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

FEBRUARY 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

CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT-EE	Computer Emergency Response Team for Estonia
CERT-EU	Computer Emergency Response Team for the EU institutions, bodies and agencies
CERT-UA	Government Computer Emergency Response Team Ukraine
CISA	Cybersecurity and Infrastructure Security Agency
CRDF Global	Civil Research and Development Fund (U.S.)
CSIS	Center for Strategic and International Studies (U.S.)
CTF	Capture the Flag
EEAS	European External Action Service
ENISA	European Union Agency for Cybersecurity
EU	European Union
FBI	Federal Bureau of Investigation
FSB	Federal Security Service (Russian Federation)
HUR	Main Directorate of Intelligence of the Ministry of Defense of Ukraine
ICS	Information and Communication Systems
ICT	Information and Communications Technology
IT	Information Technology
LLM	Large Language Module
NATO	North Atlantic Treaty Organization
NBU	National Bank of Ukraine
NCSCC	National Cybersecurity Coordination Center
NSA	National Security Agency (U.S.)
NSDC	National Security and Defense Council of Ukraine
OT	Operational Technology
RAT	Remote Access Trojan
RIA	Department of State Information Systems (Estonia)
SBU	Security Service of Ukraine
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
TAG	Threat Activity Group

KEY TENDENCIES

An important event in February 2024 was the successful operation conducted by British law enforcement against the powerful ransomware group Lockbit. Lockbit-affiliated groups account for a significant portion of ransomware attacks worldwide, and disrupting their activities will help reduce the negative impact of such attacks. The efforts of British law enforcement were complemented by actions taken by Ukrainian police, who arrested two members of the group. Overall, this marks the second significant success of law enforcement agencies in combating major ransomware groups. Recently, U.S. law enforcement disrupted the Hive group's operations and are currently seeking its leaders (the U.S. Department of State announced a reward for information about them).

Vulnerabilities in Ivanti products have been causing problems for users and cybersecurity authorities worldwide for the past two months. New data about vulnerabilities in Ivanti products continue to emerge, and the European Union Agency for Cybersecurity (ENISA) and Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) even issued joint recommendations for European consumers. This situation is unfolding against the backdrop of a significant shift in European Union (EU) cybersecurity policy, with the first European certification scheme for Information and Communications Technology (ICT) products based on the Common Criteria now in operation, which incorporates elements of various national certification schemes and aims to make the use of IT products by European consumers safer. Currently, the scheme is still being introduced, but the EU has high hopes for its success and further development.

The Government Computer Emergency Response Team Ukraine (CERT-UA) processed 15.9% more cyber incidents in 2023 compared to 2022, reaching a total of 2,543 cyber incidents. The most common types of incidents included malware dissemination, phishing, malicious connections, account compromise, and system compromise. Malicious actors traditionally conduct reconnaissance operations, engage in long-term espionage, and attempt data and information system destruction.

On February 7-8, the first Kyiv International Cyber Resilience Forum 2024, titled “Resilience During Cyber Warfare”, took place in the capital of Ukraine. The event was initiated by the National Cybersecurity Coordination Center under the National Security and Defense Council of Ukraine (NSDC) and its partners. Over 1,000 people attended the forum, including top officials from Ukraine, the U.S., EU, and NATO. The event featured 10 panel discussions and over 40 expert presentations covering topics such as the role of cybersecurity in modern warfare, Ukraine’s experience in cyber warfare, the intersection of cyber warfare and international law, cyber diplomacy, enhancing national cybersecurity resilience through education, messenger app security, the role of cyber threat intelligence, cybersecurity of regions, and more. Additionally, the forum hosted cybersecurity competitions involving 21 teams of experts from both the public and private sectors. During sideline meetings, Ukrainian and U.S. officials acknowledged the successful cooperation between the United States and Ukraine in exchanging cybersecurity expertise and discussed Ukraine’s short-term and long-term cybersecurity needs.

