S7

2021-09-01 | Challenge， 2021， 工业信息安全技能大赛， 巡回赛-杭州站

Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-杭州站 | S7

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

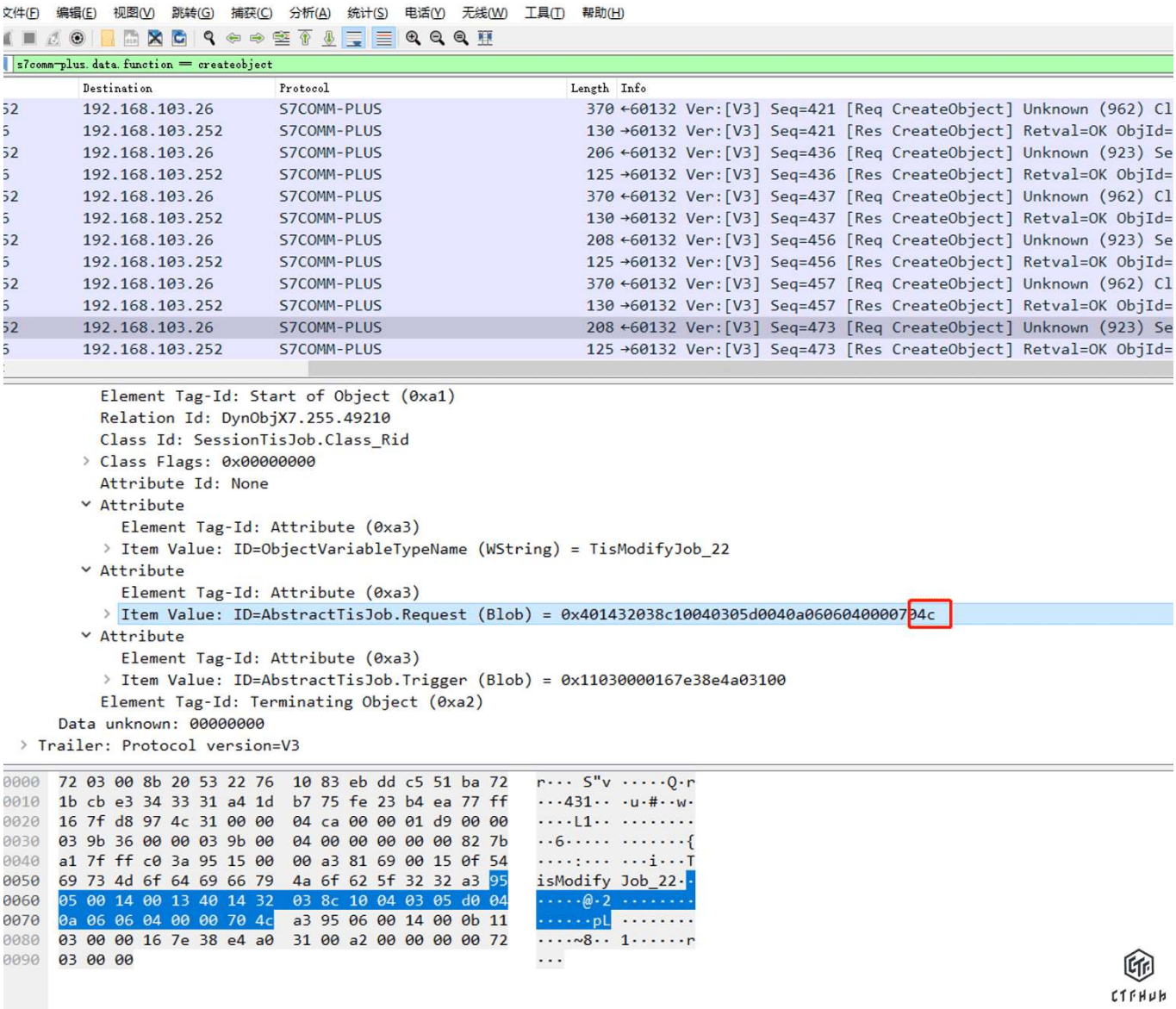
> 工业协议中存在异常数据。请通过流量中的数据找寻 flag，flag形式为 flag{}。提交时请提交括号内内容。

