工控CTF之协议分析7——OMRON

原创 Shado… 于 2022-12-20 21:16:08 发布 864 收藏 1 版权

分类专栏： CTF刷题 工控 文章标签： 安全 网络协议

CTF刷题 8 订阅 27 篇文章 订阅专栏
工控 5 订阅 9 篇文章 订阅专栏

协议分析

流量分析

主要以 工控 流量和恶意流量为主，难度较低的题目主要考察Wireshark使用和找规律，难度较高的题目主要考察协议定义和特征简单只能简单得千篇一律，难可以难得五花八门

常见的工控协议有：Modbus、MMS、IEC60870、MQTT、CoAP、COTP、IEC104、IEC61850、S7comm、OMRON等

由于工控技术起步较早但是统一的协议规范制定较晚，所以许多工业设备都有自己的协议，网上资料数量视其设备普及程度而定，还有部分协议为国家制定，但仅在自己国内使用，网上资料数量视其影响力而定

CTF之协议分析文章合集

工控CTF之协议分析1——Modbus
工控CTF之协议分析2——MMS
工控CTF之协议分析3——IEC60870
工控CTF之协议分析4——MQTT
工控CTF之协议分析5——COTP
工控CTF之协议分析6——s7comm
工控CTF之协议分析7——OMRON
工控CTF之协议分析8——特殊隧道
工控CTF之协议分析9——其他协议

文中题目链接如下

站内下载
网盘下载：https://pan.baidu.com/s/1vWowLRkd0IdvL8GoMxG-tA?pwd=jkkg
提取码：jkkg

OMRON FINS

欧姆龙厂商

命令代码(Command CODE)特别多，主要关注读写相关，如：

- Memory Area Read (0x0101)
- Memory Area Write (0x0102)
- Multiple Memory Area Read (0x0104)
- Memory Area Transfer (0x0105)
- Parameter Area Read (0x0201)
- Parameter Area Write (0x0202)
- Data Link

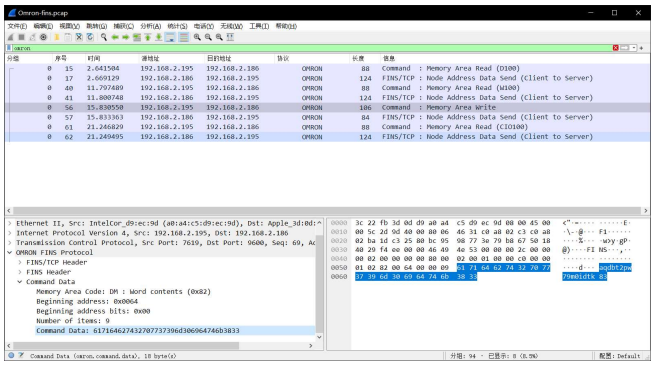
Shadow丶S 关注 0 1

- Data Link Table Write (0x0221)
- Program Area Read (0x0306)
- Program Area Write (0x0307)
- ...

例题1 2020ICSC哈尔滨站—Omron Fins

题目要求：找到写入的异常数据

协议名写在题目上，直接筛选，寥寥几条数据，只有一个是写入



得到的数据发现不是flag，但是又没有其他数据写入

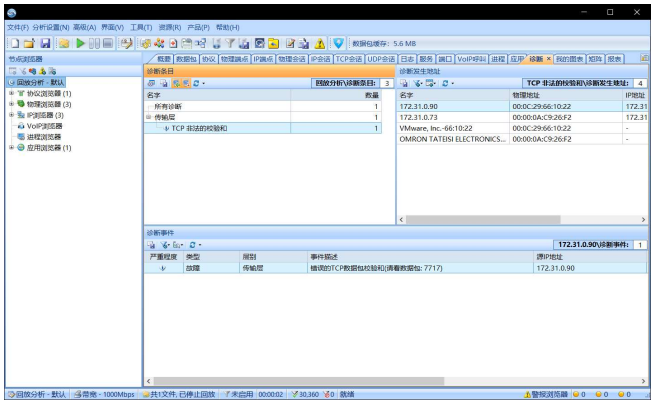
之前其实也有这样的题目，数据是两两字节存入，可能是要做前后翻转，只能去找omron协议数据存储方式或者尝试

