



Bank of Russia

OVERVIEW OF THE MAIN TYPES
OF CYBERATTACKS IN
THE FINANCIAL SECTOR
IN 2025

CONTENTS

1. Data sources	2
2. Cyber threat landscape analysis	4
2.1. Most frequent victims and attack tools	4
2.2. Attack vectors	5
2.3. Typical cybersecurity incident scheme.....	11
3. Cyber drills.....	17
4. 2026 trends	18

This overview was prepared by the Information Security Department.
The reference to the Bank of Russia is mandatory if you intend to use this document.

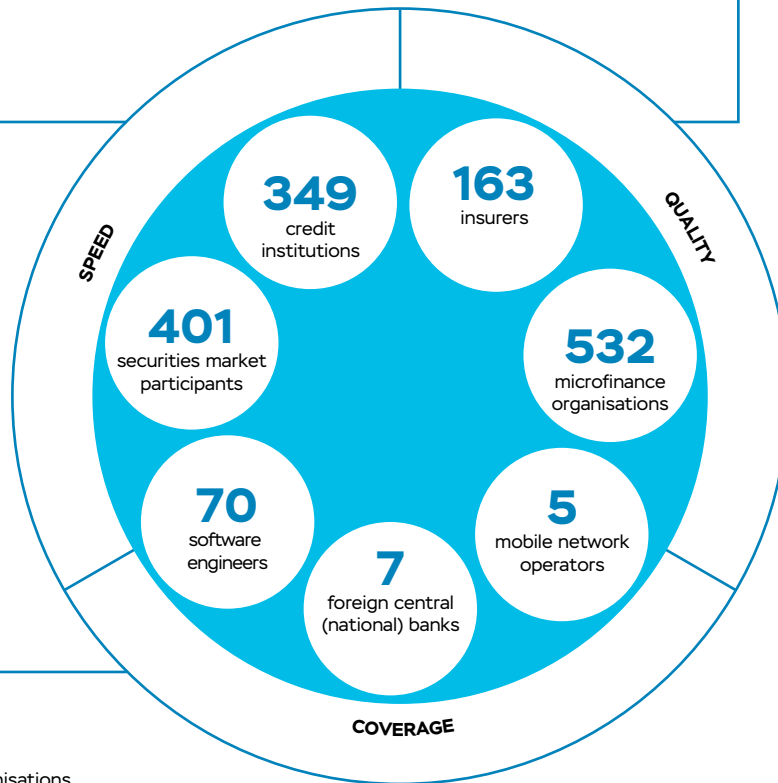
Bldg V, 12 Neglinnaya Street, Moscow, 107016
Bank of Russia website: www.cbr.ru

© Central Bank of the Russian Federation 2026

1. DATA SOURCES

Financial CERT responds to a cybersecurity incident in financial market within one hour*

Information exchange participants' score of quality of Financial CERT's data is 8.4 out of 10**



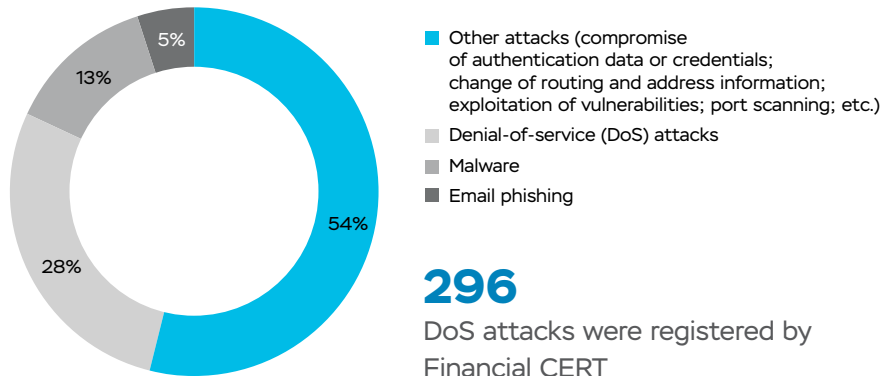
- Participants:
- Over 1,700 organisations
- Detected:
- 38,418 phishing websites (sent for blocking)
 - 761 operational incidents
 - 14 incidents at contractors with further attacks on financial institutions

* Time needed for Financial CERT's operator to process the request received.

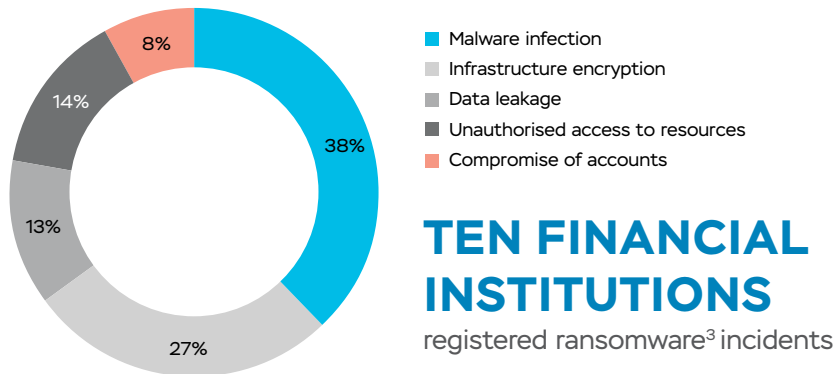
** According to the survey of financial market participants conducted in 2025.

