Cybersecurity threatscape: Year 2021 in review

Positive Technologies

ptsecurity.com

Contents

Executive summary

Year 2021 in review:

- Among all sectors of the economy, state institutions and medical organizations were attacked most often.
- The prevailing motive of cybercriminals was to obtain data. They stole huge amounts of information. To achieve this goal, in 2021 cybercriminals began to attack data storage systems more often.
- Hacking flourished, as more and more cybercriminals sought to exploit vulnerabilities in software. This method was used in one in three attacks on organizations.
- There was a sharp increase in the number of botnets. Attackers used them to carry out DDoS attacks and mine cryptocurrencies.
- Ransomware remained the most popular malware, used in 60 percent of attacks on companies involving malware.
- In 2021, the world faced an abundance of dangerous vulnerabilities that attackers tried to exploit. We compiled a list of trending vulnerabilities. If you find them in the company's infrastructure, install security updates as soon as possible.
- Ransomware operators targeted virtualization systems. The new term "ransomcloud" appeared in the IT world, which denotes ransomware targeting cloud storage.
- More and more malware developers are targeting Linux-based devices. According to CrowdStrike, the growth of malware targeting Linux amounted to 35 percent.
- Cryptocurrency regained its popularity, causing cybercriminals to turn their attention to cryptocurrency exchanges. Financial losses due to attacks amounted to hundreds of millions of dollars.
- The number of attacks on individuals remained at a high level, mostly they were victims of social engineering. We shared our predictions about which social engineering topics would be popular among criminals.

All these trends will be relevant in 2022. We also note that the damage from cyberattacks is rapidly increasing every year, and their consequences are increasingly going beyond the victim company and affecting entire industries. Therefore, it is now more important than ever to follow the principles of result-oriented cybersecurity.

Introduction

The number of attacks in 2021 increased by only 6.5 percent compared to 2020. In our opinion, this is because the world finally adapted to the new working conditions amid the coronavirus pandemic, and attacks on large companies motivated top managers to pay more attention to cybersecurity issues. The share of targeted attacks increased by 4 percentage points in comparison with 2020 and amounted to 74 percent of all attacks.

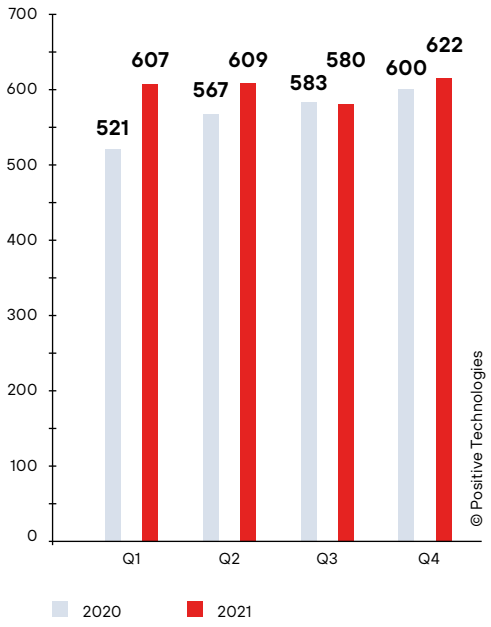

Figure 1. Number of attacks in 2020 and 2021 (per quarter)

We identified trends that appeared or became consolidated in the past year, and also shared forecasts and recommendations on how to protect yourself and your business from current cyberthreats. Before moving on to trends, let us remember the landmark events of 2021.

THE BIGGEST ATTACKS OF **2021**

FEBRUARY

ATFS payment processor in the U.S.

→ Provides services for automatic transfer of funds

- Cuba ransomware attack
- Theft of data about clients' bank accounts and cash flow

MARCH

IoT solution provider Sierra Wireless

- Ransomware attack
- Shutdown of equipment production
- The company withdraws its financial forecast for Q1

CNA insurance company

→ One of the largest insurance companies in the U.S.

- Phoenix Locker ransomware attack
- Theft of personal data of employees and clients
- The company pays a $40 million ransom

APRIL

Equipment manufacturer Quanta Computer

- REvil ransomware attack
- Theft of blueprints and information about unannounced Apple devices

MAY

Meat producer JBS Foods

→ The world's largest meat supplier

- REvil ransomware attack
- Seven beef production plants in the U.S. and Canada temporarily closed
- Food supply disruptions

Pipeline operator Colonial Pipeline

→ The largest U.S. pipeline

- Darkside ransomware attack
- Fuel supplies disrupted
- Fuel supply disruptions throughout the U.S.
- A state of emergency introduced in a number of states

JULY

IT company Kaseya

→ Manufacturer of software used by more than 40,000 companies worldwide

- REvil ransomware attack
- The attack affects 1,500 client companies worldwide, which also suffer from ransomware attacks

AUGUST

Poly Network cryptocurrency exchange

- Cybercriminals exploit a smart contract vulnerability
- More than $600 million stolen

Telecom company T-Mobile

- Theft of personal data of more than 50 million clients

Memorial Health System in the U.S.

