Bank of Russia

OVERVIEW OF THE MAIN TYPES OF CYBER ATTACKS IN THE FINANCIAL SECTOR IN 2023

Moscow
2024

CONTENTS

This review was prepared by the Information Security Department.

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

INTRODUCTION

This review provides information on the main types of cyber attacks and incidents in the financial sector detected by FinCERT in 2023, a behavioural analysis of the actions of cyber attackers, and a cyber threat landscape.

An increase in the number of attacks exploiting vulnerabilities in web services and website management systems as well as attacks targeting developers and integrators of various IT solutions used in the financial sector were the main 2023 trends. The key attack vectors did not change significantly: DDoS attacks, phishing, mass distribution of malicious software (malware), and brute force attacks to compromise the accounts of both employees and clients remain the most common ones.

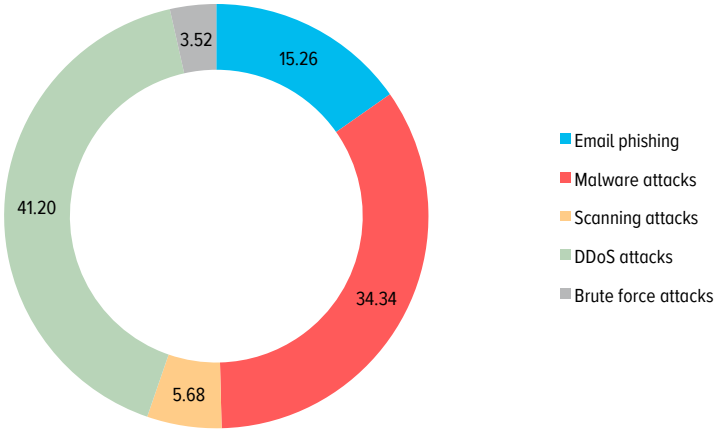
Social engineering attacks are also becoming increasingly more successful due to well-developed scenarios: attackers masquerade as government authorities more and more often in order to gain the trust of potential victims through emails and calls and then persuade them to visit a fake website, download software that will be used to steal the money, or provide critical information, such as codes from the text messages. It should be noted that these types of attacks are still gaining momentum due to their technical simplicity and high efficiency. A distinctive feature of social engineering attacks in 2023 was preliminary gathering of information about a person to make the personalised scenario used as realistic as possible. Attackers get such information both from open sources, such as social media, and by compiling leaked data from various databases obtained through successful cyber attacks against various organisations (including financial institutions) that process clients' personal data, as well as other protected information.

It should be specifically noted that attacks against third parties – providers of various IT solutions used in the financial market – became more frequent in 2023. By penetrating the infrastructure of organisations, the attackers stole data and identified ways to gain a foothold in the infrastructure of service providers for further remote connection to the infrastructure of their customers, including financial institutions. The use of various tools enabled the attackers to move horizontally within the organisations' networks. Such attacks are dangerous as they are difficult to detect: a financial institution deems the connection to the environment (network segment) available to the contractor to be authorised and does not hurry to terminate it. As a result, it may face a global leak of sensitive information, mass encryption of documents on the company's servers, and disruption of information systems.

CYBER ATTACKS AGAINST THE FINANCIAL SECTOR

In 2023, the Bank of Russia received more than 1,000 reports from information exchange participants about cyber attacks and incidents targeting their infrastructures via the Automated Incident Management System (FinCERT AIMS). A detailed comparative analysis of the received requests led to conclusions about the changes in the 2023 threat landscape and identified the most common types of attacks, main tactics and techniques used by attackers, etc.

BREAKDOWN OF CYBER ATTACKS IN 2023 *Chart 1*
(%)



In 2023, there was a decline in distributed denial-of-service attacks (DDoS attacks) (see section 'Operational resilience incidents resulting from DDoS attacks'). However, such cyber attacks remain the most common type and account for 41.20% of the total number of analysed cyber security incidents against credit and financial institutions. This is explained by simplicity of such attacks: an attacker does not need to have advanced technical background or any special knowledge to carry out a DDoS attack. For example, one can find many adverts on hacker forums for the sale of access to botnets that are used for standard DDoS attacks.

Malware attacks and email phishing also remained common in 2023, accounting for 34.34% and 15.26%, respectively, of the total number of incidents analysed. These attacks start in the same way: an email with an attachment is sent to an employee of the attacked organisation. The email may contain:

- A link for downloading a file, which requires the recipients to enter their corporate account details in order to download the attached file. If the data are entered, the user's account will be compromised and the data will be sent to a server controlled by the attacker. This is a type of email phishing attacks.
- A .doc, .docx, .xls or .xslx file that, when opened, will send a request to the server controlled by the attacker, resulting in an installation of malware on the user's computer and its launch. These are malware attacks.
- An archive or an image file that, when opened, will install malware on the user's computer. These attacks are also classified as malware attacks.

In 2023, credit and financial institutions reported nearly 50 cyber security incidents resulting in various data leaks and, in a number of cases, money thefts of over ₽51 million. More than 50% of the successful attacks occurred due to the exploitation of vulnerabilities in organisations' infrastructures. The perpetrators exploited the following common vulnerabilities and exposures (CVE) in their cyber attacks:

- CVE-2023-20198 is a vulnerability in the web interface of Cisco IOS XE, associated with endpoint privilege management errors. Exploiting this vulnerability allows attackers to escalate their privileges on a compromised device. During a cyber attack against one of the credit and financial institutions, CVE-2023-20198 was exploited resulting in a cyber security incident. However, timely detection of the compromised device and unauthorised connections from it averted any grave implications for the institution.
- CVE-2022-41352 is a vulnerability in the cpio archive unpacking utility of Zimbra Collaboration Suite – corporate email management software – which involves unrestricted uploading of malicious files. Exploitation of this vulnerability allows a remote attacker to gain unauthorised access to sensitive information. This is exactly how, during the cyber security incident mentioned above, the attackers gained access first to the mailbox of one of the institution's employees and then to the control panel of the hosting provider's server where the institution's database of external users was located, resulting in a data leak.
- CVE-2023-4966 is a buffer outflow vulnerability in Citrix Application Delivery Controller (Citrix ADC) and Citrix Gateway, a consolidating remote access infrastructure. When exploiting this vulnerability, an attacker can remotely impact the confidentiality, integrity, and availability of protected information. Timely notification of credit and financial institutions using this software made it possible to detect and localise a cyber security incident in one of the institutions before it led to adverse consequences.
- CVE-2022-27228 is a vulnerability in the vote module of the content management system (CMS) of 1C-Bitrix, entailing a possibility of sending specially crafted network packets. The exploitation of this vulnerability allows a remote attacker to execute an arbitrary code on a vulnerable system.

  The cyber attacks against credit and financial institutions included cyber security incidents related to modifying the content of financial institutions' information resources and data thefts.

In addition, there were cases of brute force attacks on technical accounts, making up 3.52% of the total number of incidents analysed. Such attacks were successful because the accounts for working with the system used dictionary passwords which the cyber criminals managed to crack.

CMS Bitrix

Numerous exploitations of CVE-2022-27228 in CMS Bitrix in 2023 (FinCERT detected nine successful hacks of information exchange participants' external infrastructure through the vulnerability in CMS Bitrix) resulted in dissemination or sale of sensitive information on the dark web. In some cases, the attackers did not steal any information, but altered the institution's website content by publishing false materials.

Let us look into this vulnerability in detail.

In 2023 Q2, the Russian segment of the Internet suffered a mass defacement of web servers. The investigation of the incidents found that the attackers targeted CMS Bitrix. It is worth noting that the information resources of financial institutions affected by the cyber security incidents were not always controlled by their owners but by contractors outsourced by these institutions. A successful attack resulted in the exporting of confidential data from the attacked website, in some cases followed by changes in the content of the website home page, along with data exfiltration. The vulnerability was found in the vote module up to version 21.0.100 and CMS up to version 22.0.400.

We know that the perpetrators used two vectors to exploit the vulnerability:

1. *Arbitrary Object Instantiation in the 'Polls, Votes'/vote module.* The 'Polls, Votes' module was used by the resource owners to receive feedback from website users. Exploiting this vulnerability allowed the remote attacker to write arbitrary files in the system through sending specially crafted network packets. Upon logging of POST requests by the web server, a string containing a successful POST request to the /bitrix/tools/vote/uf.php file was written to the log file as a result of a successful exploitation of this vulnerability:

```
***POST
/bitrix/tools/vote/uf.php?attachId[ENTITY_TYPE]=CFileUploader&attachId[ENTITY_ID][events][onFileIsStarted][]=CAllAgent&attachId[ENTITY_ID][events][onFileIsStarted][]=Update&attachId[MODULE_ID]=vote&action=vote HTTP/1.0" 200 ***
```

   A successful attack allowed the cyber criminal to remotely execute an arbitrary code, defacing the website or exfiltrating the data.

2. *Arbitrary File Write in the 'Visual Editor' module.* The 1C-Bitrix: Site Management includes the fileman service module which implements the HTML-editor feature. The module includes a vulnerable script html_editor_action.php. Thus, the exploitation of the script vulnerability allowed an unauthorised remote user to execute an arbitrary code on the target system. As a result of a successful attack, a line containing a POST request to the vulnerable /bitrix/tools/html_editor_action.php file was displayed in the web server log file:

```
***POST /bitrix/tools/html_editor_action.php HTTP/1.0" 200 ***
```

   The main actions of the attackers after exploiting the vulnerability were to:
   - replace index.php in the root directory of the web application;
   - embed a malicious code in php-scripts of modules;
   - delete the /bitrix/.settings.php file;
   - create agent scripts with a malicious code or modify existing scripts;
   - delete data from the following database tables: b_iblock, b_iblock_element, b_iblock_element_property;
   - create .htaccess files in all directories of the web application; and
   - create php-scripts in the/bitrix/admin/ directory with arbitrary file names.

Based on the incident analysis, FinCERT issued three information bulletins with recommendations for identifying and fixing the vulnerability, countering such attacks, and minimising risks to the information infrastructures of information exchange participants.

Main tactics and techniques of cyber attacks in the financial sector

As noted above, mailing was the most popular method of delivering malware to an organisation's users. In 2023, FinCERT analysed over 180 targeted cyber attacks related to the propagation of malware via emails.

The geographical breakdown of these attacks is shown in Chart 2.

FinCERT considers the following parameters to analyse the geographical breakdown of attacks:

- 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 most popular mail servers used for malware distribution and command-and-control servers were workstations located in the United States (41% of the total number of malware mailings in 2023) and the Netherlands (35%). This breakdown leads to the conclusion that mail servers in these countries are the most bulletproof[1] ones.

The most popular locations for email phishing and storing stolen user data were mail servers hosted in Southeast Asia (48% of the total number of phishing mailings in 2023).

Charts 3 and 4 do not show all countries from which cyber attacks originated as the number of attacks from some countries was small compared to others.

