抖音x-gorgon算法,mas,installid,device_register

原创

qq_45887810 于 2019-12-11 19:44:38 发布 2528 收藏 2

今天有空分享一下抖音的加密算法，作为拥有庞大用户量的App，其通信协议加密的强度肯定是不弱的，关键算法被VM，只能动态分析去理解。我们通过抓包分析，请求的url上带有as、cp两个加密字段，这两个字段是早期版本算法，后又陆续添加了mas、X-gorgon算法。我们今天先对as、cp两个字段进行分析，这个只能通过动态调试去跟踪加密过程。

首先我们通过工具调试定位到函数

```
- [IESAntiSpam testForAlert:msg:]
```

定位的详细过程忽略……，进入继续调试后发现调用sub_102E3345函数进行加密排序

1.整理分析流程

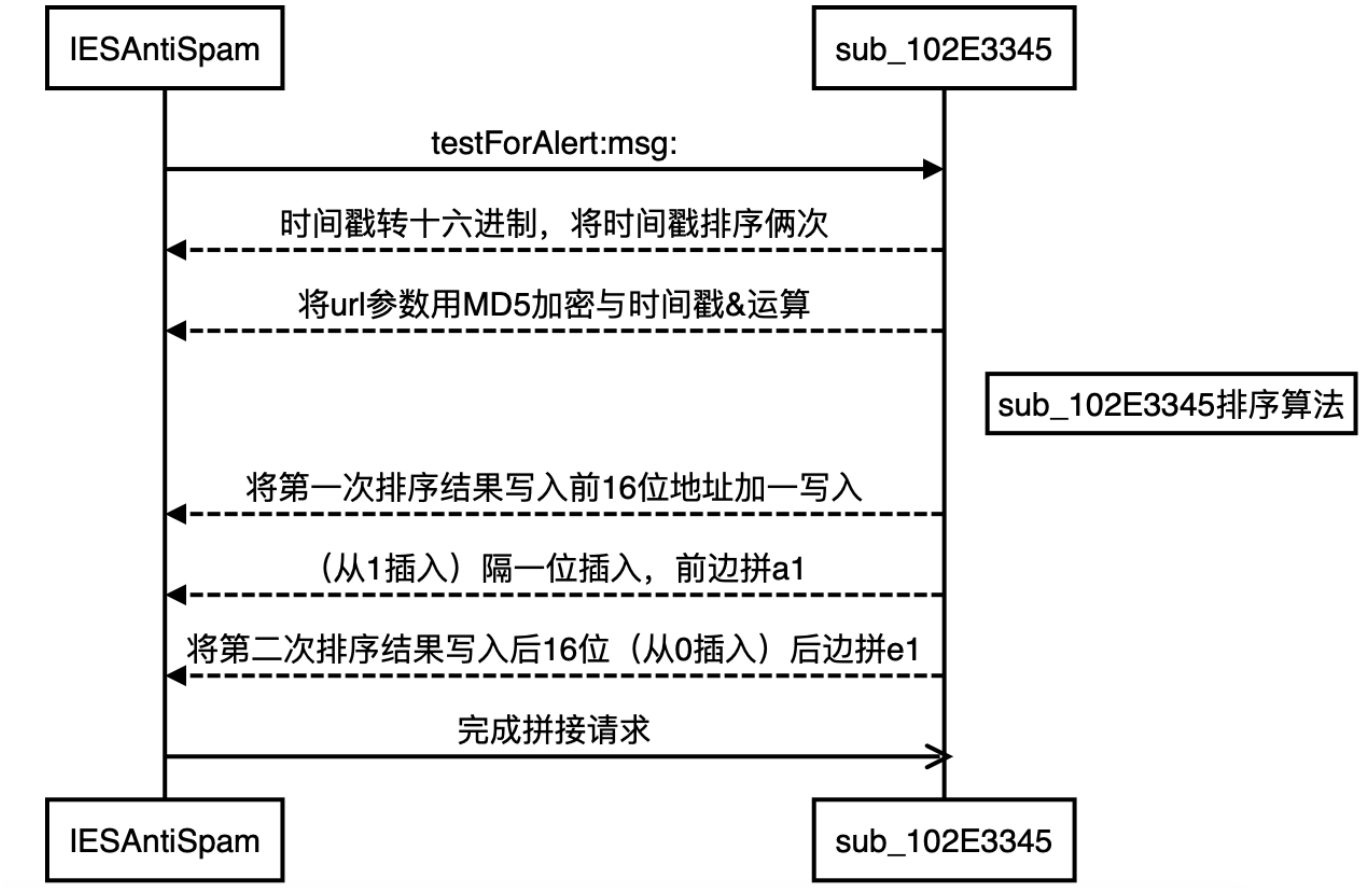
```
1.时间戳转十六进制

2.将时间戳排序俩次，
  a1 v3 是排序key
  sprintf(byte_102323F30, "%08x", a1);
  sprintf(byte_102323F3A, "%08x", v3);

3.将url参数用MD5加密一次或俩次根据时间戳&运算

4.将第一次排序结果写入前16位地址加一写入（从1插入），隔一位插入，前边拼a1

5.将第二次排序结果写入后16位（从0插入）后边拼e1
```

2.结果排序

```
a1d5b43se234dccea7

456dcd5s2320cf3e1

&cp=456fcd5s2320cfs3e1&as=a1d5b43se234dccea7

拼接完成后就可以请求了
```

后期版本添加了mas算法和最新的X-gorgon算法，目前最新系列版本算法如果需要了解的话可以交流。

3.流程详述



4.免责声明

请勿使用本服务于商用或大量抓取
若因使用本服务与抖音官方造成不必要的纠纷，本人盖不负责，存粹技术爱好，若侵犯抖音贵公司的权益，请告知！

5.技术交流

如果有什么不懂的可以联系我交流

邮箱：giulenkas@outlook.com
测试地址：https://www.showdoc.cc/527312186916410?page_id=3113306537235933

6.其他

有快手、小红书、tiktok等其他技术问题，也可随时交流。