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

March 2024

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

ACRONYMS

AI	Artificial Intelligence
CEO	Chief Executive Officer
CISA	Cybersecurity and Infrastructure Security Agency
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service
ENISA	European Union Agency for Cybersecurity
EU	European Union
EW	Electronic Warfare
FSB	Federal Security Service (russian federation)
GPS	Global Positioning System
GRU	Main Directorate of the General Staff of the Armed Forces of the rus sian federation
HUR	Main Intelligence Directorate of Ukraine
IT	Information Technology
LLC	Limited Liability Company
NATO	North Atlantic Treaty Organization
NCSCC	National Cybersecurity Coordination Center
NGO	Non-Governmental Organization
NIST	National Institute of Standards and Technology (U.S. Department of Commerce)
NSA	National Security Agency (U.S.)
NSDC	National Security and Defense Council of Ukraine
OFAC	Office of Foreign Assets Control (U.S. Department of Treasury)
PJSC	Public Joint Stock Company
SBU	Security Service of Ukraine
SIENA	Secure Information Exchange Network Application
SSSCIP	State Service of Special Communications and Information Pro tection of Ukraine
TIDE	Think-Tank for Information Decision and Execution
U.S.	United States
UAH	Ukrainian Hryvnia
UK	United Kingdom

KEY TENDESES

The European Union (EU) is finalizing the adoption and implementation of the Cyber Resilience Act, which will significantly alter security regulations within the EU. This is accompanied by the EU developing measures to regulate Artificial Intelligence (AI) use: the European Parliament intends to pass the Artificial Intelligence Act, which will govern AI based on potential risks and impacts. While the EU primarily focuses on bolstering cyber defenses, analysts are evaluating how existing cyber security agencies like the Computer Security Incident Response Team (CSIRT) could be more beneficial in ensuring cyber security across Europe. A key takeaway is the need for these organizations to adopt a more proactive approach in their operations.

President of Ukraine Volodymyr Zelenskyy identified information and cybersecurity as among the five priorities of the National Security and Defense Council (NSDC) when he presented the newly appointed NSDC Secretary, Oleksandr Lytvynenko. This includes strengthening protection against hostile destabilization operations, enhancing coordination among all state institutions, and developing Ukraine's offensive cyber potential. According to NSDC Deputy Secretary Serhii Demedyuk, considering its experience in cyber warfare with the russian federation, Ukraine is no longer a testing ground for russia's capabilities and can become a regional leader in cybersecurity, initiating changes in international approaches to aggression in cyberspace.

Following a series of cyber incidents targeting organizations in the water supply sector, the U.S. is actively reviewing its policy regarding this sector. In addition to CISA updating relevant recommendations, the White House announced plans to establish a new working group aimed at protecting the water sector from state-sponsored cyberattacks. The perception of threats in the space domain is becoming increasingly serious: the U.S. is actively enhancing its cyber defense capabilities in this domain and incidents involving physical security of underwater cables could have long-term consequences for global availability of the Internet.

There is a noticeable escalation of diplomatic confrontation between Western countries and China regarding the latter's possible responsibility for interference in the work of parliamentary institutions worldwide. The U.S. Department of Justice released its conclusion that Chinese hackers targeted European legislators, including members of the Inter-Parliamentary Alliance on China, while the British government officially accused China of cyberattacks on democratic institutions in the United Kingdom (UK). Finland and New Zealand also attribute cyberattacks on their parliaments to Chinese hacker groups. Apparently, such activity is linked to the fact that a number of democratic countries will have elections in 2024 and these countries are concerned about possible interference. For example, the European Union Agency for Cybersecurity (ENISA) updated its guidance to ensure cybersecurity in the electoral process, and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) developed procedures to protect the electoral process based on «Super Tuesday» in March 2024.

