НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ
БЕЗПЕКОВИХ СТУДІЙ

Review of cybersecurity news in Ukraine, tendencies, and world events related to the First World Cyber war

DECEMBER 2023

Prepared with the support of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity.
This publication is made possible by the support of the American people through the United States Agency for International Development (USAID). The authors' views expressed in this publication do not necessarily reflect the views of USAID or the U.S. Government.

CONTENT

KEY TENDENCIES

The United States has renewed the leadership of two important cybersecurity agencies. Former CIA officer H. Coker became the National Cyber Director, and Lieutenant General Timothy Ho replaced the U.S. Army General Paul M. Nakasone as the head of CYBERCOM and NSA, who had been heading these two agencies since 2018. These changes reflect changes in the policies of these agencies. As the Office of the National Cyber Director increasingly focuses on implementing the U.S. Cybersecurity Strategy and the Cyber Workforce Development Strategy, the NSA is increasingly issuing guidance to a wide range of organisations within the United States and is also increasing its international contacts as they are regular participants in partnership projects within the Five Eyes alliance.

After almost a year of discussions, the European Union has launched a movement to adopt the Cyber Resilience Act. This document creates a new framework for the IT sector and IT equipment manufacturers, requiring them to pay more attention to cybersecurity measures. Most likely, the implementation of this document will be complex and will occur at different speeds in European countries. This is also evidenced by the NIS2 Directive experience, which is still poorly implemented in many European countries more than a year after its adoption. At the same time, the EU clearly understands the growing role of cybersecurity and is ready to raise funds for it (the latest initiative calls to raise EUR 214 million for cybersecurity). This is complemented by the EU leadership's call for the creation of European cyber forces with offensive capabilities.

International cooperation is also becoming more systematic. For the first time, a cooperation agreement was signed between the European ENISA and the American CISA, the two key cybersecurity agencies in the EU and the U.S. This reflects the growing role of alliances and the search for international partners by the world's two largest economies in their common cybersecurity interests. This trend is complemented by the growing number of ties between Euro-Atlantic countries and their Asian partners. For example, for the first time, Japan and South Korea took part in NATO cybersecurity exercises, and the U.S. launched a new joint initiative with these two countries to counter North Korea's destructive activities

Ukraine continues to deepen international cooperation with private and public actors. In 2024, Recorded Future will help Ukraine to protect critical infrastructure from russian military and cyber aggression. Iceland joined the international cyber coalition in support of Ukraine and became the 8th member. Countering information attacks and combating financial phishing were the subject of discussion between the National Coordination Centre for Cybersecurity (NCCC) and Meta representatives. The Ministry of Digital Transformation of Ukraine and the European Cyber Security Organisation (ECSO) agreed to cooperate. The cooperation will result in strengthening Ukraine's cybersecurity system in accordance with international standards and providing access to the EU cybersecurity market for Ukrainian enterprises and professionals. Bilateral cooperation with Japan and Germany is also expanding.

russian cyberactivity does not subside. China is also becoming more active. In 2024, elections will be held in a number of countries (including the U.S. and the UK), and security agencies are already noting that russian and Chinese APT groups are preparing for these events by planning to interfere in them. This targeted activity is complemented by research on the current cyber threat landscape, which says that more than 60% of DDoS attacks are now politically motivated; and cybersecurity experts are already saying straight that cyber incident response teams will have to monitor not only their information systems, but also geopolitical events that are becoming a catalyst for new threats to the public and private sectors. The European Parliament also conducted an internal cybersecurity review ahead of the elections. According to its findings, the European Parliament's cybersecurity 'does not yet meet industry standards' and 'does not fully meet the level of threat' posed by state-sponsored hackers.

Critical infrastructure is being increasingly attacked with attempts to influence industrial processes. Although ransomware still remains the main source of threats, the attacks are reaching progressively dangerous levels. The recent cyberattacks against water supply systems at the level of small individual communities in the U.S. (as well as at least one similar organisation in Ireland) have shown how vulnerable the local level remains to cyber threats, with an even more serious lack of personnel and financial resources for proper cyber defence. It is possible to predict that local/community critical infrastructure facilities will be more frequently targeted by attackers who plan to prove the inability of the central government to protect all citizens.

