



Positive Research 2021

Positive Research 2021

4

Editorial

6

2020 in review:
hacks, attacks,
and other
incidents

10 

Most interesting
vulnerabilities
in 2020

12

Cybersecurity
2020–2021:
trends and
forecasts

48

Custom hacking
services

Contents



69

Digital twin cyber-exercises: a better way of seeing real business risks

62

Cyber-risks: proving dangers and defining criteria

76

The Standoff 2020: an exciting cyberexercise



88

Global SOC at The Standoff 2020: the all-seeing eye

101

About us

Editorial

We live in an era of total digital transformation, with both good and ill effects. This process may still have a way to go. But even now our dependence on technology leaves no doubt: we are not willing to give up high-tech conveniences, in part because of our tendency to underestimate information security threats.

This dependence puts individuals, businesses, and even governments at risk. No one is safe. Even esteemed corporate giants may at any moment face unacceptable events that jeopardize their bottom line and reputation.

News of data breaches and hacks of major companies has become all too common. Consequences include billions in damages, production shutdowns, shareholder losses, and record-breaking fines from regulators. Cyberattacks are no longer just an IT or security problem. They have become a real threat for business.

Is business up to the challenge? Join us as we look for answers in this new issue of Positive Research. This time we have focused on real-world security and the risk-oriented approach taken by business and government to their information systems.

Positive Technologies experts:

Have provided an overview of notorious hacks and breaches	6	➤
Highlighted the latest trends and outlooks for information security	12	➤
Told about critical business risks	62	➤
About the evolution and role of cyber-ranges	69	➤
About the global SOC at The Standoff 2020	88	➤

2020 in review: hacks, attacks, and other incidents

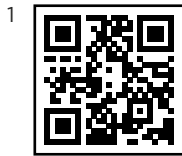
Alexander Antipov

Online Marketing

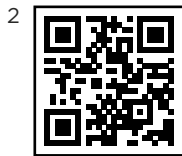
✓ 10 min
to read this article

There was more to 2020 than just COVID-19. A number of unprecedented cybersecurity events created headaches for governments, companies, and ordinary users. Unfortunately, the pandemic did not lead to a fall in digital crime. To the contrary, last year saw an increase in phishing, data breaches, and ransomware. This unhelpful trend was enabled in part by work from home and digital communication with friends and family, which during quarantine caught on like never before. Here is our pick of last year's most important incidents.

Mass Twitter and Nintendo hacks



Twitter accounts of a number of celebrities were hacked in a big way. Those compromised included Elon Musk, Bill Gates, and Barack Obama, with fake tweets posted in their names to advertise a cryptocurrency giveaway.¹ The culprits? Three teenagers who phished the admin password of a Twitter employee working from home.



The gaming industry did not escape attention: in April, many Nintendo users had their accounts hacked. In some cases hackers used these accounts to buy Nintendo games, but more often bought Fortnite in-game currency.²

Cyberattacks on COVID-19 vaccine developers



Throughout the year, cybercriminal groups (including pro-government ones) took an active interest in trials of coronavirus vaccines. Targets included companies and research centers. One cyberattack at year's end struck the European Medicines Agency, responsible for vaccine certification in the EU. This gave hackers access to documents from pharmaceutical companies Pfizer, BioNTech, and Moderna.³ A major malicious campaign targeted companies storing and transporting vaccines. In one espionage operation, North Korean hackers targeted COVID-19 vaccine manufacturers including the United Kingdom's AstraZeneca and American companies Johnson & Johnson and Novavax.⁴



Ransomware attacks on University Hospital Düsseldorf, Garmin, Software AG, and the University of California



Last year was full of ransomware attacks, which encrypted the computers of entire companies and organizations. Some perpetrators even published the stolen information online—all the better for forcing the victim to pay up for restoring it, presumably. In a first of its kind, a ransomware attack on University Hospital Düsseldorf disrupted care and caused the death of a patient.⁵

Other major ransomware incidents struck American company Garmin, which manufactures digital devices for navigation, recreation, and sports, and software developer Software AG. With Garmin, the WastedLocker group caused four days of service downtime and blocked access to GPS for millions of people (including pilots planning their flights).⁶ Software AG was hit by Clop ransomware and a demand for \$20 million—one of the largest amounts ever.

While the world held its breath in anticipation of a coronavirus vaccine, the Netwalker group hit the University of California San Francisco, one of the leading vaccine development sites in the U.S. The hackers encrypted key documents and demanded a ransom of \$3 million. In the end, the university bargained them down to \$1.14 million.⁷

8



9



10



5




6



7



Zoom breach



Many employees shifted to working from home during the pandemic, with dramatic growth in the popularity of video conferencing apps such as Zoom. Criminals were quick to catch on as well. Thousands of Zoom video recordings were uploaded to YouTube and Vimeo, including therapy sessions, school lessons, doctor's visits, and corporate meetings. Then 2,300 sets of user credentials were published on a hacker forum for all to see.⁸



Data breaches and credential dumps remain one of the thorniest security issues. The year was full of them: 5.2 million Marriott hotel clients,⁹ 900,000 Virgin Media clients,¹⁰ 4 million Quidd users,¹¹ 40 million users of popular mobile app Wishbone,¹² 235 million user profiles in a database encompassing Instagram, TikTok, and YouTube.¹³



SolarWinds: the 2020 hack that got everyone talking



The event from the last year that attracted the most attention, however, was a supply chain attack on Texas-based software company SolarWinds.¹⁴ Attackers planted a backdoor in updates for the SolarWinds Orion platform. Approximately 18,000 organizations installed the resulting malicious update. Malware was subsequently discovered on the networks of the U.S. Treasury Department, National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce, U.S. Department of Homeland Security, and FireEye, as well as infrastructure at Microsoft, Mimecast, Palo Alto Networks, Qualys, and Fidelis Cybersecurity. Microsoft President Brad Smith described the incident as "the largest and most sophisticated attack the world has ever seen."

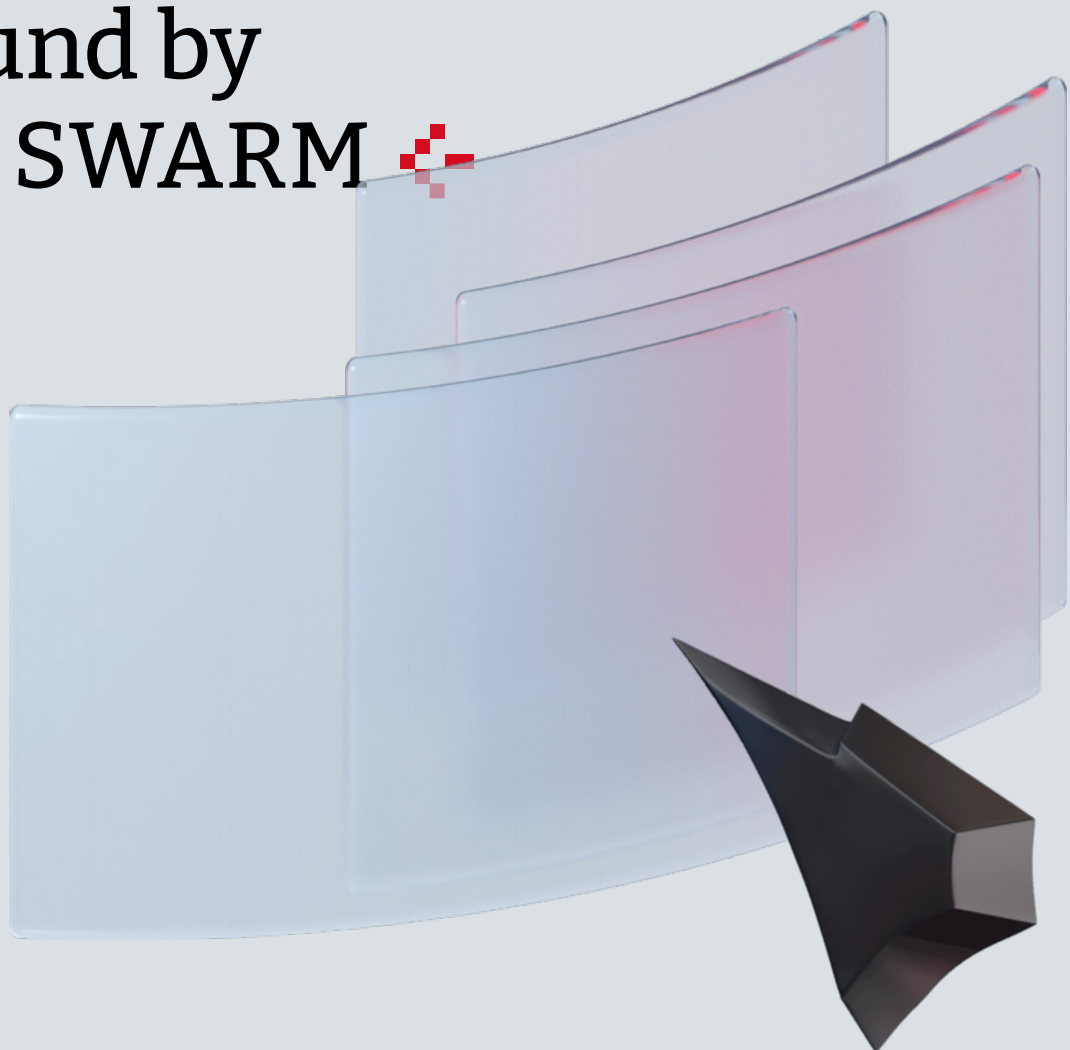


Most interesting vulnerabilities in 2020

found by

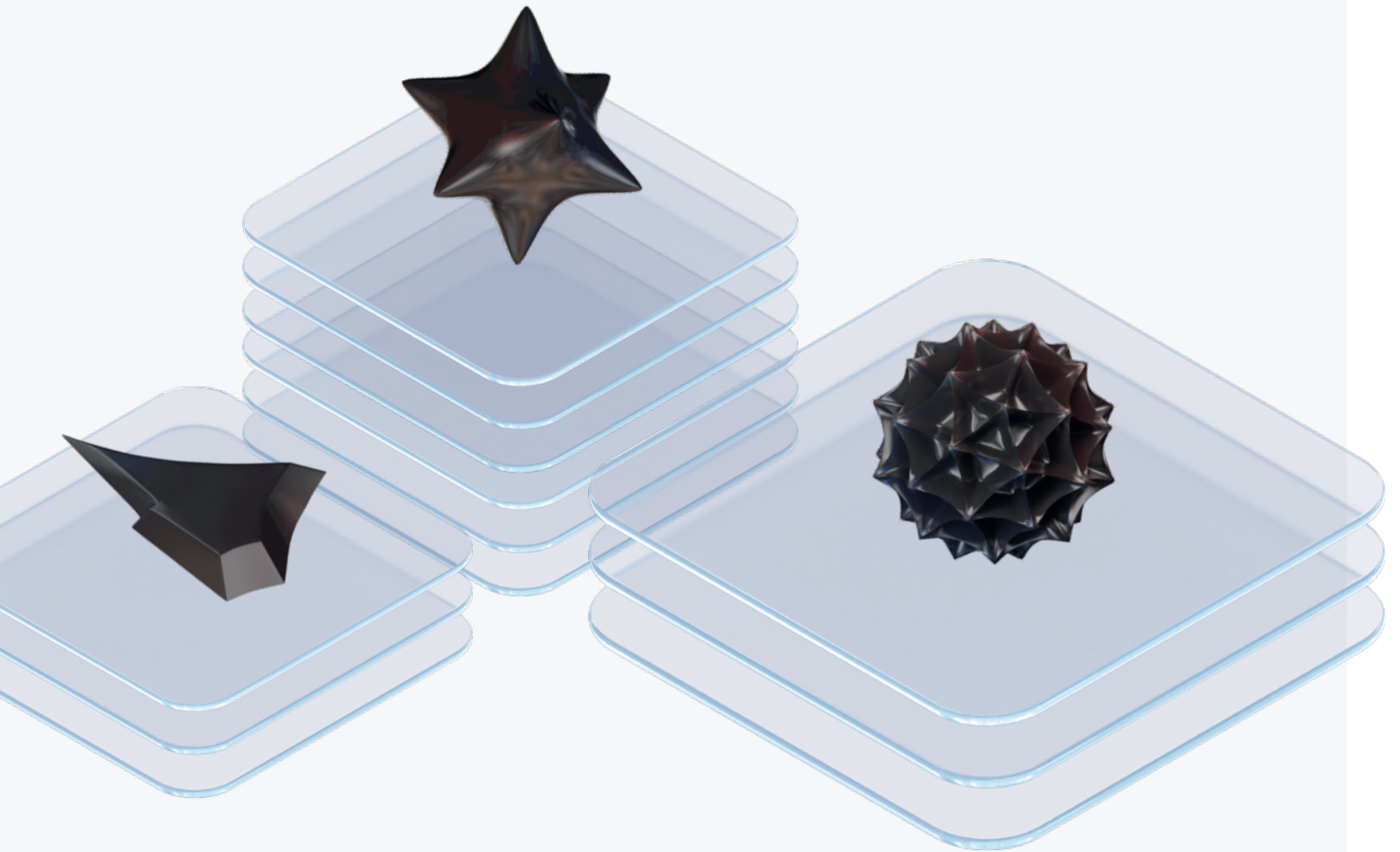


PT SWARM



Check Point	ICA Management Tool Argument Injection	CVE-2020-6020	[4.2]	  
Cisco	ASA Memory Leak	CVE-2020-3259	[7.5]	  
	ASA Unauth File Read	CVE-2020-3452	[7.5]	  
	ASA Unauth DoS	CVE-2020-3187	[9.1]	  
	Integrated Management Controller Unauth RCE	CVE-2020-3470	[9.8]	  
Citrix	XenMobile Unauth Path Traversal	CVE-2020-8209	[7.5]	  
Dell	iDRAC 9 ArbitraryFile Read	CVE-2020-5366	[7.1]	  
F5	BIG-IP Unauth DoS	CVE-2020-27716	[7.5]	  
	BIG-IP Unauth RCE	CVE-2020-5902	[10]	  
IBM	Maximo JavaDeserialization	CVE-2020-4521	[8.8]	  
Oracle	WebLogic ArbitraryFile Read	CVE-2020-14622	[4.9]	  
Palo Alto	PAN-OS Post-Auth RCE	CVE-2020-2037	[7.2]	  
	PAN-OS Post-Auth RCE	CVE-2020-2038	[7.2]	  
	PAN-OS Unauth DoS	CVE-2020-2039	[5.3]	  
SonicWall	SonicOS Unauth Buffer Overflow	CVE-2020-5135	[9.8]	  
Sophos	XG Firewall Unauth Heap Overflow RCE	CVE-2020-11503	[9.8]	  
VMware	vCenter Unauth Arbitrary File Read	—	[5.3]*	  

* As scored by PT SWARM experts



⌚ 40 min
to read this section

Cybersecurity 2020–2021: trends and forecasts

Illuminating with facts, figures, and new ideas	14	
The Great Siege of 2020	16	
Governments	22	
Attacks on users	23	
Attacks on the industrial sector	25	
Security of telecommunication networks	28	
Security of the financial sector	30	
Security of operating systems	38	
Hardware vulnerabilities	40	
Mobile security	42	
Security and AI	44	

illuminating with facts, figures, and new ideas

Information security is shaping the agenda like never before. And rightfully so: the number of threats and cybercriminals is growing every year. Management at many companies has become more responsive to cybersecurity issues. They realize that certain business risks must simply be stopped, no matter what. Of course, committing to such real-world security comes at a financial cost.

Businesses saw that 2021 would be quite different in terms of IT and security budgets. Therefore, they tried to make the most out of their existing plans and leverage all the resources they could bring to bear.

COVID-19 still impacting business outlooks



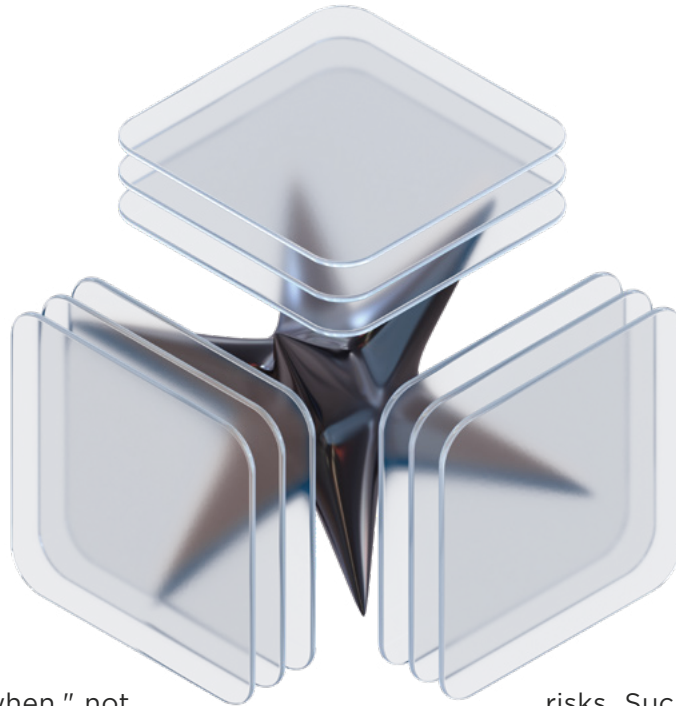
The COVID-19 pandemic has certainly affected the cybersecurity market. However, the practical impact has not been as much as feared. In late Q1 2020, the situation was precarious as the number of pilot projects dropped significantly. The

reason was obvious: lockdowns and the rapid transition to remote work made such projects more difficult or even impossible to implement on companies' premises. At the same time, the new realities underscored the importance of not stopping ongoing cybersecurity efforts. Together, these two factors created a rather dangerous dynamic, in which companies might skip pilot deployments (despite their importance for making an informed choice) and instead simply choose the lowest bidder no matter what. Fortunately, these fears did not materialize. Competition on the domestic infosec market remained strong and the demand for security that works kept companies from taking the easy way out when it came to choosing protection tools.

Opting for real information security

As we have mentioned before, the security paradigm itself is changing. The infosec community has moved away from the idea of building moats. No matter how good a security system is, getting

Businesses saw that 2021 would be quite different in terms of IT and security budgets



hacked is a matter of "when," not "if." That's why these days, the goal is to detect an attacker inside the network as soon as possible. The ability to detect is the crucial thing, in other words. However, over the last year, this concept evolved. We now see that it is possible to create a security system guaranteeing that attackers will not be able to actuate specific business risks. We still agree that any company can be hacked, but the goal of information security can and should be to keep attackers from causing any significant harm. This trend took shape quite recently, just in the last year, and will likely dominate in the years to come. It will be vital to create a new type of security operations center (SOC). Instead of being measured by 24/7 availability or the speed of incident response, these results-oriented SOCs will be subject to an SLA-like arrangement centered on the ability to stop attackers from triggering unacceptable

risks. Such SOCs will be judged on a "pass/fail" scale: was a risk triggered, or not? Cyberexercises become essential, as they are the only way (short of a real incident) to measure how well the security system and SOC work. Vague checklist-like assessments are all too common. Only properly organized cyberexercises can cut through the window dressing to provide actionable results.

This approach should ultimately expand the market and make a real difference by keeping only the solutions and technologies that work. This is Darwin's theory in action: only technologies able to quickly detect attackers, block them from pivoting and escalating, and throw them off of infrastructure entirely, will survive. As a vendor, we are already working on an automated smart solution to accomplish these tasks quickly and efficiently.



Alexey Novikov

Director of Positive
Technologies Expert
Security Center (PT ESC)

The Great Siege of 2020

The massive shift to remote work gave rise to new information security risks. Social engineering became a common method for penetrating companies' networks. All types of hacker groups took advantage of the pandemic. COVID-19 fueled both mass campaigns and targeted ones. As we predicted in 2019, the number of advanced persistent threat (APT) attacks kept growing in 2020.

Throughout the year, we monitored around 30 APT groups. Attribution is becoming more and more difficult, since hackers often combine various malware tools normally attributed to different gangs in a single attack. When we report to companies that they have been hacked by an APT group, all too often this news comes as a surprise to them. In 2020, PT ESC performed approximately 50 investigations.

2020 showed that insiders still present an acute risk for companies, as proved by the incident at Tesla.¹ People constantly communicate via social media and chat, and it is getting ever more important to protect these platforms. A notable example is the mass hijacking of celebrities' and politicians' Twitter accounts.²

Ransomware was a major headache in 2020. The ransoms for decryption were huge, and when victims refused to pay, attackers published the data on the web. Some companies had to stop operations for several days. One prominent example was the cyberattack on Garmin.³ We discussed the increase in ransomware and other destructive attacks back in 2017. Not only financially motivated hackers are encrypting entire infrastructures: APT groups have joined in as well.⁴



All types of hacker groups took advantage of the pandemic

Supply chain attacks

We warned back in 2017 about supply chain attacks, and in 2020 they caused plenty of headache. By now everyone has probably heard of what happened with SolarWinds.⁵ Our company has come across similar attacks on software vendors, security developers, IT integrators, IT contractors, and government websites in a number of countries. Security at large companies is improving, which makes them difficult targets, particularly for attackers interested in long-term persistence and not just a one-time hack. That is why APT groups are turning their sights to the partners and contractors of such companies. Only top-tier security experts are capable of protecting from such attacks.

