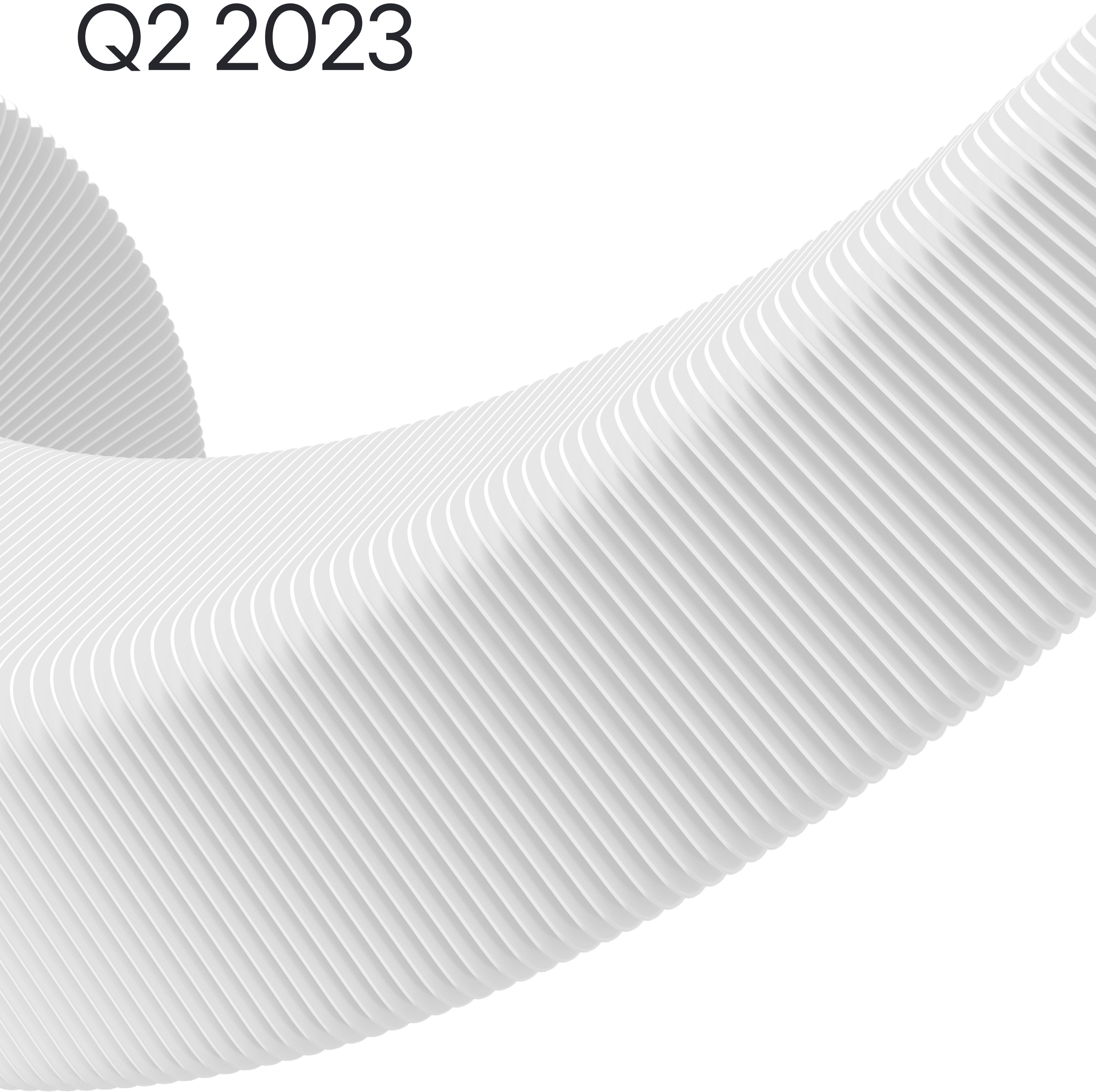
Cybersecurity threatscape: Q2 2023



Positive Technologies

ptsecurity.com

Contents

Key figures and trends

In Q2 2023, the number of incidents rose by 4% on Q1 and by 17% year-on-year. Targeted attacks accounted for 78% of the total. Successful cyberattacks on organizations most often resulted in leakage of confidential information (67%) and disruption of core operations (44%). The period saw numerous major leaks of users' personal data and large-scale attacks that exploited vulnerabilities.

Targeting secure data transfer products

In Q1, the Cl0p ransomware group executed a large string of corporate hacks that took advantage of a zero-day vulnerability (CVE-2023-0669) in GoAnywhere MFT. In Q2, they managed to successfully exploit a vulnerability they had found (CVE-2023-34362), where malicious SQL could be injected into MOVEit Transfer , a managed file transfer application by Progress Software. Cl0p had been aware of the vulnerabilities for some time, as the group tried to extract data from hacked MOVEit servers as early as April 2022.

Among the victims were the owners of well-known cybersecurity brands. For instance, Gen Digital (Avast, CCleaner, Norton LifeLock) confirmed that some of its employees' personal data was compromised as a result of the latest attack on MOVEit.[1]

