# White Paper – Kik

**Author(s):** Technology Research Program

**Date:** 21 February 2018

**More detailed information concerning Kik may be available on the NDCAC Website. Law enforcement personnel may also obtain assistance on the NDCAC website or by contacting the Technical Resource Group (TRG) at 855-306-3222.**

## 1. (U) Executive Summary

(U) Based in Ontario, Canada, Kik is a smartphone messenger application that lets users communicate through chat. Users can send text, pictures, and videos. Kik is a free messaging and sharing app available on iOS and Android, and uses an existing Wi-Fi connection or data plan to communicate with other users.

(U) Users can send and receive messages, images, videos, sketches, webpages, memes, gifs, and other content known as bots from within the app. Users can also create groups, which can have up to 50 friends at a time. Users can also create and join public groups with hashtags. Group owners and admins have the capability to add a group name, photos, and remove people from the group. Owners are the group chat originators and Admins are designated by the Owner

(U) As a security feature of Kik, users can be logged into one device per account at a time. When the user tries to log into their account on second device, Kik will reset on the first device they were signed into, and chat history will be cleared to protect privacy.[1]

(U) Kik utilizes TLSv1.2 encryption for data in motion, however some traffic was found unencrypted in packets sent over port 80.

(U) Kik is a foreign provider. Based on open source information:

- Kik is based in Ontario, Canada and governed by Canadian law
- Kik Servers may be located in the US, Canada, or other countries[2]

(U) Based on the above information, there may be special considerations that have to be taken into account when obtaining information on a Kik target.

### 1.1. (U) Information Collected at Account Sign-up

(U) When a user creates a Kik account, the following information is collected:

- First and Last Name (Not verified)
- Desired Kik Username (Unique Identifier and cannot be changed)
- Email Address (Verified but not required)
- Password
- Birthday (Not verified)
- Phone Number (Not verified)

## 2. (U//FOUO//LES) Law Enforcement Impacts

(U) Law Enforcement should coordinate with their department's legal counsel and/or prosecutor's office to address any questions concerning the requirements or restrictions governing legal authorities or if special considerations exist for obtaining data from companies located outside the US prior to making any request for information from Kik.

(U) According to Kik:

> (U) Agencies outside of Canada may need to submit a Mutual Legal Assistance Treaty (MLAT) request through the proper legal authorities in order to obtain any user data from Kik.[3] State and Local law enforcement agencies can contact the NDCAC Technical Resource Group (TRG) for information on how to begin the MLAT process. Kik will

accept a preservation order while the request goes through the MLAT process. Requests for information should be specific in nature.[3] Excessively broad requests will cause significant delays in responding, and in some cases may mean Kik will not be able to respond to the request.[3]

(U) Due to the time it takes to obtain an order, Kik states they may voluntarily preserve information once a formal preservation request is received from a law enforcement agency.

(U) Law Enforcement seeking to submit a request of Kik can email orders to Kik at lawenforcement@kik.com, using the subject line "LAW ENFORCEMENT ORDER", or mail them to the following address:[3]

Kik Interactive, Inc.
420 Weber Street North, Suite I
Waterloo, ON N2L 4E7
Canada

(U) According to Kik, all orders must include the following information:

- Addressed to 'Kik Interactive, Inc.'
- Contain a valid Kik username(s)
- Specific list of user data that you are requesting
- Signed and dated
- The way in which the disclosed data should be delivered to law enforcement[3]

(U) Data that may be available pursuant to a valid order includes:

- Subscriber data (this information is not verified by Kik)
    - Basic subscriber information provided by the user, such as first and last name and email address
    - Link to the most current profile picture
    - Device related information
    - Account creation date and Kik version
    - Birthdate (new registrations after November 2014)
    - User location information, including most recent IP address (after November 2013)[3]
- Content and/or Historical User Data
    - Photographs and/or videos sent or received by the Kik user, depending on the version of Kik used. However, photographs and videos are automatically deleted within a short period of time after they are sent.
    - Historical IP addresses used by the Kik user. (Please note that these IP addresses are provided by a third party, not by Kik).
    - Transactional chat log timestamps, these are similar to call detail records available from wireless carriers and will never include the text of the conversation or the phone numbers of the individuals involved (Kik only associates accounts with the unique Username).

