Buran 勒索病毒样本分析

目录

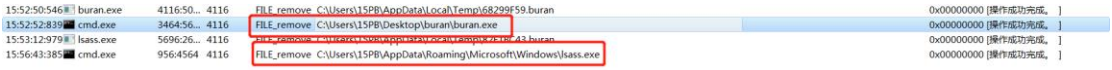
一、样本概况

SHA256：5c1141aa7d0b9fba71822607f3b1b086e2cc4529e63221a9a6ede74fa366512f

该样本启动自身后，释放新的 PE 文件，通过 CreateProcessInternalW 创建系统假进程和通过 ShellExecuteExW 启动了一个隐藏界面的进程，并且在注册表设置该程序为自启动。通过 cmd 进程，根据参数的不同来执行不同的流程；在病毒运行前，进行了国家和地区的检查对比，特定的国家不运行该病毒程序。程序运行后删除系统的备份文件，同时删除自身。

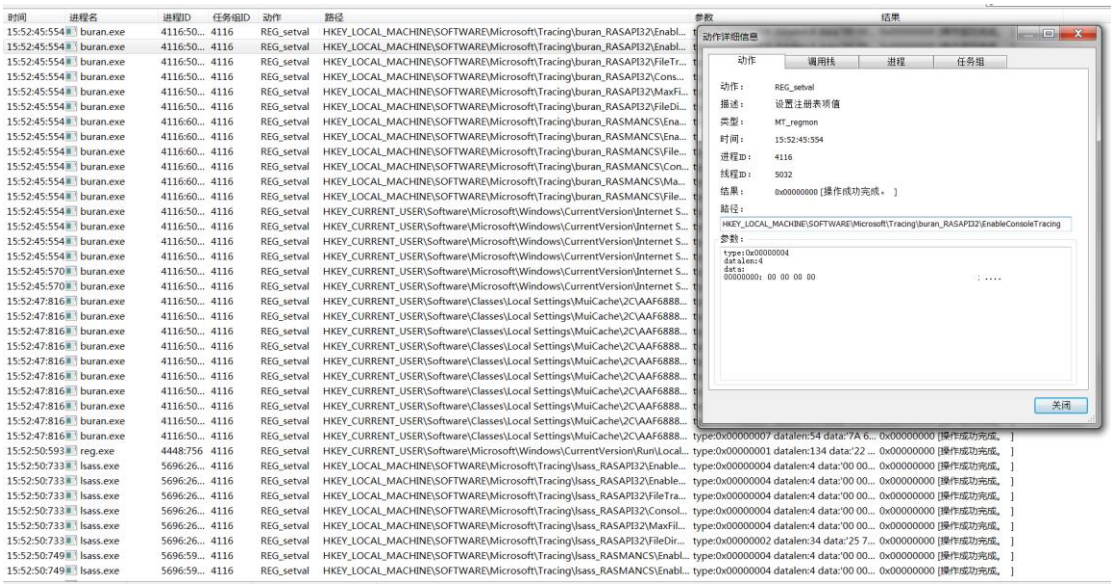