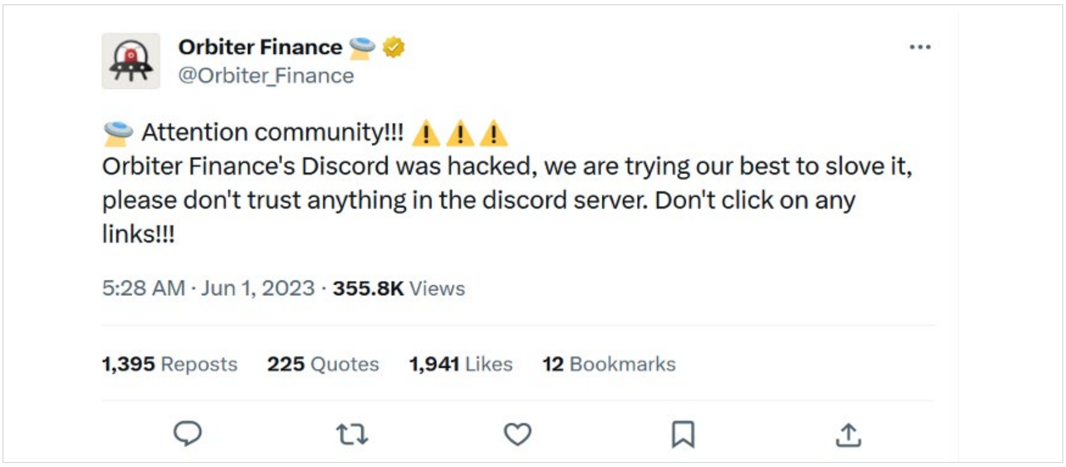
Considering how successful Cl0p has been in exploiting zero-day vulnerabilities in managed file transfer software, one can expect the group to stick to a similar strategy against other products in the category going forward. Cl0p's zero-day exploitation approach suggests that not every ransomware group wants to see its efforts produce instant financial gains, and some are capable of playing the long game to maximize their profits. Cybercriminals realize that attacking multiple victims at a time achieves greater effect, and the time invested pays off in the long run.

Blockchain projects under attack

Blockchain remains an attractive goal for attacks that target not just protocols but also social media accounts to deceive users and steal funds: blockchain projects were hit by cybercriminals twice as frequently in Q2 than in Q1. A well-prepared attack in Discord that targeted the owners of cryptocurrency exchange servers resulted in the loss of $3,000,000. Posing as journalists, the attackers used social engineering techniques to trick the server administrators into verifying their identities following an "interview". After being redirected to a malicious website, the administrator had their Discord user token stolen from them. The cybercriminals then logged in to the server using the administrator's account, removed all other administrators, and published a phishing post.

[1] At the time of publishing this text, the group has listed more than 700 companies on its leak site as victims of the MOVEit hack, demanding that they pay a ransom.

Figure 1. Warning for users that a Discord server has been hacked



Orbiter Finance 🛸
@Orbiter_Finance

🛸 Attention community!!! ⚠️⚠️⚠️
Orbiter Finance's Discord was hacked, we are trying our best to slove it, please don't trust anything in the discord server. Don't click on any links!!!

5:28 AM · Jun 1, 2023 · **355.8K** Views

1,395 Reposts **225** Quotes **1,941** Likes **12** Bookmarks

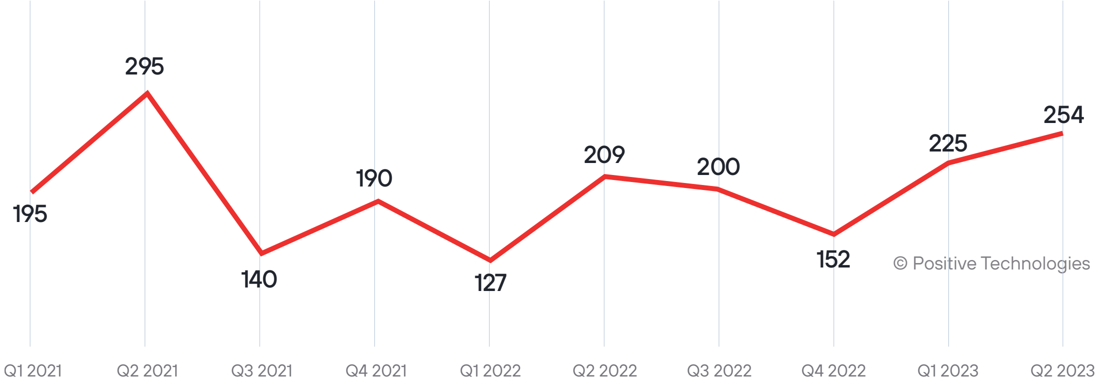
Official Twitter accounts were hacked as well. Thus, attackers posted a fake crypto giveaway tweet on behalf of KuCoin, promising that anyone who sent cryptocurrency would get twice the amount. The 45 minutes that KuCoin's Twitter account remained compromised was enough for users to make transactions totaling $22,600. The platform promised to reimburse all losses.

There were also bigger attacks on blockchain protocols by both anonymous hackers who promised to return most of the stolen funds if inquiries into their past crimes were discontinued ([1], [2]) and APT groups, such as Lazarus, which was involved in the Atomic Wallet hack and the theft of $35,000,000 from cryptocurrency wallets.

Continued growth in ransomware activity

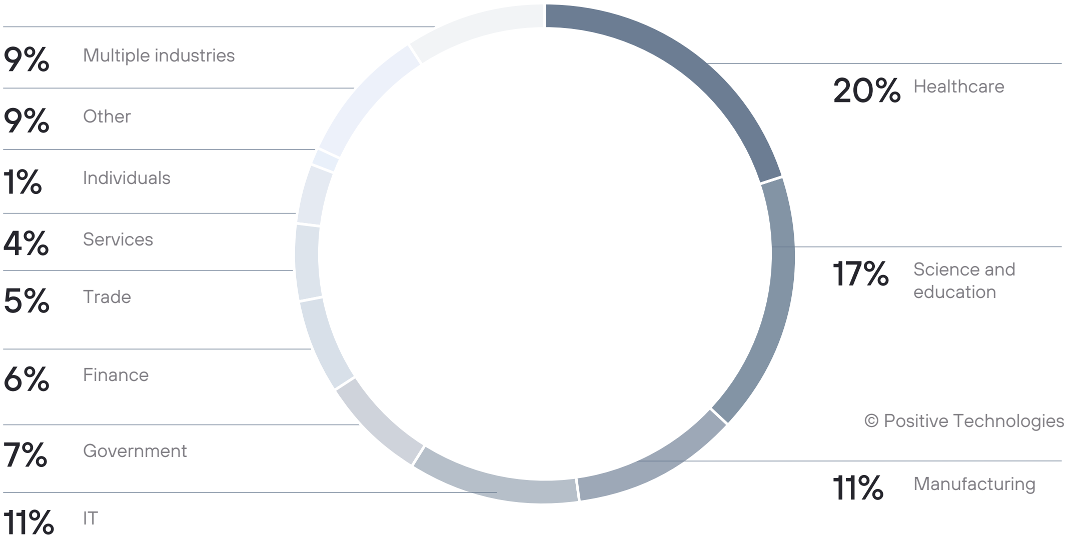
Ransomware attacks continued growing in Q2, increasing by 13%.