Breakdown of cyberattacks¹ and cybersecurity incidents² at financial institutions in 2025 (according to Financial CERT)

Cyberattacks, by type



Cybersecurity incidents, by type



¹ A cyberattack is an intentional exploitation of software and/or hardware with the purpose of compromising critical information infrastructures and telecommunications networks used for communication between these infrastructures with the aim to disrupt and/or disable them and/or to create a threat to the security of information this infrastructures process.

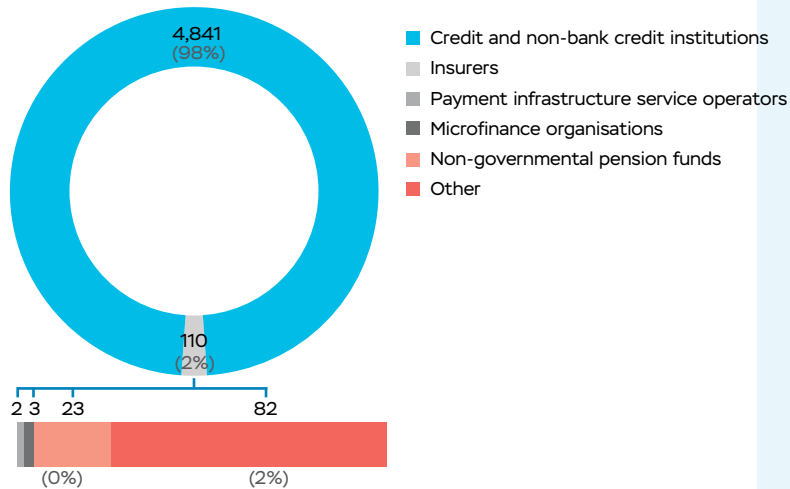
² A cybersecurity incident is an occurrence that disrupts and/or disables a critical information infrastructure or a telecommunications network used for communication between such infrastructures and/or jeopardises the security of information this infrastructure processes, including as a result of a cyberattack.

³ Ransomware is malicious software (malware) that blocks access to a user's files by encryption.

2. CYBER THREAT LANDSCAPE ANALYSIS

2.1. Most frequent victims and attack tools

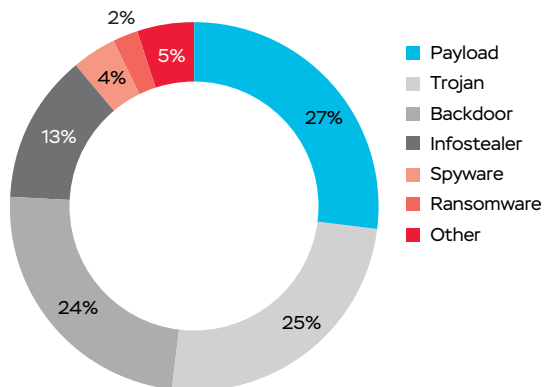
Number of attacks, by organisation type



FOCUS ON SMALL AND MEDIUM-SIZED IT PROVIDERS

Attacking smaller businesses, malefactors thus save time and resources expecting to further on obtain access to the infrastructure of a large organisation if the latter has communicated with the compromised contractor.

