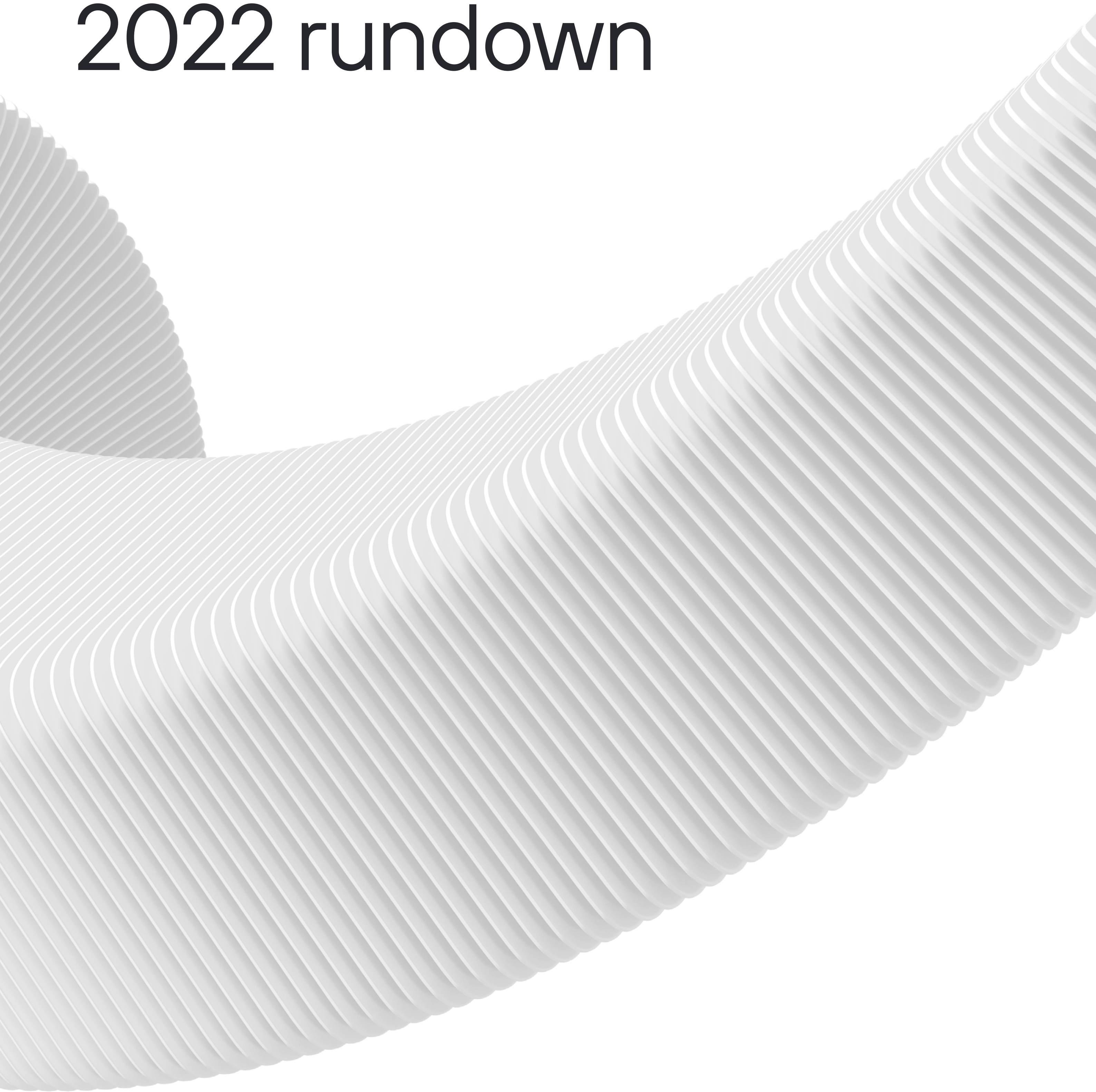
Cybersecurity threatscape: 2022 rundown



Positive Technologies

ptsecurity.com

Contents

Key figures and trends 3

Wave of attacks on web resources 4

Large-scale data leaks lead to increased popularity of social engineering 6

Spyware proliferation is on the rise 8

Ransomware and wipers 10

Social engineering: multi-factor authentication at risk 13

Attacks on IT companies have cross-industry implications 15

Rising attacks on blockchain projects 16

Statistics 17

About the research 22

Key figures and trends

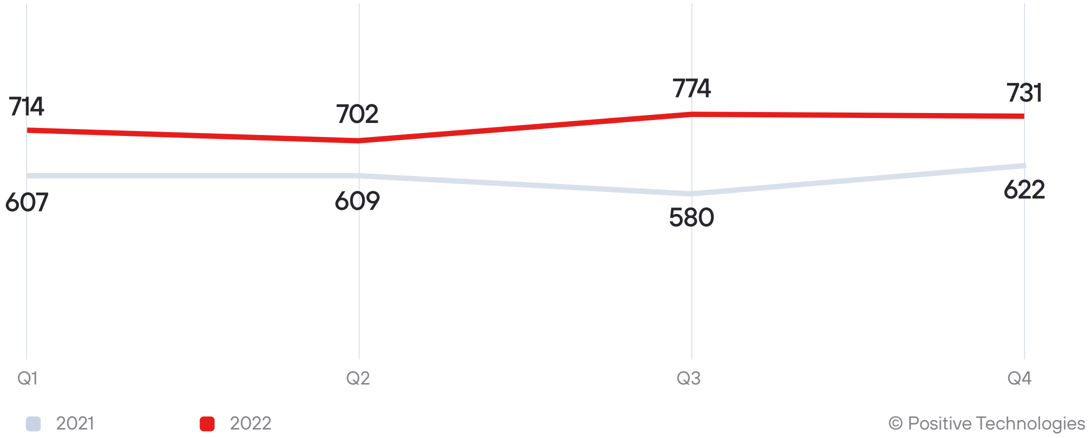
The total number of incidents[1] increased by 20.8% in 2022. We attribute this to growing tensions in cyberspace. The cybercrime market's expansion is also causing a substantial impact as cybercriminals continue to scale up their illicit operations. As a result of large-scale data leaks, attackers can use compromised user information to carry out their malicious activities. The number of attacks will grow further still in 2023 for the same reasons.

[1] Our study focuses solely on successful cyberattacks or incidents that have had detrimental effects on companies or individuals.

67%

of successful cyberattacks were targeted

Figure 1. Number of incidents in 2021 and 2022 (by quarter)



Highlights of 2022:

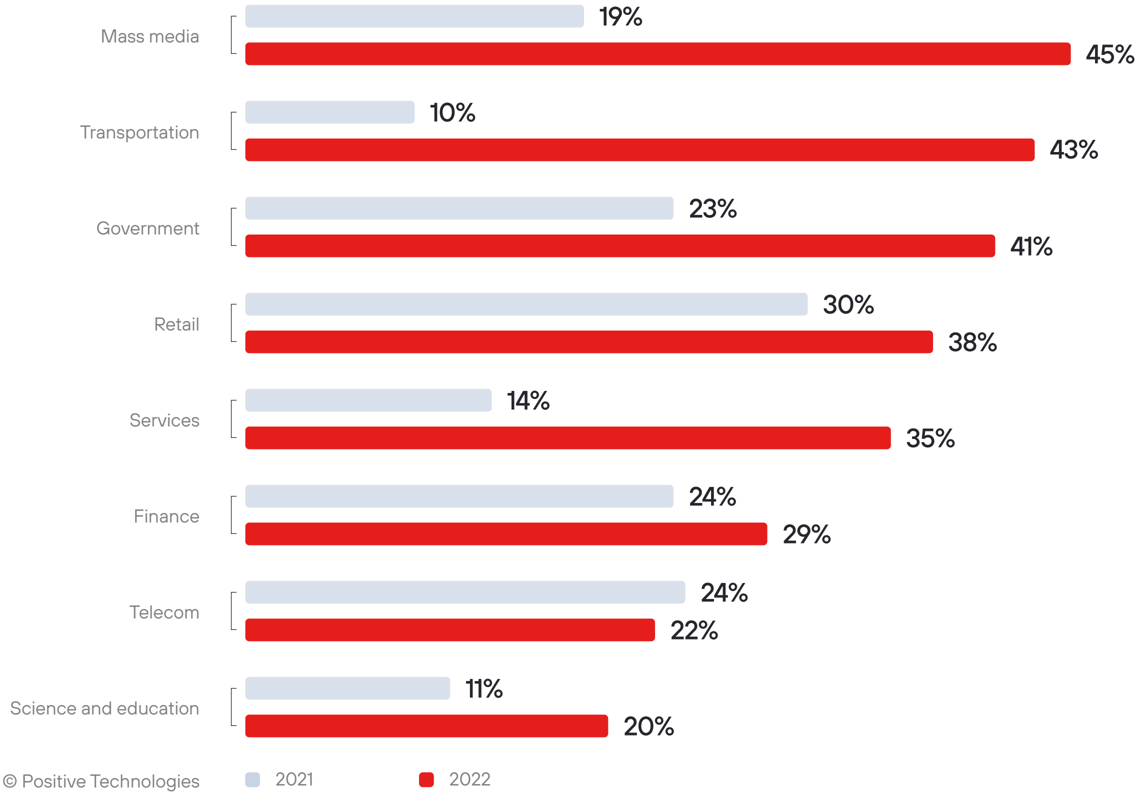
- Compared to 2021, the percentage of incidents impacting corporate web resources increased from 17% to 22%. Government institutions were hit the hardest, with successful attacks aimed at their websites more than doubling in number.
- The past year was dominated by large-scale data breaches, as numerous reports surfaced of compromised data belonging to various companies and their customers. In 47% of cases, attackers successfully stole confidential information from organizations, while in 64% of cases, they were able to steal the same from individuals.
- The use of spyware is on the rise, particularly in attacks targeting individuals. By the end of 2022, these types of malware were used in half of all successful attacks on users.
- Ransomware constituted 51% of malware used in attacks on organizations and is constantly evolving. In 2022, more groups began rewriting malware in cross-platform languages or creating versions that target both Windows and Linux systems. In 2022, we observed a surge in the use of data-wiping malware, some of which was designed to appear as ransomware.
- Social engineering remains highly effective, accounting for 43% of successful attacks against organizations and 93% against individuals. The widespread adoption of the phishing-as-a-service model has contributed to the increasing prevalence of this method. Attackers are increasingly leveraging social media and messaging platforms to target individuals, while incidents involving organizations have seen successful attacks on the second factor of authentication. These trends are likely to intensify in 2023.

- Attacks on IT companies are increasingly having cross-industry consequences, not only through subsequent hacking of customer infrastructure but also by disrupting customer business processes due to service failures.
- The popularity of cryptocurrencies continues to grow, with an increasing number of blockchain-based projects emerging. Attackers are not far behind, as the number of attacks on blockchain projects has more than doubled compared to 2021.

Wave of attacks on web resources

There was a 56% increase in successful cyberattacks targeting organizations' web resources. While web resources of companies were attacked in 17% of cases in 2021, this percentage increased to 22% in 2022. Organizations across multiple industries experienced a surge in cyberattacks, with government agencies being hit the hardest. The number of incidents targeting these agencies more than doubled, and the share of such incidents increased from 23% to 41%.

Figure 2. Percentage of incidents involving attacks on web resources in 2021 and 2022



The rising tensions in cyberspace witnessed in 2022 have led to a surge in hacktivist attacks targeting the websites of various organizations. These attacks have highly visible consequences, particularly when they impact the core business processes of companies that provide services online. Web resource incidents resulted in disruptions for organizations in 53% of cases. Attackers primarily attempted to render the website inaccessible or deface it. Compromising web resources not only enables attackers to launch large-scale attacks on visitors but also allows them to gather sensitive information about users. In Q3, the number of such attacks surged, with cybercriminals embedding malicious code in the web pages of compromised resources to carry out their nefarious activities.

Hacktivist attacks have primarily driven the rise in incidents across the mass media, transportation, and government agencies, while retail remains an attractive target for web attacks, likely due to the large amount of sensitive customer information processed by online stores. Intruders can embed malicious code into vulnerable sites to intercept personal and payment card data, leaving users at risk.

The rise in attacks on web resources is also attributed to the discovery of vulnerabilities, particularly in popular plugins like WordPress and Magento (an e-commerce plugin). The web application vulnerabilities most frequently exploited by attackers were:

- CVE-2021-44228, or Log4Shell (in Apache Log4j 2)
- CVE-2022-22965, or Spring4Shell (in Java Spring Framework)
- CVE-2022-24086 (vulnerability in Adobe Commerce)
- CVE-2021-32648 (vulnerability in October CMS)
- CVE-2022-3180 (vulnerability in the WPGateway plugin of the popular CMS WordPress)

The rise in the number of cyberattacks was significantly impacted by the growth of the shadow market, which openly distributes tools for exploiting vulnerabilities and staging DDoS attacks. We anticipate that the number of attacks targeting corporate web resources will continue to increase in 2023, particularly for companies that provide online services and collect significant amounts of customer data.

Attacks can result in unacceptable outcomes for organizations. Therefore, it is crucial to assess which business processes rely on web application performance and how an attack on web resources can impact the organization and its customers. To enhance security, we recommend conducting regular application security reviews, keeping software updated based on vendor communications, and utilizing an application-level firewall. We also advise implementing a secure web application development process to bolster security measures.

Large-scale data leaks lead to increased popularity of social engineering

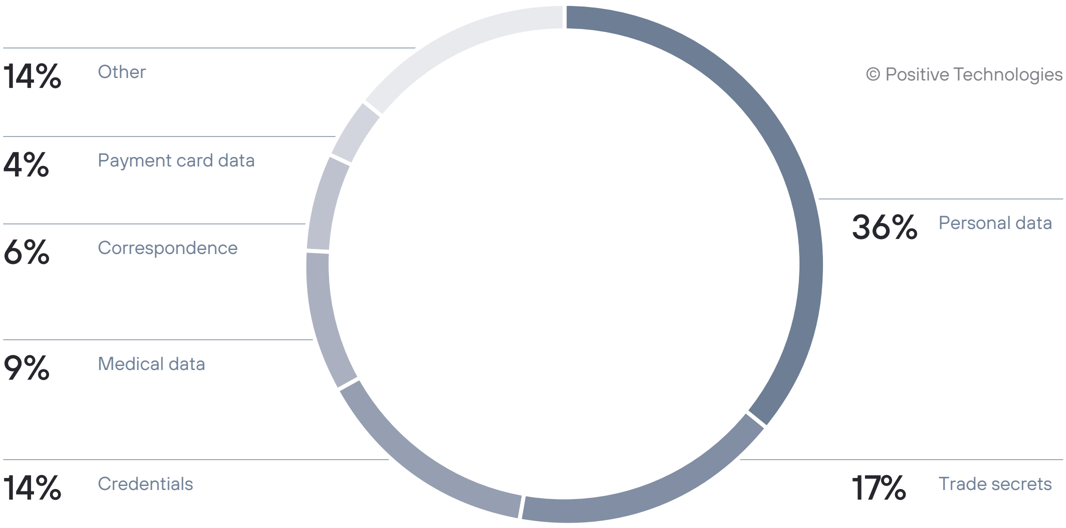
In 2022, numerous organizations and individuals worldwide, including those in Russia, were impacted by large-scale data breaches. Several incidents affected such well-known companies and services as Gemotest, CDEK, Yandex.Food, Delivery Club, and DNS. Confidential information theft occurred most frequently in medical institutions, with such incidents accounting for 82% of cases. Scientific research and educational service providers were also targeted, with 67% of such organizations falling victim, along with retailers, with 65% of these companies experiencing data theft.

The impact of data breaches around the world continues to escalate, with the average cost of such incidents reaching a record high of $4.35 million in 2022, as per an IBM report. This represents an increase of 2.6% compared to the previous year.

Sensitive information was compromised in 47% of successful attacks on organizations carried out by attackers. Of the stolen information, personal data accounted for more than a third (36%), while the attackers were also targeting information related to trade secrets (17%). Account credentials accounted for 14% of the stolen data. In successful attacks targeting individuals, attackers were able to steal data in 64% of cases. The majority of compromised data included credentials (41%), followed by personal information (28%) and payment card data (15%).

