

# Malware

发表于 2021-09-01 分类于 [Challenge](#) , [2021](#) , [工业信息安全技能大赛](#) , [巡回赛-上海站](#)  
[Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-上海站 | Malware](#)

[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

某工业企业，遭受到病毒的攻击，通过对截获的病毒样本逆向分析，分析主要功能，找出黑客的IP，flag为IP地址。

## 题目考点

- 流量分析
- modbus 协议分析

## 解题思路

附件下载下来之后是个加密的rar文件，直接丢到在线解密

□  
得到压缩包密码为1234，将解压出来的样本直接丢到VT进行行为分析，在其中找到C2地址

## Flag

```
1 flag{192.168.1.24}
```

- 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/巡回赛-上海站/jnGG85JcdQGcumeQmvKWxs.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](#) [#巡回赛-上海站](#)

[Login](#)

[Modbus](#)