总结

学到了一些关于多线程的知识

查壳

发现是upx壳，用upx脱壳

ida静态分析

IDA View-A | Pseudocode-B | Pseudocode-A | Hex View-1 | Structures | Enums | Imports

```
int __cdecl main_0(int argc, const char **argv, const char **envp)
{
  void *v3; // ecx
  HANDLE v5; // [esp+D0h] [ebp-14h]
  HANDLE hObject; // [esp+DCh] [ebp-8h]

  sub_4110FF(v3);                               // input flag
  ::hObject = CreateMutexW(0, 0, 0);
  j_strcpy(Destination, Source);
  hObject = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)StartAddress, 0, 0, 0);
  v5 = CreateThread(0, 0, sub_41119F, 0, 0, 0);
  CloseHandle(hObject);
  CloseHandle(v5);
  while ( dword_418008 != -1 )
    ;
  sub_411190();                                 // 判断函数
  CloseHandle(::hObject);
  return 0;
}
```

代码比较简单，主要注意41119F函数和Startaddress函数
Startaddress函数是判断函数

```
void __stdcall StartAddress_0(int a1)
{
  while ( 1 )
  {
    WaitForSingleObject(hObject, 0xFFFFFFFF);
    if ( dword_418008 > -1 )
    {
      sub_41112C(Source, dword_418008);
      --dword_418008;
      Sleep(0x64u);
    }
    ReleaseMutex(hObject);
  }
}
```

点进41112c

```
// positive sp value has been detected, the output may be wrong!
char *__cdecl sub_411940(int a1, int a2)
{
  char *result; // eax
  char v3; // [esp+D3h] [ebp-5h]

  v3 = *(_BYTE *)(a2 + a1);
  if ( (v3 < 'a' || v3 > 'z') && (v3 < 'A' || v3 > 'Z') )
    exit(0);
  if ( v3 < 'a' || v3 > 'z' )
  {
    result = off_418000[0];
    *(_BYTE *)(a2 + a1) = off_418000[0][*(char *)(a2 + a1) - 38];
  }
  else
  {
    result = off_418000[0];
    *(_BYTE *)(a2 + a1) = off_418000[0][*(char *)(a2 + a1) - 96];
  }
  return result;
}
```

发现有一个索引字符串的操作。

看41119f函数。

IDA View-A | Pseudocode-B | Pseudocode-A | Hex View-1 | Structures

```
1  void __stdcall sub_411B10(int a1)
2  {
3    while ( 1 )
4    {
5      WaitForSingleObject(hObject, 0xFFFFFFFF);
6      if ( dword_418008 > -1 )
7      {
8        Sleep(0x64u);
9        --dword_418008;
10     }
11     ReleaseMutex(hObject);
12   }
13 }
```

该函数只是418008处的值减1罢了

418008是个索引值

从29开始

也就是说

整个代码的逻辑使得只对source的奇数索引的值进行了修改。

写下脚本

File Edit Format Run Options Window Help

```
check ='TOiZiZtOrYaToUwPnToBsOaOapsyS'.encode()
check = list(check)
addr = 'QWERTYUIOPASDFGHJKLZXCVBNMqwertyuiopasdfghjklzxcvbnm'.encode()
addr = list(addr)
flag = []
for i in range(len(check)):
    key = check[i]
    if i%2==1:
        for j in range(len(addr)):
            if addr[j]==key:
                a = j+38
                if 65<= a and a<=90:
                    flag.append(a)
                else :
                    flag.append(j+96)
                break
    else:
        flag.append(key)
print(bytes(flag))
```