Recent attacks by Bahamut group revealed

Original 360 Beacon Lab 360 Threat Intelligence Center 2022-04-12 11:39

Included in the topic

#APT 56 #Bahamut 1 #cybermercenary 1

Bahamut

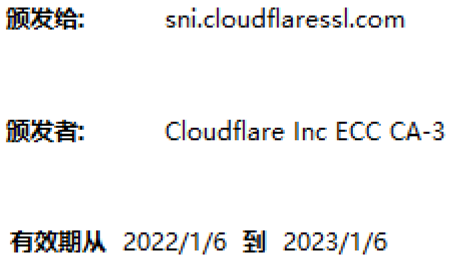
Bahamut is an advanced threat group targeting the Middle East and South Asia. It was disclosed and named by Bellingcat in 2017. Later, BlackBerry conducted a detailed and comprehensive analysis of the group and believed that the group was a cyberattack mercenary. The Bahamut group mainly uses phishing websites, fake news websites, and social networking sites to attack.

Recently, we observed a suspected mobile terminal attack activity of this group. This attack activity started in January and used phishing websites to deliver mobile RAT samples. The RAT used in the attack belongs to a new family that has not been disclosed, and we speculate that it belongs to the group's unique attack weapon.

1. Payload Delivery

We monitored that the organization used its usual attack method - phishing website to deliver payloads. The phishing website pretends to be the introduction page of the secure chat software and provides a download link for the Android software. Through the domain name and certificate information of the phishing website, it can be known that the attack started in early January 2022 and is still active today .

Figure 1 Phishing page



颁发给: sni.cloudflaressl.com

颁发者: Cloudflare Inc ECC CA-3

有效期从 2022/1/6 到 2023/1/6

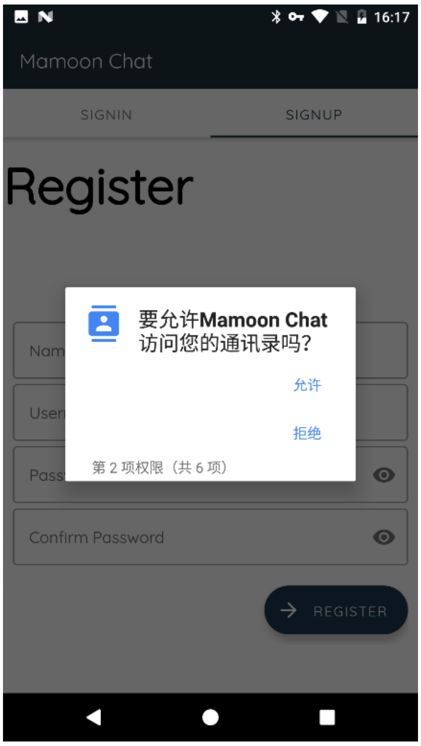
Figure 2 Validity period of website certificate

2. Sample Analysis

The basic information of the sample is as follows:

MD5	file name	Package names
ed43605e6d85c7eab473c30ec1b2271a	securechatnow_v1_0_7.apk	com.example.chatapplication

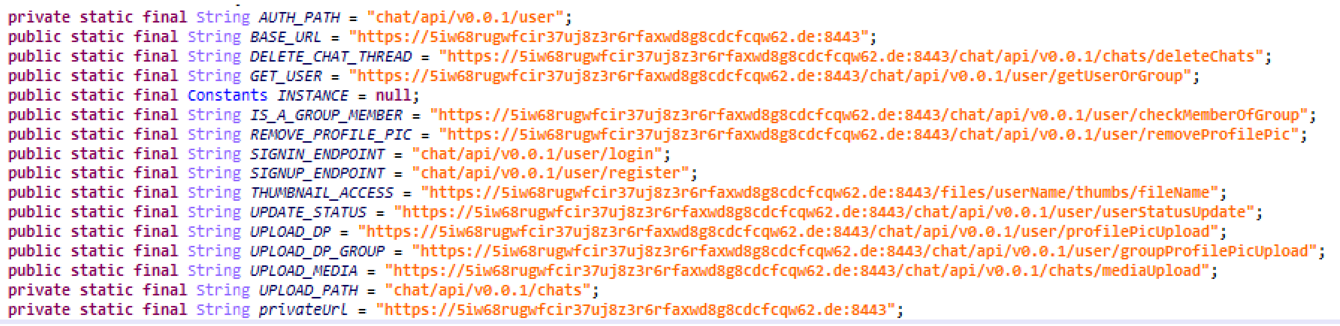
The samples used in this attack are chat software with remote control function, and the chat function and remote control function are developed separately. The server address of the chat function and the C&C of the remote control function use the same address. In view of the same C&C address used for chat and remote control, and we have not found open source or open source code similar to this chat function and remote control function in the wild, we guess that this sample is an independently developed attack weapon. So far, the sample has not been identified by other security vendors.