- Hive ransomware attack
- Disclosure of medical information about more than 200,000 patients, hospital appointments canceled

SEPTEMBER

IT company Yandex

- The largest DDoS attack (20 million requests per second) using the Mēris botnet

OCTOBER

Government of Argentina

- Identity card data of 45 million Argentine citizens stolen and posted on the dark web

Streaming platform Twitch

- More than 100 GB of data stolen, including information about payments to streamers and the proprietary code of the platform

Pichincha Bank in Ecuador

→ Ecuador's largest private bank

- A ransomware attackcrashes banking applications and ATMs
- It takes more than three days to restore the systems

NOVEMBER

Iranian state system for regulating the sale of gasoline

- Disruption of 4,000 gas stations across the country

State and medical institutions in the crosshairs

As in 2020, 86 percent of all attacks were aimed at organizations. In 2021, there were minor changes in the ranking of the most frequently attacked industries. For example, the number of attacks on state institutions decreased by 10 percent, yet they continued to top the chart. In 2020, IT companies ranked seventh by number of attacks, and a year later they climbed two positions. Medical institutions rose from third place to second.

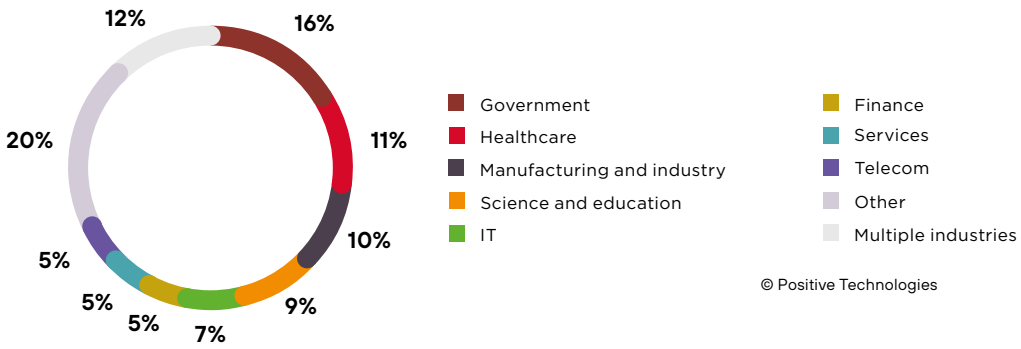

Figure 2. Victim categories among organizations

Considering the complicated geopolitical situation, we predict an increase in the number of attacks, so we recommend that companies switch from standard information security processes to the principles of result-oriented security. The main focus should be on ensuring cyberresilience. Any organization can become a victim of a cyberattack, regardless of industry specifics, but the consequences will directly depend on what measures have been taken to prevent negative events.

Victim categories

	Pre-industry classification of cyberincidents by motive, method, target and victim categories	Government	Finance	Manufacturing and industry	Healthcare	Services	IT	Science and education	Telecom	Individuals	Other	Multiple industries
	Attacks, total	**322**	**113**	**209**	**227**	**103**	**150**	**177**	**94**	**349**	**420**	**254**
Targets	Computers, servers, and network equipment	248	71	183	192	89	134	144	86	130	284	202
	Web resources	75	27	10	15	14	16	20	23	19	114	28
	People	165	68	116	154	61	50	108	34	308	164	109
	Mobile devices	3		1						84	2	5
	IoT						2			3		9
	Other		2	2			2	4	1		28	7
Method	Malware use	199	51	160	147	71	89	116	66	201	223	177
	Social engineering	165	68	116	154	61	50	108	34	308	164	109
	Credential compromise	10	3	10	5	3	4	8	2	12	23	12
	Hacking	85	17	78	56	29	81	43	19	23	136	113
	Web attacks	51	8	5	10	13	7	16	18	7	80	21
	Other	20	21	2	1	1	10	2	13	4	31	20
Motive	Financial profit	131	41	107	129	60	60	95	39	95	196	79
	Access to data	194	70	138	154	71	95	87	55	268	274	144
	Hacktivism	37	19	12	3	6	20	27	6	18	39	11
	Unknown	13	6	4	12	2	3	4	2	8	10	10
	Cyberwar	8		3	5		5	1		5	11	1
	Use of company resources to conduct attacks	2		8		7	14	5	1	5	6	45

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

Increase in stolen data

Since 2018, the main motive of cybercriminals has been to obtain data. In 2021, two-thirds of attacks on organizations were carried out for this purpose. Cybercriminals also attacked manufacturers of data storage solutions. This trend will continue in 2022.