The Ivanti vulnerability continues to pose problems for cybersecurity agencies and consumers worldwide. Agencies of the Five Eyes Alliance warn that threat actors may actively exploit this vulnerability to maintain their presence in affected systems. Meanwhile, the U.S. National Security Agency (NSA) confirmed that threat actors are already using this vulnerability to target defense sector enterprises. In an effort to strategically mitigate threats, the Pentagon promptly approved a separate Strategy for Cybersecurity of the Defense Industrial Base. CISA even had to disconnect several of its systems to prevent cyberattacks on them. For the U.S., the situation with Ivanti is further complicated by the need to address another issue: dealing with the aftermath of the February cyberattack by Blackcat hackers against Change Healthcare systems. This attack had adverse effects on the country's entire healthcare system, which heavily relies on insurance. Change Healthcare processes around 50% of medical claims in the U.S., involving approximately 900,000 physicians, 33,000 pharmacies, 5,500 hospitals, and 600 laboratories. The Department of Health and Human Services opened an investigation into the incident, and the U.S. Department of State announced a $10 million reward for information on the Blackcat group.

russia's cyber activity is becoming increasingly extensive. Cybersecurity firms continue to investigate russian cyber operations against European non-governmental organizations (NGOs), and the extent of the Midnight Blizzard group's cyber intrusions into Microsoft systems is still not fully understood. Additionally, it has been revealed that russian hackers targeted political parties in Germany and are actively testing the wiper AcidPour (a modification of AcidRain that was used at the beginning of russia's military invasion of Ukraine against KA-SAT modems), a virus designed to destroy data in the affected system. It appears that the updated virus, targeting Linux x86 systems, may have been used against several telecommunications operators in Ukraine.

In March, Ukraine's Main Intelligence Directorate (HUR) reported a successful special operation against the russian federation Ministry of Defense, during which the Security Service of Ukraine (SBU) obtained access to servers and a trove of classified documentation. SBU cyber experts halted the supply of components for russian drones and cruise missiles, and are also actively engaged on the frontlines in neutralizing enemy electronic warfare (EW) and reconnaissance systems, as well as intercepting drones coordinating missile and artillery strikes against Ukrainian defense forces.

1. CYBERSECURITY SITUATION IN UKRAINE

PRESIDENT OF UKRAINE INTRODUCED THE NSDC SECRETARY, OLEKSANDR LYTVYNENKO, AND OUTLINED FIVE KEY TASKS FOR THE COUNCIL, INCLUDING

On March 29, President Volodymyr Zelenskyy introduced the newly appointed NSDC Secretary, Oleksandr Lytvynenko. The President outlined the key tasks for the new NSDC Secretary, including strengthening Ukraine's forecasting capabilities, sanction policy, doctrinal work, and the work of the Supreme Commander-in-Chief's Staff; information and cybersecurity; drafting decisions; and monitoring their implementation.

NSDC WILL PLAY A KEY ROLE IN COORDINATING AND DEVELOPING UKRAINE'S OFFENSIVE

Cybersecurity and information security, which President Zelenskyy highlighted as paramount areas, stand at the forefront of the revamped agenda of Ukraine's NSDC. This strategic focus encompasses fortifying defenses against hostile destabilization endeavors, fostering coordination among all governmental bodies in this domain, and bolstering the nation's offensive cyber capabilities. PresidentZelenskyy underscored these priorities when introducing the newly appointed NSDC Secretary, Oleksandr Lytvynenko.

THE NCSCC IS DEEPENING COOPERATION WITH THE EUROPEAN COMMISSION TO ENHANCE CYBERSECURITY IN UKRAINE AND EU COUNTRIES

NSDC Deputy Secretary Serhii Demedyuk, Head of the Service for Information Security and Cybersecurity of the NSDC Apparatus Nataliia Tkachuk, and Head of the Department for Ensuring the Activities of the National Cybersecurity Coordination Center (NCSCC) Serhii Prokopenko held a working meeting with the Head of the National and State Security Department of the European Union Advisory Mission Juha Vehmaskoski on March 14 to discuss key aspects of cooperation between Ukraine and the EU in the field of cybersecurity. They paid special attention to ways of deepening practical cooperation to effectively develop Ukraine's national cybersecurity system and exchange of experience with EU countries.