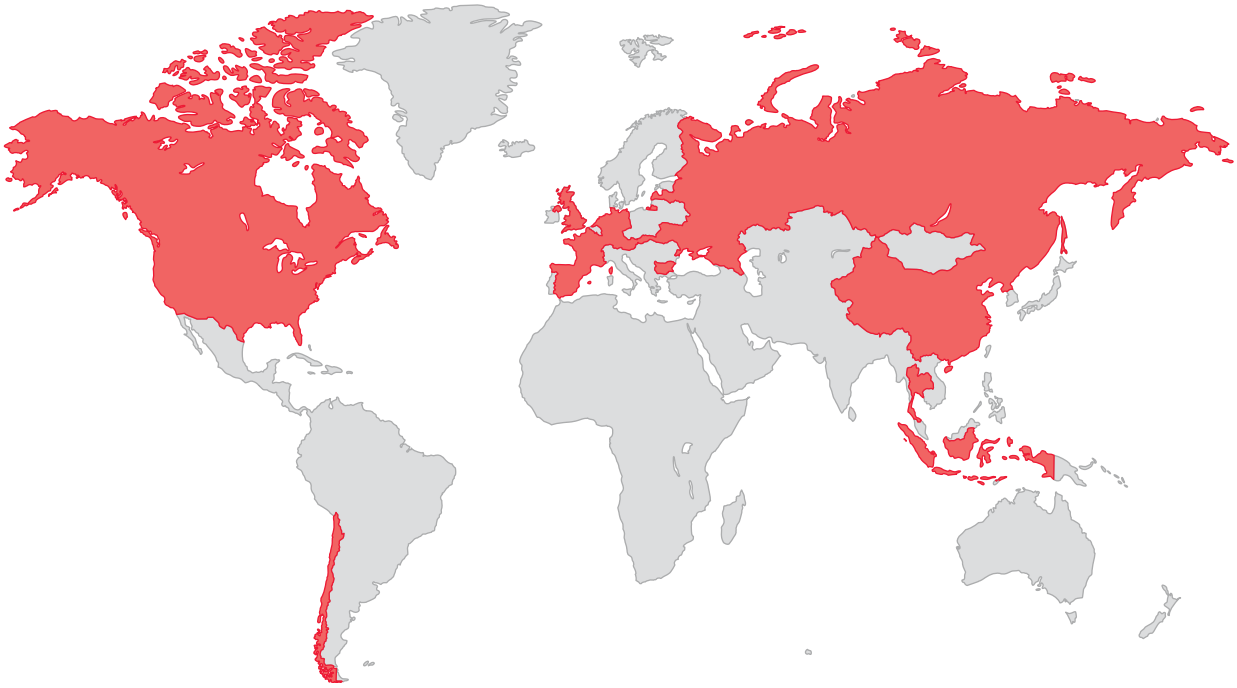
FinCERT publishes the IP addresses used in cyber attacks, malware hashes, and other indicators of compromise in machine-readable bulletins that are sent to information exchange participants on a daily basis. FinCERT regularly updates its sources of information on the geographic location and affiliation of IP addresses obtained during cyber attacks to make correct recommendations for configuring information security tools (ISTs).

FinCERT issued 242 machine-readable bulletins containing up-to-date indicators of compromise over 2023 to ensure prompt response to cyber security incidents. The machine-readable bulletins are published in five formats: .JSON, .STIX, .CSV, .IOC, and +.IOC to provide the most complete information on current threats to information exchange participants as well as to facilitate the application of the bulletins in all infrastructure-operated ISTs and endpoints. A new, sixth format of machine-readable bulletins – STIX 2.1 – has been published since 5 December 2023 and has the advantage of being able to link indicators and objects via relationships and visualise them. The STIX 2.1 format generated during the technical analysis of attacks and incidents not only contains indicators of compromise, but also allows visualising a detailed attack (incident) chain (Chart 5).

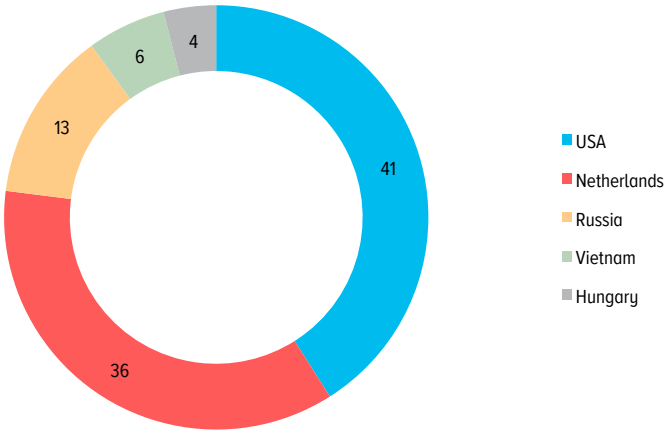
To respond quickly and minimise the risks of cyber attacks, it is necessary to understand not only where an attack is coming from, but also how the malware is delivered to its recipient:

[1] A bulletproof server is a server owned by a hosting provider that does not respond to complaints from Internet users (abuses). In case of complaints from users about the server and its content, for example, about malware on the server, the hosting provider does not respond to these complaints and does not provide personal data of its clients to law enforcement authorities.

GEOGRAPHICAL BREAKDOWN OF THE SOURCES OF TARGETED MALWARE ATTACKS VIA EMAILS IN 2023 *Chart 2*



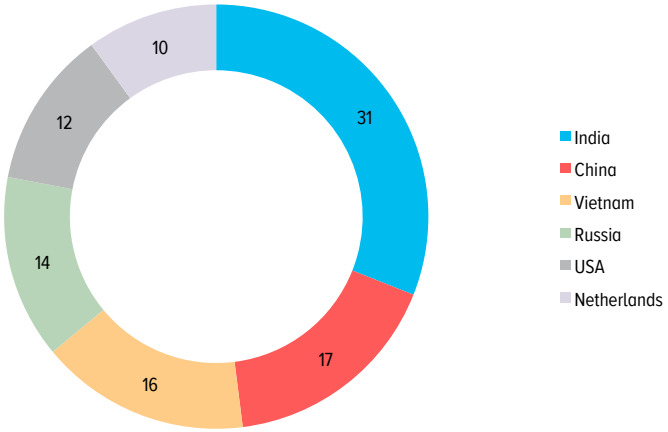
BREAKDOWN OF DETECTED MALWARE MAILINGS IN 2023 BY COUNTRY *Chart 3*
(%)



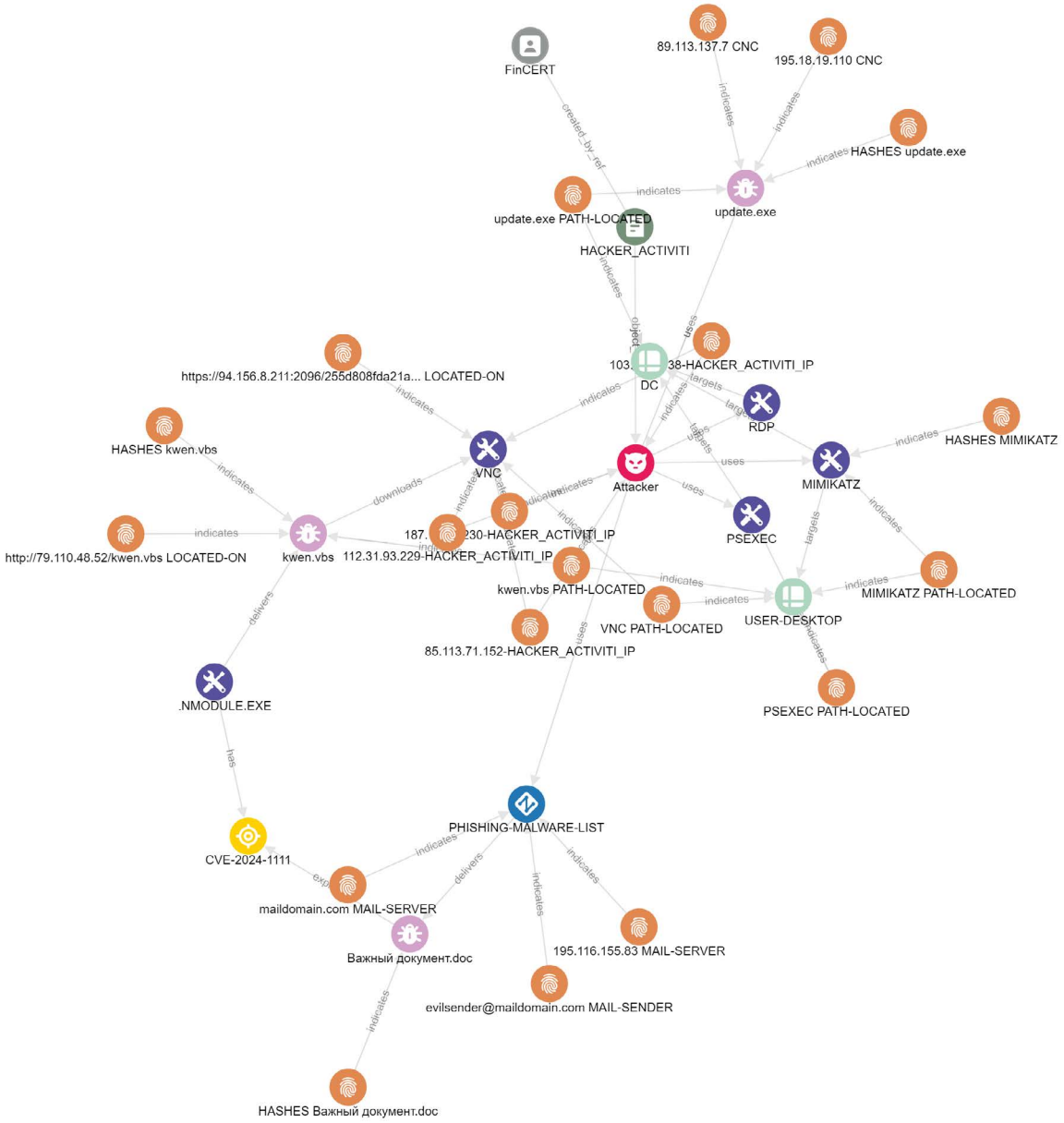
Mailing of MS Office documents

According to the results of FinCERT's analysis of malicious attachments received by FinCERT as part of reporting by information exchange participants, MS Office files, which exploit the 2017–2018 CVE-2017-11882 and CVE-2018-0802 in the Microsoft Equation Editor component, account for the bulk of the mailed malware. Such mailings were untargeted rather than targeted. It should also be noted that these malicious documents did not always download malicious files from the Internet, but instead used beacons that 'bounced' to the IP address harvesting resources, such as iplogger.org. The attacker thus conducted reconnaissance to find vulnerabilities in individual MS Office components and learn whether

BREAKDOWN OF DETECTED EMAIL PHISHING ATTACKS IN 2023 BY COUNTRY *Chart 4*
(%)



EXAMPLE OF VISUAL DISPLAY OF RELATIONSHIPS *Chart 5*



financial institutions' anti-virus systems would fail to prevent such attacks. A distinctive feature of such mailings is that reconnaissance attacks did not prematurely reveal the signatures of the 'belligerent' malicious payload.

Two main techniques of exploiting CVE-2017-11882 and CVE-2018-0802 were identified:

1. The extension of an .RTF file containing the exploit was changed to .doc, and then the file was emailed to its recipient with explanations urging the recipient to open the document. If the recipient had not patched these vulnerabilities, the malicious code was executed.
2. Another technique used a legitimate possibility of remotely uploading a macro to a Word document, including from the Internet, but instead of a macro, an .RTF file containing the exploit was uploaded and automatically processed by the application. The mailing scenario was the same. It should be noted that the same method is used to harvest the IP addresses of computer systems from which such documents were opened.

