First-of-its-kind spyware sneaks into Google Play

welivesecurity.com/2019/08/22/first-spyware-android-ahmyth-google-play/

August 22, 2019

ESET analysis breaks down the first known spyware that is built on the AhMyth open-source espionage tool and has appeared on Google Play – twice

Lukas Stefanko
22 Aug 2019 - 11:30AM

ESET analysis breaks down the first known spyware that is built on the AhMyth open-source espionage tool and has appeared on Google Play – twice

ESET researchers have discovered the first known spyware that is built on the foundations of AhMyth open-source malware and has circumvented Google's app-vetting process. The malicious app, called Radio Balouch aka RB Music, is actually a fully working streaming radio app for Balouchi music enthusiasts, except that it comes with a major sting in its tail – stealing personal data of its users. The app snuck into the official Android app store twice, but was swiftly removed by Google both times after we alerted the company to it.

AhMyth, the open-source Remote Access Tool from which the Radio Balouch app borrowed its malicious functionality, was made publicly available in late 2017. Since then, we have witnessed various malicious apps based on it; however, the Radio Balouch app is the very first of them to appear on the official Android app store.

ESET's mobile security solution has been protecting users from AhMyth and its derivatives since January 2017 – even before AhMyth went public. As the malicious functionality in AhMyth is not hidden, protected or obfuscated, it is trivial to identify the Radio Balouch app – and other derivatives – as malicious, and classify them as belonging to the AhMyth family.

Besides Google Play, the malware, detected by ESET as Android/Spy.Agent.AOX, has been available on alternative app stores. Additionally, it has been promoted on a dedicated website, via Instagram, and YouTube. We have reported the malicious nature of the campaign to the respective service providers, but received no response.

Radio Balouch is a fully working streaming radio app for music specific to the Balouchi region (for the sake of consistency, we follow the spelling used in the campaign; the most common transcriptions are "Balochi" or "Baluchi"). In the background, however, the app spies on its victims.

On Google Play, we discovered different versions of the malicious Radio Balouch app twice and in each case, the app had 100+ installs. We reported the first appearance of this app on the official Android store to the Google security team on July 2nd, 2019, and it was removed within 24 hours.

The malicious Radio Balouch app reappeared on Google Play on July 13th, 2019. This one, too, was immediately reported by ESET and swiftly removed by Google.

