Attack

发表于 2021-01-16 分类于 Challenge， 2019， 安洵杯， Misc
Challenge | 2019 | 安洵杯 | Misc | Attack

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/6911

题目考点

- *数据包流量分析*
- *蚁剑流量特征*
- *procdump的使用*

解题思路

使用wireshark打开数据包，简单看一下应该是进行了扫目录操作：

然后对TCP流进行分析，发现一处对upload.php的POST请求：

然后追踪TCP流，发现上传了一句话木马：

接着往下分析，发现一组TCP流量疑似执行了命令，请求流量经过了base64混淆，返回流量用了ROT13

继续跟TCP流发现列目录列出来了一个s3cret.zip

下一组流量中出现了一组看起来是zip的数据：

查看hex数据发现`50 4B 03 04`的zip文件头，将其拿出来导入到010editor中保存为zip：

但是发现需要解压密码，打开发现hint

然后可以得到意思是解压密码为administrator的密码，于是继续回去看流量，发现执行了procdump.exe这个工具

如果不熟悉的这个工具话可以使用搜索引擎得知该工具一般用来抓取windows的lsass进程中的用户明文密码

紧接着发现攻击者通过http下载了lsass.dmp文件

我们将该文件导出，然后导入mimikatz即可得到administrator的密码

之后再拿过去解压就得到flag

Flag

```
D0g3{3466b11de8894198af3636c5bd1efce2}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/安洵杯/Misc/4zoYoeA6SLy6BNDMuBUFmc.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 # Misc # 2019 # 安洵杯
secret
whoscion