Since the attack is limited by the size of the malicious code in the exploits, its functions are typical: downloading an executable file from the Internet and running it. However, more advanced techniques were also identified, for example, using the Mshta.exe utility (Microsoft HTML Application). The advantage of this technique is that the malicious payload is not stored on the storage medium and is only executed in RAM.

The analysis of malicious documents revealed that only 10% of the cases had malicious content downloaded, the rest of the files had no payload due to server unavailability. This could be due to the following factors:

- The hosting provider owning the server was responding quickly to complaints from Internet users. As a result, the server was blocked by the hosting provider, making a further attack impossible. The attackers had to reconfigure the malware and send it out again.
- The attackers manually shut down the servers used when the attack failed to make it more difficult to analyse the incident during the investigation and avoid complaints about the server.

Mailing of archives and iso-containers with malware

The analysis of the files in archives and iso-containers allows us to draw the following conclusions:

- The attached files were distributed in the .PE format.[2]
- 90% of the attached files were designed for use in the .NET Framework. The main types of the malware used were Stealer[3] and KeyLogger.[4]
- The data were sent to the attacker's Telegram account or email.

Let us take a closer look at the types of malware detected.

Exploit.MSOffice.CVE-2018-0802.gen (16%), Trojan-PSW.MSIL.Agensla.gen (12%), and Trojan-PSW.MSIL.Stealer.gen (12%) were the most popular types among the analysed malware samples in 2023. These types of software enable the theft of user credentials as well as remote connection to and control of an infected device.

Self-extracting (SFX) archives containing malicious JS scripts and dynamic-link libraries (.dll) – buhtrap and the like – stand out from the other types of malware detected. It is noteworthy that these attacks most often involved spoofing of the email addresses of government agencies. The explanatory text in the emails with such attachments was in Russian.

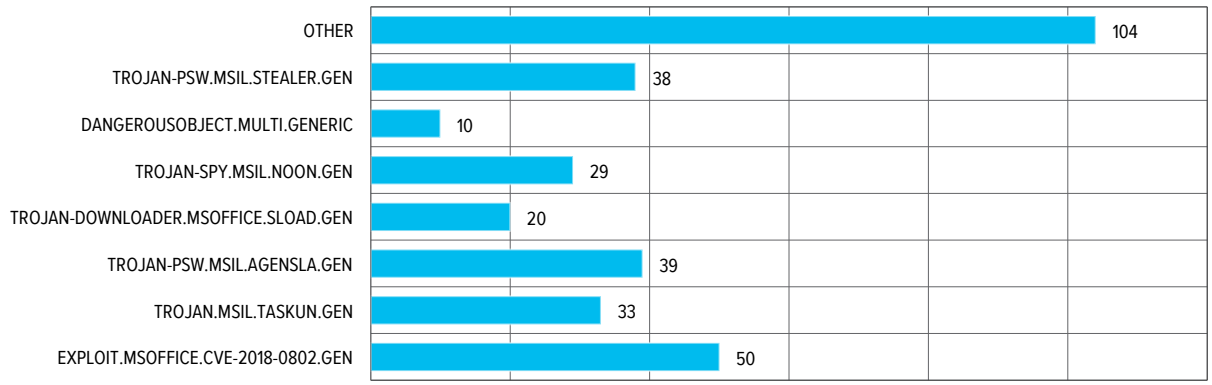
---

[2] PE (Portable Executable) is a file format for executables, object code, and dynamic-link libraries used in 32 bit and 64 bit versions of Windows operating systems.

[3] Stealer is a malware used to steal the login and password of a potential victim of a cyber attack.

[4] KeyLogger is a software that tracks various actions, keystrokes, and mouse clicks performed by a user.

TYPES OF MALWARE DETECTED OVER 2023 *Chart 6*
(NUMBER)



Based on FinCERT's analysis, the following conclusions may be drawn about the main tactics and techniques used by cyber criminals:

- Main vectors of attacks: the use of vulnerable services.
- In 2023, the attackers were able to successfully brute force passwords primarily owing to poor password policies on the accounts used for working with the system.
- The attackers used exposed credentials in third-party open source applications (e.g., projects on GitLab).
- Main methods to get foothold in organisations' network during a successful attack: cookie-backdoor, web-shell, ssh-key, creation of a new account by the attackers.
- Lateral movement when available for the compromised (created) account.

Based on these findings, FinCERT recommends the following measures to protect the infrastructure from identified attacks:

- Timely software updates.
- Strong passwords.
- Avoiding third-party applications (e.g., GitLab) to store authentication data or applying appropriate privacy settings to repositories.
- Conducting security analysis and scanning information systems for suspicious activity.

OPERATIONAL RESILIENCE INCIDENTS RESULTING FROM DDOS ATTACKS

As already mentioned in the review, in 2023, there was a decline in distributed denial-of-service (DDoS) attacks. The number of DDoS attacks decreased by 68.4% to 421 in 2023 compared to 2022. It should be noted that we are talking about atypical DDoS attacks[1] that are very different from everyday DDoS attacks. The most frequent attacks were transport layer (TCP SYN flood, UDP flood, NTP Amplification) and application layer attacks (http/https flood, SQL Injection attack, bruteforce).

The purpose of DDoS attacks is mostly to disrupt the availability of information resources; as a consequence, such attacks against the information resources of financial institutions disrupt the provision (availability) of services and facilities (online banking, mobile apps, money transfers, etc.). On 1 October 2022, Bank of Russia Regulations No. 787 P[2] and No. 779 P[3] came into force, establishing mandatory requirements for credit and non-bank financial institutions to ensure operational resilience in various operations stipulated by Federal Law No. 86 FZ, dated 10 June 2002, 'On the Central Bank of the Russian Federation (Bank of Russia)'.

FinCERT continuously monitors the availability of services and facilities provided by financial institutions and receives information on operational resilience incidents that have occurred at financial institutions. (An operational resilience incident is an incident involving a disruption in the continuity of critical processes as well as a breach of a financial institution's operational risk thresholds).

In total, FinCERT identified 719 disruptions at 174 financial institutions in 2023. At the same time, 77% (551) of the disruptions resulted in an operational resilience incident. The average process downtime was seven hours and 35 minutes.

FinCERT's analysis of disruptions at financial institutions found that most (85%) disruptions and operational resilience incidents had been caused by errors in the operation of IT systems and services used in the technological stages of critical processes. However, every seventh operational resilience incident (15% of the cases) was caused by a DDoS attack. The average downtime of financial institutions' services and facilities resulting from DDoS attacks was six hours. The largest disruption resulting from a DDoS attack lasted for six days during which the online services, processing systems, and bank payment processing systems in the acquiring network of the credit institution[4], including at several petrol stations, were completely unavailable for 36 hours. Because of this, a number of petrol stations in different regions of the Russian Federation experienced massive problems with customer service.

---

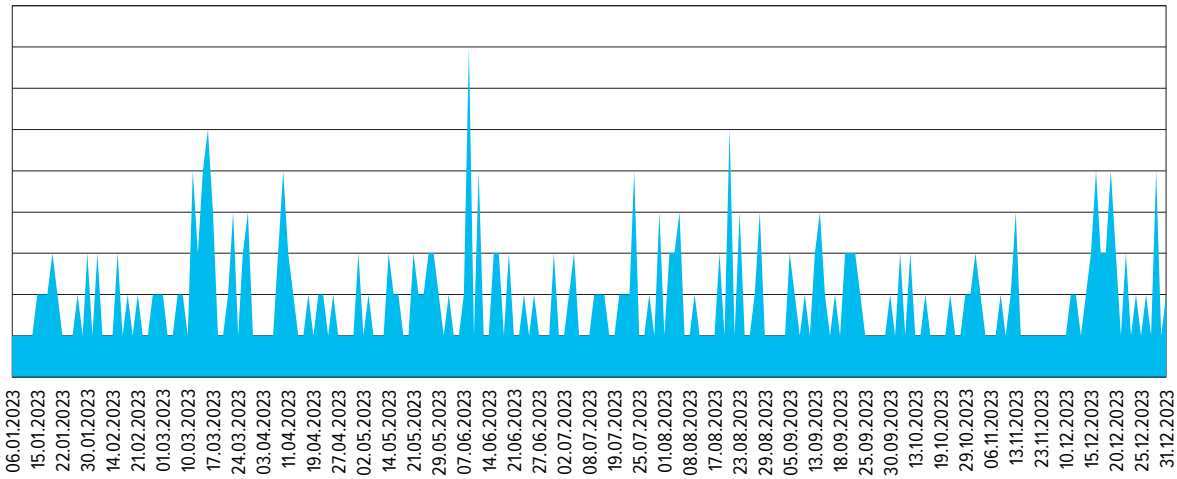
[1] In accordance with the list of cyber security incidents and cyber attacks given in Annex 18 to Bank of Russia Standard STO BR BFBO-1.5-2023.

[2] Bank of Russia Regulation No. 787 P, dated 1 October 2022, 'On Mandatory Requirements for Credit Institutions' Operational Resilience in Banking to Ensure the Continuity of Banking Services'.

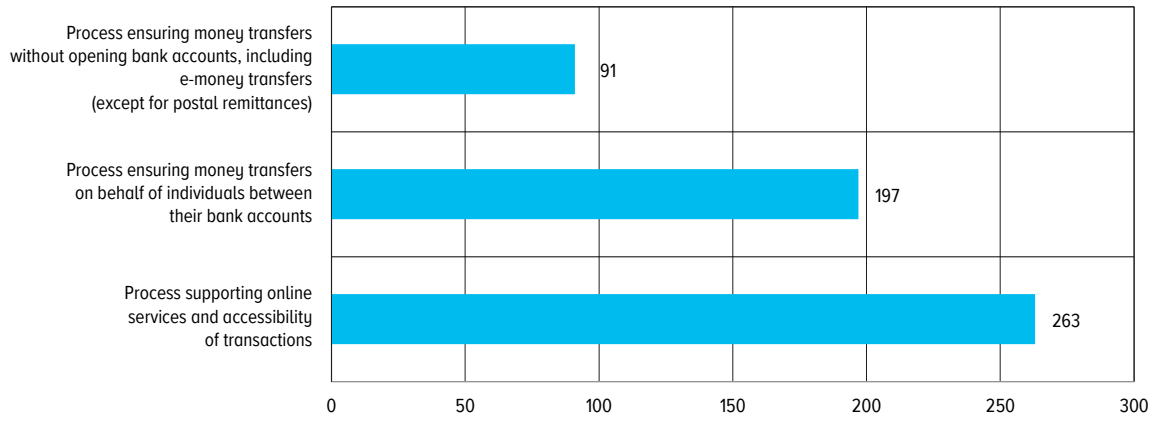
[3] Bank of Russia Regulation No. 779 P, dated 1 October 2022, 'On Mandatory Requirements for Non-bank Financial Institutions' Operational Resilience in Operations Stipulated by Part 1 of Article 76.1 of Federal Law No. 86 FZ, Dated 10 July 2002, 'On the Central Bank of the Russian Federation (Bank of Russia)' to Ensure the Continuity of Financial (Other than Banking) Services'.

[4] This credit institution is not a systemically important one.

DDOS ATTACKS AGAINST FINANCIAL INSTITUTIONS *Chart 7*



PROCESSES DISRUPTED MOST OFTEN *Chart 8*
(NUMBER)



Despite the operational resilience incidents identified in 2023, the average rate of unavailability of services and facilities at financial institutions facing disruptions did not exceed 0.5% of the total time of providing the services and facilities by these institutions.