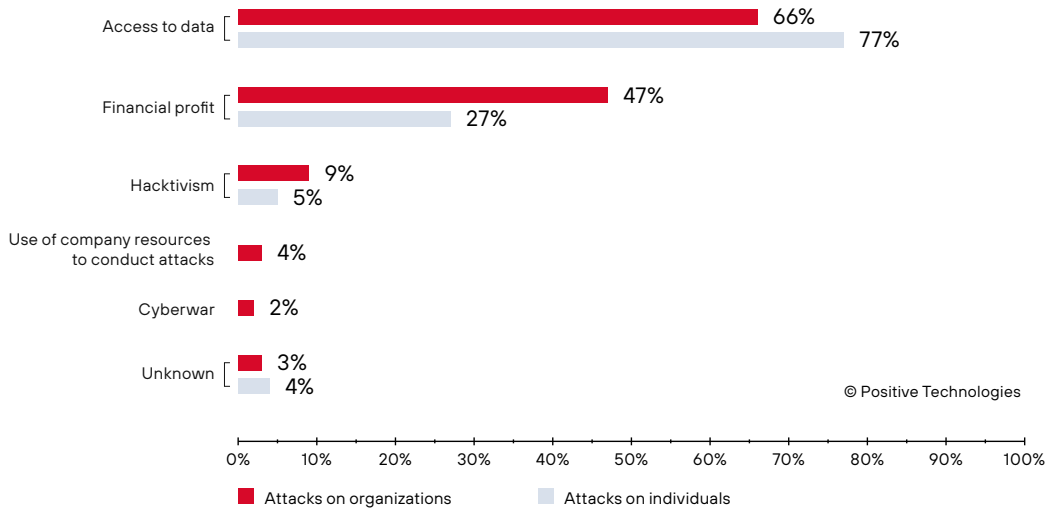

Figure 3. Attackers' motives (percentage of attacks)

> The share of attacks motivated by financial gain increased: from 37 percent in 2020 to 47 percent in 2021. This was facilitated by the abundance of ransomware distributors.

Cybercriminals mainly attacked companies, hunting for personal data, credentials, and trade secrets.

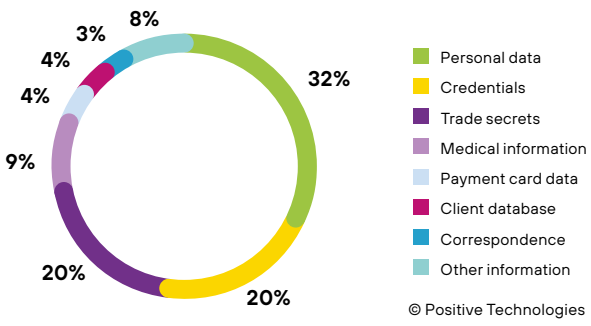

Figure 4. Types of data stolen (in attacks on organizations)

Hacking running rampant

As in 2020, the following methods of attacks were most popular: malware distribution, social engineering methods, and hacking. One in two attacks on organizations employed social engineering methods. The share of hacking (exploitation of vulnerabilities in software) increased by 8 percentage points over the year (amounting to 32 percent).

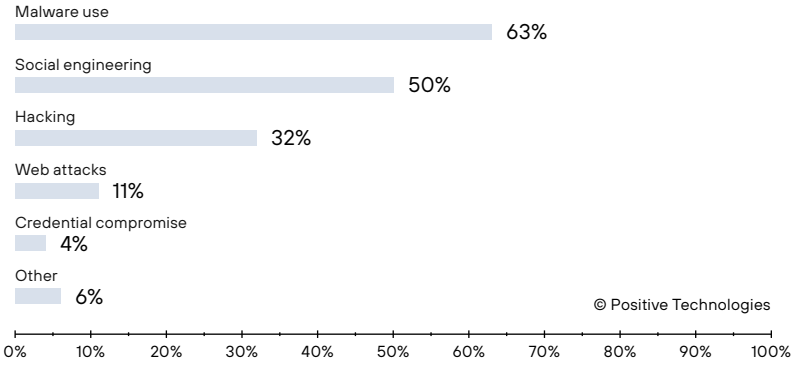

Figure 5. Methods of attacks on organizations

Roughly eight out of ten attacks on organizations affected computers, servers, and network equipment. Companies' web resources became targets of attacks in 17 percent of cases.

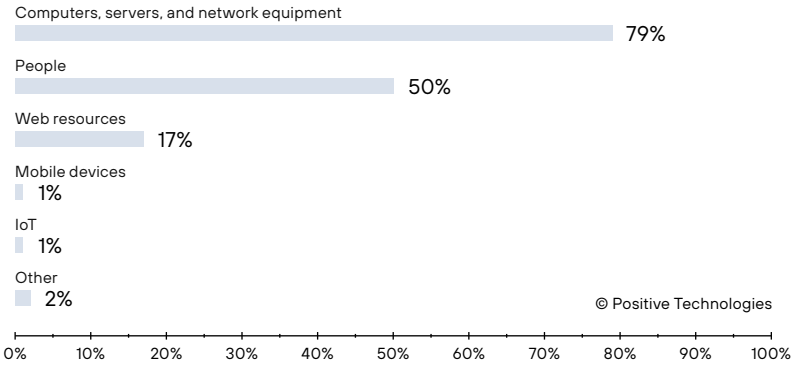

Figure 6. Targets of attacks on companies (percentage of attacks)

Malware-based attacks on companies most often involved ransomware: in six out of ten cases, according to our data, up 15 percentage points compared to 2020. Remote administration tools (RATs) were used in 27 percent of attacks involving malware and targeting organizations. Loaders ranked third among the most common malware used in attacks on companies.

