National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky
Identification number : 05800226
Data box ID: zzfnkp3

File number:
350 - 302/2022
Reference number:
2384/2022-NÚKIB-E/350

Brno, 25 February 2022

WARNING

The National Cyber and Information Security Agency, with registered office at Mučednická 1125/31, 616 00 Brno (hereinafter referred to as the "Agency"), pursuant to Section 12(1) of Act No. 181/2014 Coll., on Cyber Security and on Amendments to Related Acts, as amended (hereinafter referred to as the "Cyber Security Act"), issues the following

warning

against a cyber security threat, consisting in the implementation of cyber attacks on information and communication systems in the Czech Republic, in particular on the public administration systems, but also other strategic organisations. These attacks can have an impact on the availability, confidentiality or integrity of information in important information and communication systems.

The Agency assesses this threat as Critical - The threat is very likely to almost certain.

Given the Critical threat of cyber espionage and other cyber attacks, the Agency recommends:

1. **Increased vigilance against the most commonly used attack techniques in cyberspace, which include, in particular:**
   - T1059 (Command and Scripting Interpreter),
   - T1218 (Signed Binary Proxy Execution),
   - T1543 (Create or Modify System Process),
   - T1053 (Scheduled Task/Job),
   - T1003 (OS Credential Dumping),
   - T1055 (Process Injection),
   - T1027 (Obfuscated Files or Information),
   - T1105 (Ingress Tool Transfer),
   - T1569 (System Services),
   - T1036 (Masquerading),
   - T1486 (Data Encrypted for Impact),
   - T1082 (System Information Discovery),
   - T1497 (Virtualization/Sandbox Evasion),
   - T1498 (Network Denial of Service),

- T1566 (Phishing),
- T1078 (Valid Accounts),
- T1190 (Exploit Public-Facing Application),
- T1133 (External Remote Services),
- T1595 (Active Scanning),
- T1110 (Brute Force),
- T1561 (Disk Wipe).

2. **Perform updates of information systems and their components where such updates are possible to ensure the continuity of operation in order to prevent the exploitation of known vulnerabilities in the following systems, which are currently in particular:**
   - CVE-2018-13379 in FortiGate VPN,
   - CVE-2019-1653 in Cisco,
   - CVE-2019-2725 in Oracle WebLogic Server,
   - CVE-2019-7609 in Kibana,
   - CVE-2019-9670 in Zimbra,
   - CVE-2019-10149 in Exim Simple Mail Transfer Protocol,
   - CVE-2019-11510 in Pulse Secure,
   - CVE-2019-19781 in Citrix,
   - CVE-2020-0688 in Microsoft Exchange,
   - CVE-2020-4006 in VMware One Access and Identity Manager,
   - CVE-2020-5902 in F5 Big-IP,
   - CVE-2020-14882 in Oracle WebLogic,
   - CVE-2021-26855 in Microsoft Exchange,
   - CVE-2021-44228 in Apache Log4j.

3. **In response to the threat of distributed denial of service (DDoS) attacks, the Agency recommends the following:**

   3.1. **Preventive measures recommended to all organisations (prior to a DDoS attack)**
   - Investigate options for blocking unwanted traffic that overwhelms or otherwise restricts the operation of systems on the edge infrastructure element.
   - Identify and have the ISP contact details ready. Verify the contact persons in the organization who have the ability and authority to contact the ISP and arrange with the ISP for an alternate communication channel (ideally one off-line and one online) should their line become congested. Have the identification data of the subscribed services ready (contract number, etc.).
   - Contact the ISP to determine options for blocking unwanted traffic that overwhelms or otherwise restricts the system on the ISP's side, if these options are not known to the organisation (e.g. FlowSpec, RTBH or on request).
   - Prepare a strategy and, if necessary, configurations of elements for extreme situations to ensure controlled limitation of availability of non-essential services and maximum preservation of availability of essential services.
   - Verify the possibility of operating the system in an island mode (i.e. without Internet connection or with limited availability, e.g. outside the Czech Republic).

- Prepare for the possibility of blocking IP addresses, IP ranges or IP addresses according to the Autonomous System Number (ASN) published on the Agency's website. Block traffic according to any published indicators (the Agency will provide this information in a machine-readable format).
- Prepare for the need to block the translation of certain domains in DNS (e.g. in a DNS resolver).
- Prepare a communication strategy and communication channels (e.g. social networks) to inform the public in case of unavailability of the services provided.
- Monitor the NÚKIB website for possible further warnings or recommendations.

3.2. **Recommended actions for all organisations in the event of an ongoing DDoS attack**

- Block unwanted traffic before line congestion between the ISP and the edge element, even at the cost of blocking legitimate traffic (GeoBlocking, ASN-based blocking).
- In the event of line congestion, contact the ISP and coordinate efforts to resolve the congestion with the ISP.
- Immediately contact the Agency and report the extent of the service limitation, including the type of unwanted traffic and the IP addresses from which it originated.

3.3. **Preventive measures recommended to ISPs (prior to a DDoS attack)**

- Investigate options for blocking unwanted traffic that overwhelms or otherwise restricts the operation of systems.
- Prepare for blocking unwanted traffic for the case of customer requests, i.e. automate the blocking process as much as possible (prepare RTBH for BGP customers and communicate this option to them).
- If possible and efficient, consult and prepare with partners the possibility to provide blocking of unwanted traffic already in upstream networks, for example by using Remotely Triggered Black Hole (RTBH) technology.
- Prepare for the possibility of blocking IP addresses, IP ranges or Autonomous System Numbers (ASNs) published on the Agency's website. Block traffic according to any published indicators (the Agency will provide this information in a machine-readable format).
- Backup critical network device configurations and maintain them in a 3-2-1 backup mode (3 copies, 2 different media, 1 off-site backup) and ensure their integrity (checksums, version change tracking).
- Implement active monitoring of configuration changes.
- Carry out a physical inventory check of spare critical components (e.g. routers, switches, etc.), ensuring availability of these components when needed.
- Check that Disaster Recovery reminders are up to date and train staff to remind them.
- Ensure that all links have sufficient reserve transmission capacity.
- Prepare infrastructure monitoring for attack direction detection, e.g. MAC address monitoring to determine which direction (peer) the DDoS attack is coming from.
- Monitor the NÚKIB website for possible further warnings or recommendations.

3.4. **Recommended actions for ISPs in the event of an ongoing DDoS attack**

- Block unwanted traffic based on customer requests.

- Prioritise blocking of unwanted traffic directed at critical information infrastructure systems, essential services information systems and critical information systems.
- Immediately contact the Agency to report the extent of service limitation, including the type of unwanted traffic and the IP addresses from which it originated.

4. **Monitor the NÚKIB website for possible further alerts, recommendations or warnings.**

RATIONALE

1. Based on the facts established in the exercise of its competence, as well as the facts that the Agency has learned from authorities exercising competence in the field of cyber security abroad and domestic partners, the Agency has concluded that there is a threat in the field of cyber security associated with the possibility of serious cyber attacks on information and communication systems in the Czech Republic. This threat is associated with the armed conflict between the Russian Federation and Ukraine and is directed at multiple targets in the Czech Republic. A higher level of this threat can be expected especially for strategic public administration institutions (significant information systems), elements of critical information infrastructure, information systems of essential services or media. However, other domestic organisations may also be at risk.
2. The Agency monitors and analyses threats and risks in the field of cyber security as part of its activities under Section 22(u) of the Cybersecurity Act, as well as draws on input from partners. As part of this activity, the Agency has received information that attackers who have carried out cyber attacks on Ukrainian infrastructure and strategic organisations could also target organisations in the Czech Republic.
3. Based on the above, the Agency has already published two recommendations on securing domestic systems on 17 January 2022 and 28 January 2022. This warning thus follows on the earlier issued recommendations.
4. Based on historical data, its own above mentioned threat and risk analyses, and input from partners, the Agency identified 14 tactics, techniques, and procedures (TTPs) (hereafter referred to as "Techniques") according to the MITRE ATT&CK platform that were most frequently encountered between 2020 and 2021. In addition, 7 Techniques frequently used by malicious stakeholders in cyberspace were identified. Information about these can be used to increase an organization's resilience to cyber attacks carried out using these Techniques, as the Agency also recommends in this warning.
5. The links below for each Technique refer to recommendations for mitigating potential attacks using that particular Technique. The Agency recommends that the Techniques and corresponding mitigation processes be addressed to enhance the resilience of one's regulated ICSs.

Technique	Information
T1059 (Command and Scripting Interpreter)	Command line abuse to execute malicious code.
T1218 (Signed Binary Proxy Execution)	Legitimate binaries abuse to execute malicious code by proxy.

T1543 (Create or Modify System Process)	Abuse of the ability to create or modify operating system-level processes to re-execute malicious code.
T1053 (Scheduled Task/Job)	Abuse of task scheduling to initially or repeatedly execute malicious code.
T1003 (OS Credential Dumping)	Attempt to dump login credentials to gain access to the OS account and installed software.
T1055 (Process Injection)	Insertion of malicious code into a legitimate process, especially to avoid detection by security tools.
T1027 (Obfuscated Files or Information)	An attempt to make detection or analysis of a malicious file more difficult by obfuscation (e.g., encryption or password protection).
T1105 (Ingress Tool Transfer)	The transfer of tools or other files by an attacker from an external system to a compromised system.
T1569 (System Services)	Abuse of legitimate system services or daemons to execute malicious code or program.
T1036 (Masquerading)	An attempt to modify malicious code and files so that security tools consider them legitimate or harmless.
T1486 (Data Encrypted for Impact)	Encrypting data in the target system.
T1082 (System Information Discovery)	Attempt to obtain detailed OS and hardware information.
T1497 (Virtualization/Sandbox Evasion)	Means used to detect and evade a virtualization or analysis environment.
T1566 (Phishing)	Phishing emails that may contain a malicious attachment in the form of a link or attached document.
T1498 (Network Denial of Service)	Congestion on networks on which service delivery is dependent.
T1078 (Valid Accounts)	Abuse of legitimate user accounts compromised by an attacker (e.g., knowledge or theft of login credentials).
T1190 (Exploit Public-Facing Application)	Exploitation of vulnerabilities in applications or programs accessible from the Internet.
T1133 (External Remote Services)	Exploiting remote services (e.g. VPN) to gain initial access.
T1595 (Active Scanning)	Active scanning of IP ranges and potentially vulnerable systems.
T1110 (Brute Force)	Using brute force to gain access to accounts for which passwords are unknown or their hashes are obtained.
T1561 (Disk Wipe)	Blocking the operating system by deleting or corrupting data.

6. Based on historical data, its own above described threat and risk analyses, and input from partners, the Agency also identified the 14 most common vulnerabilities exploited by stakeholders who have carried out attacks on Ukrainian infrastructure and strategic organisations. In relation to these vulnerabilities, the Agency recommends to verify the presence of the listed systems in the infrastructure, to verify their update status and, where appropriate, to update these systems to address the known vulnerabilities listed below.

Vulnerability	Vulnerable system
CVE-2018-13379	FortiGate VPN
CVE-2019-1653	Cisco Small Business RV320 a RV325
CVE-2019-2725	Oracle WebLogic Server
CVE-2019-7609	Kibana
CVE-2019-9670	Zimbra
CVE-2019-10149	Exim Simple Mail Transfer Protocol
CVE-2019-11510	Pulse Secure
CVE-2019-19781	Citrix
CVE-2020-0688	Microsoft Exchange
CVE-2020-4006	VMware One Access and Identity Manager
CVE-2020-5902	F5 Big-IP
CVE-2020-14882	Oracle WebLogic
CVE-2021-26855	Microsoft Exchange
CVE-2021-44228	Apache Log4j

7. In response to the specific threat of Distributed Denial of Service (DDoS) attacks, the Agency has decided to recommend specific measures to help organisations mitigate the impact of cyber security incidents in relation to potential attacks. The measures recommended in sections 3.1 and 3.2 are universally applicable by any organization, either as a precautionary measure prior to an attack (3.1) or during an ongoing attack (3.2). The recommendations contained in 3.3 and 3.4 are then specifically addressed to ISPs.
8. Further alerts, recommendations or warnings may be published on the Agency's website at the following links:
    - https://www.nukib.cz/cs/infoservis/hrozby/
    - https://www.nukib.cz/cs/infoservis/doporuceni/
    - https://www.nukib.cz/cs/uredni-deska/

9. The above-mentioned facts in their totality give rise to a reasonable concern of a threat of serious cyber attacks on significant targets in the Czech Republic, and therefore the Agency issues this warning pursuant to Section 12(1) of the Cyber Security Act.
10. The Agency's authority to issue this warning is given by the provisions of 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 or on the initiative of the operator of a national CERT or from authorities exercising cyber security activities abroad. In accordance with Section 12(2) of the Cyber Security Act, the Agency shall publish such a warning on its website and notify it to the authorities and persons referred to in Section 3 of the Cyber Security Act.

11. The Agency is tasked with the prevention of cyber security pursuant to Section 22(j) of the Cyber Security Act. This preventive activity also includes the provision of information on identified cyber security threats. However, if the threat reaches such an intensity that information about it cannot be covered by the Agency's normal prevention activities, the Agency is obliged to issue a warning pursuant to Section 12 of the Cyber Security Act in accordance with the above.
12. The Agency points out that authorities or persons which are obliged to implement security measures pursuant to the Cyber Security Act shall, in the context of risk management pursuant to Section 5(1)(h)(3) of the Cyber Security Decree, take into account the measures pursuant to Section 11 of the Cyber Security Act in their risk assessment and risk management plan. 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 stated herein to be highly probable to almost certain. 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 Critical level. 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 pursuant to Article 5(1)(d) of the Cyber Security Decree.

Karel Řehka
Director
National Cyber and Information Security Agency