Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

November 30, 2023

Mobile App Security Threat Alert: WeChat by Tencent

The National Cyber and Information Security Agency (hereinafter the „Agency“) is issuing a security threat alert regarding the use of Tencent's WeChat mobile application. The Agency is concerned about the possibility of misuse of the data collected by the app, due to a combination of several factors: excessive collection of user data and methods of their collection which may facilitate precise targeting of cyberattacks; the legal environment of the People's Republic of China (PRC); and the PRC's influence operations in the Czech Republic. While the number of active users of WeChat in the Czech Republic is significantly lower compared to other social media platforms, Czech users of the app may include high-risk individuals such as diplomats, businesspeople, scholars, or Chinese dissidents. These individuals may then be targeted for collection of sensitive information that can later be used, for example, for blackmail or other forms of coercion by malicious actors.

WeChat is a social media and messaging mobile app with many additional features. It is developed and operated by Tencent, a company based in Shenzhen, China. The platform is used by approximately 1.3 billion active users worldwide. The majority is located in the PRC and in countries with large Chinese diaspora. In the Czech Republic, WeChat currently has a low number of active users; however, they often consist of high-profile individuals who frequently visit the PRC or use the app to communicate with Chinese partners and counterparts. The risks associated with the WeChat app are very similar to those associated with the use of the TikTok app operated by the Chinese company ByteDance, which the Agency warned about on March 8, 2023. Due to the lower levels of WeChat use in the Czech Republic compared to TikTok - the most significant difference between the two apps - the Agency proceeded to issue a security threat alert regarding the WeChat platform rather than a warning.

The Agency recommends that anyone who needs to use WeChat should have the app installed on a separate device. If this is not possible, we recommend keeping it on the device only for as long as necessary and to only allow permissions relevant to the functionality of the app.

Reasoning Behind Agency´s Security Threat Alert

The WeChat for Android and iOS collects an exorbitant amount of data from its users (see here and here), which is not required for proper functioning of the app. This data can be used to target cyberattacks on specific individuals, thereby increasing the risk of a successful compromise (e.g., through spear-phishing). The international version of the application also has a functionality allowing downloading and installation of code without the user's knowledge. This functionality could be abused, for example, for unauthorized installation of malicious code. WeChat also does not provide end-to-end encryption and all communications pass through servers to which Tencent has access. This may result in, among other things, censorship of private messages containing certain keywords or other content identified by Tencent as objectionable (see more here and here).

Tencent is an entity subject to Chinese national legislation and regulations. Chinese law, specifically the State Security Law of 2015, the 2017 Law on State Intelligence Activities, the 2014 Law on State Counterintelligence Activities, the Companies Law of 2013, and 2021 Regulations for Reporting Vulnerabilities in Network Devices require institutions, commercial entities, and individuals to cooperate with Chinese authorities, even against the interests of their international partners or customers. According to publicly available sources (see more here) and information from the Agency´s partners, Tencent is closely intertwined with the PRC state apparatus and the Chinese Communist Party.

Citing the 2022 Annual Report (see here) of the Czech Security Information Service (BIS), the PRC poses a growing and complex intelligence threat. According to this report, Chinese intelligence services conduct influence operations on behalf of the PRC against the interests of the Czech Republic, and their activities in our country are at a high level. In addition, according to BIS, the high level of activity of Chinese actors in the cyberspace against the Czech Republic and other members of the European Union and the North Atlantic Treaty Organization cannot be ignored. The issuing of this security threat alert is also compliant with relevant paragraphs (28 and 29) of The 2023 Security Strategy of the Czech Republic.