INFORMATION SECURITY

ENSURING CYBERSECURITY IN THE DIGITAL AGE: ROLE AND RESPONSIBILITY OF THE FUND

Information security is an integral part of stable operation of the information network, protection of national interests and maintenance of trust from the society and partners. With the development of digital technologies, Samruk-Kazyna JSC and the Fund group of companies, constantly increases the level of information security to prevent cyber threats, as well as brings the requirements in the field of information security in accordance with legislative norms.

The key strategic goals of the Fund in this area are — ensuring availability, integrity, confidentiality and fault tolerance.

CREATING A CULTURE OF SAFETY

As part of strengthening information security, the Fund started to implement the international standard ISO 27001. According to the order of the Chairman of the Board of Directors of the Fund, a working group was organized to create a register of information assets and classify them by level of importance.

This classification provides for division into the following categories:

Information:

- Special information asset;
- Strategic information asset;
- Protected information asset;
- Basic information asset.

Personnel. An access hierarchy has been introduced, defining different levels of access for employees depending on their role and responsibility.

Physical infrastructure. Work was carried out to protect information at the physical and logical levels in the IT infrastructure.

Training. Training sessions and testing using specialized software are conducted to develop cyber hygiene skills among the Fund's employees.

CREATING EFFECTIVE INFORMATION SECURITY POLICIES

The Fund has implemented the "Basic Rules of Information Security Policy" with annexes in the form of methods, guidelines and rules that regulate the activities of information security (IS) and information technology (IT) specialists, as well as all employees with regard to the implementation of information security measures.

Work is underway to develop a Corporate Information Security Standard regulating a common set of rules for ensuring information security and managing the process of coordination of activities in the Fund group of companies.

CRITICAL INFRASTRUCTURE PROTECTION

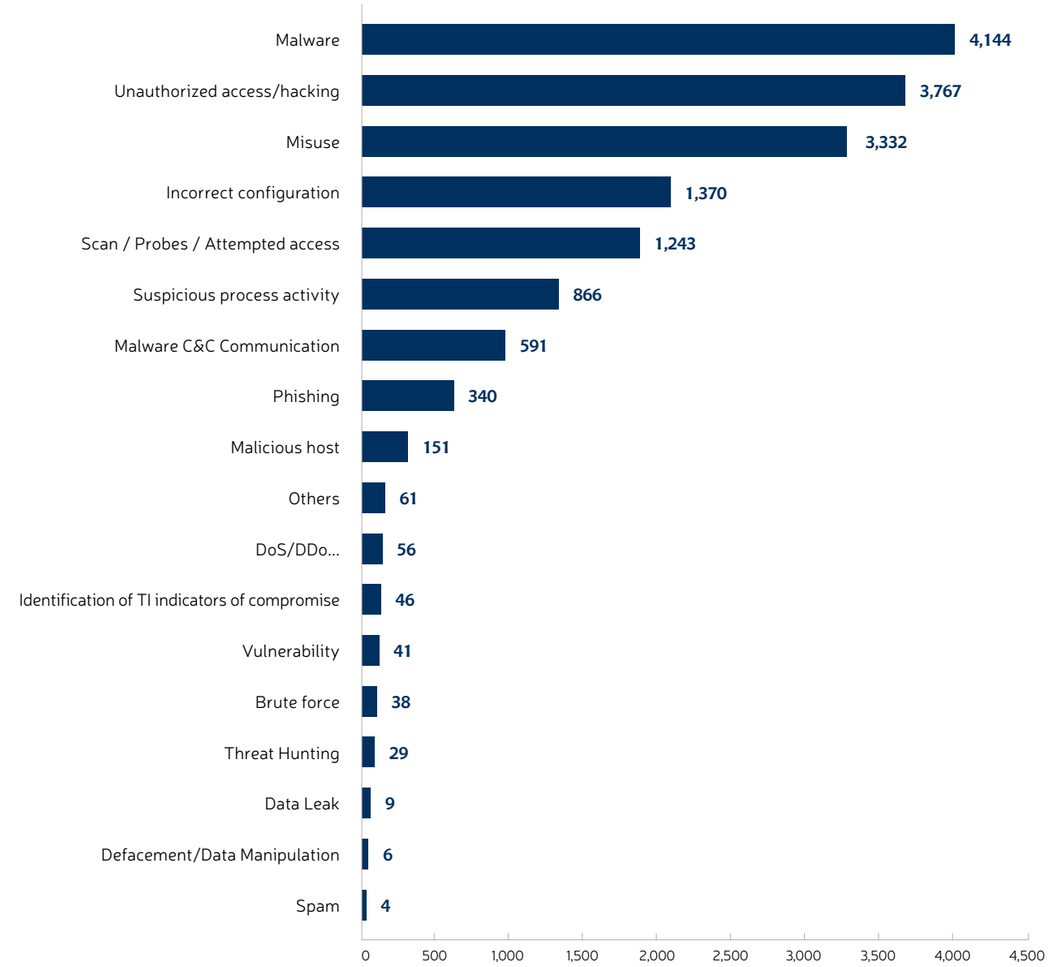
- Technical work was carried out to bring the IT infrastructure into compliance.
- Optimization of the information security products used was carried out, modern software products were introduced for monitoring, preventing information leakage, scanning and obtaining operational information on vulnerabilities.

COUNTERING CYBERATTACKS

- A monitoring center was established in the conditions of the Fund to maintain information security systems and promptly respond to external and internal threats to the IT infrastructure.
- Audit (pentest) of the external infrastructure was conducted. The identified vulnerabilities were timely eliminated by the Fund's technical specialists.

In 2023, audits of the Fund's portfolio companies for compliance with information security requirements were conducted, and recommendations to improve the level of information security were developed based on the results. A register of cybersecurity risks and quarterly risk reports, including those related to the companies of the Fund group, are prepared annually.

INCIDENT STATISTICS BY THREAT TYPES FOR 2023 IN THE FUND GROUP



INCIDENT STATISTICS FOR 2023 BY FUND GROUP