mp.weixin.qq.com /s/YAAybJBAvxqrQWYDg31BBw

Bahamut组织近期攻击活动揭露

360烽火实验室 360威胁情报中心

360威胁情报中心

CoreSec360

360威胁情报中心是全球领先的威胁情报共享、分析和预警平台，依托360安全大脑百亿级样本，万亿级防护日志等海量安全数据，整合360漏洞挖掘、恶意代码分析、威胁情报追踪等团队的安全能力，产出高质量的安全威胁情报，驱动安全的防御、检测和响应。

2022-04-12 11:39

收录于话题

#APT 56 个

#Bahamut 1 个

#网络雇佣军 1 个

Bahamut

Bahamut是一个针对中东和南亚的高级威胁组织，其于2017年被Bellingcat披露并命名，随后BlackBerry又对该组织进行了详细全面的分析，并认为该组织属于网络攻击雇佣军。Bahamut组织主要使用钓鱼网站、假新闻网站、社交网站进行攻击。

近期，我们观察到疑似该组织的移动端攻击活动，本次攻击活动开始于1月份，使用钓鱼网站投递移动RAT样本。攻击使用的RAT属于未被披露过的新家族，我们推测属于该组织的特有攻击武器。

1. 载荷投递

我们监控到该组织使用其惯用的攻击手法——钓鱼网站进行载荷的投递。钓鱼网站伪装成安全聊天软件的介绍页面，并提供Android端软件的下载链接。通过钓鱼网站的域名和证书信息，可以知道此次攻击活动开始于2022年1月初，并且至今仍然活跃。

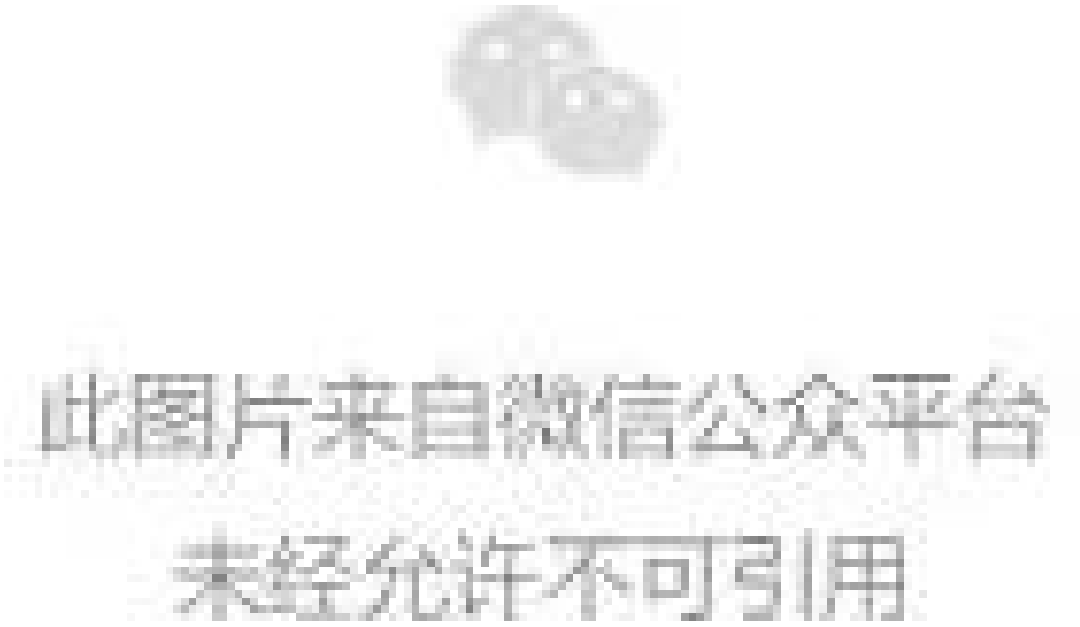

图1 钓鱼页面

图2 网站证书有效期

2. 样本分析

样本基本信息如下：

MD5	文件名	包名
ed43605e6d85c7eab473c30ec1b2271a	securechatnow_v1_0_7.apk	com.example.chatapplication

本次攻击活动中使用的样本为具备远控功能的聊天软件，聊天功能和远控功能单独开发。聊天功能的服务器地址和远控功能的C&C使用的是同一个地址。鉴于聊天和远控使用的同一个C&C地址，以及我们并没有在野外发现与此聊天功能和远控功能相似的开源或公开的源代码，因此我们猜测该样本为独立开发的攻击武器。截止目前，该样本还未被其它安全厂商识别。

