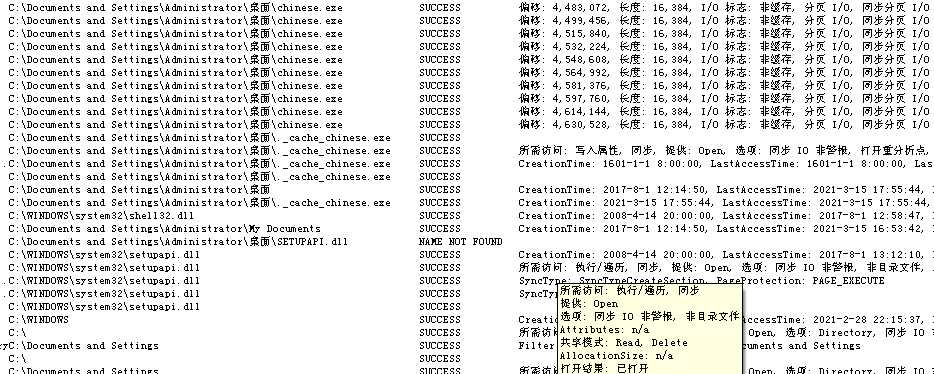


**·文件和进程检测**

一、源程序：PID:844 chinese.exe

1.文件系统活动

1.创建exe程序，查看文件



2.进程和线程活动

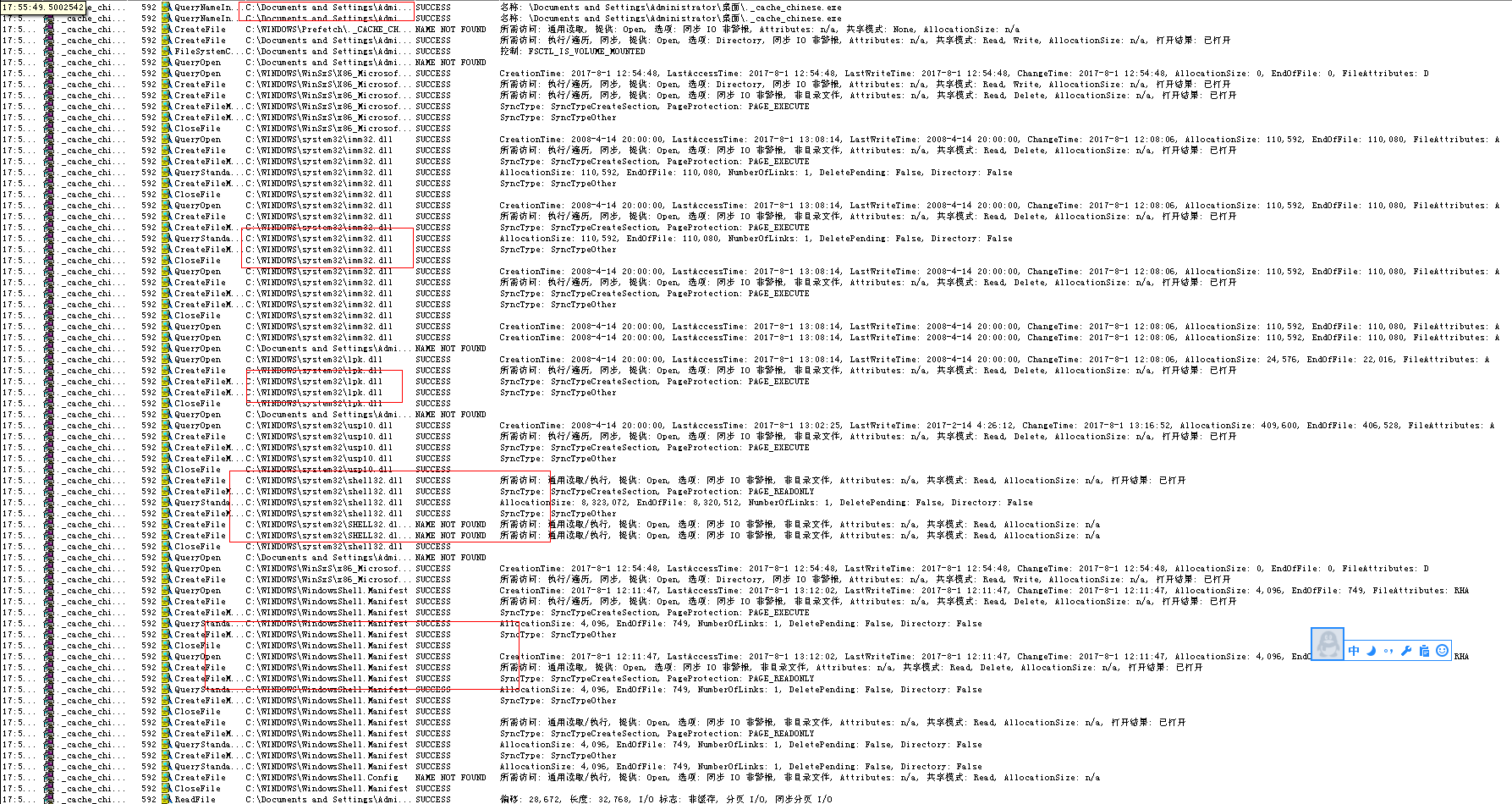
创建1条线程,2个进程，最后结束



二、创建程序：PID:592 .\_cache\_chinese.exe

