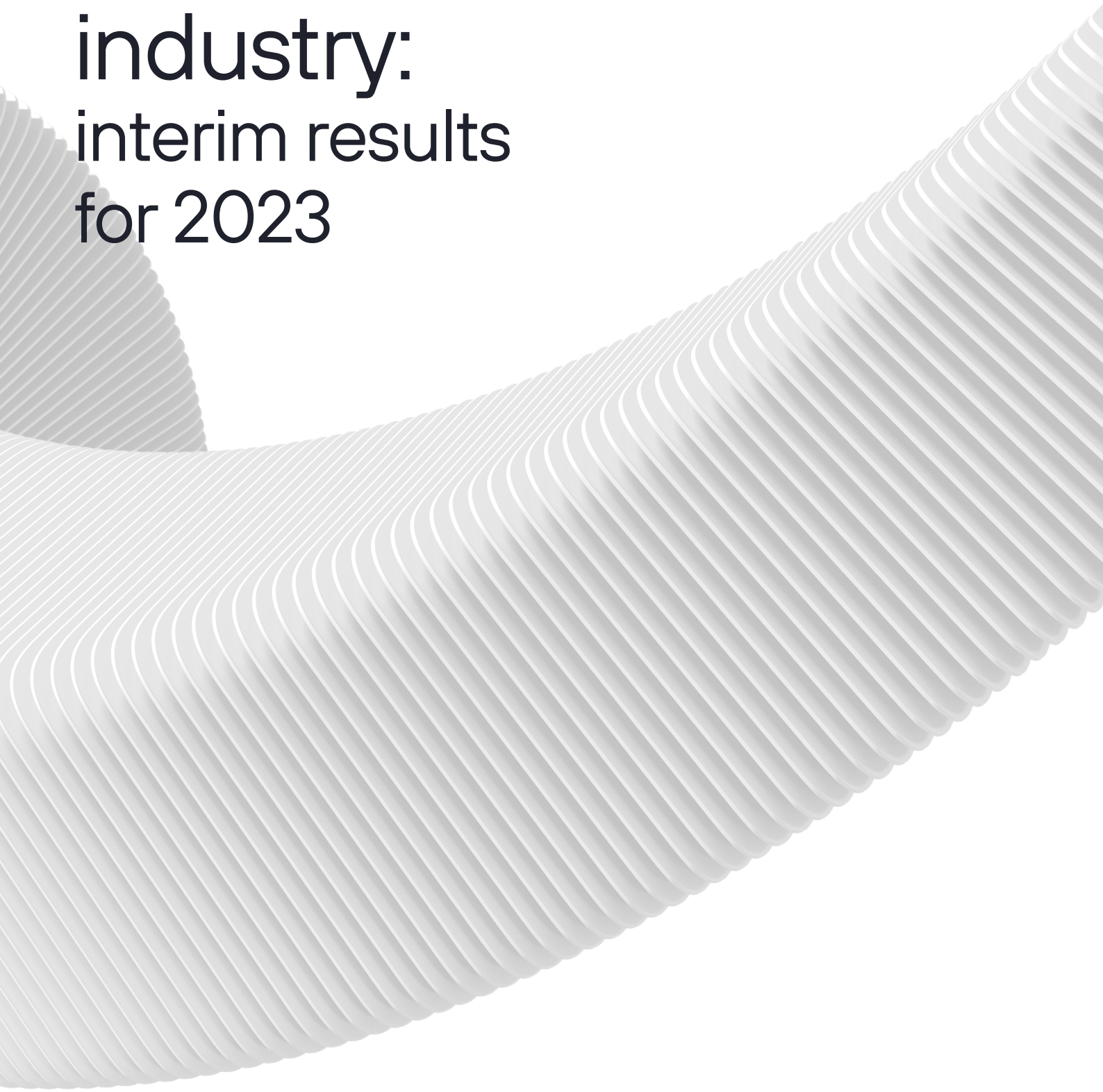
Cyberthreats to the financial industry: interim results for 2023



Positive Technologies

ptsecurity.com

Contents

According to the IBM Cost of a Data Breach Report 2023, the financial sector ranks highly in the global cyberincident damage statistics, second only to the healthcare industry. Losses incurred by financial organizations amounted to approximately $5.9 million per cyberincident, which is higher than the average across all industries ($4.45 million). This is just a slight decrease from $5.97 million in 2022. Banks and other financial institutions are losing money not only as a result of paying ransoms for the non-disclosure of stolen data and restoring infrastructure after ransomware attacks; they also suffer direct financial losses in some cases. We will discuss these and other cyberthreat trends for financial organizations below. We'll demonstrate the factors giving rise to the current cyberthreat trends affecting financial organizations today, and we'll also analyze the interests of criminals based on announcements posted on dark web shadow markets and specialized Telegram channels.[1]

The analysis is based on the expertise of Positive Technologies, as well as data from external authoritative sources[2] for the first three quarters of the year. The sample of organizations includes both banks and non-banking financial companies (such as insurance companies, professional stock market players, and investment funds).

[1] During the study, we analyzed 236 Telegram channels and dark web forums, with a total of 16,734,680 users and 112,812,462 messages. This multilingual sample included the largest platforms centered around various subjects.

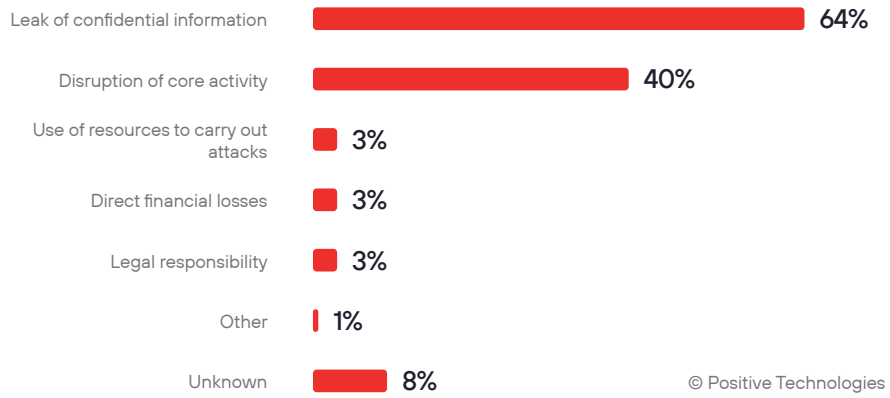
[2] External sources include analytical reports from leading companies with their own cybersecurity expertise, as well as news sources aggregating information about cyberincidents, and federal news agencies.