MINISTRY OF DEFENSE PRESENTED INNOVATIVE SOLUTIONS FOR DIGITIZING NATO

Representatives from the Ministry of Defense Innovation Center participated in the annual NATO Think-Tank for Information Decision and Execution (TIDE) Sprint 2024 conference in Dresden, Germany, which contributes to developing NATO's military IT systems and partner countries. They demonstrated how cloud computing and big data processing can be used to digitize existing NATO standards and shared their experience in developing the DELTA combat space management ecosystem. Special attention was given to improving cybersecurity processes, a technology for integrating drones into the DELTA system, and other systems. The integration is made possible through cooperation with the Ministry of Digital Transformation, partners from NGO Aerorozvidka, and the company Cossack Labs.

THE RUSSIAN FEDERATION IS CONDUCTING CYBER WARFARE NOT ONLY AGAINST UKRAINE BUT ALSO AGAINST EU AND NATO COUNTRIES

Nataliia Tkachuk, head of the NSDC Information Security and Cybersecurity Service and NCSCC Secretary, stated during an event at the Chernivtsi Military Administration that cyberattacks have become an integral tool the enemy uses against Ukraine. «However, today russia is waging cyber warfare not only against our state but also against European Union and NATO countries. We understand that the cyber war will continue even after the cessation of hostilities on the battlefield. Therefore, it is more important than ever to be able to effectively and promptly respond to cyber threats at all levels: both nationally and regionally within the country, as well as internationally, by collaborating with our partners,» – noted the NCSCC Secretary.

UKRAINE AIMS TO BECOME A REGIONAL LEADER IN CYBERSECURITY

During the National Academy of the Security Service's XV All-Ukrainian Scientific and Practical Conference «Current Issues of State Information Security Management», NSDC Deputy Secretary Serhii Demedyuk stated, «Ukraine cannot wait for the international community to start normatively distinguishing cyber aggression from cybercrime, and must initiate this process now, because Ukraine is no longer a testing ground for russian cyberattacks, it is already a frontline. Given our experience, we should become a regional leader in cybersecurity.»

THE REGIONS ACCOUNT FOR 90% OF CRITICAL CYBER INCIDENTS

Ukraine's NCSCC and the National Cybersecurity Department of Romania conducted offline cybersecurity trainings for representatives of communities, critical infrastructure facilities, and students in Chernivtsi Oblast. The NCSCC noted that 90% of critical cyber incidents occur in the regions. Therefore, during the event, over 50 representatives of cybersecurity agencies and critical infrastructure facilities in the oblast extensively discussed key cybersecurity threats in the regions and avenues for countering them. The training put special attention on problematic issues in regional-level cooperation and challenges in raising awareness about cybersecurity.

SUPPORTED BY NCSCC, TRAINING BEGAN FOR VETERANS UNDER THE "CYBER DEFENDERS" REINTEGRATION PROGRAM

The program's main goal is to provide veterans with the necessary skills and knowledge for a successful career in cybersecurity. The project includes comprehensive training in cyber defense and cybersecurity and facilitating employment in the public sector or cybersecurity institutions in Ukraine. Throughout the course, participants will learn about cybersecurity principles and their applications, encryption techniques and their role in information protection, and recognizing and responding to various types of cyberattacks.

