样本分析报告

报告管理信息

报告版本	V1.0
文档创建者	陈之健
文档更新者	陈之健
文档创建时间	2021 年 8 月 23 日
文档修改时间	
样本发现时间	
保密级别	

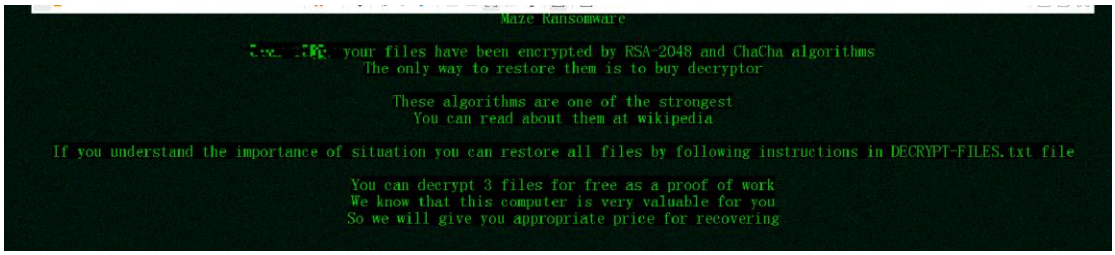
样本信息

文件名	文件大小	文件 MD5
Maze	744448 bytes	27c5ecbb94b84c315d56673a851b6cf9

木马概述

此样本为 Maze（迷宫）勒索病毒，通过 shellcode 装载自身携带的 EXE 资源到自身进程内存空间，并跳转入口点执行，开始后续行为。被装载的 EXE 对自身文件进行了反反汇编处理，包括代码控制流平坦化、垃圾指令等手段。

