RKS Global

September 2025 • rks.global

Surveillance Testing in MAX on iPhone

I. Study of MAX behavior on a user's phone with permissions enabled

Hypothesis

On iPhone, the MAX messenger uses granted permissions on its own.

Tasks

Verify how the app uses the granted permissions and whether it does anything autonomously.

Methodology

1. Analyze the sysdiagnose file with app and system logs using iLEAPP and manually
2. Monitor app traffic via PiRouge
3. Monitor app activity using iPhone's built-in App Privacy Report, which shows which apps used permissions

Study conditions

1. iPhone 13, 22G100, 18.6.2
2. All phone traffic is routed through PiRouge Wi-Fi, version 2.0.5
3. MAX messenger installed via the App Store, version 25.9.5

4. MAX was granted all permissions it requested (Contacts, Photos, Camera, Microphone)

The app was tested with a Russian IP address, geolocation, and phone number, as well as with an IP address and geolocation outside Russia.

Research process

1. For a 48-hour period, the phone with the app installed was under observation.
2. The app was in various states:
    a. Minimized with the phone locked
    b. Minimized with the phone unlocked (home screen)
    c. In the foreground
    d. In the foreground with a nearby speech source active
3. After obtaining the files, sysdiagnose logs were analyzed using iLEAPP and manually; the .pcap file was analyzed using Python.

Study results

In none of the observed test configurations was improper access detected to Contacts, Photos, Camera, or Microphone. Technically, the app is capable of collecting and transmitting these data, but we did not observe this occurring. It may occur selectively or depending on location.

Potential further research

1. Decrypt the traffic to examine the contents of these and other packets.
2. Capture anomalies (change geolocation, switch the phone number to CIS countries, etc.).
3. Investigate hosts and domains (api.oneme.ru, i.oneme.ru, tracker-api.vk-analytics.ru, pimg.mycdn.me, st.max.ru, sdk-api.apptracer.ru).

Media

Granted permissions

Last Modified Timestamp	Bundle ID	Service	Access
2025-09-01 21:12:54+00:00	ru.oneme.app	AddressBook	Allowed
2025-09-04 07:22:48+00:00	ru.oneme.app	Photos	Allowed
2025-09-04 07:23:11+00:00	ru.oneme.app	Camera	Allowed
2025-09-04 07:25:07+00:00	ru.oneme.app	Microphone	Allowed

II. Study of MAX behavior on a user’s phone with permissions revoked

Hypothesis

If MAX’s permissions are revoked on iPhone, it will try to regain them.

Tasks

Check whether the app will request permissions again, in which cases, and how persistently.

Research process

1. All previously granted permissions were revoked via iPhone settings.
2. When opening the MAX app, it does not request permissions.
3. In the Contacts tab, you can see the “Connect contacts” button. If you tap it, MAX requests access to contacts; if you don’t, it does not ask.
4. In the Calls tab, you can see “Turn on microphone.” If you tap it, the app requests access; if you don’t, it does not ask.
5. In the Chats tab, you can see the “Connect contacts” button. If you tap it, the app requests access; if you don’t, it does not ask.

6. In a chat, you can see the “Attach file” (paperclip). If you tap it, the app requests access; if you don’t, it does not ask.
7. In a chat, there is a button resembling the Instagram icon (for recording video messages/stories). If you tap it, the app requests access; if you don’t, it does not ask.
8. In a chat, there is a microphone button (for recording voice messages). If you tap it, the app requests access to the microphone; if you don’t, it does not ask.

Study results

If you do not activate a function that requires a permission, those permissions are not requested.