Background

Sarahah is a messaging application launched in November 2016 by Saudi developer Zain al-Abidin Tawfiq. The word "Sarahah" is the pronunciation of the Arabic word for "honesty." It was originally launched as a service for businesses in Arabic-speaking regions to solicit anonymous, candid feedback from their employees and co-workers. However, it quickly went viral in Saudi Arabia and Egypt as an anonymous messaging application.[2]

Building on its regional success, Sarahah rapidly gained traction in North America, Europe, and Australia. A recent update integrated its functionality and network into Snapchat, one of the most popular social media apps in the world. This prompted an explosive growth in popularity, with over 14 million registered users and 20 million unique daily visitors (it is possible to leave messages in Sarahah without creating an account). [3]

What is Sarahah?

Sarahah provides a free network to leave anonymous messages through a public profile that a user shares with other people. Anyone with a user's profile name can anonymously message that user, without necessarily creating an account.

Sarahah can be used via web browser or by installing an app on an iOS or Android device. New accounts can be created only via the mobile app. Registration is required in order to receive messages. New users register with an email address, username, password, first and last name, and "handle" or profile name. The username is used to log in to the service, but only the profile name is displayed to other users. The personal link to receive anonymous messages automatically becomes www.PROFILE_NAME.Sarahah.com, and cannot be changed. Messages can be sent by anyone using this link, or registered users can search for other people by first and last name or profile name.

Sarahah is not a social network. It does not allow for any kind of two-way communication, dialogue, or friend system. A user essentially invites anyone to send them an anonymous message when they post their link, with no way of replying or knowing who sent it. Even if the

user shares his profile with a limited number of close friends, there is no way of ensuring that the link isn't shared with other malicious users. Many have drawn parallels to similar apps (like Ask.FM, Secret, Whisper, and the now-defunct Yik Yak) with rampant cyberbullying problems. [4]

Figure 1 is a screenshot of Sarahah version 2.0 running on a Samsung Galaxy S6 smartphone.

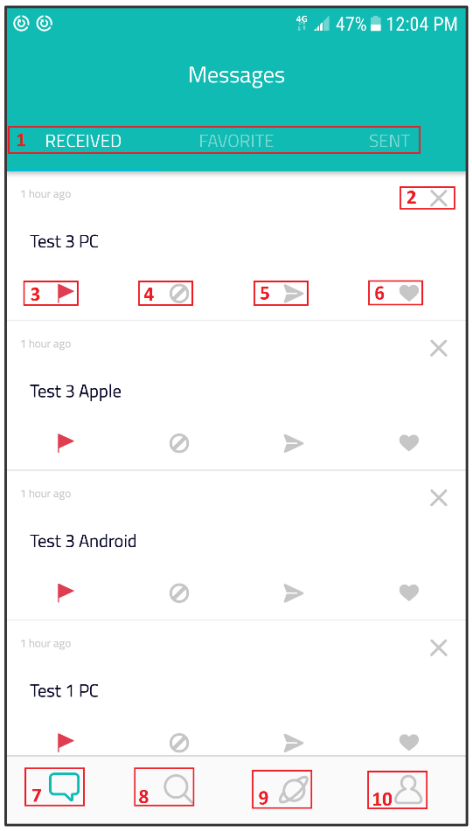

Figure 1

1: This navigation bar on the home screen allows users to navigate among messages they have received from others, messages they have "favorited" and saved, and messages they have sent.

2: This button allows a user to permanently delete a message. There is a second dialog box popup for confirmation.

3: This button allows a user to report a message for breaking Sarahah's terms of service. During testing, a fake "bullying" message containing many keywords was sent between two devices and reported. After several weeks, no action was taken. It is not clear how, if at all, Sarahah is responding to these reports.

4: This button allows a user to permanently block the source of a message. There is a second dialog popup for confirmation.

Testing revealed the following:

- **Blocking a registered user.** Blocks all messages from that user's device (if they are logged on) and blocks messages from that account if logged on elsewhere.
- **Blocking messages coming from a desktop computer (not from a logged-on user).** Blocks all messages from that computer.

The blocked user has no indication that they are blocked.

5: This button allows users to share the message to a variety of other social media applications, including Facebook, Snapchat, and Instagram. It also allows users to export the message in a formatted image that is saved locally on the device.

6: This button allows a user to "favorite" a message, permanently storing it and indexing it under the Favorite tab in the navigation bar.

7: This button shows the main screen of the Sarahah application, the Messages tab.

8: This button allows a user to search for other registered users by first and last name or by profile name.

