



Bank of Russia



OVERVIEW OF THE MAIN TYPES OF CYBER ATTACKS IN THE FINANCIAL SECTOR IN 2024

Moscow
2025

CONTENTS

INTRODUCTION	2
CYBER ATTACKS ON THE FINANCIAL SECTOR IN 2024	4
Attacks through contractors.....	6
Example of a proactive response to and combating a cyber attack through contractors' infrastructures.....	9
ATTACKS ON FINANCIAL INSTITUTIONS ARE BECOMING INCREASINGLY SOPHISTICATED: MAIN VECTORS OF THREATS IN 2024	11
Analysis of attackers' network architecture.....	13
Compromise of servers as a springboard for an attack.....	13
Hosting providers' role in growth of attacks.....	14
Growing number of Russian IP addresses in attacks.....	15
Use of mobile proxy servers.....	15
VPN solutions and traffic anonymisation.....	16
Creating a covert channel.....	17
Post-incident analysis and vulnerability management.....	19
2024 RESULTS	23
Monitoring of operational resilience incidents.....	24
Attacks on financial institutions' clients.....	26
Cyber training with financial market participants.....	28
International cooperation.....	29
FINANCIAL CERT'S COOPERATION AREAS IN 2025	32
2025 TRENDS	33
More attacks via supply chains.....	33
Shifting focus on small and medium-sized institutions.....	33
Increasing destructive effects of cyber attacks.....	33
Difficulties in identifying and attributing attacks.....	34
Growth in attack dwell time.....	34
RECOMMENDATIONS TO PREPARE FOR 2025 THREATS	35

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

Cover photo: Shutterstock/FOTODOM
Bldg V, 12 Neglinnaya Street, Moscow, 107016
Bank of Russia website: www.cbr.ru

INTRODUCTION

Following the analysis of the dynamics of cyber attacks¹ in 2023, it is possible to state confidently that malefactors were developing the existing cyber attack tactics and techniques in 2024 making them increasingly sophisticated. The key areas of successful cyber attacks include exploitation of vulnerabilities, distributed denial-of-service (DDoS) attacks, attacks through compromised information infrastructures of contractors, and account compromises as a result of carelessness and/or the lack of control over the use of password policies in financial institutions' information infrastructures.

Due to increasingly frequent cyber security incidents² through compromising contractors (attacks on supply chains), the financial sector needs to take proactive response measures to be protected against these threats. The Financial Sector Computer Emergency Response Team of the Bank of Russia's Information Security Department (Financial CERT) has been making extensive efforts to arrange communication with IT solution and service engineers and integrators whose products are actively used by the financial sector. Currently, Financial CERT cooperates with more than 60 such companies, which enables it to comprehensively enhance the level of cyber security and awareness about cyber threats among both service providers and financial institutions.

Regular evaluation of the landscape of cyber threats enables Financial CERT to timely prepare data about vulnerabilities and send them to information exchange participants for them to be able to respond to and mitigate the impacts of targeted cyber attacks.

Over 2024, Financial CERT sent over 360 machine-readable bulletins containing up-to-date indicators of cyber attacks and 38 information bulletins providing analytics on existing cyber threats and recommendations on how to counteract these threats.

Furthermore, current attack vectors and the process of communication with Financial CERT were explored as part of the annual cyber training with more than 290 participants from the financial sector.

In the course of the cyber training, jointly with the General Radio Frequency Centre Federal State Unitary Enterprise (GRFC), Financial CERT:

- conducted external scanning of the cyber training participants' information resources;
- tested the process of prompt communication of data about identified threats; and
- checked credit institutions' readiness to promptly discontinue electronic communication in the Bank of Russia Payment System in case of identification of a data protection incident in the course of money transfer processing in an information exchange participant's information infrastructure that resulted or could result in a money transfer unauthorised by the information exchange participant.

¹ A cyber attack 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 these infrastructures process.

² A cyber security 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 cyber attack.

As part of the development of international collaboration in the area of cyber security and cyber resilience, Financial CERT organised the first cross-border cyber training with the BRICS central banks' representatives. The cyber training included two stages. The first one took place remotely at the beginning of August 2024: the participants practised communication in terms of exchanging information about a detected information security threat using the bulletins prepared in accordance with the format of the BRICS Rapid Information Security Channel (hereinafter, the BRISC Channel).

The second stage was offline and hosted by the Innopolis University (the Republic of Tatarstan) in the middle of September 2024: the participants practised the skills of responding to cyber attacks, using various tools to identify attacks and evidence left behind by attackers (indicators of compromise), and eliminating consequences of cyber attacks.

In 2025, Financial CERT will continue to develop the practice of cyber training among the national (central) banks of the member countries of the interstate unions³ where Russia is a party to.

Using the tactics applied in 2024, attackers will continue to employ a combination of tools and techniques for surreptitious intrusion, establishment of a foothold, and destruction of companies' information infrastructures. To collect and steal sensitive information, fraudsters will seek to stay in systems as long as possible to explore the infrastructure in detail. Consequently, the time between a system compromise and its identification by information security units will increase.

The problem of attributing cyber attacks and finding indicators of compromise (IoCs) will continue into 2025 because malefactors conceal the attacks by using compromised servers, VPN, and mobile proxies.

Obviously, successful attacks on commercial organisations processing sensitive information entail its leaks and further use of these data for targeted attacks on individuals. Perpetrators find increasingly sophisticated techniques to attack the targets, which inevitably involves a rise in the number of thefts and the amount of stolen funds. Combating these crimes is one of the focus areas of Financial CERT.

Furthermore, as part of the efforts to counter phishing,⁴ dissemination of information about illicit financial operations and financial pyramids, and unlicensed activities in the internet, Financial CERT detected and initiated the blocking of approximately 46,000 domains over 2024, which is 33% more compared to 2023.

³ EAEU, ASEAN, SCO.

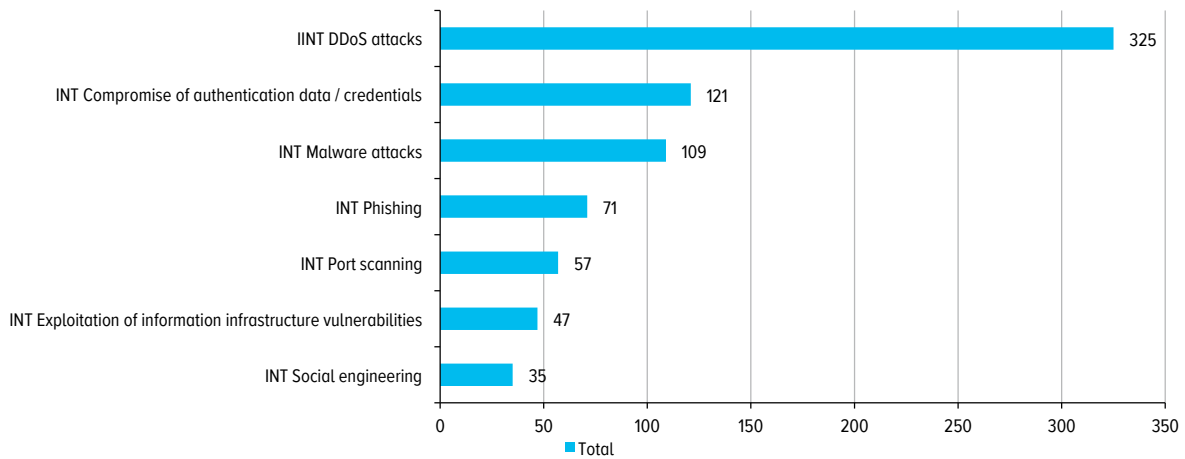
⁴ Phishing is a type of internet fraud to steal sensitive data by disguising an email or a website as a reputable source.

CYBER ATTACKS ON THE FINANCIAL SECTOR IN 2024

Over 2024, information exchange participants sent more than 750 reports about cyber attacks and incidents to the Bank of Russia via Financial CERT’s Automated Incident Management System (AIMS). Most frequently, financial institutions reported DDoS attacks, malware attacks, and compromised credentials attacks (Chart 1).

BREAKDOWN OF CYBER ATTACKS

Chart 1

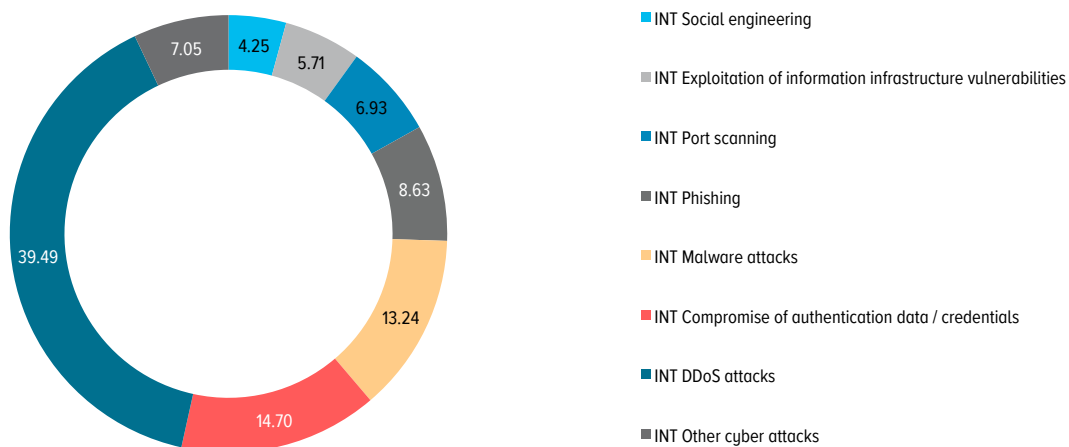


Source: Bank of Russia data.

The analysis of the reports received shows the following breakdown of attacks in 2024.

BREAKDOWN OF CYBER ATTACKS BY TYPE (%)

Chart 2



Source: Bank of Russia data.

The most widespread types of malware in 2024 were Trojan.Agensla.gen and Trojan-PSW.MSIL.Stealer.gen, which are malware used to steal user credentials as well as to remotely access and control a compromised device.

In the course of analysis of targeted malware attacks via emails, Financial CERT takes into account the following:

- the location of the mail server sending a phishing or malware email; and
- the location of the command-and-control server to which the request is sent when malware is launched.

The geographic breakdown of attacks identified in 2024 is shown in Chart 3.

BREAKDOWN OF CYBER ATTACK SOURCES, BY LOCATION

Chart 3



Trojan-Ransom malware, which encrypts user data on a compromised device, was used more actively in 2024. Most attackers demanded a ransom from the victims to decrypt their compromised data. The increase in such attacks vs 2023 was most probably caused by the release of ransomware source codes, e.g. Babuk¹ and Conti,² by large hacking groups.

