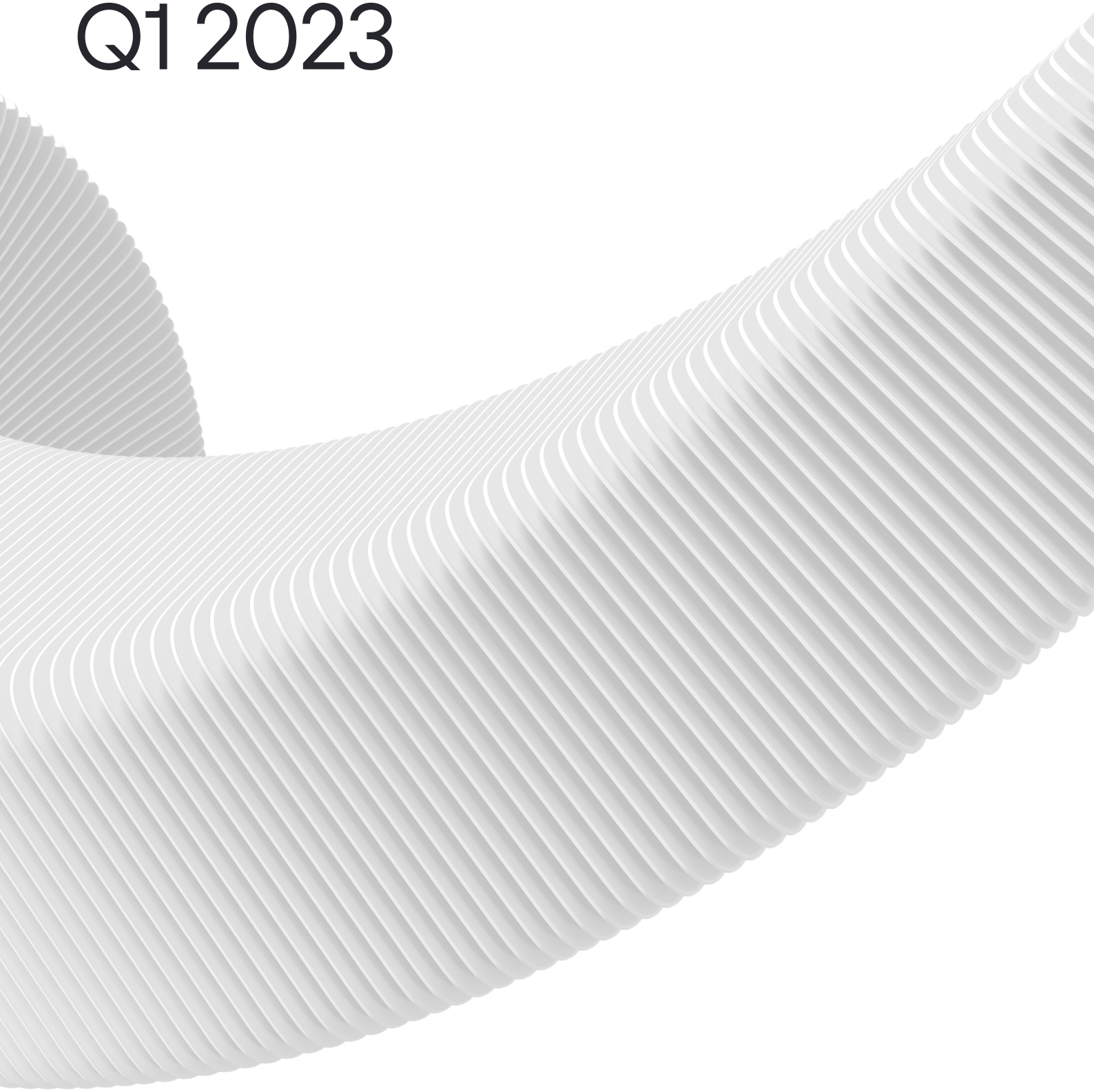
Cybersecurity threatscape: Q1 2023



Positive Technologies

ptsecurity.com

Contents

Key figures and trends

In Q1 2023, the number of incidents increased by 7% compared to the previous quarter, exceeding last year's figure for the same period by 10%. Successful cyberattacks on organizations most often resulted in leakage of confidential information (51%) and disruption of core activity (44%). Attackers used malicious software (malware) against organizations and individuals more often: the share of such incidents increased by 7 and 10 percentage points (p.p.), respectively, compared to the previous quarter. Companies and critical infrastructure objects experienced major disruptions in operation: there were large-scale data breaches, and new fraud schemes appeared.

Loaders are on the rise

The share of attacks involving loaders grew to 21% in attacks against organizations and 23% in attacks against individuals; this is respectively 2 p.p. and 8 p.p. more than in the last quarter. This increase was due to mass phishing campaigns by BlackBasta, BlackCat and Ragnar Locker ransomware operators as well as other attackers who used the Qbot and Emotet loaders as first-stage payload. Qbot and Emotet gain persistence in the system, download remote access software, collect local credentials, and only then load the ransomware. Criminals distributed Emotet by email (the most popular social engineering channel for organizations, 86%), attaching specially prepared large documents and archives (bigger than 500 MB) to messages in order to bypass antivirus protection. It is a common practice to skip scanning big files to enhance performance, and criminals take advantage of it. Hackers used the same file-enlargement technique in a campaign involving the RedLine stealer[1].

Macros[2] in files received from the Internet are blocked by default, so attackers resort to using ISO disc images and LNK files in attachments instead.

