Background

Surespot is an open source instant messaging application for both Android and iOS devices. This secure communication platform uses end-to-end encryption on all messages including text, images, and voice. With over a half a million users around the globe and over 100 million secure messages sent, surespot has become a popular means of communication.[i] The surespot application was developed by Adam Patacchiola and the business is located in Boulder, CO. The application was originally released for Android devices through Google Play in 2013 and became available for iOS through the Apple App Store in February 2014.

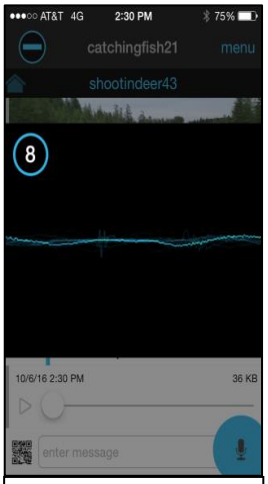
What is the Surespot App?

According to the application's law enforcement guidelines, surespot "operates in an environment of total transparency and exists to protect each person's due right to privacy.[ii] Information sent through surespot is encrypted using AES 256bit GCM and can be read only by the intended recipient. surespot collects no personal information from users at the time of download, and accounts are not associated to an email address or phone number. Users are required only to type in a unique username and password to get started. [iii]

Surespot users can invite friends by sending an invitation link through email, text, or social media. The invitation directs the recipient to install surespot on a device, allowing for communication between the two parties. Currently no group chat option is available.

One popular aspect of surespot is that messages can be controlled by the sender even after they are received. When the sender deletes messages from their device, the messages are also deleted from the recipient's device and the surespot server. The surespot server stores up to 1,000 messages per user, after which they are automatically deleted from the oldest to the newest.

***Additional features*:**



Can record up to 10 secods of voice content

Voice Messages: Through an in-app purchase, users can upgrade to get the voice message feature for $1.99. This feature allows users to hold down the microphone button and record a message up to ten seconds in length and then send it to the intended party**.** If purchased, law enforcement could potentially gain an investigative lead by tying the username to an iTunes or Google Play account.

Pictures: Surespot users can send pictures by choosing from their gallery. The images are locked by default and cannot be saved to the receiver's gallery until the sender unlocks them. However, a user can still screen shot an image and no notification is sent to the sender.

Importance to Law Enforcement

Surespot's end-to-end encryption has made it challenging for law enforcement to obtain the information needed for potential investigations. Communication through surespot has been linked to multiple national security investigations, to include Junead Khan[iv], an alleged ISIS operative plotting to kill a U.S. Airman in England. While obtaining actual content of the messages from surespot may not be possible, there are other digital artifacts that could potentially assist within an investigation.

Investigative Information

Information obtained from Surespot

Surespot is located at 2995 55th Street, #18034 Boulder CO, 80308. Legal process can be served through email at legal@surespot.me. Requests made must include:

- Law enforcement letterhead
- A valid official return email address and point of contact
- Search warrant, subpoena or other valid court order for information
- Username for account being investigated
- Date of request
- Account information being sought

Because surespot does not capture users' personal contact information such as email addresses or phone numbers, surespot claims not to have the ability to notify users if legal process is received.

According to surespot's law enforcement guidelines the following data is available

- Usernames.
- Friend relationships (who is friends with who, blocked who, ignored who, deleted who).
- Conversation relationships (how many friends currently you have a "conversation" with - meaning have a sent or received a message with).
- Messages in the amount of MAX_MESSAGES_PER_USER (currently 1000) which each have a server timestamp, to username, from username, and encrypted content, or link to encrypted content (image or file).
- Total messages sent per user.
- Total images sent per user.
- Signing (DSA) public keys and versions.
- Encryption (DH) public keys and versions.
- Encrypted "friend images" or avatars and friend aliases that are assigned to certain usernames. These are encrypted with a key generated from ECDH key derivation of assigning identity's private/public keypair.
- Google GCM id (used for push messaging) which is related to the username in the surespot database.
- Apple APN token (used for push messaging) which is related to the username in the surespot database.
- If voice messaging is purchased, a purchase token given to us by Google or Apple which is related to the username in the surespot database.
- Server logs may contain any of the above information and are in a 20 log - 5MB per log rotation.