It is worth noting that a cryptoware attack on the system of a cyber incident may occur not immediately after the system has been compromised. After gaining access to and compromising the system of the cyber incident, attackers may continuously steal data and, only after the malefactors' interest in this information is exhausted, they will begin a cryptoware attack. This means that the period between intrusion into the system and the subsequent cryptoware attack may last for several months. Therefore, it is possible to expect a large number of information security incidents caused by cryptoware attacks in 2025 as well.

¹ Babuk is ransomware used by the hacking group with the same name beginning from early 2021 to attack corporate networks. The source code for this malware was leaked on a Russian-language hacking forum in September 2021.

² Conti is ransomware used by the hacking group with the same name approximately from February 2020. Over the period from 2020 to 2022, the group attacked nearly 860 organisations worldwide. At the end of May 2022, the gang shut down its operation.

There are three initial vectors of entry into financial institutions' information infrastructures:

- brute force attacks;
- compromised accounts of a contractor; and
- exploitation of vulnerabilities of software installed at the attacked institution.

According to the received information about intrusions into the victims' compromised systems, the following conclusions can be drawn:

- Password policies in relation to technical accounts allow dictionary passwords, which is not in line with the minimum requirements established by Subsection 7.2.2.3 of National Standard of the Russian Federation GOST R 57580.1-2017 'Security of Financial (Banking) Operations. Protection of Financial Institutions' Information. The Basic Set of Organisational and Technical Measures' (approved by Order of the Federal Agency on Technical Regulating and Metrology No. 822-st, dated 8 August 2017).
- Financial institutions need to revise the access control matrix in relation to accounts of their contractors supporting the functioning of information systems. In addition, it is recommended to restrict access rights for contractors' accounts, expanding them for the system maintenance period. This will help mitigate the risks of malicious activity in case a contractor's account is compromised.
- It is advised to upgrade information systems regularly, namely to timely install updates from developers, especially cyber security updates. Where it is impossible to upgrade a system for any reason, it is recommended to explore the possibility of replacing the software with alternatives and/or develop compensating measures to strengthen the security of information infrastructures.

Attacks through contractors

The most popular way to gain access to financial institutions' systems in 2024 was compromising their contractors.

Due to a rising number of cyber security incidents through compromising financial institutions' contractors (attacks on supply chains), the financial sector needs to take proactive response measures to be protected against these threats. Beginning from 2022, Financial CERT has been collaborating with IT solution and service providers whose products are actively used by the financial sector. Through participation in information exchange, such companies can receive information about current attacks and threats targeting service providers to ensure timely protection of their infrastructures, on the one hand, and can promptly communicate in case any IoCs are detected and notify financial institutions about the identified cyber security incidents for the latter to take adequate response measures, on the other hand.

Over 2024, Financial CERT identified 17 incidents at companies providing IT services to more than 70 financial institutions, including systemically important credit institutions.

Financial CERT forwarded over 80 notices to financial institutions about compromise of their contractors' infrastructures for financial institutions to take response measures. Despite the notification, Financial CERT recorded a number of targeted attacks from contractors' infrastructures on financial institutions' infrastructures.

Certain cyber attacks on contractors providing services to the financial sector are described below.

Attack on a company developing automated banking systems

The contractor provides services of implementing the products it designs to organise and support banking activities as well as activities of management companies, exchanges, brokers, etc.

In the course of deployment and maintenance of the products, most financial institutions allowed the company's staff to remotely access their information infrastructures.

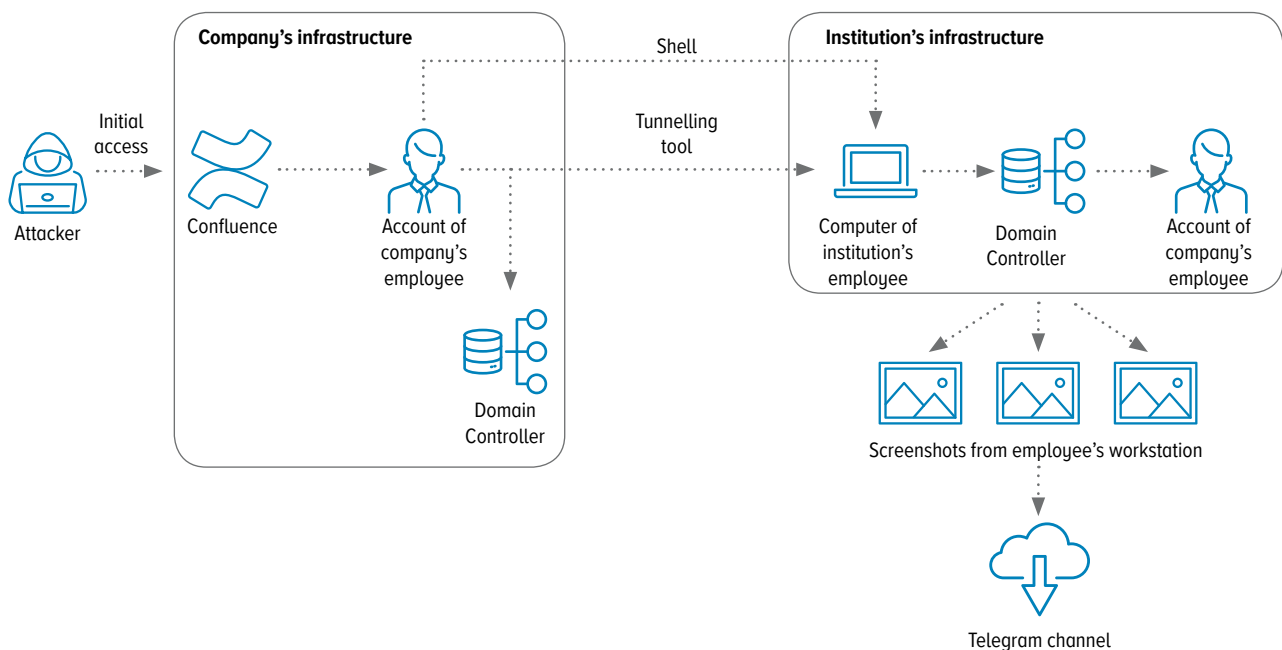
The analysis of the incident revealed that attackers had intruded into the company's network by exploiting a vulnerability in the Confluence system. After the intrusion, the perpetrators compromised the account of the company's employee, then the domain of the RDS controller, and subsequently the ESXi virtualisation environment.

Having entrenched themselves in the company's network, the malefactors started an attack on its client – a financial institution. Exploiting the compromised account of the company's employee, the attackers installed tunnelling software on the computer of the financial institution's employee. Later, this tunnel was used to install a special shell³ on the employee's computer enabling external remote access to the computer and execution of remote commands. The attackers could thus directly access the institution's IT infrastructure.

Then, through the escalation within the domain, the attackers gained access to the computer of one of the institution's employees. Having accessed the computer, the attackers made a number of screenshots as evidence of their success. The screenshots were posted in the attackers' Telegram channel. However, despite the attackers' access to the employee's computer, the analysis of the incident did not corroborate the fact of data leakage. The scheme of the incident is presented in Chart 4.

ATTACK SCHEME

Chart 4



³ A shell is an executable code that gives control to the shell process.

Attack on a fintech engineering company

A related entity of the fintech engineering company is engaged in the development of IT solutions and online lending and market funding technologies.

After the entity's database had been compromised, information on financial institutions leaked. These data had been processed by the entity.

The investigation of the incident revealed that the perpetrators had used a password to enter the compromised account of the entity's employee through a VPN server to conceal the source of the attack.

The vector of compromise of the employee's first account was not identified. Nevertheless, the investigation established that at least one more account of the entity's employee had been compromised: the attackers had accessed it using the same VPN server. Overall, to connect to the compromised accounts of the entity's employees, the malefactors used five VPN addresses rented from hosting providers in Russia and Germany.

When connecting to the compromised accounts, the perpetrators viewed data about the entity's projects through the Grafana system, looking for information on other accounts and connection parameters (keys) stored in an unencrypted form. Moreover, the attackers were searching for logins and passwords in GitLab repositories.

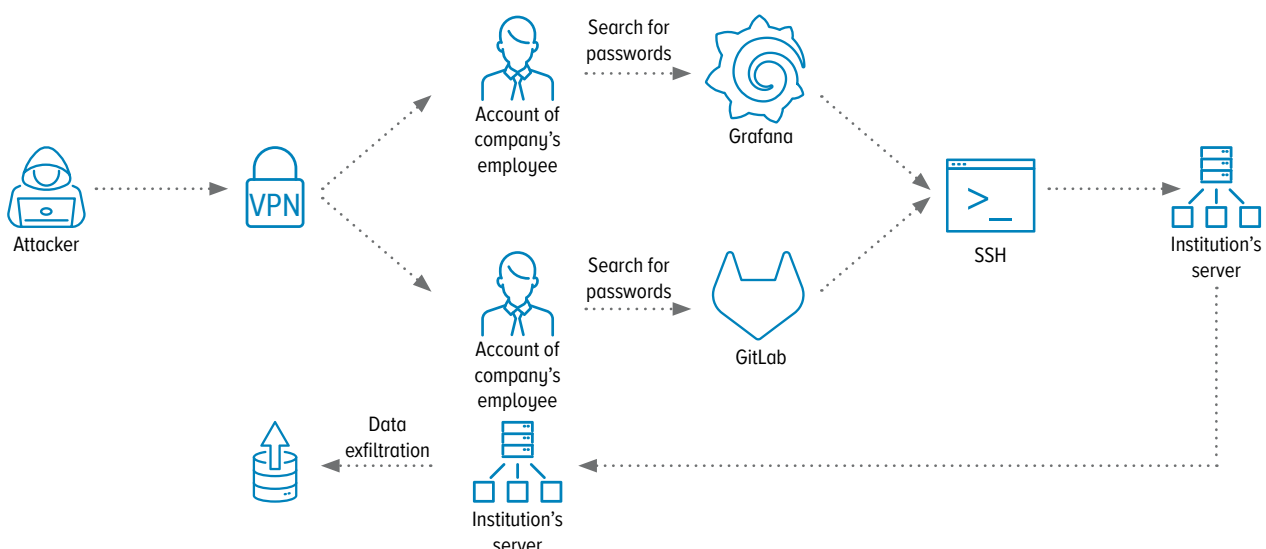
The malefactors then attempted to penetrate the entity's infrastructure via secure shell (SSH) connections as well as exploit the CVE-2022-2992 vulnerability in GitLab so as to execute arbitrary code on the compromised device.

In the course of the incident, the perpetrators collected data needed to successfully penetrate the infrastructure of a financial institution. Other computers of the entity were accessed by the attackers from a compromised server through an SSH server using the identified accounts.

