****

**分析报告**

|  |  |
| --- | --- |
| **样本名** | **永恒之蓝** |
| **班级** | **43期** |
| **作者** | **王昊** |
| **时间** | **2021.5.29** |
| **平台** | **Windows 7** |

15PB信息安全研究院(病毒分析报告)

目录

[1．样本概况 3](#_Toc2718)

[1.1 样本信息 3](#_Toc7042)

[1.1.1 基本信息 3](#_Toc29996)

[1.1.2 资源信息 3](#_Toc16989)

[1.2 测试环境及工具 4](#_Toc3760)

[1.3 查壳 4](#_Toc1715)

[2．具体行为分析 4](#_Toc23972)

[2.1 网络监控 4](#_Toc23060)

[2.2 注册表监控 4](#_Toc26220)

[2.3 文件监控 5](#_Toc27676)

[2.4 进程监控 5](#_Toc3030)

[3． 恶意代码分析 6](#_Toc18298)

[3.1 永恒之蓝母体病毒分析 6](#_Toc31876)

[3.1.1主要功能： 6](#_Toc15411)

[3.1.2恶意代码分析： 6](#_Toc23724)

[3.2 Tasksche.exe恶意代码分析 11](#_Toc10465)

[3.2.1主要功能： 11](#_Toc5844)

[3.2.2恶意代码分析： 11](#_Toc763)

[3.3 对t.wnry中解密出来的dll进行分析： 21](#_Toc21362)

[3.3.1 主要功能： 21](#_Toc15990)

[3.3.2 恶意代码分析： 21](#_Toc22175)

[4.程序行为总结 27](#_Toc30516)

[4.1 病毒母体 27](#_Toc15416)

[4.2 taskshe.exe 28](#_Toc4889)

[4.3 TaskStart核心dll 28](#_Toc3612)

[5．解决方案 28](#_Toc2510)

[参考文献 29](#_Toc19831)

# 1．样本概况

## 1.1 样本信息

**1.1.1 基本信息**

文件: C:\Users\15PB\Desktop\永恒之蓝.exe

大小: 3723264 bytes

文件版本:6.1.7601.17514 (win7sp1\_rtm.101119-1850)