要允许**Mamoon Chat**访问您的通讯录吗？

第 2 项权限（共 6 项）

Figure 3 Screenshot of application running



```java
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";
```

Figure 4 Network configuration of chat and remote control functions

The remote control function code of the sample is mainly in the com.example.chatapplication.monitoring package . The malicious code is highly modularized and written with high quality, and uses a database to store various information. In addition to stealing common user privacy information such as text messages, contacts, and call records, it also uses auxiliary functions to focus on stealing chat information from a large number of well-known social software.

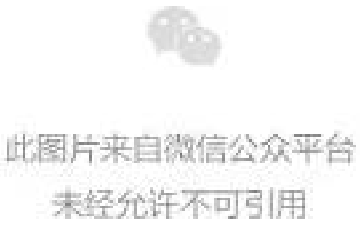


Figure 5 Malicious packet structure

The related commands and corresponding functions are as follows:

instruction	Features
whatsapp	get whatsapp data
telegram	Get telegram data
imo	get imo data
viber	Get viber data
messenger	get facebook data
conion	Get conion data
signal	Get signal data
info	Upload file or update operation
callLogs	Get call history
contacts	get contacts
protectedText	steal text messages
liveInfos	Get real-time location
fileListing	get file list
smsLogs	Get SMS

3. Traceability and attribution

According to the signature information of the samples from the same family, we have associated a sample suspected to belong to the B ahamut organization. The C & C format of the suspected sample is very similar to that of the sample analyzed this time. Both use random combination strings of numbers and letters. There is a URL with the same path (/auth/login) that shows the same login page . And among the samples of the same family of the suspected sample, there are two samples whose download address is jamaat-ul-islam.com, and the download address was disclosed by Blackbarry in 2020 and belongs to the Bahamut organization. Therefore, we attribute the attack samples discovered this time to the Bahamut group.