二、具体行为分析

删除文件

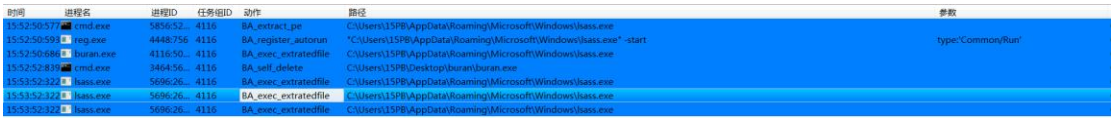


循环遍历系统中的文件并加密

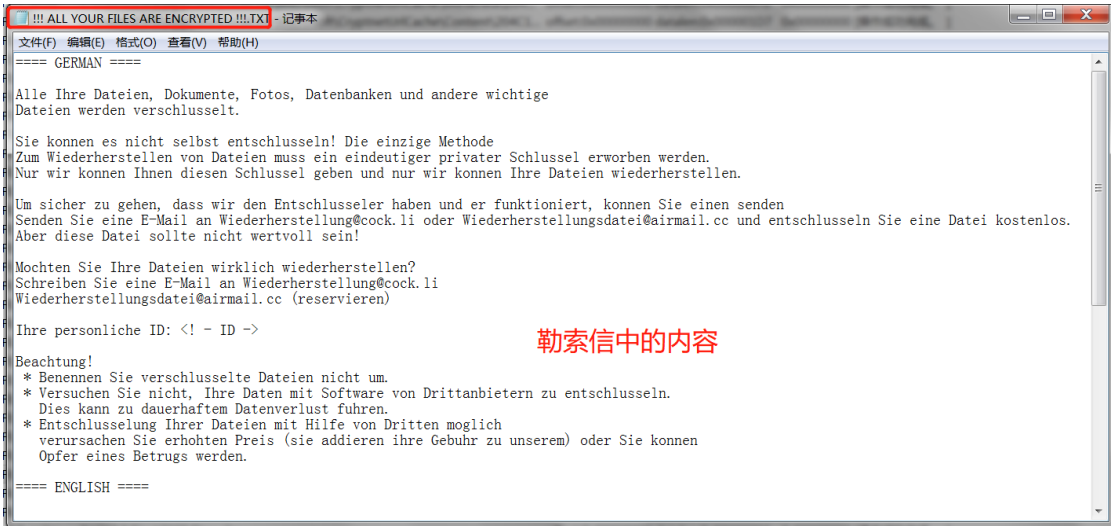
设置注册表项



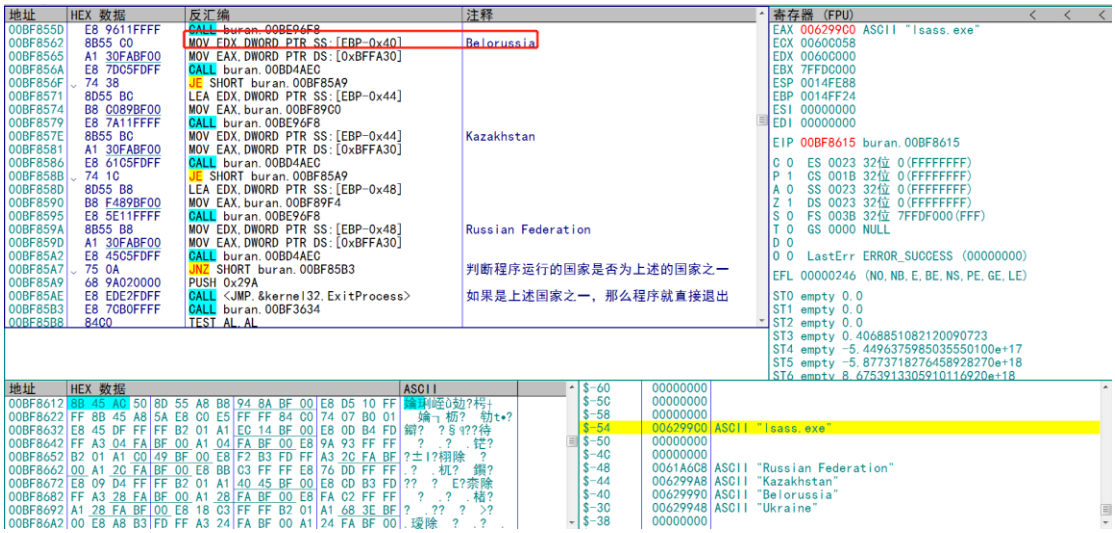
释放 PE 文件，修改注册表自启动项，删除病毒程序本体，启动自释放的文件。



勒索信中的内容

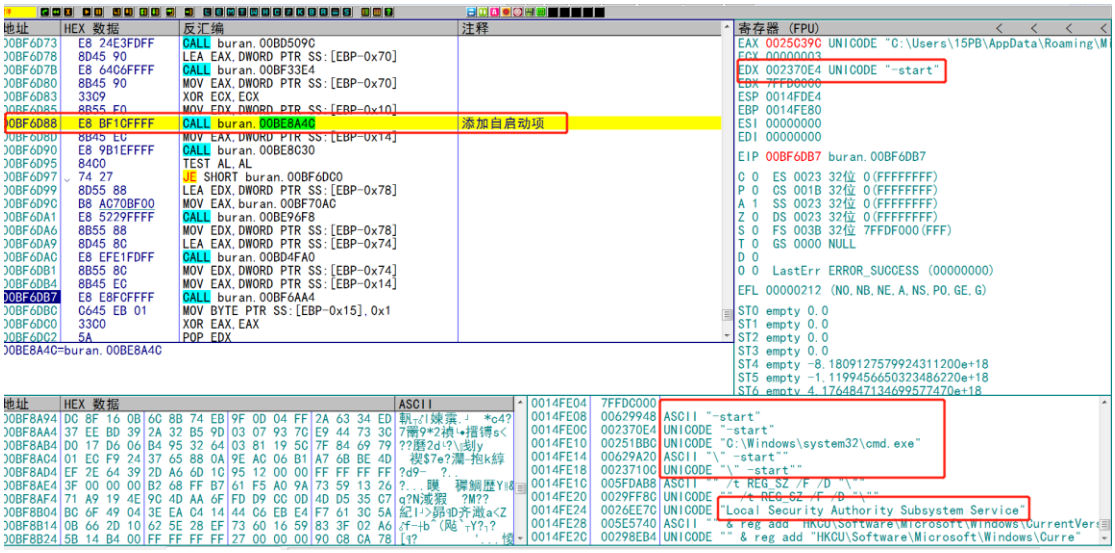


打开 url：http://geoiptool.com，对比国家和地区，特定国家和地区不会发起攻击

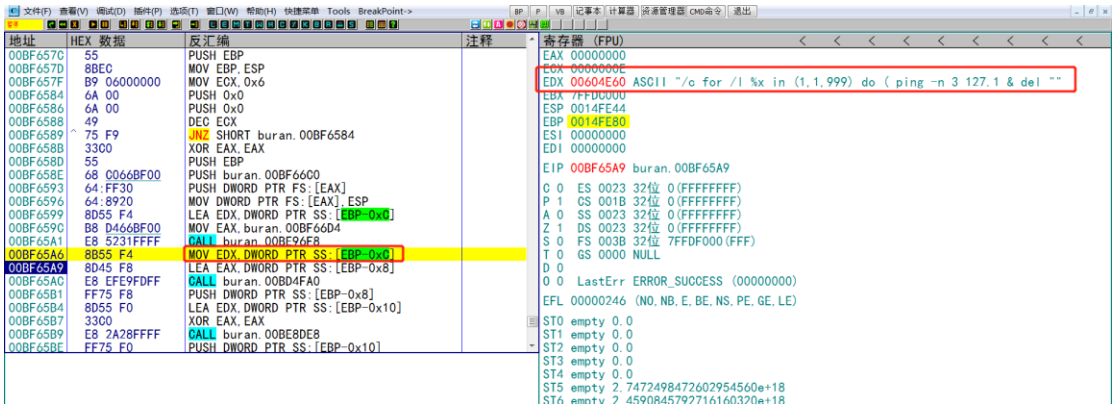


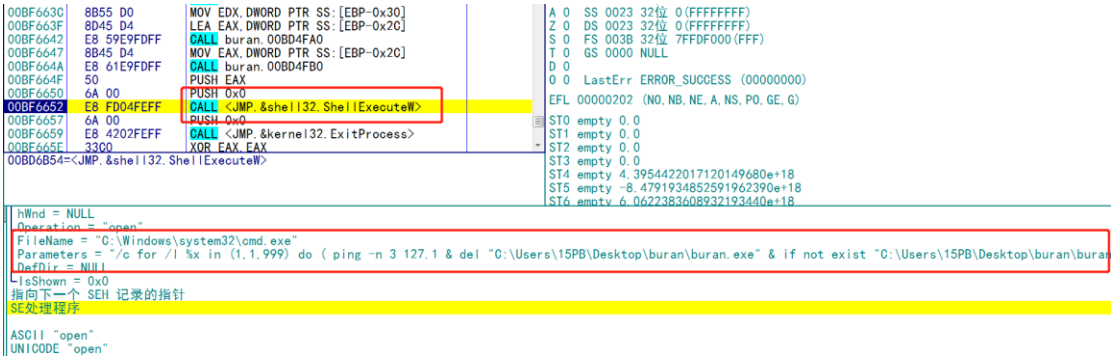
添加自启动项服务，调用 cmd 进程，创建 lsass.exe 并添加自启动项 Local Security Authority Subsystem Service,如下图：

```
0014FE14   00629A20  ASCII "\" -start""
0014FE18   0023710C  UNICODE "\" -start""
0014FE1C   005FDAB8  ASCII "" /t REG_SZ /F /D "\""
0014FE20   0029FF8C  UNICODE "" /t REG_SZ /F /D "\""
0014FE24   0026EE7C  UNICODE "Local Security Authority Subsystem Service"
```