Figure 2. Number of ransomware attacks (by quarter)



The situation in the research, academic, government, and healthcare sectors remained tense despite hacker infighting and prosecution by security agencies: the LockBit ransomware gang blocked one of its affiliates for targeting Keystone SMILES Community Learning Center, a nonprofit serving preschoolers, while Cl0p said it had deleted any data stolen from U.S. Federal agencies after the government offered a bounty for information about the group.

Figure 3. Ransomware attacks by category



© Positive Technologies

We saw the share of IT companies in the total number of ransomware victims rise by 5 p.p. to 11% in Q2 compared with Q1. The driving factor was potential benefits for cybercriminals: successful attacks on IT companies provide access to the companies' and their clients' confidential data and open up possibilities for both supply chain and trusted relationship attacks.

New names are appearing among active ransomware gangs: 8Base is an experienced player that has been hitting organizations everywhere in the world. After a period of silence and low popularity, the group launched a new leak site and took second place, after LockBit, in June in terms of the number of victims. First detected in March 2023, the Akira ransomware operators upped their game in Q2 by entering the rankings of 10 most prolific groups. However, already in late June, Avast released a free decryption utility for Windows systems. Akira then targeted Linux systems, which had no decryptor support.

Q2 was not without unique campaigns. MalasLocker, first detected in April 23, attacks Zimbra servers by exploiting the CVE-2022-24682 vulnerability and encrypts victim systems, but demands that the victim make a charitable donation, rather than pay a ransom. In Q2, MalasLocker became the second-largest group by number of victims. Most of the attacked companies were based in Italy, the United States, and Russia.

Extortion without encryption

Extortion in the cyberspace has evolved from demanding ransom for decrypting data to encrypting data and threatening to publish it (also known as double extortion).

Companies have responded by increasing the focus on cybersecurity, implementing cyberattack response protocols, endpoint monitoring and response tools, and backup systems. Ransomware does not always produce the desired effect on the victim, while requiring the attacker to exert significant effort to bypass security and deploy the malware. All of the above has prompted hackers to abandon the encryption stage and adopt the use of stolen confidential information as the main tool for pressuring victims, as also reported by Barracuda. Cl0p's attacks on organizations, which did not use double extortion, suggests that this is an effective and still-relevant type of attack. The Karakurt and RansomHouse groups, which originally aimed only at stealing data to extort money, continued to pursue their campaigns into Q2 2023.

A further reason for the groups to give up encryption and switch to threats of publishing stolen data might be the inflow of decryption tools released by security professionals. For example, White Phoenix helps to recover files encrypted with the popular intermittent encryption method. The BianLian group continued its extortion campaign, but stopped to encrypt victim systems because a decryptor was published.

Spyware on the rise

Q2 saw the share of malware attacks on organizations drop by 8 p. p. compared to Q1. The decrease is due to a rise in vulnerability exploitation attacks, with their share reaching 35%. The usage of malware in attacks on individuals increased by 5 p. p.

According to ANY.RUN, the RedLine infostealer became the top malware family, experiencing a surge in popularity in Q2. The most popular Android malware, according to a Check Point study, was SpinOk, also a type of spyware. The trend for using this malware type in attacks on organizations (21%) and individuals (62%) continued.

In Q2, the PT Expert Security Center team managed to discover a new lightweight stealer written in Go that searched for files (by name extension) in the home directory and on local drives, and then sent these files to the C&C server, along with screenshots and the contents of the clipboard. The stealer was delivered with phishing email messages that contained a link to an NSIS installer. Phishing email is one of the most widely used (57%) malware delivery vectors in attacks on organizations. When launched, the installer opened a PDF file and simultaneously attempted to deliver a payload to the user's device.

In attacks on individuals, malware is delivered mainly with the help of websites (40% of all cases). The trend for using SEO poisoning, which we described earlier, remained active in Q2. Threat actors combined SEO poisoning and malvertising on websites ([1], [2], [3]) to spread malware.

Trending vulnerabilities

The number of vulnerabilities discovered per quarter is on the rise: 7% more were detected in Q2 than in Q1. The number of new vulnerabilities exceeded 7,500, according to the data released by the U.S. National Institute of Standards and Technology (NIST). Cybercriminals continue to exploit older vulnerabilities, as some systems still run outdated operating systems and software. The following vulnerabilities were actively exploited in Q2:

- CVE-2023-34362. A widely exploited zero-day vulnerability in MOVEit MFT that allows attackers to gain access to any files and escalate their privileges on a server by injecting malicious SQL code into requests sent to the server.
- CVE-2023-27350 and CVE-2023-27351. Critical vulnerabilities in PaperCut MF and NG print management software. The Lace Tempest group has been able to compromise vulnerable servers, gain remote access, deliver ransomware, and then exfiltrate confidential information.
- CVE-2023-2868. A zero-day vulnerability in Barracuda Email Security Gateway, associated with incomplete validation of incoming data in the email attachment scanning module. The flaw allows injecting remote commands using specially generated malicious TAR files. The APT group known as UNC4841 took advantage of the vulnerability to conduct a cyberespionage campaign by mass-mailing a malicious attachment. Barracuda releasing a security patch for vulnerable appliances was deemed insufficient: the company insists that compromised appliances be replaced.
- CVE-2018-9995 and CVE-2016-20016. In April 2023, researchers from FortiGuard recorded significant upsurges in attacks that exploited the CVE-2018-9995 vulnerability in DVR devices by TBK (more than 50,000 unique attempts) and the CVE-2016-20016 vulnerability in MVPower digital video recorders. Exploiting CVE-2018-9995 allows attackers to bypass authentication on the device and gain access to a vulnerable network, while exploiting CVE-2016-20016 allows executing commands unauthenticated with the help of malicious HTTP requests. Spikes like this one suggest that old and vulnerable devices are susceptible to attacks years after the exploit is first discovered.