Malware used in 2025, by type



GROWING NUMBER OF RASS (RANSOMWARE AS A SERVICE) ATTACKS

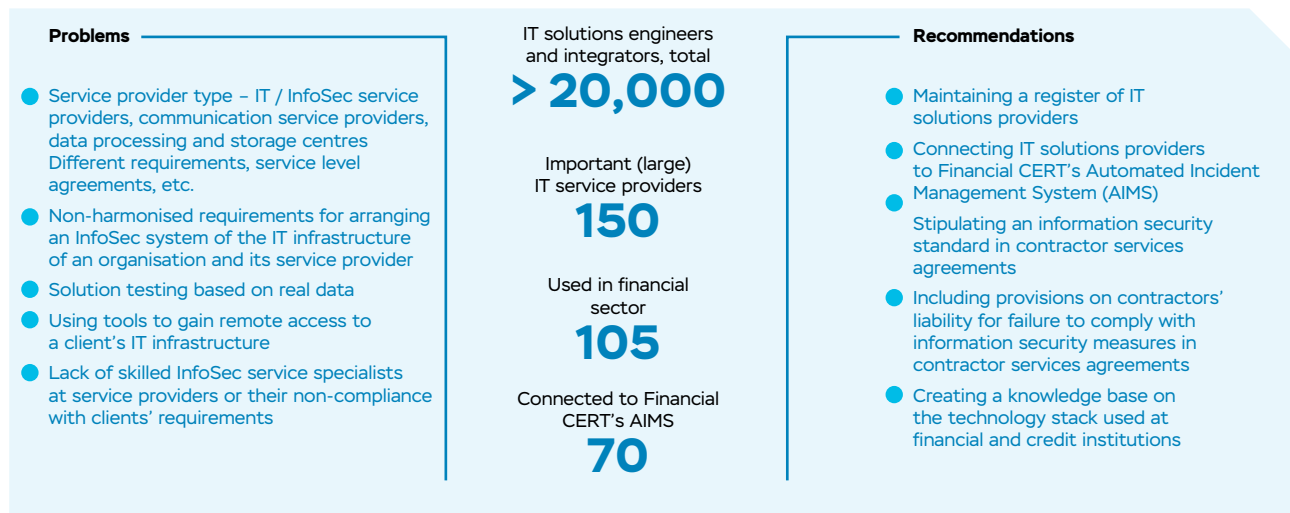
Attackers can modify available tools to fit their needs or rent them.

2.2. Attack vectors⁴

2.2.1. Contractors – IT / InfoSec service providers, communication providers, data processing and storage centres

In 2025, the number of targeted attacks on financial institutions remained persistently high. Moreover, the year 2025 saw an increased number of attacks against more vulnerable IT infrastructures of contractors and service providers offering a wide range of services for optimising financial institutions' technological activities and operations or providing support services through remote access tools. In such conditions, credit institutions accept the risk of a possible cyberattack on their infrastructures via contractors. Therefore, it is crucial for financial institutions to thoroughly analyse the models of threats arising from such interaction, adjust the parameters of risk-based contractor management, and implement adequate organisational and technical measures to counter such threats.

Compliance with recommendations for organising business relations with service providers mitigates the risks of attacks via contractors



⁴ An attack vector is a pathway used by attackers to hack a victim's information infrastructure, breach a security system, and gain unauthorised access.

2.2.2. Analysis of software vulnerabilities based on international data

In 2025, using software vulnerabilities was an initial vector of attacks against the financial sector and other industries.

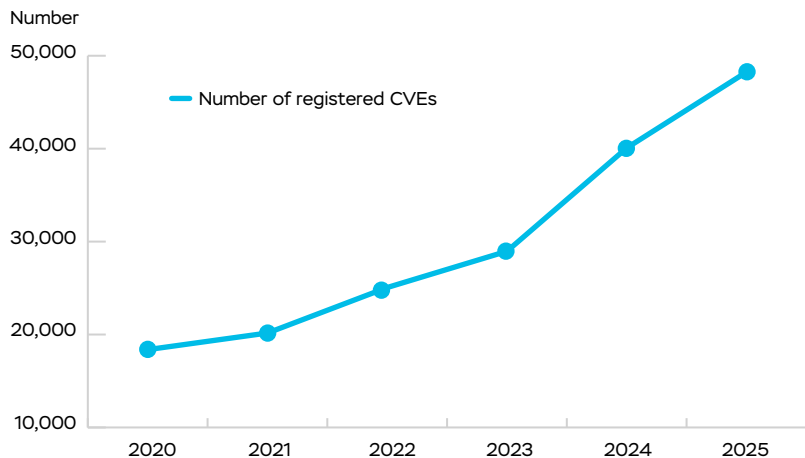
According to the data available to Financial CERT, the point of entry into organisations' infrastructures in most cybersecurity incidents was Bitrix vulnerabilities identified back in 2023.

The trend and attempts of attacks through 1C-Bitrix software continue. Financial CERT's extensive efforts to inform financial market participants about 1C-Bitrix vulnerabilities helped significantly reduce the number of related incidents. Nevertheless, credit and financial institutions registered 1C-Bitrix vulnerability exploitation incidents in 2025.

Financial CERT regularly releases up-to-date information on software vulnerabilities existing and exploited in the credit and financial sector and publishes its weekly digests and bulletins to notify market participants about possible exploitation of these vulnerabilities by attackers.

By promptly processing the data received from Financial CERT and taking appropriate response measures, information exchange participants are able to quickly counter cybersecurity threats and prevent potential cybersecurity incidents.