- Roster log is a record showing who the user has added and/or blocked.[3]

(U) Kik states they do not have access to the text in Kik conversations.[3] For some versions of Kik, conversations are only stored on the phones of the Kik users involved in the conversation.[3] For other versions of Kik (which allows users to access their message history after logging out and then back in to their Kik account), the text of recent conversations is temporarily stored by Kik in a format that Kik cannot read.[3]

## 3. (U//FOUO//LES) Forensics

(U//FOUO//LES) Forensics analysis for the Kik app was conducted on iOS 9.3.3 and Android 7.1.1. There is no generalized extraction information that can be extrapolated to apply to all devices. However, the information specific to the platform tested is provided in (LES) Table 1 and

(LES) Table 2.

**(LES) Table 1: iOS [Kik Forensics Information]**

| [Kik, v11.37.0] |
|---|
| [iOS 9.3.3] |
| **Documents –**<br>**PLIST Files**<br>• com.kik.chat.plist (/Applications/group.com.kik.chat/globalDefaults/defaults<br>o Contains Subject registration name and associated e-mail and profilepicURL<br>o Contains kik messaging server ipv4 and ipv6 DNS cache<br>▪ talk11370ip.kik.com - 184.106.22.135<br>▪ talk11370ip.kik.com_2607:7700:0:24::c0ed:96190<br>o XMPP artifacts<br>▪ Password Digest key<br>▪ Password SHA1<br>▪ Username<br>• kik.default (/Applications/group.com.kik.chat/globalDefaults)<br>o This plist contained Kik UserName (PrevJIDUserDefaultsKey), Application version and last used user name (lastUsedUsername)<br><br>**Databases**<br>• Kik.sqlite (/Applications/group.com.kik.chat/cores/private/442827162c944a0d8a7146a45e10867f/kik.sqlite)<br>o Contained Application Contacts – Application prompts for contact permission and imports contacts using the application<br>o Chat – conversations between subject and associate to include images<br>o Group Chat – Contents of chat, participants, Group Chat creator application email (username_lk2@talk.kik.com) and the Group name chosen by the user.<br>▪ Participants of chat information included the app provided email, Registered Name<br><br>**Media**<br>• Images sent and attached through kik messenger chats are stored in the following location: |

/Applications/group.com.kik.chat/cores/private/442827162c944a0d8a7146a45e10867f/attachments
  - Files within this directory contained memes and drawings created in app by users.
- Application Profile images are stored from both the Subject and Associate users /Applications/group.com.kik.chat/cores/private/442827162c944a0d8a7146a45e10867f/profpix
  - Images are titled by the associated username in both original and thumbnail version

**Additional files of interest**

- Mixpanel-data – advertising / analytical /Applications/com.kik.chat/Documents/mixpanel-data
  - peaugmentumstorage-directorybeneath – contains application (Client) version, user id (KIK User name), network type (Cellular), Platform (iOS), Device ID.

**(LES) Table 2: Android [Kik Forensics Information]**

| [Kik, v11.39.0.19149] |
|---|
| [Android, v7.1.1] |
| Databases<br>• **userdata (ExtX)/Root/data/kik.android/databases/**<br>Several database files containing artifacts of interest, including;<br>• Application Usernames, Subject and Associate.<br>o Party Name- User entered full name<br>o Party Identifier – User application assigned group id#<br>o Chat Start Time, Chat Last Activity with timestamps<br>o Chat Instant Message Body – User generated messages to associate, group and Bot with replies.<br>o Group chat creation time stamp and group members list<br>o Contact matching dialog from application – Application matches Mobile contacts with associated application users.<br>• LOGS_DB-journal<br>o Mobile OS and app version<br>o {"app_version":"11.39.0.19149","event_name":"app_launch","network_type":"4g","os":{"type":"android","version":"7.1.1"} Application ID for mobile, Mobile Carrier identified, Subject IMEI<br>o Video start and stop events with associated timestamps<br>Application Cache<br>• **userdata (ExtX)/Root/data/kik.android/cf528e19-804b-46c7-bdf4-dd6791b56745/cache/**<br>o Cache files retained GIF images, both user sent and images viewed through application<br>Metrics<br>• **userdata (ExtX)/Root/data/kik.android/app_augmentum-metrics/**<br>o Contained numerous artifacts of interest, to include:<br>▪ Device ID, OS, Orientation,<br>▪ Instance ID, Application UserID,<br>▪ Timestamps with associated triggering event<br>▪ Event counters – i.e.- Images received, messages received with timestamps<br>"Vidyo" information on application video conferencing client:<br>• **userdata (ExtX)/Root/app/kik.android-1/lib/arm/**<br>o Shared library files pertaining to the Vidyo Client. Files appear to be partially encrypted / obfuscated which limits the usefulness of the information found within. |

## 4. (U//FOUO/LES) Technical Analysis on Local Broadband

(U//FOUFO//LES) Analysis of the Kik app was conducted via local broadband test collection in January 2018. A full broadband intercept may provide different information and results.