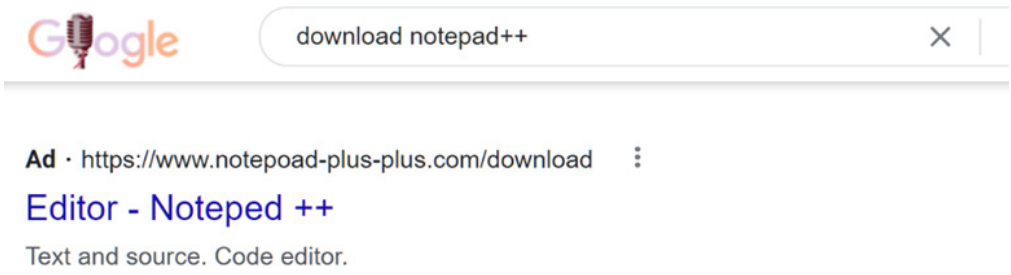
[1] A stealer is a malicious program designed to steal sensitive information such as logins, passwords, and cryptocurrency wallet data from an infected device.

[2] A macro is a small program that performs a predefined sequence of actions in an application.

SEO poisoning

We noted an increase in the amount of malicious ads in search engines (a sign of a SEO poisoning attack) during Q1 2023, which was also reported by SentinelOne specialists. The method uses SEO (search engine optimization) to put malicious domains before legitimate ones in search results. In addition, SEO poisoning can be used to attract a large number of users to websites and to facilitate ad scams.

Figure 1. Malicious advertising in Google search results



In Q1 we detected fake websites that distributed malware presented as legitimate software through the Discord and Dropbox content delivery networks. Attackers disguised the RedLine and Raccoon infostealers as popular products (such as Blender and OBS Studio). These attacks resulted in credential leaks, as well as theft of money and NFT tokens.

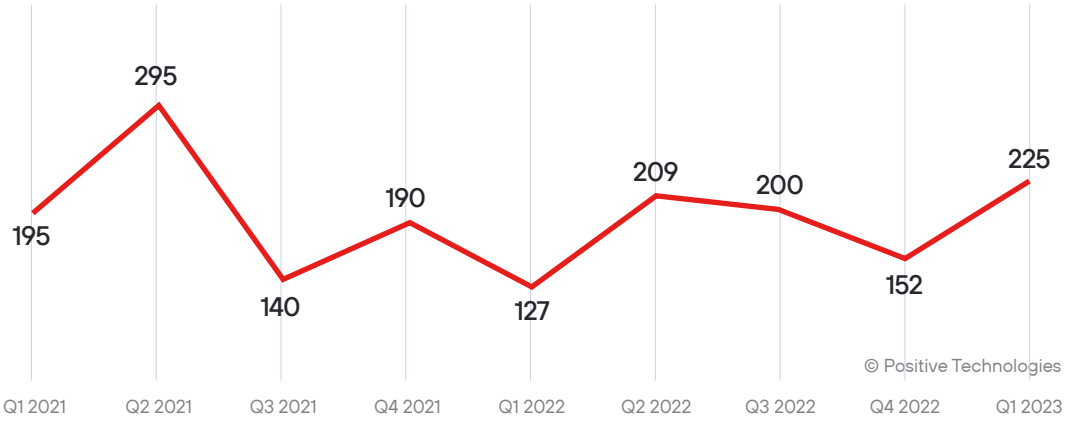
Another type of attacks involving malicious advertising is populating search results with phishing entry forms. Permiso reported such an attack on the users of Amazon Web Services.

Surge in ransomware cyberattacks

Ransomware activity significantly increased in Q1 2023: the share of ransomware in malware attacks against organizations was 53%, up 9 p.p. from the previous quarter, and the number of incidents increased by 77% compared to Q1 2022. The situation is especially grave in the science and education sector, which accounted for a large share of ransomware attacks (19%), with schools and higher education institutions around the world targeted ([1],[2]).

Ransomware operators BlackCat and HardBit got creative with their extortion tactics in Q1. BlackCat published stolen data on a website with the URL mimicking the domain of the compromised organization, so that the leak could become known to a large number of customers or partners of the victim. HardBit demanded victims to disclose details of their cyberinsurance coverage to negotiate ransom demand and secure a payment (learn more about the value of cyberinsurance information from our earlier report). The ongoing trend to develop cross-platform malware versions is continued by known ransomware operators Royal, IceFire, and Cl0P, as well as newcomer Nevada Ransomware.