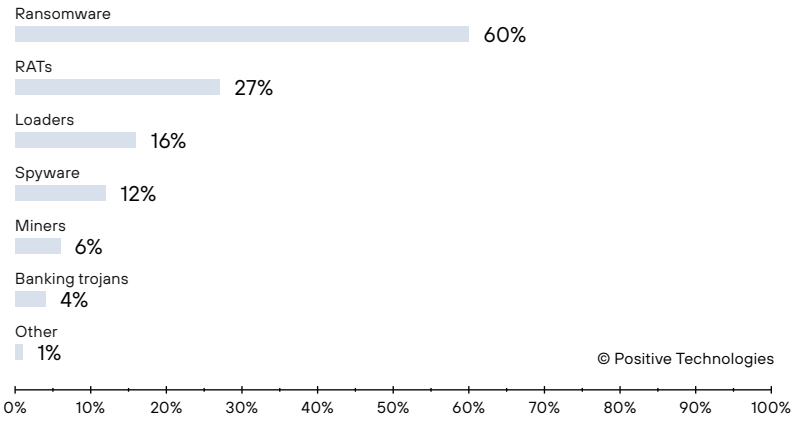

Figure 7. Types of malware in attacks on organizations (share of attacks involving malware in 2021)

Starting in Q3, we noted explosive growth in the use of RATs in attacks on organizations: compared to Q2, its share more than doubled and amounted to 36 percent. Over the year, the increase was 9 percentage points.

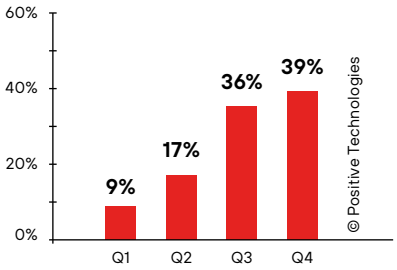

Figure 8. Increase in the share of attacks using RATs (in attacks on organizations)

The main methods of malware distribution were phishing, compromise of computers, servers, and network equipment, and hacked websites.

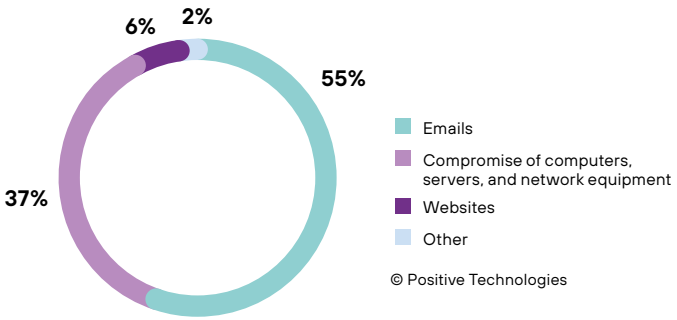

Figure 9. Methods used for malware distribution (in attacks on organizations)

Every year, we note an increase in the number of attacks using malware. Since 2018 the number of such attacks has increased by 137 percent. And we presently see no reason for a decrease in the number of attacks using malware in 2022. We strongly recommend that you focus primarily on protecting key and target assets and points of penetration into the company's internal network. When building a protection system for the company, use modern security means that will not only detect an attack when it happens, but also prevent its implementation. The use of a sandbox, for example, will help identify malware before it causes irreparable damage to the company.

The rise of botnets

The boom in attacks aimed at replenishing botnets was another trend of 2021. Experts from Spamhaus also reported in Q3 a record number of new botnets, with more than 900 new instances found in September alone.

After analyzing our data, we made a list of the most active botnets of 2021:

- Mēris
- Glupteba
- Mirai (and its varieties)
- Gafgyt

Throughout 2022, the number of botnets and, consequently, DDoS attacks will increase, facilitated by vulnerabilities enabling mass attacks on multiple assets and benefits for criminals from such attacks. This is how cybercriminals can harness the computing power of the victim company to conduct DDoS attacks on other organizations or mine cryptocurrencies.

Attackers are increasing the power of their botnets by compromising poorly protected devices through mass exploitation of vulnerabilities, including on IoT devices, and successful password bruteforce attacks on Internet-accessible devices. We recommend setting secure passwords, avoiding using default accounts, and regularly installing security updates. In addition, it is advisable to monitor for processes indicating the activity of miners, and, in case of a sharp decrease in performance, conduct a full system check. These recommendations hold for both companies and individuals.

In attacks using botnets, cybercriminals may not only pursue the goal of using the company's resources to carry out attacks, but also seek financial gain. According to Check Point, in one year, attackers managed to intercept 969 transactions and steal about $500,000 using the Phorpiex botnet by substituting the addresses of cryptocurrency wallets.

Ransomware troubles

Let us summarize the episodes involving ransomware and highlight the main figures and trends that emerged in 2021:

- $50 million—the largest ransom demand.
- $40 million—the highest amount paid
- $1.85 million—the average cost of eliminating the consequences of a ransomware attack
- 60 percent—the share of ransomware among malware attacks on organizations

Industry-specific focus

In 2021, medical and government institutions, scientific and educational organizations, and industrial companies were most often victims of ransomware attacks.