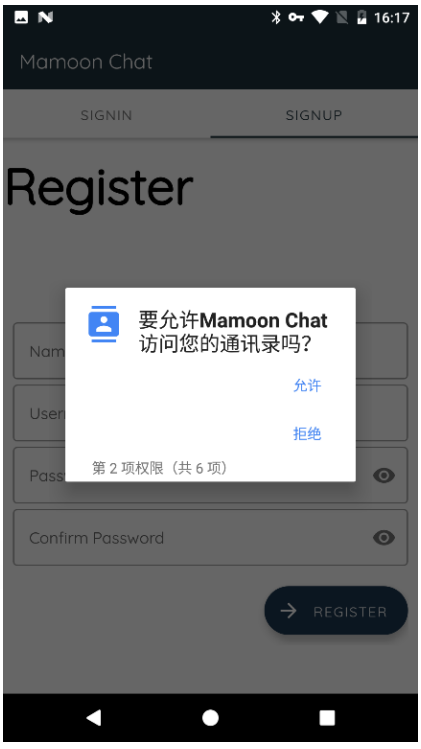

图3 应用运行截图

```
private static final String AUTH_PATH = "chat/api/v0.0.1/user";
public static final String BASE_URL = "https://5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de:8443";
public static final String DELETE_CHAT_THREAD = "https://5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de:8443/chat/api/v0.0.1/chats/deleteChats";
public static final String GET_USER = "https://5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de:8443/chat/api/v0.0.1/user/getUserOrGroup";
public static final Constants INSTANCE = null;
public static final String IS_A_GROUP_MEMBER = "https://5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de:8443/chat/api/v0.0.1/user/checkMemberOfGroup";
public static final String REMOVE_PROFILE_PIC = "https://5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de:8443/chat/api/v0.0.1/user/removeProfilePic";
public static final String SIGNIN_ENDPOINT = "chat/api/v0.0.1/user/login";
public static final String SIGNUP_ENDPOINT = "chat/api/v0.0.1/user/register";
public static final String THUMBNAIL_ACCESS = "https://5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de:8443/files/userName/thumbs/fileName";
public static final String UPDATE_STATUS = "https://5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de:8443/chat/api/v0.0.1/user/userStatusUpdate";
public static final String UPLOAD_DP = "https://5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de:8443/chat/api/v0.0.1/user/profilePicUpload";
public static final String UPLOAD_DP_GROUP = "https://5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de:8443/chat/api/v0.0.1/user/groupProfilePicUpload";
public static final String UPLOAD_MEDIA = "https://5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de:8443/chat/api/v0.0.1/chats/mediaUpload";
private static final String UPLOAD_PATH = "chat/api/v0.0.1/chats";
private static final String privateUrl = "https://5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de:8443";
```


图4 聊天和远控功能的网络配置

样本的远控功能代码主要在com.example.chatapplication.monitoring包中，恶意代码高度模块化编写质量高，使用数据库存储各类信息。除了窃取短信、联系人、通话记录等常见用户隐私信息外，还会借助辅助功能重点窃取大量知名社交软件的聊天信息。

图5 恶意包结构

相关的指令和对应功能如下：

指令	功能
whatsapp	获取whatsapp数据
telegram	获取telegram数据
imo	获取imo数据
viber	获取viber数据
messenger	获取facebook数据
conion	获取conion数据
signal	获取signal数据
info	上传文件或更新操作
callLogs	获取通话记录
contacts	获取联系人
protectedText	窃取文本消息
liveInfos	获取实时位置
fileListing	获取文件列表
smsLogs	获取短信

3. 溯源和归属

根据同家族样本的签名信息，我们关联到了一个疑似归属于Bahamut组织的样本，该疑似样本和本次分析样本的C&C格式极其相似，都是使用的数字和字母的随机组合字符串，都存在一个包含相同路径(/auth/login)的URL，该URL地址显示的是相同的登录页面。并且该疑似样本的同家族样本中，存在两个下载地址是jamaat-ul-islam.com的样本，而该下载地址曾于2020年被Blackbarry披露且归属于Bahamut组织。因此我们将本次发现的攻击样本归属于Bahamut组织。