GOOGLE IS LAUNCHING A FREE ONLINE EDUCATIONAL PROGRAM, «CYBERSECURITY

The «Safer with Google» program is designed for owners, managers, and employees of small and medium-sized enterprises who want to protect their business from cyber threats, gain practical knowledge about cyber hygiene, and recognize cyber attacks. The curriculum includes four educational modules with practical tasks, business cases, and optional one-on-one consultations. Participants will benefit from the experience of leading Ukrainian experts in business and customer data protection. More information about the program and registration: eventsonair.withgoogle.com/events/google-for-business-ua-smb

MINISTRY OF DIGITAL TRANSFORMATION, CYBER POLICE, AND NGO MAGNOLIA LAUNCHED A PORTAL FOR REPORTING INCIDENTS OF CHILD SEXUAL VIOLENCE

On March 4, Ukraine launched its first portal for reporting materials related to child sexual violence online, called StopCrime. Anyone can anonymously report a possible crime related to sexual violence against children on the internet at stopcrime.ua/net-crime. The most important thing is to provide the link where the content is posted. For further investigation and blocking of such content, NGO Magnolia, as a member of the International Network, will collect, analyze, and transmit it to the Cyber Police Department and Interpol.

CYBER POLICE HEAD YURIY VYHODETS PARTICIPATED IN A 2-DAY TRAINING ON IMPROVING THE UNIT'S WORK

Public association Global Cyber Interactions Center initiated a session on shaping the image of the Cyber Police, where participants discussed strategies for cooperating with the public and increasing trust in the Cyber Police. They also explored development strategies for the Cyber Police to enhance its effectiveness and international image, including tackling online fraud, participating in international operations, and collaborating with Europol through the Secure Information Exchange Network Application (SIENA). Participants also discussed cybersecurity, combating cybercrime, and obtaining digital evidence.

REPRESENTATIVES OF THE NCSCC AND THE ROMANIAN CYBERSECURITY DIRECTORATE CONDUCTED LECTURES FOR STUDENTS OF YURIY FEDKOVYCH CHERNIVTSI NATIONAL

As part of their working visit to Chernivtsi, representatives of the NSDC's NCSCC and the National Cybersecurity Directorate of Romania held an event for students of Yuriy Fedkovych Chernivtsi National University. NCSCC experts emphasized the importance of cybersecurity professions and shared their experience and knowledge of international cooperation and countering hacker groups. The Romanian guests presented important information about cyber hygiene rules and introduced a guide on the safe use of social media, which will serve as a useful tool for the younger generation in the modern world.

STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE (SSSCIP) ACTIVELY USES CYBER RANGES FOR TRAINING AND EXERCISING CYBERSECURITY PROFESSIONALS

At the conference «Digital Transformation as a Catalyst for European Integration of Ukraine», SSSCIP Deputy Chairman Oleksandr Potii revealed that the SSSCIP actively uses cyber ranges for training not only its own specialists but also professionals from other government institutions and critical infrastructure facilities. Training takes place both at the SSSCIP's own facilities and at platforms provided by partners from the United States, Estonia, and other countries. In the near future, similar ranges are planned to be built at regional cybersecurity centers, which will enable creating a network that will provide training both locally and remotely for specialists across the country.

THE SSSCIP'S INDUSTRY COUNCIL BEGAN WORKING ON DEVELOPING PROFESSIONAL

The industry council will be involved in organizing and developing professional standards in information technology, cybersecurity, and information protection. Council members will also participate in developing education standards, standards, and tools for assessing qualifications and learning outcomes, and in forecasting the needs for relevant personnel. The industry council includes representatives of state bodies responsible for cybersecurity, educators, researchers, and professional and public community representatives. During the first meeting, they discussed issues related to building human resource capacity and creating the National Qualifications Framework for Cybersecurity in Ukraine, introducing professional standards in the industrial sector and educational institutions, and the 2024 work plan.

«CYBER DIAGNOSTICS OF CRITICAL INFRASTRUCTURE: STRENGTHENING DIGITAL PROTECTION» CONFERENCE TOOK PLACE WITH USAID SUPPORT

Participants exchanged experiences and ideas gained during the Cybersecurity Diagnostics Program for Critical Infrastructure Operators from the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The program was developed based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework guidelines, which help organizations enhance digital protection. Currently, 40 cyber diagnostics have been launched, and 20 organizations have received initial results. Participants also familiarized themselves with the regulatory requirements for conducting cyber diagnostics and approaches to assessing the level of cybersecurity for critical infrastructure operators.