Relations are becoming increasingly tense between the U.S. and China in cyber competition. Hearings before the Special Committee of the House of Representatives on the Communist Party of China highlighted growing concerns of U.S. security agencies regarding Chinese cyber activity. In some of the testimonies, such as those by the Federal Bureau of Investigation (FBI) director or former National Security Agency (NSA) Director Paul Nakasone, speakers made harsh assessments about the actions of Chinese hacker groups (such as the Volt Typhoon group), which significantly deviate from cyber espionage activities to direct attacks on critical infrastructure objects or positioning for a large-scale conflict (using the Living-Off-the-Land attack method). According to the FBI, the Volt Typhoon group implanted malicious software on hundreds of network routers and other Internet-connected devices, posing a threat to water supply, electricity, and railway transportation, which could cause real harm. Another threat from Chinese hackers is the potential negative impact on the U.S. military base in Guam. U.S. security agencies are concerned that Chinese cyberattacks could have a significant impact on its functioning. As an interim measure, on February 7, the Cybersecurity and Infrastructure Security Agency (CISA), NSA, and FBI, together with key U.S. and international government agencies (Australia, Canada, and New Zealand), published a joint cybersecurity advisory regarding the activities of Volt Typhoon. Another consequence will be the adoption of stricter cybersecurity requirements for port infrastructure in the U.S., which significantly rely on Chinese equipment. The U.S. president is expected to issue a relevant Executive Order in the near future.

Among the achievements of Ukrainian cyber experts in February were the arrests of two international criminals and winning places in two international cybersecurity competitions. A joint operation involving the Security Service of Ukraine (SBU) and U.S., United Kingdom (UK), EU, and other partner countries' law enforcement agencies, exposed participants of the powerful international LockBit ransomware group. Additionally, the Main Directorate of Intelligence of the Ministry of Defence of Ukraine (HUR) reported an attack on the Russian drone management system, which resulted in Russians losing access to servers. The SBU also emphasized the importance of information collected through cyber reconnaissance for conducting complex kinetic operations.

Government concerns about offensive actions in cyberspace have also affected the commercial sector. In February, the UK and France held the inaugural conference dedicated to combating the threat of commercial cyber proliferation, i.e., the unauthorized dissemination of tools created by commercial companies for malicious purposes that could be used in offensive cyber operations. As a result, participants signed the Pall Mall Process Declaration, which outlines initiative members' plans to explore alternative policies and innovative methods to counter this threat. Currently, Israel is not actively participating in these initiatives, as Israeli companies hold a significant share of the export market for spyware.

Cybersecurity threats to Operational Technology (OT) are not only not diminishing but are becoming increasingly systemic. Equipment manufacturers and OT solution providers are increasingly discovering new vulnerabilities in their products. In February alone, Siemens identified 275 vulnerabilities in its products actively used for industrial process automation. A Dragos Inc report confirms that malicious actors are increasingly entering this relatively new field: in 2023, three more cyber groups targeting OT infrastructure emerged, bringing the number of such groups that Dragos currently tracks to 21. The problems not only lie in identifying vulnerabilities but also in attempting to address them. Research has shown that organizations with OT systems often know about flaws being exploited in their environment, but cannot solve the problem because, for example, the warranty period of some outdated systems has expired or technical processes or business interests may hinder updating the assets to the latest operating systems.

The global cyber warfare continues, with a significant portion involving Russian-Ukrainian confrontation. Russian hacker groups continue to conduct cyber espionage operations against Ukraine, as evidenced by Securonix Threat Research tracking one such attack against Ukrainian military targets, or by targeting government websites, such as the website of the Ministry of Education of Ukraine. Ukrainian cyber experts actively counter these attempts, including ongoing investigations into the consequences of the large-scale cyber attack in 2023 against Kyivstar telecommunications operator. According to the SBU, Russian hackers were preparing a second wave of attacks to inflict even greater damage to the operator.