Cyber attack trends indicate that the use of DDoS attacks as a primary vector (to disrupt the availability of information resources and the functioning of services) and a secondary vector (to conceal a parallel attack (impacting the infrastructure)) will be relevant in 2024–2025. FinCERT recommends financial institutions to use up-to-date DDoS attack mitigation systems, web application firewalls, and anti-spam (anti-bot) services.

DATA LEAKS IN THE FINANCIAL SECTOR

Full-scale attacks on Russians are carried out using information gathered in advance and containing data on individuals, their income, place of residence, availability of various banking products, social status, etc.

Therefore, a direct attack on an institution processing personal and other protected data involves potential high risks of subsequent fraudulent campaigns against the individuals whose data have been leaked.

According to FinCERT, in 50% of the cyber security incidents that occurred at both financial institutions and their contractors providing various solutions and services to them, the attackers exfiltrated confidential information, including personal and other protected data. Those were mainly personal data (59.6%), account credentials (21%), and payment card/bank account details (19.4%).

The Bank of Russia initiated and took part in the development of a draft law on qualification and business reputation requirements applicable to a financial institution's deputy information security officer. The current version of the document provides for, among other things, a higher level of personal liability of a financial institution's deputy officer for violations of information security requirements that resulted in the leak of personal or other protected data. The draft law is currently undergoing an interagency approval procedure. As a rule, for social engineering attacks, malefactors use compiled data from the databases of different companies from which the information has been stolen before. Taken alone, each of the stolen databases may contain no significant sensitive information. However, the compiled data provide insight into the life of each individual whose information has been leaked, including where they live, work, spend their free time, what their hobbies are, etc.

With the help of leaked information, attackers develop scenarios applicable to certain categories of people and then launch attacks using social engineering techniques. In doing so, they are able to ensure high efficiency of their calls and convince deceived people that their money is really at risk and needs to be 'protected'.

Another 2023 trend is brute force attacks to access email services, social media, online shops, marketplaces, and personal accounts of online banking customers. Attackers used stolen credentials for social media accounts, food delivery services, and other resources to guess a login – password pair (including using botnets) for authorisation. Having guessed the correct authorisation credentials, the attacker accessed the personal account and used it to continue the attack or stole confidential information or money.

FinCERT recommends the following measures to counter such attacks:

- regularly change passwords to personal accounts on the service platforms where confidential (personal) data as well as other protected information (payment card details, data on financial transactions, loans, etc.) are processed;
- avoid using identical passwords to personal accounts on different service platforms; and
- enable mandatory two-factor authentication, if available.

HYBRID ATTACKS AGAINST CLIENTS IN THE FINANCIAL SECTOR

During 2023, FinCERT received data from information exchange participants about over 100,000 successful cyber attacks against clients in the financial sector which were conducted using social engineering techniques. This number is more than twice the number reported in 2022. Most of these attacks involved making calls both over telecom networks and via messengers.

To counter such attacks, the Bank of Russia continues its joint work with the Ministry of Finance, financial market participants, and telecom operators. The number of calls using landline phone numbers (ABC numbering) declined by more than 75% in 2023. Nevertheless, attackers continue to actively use mobile numbers (DEF numbering) as well as messengers where they both make calls and send malware and forged documents. In addition, the number of calls using 8-800 numbering more than doubled this year, however, in relation to the total number of calls, it is still insignificant and accounts for no more than 1%.

The analysis shows that attacks are carried out by highly organised groups of attackers whose main centres are located outside the Russian Federation.

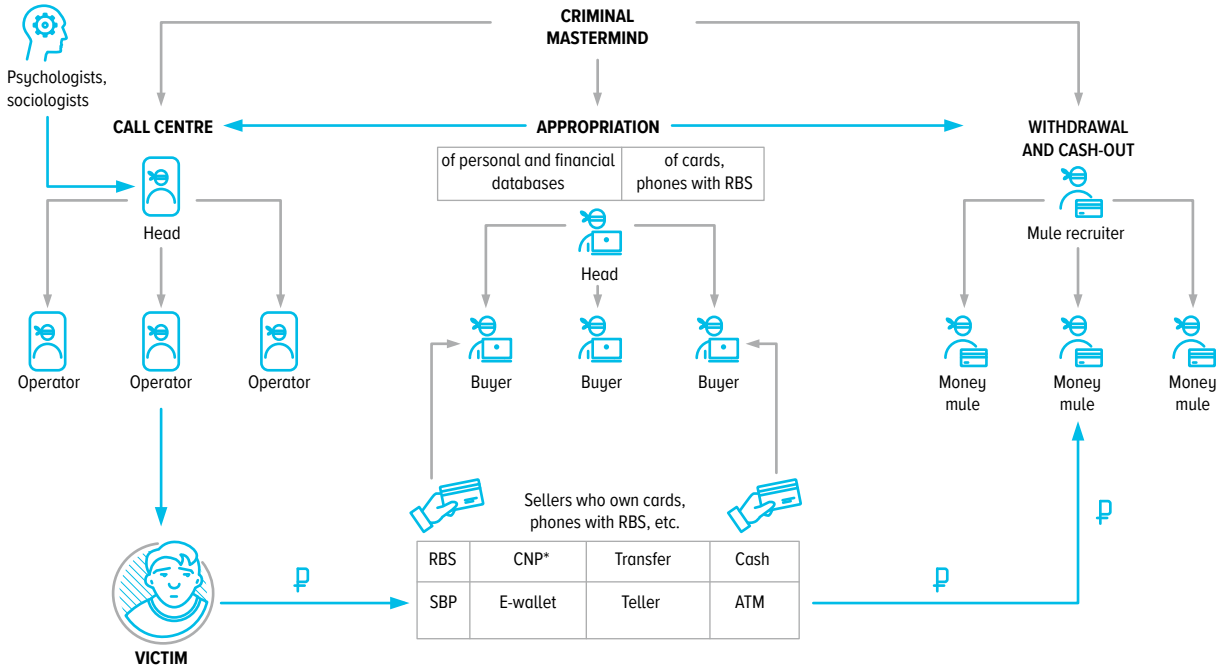
A typical structure of such a group includes:

- organisers who coordinate the call centre operations and are engaged in fund-raising; and
- staff making direct calls to Russians according to pre-prepared scripts (scenarios) and involved in withdrawal and cashing of money obtained unlawfully (money mules).

In 2023, attackers used the following common scenarios:

- Fraudulent calls on behalf of law enforcement agencies, the Bank of Russia, and telecom operators.

TYPICAL ORGANISATION OF CYBER FRAUD ACTIVITY *Chart 9*



** CNP means a card-not-present transaction (without presenting a physical payment card).*

The goal of fraudsters is to gain trust, including by sending forged documents to a potential victim via a messenger or email, prove the caller's identity using a fake agency website, and force the potential victim to take out a loan, cash out all personal funds, and deposit cash at an ATM into the fraudster's bank account.

- Fake messenger accounts of senior executives.

Using fake accounts of supposedly senior company executives, attackers send messages to employees asking them for help, for example, in apprehending fraudsters in the company and giving notice of an imminent call from an authorised law enforcement officer. The callers recommend the potential victims to follow their instructions clearly and not to tell anyone about the conversation. The attackers then call their potential victims and, on a variety of pretexts, try to gain access to their banking (both personal and corporate) data or persuade them to voluntarily transfer money to the accounts controlled by the fraudsters.

- Fraudulent websites where people are requested to take a survey on behalf of a well-known company for 'investment' purposes.

The goal of fraudsters is to obtain personal and financial data to entice the victim to make investments using a pseudo-investment platform.

- Fake resources of operating credit institutions and resources offering financial benefits on behalf of credit institutions.

The goal of fraudsters is to make users think the resource is authentic, obtain credentials for logging into their personal accounts, and install a remote access application on the victims' devices to steal funds through their personal accounts.

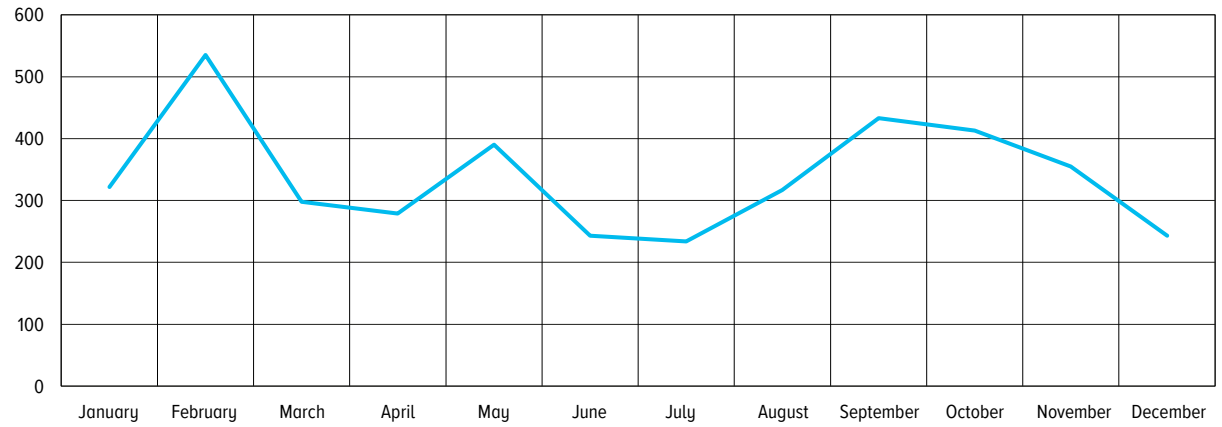
The above scenarios can be divided into a number of stages:

1. Reconnaissance

At this stage, perpetrators search for and obtain various databases containing information on individuals who are potential victims. As a rule, such a database is a compiled single document with data stolen from various shops, platforms, and information websites. One such file may contain data from leaked databases of delivery services, medical centres, financial and non-financial companies.

Additionally, cyber criminals turn to third parties and different platforms for collecting victims' data online. These platforms produce and deploy phishing resources that offer potential victims to take a survey, receive a bonus, and provide their data which are then sent to call centres.

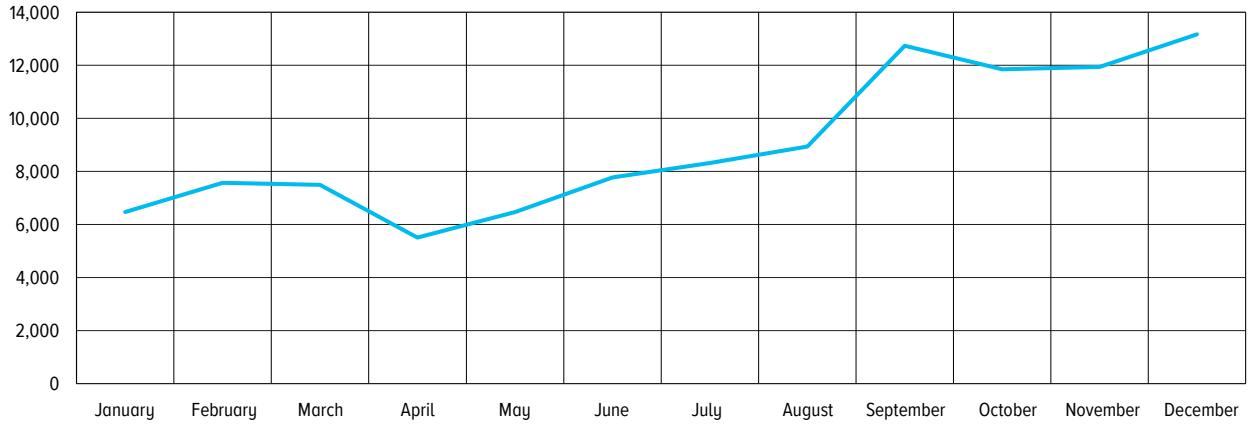
MEDIA REPORTS ON DATA LEAKS IN 2023 *Chart 10*
(NUMBER)



2. Preparing an attack

Based on the information contained in the database and identified potential connections, including those related to the employer, offenders tailor an attack scenario to a potential victim. This could be a call on behalf of a law enforcement officer, a credit institution' representative, a telecom operator, the Bank of Russia, or the management of an employer company.