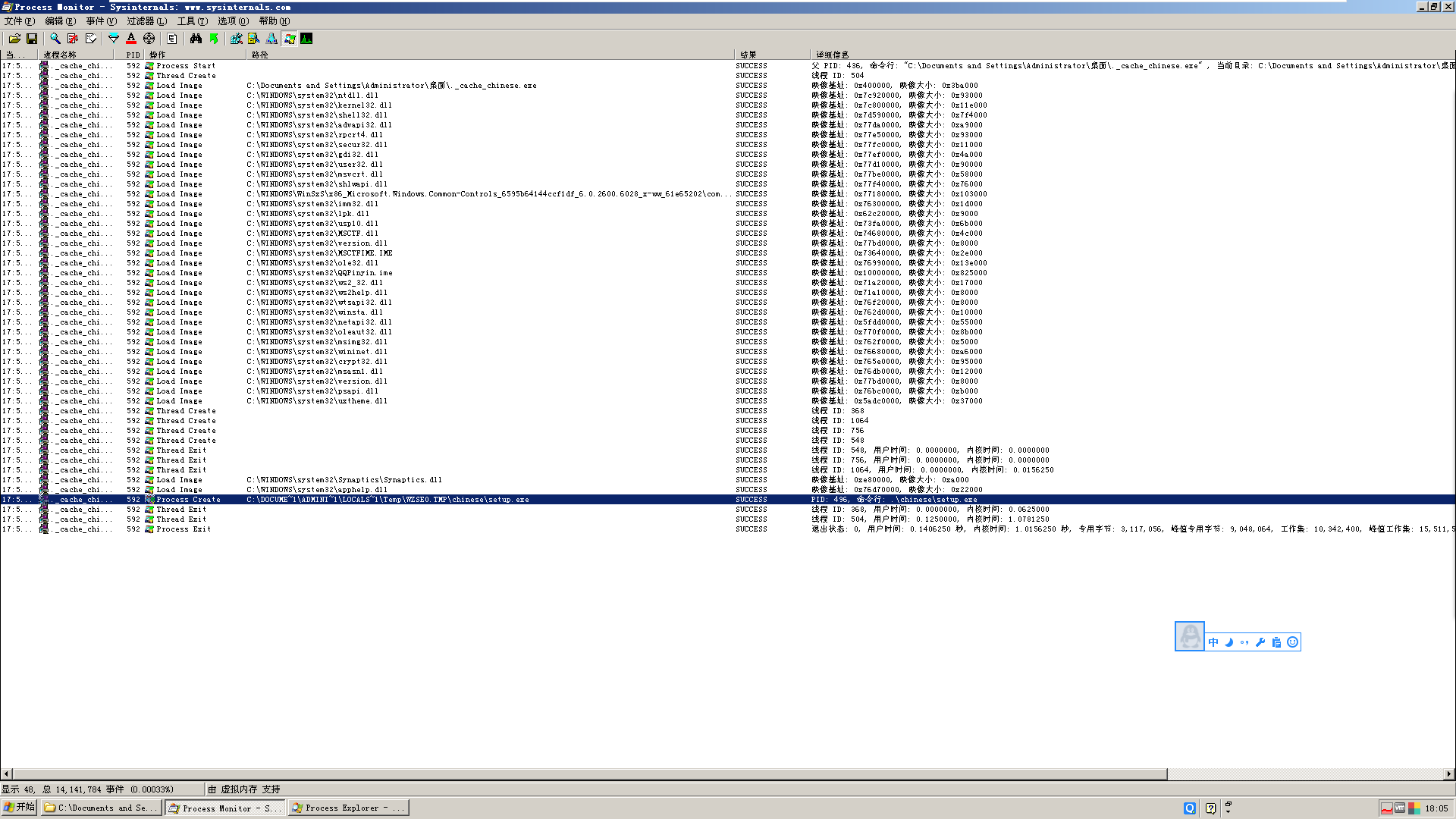
1.文件系统活动

首先在当前目录下访问dll文件，然后去系统文件夹访问



2.进程和线程活动

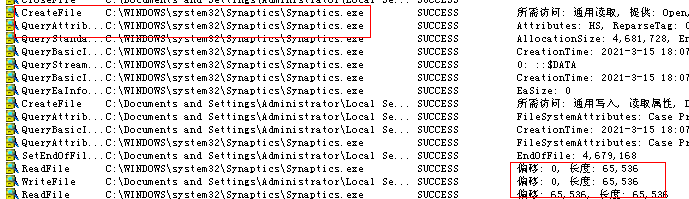
创建5条线程,创建1个程序，加载2个镜像，最后结束



三、创建程序：PID:1072 synaptics.exe

1.文件系统活动