Forecasts

In 2021, we expect hackers to refine social engineering methods for taking advantage of current events, especially COVID-19. We also anticipate that phishing attacks will become more tailored, with use of instant messaging and social media to make contact with victims. To overcome corporate protection systems, attackers will try to hack personal computers of employees.

In 2020, many APT attacks targeted pharmaceutical companies, including vaccine development laboratories. The virus is mutating and research



is ongoing, which means that hackers will stay interested in these companies for the foreseeable future. We also expect APT attacks to keep climbing in 2021.

Groups such as APT 27 are increasingly using ransomware in targeted attacks. In 2021, we expect that such attacks will grow.

We will probably see supply chain attacks similar to the SolarWinds hack, as well as more attacks on IT and infosec companies and cloud infrastructures.

We recommend that all companies get to know their infrastructure in detail, quickly respond to any anomalies, and keep an eye on network entry points used by remote workers. As a minimum, the starting point for security-minded companies should include antivirus software, SIEM, NTA, and a web application firewall (WAF).

The flip side of working from home: attacks on remote desktops and collaboration software

COVID-19 and the shift to remote work led to a worldwide rise in attacks on web-accessible corporate services. Companies had to urgently push their services to the perimeter. Because of the large number of people working from home for the first time, more corporate hosts became accessible for RDP connections. As a result, the share of attacks exploiting software vulnerabilities and configuration flaws increased to 36 percent in Q4 (compared to 9% in Q1).

From quarter to quarter, we saw an increase in malware attacks with exploitation of vulnerabilities on the network perimeter. Attackers actively exploited vulnerabilities in VPN solutions and remote access systems, such as those from Pulse Secure, Fortinet, Palo Alto, and Citrix. They also



In 2020 supply chain attacks caused plenty of headache

looked for vulnerabilities in web applications and bruteforced RDP passwords.

Another pandemic-related trend is the theft of credentials for audio- and videoconferencing services, such as Skype, Webex, and Zoom, as well as tampering with these conferences.

In 2020, criminals pursued a wide range of goals, from cryptocurrency mining to cyberespionage against large companies. They have multiple types of malware at the ready and increasingly use multifunctional trojans or plant a wide array of malware on compromised devices. Malware operators can transfer access to infected devices to other criminals. Malware itself is evolving in the direction of greater stealth and evasion capability against antivirus and protection software, including sandboxes. New functionality and exploits for new vulnerabilities are being added as well.

Ransomware booming

In 2020, we saw a constant increase in ransomware attacks. In Q1, ransomware accounted for 34 percent of malware attacks on organizations. In Q4, it reached 56 percent. Mass ransomware attacks became less common. Malware operators are deliberately choosing large companies that have deep pockets or for which downtime





Ransomware is one of the fastest-growing varieties of cybercrime

could be catastrophic. Once the target is chosen, hackers strike.

Ransomware is one of the fastest-growing varieties of cybercrime. It has become a common practice for attackers to threaten to disclose the stolen data unless the victim pays a ransom. Maze, Sodinokibi, DoppelPaymer, NetWalker, Ako, Nefilim, and Clop operators were the most active perpetrators of such attacks in 2020. Some of them even implemented a "double extortion" scheme by demanding separate ransoms for decryption and non-disclosure of data. To sell the stolen data, many ransomware operators create special websites where they publish a list of victims and the stolen data. They may even auction it off. There are ransomware alliances that publish stolen data as part of partnership agreements.

Access for sale, ransom for non-disclosure

Other criminals have quickly caught up with the trend of demanding ransom for non-disclosure of data. For example, hackers can demand a ransom from online stores by threatening to sell the stolen data to third parties. Compared to ransomware operators who demand millions

of dollars as a ransom, their appetites are more modest, on the order of \$500. Nevertheless, this business model can offer significant profits: database owners are often willing to pay to protect their reputation, while the criminals never run out of potential buyers.

Attackers sometimes buy access to companies' networks from other criminals. Ransomware operators were among the first to use this scheme. They propose cooperation, recruit affiliates to spread ransomware, and share a percentage of any ransom received. On the darknet, this access-for-sale scheme allows even low-skilled hackers to earn money. All they need to do is find vulnerabilities on external resources of the victim company and sell this information.

Forecasts

In late 2020, we saw a slowdown in the explosive growth in attacker activity that had accompanied the beginning of the COVID-19 pandemic in the first two quarters of the year. But the number of attacks remains persistently high and quarter-over-quarter growth in the number of incidents continues.



Use of cyber-ranges to model business risks will become a driving trend in information security

We expect to see new criminals motivated by high ransomware profits. These will include malware operators and those who provide access to victim infrastructure in return for a percentage of the ransom. We will likely see new cybergroups and platforms for selling stolen data. Ransomware owners will likely keep the blackmail strategy, honed in 2020, of demanding separate ransoms for infrastructure recovery and non-disclosure of stolen data. However, even without taking into account ransom payments, ransomware attacks come at a high cost, including system recovery, downtime, possible loss of clients, and other consequences. For example, IT service provider Sopra Steria estimated losses as high as €40–50 million due to a Ryuk ransomware attack on the company in October 2020.

Most companies continue to work remotely, either partially or fully, which means that attackers keep looking for any security lapses in systems on the network perimeter. At the same time, the rise of access-for-sale on the dark-web makes companies, including large ones, a target for low-skilled hackers eager to make a fast buck. External attacks on corporate infrastructures will continue to grow. That is why

companies need to assess the security of their network perimeter, take an inventory of externally accessible resources, and build an effective vulnerability management process.

But there is also good news

Many companies have learned to accommodate remote work. In early 2020, they had to rapidly shift employees to working from home. In 2021, they can correct past mistakes by allocating budgets for protection tools and implementing best practices.

Companies can no longer ignore the risks. They want to measure the real consequences of possible cyberattacks and, when an attack does take place, minimize negative outcomes. A number of platforms now offer the ability to conduct training and exercises. The most effective cyberexercises use digital models to re-create real corporate infrastructures. Use of cyber-ranges to model business risks will become a driving trend in information security.



Governments



Government institutions remain the most attractive targets for hackers, receiving 19 percent of all attacks on organizations. In 2020, we recorded 359 attacks on such targets. Compared to 2019, these attacks were significantly more likely to involve malware (71%) and social engineering (64%). The pandemic may have been a factor: many attackers sent emails to governments in various countries with malicious attachments that preyed on the coronavirus situation. Cyberespionage attacks accounted for 58 percent of cases.

In early 2020, our experts observed phishing attacks by APT groups SongXY, APT36, TA428, TA505, and Higaisa, in which they spread malicious documents with pretexts related to COVID-19. The pandemic was also leveraged in attacks with Chinoxy and KONNI malware. Throughout 2020, the Positive Technologies Expert Security Center recorded attacks by the Gamaredon group targeting government institutions in Ukraine and Georgia.

Forecasts

Many government services have become available online for the first time. Even elections can now be held electronically. The pandemic, with resulting lockdowns and monitoring, has driven governments to use technology like never before. As new electronic services appear, they will inevitably attract criminals and require special attention with regard to information security.



In 93% of attacks ordinary users become victims of mass campaigns

1



2



Attacks on users

In 2020, we recorded 325 campaigns against individuals. The number of such attacks increased by 11 percent compared to 2019. In most cases (93% of attacks), ordinary users become victims of mass campaigns. Most times, attackers used social engineering (69% of attacks). In 59 percent of attacks, hackers infected user devices with malware. In most cases, they spread malware via websites, email, and official app stores. Half of malware attacks against individuals involved spyware, and in 22 percent of cases attackers used banking trojans. Attacks were mostly driven by theft of credentials. Credentials accounted for 36 percent of all stolen data, followed by personal data and payment card information (19% each).

COVID-19 phishing attacks mostly affected ordinary users. Techniques went beyond just malicious emails. Attackers also hosted malware on fake pandemic-themed websites and distributed malicious mobile apps.¹ At the beginning of the pandemic, criminals lured their victims with personal protective equipment or additional information about the virus. More recently, they have started playing the vaccine card.²

In the first half of 2020, many companies shifted their employees to work from home. Criminals took advantage by using individuals as a stepping-stone for access to corporate targets. People are often unaware of basic security rules or neglect them when working from home, which places them and their employers at greater risk. Lack of software updates, unlicensed software,



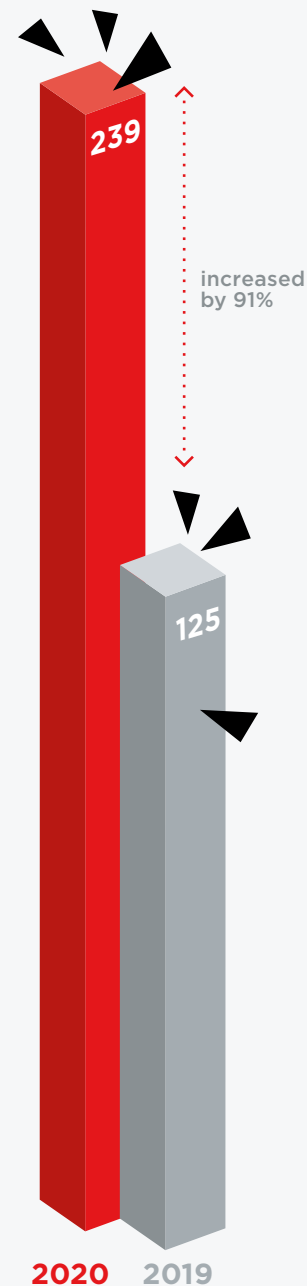
old OS versions that are no longer supported, lack of antivirus software, use of weak passwords, and other gaps on personal computers can all give attackers a way in to corporate networks.

Forecasts

The pandemic will remain a tool for spreading malware as well as stealing money and card numbers from ordinary users. Possibilities for fraud include websites purporting to offer COVID-19 treatments, paid vaccinations, or vaccination certificates. Phishing messages will disguise malware as information about vaccinations, related timeframes, or so-called vaccine passports.

The UEFA European Football Championship is another likely topic for social engineering attacks. Such large events tend to inspire fake websites aimed at stealing data and money.

Magecart-like attacks will continue targeting online stores and other merchants. In these attacks, malicious scripts are injected into the websites of hacked companies. These scripts collect all data entered by website users—including, of course, payment card information. These techniques are highly effective because the security of web applications is often neglected. In many cases, attackers can simply leverage known vulnerabilities in popular content management system (CMS) software. But ordinary web visitors are the victims.



Attacks against industrial and energy companies



Dmitry Darensky

Head of Industrial Cybersecurity
Practice, Positive Technologies

Attacks on the industrial sector

2020 saw an increase in attacks against industrial and energy companies. We recorded 239 attacks on such companies, which represents an increase of 91 percent over 2019 (125 attacks). In nine out of ten cases, attackers used malware. Ransomware and spyware were present in 41 and 25 percent of malware attacks, respectively.

Attackers sent phishing emails to spread malware and gain a foothold on local networks. They also exploited vulnerabilities on the network perimeter.

In most cases, industrial companies were attacked by ransomware operators and APT groups. One out of six ransomware attacks against organizations was aimed at the industrial sector. At the beginning of the year, many cybersecurity experts turned their attention to the new ransomware called Snake, capable of

deleting shadow copies and stopping industrial control system (ICS) processes. Snake can stop such processes as GE Proficy and GE Fanuc Licensing, Honeywell HMIWeb, FLEXNet Licensing Service, Sentinel HASP License Manager, and ThingWorx Industrial Connectivity Suite. The first victims of the Snake ransomware were automaker Honda and energy giant Enel Group. Throughout the year, industrial companies were also struck by other ransomware operators, including Maze, Sodinokibi, Ryuk, NetWalker, Nefilim, DoppelPaymer, RansomEXX, and Conti.

The industrial sector is targeted by many APT groups worldwide. For instance, one APT attack by the Bisonal group in Q1 2020 targeted Russian aerospace organizations. Attacks by the RTM group continue at a high pace in Russia and the CIS countries: PT ESC detected over 100 malicious mailings by the group in 2020.

Forecasts

Since the beginning of 2021, the number of attacks against industrial companies has increased and remained consistently high. We do not expect that attackers will lose interest anytime soon. The main motive will not only be espionage, but also the possibility to receive large ransoms in return for data recovery and non-disclosure of stolen information.

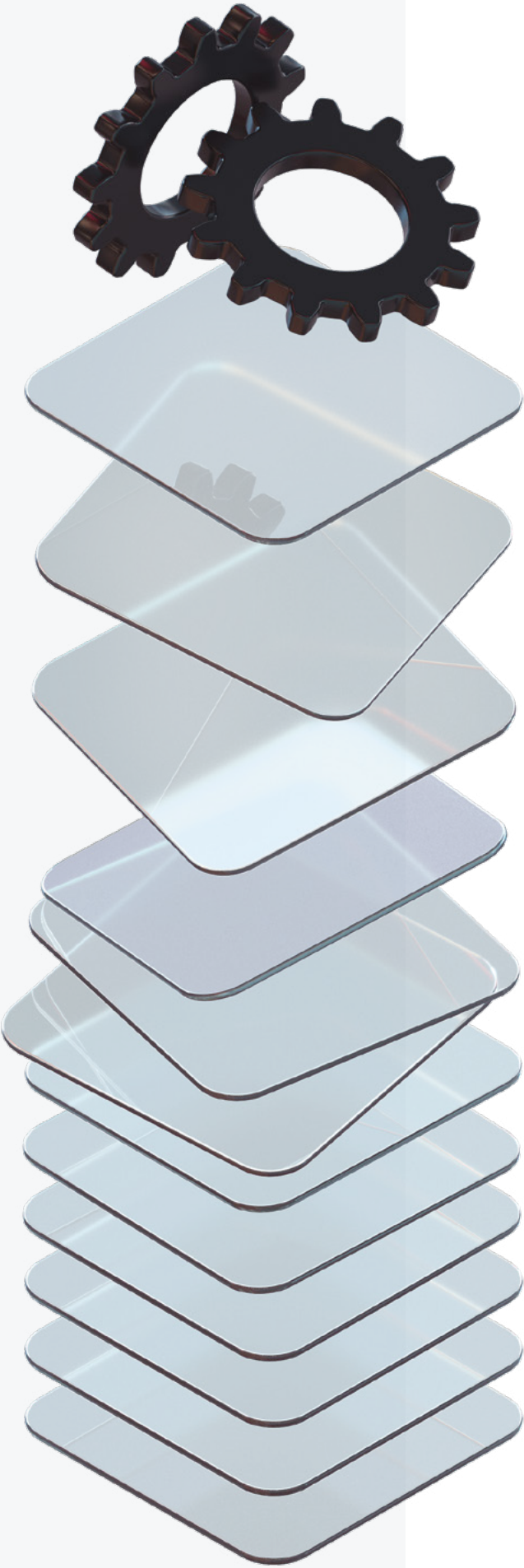
News reports of an industrial company stopping operations due to a cyberattack used to be rare. There were two reasons. For one thing, companies wanted to hush up such incidents. And for another, they often could not determine whether the disruption was actually the result of a cyberattack or something else. But today, hacks of major energy and industrial companies are a frequent occurrence. Most often this takes the form of a targeted ransomware attack. These attacks are difficult to hide, and the culprit is obvious: the criminals themselves inform of the hack by way of demanding a ransom.

All this shows an extremely low level of protection against external threats, plus the inability to detect and stop attackers in a timely way. One can only guess how many spyware campaigns remain undetected and undisclosed. Criminals will likely continue pursuing these victims, with a preference for large companies. At the same time, they will try to minimize the outlays necessary for performing a hack or purchasing access from other criminals. Data leaks and disruptions at industrial companies are a sure bet for 2021. Ransoms will also likely increase. They already reach tens of millions of dollars in some cases, and the more companies fall victim to attacks, the more motivated hackers are to go on. We also expect to see new

attacker groups and cooperation among criminals to make money off security vulnerabilities at industrial companies.

At the same time, on top of ensuring formal compliance with regulatory requirements, industrial companies are busy working to secure their assets in real-world ways. The following trends will be relevant in 2021:

- **Risk-oriented threat modeling.** Industrial companies will start understanding digital security risks in a more rigorous and meaningful way. Instead of classic probabilistic methods that look only at individual systems or components, the new approach places cyberthreats in a risk context at the operational and business-wide level.
- **SCADA data-driven anomaly detection and response.** Companies with ICS infrastructure are analyzing SCADA data to spot anomalies and attacks. This trend will be especially pronounced on NTA/NDR, EDR, and SIEM systems.
- **Automation of security management processes.** Security management processes, especially for detection and incident response, are becoming increasingly automated.
- **Digital twins and cyber-ranges.** Modeling of virtual copies ("digital twins") of industrial systems is coming into its own as a way to study ICS vulnerabilities and emulate attacks. At cyber-ranges, companies can safely use this method to test the feasibility of business risks and analyze potential attack methods.



Since the beginning of 2021, the number of attacks against industrial companies has increased and remained consistently high

The Standoff: successful attacks without real consequences

Digital modeling offers unique capabilities for understanding cyberattacks on information infrastructure. Participants at The Standoff cyber-range have the run of the same real equipment and software used at industrial companies and can verify the feasibility of various risks in practice. At The Standoff in November 2020, red teams pulled off several attacks on a petrochemical plant and an oil refinery. In real life, such attacks would have caused enormous damage. Attackers gained access to the plant management system, which allowed them to disrupt and completely halt the production process. The resulting modeled accident released toxic substances. At the virtual oil field, attackers disrupted oil extraction machinery. In addition, hackers gained access to the oil storage management system and disrupted pumping to oil terminals. Later, they also halted the petroleum transport controller. It takes a cyber-range to truly model these risks in full. Attempting such experiments as part of penetration testing or cyberexercises would have damaged equipment, forcing companies to settle for the ability to demonstrate only to a certain point. The cyber-range, however, allowed finishing the attack and assessing the real consequences.



Pavel Novikov

Head of Telecom Security
Research, Positive Technologies

Security of telecommunication networks

The main security challenge for telecom systems consists of the vulnerable protocols used in 2G, 3G, and 4G networks. For example, SS7 vulnerabilities in 2G and 3G networks allow all sorts of attacks, from information disclosure to SMS interception, eavesdropping, and disruption of subscriber service. The Diameter protocol in 4G networks has vulnerabilities that allow tracking subscriber geolocation, bypassing operator blocks, and causing denial of service. Flaws in the GTP protocol allow attackers to interfere with network equipment and leave an entire city without communication, impersonate users to access various resources, and use network services at the expense of the operator or subscribers.

Moreover, all these security issues remain relevant for 5G Non-Standalone networks, which are built on the infrastructure of previous-generation

networks. Just like 4G, most 5G networks are vulnerable to disclosure of subscriber information (including geolocation data), spoofing (such as for fraud), and DoS attacks on network equipment, resulting in mass disruption of mobile service.

As for 5G Standalone (5G SA) networks, we can say that despite all the protections present in the HTTP/2 protocol (the successor to SS7 and Diameter in 5G SA), attackers can still spoof or remove network elements, which can lead to network malfunction. In addition, with access to internal interfaces, attackers can perform DoS against subscribers and intercept incoming traffic by exploiting vulnerabilities in the PFCP protocol (the 5G SA successor to GTP-C).

Denial of service is a serious threat to IoT devices. These devices, which are becoming the main

The main security challenge for telecom systems consists of the vulnerable protocols used in 2G, 3G, and 4G networks



"subscribers" of mobile operators, are key to the functioning of smart homes as well as the urban and industrial infrastructures in which they are embedded.

Mobile operators are aware of the threats but rarely take a systematic approach to security. As a result, even when expensive niche solutions are installed, networks still tend to be poorly protected in practice.

Forecasts

The vast majority of people will still be served by 2G, 3G, and 4G networks, which means that all the "old" vulnerabilities will be as important as ever. Many operators are starting 5G SA deployment in 2021, but full-fledged commercial rollouts will be slower in coming. The insecurities of 2G, 3G, and 4G networks will still be with us for a while. What's more, 5G networks interwork with other mobile networks. Hackers can perform cross-protocol attacks by exploiting vulnerabilities in multiple

protocols as part of a single attack. For example, an attack on 5G might begin with exploiting 3G vulnerabilities to obtain subscriber identifiers. That is why protecting previous-generation networks is essential for 5G security.

Researchers continue to investigate the 5G architecture and protocols, searching for vulnerabilities and flaws. Even though the specification developers took into account the security flaws of previous-generation mobile networks, new technologies come with new risks.