It should be noted that, after successful compromise of the financial institution's server, the malefactors used it for a reverse attack on one of the servers of the fintech engineering company. After that, the attackers exfiltrated information from the databases on the entity's server. The perpetrators exfiltrated the information related to users of other financial institutions (the full scheme is presented in Chart 5).

ATTACK SCHEME

Chart 5



Brute force attack on a website development company

The company is engaged in the development of websites and mobile apps and application programming interface (API) integration, as well as client website support. One of its clients is a financial institution. Information on the leakage of its customers' personal data was published on a popular internet resource.

The investigation of the incident revealed that the server of the institution's business card website had been compromised. The server stored information provided by filling in the feedback form and not classified as personal data of the institution's customers. The attackers accessed the server through a web shell⁴ that they had installed on the server and exfiltrated information using the software Adminer v. 4.8.1.

When the affected financial institution started the investigation, it found out that the web shell had been uploaded onto the server from the technical account of an employee of the contractor providing server and business card website support services. After this, the institution initiated the investigation of the incident in the company's infrastructure suspecting that the system had been compromised earlier.

The fact of compromise of the company's infrastructure was confirmed. The investigation detected that the attackers had cracked the password to the technical account. The password was a dictionary combination of letters and numbers, which made it easier for the attackers to brute-force the password to the technical account. Having thus compromised the company's infrastructure and found authorisation data for the financial institution–client's infrastructure, the attackers intruded into the financial institution's internal network and stole the data from the server.

Example of a proactive response to and combating a cyber attack through contractors' infrastructures

The above-described attacks on financial institutions through their contractors' infrastructures and vulnerabilities could have been avoided if all the parties, including financial institutions, contractors, telecommunications and cloud providers, cyber security service providers, and IT service and solution companies, had organised comprehensive, timely, and more efficient information exchange.

To consolidate comprehensive information about cyber attacks made by malefactors on financial institutions, Financial CERT uses a wide range of tools, including monitoring of public internet sources where it found information about possible compromise of a corporate software and cloud solution development company. To mitigate risks, the Bank of Russia's Financial CERT decided to launch two concurrent processes:

- communication with specialists of the company's cyber security units to organise collaboration in view of that incident and provide consulting assistance for localising the cyber security incident and eliminating its consequences; and
- notification of financial institutions about possible compromise of the company providing IT solutions to financial institutions.

⁴ A web shell is a command shell that allows remote control of a web server.

Thus, as a result of Financial CERT's prompt response to the information received, it notified more than 15 financial institutions, including systemically important ones, as well as timely identified and localised the incident inside the company's infrastructure, which helped avoid the following consequences:

- leakage of personal data;
- leakage of other sensitive information;
- encryption of institutions' infrastructures;
- spoofing and discreditation of institutions' websites, and other serious consequences.

ATTACKS ON FINANCIAL INSTITUTIONS ARE BECOMING INCREASINGLY SOPHISTICATED: MAIN VECTORS OF THREATS IN 2024

As part of the measures taken to respond to cyber attacks in the financial sector, Financial CERT specialists continue to track and analyse new vectors of threats and techniques used by malefactors.

Attack methods are becoming increasingly sophisticated and multi-level, due to which financial institutions need to continuously enhance their approaches to responding to cyber attacks and ensuring cyber security.

Perpetrators are developing methods to conceal their attacks, which enables them to bypass traditional information protection tools and makes it much more complicated to identify and promptly suppress cyber attacks.

This section describes the main vectors of attacks that financial institutions had to face in 2024 and the key mechanisms and techniques employed by malefactors.

Attacks in the traditional sense of a money theft are gradually giving way to more complicated and multi-phase schemes. Given the high complexity of large financial institutions' infrastructures and advanced security systems, perpetrators are adapting their objectives and techniques. Today, they not only target financial assets but also seek to disrupt confidence in institutions through data manipulation and information pressure.

Over 2024, malefactors committed their attacks to:

- **destabilise business** by leaking sensitive data, which might undermine an institution's reputation and entail legal and regulatory risks;
- **provoke a public outcry** by disseminating false or compromising information through social media and other channels to cause panic and create a negative image of both the credit and financial sector as a whole and a given financial institution in particular;
- **exert information pressure** on employees by threatening to leak compromising information, demonstrating control over an institution's internal processes, or blackmailing them; and
- **block data and demand a ransom** through ransomware attacks aiming to encrypt critical information.

Attacks on financial infrastructures generally include several phases from preparing an attacking infrastructure to intruding into a target infrastructure, establishing a foothold, and organising a covert channel to exfiltrate, retrieve, and monetise data.

Modern attack techniques increasingly frequently incorporate elements of putting information pressure, influencing the perception of events, and exploiting the human factor, which makes it even more difficult to combat such attacks.

Attackers seek to influence an institution's information landscape and ecosystem, strengthening the pressure through a combination of technical and information tools.

The summary of the main phases of a cyber attack on an institution's infrastructure is presented below.

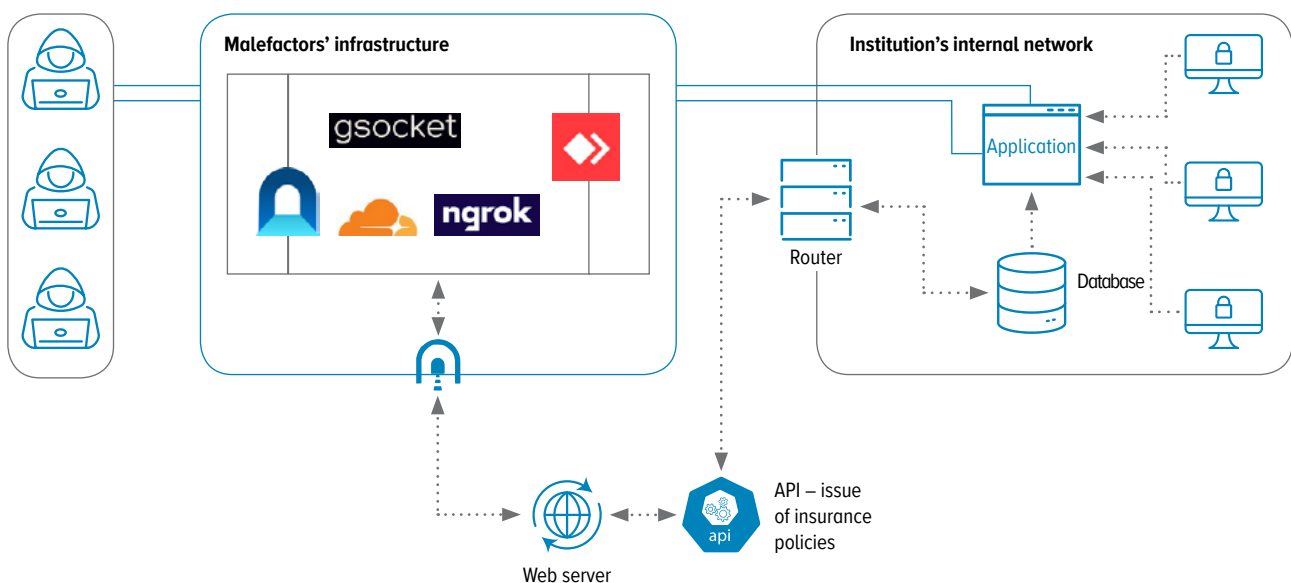
- **Preparation of infrastructure.** Perpetrators create an attacking infrastructure that will allow them to conceal their actions from security systems. This infrastructure may include rented servers, compromised vulnerable servers and proxies, VPN, and mobile proxies to hide attackers' real location.
- **Penetration and exploitation of vulnerabilities.** In this phase, perpetrators intrude into an institution's information system. They may exploit various vulnerabilities from weak passwords to vulnerabilities in web apps or outdated versions of server systems.
- **Establishing a foothold in the target infrastructure and organising a covert channel to exfiltrate data.** After the intrusion into the target information infrastructure, attackers establish a foothold in it to maintain access and minimise the probability of detection. To this end, malefactors install tools and malware to get entrenched for a long time, such as a backdoors,¹ legitimate accounts with increased privileges, and malicious services masquerading as regular normal processes. Concurrently, attackers create covert channels to exfiltrate data using encryption and traffic obfuscation² techniques. They adjust these channels depending on the target institution's specifics in order to minimise abnormalities in network traffic. Installation and data exfiltration are parallel processes where perpetrators employ the same tools to maintain control and steal data without high risks. The duration of this phase depends on the complexity of the target infrastructure and the need to thoroughly conceal criminal actions.
- **Data monetisation and exfiltration.** In the last phase, malefactors choose the ways to monetise the data they obtained as a result of a successful attack: sell the stolen information, use it for subsequent attacks (e.g. phishing), or racketeer through blackmail.

Example of a typical attack scheme

According to Financial CERT specialists, one of the most frequent scenarios in 2024 was a **phased attack through a target financial institution's web infrastructure** (Chart 6).

POPULAR SCHEME OF ATTACK ON TARGET INFRASTRUCTURE

Chart 6



¹ A backdoor is a defect of a computer system intentionally installed by a malefactor to gain unauthorised access to data.

² Obfuscation is a technique of deliberately making information difficult to understand.

In the first phase, malefactors compromised a third-party server not directly related to the target institution. The attackers installed **GSocket** on this server to organise a covert C&C³ channel and tunnel traffic. This server became an intermediate point for the subsequent attack.

In the next phase, the perpetrators attacked **the target institution's web server** operating on the Bitrix content management system (CMS), exploiting vulnerabilities in the configuration or an obsolete version of the CMS. Having gained access to the server, the attackers found out that it was connected to the target institution's **internal infrastructure** via **API** ensuring communication with a database. This API was used to record and **process financial documents**.

After the intrusion, the malefactors established a foothold, arranged clandestine channels to retrieve data, and exfiltrated **information** from the database. This information was then sold in grey markets. The attackers also employed an API vulnerability to conduct unauthorised **financial transactions**.

Thus, the attack was carried out step by step from compromising the third-party server to exploiting the vulnerabilities in the target web infrastructure and profiteering through manipulations with the institution's internal data.

Analysis of attackers' network architecture

Today, cyber attackers employ a variety of techniques and approaches to building an attacking infrastructure.

Perpetrators' main objective is to establish technical infrastructure, methods, and telecommunications tools to hide network traffic profiles and/or disguise them as legitimate for the target institution.

Compromise of servers as a springboard for an attack

In the initial phase, when building infrastructure meant to conceal their actions and disguise traffic as legitimate in order to minimise the probability of attack detection and suppression, malefactors often choose to compromise servers located inside Russia. This is because they can use regional IP addresses that most security systems installed at financial institutions recognise as internal and secure ones. This is especially relevant for small financial institutions who do not have sufficient resources to ensure comprehensive information protection.