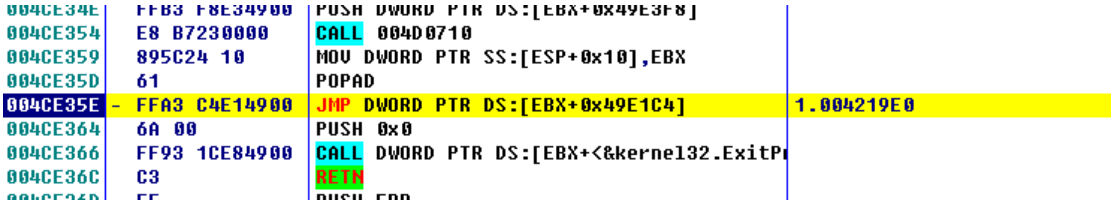
木马勒索界面截图



木马特点：

木马执行细节

解密自身携带数据装载 PE，跳到装载后的入口点位置



IsDebugPresent

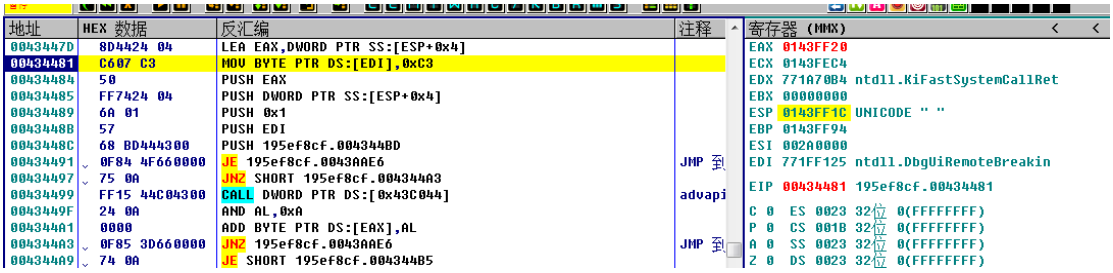
在迷宫内检测[PEB+2]，如果被调试则进入死循环

RUN 跟踪，找迷宫出口

在本样本中的出口为 0x423815

反调试

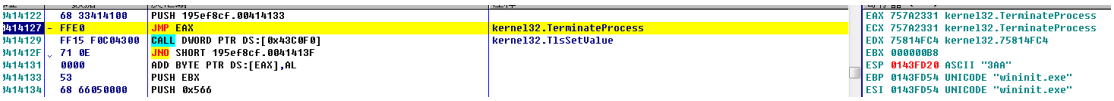
InlineHook DbgUiRemoteBreakIn

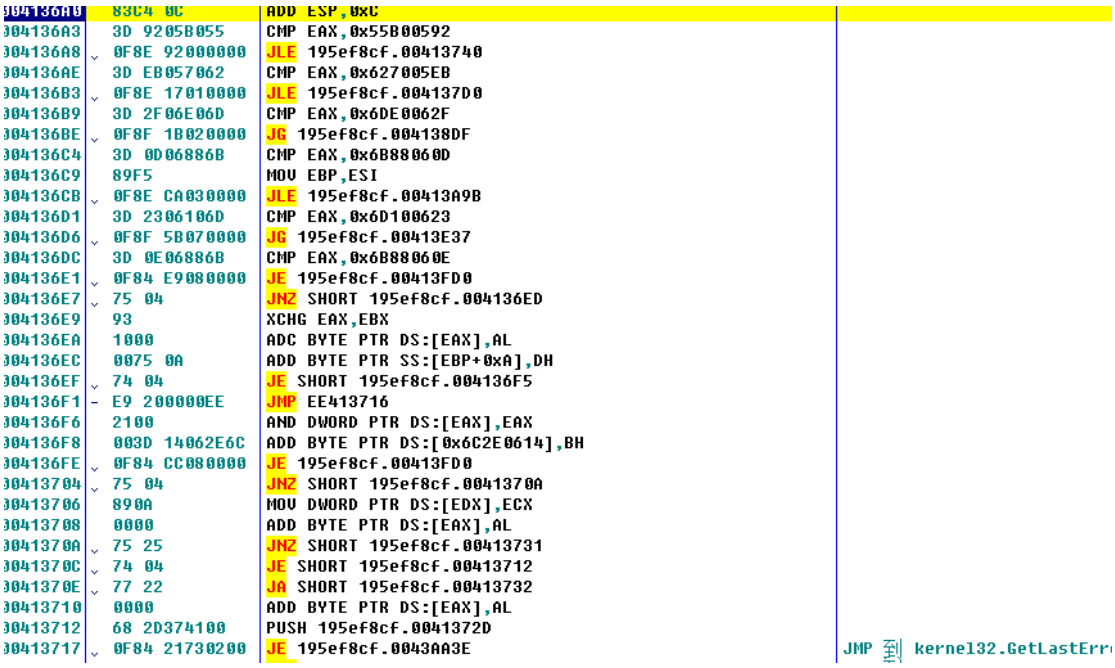


遍历进程，关闭进程

先将进程名进行简单加密，加密规则小写 Asc 码值减去 20 再与将差与差值右移 5 位值异或

查询相关资料，样本将加密后的进程名利用 Alder32 检验算法计算其校验值，初始值为（29a）如果找到对应的就关闭进程





之后多次调用 IsDebuggerPresent，检测是否被调试。

获取用户信息

GetUserNameW 获取用户名
GetComputerNameW 获取计算机名
查询注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion 中的 ProductName 获取 Windows 产品名称
执行 WQL 搜索反病毒产品，wql select * from antivirusproduct 如果没有保存字符串”none|”
GetDriveTypeW,GetDiskFreeSpaceW 磁盘属性和空闲空间信息
GetVolumeInforMationW 获取系统盘序列号信息

地区避免

GetUserDefaultUILanguage、GetSystemDefaultLangID 获取语言标识
和下列标识 id 比较，如果相同释放保存信息的内存，退出当前线程
419：Russian
422：Ukrainian
423：Belarusian
428：Tajik
42B：hy-AM
42C：Azeri - Latin
437：Georgian
43F：Kazakh
440：Kyrgyz - Cyrillic
442：Turkmen

443：Uzbek - Latin

444：Tarta

818：Romanian - Moldova

819：Russian - Moldova

82C：Azeri - Cyrillic

843：Uzbek - Cyrillic

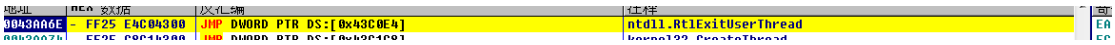
7C1A：Serbian

6C1A：Serbian – Cyrillic

1C1A：Serbian (Cyrillic, Bosnia and Herzegovina)

281A：Serbian (Cyrillic, Serbia)

