Dissecting a RAT. Analysis of the HawkShaw.

stratosphereips.org/blog/2021/5/6/dissecting-a-rat-analysis-of-the-hawkshaw

Kamila Babayeva May 10, 2021

This blog post was authored by Kamila Babayeva (@_kamifai_) and Sebastian Garcia (@eldracote).

The RAT analysis research is part of the Civilsphere Project (https://www.civilsphereproject.org/), which aims to protect the civil society at risk by understanding how the attacks work and how we can stop them. Check the webpage for more information.

This is the sixth blog of a series analyzing the network traffic of Android RATs from our Android Mischief Dataset [more information here], a dataset of network traffic from Android phones infected with Remote Access Trojans (RAT). In this blog post we provide the analysis of the network traffic of the RAT03-HawkShaw [download here]. The previous blogs analyzed Android Tester RAT, DroidJack RAT, SpyMax RAT, AndroRAT RAT and AhMyth RAT.

RAT Details and Execution Setup

The goal of each of our RAT experiments is to configure and execute the RAT software and to do every possible action while capturing all traffic and storing all logs. These RAT captures are functional and used as in real attacks.

The HawkShaw RAT is the only RAT in our Android Mischief dataset that has the controller and the builder hosted in the cloud. The controller is the main program that allows an attacker to control the targeted device. Usually, this main program comes with a graphical user interface to make the RAT main program more interactive. The builder is a program that builds the APK for a targeted device. The HawkShaw RAT service in the cloud is based on the Firebase platform. Firebase is a platform developed by Google for creating mobile and web applications. We executed the online service of the HawkShaw RAT on Ubuntu 20.04 Virtualbox virtual machine with Ubuntu 20.04 as a host. The Android Application Package (APK) built by the online RAT builder was installed in a real Nokia phone with Android version 10.

While performing different actions on the RAT controller (e.g. upload a file, get GPS location, monitor files), we captured the network traffic of the RAT controller on the Android virtual emulator. The network traffic of the phone was captured using Emergency VPN.

The details about the network traffic capture are:

- The controller IP address: 35.201.97.85 (provided by the creator of the RAT)
- The phone IP address: 10.8.0.249
- UTC time of the start of the infection in the capture: 2020-07-24 07:20:03 UTC

Analysis Problem

The HawkShaw RAT online service was created using the Firebase platform. It means that the malicious APK communicates with the RAT service using various Firebase suite products such as Firebase Authentication, Cloud Messaging, Cloud Storage, Realtime Database, Analytics, Installations, etc. The Firebase platform provides secure communication, so all the connections going from the victim's phone to the HawkShaw online service are encrypted. Considering that, our analysis is performed on the flow level, i.e. we analyze only the connections as flows going from the victim to the C&C (not packet by packet).

Infection and Initial Communication

Once the APK was installed in the phone, it tries to connect to the IP address 216.58.201.106 by using the server name *firebaseinstallations.googleapis.com* (Figure 1). This server name indicates a Firebase installation service (FIS) that provides a Firebase installation unique identifier and auth token for this malicious APK instance.

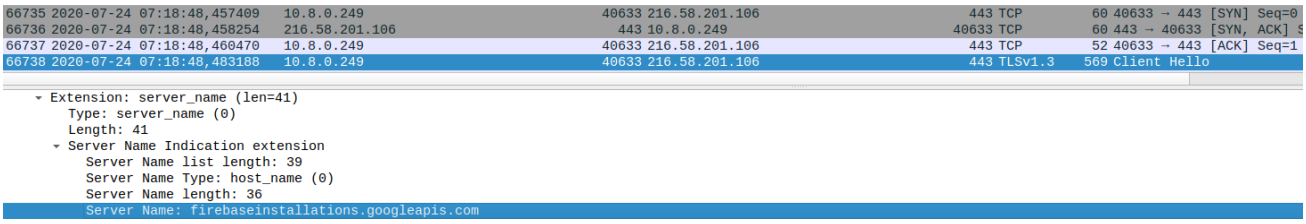

Figure 1. The victim phone starts by connecting to the IP 216.58.201.106 with the server name *firebaseinstallations.googleapis.com* that indicates a Firebase installation service (FIS).

With the retrieved auth token and the unique identifier, the phone established a connection to the online HawkShaw RAT service. The victim successfully connected to the Firebase platform (35.201.97.85) with the server name *hawkshaw-cae48.firebaseio.com* (Figure 2). Throughout the whole communication, the server name of *hawkshaw-cae48.firebaseio.com* is changed to *s-usc1c-nss-283.firebaseio.com* due to the Firebase policy of decreasing the load.