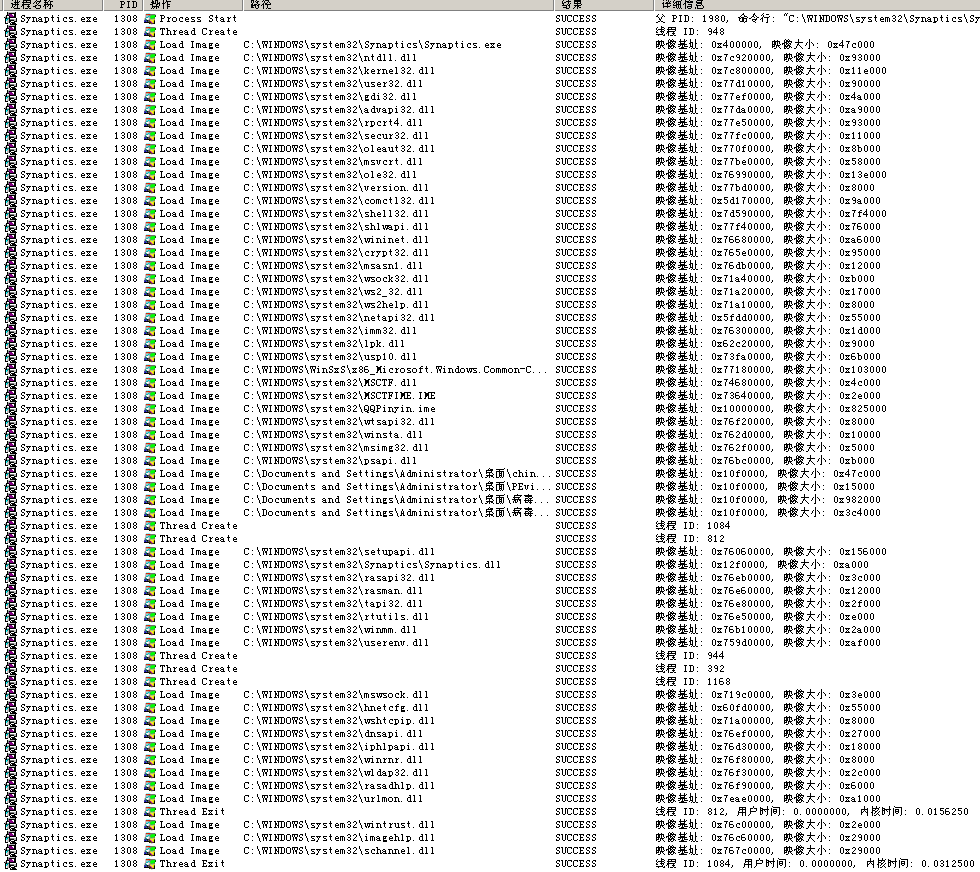
遍历目录，写入文件



一直写入文件

2.进程和线程活动

创建6条线程，最后结束



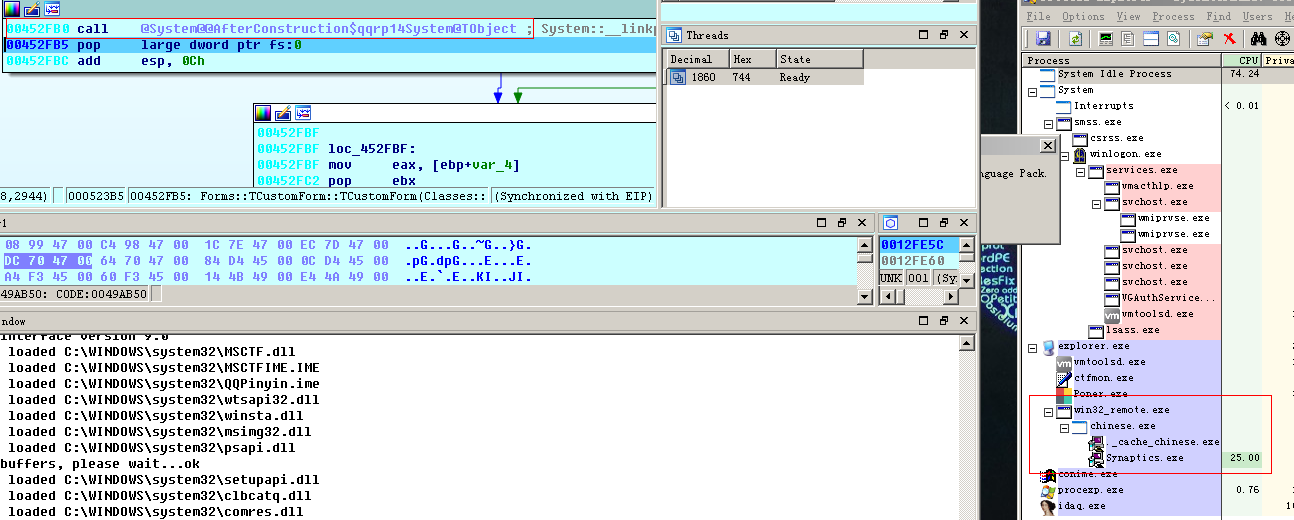
**·ida分析**

一、主要流程

1.首先在入口处下断点49ab80，然后跟进

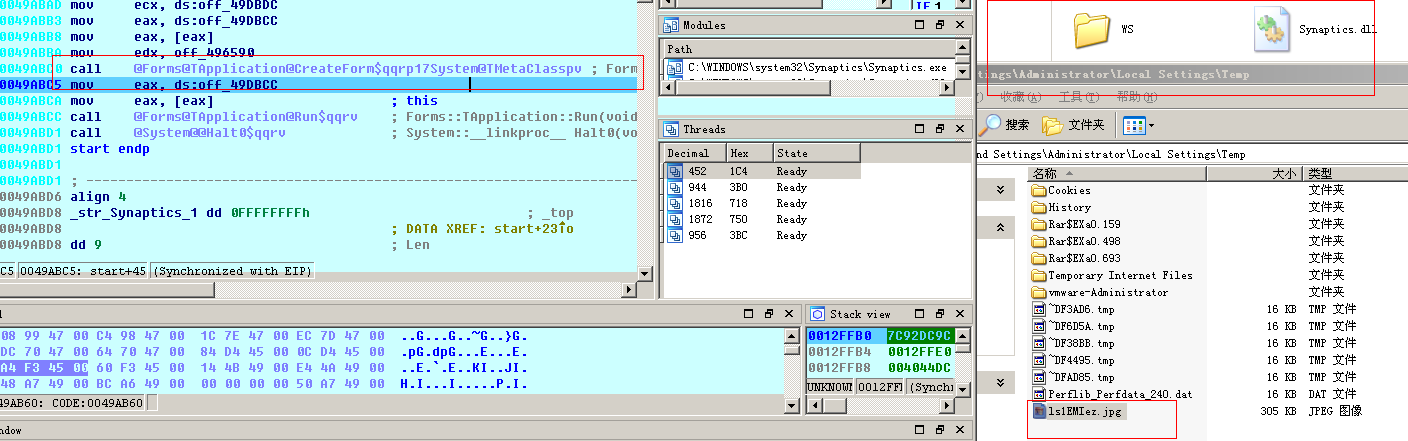