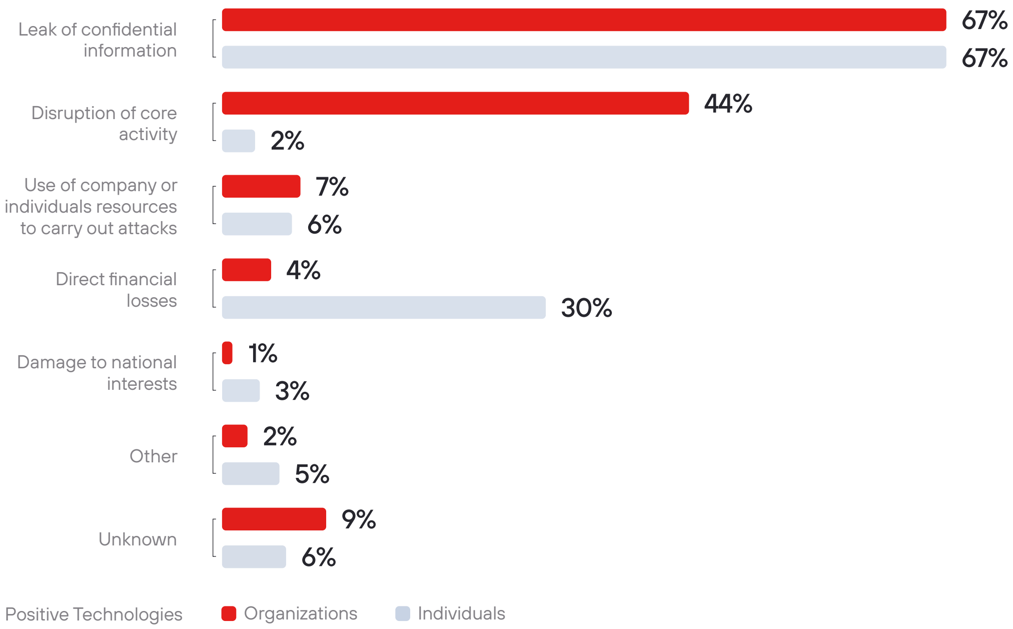
Recommendations

To protect yourself against attacks, we first and foremost suggest following our general guidelines on personal and corporate cybersecurity. Considering the types of incidents we saw in Q2 2023, we strongly recommend treating incoming email, instant messages, and messages you get on social media with caution: checking the sender and refraining from clicking any suspicious links to avoid falling for social engineering attacks or having your device compromised by malware. Be prudent and think through your decisions, especially when you see attractive offers. Download applications from trusted sources only, use file backup services, and install security patches as they become available. In addition, we recommend thoroughly investigating every major incident to identify points of compromise and vulnerabilities exploited by attackers, making sure that the cybercriminals did not leave any backdoors open. You can harden the perimeter with the help of modern security tools, such as web application firewalls (WAF). To prevent malware infection, we recommend using sandboxes to analyze the behavior of files in a virtual environment and detect any malicious activity.

Attack consequences

The consequences of attacks in Q2 were varied, with successful cyberattacks affecting both small and large businesses, as well as whole cities and districts. Most often, cyberattacks resulted in the bad actors obtaining confidential information and business operations being disrupted. A ransomware attack on the U.S. megalopolis of Dallas is an example of a cyberattack impacting a city. The attack disrupted city services: police had to manually dispatch teams to emergency calls, some jury trials were postponed, and water utilities could not process online payments.

Figure 4. Attack consequences (percentage of attacks)