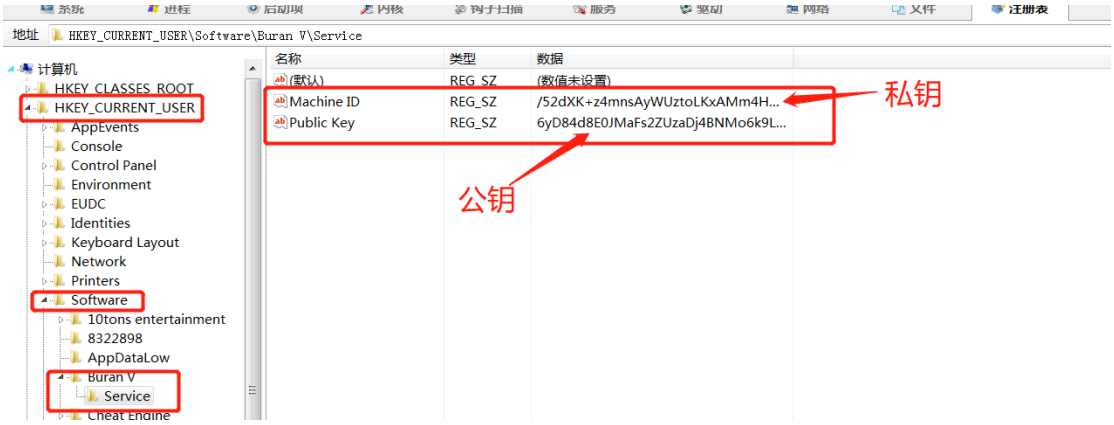
退出当前进程并删除执行目录下的病毒文件：





生成对用户文件加密的公钥和私钥：

病毒程序为当前用户生成一对 RSA 私钥和私钥，其中私钥通过攻击者 RSA 公钥处理并 base64 编码后放入注册表。如下图：




```
lea     edx, [ebp+var_9C]
mov     eax, [ebp+var_4]
call    sub_419660      ; RC4加密
mov     eax, [ebp+var_9C]
lea     edx, [ebp+var_98]
call    sub_416FC0      ; base64加密
mov     edx, [ebp+var_98]
lea     eax, [ebp+var_4]
call    sub_404780      ; RC4加密
lea     edx, [ebp+var_A0]
mov     eax, [ebx+24h]
call    sub_419660      ; base64加密
mov     eax, [ebp+var_A0]
lea     edx, [ebp+var_8]
call    sub_416FC0      ; RC4解密
lea     edx, [ebp+var_A4]
mov     eax, offset dword_422248
call    sub_4196F8
mov     edx, [ebp+var_A4]
mov     ecx, [ebp+var_4]
mov     eax, 80000001h
call    sub_416970      ; 公钥
lea     edx, [ebp+var_A8]
mov     eax, offset dword_422294
```

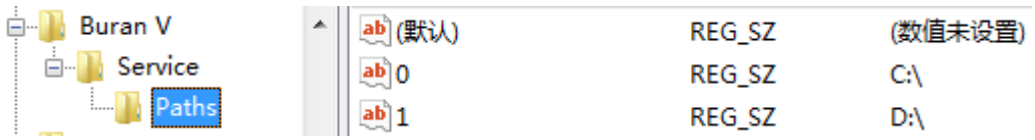
删除备份的文件和日志，首先进行提权操作，如下图：

```
  sub_404B44(a2);
  v8 = &savedregs;
  v7 = &loc_418868;
  v6 = __readfsdword(0);
  __writefsdword(0, (unsigned int)&v6);
  v2 = 0;
  v3 = GetCurrentProcess();                     // 获得当前进程
  if ( OpenProcessToken(v3, 0x20u, &TokenHandle) )// 进行提权相关的操作
  {
    NewState.PrivilegeCount = 1;
    v4 = (const CHAR *)sub_404B54();
    LookupPrivilegeValueA(0, v4, (PLUID)NewState.Privileges);// 查看进程的权限
    if ( v12 )
      NewState.Privileges[0].Attributes = 2;
    else
      NewState.Privileges[0].Attributes = 2147483648;
    AdjustTokenPrivileges(TokenHandle, 0, &NewState, 0x10u, 0, &ReturnLength);// 提权
    if ( !GetLastError() )
      LOBYTE(v2) = 1;
    CloseHandle(TokenHandle);
  }
  __writefsdword(0, v6);
  sub_4046E8(&loc_41886F);
  return v2;
}
```