Cyberthreat trends in the financial sector

According to our data, the number of successful cyberattacks in the financial sector is growing year on year. In the third quarter of 2023, we recorded twice as many unique cyberincidents as in the same period a year earlier. This indicates the increased attention of criminals to this industry.

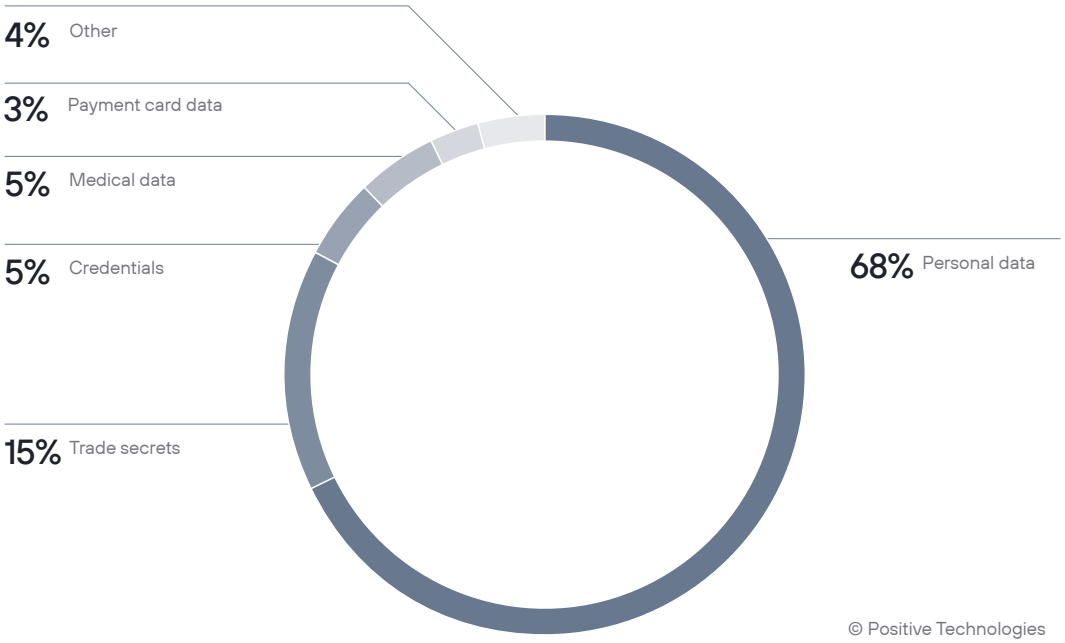
Among the consequences of attacks, data leaks (64%) and disruption of services or key business processes (40%) stand out. A year earlier, the proportion of leaks was 51%, while disruption of the company's core activities occurred in 42% of incidents. This trend is understandable: sophisticated attacks on well-protected financial organizations with the goal of stealing money have become a rare occurrence amid the rise of easier-to-implement ransomware attacks and large-scale customer data leaks. Today, criminals not only sell databases but also distribute them for free to punish organizations for refusing to pay ransoms or to draw more public attention to the incident, thus causing more damage. The latter especially applies when hacktivists are behind the attack. The cost of such databases and the frequency of offers for their sale and purchase on shadow markets are discussed in the following section.

Figure 1. Consequences of successful attacks on financial organizations (Q1–Q3 2023)



The vast majority of leaks contain clients' personal data and commercial information about organizations. Leaks also often include payment card numbers and account details, while leaks from insurance companies include medical information.

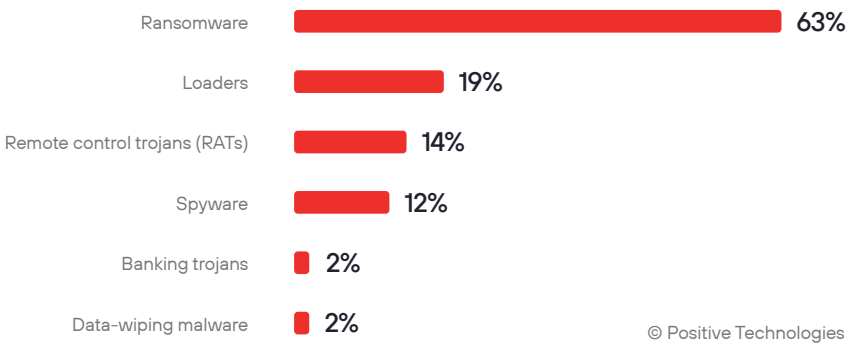
Figure 2. Types of data stolen in successful attacks on financial organizations (Q1–Q3 2023)



Such incidents have a negative impact on the victim company's reputation. For example, following a cyberattack and leak of confidential data at the Angel One brokerage firm, its shares fell in price by 2%.

Geopolitics has become one of the determining factors shaping how cyberattacks on this industry differ from region to region. For example, Russian banks not only suffer from leaks but also continue to face powerful DDoS attacks. One such example is an attack on Sberbank that was deemed the most serious in the organization's history. Globally, the main cause of interruptions to financial services is ransomware, standing out significantly (63%) in the statistics as the most commonly used malware. For comparison, in the previous year, ransomware accounted for only 18%, with loaders occupying the top spot at 59%.