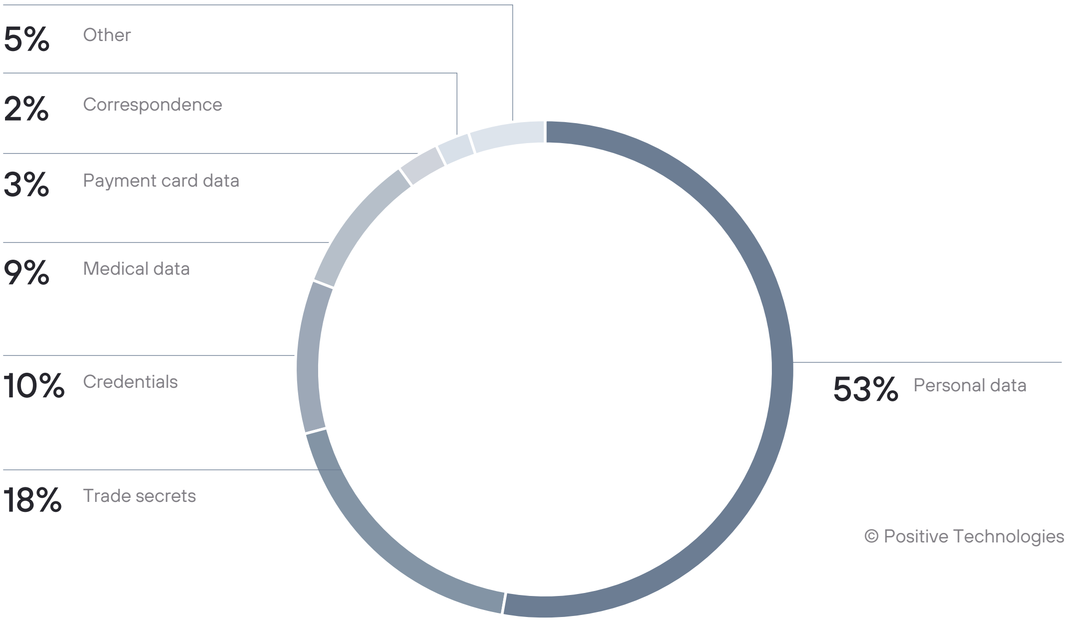
© Positive Technologies

The top five attacks in Q2 to cause a negative impact and wider repercussions

- A Cyberattack on Bitmarck, a major German ISP, forced the company to shut down all of its internal and client-facing systems. The downtime negatively affected mandatory health insurance organizations that used Bitmarck's IT services. Among the disrupted services were access to patient health records, processing of electronic sick leaves, centralized processing of companies' data, submission of monthly statistical reports, and digital communications.
- The hospitals in Idaho Falls and Mountain View, as well as their partner clinics were attacked by ransomware, forcing some of them to stay closed. Idaho Falls confirmed that several ambulances were redirected to neighboring hospitals. It took the clinics more than a month to fully restore their processes.
- Large-scale DDoS attacks on Microsoft applications caused failures on the Outlook, OneDrive, and Azure websites. Customers who saw service disruptions were unable to use the email or cloud services. As many as 18,000 users could not get access to Outlook as the attack reached its peak. The attacks were launched one at a time for three days by the hacktivist group Anonymous Sudan.
- LockBit demanded that TSMC, Asia's highest-valued company and one of the world's largest manufacturers of semiconductors, pay a ransom of $70,000,000 to prevent its data from being published. The data had been leaked from a misconfigured server belonging to the IT equipment vendor Kinmax Technologies.
- The Russian company Infotel, which provides integration of banks and companies with the Bank of Russia automated digital communications system, faced a cyberattack by the hacktivist group Cyber.Anarchy.Squad. The attack left several major client banks cut off from the national banking systems. It took the telecommunication operator 32 hours to restore service.

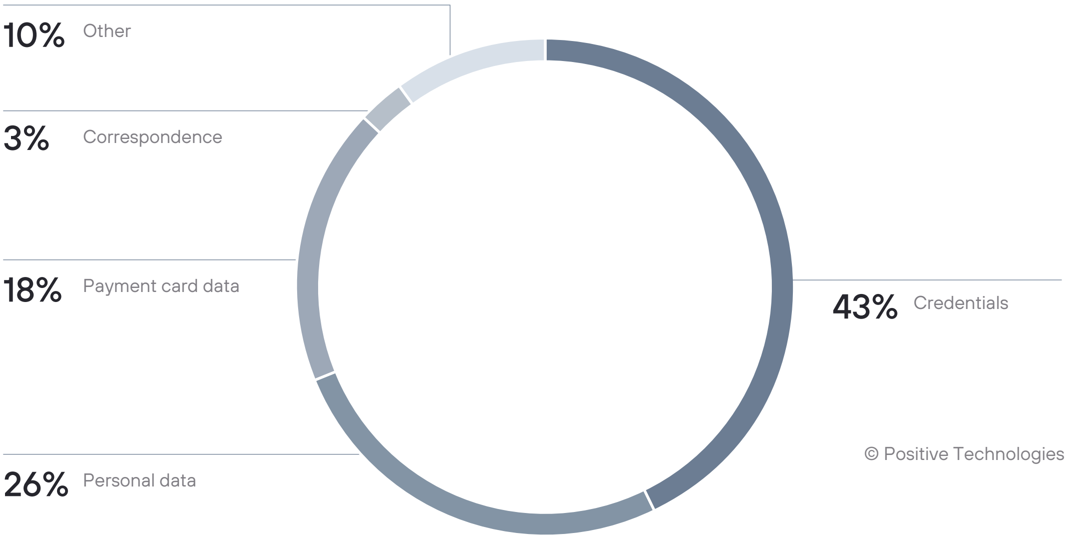
Attacks that led to leaks of confidential data mostly aimed to steal personal data (53%) and trade secrets (18%) from organizations. Attacks on individuals largely aimed at stealing their credentials (43%).

Figure 5. Types of data stolen (in attacks on organizations)



© Positive Technologies

Figure 6. Types of data stolen (in attacks on individuals)



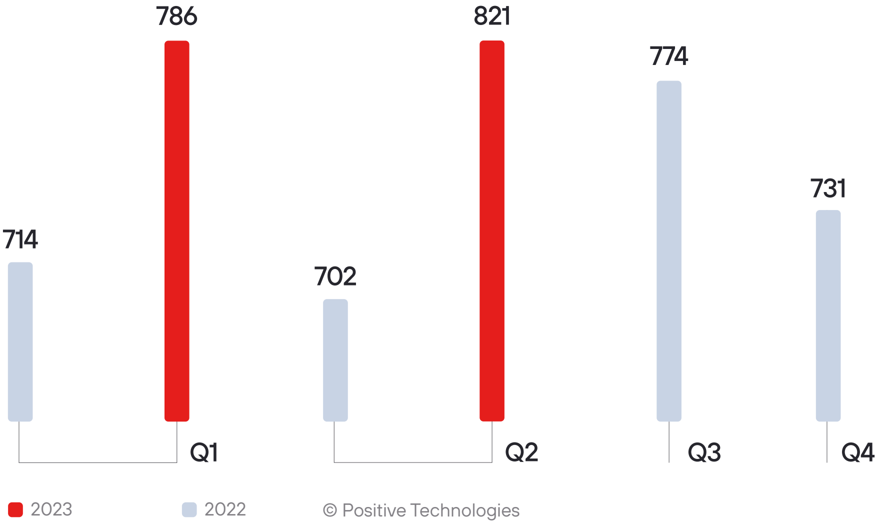
© Positive Technologies

The most notable leaks in Q2

- Some of the notable victims of the Cl0p attack on MOVEit Transfer were Louisiana's Office of Motor Vehicles (OMV) and the Oregon Department of Transportation (ODOT). The leak affected 3,500,000 holders of IDs and driver's licenses in the State of Oregon, and 6,000,000 in Louisiana.
- Affected customers of Harvard Pilgrim Health Care filed four class-action lawsuits against the company, accusing it of failure to ensure the security of personal and health data. In April, the organization was hit by a malware attack that resulted in 2,500,000 individuals' data being leaked.
- Personal details belonging to the customers of 12 Russian companies were leaked online for three days: full names, phone numbers, email addresses, and in certain cases, even password hashes. The list of the companies featured the Auchan, Tvoy Dom, and Leroy Merlin retail chains, Gloria Jeans, book24.ru, Askona, Bukvoed, Tvoe, and Chitai-Gorod online stores, cooking website edimdoma.ru, AST and Eksmo publishers, and Roza Khutor mountain resort. Auchan, Gloria Jeans, book24.ru, Askona, and the Eksmo-AST group confirmed the leaks.
- After negotiations over a $4,000,000 ransom fell through, The Money Message ransomware group published Intel Boot Guard private keys and firmware keys stolen from hardware company MSI. The extortionists claimed to have stolen 1.5 TB of MSI data. The leak affected the entire Intel ecosystem and posed a direct threat to MSI customers. The keys could be used by an attacker to create malicious firmware updates, and then deliver these with the help of BIOS and MSI update tools.
- Medical treatment and laboratory diagnosis data on 2,500,000 Enzo Biochem patients was compromised during a ransomware attack. Some of the data was wiped from the company's systems altogether. Enzo Biochem did not suspend service even as its internal business processes were disrupted while it worked to limit the scope of the attack. Enzo Biochem, along with its Enzo Clinical Labs affiliate, were hit with four class-action lawsuits that accused the company of failing to ensure sufficient security of the client data it stored.