### 4.1 (U//FOUO//LES) Apple iOS

(U//FOUO//LES) From a Pen Register perspective, Kik utilized both IPv4 and IPv6 addressing for the applications communications. Although the application itself could not be identified through a Pen Register, numerous connections to associated Amazon Web Services (AWS) Cloud servers and Rackspace hosted addresses were found.

(U//FOUO//LES) From a Lawful Intercept perspective, this application was found to communicate to various cloud based servers such as; AWS, Rackspace, and Google. Amazon and Rackspace appeared to contain the majority of user communications and associated GIFs, Emojis and Images via the KIK application. Traffic from Rackspace contained the talk10100an and talk1080an and was found using TCP port 5223 for the messaging (text) feature of the app. Google provided additional content (GIFs, Images) and analytics traffic.

(U//FOUO//LES) The application utilized AWS hosting for a majority of the network connections. These connections included clientmetrics-augmentum.kik, profilepics.cf.kik, smily-cdn.kik.com, my.kik, home.kik, kik.platform.s3.amazonaws. Also hosted by Amazon were some of the application content providers for GIF, stickers and images. These included media.riffsy, api.riffsy, getscribblechat, and card-sketch.appspot. The majority of the AWS traffic was encrypted using TLSv1.2 over port 443. While some of the traffic was discovered in plaintext over port 80, no actual user transmitted messaging content was viewable in plaintext.

(U//FOUO//LES) It should be noted, when using a third-party IP search service such as Robtex, addressing could be resolved to Kik servers. Specifically, 104.130.110.7 resolves to host talk10100an.kik.com on Rackspace.

(U//FOUO//LES) Network traffic used for the Video Chat feature were found on an Abstract Syntax Notation (ASN) of AS200130, Digital Ocean LLC. This traffic was identified with both IPv4 and IPv6 addressing.

- IPv4 video traffic used *IP 165.227.79.73* over User Datagram Protocol (UDP). Ports *49680, 49681, 49682* contained a Real-Time Transport Protocol (RTP) stream using PT=DynamicRTP-Type-120 while Ports *58410* and *58411* used PT=DynamicRTP-Type-96. Dynamic-RTP-Type-96 traffic included information regarding video codec "VidyoCodecVerNum2:2.1.5.9". The IPv4 Real-Time Transport Control Protocol (RTCP) streams included "Transport=TLS", indicating the implementation of Transport Layer Security.

- IPv6 traffic destination address of *2604:a880:800:a1::c0:d001* over Transport Control Protocol (TCP) port *50001* on ASN: AS200130, Digital Ocean LLC. The TCP traffic utilized TLSv1.2 encryption preventing the RTP specific identification. Header information did however, include media.kik.com. Corresponding Session Transversal of UDP through Network Address Translation (STUN) traffic utilized UDP over port *13152* and *13153*. IPv6 traffic was found to carry a majority of the video related traffic.

### 4.2 (U//FOUO//LES) Android

(U//FOUO//LES) From a Pen Register perspective, Kik utilized IPv4 addressing for the applications communications. Although the application itself could not be identified through a Pen Register, numerous connections to associated AWS Cloud servers were found.

(U//FOFUO//LES) From a Lawful Intercept perspective, this application was found to communicate to various cloud based servers from Google and AWS. Most notably were the servers from AWS with hostnames of api.kik.com, bots.kick.com, captcha.kick.com, clientmetrics-augmentum.kik.com, cdn.kik.com, home.kik.com, media.kik.com, meme.kik.com, platform.kik.com, profilepics.cf.kik.com, sketch.kik.com, talk11390an.kik.com, videos.kik.com. All the aforementioned servers communicated in a secure fashion via TCP Port 443, except for the servers, sketch.kik.com, meme.kik.com, videos.kik.com and profilepics.cf.kik.com which communicated unencrypted via TCP Port 80. With the insecure network traffic the device information is seen in the USER_AGENT string located within the header. The associate's and subject's profile image were also found unencrypted and viewable as well.