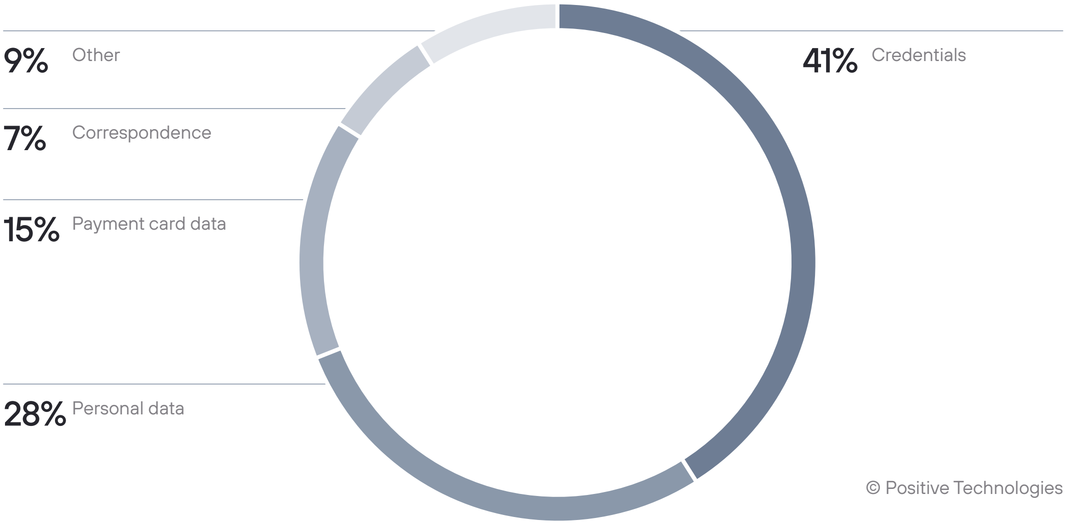
The proportion of personal data among the stolen information increased in 2021, with organizations seeing an increase of 4 percentage points (from 32% to 36%), while individuals experienced a rise of 8 percentage points (from 20% to 28%).

Figure 3. Types of data stolen (in successful attacks on organizations)



© Positive Technologies

Figure 4. Types of data stolen (in successful attacks on individuals)



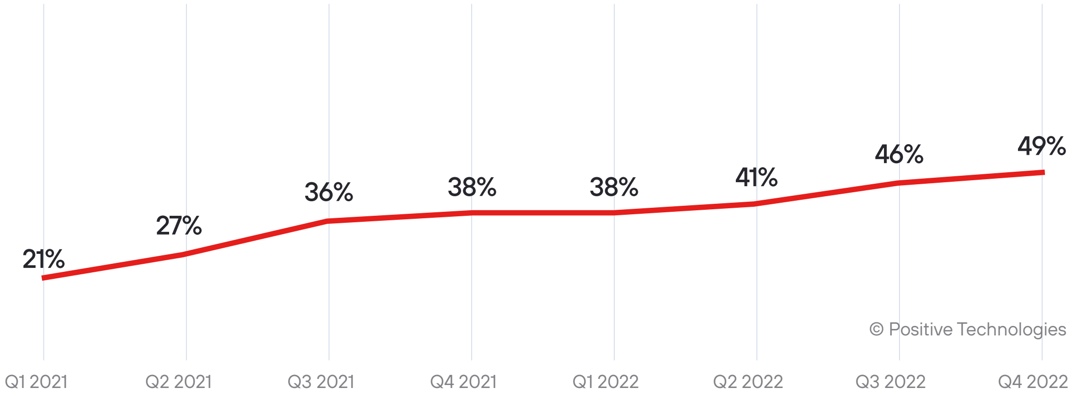
Archives containing stolen data were frequently sold on illicit forums. In the future, such large datasets will enable attackers to create digital profiles of their victims, enabling them to carry out increasingly sophisticated social engineering attacks.

To secure target and key systems, we recommend that organizations utilize information security event monitoring tools, as well as monitor external resources, which can serve as potential points of penetration. Timely education of employees on new attack techniques employed by intruders is critical, along with conducting dcyberexercises to ensure continued awareness of information security issues. Each company faces its own set of unacceptable outcomes linked to leaks of different types of information, and we recommend reviewing them to evaluate the efficacy of the measures in place.

Spyware proliferation is on the rise

Over the course of the year, there was a noticeable uptick in the use of spyware. In 2021, the usage rate of spyware in attacks on organizations was 12%, while attacks on individuals experienced a higher rate of 32%. Throughout 2022, the number of incidents involving spyware witnessed a steady rise, resulting in a corresponding increase in the share of this type of malware, with 13% being used in attacks on organizations, and a higher rate of 43% being used in attacks on individuals.

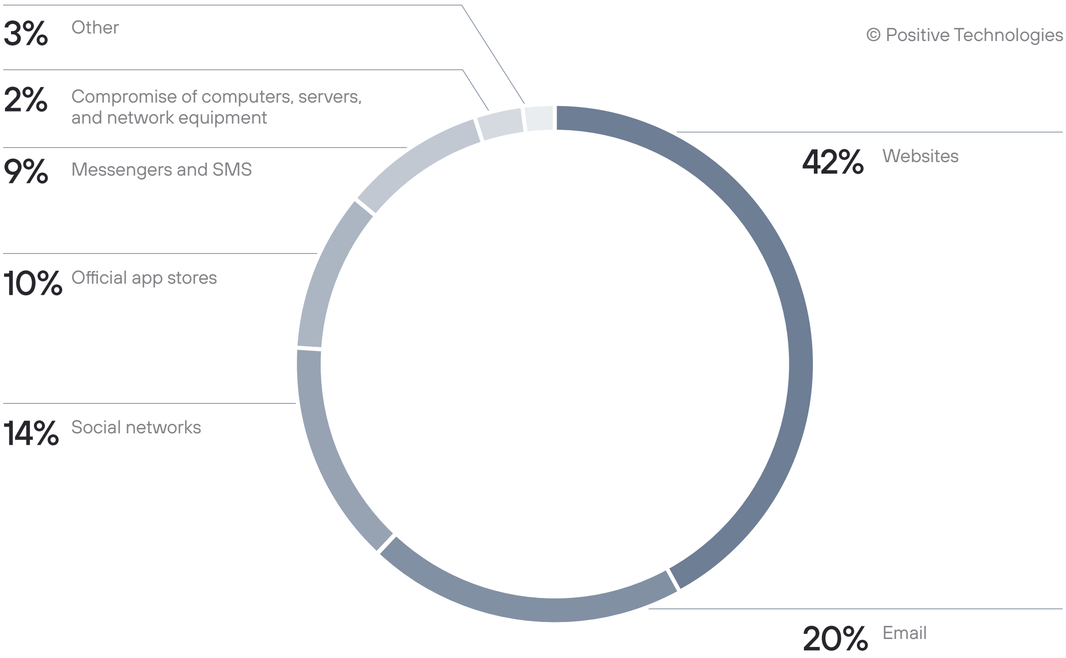
Figure 5. Use of spyware in attacks on individuals (percentage of successful attacks)



© Positive Technologies

Phishing sites are the primary distribution channel for spyware in attacks targeting individuals, accounting for 42% of all cases. Attackers opted for the traditional vector of attack, that is, email, less frequently, accounting for only 20% of incidents. Meanwhile, users of social networks and messaging apps should exercise caution, as criminals employed these channels in 14% of cases to spread malware, and 9% of attacks were carried out through messaging and text services. Throughout 2022, there were numerous incidents of spyware found in official app stores (10%). The majority of these attacks were aimed at users of Android mobile devices.

Figure 6. Methods of spyware distribution in successful attacks on individuals



© Positive Technologies

According to experts at Accenture, the most commonly used spyware viruses were RedLine, Vidar, and Raccoon Stealer. The rise of new players such as BlueFox, Aurora, and Erbium, as well as frequent updates and the increasing use of malware-as-a-service schemes have made spyware a popular choice among attackers, lowering the entry threshold for cybercrime.

The expansion of the shadow market has had a significant impact on the growth of spyware attacks. In mid-2022, we conducted an analysis of the cybercrime services market on Telegram and found that remote control malware and spyware were the most discussed types of malware, accounting for 48% of messages related to malware. It is worth noting that many commonly used remote control malware tools also have stealer features, such as intercepting text messages, tracking the user's location, screen capture, and more. Prices for such malware start at $10, and some of the spyware tools are distributed by criminals free of charge.