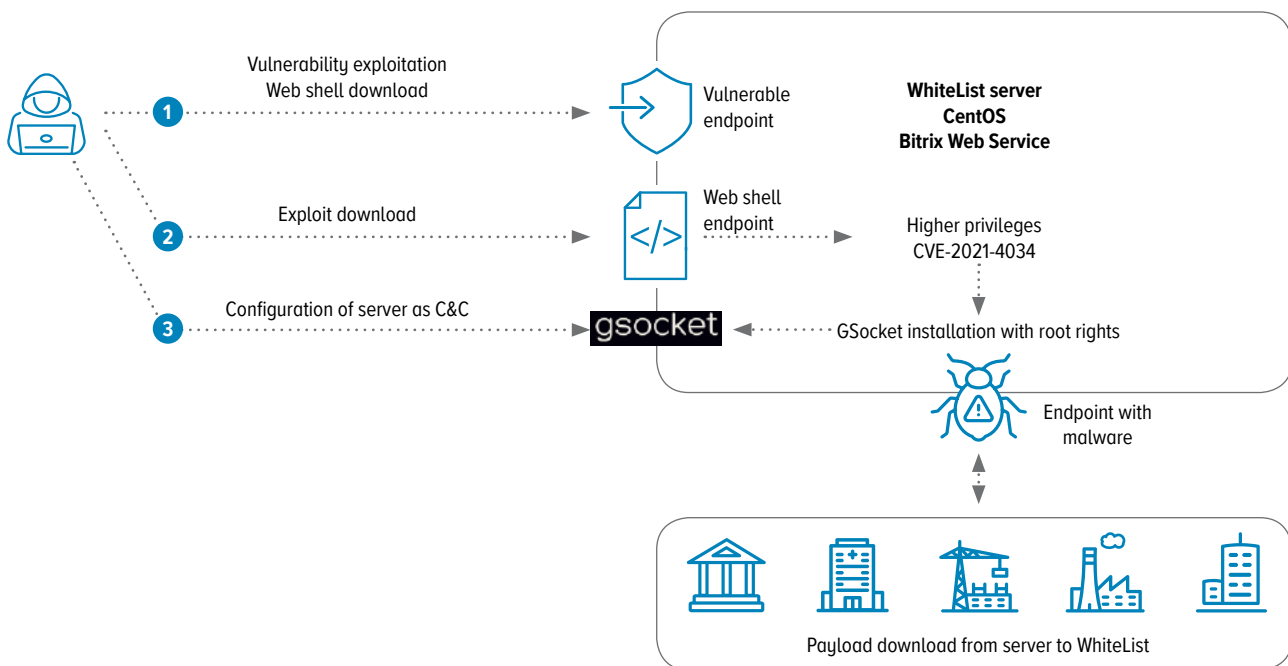
Thus, Financial CERT, jointly with the National Computer Incident Response and Coordination Centre (NCIRCC) of the Federal Security Service of the Russian Federation, recorded facts of compromise of financial institutions through a vulnerability in the **1C-Bitrix** CMS.

In one of the incidents, after the intrusion, the perpetrators used a server of the target institution as a **C&C server**. Supposedly, the attackers either were not fully aware how they could effectively use the financial institution's entire infrastructure or their approach to the attack was automated. The malefactors continued to use the C&C server for a long time, which might be because they were seeking to collect additional data about the system. Later on, **information leaked** from this server.

³ A C&C server is a command-and-control server to send commands to a system compromised by malware.

USE OF INFORMATION EXCHANGE PARTICIPANT'S SERVER AS C&C SERVER

Chart 7



Hosting providers' role in growth of attacks

As long as it takes effort and time to compromise a server, malefactors frequently opt to rent servers from hosting providers, which enables criminals to quickly build an attacking infrastructure without time consuming technical configuration operations and reduces the risk of being revealed.

Hosting services continue to advance actively, despite a rather long history of development in this area. Technological progress, greater digitalisation of the economy, and an increase in provided services involve new challenges to both the financial sector and regulators.

However, the legal and regulatory framework in this area is still evolving, which is why there are still legal deficiencies and difficulties associated with technological gaps and the need for adequate control over cyber security. The main issues are as follows:

- **Client identification** is becoming increasingly important given a growing number of cyber attacks. Despite the measures taken to enhance control, there are currently no stringent requirements for client verification. In particular, there is no mandatory identification procedure for a person wishing to rent a virtual private server, especially from a small regional provider. Consequently, servers may be used by malefactors anonymously without providing true data.
- **Anonymity in payments for services:** as a result of the development of digital financial assets, a number of hosting providers accept cryptocurrency payments, which makes it difficult to unmask perpetrators and hold them liable. This makes it even more complicated to detect and track financial transactions.

It should be emphasised that the development of hosting services requires a flexible approach to regulation so as to ensure a balance between effective control and support for innovation.

Growing number of Russian IP addresses in attacks

In recent years, there has been an increase in attacks from servers located in the Russian Federation. This rise is associated with several factors.

Specifics of traffic blocking: the competent government authorities, such as the GRFC, make extensive efforts to counteract attacks by implementing filtration and blocking mechanisms, including deep packet inspection (DPI), which makes it much more difficult for perpetrators to employ foreign servers forcing them to switch to Russian servers. However, it is more complicated to organise comprehensive filtration on Russian servers without affecting legitimate services.

Legitimate traffic type: regional IP addresses provided by such servers are often recognised as safe by financial institutions' security systems, due to which information security units shall pay particular attention to traffic from IP addresses located in the Russian jurisdiction.

Today's challenges associated with cyber threats and an increase in illicit operations in the digital environment require prompt response measures. In 2023, the legislative authorities drafted and approved key regulations for the hosting services industry so as to protect information systems and improve the resilience of infrastructures. These regulations enhance control over data processing and storage and communication between providers and government security systems.

As part of these efforts, the Russian Ministry of Digital Development, Communications and Mass Media issued Order No. 935, dated 1 November 2023, to create conditions enabling investigation and search operations. The Order obliges hosting providers to connect to the system of investigation and search operations and supply computing resources for these operations. In turn, the law enforcement agencies promptly respond to cyber threats, including by suppressing crimes committed using digital resources. A principal objective is to reduce the level of anonymity of perpetrators employing the Russian infrastructure.

In order to enhance the comprehensive approach to data protection, the Russian Ministry of Digital Development, Communications and Mass Media enacted Order No. 936, dated 1 November 2023, establishing the requirements for data protection in internet-connected systems. Among other things, hosting providers must collaborate with the State System for Detecting, Preventing and Eliminating Consequences of Computer Attacks on Information Resources of the Russian Federation (GosSOPKA), promptly eliminate vulnerabilities, prevent DDoS attacks, and store data on user communications.

These measures aim to prevent data leaks and ensure stable operation of critical information infrastructures.

Use of mobile proxy servers

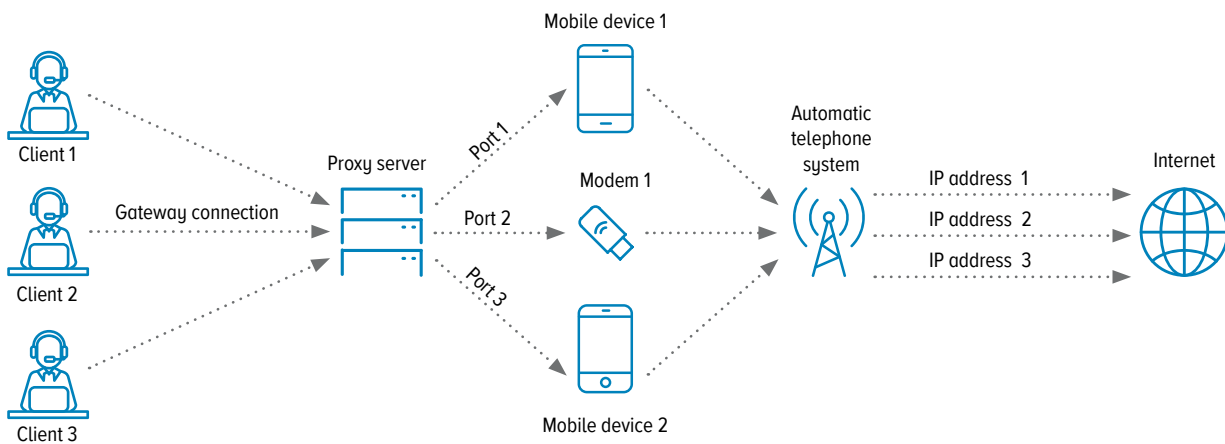
Malefactors have been increasingly frequently using proxy servers, including mobile proxies, deployed on rented servers in order to better conceal their actions. This may be done by employing **GoIP devices⁴ (in the case of telephone fraud – to make VoIP⁵ calls anonymous)**. As long as IP addresses for mobile devices are assigned dynamically, malefactors use modems with SIM cards as a dynamically changing (mobile) proxy.

⁴ A GoIP is a network device to transmit voice traffic over IP networks (Voice over Internet Protocol) using mobile operators' SIM cards.

⁵ Voice over Internet Protocol (VoIP) traffic is voice communications that are transmitted over IP networks.

TRAFFIC ROUTING. MOBILE PROXIES

Chart 8



Perpetrators use such servers to mask the infrastructure they build for an attack, including its actual location.

The main reasons why attackers use mobile proxies are as follows:

- **Constantly rotating IP addresses:** normally, mobile proxies frequently change IP addresses, which complicates their blocking since one IP address may be assigned to dozens of users during a day.
- **Traffic recognised as legitimate:** by employing mobile proxy networks or autonomous system numbers (ASNs), perpetrators can make traffic hardly distinguishable from normal user traffic. This is critical for financial institutions as part of their users may access services through mobile networks.
- **Accessibility and low costs:** malefactors may easily rent mobile proxy networks in grey markets. These services are rather cheap, while access is almost instantaneous. In 2024, the authorities adopted a number of regulations establishing new rules for registering SIM cards:
 - in accordance with the amendments to Federal Law No. 126-FZ 'On Communications' to become effective from 1 January 2025, foreign citizens and stateless persons will only be allowed to conclude a mobile service agreement personally in a mobile phone store with mandatory biometric identification; and
 - from 1 April 2025, Russian citizens will be allowed to have no more than 20 registered SIM cards per person.

These measures are intended to prevent the use of anonymous SIM cards for illicit purposes.

VPN solutions and traffic anonymisation

In recent years, there has been a growing number of attacks made using compromised local servers or servers rented from regional hosting providers, which significantly complicates the investigation of such incidents. Despite this trend, VPN solutions remain a key element of infrastructure enabling perpetrators to conceal their attacks.

Analysis of a number of incidents shows that malefactors frequently rent servers from various providers, e.g. Hetzner, DigitalOcean, OVH, Linode, Vultr and AWS, and from Russian regional hosting providers. These servers are often used as intermediary nodes to mask the actual IP address and reroute traffic.