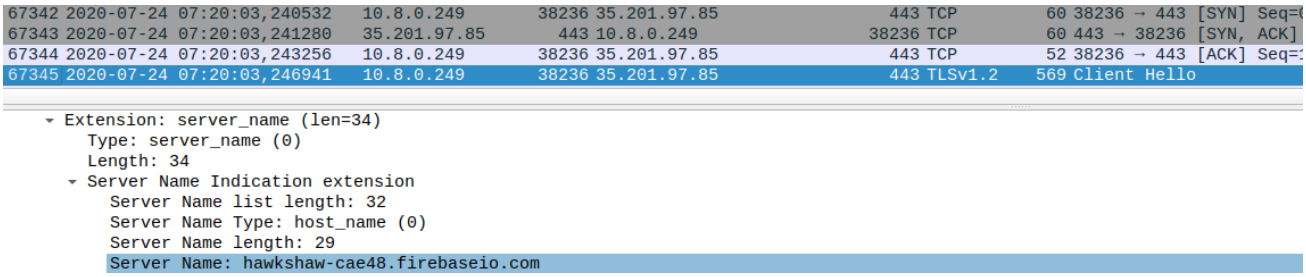

Figure 2. The victim connects to the Firebase platform (35.201.97.89) with the HawkShaw RAT service to the server name *hawkshaw-cae48.firebaseio.com*.

After the successful infection and connection to the C&C online service, the infected phone connects to two services: *api.ipify.org* and *api6.ipify.org* to retrieve the IPv4 and IPv6 addresses of the device. The connections to api.ipify.org and api6.ipify.org are invoked by the APK code shown in Figure 3. This part of the code belongs to a function called after receiving the C&C command 'Device Information'. It might mean that the controller automatically calls the command 'Device Information' that aims to retrieve details about the targeted device hardware, software, settings, etc. Figure 4 shows the screenshot from the C&C interface with all the data retrieved from the phone from the command 'Device Information'.

```
try {
    hashMap.put("/ip/ipv4address", new String(C3609d.m7582a(new URL("https://api.ipify.org")), C3682a.f8825a));
    hashMap.put("/ip/ipv6address", new String(C3609d.m7582a(new URL("https://api6.ipify.org")), C3682a.f8825a));
    StringBuilder sb = new StringBuilder();
    sb.append("http://ip-api.com/json/");
    Object obj = hashMap.get("/ip/ipv6address");
    if (obj == null) {
        obj = hashMap.get("/ip/ipv4address");
    }
    sb.append(obj);
    sb.append("?fields=9168895");
    hashMap.put("/ip/ipv4location", new String(C3609d.m7582a(new URL(sb.toString())), C3682a.f8825a));
} catch (Exception e2) {
    C3887c.m7915a("<font color='orange'>Device Info IP location error, " + e2 + "</font>", (Long) null, 2);
}
```

Figure 3. Code from the RAT in the infected device that takes care of connecting to the services *api.ipify.org* and *api6.ipify.org* to retrieve the IPv4 and IPv6 IP addresses. This function gets executed after the C&C command sends the command 'Device Information'.