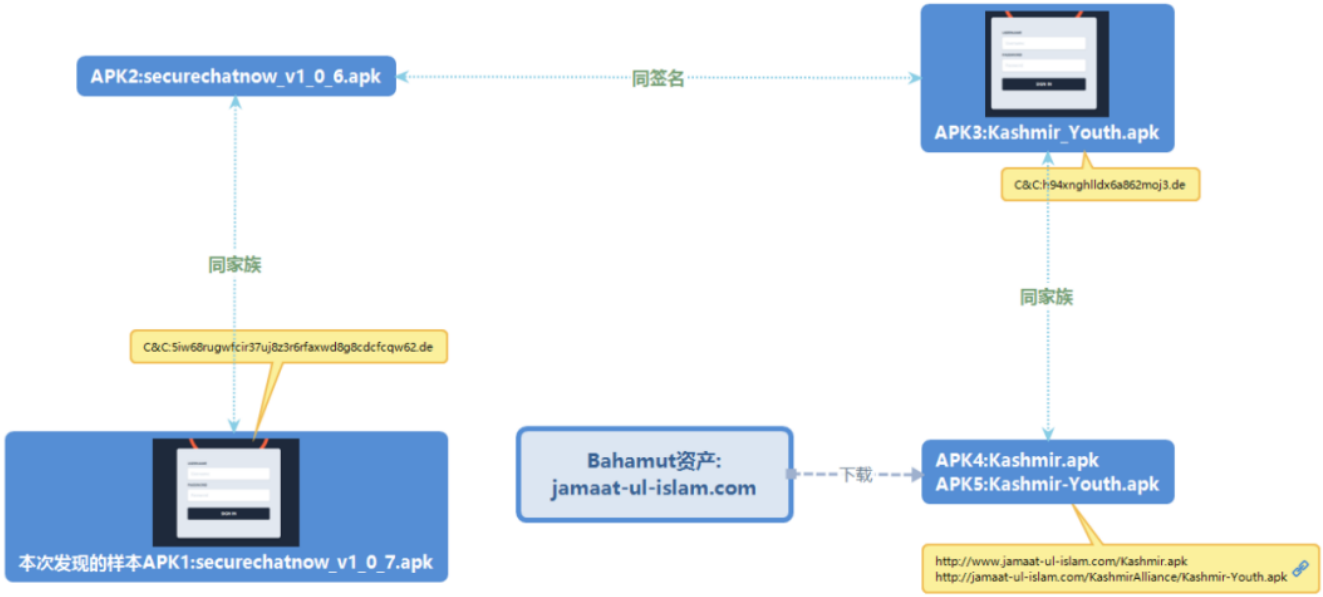

图6 组织归属

图7 Blackbarry披露的Bahamut组织的资产

4. 攻击活动和受害者分析

通过分析该家族样本的创建时间和对样本进行溯源，我们发现，该家族样本最早出现在2020年10月，并在2021年2月出现短暂活跃后一直处于平静状态，直到今年1月份又开始活跃，并且活跃至今。两次活跃期使用了不同的钓鱼网站进行载荷的投递。

图8 同家族样本活跃时间线

通过查询同家族早期样本的用户感染情况，我们发现受害用户的最早感染时间是2021年2月底，这与首次活跃期间钓鱼网站的出现时间相符，地理位置主要集中在沙特阿拉伯、巴基斯坦，这些地区也都与Bahamut组织的主要攻击目标相符。

总结

能够独立开发聊天软件和远控木马，代码结构清晰、质量高，这说明Bahamut组织的开发人员具备较高的开发水平。同时，开发木马化的聊天软件，使用随机化的字符串作为C&C、频繁的网络钓鱼等也说明了该组织具备较强的伪装和攻击技巧。在我们跟进Bahamut此次攻击事件期间，又出现了几个属于该组织的其它家族样本，可见该组织在近期应该有集中的攻击活动。我们会持续关注该组织的攻击动态。

附录 IOC

ad6f124d00ca05f2a19b5215b85e25a8

ed43605e6d85c7eab473c30ec1b2271a

88d421b5b9a7f52f1a961e52c49019b1

45c8120d7108d4d363cddf06e662f0e9

cc2f12845d1eb4023b90c02a73827e23

869ae17c011a213560c04e97e5b53a63

241b578fe963ad199fd5bdc0bb50f4ca

http://www.jamaat-ul-islam.com/Kashmir.apk

http://jamaat-ul-islam.com/KashmirAlliance/Kashmir-Youth.apk

https://www.securechatnow.com/apk/v1/securechatnow_v1_0_6.apk

https://www.securechatnow.com/apk/v1/securechatnow_v1_0_7.apk

https://freesexvideos.ch/adult-v1.apk

h94xnghlldx6a862moj3.de

5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de

参考

https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html

https://www.blackberry.com/us/en/forms/enterprise/bahamut-report

https://blog.cyble.com/2021/08/10/bahamut-threat-group-targeting-users-through-phishing-campaign/