1. CYBERSECURTY SITUATION IN UKRAINE

THE INTERNATIONAL CYBER RESILIENCE FORUM 2024 TOOK PLACE IN KYIV

On February 7-8, the first Kyiv International Cyber Resilience Forum 2024, titled "Resilience during Cyber Warfare", took place in the capital of Ukraine. The NSDC National Cybersecurity Coordination Center (NCSCC) and its partners initiated the event. NSDC Secretary Oleksiy Danilov opened the Forum. Also addressing the forum were Mykhailo Fedorov, Vice Prime Minister for Digital Transformation, and representatives of the international cybersecurity community, including Nathaniel Fick, U.S. Ambassador at Large for Cyberspace and Digital Policy of the U.S. Department of State; Johannnes Belfort, Director for Security and Defense Policy at the European External Action Service (EEAS); Juhan Lepasar, ENISA Director; Mart Noorma, Head of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE); and Jen Easterly, CISA Director.

Over 1,000 people attended the forum. Over the course of the 2-day event, there were 10 panel discussions and over 40 expert presentations covering a wide range of topics, including the role of cybersecurity in modern warfare, Ukraine's experience in cyber warfare, cyber warfare and international law, cyber diplomacy, enhancing the resilience of the national cybersecurity system through education, messenger app security, the role of cyber threat intelligence, cybersecurity in regions, and more.

As part of the forum, a 2-day Capture the Flag (CTF) cybersecurity competition was held, with 21 teams participating, comprised of 121 professionals from both the public and private sectors.

UKRAINE AND THE U.S. ARE DEEPENING THEIR STRATEGIC PARTNERSHIP IN CYBERSECURITY

During the Kyiv International Cyber Resilience Forum, Vice Prime Minister for Innovations, Development of Education, Science, and Technology - Minister of Digital Transformation Mykhailo Fedorov and Head of the State Special Communications Service and Information Protection (SSSCIP) Yuriy Mironenko met with the U.S. Ambassador-at-Large for Cyberspace and Digital Policy of the U.S. Department of State Nathaniel Fick and CISA Director Jen Easterly. U.S. Ambassador to Ukraine Bridget Brink also participated in the meeting. The parties agreed that the previously planned cooperation, including exchanging experience between the two countries on cyber-related issues, has been successful and they shared their vision of current areas of work that need to be intensified. They also discussed Ukraine's short- and long-term cybersecurity needs.

UKRAINIAN AND ESTONIAN CYBERSECURITY EXPERTS AGREED TO ENHANCE COOPERATION

To determine further areas for collaboration in cybersecurity, a delegation of cyber experts from Estonia visited the SSSCIP. During the meeting, CERT-UA and its Estonian counterpart CERT-EE actively discussed prospects for enhancing cooperation. The key focus was on ensuring effective and timely bilateral exchange of information regarding cyber threats, the results of cyber attack investigations, vulnerabilities in information systems' defenses, and sharing experience in responding to Russian hackers' actions. The meeting participants also discussed further implementing initiatives as part of the Memorandum of Cooperation with the Department of State Information Systems (RIA), which is responsible for cybersecurity in Estonia.

SSSCIP STRENGTHENS COOPERATION IN CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

SSSCIP Deputy Chair Oleksandr Potii met with U.S. Civilian Research and Development Foundation (CRDF Global) representatives, including Director General Mike Dignam, Senior Advisor Thomas Kalahen, and Regional Director Mykhailo Verich, during their visit to Ukraine. They discussed key topics such as protecting Ukrainian information resources in cyberspace and critical infrastructure objects, which are subject to various threats, primarily related to Russia's aggression against Ukraine. The partners expressed their readiness both to continue comprehensive support for Ukraine and to enhance cooperation.