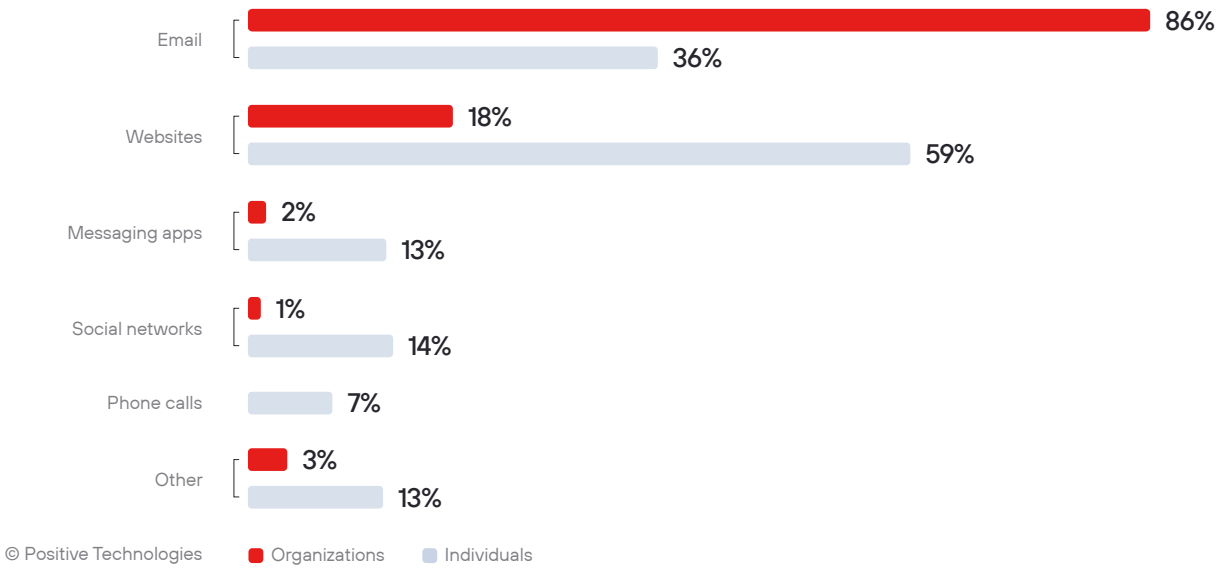
Figure 2. Number of ransomware attacks (by quarter)



QR phishing: quick and invisible

Social engineering remains one of the most popular methods of attacks on organizations (50%) and individuals (91%). Social engineering attacks on organizations are mainly performed via email (86%). As for social engineering attacks on individuals, attackers prefer to use web resources and services (59%).

Figure 3. Social engineering channels used by attackers



In Q1 we noticed an increase in the number of fraudulent job postings and phishing emails promising new benefits packages. In such campaigns, attackers send emails with malicious attachments (credential stealers) or links to phishing pages, for example, fake Microsoft 365 or Amazon Web Services login forms. In addition to emails with malicious links and attachments, attackers use QR codes to bypass anti-spam filters and other protections, as such codes are images with no suspicious links or distinctive metadata (which is why the number of such phishing campaigns may increase).

New trends in cryptocurrency scams

Fraudsters created fake crypto websites, advertised them among potential investors, called them with "unique" offers, and disappeared after receiving money. Several such call centers taken down by Europol had profits amounting to millions in cryptocurrencies. Sophos researchers reported that fraudulent applications were distributed via official stores: cryptoinvestors entered their personal data to register and then were tricked into transferring money to the accounts belonging to criminals. These applications are difficult to track, as their malicious content is not in the code but on a remote web server.

Cloud services as a foothold for phishers

The proliferation of fraud schemes forces users to be vigilant, but what if the messages or links come from reputable sources? Fraudsters place their phishing resources in the domains of cloud services (software as a service, SaaS) so as not to raise user suspicions and remain invisible to security tools. Palo Alto Networks researchers reported that the number of phishing pages hosted on cloud platforms increased more than tenfold since mid-2021. Attackers use such services as Dropbox or OneDrive to spread malware because protection tools do not always respond to files obtained from these services.

Cybercriminal arrests and dark web forum shutdowns

In Q1, law enforcement and intelligence agencies increased their efforts in fighting cybercrime. Previously, the officials tried to constrain cybercriminals mainly in the legal field, but now law enforcement agencies are going all out to stop them.

- After a lengthy operation, Dutch police announced that they seized control of the encrypted messenger Exclu popular among criminals. The police managed to read messages of the service administrators, users, and owners, performed 79 searches, and made 49 arrests.
- After a long investigation, FBI arrested Pompompurin, the administrator of the popular dark web forum Breached, after which the resource was permanently shut down. The FBI also reported to have accessed the Breached database, which could lead to more arrests.
- In January, the FBI reported about seizing the servers of the Hive ransomware gang. Monitoring the attackers' activity allowed the FBI to save the data of compromised organizations from encryption, to obtain decryption keys, and to deprive the ransomware operators of their network infrastructure and multimillion-dollar profits.

Further such actions by law enforcement agencies can affect criminal activity: dark web forums used to sell stolen data, malware, and other tools are getting shut down, which makes it more difficult for hackers to access this information, complicating cyberattacks and making them less frequent. However, in the near future criminals are likely to switch to messengers or specialized applications for communication. The wave of arrests and searches serves as a warning to attackers that are still at large, and those who have decided to enter the world of cybercrime are advised to think twice about it.

Trending vulnerabilities

According to data from the U.S. National Institute of Standards and Technology (NIST), more than 7,000 vulnerabilities were reported in Q1, a 24% increase over the same period last year. 29 new flaws were seen to be actively exploited in attacks, according to ReliaQuest. Our forecasts about old security flaws remaining widely used by attackers are becoming reality, because not all users update software in time and keep track of security patches. The following vulnerabilities were actively exploited in Q1:

- CVE-2023-23397. A serious privilege escalation flaw not requiring user interaction was identified in Microsoft Outlook and exploited in real attacks. Attackers can exploit this vulnerability on a user's computer by sending an email. After the victim receives a malicious email, a request to the criminals' SMB server[3] is initiated on the victim's device. The request contains an NTLMv2 hash that can be intercepted and used to log in to other systems or to recover a password.
- CVE-2023-0669. A zero-day vulnerability found in the GoAnywhere MFT solution. The vulnerability is related to insecure data deserialization[4] and allows attackers to execute arbitrary code. Security researchers identified over 1,000 vulnerable instances of GoAnywhere around the world, and the Cl0P ransomware gang compromised over 100 organizations.
- CVE-2021-21974. In February, attackers successfully exploited a long-known and patched vulnerability in VMware ESXi servers that allows hackers to remotely execute commands via OpenSLP. The flaw was detected on 19,000 servers around the world and successfully exploited by known ransomware gangs and a new ESXiArgs ransomware group.
- CVE-2022-41080 and CVE-2022-41082. In September, the ProxyNotShell exploit for Microsoft Exchange Server was used in attacks, and in November the vulnerabilities were fixed by Microsoft. In Q1, however, attackers found another way[5] to exploit these vulnerabilities through server-side request forgery (SSRF) in Outlook Web Access (OWA): Cuba and Play ransomware groups were among the first to use the new method.