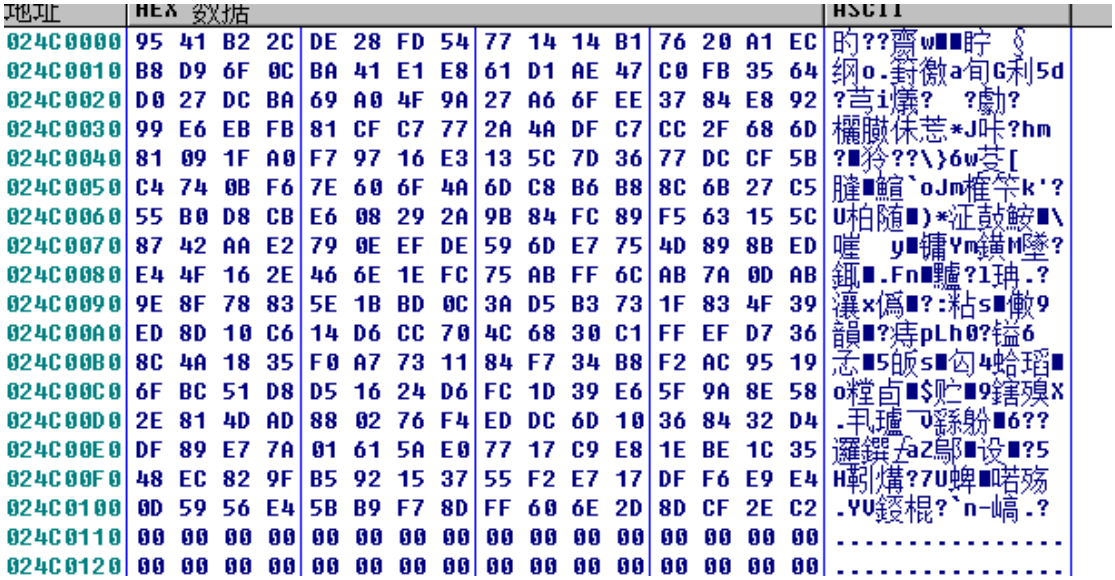
81A：Serbian - Latin



创建线程发送获取的数据

加密数据

837293049583729 30dhejskrlt9483s



发送前又加密了一次

合成 URL

URL 格式为 Http://IP/(dir+/){0,2}/[a-y]{1,10}suffix?{ [a-y]{1,4}=[a-z0-9]{1,10} }{0-4}

各个参数间用”&”隔开

1. IP 地址为以下 IP 中顺序挑选

91.218.114.4

91.218.114.11

91.218.114.25

91.218.114.26

91.218.114.31

91.218.114.32

91.218.114.37
91.218.114.38
91.218.114.77
91.218.114.79
以 GetTickCount 的返回值作为随机数种子
随机数每次使用后更新

```
0423B90   8B4C24 04       MOV ECX,DWORD PTR SS:[ESP+0x4]
0423B94   6901 FD430300   IMUL EAX,DWORD PTR DS:[ECX],0x343FD
0423B9A   05 C39E2600     ADD EAX,0x269EC3
0423B9F   8901            MOV DWORD PTR DS:[ECX],EAX
```

2. dir 个数为(rand()&0x7fff)%3
每个通过（rand()&0x7fff）%31 在下列字符串中选取
"news" "login" "register" "logout" "edit" "content" "private" "messages" "account" "view" "webauth" "webaccess" "archive" "forum" "post" "signin" "signout" "update" "support" "ticket" "task" "tracker" "analytics" "check" "checkout" "payout" "withdrawal" "sepa" "create" "transfer" "wire"
3. 生成资源名 src 小写字母 a-y,字符个数为 1-10
4. 选取后缀名 suffix (rand()&0x7fff)%11
'.php','.asp','.aspx','.cgi','.jsp', '.jspx','.do', '.action', '.html','.phtml','.shtml'
5. 参数的个数为((rand()&0x7fff)%5)
参数名字符长度为 1-4,字符为 a-y
参数值长度为 1-10，先判断随机数(rand()&0x7fff)是奇数还是偶数，如果是奇数，再次随机(rand()&0x7fff)%9 再加上 0x30,即为数字 0-8，如果为偶数，则为字母[a-z]。