Figure 3. Types of malware in successful attacks on financial institutions (Q1–Q3 2023)

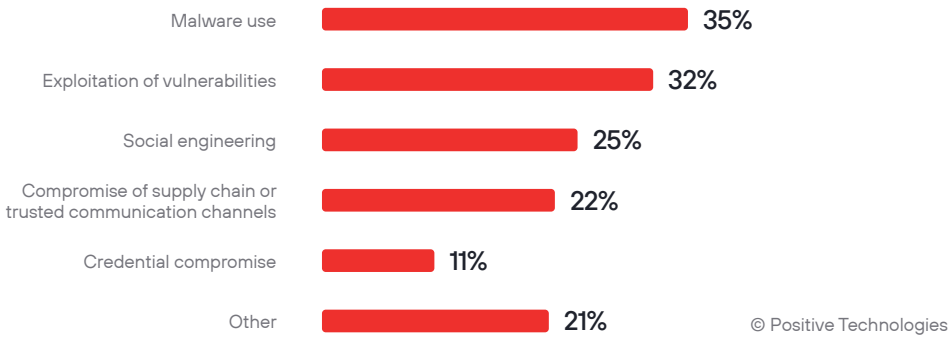


This trend is confirmed by other researchers. For example, Sophos observes in its report the highest-ever level of ransomware attacks in the financial sector: 64% of respondents reported falling victim to such attacks. In 2021, this figure was just 34%, so it nearly doubled. According to the report, among financial organizations facing ransomware-related cyberincidents, 81% had their data encrypted, with only 14% managing to stop the attack before their systems were locked. In 25% of successful attacks, the criminals not only encrypted data but also exfiltrated it. For instance, the LockBit ransomware attack on one of Indonesia's largest banks, BSI, disrupted the operations of the bank's branches and ATMs. The attackers demanded a ransom of $20 million but were refused, so they posted 1.5 TB of the bank's confidential data online. However, not all companies refused the criminals' offer—about 43% of financial companies paid the ransom. The average payout size was estimated at $1.6 million, with every tenth paying organization (11%) giving more than $5 million to the cybercriminals.

If we consider cyberattacks in terms of methods used, a significant decrease in the proportion of social engineering (25%) is notable. In the previous year's study, its share was 47%. This doesn't necessarily mean a reduction in the number of phishing attacks as such; rather, we attribute this change to an increased share of other methods—we observed significantly more incidents exploiting software vulnerabilities. In particular, a significant contribution to this category was made by attacks exploiting the vulnerability in the secure data transfer application MOVEit Transfer (CVE-2023-34362). The Cl0p group was actively exploiting it at the beginning of the year, and a patch to fix the flaw was only released in May. A large number of incidents occurred in Q2 and Q3 when other criminals began leveraging the exploit. This indicates that not all financial companies using such software (widespread in North American countries) responded to the threat in time. So, in 2023, attackers compromised financial organizations not only through traditional means (via phishing messages) but also by actively exploiting vulnerabilities in the network perimeter—to the profit of so-called initial access brokers. Further in this study, we'll show some access sale ads and assess the cost of this service on shadow markets. Financial organizations need to build reliable protection for their external network perimeter and strengthen the vulnerability management process.

Regarding the most common attack methods, there was also a significant percentage of incidents (22%) in which the compromise primarily occurred through supply chain attacks.

Figure 4. Methods for compromising the information infrastructure of financial organizations (Q1–Q3 2023)



For example, experts at Checkmarx identified several successful attacks on the supply chain of open-source software in the banking sector. In one attack, the cybercriminals even created a fake LinkedIn page where they impersonated an employee of the targeted bank to avoid suspicion while distributing malicious npm packages. Such attacks could become a trend in the coming years, given the widespread use of open-source software by companies, including financial organizations, in their in-house software development projects.

To summarize, several important trends can be identified:

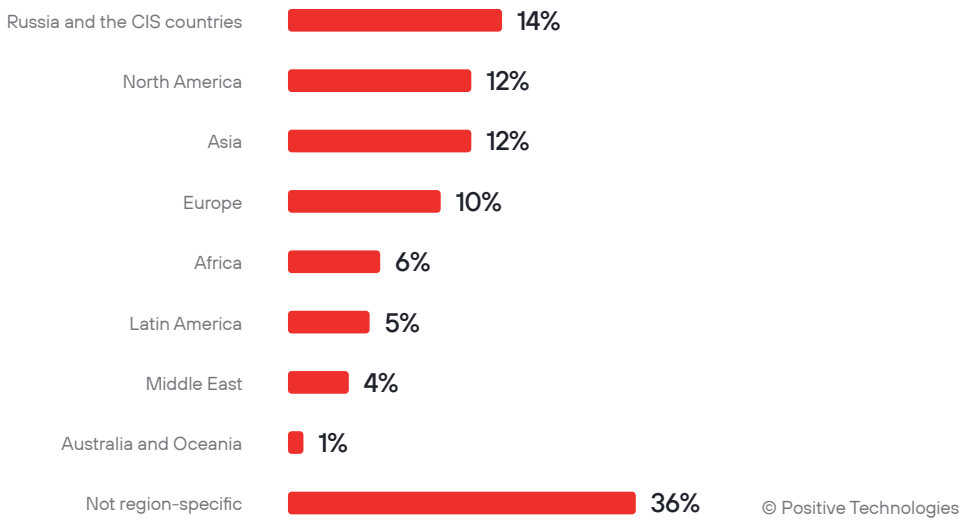
- Attacks are becoming simpler yet continue to bring considerable profits to criminals.
- Database leaks pose substantial risks to clients of financial companies; access to stolen information enables criminals to carry out their fraudulent schemes more efficiently, as they can cite personal data, account and card numbers, and sometimes account balances while conversing with victims, increasing their trust and thereby the likelihood of a successful attack.
- Attacks are not only carried out by financially motivated criminals; hacktivists also pose a serious threat in certain regions.
- Ransomware is used to compromise the infrastructure of financial organizations, causing significant damage to businesses.
- Criminals actively exploit vulnerabilities in organizations' network perimeters for infiltration.
- Attacks involving the replacement of npm packages with malicious ones could become a serious threat to financial organizations using open-source components in their systems.

An assessment of current threats would be incomplete without analyzing how the attackers themselves view the financial sector. So next we will examine which topics appear most prominently in the communications of criminals on shadow markets.