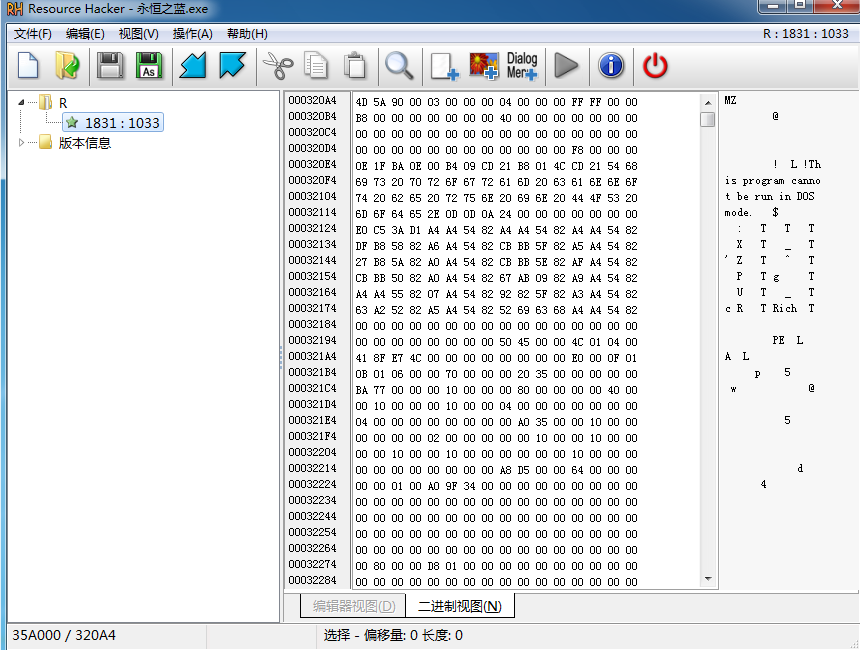
修改时间: 2017年5月13日, 13:55:05

MD5: DB349B97C37D22F5EA1D1841E3C89EB4

SHA1: E889544AFF85FFAF8B0D0DA705105DEE7C97FE26

CRC32: 9FBB1227

**1.1.2 资源信息**

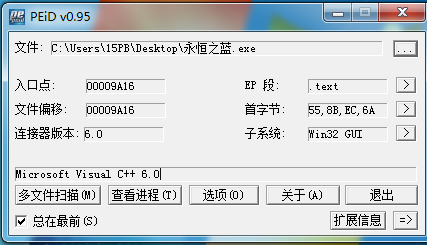


## 1.2 测试环境及工具

32位win7，火绒剑，OD，PEiD，exeinfo，IDA

## 1.3 查壳

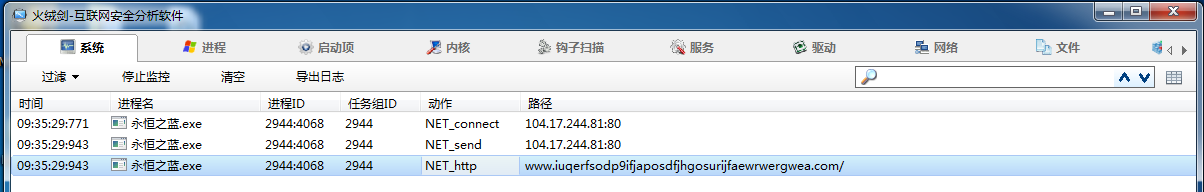
Peid工具进行壳查询：无壳，为VC6.0



# 2．具体行为分析

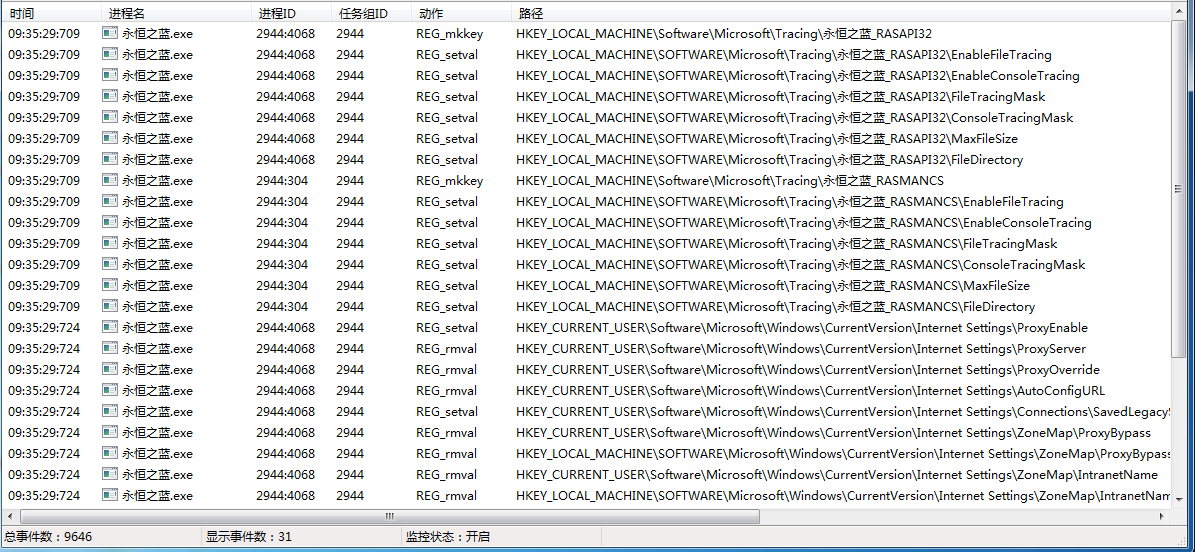
## 2.1 网络监控

对指定ip进行连接



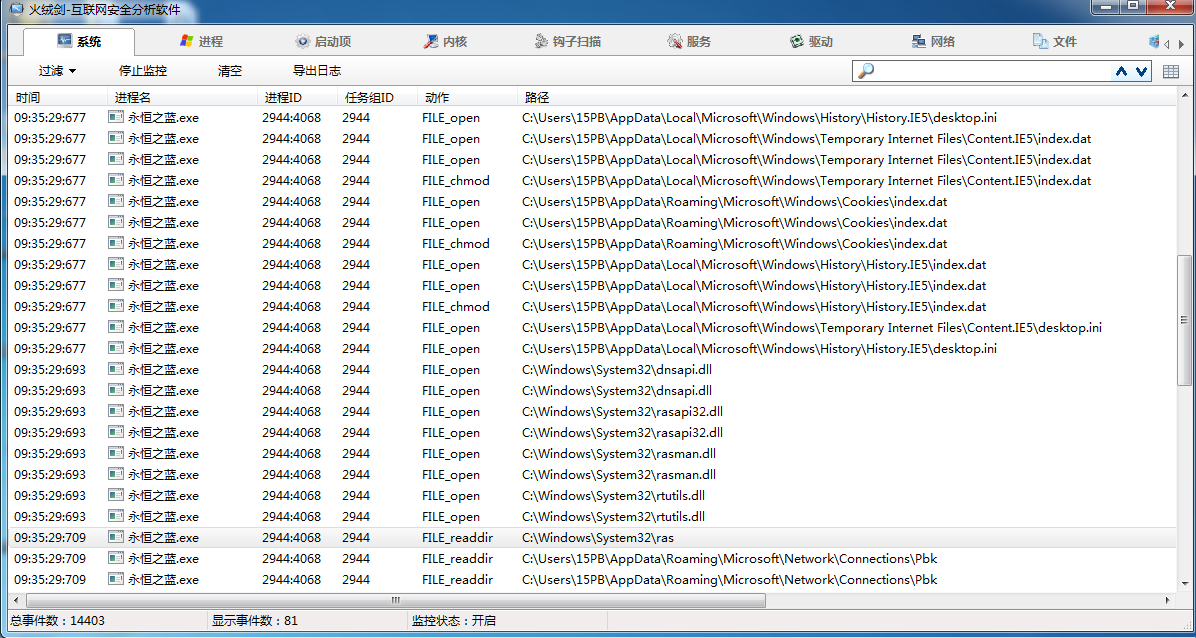
## 2.2 注册表监控

存在大量的创建注册表键值和设置注册表键值等操作



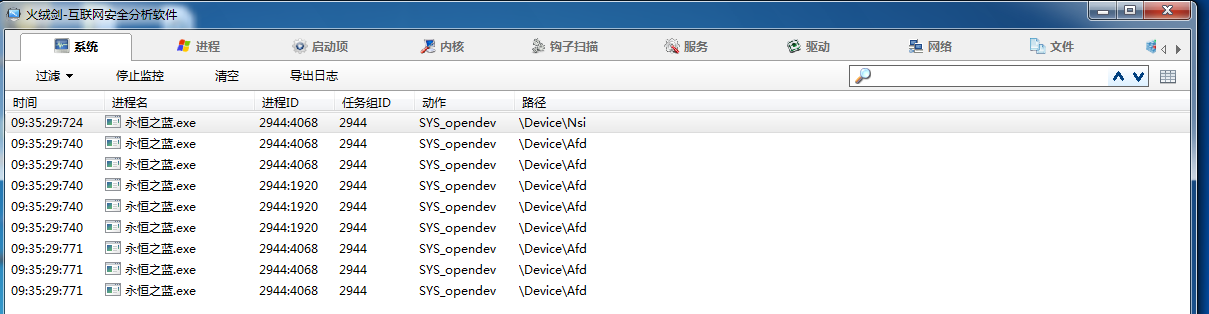
## 2.3 文件监控

进行了文件遍历，并设置了一些文件的属性

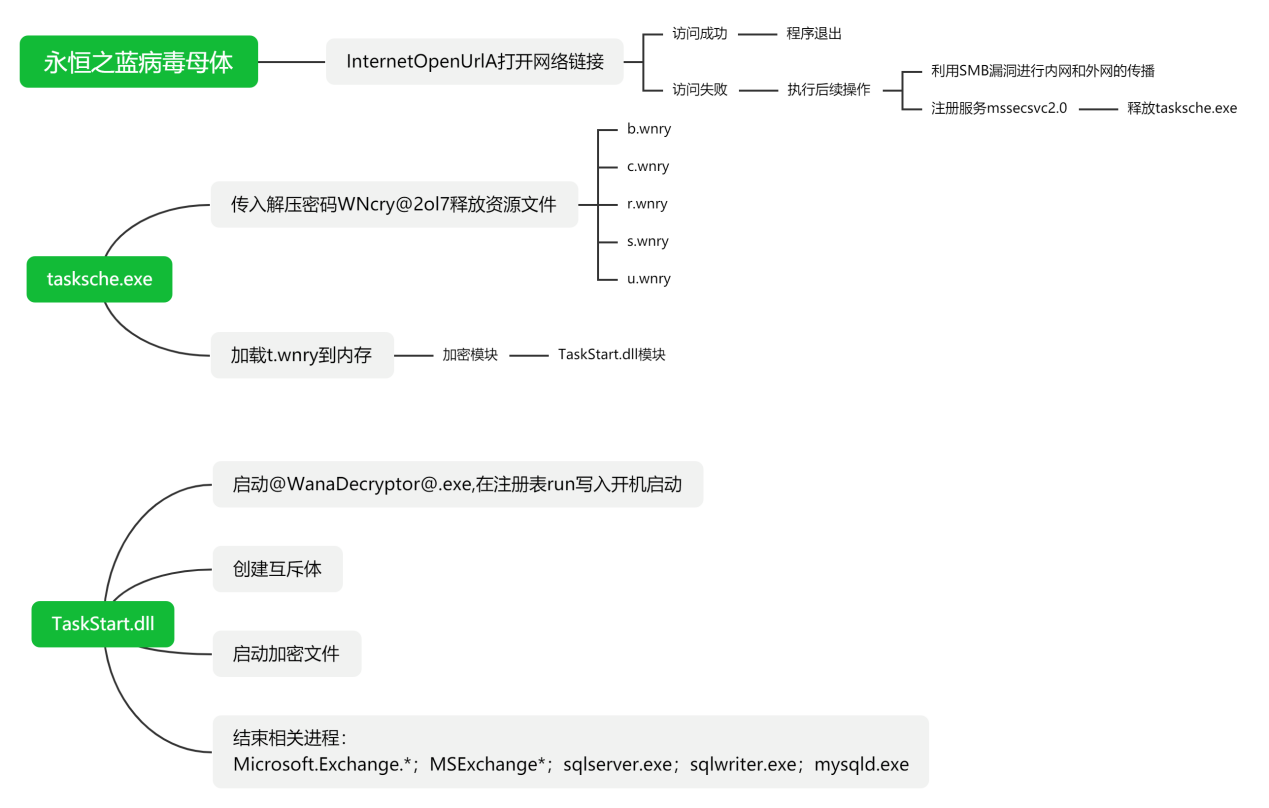


**2.4 进程监控**

打开了设备



1. **恶意代码分析**



**3.1 永恒之蓝母体病毒分析**

**3.1.1主要功能：**

1. 对网址http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com进行访问，如果访问成功，就直接结束进程，停止感染。
2. 将源程序以服务的方式创建，创建服务名为mssecsvc2.0显示名为Microsoft Security Center (2.0) Service的服务。
3. 进行内网和外网的ip感染（445端口）。
4. 释放资源tasksche.exe，并创建进程用于启动tasksche.exe。