In staging mass attacks, criminals seek to collect user data and sell it on illicit sites. Credentials for logging in to various services, social networks, and messengers are particularly valuable, and with the growing popularity of cryptocurrencies, almost every stealer has added a data interception function to access cryptocurrency wallets. Furthermore, spyware can also compromise corporate credentials by infecting employees' personal devices when they connect to work resources.

How to protect your data? When downloading applications, it is important to verify the developer's information and carefully review other users' feedback before installation. When using social networks and messaging apps, it is important to prioritize the security of personal information by avoiding opening suspicious attachments and links. When downloading an application from a website, it is important to verify that the site is trustworthy.

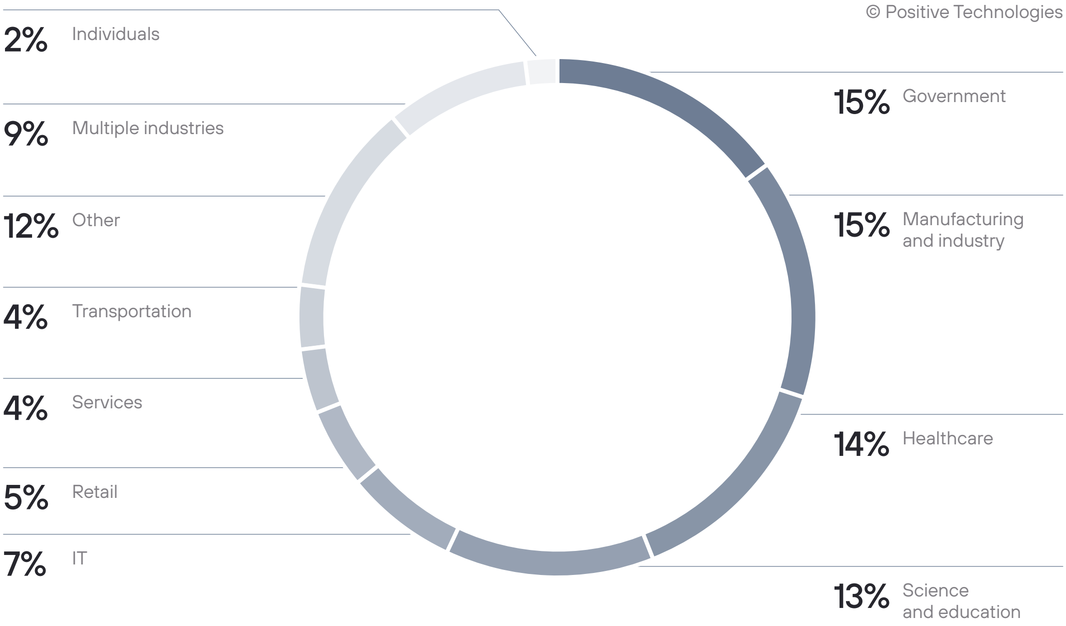
To ensure the security of corporate resources, organizations should protect employees' personal devices if they are used to access company systems. To enhance protection against spyware, we recommend using reputable antivirus software and analyzing suspicious files in a sandbox, which is a secure, isolated environment for identifying malicious conduct.

Ransomware and wipers

In 2022, ransomware continued to evolve with attackers incorporating such tools in every other successful attack (51%) on organizations with the use of malware. Ransomware operators targeted state institutions (15%), industrial enterprises (15%), medical organizations (14%), and scientific and educational institutions (13%) the most frequently.

Figure 7. Distribution of ransomware incidents by industry

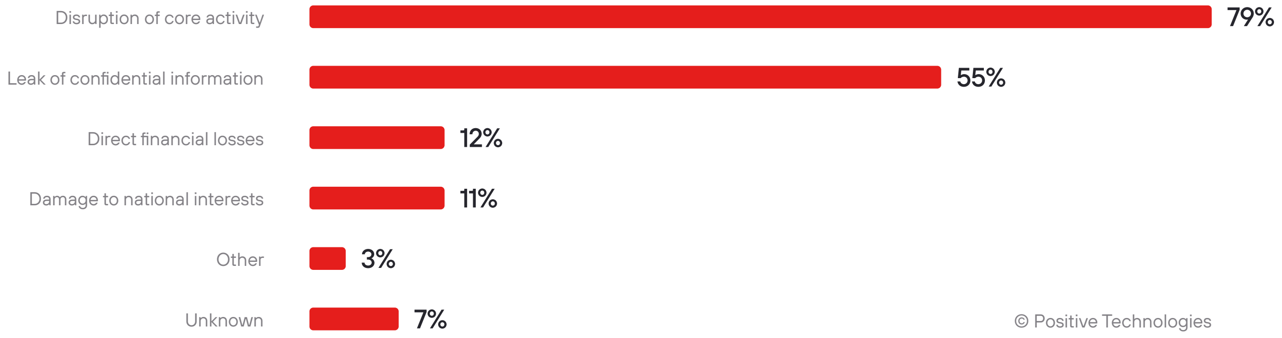
© Positive Technologies



In eight out of 10 incidents involving ransomware, the core business of the affected organizations was disrupted, leading to loss of access to infrastructure and data, disruption of services to clients, and internal business processes. In 55% of incidents, attackers were able to steal confidential information from organizations, with personal data and trade secrets being the most common types of data stolen. In 12% of cases, victims suffered financial losses such as ransom payments and losses due to downtime.

Chainalysis analysts reported a 40% decrease in profits for ransomware groups in 2022. A Coveware study reveals that the percentage of victims who paid ransom to attackers has almost halved in the past four years, from 76% in 2019 to 41%, which could be one of the reasons why profits of ransomware groups have decreased.

Figure 8. Consequences of ransomware attacks (percentage of successful attacks)



© Positive Technologies

In 2022, the following ransomware groups were most prominent for using ransomware of the same name:

- LockBit. One of the most active ransomware gangs. The ransomware group has updated its malware several times, which is now capable of executing on multiple platforms. It is notable for its careful selection of both affiliates and victims.
- Hive. The group is known for its particularly aggressive behavior, targeting critical infrastructure facilities in different countries, as well as socially important institutions such as hospitals, transportation, and police. At the beginning of 2023, the FBI successfully hacked into the servers of the attackers, resulting in the release of a decryptor.
- Vice Society. Active since 2021, this ransomware group primarily targets educational and scientific institutions, as well as medical organizations.
- BlackCat (ALPHV). A relatively new but no less formidable ransomware group, consistently targeting large organizations. With roots in DarkSide and BlackMatter, this gang has extensive experience in deploying ransomware, and is among the first to have used the Rust language to create a cross-platform version of its malware.
- Conti. A long-standing threat and a leader of the ransomware-as-a-service market until it was forced to leave the scene in May 2022 due to being targeted by intelligence agencies and disintegrating into smaller groups.

In 2021, we observed an increased interest in Linux-based systems among ransomware groups, and a notable trend in 2022 was the transition towards cross-platform versions of their malware developed using the Rust programming language. They enable attacks on both Linux and Windows systems and make it more difficult for defenses to detect the use of malware due to the scarcity of examination tools. Among major players, RansomEXX, Black Basta, and Hive rolled out cross-platform solutions.

Ransomware attacks rely primarily on speed and surprise. Attackers aim to compromise as many devices as possible within a short period, launch the malware on them, and quickly encrypt as much information as possible before being detected. In 2022, there was a trend towards using intermittent file encryption with specific byte-by-byte steps. The encryption process becomes faster and less noticeable to suspicious activity monitoring tools, as it involves a smaller number of operations on the encrypted file and results in a higher similarity to the original file. The BlackCat group adopted an unconventional approach by skipping the encryption step and using an exfiltration tool to send the data to a remote server and corrupt the local copies of the files. This approach is faster, less time-consuming, and ensures that the victim will be motivated to negotiate, as the files cannot be recovered and the working copies are solely in the possession of the attackers.

In 2022, there were instances where the source codes of well-known ransomware families, such as Conti and Yanluowang, were leaked. This may result in a slowdown in the growth of ransomware attacks in 2023, as security researchers will be able to analyze the malware code and techniques more thoroughly, potentially leading to better defense against these attacks. On the flip side, there is also the risk of new ransomware groups forming and using the leaked source code to develop their own encryption samples and launch attacks.