FINANCIAL SECTOR PROFESSIONALS TRAINED IN DEFENDING AGAINST CYBERATTACKS

With support from the EU4DigitalUA project, the SSSCIP conducted CIREX.CYBER. Ransomware joint-staff exercises, in which nearly three dozen experts from government agencies and private financial sector organizations learned how to combat cyberattacks using ransomware programs and about how various bodies, institutions, and enterprises can effectively interact with each other, promptly exchange information about cyber incidents, and, in case of problems, find ways to resolve them.

STATE CYBERSECURITY CENTER, IN COLLABORATION WITH UNIT 42 PALO ALTO NETWORKS, CONDUCTED RESEARCH ON SMOKELOADER MALICIOUS SOFTWARE

The SSSCIP State Cybersecurity Center collaborated with the Unit 42 threat research team at Palo Alto Networks to conduct a detailed analysis of the SmokeLoader malware. The investigation focused on tracking the distribution of SmokeLoader in Ukraine from May to November 2023. During this period, a significant increase in attacks associated with this software was recorded, targeting the government, defense, and financial sectors. The report analyzed 23 waves of phishing attacks.

MAIN INTELLIGENCE DIRECTORATE REPORTED ON NEW LARGE-SCALE ATTACKS ON RUSSIA

Both russian state entities and private organizations that pay taxes and finance the war against Ukraine have come under attack. During March 11-18:

- PJSC Rostelecom resources were targeted – communication equipment was disabled in the Zabaykalsky and Krasnoyarsk oblasts of the russian federation
- Access was gained to the electronic document management system of the Government of the Belgorod Oblast and fake emails were sent to 12,000 local officials
- Belznak LLC communication equipment was attacked and disabled
- Server infrastructure and backup copies of the 1Gb.ru hosting provider and tens of thousands of websites it serviced were seized and destroyed
- Over 40 Mikrotik networking devices were disabled in the City Electric Transport Management Center in Novosibirsk

The losses inflicted on the enemy could amount to hundreds of thousands of dollars.

SBU CYBERSECURITY EXPERTS BLOCKED THE SUPPLY OF COMPONENTS FOR A BATCH OF RUSSIAN SHAHED DRONES AND CRUISE MISSILES

Head of the SBU Cybersecurity Department Ilya Vitiuk stated during the telethon, «We are disrupting the supply chains of components for russian weapons. One example is the blocking of servo motors for 1,600 Shahed drones and 4,000 microchips for cruise missiles.» He also mentioned that cyber specialists are working on the front line to destroy enemy EW and reconnaissance systems, as well as intercept enemy drones coordinating missile and artillery strikes against Ukrainian defense forces.

HUR REPORTED ON A BREACH OF RUSSIA'S MINISTRY OF DEFENSE

HUR reported that it carried out another successful special operation against the aggressor state of russia, which resulted in obtaining access to russian federation Ministry of Defense serversrussia. The Ukrainian special service now possesses software for information protection and encryption that was used by russia's Ministry of Defense, as well as a large amount of the Ministry's classified official documentation,russia including orders, reports, directives, and other documents that circulated among more than 2,000 units of russia's military agency. The information obtained makes it possible to establish the complete structure of the russian federation Ministry of Defense and its branches.

THE SBU AND LAW ENFORCEMENT AGENCIES IN LATVIA NEUTRALIZED AN UNDERGROUND CALL CENTER THAT EXTORTED MONEY FROM EU CITIZENS

SBU cybersecurity experts, the National Police, Prosecutor's Office, and law enforcement agencies of the Republic of Latvia dismantled an international scheme for extorting money from investors on electronic exchanges. The criminals set up an underground call center posing as one of the EU's independent financial regulators and offered European depositors online exchange projects under the guise of «investment protection». In this way, the fraudsters hoped to extort millions of hryvnia from the victims. However, SBU operatives exposed the criminals at the outset, documented several instances of fraudulent manipulations, and apprehended the key perpetrators. They face up to eight years in prison.