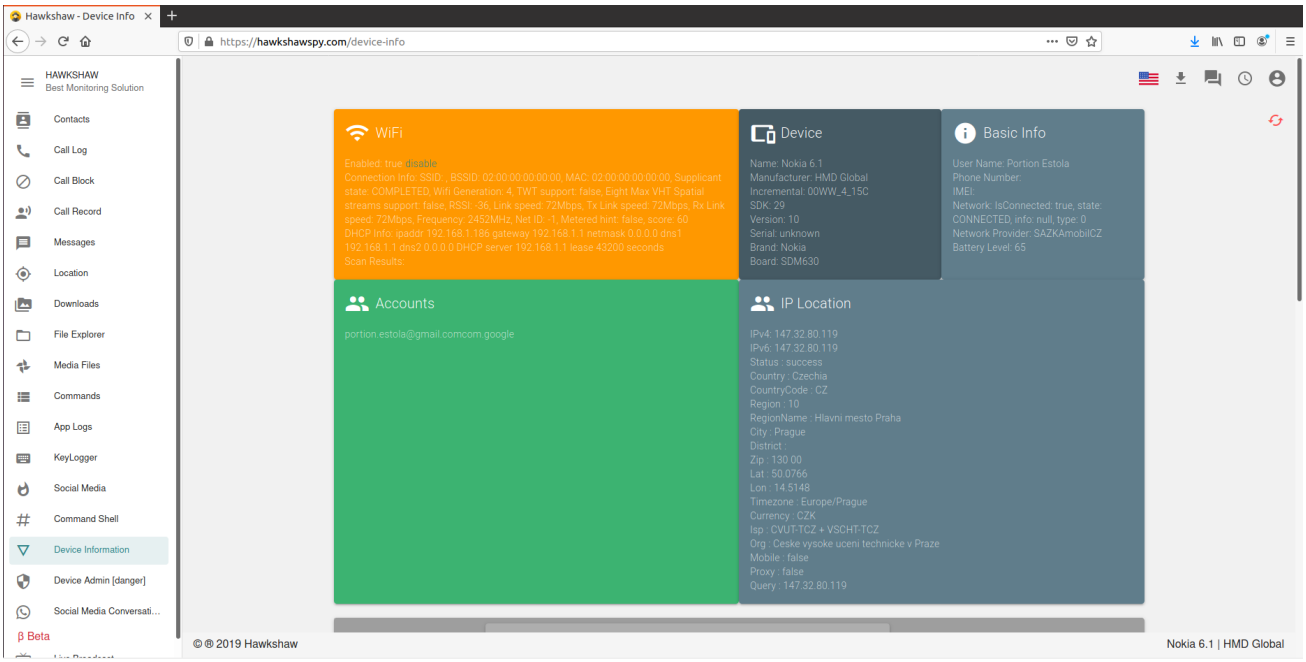

Figure 4. The C&C interface after the controller sends the command 'Device Information' to the victim, that aims to retrieve the details of the victim's device.

Simultaneously with the connections to api.ipify.org and api6.ipify.org, the phone connects to the IP address 216.58.201.74 with the server name *firebasestorage.googleapis.com* (Figure 5). This server name indicates Firebase Storage to store the data. The phone sends all retrieved data from the C&C command 'Device Information' to store in the Firebase storage.

```
67584 2020-07-24 07:20:26,552886   10.8.0.249      44562 216.58.201.74    443 TCP      60 44562 → 443 [SYN] Seq=0
67585 2020-07-24 07:20:26,553618   216.58.201.74     443 10.8.0.249       44562 TCP    60 443 → 44562 [SYN, ACK]
67586 2020-07-24 07:20:26,555512   10.8.0.249      44562 216.58.201.74    443 TCP      52 44562 → 443 [ACK] Seq=1
67587 2020-07-24 07:20:26,558756   10.8.0.249      44562 216.58.201.74    443 TLSv1.3  569 Client Hello
```

```
▾ Extension: server_name (len=35)
    Type: server_name (0)
    Length: 35
  ▾ Server Name Indication extension
      Server Name list length: 33
      Server Name Type: host_name (0)
      Server Name length: 30
      Server Name: firebasestorage.googleapis.com
```

Figure 5. The victim connects to the IP 216.58.201.74 with the server name *firebasestorage.googleapis.com* that indicates Firebase Storage.

Example of C&C Commands

Compared to other RATs in the Android Mischief Dataset, Hawkshaw RAT is the most sophisticated in its functionality. Like other RATs, HawkShaw was able to control victim's calls, SMS, camera, location, system files, and device's settings, but also it was able to interfere social media conversations (Figure 6), and its keylogger worked perfectly (Figure 7).