在高权限的情况下，调用 cmd 执行命令，实现备份数据的删除，禁用系统开机自动修复，清空注册表记录，清空系统日志，禁用事件记录。如下图：

```
.text:00425AF2 loc_425AF2:                             ; CODE XREF: sub_425A80+FF↓j
.text:00425AF2                 lea     eax, [ebp+var_C]
.text:00425AF5                 mov     edx, [ebp+var_4]
.text:00425AF8                 movzx   edx, byte ptr [edx+ebx-1]
.text:00425AFD                 call    sub_4048D0
.text:00425B02                 mov     eax, [ebp+var_C]
.text:00425B05                 push    eax
.text:00425B06                 lea     edx, [ebp+var_10]
.text:00425B09                 mov     eax, offset dword_425F14
.text:00425B0E                 call    sub_4196F8      ; 解密字符串
.text:00425B13                 mov     edx, [ebp+var_10]
.text:00425B16                 pop     eax
.text:00425B17                 call    sub_404AEC      ; 0:相等
.text:00425B17                                         ; 1:不相等
.text:00425B1C                 jnz     short loc_425B62
.text:00425B1E                 lea     edx, [ebp+var_18]
.text:00425B21                 mov     eax, offset nullsub_3
.text:00425B26                 call    sub_4196F8
.text:00425B2B                 lea     eax, [ebp+var_18]
.text:00425B2E                 mov     edx, [ebp+var_8]
.text:00425B31                 call    sub_404990
.text:00425B36                 mov     edx, [ebp+var_18]
.text:00425B39                 lea     eax, [ebp+var_14]
.text:00425B3C                 call    sub_404FA0
.text:00425B41                 mov     eax, [ebp+var_14]
.text:00425B44                 push    eax
.text:00425B45                 lea     eax, [ebp+var_1C]
.text:00425B48                 call    sub_4233E4
.text:00425B4D                 mov     eax, [ebp+var_1C]
.text:00425B50                 xor     ecx, ecx
.text:00425B52                 pop     edx
```

Buran 通过 WNetResourceW 等相关系统 API 枚举可访问的网络资源，记录本地磁盘中并将所有资源写入注册表项 HKCU\\Software\\Buran V\\Service\\Paths，键值为资源根目录名。如下图：



```
.itext:00428759 loc_428759:                             ; CODE XREF: .itext:004287AA↓j
.itext:00428759                 lea     edx, [ebp-74h]
.itext:0042875C                 mov     eax, offset byte_428B30 ; 参数
.itext:00428761                 call    sub_4196F8      ; RC4 字符串解密
.itext:00428766                 lea     eax, [ebp-74h]
.itext:00428769                 push    eax
.itext:0042876A                 lea     edx, [ebp-78h]
.itext:0042876D                 mov     eax, esi
.itext:0042876F                 call    sub_407F6C
.itext:00428774                 mov     edx, [ebp-78h]
.itext:00428777                 pop     eax
.itext:00428778                 call    sub_404990
.itext:0042877D                 mov     edx, [ebp-74h]
.itext:00428780                 lea     eax, [ebp-70h]
.itext:00428783                 call    sub_404FA0
.itext:00428788                 mov     eax, [ebp-70h]
.itext:0042878B                 push    eax
.itext:0042878C                 lea     edx, [ebp-7Ch]
.itext:0042878F                 xor     eax, eax
.itext:00428791                 call    sub_418DE8
.itext:00428796                 mov     eax, [ebp-7Ch]
.itext:00428799                 mov     cx, 1
.itext:0042879D                 pop     edx
.itext:0042879E                 call    sub_418B4C
.itext:004287A3                 mov     [edi], eax
.itext:004287A5                 inc     esi
.itext:004287A6                 add     edi, 4
.itext:004287A9                 dec     ebx
.itext:004287AA                 jnz     short loc_428759
.itext:004287AC
.itext:004287AC loc_4287AC:                             ; CODE XREF: .itext:0042874F↑j
.itext:004287AC                 mov     ebx, esi
```