[3] SMB server is used to exchange data via the SMB protocol in a local or global network, and to share printers and other devices.

[4] Deserialization is the process of reconstructing data structures or objects from a series of bytes or a string.

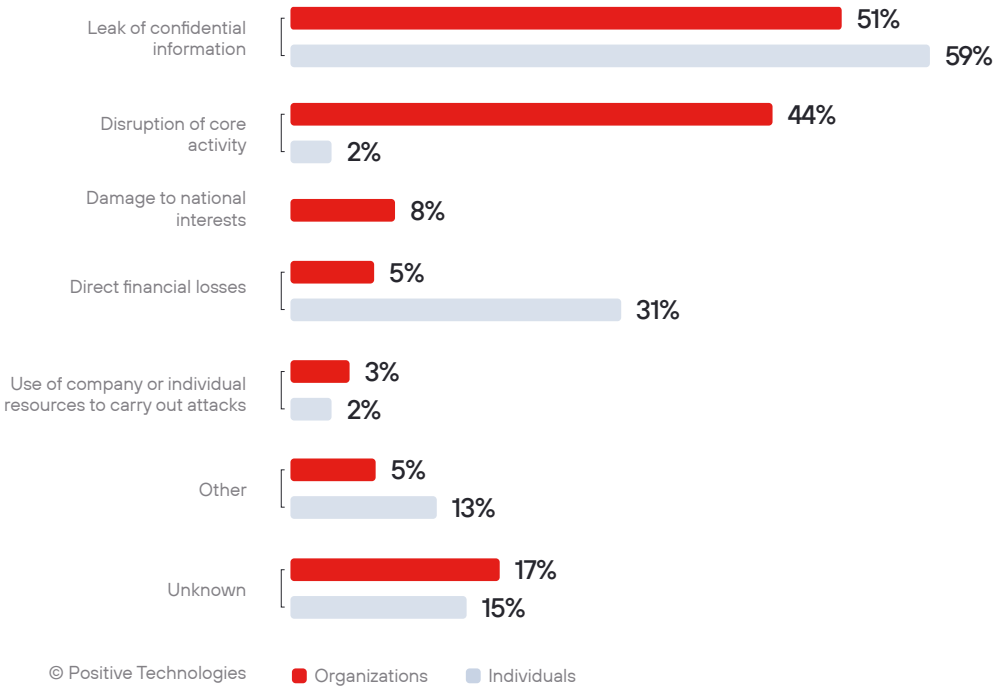
[5] The method was called OWASSRF because of the SSRF vulnerability in OWA.

To protect from cyberattacks, we recommend following our recommendations for personal and corporate cybersecurity. Considering the types of incidents we have seen in Q1 2023, we strongly recommend that you treat incoming emails and messages from social networks and instant messengers with caution: check the sender and don't click on any suspicious links to avoid becoming a victim of social engineering or having your device compromised by malware. Download applications only from trusted sources, use file backup solutions, and install security updates in a timely manner. In addition, we advise to thoroughly investigate all major incidents to identify points of compromise and vulnerabilities exploited by attackers and to swiftly shut any backdoors that the criminals may have left. You can strengthen security at the corporate perimeter with the aid of cutting-edge security tools, such as web application firewalls (WAF). To protect your devices from infection, we recommend using sandboxes to analyze the behavior of files in a virtual environment and detect malicious activity.

Attack consequences

In Q1, cybercriminals successfully attacked small businesses and industry giants, as well as critical information infrastructure. Most attacks aimed to disrupt operations and steal confidential information. There were also cases of significant financial losses: a ransomware attack on MKS Instruments seriously disrupted its supply chain operations, and the recovery process was difficult. The attack resulted in a $200M hit to the company revenue. Information security incidents can also affect a company's stock price: following a ransomware attack, DISH Network's market value slumped almost 7%.

Figure 4. Attack consequences (percentage of attacks)



The top five attacks in Q1 that had negative impact and wider repercussions

- Royal Mail, the UK's national postal service provider and a critical infrastructure organization, was hit by an attack involving the LockBit ransomware, which caused severe disruption of all overseas deliveries.
- ION Group, a developer of software for financial institutions, banks, and stock exchanges, was hit by a ransomware that affected at least 42 of ION's clients, including brokerage companies, hedge funds, and some of the world's biggest banks.
- A ransomware attack on the cities of Oakland and Modesto (U.S.) forced them to shut down government services and resort to "old-school policing", including the use of pens, paper, and walkie-talkies during patrols.
- A satellite television and internet provider Dish Network and some of its subsidiaries suffered a ransomware attack causing a multi-day outage of the company's websites, networks, and services.

- A ransomware attack hit Ross Memorial Hospital (Canada) disabling critical diagnostic systems and access to medical files. The hospital declared, "Code Gray" which means a loss of a functionality resulting in the potential loss of use of the hospital facilities.

High-profile data breaches were also an issue in Q1. In such attacks, criminals most often targeted personal data (36%) and intellectual property (14%).