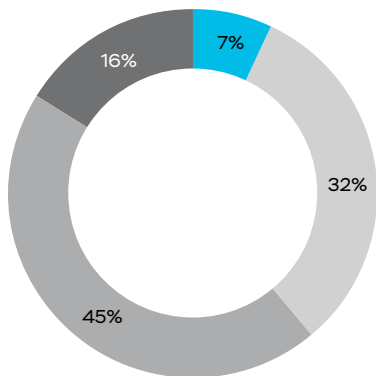
Global growth in CVEs in 2025

**+20%**

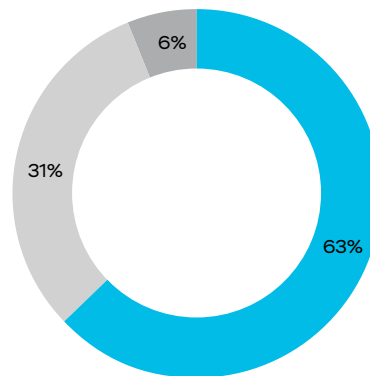
vs 2024

**OVER
48,000**

CVEs in 2025

CVE severity score according
to CVSS in 2025

- Critical (9.0–10.0)
- High (7.0–8.9)
- Medium (4.0–6.9)
- Low / None (<4.0)

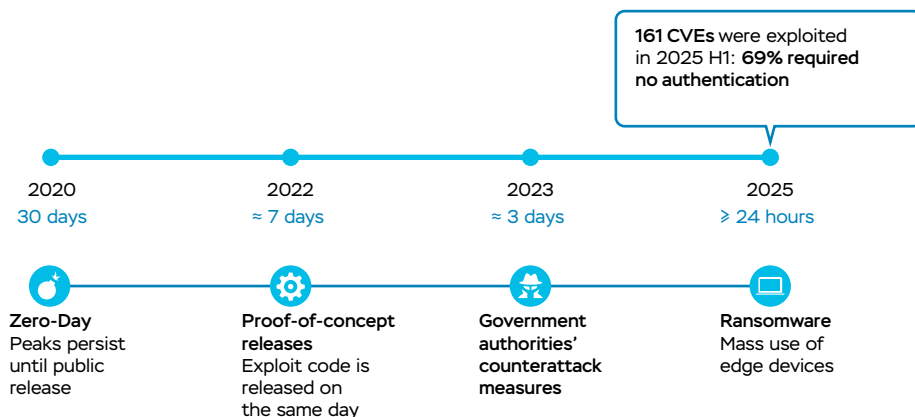
Breakdown of vulnerabilities
in 2025, by vendor

- Microsoft OS and software
- 7-Zip and WinRAR file archivers
- 1C-Bitrix software

In 2025, the largest number of attacks against the financial sector through software vulnerabilities was recorded in the following groups of software vendors:

1. **CVE-2025-24071** allows unauthenticated attackers to steal NTLM hashes.
2. **CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, and CVE-2025-53771** identified in Microsoft SharePoint involve deserialisation of untrusted data.
3. **CVE-2024-35250** allows attackers to dereference an untrusted pointer and execute an arbitrary code.
4. **CVE-2020-1472 (Zerologon)** allows attackers to compromise a domain controller's computer account and gain control over the entire Active Directory domain.
5. **CVE-2017-11882 and CVE-2018-0802** affect the Equation Editor component in Microsoft Office.
6. **CVE-2017-0199** is a vulnerability in Microsoft Office and WordPad.
7. **CVE-2023-38831, CVE-2025-6218, and CVE-2025-8088** are WinRAR directory traversal vulnerabilities.
8. **CVE-2025-11001 and CVE-2025-11002** are vulnerabilities in the 7-Zip file archiver that lie in the improper handling of symbolic links in ZIP files.
9. **CVE-2022-27228** is a critical vulnerability in CMS 1C-Bitrix.

Reduction in the time of detection and exploitation of zero-day vulnerabilities by attackers



Reduction in the time of exploitation – attackers now transform new vulnerabilities into a tool for attacks within several hours after public release.

24 HOURS

In early 2025, around 28% of all registered attacks through exploitation of vulnerabilities were committed within 24 hours after their identification. This means that by the moment when a vendor issues a patch for a vulnerability or releases a notice thereof, malefactors have already started scanning and compromising unprotected systems.

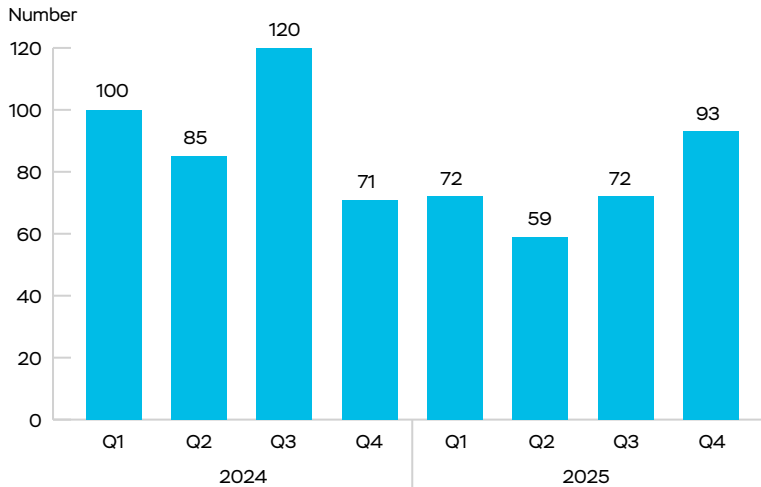
ATTACKERS USED OVER 160 VULNERABILITIES IN 2025 H1

Those were both new zero-day vulnerabilities and older errors that vendors had failed to patch. For about 42% of exploited CVEs, there were either publicly available exploits or proof-of-concept (PoC) exploits, which considerably reduced the time needed for large-scale attacks.