Ukraine continues its confrontation with russian cyber forces. In December 2023, there was a serious cyberattack against one of the national mobile operators, called Kyivstar. The consequences of the attack were devastating: the company's customers were cut off from communication for at least several days, and the recovery process lasted for several weeks. russian hackers also took advantage of this situation by sending out malware emails. russian hackers are still active and synchronise their actions with the overall russian military strategy (for example, attacking Ukraine's agricultural sector while launching missile strikes). Likewise, the ART groups working against Ukraine hardly change.

Ukraine is strengthening its national cybersecurity system. On a closed-door meeting of the National Coordination Centre for Cybersecurity (NCCC) of the National Security and Defence Council of Ukraine (NSDC) a number of decisions were made to urgently strengthen the security of Ukraine's electronic communications system, its facilities and infrastructure. The participants also discussed the priority areas for the implementation of the Tallinn Mechanism and the optimisation of international cooperation in the cybersecurity field. In addition, the scenario of the third annual command and staff exercises held by the NCCC in December, for the first time included the task of practicing offensive measures of active cyber defence.

1. CYBERSECURTY SITUATION IN UKRAINE

AT THE NATIONAL COORDINATION CENTRE FOR CYBERSECURITY (NCCC) MEETING, IT WAS DECIDED TO STRENGTHEN THE SECURITY OF UKRAINE'S ELECTRONIC COMMUNICATIONS SYSTEM, ITS FACILITIES AND INFRASTRUCTURE

The National Coordination Centre for Cybersecurity (NCCC) of the National Security and Defence Council of Ukraine (NSDC) held a meeting on 21st December 2023. During the meeting the participants discussed important issues related to the creation of a big data processing system based on Big Data technologies in the interests of the state's security and defence; the relevant instructions were given following the results of the meeting, The participants also considered a number of legislative initiatives in the cybersecurity field proposed by the Security Service of Ukraine (SSU), in particular those aimed at ensuring effective counteraction to attacks on the foundations of Ukraine's national security committed through cyberspace.

A number of decisions were made in a closed session aimed at urgently strengthening the security of Ukraine's electronic communications system, its facilities, and its infrastructure. The participants also discussed the priority areas for the implementation of the Tallinn Mechanism and the optimisation of international cooperation in the cybersecurity field.

THE NATIONAL COORDINATION CENTRE FOR CYBERSECURITY (NCCC) HELD THE STRATEGIC-LEVEL TABLE-TOP EXERCISES

For the third time the National Coordination Centre for Cybersecurity (NCCC) of the National Security and Defence Council of Ukraine (NSDC) held the annual strategic-level table-top exercises (TTX) 'National Cyber Readiness 2023' aimed at strengthening the national cybersecurity system. During the exercise, experts practiced mechanisms and skills for making strategic decisions in responding to large-scale cyberattacks and special information operations that accompany such attacks. The scenario included a task to practice offensive measures of active cyber defence for the first time.

RECORDED FUTURE CONTINUES TO PROVIDE CRITICAL INTELLIGENCE TO PROTECT UKRAINE FROM CYBER AND PHYSICAL THREATS RECORDED FUTURE CONTINUES TO PROVIDE CRITICAL INTELLIGENCE TO PROTECT UKRAINE FROM CYBER AND PHYSICAL THREATS

Recorded Future, the world's largest private intelligence and analysis company, will continue helping Ukraine to protect its critical infrastructure from russian military and cyber aggression in 2024. The total investment in support of Ukraine this year will exceed $23 million.

Since the beginning of the full-scale invasion, the company has provided intelligence to protect Ukraine's critical infrastructure, helped to investigate russian war crimes, and opened access to the Intelligence Cloud software platform for more than $10 million.

ICELAND JOINS THE IT COALITION

Iceland joins the IT Coalition. Since the beginning of russia's full-scale invasion of Ukraine, Iceland has provided humanitarian, economic and security support to Ukraine, mostly through international organisations such as the UN, the World Bank, NATO, and other multinational forums.

Rustem Umierov, the Minister of Defence of Ukraine, thanked the government and people of Iceland for their strong support, which will help Ukraine strengthen its information technology, communications, and cybersecurity sectors. The IT Coalition currently includes eight countries: Estonia, Luxembourg, Belgium, Denmark, Iceland, Latvia, Lithuania, and Japan. The UK and Italy have also announced their intention to join.