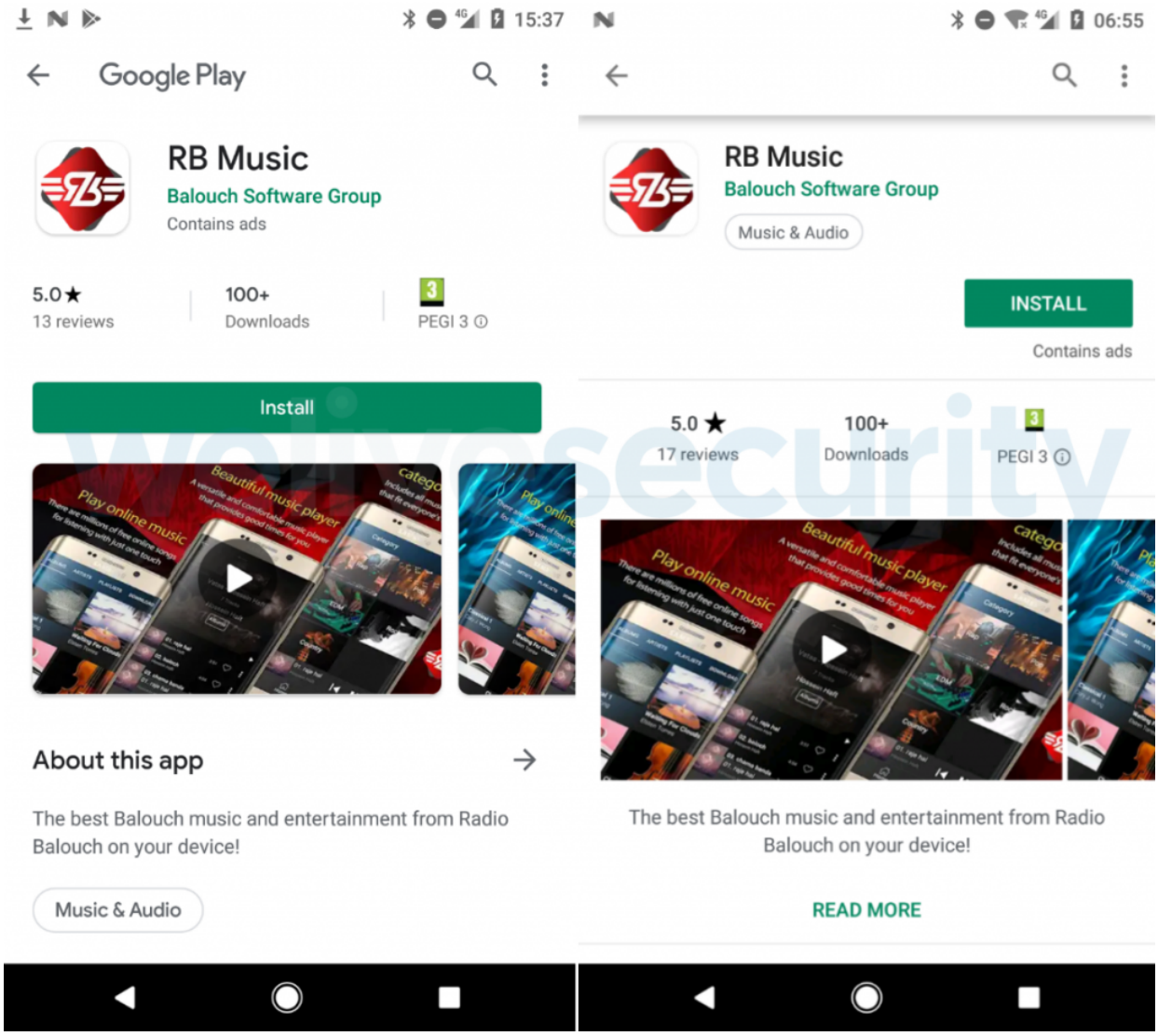

Figure 1. The malicious Radio Balouch app appeared twice on Google Play

After being removed from Google Play, the malicious radio app is only available on third-party app stores at the time of writing. It has also been distributed from a dedicated website, radiobalouch[.]com, via a link promoted via a related Instagram account. This server was also used for the spyware's C&C communications (see below). The domain was registered on March 30th, 2019, and shortly after our complaint, the website was down and still is at the time of writing.

The attackers' Instagram account still, at the time of writing, serves a link to the app that has been removed from Google Play. They have also set up a YouTube channel with one video introducing the app; apparently, they don't promote it as the video has a mere 21 views at the time of writing.