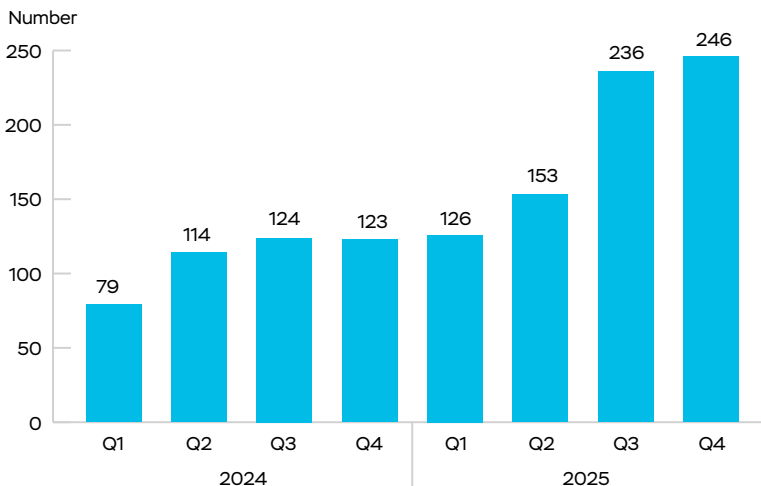
Moreover, 69% of exploited vulnerabilities required no authentication, e.g. any internet user could exploit them remotely, and nearly 30% of them allowed remote code execution (RCE).

2.2.3. DDoS attacks

Dynamics of DDoS attacks



Dynamics of operational incidents



296 DDoS ATTACKS

were committed in 2025, which is 21% less than in 2024

EVERY NINTH DDoS ATTACK

caused an operational incident (36 operational incidents stemmed from DDoS attacks)

FOUR DAYS – period when a financial institution's services were unavailable as a result of a DDoS attack

DISRUPTIONS OF ACCESS TO SERVICES, INCLUDING DDoS

1,717

detected events supposedly related to disruptions

963

confirmed disruptions

761

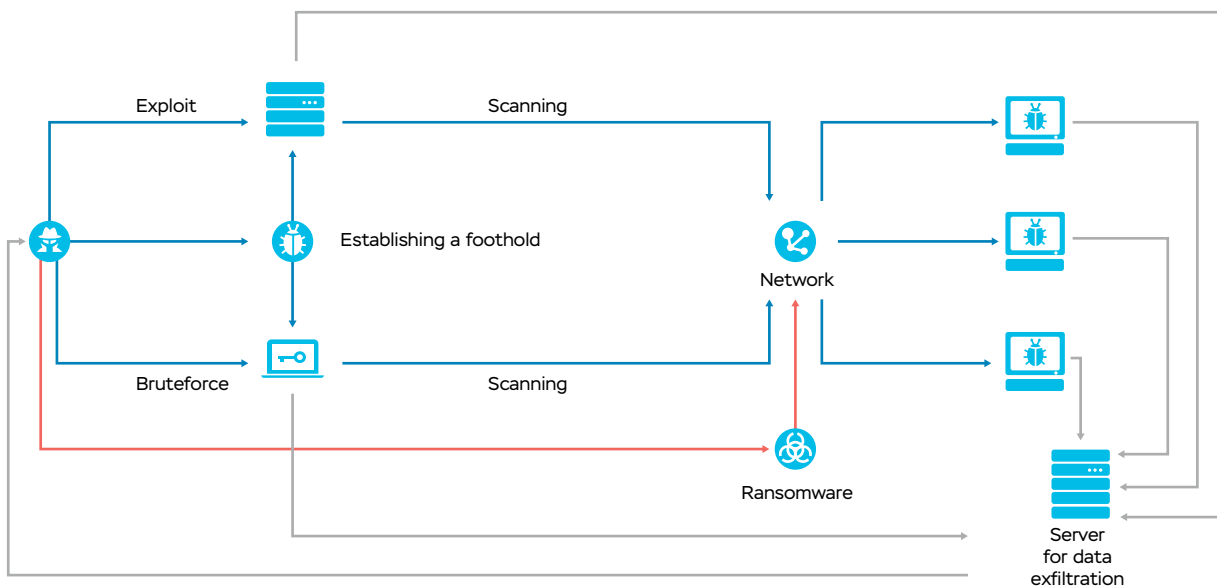
operational incidents

166

days – total duration of operational incidents identified in 2025

2.3. Typical cybersecurity incident scheme

In 2024, attacks were multi-vector and sophisticated, while in 2025, the scheme of a typical attack on an organisation was as follows:



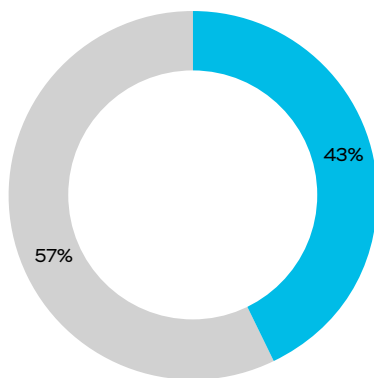
1. Gaining initial access through exploiting a vulnerability / brute force attack.
2. Establishing a foothold in the target infrastructure by adding a process to startup / creating a tunnel.
3. Collecting information about the infrastructure and available data.
4. Lateral movement (where possible).
5. Data exfiltration.
6. Infrastructure encryption.

Cyberattackers were increasingly using red team⁵ software, as well as publicly available vulnerability detection software and operating system utilities, while moving away from developing their own malware.

Furthermore, no new types of ransomware families used to attack the financial sector were detected in 2025. However, there was a considerable number of registered attacks using ransomware with publicly available source codes.

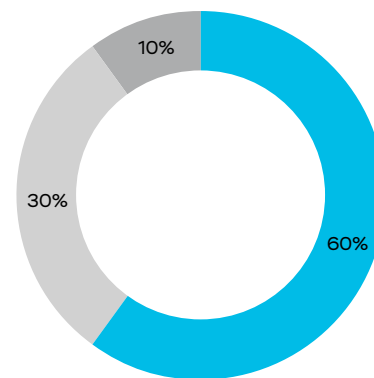
2.3.1. Ransomware

Incidents in 2025



■ Ransomware
■ Other

Ransomware detected as part of incident response measures in 2025



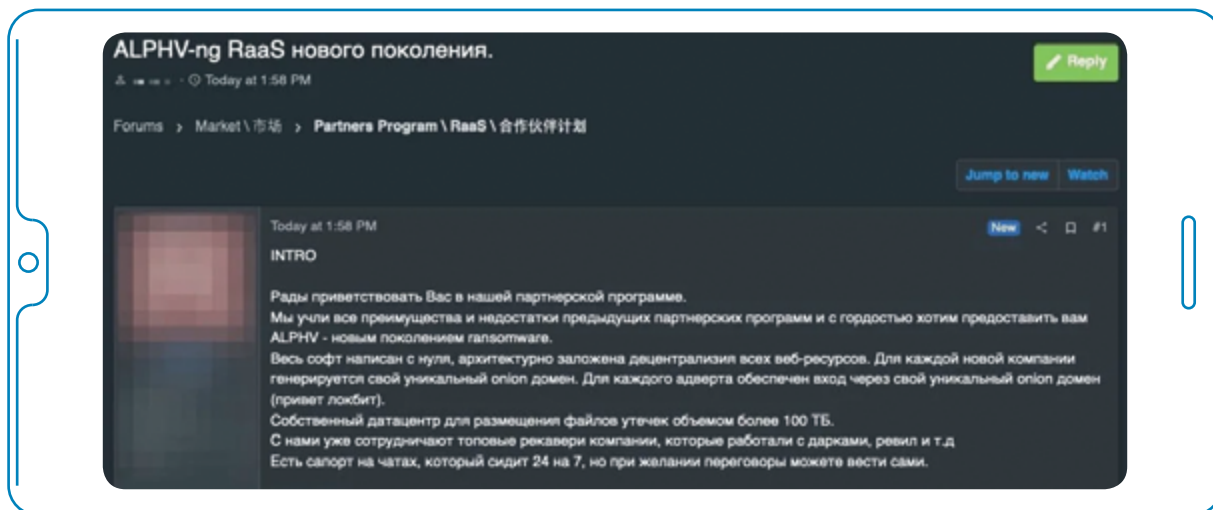
■ Babuk
■ Lockbit
■ Other

⁵ A red team is a group of cybersecurity experts that simulates real, covert, and multi-stage attacks on a company's infrastructure to test its defences.

Based on information available to Financial CERT, in 2025, the Bank of Russia recorded a larger number of incidents at financial institutions, causing infrastructure encryption.

Previously, attackers wanted to receive a ransom, whereas closer to the end of 2025, they were seeking to damage organisations' infrastructures as much as possible.