Proliferation of wipers

The number of incidents involving data deletion software—wipers—increased by 175% since the year before. The first half of the year saw a rise in the incidence of wipers, with notable examples including HermeticWiper (Foxblade), DoubleZero, and IsaacWiper, among others.

After some time, a new variant of wipers emerged, disguised as ransomware and demanding a ransom for the recovery of data. However, the keys for decryption were not provided, and the data itself could be encrypted randomly. Recovery, especially when multiple systems have been affected by malware, can be time-consuming. Industrial organizations are particularly vulnerable to wipers, as they can cause the shutdown of critical technological processes and lead to industrial accidents. It is worth noting that wiper attacks have traditionally targeted Windows systems, but in 2022 experts identified malware samples that posed a threat to Linux-based systems.

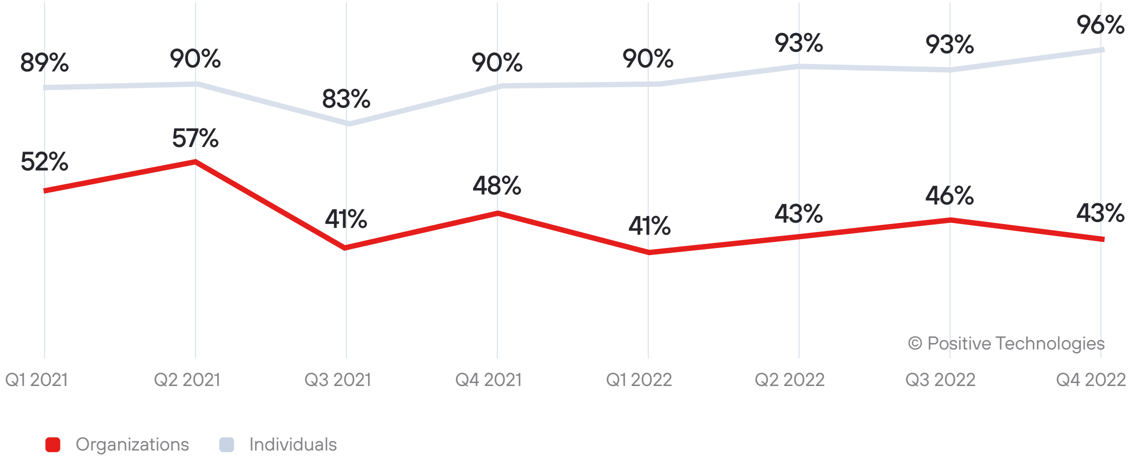
To safeguard against attacks involving ransomware and wipers, we recommend to:

- Use data backup solutions. In the event of a successful attack, specialists can quickly restore data and systems from offline backups that are preferably stored on servers located outside the office network perimeter.
- Use antivirus tools and sandboxes.
- Monitor network activity and endpoint activity.
- Install security updates and promptly respond to information security incidents.
- Have an IT infrastructure recovery plan

Social engineering. multi-factor authentication at risk

The percentage of social engineering incidents in attacks on individuals increased from 88% in 2021 to 93% in 2022. Although the number of attacks on organizations remains steady, the percentage of incidents using this method has dropped from 50% to 43%. Against the backdrop of numerous data leaks, attackers are able to stage attacks with the use of compromised data, including credentials. In 2022, attackers were able to gain access to target systems and resources in 16% of successful attacks on organizations by compromising credentials. This was achieved either by mining passwords or by using compromised credentials from data breaches.

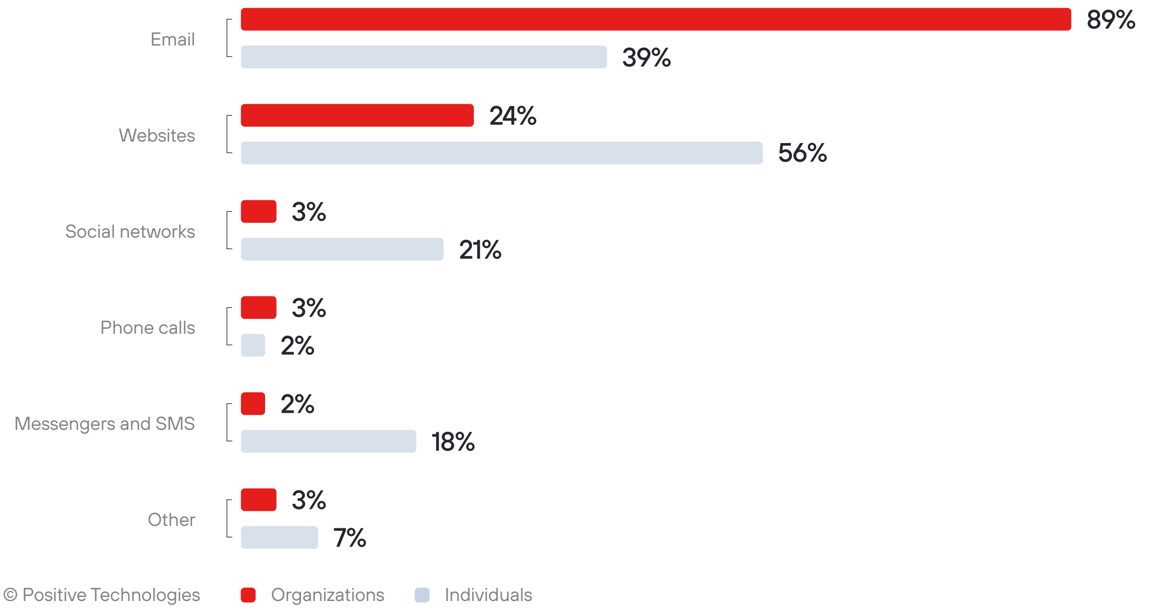
Figure 9. Share of incidents with the use of social engineering



© Positive Technologies

In nearly nine out of 10 successful attacks on organizations involving social engineering, attackers used malicious emails. In attacks on individuals, fraudsters primarily used phishing sites (56%). Throughout the year, we also observed a rise in successful attacks through messengers and SMS messages (18%) and social networks (21%).

Figure 10. Social engineering channels used by intruders



In 2022, we witnessed a proliferation of the phishing-as-a-service model, with attackers utilizing ready-made phishing kits in their attacks, and in some incidents, using tools to bypass multifactor authentication. At the end of the year, there was a surge in MFA Fatigue-type attacks, where attackers made multiple attempts to log into an account using stolen credentials, causing an endless stream of MFA push notifications to be sent to the account holder's mobile device. Eventually, some users would confirm the login to the resource to stop the barrage of messages. We anticipate a rise in the number of attacks aimed at circumventing the second factor of authentication in the future.

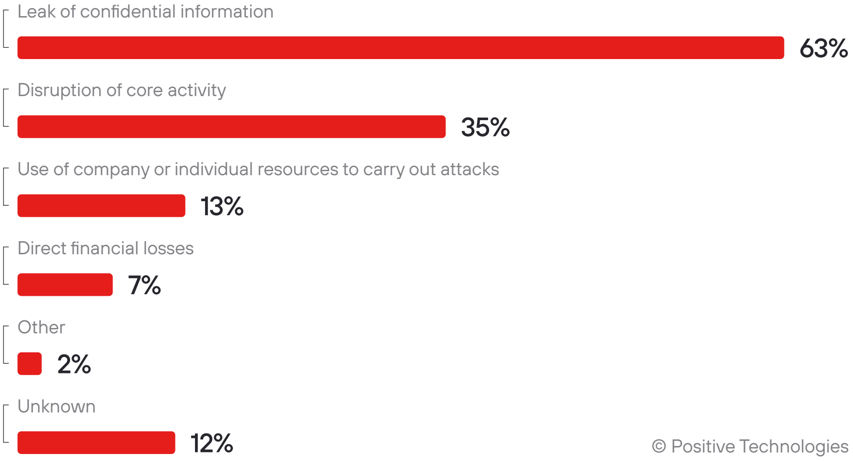
To enhance security, we recommend setting a threshold for the number of login attempts and temporarily blocking the account if the limit is exceeded. If you receive an excessive number of login notifications, and you are not the one attempting to log in, it is recommended that you report the incident to your organization's information security officer

This could indicate that your credentials have been compromised.We recommend that individuals exercise caution when using social networks and messengers by refraining from clicking on suspicious links, sharing personal information, and transferring funds to unknown or unverified recipients.