**3.1.2恶意代码分析：**

1.访问网址，进行判断：如果访问成功，就直接结束进程，停止感染

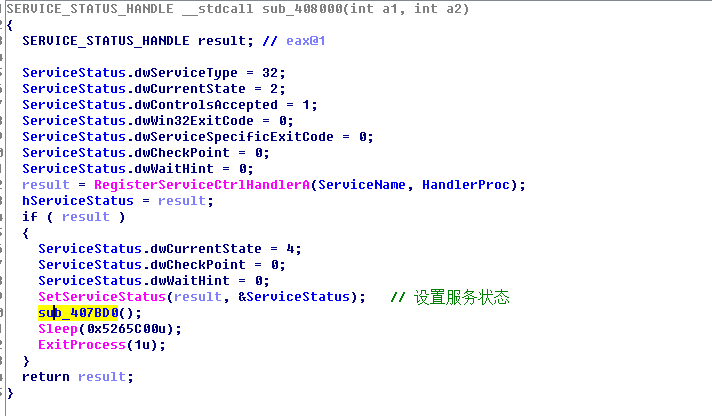


2.如果访问网址失败，进入函数sub\_408090：根据参数个数的不同进行不同的操作



3.如果参数的个数小于2时，就打开服务mssecsvc2.0，并执行回调函数sub\_408000

sub\_408000:进行网络连接，并对内网和外网进行445端口的网络攻击



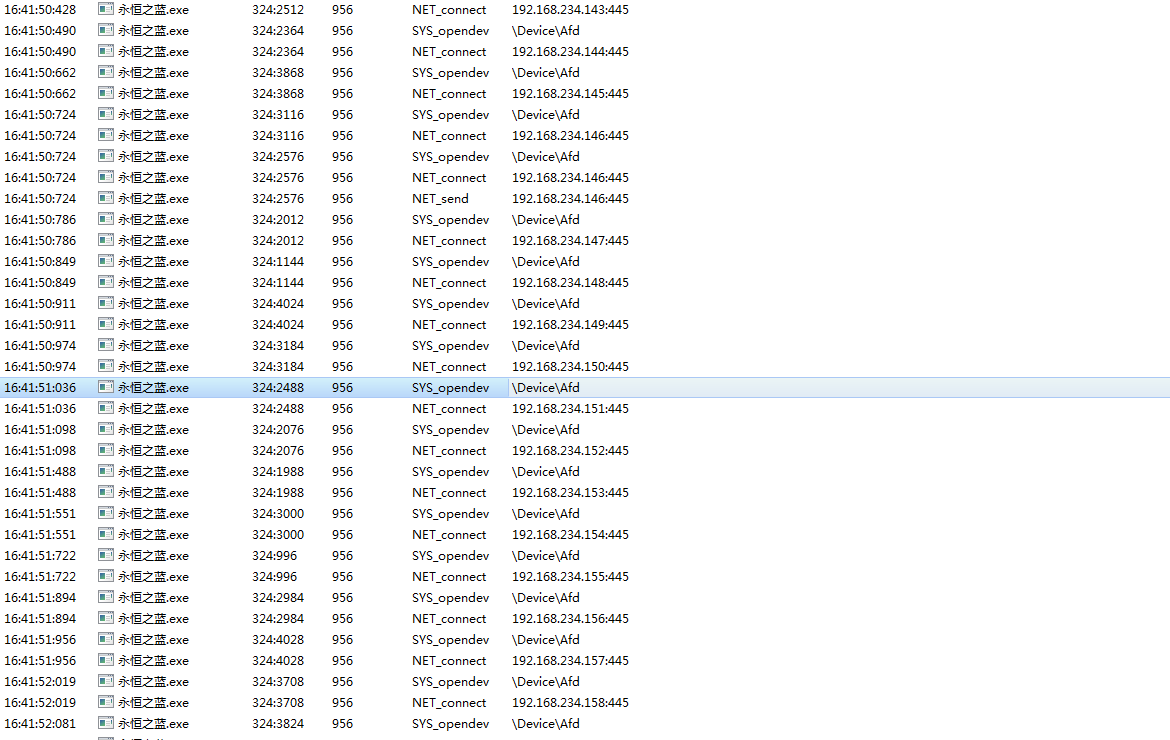
跟进函数407BD0：



线程回调函数sub\_407720:进行网络连接，并对内网ip进行攻击



对其线程进行x32dbg动态调试，并用火绒剑进行行为监控：

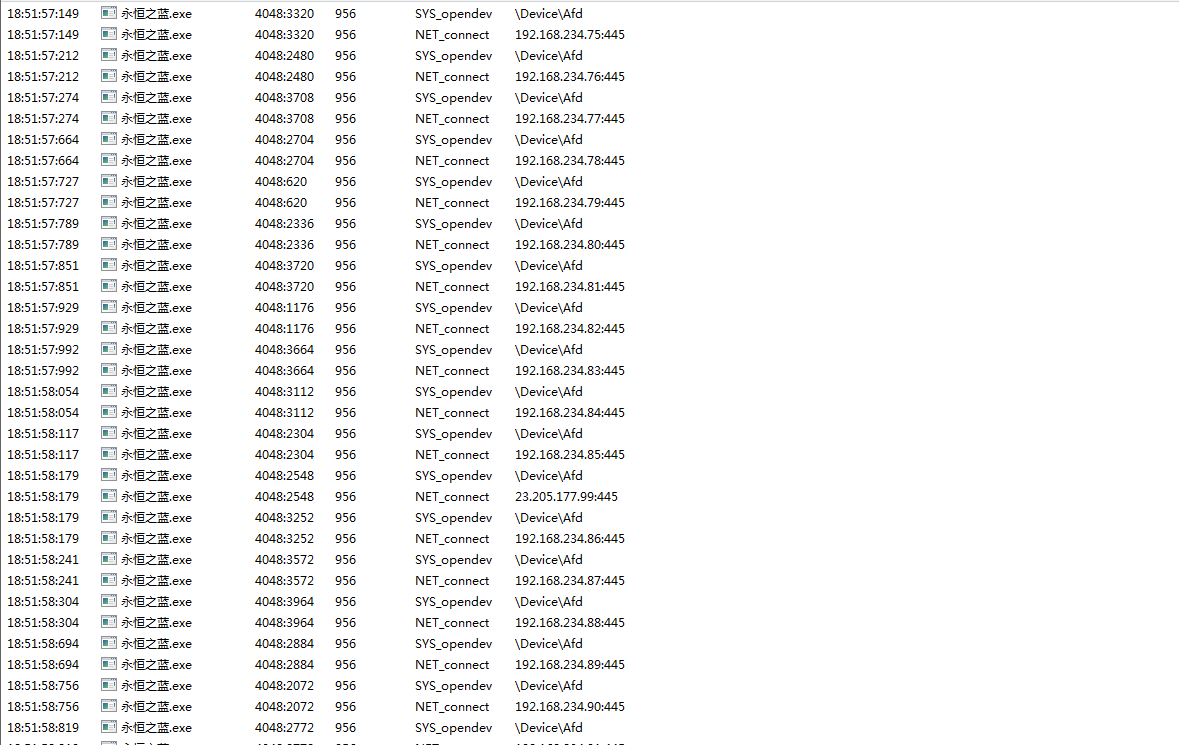


发现其在对局域网内所有ip进行445端口的连接以及攻击。

线程回调函数sub\_407840:

同理，对其进行x32dbg动态分析，并结合火绒剑进行行为监控：

可以推测该回调函数应该是随机对外网ip的445端口发起攻击

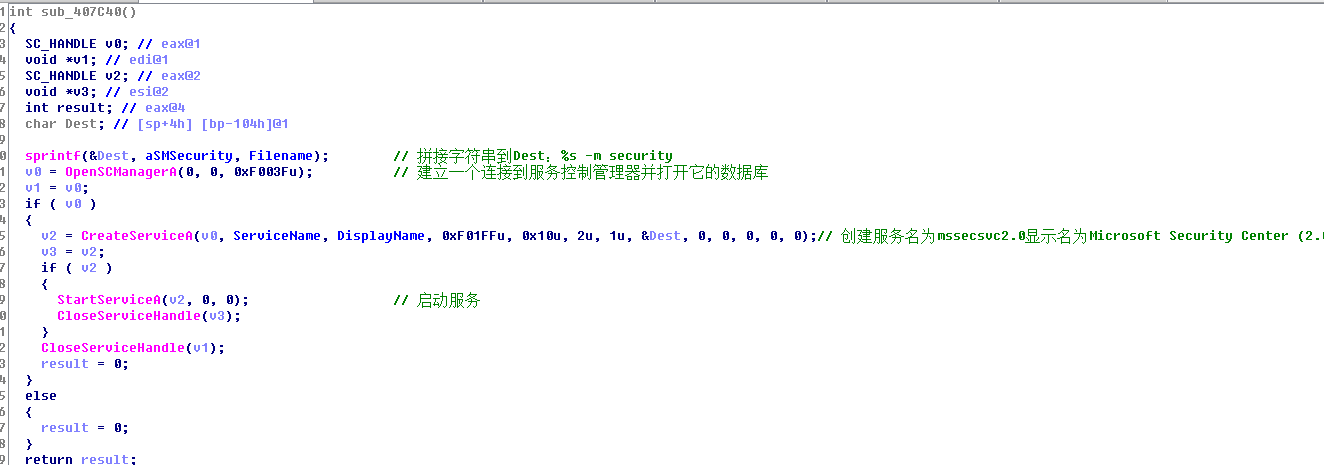


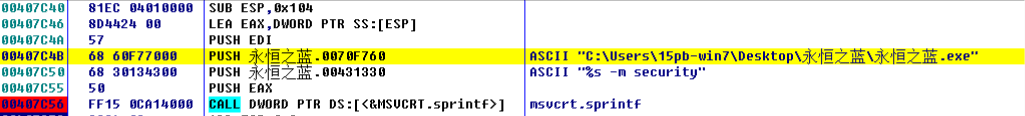
4.如果参数的个数为2时，进行函数sub\_407F20:



sub\_407C40:

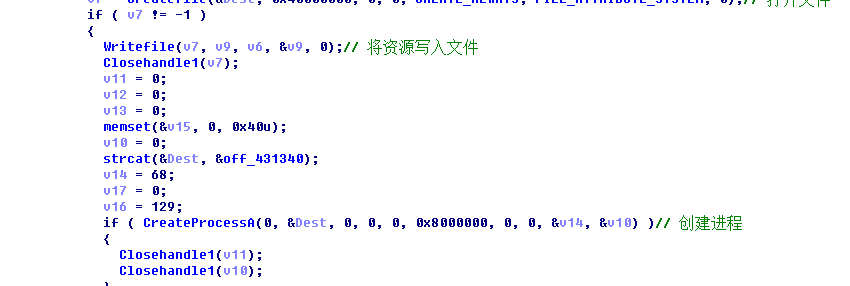
获取当前病毒完整路径，并将其以服务的方式创建，创建服务名为mssecsvc2.0显示名为Microsoft Security Center (2.0) Service的服务。





sub\_407CE0:加载资源,并打开C:Windows\tasksche.exe,如果打开失败，就把资源写入"C:\windows\tasksche.exe"，并创建一个进程用于启动tasksche.exe。





**3.2 Tasksche.exe恶意代码分析**

**3.2.1主要功能：**

1. 传入解压密码WNcry@2ol7，解压资源文件
2. 导入RSA公钥和AES私钥
3. 内存加载t.wnry,并释放核心代码TaskStart

**3.2.2恶意代码分析：**

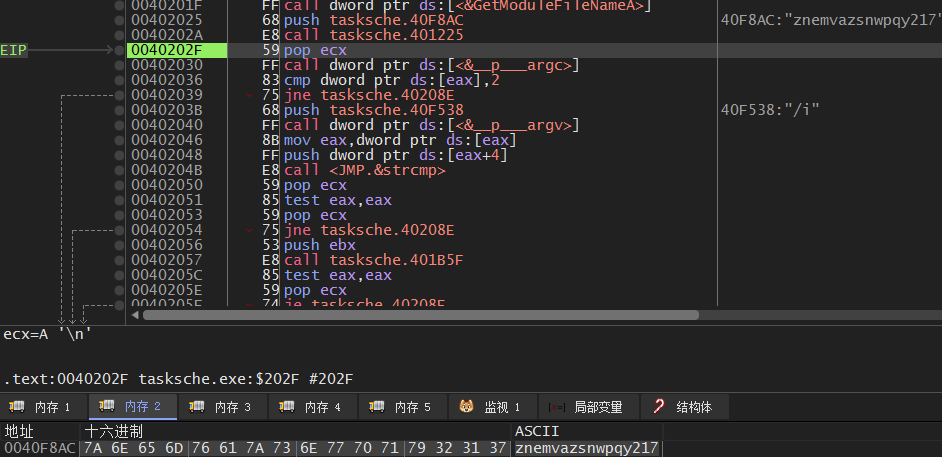
外部总体分析：

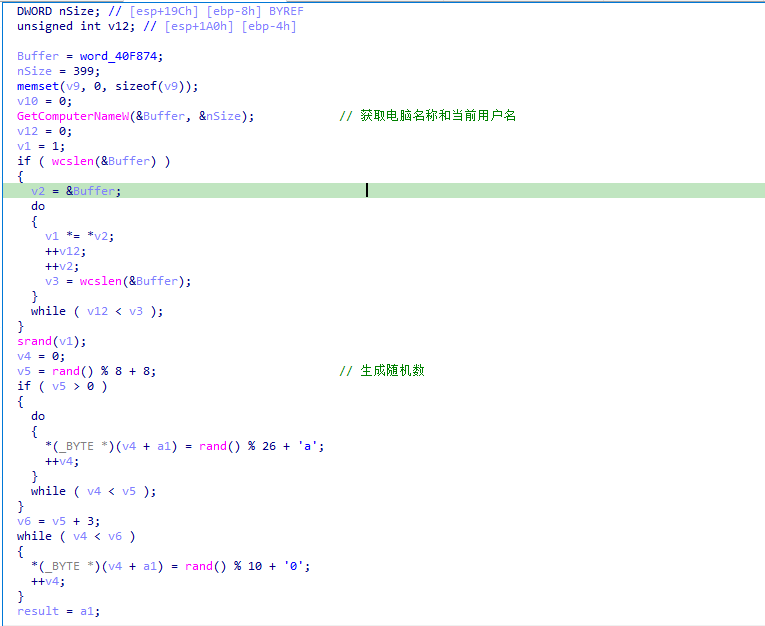


函数分析：

1.sub\_401225:

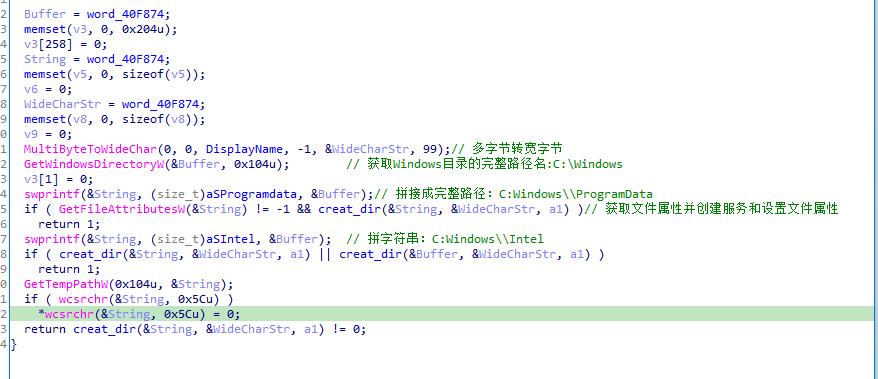
获取电脑名称和用户名，并生成一串随机字符串作为服务名：



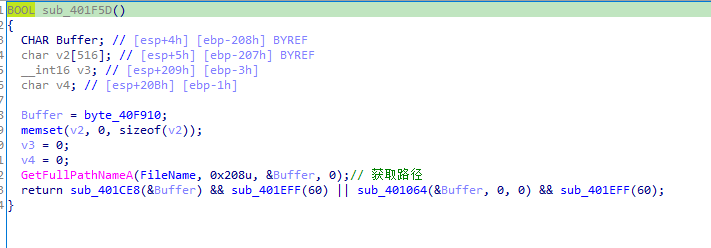


2.sub\_401B5F:

根据条件判定创建C:Windows\\ProgramData的目录或者创建C:Windows\\Intel的目录



3.sub\_401F5D:

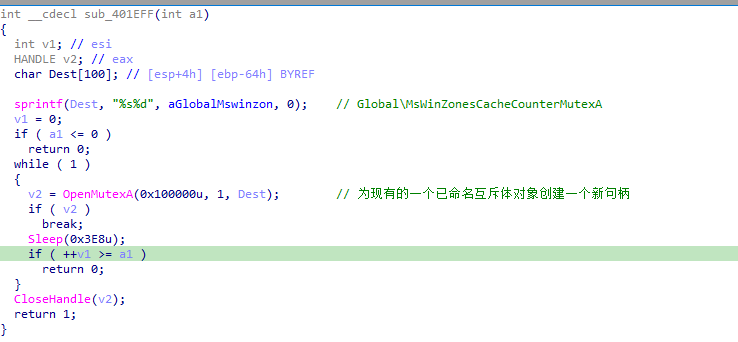


分别对return后面跟的3个函数进行分析：

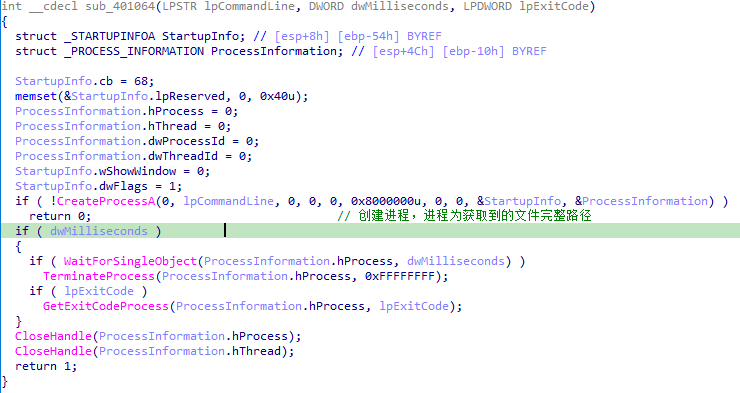
sub\_401CE8:打开随机生成的字符串名字的服务，如果打开成功就启动服务，如果打开失败，就再次创建服务，再启动服务。



sub\_401EFF:发现有互斥体的相关操作，应该是防止多个实例运行



sub\_401064:创建了一个进程，并等待其执行结束。

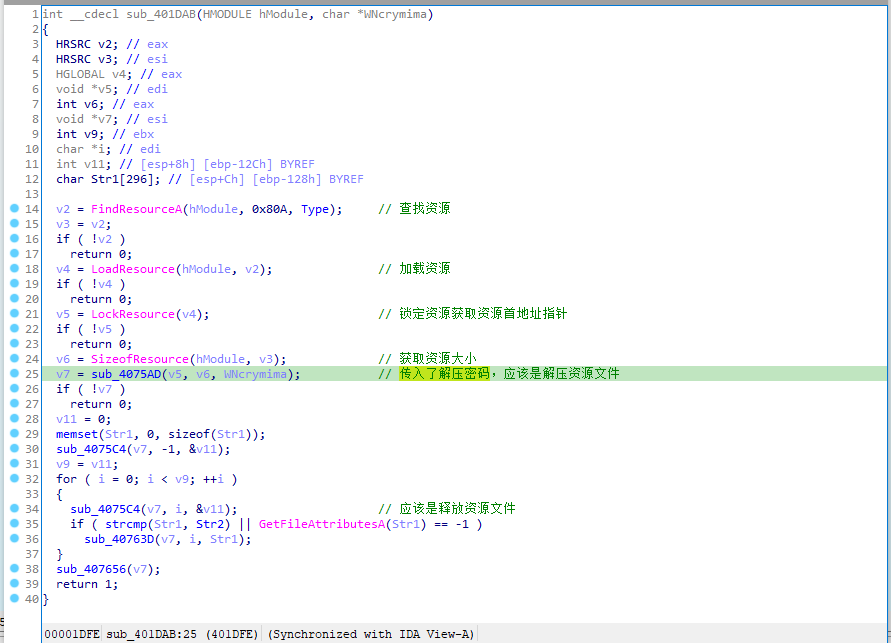


4.sub\_4010FD:创建注册表键值：HKEY\_CURRENT\_USER\Software\WanaCrypt0r并设置键值到获取到的当前目录下。

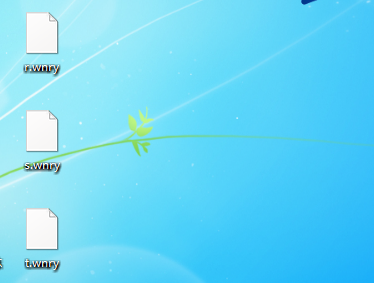
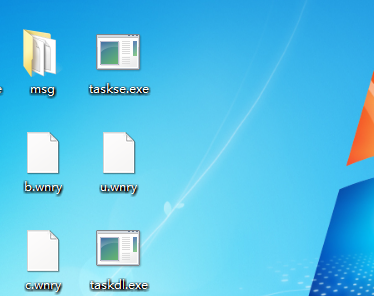


5.sub\_401DAB:

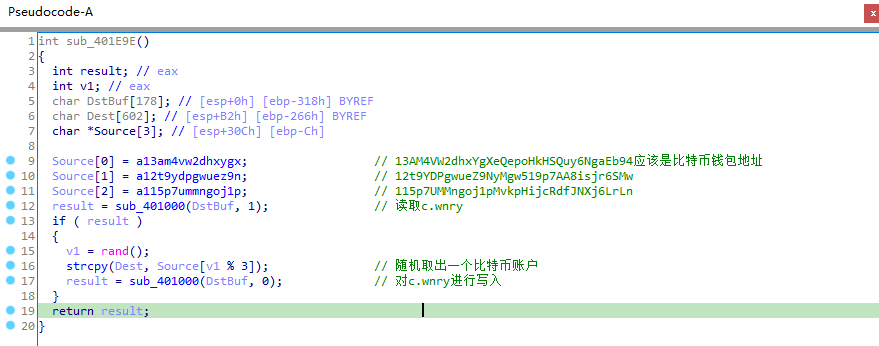
传入解压密码传入解压密码WNcry@2ol7，并可以看到释放资源所用到的几个API，可以判断该函数应该是用来解压并释放资源压缩包的



再通过x32dbg进行动态调试，观察是否有资源被释放：发现的确有资源被释放至桌面。



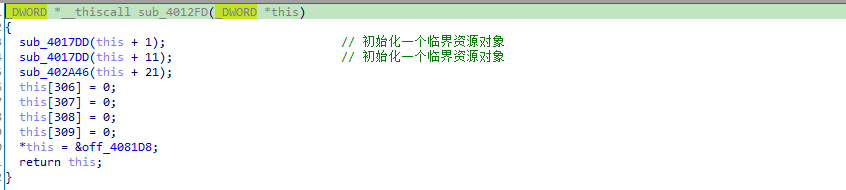
6.sub\_401E9E:应该是从三个比特币账户中随机挑选一个写入到c.wnry文件中