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

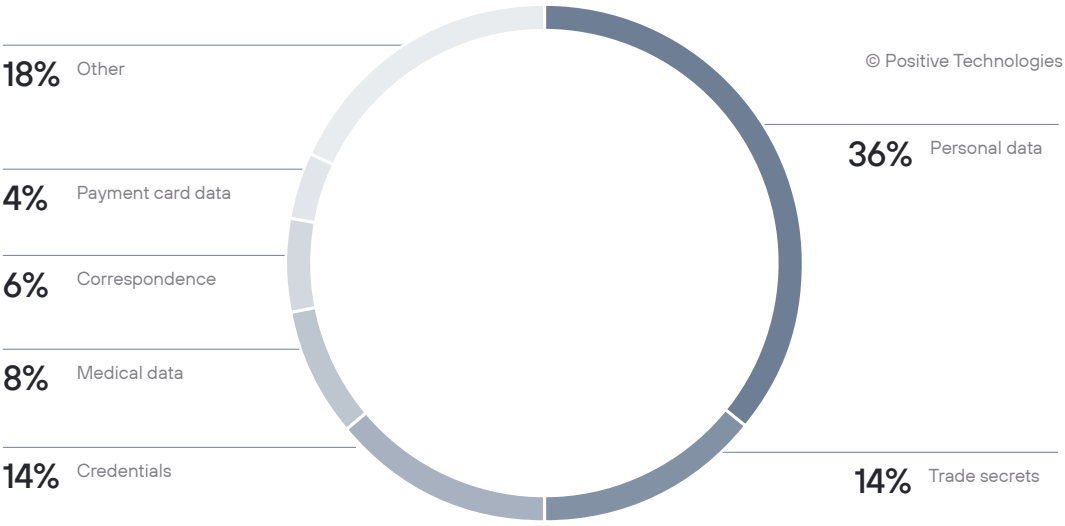
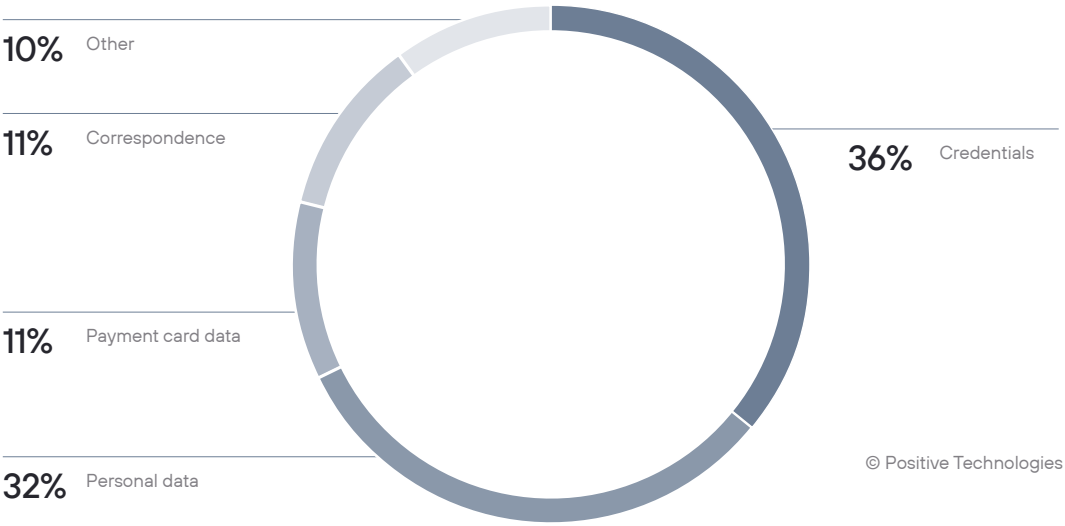


Figure 6. Types of data stolen (in attacks on individuals)



The most notable data breaches in Q1

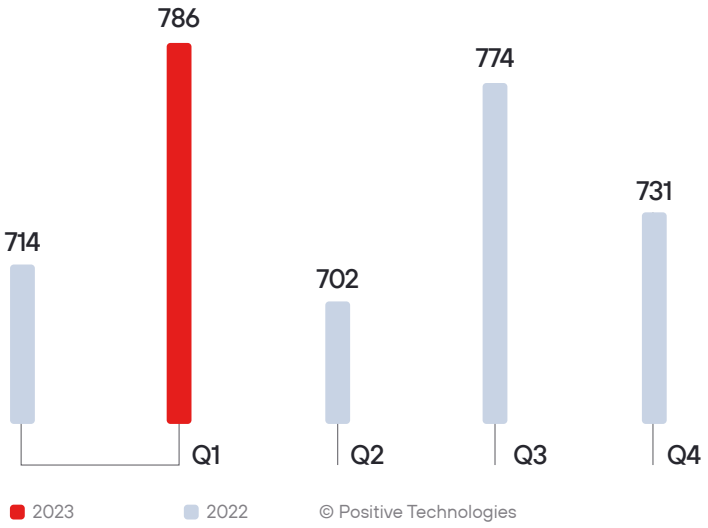
- Unknown hackers attacked data center operators GDS Holdings and ST Telemedia and got hold of login credentials for Asian data centers. These operators serve some of the world's biggest companies, such as AG, Amazon, BMW, Huawei, and Walmart. Hackers posted the stolen confidential information for sale on the dark web for $175,000.
- Customer data belonging to HDB Financial Services, a subsidiary of India's largest private bank, HDFC Bank, were posted on the hacker forum Breached[6]. The stolen data included customers' personal information, such as full names, dates and places of birth, employment information, and credit scores, as well as some employee information. The stolen sensitive data was almost immediately used in phishing attacks.
- The BlackCat ransomware group stole 2 TB of confidential military data from Solar Industries India, a major industrial explosives manufacturer. The leaked data included engineering specifications, drawings, details of armament supply chains, documents on government cooperation, and even records from production cameras. The breach drew considerable attention from the government and the defense ministry of India.
- After criminals put up the data stolen from Taiwanese computer giant Acer for sale on a hacking forum, the company confirmed that it suffered a data breach. The data contained technical manuals, server infrastructure information, BIOS images, product documentation, and replacement digital product keys.
- The LockBit ransomware group claimed responsibility for compromising the systems of SpaceX's tech contractor Maximum Industries and stealing over 3,000 technical drawings. The hackers announced that they would auction the drawings if the company does not pay a ransom.