THE NATIONAL COORDINATION CENTRE FOR CYBERSECURITY (NCCC) STEPS UP COOPERATION WITH META TO STRENGTHEN UKRAINE'S INFORMATION AND CYBER RESILIENCE

Nataliia Tkachuk, Head of the Information Security and Cybersecurity Service of the National Security and Defence Council of Ukraine (NSDC), held a working meeting with Kateryna Kruk, Head of Regional Public Policy for Central and Eastern Europe at Meta. The parties discussed strategic cooperation in countering information attacks and combating financial phishing. Among other things, the parties discussed cooperation on the Protective DNS phishing domain filtering system and countering the spread of phishing campaigns on social media.

THE MINISTRY OF DIGITAL TRANSFORMATION OF UKRAINE AND ECSO SIGNED A MEMORANDUM OF COOPERATION

The Ministry of Digital Transformation of Ukraine and the European Cyber Security Organisation (ECSO) have signed a memorandum of cooperation. This will help strengthen Ukraine's cyber defence system in line with international standards. It will also provide access to the EU cybersecurity market for Ukrainian companies and specialists. In addition, cooperation with the ECSO will help to:

- provide Ukrainian specialists with access to training resources for advanced training and professional development;
- organise the promotion of Ukrainian startups in the field of cybersecurity and attract investors;
- provide support for scientific and technical projects.

THE STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE (SSSCIP) ESTABLISHES COOPERATION WITH JICA

Satoshi Sugimoto, the Resident Representative of the Japan International Cooperation Agency (JICA) in Ukraine, visited the State Service of Special Communications and Information Protection of Ukraine (SSSCIP). The Japanese guest had the opportunity to get acquainted with the work of the SSSCIP and discuss potential areas of cooperation, in particular, cyber defence of public information systems, critical infrastructure protection, the Army of Drones, ensuring the broadcasting of Ukrainian television and radio, etc.

THE CABINET OF MINISTERS OF UKRAINE ADOPTS THE ACTION PLAN FOR FURTHER IMPLEMENTATION OF THE CYBERSECURITY STRATEGY OF UKRAINE

The Government has enacted the Ordinance 'On Approval of the 2023–2024 Action Plan for the Implementation of the Cybersecurity Strategy of Ukraine'. The document specifies tasks and measures to achieve the Strategy's objectives and lays down performance indicators and deadlines. The key areas of activities under this plan include regulatory and legal framework for cybersecurity, cyber protection, and cyber defence, establishing closer cooperation with international partners, etc.

CERT-UA TEAM RANKS FIRST AT THE U.S. MARINE CORPS CYBER TRAINING

Experts of the Computer Emergency Response Team of Ukraine CERT-UA has won the first place at the Cyber Gators 2023, the international cybersecurity competition, which took place at the CYBER RANGES technology training ground in Orlando, Florida (USA) and was organised by the U.S. Marine Corps.

Seven cyber defence teams from Ukraine, the United States, Canada, and other countries, took part in the competition. The training included the implementation of defence scenarios against multiple complex threats. Ten hours were provided to complete 109 tasks. Ukrainian cyber defenders managed to complete all within six hours.

THE MINISTRY OF DIGITAL TRANSFORMATION OF UKRAINE HAS LAUNCHED CISCO EDUCATIONAL COURSES ON DIIA.EDUCATION

Cisco Academy has translated 9 of its own educational courses into Ukrainian to help Ukrainians expand their knowledge in these areas. These include introduction to cybersecurity, network devices and initial configuration, endpoint security, network defence, cyber threat management, and more. You can view the courses by following the link – https://osvita.diia.gov.ua/korysni-posylannya?category=cisco-courses

THE STATE SERVICE OF SPECIAL COMMUNICATION AND INFORMATION PROTECTION OF UKRAINE (SSSCIP) PERSONNEL WERE TRAINED AS FACILITATORS ACCORDING TO AMERICAN STANDARDS

At the end of November, a training session for facilitators of Table-top Exercises was held in Krakow, Poland. This training marked the first of its kind within the framework of exchanging best practices and participating in cybersecurity through courses, training, joint exercises, and the implementation of collaborative cybersecurity projects, following the Memorandum of Cooperation on Cybersecurity between the State Service of Special Communication and Information Protection of Ukraine (SSSCIP) and Cybersecurity and Infrastructure Security Agency (CISA).