The investigation of the chain of communications and the analysis of attackers' infrastructure ultimately detect VPN services or the Tor network. These technologies are used to ensure anonymity and reduce the risk of detection of the source of an attack. Such an approach makes it much more complicated to obtain information necessary to identify persons and groups involved in an attack.

Malefactors extensively use encrypted connections and servers located in jurisdictions with a high level of personal data protection, which involves additional difficulties in implementing legal and technical measures.

Creating a covert channel

In 2024, the financial market faced a change in remote access tooling. Perpetrators began to use new tools to set up a covert channel, such as Ngrok, Cloudflare Tunnel, and GSocket.

The most vivid example was Microsoft Dev Tunnels. This tool intended for developers enables malefactors to create connections perceived as legitimate traffic. Communicating data through Microsoft servers, perpetrators actually exploit the corporation's reputation to hide their actions. This seriously hinders the detection of cyber attacks as security analysts have to examine telecommunication traffic that is hardly distinguishable from standard connections between Microsoft products.

Previously, malefactors used to employ TeamViewer and AnyDesk for these purposes.

The most popular technique is domain name system (DNS) tunnelling which was created long ago but is still widely used as a result of its adjustment to modern conditions. This method was first used when internet traffic was limited to bypass network restrictions. However, it remains very popular, which is confirmed by an incident recorded in 2024 with the Zloader malware that used DNS to conceal C&C communications.

Malefactors employ modern versions of DNS tunnelling to command and control infected systems and bypass security mechanisms.

A covert channel is a mechanism masking start and end addresses and traffic itself, which makes its detection by standard security systems extremely difficult. Covert channels are used to:

- command and control compromised systems remotely;
- steal confidential data; and
- bypass security mechanisms, e.g. network firewalls and threat detection systems.

Financial CERT analysts use 'a covert channel' and 'traffic tunnelling' as complementing terms to refer to both technical and theoretical aspects of a threat.

Covert channel types

Two main approaches to establishing a covert channel are as follows.

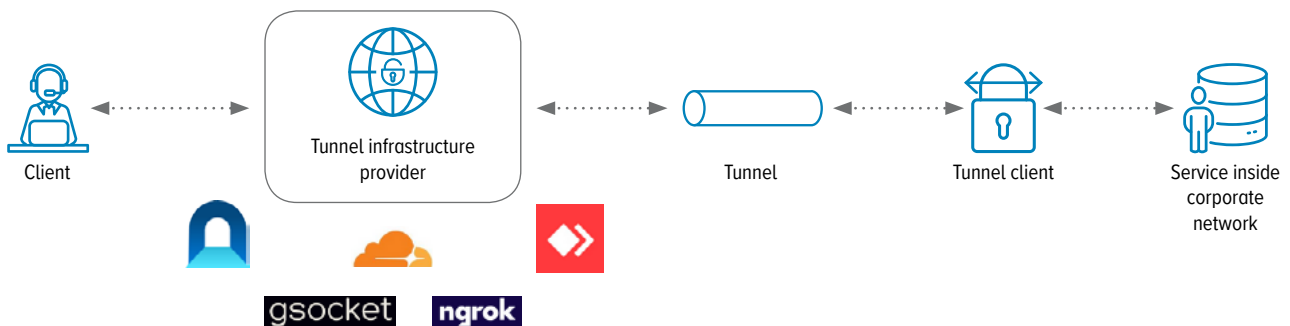
- **Use of existing infrastructure.** Such tools as Ngrok, Cloudflare Tunnel, GSocket, Microsoft Dev Tunnels, TeamViewer, and AnyDesk provide infrastructure as a service, thus eliminating the need for perpetrators to set up servers on their own. These tools operate as a packaged solution, disguising traffic as legitimate requests and reducing the risk of detection. Traffic transmitted via servers of such corporations, as Microsoft, is hidden by standard protocols, e.g. HTTPS or DNS, which makes it hardly distinguishable from normal network communications. Due to masking and complicated analysis, these tunnels easily bypass network firewalls, intrusion detection and prevention systems (IDS/IPS), and other standard detection tools. This approach reduces costs and time needed for intrusion.
- **Development of new infrastructure.** The second approach implies creation and management of infrastructure for tunnelling. To establish new infrastructure, perpetrators may use various techniques, e.g. DNS tunnelling, or such tools as Chisel. However, setting up new infrastructure requires special qualifications and leaves more evidence, which increases the risk of detection. Thus, in the case of DNS tunnelling, just as with Zloader, malefactors need to generate domain names and set up servers, which makes this approach more vulnerable to detection.

Urgent threats and approaches used to create covert channels in 2024

In 2024, malefactors extensively used the first approach to establish a covert channel, that is, tools providing infrastructure as a service (IaaS).

TRAFFIC ROUTING WHEN USING STANDARD TOOLS FOR TUNNELLING (NGROK, GSOCKET, ANYDESK, TEAMVIEWER, CLOUDFLARE TUNNEL, MICROSOFT DEV TUNNELS)

Chart 9



In 2024, Financial CERT focused on the analysis of tunnelling methods developed and used by malefactors. The key areas of the work were as follows:

- in-depth analysis of attacking infrastructures, including identification of patterns in the use of IP addresses and generation of domain names that are typical of these tunnelling systems;
- demonstration of the mechanisms of operation of tunnels, including methods of their detection and prevention; and
- development of practical recommendations to enhance the resilience of systems to such attacks.

Countering threats of covert channels

Covert channels established and employed by perpetrators constitute a major problem for cyber security specialists. Modern information security systems are frequently unable to effectively identify traffic generated by such channels. Malefactors employ protocols widely used in legitimate business processes, e.g. HTTPS, WebSocket, or DNS, which complicates the detection of covert channels with standard traffic analysis tools.

To ensure preventive protection, it is crucial to explore mechanisms employed to establish covert channels, including protocols used as well as masking and firewall bypassing techniques. Deep understanding of network technologies and the principles of traffic inside corporate infrastructures is critical to effectively counteract these threats.

However, standard tools, such as IDS/IPS, are frequently unable to detect covert channels, especially when the latter masquerade as legitimate traffic. Therefore, adaptive methods should be applied, including:

- **analysis of abnormalities** to detect deviations in the behaviour of network nodes;
- **machine learning technologies** to identify hidden patterns in traffic; and
- **in-depth network monitoring** with segmentation and identification of critical network zones.

Tackling these tasks requires highly qualified network technology specialists and protocol analysts.

To mitigate the risk of successful use of these techniques by malefactors, it is essential to apply a comprehensive approach incorporating advanced examination of the creation of covert channels.

Post-incident analysis and vulnerability management

The analysis of the incidents explored by Financial CERT specialists in 2024 identified the following patterns.

Time of compromise

Investigation revealed that, in a number of the incidents, information systems had been compromised up to 12 months before they became an object of investigation.

This fact is corroborated by the incidents when malefactors exploited vulnerabilities, in particular **remote code execution** (RCE), to intrude into a system and get a foothold therein without performing any destructive actions. Their presence in the system thus remained undetected for a long time. Perpetrators frequently started active operations only after **PoC exploits**⁶ had been publicly released, which enabled attack automation and extensive deployment of shells and **backdoors** in target systems.

Use of publicly available PoC exploits

The release of PoC exploits has a critical impact on the scale and pace of attacks on vulnerabilities. [According to the Cloudflare company](#), global leader in network security and content delivery, it has seen exploits as fast as 22 minutes after a PoC was released.

⁶ A PoC (proof-of-concept) exploit is a method or trick used to take advantage of a vulnerability.

Perpetrators can thus quickly customise exploits to use them in automated tools, e.g. Nuclei⁷ and Metasploit,⁸ that are regularly updated with attack templates and scenarios. Such tools make it easier to find and exploit vulnerabilities making them usable for less skilled attackers.

In addition to active scanning of networks, perpetrators extensively use specialised platforms for analysing internet resources, such as Fofa,⁹ Shodan,¹⁰ Censys,¹¹ Netlas,¹² and ZoomEye.¹³ These tools provide comprehensive data on configurations, network infrastructure, and possible vulnerabilities in target systems.

Thus, malefactors frequently do not have to initiate scanning on their own as the largest part of information about target systems is already available in open sources. It is vital for institutions to track data that may be released on such platforms and take timely measures to eliminate potential risks.

The pace of security upgrades in these conditions is critical. [According to the analysis by Mandiant](#), a leader in threat intelligence, incident response, and dynamic cyber defence, the average time-to-exploit (the time taken to exploit a vulnerability before or after a patch is released) decreased from 63 to 5 days over the period from 2018 to 2023. However, this was insufficient since exploitation activity was seen immediately following the release of a PoC. Furthermore, [Kaspersky Lab's statistics](#) show that the total number of first-time publications of PoCs for new common vulnerabilities and exposures (CVEs) rose by 2–3%, which proves that it is critical to reduce the time between the detection of a vulnerability and the release of a patch.

Effective vulnerability management should become a priority area of the work of institutions' cyber security units. As a result of evolution of artificial intelligence (AI) technologies, malefactors can access tools that make it easier to develop exploits and automate attacks.

AI accelerates customisation of existing PoC exploits and helps create new attack methods with minimum human participation. Therefore, institutions need to apply a proactive approach to monitoring threats and implementing advanced security tools. To achieve this objective, it is necessary to implement comprehensive vulnerability assessment and patching processes, integrate efficient threat detection methods, and enhance monitoring and infrastructure mechanisms. A proactive approach incorporating regular analysis, timely installation of security patches, and control over potentially accessible information will help reduce the time for a possible attack and ensure a prompt response to it. These measures will improve institutions' resilience to modern threats and prevent vulnerability exploitation.

⁷ Nuclei is a scanner for automated security testing that uses templates to find vulnerabilities and configuration errors in infrastructure.

⁸ Metasploit is a platform for engineering, testing, and vulnerability exploitation widely used by both security researchers and malefactors.

⁹ Fofa is a platform for passive analysis of internet resources to discover open ports, services, and configurations of network infrastructure.

¹⁰ Shodan is a search engine to find devices and services connected to the internet, including the internet of things (IoT), servers and control systems.

¹¹ Censys is a tool offering analytics about the security of internet resources and helping identify vulnerabilities.

¹² Netlas is a platform to explore network resources and analyse their accessibility, configurations, and vulnerabilities.

¹³ ZoomEye is platform to scan and analyse internet resources, including IoT devices and server apps.

Repeated attacks and sale of access

Investigating the incidents of 2024, Financial CERT identified a number of repeated attacks on earlier compromised systems of financial institutions.

A critical issue is that not all traces of compromise can always be erased when vulnerabilities are patched. In one of the incidents with CVE-2022-27228 in 1C-Bitrix, even after the problem had been fixed, the perpetrators still managed to leave hidden components (backdoors or web shells) that they later on used to repeat attacks. Therefore, without thorough post-analysis, patching a vulnerability cannot guarantee the security of a system.