NCSCC STARTED TRAINING ON VULNERABILITY MANAGEMENT FOR SPECIALISTS IN REGIONAL MILITARY ADMINISTRATIONS

As part of strengthening measures to ensure cybersecurity at the regional level, the NCSCC under NSDC of Ukraine and the National Bank of Ukraine (NBU) Cybersecurity Center initiated Vulnerability Management (VDP) training for regional military administrations, with support from CRDF Global in Ukraine. More than 70 technical specialists from all regions of Ukraine are participating in the 7-week training program. Cybersecurity specialists will acquire theoretical and practical knowledge on network technologies, assessing compliance with best practices, testing information systems and web applications for vulnerabilities, and handling interaction during incident and vulnerability reporting.

SSSCIP IS ENHANCING KNOWLEDGE AND SKILLS FOR RESPONDING TO CYBER INCIDENTS FOR THE LEADERSHIP OF CRITICAL INFRASTRUCTURE FACILITIES AND GOVERNMENT AGENCIES

The SSSCIP and its partners conducted the second 1-day in-person seminar "Response to Cyber Incidents" for deputy heads of state agencies and critical infrastructure facilities on issues related to digital development, digital transformation, and digitization. Tasks addressed included simulating detecting unauthorized access to information and communication systems (ICS), developing procedures for isolating ICS, implementing measures to identify an attack surface, and reducing its impact.

INTELLIGENCE GATHERED THROUGH CYBER METHODS HELPS THE SBU CONDUCT UNIQUE SPECIAL OPERATIONS

At the Kyiv International Cybersecurity Forum “Resilience During Cyber Warfare”, Chief of the SBU Cybersecurity Department Illia Vitiuk said, “We act proactively: penetrating deep into enemy systems. Our main goal is to obtain important intelligence information, which is then used in top-level SBU special operations. This includes eliminating war criminals, targeting military objects and infrastructure that serve the Russian military-industrial complex, and more. Many SBU special operations today involve a cyber component.” Furthermore, according to him, the intelligence gathered is transferred to the Defense Forces or international partners if it concerns, for example, Russian Federation attempts to evade sanctions. In this way, the SBU prevents Russia from establishing new supply chains to continue the war against Ukraine.

THE UKRAINIAN TEAMS EMERGED VICTORIOUS AT THE NATO TIDE HACKATHON 2024

The NATO Think-Tank for Information Decision and Execution (TIDE) Hackathon is an annual competition organized by NATO’s Transformation Command to seek innovative solutions and address compatibility issues within the Alliance. It is part of a series of events to improve NATO and allied interoperability through innovative solutions and approaches. This year, NATO and the Dutch IT Command jointly organized the hackathon in Amsterdam, the Netherlands. It involved 34 teams from 21 countries, including representatives from governmental and defense agenices and five teams from the private sector. The competition focused on three key areas: Wargaming Large Language Module (LLM), Pharmaceutical Thesaurus, and Noisy Speech to Text. Ukrainian teams Valkyrie-1 and Valkyrie-2 emerged victorious in the first two categories.

SSSCIP STATE CYBER PROTECTION CENTER TEAM TOOK SECOND PLACE AT CYBER TRAINING IN WARSAW

The Ukrainian team Netflix&Chill took second place in the overall ranking of the competition, held February 5-9 in Warsaw, Poland, as part of a cyber training on critical infrastructure protection. In total, 16 teams from Germany, Albania, Poland, Estonia, Lithuania, Slovakia, Slovenia, Moldova, and Romania took part in the competition. The cyber training also provided an in-depth study of targeted attacks on critical infrastructure in the energy sector, identifying compromise indicators, and developing strategies to mitigate the impact on the energy sector.

RUSSIAN HACKERS ATTACKED WELL-KNOWN UKRAINIAN MEDIA OUTLETS

Enemy hackers carried out another attack on a number of Ukrainian media outlets and posted fake information on their resources. Ukrainska Pravda, Liga.net, Apostrof, and Telegraph contacted CERT-UA about the incident. Investigations into the incident are currently underway.