题目考点

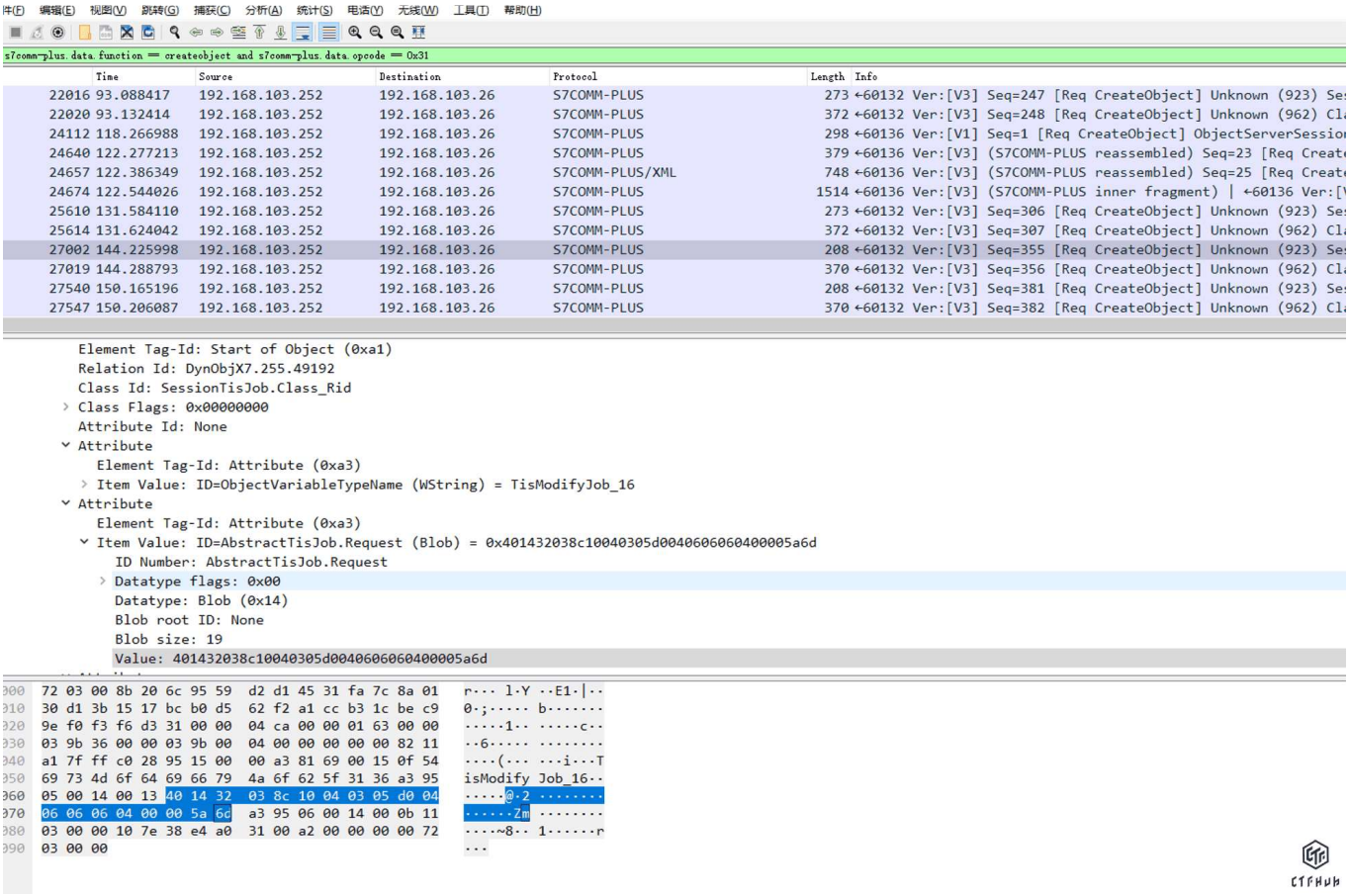
- 流量分析
- S7Comm协议

解题思路

过滤 `s7comm-plus.data.function == createobject`， 发现有写操作



添加过滤条件 `s7comm-plus.data.opcode == 0x31` ，筛选写操作数据



得到字符串 `ZmxhZ3s5d3pLc0x0bVdmWVduTk00fQ`

Base解密得到flag

Flag

```
flag{9wzKsLtmWfYWnNM4}
```


Challenge # 2021 # 工业信息安全技能大赛 # 巡回赛-杭州站

‹ Industry_noaCry 三句话让 PLC 为你吐 FLAG ›