2.启动其他程序，同时创建其他文件

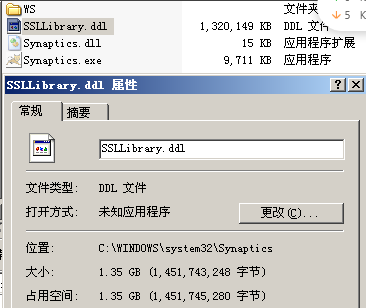


二、其他程序

1.看一下另外一个程序，对当前主机截图，创建文件

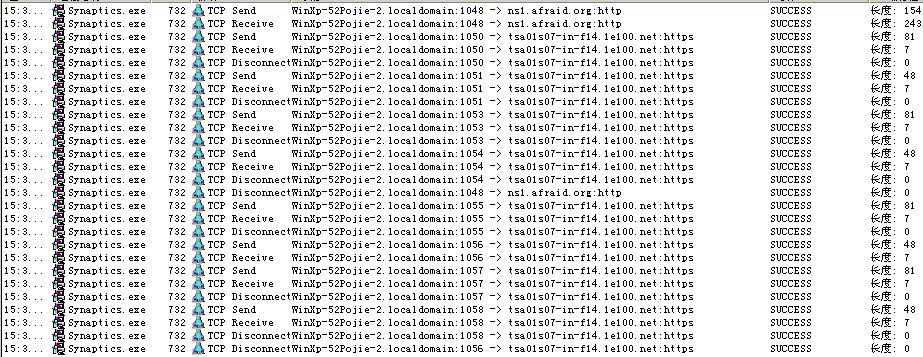


2.不停向SSLLibrary.dll文件写入，关机重启后，会继续上次位置写入



4.网络活动

一、对同网段的主机进行感染



二、对http服务器访问