Nor will GTP security issues go away completely, even after the transition to 5G Standalone. GTP is planned for use on Standalone networks, too, including roaming, even if only to transmit user data over the GTP-U protocol. Attacks on GTP-U allow encapsulating management protocol packets in user sessions or obtaining data about subscriber connections. This is why, when 5G SA networks arrive, additional research will be required to see whether the new management protocols remain vulnerable.





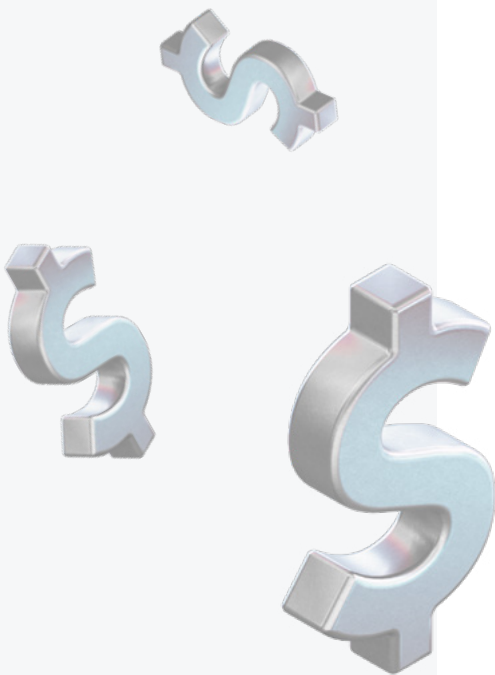
Maxim Kostikov

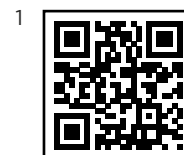
Head of Banking Security,
Positive Technologies

Security of the financial sector

In 2020, we recorded 126 attacks against financial companies, compared to 92 in 2019. Phishing factored into 61 percent of attacks. It remains the main method for breaching the local networks of financial companies. Hacking (defined as exploitation of software vulnerabilities and flaws) figured in 21 percent of cases. Malware was present in 65 percent of attacks. The most common malware types were spyware (28% of malware attacks), ransomware (29%), and banking trojans (23%). Ransomware attacks against financial institutions increased, just like in other sectors.

According to the Positive Technologies Expert Security Center, the RTM group kept attacking financial organizations with malicious emails throughout the year. During the first two quarters of 2020, our experts recorded phishing attacks by the Cobalt group.





The European Association for Secure Transactions (EAST) has reported an increase in ATM logical attacks in Europe.¹ All the attacks reported in the first half of 2020 were black-box attacks.

Forecasts

No new major hacking groups specialized in withdrawing money from bank accounts appeared in 2020, nor are any more expected to appear in 2021. Attacks on small banks are less profitable than targeted ransomware attacks. In addition, they are much more difficult to perform, since they require specialized knowledge of banking processes and software. We will most likely encounter attacks by known groups that conceal their attacks by using multiple techniques for penetrating and gaining persistence, refine their malware, and vary the regions they target.

We may expect an increase in ransomware attacks on banks. Such attacks have become a common practice, pay off well, and do not involve any extra costs. Attackers will keep searching for known vulnerabilities on the perimeter to spread malware. Our penetration tests at financial institutions demonstrate a low level of security: at seven out of eight companies, real attackers would have been able to penetrate local networks from the Internet.

Key issues with ATM security

Banks are actively upgrading their ATMs to Windows 10. It has more features than previous versions, which means that attackers have more options for bypassing kiosk mode and gaining access to the operating system.

Our experience shows that ATMs do not securely implement software access control. Attackers can execute arbitrary code after gaining access to the OS and tampering with executable files on the device. With this code, they can dispense cash or steal personal data.

Black-box attacks remain a major concern, as they can lead to ATM cash thefts. Banks are considering whether to implement authentication of ATM-connected devices (such as USB flash drives and keyboards), which should significantly reduce the risk of attacks and kiosk mode bypasses.

As for network security, we have noticed an improvement in network policies and the use of VPNs to protect ATMs. However, not all banks have taken these steps. This absence enables attackers to tamper with traffic between the ATM and processing center. Results include theft of sensitive information or withdrawal of funds. In addition, traffic inside the VPN is often not protected with additional encryption, making it vulnerable to an insider.

Security of banking web applications

In 2020, the security of banking web apps took a turn for the better. The number of standard web vulnerabilities (XSS, SQLi, and RCE) decreased, and the transition towards a micro-service architecture enhanced system resiliency. The bad news is the increasing number of logical vulnerabilities that may allow attackers to steal money and user data and perform denial-of-service attacks. Instead of trying to fully compromise banking web apps, attackers are focusing on vulnerabilities in application logic in order to:

- Get a more advantageous exchange rate, transfer funds from client accounts, or avoid fees.
- Obtain as much information about bank clients as possible for social engineering attacks.
- Overload the system and cause denial of service.

We expect banks to pay more attention to eliminating logical vulnerabilities in 2021.

Security of banking infrastructure

Financial institutions are still poorly protected from APT attacks. Attackers are successfully actuating the most dangerous business risks by accessing bank workstations, ATM management systems, and card processing systems. In 2020, Positive Technologies pentesters



We will most likely encounter attacks by known groups that conceal their attacks by using multiple techniques for penetrating and gaining persistence, refine their malware, and vary the regions they target



regularly helped banks to verify business risks by emulating attacker actions, and each time they were successful (with an average of three to five business risks confirmed at each bank).

When the internal attacker model was used, our pentesters managed to obtain maximum privileges on infrastructure in 100 percent of cases and demonstrate the feasibility of business risks. These risks refer to unacceptable events defined jointly with our clients in advance, such as unauthorized access to critical systems, including bank workstations, SWIFT terminals, ATM network, and processing center, depending on the particular bank.

In some cases, our experts did not act as internal attackers. Instead, they used the external attacker model, in which a pentester does not have pre-existing access or any privileges on the tested systems—just a “person off the street.” Yet even in these cases, our testers still managed to breach the perimeter, obtain maximum privileges, and trigger key business risks.

Problems of new financial technologies

Modern financial technologies—hyperlinked payments, QR codes, digital currencies, biometrics, and the latest web technologies—all have their advantages and disadvantages.



❑ Anti-fraud flaws

Automation errors and related risks are the bane of modern anti-fraud solutions. Algorithms designed to spot unusual transactions can sometimes flag legitimate purchases by accident. Widespread automation, aided by big data, should reduce false positives and let legitimate payments go through. But eliminating false positives entirely will be a tall order.

The more banks try to protect their clients, the more inconvenience they are liable to cause. Any automated system has to make trade-offs. An algorithm for identifying fraudulent transactions can be strict, which will catch more suspicious transactions but also block legitimate payments more often. Conversely, a "looser" algorithm reduces client hassle but will leave more fraudulent payments undetected. The challenge will be to find the delicate balance between security, frictionless convenience, and business requirements.

❑ Blockchain risks

Blockchains, as a distributed ledger that makes payments transparent at every step, have the potential to streamline the payment process. In such systems, the weakest point is client access to the payment system and digital wallet itself. Even a supersecure blockchain cannot stop hacks that target a web interface or the client's device.

Businesses are curious about smart contracts—instead of a wall of legal text, they

comprise a self-executing algorithm that automatically verifies whether each side has fulfilled its obligations. However, these algorithms are written by people, and people make mistakes. The code of a smart contract can have errors and even backdoors, which opens a new chapter in the history of financial fraud. Having the text of an agreement contain "vulnerabilities" is a new problem for the industry. Learning how to find such vulnerabilities in smart contracts and preventing related types of fraud will be vital.

Distributed ledgers also have implications for fraud. Rolling back a single ledger transaction is not possible because this would also affect legitimate transactions that happened to be occurring at the same time. Authenticating transactions is key for digital currencies, which is why each transaction must be signed cryptographically. At the national level, it will become important to implement domestically devised cryptographic algorithms in the software used for digital money and smart contracts.

Businesses and regulators should combine efforts to facilitate successful implementation of smart contracts and distributed ledgers. Doing so will take effort and commitment.

❑ Mobile phones and money

Reliance on mobile phones carries additional risks. Perhaps the most obvious of these is SIM swapping, in which a fraudster

Automation errors and related risks are the bane of modern anti-fraud solutions



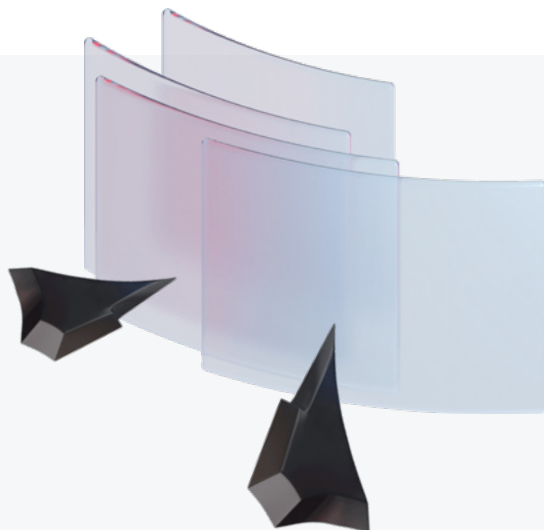
impersonates a bank client to obtain a "replacement" SIM card in order to change the password for the client's bank account. Another is exploitation of vulnerabilities in financial applications, which make it possible to link any phone number to an attacker-specified account. Funds sent to that phone number will then be received by the attacker. And attackers keep inventing new techniques all the time.

Biometric identification is becoming popular, but also creates serious risks. Iris and fingerprint recognition are regarded as highly reliable, for example, thanks to their low error rate. However, these are not the same biometric methods used for remote identification, such as facial recognition and voice recordings. Those methods are not nearly as reliable. Attackers could use

deepfakes to automatically generate images and voices that successfully pass biometric identification.

Moreover, practice shows that even robust identification will not stop attackers, who instead bypass such mechanisms entirely by taking advantage of social engineering or vulnerabilities in payment applications.

Unfortunately, many initiatives by the banking sector to limit fraud, such as creating a central database of SIM cards or placing per-transaction limits on rapid payments, have received pushback from clients. Overcoming this attitude and teaching users basic digital hygiene will be a serious challenge for the banking community around the world in coming years.



Even a supersecure blockchain cannot stop hacks that target a web interface or the client's device



Cyber-ranges: stresstesting bank security


Simulated cyberattacks at The Standoff in November 2020 tested the security of digital replicas of the infrastructure of real companies. Among the companies modeled on the cyber-range was a digital bank.

Attackers tried their hand at triggering a number of business risks:

- Disrupting transaction processing
- Stealing money from client bank accounts or cards
- Stealing personal data of bank employees and clients

As a result, the attackers triggered half of the total designated risks:

- They transferred money from client cards to attacker-controlled accounts.
- Obtained access to personal data of bank employees and online banking clients.



Almost all attacks (except one attack conducted in the closing minutes of the contest) were detected and investigated by defenders. The Standoff is an ideal opportunity for security specialists to gain experience and boost their professional skills.

The business risks modeled at The Standoff are highly relevant to financial organizations. In penetration tests at financial organizations, our experts managed to obtain maximum privileges on corporate infrastructure in 100 percent of cases. In some cases, the experts also checked whether potential attackers would be able to steal funds; all such attempts were successful. Security assessments of mobile banking systems also revealed security problems: in half of mobile banking apps, hackers could perform fraud and steal money.



Alexander Popov

Lead OS and Hardware Security
Researcher, Positive Technologies

Security of operating systems

2020 was very productive for operating system security. A number of important developments made for an eventful year. Fortunately, the pessimists were wrong and the pandemic did not slow down the development of system software. In their annual reports, both the Linux Foundation¹ and GitHub² even noted growing open-source engagement.

Operating system security continues to be an important area for innovation. There can be no easy one-size-fits-all solutions. Thoughtful and comprehensive approaches are required. Three main vectors point the way forward for improving the security of operating systems.

One: secure processes for software development. The operating system cannot be secure if the development process does not include



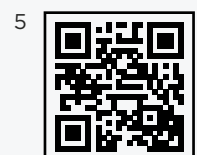
cross-review, fuzzing, static analysis, and control over the software supply chain.

Two: developing and implementing OS mechanisms that increase the difficulty of vulnerability exploitation. If an attacker wants to exploit an error in the OS kernel, we can frustrate that attempt as much as possible.

And three: new hardware technologies for eliminating entire classes of OS vulnerabilities. These tools include ARM Pointer Authentication Code (PAC), ARM Memory Tagging Extension (MTE), and Intel Control-flow Enforcement Technology (CET). The relationships between these and other technologies, vulnerability classes, and exploitation techniques can be seen in the Linux Kernel Defence Map that I have developed.³

A good example of a comprehensive approach to OS security is the recently published Android Security Model (the second version was released in December 2020⁴). System security is guided by the threat model. Each component of security is chosen intentionally and helps to mitigate a certain threat.

At the same time, 2020 proved that OS security still has a long way to go. Google Project Zero published an analysis of a complex malware system that used a chain of zero-day vulnerabilities.⁵ Serious malware is a high-quality product that has a modular architecture, command and control, and swappable components with exploits. As defenders, we should never underestimate attackers. Developing effective security tools requires that we look at OS security from an attacker's viewpoint.





Mark Ermolov

Lead OS and Hardware Security
Researcher, Positive Technologies

Hardware vulnerabilities

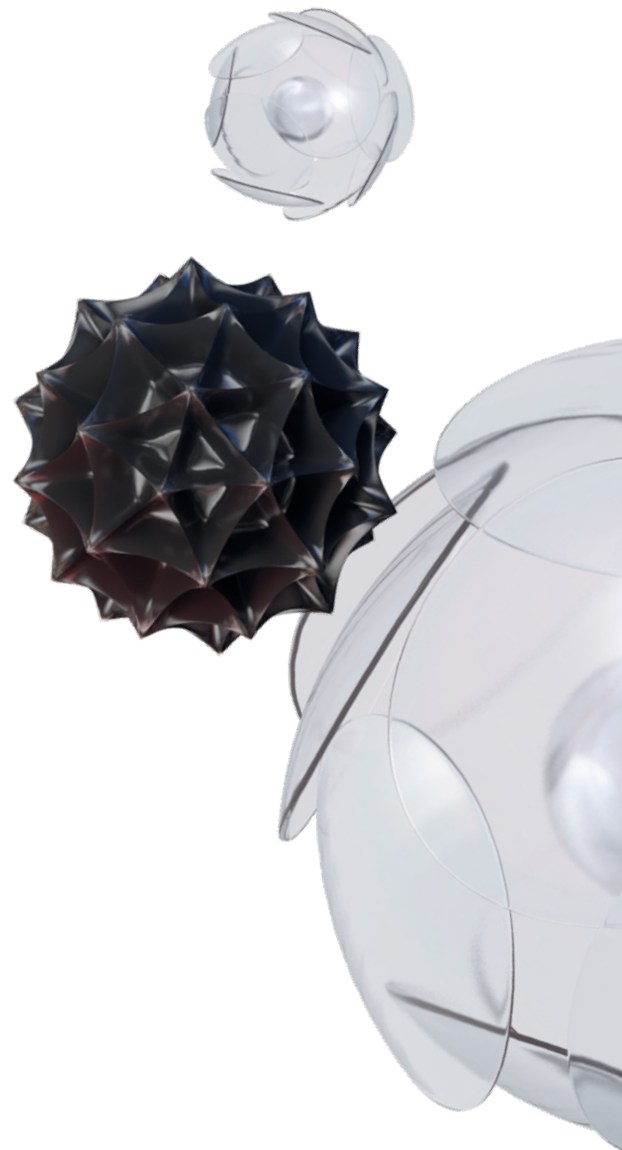
In 2020 we saw a softening of activity in information security and especially hardware security. I reckon this is because all the conferences went online and the number of participants declined sharply. However, it's not as if security experts stopped studying hardware vulnerabilities. If anything, right now is the lull before the storm. Researchers tend to keep their discoveries quiet, in order to make a show of them at upcoming conferences. In 2020, researchers were finally able to do pure research without having to spend time making slide decks or otherwise preparing for talks. The curtain will be sure to lift soon.



Exconfidential Lake, a recent major leak of confidential data related to Intel platforms, has spurred interest

So we should expect to see a surge of hardware vulnerabilities. A recent major leak of confidential data related to Intel platforms (Exconfidential Lake) has spurred interest. It was certainly a unique event: the public gained access to software emulators for new Intel platforms that were not yet on the market, which allowed researchers to look for vulnerabilities in firmware without even having to purchase the real thing. Researchers gained a head start by having the opportunity to study hardware long before release. This means that 2021 will likely bring plenty of discoveries of vulnerabilities in Intel firmware and hardware. Of course, the legality of using the leaked information is a separate issue. Researchers will hardly advertise the use of illegally obtained data or mention this in their articles. However, the bottom line is that researchers have become able to analyze many of the inner workings of Intel products for the first time. This leak is a vivid example of why security through obscurity does not work. I'm sure that soon we will reap the sad rewards of decisions made at some point by industry leaders. Unfixable hardware vulnerabilities and architecture flaws that can only be addressed in new products will hurt end users and, ultimately, vendor credibility.

We should expect to see a surge of hardware vulnerabilities





Nikolay Anisenya

Head of Mobile Application
Security, Positive Technologies

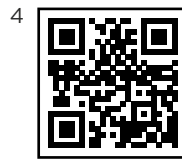
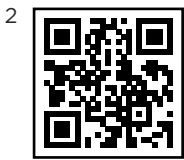
Mobile security

In 2020 the world slowed down just a bit, which affected even the virtual world of IT, and especially mobile applications. We had to learn to live in a new way. In spite of that, some exciting developments happened in mobile security.

The slogan of last spring was "Stay home." This was the message from leaders in most countries. Business also had to adjust and shift to being at home wherever possible. Remote work has raised questions of supervision, communication, and security. There are 10 billion personal mobile devices in the world, with two thirds of users combining personal enjoyment with work on their devices.¹ Clearly, many people use more than one device for work, and in most cases the second device is a smartphone. And now, with working from home becoming the new standard, these numbers have only increased.

¹





Desktop operating systems make it easier for system administrators to protect desktop PCs and laptops: security software can be run with superuser privileges, while employees use accounts with only the privileges needed to do their jobs. But mobile devices are a different story. Popular mobile operating systems do not support privileged processes, leaving system administrators to rely on OS tools for mobile device management (MDM).

Privacy protection

There is also the question of privacy. Whether your smartphone belongs to you or your employer is not so important. In either case, you can still install non-work apps. Users have an average of 67 apps on their phones, which raises security concerns.²

With iOS 14, Apple introduced a number of important features intended to protect user privacy. For instance, app permissions now distinguish precise location from approximate location. Users can select which one they want to share with apps. Also, if an app wants to track users, it must explicitly ask for permission. And finally, a new banner alert informs when an application is pasting from the clipboard (and therefore can read data you copied). In the first days after the release of iOS 14, dozens of popular applications were accused of spying on users.³ Given that people tend to use their smartphones

for remote work, such incidents may become a serious threat to corporate security. On the part of Apple, it was a major step towards increasing app transparency.

However, privacy should concern both business and ordinary cyberdenizens. Google and Apple, the two major mobile OS developers, meant well when creating the Exposure Notifications System—an API used to trace contacts with people infected by the coronavirus.⁴ It has long been available in the latest versions of Android and iOS. However, like any technology, the Exposure Notification API can also be used in harmful ways: instead of tracing those who have been infected, the API can allow potential attackers to create a map of the user's movements.⁵ This is a good example of how new solutions can cause new problems, new questions, and—for security experts—new challenges.

Incidentally, these concerns do not apply to the owners of Huawei devices, which do not have this API. In 2020, Huawei moved from words to action as it started to abandon Google services and shift to the company's self-developed HarmonyOS 2.0 operating system. The first HarmonyOS 2.0 smartphones are expected to hit the market this year. It looks like the two mobile OS giants will have to make room for a newcomer. As for us, meanwhile, we will continue monitoring industry changes and contributing to the security of mobile apps.



Alexandra Murzina

Lead Advanced Technologies
Specialist, Application Security
Research, Positive Technologies

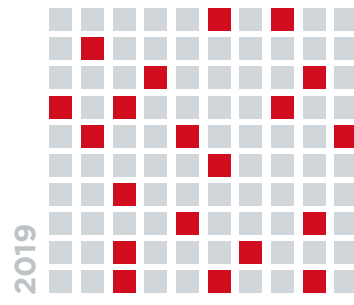
Security and AI

Machine learning in information security long ago stopped being "rocket science." It has matured nicely with certain methods and solutions for approaching typical tasks. There are both advantages and pitfalls of using AI for analysis, quick response, and protection. The best option is to combine traditional techniques with the latest inventions.

According to the Capgemini Research Institute, nearly two thirds of companies surveyed in 2019 think that AI will help to identify critical threats.¹ And 69 percent believe that AI will be essential for quickly responding to cyber-attacks. In 2019, only one in five organizations used AI. However, in 2020, this figure increased to almost two out of three.