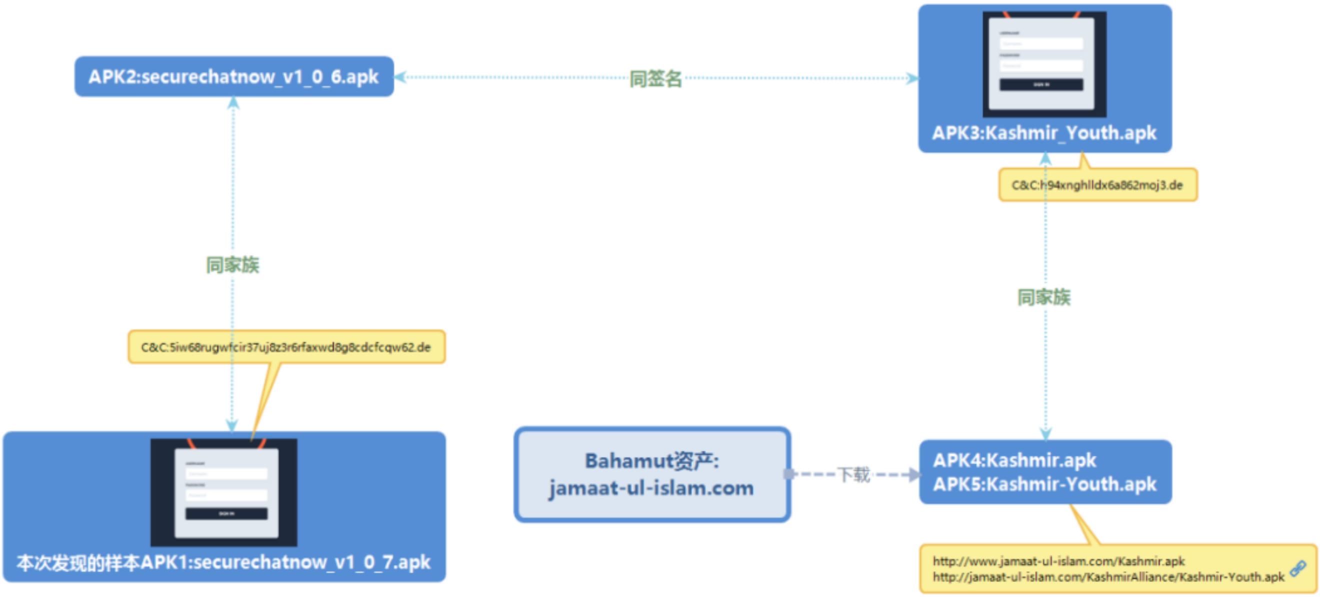

APK2:securechatnow_v1_0_6.apk
同签名
APK3:Kashmir_Youth.apk
C&C:h94xnghlldx6a862moj3.de
同家族
同家族
C&C:5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de
本次发现的样本APK1:securechatnow_v1_0_7.apk
Bahamut资产:
jamaat-ul-islam.com
下载
APK4:Kashmir.apk
APK5:Kashmir-Youth.apk
http://www.jamaat-ul-islam.com/Kashmir.apk
http://jamaat-ul-islam.com/KashmirAlliance/Kashmir-Youth.apk

Figure 6 Organizational Attribution

Figure 7 The assets of the Bahamut group disclosed by Blackbarry

4. Attack activity and victim analysis

By analyzing the creation time of the family sample and tracing the source of the sample, we found that the family sample first appeared in October 2020, and remained calm after a brief activity in February 2021, until it became active again in January this year , and is still active today. In the two active periods, different phishing websites were used for payload delivery.

Figure 8 Active timeline of samples from the same family

By querying the user infection status of the early samples of the same family, we found that the earliest infection time of the victim user was at the end of February 2021, which is consistent with the appearance time of phishing websites during the first active period. The geographical locations are mainly concentrated in Saudi Arabia and Pakistan. They are also consistent with the main target of the Bahamut group.

Summarize

The ability to independently develop chat software and remote control Trojans, with clear code structure and high quality, shows that Bahamut's developers have a high level of development. At the same time, the development of Trojanized chat software, the use of random strings as C &C , and frequent phishing also show that the organization has strong camouflage and attack skills. During our follow-up of the Bahamut attack, several other family samples belonging to the group appeared, which shows that the group should have concentrated attack activities in the near future. We will continue to monitor the group's attack dynamics.

Appendix 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

refer to

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/

360 Beacon Lab

360 FiberHome Lab is committed to in-depth research in the field of mobile security, such as mobile malware analysis, mobile gray and black product research, mobile threat warning, and mobile APT discovery and tracking. As the world's top mobile security ecological research laboratory, 360 FiberHome Lab not only published a number of mobile security ecological research results with international influence, but also successfully hunted many APT organizations such as Manlinghua and Paipaixiong. Attacks against important targets in my country and abroad. While providing core security data for company products such as 360 Mobile Guard, 360 Mobile Assistant, and 360 Guarantee, the laboratory also provides mobile application security testing services for scientific research institutions, mobile phone manufacturers, application stores and hundreds of domestic and foreign partners , all-round protection of mobile security.

Posted in topic #APT 56

Next · Waves Hidden in Peaceful Seas——Analysis on the Dynamics of APT-C-00 Sea L...

People who liked this content also liked

Quantum Attack System – Technical Analysis Report on High-end Cyber Attack Weapons of the National Security Agency "APT-C-40" Hacker Grou ...

360 Threat Intelligence Center

Waves Hidden in Peaceful Seas——Analysis on the Dynamics of APT-C-00 Sea Lotus Organization's Attack Activities

Snow abuse and gluttony: Analysis of suspected Lazarus attack activities against Korean companies

Qi Anxin Threat Intelligence Center