Tel. +370 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

NATIONAL CYBER SECURITY CENTRE
UNDER THE MINISTRY OF NATIONAL DEFENCE REPUBLIC OF LITHUANIA

INFORMATION BULLETIN ON INVESTIGATION OF THE „YANDEX. TAXI“ APPLICATION AND RECOMMENDATIONS FOR APPLICATIONS SAFE USAGE

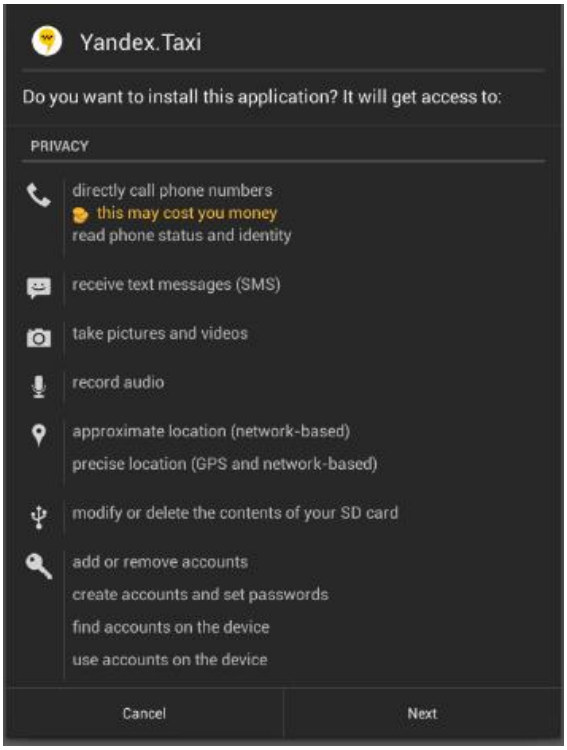
9 August 2018

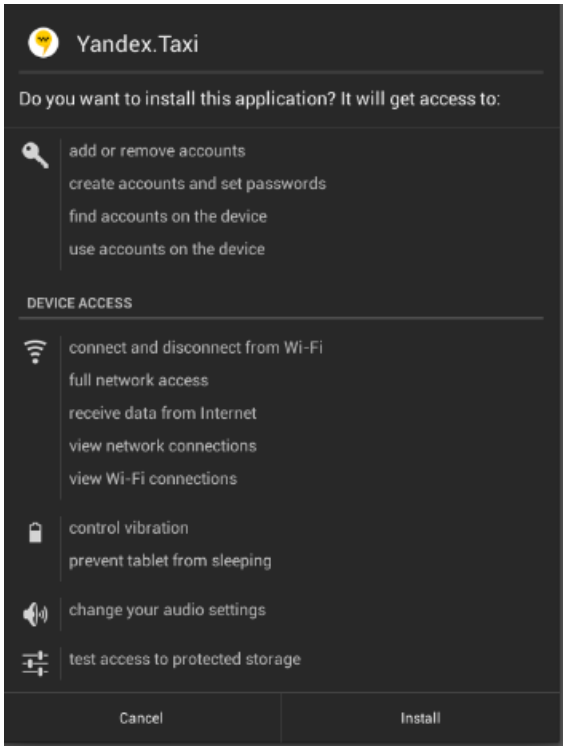
TLP: WHITE

The National Cyber Security Centre under the Ministry of National Defence carried out initial analysis of “Yandex. Taxi” application for smartphones, which was actively offered for Lithuanian users since 26 July 2018.

The analysis of the application revealed that it requires access to a large amount of sensitive data and permissions to device functions, which might be excessive. The app has the ability to turn on the device camera and microphone (take pictures and videos, record sound), access contact list (phone book, social media accounts’ information), control the phone call services, identify phone status and identity, control the text message service (intercept messages), modification or deletion of the contents on the smartphone’s storage, determine precise GPS location of the device, manage network access (receive data, monitor and control network connections, manage Wi-Fi access).

Tel. +370 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt





It is worth to mention that, later versions of the application may require additional permissions after an update.

However, despite the abundance of requirements to access the functionalities of the device, application is properly optimized, uses encrypted channels and standard protocol ports for data transfers.

