恶意软件样本分析

发表于 2021-01-25 更新于 2021-02-17 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 | 恶意软件样本分析

点击此处获得更好的阅读体验

WriteUp来源

来自MO1N战队

题目描述

> *某家工厂曾发生过宕机事件案例，为防止再发生此事找了技术人员分析攻击行为流量数据包后发现许多异常端口连接记录，最终得到了这个罪魁祸首的病毒样本，请分析病毒样本尝试复现事件案例帮助工厂实施应急演练*

题目考点

- *代码审计*

解题思路

nc 监听 1502/udp 端口，然后把程序跑起来，用 tcpdump 抓包

Flag

```
1 flag{0100000001fc}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/山东站/jzTeGekVA89DzkGWeK3dy4.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 # 2019 # 工业信息安全技能大赛 # 山东站
Tesla工业APP分析
异常的S7数据