CYBER ATTACKS AGAINST CLIENTS OF FINANCIAL INSTITUTIONS IN 2023 *Chart 11*
(NUMBER)

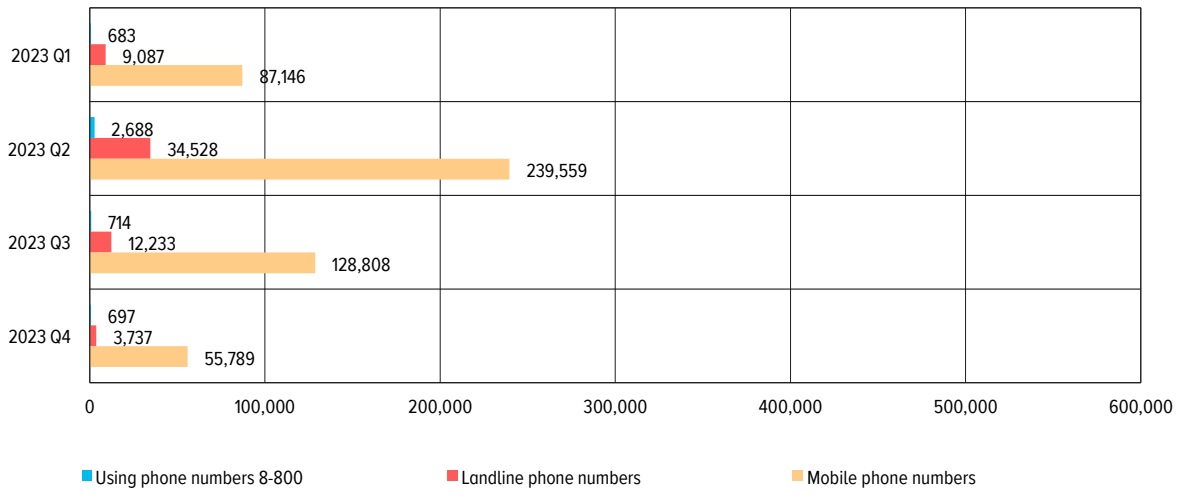


If attackers have planned an attack, this means that they already have a large amount of information about the potential victim chosen as a target.

3. Attacking and gaining control over the victim

As a rule, fraudsters call a person from an unknown phone number or via messengers. The purpose of the attack is to gain control over the user's actions as well as access to personal remote banking accounts, the Public Services Portal, or the telecom operator platform. In addition, attackers generally try to restrict the victim's communication with colleagues, family and friends on the pretext of secrecy and criminal liability for information disclosure.

DETECTED FRAUDULENT CALLS OVER TELECOM NETWORKS AND VIA MESSENGERS *Chart 12*
(NUMBER)



4. Gaining access to accounts

Attackers, on a variety of pretexts, make the victim download the malware from a phishing website or messenger and install it on the phone (their goal is to gain full access to the victim's phone and banking applications and obtain the passwords to these applications), cash out all personal funds from the accounts with financial institutions, and take out a bank loan.

5. Stealing money

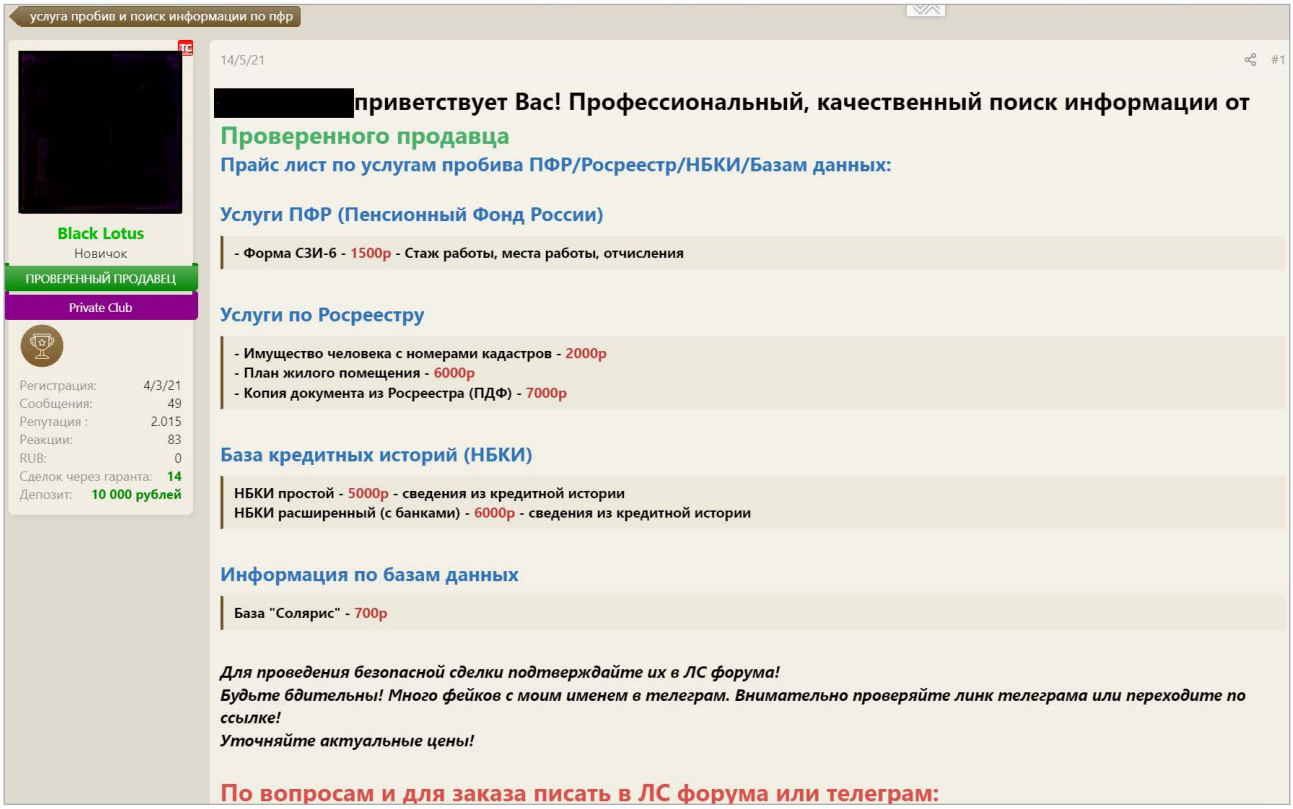
After gaining access to the personal account in a remote banking system (RBS) or persuading the victim to transfer the money to a 'safe account', attackers receive transfers to prearranged cards/accounts/telephone numbers/e-wallets and then proceed to the last stage of the criminal scheme – cashing out the funds. In a short period of time, these funds are transferred to dozens and sometimes hundreds of different accounts, getting mixed with other cash flows (financial transactions) actively passing through the accounts of money mules[1].

The funds are then cashed out and/or exchanged for cryptocurrency. The cash-out gangs simply transfer an equivalent amount of cryptocurrency to the crypto wallets controlled by them from which the funds are then withdrawn in other countries in fiat currency.

It is worth noting that from 2022 to the present, FinCERT has been observing a trend of combining a number of different stages of a crime. There has been a decrease in the number of dark web offers for sale of copies of databases obtained as a result of cyber attacks.

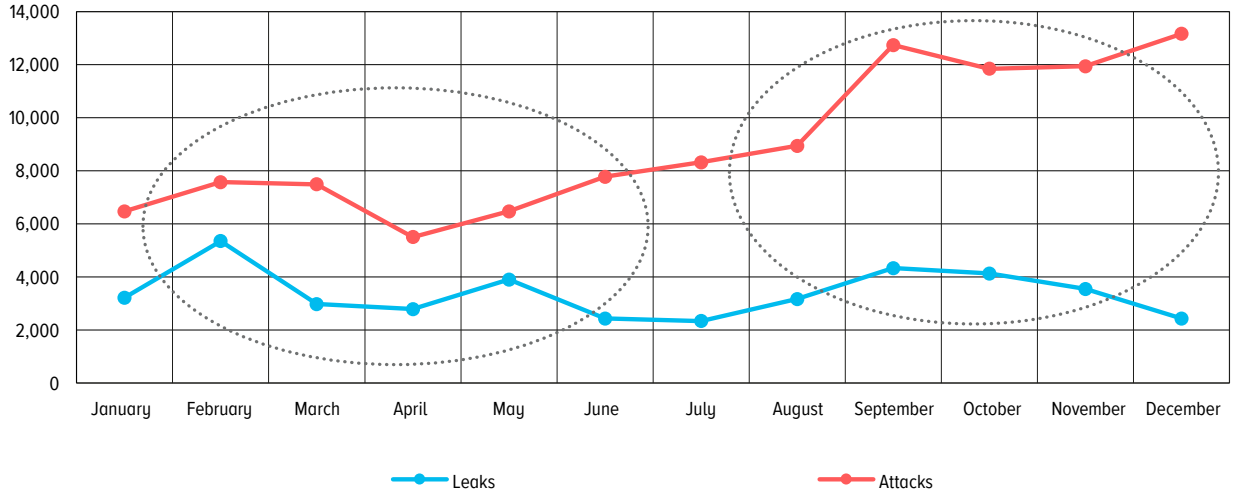
At the same time, the number of service platforms with free access to Russians' personal data went up.

There was also an increase in the number of announcements offering information on individuals or legal entities from the databases maintained by mobile operators. Active discussions on the dark web indicate a rising demand for this service.

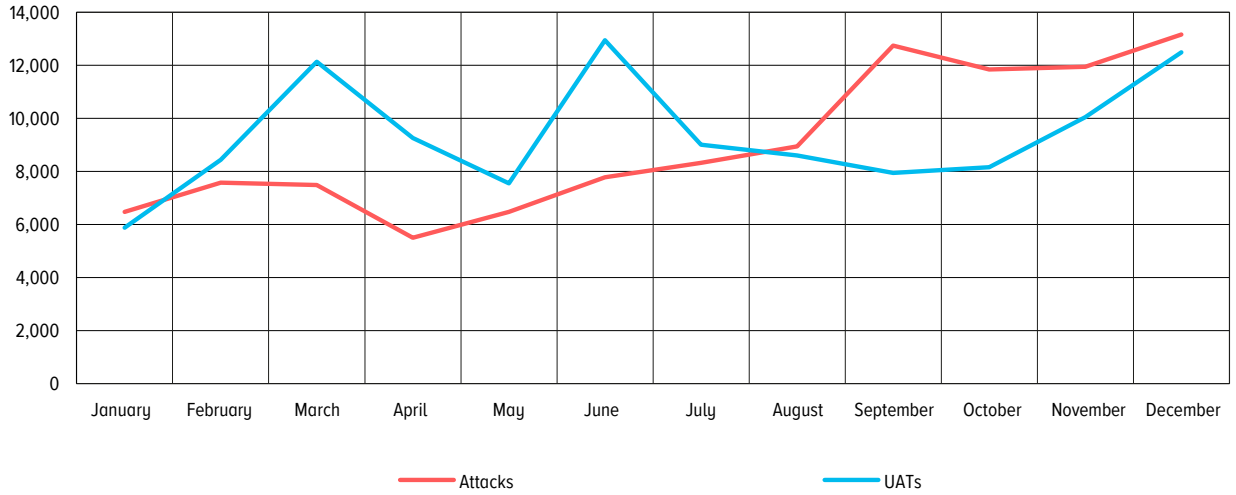


[1] A money mule is someone who withdraws and cashes out the money obtained unlawfully, including by using their electronic payment facilities.