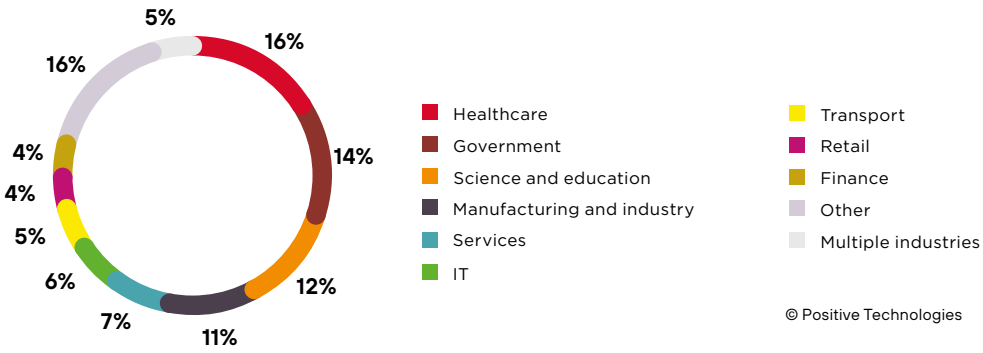

Figure 10. Ransomware attacks by industry

In 68 percent of attacks, cybercriminals distributed ransomware via email, and in 29 percent, they compromised computers, servers, and network equipment. We believe that vulnerabilities will soon become one of the main vectors for ransomware distribution. Experts from Ivanti arrived at the same conclusions. In their annual report, they stressed that ransomware distributors used about 300 known vulnerabilities to infect devices—29 percent more than in 2020.

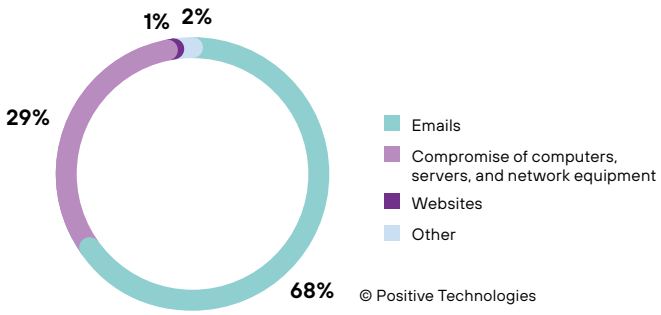

Figure 11. Methods used for ransomware distribution (in attacks on organizations)

Five most active ransomware programs in 2021:

- REvil
- Conti (Ryuk)
- Avaddon
- Clop
- PayOfGrief

> On July 13, 2021, REvil infrastructure was destroyed. In January 2022, members of the group were arrested.

New extortion tactics

In 2020, ransomware distributors threatened victims who refused to pay up with informing their customers of the attack. In 2021, cybercriminals took it a step further. They started threatening to publish the stolen data if the victim asked the police for help or hired a negotiator. This tactic had already been used by Grief and Ragnar Locker.

Updating the interaction policy within groups

Some ransomware operators abandoned the distributed system, with its multiple distributors of malware. This is because such systems are hard to manage; many of the distributors attacked companies using the same malware several times. Faced with a series of such attacks, victims refused to pay repeated ransom demands. In Q2 2021, we noted that, according to Cybereason's research, 80 percent of organizations that paid ransomware operators were attacked again; 46 percent of those attacked repeatedly believe that they suffered at the hands of the same cybercriminals as the first time. The new structure suggests that cybercriminal groups have centralized management and in-house distributors.

Cybercriminals demand more

In 2021, the ransom sums increased significantly. This was also reported by the research group Unit 42. In the first half of 2021 alone, the average sum paid to attackers amounted to $570,000, which is 82 percent more than in the whole of 2020. According to Group-IB, the average ransom that Russian companies transferred to cybercriminals amounted to 3 million rubles.

Attack consequences stretch further

The consequences of ransomware attacks in 2021 went beyond local victim companies and their customers and affected entire industries and ordinary citizens. Illustrative examples were the attacks on Colonial Pipeline and JBS.

We predict an increase in the number of ransomware attacks in 2022. In this regard, it is advisable to protect key business systems and ensure regular backups by, for example, saving copies to the cloud. Owners of cloud services, in turn, need to provide the necessary level of cyberresilience. In case of an attack, do not blindly comply with the demands or pay a ransom, because, according to statistics, cybercriminals rarely return all of the stolen data and often not all information can be restored, while the victims then suffer from new attacks.

Trending vulnerabilities

In every quarter of the year, we identified new high-profile vulnerabilities that attackers immediately tried to exploit. Among them were ProxyLogon in Microsoft Exchange Server, PrintNightmare in the Windows print manager, CVE-2021-40444 in the MSHTML module of Internet Explorer—hundreds and thousands of organizations around the world fell victim to them. In December 2021, the term **cyberpandemic** was coined to describe the abundance of attacks using the vulnerability CVE-2021-44228 in the Log4j library. In 2021, the share of hacking and web vulnerability exploitation totaled 43 percent of all methods used in attacks on organizations, which was up 8 percentage points on the previous year.

We prepared our own list of the most frequently exploited vulnerabilities of this year (see Table 1). If your infrastructure uses software in which these vulnerabilities were identified, we recommend checking whether relevant security updates have been installed.