合成 Http 请求字符串，通过 send 发送给 IP 主机，之后再发送 Http 请求。

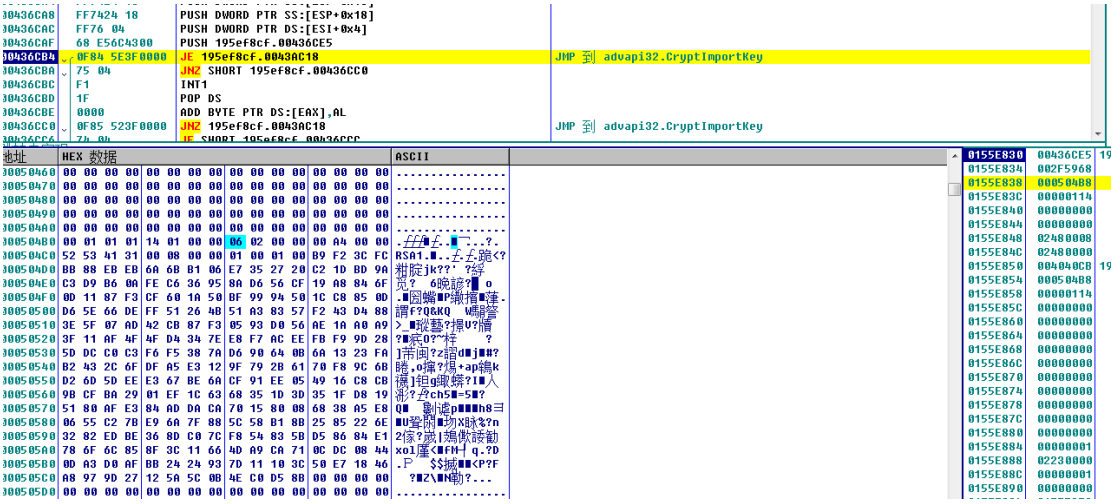
加密流程

1. 生成提示文件文本
CryptGenKey 和 CryptExportKey 导出 Rsa 密钥对，参数 0xA400 表示为 RSA 密钥交换算法

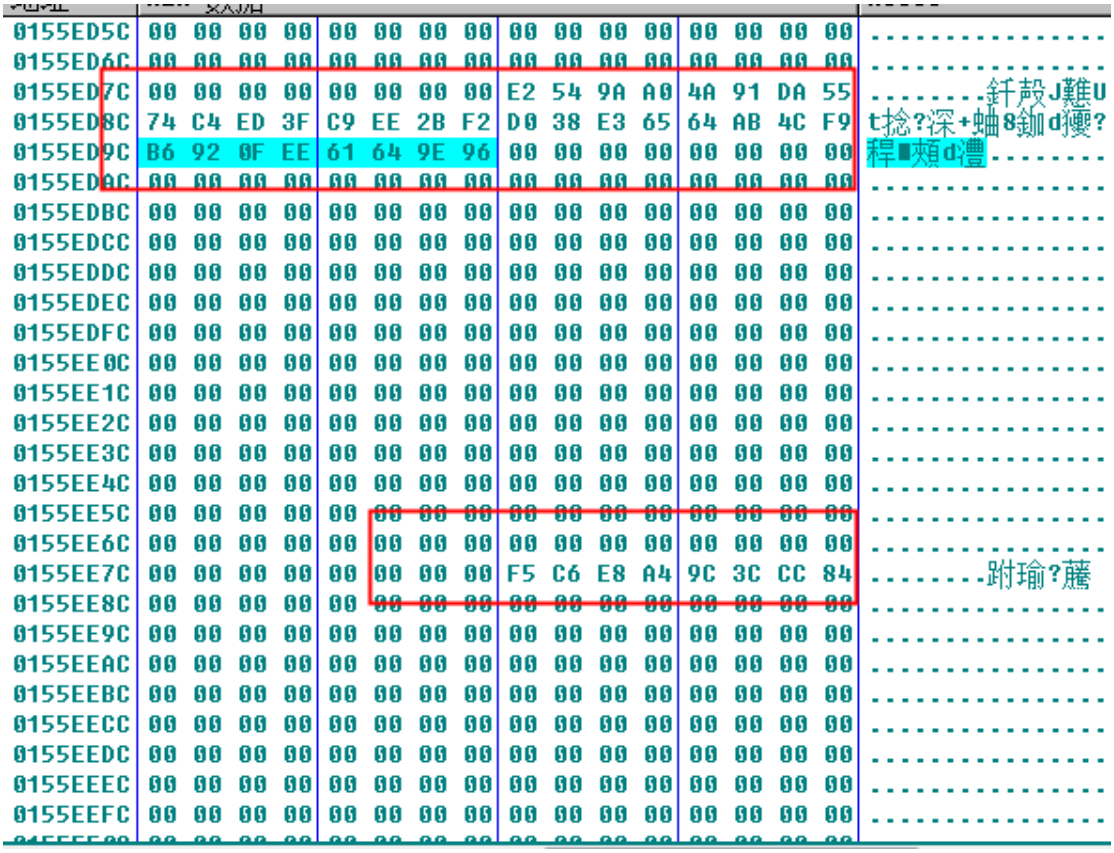
```
00403ACF   50              PUSH EAX
00403AD0   68 01000008     PUSH 0x8000001
00403AD5   68 00A40000     PUSH 0xA400
00403ADA   FF7424 18       PUSH DWORD PTR SS:[ESP+0x18]
00403ADE   68 213B4000     PUSH 195ef8cf.00403B21
00403AE3   0F84 FF700300   JE 195ef8cf.0043ABE8          JMP 到 advapi32.CryptGenKey
00403AE9   75 0A           JNZ SHORT 195ef8cf.00403AF5
00403AEB   FF15 4CC04300   CALL DWORD PTR DS:[0x43C04C]  advapi32.EqualDomainSid
```