Attacks on IT companies have cross-industry implications

Throughout 2022, the number of successful attacks targeting IT companies gradually increased, with the number of attacks in the fourth quarter nearly twice as high as in the first quarter. The most frequent incidents that occurred at IT companies involved leaks of confidential information, which accounted for 63% of the total incidents, followed by the disruption of core business (35% of cases), and the use of company resources to conduct attacks (13% of cases).

Figure 11. Consequences of attacks on IT companies (percentage of successful attacks)



© Positive Technologies

The compromised confidential information mainly included intellectual property (31%), with numerous leaks of the source code of IT products being the most frequent type of incident. At the beginning of the year, for example, we saw a series of attacks by the Lapsus$ group aimed at stealing information from Globant, Microsoft, Nvidia, and Samsung. The compromised data was subsequently exploited by the attackers; for instance, the stolen Nvidia certificates were used by cybercriminals to sign malware, making it appear legitimate.

IT solutions provided by companies are utilized by various organizations and individuals. Therefore, the disruption of IT companies can have negative consequences for their customers. For example, in 46% of such incidents, organizations experienced service delivery failures. Intrusion by criminals in several successful attacks rendered inoperable various organizations from different sectors such as healthcare institutions, government agencies, and rail companies. In some instances, attackers targeted users through IT product and service providers. Okta, a provider of multifactor authentication solutions, was targeted in a series of successful attacks that occurred throughout the year. In one of these attacks, intruders managed to access the data of more than 300 company customers.

Attacks on cloud services and virtualization environments continued to occur in 2022. In attacks on developers, attackers actively spread malware through libraries for popular frameworks.

We expect attacks on software supply chains and IT companies' customers to continue in 2023. Developers of IT solutions need to be vigilant about such non-tolerable events and provide effective protection measures. We recommend that developers regularly analyze their code for security vulnerabilities, thoroughly check third-party libraries used during development, and participate in bug bounty programs to promptly identify and fix any security issues in their products.

Rising attacks on blockchain projects

As predicted earlier, the interest of attackers in cryptocurrency exchanges and DeFi protocols significantly increased in 2022, with the number of attacks on blockchain projects more than doubling compared to 2021. In 78% of the incidents, attackers successfully managed to steal funds, resulting in damages in some cases amounting to several hundred million dollars. According to Chainalysis, the year 2022 witnessed the highest financial losses caused by cyberattacks targeting cryptocurrency companies, with a staggering $3.8 billion stolen. The most high-profile hacks include:

Ronin sidechain ($617 million stolen)

BSC Token Hub ($566 million stolen)

Wormhole ($326 million stolen).

Attackers most commonly exploited smart contract vulnerabilities (78%), with flash loan attacks being the most popular[2].

The number of attacks targeting owners of cryptocurrency assets has been increasing as well. Attackers spread messages on social networks and messengers about free giveaways of tokens and NFTs, urging users to transfer funds and promising a much greater return. Meanwhile, almost every stealer has already acquired the capability to steal the credentials of popular cryptocurrency wallets.

We expect to see a continued rise in the number of attacks on blockchain projects in 2023, as well as an increase in fraud targeting cryptocurrency asset owners.

To protect themselves, we advise users to exercise caution when receiving messages that promise significant profits, conduct thorough research on projects before investing, and secure their accounts at cryptocurrency exchanges and wallets with two-factor authentication. Developers should audit smart contracts, follow secure development processes, and participate in bug bounty programs to identify vulnerabilities.

[2] A flash loan attack occurs when a vulnerability in a specific platform's smart contract is exploited. The perpetrator borrows a large amount of funds that do not require collateral. The borrowed funds are then used to conduct transactions on the exchange, artificially inflating or deflating the value of cryptocurrencies. All actions are performed in a single transaction.

17%

of successful attacks targeted individuals

Statistics

Figure 12. Categories of victims among organizations

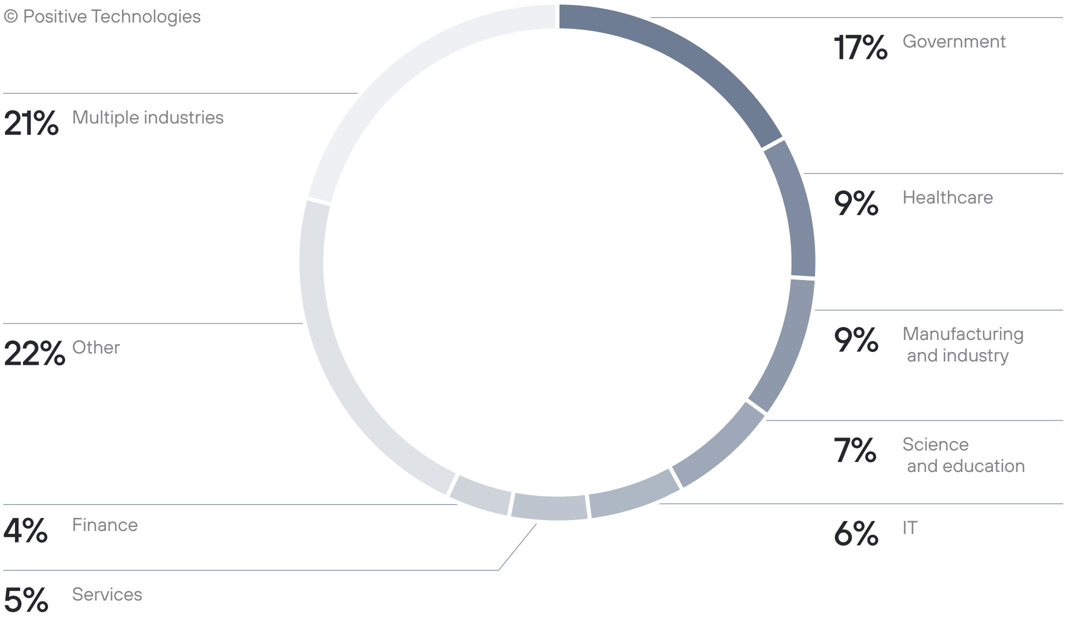


Figure 13. Consequences of attacks (percentage of successful attacks)

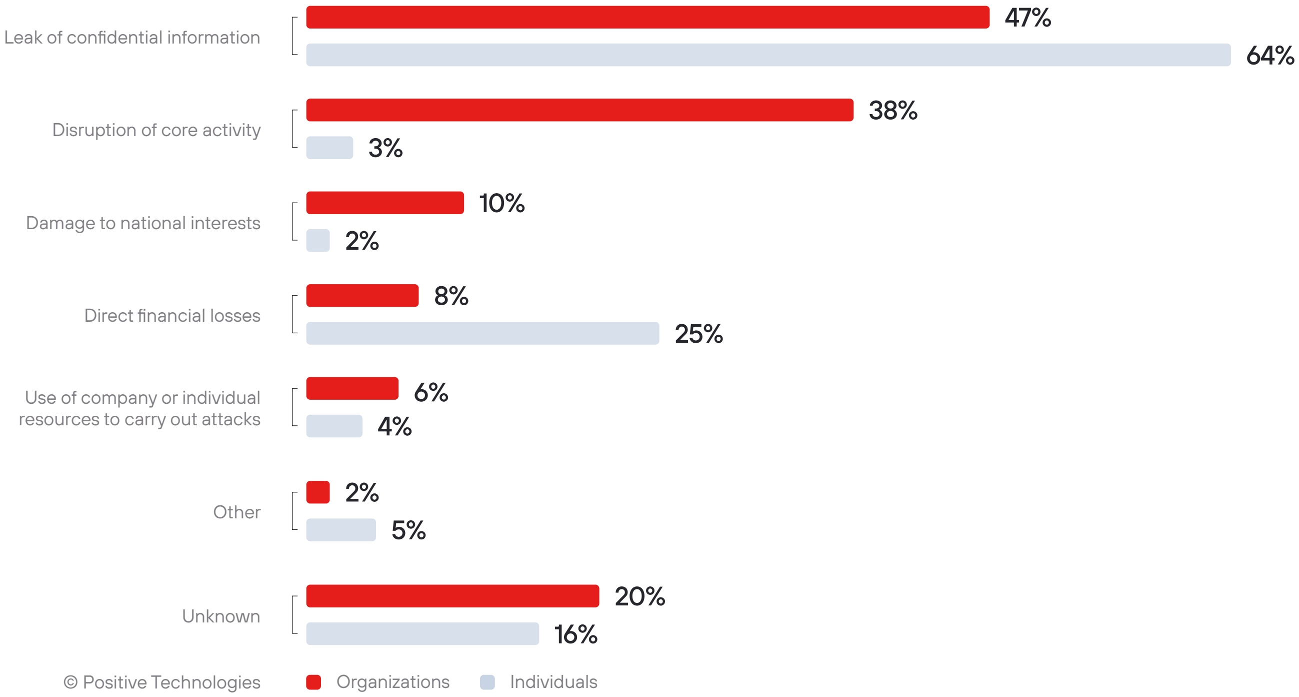


Figure 14. Targets of attacks (percentage of successful attacks)

