National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky
Company ID No: 05800226
Data box ID: zzfnkp3

File No:
350 - 303/2023
Reference No:
2236/2023-NÚKIB-E/350

Brno, 8 March 2023

WARNING

The National Cyber and Information Security Agency, with its registered office at Mučednická 1125/31, 616 00 Brno (hereinafter the "Agency"), pursuant to Section 12(1) of Act No 181/2014 Coll., on cyber security and on the amendment of related laws, as amended (hereinafter the "Cyber Security Act"), issues this

Warning

about a cyber security threat of installation and use of TikTok on devices that have access to information and communication systems of critical information infrastructure, information systems of essential services and important information systems.

The National Cyber and Information Security Agency has evaluated this threat as "High" – the likelihood of the threat is considered as likely up to very likely.

Authorities and persons who are obliged to implement security measures under the Cyber Security Act are required to address the threat in the context of risk management pursuant to Section 5(1)(d) of Decree No 82/2018 Coll., on cyber security, security measures, cyber security incidents, reactive measures, cyber security filing requirements and data disposal (hereinafter the "Cyber Security Decree"), evaluate this threat as "High" – the threat is likely up to very likely. If an obliged person uses a different method for risk assessment, pursuant to Section 5 of Attachment 2 of the Cyber Security Decree, this threat must be assessed according to this method at a comparable level as would be the case pursuant to Section 5(1)(d) of the Cyber Security Decree.

JUSTIFICATION

1. On the basis of the facts established in the exercise of its powers, the Agency concluded that the installation and use of the TikTok application on devices accessing information and communication systems of critical information infrastructure, information systems of essential

services and important information systems constitutes a cyber security threat and is therefore issuing this Warning about this threat pursuant to Section 12(1) of the Cyber Security Act.

2. A combination of the following observations and findings led to the issuance of this warning.

3. Cyber security consists in not only assessing the technical aspects of the technologies used; when selecting the technical and software tools used for ensuring the proper functioning of information and communication systems and their suppliers, it is necessary to consider the non-technical aspects of the security of the technology, i.e. to assess the credibility of the suppliers and subcontractors (manufacturers) of the technology. The trustworthiness of the supplier is then directly reflected in the trustworthiness of the technology supplied and determines the level of risk associated with the use of such technology. Trust in the supplier must be present both at the level of the final form of the delivered solution (quality) and at the strategic - non-technical - level, and it also involves trust in the business, legal and political environment in which the supplier operates.

4. The level of trustworthiness of the legal environment of some countries has a direct impact on the trustworthiness of the companies that are headquartered in them and are subject to such legal environment. In states with less credible legal environments, it cannot be excluded that the companies concerned will be forced by the state to put the interests of that state before those of their customers.

5. The social platform TikTok, developed and operated by the Chinese company ByteDance, is one of the most widely used in its categories worldwide. TikTok is experiencing strong growth in the Czech market where it currently has about two million active users.

6. ByteDance is an entity subject to Chinese national legislation. The State Security Law (国家安全法) of 2015 imposes a general obligation on all Chinese citizens and organisations to provide assistance to state authorities in matters of state security. The 2017 Law on State Intelligence Activities (中华人民共和国国家情报法) stipulates in Article 7 that every citizen and organisation must support national intelligence activities, provide cooperation and collaboration, and maintain confidentiality of classified matters that come to their attention in connection with national intelligence activities. The 2014 Law on State Counterintelligence Activities (中华人民共和国反间谍法) imposes an obligation to provide cooperation and information on foreign clients of Chinese companies in case they are suspected of espionage activities by state authorities. According to Article 6, this law is also applicable to institutions, organisations and individuals that organise or finance espionage activities against the People's Republic of China ("PRC") outside its territory, with a wide range of activities that can be defined as espionage by Chinese authorities. All this without the possibility of independent judicial review. The Companies Law of 2013 (中华人民共和国公司法2013修订) allows the Communist Party of China ("CPC") to effectively influence the operation of private companies. According to Article 19, an organisation of the CPC must be established in the company to carry out the activities of the CPC in accordance with its Constitution. The company must provide the necessary conditions for these activities. According to the 2021 Rules for Reporting

Vulnerabilities in Network Devices (**公安部关于印**发网络产品安全漏洞管理规定的通知), technology manufacturers are required to report security vulnerabilities to the Chinese Ministry of Industry and Information Technology ("MIIT") no later than two days after discovery. MIIT then reports the finding to the PRC Ministry of State Security and other relevant authorities. It is prohibited to disclose these vulnerabilities to the public or report them to foreign organisations and individuals. Thus, the above creates concerns that the PRC's interests may be placed above the interests of technology users of companies subject to the PRC's legal environment.

7. With reference to the 2021 Annual Report of the Security Information Service of the Czech Republic ("BIS"), the PRC poses a growing complex intelligence threat. According to this report, Chinese intelligence services conduct influence operations for the PRC against the interests of the Czech Republic and their activities are at a high level on our territory. In addition, according to BIS, the high level of activity of Chinese actors in the area of cyber-attacks against the Czech Republic and other members of the European Union and the North Atlantic Treaty Organisation cannot be ignored.

8. The information gathered shows that TikTok collects an excessive amount of user data. In particular, it does so in the following ways:

    - device mapping, where applications find out information about other applications running and installed,
    - the content of private communications is stored on ByteDance's servers,
    - periodically checking the location of devices,
    - access to contacts on the device,
    - device information including Wi-Fi SSID, previous Wi-Fi configuration, device and SIM card serial number, device ID, device IMEI, device MAC address, phone number, a listing of all user accounts used on the device, and complete clipboard access,
    - persistent access to the calendar to read and change it, or
    - enforcing the use of a native browser that allows tracking of almost all user activity (e.g. keystrokes on the screen).

9. The amount of data and the manner in which it is collected can serve to target cyber-attacks on specific individuals, thereby increasing the risk of success (e.g. through spear phishing). At the same time, this data can be used to blackmail persons of interest and thus undermine the security or strategic interests of the Czech Republic.

10. The TikTok application operator publicly declares that, although the data of European users is stored in the United States and Singapore, it is granted remote access by certain entities based in Brazil, the PRC, Malaysia, Singapore, the USA and the Philippines.

11. An investigation is currently under way by the European Commission to determine whether, in light of the extensive data collection, including personal data, carried out by the TikTok application, the handling of and access to such data violates Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

12. The amended version of the TikTok application for the Chinese market, the Douyin application, has the functionality to download and install code without the user's knowledge. This poses a risk of downloading and installing malicious code which may lead to the compromise of the device and consequently the regulated system to which the device has access. It cannot be excluded that a similar functionality may be part of the international version of the TikTok application in the future.

13. Open-source technical analyses together with other information point to problematic handling and access to user data by ByteDance employees in the PRC, despite repeated claims by its representatives against it.

14. The TikTok application is designed for use on mobile devices (especially mobile phones and tablets). In many cases, mobile devices are part of information systems regulated by the Cyber Security Act or their information security management scope. Such devices access the core assets that make up the regulated systems, and a breach of their security leads to a direct threat to the security of those systems, as well as to the proper delivery of the service for which the systems were included in the regulation. At the same time, however, even those devices that are not part of the regulated systems or their information security management scope, but which are used by strategically important persons in organisations managing or operating regulated systems, may be the target of activities consisting in the collection of sensitive information about these persons and the subsequent misuse of this information, for example for blackmail or other forms of advancing the interests of attackers.

15. The above-mentioned facts overall lead to a reasonable concern about the potential security risks arising from the installation and use of the TikTok application on devices accessing information and communication systems of critical information infrastructure, essential service information systems and important information systems.

16. The Agency assesses the threat level as high, i.e. in accordance with the threat rating scale contained in Annex 2 to the Cyber Security Decree as likely up to very likely. The threat level is primarily due to the combination of the large number of TikTok users in the Czech Republic, the technical specifics of the application which collects an excessive amount of sensitive and highly exploitable information and data about its users, and the legal environment which ByteDance operates in and is bound by. At the same time, we cannot ignore the fact that the problematic nature of the application has long been highlighted by both national and international partners, and many EU Member States and institutions have already taken preventive measures against it.

17. Depending on nature and manner of use of a specific device and nature and sensitivity of information and data which are accessible by the device, the Agency recommends taking adequate security measures to eliminate the threat that this warning points to. The Agency recommends prohibiting the installation and use of the TikTok application on devices with access to the regulated system (both work and private devices used for work purposes). If authorities or persons who are required to implement security measures under the Cyber Security Act do not have such devices included in the scope of the organisation's information security management, the Agency strongly recommends a review of such a decision. Any use

of the TikTok application on devices accessing regulated systems or affecting the security of regulated systems should be included in the risk management process. Identified risks and measures taken should be adequately communicated within the organisation and to relevant suppliers.

18. At the same time, the Agency recommends that all natural persons whose data could be targeted by the activities of foreign intelligence services (so called persons of interest, i.e. persons who are e.g. in high political, public or decision-making positions) consider limiting or completely prohibiting the installation and use of the TikTok application on their personal devices.

19. The Agency recommends the general public to pay attention to what access the TikTok application requires, what data it collects and how it is handled. The Agency generally recommends installing and using only applications trusted by the user.

20. The fact that this warning highlights the existence of a cyber security threat to a specific technology does not mean that the facts contained in the justification, in particular concerning the legal environment which ByteDance operates in, are not also relevant for other technologies originating from the same legal environment. However, based on all the information gathered in relation to TikTok, the Agency has found this threat to be likely up to very likely.

21. The Agency's authority to issue this warning is provided by Section 22(b) of the Cyber Security Act, which empowers it to issue measures. According to Section 11(2) of the Cyber Security Act, these measures include warnings under Section 12 of the Cyber Security Act. The Agency shall issue a warning pursuant to Section 12(1) of the Cyber Security Act if it becomes aware of a cyber security threat, in particular as a result of its own activities, on the initiative of the national CERT's operator, or from cyber security authorities abroad. In accordance with Section 12(2) of the Cyber Security Act, the Agency shall publish the warning on its website and notify the authorities and persons referred to in Section 3 of the Cyber Security Act.

22. According to Section 22(j) of the Cyber Security Act, the Agency's task is to ensure prevention in the field of cyber security. This preventive activity also includes the provision of information on identified cyber security threats. However, if the threat reaches such an intensity that informing about it cannot be covered by the Agency's standard prevention activities, the Agency is obliged to issue a warning under Section 12 of the Cyber Security Act, in accordance with the above.

23. The Agency notes that authorities or persons obliged to implement security measures pursuant to the Cyber Security Act shall take into account the measures pursuant to Section 11 of the Cyber Security Act in the risk assessment and risk management plan in the context of risk management pursuant to Section 5(1)(h)(3) of the Cyber Security Decree. One of these measures is a warning pursuant to Section 12 of the Cyber Security Act. On the basis of the above, the Agency considers the threat in the statement of this warning to be likely up to very likely. Authorities and persons who are obliged to implement security measures under the Cyber Security Act are therefore obliged to assess this threat at the appropriate level, i.e. at

the level High. If the obliged person uses another method for risk assessment in accordance with paragraph 5 of Annex 2 to the Cyber Security Decree, the threat must be assessed under this method at a comparable level as would be the case under the procedure under Section 5(1)(d) of the Cyber Security Decree.

24. The Agency further notes that in accordance with Section 4(4) of the Cyber Security Act, the authorities and persons referred to in Section 3(c) to (f) of the Cyber Security Act are obliged to take into account the requirements resulting from security measures when selecting a supplier for their information or communication system and to include these requirements in the contract they conclude with the supplier. Taking into account the requirements resulting from the security measures referred to in the first sentence to the extent necessary to fulfil the obligations under the Cyber Security Act shall not be regarded as an unlawful restriction of competition or an unjustified barrier to competition.

Ing. Lukáš Kintr
Director
National Cyber and Information Security Agency