Abuse (responsible scanning) Policy

1. Introduction

One of the main areas of activity of the Joint Stock Company "Cyber OK" (hereinafter referred to as the Company or we) involves searching for vulnerabilities in infrastructures, systems, and software. In the course of our work, we may detect vulnerabilities of varying threat levels, including critical ones.

In our work, we adhere to the following principles:

- we care about information security and do not use the vulnerability information we obtain unlawfully;
- we make significant efforts to secure the digital component of our society, ensuring transparency and availability of information about exposed and potentially vulnerable resources;
- we adhere to a responsible disclosure policy and always notify vendors of the finding vulnerabilities free of charge.

Our scanning actions on Internet devices are regulated by this document, which explains how and why we conduct scanning.

2. Scanning methodology

2.1. During scanning, we use tools that:

- devices connected to the Internet, their types, and characteristics (e.g., used ports, software versions);
- SSL certificates and their associations with specific IP addresses or domains.

2.2. Scanning frequency: IP addresses and domains are scanned no more frequently than once a day.

2.3. Scanning objectives: identifying open ports, outdated or vulnerable software, and other potential security threats.

2.4. IP addresses from which scanning is carried out be checked by PTR (Reverse DNS) records scan-[dd].skipa.cyberok.ru where dd — digits from 00 to 300. You can check their ownership using a reverse DNS query with ping -a [IP], host [IP], or dig [IP]. At the moment, all the used IP addresses belong to the 85.142.100.0/24 network.

2.5. During our scanning procedures, we also utilize the SKIPA software — the Attack Surface Control and Information System (hereinafter referred to as SKIPA), developed in-house. SKIPA falls under the category of "Threat Detection and Network Incident Investigation Tools" software, serving as an attack surface management (ASM) system encompassing network security monitoring and analysis mechanisms. While the operation of such software may trigger defense mechanisms, it is not considered malicious software.

The fact that SKIPA is not malicious software is further confirmed by the following:

- on September 15, 2023, it was registered in the Unified Register of Russian Programs for Electronic Computers and Databases (hereinafter referred to as Registry) under registration number 18867. During registration, each instance of the software undergoes comprehensive scrutiny by experts from the Ministry of Digital Development, Communications, and Mass Media of the Russian Federation. You can review the information about SKIPA from the Registry here: https://reestr.digital.gov.ru/reestr/1765596/?sphrase_id=4356720;
- on May 10, 2023, it was registered in the registry of computer programs by the Federal Service for Intellectual Property, Patents and Trademarks, evidenced by the issuance of Certificate of State Registration of Computer Program No. 2023619366.

3. Exclusions from the scanning list

If you wish to exclude your resources from our scanning list, you can:

- independently block access from the IP addresses from which we conduct scanning;
- write to us at abuse@cyberok.ru, specifying the relevant IP addresses or domains.

4. Incident response procedure

If you detect activity from the Company that causes concerns, please contact us immediately at: abuse@cyberok.ru. We guarantee prompt consideration of all requests and the implementation of necessary measures.

5. Contacts

For general inquiries, please contact us at info@cyberok.ru.

6. Confidentiality assurance

The discovered information is used exclusively for research and analytical purposes. No personal data or confidential information is processed or transferred to third parties. If we inadvertently access personal data during scanning, it will be promptly deleted. The data obtained from scanning are stored in encrypted form, and access to it is role-based, meaning only authorized employees have access.

7. Conclusion

Based on this policy, we make every effort to ensure the safety and reliability of the internet space, interacting with the community on principles of openness and transparency.