通过 cmd 参数 -start 运行进程等待新创建的加密子进程执行完毕后，在桌面创建勒索信息提示文件，使用记事本 notepad.exe 打开文件以提示用户，最后自我删除退出。

```
.itext:004287E3                 call    sub_4222D8
.itext:004287E8                 lea     edx, [ebp-84h]
.itext:004287EE                 xor     eax, eax
.itext:004287F0                 call    sub_418920      ; 获得桌面路径
.itext:004287F5                 mov     edx, [ebp-84h]
.itext:004287FB                 mov     cl, 1
.itext:004287FD                 mov     eax, ds:dword_42FA2C
.itext:00428802                 call    sub_42542C      ; 打开记事本
.itext:00428807                 mov     al, 1
.itext:00428809                 call    sub_42657C      ; 退出进程
.itext:0042880E ; ---------------------------------------------------------------------------
.itext:0042880E                 xor     eax, eax
.itext:00428810                 pop     edx
.itext:00428811                 pop     ecx
.itext:00428812                 pop     ecx
.itext:00428813                 mov     fs:[eax], edx
.itext:00428816                 push    offset loc_4288A7
.itext:0042881B
.itext:0042881B loc_42881B:                             ; CODE XREF: .itext:004288A2↓j
.itext:0042881B                 lea     eax, [ebp-84h]
```