[6] At the time of publication of this report, the forum was closed, with its owner arrested.

Statistics

68%
of attacks were targeted

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



16%
of attacks were aimed at individuals

Figure 8. Categories of victim organizations

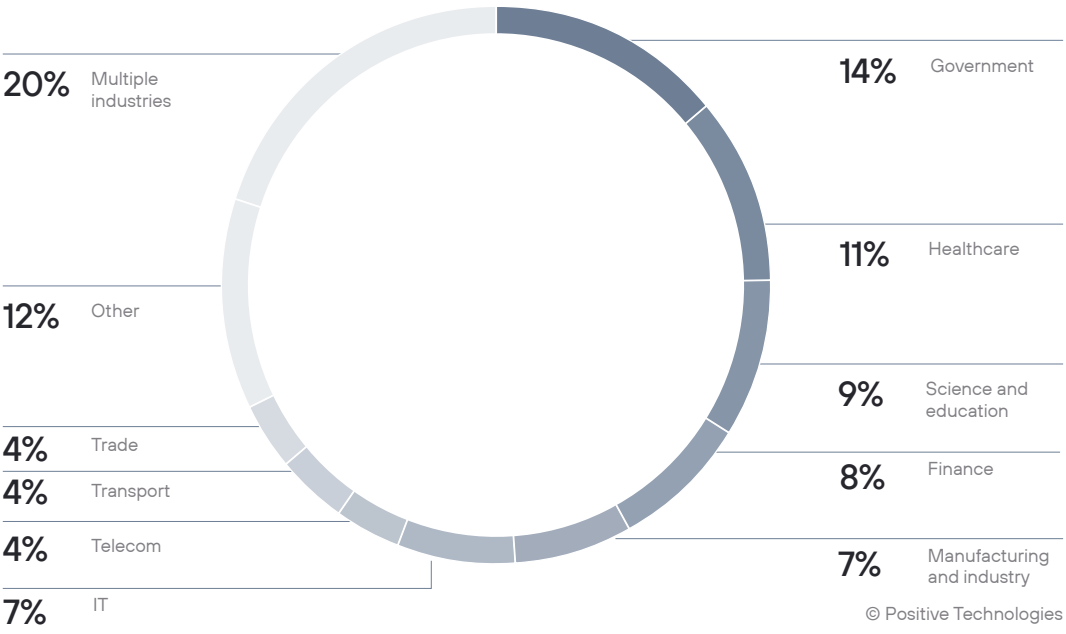


Figure 9. Attack targets (share of attacks)

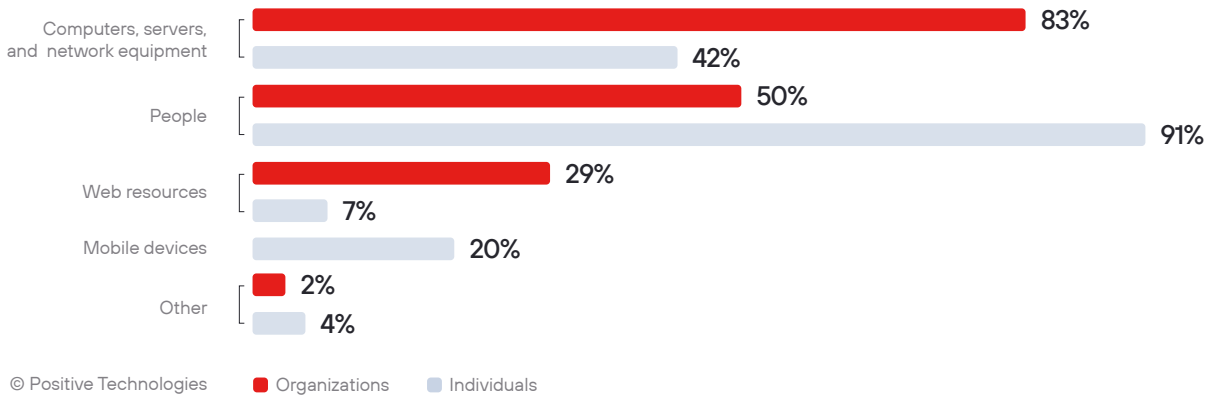


Figure 10. Attack methods (share of attacks)