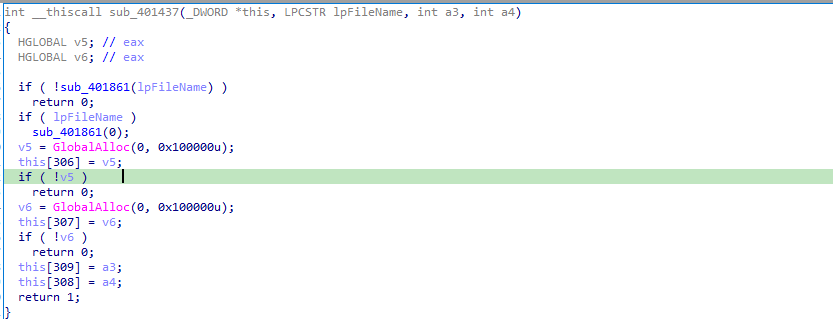
7.sub\_40170A:加载模块，并获取函数地址



8.sub\_4012FD:传入了this指针，应该是类内用于初始化的构造函数



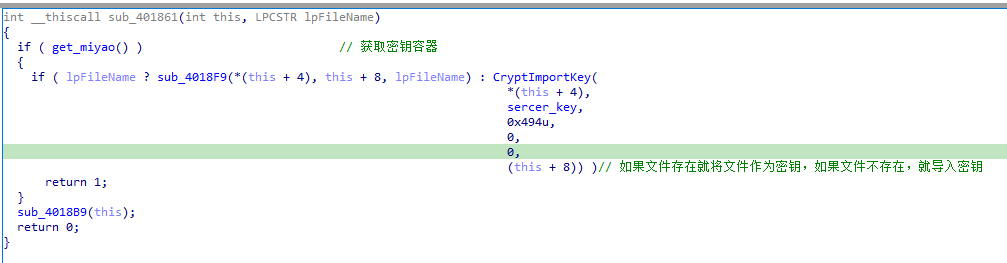
9.sub\_401437:主要功能：导入RSA公钥秘钥



跟进sub\_401861:

可以看出调用了调用了秘钥容器的相关API，并导入的秘钥,并且跟进sercer\_key数据区可以看到RSA标志：

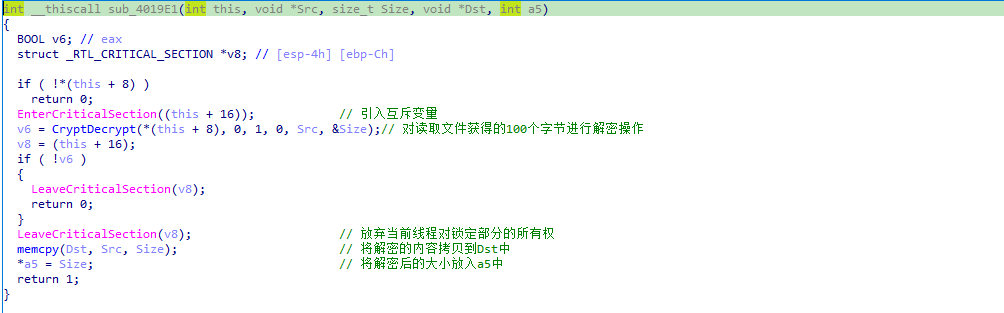




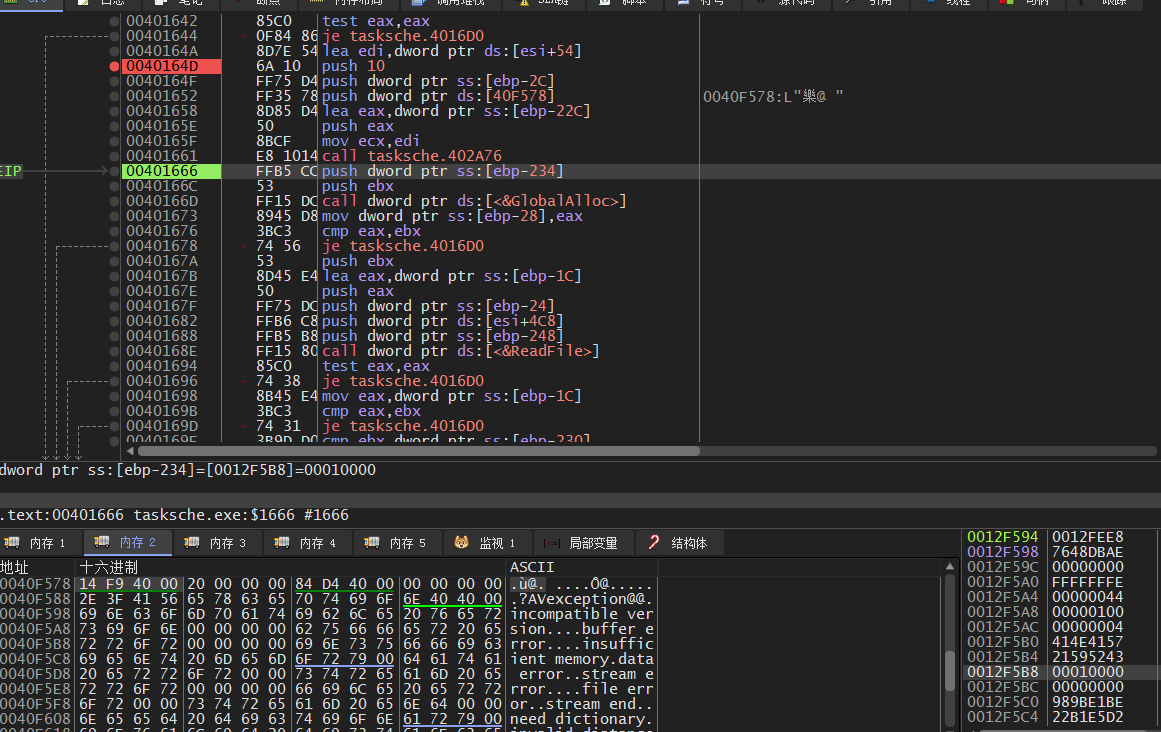
10.sub\_4014A6:传入参数：t.wnry,对内容进行解密，释放核心代码带内存中执行

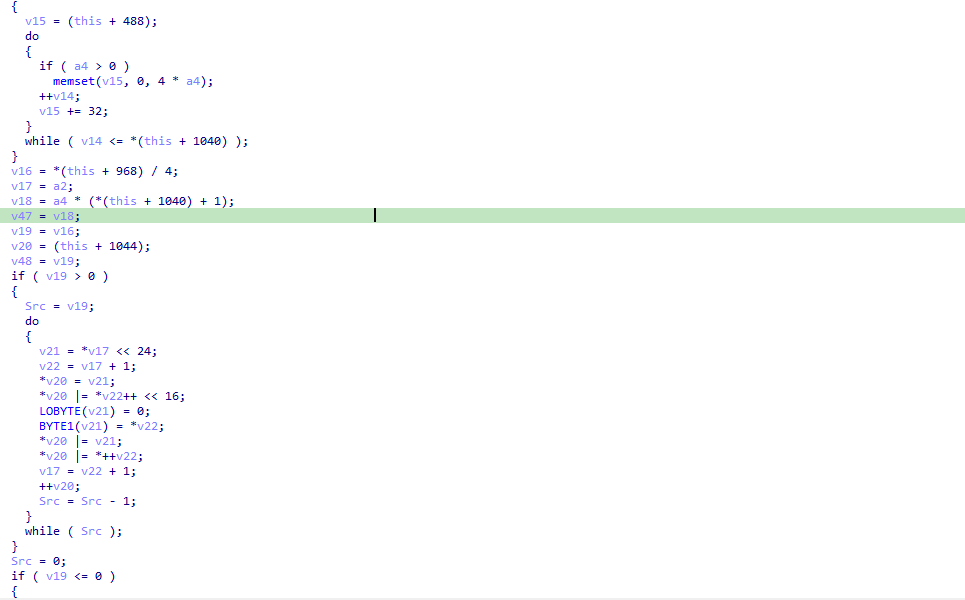


跟进sub\_4019E1:



跟进sub\_402A76:能看到一系列复杂的算法，因此单步分析可能行不通，可以用x32dbg进行动态调试查看内存和寄存器的值对其功能进行大概判断：AES的一个秘钥扩展





**3.3 对t.wnry中解密出来的dll进行分析：**

**3.3.1 主要功能：**

1.创建互斥体

2.启动加密文件

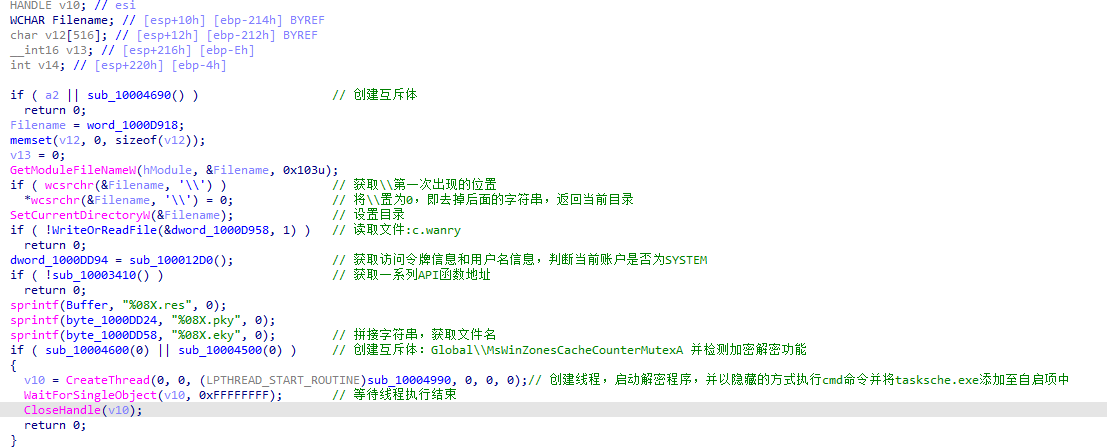
3.写加密文件

4.结束相关进程：Microsoft.Exchange.\*；MSExchange\*；sqlserver.exe；sqlwriter.exe；mysqld.exe

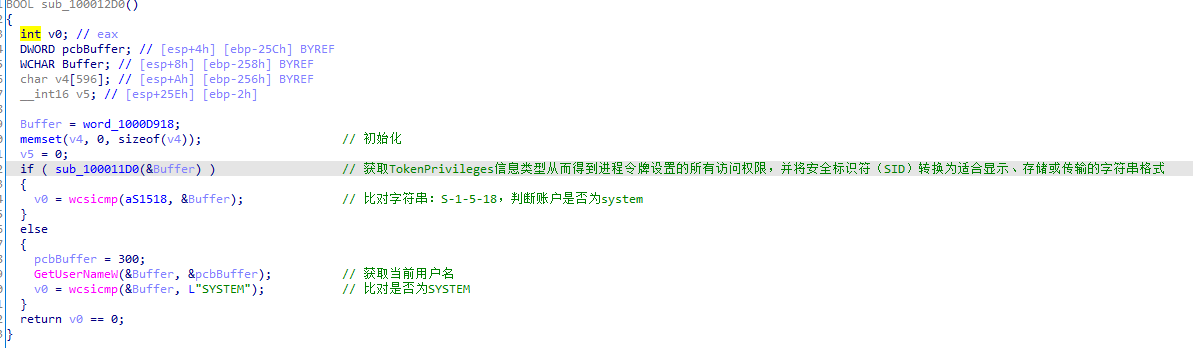
4.启动@WanaDecryptor@.exe和taskse.exe,在注册表run写入开机启动

**3.3.2 恶意代码分析：**

总体概览：



1.sub\_100012D0:通过获取到的访问令牌信息，判断当前用户是否是SYSTEM账户。



跟进100011D0:获取进程令牌设置的所有访问权限，并将安全标识符（SID）转换为适合显示的字符串格式。



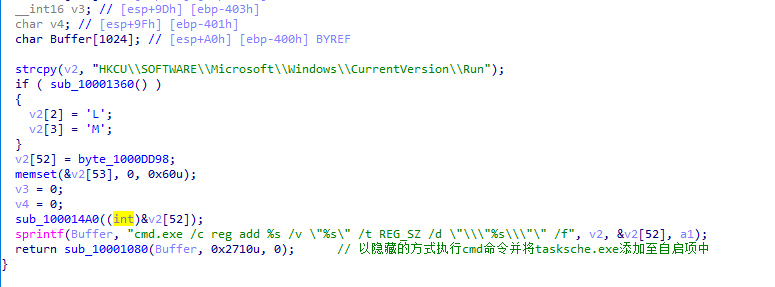
2.线程回调函数sub\_10004990:判断当前账户是否为系统权限账户，并创建taskse.exe和WanaDecryptor@.exe两个进程，然后通过隐藏的方式执行cmd命令并将tasksche.exe添加至自启项中。



跟进10004890：判断权限是否为系统用户权限，如果是就创建taskse.exe和WanaDecryptor@.exe两个进程，如果不是就创建WanaDecryptor@.exe进程。

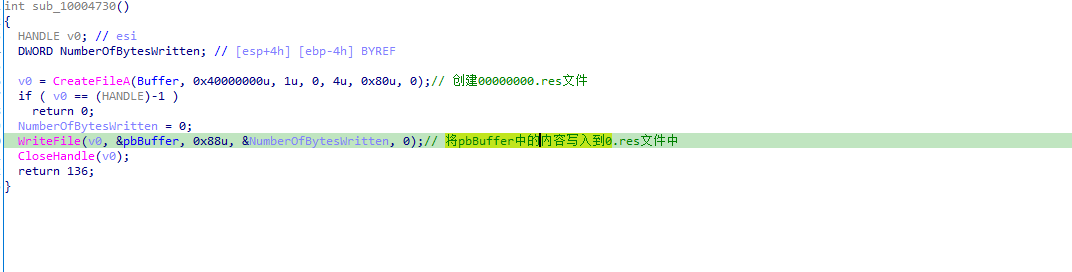


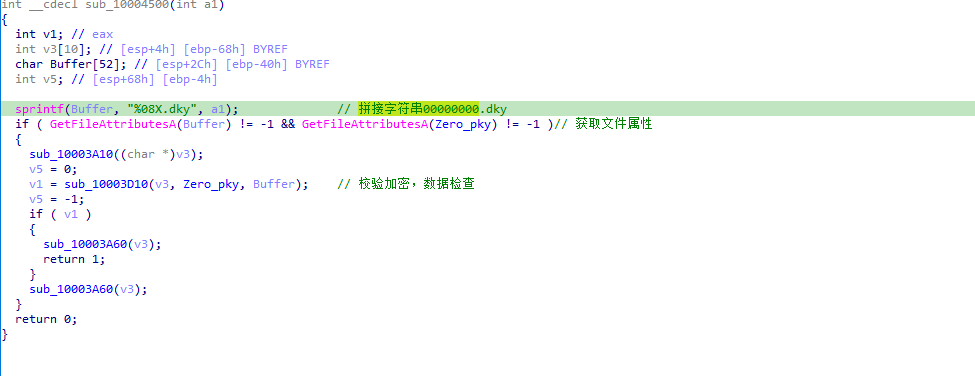
跟进sub\_100047F0：通过隐藏的方式执行cmd命令并将tasksche.exe添加至自启项中。



