恶意软件后门分析

发表于 2021-01-25 更新于 2021-02-16 分类于 Challenge ， 2019 ， 工业信息安全技能大赛 ， 山东站
Challenge | 2019 | 工业信息安全技能大赛 | 山东站 | 恶意软件后门分析

点击此处获得更好的阅读体验

WriteUp来源

https://www.dazhuanlan.com/2019/12/30/5e09dcd470284/

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{}*

题目考点

- *逆向分析*

解题思路

拖到IDA里

分析和反编译调用的函数，查看外连的ip地址，在函数sub_402174函数发现了一个外网ip,如下图，反编译进一步分析

发现，与本地`10.15.1.68:3128`端口进行了交互，继续深入查看找到后门IP

Flag

```
1 flag{5.39.218.152}
```


 # Challenge # 2019 # 工业信息安全技能大赛 # 山东站
工控安全取证
简单的APK分析