Attackers target customer data

Analysis of postings on themed dark web sites and messages in specialized Telegram channels revealed that the trends described above are generally reflected in attackers' communication. Their messages reflect not only the specifics of attacks but also the geography of compromised companies.

Figure 5. Distribution of messages on shadow markets by the geography of compromised organizations



One-third of the analyzed ads (36%) contain topics not tied to any specific region, where the victim's location is irrelevant to the criminals. However, most messages about the sale or purchase of goods and services include references to specific regions. Russia and the CIS countries are the most frequently mentioned due to the particularly acute geopolitical situation, which is also reflected in cyberspace. Large-scale attacks driven by ideological motives (hacktivism) were directed towards Russian companies, including those in the financial sector. The attackers tried to destabilize Russia's financial industry not only by disrupting banking systems but also by undermining citizens' trust in the country's financial system as a whole. Attempts to achieve these goals included, among other things, spreading misinformation and extensively publicizing each cybersecurity incident related to financial institutions. Criminals with negative sentiments toward Russia released leaked databases online; as a result, approximately 83% of postings on shadow markets which are in some way connected to the Russian financial sector are focused specifically on customer databases.

[3] Translation of image text: «Renaissance insurance company data dump www.renins.ru»

Figure 6. A dark web forum post providing access to the client database of the Russian insurance company Renaissance[3]

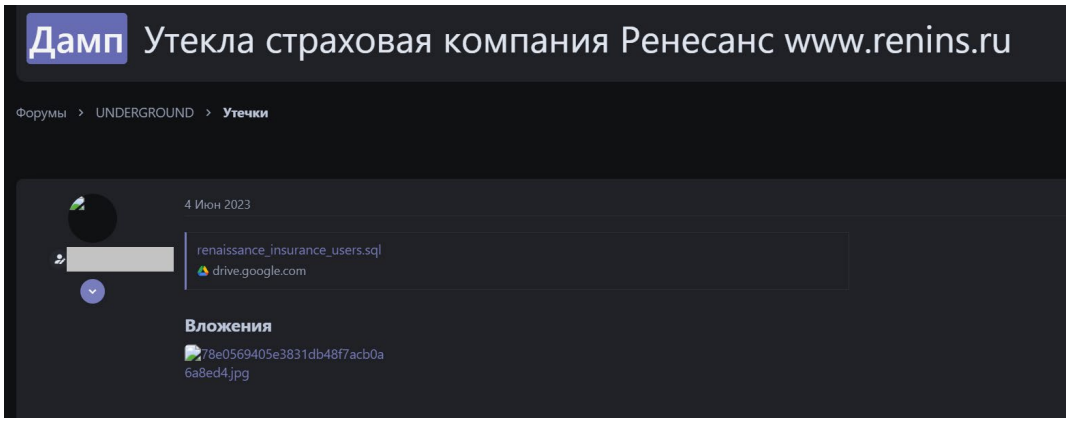


Figure 7. The client database of the Russian insurance company Sogaz-Life offered for download in a Telegram channel

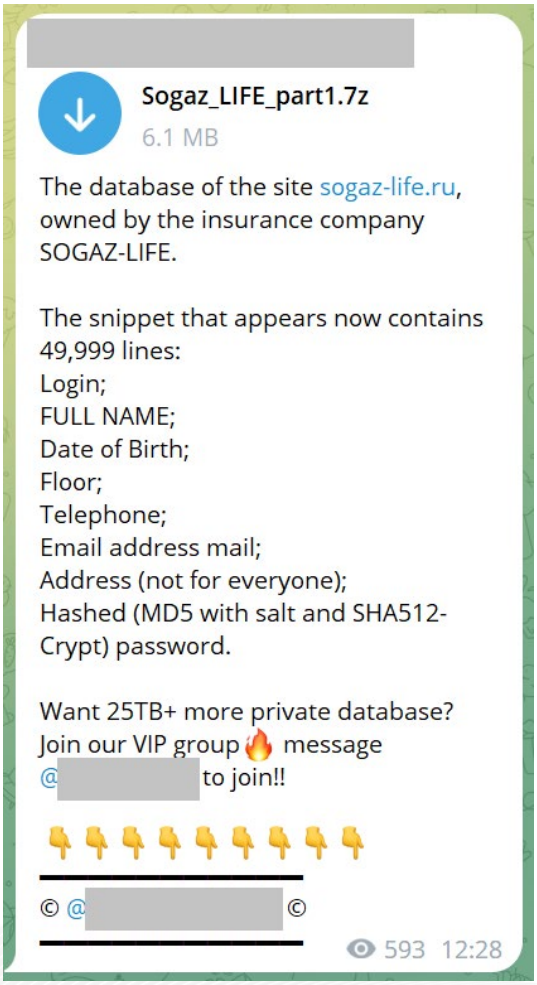
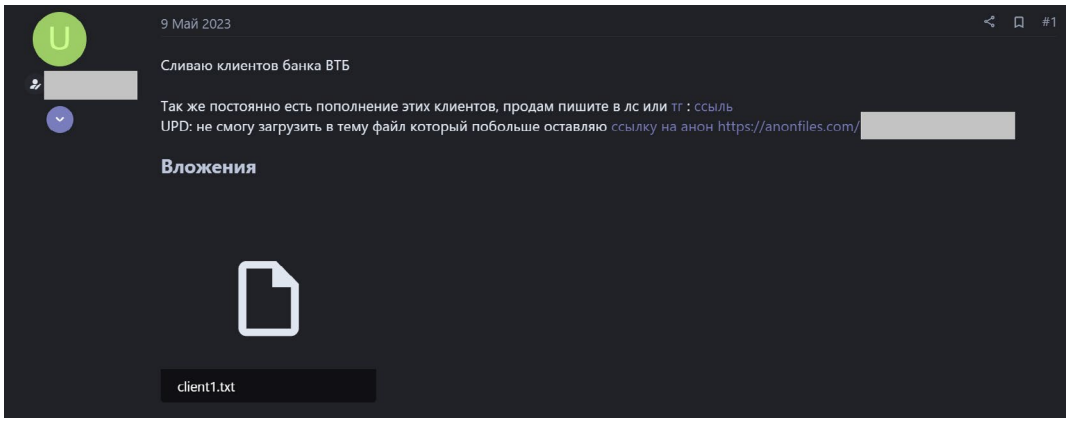


Figure 8. Advertisement for the sale of client data of the Russian bank VTB[4]



[4] Translation of image text: «May 9, 2023

I'm leaking data of VTB Bank clients

This client data is also constantly replenished and for sale. Write in private messages or Telegram: link

I can't upload a larger file to the topic, I'll leave a link to anon https://anonfiles.com/...