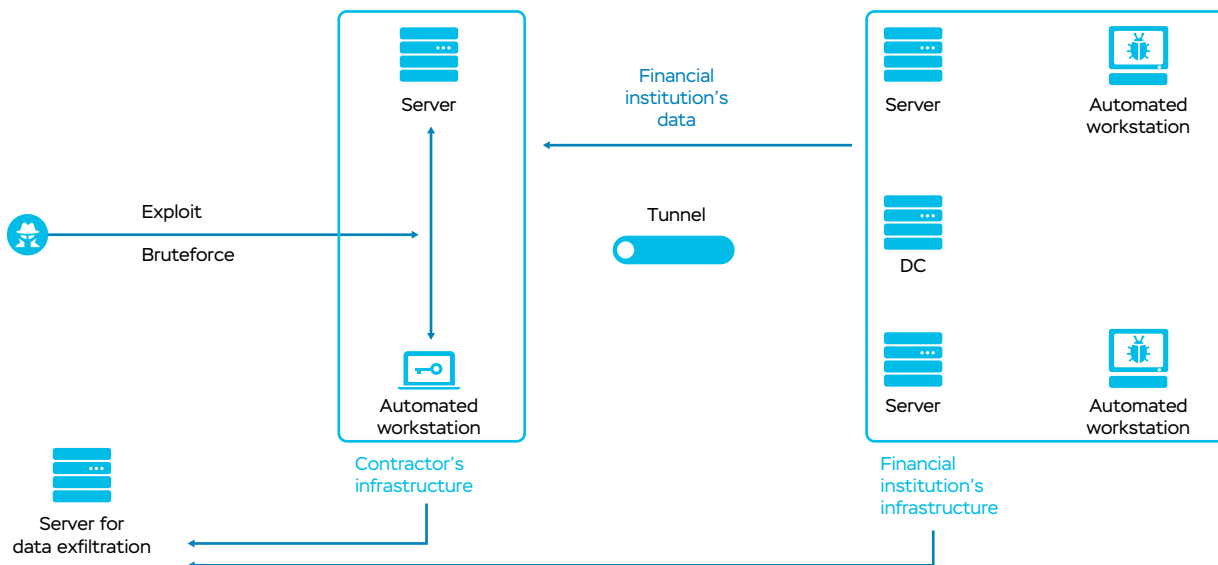
A growing number of incidents may be attributable to the rising popularity of the RaaS model in the darknet and, as was reported by Financial CERT in its overview of cyberattacks on the financial sector in 2024, to the leaked source codes of the Babuk⁶ and LockBit⁷ ransomware. An example of a dark web offer:



⁶ Babuk is a ransomware family using a 'double extortion' tactic. It was first detected in 2021.

⁷ LockBit is one of the most active malware families operating as a RaaS model. It was first detected in 2019.

Brief description of a typical ransomware attack



1. An attacker explores a contractor's infrastructure, identifying vulnerabilities. In most cases, malefactors enter infrastructures by exploiting a software vulnerability or through a dictionary attack.
2. The attacker establishes a foothold in the contractor's infrastructure and uses lateral movement to take control over the maximum possible number of servers and automated workstations.
3. Having established a foothold in the infrastructure, the attacker explores the accessible information resources to identify those that would allow penetration into the infrastructure of another organisation (the target organisation) that the contractor interacts with. Malefactors can use both credentials or technical data, e.g. SSH keys⁸.
4. Having found such information, the attacker uses it to penetrate the target organisation's infrastructure and establish a foothold there.
5. As an additional channel for data exchange, the attacker creates a tunnel between the two organisations' infrastructures or, less frequently, between the attacker's command-and-control (CnC) server and the compromised infrastructure through the target organisation's contractor.

⁸ An SSH key is a pair of cryptographic keys (a public key and a private key) used for secure passwordless authentication on a remote server.

6. The attacker explores the target organisation's network and information resources, identifies data processing and storage facilities, account parameters, software used, and information security tools applied. At this stage, the attacker attempts to gain access to servers that are critical for the functioning of the target organisation and its information storage facilities. These are mostly domain controllers, database servers, and the infrastructure of information backup tools and accounting and software configuration tools of the organisation's IT infrastructure.
7. After the attacker completes the collection of data from all the hacked systems or finds out that the attack has been detected, the data encryption process is initiated.

In the course of data exfiltration, the attacker may begin uploading data both to its server or to the contractor's server used for the attack.

Despite the destructive effects of such attacks, in all cases, financial institutions managed to restore their infrastructures and client services as quickly as possible. In rare cases where the attackers managed to gain access to system backup copies, the restoration of the infrastructures took a longer time.

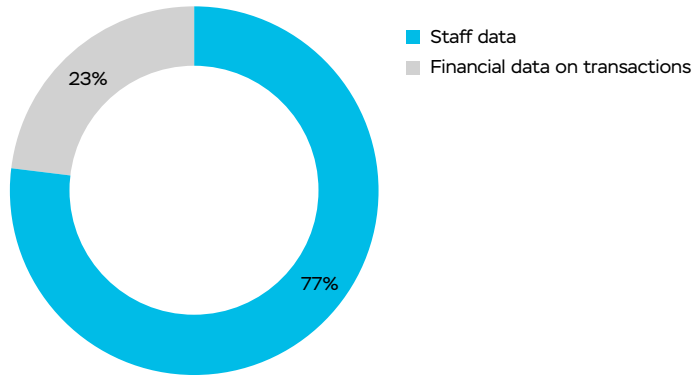
To be protected against such attacks, organisations are advised to:

- use regularly updated software patched against detected vulnerabilities;
- integrate modern information security systems into the infrastructure;
- organise backup storage in a way that would prevent access to backup copies from the local network in case of an attack;
- implement a zero-trust policy to all 'external' accounts and introduce restrictions on the operation of RDP⁹ services;
- use multi-factor authentication to access the infrastructure;
- apply a strict password policy to both technical and user accounts; and
- conduct cyber drills for employees.