20%
of organizations



2019

use AI

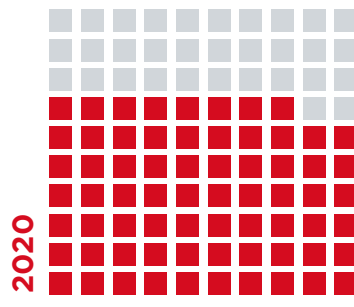
AI has huge potential for strengthening cybersecurity. It can analyze user behavior, deduce patterns, and spot anomalies. Network vulnerabilities can be spotted quickly. AI can also help to automate routine security operations, letting teams focus on tasks requiring more human involvement and judgment. Companies can use AI to speed up malware detection.

AI is being increasingly used in areas outside IT. AI techniques, especially machine learning, require large amounts of data. Big data can help to improve products, but it can also be used to analyze user behavior for profit.

Finding and hiring a security expert or data scientist is already hard enough. The number of pros who know both fields is smaller still. Security is getting more and more difficult, because developers either do not know about the possible risks or prefer to put off dealing with them until only after a product is released. The consequences can be dangerous. In Q1 2020 alone, large-scale data breaches increased by 273 percent.²

At the same time, AI itself is code that can be vulnerable and create risks. In fall 2020, MITRE and Microsoft released a threat matrix for machine learning systems.³ In addition to Microsoft, 16 research groups took part in the project. The risks, having been verified on machine learning

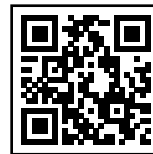
2/3
of organizations



2020

use AI

2



3





AI itself is code that can be vulnerable and create risks

(ML) systems, are more than just theoretical. The resulting matrix resembles the ATT&CK matrix already familiar to researchers. Some of the risks are ML-specific. Others are characteristic of software in general but, because of residing in the software projects in which ML is used, may affect it indirectly.

Speaking about AI as a tool for attacks, it is important to mention deepfakes incorporating powerful face- and voice-swapping techniques. Making convincing fakes is no longer difficult. There are many examples and trained machine learning models available on the Internet. App stores offer a variety of programs that allow ordinary users to swap faces and achieve very realistic results. In 2019, criminals used AI-based software to steal €220,000.⁴ In 2021, fraudsters made easy money by copying the face of neuroscience popularizer and Dbrain founder Dmitry Matskevich for a deepfaked announcement inviting users to join a blockchain platform.⁵

On the one hand, the few AI security incidents to date hardly merit an all-hands-on-deck response. On the other hand, cases involving major companies (including Google,⁶ Amazon,⁷ and Tesla⁸) have become a wake-up call for researchers and the whole IT industry to take the issue seriously. Overall we see a trend toward improved awareness regarding AI security, as well as development and implementation of better approaches.



7



8



Custom hacking services

Yana Yurakova,
Vadim Solovyev

Information Security Analytics,
Positive Technologies



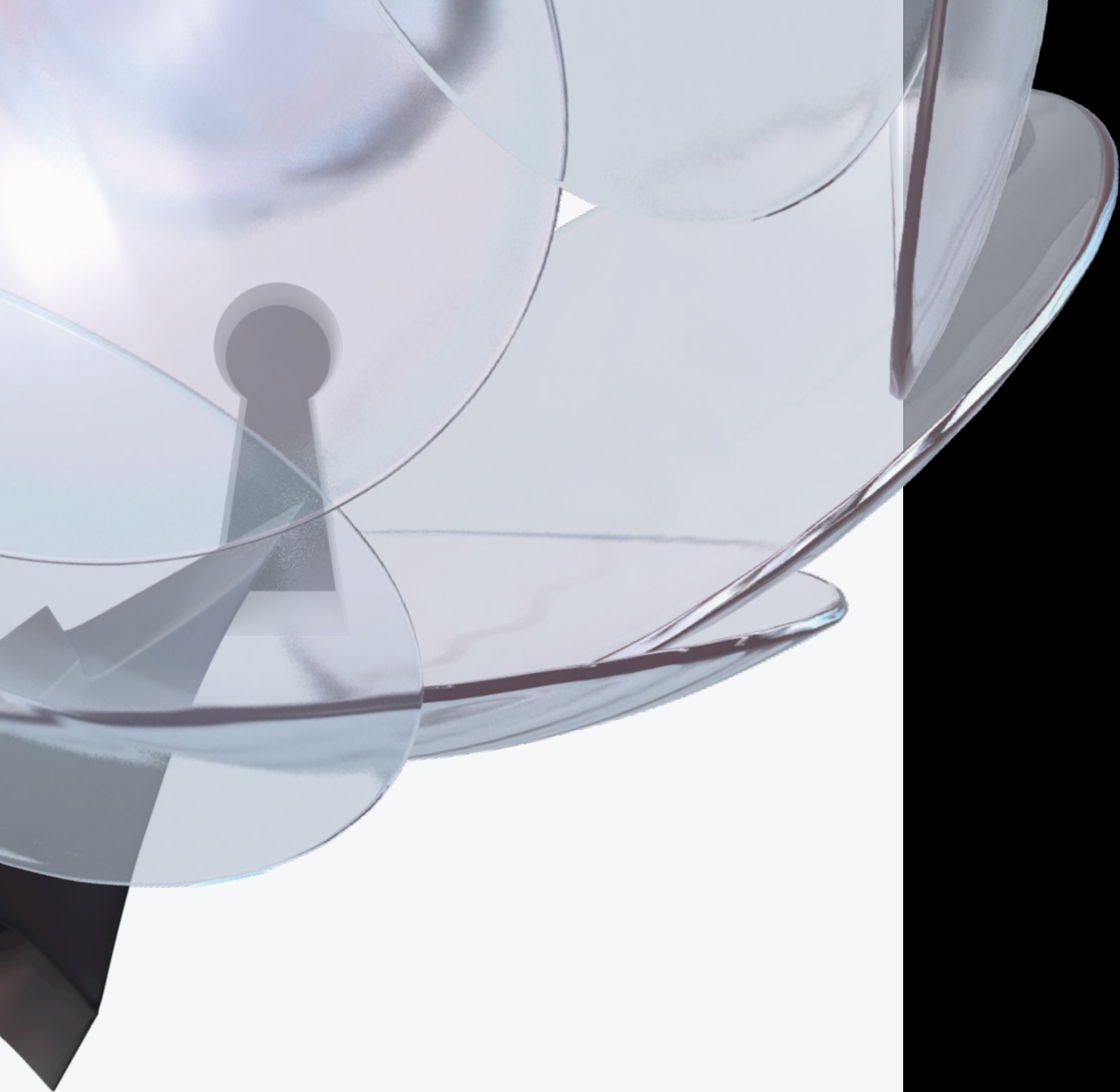
25 min
to read this article

Many businesses make active and productive use of corporate sites, online stores, and web services. Customers register on these websites by leaving their personal data, make purchases by entering credit card information, and use cloud services to store information or use the resources provided to send their sensitive information. It is obvious that not only competitors, but also cybercriminals, would like to have access to such precious data, so it is no surprise when clients' personal data makes its way from yet another big company into the hands of criminals. Often, these events are associated with a successful attack on a company's web applications, as a result of which attackers gain access to the user database or steal other information. For example, in September 2020, hackers broke into more than 2,800 Magento-based online stores where they injected a malicious script

to scrape customers' personal information and payment card data.¹

As a result of hacking, both users and companies themselves may be affected. Web application security analysis by Positive Technologies shows that criminals can attack clients in 92 percent of web applications; in 68 percent of cases, there is a danger of a data breach; and in 16 percent of cases, attackers can gain control over the application and the server OS.²

We selected the ten most active forums on the dark web³ that offer services for hacking websites, buying and selling databases, and accessing web resources. In this article, we will talk about why criminals hack websites, and what consequences there may be for the owners and users of hacked resources.⁴



1

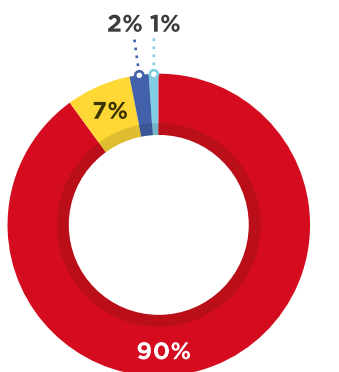
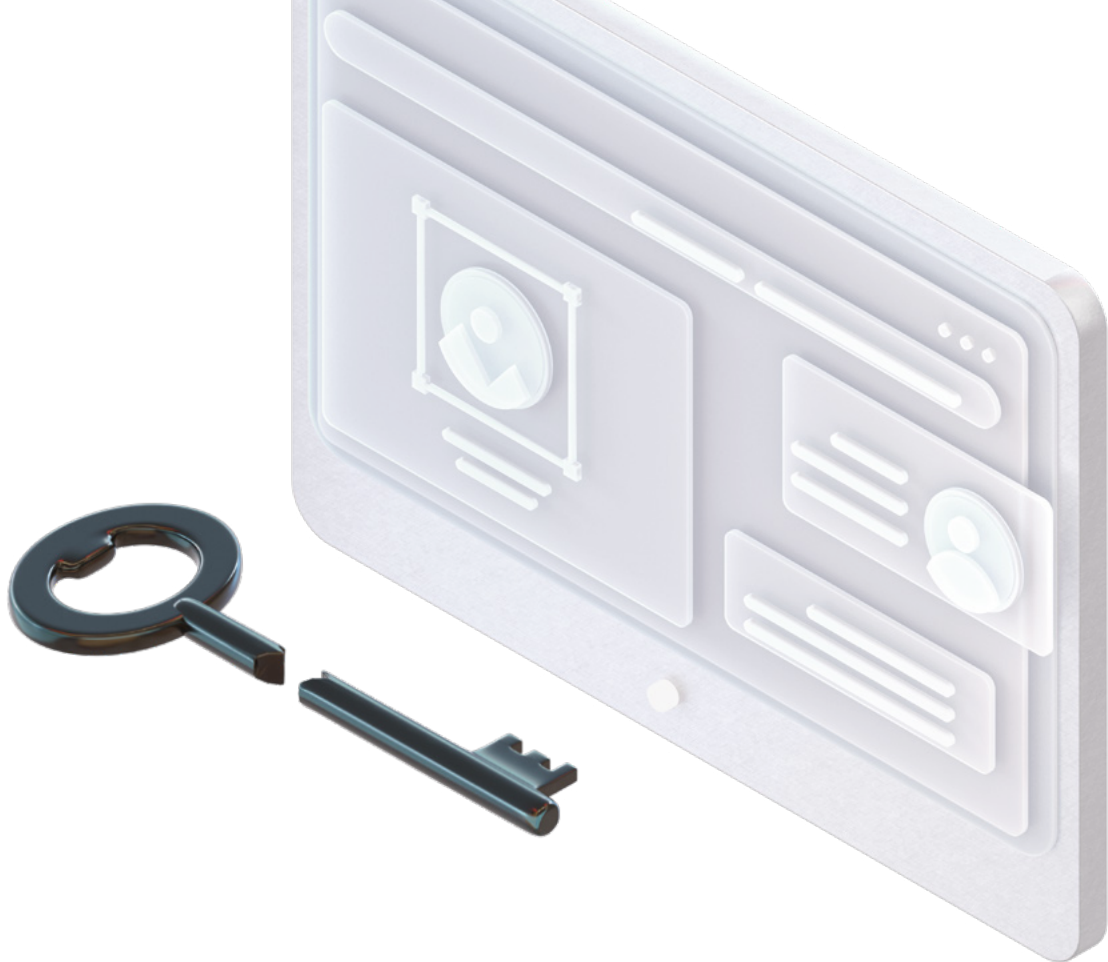


2



3 In total, more than 8 million users are registered on these forums, more than 7 million topics have been created, and more than 80 million messages have been published.

4 For the purposes of this research, we did not include advertisements for DDoS attacks against websites.



- Buying hacking services
- Selling hacking services
- Selling hacking tools and programs
- Searching for accomplices

Figure 1. Categories of inquiries related to hacking websites

Why criminals hack websites

In 90 percent of cases, users of dark web hacking forums search for a hacker who can provide them with access to a particular resource or who can download a user database. Seven percent of the messages include offers to hack websites. The rest of the messages are aimed at promoting hacking tools and programs and finding like-minded people to share hacking experience.

By "offers," we mean ads published by service owners and hacker groups. They cannot act as indicators of supply and demand, as they are often posted only once. Our only way to estimate demand for services is to look at individual inquiries from users who, for various reasons, did not make use of the information about the offers.

Since March 2020, we have noticed a surge of interest in website hacking. This might have been caused by an increase in the number of companies available via the Internet, which was triggered by the COVID-19 pandemic. Organizations that previously worked offline were forced to go online in order to maintain their customers and profits, and cybercriminals, naturally, took advantage of this situation.

Figure 2 shows the number of new ads on dark web forums. Ads are posted not only by new members, but also by hackers with an established reputation. The latter do this as a form of self-promotion. It is difficult to determine which ads are duplicates and which have lost relevance, so we do not give the number of hackers or groups that actively provided hacking services at the beginning of 2019 or who are doing it today.

In about seven out of ten inquiries related to website hacking, the main goal is to gain access to a web resource. Not only can attackers steal sensitive information, but also sell access to web applications to so-called fences.

Inquiries aimed at obtaining user or client databases from a targeted resource account for 21 percent of all ads. Competitors

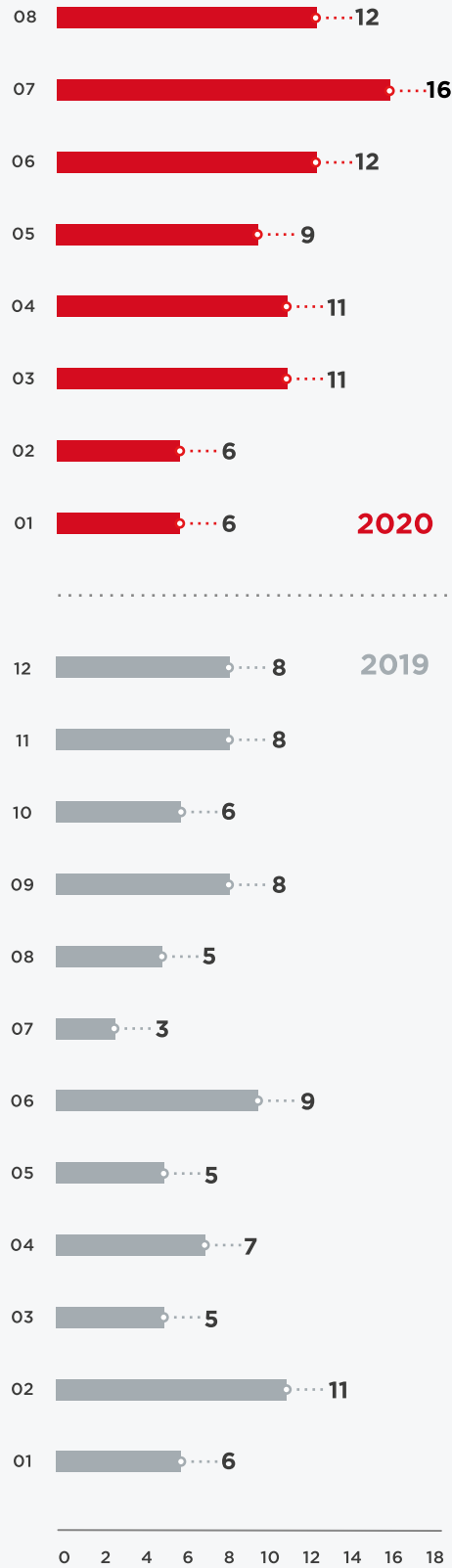


Figure 2. Number of new ads related to hacking web resources on forums in 2019-2020

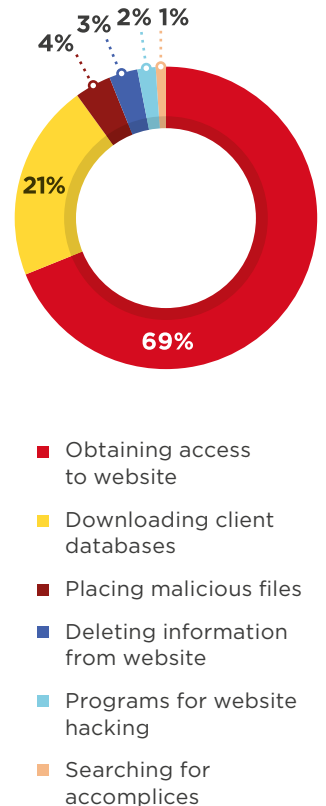


Figure 3. Distribution of inquiries by topic

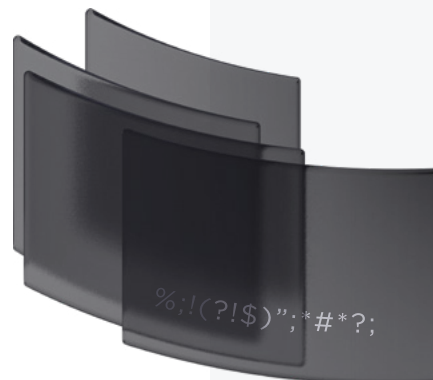
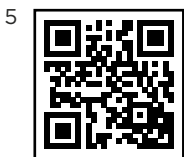
and spammers who collect lists of addresses for targeted phishing attacks aimed at a specific audience are primarily interested in acquiring this type of information (figure 4, figure 5).

In 4 percent of inquiries, the main goal of attackers is not to hack the website, but to inject malicious programs into it, for example, for conducting watering hole attacks or placing web skimmers.

In August 2020, during one of its campaigns aimed at scientists from the universities of Haifa and Tel Aviv, the APT group Charming Kitten hacked the Deutsche Welle website in order to place a malicious link on it. After clicking this link, the victim was asked to pass authorization, and the credentials they entered were sent to the attackers.⁵

Three percent of ads are aimed at finding a person who can hack a website and delete certain data specified by the customer. This service may be in demand among those who want to remove negative reviews about a company posted on resources not controlled by that company, as shown in the following example (figure 7).

Offers for the sale of ready-made programs and hacking scripts were found in 2 percent of the analyzed inquiries.



Watering hole attack

This kind of attack starts with determining which websites are frequently visited by potential victims (such as employees of a company of interest). The attackers then compromise these websites and place malware on them. When victims subsequently visit these websites, malware may be downloaded to their devices



Web skimmer

Malicious code injected into a page on a hacked site where the user enters payment card information, with the purpose of stealing such information

break the site 10k \$
 By [redacted], [redacted] in [Job] - search, execution of work

Start new topic Reply to this topic

Posted March 1 (edited) Report post

there is a corporate website, all services are available only after authorization.
 there are a couple of accounts for access inside.
 there are many different services inside (such as chats, forums, file hosting, etc.)
 all accounts are delimited by access levels: everyone has access to their information.
 tasks:
 1) get access to other (not accessible by rights) information and merge it - 5k \$
 2) merge the database of all users (and password hashes) and, if possible, webshell - 7k \$
 3) root - 10k \$
 4) if you get something from the list, there will be further tasks for promotion - we will discuss the price.

I think the hack is quite real - since the site is crooked and was clearly written by coders for internal needs, there is no protection as such.
 I ask for contacts (jaber in PM), I work with pleasure through a guarantor,

Paid registration
 30 posts
 Joined
 Activity
 other / other

Figure 4. Custom website hacking

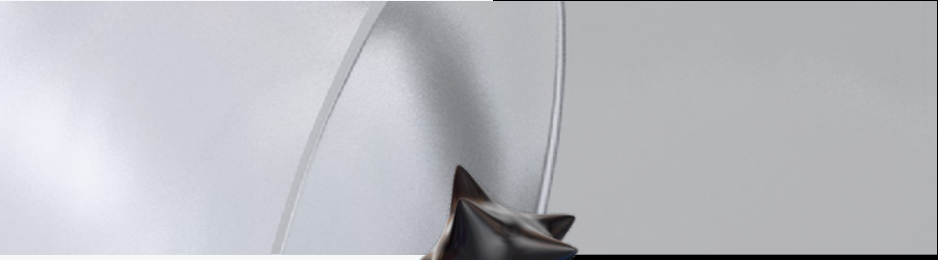


Figure 5. Collecting information from competitors' websites

=== We need a service to "pull" applications from competitors' sites ===

I'm interested in the service of submitting applications from competitors' websites, work only through trusted people or a guarantor. Websites are mostly one-page type. We will discuss the details in the PM.



need a site hacker \$ 2000
 By [redacted], [redacted] in [Job] - search, execution of work

Posted [redacted]

byte

I'm looking for a site and server hacker to hack into this site:
[https://\[redacted\]](https://[redacted])
 I found most of the emails of people who have access to this site.
 I'm looking for Isat questions and answers

I am looking for a person who will hack the site and delete the topic or delete comments

Mar 1, 2020

Watch

Mar 1, 2020

Hello, I am looking for a person to hack this site

Figure 6. Search for a website hacker

Figure 7. Ad seeking a hacker

Some hack, and some buy


We noted the appearance on the dark web of fences buying and selling access to websites.⁶ Now that this phenomenon has taken root, we can categorize cases by type. In some cases, users buy web shells, some buy access to the administration interfaces of websites, and others buy ready-made exploits for injecting SQL code into specific resources.