Attachments»

The overall statistics from all the analyzed advertisements also indicate that cybercriminals are greatly interested in the client data of financial companies worldwide. In 42% of the messages, there are announcements for the sale, purchase, or free distribution of databases.

Figure 9. Topics of messages on shadow markets in the context of attacks on financial organizations

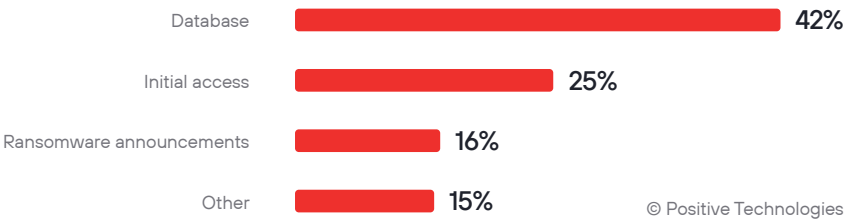


Figure 10. Advertisement for the sale of the database of a Chinese insurance company

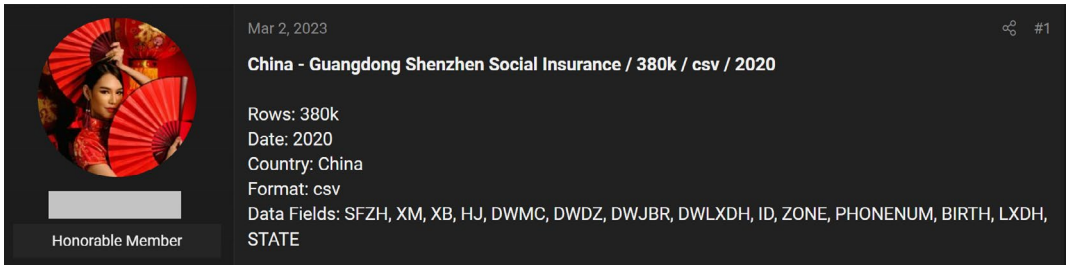


Figure 11. Advertisement for the sale of an Indian bank's employee database

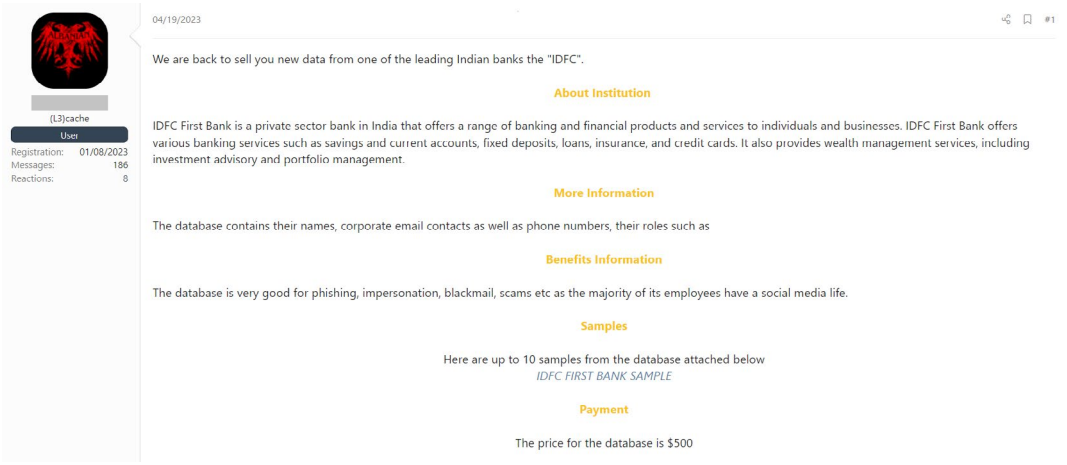
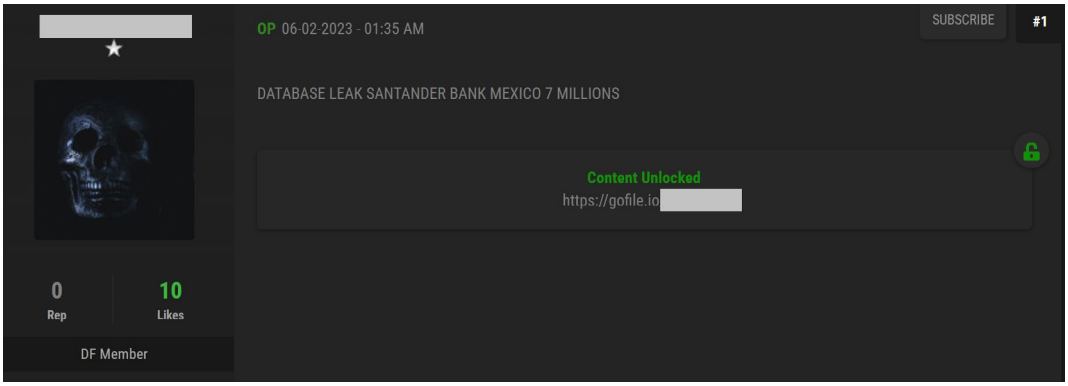
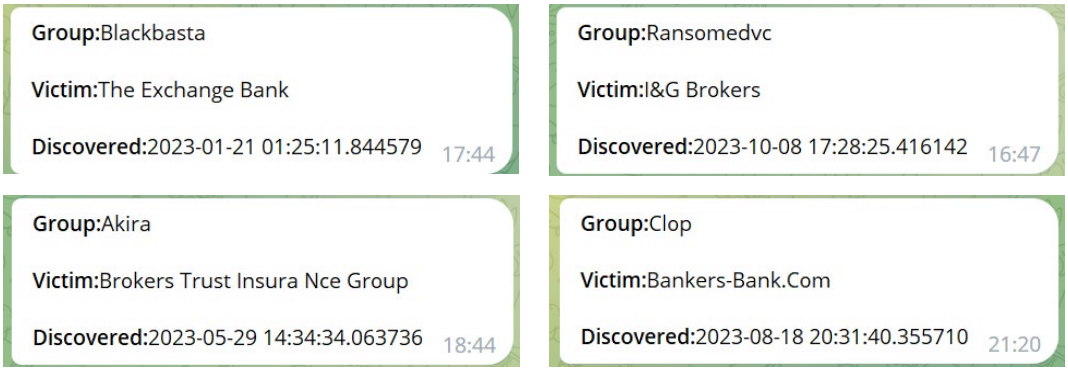