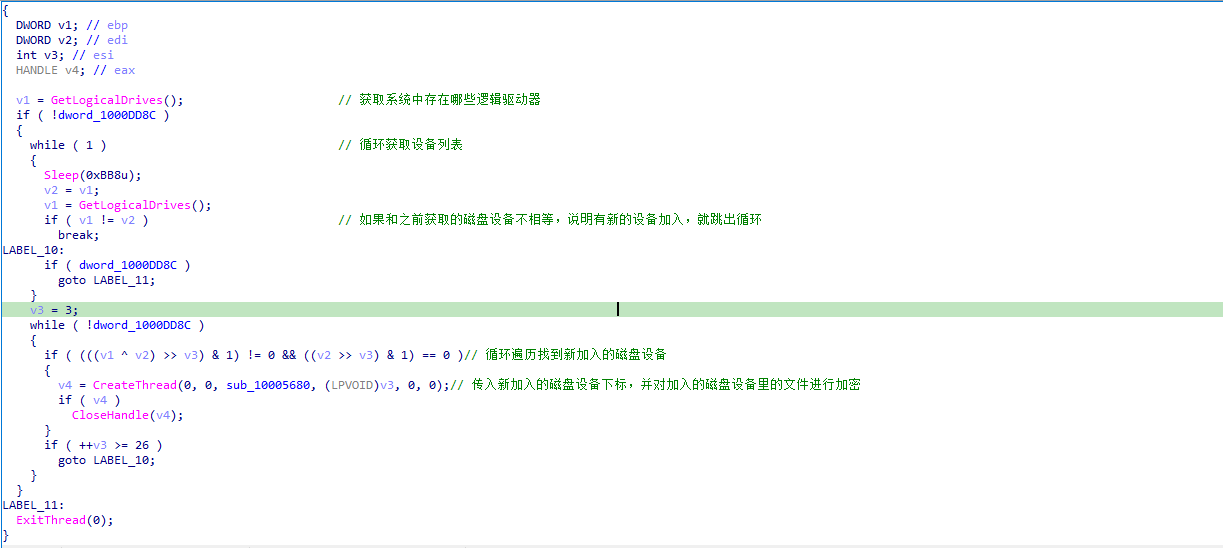
3.Sub\_10003AC0:用于判断00000000.pky文件是否存在，不存在就创建，并导出公钥写入到00000000.pky文件中，然后创建00000000.eky文件，并导出私钥经加密后写入00000000.eky文件中。



4.线程回调函数sub\_10004790:创建00000000.res文件，并将之前pbBuffer中的内容写入到0.res文件中。  
 5.线程回调函数sub\_100045C0:获取00000000.dky文件属性，以此来判断该文件是否存在，并对加密进行测试。



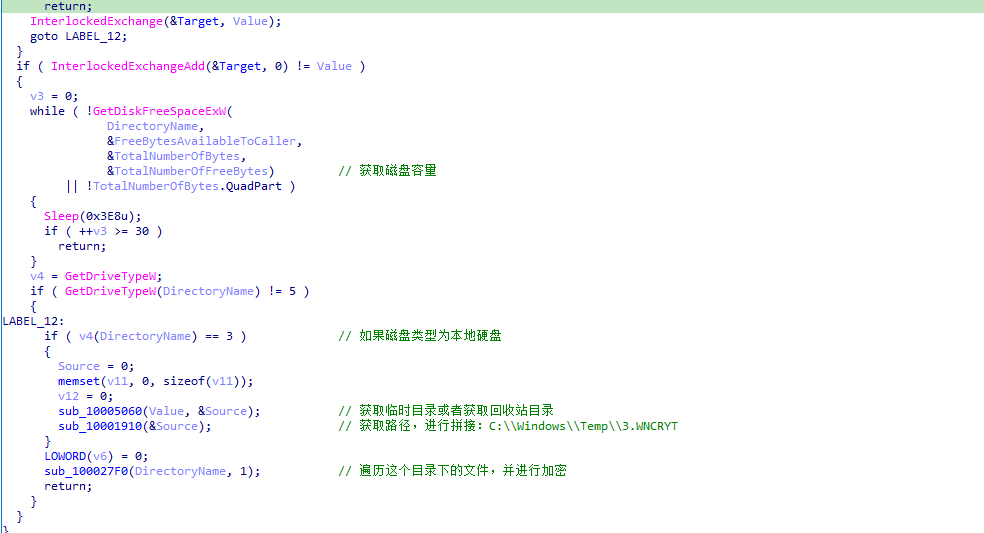
6.线程回调函数sub\_10005730：如果有磁盘设备加入，就遍历目录，进行文件加密



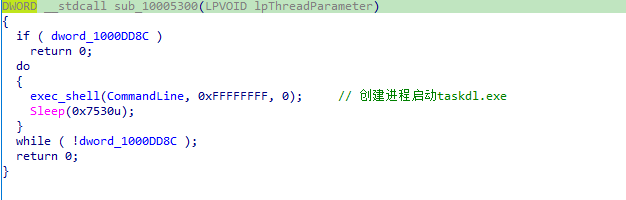
7.关键函数sub\_10005680分析：传入新加入的磁盘设备下标，并对加入的磁盘设备里的文件进行加密



跟进sub\_10005540:对新加入的磁盘设备进行文件加密



8.线程回调函数sub\_10005300：启动资源中的Taskdl\_exe



9.线程回调函数sub\_10004990：[启动@WanaDecryptor@.exe和taskse.exe,在注册表run写入开机启动](mailto:启动@WanaDecryptor@.exe和taskse.exe,在注册表run写入开机启动)



10.sub\_100057C0：结束相关进程，并创建bat脚本，执行恶意代码



关键函数sub\_10004CD0：



# 4.程序行为总结

## 4.1 病毒母体

释放并运行病毒程序

利用MS17-010漏洞，攻击内网、外网，实现病毒的网络传播

## 4.2 taskshe.exe

①释放文件0x24个文件

②对c.wnry文件写入了一个比特币账号，而这个比特币账号很眼熟，其实就是1.3中图片显示的比特币账号

③创建目录，设置为隐藏属性，创建cmd控制台，获取最高权限

④设置注册表项

⑤创建临界区，申请堆空间，释放dll文件到堆空间中，从释放的dll中导出的TaskStart函数

⑥调用导出的函数(核心函数)

## 4.3 TaskStart核心dll

①检查防多开，读取c.wnry文件的内容，获取API地址

②测试本机是否能够正常加密解密

③循环启动tasksche.exe程序，向c.wnry写入数据

④创建00000000.pky和00000000.eky文件，导出密钥，将密钥写入到这两个文件，后面再从这两个文件中导入密钥

⑤创建00000000.res文件，并将8字节的加密随机字节写入到res文件中

⑥每30秒启动一次taskdl.exe和tasksche.exe

⑦遍历文件，判断是否需要加密，将一部分文件移动到系统盘的临时目录下，这里的数据是没有加密的，可以通过修改后缀名来恢复文件，但是后续会删除大多数的文件。

⑧遍历桌面，桌面释放@WanaDecryptor@.exe，@Please\_Read\_Me@.txt，加密桌面文件，然后释放一个同名的.WNCRY文件。

⑨遍历磁盘，加密文件，不断向磁盘写入数据，占满磁盘空间

⑩运行taskdl.exe和taskse.exe，删除系统盘临时目录下的.WNCRYT文件，提权操作

# 5．解决方案

电脑安装杀毒软件，定期体检，定期杀毒，关闭445等不必要的端口

及时更新电脑系统，安装ms17010漏洞补丁

参考文献

1. 看雪学院
2. HACK编程技术详解
3. 吾爱破解