THE SBU DETAINED AN «FSB MOLE» WHO WAS ATTEMPTING TO INFILTRATE THE POLICE IN ORDER TO SPY ON THE ADVANCE GUARD AND ARMED FORCES OF UKRAINE

SBU cybersecurity experts thwarted an attempt by the russian federation Federal Security Service (FSB) to «plant» an agent within the ranks of the Armed Forces of Ukraine. As a result of the special operation in Kyiv Oblast, a traitor was detained, who had, at the direction of the FSB, attempted to join the National Police and gather information about law enforcement agency units, particularly those belonging to the Ministry of Internal Affairs Advance Guard. He was recruited by the russian federation special services due to his pro-Kremlin comments on russian Telegram channels. He provided the geolocation of «desired» objects to his russian handler and received monetary rewards for it. During the search, his mobile phone with evidence of communication with the FSB was seized. The detainee is suspected of treason and could face life imprisonment.

CYBER POLICE IN KHARKIV OBLAST EXPOSED MEMBERS OF A CRIMINAL GROUP THAT MISAPPROPRIATED INTERNET USER ACCOUNTS

Law enforcement officials officially charged three members of an organized criminal group who misappropriated others' email accounts and Instagram profiles. The suspects used brute-force methods to guess passwords and, over the course of a year, amassed a database of stolen accounts belonging to over 100 million users worldwide. They resided in various regions of Ukraine and coordinated their activities online, forming databases to sell on the darknet. Currently, the perpetrators have been charged and face up to 15 years of imprisonment. Additionally, police are investigating the possibility of collaboration between the suspects and russian agents, as the stolen accounts were used for conducting information-psychological operations in the interests of the russian federation.

POLICE UNCOVERED A CRIMINAL GROUP THAT WAS LURING MONEY FROM PEOPLE THROUGH A PHISHING WEBSITE

Law enforcement authorities shut down the operations of scammers who, using phishing websites, stole personal data from citizens for unauthorized access to internet banking and conducted transactions from the victims' bank accounts. It has been determined that the losses from their actions amount to nearly UAH 119,000. Four suspects have been charged, facing up to eight years in prison.

SINCE THE BEGINNING OF THE YEAR, RUSSIAN HACKERS HAVE INTENSIFIED ATTACKS AGAINST UKRAINE

The first months of this year saw an increase in the number of cyber attacks carried out by russian hackers against Ukrainian information systems. Therefore, SSSCIP Head Yuriy Mironenko expects that 2024 will be more challenging for the country in terms of cyber warfare, according to his comment in The Economist. According to Mironenko, 10% of attacks are carried out by russian special services cyber units, while the rest are by affiliated criminal hacker groups. The most active russian cyber unit is Armageddon, which belongs to the FSB.

2. THE FIRST WORLD CYBER WAR

RUSSIA SEEKS TO EXPLOIT THE «WAR FATIGUE» IN THE WEST TO ACHIEVE VICTORY IN UKRAINE

A new study by the Insikt Group, published on February 29, focuses on russia's strategic approach to its war against Ukraine and how this approach interacts with Western perceptions and policies. In the Kremlin's view, Western countries are experiencing «war fatigue,» which makes further economic and military support for Ukraine increasingly unpopular. Despite this, russia acknowledges that the West has the capability to continue supporting Ukraine and seeks to influence elections in the West in 2024 and exploit political concerns about further support for Ukraine.