Vulnerability identifier	Vulnerability type	CVSS base score	Vulnerable software
CVE-2021-27101	Remote Code Execution	9,8	Accellion FTA
CVE-2021-27103	Server-Side Request Forgery	9,8	
CVE-2021-27104	Remote Code Execution	9,8	
CVE-2021-27102	Remote Code Execution	7,8	
CVE-2021-26855 (ProxyLogon)	Server-Side Request Forgery	9,8	Microsoft Exchange Server
CVE-2021-26857, CVE-2021-26858, CVE-2021-27065 (ProxyLogon)	Remote Code Execution	7,8	
CVE-2021-44228	Remote Code Execution	10,0	Apache Log4j2 library
CVE-2021-28799	Remote Code Execution	9,8	QNAP NAS
CVE-2021-34527 (PrintNightmare)	Remote Code Execution	8,8	Windows print manager
CVE-2021-34473 (ProxyShell)	Remote Code Execution	9,8	Microsoft Exchange Server
CVE-2021-34523 (ProxyShell)	Privilege Escalation	9,8	
CVE-2021-31207 (ProxyShell)	Authentication Bypass	7,2	
CVE-2021-40444	Remote Code Execution	7,8	MSHTML module of Internet Explorer
CVE-2021-21972 (discovered by Positive Technologies expert Mikhail Klyuchnikov)	Remote Code Execution	9,8	VMware

Table 1. Popular vulnerabilities published in 2021

We believe that the upward trend in the number of attacks using known vulnerabilities will continue in 2022. This is mainly because in many companies the vulnerability management process is not carried out efficiently; companies do not install security updates in a timely manner. Cybercriminals act very quickly, especially when a publicly available exploit appears online. According to our data, it takes an average of 24 hours to create an exploit. For example, for the vulnerability in the Log4j library, more than 60 public exploits appeared within a few days.

We strongly recommend you to pay attention to how the vulnerability management process is organized in your company. The main problem faced by information security specialists is the prioritization of vulnerabilities for elimination. At the end of 2021, we published our recommendations for solving this problem.

Targeting Linux

In Q2 2021, we noted that the trend toward targeting software for Linux had finally consolidated. Trend Micro reported more than 13 million attempted malware attacks on this OS in the first half of 2021. According to CrowdStrike, in 2021 the increase in Linux-oriented malware was 35 percent.

Such an interest in Linux was expected, since it is a widely used OS: according to the Censys search engine, there are about 14 million Linux-based devices available on the Internet. However, Linux security issues were given much less attention than Windows ones.

We observed the emergence of Linux versions of ransomware, banking trojans, miners, and RATs. Similar statistics were presented in the Trend Micro report.

Here are the most interesting examples of how criminals attacked Linux-based devices:

- They grouped devices with this OS into botnets for cryptocurrency mining, distributing such malware as DreamBus and HolesWarm, used the resources of companies infected with FreakOut, Gafgyt, or Mirai to carry out DDoS attacks on other organizations.
- Attacked supercomputers, infecting them with the Kobalos trojan and stealing credentials for SSH connection.
- Distributed ransomware, such as Pysa and TellYouThePass.
- Stole money using the CronRAT banking trojan and the remote administration tool linux_avp.
- For the first time, used the infrastructure-as-code (IaC) tools to deliver malware, for example, Ansible, Salt Stack, and Chef.
- Developed malicious libraries and distributed them among software vendors, imitating, for example, the popular NPM packets Browserify and UA-Parser-JS.

APT groups, such as TeamTNT (including as part of the Chimaera campaign) and Winnti also wanted a slice of the juicy Linux pie. Find out more about other examples of malware in our Q2, Q3, and Q4 2021 reports.

Linux is becoming an increasingly popular and high-demand system year after year, for which reason we believe that attackers will continue to invest resources in the development of Linux-targeted malware. If this OS is used in your infrastructure, scan it for malicious activity, check files in a sandbox before they are launched in the system, and install security updates in a timely manner.

Virtualization environments and orchestrators at risk

One of the trends of the past year was attacks on virtualization environments and platforms for managing container clusters. Malware developers are actively adjusting their products for attacks on virtual infrastructure. Ransomware operators paid special interest to virtualization environments. Groups distributing ransomware actively exploited vulnerabilities. For example, RansomExx, Darkside, and Babuk Locker exploited vulnerabilities to send malicious SLP requests to VMware ESXi devices and thus gain control over them.

> If VMware ESXi is in your infrastructure, we recommend installing security updates for these vulnerabilities or disabling SLP support altogether to prevent attacks (if support for this protocol is not required).

Another method that grew in popularity in 2021 was the use of a virtualization environment to avoid detection by information security tools. This technique is very effective, because a virtual machine can have access to computer files and directories through shared folders, which allows the ransomware hosted on the virtual machine to encrypt files on the computer. This method was used, for example, by such groups as Ragnar Locker and Conti.

To protect against such attacks, monitor the lists of software deployed on virtual machines. This can be done using special inventory tools. Also, limit the ability to create new unauthorized virtual machines.

Throughout 2021, we noted the interest of malware developers in the Kubernetes orchestration tool. The Hildegard trojan, Siloscape backdoor, Kaiten botnet, and XMRig Monero miner are designed for such environment. Cloud storage also became one of the favorite targets for attacks, and a new term was coined in the IT world—ransomcloud—collectively referring to ransomware targeting cloud storage.