CORRELATION BETWEEN LEAKS AND ATTACKS AGAINST CLIENTS OF FINANCIAL INSTITUTIONS *Chart 13*



CORRELATION BETWEEN UNAUTHORISED TRANSACTIONS (UATS) AND CYBER ATTACKS *Chart 14*



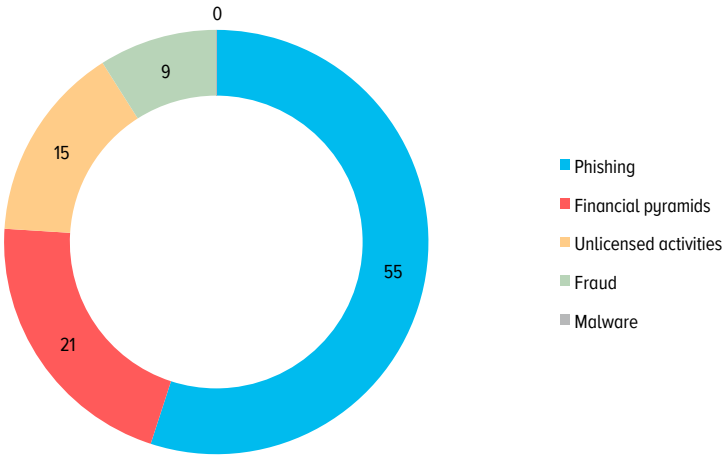
Over 2023, there were about 25% fewer personal information databases offered for sale than in 2022. The total number of database rows published also decreased. The total volume of the personal data black market was down by about 20% compared to 2022.

The period of personal data collection and processing for targeted attacks against individuals has also been shortening. Now, attacks against individuals take place at around the same time the personal data leaks happen, whereas in 2019–2021, the periods of a decline in attacker activity lasted for about a month.

As shown in Chart 13, leaks contribute to successful cyber attacks as well as social engineering attacks against individuals.

FinCERT is actively taking measures to take down fraudulent websites as well as websites that steal personal data and deceive Internet users. For example, in 2023, most websites (55%) that were subject to enforcement measures initiated by the Bank of Russia were in the ‘Phishing’ category. The main goal of such resources is to steal the data of financial institutions’ clients. Unlike last year, the ‘Financial pyramids’ category ranked second (21%) rather than first, despite the fact that the number

TYPES OF RESOURCES USED BY FRAUDSTERS IN 2023 *Chart 15*
(%)



of resources subject to enforcement measures actually doubled. Fraudulent resources used by cyber criminals to carry out unlicensed activities in the securities market as well as non-existent credit institutions and microfinance organisations' operations are still widespread (accounting for 15% of all resources). The 'Other fraud' category accounts for about 9%. Websites disseminating malware make up less than 1% of all resources.

As part of its efforts to counter both leaks of people's personal data from banking systems and fraud aimed at stealing individuals' funds, the Bank of Russia is continuously working on updating/amending the regulations on data protection in the financial sector and countering fraud.

CYBER TRAININGS

In 2023 Q3, the Bank of Russia conducted cyber trainings to mitigate risks associated with unauthorised impact on financial institutions' information infrastructures and to enhance the efficiency of the information exchange with the regulator on countering cyber attacks and cyber security incidents.

The participants were trained to respond to cyber security incidents and promptly exchange information on cyber security threats with the Bank of Russia.

The cyber trainings covered the following:

- interaction between financial institutions and FinCERT using the Bank of Russia's technical information infrastructure – the FinCERT Automated Incident Management System (FinCERT AIMS);
- responding to a detected cyber security incident, analysing the malware involved and the causes of the incident;
- filling out an incident card and sending all available information about the detected cyber attack/cyber security incident to FinCERT following a format established by the Bank of Russia (in accordance with Bank of Russia Standard STO BR BFBO-1.5-2018) via the FinCERT AIMS;
- manual and/or automated application of bulletins containing indicators of compromise (IOCs), published by FinCERT, in cyber security systems by financial institutions participating in the cyber trainings.

The cyber trainings were attended by 373 financial institutions (hereinafter, the Participants).

During the cyber trainings, phishing emails were sent from 19 different domains to the email addresses of the Participants' employees according to eight scenarios. A total of 16,911 phishing emails were sent during the trainings. The mailing was done in two stages using eight scenarios.

As part of the phishing simulation, the recipients performed unsafe actions (opened attachments and/or clicked on the links) on manufactured pretexts provided in the email.

The main factors motivating the recipients' unsafe actions as a result of phishing were the following:

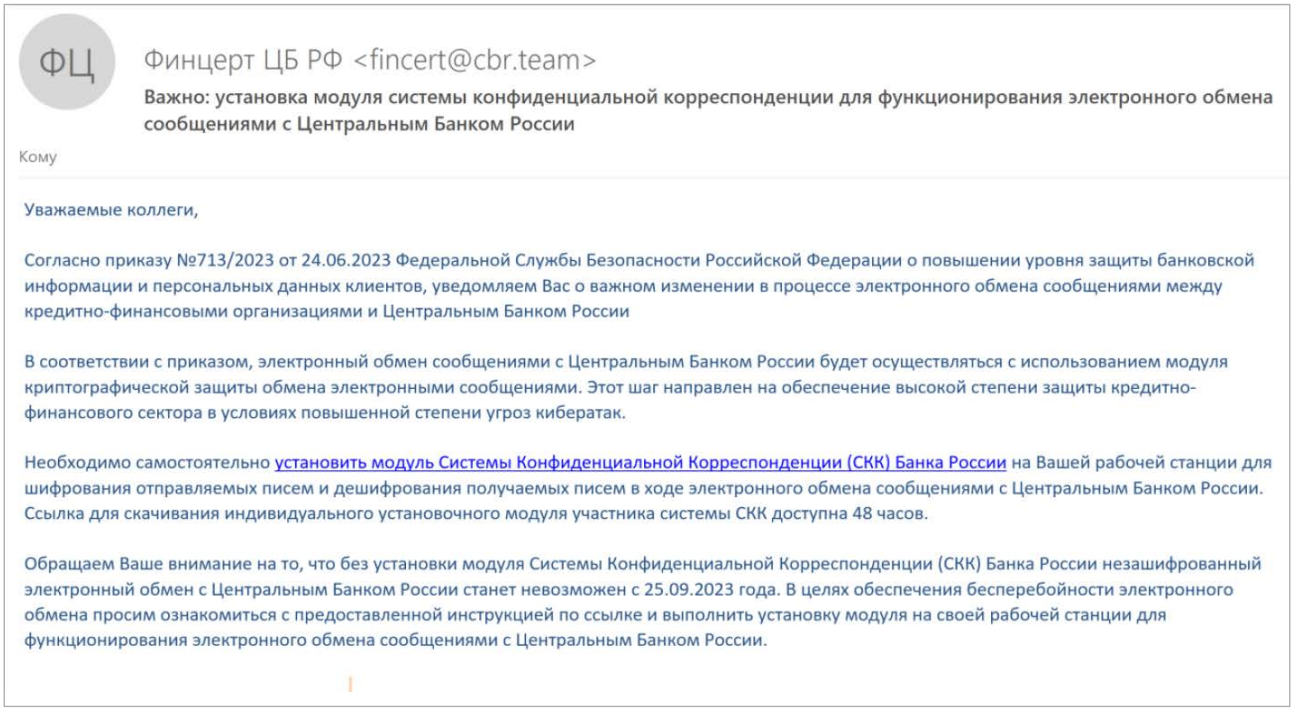
- fear of failing to take the required action;
- authority of the sender masquerading as various government agencies;
- curiosity; and
- desire to help.

In a number of phishing cases, the spoofed[1] domain of the Bank of Russia (cbr.ru) was used, which made it impossible for the Participants' employees to identify phishing emails by the domain name.

[1] The addresses from which the emails were sent imitated the email addresses of the Bank of Russia's employees (spoofing).

According to FinCERT, the following phishing scenarios were the most effective ones:

- Sending emails on behalf of the Bank of Russia requiring the recipients to install software, with a link to a website for downloading the file.



ФЦ

Финцерт ЦБ РФ <fincert@cbr.team>

Важно: установка модуля системы конфиденциальной корреспонденции для функционирования электронного обмена сообщениями с Центральным Банком России

Кому

Уважаемые коллеги,

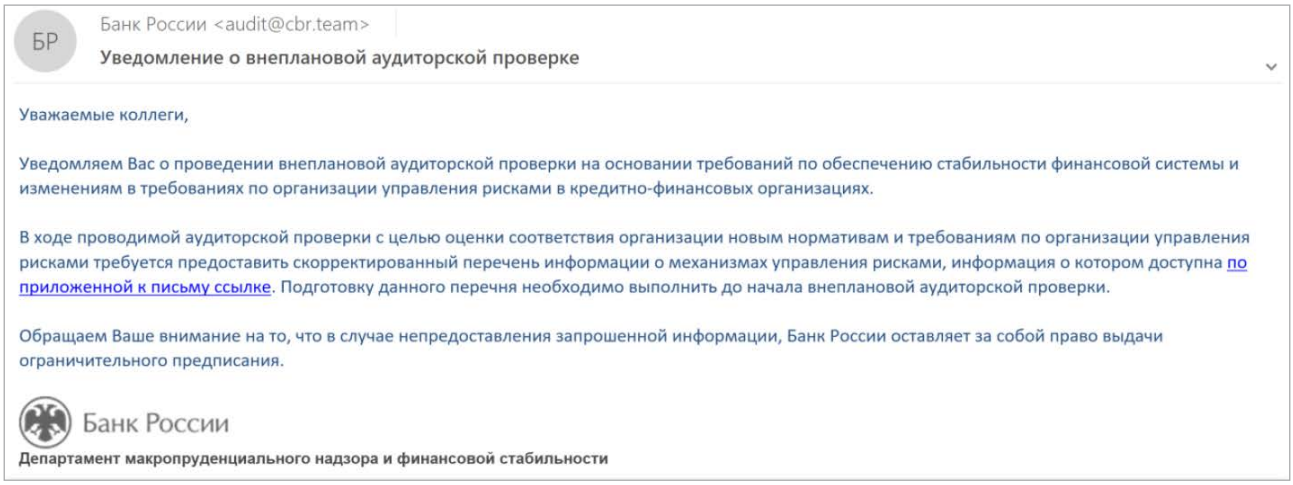
Согласно приказу №713/2023 от 24.06.2023 Федеральной Службы Безопасности Российской Федерации о повышении уровня защиты банковской информации и персональных данных клиентов, уведомляем Вас о важном изменении в процессе электронного обмена сообщениями между кредитно-финансовыми организациями и Центральным Банком России

В соответствии с приказом, электронный обмен сообщениями с Центральным Банком России будет осуществляться с использованием модуля криптографической защиты обмена электронными сообщениями. Этот шаг направлен на обеспечение высокой степени защиты кредитно-финансового сектора в условиях повышенной степени угроз кибератак.