公钥导出 Blob

导入攻击者公钥



获取随机值 CryptGenRomdon,32 字节 key 和 8 字节 nonce，备份到内存的其他位置

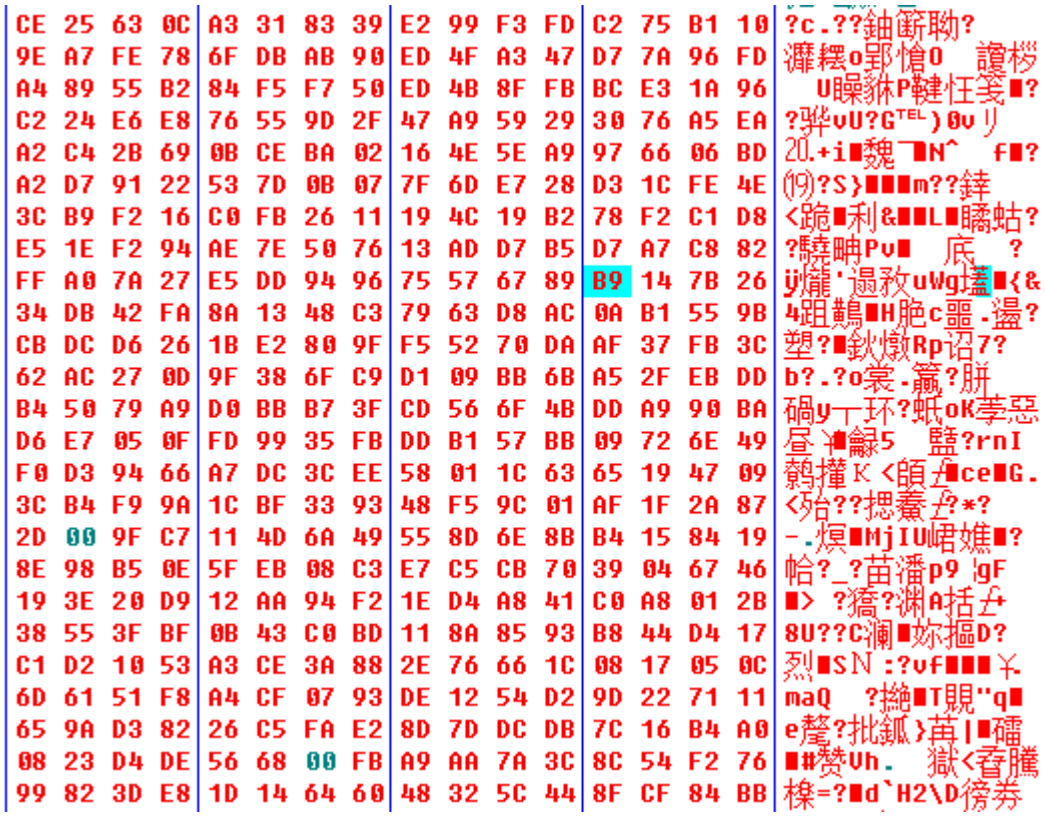


使用非常规 chacha 加密算法加密私钥

在网上找了一篇描述 salsa 算法，与 chacha 算法类似

https://www.cnblogs.com/init0ne/p/14772868.html

Expand 32-byte key 0 noncy 的初始矩阵，生成随机字节流 64 字节，每次处理 64 字节与原文异或生成密文，剩余的部分按字节异或，加密密钥共 0x494 字节.