Web shells are inexpensive relative to, say, databases, which we will talk about later: their prices range from a few cents to \$1,000. This is mainly due to the fact that the privileges obtained by uploading the web shell to the file system are limited. Selling a web shell means sending the customer a link to the file path and, possibly,

credentials for authorization. The most common web shells are on websites in the .com domain zone—they account for 54.3 percent of the offers for sale.

Fences, first of all, have to keep track of what is appealing to their customers. It is difficult to infer which industries have access sold or bought most often, but we can safely say that access to online stores is in its own category. Demand for it is consistently high: this is due to the fact that when paying online, users enter their credit card details. Thus, attackers can inject malicious JavaScript code into the website to intercept the information entered by the user and use it for their personal gain. Another way to cash in on

Figure 8. Ad for purchasing access to online stores



[PURCHASE] [SNIFF FOR%] accesses [Shops] [Best prices on the market]

By [redacted], [redacted] in [Access] - FTP, shells, root, sql-inj, DB, Servers

1 2 3 4 five 6 NEXT » Page 1 of 8

Posted [redacted]

I will purchase your access to shops.
Requirements:
Number of orders: **5+ (per day)**
Rights: **any**
Countries: **any (except for the countries of the Soviet bloc)**
Payment: **With the form of payment on the site**
Reward: **\$ 300 - \$ 20,000**
Note: The price of each shell is considered individually.
Regular partners - good prices +%.
I have the best prices on the market, no one will give you more than me.
Example:
US - 15 orders daily / 1000-2000 \$ (minimum price)

Seller
21
280 posts
Joined
Activity

6





A web shell

is a file uploaded to a server that an attacker can use to execute OS commands on that server through the web interface and gain access to other files.

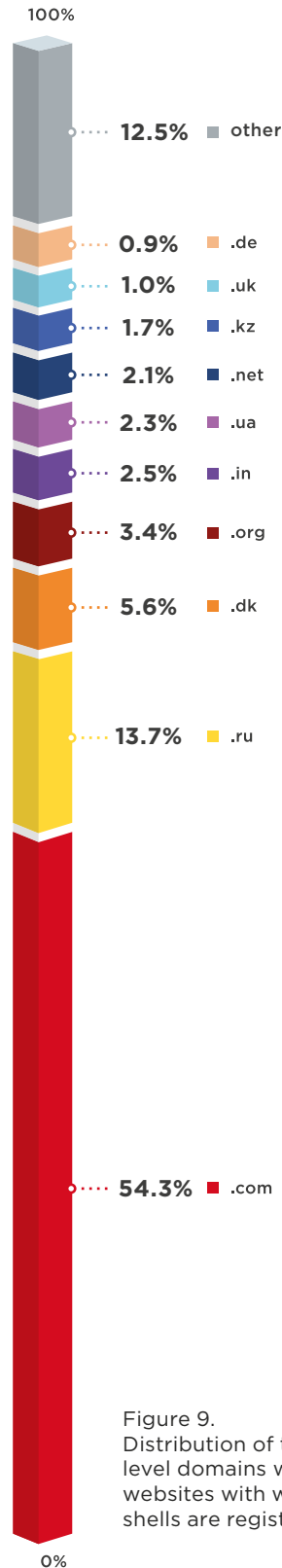
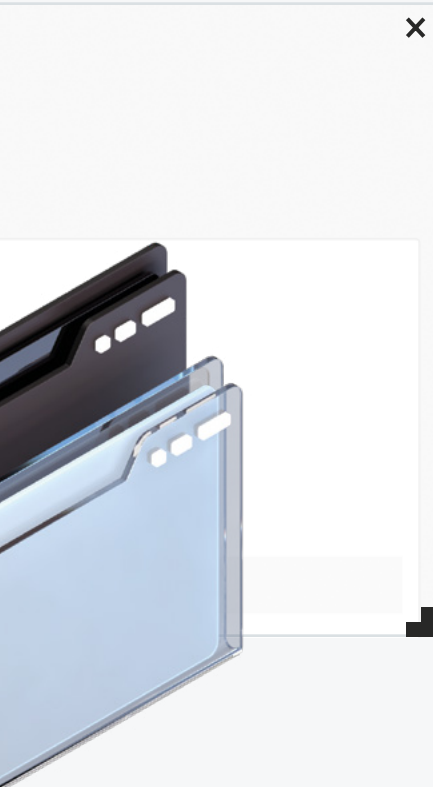
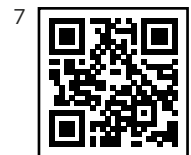


Figure 9. Distribution of top-level domains where websites with web shells are registered

users is to obtain privileged access to an online store, then place orders using other people's cards, or not pay at all. Prices for access to online stores range between \$50 and \$2,000.

If the web service is hosted on a server connected to the company's internal network, the main risk for the organization is that an attacker (or someone who buys access to the server through a web shell) can develop an attack and penetrate the company's infrastructure. The results of external pentests conducted by Positive Technologies experts in 2019 show that at 86 percent of companies there is at least one vector for penetration into the local network associated with insufficient protection of web applications.⁷ At one out of every six tested companies, we found traces of prior attacks. For instance, we found web shells on the network perimeter, malicious links on official sites, or valid credentials in public data dumps.



Attackers use access to the administration web interfaces of popular CMSs in order to place web shells and malware on them and use them for illegal advertising. For example, in August and September 2020, a series of attacks were observed targeting the websites of the WHO, UNESCO,⁸ government agencies (such as the National Institutes of Health), and major educational institutions.⁹ On these resources, hackers posted phishing ads for tools used to hack accounts on well-known social networks and for cheating in online games. They had two goals: stealing payment card data and spreading malware. Some users were redirected to a payment page where they were asked to enter their card information, while others immediately downloaded malware to their devices.

It is worth noting that a website's involvement in illegal advertising campaigns may damage its position in the search results of popular search engines.

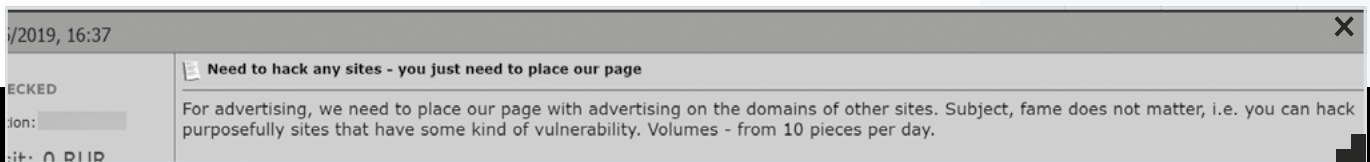


Figure 10. Search for a hacker to place ads



User databases

Dumps, or databases from hacked websites, can be bought by competitors or criminals who plan targeted phishing attacks (figure 11).

Custom-hacked databases cost between \$100 and \$20,000, or between \$5 and \$50 per 1,000 entries.

User entries may, for example, contain the following information: username, email address, full name, phone number, address of residence, social security number, and date of birth. This information can be used in social engineering attacks.

I am looking for someone who can open the site.

by [redacted] · Jul 8, 2020

Watch

Jul 8, 2020

There is a website.
The task is to pull out the database, extract email: password from it.
Password to decrypt to the maximum. Payment from 1000 \$ and further by agreement.
We agree to the guarantor, further details in the PM on the forum or in the cart @ [redacted]

Figure 11. Ad for a website hacker

Ad Title	Category	Author	Date	Replies	Views	Last Post
2020 DB & Combos 110 Million Lines !!	SELLING	[redacted]	July 17, 2020 at 04:17 PM	4	805	August 04, 2020 at 11:48 AM
FB Database	BUYING	[redacted]	August 04, 2020 at 08:18 AM	1	336	August 04, 2020 at 09:22 AM
Buying Japanese Gaming databases	BUYING	[redacted]	July 21, 2020 at 07:18 PM	2	398	August 04, 2020 at 07:19 AM
AT&T 63K PHISHED ACCOUNTS FRESH	SELLING	[redacted]	August 03, 2020 at 09:47 AM	7	678	August 04, 2020 at 06:45 AM
Buying high quality data and combos. Can pay high looking for long term business!	BUYING	[redacted]	August 04, 2020 at 12:21 AM	0	256	August 04, 2020 at 12:21 AM
Big DB Collection	SELLING	[redacted]	May 16, 2020 at 12:50 PM	7	1,638	August 03, 2020 at 06:11 PM
Fresh, hq antipublic @	BUYING	[redacted]	August 03, 2020 at 04:17 PM	0	445	August 03, 2020 at 04:17 PM

Figure 12. Ads for the sale of accounts obtained through phishing

Is it difficult to hack a website?

Our web application security analysis revealed that, on average, each web application has 4 high-severity and 12 medium-severity vulnerabilities.¹⁰ Even if we do not take into account the large number of vulnerabilities, criminals can use social engineering techniques to conduct attacks, such as targeted phishing campaigns, on a resource administrator in order to obtain their username and password. These credentials allow attackers to access the company's website.

Based on our research data, we can conclude that most web resources are not sufficiently protected from intruders. The number of ads on the dark web offering services for hacking web resources should also be taken into account. If required, criminals can easily hire an experienced hacker or buy a ready-made hacking tool.

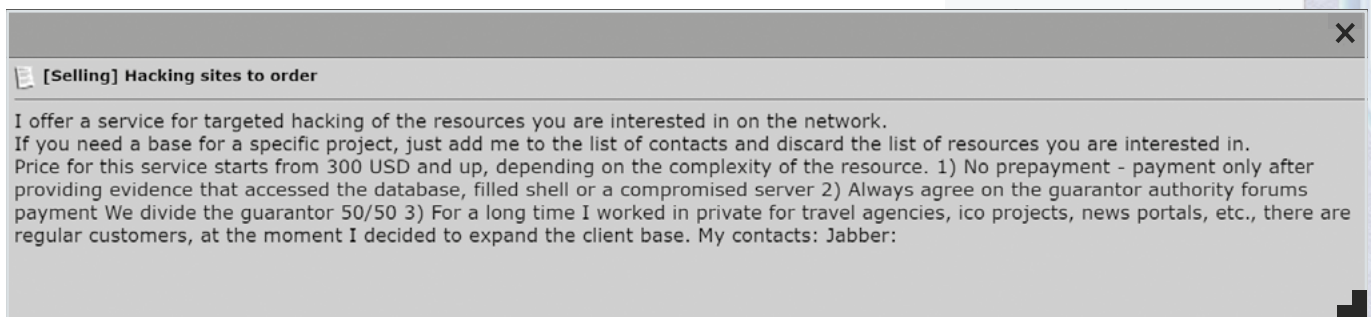
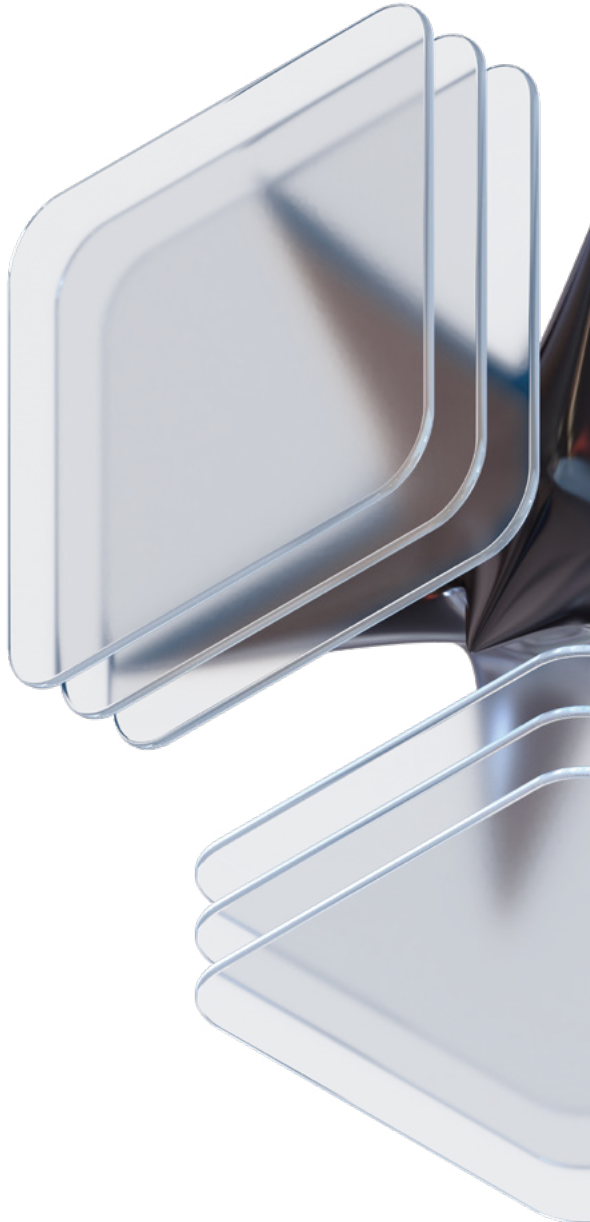


Figure 13. Ad for custom website hacking



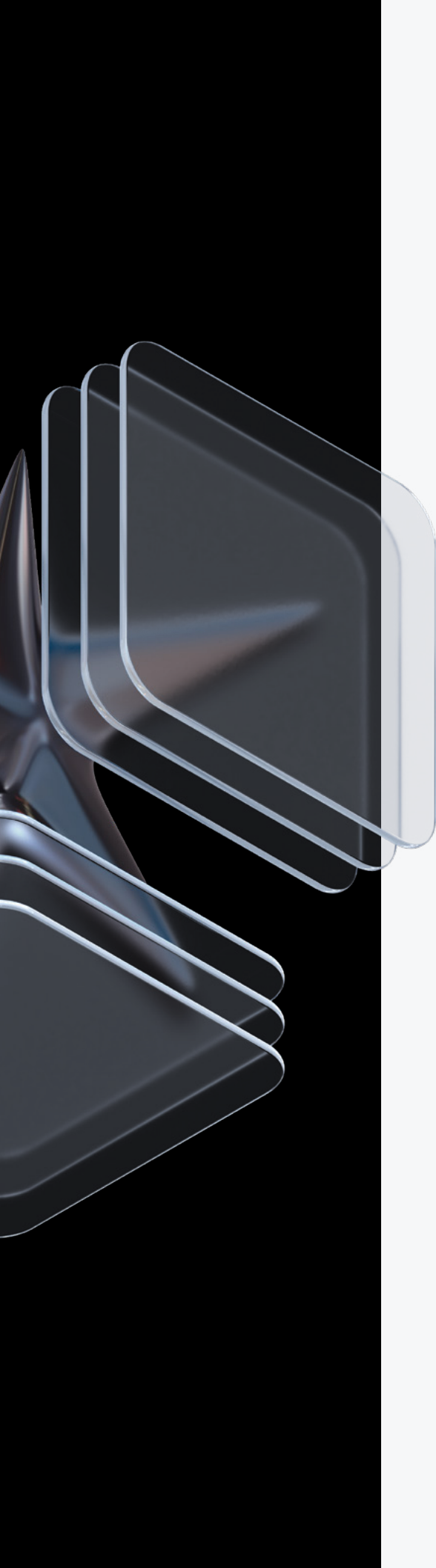




Conclusions and recommendations

Web application hacking services are in high demand. Ads for custom website hacking are not exclusive to any one industry; however, most customers purchasing such services are interested in online stores. This is primarily due to the fact that users of these resources enter their personal data and credit card information there. We believe that there is a definite trend towards a further increase in demand, as more and more companies go online as a result of the COVID-19 pandemic.

Hacking a company's web applications can lead to global consequences: from data breaches and penalties for non-compliance (such as violation of the GDPR) to penetrating the company's local network and using its resources in subsequent attacks—as a platform for spreading malware or for storing tools that will be downloaded during



There is a definite trend towards a further increase in demand, as more and more companies go online as a result of the COVID-19 pandemic



the attack. When building a security system, we recommend following a risk-oriented approach, based on an understanding of the magnitude of negative consequences that are acceptable for your company. It will be easier and cheaper to proactively protect the most vulnerable part of your company's network than to pay huge fines and have your company's reputation ruined.

To protect your company, you should adhere to secure development practices and use automated source code analysis tools to search for errors and vulnerabilities, since web application security analysis in 2019 revealed that 82 percent of all vulnerabilities are found in web application code. It is essential to regularly analyze your web application security and to use a web application firewall for proactive protection against attacks.



Cyber-risks: proving dangers and defining criteria



2000
Brazil

Accident at Petrobras refinery



2009
Russia

Accident at Sayano-Shushenskaya hydroelectric power station



2019
China

Explosion at chemical plant



2020
Russia

Accident at heat and power plant in Norilsk

A company's management can build an impeccable strategy, develop sound business plans, and meet all KPIs—just to see it all slip out of control the moment a business risk strikes. Any business risk is a problem with the potential to cause financial and sometimes even human losses.

Let's take a look at several real-life examples from the industrial sector when business risks led to dreadful consequences.

Olga Zinenko

Information Security Analytics,
Positive Technologies



10 min

to read this article

Oil spill (1.3 million liters)

Cleanup costs:
more than \$100 million



75 people killed, 13 injured

Damage: more than 40 billion rubles (**\$1.3 billion** at then-current exchange rates), including environmental harm. **Criminal charges** brought against seven executives and engineers



78 people killed, over 600 injured

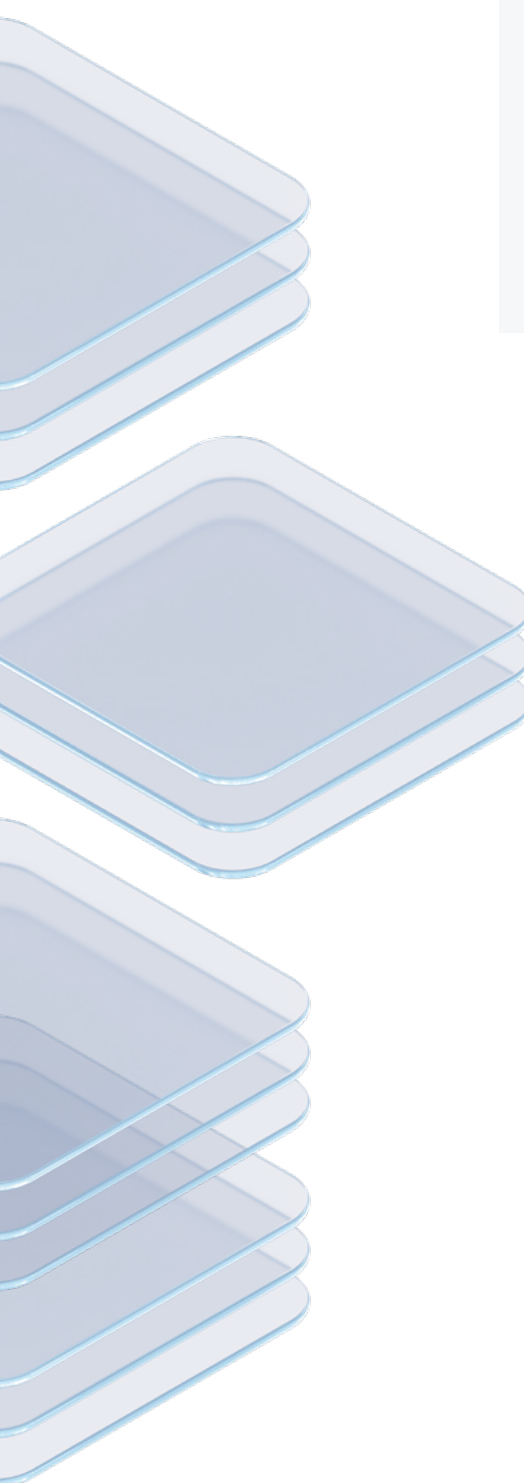
Direct economic losses:
approximately **\$280 million**



Diesel spill (approximately 20,000 tons)

Environmental harm: 148 billion rubles (**\$2 billion** at then-current exchange rates). Mining giant Nornickel commits to remediation





To prevent serious industrial accidents that can be caused by cyberattacks, it is important to thoroughly verify all the risks. Simply knowing which business risks are relevant to a company is not enough. Understanding the criteria needed to actuate these risks is equally important. For example, these criteria might be the ability of an attacker to modify PLC firmware or obtain operator privileges.

Only a quarter of companies set specific objectives for penetration testing

Penetration testing is a standard practice for information security and one of the most popular security assessment services on the market. However, penetration testing does not guarantee protection. Can pentesting actually protect business from undesirable events? Will it measure how well a company is protected in practice? Let's try to answer these questions.