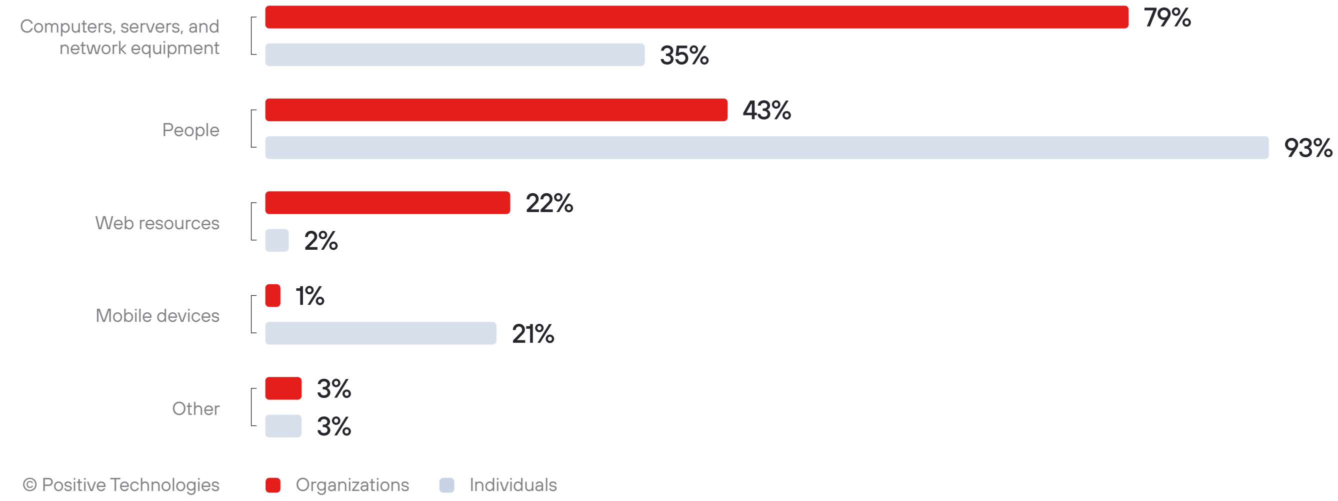


Figure 15. Methods of attacks (percentage of successful attacks)

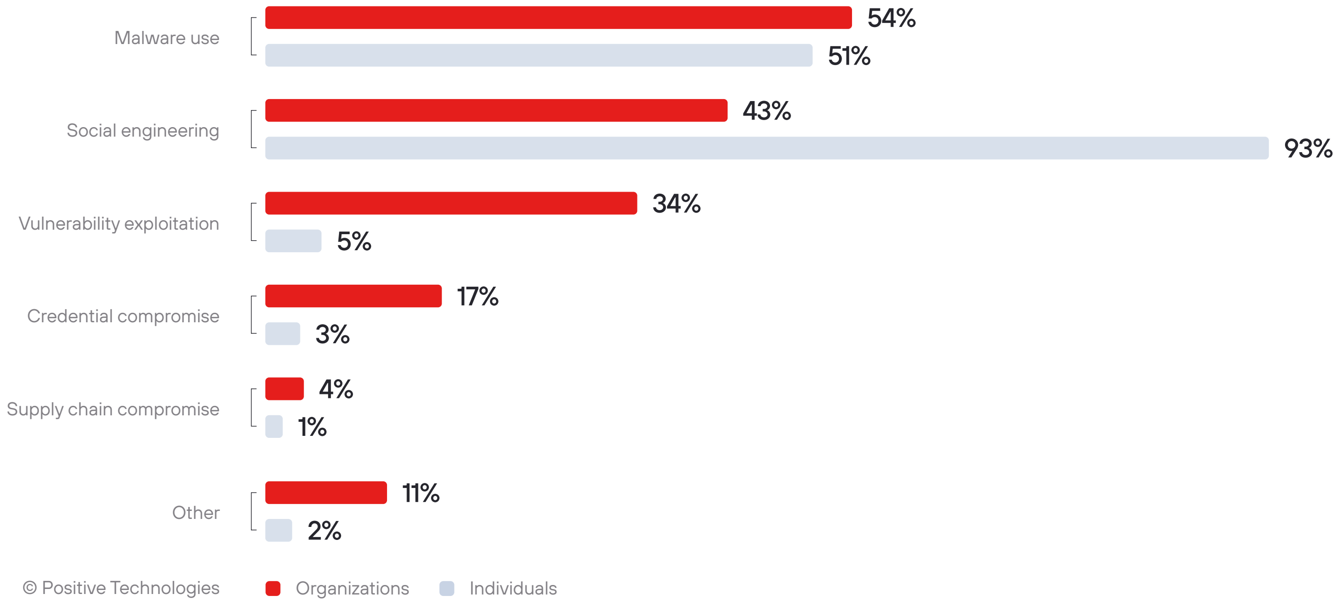
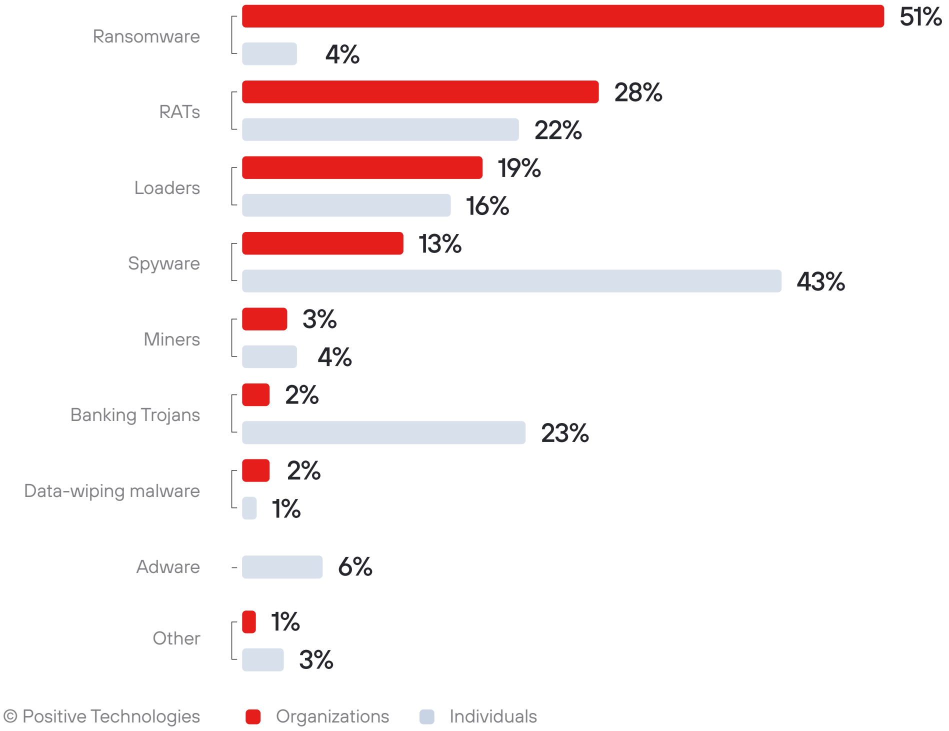