文件的加密：

病毒程序对本地资源和局域网资源文件加密；在对本地资源进行加密时，搜索判断文件资源所在的目录，对于用户浏览器需要用到的资源不加密，而在网络资源加密则是通过文件名的后缀来进程加密的。

```
.itext:004284C2                call    sub_4196F8
.itext:004284C7                mov     edx, [ebp-34h]
.itext:004284CA                lea     eax, [ebp-30h]
.itext:004284CD                call    sub_404FA0
.itext:004284D2                mov     edx, [ebp-30h]
.itext:004284D5                pop     eax
.itext:004284D6                call    sub_4050E4
.itext:004284DB                jnz     short loc_4284F5 ; 本地文件
.itext:004284DD                push    1
.itext:004284DF                mov     ecx, ds:dword_4304A0
.itext:004284E5                mov     dl, 1
.itext:004284E7                mov     eax, ds:off_425968
.itext:004284EC                call    sub_4259D8
.itext:004284F1                mov     ebx, eax
.itext:004284F3                jmp     short loc_42850B ; 网络文件
.itext:004284F5 ; ---------------------------------------------------------------------------
.itext:004284F5
.itext:004284F5 loc_4284F5:                            ; CODE XREF: .itext:004284DB↑j
.itext:004284F5                push    0
.itext:004284F7                mov     ecx, ds:dword_4304A0
.itext:004284FD                mov     dl, 1
.itext:004284FF                mov     eax, ds:off_425968
.itext:00428504                call    sub_4259D8
.itext:00428509                mov     ebx, eax
.itext:0042850B
.itext:0042850B loc_42850B:                            ; CODE XREF: .itext:004284F3↑j
.itext:0042850B                mov     eax, ebx
.itext:0042850D                call    sub_414554
.itext:00428512                push    0FFFFFFFFh
.itext:00428514                mov     eax, [ebx+4]
.itext:00428517                push    eax
.itext:00428518                call    WaitForSingleObject
.itext:0042851D
.itext:0042851D loc_42851D:                            ; CODE XREF: .itext:0042840A↑j
.itext:0042851D                push    0
```

```
00422EE1   8BD0           MOV EDX,EAX
00422EE3   8B8D 24FDFFFF  MOV ECX,DWORD PTR SS:[EBP-0x2DC]
00422EE9   8B45 F0        MOV EAX,DWORD PTR SS:[EBP-0x10]
00422EEC   E8 AB47FFFF    CALL <buran.WriteFile>                加密后的内容写入文件
00422EF1   8D45 E0        LEA EAX,DWORD PTR SS:[EBP-0x20]
00422EF4   50             PUSH EAX
00422EF5   8D85 E8FCFFFF  LEA EAX,DWORD PTR SS:[EBP-0x318]
00422EFB   8B4D F8        MOV ECX,DWORD PTR SS:[EBP-0x8]
00422EFE   8B55 FC        MOV EDX,DWORD PTR SS:[EBP-0x4]
00422F01   E8 D61AFEFF    CALL buran.004049DC
00422F06   8B85 E8FCFFFF  MOV EAX,DWORD PTR SS:[EBP-0x318]
00422F0C   8B55 F4        MOV EDX,DWORD PTR SS:[EBP-0xC]
00422F0F   8D4A 0C        LEA ECX,DWORD PTR DS:[EDX+0xC]
00422F12   8B55 F4        MOV EDX,DWORD PTR SS:[EBP-0xC]
00422F15   83C2 14        ADD EDX,0x14
00422F18   E8 4FE3FFFF    CALL buran.0042126C                   RSA加密
00422F1D   8D95 E4FCFFFF  LEA EDX,DWORD PTR SS:[EBP-0x31C]
00422F23   8B45 E0        MOV EAX,DWORD PTR SS:[EBP-0x20]
00422F26   E8 3567FFFF    CALL <buran.EncodeFile>
```

```
00421288   8945 FC        MOV DWORD PTR SS:[EBP-0x4],EAX
0042128B   8B45 FC        MOV EAX,DWORD PTR SS:[EBP-0x4]
0042128E   E8 B138FEFF    CALL buran.00404B44
00421293   8D45 E8        LEA EAX,DWORD PTR SS:[EBP-0x18]
00421296   8B15 CCED4100  MOV EDX,DWORD PTR DS:[0x41EDCC]       buran.0041EDD0
0042129C   E8 C73FFEFF    CALL buran.00405268
004212A1   8D45 E0        LEA EAX,DWORD PTR SS:[EBP-0x20]
004212A4   8B15 CCED4100  MOV EDX,DWORD PTR DS:[0x41EDCC]       buran.0041EDD0
004212AA   E8 B93FFEFF    CALL buran.00405268
004212AF   8D45 D8        LEA EAX,DWORD PTR SS:[EBP-0x28]
004212B2   8B15 CCED4100  MOV EDX,DWORD PTR DS:[0x41EDCC]       buran.0041EDD0
004212B8   E8 AB3FFEFF    CALL buran.00405268
004212BD   8D45 D0        LEA EAX,DWORD PTR SS:[EBP-0x30]
004212C0   8B15 CCED4100  MOV EDX,DWORD PTR DS:[0x41EDCC]       buran.0041EDD0
004212C6   E8 9D3FFEFF    CALL buran.00405268
004212CB   33C0           XOR EAX,EAX
004212CD   55             PUSH EBP
```

```
0040525C   85C0           TEST EAX,EAX
0040525E   0F84 88FBFFFF  JE buran.00404DEC
00405264   8902           MOV DWORD PTR DS:[EDX],EAX
00405266   C3             RETN
00405267   90             NOP
00405268   31C9           XOR ECX,ECX                           加密
0040526A   53             PUSH EBX
0040526B   8A4A 01        MOV CL,BYTE PTR DS:[EDX+0x1]
0040526E   56             PUSH ESI
0040526F   57             PUSH EDI
00405270   89C3           MOV EBX,EAX
00405272   8D7411 0A      LEA ESI,DWORD PTR DS:[ECX+EDX+0xA]
00405276   8B7C11 06      MOV EDI,DWORD PTR DS:[ECX+EDX+0x6]
0040527A   8B16           MOV EDX,DWORD PTR DS:[ESI]
```

三、清理病毒残留思路

1. 杀死进程 C:\Windows\System32\cmd.exe
2. 删除自启动注册表项

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Local Security Authority Subsystem Service

3. 删除文件

"%HOMEPATH%\AppData\Roaming\Microsoft\Windows\lsass.exe" -start

"C:\Windows\system32\cmd.exe" /C bcdedit /set {default} bootstatuspolicy ignoreallfailures

bcdedit /set {default} bootstatuspolicy ignoreallfailures

%HOMEPATH%\AppData\Local\Temp\C46E9A24.buran

%HOMEPATH%\AppData\Local\Temp\58AE9100.buran

bcdedit /set {default} recoveryenabled no

4. 恢复注册表值

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\D1EB23A46D17D68FD92564C2F1F1601764D8E349\Blob