9: This button currently has no function, but is planned to be a "Discovery" tab, allowing a user to automatically find and message other users in their phone's contacts or proximity.

10: This button is the profile, where a user can access their settings and manage their account.

Importance to Law Enforcement

Sarahah, is similar to other anonymous messaging apps, many of which have a track record of enabling bullying. While there is no federal law pertaining to bullying, all 50 states have individual laws and regulations that can be found here.[5] The easily accessible nature of the application, the anonymity, and the school-aged demographic making up the vast majority of the user base combines to create an almost perfect medium for bullying and harassment.

Investigative Information

Information obtained via Sarahah.com/home/About[6]and Sarahah.com/home/Privacy[7]

Sarahah has no publicly listed address. The founder and CEO's personal Twitter lists several jobs available, based in "Sarahah in Khobar, Kingdom of Saudi Arabia." This physical location and absence of any presence in other countries or jurisdictions will make serving any legal process difficult.

The terms of service[8] and privacy policy[9]are minimal. Most of the English-language version of Sarahah's website appears to have been translated from another language (presumably Arabic), and contains spelling and grammatical errors as well as incomplete sentences.

The privacy policy states that IP addresses, date, and time are recorded any time the service is used. The privacy policy also states "Sarahah will comply with any lawful or legal requirement." It is unclear if this extends to jurisdictions outside of the Saudi Arabia.

Information Retrieved from an iOS Device

The National White Collar Crime Center (NW3C) Cybercrime Section downloaded, installed, and used the Sarahah application version 2.0 on an Apple iPod Touch, 5th Generation model A1509 running iOS version 9.3.5. The test machine was a Dell Latitude E6500 running Windows 8.1 Enterprise. A logical extraction of the device was completed using Micro Systemation's XRY version 7.4.1. A manual search of the results and keyword search for the word "Sarahah" located potentially useful artifacts during the examination. The files and folders of interest were exported and viewed manually with database and property list viewers.

- com.sarahah.plist, with the path of /private/var/mobile/Containers/Data/Application/com.sarahah/Library/Preferences, has several identifying values.
    - <key>email</key> stores the registered email used to create the Sarahah account.
    - <key>name</key> stores the user's registered name used to create the Sarahah account.
    - <key>subdomain</key> stores the user's "handle" or screenname, which can be combined with the URL www.Sarahah.com to access the user's profile and message box.
    - <key>photoURL</key> stores a URL that links to the user's profile picture. This value will exist but be empty if no photo was uploaded.

Information Retrieved from an Android Device

The National White Collar Crime Center (NW3C) Cybercrime Section downloaded, installed, and used the Sarahah application version 1.7 on a Samsung Galaxy S3, model SCH-i535, running Android version 4.1. The test machine was a Dell Latitude E6500 running Windows 8.1 Enterprise. A logical extraction of the device was completed using Micro Systemation's XRY version 7.4.1. A manual search of the results and keyword search for the word "Sarahah" located potentially useful artifacts during the examination. The files and folders of interest were exported and viewed manually with database and property list viewers.

- com.sarahah.xml, with the path of /userdata/data/com.sarahah/preferences stores a table with identical values of those retrieved from the iOS application.
    - <key>email</key> stores the registered email used to create the Sarahah account.
    - <key>name</key> stores the user's registered name used to create the Sarahah account.
    - <key>subdomain</key> stores the user's "handle" or screenname, which can be combined with the URL www.Sarahah.com to access the user's profile and message box.
    - <key>photoURL</key> stores a URL that links to the user's profile picture. This value will exist but be empty if no photo was uploaded.

Feedback

For additional information or suggestions please contact cyberalerts@nw3c.org.

Sources

1 http://mashable.com/2017/07/23/the-story-of-sarahah-app/#d9LN9LV7Luq2

2 http://www.businessinsider.com/sarahah-app-store-bullying-harassment-2017-7

3 http://mashable.com/2017/07/23/the-story-of-sarahah-app/#d9LN9LV7Luq2

4 http://money.cnn.com/2017/08/23/technology/culture/sarahah-anonymous-apps/index.html

5 https://www.stopbullying.gov/laws/index.html

6 https://sarahah.com/home/About

7 https://Sarahah.com/home/Privacy

8 https://Sarahah.com/Home/Terms

9 https://Sarahah.com/home/Privacy

This project was supported by Grant No. 2015-BE-BX-0011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Photo Credits: "179774230 Copyright darrenmbaker. 2017 Used under license from Bigstockphoto.com"