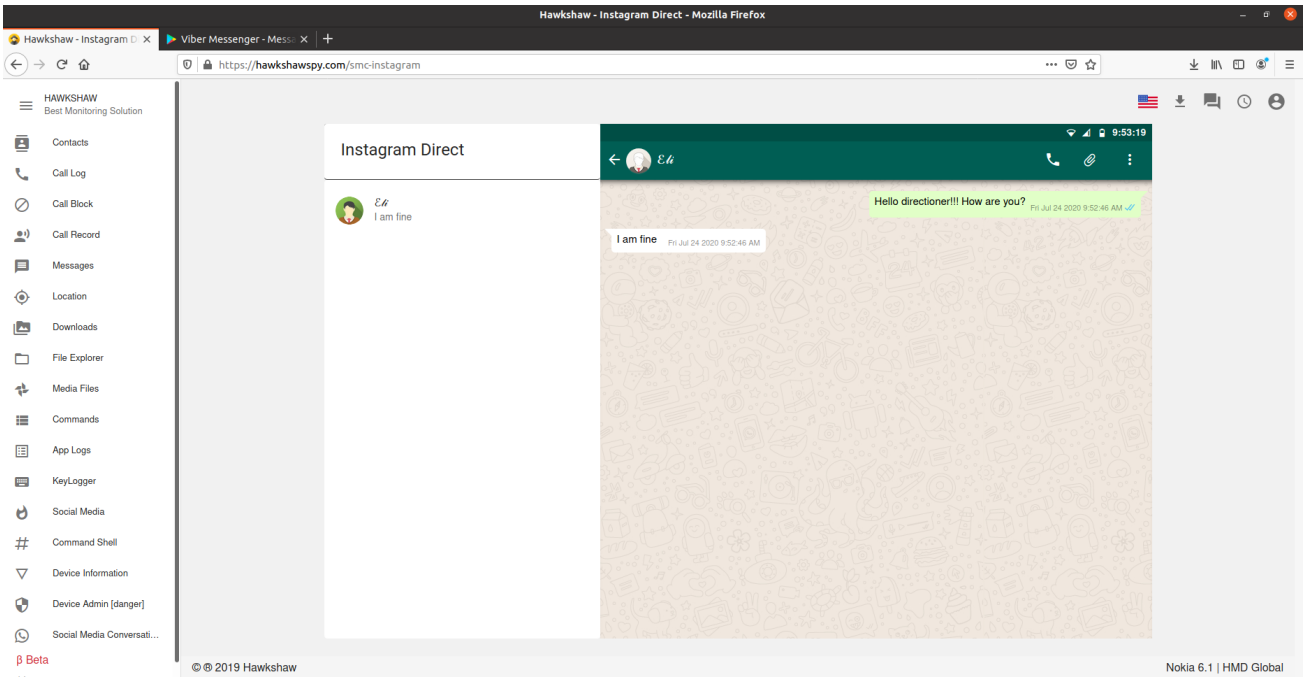

Figure 6. HawkShaw controller interferes Instagram conversation of the victim's device. The C&C can send and receive messages in the chat.