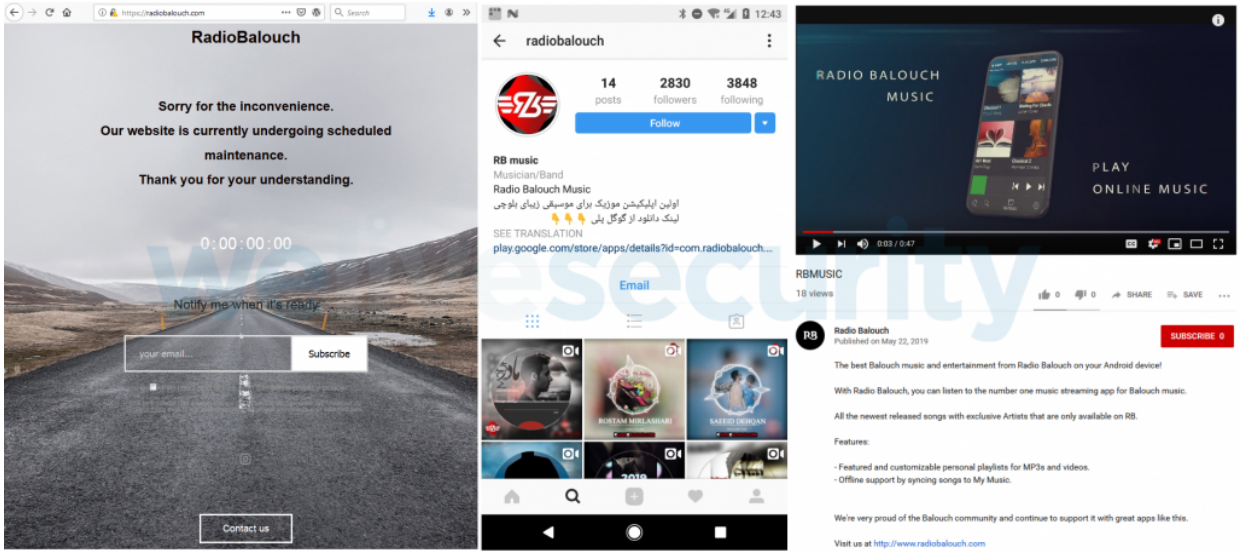

Figure 2. The Radio Balouch website (left), Instagram account (center) and promotional YouTube video (right)

Functionality

The malicious Radio Balouch app works on Android 4.2 and above. Its internet radio functionality is bundled with the functionality of AhMyth into one malicious app.

After installation, the internet radio component is fully functional, playing a stream of Balouchi music. However, the added malicious functionality enables the app to steal contacts, harvest files stored on the device and send SMS messages from the affected device.

Functionality for stealing SMS messages stored on the device is also present. However, this functionality can't be utilized since Google's recent restrictions only allow the default SMS app to access those messages.

As AhMyth has more variants whose functionalities vary, the Radio Balouch app and any other malware based on this open-source espionage tool might get further functions in the future via an update.

After launch, users choose their preferred language (English or Farsi); in the next step, the app starts requesting permissions. First, it requests access to files on the device, which is a legitimate permission for a radio app to enable its functionality; if declined, the radio would not work.

Then, the app requests the permission to access contacts. Here, to camouflage its request for this permission, it suggests this functionality is necessary should the user decide to share the app with friends in their contact list. If the user declines to grant the contact permissions, the app will work regardless.