To evaluate how well infrastructure is protected from attacks, companies should start with an understanding of which business systems are critical and why they might be attractive for hackers. Unfortunately, not all customers are aware of the benefit of setting specific objectives for penetration testing. Pentesters are all

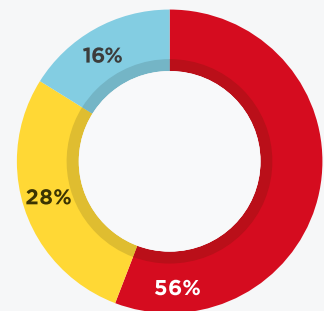


Over the last two years only 16 percent directly participated in the process of defining the risks to be verified

too often given the abstract task of obtaining maximum domain privileges. Only 28 percent of companies indicate which systems they want to check prior to the start of security assessment.¹

Over the last two years, even fewer clients—only 16 percent—directly participated in the process of defining the risks to be verified. Risks were most often articulated in these cases by the client’s IT and infosec teams, but sometimes they cannot say which conditions are needed for triggering these risks.

Some risks can be easily verified: for example, what data can be stolen if attackers compromise an executive’s computer. Other



- Conducted penetration tests without specific objectives
- Set specific objectives for penetration tests
- Verified business risks

Figure 1. Percentage of clients for security assessment and risk verification services in 2019–2020

¹ Based on the results of 42 internal security assessments of corporate information systems and risk verification projects performed by Positive Technologies in 2019–2020 at 32 companies



When companies don't see clear-cut consequences, they may start doubting whether the risk could be triggered at all

risks, such as tampering with ICS processes, are much harder to verify. It is vital to define the criteria for actuation of such risks because the damage can be disastrous.

Internal security assessments of corporate information systems show that at 75 percent² of industrial companies, attackers would be able to penetrate the ICS network, obtain access to equipment, send PLC commands, and change the ICS configuration. In real life, such actions may lead to accidents, equipment failure, production shutdown, damage to goods and products, breach of contract, and large recovery costs. At one company, our pentesters obtained access to the workstation of an ICS operator used to monitor equipment parameters. In a penetration test, we can only hypothesize that attackers would be able to tamper with processing of ICS equipment readings in a way that would eventually cause the equipment to fail. We cannot actually complete the attack chain on real infrastructure, since doing so could cause real-life harm. But when companies don't see clear-cut consequences, they may start doubting whether the risk could be triggered at all.

² Based on the results of 12 internal security assessments of corporate information systems performed by Positive Technologies in 2018-2020 at industrial companies to verify whether attackers could penetrate industrial control systems.



At 75 percent of industrial companies attackers would be able to penetrate the ICS network

In the financial sector, our experts were able to obtain access to ATM management from the internal network at a fifth of banks.³ At one bank, attackers could access ATM network monitoring and management software and subsequently create their own commands and upload them to any ATM. Naturally, our experts did not upload these commands—doing so could stop the ATMs from working—which meant that our assessment of consequences was only hypothetical.

And then, when analyzing the results afterward, pentesters and the client may reach different conclusions regarding the dangers of attack vectors and their consequences. The client's IT and security teams tend to be confident that automated protections would have protected ICS processes, or that the anti-fraud system would have stopped suspicious transactions—in short, that any attempts to trigger risks would have been stopped by an existing security measure. And how can pentesters prove otherwise? Doing so would require checking these assumptions on real equipment.

³ Based on the results of 15 internal security assessments of corporate information systems performed by Positive Technologies in 2018-2020 at financial institutions

Cyber-range: a way to reconcile differences in risk interpretation

Modeling company infrastructure on a special cyber-range may offer the best solution to the problem of interpreting cyber-risks. By re-creating the true context with all related business processes and systems, a cyber-range allows verifying critical risks and defining the criteria needed for triggering these risks—in other words, the conditions needed for an unacceptable event to occur. When these criteria are known, penetration testing and risk verification on real infrastructure become more informative.

During The Standoff, for instance, attackers caused a fire at the petrochemical plant by shutting off the cooling valve in Rapid SCADA software. This means that if pentesters gain remote desktop access to an ICS workstation, they could indeed trigger this risk. At the amusement park, hackers tampered with the controls of the Ferris wheel after they obtained administrative rights

on the relevant SCADA host. They triggered the risk by sending a command to change the rotation speed of the Ferris wheel. As a result, the Ferris wheel collapsed (see page 83).

At The Standoff, attackers managed to trigger 47 percent of the risks embedded in the mock digital city's infrastructure. It only took them two hours and 50 minutes to trigger the first risk by accessing confidential documents belonging to the petrochemical plant.

By verifying risks and defining the trigger criteria, businesses get priceless information about which dangers they face and where they come from. Businesses can then act in time by planning and deploying protection measures to rule out unacceptable events and maintain performance at the required level.

At The Standoff, attackers managed to trigger 47 percent of the risks embedded in the mock digital city's infrastructure





We enclosed a poster
that illustrates the
history of information
security contests

Digital twin cyberexercises: a better way of seeing real business risks

Olga Zinenko

Information Security Analytics,
Positive Technologies



15 min
to read this article





Corporate security is a prudent investment in the face of potentially catastrophic costs from a hack

Despite the pandemic-related economic slowdown and strained corporate IT budgets, companies are still spending more on cybersecurity. Gartner projected worldwide IT outlays of approximately \$3.6 trillion for 2020, a decrease of 5.4 percent from 2019.¹ Yet for the same year, Gartner also expected an increase of 2.4 percent in spending on information security, to \$123.8 billion.² These expenses primarily go toward protecting infrastructures, networks, and user data.

Corporate security is a prudent investment in the face of potentially catastrophic costs from a hack. Cybersecurity Ventures estimates that cybercrime will cost the world \$6 trillion in 2021.³ This figure includes damage and destruction of data, lost productivity, theft of money and intellectual property, theft of personal and financial data, post-attack disruption of business processes, reputational damage, and other losses.

But market research agencies cannot answer the question: "How dangerous will a cyberattack be for my company?" For 50 years, security experts have been looking for ways to measure the potential damage from cyberattacks. They started developing audit scenarios,⁴ creating methodologies for risk management,⁵ and performing penetration tests and



For 50 years, security experts have been looking for ways to measure the potential damage from cyberattacks



security assessments of information systems. Companies now train their employees and test security awareness: users are the weakest link in the security chain, which is why mal-factors target them in social engineering attacks. While all these steps help to boost corporate security, they still fall short at determining whether a risk is truly "triggerable."



One way to simulate a real attack is with red team penetration testing. Red teams, consisting of security experts, emulate targeted attacks against a company. The difference from traditional penetration testing is that the company's security team (blue team) practices countering attacks, which better prepares them for responding in real life. However, this method, just like pentesting in general, has an important drawback: all the testing takes place on real infrastructure. Risks cannot actually be triggered.

The need for no-holds-barred contests has contributed to the popularity of the capture the flag (CTF) format. CTF players look for vulnerabilities in services and use them against other teams, without endangering any real-life corporate infrastructure. CTFs are also an excellent learning opportunity for researchers, pentesters, red team participants, and bug hunters. For business, CTFs are no longer just fun and



games. Many former CTF players have gone on to become prominent security experts and hold major corporate positions.

Attacker appetites are increasing every year, and so is the resulting damage. Costly, well-publicized incidents have made companies take digital risks more seriously, with measures to both reduce the likelihood of attacks and minimize damage.

The shift to result-oriented security has inspired a whole new competition format. Cyberexercises can engage infosec pros of all stripes, including pentesters, researchers, security staff, and SOC operators.

Cyberexercises are, in essence, controlled attacks conducted to assess and improve skills at detection and response. Attack scenarios can be fully automated or performed by a team of attackers. Here, red teams do just what real attackers would, making the exercises as realistic as possible. Having several attacker teams participate simultaneously truly puts infrastructure to the test, enabling fuller analysis with more techniques and attack scenarios.

Cyberexercises can be conducted either on real company infrastructure (which limits attackers to only checking the feasibility of risks) or on a special cyber-range.

Large-scale cyberexercises include Locked Shields, organized by the NATO-accredited cyberdefense center in Tallinn (more than 1,200 experts took part in Locked Shields 2019), and the Cyber Defense Exercise, which has been held by the U.S. National Security Agency since 2001. Cyberexercises can have a special theme. For example, in December 2020, the European Union Agency for Cybersecurity (ENISA) was supposed to hold Cyber Europe 2020, an event designed to model attack scenarios targeting healthcare institutions. The event was postponed indefinitely due to the pandemic.

In 2016, Gartner introduced its annually updated Magic Quadrant for training solutions, a sign of high demand in this area.⁶

For small companies with less potential downside from attacks, smaller-scale training platforms with pre-defined attack scenarios may



Cyberexercises are, in essence, controlled attacks conducted to assess and improve skills at detection and response



offer a budget-friendly option. Such platforms are gaining popularity due to low costs and broad audience coverage—from regular employees to executives. For approximately \$90,000, Cyberbit provides cybersecurity education for key employees, starting at three hours for executives and up to two days for SOC staff. Training programs by CrowdStrike, Security Innovation, and Vector Synergy are intended to help work through cyberattack response scenarios. Attacker actions are emulated as part of this. The catch is that the exercises take place on specially crafted infrastructure (or cloud infrastructure) without being customized to the needs of a particular customer.



The best solution today is to conduct cyberexercises with multiple attacker teams. These teams attack a digital model that re-creates the company's real infrastructure. Digital twins were first used to model various abnormal situations at industrial facilities, taking into account such factors as equipment location and movements of employees. According to a report by Grand View Research, the global market for digital twins was valued at \$3.3 billion in 2018 and is





Instead of attempting abstract tasks, attackers trigger concrete business risks corresponding to a particular target

expected to reach \$38.61 billion by 2026, growing by an average of 35 percent each year.⁷

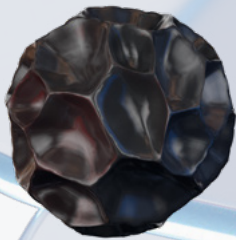
For major companies at risk of enormous losses in an attack, a cyber-range that combines the advantages of digital twins and cyberexercises can become a powerful and cost-effective solution. Cyber-ranges are a good fit for organizations pursuing result-oriented security—transparent, efficient, and practical. Each company has its unique infrastructure and business risks. In order to correctly verify these risks and their consequences, it is vital to take into account this uniqueness. On a cyber-range, companies can better see the value of their resources and understand what attackers are after. The red team, meanwhile, verifies company-specific risks and their consequences. In some cases, it is impossible to verify risks without a cyber-range, such as when these risks could involve industrial accidents, environmental damage, or bodily harm. A cyber-range allows modeling risks to more than just a single company, but an entire city, industry, or even country.

Creating cyber-ranges is expensive and time-consuming, which is why it is often addressed at the government level. For example, Lockheed Martin was allocated \$33.9 million to build the National Cyber Range (NCR) in the U.S.⁸ Russian company Rostelecom received a subsidy of 364.55 million rubles (worth approximately \$6 million at 2019 exchange rates) for the creation of a cyber-range under the country's "Digital

Economy" program.⁹ In the meantime, and without outside help, Positive Technologies has set up its own cyber-range by building on ten years of experience in international cyberexercises at the Positive Hack Days forum. The cyber-range concept has significantly evolved at Positive Technologies in that time. What was initially a confrontation on artificially modeled infrastructure has matured into a global cyber-range. The Standoff has grown to include infrastructures of real organizations, real business and industrial processes, real protection tools, and real defenders. Instead of attempting abstract tasks, attackers trigger concrete business risks corresponding to a particular target.

The Standoff offers a wide-open environment to model cyberattacks, assess the importance of assets, and verify the feasibility of risks in a mock digital metropolis. Real-life scenarios play out at an oil and gas company, power plant with substations, petrochemical plant, airport, bank, railroad, and seaport. Participants work with the real equipment and services used in these industries. The Standoff is a unique opportunity to complete the attack chain and see the possible consequences. Can attackers actually steal a billion from the bank? How long will the city be left without electricity after a turbine failure at the power plant? The Standoff incorporates the same controllers used on similar critical infrastructures. If the power plant shuts down because of an attack, the same would happen in real life.

7



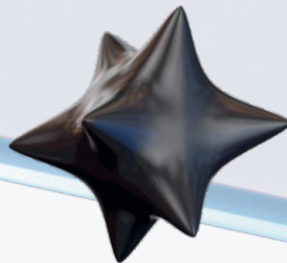
Is there a risk that a billion will be stolen?

8



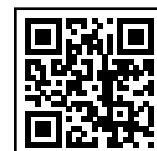
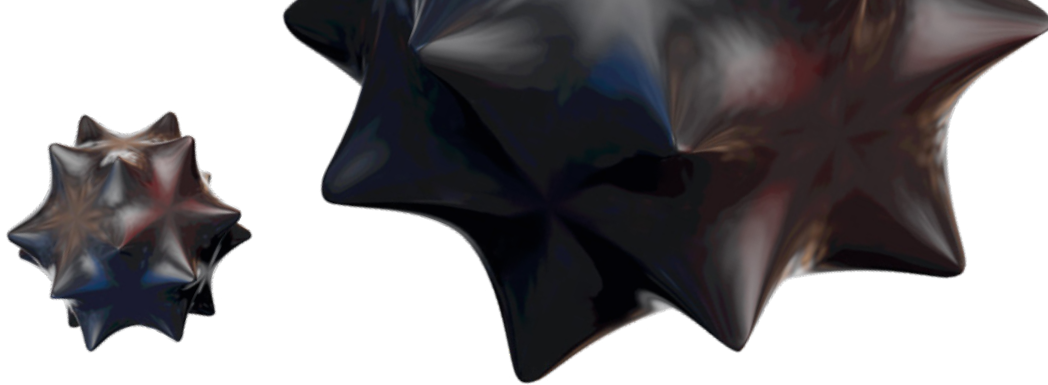
Is it possible to turn off all traffic lights and cause traffic collapse?

9



How long will the city remain without electricity?





The Standoff website

The Standoff 2020:



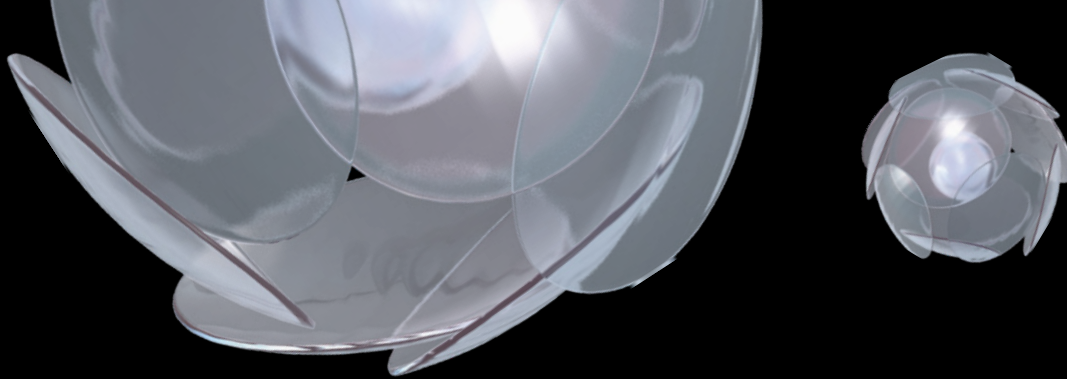
12-17
november

29 attacker
teams

6 defender
teams

13 city infrastructure
facilities





**Olga Zinenko,
Yana Yurakova**

Information Security Analytics,
Positive Technologies



20 min
to read this article

an exciting cyberexercise

On November 12-17, hundreds of security experts put systems to the test at The Standoff cyber-range. A total of 29 attacker teams and 6 defender teams took part. For this massive clash, the organizers built a mock digital city with virtual infrastructure spanning 13 different facilities, managed by six fictional companies:

- Amusement park, business center, and traffic lights (managed by fictional company 25 Hours)
- Airport, railway station, and sea port (Heavy Ship Logistics)
- Oil field and petrochemical plant (Nuft)
- Bank (Bank of FF)
- Broadcasting company, gas distribution station, and transformer substation (Tube)
- Power station (Big Bro Group)





The main task for attackers was to trigger business risks relevant to each of the companies. For additional points, they could also look for vulnerabilities on office infrastructure and install miners.

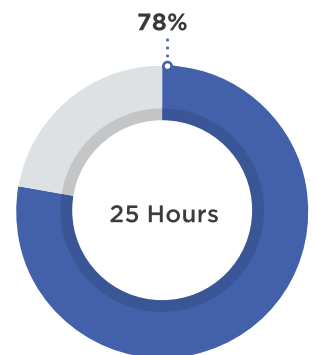
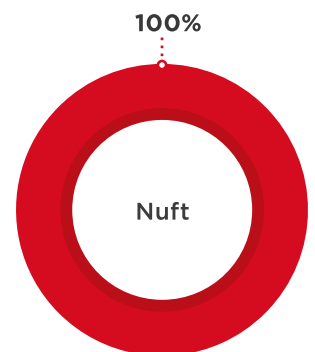


The objective of defenders: to quickly detect incidents and maintain infrastructure uptime.

This cyberbattle was a source of invaluable experience for both sides. Attackers got acquainted with the hardware and software in use at real companies. Meanwhile, defenders practiced rapid detection and investigation of incidents, as they saw for themselves new attack vectors without running the risk of actual damage to business or real-life infrastructure.

Conditions on the cyber-range matched reality as closely as possible: for example, even network interaction took place over standard ICS protocols:

- OPC DA
- Modbus TCP
- UMAS
- IEC 60870-5-101
- Siemens Simatic S7
- Siemens DIGSI
- Vnet/IP
- CIP (Ethernet/IP)
- IEC 61850
- BACnet/IP



Attackers causing havoc

In total, the attackers triggered 47 percent of the risks designed by the organizers of The Standoff. The largest numbers of risks were triggered at the airport, oil field, and petrochemical plant.

During the competition, two new unique business risks were discovered even though they had not been explicitly intended by the organizers. Besides verifying known risks, the cyber-range helps to identify unforeseen risks that have not been defined in advance.