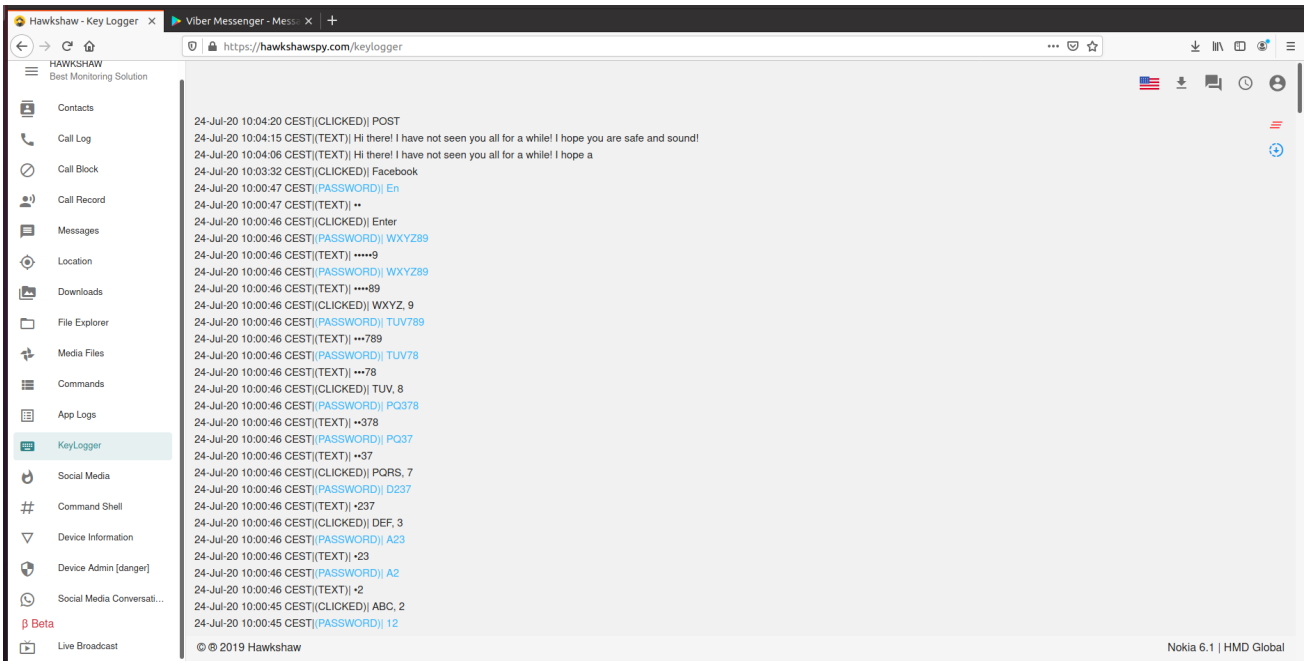

Figure 7. Keylogger C&C command. The C&C captures all the keys clicked on a compromised device.

Complete communication between the C&C and victim phone

Through the whole infection, 17 malicious connections to the Firebase platform were performed: 10 connections to Firebase App, 3 connections to Firebase Cloud Storage, 2 connections to Firebase installation service, and 2 connections to api.ipify.org and api6.ipify.org. Due to the poor quality of code, the connections between the victim's phone and the C&C were interrupted often and had very short duration of the connections (Figure

8). The phone was connected to the Firebase storage in order to send large files such as video, photos, documents, and audio. The connections to the Firebase Installation service might be explained with the initializing or updating instance ID and auth token.

Address A	Port A	Address B	Duration
10.8.0.249	38236	35.201.97.85	274.7860
10.8.0.249	38264	35.201.97.85	172.6580
10.8.0.249	38364	35.201.97.85	69.3758
10.8.0.249	38406	35.201.97.85	785.3423
10.8.0.249	38518	35.201.97.85	163.4944
10.8.0.249	38532	35.201.97.85	578.5400
10.8.0.249	38610	35.201.97.85	61.6597
10.8.0.249	38614	35.201.97.85	107.6462
10.8.0.249	38642	35.201.97.85	63.4585
10.8.0.249	38646	35.201.97.85	60.4909

Figure 8. The duration of the connections between the victims and the HawkShaw online service is short, no more than approx. 13 minutes (785 seconds).

After a careful analysis of each malicious connection, we found no heartbeat performed in any of them. Even though there were 10 connections established between the HawkShaw C&C service and the victim, there were no simultaneous connections performed between the C&C and the victim.

Conclusion

In this blog we have analyzed the network traffic from a phone infected with the HawkShaw RAT that uses Firebase platform to operate and control devices. All the retrieved data from the devices is stored in the Firebase database to which the creator of the HawkShaw RAT probably has access. We were not able to decode its connection due to Firebase secure connection. The HawkShaw RAT seems to be complex in its communication protocol, and it is sophisticated in its work.

To summarize, the details found in the network traffic of this RAT are:

- The RAT is hosted on the cloud with the use of Firebase platform.
- Firebase provides an encrypted connection between the HawkShaw online service and the victim.
- The targeted device connects to api.ipify.org and api6.ipify.org to retrieve and send its IPv4 and IPv6 addresses.
- There is no heartbeat in the communication between the C&C and the phone.
- There are no simultaneous connections established to the C&C.
- There are a lot of connections to the Firebase platform, but of a very small size.

Biographies


KAMILA BABAYEVA

Sebastian Garcia is a malware researcher and security teacher with experience in applied machine learning on network traffic. He founded the Stratosphere Lab, aiming to do impactful security research to help others using machine learning. He believes that free software and machine learning tools can help better protect users from abuse of our digital rights. He researches on machine learning for security, honeypots, malware traffic detection, social networks security detection, distributed scanning (dnmap), keystroke dynamics, fake news, Bluetooth analysis, privacy protection, intruder detection, and microphone detection with SDR (Salamandra). He co-founded the MatesLab hackspace in Argentina and co-founded the Independent Fund for Women in Tech. @eldracote. https://www.researchgate.net/profile/Sebastian_Garcia6

Kamila Babayeva is a 20 years old and third-year bachelor student in the Computer Science and Electrical Engineering program at the Czech Technical University in Prague. She is a researcher in the Civilsphere project, a project dedicated to protecting civil organizations and individuals from targeted attacks. Her research focuses on helping people and protecting their digital rights by developing free software based on machine learning. Initially, she worked as a junior Malware Reverser. Currently, Kamila leads the development of the Stratosphere Linux Intrusion Prevent System (Slips), which is used to protect the civil society in the Civilsphere lab.

SEBASTIAN GARCIA