⁹ RDP is a remote desktop protocol enabling a user to remotely access a server.

2.3.2. Data leakage

Confidential data leaks in 2025



According to Financial CERT's data, the number of significant confidential data leaks from credit and financial institutions decreased in 2025. However, certain malware attacks against contractors resulted in the leakage of information related to financial institutions' operations. This confirms a shift in the attack vector from targeted attacks on financial institutions to attacks on more vulnerable infrastructures of service providers and other contractors.

3. CYBER DRILLS

Cyber drills

Over past three years

987

institutions
participated
in cyber drills

> 30,000

phishing
emails sent

> 30

scenarios
tested

Objectives of cyber drills

- Enhancing the quality of response to targeted cyberattacks
- Ensuring faster communication with Financial CERT
- Practising measures to ensure the security of financial institutions' information infrastructure

Scenarios tested

Findings

- Participating in the Bank of Russia's cyber drills, each institution identifies weaknesses in its internal business processes and adjusts them accordingly

Recommendations

- Bank of Russia guides financial institutions to improve specific indicators of response to detected threats



Vulnerability exploitation

Check of the speed of patching identified vulnerabilities and external communication



Email phishing

Check of InfoSec specialists' knowledge. Adequacy of response to external threats



Money thefts

Check of institutions' preparedness for prompt communication with Financial CERT. Existence of specific procedures

IN 2025, OVER 320 INSTITUTIONS TOOK PART IN THE CYBER DRILLS, WHICH IS 10% MORE THAN IN 2024. FINANCIAL INSTITUTIONS' EMPLOYEES WERE COMPROMISED IN 6.5% OF SIMULATED INCIDENTS, WHICH INDICATES A RELATIVELY HIGH LEVEL OF FINANCIAL INSTITUTIONS' PREPAREDNESS TO COUNTER THIS ATTACK VECTOR.

OVERALL, IN THE COURSE OF THE CYBER DRILLS, 25 EMPLOYEES OF 21 FINANCIAL INSTITUTIONS WERE COMPROMISED IN SIMULATED INCIDENTS.

4. 2026 TRENDS

Based on the analysis of cybersecurity incidents in financial institutions' infrastructures and the findings of the analysis of cyberattacks, the following threats might become the most pressing in 2026:

- **Ransomware attacks.** The number of ransomware attacks will only be growing. However, it is important to note a trend of the changing goal of these attacks: previously, malefactors wanted to receive a ransom, whereas now, they are seeking to destroy target infrastructures. This means that a ransom is no longer the goal of attackers. Now, they attempt to damage target organisations as much as possible by disrupting their business processes and widely covering the incidents online.
- **Use of artificial intelligence.** Artificial intelligence (AI) has transformed cyberattacks, making them highly automated and requiring low technical skills from attackers, which might provoke a rise in such attacks.
AI-based attacks allow both mass mailing of phishing messages and malware and penetration into infrastructures.
- **Shift in the attack vector to data theft.** Stealing user data is a common goal of cyberattacks. However, previously, stolen data were used to receive a ransom or damage reputation, whereas now, attackers steal information, such as corporate data, to advance the attack on the organisation.
- **Attacks on small and medium-sized businesses.** These attacks were very frequent in 2025. As a result of compromising smaller businesses having remote access to other organisations' infrastructures as part of fulfilling contractor services agreements, attackers gained access to larger companies' infrastructures. Therefore, the trend of attacking small and medium-sized businesses will persist.

- **Development of banking trojans and malware for mobile devices.** Malware used to covertly control mobile devices is being constantly modified, which complicates its detection. Operating systems for mobile devices provide access to SMS / push notification channels, which makes it easier for attackers to covertly intercept and modify notifications related to remote banking services. Techniques used to steal data with the help of mobile devices are constantly evolving, which requires closer attention to ensuring the security of clients' communication with banks when receiving remote banking services using their mobile devices.

Cyber drills with financial institutions

Expanding the geographical scope of cyber drills and introducing additional scenarios

Analysis of contractor-related threats by category

Ensuring the participation of IT solutions providers in the information exchange with Financial CERT's AIMS

Database of indicators of compromise (IoC) accessible 24/7

Financial CERT plans to automate IoC receipt by organisations connected to its AIMS



2026