例题2 2021ICSC线上—异常的Fins协议分析

题目要求：找到异常的数据流，flag为其数据流序号

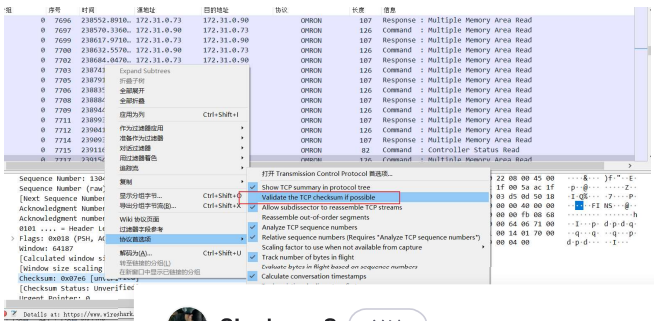
偏脑洞，不太像工控题目

打开看看omron协议很多，很杂，无从下手，在科来网络分析系统中诊断出一个问题，tcp校验和异常



这个其实就是flag，题目名叫Fins协议，但是实际题目和工控基本没有什么关系，最多也就是omron是tcp下级

做题实在没思路就把wiresharktcp校验检查打开看看

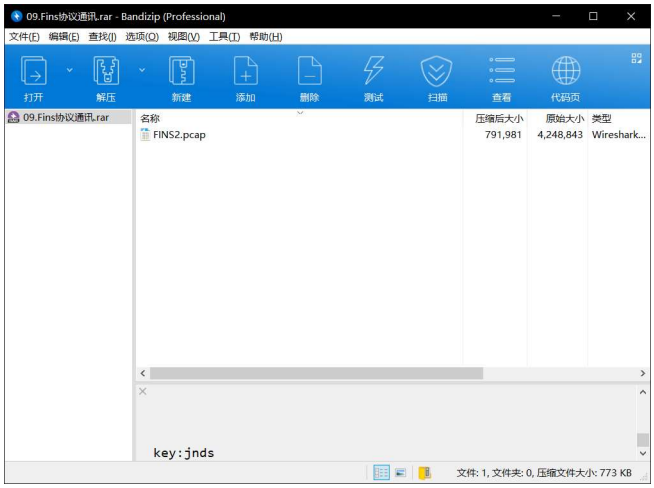


Shadow丶S 关注 0 1

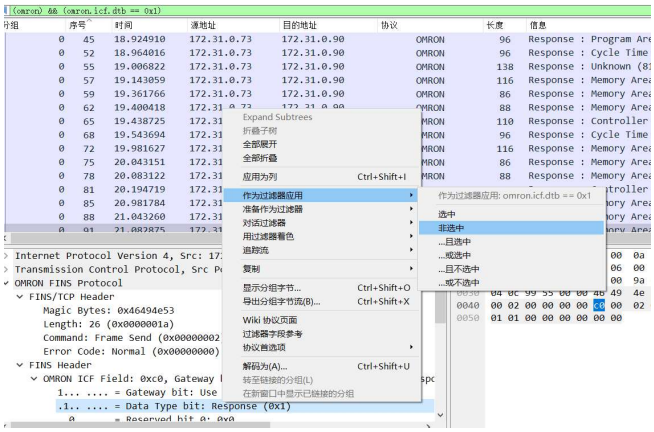
例题3 2021ICSC线上—Fins协议通讯

偏脑洞

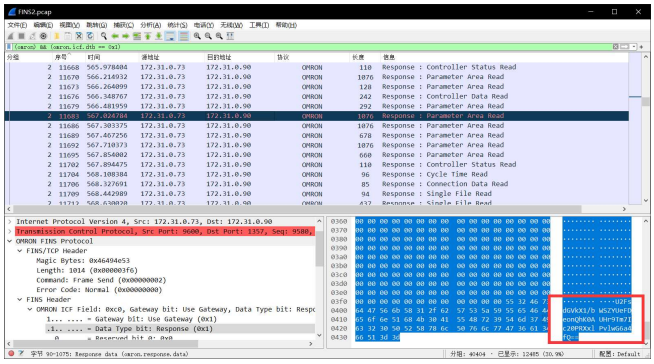
在压缩包底部注释发现key:jnds



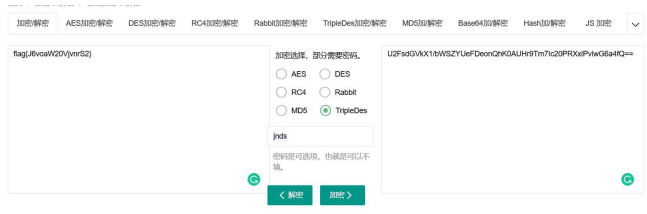
omron协议一般没有很好地过滤方法，大致看了看，都是read，一般来说read的结果都在返回数据中，先筛选看一看



大致看了一遍 发现一个错误数据，发现还是tcp校验和，也可以根据数据包的长度筛选，要么flag是明文很短，要么加密后数据很长



U2fsd一般都是对称加密的结果



基本这种不怎么好分析的协议大多偏脑洞，碰运气，想到了就想到了

Shadow丶S 关注 0 1

文章知识点与官方知识档案匹配，可进一步学习相关知识

网络技能树 支撑应用程序的协议 应用层的作用 35916 人正在系统学习中

欧姆龙FinsTCP/UDP模拟器与协议解析文档 09-25
欧姆龙FinsTCP/UDP模拟器与协议解析文档，测试可用。 协议解析…

OmronFins通讯协议 04-24
FINS(factory interface network service) 通信协议是欧姆龙公司开发…

如何安装OMRON的FINS协议_久久爆品汇的博客 7-18
首先,从OMRON的官方网站下载FINS协议的安装程序。 运行安装程序,并按…

OMRON_PLC_CP1H_HostLink通讯协议解析_欧姆龙hostlink… 7-7
OMRON_PLC_CP1H_HostLink通讯协议解析 前言:欧姆龙的硬件连接,见文…