THE STATE SERVICE OF SPECIAL COMMUNICATION AND INFORMATION PROTECTION OF UKRAINE (SSSCIP) AND THE GERMAN PARTNERS STRENGTHEN PARTNERSHIPS ON CYBERSECURITY

The Cybersecurity Training Program for Public Sector specialists is currently being designed at the State Service of Special Communication and Information Protection of Ukraine (SSSCIP) initiative and supported by the Government of Germany and implemented by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH. It is aimed at supporting Ukraine in fostering professionals in line with European cybersecurity standards and requirements to enhance global cyber resilience.

Three pilot trainings for public officials of various levels have already taken place, they were held online and implemented by Deloitte. The next phase of the project is scheduled to begin in 2024. In the long term, the project will help build a sustainable, open, and secure cyber environment between European partners and Ukraine, share experience in European cyber policy and law making given our country's path to EU accession, and increase human resources in the field of cybersecurity.

THE STATE SERVICE OF SPECIAL COMMUNICATION AND INFORMATION PROTECTION OF UKRAINE (SSSCIP) REPRESENTATIVES ATTEND A TRAINING EVENT ARRANGED BY THE INTERNATIONAL TELECOMMUNICATION UNION (ITU)

The State Service of Special Communication and Information Protection of Ukraine (SSSCIP) representatives took part in interregional trainings of European and Asia-Pacific countries organised by the International Telecommunication Union (ITU). Ukrainian cyber defenders took first place twice during practicing exercises in a joint team with the Spanish National Institute of Cybersecurity (INCIBE) delegation, and they respectively took second and seventh place in two more exercises.

Furthermore, Ukrainian cyber defenders participated in panel discussions on cybersecurity situation in Europe and Asia-Pacific, critical information infrastructure protection strategies, national planning of cyber crisis response, and the role of partnerships in cyber diplomacy. In total, more than 70 teams and more than 200 participants from 40 countries took part in the event.

FRENCH LAW ENFORCEMENT OFFICERS CONDUCTED TRAINING FOR UKRAINIAN POLICE OFFICERS

Law enforcement officers from various departments, in particular, the National Police Criminal Analysis Department and the Cyberpolice Department officials have improved their skills in the criminal analysis field during the week. Foreign colleagues shared their experience of using the latest methods and tools in the field of collection, processing, systematisation, and analysis of the information on crime prevention and countermeasures. Special attention was paid to the practical aspects of strategic analysis, as well as countering cybercrimes.

THE SECURITY SERVICE OF UKRAINE (SSU) AND THE NATIONAL POLICE OF UKRAINE (NPU) LIQUIDATED MORE THAN 100 FRAUDULENT CALL-CENTRES THAT STOLE PERSONAL DATA AND MONEY OF UKRAINIANS DURING THE ONE DAY

The Security Service of Ukraine (SSU) cyber specialists and the National Police of Ukraine (NPU) officials have conducted a multi-stage special operation throughout the territory of Ukraine. As a result of comprehensive measures, more than 100 call-centres who stole personal data, including passport details, phone numbers, etc., and savings of Ukrainians and foreign citizens, were stopped in one day. Further this information could be passed to the russian special services, which use it for remote recruitment of new agents.

RUSSIAN HACKERS ATTACKED USERS IN UKRAINE AND POLAND USING EMAILS CONTAINING LINKS TO 'DOCUMENTS'

On 15th-25th December the Computer Emergency Response Team of Ukraine (CERT-UA) discovered the APT28 group sending e-mails with links to 'documents', following which caused malware infections. The entities from Poland were also targeted alongside Ukrainian users. See more about the incident on the CERT-UA website: https://cert.gov.ua/article/6276894

THE GOVERNMENT HAS APPOINTED YURII MYRONENKO AS A NEW HEAD OF THE STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE (SSSCIP)

The Cabinet of Ministers of Ukraine has appointed Yurii Myronenko, the military officer and the unmanned aerial vehicles (UAV) strike squadron commander, at the position of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) Head. The new head announced that he will present a plan for the SSSCIP development in the nearest time.

Yurii Myronenko has experience in corporate management and a great expertise in UAV specifics. Prior to his assignment, he served as commander of a UAV strike squadron operating in the Zaporizhzhia region.