In certain cases, malefactors can sell the access they gained to other hacking groups. Sometimes, a system remains compromised for a long time after an attack, until the moment of investigation and regular security audit.

Post-incident analysis

Due to the risk of repeated attacks and subsequent sale of access, post-incident analysis of a system after installation of updates (patches) and removal of vulnerabilities is becoming crucial.

Financial CERT frequently records cases where systems are not examined for IoCs after vulnerabilities have been patched, which entails repeated attacks. Thus, many specialists only deal with installation of software updates and fail to do post-incident analysis, which becomes the principal reason for repeated incidents.

In its weekly digests, Financial CERT always focuses not only on describing vulnerabilities and their exploitation but also on traces left after an attack. The main objective of these digests is to inform cyber security specialists of components and files that perpetrators can leave in a system as well as to provide very detailed recommendations on checks to be done as part of post-incident analysis.

This approach helps not only fix a vulnerability but also protect the system against future attacks.

Recommendations on improving vulnerability management

To enhance the efficiency of post-incident analysis and address complex tasks of vulnerability management, Financial CERT recommends the following measures.

- **Thorough retrospective analysis of a system.** When a vulnerability, especially a **preauth RCE**,¹⁴ is detected, it is not enough just to upgrade hardware or software. It is essential to comprehensively analyse the system for IoCs. This approach comprises exploration of configurations and logs, search for hidden objects or files left by malefactors, and analysis of abnormalities.
- **Search for PoC exploits.** Specialists should keep a close eye on public PoC exploits and check their employers' systems for vulnerabilities that have already become public. After PoC exploits are released, it is critical not only to install updates but also to thoroughly analyse the system to understand whether a particular vulnerability may be used repeatedly.

¹⁴ A preauth RCE is a vulnerability allowing pre-authentication remote code execution.

- **Early detection of traces of compromise.** It is critical to remember that, even if a vulnerability has been fixed, malefactors can leave IoCs. They may use software and utilities, such as backdoors, to access the system again. Therefore, regular scanning and analysis of activities in a system are critical security elements.
- **Monitoring of access rights and configuration settings.** In the course of server configuration, it is necessary to thoroughly control access rights so as to avoid excessive privileges that may be later on used by an attacker to establish a foothold.

Targeted cyber attacks on financial institutions' information infrastructures in 2024 were mostly the result of exploitation of vulnerabilities by brute-forcing dictionary passwords frequently left by contractors in the course of infrastructure upgrades and so on.

2024 RESULTS

This section analyses in greater detail the causality between cyber incidents resulting from vulnerability exploitation and implications of these attacks.

As noted above, Financial CERT regularly notifies financial market participants of attacks and threats relevant to financial institutions. Specifically, a key reason for cyber incidents in 2024 was the exploitation of CVE-2021-4034 (PolKit vulnerability) and CVE-2022-27228 (Bitrix vulnerability).

According to the data available, most incidents could have been avoided had financial institutions taken adequate response measures to counter the risks of attacks on their infrastructures and complied with Financial CERT's recommendations given in recent bulletins and information digests (see the Table below).

INFORMATION ON BULLETINS

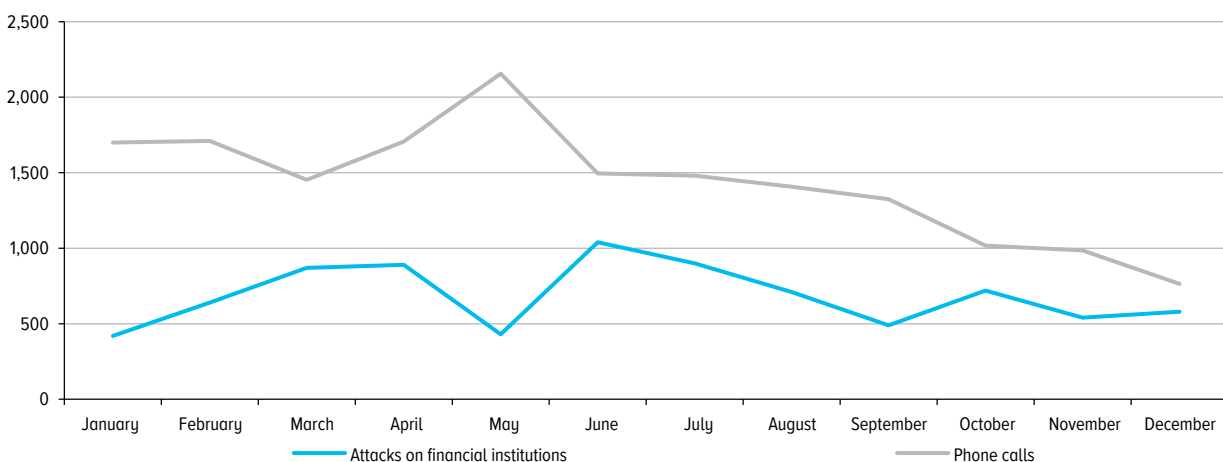
Bulletin	Publication date	Date of attack described in bulletin (for 2024)	Period between bulletin publication and attack
Bitrix vulnerability (CVE-2021-4034)	7 July 2024	22 July 2024	Over two weeks
Bitrix vulnerability (CVE-2022-27228)	29 May 2023	9 March 2024	Over eight months
Use of GSocket	26 July 2024	5 September 2024	Over one month

The incidents created conditions that allowed the attackers to leak client data of the compromised institutions, disrupt the functioning of technological processes and hardware complexes, and spoof information on websites.

The effect of the exploitation of a vulnerability in a financial institution's infrastructure by perpetrators becomes evident during the next two to three months in the form of target attacks on the institution's clients through using stolen client data and means of payment (Chart 10).

CORRELATION BETWEEN ATTACKS ON FINANCIAL INSTITUTIONS AND NUMBER OF AUTHORISED FRAUDS

Chart 10



Source: Bank of Russia data.

Financial CERT started in 2023 and continued in 2024 active work to collect and analyse data about information infrastructures, including data processing centres, critical nodes of technological processes, cloud computations, processing centres, etc.

As a result, Financial CERT has comprehensive data about information infrastructures, which enables Financial CERT to find and analyse data about threats to particular information exchange participants or technological infrastructures and to prepare recommendations on response measures and lists of relevant organisational and technical measures.

Timely processing of information provided by Financial CERT is an important business process in financial institutions' operations, alongside other key processes intended to ensure cyber security of information infrastructures.

Monitoring of operational resilience incidents

In 2024, as part of the monitoring of accessibility of services and platforms provided by financial institutions, Financial CERT identified over 1,500 occurrences supposedly connected with malfunctioning of various technological segments and sent the related information to financial institutions. The latter confirmed 680 of the identified occurrences (44%) as failures of various information infrastructures. Financial institutions recognised 429 occurrences as operational resilience incidents, which is 63% of the total number of the identified failures.

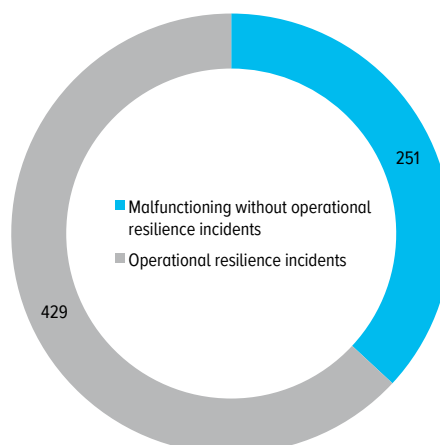
The operational resilience incidents were mostly associated with IT disruptions in financial institutions' information infrastructures (86.8%). However, 13.2% of these incidents were caused by cyber attacks, in particular DDoS attacks.

The main technological processes affected by these operational resilience incidents were online platforms for remote services and accessibility of transactions (47%) and money transfers on behalf of individuals between their bank accounts (33%).

The most serious operational resilience incident occurred in 2024 Q2 and lasted for five days. As a result of that disruption, the financial institution faced significant problems with servicing clients, namely opening accounts, issuing loans, etc. The average downtime of services and platforms was 5.6 hours.

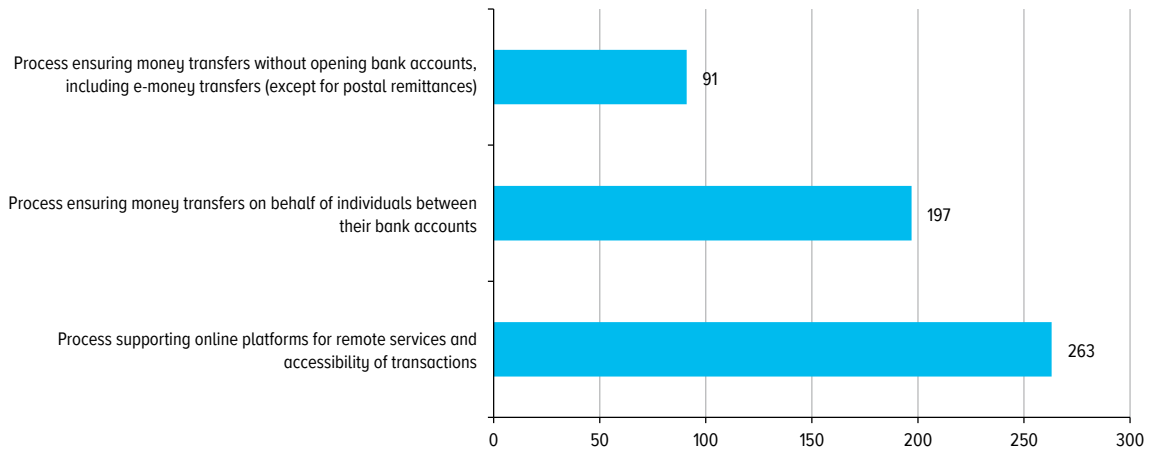
OPERATIONAL RESILIENCE INCIDENTS

Chart 11



PROCESSES DISRUPTED / UNAVAILABLE MOST FREQUENTLY

Chart 12



Source: Bank of Russia data.