Information Retrieved from an iOS Device

The National White Collar Crime Center (NW3C) Cybercrime Section downloaded, installed, and used the surespot application version 12 on an Apple iPhone 6 model MG4X2LL/A running iOS version 10.0.2. The test machine was an Apple MacBook running MacOS Sierra. A logical extraction of the device was completed using Katana Forensics Lantern. The only artifact recovered during the logical extraction was the private/var/mobile/media folder, which contained pictures and videos from the camera roll, as well as voice memos. Examining the "Files" button located no files relating to apps or their usage.

In a second test on a machine running Windows 7 Ultimate Service Pack 1 – 64 bit and MSABs XRY, the installed app was designated as com.twofours.surespot in the "installed apps" section and the name (surespot). The package name (com.twofours.surespot), version, permission

(Locations – Disabled), and path (/private/var/mobile/containers/data/application/28AF29DF-8114-4C62-8AFF-7641EABA148A) were also identified. Looking into the device event logs, every time the app was logged into an entry was generated showing the "Apple Network Usage" which gave the date and time of log in, as well as the TraffficIn (cellular) and TrafficOut (cellular) usage.

There were also other files in the Cookies, Documents, and Unrecognized views.

Under Apple Cookies was a file with the "value" of s% 3ajHc7voFHuokZuDRU10QBaTYa.1PlfUiVyQajds15Hgw46A0ev0HiMcfP4Uqnn0Y5xwv, the domain of server.surespot.me, as well as created and expiration times and the name of connect.sid.

Under Documents were two files called com.twofours.surespot.plist with the path of /private/var/mobile/Containers/Data/Application/com.twofours.suresport/Library/preferences and com.twofours.surespot.pushstore with the path of /private/var/mobile/Library/SpringBoard/Pushstore.

Inspecting the com.twofours.surespot.plist file showed the last_user logged in, whether they clicked the Terms of Service, the version and build number of the program. The other file did not appear to have anything relevant to the chats.

Under Unrecognized were two files called catchingfish21.ssi (username.ssi) with the path of /private/var/mobile/Containers/Data/Application/com.twofours.surespot/Documents and cookies.binary.cookies with a path of /private/var/mobile/Containers/Data/Application/com.twofours.surespot/Library/Cookies. After inspecting each file with a hex editor they appeared to have a binary plist header, but opening with XCode did not reveal any relevant information pertaining to chats.

Examining the rest of the data extracted show no signs of pictures, graphics, avatars, posting, users, etc. linking back to the program or the logged in user.

Information Retrieved from an Android Device

The NW3C Cybercrime Section downloaded, installed, and used the surespot application version 65 on a Samsung Galaxy S7 model SM-G930O running Android version 6.0 Marshmallow. The first test machine was running Windows 8.1 Enterprise and Oxygen Forensic Detective 8.5.1.5. The second test machine used was running Windows 7 Ultimate Service Pack 1 – 64 bit and MSABs XRY 7.1. Both forensic utilities extracted the location where the application is stored (/storage/emulated/0/Android/data/com.twofours.surespot); however no

pertinent data was recovered. Both utilities were also able to extract a folder containing images that were taken from inside of the app (/storage/emulated/0/Pictures/surespot).

Feedback

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

Sources

[i] "Surespot Law Enforcement Guidelines," Surespot Encrypted Messenger, accessed October 31, 2016, https://www.surespot.me/documents/surespot_law_enforcement_guidelines.html.
[ii] Ibid i
[iii] ibid i
[iv] Cruickshank, Paul, Andrew Carey, and Miachael Pearson. "British Police Tricked Terror Suspect into Handing over Phone, Source Says." *CNN World*. CNN, 1 Apr. 2016. Web. 1 Nov. 2016.

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.