Figure 16. Types of malware (percentage of successful malware attacks)



© Positive Technologies

Figure 17. Malware distribution methods in successful attacks on organizations

© Positive Technologies

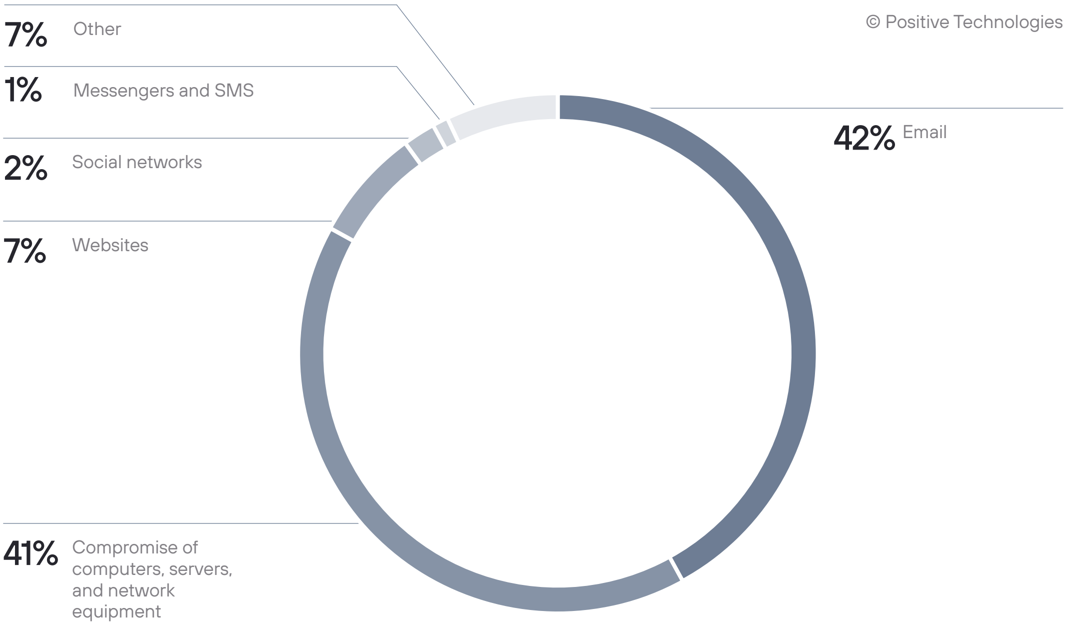


Figure 18. Methods of malware distribution in successful attacks on individuals

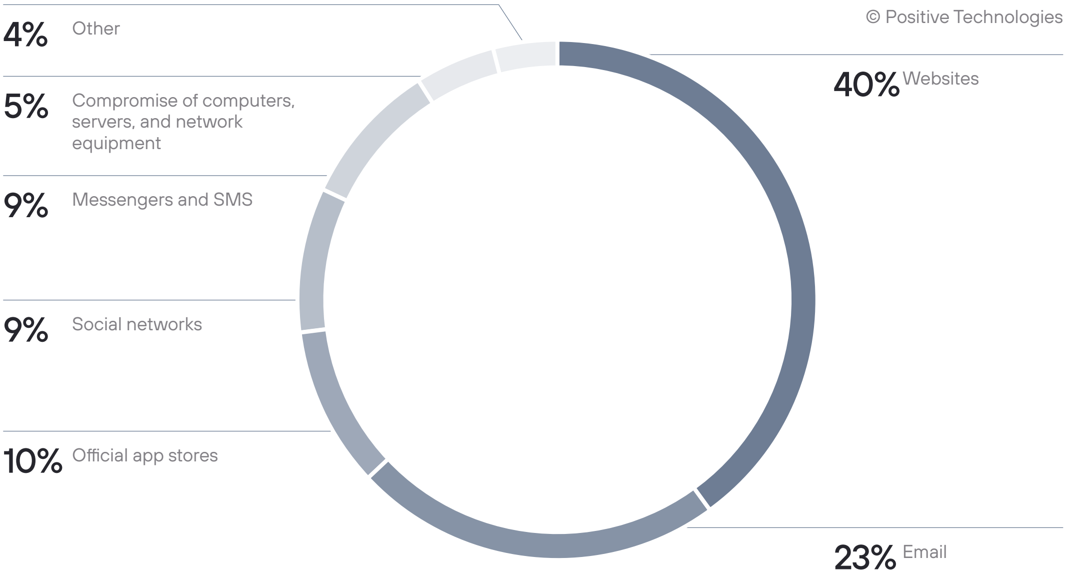
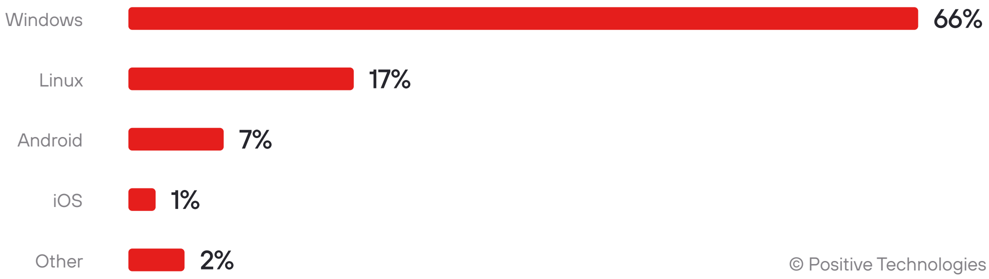


Figure 19. Target OS in malware attacks (percentage of successful attacks)



	Distribution of cyberattacks by target, method, consequence, and victim category	Victim categories									
		Government	Manufacturing and industry	Science and education	Services	IT	Healthcare	Finance	Other	Multiple industries	Individuals
	Total attacks	403	223	170	113	136	228	105	528	511	504
Target	Computers, servers, and network equipment	289	193	150	70	114	194	92	378	435	177
	Web resources	165	26	34	40	20	13	30	161	50	11
	People	164	99	100	44	42	118	50	162	265	468
	Mobile devices	4	—	1	—	—	1	1	4	10	105
	Other	5	5	2	—	3	1	2	31	12	17
Method	Malware use	190	159	124	30	86	121	53	212	337	255
	Social engineering	164	99	100	44	42	118	50	162	265	468
	Credential compromise	51	47	43	20	47	58	16	81	38	16
	Vulnerability exploitation	106	92	35	40	47	57	28	196	224	26
	Supply chain compromise	19	5	6	3	7	9	1	18	18	6
	Other	98	4	5	11	5	2	16	91	39	10
Consequences	Disruption of core activity	206	104	100	29	48	77	43	232	78	14
	Leak of confidential information	141	121	114	71	85	187	56	201	165	323
	Damage to national interests	164	13	2	—	1	1	2	63	4	11
	Direct financial losses	15	17	6	7	9	10	6	83	39	124
	Use of company or individual resources to carry out attacks	9	3	5	13	18	4	6	21	69	18
	Other	1	3	4	1	2	3	—	12	28	23
	Unknown	85	46	24	10	16	9	28	69	200	80

Darker colors indicate a greater proportion of attacks within a particular victim category

0%	10%	20%	30%	40-100%

About the research

This report contains information about information security incidents around the world, based on Positive Technologies' own expertise, study findings, and data from reputable sources.

We believe that the majority of cyberattacks are not made public due to reputational risks. The result is that even organizations that investigate incidents and analyze activity by hacker groups are unable to do a precise count of threats. This research aims to draw the attention of companies and individuals who care about the state of information security to the key motives and methods of cyberattacks, and to highlight the main trends in the changing cyberthreat landscape.

This report considers each mass attack (for example, phishing emails sent to multiple addresses) as one incident, not several. For explanations of terms used in this report, please refer to the Positive Technologies glossary.

ptsecurity.com
pr@ptsecurity.com

Positive Technologies is an industry leader in results-oriented cybersecurity and a major global provider of information security solutions. Our mission is to safeguard businesses and entire industries against cyberattacks and non-tolerable damage. Over 3,300 organizations worldwide use technologies and services developed by our company.

Positive Technologies is the first and only cybersecurity company in Russia to have gone public on the Moscow Exchange (MOEX: POSI), with 180,000 shareholders and counting.

Follow us on social media (Twitter, Habr) and in the News section at ptsecurity.com.