Необходимо самостоятельно установить модуль Системы Конфиденциальной Корреспонденции (СКК) Банка России на Вашей рабочей станции для шифрования отправляемых писем и дешифрования получаемых писем в ходе электронного обмена сообщениями с Центральным Банком России. Ссылка для скачивания индивидуального установочного модуля участника системы СКК доступна 48 часов.

Обращаем Ваше внимание на то, что без установки модуля Системы Конфиденциальной Корреспонденции (СКК) Банка России незашифрованный электронный обмен с Центральным Банком России станет невозможен с 25.09.2023 года. В целях обеспечения бесперебойности электронного обмена просим ознакомиться с предоставленной инструкцией по ссылке и выполнить установку модуля на своей рабочей станции для функционирования электронного обмена сообщениями с Центральным Банком России.

- Sending emails on behalf of the Bank of Russia with a notice of an unscheduled inspection and a link to the website for downloading the file.



БР

Банк России <audit@cbr.team>

Уведомление о внеплановой аудиторской проверке

Уважаемые коллеги,

Уведомляем Вас о проведении внеплановой аудиторской проверки на основании требований по обеспечению стабильности финансовой системы и изменениям в требованиях по организации управления рисками в кредитно-финансовых организациях.

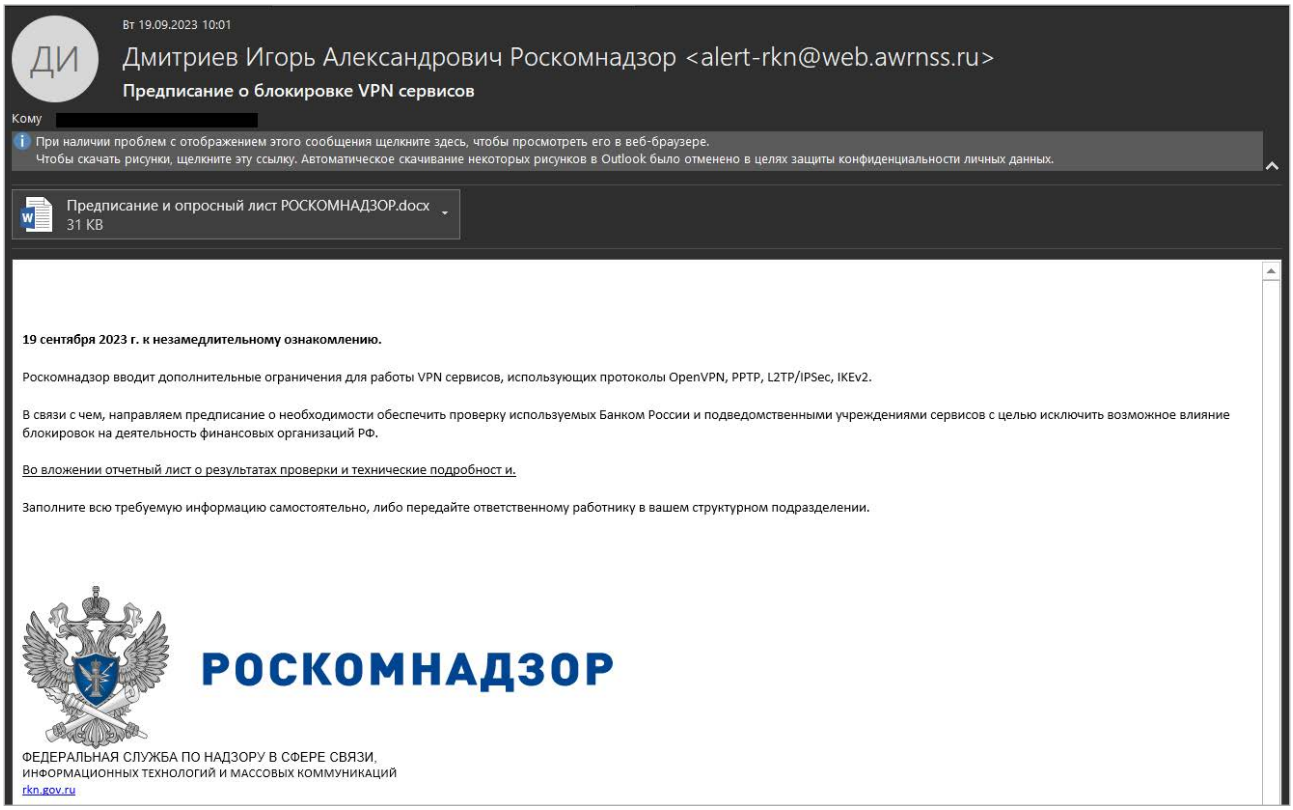
В ходе проводимой аудиторской проверки с целью оценки соответствия организации новым нормативам и требованиям по организации управления рисками требуется предоставить скорректированный перечень информации о механизмах управления рисками, информация о котором доступна по приложенной к письму ссылке. Подготовку данного перечня необходимо выполнить до начала внеплановой аудиторской проверки.

Обращаем Ваше внимание на то, что в случае непредоставления запрошенной информации, Банк России оставляет за собой право выдачи ограничительного предписания.

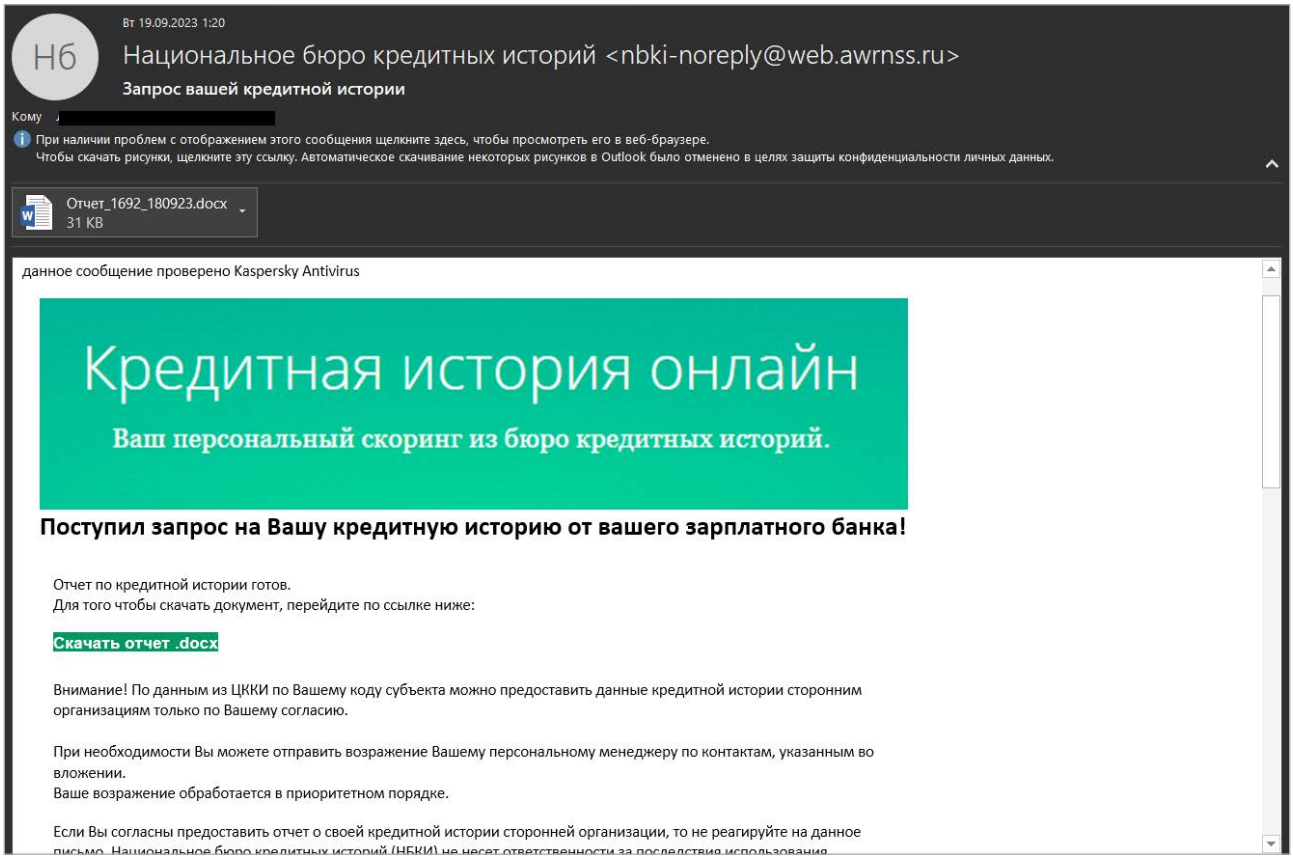
Банк России

Департамент макропруденциального надзора и финансовой стабильности

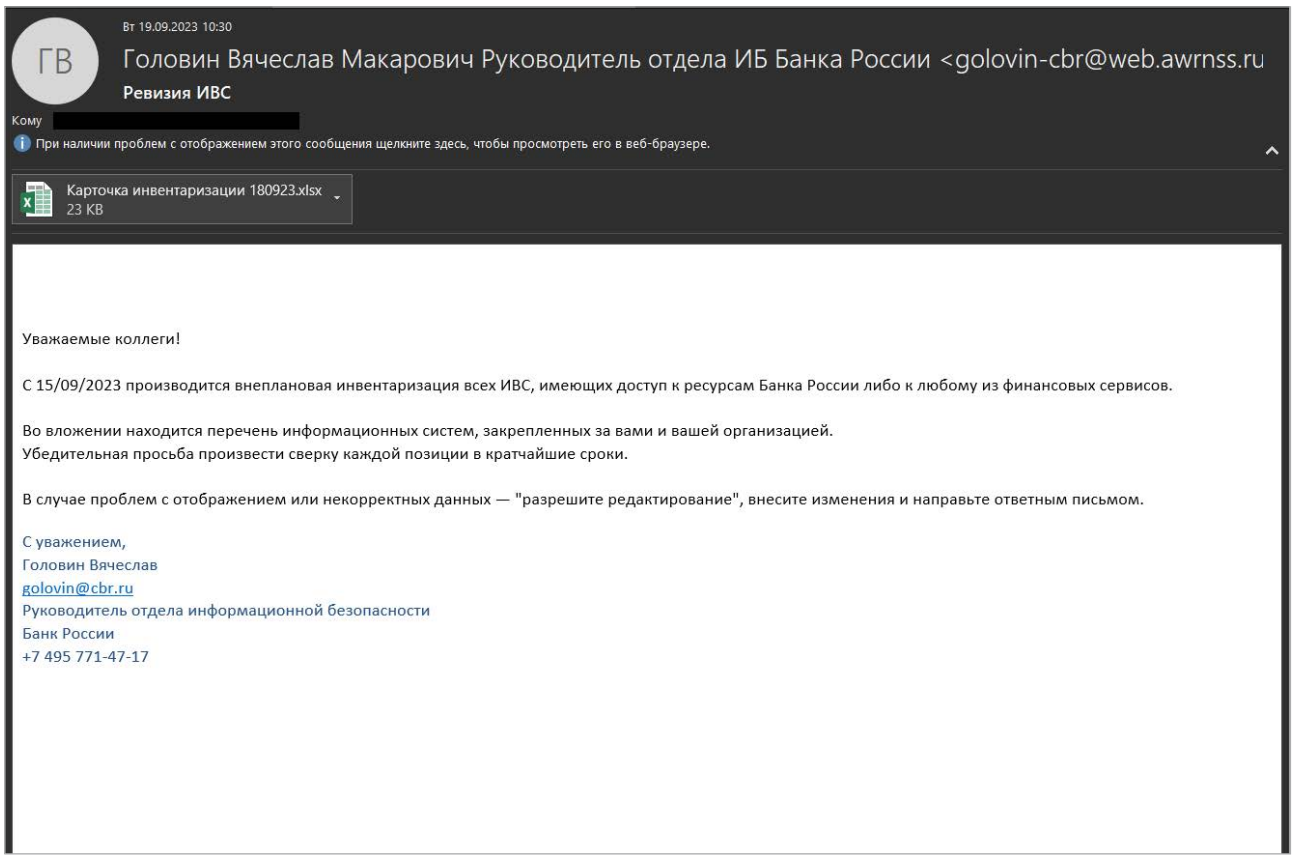
- An email from the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) giving information about further blocking of VPN protocols and requiring the Bank of Russia and subordinate agencies to perform necessary checks before the blocking takes effect and to report on the results of the checks.



