窃取数据的黑客

发表于 2021-01-25 分类于 Challenge， 2019， 工业信息安全技能大赛， 哈尔滨站
Challenge | 2019 | 工业信息安全技能大赛 | 哈尔滨站 | 窃取数据的黑客

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

> *黑客在入侵了工业上位机后试图用网络中合规通信信道传输敏感文件来躲避流量审计设备对异常流量的告警。分析黑客通过工业协议窃取了什么敏感文件。flag格式{}*

题目考点

- *MMS规约*

解题思路

打开是MMS规约。为2018年原题，

对比发现多读了一个flag.7z，把这个文件提取出来

```
import pyshark

try:
    captures = pyshark.FileCapture("1.pcap")
    flag_frsm = False
    flag_frsm_id = None
    flag_read = False
    for capture in captures:
        for pkt in capture:
            if pkt.layer_name == "mms":
                # file open
                if hasattr(pkt, "confirmedservicerequest") and int(pkt.confirmedservicerequest) == 72:
                    if hasattr(pkt, "filename_item"):
                        filename_items = pkt.filename_item.fields
                        for f in filename_items:
                            file_name = str(f.get_default_value())
                            if file_name == "flag.7z":
                                flag_frsm = True
                if hasattr(pkt, "confirmedserviceresponse") and int(pkt.confirmedserviceresponse) == 72 and flag_frsm:
                    # print(pkt.field_names)
                    if hasattr(pkt, "frsmid"):
                        flag_frsm_id = pkt.frsmid
                    flag_frsm = False
                # file read
                if hasattr(pkt, "confirmedservicerequest") and int(pkt.confirmedservicerequest) == 73 and flag_frsm_id:
                    if hasattr(pkt, "fileread"):
                        if str(pkt.fileread) == str(flag_frsm_id):
                            flag_read = True
                    flag_frsm_id = None
                if hasattr(pkt, "confirmedserviceresponse") and int(pkt.confirmedserviceresponse) == 73 and flag_read:
                    if hasattr(pkt, "filedata"):
                        data = str(pkt.filedata).replace(":", "")
                        print(data)
                    flag_read = False
except Exception as e:
    print(e)
```

然后写入hex为7z文件打开即为flag

Flag

```
flag{flag.txt.flag.txt}
```

 # Challenge # 2019 # 工业信息安全技能大赛 # 哈尔滨站