IN RUSSIAN UNIVERSITIES, STUDENTS ARE SYSTEMATICALLY TAUGHT HACKING, ACCORDING TO THE SBU

In an interview with Forbes magazine, head of the SBU Cybersecurity Department Ilya Vitiuk stated, among other things, that the SBU has documents indicating that the national system for scaling cyber aggression in russia has been operating since at least 2016. Active reserve officers of the Main Directorate of the General Staff of the Armed Forces of the russian federation (GRU) and the FSB teach students cyber warfare disciplines at military and technical universities. Students conduct scientific and technical work on creating software tools; study the architecture of Ukrainian and other countries' logistics, energy, and water supply systems; and write term papers and master's theses on the topic. After training, talented students may be employed by government intelligence agencies or special services.

MICROSOFT CONFIRMS THAT RUSSIAN HACKERS STOLE SOURCE CODE AND SOME CLIENT SECRETS

On March 8, Microsoft reported that the Kremlin-backed threat actor Midnight Blizzard (also known as APT29 or Cozy Bear) was able to access some of its source code repositories and internal systems following a breach disclosed in January 2024. The company emphasized that it has not found evidence that client systems hosted on Microsoft servers were compromised. Continuing to investigate the extent of the breach, Microsoft stated that a russian state entity is attempting to leverage various types of sensitive information obtained during the attack, including information exchanged via email between clients and Microsoft.

UKRAINIAN HACKERS HACKED THE MOSCOW METRO PAYMENT SYSTEM

On March 13, the Ministry of Digital Transformation reported that the Ukrainian IT army had attacked a number of russian government and local portals, including the Troika fare payment system, one of the largest ticket payment systems in russia, serving 38 regions. As a result of the «malfunction,» transportation card owners in Moscow and Kazan were unable to pay for tickets, top up their travel cards, or pay for parking.

ACCORDING TO THE NSA, RUSSIA WILL ATTEMPT TO INFLUENCE AMERICAN ELECTIONS IN ORDER TO WEAKEN SUPPORT FOR UKRAINE

On March 15, responding to journalists' questions, U.S. cybersecurity official Rob Joyce, said that, according to NSA data, russia's main efforts to undermine American elections will be aimed at reducing support for Ukraine. Special tools such as ChatGPT or other generative AI may play a significant role in this, allowing one person to produce a lot of authentic content at once.

GROUP ASSOCIATED WITH SANDWORM LIKELY DISRUPTED UKRAINIAN INTERNET SERVICE PROVIDERS

russian government-affiliated hackers are believed to be behind recent attacks on four small Ukrainian Internet service providers, leading to their week-long disruption. The Solntsepiok Group claimed responsibility for the incidents on its Telegram channel. Ukrainian officials have stated that there is evidence suggesting that this group is likely also responsible for the 2023 cyberattack on Kyivstar.

THE GPS AND COMMUNICATION OF MINISTER OF DEFENSE GRANT SHEPP'S AIRCRAFT WERE DISRUPTED DUE TO AN EW ATTACK

On March 15, russian hackers compromised the GPS and communication systems of the Dassault Falcon 900 aircraft belonging to the UK Secretary of State for Defence Grant Shapps using EW attack methods. The aircraft departed from Poland, where Defence Secretary Shapps visited British troops participating in the Steadfast Defender exercises, and was en route to the United Kingdom. During his visit, Shapps reaffirmed his country's full support for Ukraine. Royal Air Force pilots confirmed that the aircraft's GPS and other communication signals were jammed for nearly 30 minutes while the secretary was flying near the russian city of Kaliningrad, which is adjacent to Poland.

RUSSIAN ENTITIES WILL NO LONGER BE ABLE TO ACCESS MICROSOFT'S CLOUD SERVICES AND BUSINESS ANALYTICS TOOLS.

Microsoft plans to suspend access to its cloud services for russian users this month due to European sanctions imposed on russia following its invasion of Ukraine. Softline, one of the largest distributors of Microsoft products in russia, announced that local users will lose access to Microsoft's cloud services on March 20. Several other local technology companies also received warnings from Microsoft about the suspension. However, according to unofficial information, the suspension may be postponed until the end of the month.

