恶意文件分析

发表于 2021-09-01 分类于 Challenge， 2021， 工业信息安全技能大赛， 线上赛-第一场
Challenge | 2021 | 工业信息安全技能大赛 | 线上赛-第一场 | 恶意文件分析

点击此处获得更好的阅读体验

WriteUp来源

来自Venom战队

题目描述

题目考点

解题思路

使用DIE查壳，没查到壳。

进去类似一个shell

程序流程，输入32长度的哈希字符串，bytes.fromhex然后运行关键 crackme 函数。

findcrypt发现文件中有CRC32常量。

crackme函数中包含了一个硬编码的key

从开源项目中可以检索到。

https://github.com/TurboPack/LockBox3/blob/master/run/ciphers/uTPLb_AES.pas

https://chromium.googlesource.com/chromiumos/platform/ec/+/refs/heads/stabilize-7797.B/test/tpm_test/crypto_test.xml

输入与硬编码的Key、加密结果作比较。16轮。

循环16次看ECX值即可dump出预期输入。拼起来可以得到： `22d72a581f3a61e61e5b127e47ad8c0c`

将这个值输入程序，得到flag

Flag

```
1 flag{robotSayHi}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/线上赛-第一场/qKFsrSPACt5ULrvZZf2DtG.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2021 # 工业信息安全技能大赛 # 线上赛-第一场

OPC协议分析
Modbus采集分析