Figure 12. Giveaway of the leaked database of a Mexican bank



We've separately highlighted the category "Ransomware announcements," which includes posts about the activities of criminal groups engaged in cyber extortion. In these announcements, the authors of Telegram channels and forum threads aggregate information about ransomware attacks on organizations, announce imminent leaks, or release the confidential data of victims who haven't paid the ransom.

Figure 13. Examples of messages in Telegram channels about ransomware attacks on financial institutions



A new form of extortion is emerging, in which criminals draw the attention of regulators to the incident and thereby force the victim to pay the ransom. This precedent was set in connection with MeridianLink, a developer of digital solutions for financial organizations and banks. The operators of the BlackCat ransomware accused the company of failing to meet the deadline for officially disclosing information about the cyberattack and filed a corresponding complaint with the U.S. Securities and Exchange Commission (SEC). MeridianLink is not directly related to the financial sector, but criminals attacking this sector could easily adopt such an extortion method given the industry's high regulation.

In the largest percentage of the analyzed messages (43%), databases are given away for free, while the shares of announcements for the purchase and sale of databases are almost equal to each other. Usually, databases from recent leaks of major companies are sold, as well as the services of insiders providing information about clients upon request. Purchase advertisements mainly contain requests for specific data or companies not found among the active offers. The fact that there is a significant amount of such requests (29%) is the result of attackers targeting specific organizations or groups of organizations. According to our statistics, targeted attacks predominate in the financial sector (98% of all incidents).

Figure 14. Distribution of messages about buying, selling, and giving away databases of financial organizations' clients by type

The price in the ad can be indicated either for the entire database or as a fixed cost for each row (also known as record or line). One database record will cost the buyer approximately five dollars. The cost of half of the databases from the analyzed sources does not exceed $1,000, but, depending on the volume of the information contained in the database (and its significance for criminals), the price can reach up to $10,000 and even significantly exceed this amount.

Figure 15. Cost of databases on shadow markets ($)

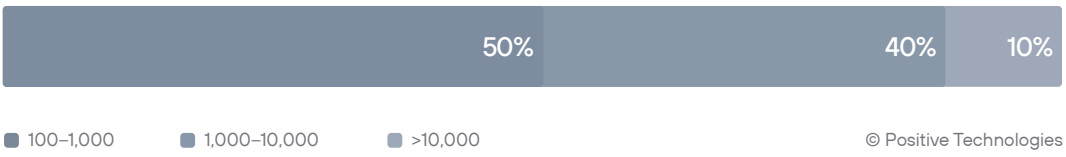


Figure 16. Announcement for the purchase of a bank's customer database with per-row payment

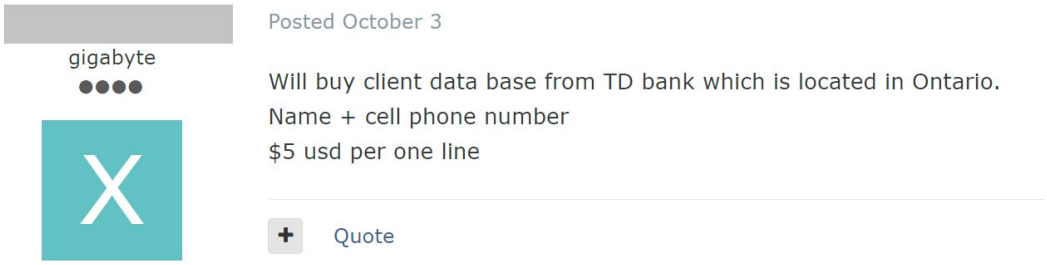
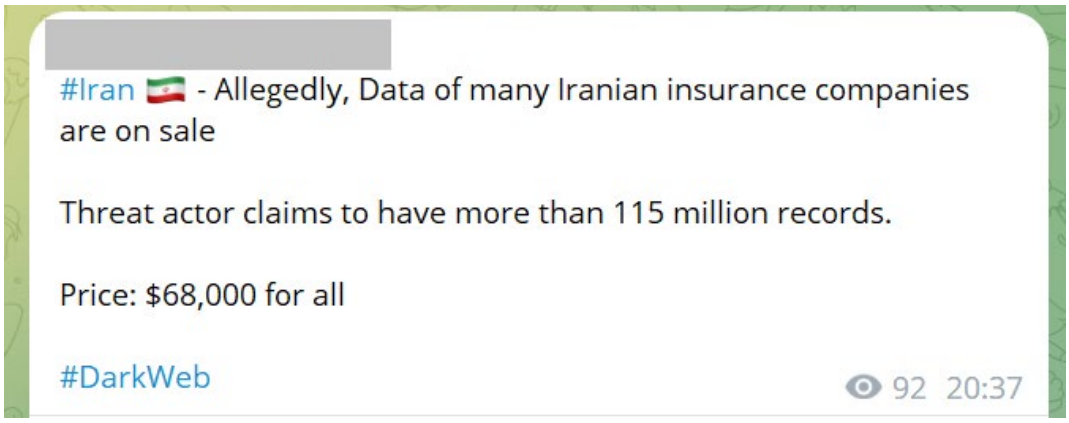


Figure 17. Advertisement for the sale of databases of Iranian insurance companies



The purchased databases are used in further attacks on clients of financial organizations using social engineering methods, as well as for hacking accounts if the databases contain account credentials (for example, logins and password hashes). With each new leak, criminals gain additional information about potential victims; they can aggregate different databases, enriching the information they've already collected. As a result, criminals can gather such a wealth of information that they can form detailed digital profiles[5] of their victims for use in fraudulent schemes or further resale.

