2021年中国工业互联网安全大赛核能行业赛道writeup之鱿鱼游戏

原创

苦行僧(csdn) 于 2021-10-21 21:13:03 发布 1546 收藏
分类专栏： 信息安全 文章标签： CTF writeup

本文链接：https://blog.csdn.net/qpeity/article/details/120818960

目录

附加题 鱿鱼游戏（来自最近一部很火的韩剧）

题目描述：

> 小王由于操作不规范，误将不明U盘插入到上位机中，导致上位机中的某些关键文件被加密，但攻击者在U盘中还留下了一个可执行文件，并且留下了一段话：该程序只有在特定的时间段内才能打开，如果过早或过晚打开该文件，会导致当前目录下的所有文件被加密。如果在规定时间打开了该文件，则会直接得到解密的key来恢复被加密的文件。

附件下载

2021-10-12T15_40_42.709833+00_00Squid_game_.exe.zip-网络攻防文档类资源-CSDN下载

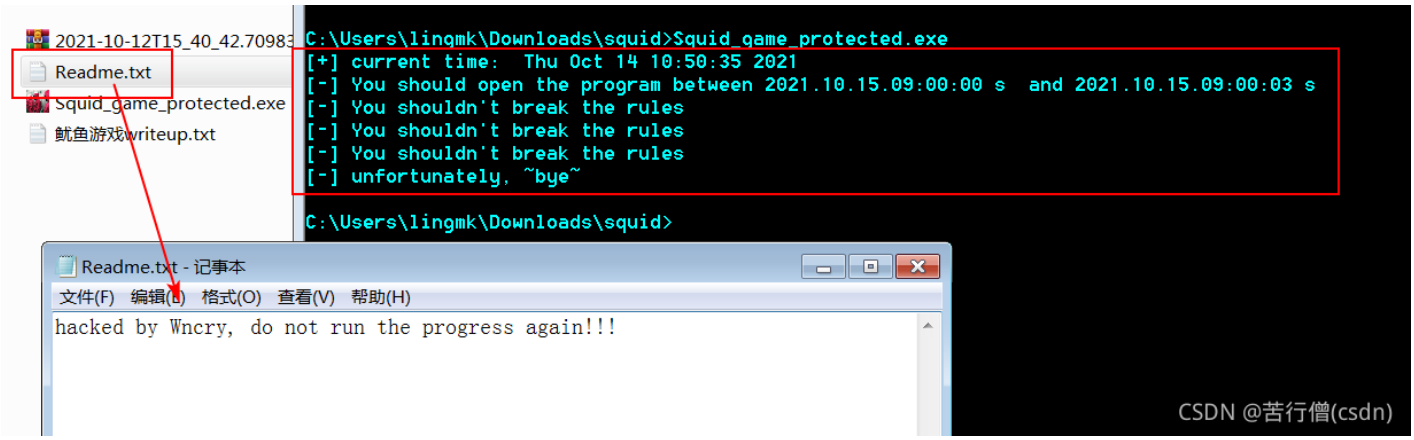
注意，题目里的EXE文件不要直接执行，应放入虚拟机，做好快照，再在一个文件夹中执行，避免不必要的损失。

这道题很有意思，不是靠技术破解到 flag！

一、尝试

附件解压缩，一个可执行文件 squid_game_protected.exe 。

执行一下 squid_game_protected.exe 。

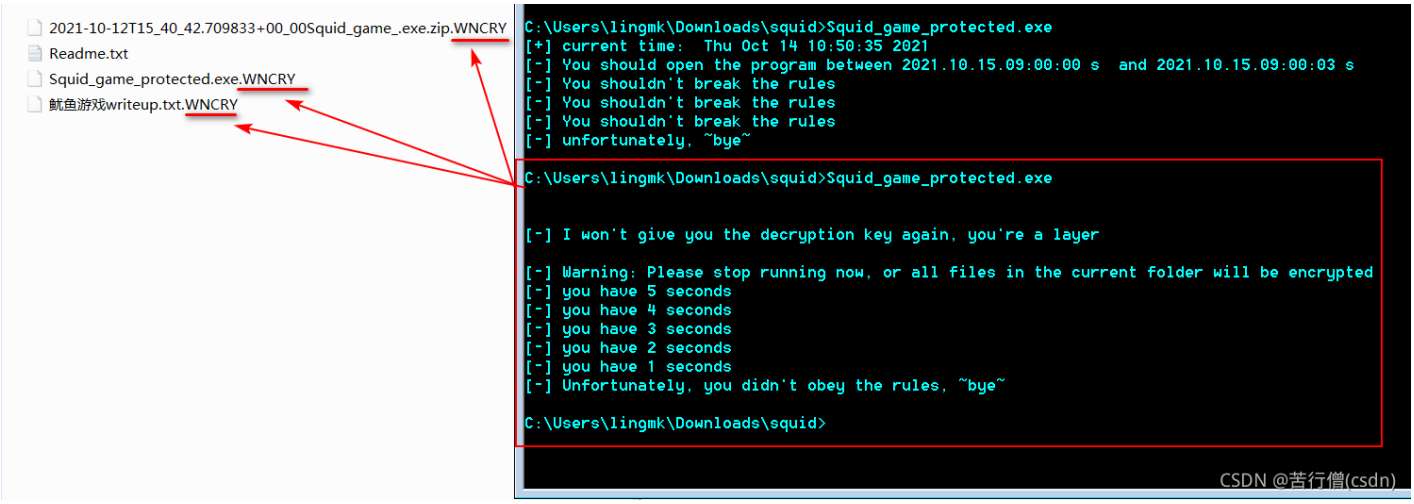


多出个文件，Readme.txt 里面是句狠话，出自臭名昭著的勒索病毒 WannaCry ，我偏要再次执行一下。

再次执行时，程序停顿了几秒，然后提示，结果文件夹里的文件都被加密了，实际上只是每个文件的扩展名都变成了.WNCRY。模拟了Wanna Cry 勒索病毒的加密过程，恢复文件只要把扩展名改回去就行。