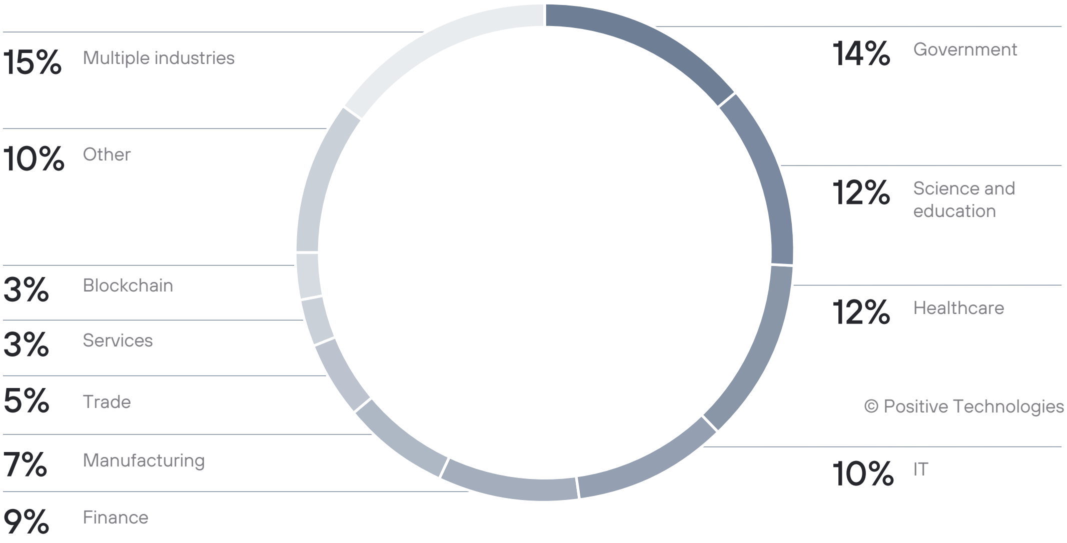
Statistics

Figure 7. Number of incidents in 2022 and 2023 (by quarter)



© Positive Technologies

Figure 8. Categories of victim organizations



© Positive Technologies

Figure 9. Attack targets (percentage of attacks)

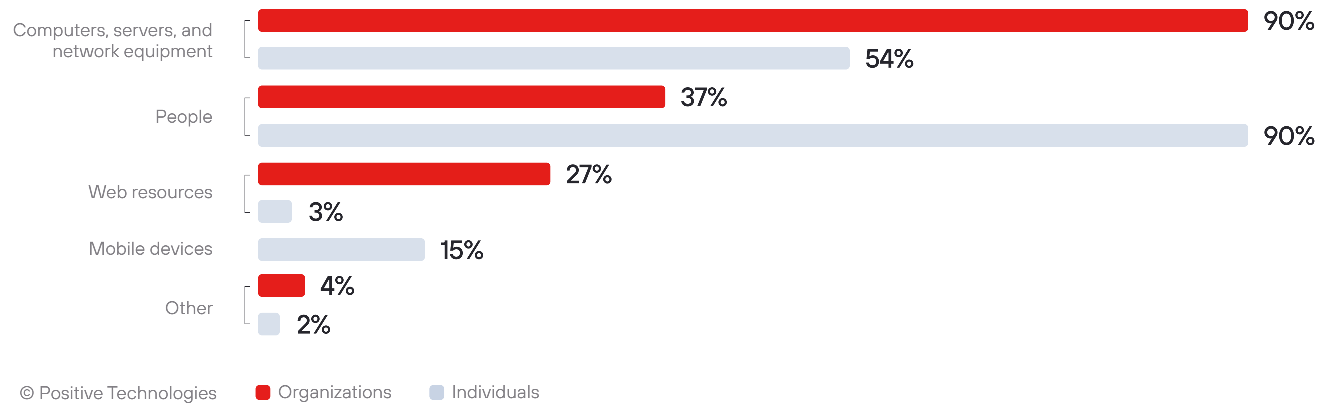


Figure 10. Attack methods (percentage of attacks)