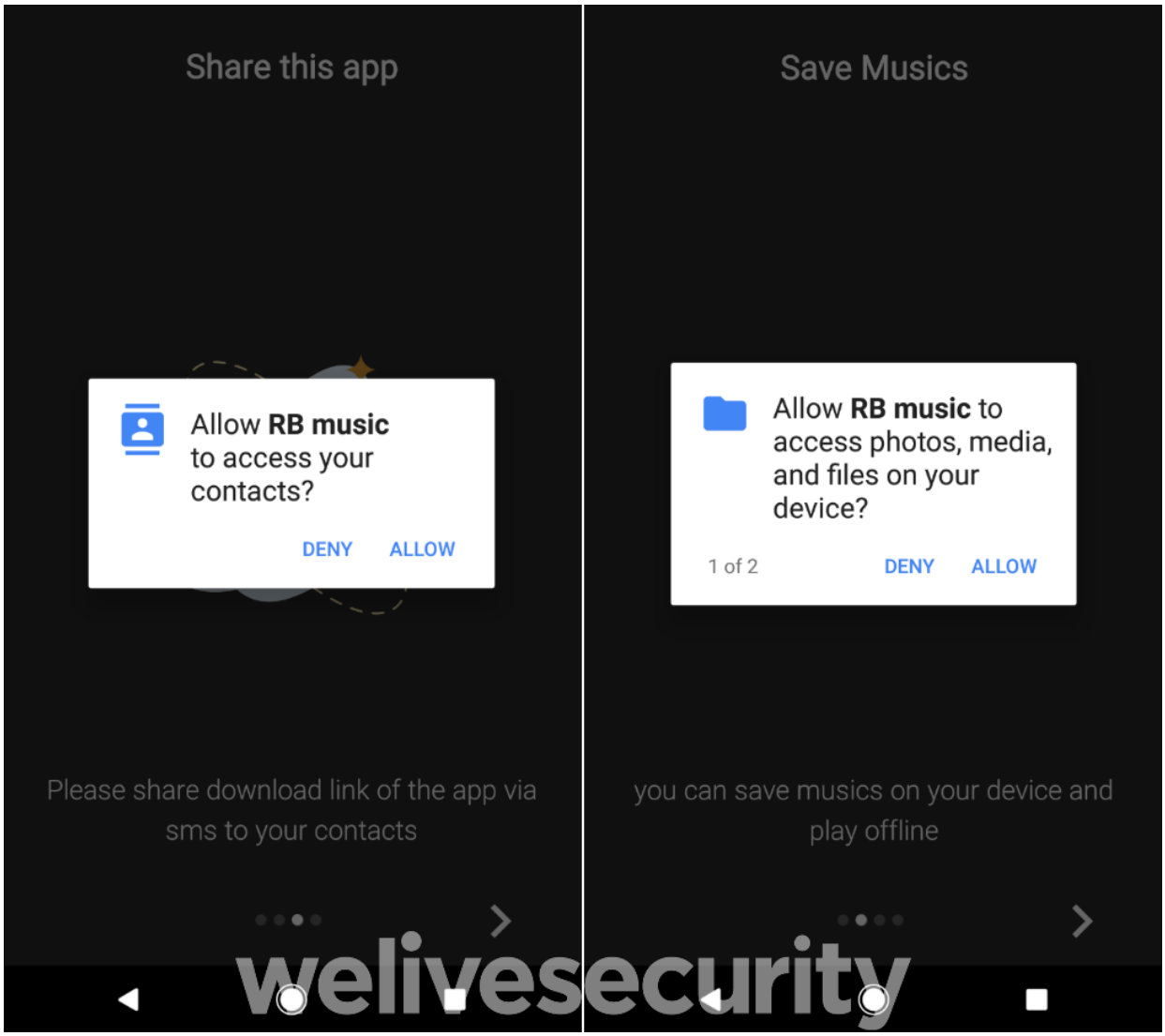

Figure 3. Radio Balouch app's permissions requests

After the setup, the app opens its home screen with music options, and offers the option to register and login. However, any "registering" is meaningless as any input will bring the user into the "logined" state, in the operators' poor English. Probably, this step has been added to lure credentials from the victims and try to break into other services using the obtained passwords – a reminder to never reuse passwords across services. On a side note: the credentials are transmitted unencrypted, over an HTTP connection.