The rise of cryptocurrency attracts criminals

Cryptocurrency again hit peak popularity. Attackers who closely follow the trends also paid special attention to it. Our data shows that the number of attacks on cryptocurrency exchanges increased by 44 percent compared to 2020. According to analysts at Chainalysis, in 2021 cybercriminals stole a total of $14 billion.

Five largest attacks on cryptocurrency exchanges (by amount stolen):

1. PolyNetwork: about $600 million stolen. Despite the fact that the attackers returned $260 million, this attack remains one of the largest cryptocurrency thefts in history.
2. Cream Finance: $130 million stolen; attacked three times in 2021.
3. Badger: $120 million stolen.
4. Liquid: $94 million stolen.
5. EasyFi: $81 million stolen.

Cybercriminals exploited vulnerabilities in interaction protocols. Another method that is gaining popularity is the exploitation of web vulnerabilities on websites of cryptocurrency platforms.

The number of attacks related to the theft of cryptocurrencies, both from individuals and from cryptocurrency exchanges, will continue to grow in 2022. This is because just one successful hacking attempt can fully recoup all the attack costs and complexities. The main reason for successful attacks and theft of money is vulnerabilities in protocols and platforms. Therefore, we recommend taking preventive measures to detect vulnerabilities, for example, by implementing a bug bounty program. We advise individuals to be careful: do not enter your cryptocurrency wallet credentials on third-party resources, and always double-check information about all cryptocurrency offers online. Use strong passwords to access your wallet. To facilitate this process, use a password manager, where you can also set a change password reminder.

Also, we do not rule out an increase in the number of attacks related to blockchain technologies, such as hacking of smart contracts and fraud with NFTs.

Rising attacks on individuals: what to expect from 2022

Attacks on individuals amount to 14 percent of all the attacks we registered in the past year.

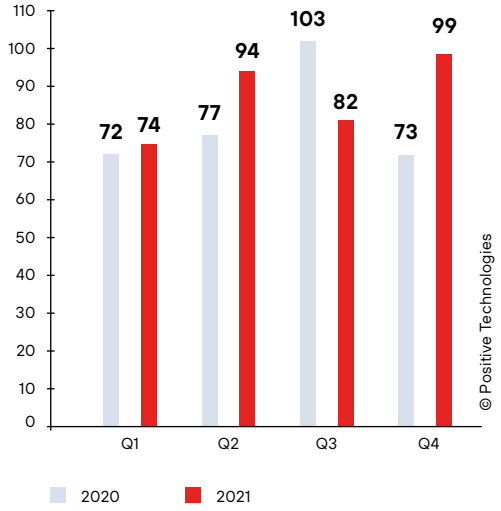

Figure 12. Number of attacks on individuals in 2020 and 2021

In such attacks, cybercriminals' main objectives are data theft (77% in 2021) and financial gain (27%). Credentials constituted almost half of the stolen information (46%). A fifth of the stolen information was personal data.

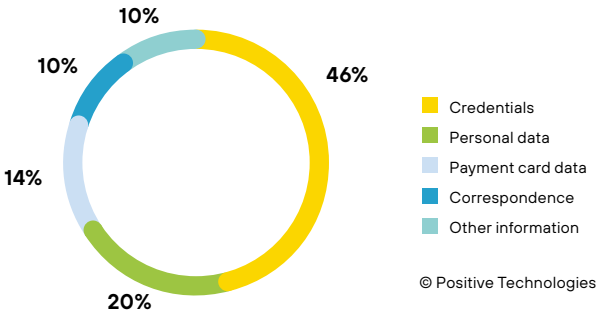

Figure 13. Types of data stolen (in attacks on individuals)

Computers and network equipment of individuals were the targets of attacks in 37 percent of cases, while one in four attacks targeted mobile devices.

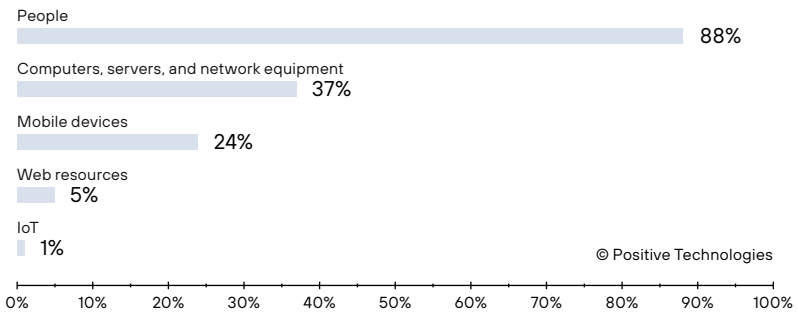

Figure 14. Targets of attacks on individuals (percentage of attacks)

In 88 percent of attacks, cybercriminals used social engineering. Through social engineering, attackers try to exploit current topics and socially significant events. Popular phishing topics in 2021 included the COVID-19 pandemic, movie and TV premieres, investments, and corporate mailings.