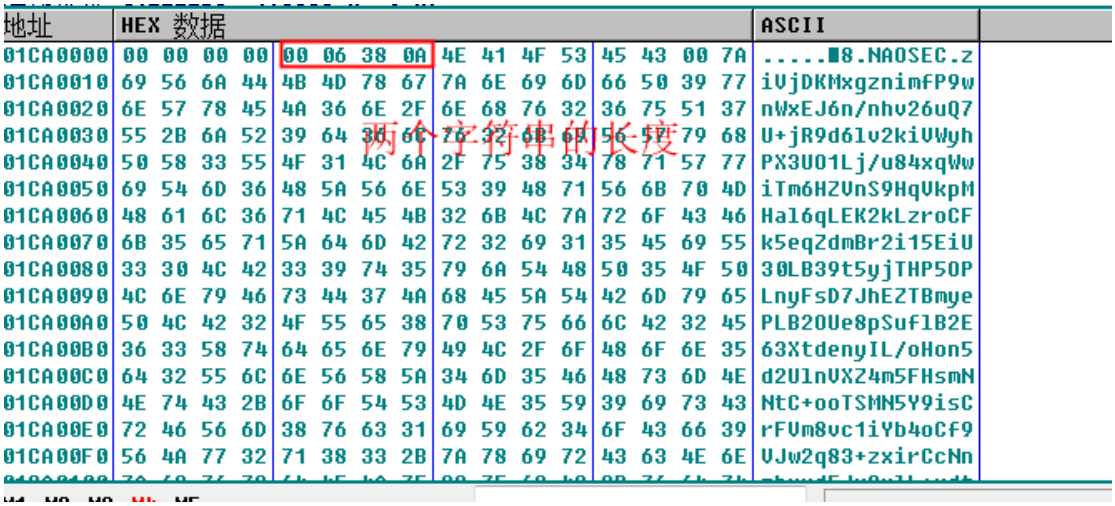


加密备份到内存的 key 和 noncy

CryptEncrypt

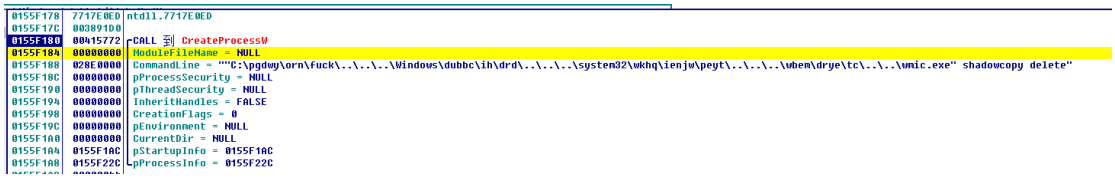
创建文件 C：/PragramData/data1.tmp,写入末尾为 0x66611166 的 109 字节数据

CryptBinaryToStringA Base64 加密私钥+公钥+加密后的 key 和 noncy，加上字符串 NAOSEC，通过函数 ZwSetEaFile 设置为文件扩展属性



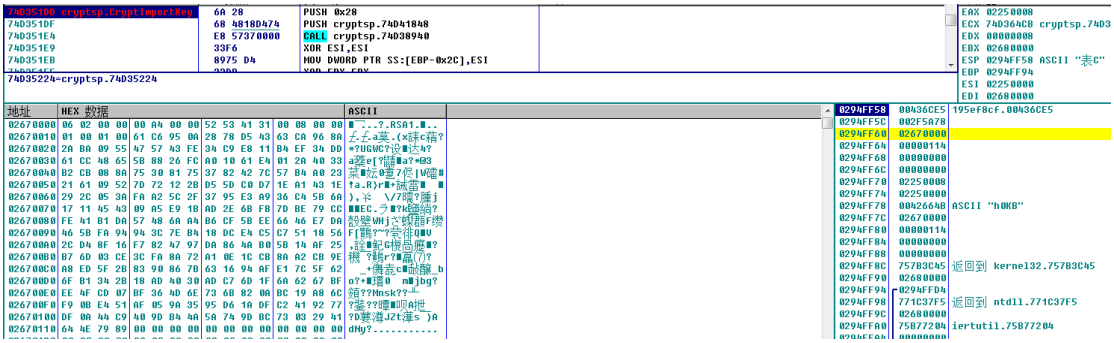
填充勒索提示文件中 Base64key 为 CryptBinaryToStringA Base64 私钥+获取的用户信息