THE ARMED FORCES OF UKRAINE (AFU) CYBER SPECIALISTS ATTACKED 15 WEBSITES OF RUSSIAN ENTERPRISES

On the day of the russian strategic missile forces on 17th December, the Armed Forces of Ukraine (AFU) cyber specialists attacked 15 websites of companies participating in the engineering support of russian troops. On the websites of 15 russian companies appeared the inscription 'They aim at NATO but will hit moscow'. This is how the Ukrainian military reminded the russians about the failed tests of the Yars and Bulava missiles, which went off course during the tests.

THE TELECOMMUNICATION SERVICES OPERATOR KYIVSTAR WAS SUBJECTED TO A POWERFUL CYBERATTACK BY THE SANDWORM (THE GROUP CONTROLLED BY THE RUSSIAN MAIN INTELLIGENCE DIRECTORATE)

A large-scale technical failure in the Kyivstar network, which caused the unavailability of communication and Internet services for some subscribers occurred in the morning of 12th December. The mobile operator confirmed that the cause of the large-scale disruption on the morning of 12th December was a powerful hacker attack and assured that the personal data of customers were safe. The outage in the operator's network affected national roaming, preventing users from switching to another operator. The air warning system did not work in several cities.

Responsibility for the attack was claimed by one of the russian hacker groups, which the russian media call 'solntsepek'. According to the Security Service of Ukraine (SSU), it is a hacking unit of the main department of the russian federation armed forces general staff, which in this way publicly legalises the results of its criminal activities. The SSU has initiated a criminal proceedings under eight articles of the Criminal Code of Ukraine.
The company general director reported that hackers broke the Kyivstar protection through an employee account.

RUSSIAN HACKERS USED THE KYIVSTAR DISRUPTION ISSUE TO SEND EMAILS WITH MALICIOUS SOFTWARE

The Computer Emergency Response Team of Ukraine (CERT-UA) specialists detected mass emails with the subject related to 'overdue payment under the Kyivstar contract' and an attached archive 'Заборгованість абонента.zip' ('Contractor's debts.zip'). Ukrainians received emails related to 'overdue payment under the Kyivstar contract' containing an attached archive 'Заборгованість абонента.zip' ('Contractor's debts.zip') with embedded password-protected RAR archives.

CERT-UA specialists recommend filtering emails containing password-protected attachments (both archives and document files) at the email gateway level. See more about the incident at: https://cert.gov.ua/article/6276824

2. THE FIRST WORLD CYBER WAR

RUSSIAN HACKERS USE ISRAEL-HAMAS WAR TO CONDUCT CYBER ESPIONAGE CAMPAIGNS – IBM X-FORCE

On 8th December IBM X-Force has declared that uncovered multiple lure documents (relating to the Israel-Hamas war) which are used by criminals from ITG05 to facilitate the delivery of the ITG05 Headlace backdoor. The campaign is directed against targets based in at least 13 nations worldwide (including Ukraine, Germany, Hungary, Italy, Poland, and others) and leverages authentic documents created by academic, finance, and diplomatic centres. The campaign has a highly targeted nature. X-Force tracks ITG05 which is likely sponsored by russia, the activity of which intersects with such permanent threats groups as APT28, UAC-028, Fancy Bear, and Forest Blizzard.

APT GAMAREDON REMAINS THE MAIN RUSSIAN CYBER THREAT AIMED AT UKRAINE – THE CISCO TALOS REPORT

On 5th December, the cybersecurity company Cisco Talos released its annual report on cybersecurity trends in 2023. A separate section is devoted to Ukraine. It emphasies that russian state company APT Gamaredon remains a major player in threats against Ukraine. Almost ¼ of their attacks are targeted at Ukraine's transport sector.

IN SUMMER 2023, RUSSIA TRIED TO CARRY OUT CYBERATTACKS AGAINST ENTERPRISES OF UKRAINE'S AGRICULTURE SECTOR – MICROSOFT REPORT

Microsoft published the results of its next study on russia's hostile activity in information space and cyberspace. Among the conclusions about the convergence of cyber, information and kinetic efforts of russia in relation to Ukraine, a noticeable trend in summer 2023 was mentioned, when russia changed the focus of its efforts to the agriculture sector. This was manifested not only in cyberattacks on product storage systems, but also in cyberattacks on agriculture business with the aim of stealing data and malware deploying. Among such examples, a successful cyberattack on an unnamed Ukrainian agricultural equipment organisation was mentioned.

