National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky
Company ID: 05800226
Databox ID: zzfnkp3

File No:
350 - 231/2020
Ref. No:
2066/2020-NÚKIB-E/350

Brno, 16 April 2020

WARNING

Pursuant to Section 12(1) of Act No 181/2014, on cyber security, the National Cyber and Information Security Agency, registered office Mučednická 1125/31, 616 00 Brno (hereinafter referred to as "the Agency") is issuing this

warning

against a cybersecurity threat in the form of an extensive campaign of cyberattacks on information and communication systems in the Czech Republic, and on the systems of healthcare facilities in particular. This campaign could have severe impacts on the availability, confidentiality, and integrity of the information in important information and communication systems.

The Agency has information that the threat could be carried out in the coming days, however there are also indications that the preparatory phase of the attacks is already in progress, namely via a spear-phishing campaign.

The National Cyber and Information Security Agency assesses this threat level as High – the threat is probable to highly probable.

In the light of this threat, the Agency strongly recommends taking the following actions:

- Draw users' attention to the dangers of spear-phishing and include a request for any users who have opened suspicious attachments in the last few days to contact the infrastructure administrator;
- Draw users' attention to the possibility that phishing might contain "masked" executable files, such as "obrazek.png.exe", "text.txt.exe", "dokument.pdf.exe" etc.;
- If possible, use a central setting to prevent the launching of active content and macros, especially in .doc and .docx documents;
- Immediately block remote access to the infrastructure as well as open services to the public network, with the exception of strictly necessary ones (public IP ranges can be checked

in the available search engines of devices connected to the network, and thus ports that were opened or forgotten in the past, or services available from the public network, can be secured);

- Immediately create offline backup files and perform such backups based on the importance of the data for the organisation;

- Check the consistency of already created backup files and immediately update antivirus solutions in the infrastructure.

The Agency further provides the following hashes of harmful files for potential checking for harmful activities:

File type: Win32 EXE

- MD5 28e1786bd652942f0be31080a9452389
- SHA-1 44cb931ee16f1f6e3b408035efcd795d8aa0c9be
- SHA-256 7aa996ff7551362f42ba31d4cd92d255a49735518b3f4dc33283fdd5c5a61b42

File type: Win32 EXE

- MD5 e20ee9bbbd1ebe131f973fe3706ca799
- SHA-1 4e92e5cbe9092f94b4f4951893b5d9ca304d292c
- SHA-256 f632b6e822d69fb54b41f83a357ff65d8bfc67bc3e304e88bf4d9f0c4aedc224

File type: Win32 EXE

- MD5 9dbbfa81fe433b24b3f3b7809be2cc7f
- SHA-1 b87405ff26a1ab2a03f3803518f306cf906ab47f
- SHA-256 dfbcce38214fdde0b8c80771cfdec499fc086735c8e7e25293e7292fc7993b4c

File type: Win32 EXE

- MD5 7def1c942eea4c2024164cd5b7970ec8
- SHA-1 b2f4288577bf8f8f06a487b17163d74ebe46ab43
- SHA-256 c3f11936fe43d62982160a876cc000f906cb34bb589f4e76e54d0a5589b2fdb9

File type: Win32 EXE

- MD5 e6ccc960ae38768664e8cf40c74a9902
- SHA-1 d29cbc92744db7dc5bb8b7a8de6e3fa2c75b9dcd
- SHA-256 b780e24e14885c6ab836aae84747aa0d975017f5fc5b7f031d51c7469793eabe

File type: Win32 EXE

- MD5 b1349ca048b6b09f2b8224367fda4950
- SHA-1 44fac7dd4b9b1ccc61af4859c8104dd507e82e2d
- SHA-256 c46c3d2bea1e42b628d6988063d247918f3f8b69b5a1c376028a2a0cadd53986

File type: Win32 EXE

- MD5 0d7dbda706e0048aca27f133d4fc7c51
- SHA-1 1ed9dc8be0f925a5c23e6b516062744931697c78
- SHA-256 ac6b3f9e0848590e1b933182f1b206c00f24c3aa0aa6c62ca57682eff044d079

JUSTIFICATION

1. Based on facts established during the course of its activities, and obtained from bodies involved in cybersecurity abroad and domestic partners, the Agency has identified a cybersecurity threat associated with an ongoing campaign of major cyberattacks on information and communication systems in the Czech Republic aiming at multiple targets in the Czech Republic, and at healthcare facilities in particular.

2. As part of its activities pursuant to Section 22(u) of the Act on Cyber Security, the Agency monitors and analyses cybersecurity threats and risks, and pursuant to Section 20(b)(f) receives reports of cybersecurity incidents from entities obliged under the Act on Cyber Security, from other entities not obliged under the Act on Cyber Security, and from other partners. During these activities, the Agency has acquired indications that the preparatory phase of the attack is already in progress, namely in the form of a spear-phishing campaign.

3. The Agency has noticed an increased number of cyberattacks with particularly dangerous impacts in the context of the current situation associated with the occurrence of coronavirus (SARS CoV-2) in the Czech Republic, the state of emergency, and the need to ensure the functioning of important information and communication systems and the services they support.

4. Taken as a whole, these facts have led to well-founded concern that serious cyberattacks aimed at important targets in the Czech Republic might be carried out. Hence the Agency is issuing this warning in compliance with Section 12(1) of the Act on Cyber Security.

5. The Agency has the right to issue this warning under Section 22(b) of the Act on Cyber Security, which entitles it to issue measures. In line with Section 11(2) of the Act on Cyber Security, these measures also include warnings pursuant to Section 12 of the Act on Cyber Security. A warning is to be issued by the Agency pursuant to Section 12(1) of the Act on Cyber Security if it becomes aware of a cybersecurity threat through its activities or based on the instigation of the National CERT or bodies active in cybersecurity abroad. In compliance with Section 12(2) of the Act on Cyber Security, the Agency issues such warning on its website and notifies the bodies and entities mentioned in Section 3 of the Act on Cyber Security.

6. According to Section 22(j) of the Act on Cyber Security, the Agency is obliged to ensure prevention in the area of cybersecurity. These preventive actions also include the provision of information about identified cybersecurity threats. If a threat reaches such intensity that the Agency cannot provide sufficient information through its standard preventive activities, the Agency is obliged to issue a warning in line with the above and pursuant to Section 12 of the Act on Cyber Security.

7. The Agency notes that the bodies or entities obliged to adopt safety measures pursuant to the Act on Cyber Security are obliged to factor this warning into their risk management. Based on the above, the Agency considers the threat associated with the cyber attacks

mentioned in the statement of this warning to be probable to highly probable. The bodies and entities obliged to adopt safety measures pursuant to the Act on Cyber Security are therefore obliged to assess this threat at the respective level, i.e. at the level High.

Ing. Karel Řehka
Director
National Cyber and Information Security Agency
Electronic signature