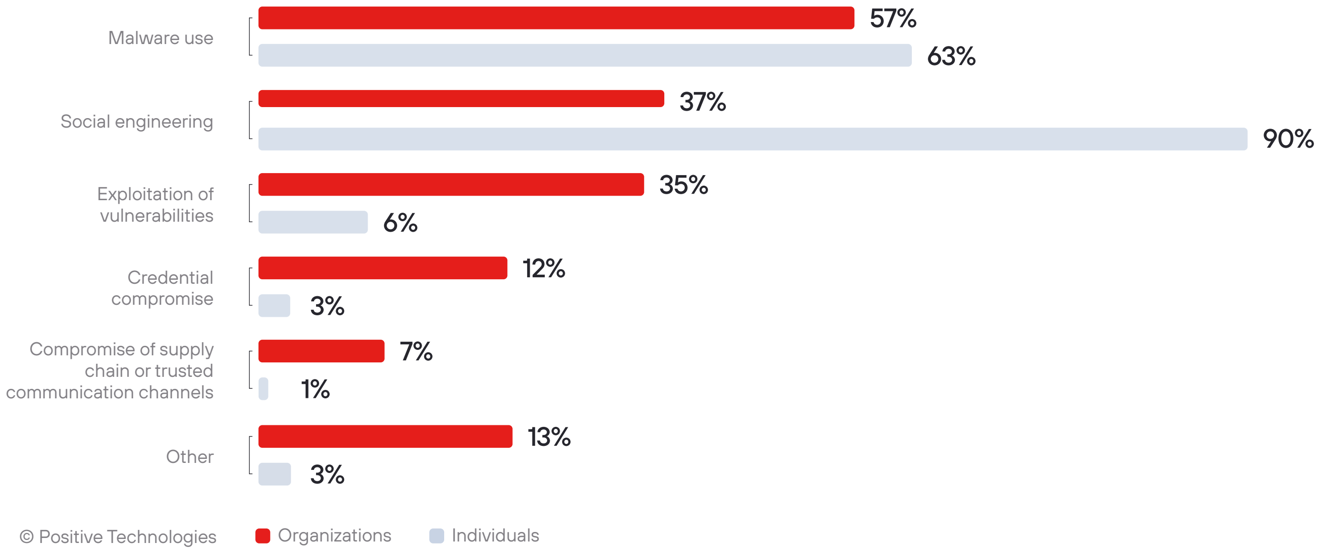


Figure 11. Types of malware (percentage of malware attacks)