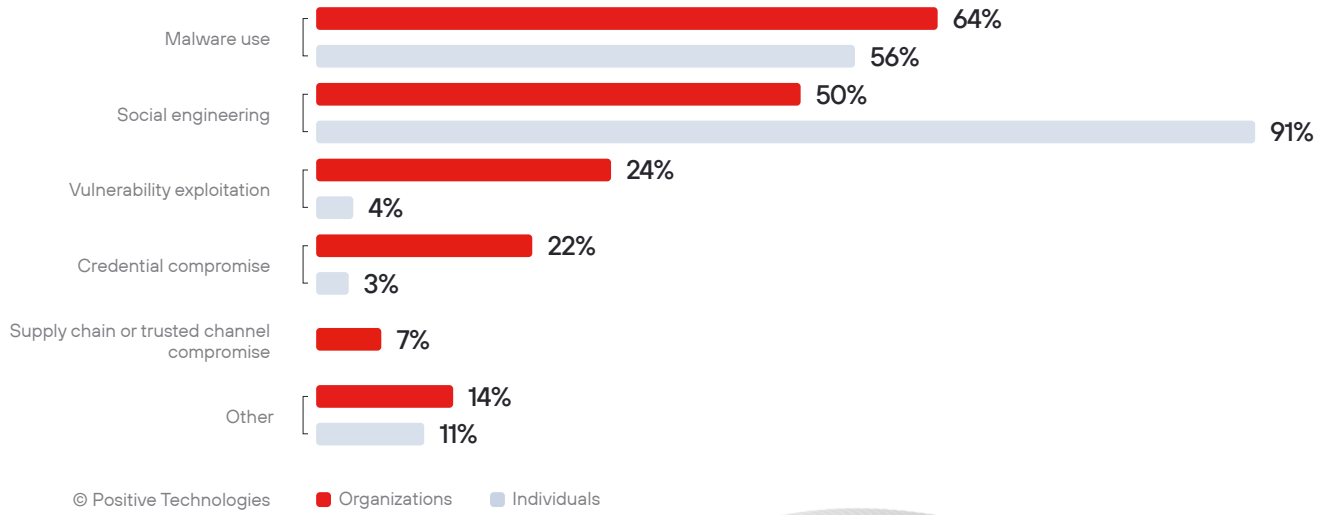


Figure 11. Types of malware (share of malware attacks)