National Cyber Security Centre's analysis showed that the app regularly connected and exchanged data with 11 unique IP addresses (10 of which are of the Russian Federation) via encrypted channels. Data transfers were conducted at different time intervals, randomly.

It was determined, that the app has the ability to send data packages at different times to different regions of the Russian Federation IP addresses (according to geolocation IP database information) via encrypted channels, regardless of whether the app works in a standby or active mode. NCSC notes that "Yandex. Taxi" application maintained a constant connection with three IP addresses. **Table 1** provides systemised information of the primary analysis.

Tel. +370 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

Table 1. Primary analysis of the program package network traffic flow (*NOTE: IP addresses are known to National Cyber Security Centre*)

Trade name: **Yandex. Taxi**					
System name: **ru.yandex.taxi**					
No	Active network connections	City	Hostname	Data transfers while the app is in standby mode	Data transfers while the app is in active mode
1		Moscow	*.yandex.net	*Yes*	*Yes*
2		Moscow	*.yandex.net	*Yes*	*No*
3		Moscow	*.yandex.net	*Yes*	*No*
4		New Jersey, Absecon	*.linode.com	*Yes*	*Yes*
5		Yekaterinburg	*.yandex.net	*Yes*	*Yes*
6		Moscow	*.yandex.ru	*No*	*Yes*
7		Yekaterinburg	*.yandex.ru	*No*	*Yes*
8		Yekaterinburg	*.yandex.net	*No*	*Yes*
9		Yekaterinburg	*.yandex.net	*No*	*Yes*
10		Moscow	*.yandex.net	*No*	*Yes*
11		Moscow	*.yandex.ru	*No*	*Yes*

In addition, referring to the annual report by the State Security Department and the Second Investigation Department under the Ministry of National Defence "Assessment of Threats to National Security 2018": "*Russian intelligence and security services have legal authority and technical capabilities to access the data of Russian and foreign citizens, who are using Russian electronic communication platforms.*". In The Threat Assessment it is also being pointed out that *: "(...) all citizens of The Republic of Lithuania who are using Russian social media and e-mail services, e.g., odnoklasniki, mail.ru, yandex, etc., are under the threat of their personal data being used by Russian intelligence and security services."*

Tel. +370 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

Mobile application threats

National Cyber Security Centre warns that the risks of malware on the device are real: criminals can steal money and confidential information, spy on the user, blackmail the owner of the smartphone in regards of disclosing private information, send high-cost SMS messages at owner's expense, exploit the device for spreading spam and viruses, hacking other devices or conducting cyber-attacks.

It is also important to keep in mind the rise of ransomware attacks. Ransomware holds your mobile device and data as a hostage until you pay the ransom. This type of malware locks your device's screen or prevents you from accessing some of the files and features. Sometimes even restoring to factory default settings or reverting the phone OS leaves your device infected.

Unfortunately, most of the people still do not realize the importance of protecting their mobile device. NCSC provides some tips on how to securely manage mobile devices daily , while using applications and how to protect or at the least reduce the risks of mobile apps' threats.

Recommendations

Use only applications from official app store platforms - Google Play (Android) or App Store (iOS). Avoid apps from third parties. Do not install cracked applications, because typically these apps do more than they claim and conduct malicious activity.

Be cautious of the links sent via e-mail or text messages, they may be tricking you into installing third party or unknown source apps.

Find out more about the app and its publishers before downloading, check other users' ratings and reviews, download count.

Check which permissions the application requires – what data is accessed and whether the app can share your data with third parties. Evaluate whether the

Tel. +370 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

permissions that are specified for performing its functions are not excessive. For e.g. a flashlight does not need to access your microphone function.

Keep your apps and operating system updated, turn on automatic updates. if possible, to escape risks related to outdated and vulnerable versions.

Do not modify your operating system, by rooting it (Android) or jailbreaking (iOS). This might weaken existing phone protections and increase the risks of being infected by malware. This could also violate the terms and conditions of the warranty of your device and lead to warranty void.

Install a mobile security solution to monitor apps on your device for malware and suspicious activities.

Make backups of your data frequently. Use backup software to make data copies to your computer or use automatic backup services.