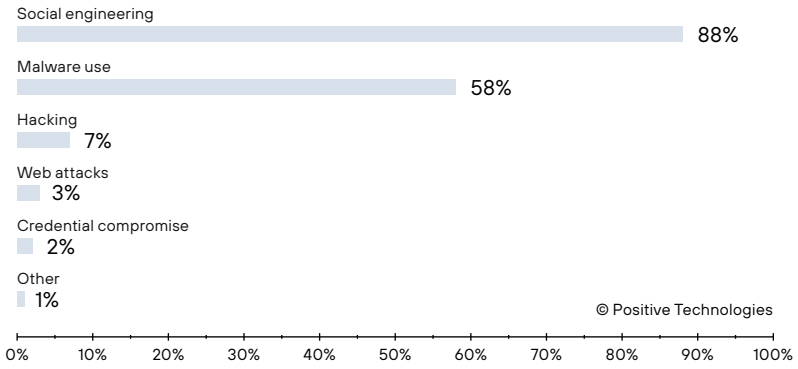

Figure 15. Methods of attack on individuals

In 2021, the topic of investments was particularly popular among criminals. We associate such interest with the influx of nonprofessional investors. For example, over the past year alone, more than 6 million people joined the trading on the Moscow Stock Exchange.

Another popular attack method was infecting devices of individuals with malware. Among the main types of malware that cybercriminals most often used in attacks on individuals in 2021 were RATs, spyware, and banking trojans. The share of remote administration tools increased from 16 percent to 34 percent over the year. Banking trojans also became more common in attacks on individuals; their share increased by 10 percentage points (amounting to 32 percent). Anubis was one example of this type of malware. The attackers who distributed it among owners of Android mobile devices aimed at collecting credentials for 394 banking applications and cryptocurrency wallets.

The share of attacks using spyware in 2021 decreased by 18 percentage points (amounting to 32 percent). The number of attacks using bootloaders for installing additional malware on the victim's devices increased significantly: their share amounted to 21 percent.

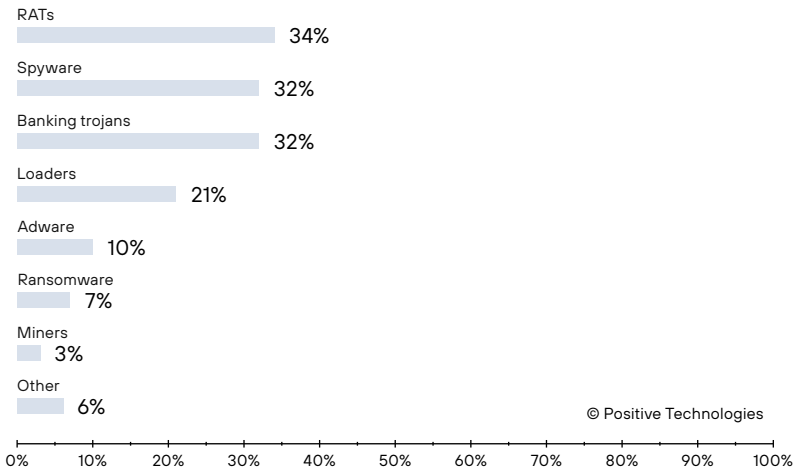

Figure 16. Types of malware in attacks on individuals (percentage of malware-related attacks in 2021)

To deliver malware, cybercriminals used websites (35%), sent attachments by email (29%), and placed malware in official app stores (12%).

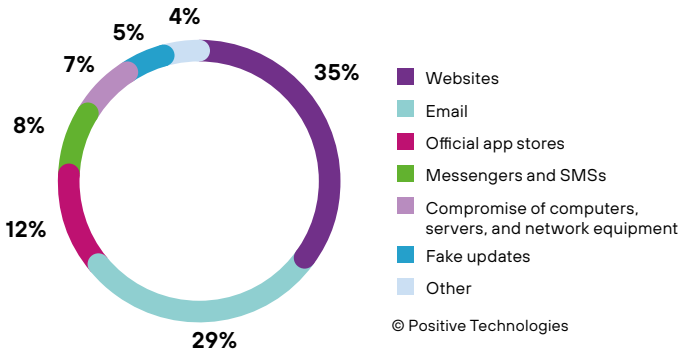

Figure 17. Methods used for malware distribution (in attacks on individuals)

In our opinion, in 2022 the ratio of attack methods will remain approximately the same, and most attacks will involve social engineering. The most prevalent social engineering topics will likely be related to socially significant events. To protect against social engineering attacks, we recommend following the basic rules of information security:

- Do not click suspicious links and do not enter credentials on resources without making sure of their legitimacy.
- Do not launch attachments if received from an unknown sender.
- Install applications only from official stores and pay attention to what permissions the application requests (for example, a photo processing application should not request access to contacts).
- Use strong passwords that are unique for each resource, and store them in a password manager.
- Be careful and double-check information from emails, newsletters, and news communities on third-party Internet resources.

About the research

This report contains information on current global information security threats based on Positive Technologies' own expertise, the outcomes of investigations, and data from authoritative sources.

In our view, the majority of cyberattacks are not made public due to reputational risks. The result is that even organizations that investigate incidents and analyze hacker activity are unable to do a precise count of the number of threats. Our research, aimed at companies and individuals with a keen interest in information security, seeks to draw attention to cybercriminal methods and motives and highlight the main trends in the changing cyberthreat landscape. This report counts each mass attack—for example, a phishing email sent to multiple addresses—as a single incident. Definitions of terms used in this report are available in the glossary on the Positive Technologies site.