[5] A digital profile in this case is understood as a set of data that allows for the complete identification of an individual in the digital space (identifiers and scans of identity documents, driving license and insurance numbers, contact information, date and place of birth, medical information, bank account and credit card numbers, account balances, information about loans and property, and other data).

Access is still valued

An equally valuable commodity in the criminal service market is initial access[6] to the information infrastructure of financial organizations. Every fifth advertisement we studied mentions sale of access. As early as 2020, we noticed a trend that we called "access for sale" (some sources also use the term "access as a service"); later, we researched the development of this trend.

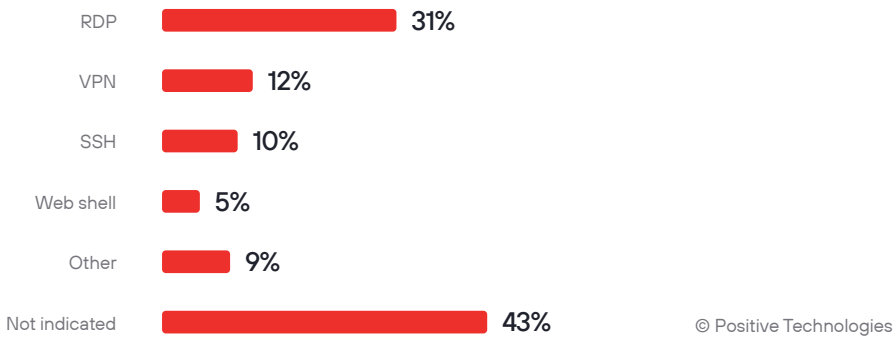
Today, access is actively sold on shadow markets alongside personal data and malware, and the supply (90% of ads) significantly exceeds the share of purchase ads (10%). This could indicate that the number of successful penetrations into the networks of financial companies is so high that criminals do not need to place purchase ads: they can get the access they need from existing offers on the market. Purchase messages usually demand access to specific organizations or banking systems.

Figure 18. Announcement about purchasing access to a payment switch application server

There are different types of access available on dark web forums. The most common accesses are via RDP, VPN, and SSH protocols as they allow attackers to execute operating system commands on the targeted host interactively. The compromised computer or server is typically located within the organization's internal infrastructure. Less common is access through a web shell, which allows attackers to execute commands through a compromised web application. Access via a web shell also grants the attacker control over a server, but usually this server is located on the external network perimeter rather than within the local network, and commands are executed in a non-interactive mode, limiting the range of possible actions. The criminals must further develop the attack to gain a more convenient, covert, and stable control channel.

[6] "Access" sold on the dark web is a generic term, referring to software, exploits, credentials, or anything else that provides attackers with unauthorized control of one or more specific remote devices.

Figure 19. Types of access traded on shadow markets



The listed connection types typically grant the attacker local privileges (administrative or user) on an endpoint. These are the most common (38% and 16% respectively) privilege levels advertised for sale. The value of such access directly depends on the importance of the corresponding server or computer. The most extensive privileges an intruder can acquire involve gaining an Active Directory domain administrator access (12% of announcements). These privileges enable attacks on all critical systems connected to the domain, including the computers of key company employees and business systems. Obtaining such a high level of access is much more challenging than local access on individual servers. It requires attackers not only to penetrate the organization's internal network but also to establish their presence, remain unnoticed, and further develop the attack. Consequently, the cost of such access is higher, and it's offered for sale less commonly.

Figure 20. Privilege level from advertisements for access trading on shadow markets

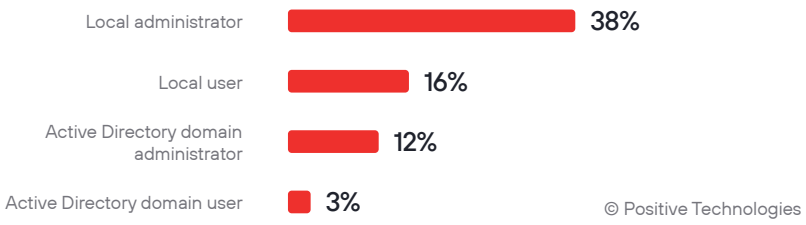


Figure 21. Advertisement selling access with domain administrator privileges

Figure 22. Advertisement selling access with system privileges on a Windows host

The price in most access ads doesn't exceed $1,000, primarily due to the widespread availability of local privilege access. However, expensive offers are not uncommon. For example, one advertisement offers privileged access to a major bank's domain for 15 bitcoins (at the time of posting, this amount was equivalent to several hundred thousand dollars).

Figure 23. Cost of initial access on shadow markets ($)