XDSPY CYBER SPIES FROM ATTACKED RUSSIAN METALLURGISTS AND MILITARY-INDUSTRIAL COMPLEX (MIC) ENTERPRISES

On 4th December the Cyber Wire reported with reference to the russian company F.A.C.C.T. that malicious mailings targeting the mail of one of the russian metallurgical enterprises, as well as a Research Institute (RI) engaged in the development and production of guided missiles were detected. Technical details were given in the blog on Habr.

RUSSIAN APT28 USED ZERO-CLICK OUTLOOK EXPLOIT

On 8th December, Security Week reported with reference to Palo Alto Networks that the russian state threat group APT28 exploited the Outlook vulnerability (CVE-2023-23397) in attacks targeting nearly 30 organisations in 14 countries, including NATO countries. This critical vulnerability, which can be activated via crafted email messages without requiring the recipient to open the email, was first discovered in March 2023, and was exploited by APT28 for approximately 20 months.

The targets of the attack were mainly organisations in NATO countries, including defence, energy, transport, and government organisations. Despite public awareness APT28 continued to exploit the vulnerability, indicating significant value of the intelligence data obtained for russian military interests.

This exposure follows a recent Microsoft update that attributes the use of CVE-2023-23397 to APT28, also known as Fancy Bear, which is notorious for various cyberattacks, including hacking attacks during the 2016 USA elections.

HACKERS FROM ASIA ARE THE MOST ACTIVE AMONG THE ADVANCED GROUPS, – THE RUSSIAN STATE COMPANY SOLAR PRESENTED THE CYBER THREATS TRENDS

The russian state cybersecurity company Solar report indicates that China and North Korea are the key sources of offensive cyber campaigns against russia in 2023. The report identifies China-related activities as aggressive cyber espionage campaigns targeting russian organisations, while North Korean actors focus on gathering information on developments in missile technology. Commentators note that these actions raise questions about diplomatic relations between the russian federation and these countries, considering russia's efforts to strengthen ties with China and North Korea. Despite their alleged cyber activity, moscow seems to be tolerating these actions, probably because of the help these countries are giving russia in the war against Ukraine. The report says that diplomatic relations do not necessarily extend to cyberspace, emphasising the complex dynamics in the geopolitical landscape.

LEADER OF RUSSIAN HACKTIVIST GROUP KILLNET 'RETIRES' AND APPOINTS NEW HEAD

Killmilk, the leader of the pro-russia hacktivist group Killnet, announced his 'retirement' in early December. Killnet's new 'owner' according to a separate post on the group's official Telegram channel is the Deanon Club group head. He stated that he and Killmilk had been friends for a long time, and that 'this is the person who brought me to the masses'.

Two groups did indeed have collaborated in the past. In February 2023, they established a forum and marketplace called Infinity, which offers a range of hacking services and even paid tutorials for would-be criminals.

THE DEFENCE INTELLIGENCE OF UKRAINE (DI) REPORTED THAT THEY ATTACKED RUSSIA'S TAX SYSTEM

During the attack of the special operation, the military intelligence agents managed to penetrate one of the well-protected key central servers of the russian federal tax service and then into more than 2,300 of its regional servers throughout russia, as well as in the territory of temporarily occupied Crimea. Simultaneously, the russian IT company Office.ed-it.ru, which served the russian federal tax service was attacked in the same way.

The Defence Intelligence of Ukraine (DI) reports that as a result of two cyberattacks, the configuration files, which for years ensured the functioning of the russian federation extensive tax system, were eliminated; the entire database and its backup copies were destroyed. The connection between the central office in moscow and 2,300 russian territorial administrations is paralysed, as well as between the russian federal tax service and Office.ed-it.ru, which was a tax data centre (data bank).

RUSSIAN FOREIGN INTELLIGENCE SERVICE SPOTTED EXPLOITING JETBRAINS VULNERABILITY

On 13th December government agencies in the U.S., Poland, and the U.K. said that russia's foreign intelligence service (SVR) were exploiting a vulnerability that had been exposed earlier in 2023 in a popular product from Czech software company JetBrains. The attacks which were attributed to APT29, also known as CozyBear or Midnight Blizzard began in September.

Numerous companies around the world were compromised, affecting sectors, such as energy, software, customer service, financial management, and IT. JetBrains published a patch for the issue in September, but unpatched servers led to its exploitation by a range of ransomware groups.