CERT-UA PROCESSED 2,543 CYBER INCIDENTS IN 2023

In 2023, CERT-UA processed 2,543 cyber incidents, 15.9% more than in 2022. The attackers' main targets included government and governmental organizations, local authorities, the security and defense sector, commercial organizations, the energy sector, telecommunications, and many other institutions. The most common types of incidents were the dissemination of malware, phishing, malicious connections, account compromise, and system compromise. The attackers' goals included reconnaissance operations, long-term espionage, and data and information system destruction. The number of

THE SSSCIP OPERATIONAL CENTER FOR RESPONDING TO CYBER INCIDENTS PROCESSED 46,000 CRITICAL CYBERSECURITY EVENTS, ACCORDING TO ITS REPORT

The SSSCIP Operational Center for Responding to Cyber Incidents released a report on the results of the Vulnerability Detection and Response System (VDRS) for the fourth quarter of 2023. During this period, the VDRS processed 1.4 billion events received through monitoring, analysis, and telemetry transmission tools for cyber incidents and attacks; detected 2 million suspicious cybersecurity events (upon initial analysis); and processed 46,000 critical cybersecurity events (potential cyber incidents identified through filtering of suspicious cybersecurity events and secondary analysis). Additionally, security analysts identified and processed 357 cyber incidents directly.
Full report: scpc.gov.ua/uk/articles/341

THE SBU AND U.S., UK, AND EU LAW ENFORCEMENT AGENCIES UNCOVERED AN INTERNATIONAL CYBERCRIME GROUP OF RANSOMWARE HACKERS

SBU cybersecurity experts conducted a large-scale special operation in various parts of the world, in collaboration with law enforcement agencies from the U.S., UK, EU, and other partner countries. As a result of joint efforts, participants of a powerful international hacker group known as LockBit were exposed. According to the case materials, the criminals stole confidential information and personal data from well-known companies and then demanded ransoms for them. Among the organizers and participants of the group were citizens of Ukraine and Russia. Over nearly five years, the hackers carried out over 3,000 cyberattacks against financial institutions and corporations of Western countries providing defense assistance to Ukraine. To steal corporate information, the hackers used specially designed ransomware programs.

POLICE EXPOSED AN ODESA RESIDENT WHO OBTAINED INFORMATION ABOUT UKRAINIAN BANK CARDS BY DECEPTION

Police established that a resident of Odesa created and posted on popular social media platforms links to a website whose design completely copied the appearance of the State Aid website for the eSupport program. By directing citizens to the phishing forms for financial assistance from the government, the fraudster obtained the details of their bank cards: card number, CVV code, expiration date, and other details. He faces imprisonment for his actions.

THE SBU DETAINED INDIVIDUALS WHO ASSISTED THE FSB TO GAIN CONTROL OVER ALMOST ALL INTERNET TRAFFIC IN TEMPORARILY OCCUPIED DONETSK

SBU cyber specialists detained in Kyiv the heads of an internet provider from Donetsk controled by the Russian Federal Security Service (FSB). The criminals collaborated with the aggressor in the temporarily occupied part of Ukraine but attempted to "legalize" themselves in the capital. They installed specialized Russian special services equipment on the provider's servers, allowing the FSB to monitor all internet activity of the region's peaceful residents. The information the FSB obtained is used to recruit residents of the region and involve them in intelligence and subversive activities against Ukraine. The perpetrators are in custody and face up to 15 years in prison.

CYBERPOLICE OFFICERS IN VINNYTSIA EXPOSED A HACKER WHO "EARNED" OVER 3.5 MILLION UAH BY STEALING DATA FROM U.S. AND CANADIAN RESIDENTS

The hacker created and administered several websites where he offered users to download various software for free. The suspect deployed a whole advertising campaign on the internet to "promote" the controlled websites, but in reality, he stole and sold personal data of residents of Canada and the USA using malicious software. The perpetrator has been charged and faces up to eight years in prison with property confiscation.

