Tesla工业APP分析

发表于 2021-01-25 更新于 2021-02-16 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 | Tesla工业APP分析

点击此处获得更好的阅读体验

WriteUp来源

https://www.cnpanda.net/ctf/415.html

题目描述

> *某安全团队捕获间谍发送的工业APP，安全人员怀疑间谍以某种方式将机密信息传递出去，尝试分析该文件，找出flag。*

题目考点

解题思路

题目为TeslaMultiSCADA软件，版本号已经被修改，以免参赛者快速找到对应版本的正版app。同时对该apk和1.10.3版本的正版软件进行反编译对比，很快可以发现有一个apk被伪装成字体文件。发现该apk已经被加固保护，使用IDA或DexHunter等工具对其脱壳，反编译的java层代码如下图：

需要识别出java层的加密算法为base85，关键反编译代码如下：

java层要求我们输入一行字符串，进行base85算法编码后传入so层，将`libnative-lib.so`拖入IDA进行反汇编操作，从函数`Java_bin_crack_easyandroid_MainActivity_stringFromJNI`开始分析。

该函数并没有关键逻辑，值得提醒的是，so进行了字符串加密保护，选择手动逆向`datadiv_decode1035220665707354481 4`函数并解密字符串，或者直接动态调试apk。

当apk运行起来后，字符串会自动解密，接下来重点关注sub_2E74函数。

该函数流程已经被高度混淆，可以有选择的对其调用的子函数进行断点跟踪（需要注意apk的断点扫描检测，发现断点会直接崩溃），根据动态调试的数据分析并识别出重点函数sub_1228（变异SM4算法ECB模式），sub_DA4（变异base91算法）。分析出SM4魔改的数据如下：

Base91魔改的数据如下：

至此了解了程序加密流程以及加密算法，但依然缺少SM4加密密钥和最终的密文，对apk进行res资源反混淆，发现如下图文件：

爆破解密脚本如下：

```
data = "D4E8E5A0EBE5F9A0E9F3A0D9EFF5F2E5DFF6E5F2F9DFF3EDE1F2F4ACC3E9F0E8E5F2F4E5F8F4A0E3EFEEF3E9F3F4F3A0EFE6A0F4E8F2E5E5A0F0E1F2F4F3ACC3EFEDE5A0EFEEA1".decode("hex")
for i in range(256):
    string = ''
    for j in data:
        string += chr(ord(j)-i)
    print string
```

得到key为`Youre_very_smart`，密文分为三部分，通过文件比对软件很容易找到三处位置

- *`functions_fr.properties`文件*
- *`smali/d/a/a/a/b/a`*
- *`smali/android/support/v7/internal/view/menu/ActionMenuItemView`*

逐个进行查看

`s_fr.properties`文件

看着像摩尔斯电码，其实是brainfuck，'/'对应'!'，'-'对应'?'。解密结果为

`smali/d/a/a/a/b/a`文件

看着像brainfuck，其实是摩尔斯电码，`!`对应`-`，`?`对应`/`。

解密结果如下（摩尔斯电码不分字母大小写，其实正确的结果为全部字母小写）

`smali/android/support/v7/internal/view/menu/ActionMenuItemView`文件

看着像brainfuck，其实就是brainfuck，`!`对应`?`，`?`对应`!`。解密结果如下

接下来就是三部分密文的排列组合问题，必有一个字符串可以通过base91解密->SM4解密->base85

解密即可得到正确的flag

Flag

```
1 flag{Andr01dReMi3clsS0Ea5y!!!}
```

- ***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/哈尔滨站/9JMkZuzbDtLjU1oFvDYjSo.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 # 哈尔滨站
西门子DOS攻击事件
恶意软件样本分析