此后不管怎样执行，提示信息都一样，不会再提示日期时间信息，因此这个程序第一次执行就要破解。

所以要注意，题目里的EXE文件不要直接执行，应放入虚拟机，做好快照，再在一个文件夹中执行，避免不必要的损失。

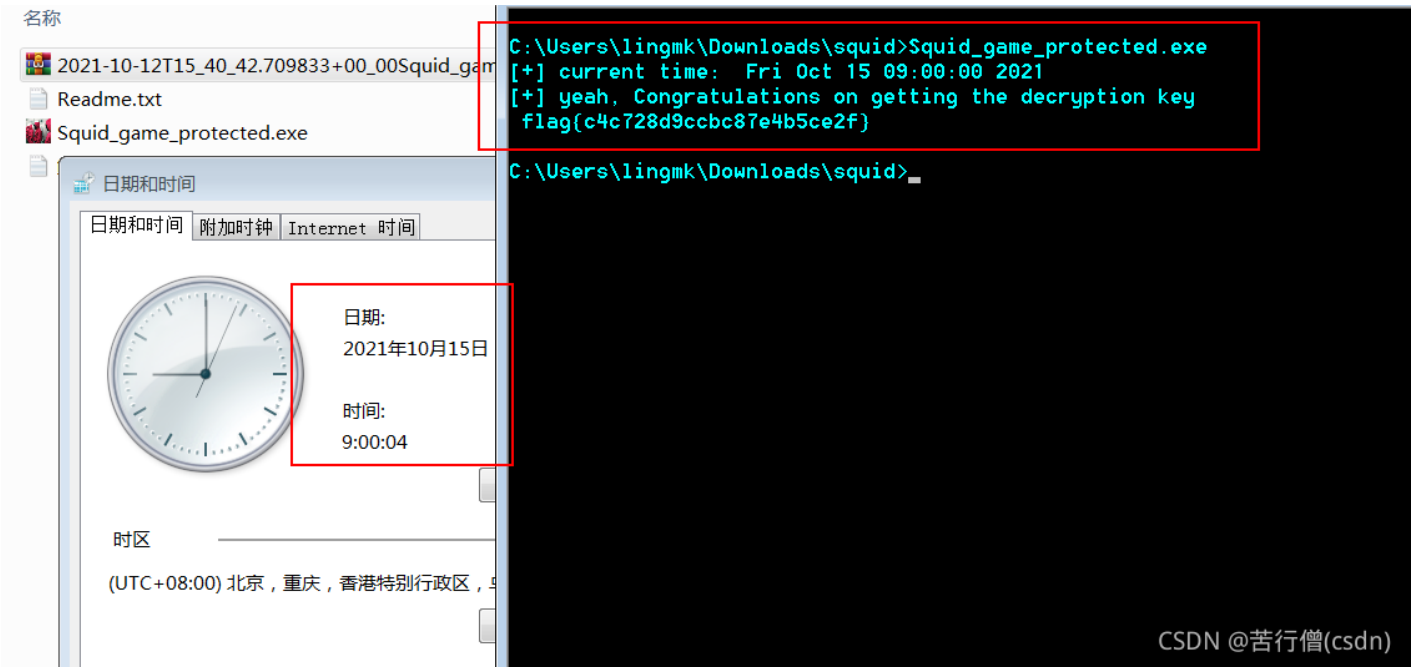


二、Writeup

结合提示信息，分析这个程序只能在 2021.10.15.09:00:00 s 到 2021.10.15.09:00:03 s 之间的时间段内才能执行。那就把操作系统时间改了吧。

先重新解压缩一个 squid_game_protected.exe ，把操作系统时间改成 2021.10.15.08:59:50，再赶紧到命令行窗口，为确保能在 2021.10.15.09:00:00 s 到 2021.10.15.09:00:03 s 之间第一次执行 squid_game_protected.exe，要再大约 2021.10.15.08:59:54 的时候按下回车。

执行直接得到flag —— flag{c4c728d9ccbc87e4b5ce2f}


名称
2021-10-12T15_40_42.709833+00_00Squid_gam
Readme.txt
Squid_game_protected.exe
日期和时间
日期和时间
附加时钟
Internet 时间
日期:
2021年10月15日
时间:
9:00:04
时区
(UTC+08:00) 北京，重庆，香港特别行政区，
C:\Users\lingmk\Downloads\squid>Squid_game_protected.exe
[+] current time: Fri Oct 15 09:00:00 2021
[+] yeah, Congratulations on getting the decryption key
flag{c4c728d9ccbc87e4b5ce2f}
C:\Users\lingmk\Downloads\squid>
CSDN @苦行僧(csdn)