2. 删除卷影副本

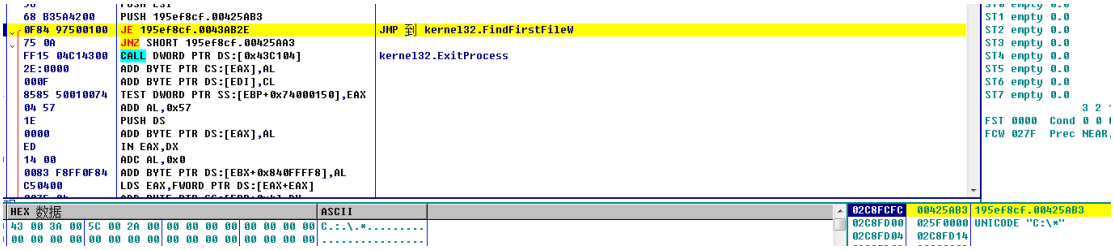


C：\Windows\system32\wmic.exe　执行 shadowcopy delete 删除卷影

3. 导入用户公钥



4. 遍历文件加密



排除路径中含有以下字符串的文件，如果目录中不存在这些字符，则创建两个文件 DECRYPT-FILES.txt 勒索提示文件，{UID}.tmp 文件为空

\Program Files

:\Windows

\Games\

\Tor Browser\

\ProgramData\

\cache2\entries\

\Low\Content.IE5\

\User Data\Default\Cache\

\All Users

\IETldCache\

\Local Settings\

\AppData\Local

AhnLab

{0AFACED1 - E828 - 11D1 - 9187- B532F1E9575D}

排除文件名位以下的文件

DECRYPT-FILES.txt

autorun.inf

boot.ini

desktop.ini

ntuser.dat

iconcache.db

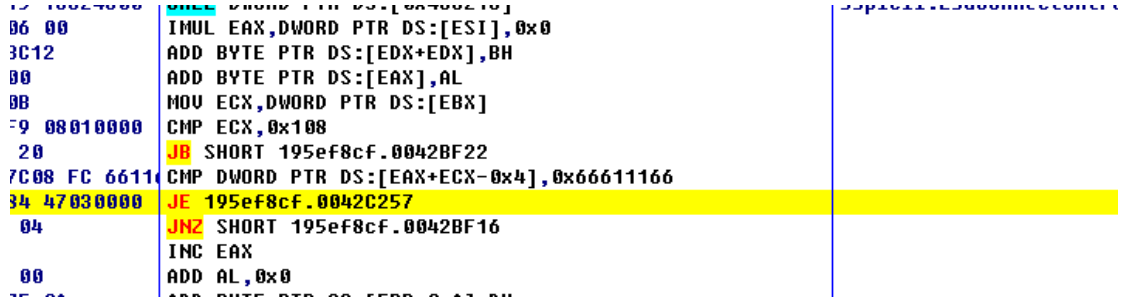
bootsect.bak

ntuser.dat.log

thumbs.db

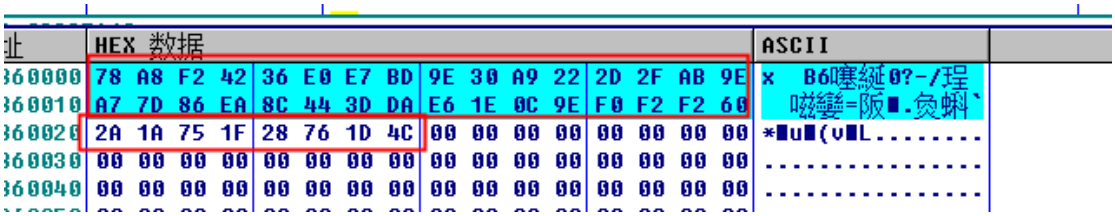
Bootfont.bin
排除以下后缀名文件
lnk.exe.sys.dll

SetFileAttributeW测试文件是否存在
使用CreateFileW打开文件，获取文件的大小，判断是否小于等于0x50000,再次判断文件大小是否大于108个字节时，再判断文件末尾4个字节是否是0x66611166