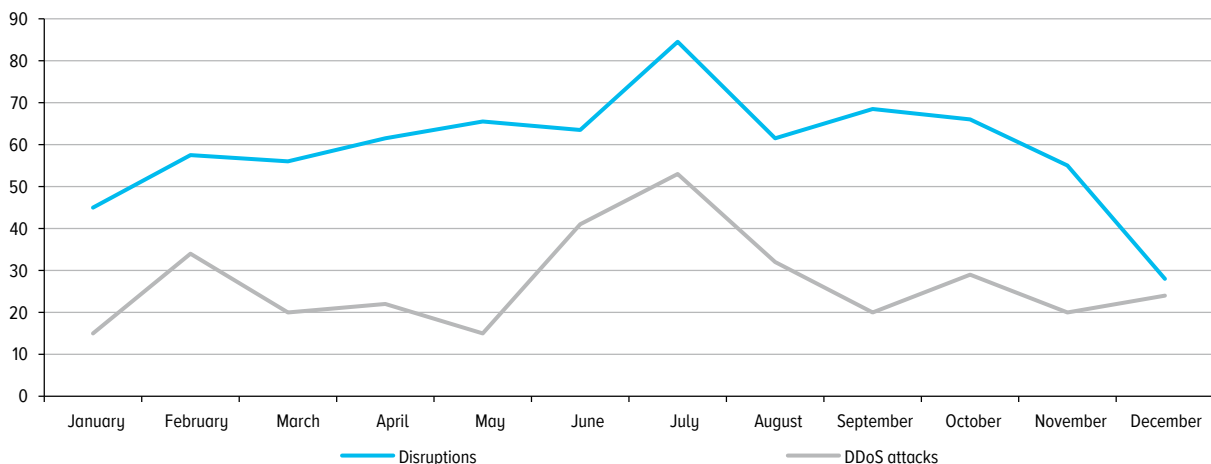
It is worth noting that as little as 8% of the disruptions were caused by attacks on financial institutions' information infrastructures. However, the correlation between the events is rather high. Thus, circumstantial evidence suggests that the disruptions were directly related to cyber attacks on financial markets.

Timely measures to counter potential risks of malfunctioning or failures of technological equipment in information infrastructures located in critical technological segments will improve the accessibility of services and platforms provided by financial institutions and thus strengthen people's confidence in financial institutions.

When informing Financial CERT about identified operational resilience incidents, information exchange participants use a special form approved by Bank of Russia Standard STO BR BFBO-1.5-2023. Filling in the form, an information exchange participant should specify the technological process affected as a result of an operational resilience incident and the reasons for the latter.

CORRELATION BETWEEN DISRUPTIONS AT FINANCIAL INSTITUTIONS AND CYBER ATTACKS ON THEM

Chart 13



Source: Bank of Russia data.

Financial CERT also uses this information to notify financial market participants having similar hardware and software about existing problems so as to prevent risks of such operational resilience incidents in their infrastructures.

Therefore, by timely updating the information about hardware and software, financial market participants greatly contribute to the stability of services and platforms provided by financial institutions in the Russian Federation.

Attacks on financial institutions' clients

Following a successful attack on commercial institutions processing sensitive data, perpetrators leak the information that is then used for targeted attacks on individuals. Malefactors' techniques are becoming increasingly sophisticated, which inevitably increases the number and amount of thefts from attacked individuals.

Countering social engineering and phishing attacks requires all organisations concerned to take joint measures.

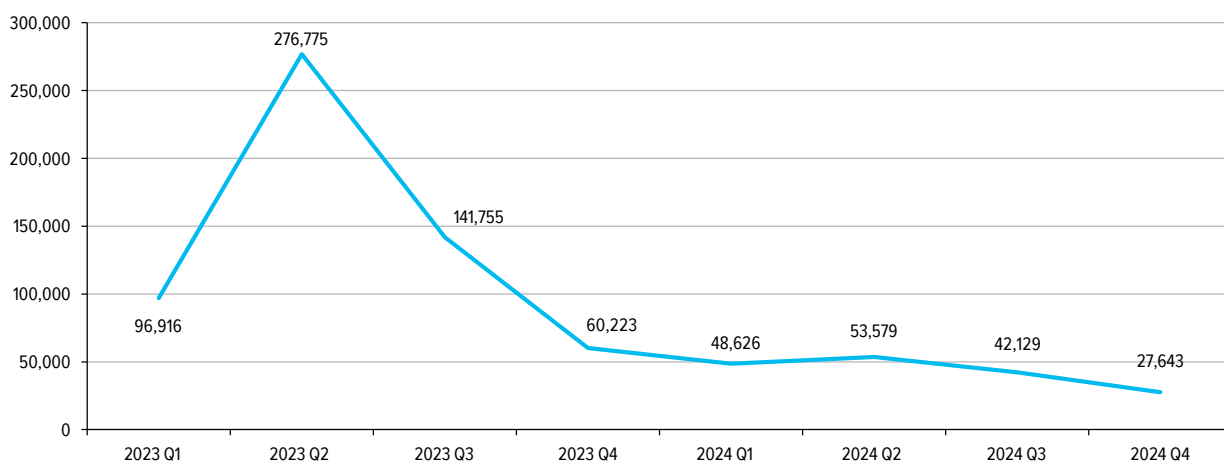
From the middle of the previous year, Financial CERT records a reduction in the number of fraudulent phone calls (Chart 14).

As a result of the comprehensive state regulation and approach to ensuring communications providers' compliance with the requirements for rendering communications services and traffic transmission to public communications networks (a number of relevant amendments were introduced in 2023–2024 to Federal Law No. 126-FZ, dated 7 July 2023, 'On Communications' (Federal Law No. 126-FZ), it is becoming more difficult and expensive for malefactors to make mass phone calls.

In particular, beginning from 2023, all communications providers are obliged to verify the information about phone calls when transmitting traffic via their networks and stop rendering communications services as soon as they detect violations of the requirements stipulated by Federal Law No. 126-FZ. Furthermore, at the end of 2024, the Government of the Russian Federation adopted Resolution No. 1898, dated 26 December 2024, 'On Amending Certain Acts of the Government of the Russian Federation' restricting opportunities for telephone fraud.

PHONE NUMBERS SUBJECT TO BLOCKING

Chart 14



Source: Bank of Russia data.

The regulation amends the list of licensed activities in the course of provision of communications services. In particular, the Government excluded the services of VoIP phone services from the list of licensed activities. VoIP technology made it possible to communicate through the internet (organise phone calls) with a person who used a landline or mobile phone.

However, social engineering is still one of the most acute problems. Traditional mass phone calls have been replaced with calls via popular messengers.

The main scenarios used by malefactors in 2024 can be grouped into several topics.

1. Extension of various contracts

Fake stories in this category of scenarios were as follows:

- extension of a compulsory medical insurance (CMI) policy: scammers, impersonating insurance companies' and healthcare organisations' employees, notified people that they needed a new CMI policy;
- renewal / extension of a mobile service agreement: malefactors, impersonating mobile operators' employees, notified people that they needed to immediately extend their mobile service agreement;
- expiry of a bank payment card: perpetrators made similar calls, only changing the name of their alleged employers; and
- extension of a comprehensive motor insurance or compulsory motor third-party liability insurance policy: malefactors used the same scenario as in the case of a CMI policy.

2. Phone calls from financial institutions' security units

Perpetrators continue to use this traditional scheme. In 2024, malefactors tended to switch to phone calls with recorded announcements instead of impersonating security officers as before. After a brief phone survey, the victims were allegedly rerouted to a call centre agent or an employee of law enforcement agencies.

3. Phone calls from law enforcement agencies

Impersonating an officer of the Ministry of Internal Affairs or federal services, a fraudster notifies a person about a criminal case initiated against him/her or a fact of using his/her personal data to steal his/her funds or commit other illegal actions and asks the person to assist the authorities in detaining the criminals. In most cases, perpetrators steal the borrowings obtained by the victim at a financial institution.

4. Public services, government support, and compensations

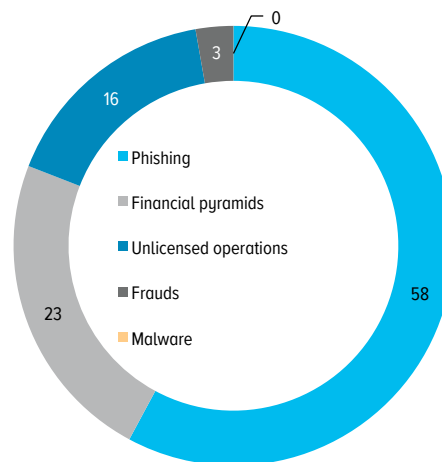
Depending on a particular scenario, malefactors call and inform a person about the opportunity to receive social and other payments, join various federal and municipal support programmes, or take part in a volunteer movement, or the need to check fines or access to school online accounts, and so on.

In 2024, there was also a large number of attacks on customers through phishing websites and websites created for unlawful financial operations, etc.

Thus, over 2024, Financial CERT detected and initiated the blocking of over 46,000 domains used to carry out phishing attacks and disseminate information about illicit financial operations and financial pyramids. This indicator was 20% higher than in 2023.

TYPES OF RESOURCES USED BY PERPETRATORS

Chart 15



Source: Bank of Russia data.

Over half of the blocked resources were phishing websites (58%) mirroring the names of popular banks and investment companies. The second most widely used type was financial pyramids (23%) which most often masqueraded as online games offering a user to earn up to 1,000% per annum after the purchase of a player character or game merchandise. Unlicensed operations in the financial market were also popular, accounting for approximately 16% of the total number of the blocked resources.

Cyber training with financial market participants

In 2024 Q4, Financial CERT organised cyber training with financial institutions (hereinafter, cyber training participants).

The scanning revealed 3,166 potential vulnerabilities at 130 financial institutions participating in the cyber training, which is 44% of the overall number of the participants. Furthermore, 666 (21%) of the identified vulnerabilities were high (with a CVSS1 score of 7–8.9) and 234 (7%) were critical (with a CVSS1 score of 9 or more).

Almost all cyber training participants promptly responded to the mailing and explored the notices about potential vulnerabilities in their information resources.

Having analysed the data about these vulnerabilities sent by Financial CERT, the participants implemented adequate measures to patch the vulnerabilities and/or take compensatory measures.

At the second stage of the cyber training, a number of financial institutions practised the procedure for submitting a request to pause electronic communication in the Bank of Russia Payment System (PS).

At this stage, Financial CERT tested the knowledge of financial institutions' specialists about the procedure for suspending electronic communication in the Bank of Russia PS in case of detection of unauthorised transactions in the Bank of Russia PS initiated by a participant as a result of a data protection incident caused by non-compliance with information security requirements in the course of money transfers, as well as the relevance of the list of authorised employees that should be regularly updated by financial institutions upon amendment.

Eight of the 42 participants (19%) failed to update the information about the employees authorised to sign and/or submit requests for pausing electronic communication in the Bank of Russia PS, which in reality might entail serious losses in case of compromise of the payment network of the information infrastructures of participants in the Bank of Russia PS.

The request to pause / resume electronic communication was filled in properly by 28 participants (67%). However, as little as 12 institutions coped with the task and sent the request for suspension at the first attempt. The rest of the participants needed two to five attempts to properly fill in and submit the form. Consequently, the participants lost a lot of time to fill in the request form appropriately.

The remaining 14 participants failed to prepare a proper request to be submitted to Financial CERT within the established period of the cyber training.