(U//FOUO//LES) The messaging protocol employed by Kik uses TCP port *5222-5223* to transmit data across the network. This communication was identified as traffic primarily going to and from the talk11390an.kik.com servers hosted by Rackspace.

(U//FOUO//LES) Video traffic is identified with RTCP, STUN and finally the associated RTP stream, with a dynamic payload type of DynamicRTP-Type-120 and Type-96. Dynamic-RTP-Type-96 traffic included information regarding video codec "VidyoCodecVerNum2:2.1.5.9". Vidyo is a Video conferencing client used for the video chatting within the KIK application.

- Also included, "transport = TLS", indicating the RTCP portion of the video traffic incorporates some type of TLS / encryption. However, the RTCP traffic headers included KIK user names of both the subject and associate.

### 4.3 (U//FOUO//LES) Technical Analysis Diagrams

(LES) Table 3 and (LES) Table 4 summarizes the information that can be gleaned from the iOS communication stream when encountered as part of a local broadband test collection.

**(LES) Table 3: iOS Kik Features in Full Content Broadband**

| | Encryption Status | Features | Notes |
|---|---|---|---|
| **App Features & Content** | Encrypted, but Partially Visible | • Picture Message<br>• Emoji Message | Subject and Associate profile picture can be seen in plaintext in all features of this app. Additional images are also found in the application network traffic. |
| | Encrypted | • Video Message<br>• Text Message<br>• Video Call | Others available features Kik bots: Traffic from messaging-bots to subject |

**(LES) Table 4: iOS Kik Metadata in Full Content Broadband**

| | Identifiable Status | Metadata | Notes |
|---|---|---|---|
| **App Metadata** | Identifiable | • Devices<br>• App Name<br>• DNS Queries<br>• Encryption Info<br>• Other Identifiable Info | Application name and version as well as the device are identified from HTTP Traffic User-Agent string: Application: Kik/v11.37.0 iOS- 9.3.3.<br>DNS Queries were readable<br>Encryption Info: TLS Certificates were captured.<br>Application User Id for Subject and Associate discovered in RTCP traffic. |

(LES) Table 5 and (LES) Table 6 summarizes the information that can be gleaned from the iOS communication stream when encountered as part of a local broadband test collection.

**(LES) Table 5: Android Kik Features in Full Content Broadband**

| | Encryption Status | Feature | Notes |
|---|---|---|---|
| **App Features & Content** | Encrypted | • Picture Message<br>• Video Message<br>• Emoji Message<br>• Text Message<br>• Video Call | Subject and Associate profile picture can be seen in plaintext in all features of this app.<br>Others available features Kik bots: Traffic from bots goes through Kik app but uses its own apps servers. |

**(LES) Table 6: Android Kik Metadata in Full Content Broadband**

| | Identifiable Status | Metadata | Notes |
|---|---|---|---|
| **App Metadata** | Identifiable | • Devices<br>• App Name<br>• DNS Queries<br>• Login/User ID<br>• Encryption Info<br>• Other Identifiable Info | Application name and version as well as the device are identified from HTTP Traffic User-Agent string: User-Agent: Kik/11.39.0.19149 (Android 7.1.1) Mozilla/5.0 (Linux; Android 7.1.1; Nexus 6P Build/NUF26K) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/58.0.3029.83 Mobile Safari/537.36\r\n<br>Associate username can be seen in plaintext.<br>Encryption Info: TLS Certificates were extracted.<br>Application User Id for Subject and Associate discovered in RTCP traffic. |

(U) All data sent/received will have a notation of date and time associated with the activity.

(U) For additional technical information and examples of information gathered, please visit the NDCAC App Catalog on the NDCAC website.

## 5. (U) References

[1] https://kikinteractive.zendesk.com/hc/en-us/articles/217680378-Can-I-log-in-to-the-same-Kik-account-on-more-than-one-device-
[2] https://www.kik.com/privacy-policy/
[3] https://lawenforcement.kik.com/hc/en-us/articles/203419779-Download-our-Guide-for-Law-Enforcement