RUSSIAN OCCUPIERS ARE INTENSIFYING MEASURES OF INFORMATIONAL AND PSYCHOLOGICAL INFLUENCE ON UKRAINIANS IN THE OCCUPIED TERRITORIES

The HUR announced that residents of the occupied communities in Kherson Oblast are being massively connected to Russian satellite television called "Russian World" in order to cut off channels of access to information about the real situation on the front line, in Ukraine, and the world. Currently, the Russians have installed over 18,000 corresponding devices.

Additionally, in the temporarily occupied Ukrainian communities in Donetsk Oblast, the occupiers are transferring the occupation administration's work to their own software and communication services, and expanding the network coverage of Russian mobile communication. In 2023-2024, over 700 base stations were installed, and in Kherson Oblast, over 200, constituting over 85% of the total mobile coverage in the occupied region.

HUR REPORTED A SUCCESSFUL CYBER ATTACK ON RUSSIAN FEDERATION DRONE CONTROL PROGRAMS

HUR cyber experts conducted another successful operation against the Russian occupiers, leading to a massive failure of the drone control program. This software was installed by Russians to reflash DJI drones for military operations needs, ensuring the functioning of the "friend or foe" system. According to preliminary data, as a result of the HUR cyber attack, the servers stopped working, so all software was recognized as "foreign," denying access to the invaders.

CERT-UA REPORTED A CYBER ATTACK ON THE UKRAINIAN DEFENCE FORCES.

CERT-UA detected and took measures to neutralize a new cyber attack targeting representatives of the Armed Forces of Ukraine. The perpetrators attempted to infect military computers with malicious software through the Signal messenger. According to CERT-UA, this activity has been ongoing at least since the fall of 2023, it is targeted, and is tracked under the identifier UAC-0149.

OVER 2,000 COMPUTERS AFFECTED; CERT-UA TOOK MEASURES REGARDING AN ATTACK ON A UKRAINIAN STATE ENTERPRISE

CERT-UA provided practical assistance to a state enterprise whose computers were affected by the malicious program DIRTYMOE (PURPLEFOX), which provides remote access to infected devices. The CERT-UA team conducted an investigation of the collected samples of malicious programs, identified the functioning features of the command and control servers infrastructure, and discovered more than 2,000 affected computers in the Ukrainian segment of the Internet. The activity is tracked under the identifier UAC-0027. More details about the attack can be found on the CERT-UA website: cert.gov.ua/article/6277422

2. THE FIRST WORLD CYBER WAR

RUSSIAN SPIES POSE AS WESTERN RESEARCHERS

On February 1, The Record reported the exposure of a hacking campaign in which hackers from Russian intelligence services pose as researchers and scholars to gain access to their colleagues' email accounts. The attackers' technique involves creating seemingly authentic articles to lure victims into providing feedback, then stealing data from their accounts. Secureworks and Mandiant independently analyzed the cyberattack and confirmed its origins. It is attributed to a state-sponsored threat group known as Iron Frontier, Calisto, Coldriver, or Star Blizzard/Seaborgium, believed to be working for Russian intelligence services.

THE U.S. SHOULD PAY SPECIAL ATTENTION TO CYBERSECURITY IN MOLDOVA AGAINST THE BACKDROP OF THE SITUATION IN UKRAINE – CSIS

On February 2, Leah Kiff from the Center for Strategic and International Studies (CSIS) published an extensive piece on the cyber threats facing Moldova and possible U.S. policies toward the country. The article emphasizes the importance of the U.S. providing cybersecurity assistance to prevent large-scale cyberattacks and disruptions to the electoral process. It underscores that Moldova should draw on Ukraine's experience to better prepare for destructive Russian cyber activity, including developing public-private partnerships, combating recruited insiders in the government, and countering influence operations.

THE CAMPAIGN "STEADY#URSA ATTACK" TARGETS UKRAINIAN MILITARY PERSONNEL

The Securonix Threat Research team is monitoring an ongoing campaign that is likely associated with Shuckworm and targets Ukrainian military personnel (tracked by Securonix Threat Research as STEADY#URSA). The malicious payload is delivered through compressed files, possibly via phishing emails. Many of the samples the team identified contained multi-word references to Ukrainian cities and military terminology. The attack is likely linked to Shuckworm because it contains several exclusively used tactics, techniques, and procedures (TTPs) unique to the group previously reported in past campaigns against Ukrainian military personnel.