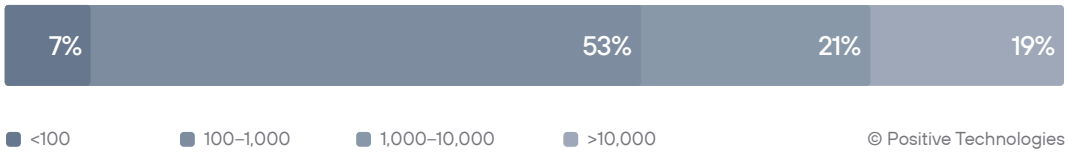
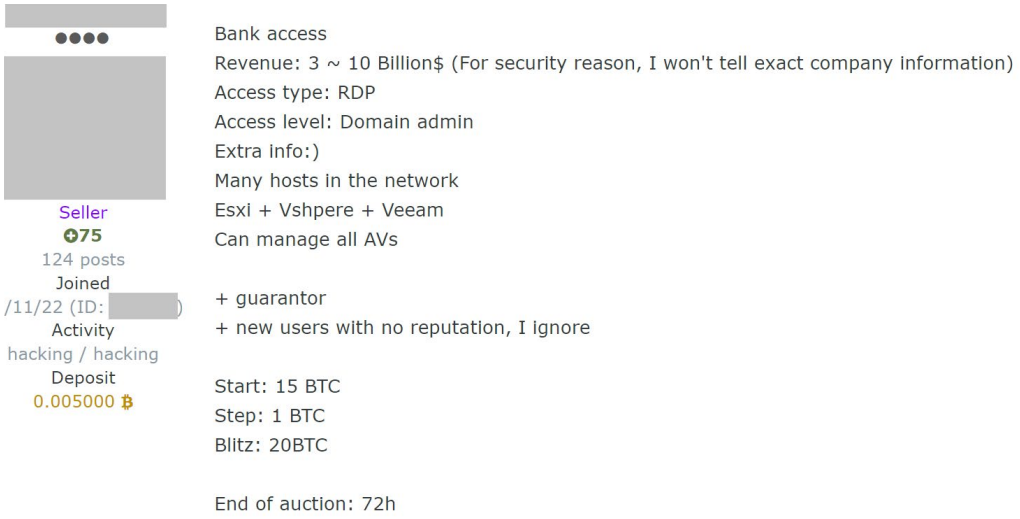


Figure 24. Privileged access to the network of a major bank for sale



High-cost offers for access to the networks of non-banking financial companies are less common. Presumably this is due to the fact that, unlike in the case with non-banking financial companies, attackers can potentially steal from banks not only a wealth of confidential information and customer data for subsequent attacks, but also substantial amounts of money directly. This was exemplified in the attack on the Indian Mahesh Bank, whose security measures were found lacking.

Figure 25. Cost of access to bank networks ($)

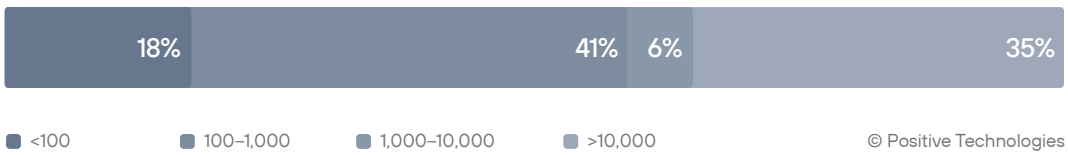
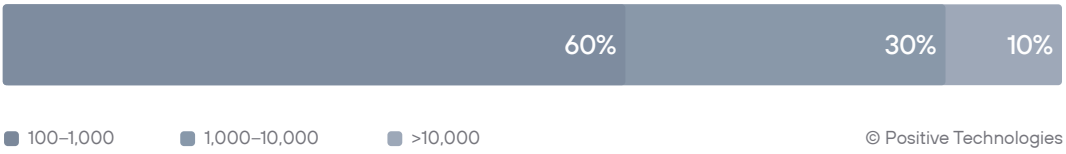


Figure 26. Cost of access to non-banking financial company networks ($)



The examples and figures above demonstrate that there are serious problems in the security of corporate network perimeters worldwide. We've confirmed this in practice. The results of penetration tests into the networks of financial organizations conducted by our experts in 2023 indicate that an external attacker can gain access to the corporate local area network of all tested banks. In all cases, vulnerabilities in software accessible from the Internet were exploited, with the oldest vulnerability dating back to 2017. Only in one bank was the perimeter so well protected that the pentesters had to identify and exploit a zero-day vulnerability to gain access. This confirms the thesis that a motivated external attacker will always find a way to penetrate even a well-protected bank. Therefore, it's extremely important to employ a security system that eliminates the possibility of non-tolerable damage to the business of a financial organization—even in the event of a breach by an intruder.

Conclusions

Stealing money from a bank through a cyberattack is a complex task for criminals: it requires in-depth knowledge of the financial organization's systems and processes. However, stealing information is another matter. Criminals leak confidential data from company networks, monetize the leaks, and attack the financial institution's clients using the obtained information. The more databases fall into criminal hands, the more detailed collections of data they can compile. Such a detailed digital profile of the victim increases the effectiveness of sociotechnical attacks. Financial organizations need to pay special attention to this issue.

Regulators should also closely monitor this area. For example, in Europe, the General Data Protection Regulation (GDPR) has been in effect for many years, and non-compliance results in significant fines in case of data breaches. Similar practices need to be developed around the world, but the potential negative consequences of such regulations must also be taken into account. On the one hand, high fines for breaches may play into the hands of criminals demanding ransom for non-disclosure: they might raise the price. On the other hand, when faced with the risk of paying a hefty fine for a breach, the company might be more motivated to pay the criminals rather than the regulatory authorities.

Regarding threats to financial organizations themselves, criminals are continuing the established tradition of demanding ransom for restoration of systems and non-disclosure of leaks while actively monetizing the results of their attacks by selling databases and ready-made access to other criminals. Financial companies should improve their vulnerability management processes and focus on securing their network perimeters. It's also crucial to pay attention to the threat associated with the distribution of malicious packages disguised as legitimate open-source software components. Developers need to monitor the dependencies in their code and check third-party code for backdoors and vulnerabilities.

Hacktivism remains relevant against the backdrop of aggravated geopolitical situations in specific regions, such as the conflict in Ukraine. It's important to note that the primary goal of hacktivists in attacks on financial organizations in this case is to destabilize the country's financial system as a whole, despite the fact that they're attacking individual companies. Attackers aim to sow panic among the population, spreading distrust toward financial institutions and government authorities. This is an industry-level threat, so individual enterprises cannot solve it alone. A centralized approach involving an industry competence center or CERT is needed. Coordinated response at the industry level based on an understanding of industry-wide non-tolerable consequences, as well as analysis of potential chains of events that could lead to such consequences, will help develop and implement an effective plan to neutralize such threats.

ptsecurity.com
pr@ptsecurity.com