欧姆龙Fins协议（FinsUDP/FinsTCP） zouzh的专栏 3953

黑马物联云盒子连接Omron HOSTLINK 串口… heimaiot的博客 2104
Omron Hostlink Serial 协议是欧姆龙公司专为其 PLC 开发的通讯协议。提供…

写OMRON FINS协议解析脚本_Nate Hillick的博客 7-18
写OMRON FINS协议解析脚本 OMRON FINS协议是一种用于工业自动化设…

2021-12-14 WPF上位机 113-欧姆龙协议之读写方法流程解析 7-17
随着人工智能的不断发展,物联网这门技术也越来越重要,很多人都开启了物…

欧姆龙OMRON PLC之Host Link协议（一） hulxprox的博客 3437
//写在前面： 自2010年起，陆续在新浪博客上面发了几篇OMRON PLC的应…

工控CTF（wp） aarong的博客 7089
这里写自定义目录标题欢迎使用Markdown编辑器新的改变功能快捷键合理…

Omron HostLink通讯协议_欧姆龙cp2e 485接受_两岸青山相… 7-16
Omron HostLink通讯协议 Omron HostLink 通信协议是一种串口通信协议。…

欧姆龙OMRON PLC之HostLink通讯协议… hulxprox的博客 8138
//写在前面： 自2010年起，本人陆续在新浪博客上面发了几篇OMRON PLC…

OMRON-FINS(TCP)协议详细解析和攻击 Chary的Blog 1万+
1. FINS协议简介 欧姆龙(Omron)是来自日本的全球制造公司，产品是工业和…

欧姆龙PLC的FINS协议解释（实测通过） 芯动的技术专栏 3万+
欧姆龙PLC的FINS协议解释 UDP访问方式： 读取示例：读取DM区20个字, …

工控CTF之协议分析2——MMS song123sh的博客 1034
工控CTF之协议分析2——MMS

欧姆龙OMRON PLC之Host Link协议 11-24
欧姆龙OMRON PLC之Host Link协议

工控CTF协议分析学习题目合集 12-20
主页工控CTF学习配套题目，搭配学习

CTF之二维码扫描.7z 12-02
CTF入门之二维码扫描神器，支持二维码修复

从CTF到工控安全.pdf 02-26
从CTF到工控安全.pdf

一道MMS工控协议CTF题的WriteUp-附件资源 03-02
一道MMS工控协议CTF题的WriteUp-附件资源

2021-12-05 WPF上位机 112-欧姆龙协… 热门推荐 时光隧道 3万+
FinsTCP协议 1、Fins是一个公开的协议 网口（Fins-》UDP FinsTCP） Fin…

2022工业互联网大赛-杭州-CTF题目 09-14
第一次参加工控类的CTF，然后正好团队中有一个小伙伴电脑连不上…

2021CTF工业 Shadow丶S 关注 0 1

2021CTF工业信息安全技能大赛-异常的Fins协议分析 某天工业现场生产线…

工控ctf qq_45951598的博客 6352
文章目录黑客的大意 黑客的大意 下载后得到mail，在文件后面jpg 打开图片…

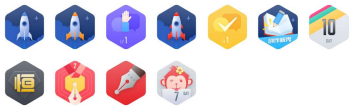
ctf中常用的PHP伪协议 最新发布 02-15
在CTF比赛中，常常会使用PHP伪协议来绕过服务器的安全限制或者执行本…

“相关推荐”对你有帮助么？
非常没帮助 没帮助 一般 有帮助 非常有帮助

关于我们 招贤纳士 商务合作 寻求报道 400-660-0108 kefu@csdn.net 在线客服 工作时间 8:30-22:00
公安备案号11010502030143 京ICP备19004658号 京网文〔2020〕1039-165号
经营性网站备案信息 北京互联网违法和不良信息举报中心 家长监护 网络110报警服务
中国互联网举报中心 Chrome商店下载 账号管理规范 版权与免责声明 版权申诉 出版物许可证
营业执照 ©1999-2023北京创新乐知网络技术有限公司

Shadow丶S
码龄4年 高校学生

126	4万+	2万+	25万+	
原创	周排名	总排名	访问	等级
1830	202	306	48	1675
积分	粉丝	获赞	评论	收藏



私信 关注

搜博主文章

热门文章

分类专栏

最新评论

【计算机网络】IP地址详解
大口喝咖啡: 应该是本地地址吧

域——windows服务器域详解
Shadow丶S: 什么参数，具体点

域——windows服务器域详解
sweet-琉璃: 参数不正确怎么办呢?

华为模拟器eNSP免费下载
打码不打你: 文件没了

最新文章

LitCTF2023 WP

工控CTF之协议分析6——s7comm

工控CTF之协议分析8——特殊隧道

2023年 1篇　　2022年 91篇
2021年 34篇

目录

Shadow丶S 关注

0 1