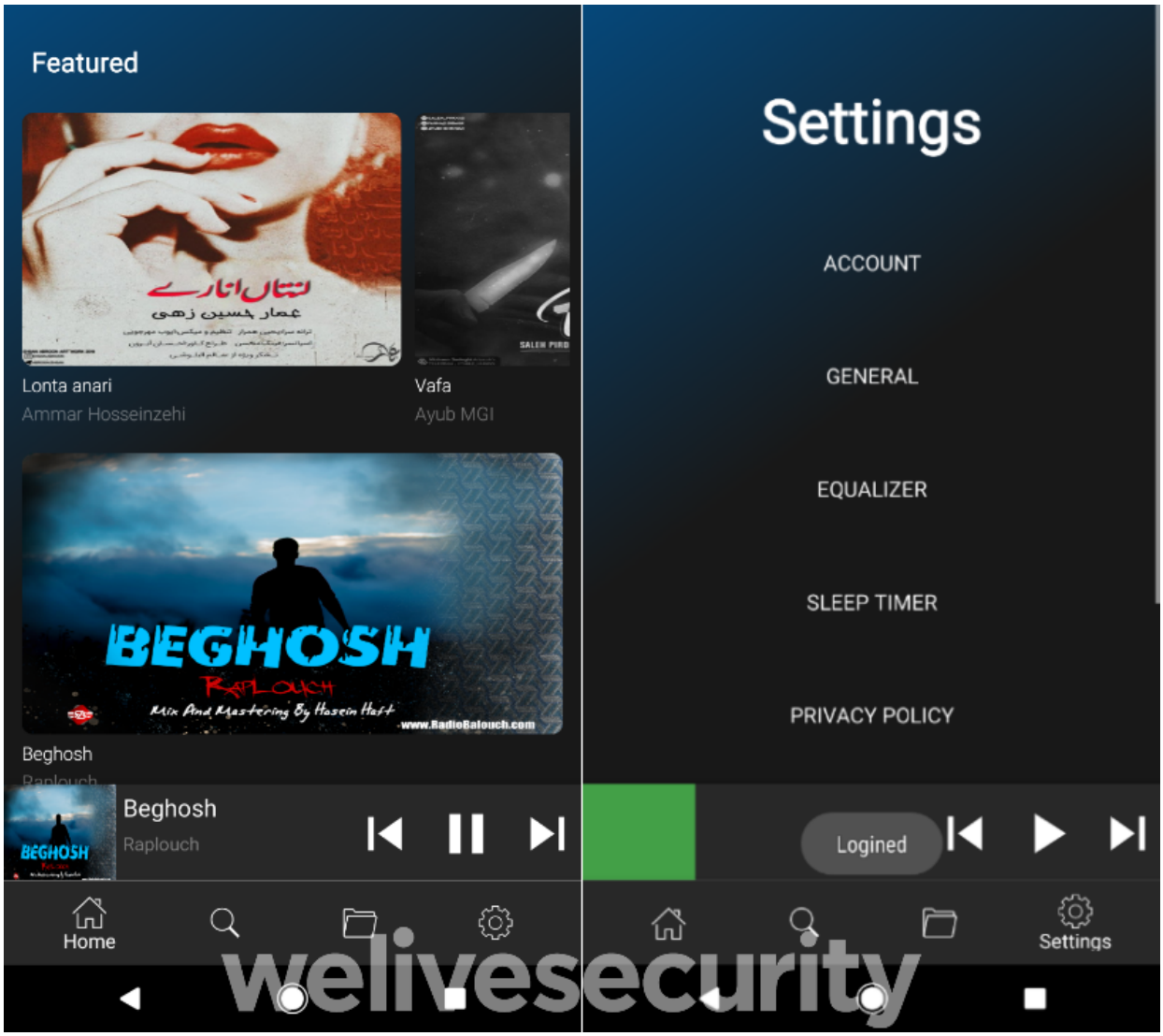

Figure 4. Radio Balouch app's Home (left) and Settings (right) screens

For C&C communication, Radio Balouch relies on its (now defunct) radiobalouch[.]com domain. This is where it would send information it has gathered about its victims – notably information about the compromised devices, and the victims' contacts lists. As with the account credentials, the C&C traffic is transmitted unencrypted over an HTTP connection.

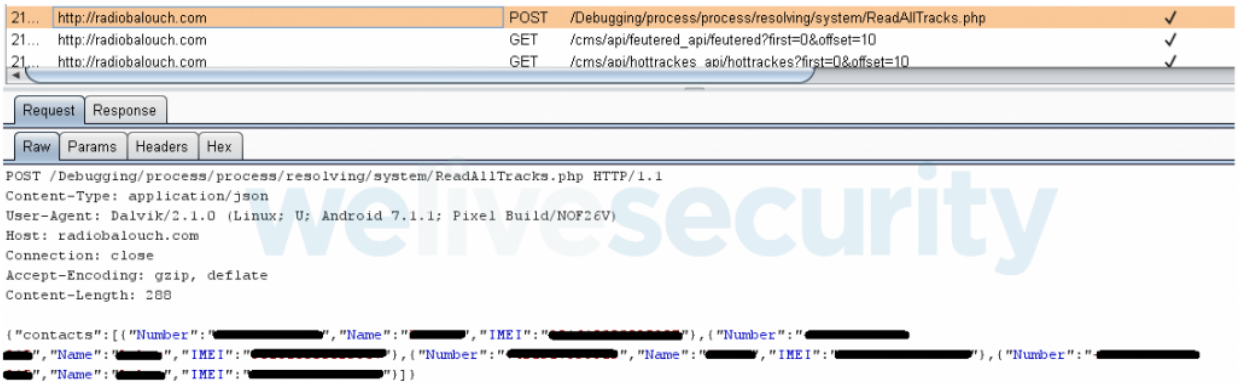

Figure 5. Radio Balouch's communication with its C&C server

Conclusion

The (repeated) appearance of the Radio Balouch malware on the Google Play store should serve as a wake-up call to both the Google security team and Android users. Unless Google improves its safeguarding capabilities, a new clone of Radio Balouch or any other derivative of AhMyth may appear on Google Play.

While the key security imperative “Stick with official sources of apps” still holds, it alone can’t guarantee security. It is highly recommended that users scrutinize every app they intend to install on their devices and use a reputable mobile security solution.

Indicators of Compromise (IoCs)

Hash	ESET detection name
F2000B5E26E878318E2A3E5DB2CE834B2F191D56	Android/Spy.Agent.AOX
AA5C1B67625EABF4BD839563BF235206FAE453EF	Android/Spy.Agent.AOX

22 Aug 2019 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion