www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Abuse (responsible scanning) Policy

1. Introduction

One of the key areas of activity of the Joint Stock Company "Cyber OK" (the "Company", "we") is piloting technologies for digital resilience auditing and checking the correctness of security-related configurations for website certificates, DNS, and mail servers.
In our work, we follow these principles:

- we support digital resilience and do not use any information obtained by us for unlawful purposes;
- we make significant efforts to improve the safety of the digital environment by ensuring transparency and availability of information about exposed and potentially unsafe resources;
- we follow a responsible disclosure approach.

All of our activities related to analyzing Internet-facing devices are governed by this document, which explains how and why we perform such analysis.

2. Analysis methodology

During analysis, we use tools that identify:

- devices connected to the Internet, their types and characteristics (for example, open ports and software versions);
- SSL certificates and their association with specific IP addresses or domains.

Analysis frequency: IP addresses and domains are analyzed no more than once per day.
Analysis objectives: piloting digital resilience audit technologies and verifying the correctness of security-related configurations for website certificates, DNS, and mail servers.
The IP addresses from which analysis is performed have DNS names of the form scan-[dd].skipa.cyberok.ru, where dd ranges from 00 to 300. You can verify their association using a reverse DNS query: ping -a [IP], host [IP], or dig [IP]. At present, all IP addresses used belong to the 85.142.100.0/24 network.
When performing analysis, we also use SKIPA software — the Attack Surface Control and Information System ("SKIPA"), developed in-house. SKIPA is software in the class of "tools for detection and investigation of network incidents", serves as an attack surface management (ASM) system, and includes mechanisms for network monitoring and security configuration analysis.
SKIPA software:

- On 05 September 2023, it was registered in the Unified Register of Russian Programs for Electronic Computers and Databases (the "Registry") under registration number 18867. During registration, each software instance undergoes comprehensive review by experts of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation. Information from the Registry about SKIPA is available here: https://reestr.digital.gov.ru/reestr/1765596/?sphrase_id=4356720.
- On 10 May 2023, it was registered as a computer program by the Federal Service for Intellectual Property, Patents and Trademarks, as evidenced by Certificate of State Registration of Computer Program No. 2023619366.

3. Exclusions from the analysis list

If you would like to exclude your resources from our analysis list, you may:

- independently block access from the IP addresses from which we perform analysis;
- contact us at abuse@cyberok.ru and specify the relevant IP addresses or domains.

4. Incident response procedure

If you notice activity originating from the Company that raises any questions, please contact us immediately at: abuse@cyberok.ru. We guarantee prompt review of all requests and the implementation of necessary measures.

5. Contacts

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

6. Confidentiality assurance

Any information identified is used exclusively for research and analytical purposes.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

No personal data or confidential information is processed or transferred to third parties.

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 the principles of openness and transparency.