- An email informing the recipient of a credit history enquiry from the payroll bank and inviting them to see the result of the check.



- An email, supposedly from the head of the information security section of the Bank of Russia, about an unscheduled inventory of computer equipment with access to the Bank of Russia information resources.



All emails had various signs of phishing:

- a non-existent employee or section/department, a non-existent internal address of the sender;
- the domain of the organisation sending the email not matching the domain of the actual sender;
- a text urging the user to take a certain action;
- an important reason for taking the action;
- dubious content and errors in the email;
- an attachment that the recipient did not expect; and
- absence of the announced content in the attachment.

As a result of the cyber trainings, 43 financial institutions, accounting for 11.5% of the total number of the Participants, were compromised during this simulation.

In addition, FinCERT prepared and sent to the Participants a report and recommendations on improving security at the institutions and enhancing information security awareness of their employees.

INTERNATIONAL COOPERATION OF FINCERT

In 2023, the Bank of Russian continued to expand its multilateral agenda for engagement of its international partners and outreach to them, strengthening and enhancing the existing ties through closer and deeper cooperation.

The regulator is studying best global practices and experiences in information security for their further implementation in Russia. These include issues of operational resilience, risk management, and the information security methodology and standardisation.

As part of multilateral cooperation, the Bank of Russia collaborates with the national (central) banks of the EAEU and BRICS member states.

The EAEU has a working group on cyber security to coordinate information security efforts. The Bank of Russia provides its assistance in setting up CERT[1] units where necessary. The regulator annually prepares and publishes an overview of regulatory innovations and best practices, develops and introduces uniform methodological approaches to information security into national practices, and regularly organises advanced trainings for CERT staff.

BRICS has a special working group – the BRICS Rapid Information Security Channel. As Russia will be chairing BRICS in 2024, the Bank of Russia has also assumed the chairmanship of the working group.

Together with its BRICS counterparts, the Bank of Russia published reviews of international practices: an e-booklet on information security, a review of best practices in information security supervision and control, and a report on the accessibility of financial services.

As part of the information exchange, FinCERT prepared and sent four bulletins to the BRICS member states in 2023.

For the first time, the Bank of Russia plans to hold cyber trainings with its partners from the BRICS and EAEU countries.

The cyber trainings with the participation of the counterparts from the national banks of the BRICS countries are to be held in 2024. The plan and scenario of the event were prepared in 2023, with the relevant questionnaires sent to the participants.

The joint cyber trainings with the banks of the EAEU member states are to take place in 2024–2025. The aim is to train the collaboration, including in the event of unauthorised cross-border transactions using various payment tools.

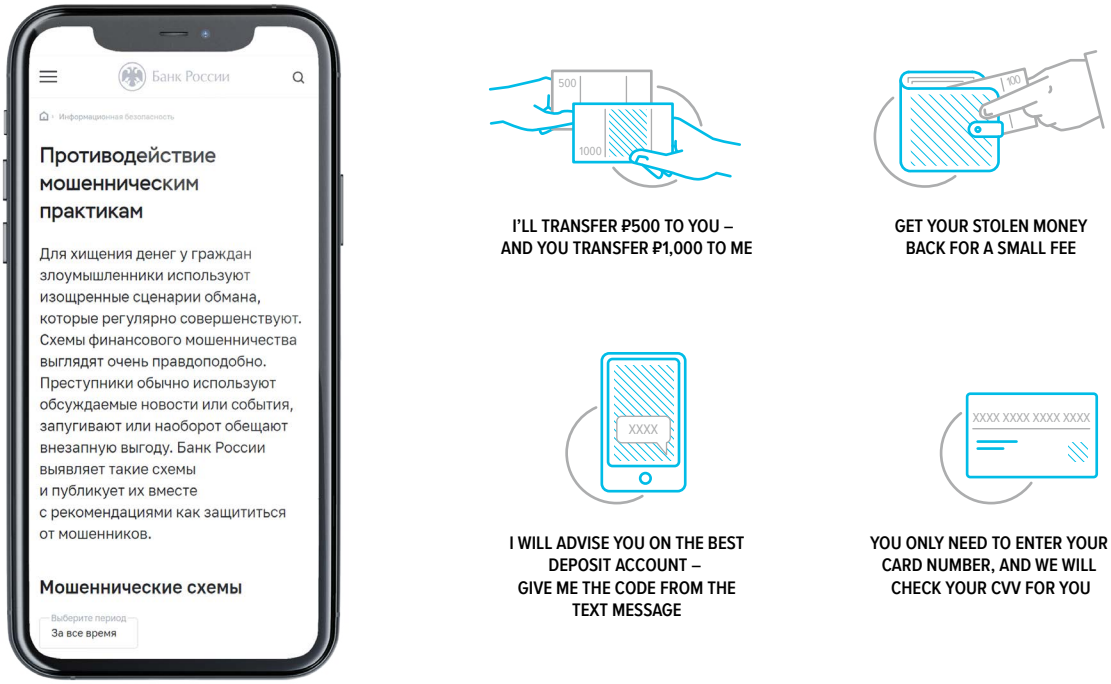
Within the framework of bilateral cooperation with the national (central) banks of the BRICS/EAEU member states, the Bank of Russia studies the unique experience of its counterparts in regulating and countering fraudsters. Joint activities are carried out to improve digital financial literacy, develop approaches to reducing the number of unauthorised transactions, countering credit fraud, and combating money mules.

[1] CERT means a Computer Emergency Response Team.

DIGITAL FINANCIAL LITERACY

The Bank of Russia's digital financial literacy efforts in 2023 focused on informing people about common tricks used by fraudsters and giving tips on how to confront attackers and safely use various financial instruments.

RAISING AWARENESS ABOUT NEW AND EXISTING CYBER FRAUD SCHEMES *Chart 16*



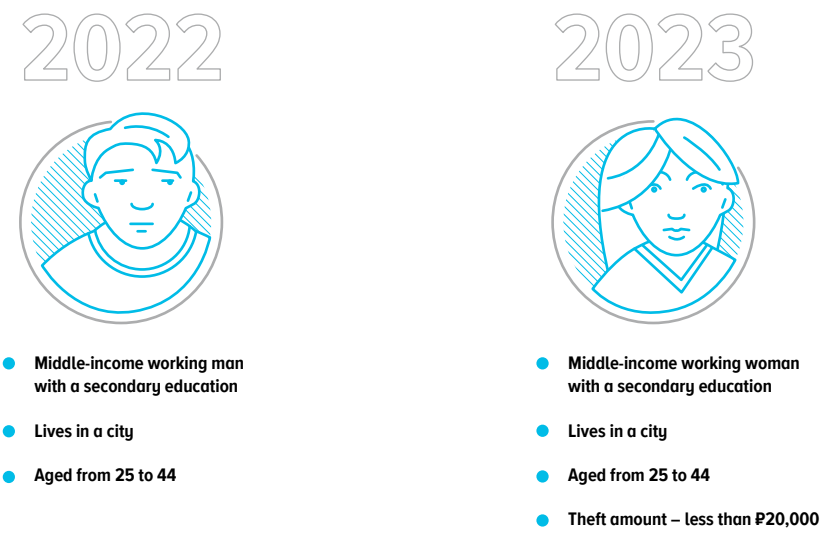
The Bank of Russia regularly disclosed new fraudulent schemes on its official website in the special section – Antifraud. As a result of this comprehensive work, such schemes gained wide publicity, and criminals stopped using them.

The Bank of Russia also published educational materials on its social media pages to warn individuals about the risks of fraud in the credit and financial sector. The Bank of Russia used various communication formats: texts with creative illustrations, videos, cards, interactive resources, and live broadcasts. In addition, a number of projects were implemented in partnership with the social media outlets, such as VK, OK, and RuStore.

The Bank of Russia paid special attention to working with comments on social media platforms. Financial fraud is a subject of unfailing interest and triggers many questions which the regulator was promptly answering. In some cases, individuals contacted the Bank of Russia's chat room in Telegram or left comments on the platforms when fraudsters were trying to trick them, which helped prevent money thefts. Such appeals resulted in a number of fraudulent web pages and accounts blocked.

The Bank of Russia produced posters and videos to help raise public awareness about ways and methods of stealing money from bank accounts. The Bank of Russia's social ads on financial cyber security were placed at more than 36,600 spots. Materials on digital financial literacy and cyber security developed by the Bank of Russia were sent to federal and regional executive authorities to be placed on Russian transport and social infrastructure facilities. These materials were placed on outdoor screens and displays, in airports, at railway stations, and on public transport. The videos were

PROFILE OF A CYBER FRAUD VICTIM *Chart 17*



broadcast in the cinema network – Center Kino – across the country. Additionally, leaflets, brochures, and booklets were distributed in cinemas and libraries, multifunctional centres and shopping malls, organisations helping orphans and pensioners, polyclinics and social support centres.

In 2023, the regulator conducted an online social advertising campaign to counter phone scammers. Financial Culture (fincult.info), an educational resource of the Bank of Russia, published more than 40 materials on popular fraud schemes and ways to counter them. Over 2023, 11.1 million unique visitors (an average of 931,900 monthly visitors) used the materials offered by the resource.

2024 TRENDS

FinCERT predicts the following trends in cyber attacks targeting financial institutions and individuals:

- Attacks through third-party integrators and vendors of IT solutions used in the financial market, through both the supply chain and trusted relationship. To counter the risks of malicious attacks along this vector, it is recommended to apply a zero-trust policy to all service providers and their connections. It is also necessary to analyse the maturity level of service providers, including the risks of exposure to the contractor's infrastructure and the contractor's liability under direct contracts.
- DDoS attacks, including those using botnets and Internet of Things (IoT) devices.
- Exploitation of vulnerabilities in the software provided by companies that have stopped updating and supporting the products of clients operating in Russia.
- Using neural networks to conduct targeted social engineering and phishing attacks.

In general, the 2024 cyber attack trends clearly demonstrate the need for continuous enhancement of cyber security both at the level of users (individuals) and at the level of businesses and government agencies. The best approach includes comprehensive protection measures, timely software updates, personnel trainings, cyber literacy campaigns, and constant monitoring of information infrastructure security.