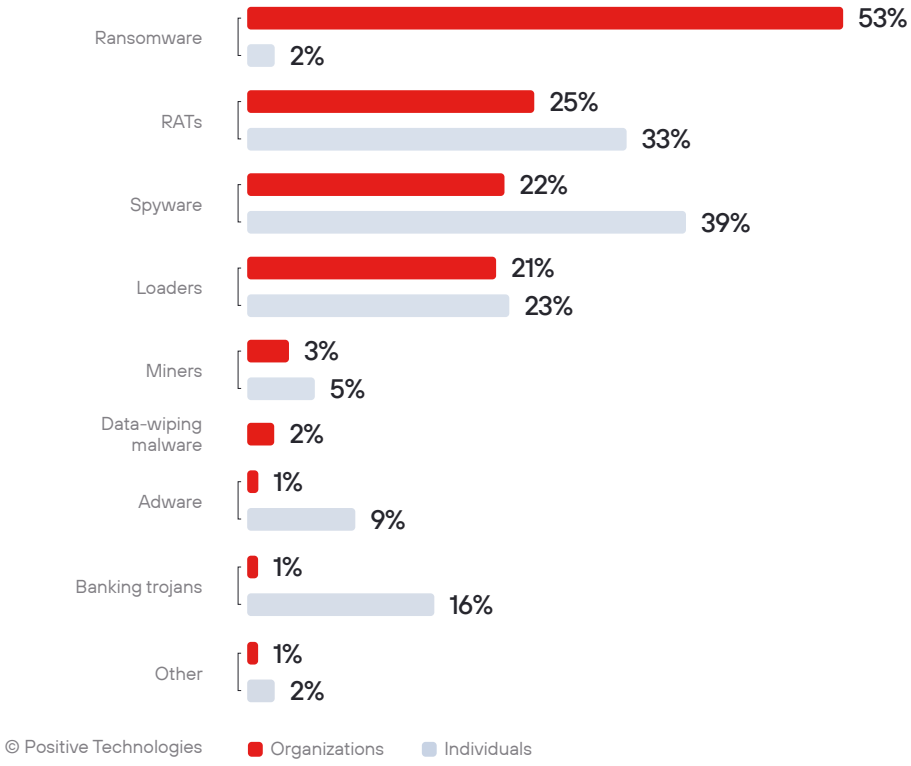


Figure 12. Malware distribution methods in attacks on organizations

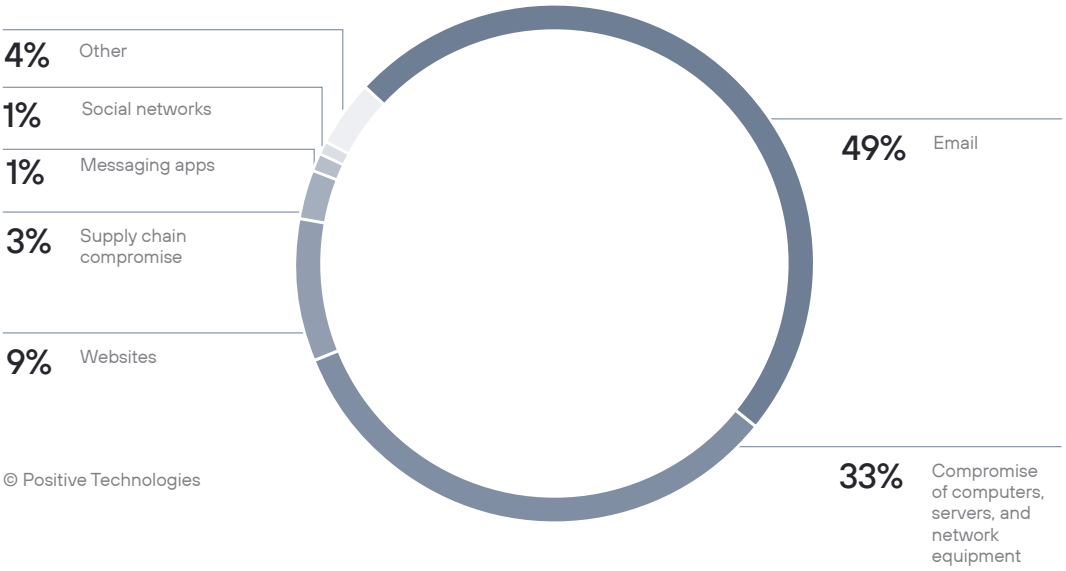


Figure 13. Malware distribution methods in attacks on individuals

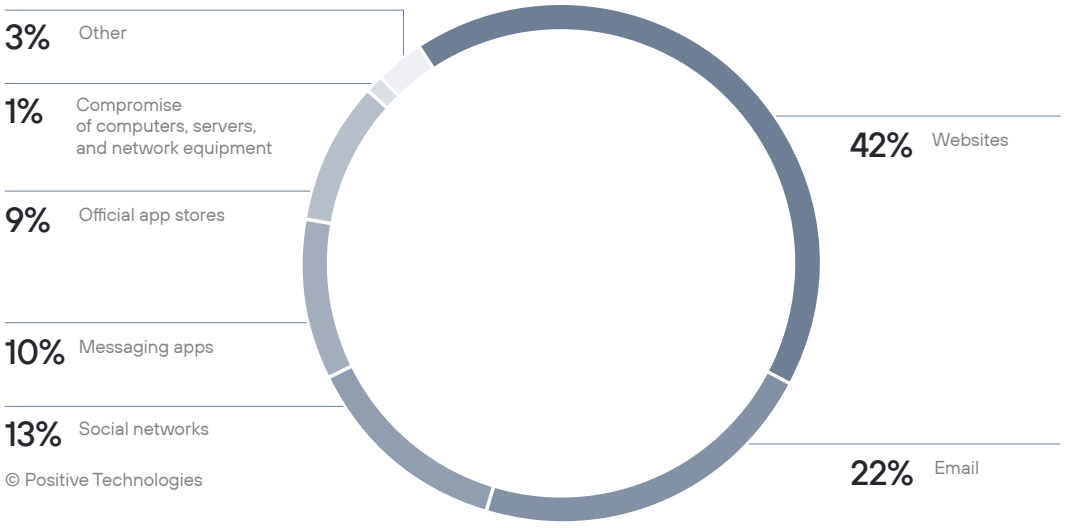
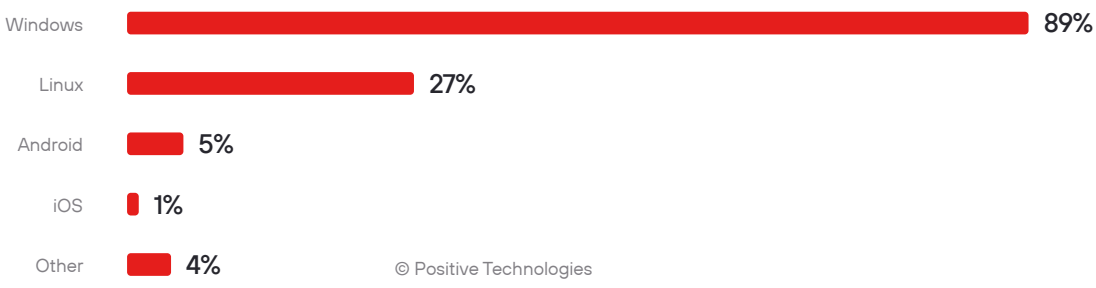


Figure 14. Target OS in malware attacks (share of malware attacks)



Victim categories

	Distribution of cyberincidents by metrics (attack targets, methods, consequences) and victim categories	Government	Healthcare	Science and education	Finance	Manufacturing and industry	IT	Telecom	Transport	Trade	Other	Multiple industries	Individuals
	Total attacks	92	70	59	50	49	47	29	24	23	80	133	130
Target	Computers, servers, and network equipment	81	52	54	45	45	36	25	23	14	50	118	55
	Web resources	37	27	9	22	5	20	13	15	8	27	10	9
	People	43	42	41	17	31	19	5	1	6	43	78	118
	Other	—	—	—	—	—	—	—	—	—	5	5	5
Method	Malware use	55	42	50	27	40	18	11	5	17	43	111	73
	Social engineering	43	42	41	17	31	19	5	1	6	43	78	118
	Compromise of credentials	18	27	18	8	13	22	4	4	3	14	14	4
	Vulnerability exploitation	18	10	5	6	12	15	10	1	9	22	50	5
	Compromise of supply chain	1	1	—	8	1	1	5	3	4	4	15	—
	Other	22	9	5	16	—	—	9	15	2	8	4	14
Consequences	Disruption of core activity	47	36	46	31	32	11	19	18	8	22	20	3
	Confidential data leak	40	45	37	17	32	37	16	9	15	44	42	77
	Damage to national interests	42	—	—	—	4	1	3	1	—	1	1	—
	Direct financial losses	3	1	—	3	5	1	4	—	3	15	1	40
	Use of company or individual resources to carry out attacks	1	—	—	1	—	6	1	—	1	5	5	3
	Other	4	1	—	3	2	2	2	—	—	2	17	17
	Unknown	20	4	4	8	3	3	—	—	4	12	55	19

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 quantify the precise number of threats. Our research seeks to draw the attention of companies and 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