THE MINISTRY OF EDUCATION WEBSITE WAS NOT FUNCTIONING DUE TO A RUSSIAN CYBERATTACK

On February 7, the Ministry of Education of Ukraine reported that its website was not functioning due to an attack by Russian hackers. Details of the incident were not disclosed.

THE U.S. LIKELY CONDUCTED A CYBERATTACK ON AN IRANIAN SPY SHIP

On February 15, NBC News reported that the United States conducted a cyberattack on an Iranian military ship in the Red Sea. The ship was gathering intelligence on cargo vessels. The operation aimed to disrupt the ship's ability to share intelligence with Houthi fighters in Yemen. The attack was carried out as part of efforts to counter Houthi activity in Yemen.

THE ENEMY WAS PLANNING A SECOND WAVE OF CYBERATTACKS ON KYIVSTAR, WHICH COULD HAVE "ZEROED OUT" THE BASE STATIONS – SBU

On February 7, Head of the SBU Cybersecurity Department Ilya Vitiuk announced that after the hacker attack on the mobile operator Kyivstar in December 2023, the enemy was planning a second wave that could have "zeroed out" all base stations. Vitiuk emphasized that the investigation is still ongoing and will continue for a very long time because hundreds of servers were destroyed during the attack, and thousands of computers were completely wiped out.

RUSSIAN HACKERS ATTACK UKRAINE THROUGH DISINFORMATION CAMPAIGNS AND COLLECTING PERSONAL DATA

Cybersecurity researchers from the Slovak company ESET discovered a new influence operation targeting Ukraine, which uses spam to spread war-related disinformation. ESET links this activity to threat actors associated with Russia. The operation, codenamed Texonto, was not directly attributed to a specific threat actor, although some elements, such as phishing attacks, coincide with COLDRIVER, which has a history of collecting credentials through fake login pages. More details about the operation can be found in the company's report: www.welivesecurity.com/en/eset-research/operation-texonto-information-operation-targeting-ukrainian-speakers-context-war

TAG-70, ASSOCIATED WITH RUSSIA, IS TARGETING EUROPEAN GOVERNMENTAL AND MILITARY MAIL SERVERS AS PART OF A NEW ESPIONAGE CAMPAIGN

On February 19, Recorded Future reported that it had uncovered perpetrators acting on behalf of Belarus and Russia, associated with a new cyber espionage campaign. This campaign likely exploited cross-site scripting (XSS) vulnerabilities on Roundcube webmail servers to target over 80 organizations. The company is tracking this hacker group under the name Threat Activity Group 70 (TAG-70).

The campaign that Recorded Future identified lasted from early October 2023 until mid-February 2024 with the aim of gathering intelligence on Europe's political and military activities. These attacks coincidde with additional activity by TAG-70 against governmental mail servers in Uzbekistan, which were discovered in March 2023.

A BACKDOOR FOR DEPLOYING THE KONNI RAT MALWARE INTRODUCED INTO THE RUSSIAN GOVERNMENT SOFTWARE

The installer for a tool that is believed to be used by the Consular Department of the Russian Ministry of Foreign Affairs introduced a backdoor for delivering a Remote Access Trojan (RAT) named Konni RAT (also known as UpDog). According to the findings of the German cybersecurity company DCSO, this activity is associated with North Korean activities targeting Russia.

UKRAINIAN HACKERS ATTACKED RUSSIAN SERVERS AND GAINED ACCESS TO OVER 5 TB OF INFORMATION

The StratCom of the Armed Forces of Ukraine reported that on February 25, a large-scale hacker attack on Russian websites was detected. As a result of the work of the hacker group UA25, 5 terabytes of personal and corporate confidential information were extracted.