The Bank of Russia sent recommendations to all cyber training participants on how to enhance the security of their information infrastructures and update the information in Financial CERT's AIMS.

International cooperation

The Bank of Russia stipulates its competent participation in the development of an up-to-date agenda meeting Russia's interests as a key goal of international cooperation in information security and cyber resilience.

In accordance with the Guidelines for the Advancement of Information Security in the Financial Sector for 2023–2025, Financial CERT continued the development of international cooperation with national (central) banks during the period under review, in particular:

1. Financial CERT collaborated with foreign central (national) banks in the area of notification about urgent information security threats to effectively combat cyber attacks

As part of cooperation with the central (national) banks of the member states of the Eurasian Economic Union (EAEU) as well as Tajikistan and Uzbekistan, Financial CERT sent more than 470 bulletins with data about detected information security threats, including indicators of attacks of various hacking groups targeting financial institutions in the EAEU member states, Tajikistan, and Uzbekistan.

During the period of Russia's presidency in BRICS, Financial CERT intensified the efforts to inform the BRICS central (national) banks about urgent threats to information security by sending its bulletins through the special BRISC Channel.

Over the course of 2024, Financial CERT sent 13 bulletins about the most serious cyber attacks and vulnerabilities identified by Financial CERT.

2. Bank of Russia experts took part in the exchange of best practices aimed at aligning the approaches to elaborating information security and cyber resilience requirements as well as at improving professional skills of the central (national) banks' employees

As part of the measures implemented by the working group for ensuring information security of the financial market and countering cyber attacks in credit and finance, which consists of representatives of the EAEU central (national) banks, Financial CERT prepared the following documents:

- Recommendations on information security when using distributed ledger technology (DLT) that describe standard distributed ledger architectures, name possible violators, and list specific threats and measures aimed at neutralising these threats when using DLT in the banking sector.
- The regulatory digest describing the main changes in the Russian laws on information security.

Based on the results of BRICS collaboration, Financial CERT, jointly with experts, explored the BRICS countries' laws on cyber resilience in the financial sector as well as best practices in vulnerability analysis and intrusion tests and prepared two reports, namely:

- [Information Security Regulations in Finance](#), BRICS, 2024 (published on the Bank of Russia website); and
- [Best Practices in Conducting Penetration Testing and Vulnerability Assessments of Information Infrastructure Facilities](#), 2024 (published on the Bank of Russia website).

The content and progress of these studies were regularly discussed at the meetings of the BRICS central bank governors and ministers of finance that took place in 2024, including at the sites of the International Monetary Fund, the World Bank Group, and the Group of Twenty.

Furthermore, Financial CERT specialists took part in the Bank of Russia's practice-oriented information security training CyberCourse where they shared best practices of responding to information security threats with foreign colleagues from the EAEU and BRICS member states and representatives of other countries in the course of the event in June 2024.

3. Financial CERT collaborated with international cyber incident response teams and groups of the BRICS central (national) banks to organise the first cross-border cyber training

In 2024 Q3, Financial CERT organised the first cross-border cyber training with the BRICS central banks' representatives.

The cyber training included two stages. The first one took place remotely at the beginning of August 2024: the participants practised communication in terms of exchanging information about a detected information security threat using the bulletins prepared in accordance with the format of the BRISC Channel.

The second stage was offline and took place at the Innopolis University (the Republic of Tatarstan) from 16 through 19 September 2024: the participants practised the skills of responding to cyber attacks, using various tools to identify attacks and IoCs, and eliminating consequences of cyber attacks.

Based on the results of the cyber training, the participants approved the following promising areas for the development of the BRISC Channel:

- Annual BRICS cyber drills to expand the collaboration and ensure that the BRISC Channel can help effectively combat urgent threats to information security.
- Advancement of the BRISC Channel by adding new data and practices aimed at strengthening information security in the financial sectors of the BRICS member states.
- Enhancement of cross-border security of payment instruments used by BRICS citizens and the level of their confidence in these instruments.

Following the two stages of the cyber training, BRICS representatives highly praised the organisation of the events, expressing the hope that the BRICS countries would further deepen their cooperation in the area of information security of their financial sectors.

In 2025, Financial CERT will continue to develop the practice of cyber training among the national (central) banks of the member countries of the interstate unions.¹ The main areas of the cooperation will be as follows:

- increasing the quality and pace of communication among the national (central) banks; and
- practising the skills of identifying and responding to operational risks caused by cyber attacks.

¹ EAEU, ASEAN, SCO.

FINANCIAL CERT'S COOPERATION AREAS IN 2025

In 2024, Financial CERT completed the work within the established working group to organise the exchange of machine-readable bulletins among the participants in the information exchange with Financial CERT.

As a result of this work, Financial CERT organised daily publication of machine-readable bulletins in six adapted formats allowing download directly to monitoring and information security tools.

Today, Financial CERT continues to enhance its bulletins containing IoCs by increasing the number of suppliers of cyber attack data and improving the format of released information.

In 2025, Financial CERT plans to divide the data it releases into groups by type of IoCs, linking them through a unified key – event identifier.

This approach will enable information exchange participants to collect either automatically or manually comprehensive information about cyber attacks by any indicator of detection.

It will become possible to download indicators of detection directly to particular monitoring and information security tools, and information exchange participants will be able to easily apply the rules and correlate events without using additional measures to single out specific indicator types.

In 2025, Financial CERT plans to create a unified database of cyber attack indicators. By accessing this database, information exchange participants will see all historical records on all cyber attack indicators published by Financial CERT.

If financial institutions timely update the information on IP addresses, domain names, and URL addresses used in their operations, this will help Financial CERT more efficiently identify suspicious behaviours supposedly connected with cyber attacks and notify all information exchange participants thereof.

2025 TRENDS

Taking into account the current level of information security, key trends in cyber attacks in 2025 will most likely be as follows.

More attacks via supply chains

A key trend in cyber attacks will be a growing number of attacks via supply chains, which is because clients fail to set specific requirements for the level of IT providers' information security. Malefactors increasingly frequently exploit vulnerabilities in providers' products or infrastructures to compromise larger institutions. Attackers are thus able to bypass traditional protection tools, exploiting trust relationships between target companies and their contractors.

Shifting focus on small and medium-sized institutions

Malefactors continue to adjust their techniques focusing on companies having limited resources for ensuring their information security. The main reasons why small and medium-sized institutions are becoming the main target are as follows:

- **poor protection:** as long as the budgets for technical and organisational security measures are limited, these institutions are unable to implement advanced threat monitoring and prevention systems and organise adequate operational control over security measures;
- **insufficient experience and resources:** small companies often have only limited capacities to engage highly qualified information security and incident response specialists or lack experience in high quality organisation of and support for this work under service contracts; and
- **simplicity of compromise:** typical attacks (phishing, brute force, exploitation of outdated or misconfigured systems) on small institutions are especially effective.

Small **regional firms** or subsidiaries of large companies are particularly vulnerable. Their awareness of modern cyber threats is lower, while operational control over information security measures is not always harmonised within the overall information security strategy. These companies either invest insufficient funds in their cyber security or fail to adhere to a unified risk-based approach, thus becoming an easy target for attackers.

Increasing destructive effects of cyber attacks

1. Growth in reputation attacks: the number of attacks aimed at disrupting confidence in institutions is expected to increase. It is possible to predict data leaks, manipulations with corporate systems, and publications of data causing public distrust (e.g. compromise of financial statements).

2. Evolution of ransomware¹ attacks. In 2025, ransomware attacks will remain one of the main types, but their focus will shift:

- **blackmail by threatening destruction:** instead of encrypting data, malefactors may demand a ransom by threatening to destruct data;

¹ Ransomware is a type of malware that encrypts a victim's data and prevents access until a ransom is paid.

– **more sophisticated attacks:** taking into account the release of a number of ransomware source codes (Babuk, Conti, and LockBit 3 (Black)), it is possible to expect new increasingly sophisticated and destructive ransomware modifications developed even by small low-skilled hacking groups.

3. Growth in ransomware as a service (RaaS): the leak of source codes in 2024 will make the ransomware ecosystem more complicated. More advanced ransomware versions will be provided as a service via platforms where malefactors will be able to rent tools for an attack, thus reducing development costs.

Difficulties in identifying and attributing attacks

To conceal attacks, perpetrators extensively use complex chains of intermediary nodes, such as compromised servers, VPN, and mobile proxies, thus making it more difficult to:

- **detect attacks:** perpetrators disguise their actions as legitimate user traffic, perform attacks in several phases, and use various attack vectors;
- **attribute attacks:** by using a chain of Russian addresses, mobile ASNs, and traffic tunnelling, malefactors make it impossible to identify the actual initiator of an attack.

Moreover, companies with a complex organisational structure and a variety of IT assets that will be the main target of attacks often lack monitoring tools to detect sophisticated cyber attack schemes and adequate experience to combat these attacks.

Growth in attack dwell time

A key tactic predicted in 2025 is an increase in the dwell time of an attack, that is, the interval between an attacker's initial intrusion into a system and its detection. The objectives of this tactic are:

- **collection of information about infrastructure:** perpetrators will stay in a system as long as possible to explore its network infrastructure, identify technical parameters of information security tools, and find vulnerabilities in the entire infrastructure;
- **delayed exploitation:** backdoors and implants left by malefactors will be used months and even years after the initial compromise.

This approach is especially effective against companies that fail to conduct information security audits of their computer systems on a regular basis.

RECOMMENDATIONS TO PREPARE FOR 2025 THREATS

Small and medium-sized, including regional, firms are advised to:

- invest in basic monitoring and security systems; implement security event monitoring systems (endpoint detection and response systems / antivirus software with centralised control);
- enhance staff training, especially in anti-phishing protection; and
- conduct regular audits of information security, as well as engage certified specialists to examine the security of the perimeter, network configurations, and servers.

Attacks on supply chains require particular attention to contractors and partners, which is why it is critical to:

- assess the maturity of suppliers' information security processes;
- make sure that contractors use secure communication channels and regularly update software;
- establish stringent rules for external partners' access to internal systems; and
- use an isolated environment to work with data received from contractors.

To counter attacks from Russian IP addresses, it is necessary to:

- analyse behaviour patterns based on the reputation of the source to identify network abnormalities; and
- limit access to critical segments for users and services from general-purpose networks.

To protect infrastructures against attackers' persistent access, it is needed to:

- conduct regular audits of information assets;
- carry out regular cyber drills for both operations staff and information security units of an institution; and
- regularly check systems for backdoors and malware, as well as do post-incident analysis of computer systems.

To combat cryptoware attacks, it is essential to:

- isolate backup copies and regularly test data restoration from them;
- implement centralised patch management to fix vulnerabilities; and
- introduce multi-factor authentication, as well as limit access to critical data.