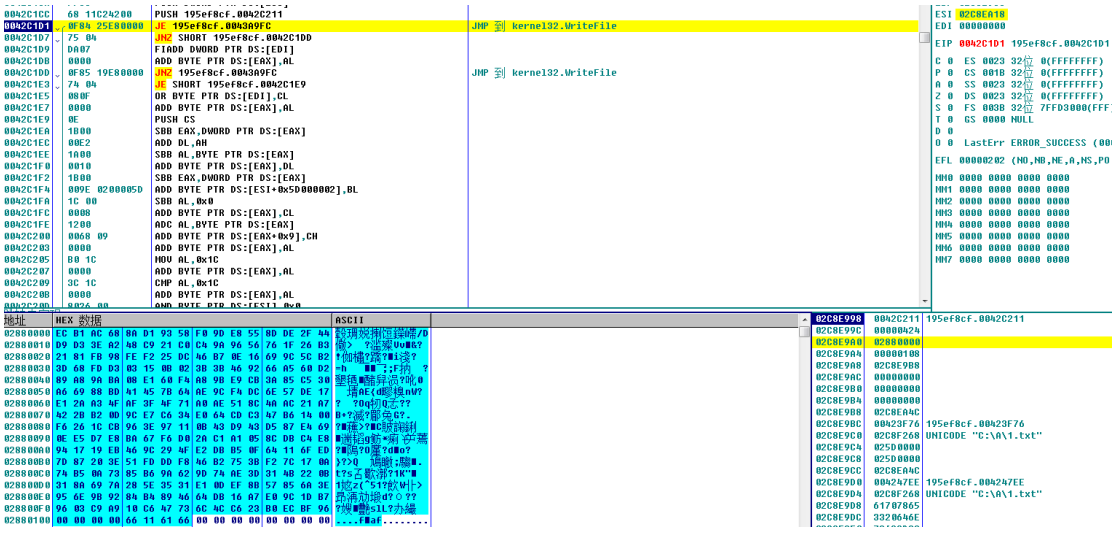


判断条件成功后，开始加密

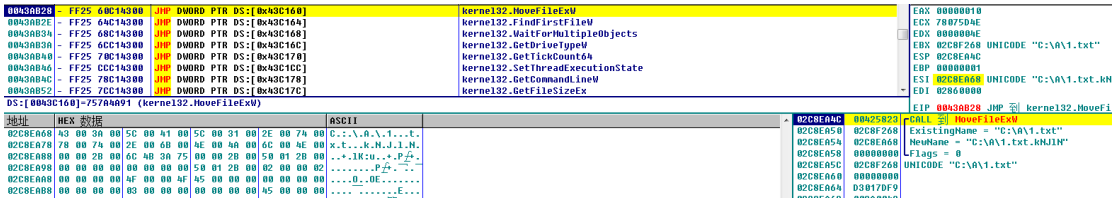
1. 获取随机的32字节的key和8字节的nonce
   CryptGenRandom



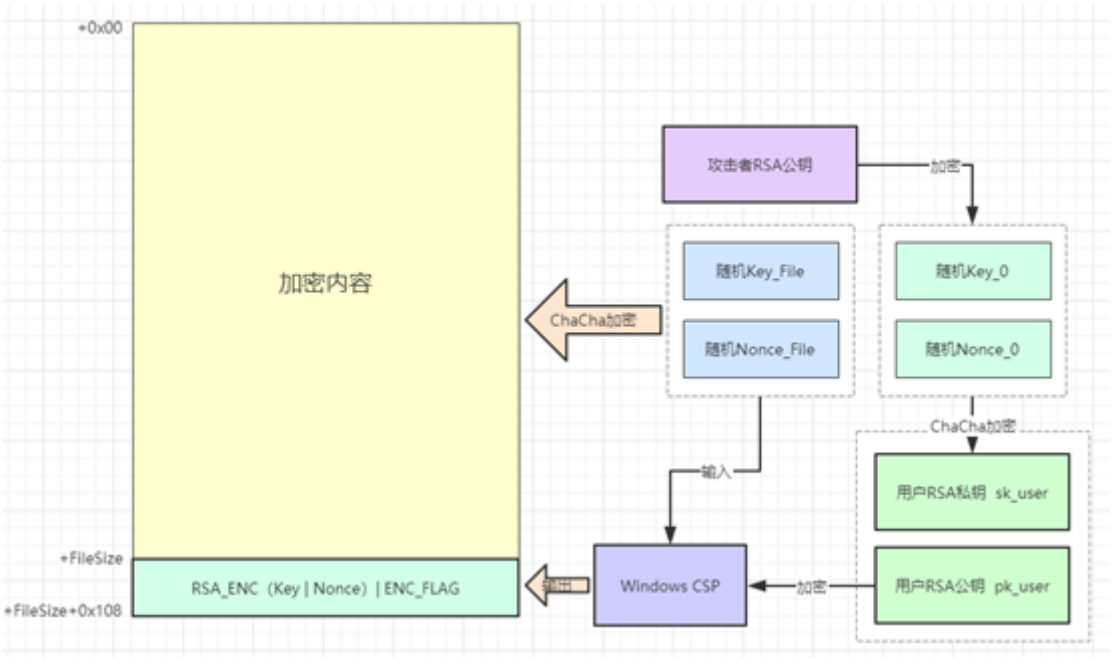
2. 备份key和noncy，然后RSA加密这两个值 CryptEncrypr　末尾增加感染标记
3. 使用chacha加密
4. 将108字节的数据，被加密的key值和nonce值写到文件末尾



5. 生成随机的文件后缀名，随机方式类似URL字符串随机生成方式，字符组成为大小写字符和0-9数字



加密流程图为参考文章中的图



IOCs

91.218.114.4
91.218.114.11
91.218.114.25
91.218.114.26
91.218.114.31
91.218.114.32
91.218.114.37
91.218.114.38
91.218.114.77
91.218.114.79
合成的 URL

参考文章

https://bbs.360.cn/thread-15826039-1-1.html