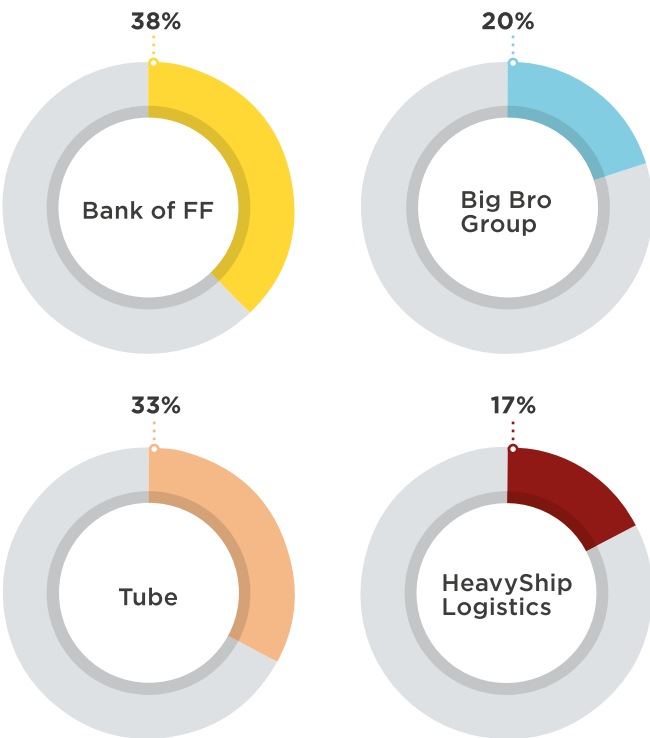


Figure 1. Percentage of business risks triggered

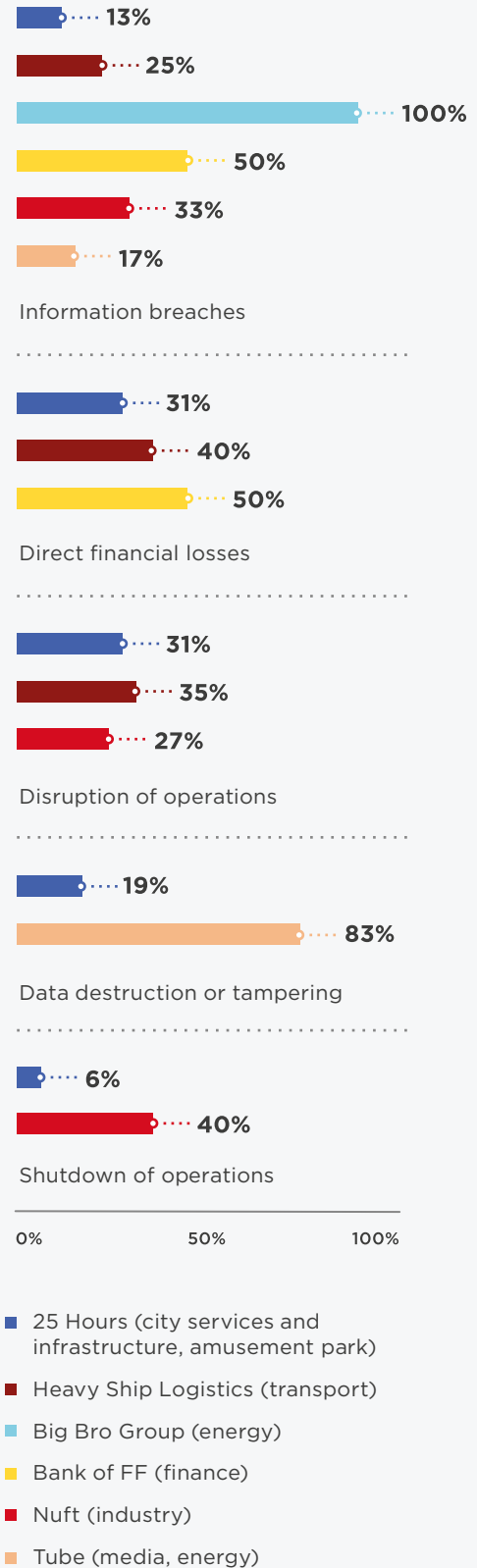
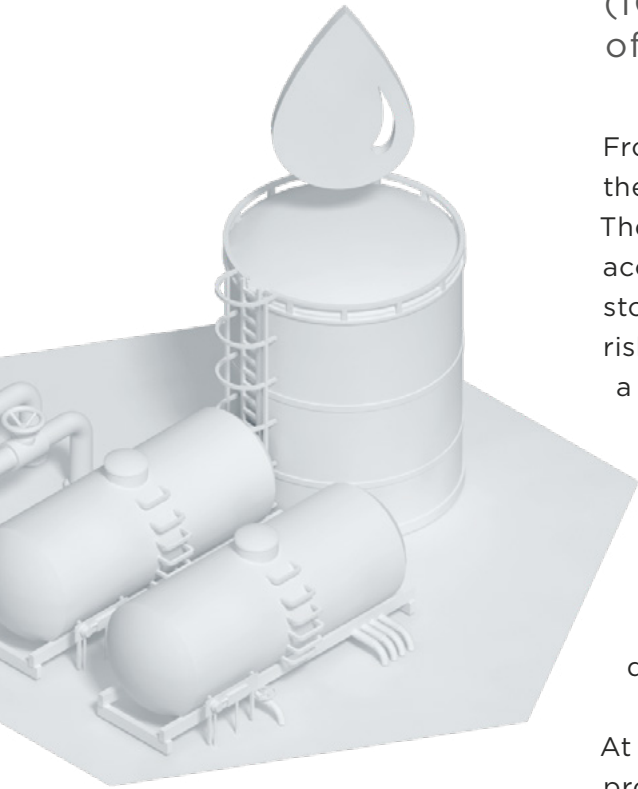


Figure 2. Consequences of cyberattacks at The Standoff (percentage of risks triggered for each company)

Industrial disaster

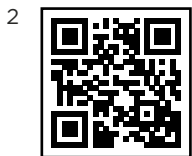
According to 60 percent of industrial companies, disruption of production (ICS processes) may be the main goal of cyberattacks



From the opening minutes of The Standoff, attackers targeted the infrastructure of Nuft, one of the city's fictional companies. The back2oaz team breached the company's network, gained access to the computer of the head of the oil department, and stole files containing procurement information. This was the first risk triggered by attackers at The Standoff. In real life, preparing a similar attack could take weeks or even years, since attackers try to conceal their actions in order to obtain as much valuable information as possible.

Later on in the competition, attackers gained access to the management system of the petrochemical plant. By blocking the refrigeration inlet valve, they caused overheating and disrupted production.

At the oil field, attackers managed to disrupt the operation of oil production equipment. Two teams gained access to the controller of the oil terminal management system and caused an overflow, disrupting the transportation of petroleum products to the oil terminals. The controller for the petroleum product transportation system was later disabled as well. In real life, an incident like this could lead to an oil spill and environmental disaster.



In 2002, the Prestige oil tanker split in two, spilling 64,000 tons of heavy fuel oil into the sea. 300,000 volunteers from across Europe helped clean up the coastline, with total damages estimated at €4 billion.¹ Another example: in 2000, 1.3 million liters of oil were released into Guanabara Bay after an accident at a Petrobras refinery in Brazil. Cleanup cost Petrobras over \$100 million.²

Bank robbery

In 2020, 71 percent of attacks against financial institutions included theft of data

The virtual city's bank was identical to a real one, complete with an acquiring system, money transfers, and processing center. Virtual banking systems ran standard transactions with bank accounts and cards, enabled online payments, and supported the bank's internal operations. The bank had 236 accounts, corresponding to one for each citizen and each attacker team (with starting amounts of 10,000 credits for each citizen and 1,000 credits for each attacker team). In addition, each of the city's companies had a settlement account containing 1 million credits. Regular activity was maintained by special bots: every 15 minutes they performed transactions varying from 10 to 1,000 credits.

On the third night, the DeteAct team managed to hack the bank. They gained access to the card details of bank clients and transferred funds to their own account. Later, the personal data of bank employees (names, addresses, phone numbers, account numbers, job titles, and salaries) was stolen from the ERP system. The bank faced direct financial losses and a data breach as a result.



Data theft in the financial industry in 2020

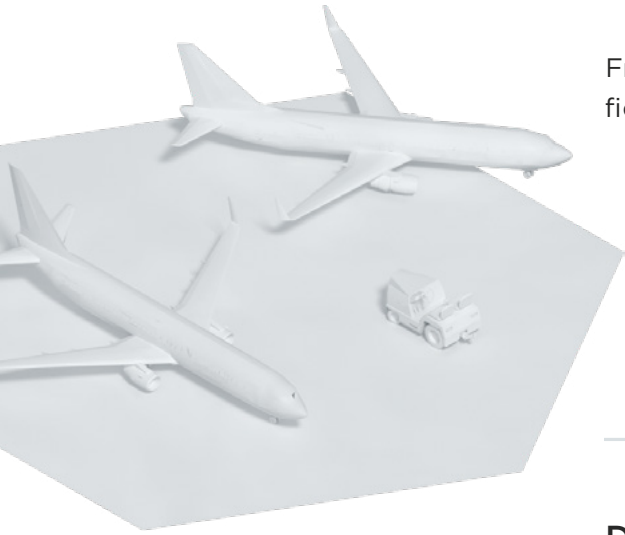
- 25% personal data
- 14% credential theft
- 11% card information

In 2020, 71 percent of attacks against financial institutions included theft of data, such as credentials (14%), card information (11%), and personal data (25%). Data breaches can attract significant unwanted attention from regulators and from the media, as demonstrated two years ago in an incident affecting over 900,000 customers of Russia's Alfa Bank, Home Credit Bank, and OTP Bank.³

3



Breakdown of airline ticket sales

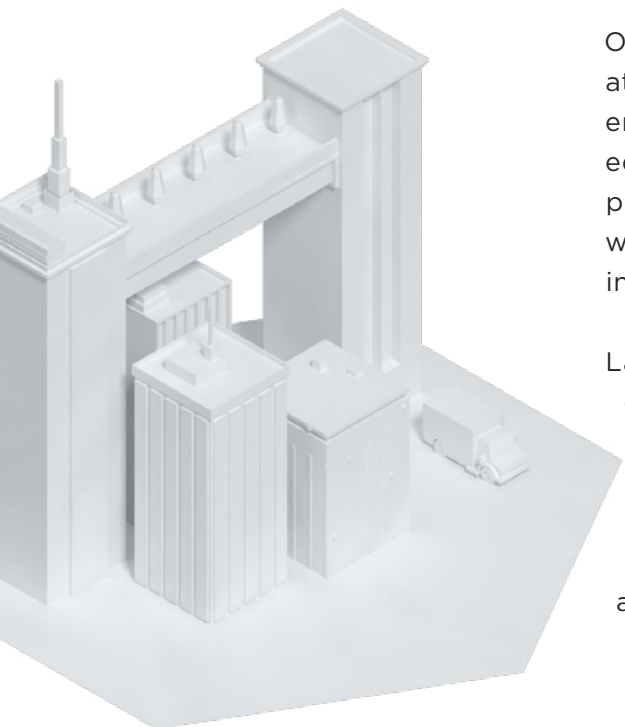


Frightened by accidents at the petrochemical plant and the oil field, citizens hurried to the airport. However, the Hack.ERS team triggered a business risk (breach of passengers' personal data) at the city airport. On the same day, DeteAct caused failure of ticket sales and passenger check-in systems. Tickets could no longer be bought through the airport's website, and those who had already purchased tickets could not check in for their flights.

Document theft from encrypted storage

In 2020, 64 percent of attacks on government institutions involved malware

Remote code execution was used to trigger 73 percent of risks at 25 Hours



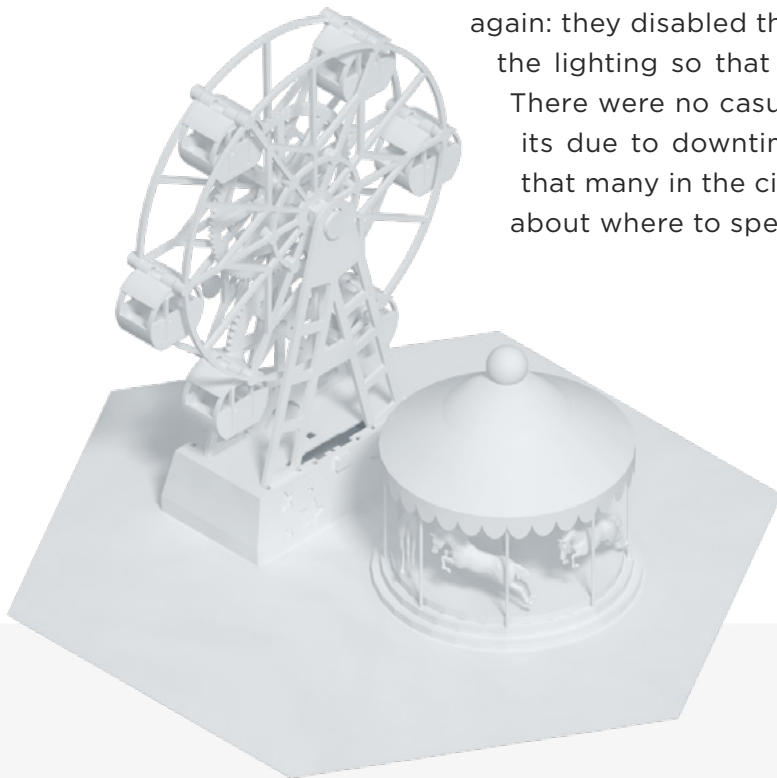
On the first night of the battle, the city's business center was attacked twice. In the space of a few hours, two different attacker teams obtained access to the city portal database and deleted information on fines and debts owed by citizens. Attackers penetrated the company's network due to a vulnerability in a web application: they exploited it by uploading a malicious file, instead of a photo, on their profile page.

Later, attackers stole the personal data of employees at 25 Hours, gained access to the CEO's encrypted storage, and stole important documents. They could then pass on sensitive data to business rivals or make the information public. In the final minutes of the contest, attackers gained access to the heating and cooling systems of office buildings and were able to adjust temperature settings.

Ferris wheel collapse

At the 25 Hours amusement park, attackers went above and beyond by triggering all the intended business risks—and also discovering and implementing one of their own. They made their childhood dreams come true by getting free tickets to the amusement park and giving them away to anyone who wanted. However, this was done with malicious intent: they were gathering their victims in preparation for a strike. They managed to take over the Ferris wheel controls. The back2oaz team increased the rotation speed, causing the wheel to rip off and collapse. It is difficult to even imagine how many victims this would have affected in real life!

After the Ferris wheel was repaired, the attackers struck again: they disabled the wheel controller and turned off the lighting so that visitors could not leave the ride. There were no casualties, but the company lost profits due to downtime and repair costs. We imagine that many in the city will now have second thoughts about where to spend their free time.



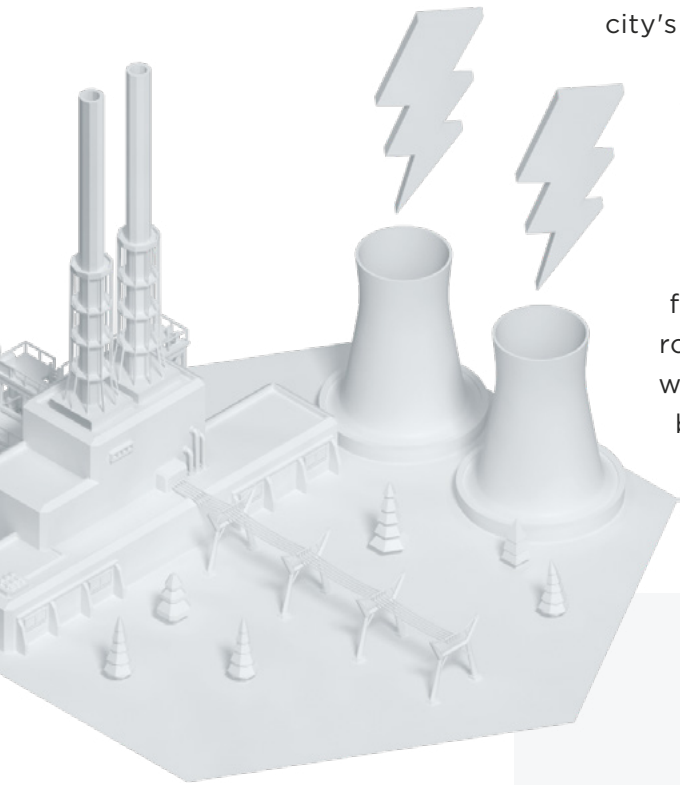
The back2oaz team increased the rotation speed, causing the wheel to rip off and collapse

Energy sector at risk

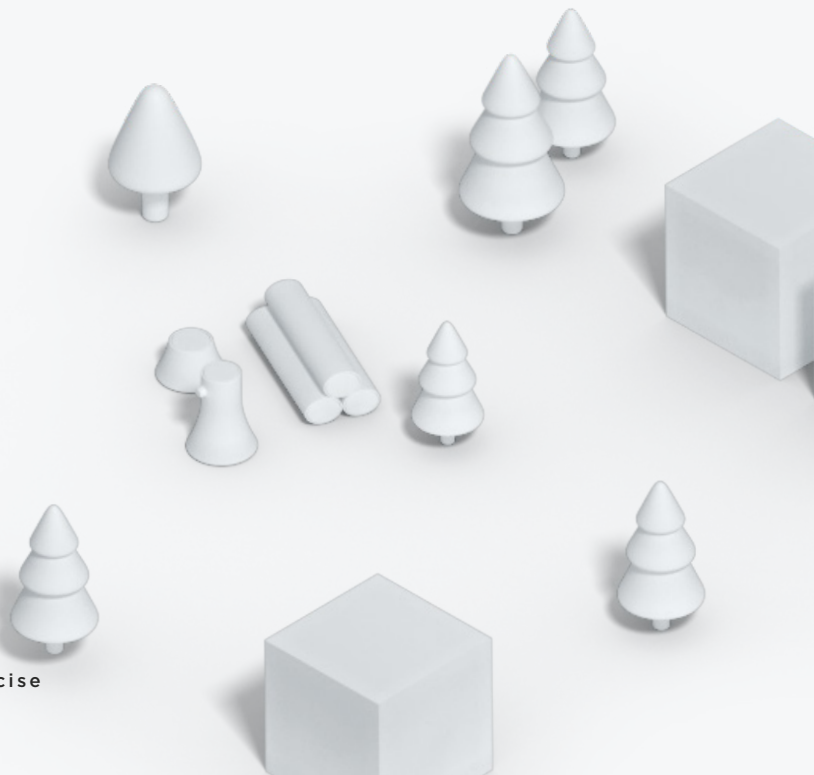
Just as in real life, hackers tried to stay unnoticed by attacking at night

On the last night of the competition, hackers attacked Big Bro Group, the city's electricity provider. They gained access to the company's ERP database and stole employee-related information. Fortunately, power generation was uninterrupted and the city's lights did not go out.

One real-world example of a halt in power generation is the incident at the Sayano-Shushenskaya hydroelectric power station (Sayanogorsk, Russia) in 2009. The incident caused a power outage across large parts of Siberia and disrupted electrical supply to the city of Tomsk. Several industrial facilities, including Siberian aluminum smelters, suffered rolling blackouts. As a result of the incident, 75 people were killed and 13 were injured. Damages totaled over 7.3 billion rubles (\$230 million at then-current exchange rates), including environmental damage.⁴



4

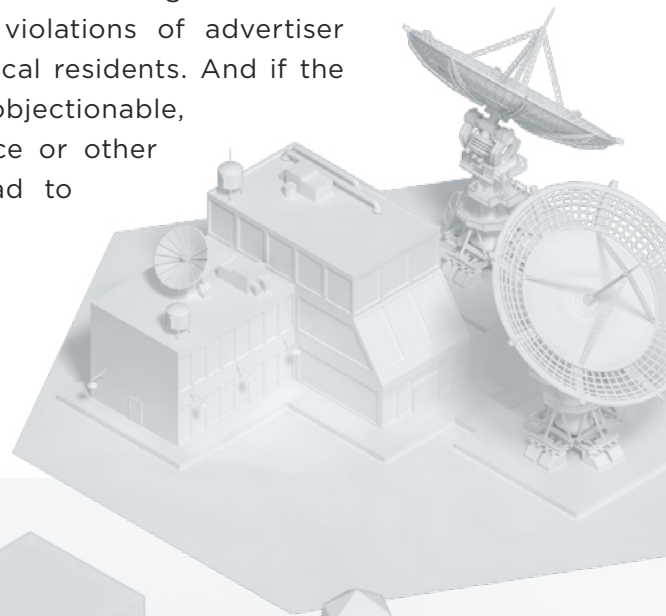


Pirate broadcasting

The Tube TV and radio broadcasting company was repeatedly targeted. Attackers gained access to the management system for the city's video billboards, which they used to broadcast their own content.

Because of a vulnerability in the streaming platform, the attackers did not even have to know the password. They simply reset the administrator's password and replaced it with their own, and then uploaded their own video for broadcasting throughout the city.

In real life, such pirate broadcasting can cause financial losses (due to violations of advertiser agreements) and upset local residents. And if the materials in question are objectionable, due to promoting violence or other reasons, it can even lead to lawsuits.



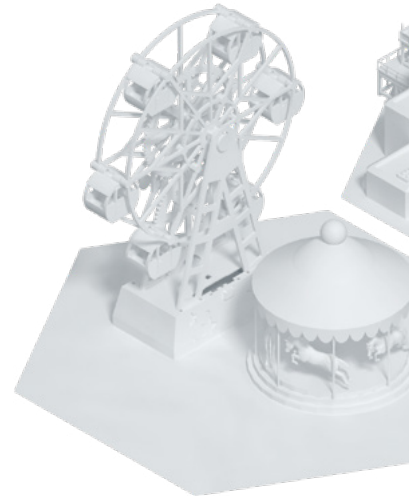
Defenders busy investigating

Defenders recorded all incidents and investigated the attacks that triggered risks. On average, they recorded 35 incidents per day. By comparison, Cisco's internal incident response team handles an average of 22 incidents every day. A total of 213 incidents were identified, of which a fifth related to obtaining initial access and about a quarter involved malicious code execution.

Collecting data and performing a full investigation took the teams an average of 11 hours and 50 minutes. However, defenders spent more than 24 hours investigating the breach of airline passengers' personal data and disruptions in online ticket sales for the amusement park. Some incidents were not investigated due to time constraints. The work of the defenders was complicated by the fact that multiple attackers could use similar techniques simultaneously in parallel attacks, while defenders had to walk back the chain of events for each incident separately.



During the competition, the defenders encountered many techniques from the MITRE ATT&CK matrix in practice. In most cases, attackers lived off the land by abusing legitimate tools already present on target systems, such as by running PowerShell scripts and creating scheduler tasks. Many APT groups do the same.





Interpreting the results

It is worth noting that not all the attacker teams were able to trigger business risks, even though many had found vulnerabilities on network perimeters. Similarly, during penetration testing, not every pentester team will be able to emulate a complex multi-stage attack that will ultimately trigger a business risk. Ordinary pentesting fails when it comes to verifying certain risks, since, in addition to disrupting business processes, these risks may threaten the environment or human life and health. The incident with overflow of oil storage is a case in point.

Cyberexercises provide great practice for specialists from any infosec discipline: in real life it would take years to encounter such a large number and variety of incidents. The Standoff gave defenders a great opportunity to get acquainted with diverse attack scenarios and improve their skills in just days.