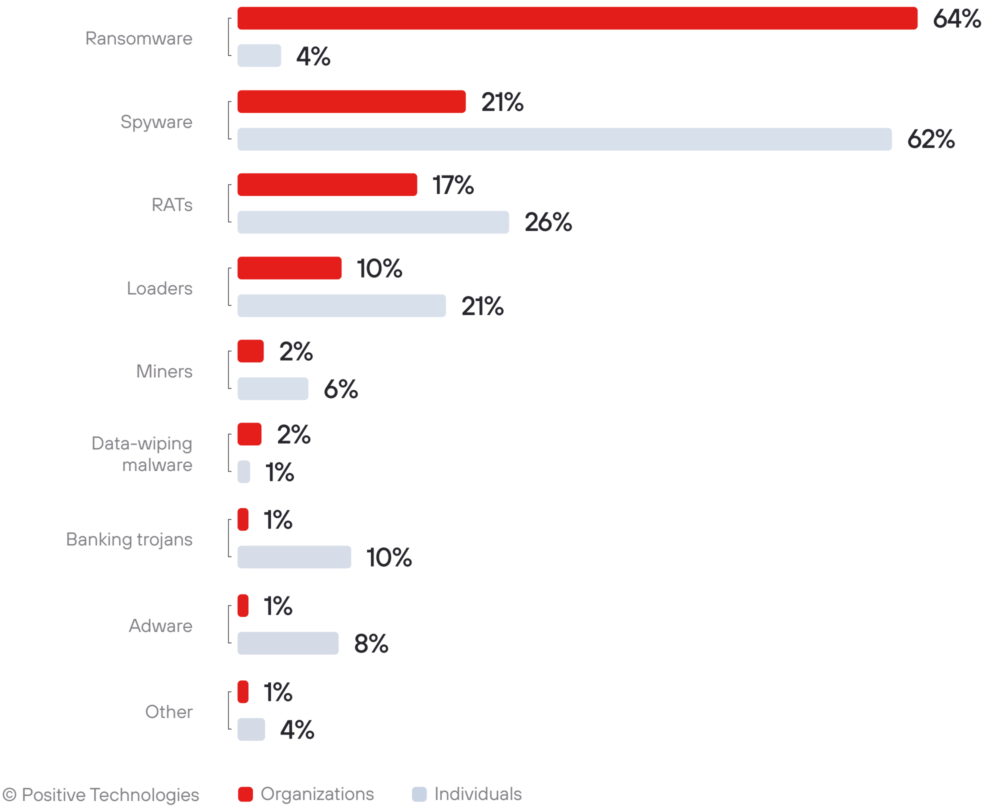


Figure 12. Malware distribution methods in attacks on organizations

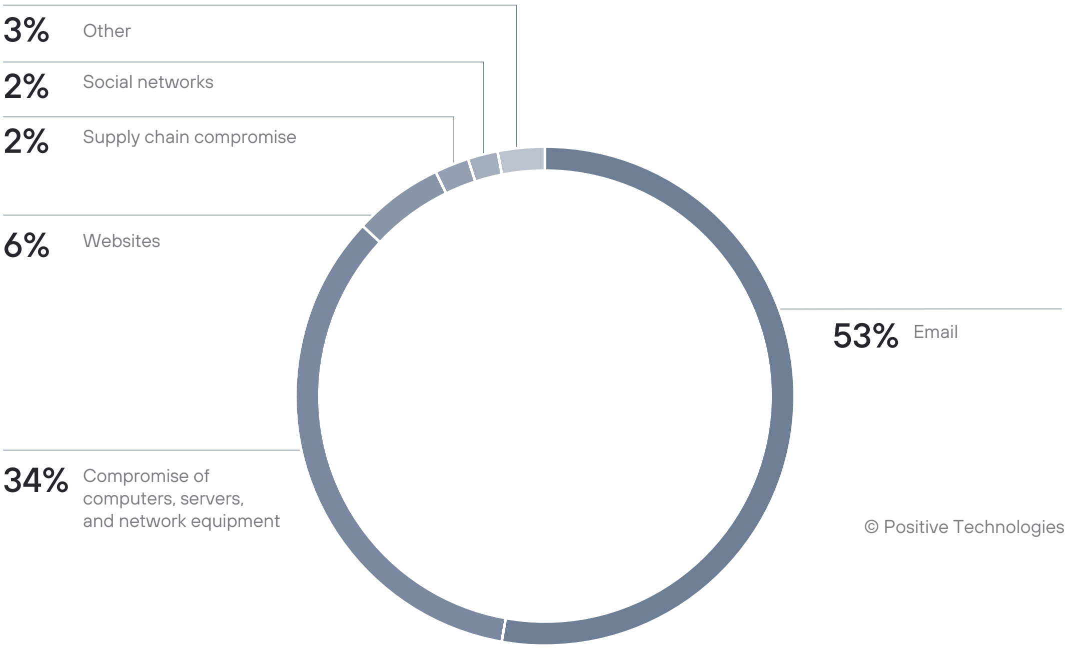


Figure 13. Malware distribution methods in attacks on individuals

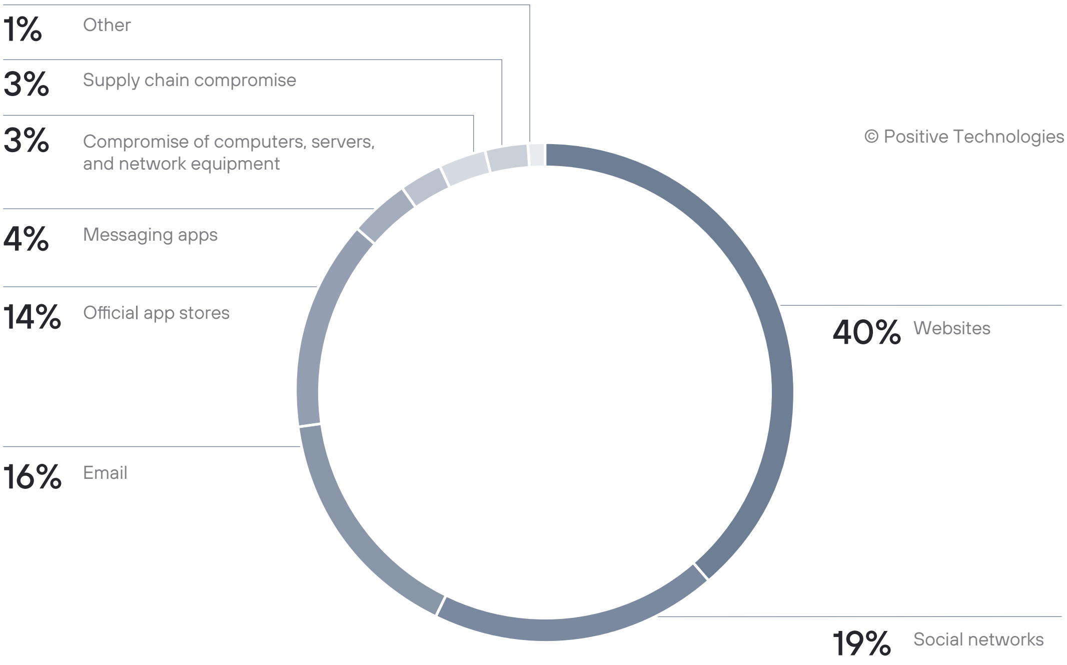
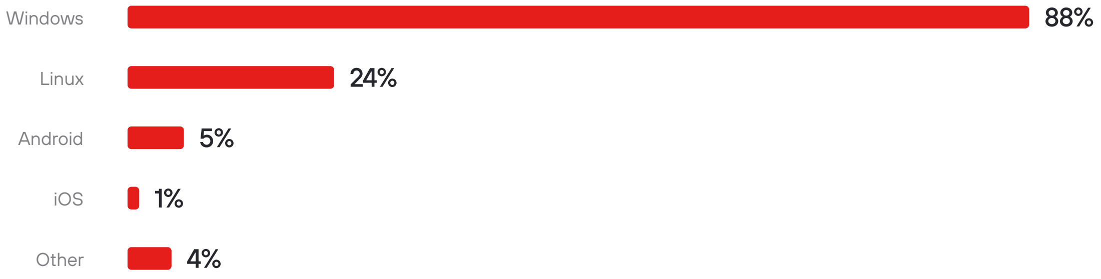


Figure 14. Target OS in malware attacks (percentage of attacks)



Distribution of cyberincidents by targets, methods, consequences, and victim categories

Victim categories

		Government	Manufacturing	Science and education	Services	IT	Healthcare	Blockchain	Finance	Trade	Other	Multiple industries	Individuals
	Total attacks	95	49	84	23	71	82	21	66	32	71	103	124
Target	Computers, servers, and network equipment	94	47	79	22	64	81	1	63	21	65	93	67
	Web resources	42	5	23	5	25	5	2	19	16	19	25	4
	People	37	23	46	10	14	39	2	16	8	18	46	112
	Mobile devices	—	—	—	—	1	—	—	—	1	—	—	19
	Other	—	1	—	—	—	—	18	—	—	2	8	2
Method	Malware use	47	35	48	14	34	64	1	23	12	39	79	78
	Social engineering	37	23	46	10	14	39	2	16	8	18	46	112
	Credential compromise	8	4	7	5	11	16	1	6	4	11	13	4
	Exploitation of vulnerabilities	27	17	18	7	36	20	2	16	19	36	49	8
	Compromise of supply chain or trusted communication channels	6	3	7	1	4	5	—	18	1	2	2	1
	Other	25	5	10	—	7	3	17	11	1	5	5	4
Consequences	Disruption of core activity	45	30	53	9	33	45	—	27	9	29	24	3
	Leak of confidential information	45	37	54	21	58	67	—	50	31	46	60	83
	Damage to national interests	7	1	—	—	—	—	—	—	—	1	—	4
	Direct financial losses	1	2	3	—	—	—	19	1	—	1	2	37
	Use of organizations' or individuals' resources to carry out attacks	4	2	3	1	13	1	2	3	2	4	13	8
	Other	—	1	1	2	1	1	—	1	1	—	6	6
	Unknown	13	1	2	2	2	6	1	4	—	9	25	7

Darker colors indicate a greater proportion of attacks within a particular industry for each victim

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

About the report

This report contains information on current global information security threats based on Positive Technologies' own expertise, investigations, and reputable sources.

We estimate that most cyberattacks are not made public due to reputational risks. As a consequence, even companies specializing in incident investigation and analysis of hacker activity are unable to calculate the precise number of threats. Our research seeks to draw the attention of companies and ordinary individuals who care about the state of information security to the key motives and methods of cyberattacks, as well as 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.