ACCORDING TO CISA , CHINA MAY USE THE RUSSIAN TACTIC OF ATTACKING CRITICAL INFRASTRUCTURE FACILITIES

On March 21, CISA director Jen Easterly discussed the critical importance of U.S. support for Ukraine amid russian kinetic and cyber attacks. The article highlights the conflict's broader implications for global cybersecurity and how adversaries like China may employ similar tactics against the critical infrastructure of the United States and its allies. She emphasized the need for ongoing support to deter adversaries andprotect democratic values from authoritarian threats.

THE USA IMPOSED SANCTIONS ON RUSSIANS BEHIND THE DOPPELGÄNGER CYBER INFLUENCE CAMPAIGN

On March 21, the U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) announced sanctions against two russian citizens and their respective companies for their involvement in cyber influence operations. Ilya Gambashidze, founder of moscow-based Social Design Agency, and Nikolai Tupikin, CEO and current owner of the russian company Group Structura LLC, were accused of providing services to the russian government related to «a foreign malicious influence campaign.» The disinformation campaign is being tracked by the broader cybersecurity community under the name Doppelgänger, known to target audiences in Europe and the USA through inauthentic news websites and social media accounts.

RUSSIAN HACKERS LIKELY TARGETED UKRAINIAN TELECOMMUNICATIONS USING UPDATED ACIDPOUR MALWARE

According to new findings from SentinelOne published on March 22, the malicious software AcidPour, which destroys data, may have been used in attacks against four telecommunications operators in Ukraine. The company also confirmed a connection between the malware and AcidRain, linking it to threat clusters associated with russian military intelligence. AcidPour is a variant of AcidRain, a wiper that was used to disrupt Viasat KA-SAT modems at the beginning of the full-scale russian-Ukrainian war in early 2022 and disrupt military communications in Ukraine.

RUSSIAN HACKERS USE WINELOADER MALWARE TO ATTACK POLITICAL PARTIES IN GERMANY, ACCORDING TO MANDIANT

According to a report by Mandiant, the WINELOADER backdoor, which was used in recent cyberattacks on diplomatic institutions that used phishing lures related to wine tasting, is attributed to a hacker group linked to russia's foreign intelligence service (GRU) responsible for the SolarWinds and Microsoft breaches. Mandiant stated thatMidnight Blizzard (also known as APT29, BlueBravo, or Cozy Bear) used malicious software around February 26, 2024, to conduct a phishing attack on German political parties, using emails with the logo of the Christian Democratic Union. This APT29 cluster attack on a political party marks a departure from its typical targeting of diplomatic missions. According to the company, such an attack poses a broader threat to political parties in the EU.

THE U.S. IMPOSED SANCTIONS ON THREE CRYPTOCURRENCY EXCHANGES THAT AIDED RUSSIA IN CIRCUMVENTING SANCTIONS

On March 26, OFAC imposed sanctions on three cryptocurrency exchanges for providing services used to evade economic restrictions imposed on russia following its invasion of Ukraine in early 2022, including the exchanges Bitpapa IC FZC LLC, Crypto Explorer DMCC (AWEX), and Center for Electronic Payment Processing LLC (TOEP). In total, the sanctions affected 13 organizations and two individuals working in the russian financial services and technology sectors.

THE GOVERNMENT OF FRANCE EXPERIENCED CYBERATTACKS OF "UNPRECEDENTED" INTENSITY

On March 11, the Prime Minister of France stated that the country's government institutions had been subjected to cyberattacks of «unprecedented intensity.» Descriptions of the incidents suggest a distributed denial-of-service (DDoS) attack. The French government established a crisis unit to address the situation. The perpetrators behind the attacks are currently unknown. On its Telegram channel, the pro-russian hacker group Anonymous Sudan claimed responsibility for a «massive cyberattack» on the infrastructure of France's Interministerial Directorate of Digital Affairs.