Global SOC at The Standoff 2020: the all-seeing eye

Paul Kuznetsoff

Deputy Managing Director
for Cybersecurity



20 min
to read this article

The Positive Technologies Expert Security Center has been involved in The Standoff for several years now—since 2018, when the event was still part of Positive Hack Days. That year, we followed the state of play using MaxPatrol SIEM, PT Network Attack Discovery (for network traffic analysis), and PT MultiScanner (for multitiered protection from malware). Our task was to observe goings-on, track the techniques and tools used by participants, and of course, put our products through the paces under intense conditions. During such events, we push our tools to the limits of their abilities (and even slightly beyond). For example, in 2018, we followed 12 teams for two days, during which MaxPatrol SIEM processed an average of 20,000 EPS and PT NAD analyzed more than 3 TB of network traffic. All the while,

our team was busy identifying successful attacks and looking for indicators of compromise (such as web shells, remote consoles, and host logins). This "battle-won" knowledge helped to shape the future direction of our products.

A year later, at the next PHDays, we increased SOC visibility by adding another two tools to the mix: PT Application Firewall and PT Industrial Security Incident Manager. This combination gave us an exceptionally complete picture of all the events in the mock digital city, no matter where on the infrastructure they were happening. The Standoff that year also lasted for two days, but now we were following a larger number of participants: 18 attacker teams, 6 defender teams and 3 SOC teams, which made for plenty



of activity. Unlike the teams, we in the global SOC only observed passively and did not interfere. Like before, we wanted above all to demonstrate the effectiveness of modern systems at detecting and investigating cyberincidents in practice. We also wanted to study the tactics and techniques used by participants in real time, of course. This is no small feat since attacker teams at The Standoff have always been second to none at using cutting-edge tools and methods.

So it's fair to say that, as we looked ahead to The Standoff in 2020, things seemed familiar. However, the sheer scale of the cyberexercises was still something to behold.

"Purple teaming"

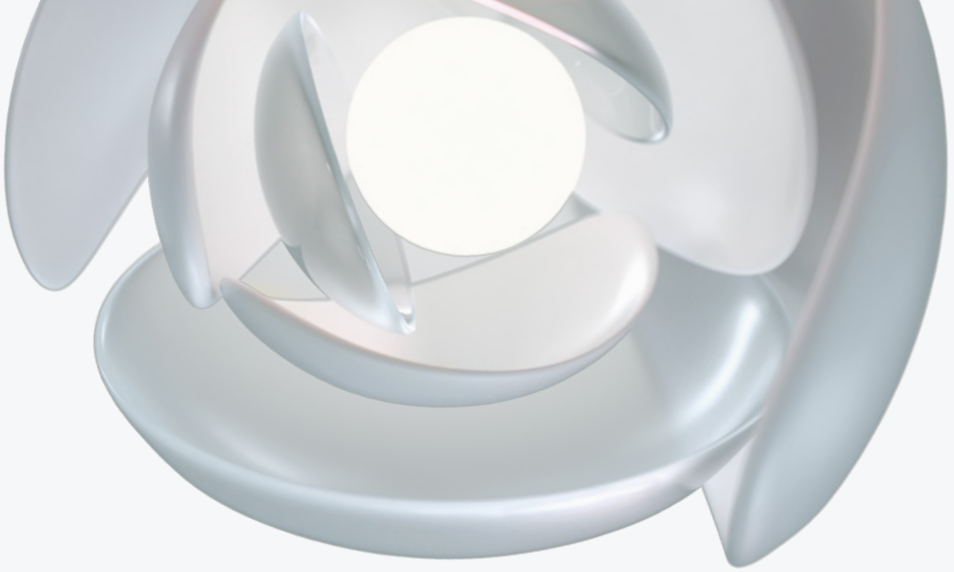
In 2020, our SOC included specialists responsible for non-stop monitoring and threat hunting on the cyber-range as well as sharing the results with shift analysts, who in turn put together the bigger picture for recreating the kill chains used to trigger specific threats and risks. The skillsets of our experts included ICS, malware analysis, and creation of detection rules to catch malicious actions on infrastructure. This diversity is needed in order to fully assess what is happening and detect, classify, and investigate all the attack vectors down to the smallest technical details in the context of specific risks.

Throughout the event, our specialists conducted 24/7 monitoring of security events throughout the virtual city's infrastructure (which,

incidentally, was physically represented by a miniature diorama). In other words, we kept a close eye on the actions of the attacker teams. And then, based on this information, we evaluated the quality, completeness, and correctness of reports submitted by attackers who had accomplished a particular task. This constant work gave us a full timeline of events, which helped the jury to do its job and provided the latest information to the professional community observing the battle on The Standoff portal. In much the same way, we evaluated the completeness of the information provided by the blue teams in their own reports on detected incidents.



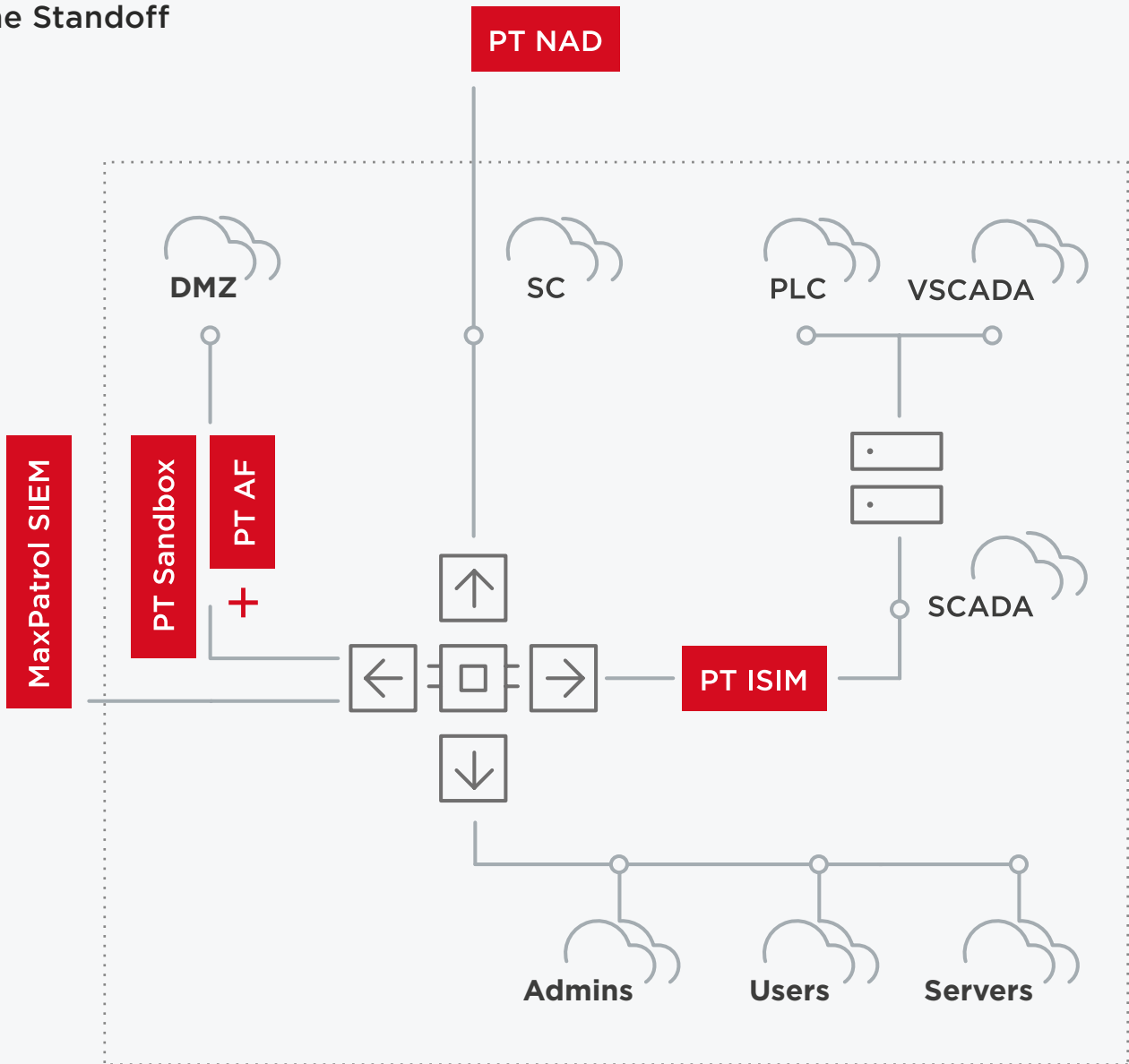
The skillsets of our experts included ICS, malware analysis, and creation of detection rules to catch malicious actions on infrastructure



What's in an all-seeing eye

What technologies did our SOC have?

Infrastructure of one of the offices created for The Standoff



We used PT Application Firewall to protect perimeter services (located in the demilitarized zone, or DMZ) and monitor attacks on them. At the heart of our SOC was MaxPatrol SIEM.



SIEM systems are traditionally used to collect, store, and process data about security events in a timely way. However, their scope of application can be far broader: SIEM can also help to identify and investigate information security incidents, take asset inventories, and monitor the security of information resources.

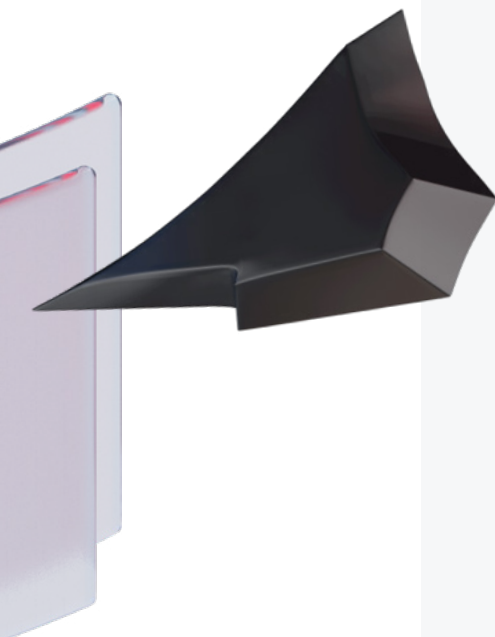
The search for incidents starts with connecting sources that generate a wide range of events. For the fullest possible picture of what is happening on infrastructure, we recommend connecting all sources of IT and security events to SIEM.

Security event sources are specially made software or hardware products that generate security events. These sources are enriched with the external knowledge needed to interpret any given event as "good" or "bad" for security. Examples: IDS/IPS (for collecting data on network attacks), antivirus software (for detecting malware).

Almost all the hosts in our virtual city were connected to the SIEM system as event sources. Why "almost all?" Because on the ICS network segments, for obvious reasons, we relied more on PT Industrial Security Incident Manager. PT Network Attack Discovery together with MaxPatrol SIEM have become a kind of Swiss Army knife for our global SOC. This combination allows us to conduct deep network traffic analysis and identify anomalies and malicious actions, both automatically and with direct human intervention. And, last but not least, PT Sandbox with its customizable virtual environments allowed us to quickly identify social engineering attacks, including phishing, and analyze them. PT Sandbox has strengthened our ability to detect malware attacks by red teams.



In this context, an "attack" means any detected attempt to illegitimately affect monitored systems in order to achieve certain goals. Goals could include obtaining information about a subnet or gaining the ability to execute OS commands on a specific host. But by the point when we knew an attack had been successful, the term "incident" was more appropriate. Then, for the incidents that we detected, we built risk implementation chains. Chain-building gave us information for attributing one-off incidents to particular attacker teams. Experimental modules for network behavior profiling helped in this process.





Attackers triggered
47 percent of all risks
embedded in the virtual
city's infrastructure

However, preparing for the event created a number of challenges for us and the infrastructure team. This meant getting a huge number of technical solutions emulating real business processes to "play nicely," as well as setting up subnet routing and keeping everything stable. And it was critical for us as SOC specialists to ensure consistent 100 percent visibility into everything happening on the cyber-range. It was also important not to interfere with working processes on corporate or ICS networks (such as by copying network traffic) while still managing not to miss anything. For this purpose, our SOC assigned two monitoring architects to the

project while the infrastructure was still under construction. They worked with subject matter experts on detecting attacks on hosts and the network as they meticulously checked network availability, visibility of network traffic throughout the infrastructure, and actual visibility of requests to web applications in PT AF.

We created a ruleset for MaxPatrol SIEM and signatures for PT ISIM and PT NAD, including experimental ones that needed to be ironed out under conditions nearly indistinguishable from the real thing.

Monitoring in action

We expected that attackers at The Standoff would "dip their toes in the water" by performing reconnaissance first and attacking only later. This is not what happened, however. Attacker teams went into battle during the first minute and kept the pressure up throughout

almost the entire event. The global SOC detected more than a hundred security incidents by the first night. The pace did not lessen and, if anything, even increased by the final days when teams were racing to score points by triggering additional risks.

By the end of The Standoff, the defenders were able to detect and build chains for more than 200 incidents (some of them were classified as isolated, being within a single incident report) and conduct 21 investigations



By the end of The Standoff, the defenders were able to detect and build chains for more than 200 incidents (some of them were classified as isolated, being within a single incident report) and conduct 21 investigations.

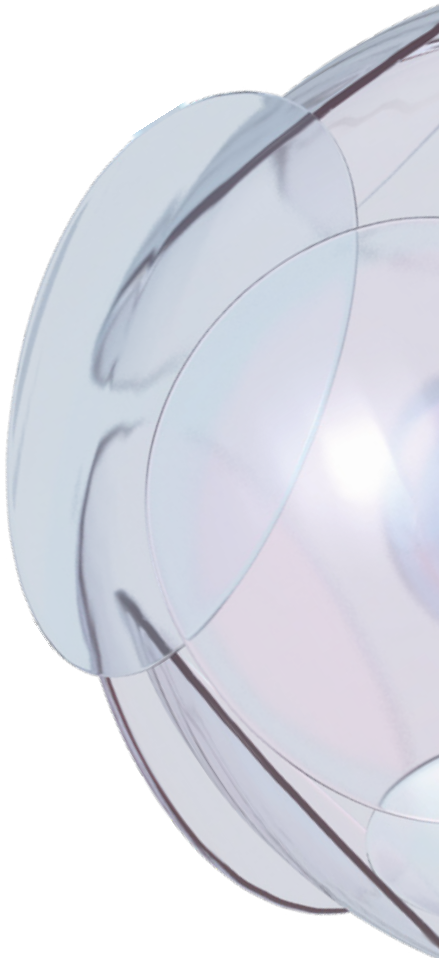
Interestingly, while investigating individual incidents could be as quick as a few minutes, the average time for a full investigation was around 11 hours. Attackers triggered 47 percent of all risks embedded in the virtual city's infrastructure, from bringing down the Ferris wheel in the amusement park to stealing personal data of airline passengers.

While tracking what was happening on the cyber-range, we found out a few interesting things. For example, defenders often detected attacker actions at the stage of reconnaissance on a particular host or at the beginning of lateral movement within the office network, but missed the primary penetration vector, such as brute force with login attempts cleverly distributed in time. Our SOC was able to identify such incidents by profiling user behavior and applying logic-based rules that took time delay techniques into account. In addition, the correlation rules

we developed allowed identifying individual actions of attackers in offices and, by linking them to initial compromise of hosts and accounts, classifying them as incidents. Taken by itself, each of the attacker actions looked legitimate. What made the difference was "building the chain" all the way back to the initial point of entry. In the same way, our SOC was able to identify illegitimate launches of various utilities, including ones used to gather information about hosts and networks, as well as access files. With the help of our solution for deep traffic analysis and sandbox, we identified successful phishing attempts. And of course, we benefited immensely from having network traffic analysis experts on hand. In the context of non-stop monitoring, we should emphasize the importance of constantly refining rules (such as by supplementing the relevant tabular lists, at a minimum) for better determining which events are legitimate. Thanks to this flexibility, we were able to detect attackers at certain steps and subsequently track all their activity. This approach proved effective and ultimately provided us with a number of advantages over the defender teams.

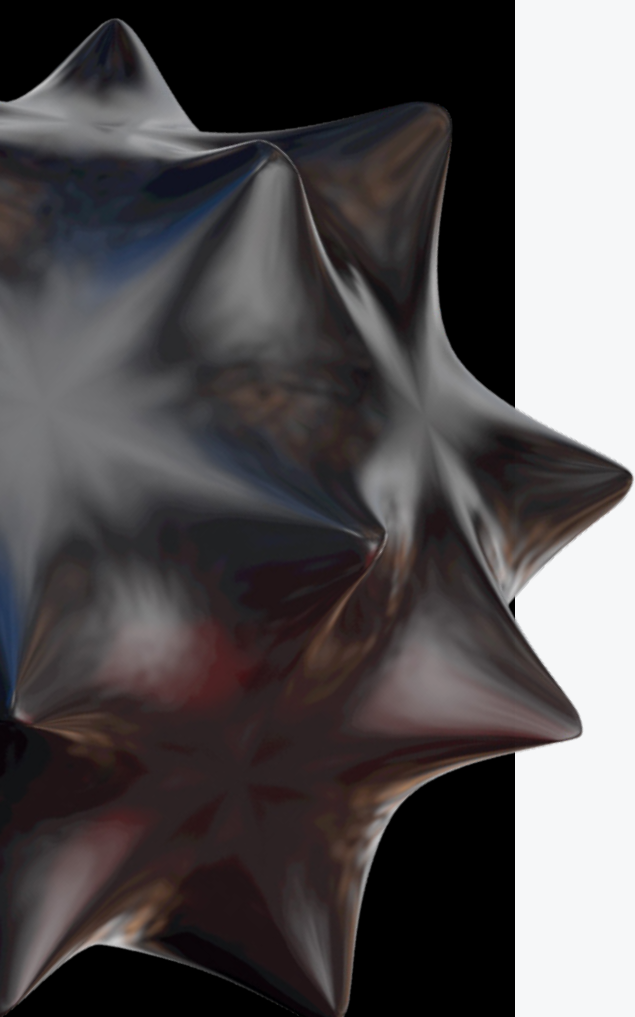


Software and hardware developers got an excellent opportunity to see how their products stood up against real offensive security professionals



Who and what is The Standoff for?

Everyone can make their own conclusions from The Standoff. For me personally, it confirmed the importance for the infosec community of constant collaboration and cooperation. For instance, software and hardware developers got an excellent opportunity to see how their products stood up against real offensive security professionals. Information security vendors, service providers, and integrators can see how their products and teams measure up in practice as they defend infrastructure. Everyone walked away with new technical data about products, vulnerabilities, and ways to perform, detect, and



Visit the PT ESC
blog to learn about
investigations of real
incidents



counteract digital attacks. They can apply this new experience to strengthen the security of real facilities and, therefore, help us all take another step into a secure future.

In addition, the entire PT ESC team strengthened its capacity for performing full-visibility monitoring on truly complex infrastructure, collected data for improving products, and engaged directly with other departments as part of SOC activity. The Standoff was, among other things, an occasion for us to look at the collaboration process from a new angle.



Authors



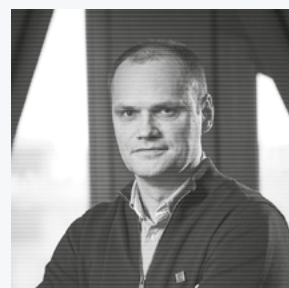
**Nikolay
Anisenya**

Head of Mobile
Application Security



**Alexander
Antipov**

Head of Online
Projects



**Dmitry
Darensky**

Head of Industrial
Cybersecurity Practice



**Mark
Ermolov**

Lead OS and Hardware
Security Researcher



**Evgeny
Gnedin**

Head of Information
Security Analytics



**Ekaterina
Kilyusheva**

Head of Research
in Information
Security Analytics



**Maxim
Kostikov**

Head of Banking
Security



**Dmitry
Kuznetsov**

Director of Methodology
and Standardization



**Paul
Kuznetsoff**

Deputy Managing
Director for Cybersecurity



**Alexander
Morozov**

Head of Penetration
Testing



**Alexandra
Murzina**

Lead Advanced
Technologies Specialist



**Alexey
Novikov**

Director of PT Expert
Security Center



**Pavel
Novikov**

Head of Telecom
Security Research



**Alexander
Popov**

Lead OS and Hardware
Security Researcher



**Vadim
Solovyev**

Senior Information
Security Analyst



**Yana
Yurakova**

Information
Security Analyst



**Olga
Zinenko**

Senior Information
Security Analyst

Chief Editor Nataliya Frolova
Editing Svetlana Isaeva, Olga Moskvicheva
Translation Sofya Korobkova, Vasily Pantyushin
Design Yana Aksakova
Illustrations Timofey Litovchenko

About us

For 19 years, Positive Technologies has created innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

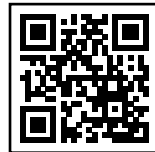




Positive Technologies



Positive Technologies



PT SWARM



The Standoff



PHDays

Positive Research 2021