NCSCC
NATIONAL CYBERSECURITY COORDINATION CENTER

USAID
FROM THE AMERICAN PEOPLE

UKRAINIAN FOUNDATION FOR SECURITY STUDIES

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

April 2024

The Cyber Digest was made possible through support provided by the U.S. Agency for International Development, under the terms of the Award to Non-Governmental Organization "Ukrainian Foundation for Security Studies", within the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The author's views expressed in the Cyber Digest do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

CONTENT

ACRONYMS 5

KEY TENDESES 6

1. CYBERSECURITY SITUATION IN UKRAINE 9

Ukraine is deepening cooperation with cybersecurity agencies in the EU, NATO, and Romania 9

The NCSCC Secretary urged EU and NATO countries to collaborate in countering russia's cyber aggression 9

Ukraine participated in NATO CCDCOE cyber defense training Locked Shields 9

For the first time, Ukraine participated in an explanatory session of the European Commission dedicated to digitalization 10

Unified cybersecurity standards: The Ministry of Defense strengthens the protection of information systems in accordance with NATO standards 10

NCSCC representatives met with a Republic of Kenya delegation 10

The NCSCC conducted «Vulnerability Management» training for cybersecurity specialists from oblast military administrations 10

Army+ has a specific architecture that allows data to be protected as securely as possible – Kateryna Chernohorenko 11

Nataliya Tkachuk highlighted the importance and urgency of refining sectoral and interagency collaboration in responding to cyberattacks 11

The SSSCIP, critical infrastructure facilities, and state agencies developed cybersecurity protection plans for institutions 11

Medical institution representatives learned how to combat ransomware cyberattacks 11

Ukraine launched an interdepartmental educational platform for the security and defense sector 12

In Khmelnytskyi, cyber police conducted training on digital security for government authorities and local self-governments 12

SSSCIP experts conducted a training for facilitators of command and staff exercises 12

The Ministry of Foreign Affairs announced a scientific-practical conference on cyber diplomacy 12

The SBU identified hackers from the russian group responsible for attacking Kyivstar 13

The Cyber Police and the Center for Countering Disinformation signed a memorandum of cooperation 13

The Cyber Police launched the new project «Cyber Gate» to improve the level of cyber hygiene among Ukrainians 13

CERT-UA published instructions for setting up 2FA in popular messengers 13

SSSCIP Head met with American Chamber of Commerce leadership 14

CERT-UA warned of a cyber threat to the Armed Forces of Ukraine (AFU) 14

russian hackers use social engineering for cyberattacks on the AFU 14

Scammers steal WhatsApp accounts by using fake petitions asking to confer the title of «Hero of Ukraine» on fallen defenders 14

The SBU detained pro-russian hackers in Kyiv who created fake accounts of Ukrainian special service officials 15

2. THE FIRST WORLD CYBER WAR 16
Inside russia's shadow trade in weapon parts fueled by cryptocurrency 16
Hackers stole the russian prisoner database to retaliate for Navalny's death 16
Researchers discovered a new ransomware gang that targets russian businesses, Mulyaka 16
Ukraine awarded foreign IT professionals for their assistance in cyber defense against russia 17
Claroty analyzed the pro-Ukrainian group Blackjack's cyberattack on the physical infrastructure of russia's Moscollector 17
According to Microsoft, russia has significantly intensified its influence operations against the U.S. over the past two months 17
russian hackers managed to influence the water supply system of the small Texas town of Mulshou 17
The laptop of the Chair of the Belgian parliamentary committee on foreign affairs was hacked by Chinese hackers 18
How Ukrainian hacker-volunteers created a «coordinated machine» around low-level attacks 18
russian APT uses new backdoor Kapeka during attacks in Eastern Europe 18

ACRONYMS

2FA	Two-Factor Authentication
AFU	Armed Forces of Ukraine
AI	Artificial Intelligence
AmCham	American Chamber of Commerce
APT	Advanced Persistent Threat
CCDCOE	The NATO Cooperative Cyber Defence Centre of Excellence
CEO	Chief Executive Officer
CERT-UA	Government Computer Emergency Response Team Ukraine
CISA	Cybersecurity and Infrastructure Security Agency
C-PROC	Council of Europe Convention on Cybercrime
CRDF Global	Civil Research and Development Fund (U.S.)
DNSC	National Cyber Security Directorate (Romania)
EARC	Euro-Atlantic Resilience Center
ECCC	European Cybersecurity Competence Center
EU	European Union
EU4PAR	Support to Comprehensive Reform of Public Administration in Ukraine
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
HUR	Main Intelligence Directorate of Ukraine
ICC	International Criminal Court
ICS	Industrial Control System
IoT	Internet of Things
IPAC	Inter-Parliamentary Alliance on China
IT	Information Technology
NATO	North Atlantic Treaty Organization
NCSCC	National Cybersecurity Coordination Center
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
	PaaS Platform as a Service
SBU	Security Service of Ukraine
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
TTX	Table Top Exercise
U.S.	United States
UN	United Nations
UNDP	United Nations Development Programme
VDP	Vulnerability Management
VPN	Virtual Private Network

KEY TENDESES

The USA continues to rotate cybersecurity specialists and expand its cybersecurity community. Against the backdrop of the White House's request of $13 billion for the cybersecurity component of the 2025 budget, a new cybersecurity director was appointed at the National Security Agency (NSA), and a cyber policy department was created at the Pentagon. The NSA and Cybersecurity and Infrastructure Security Agency (CISA) continue to issue security recommendations, primarily regarding the implementation of Zero Trust. However, the number of incidents is increasing. In April, a wave of cyberattacks targeted municipal resources and city IT systems, and attacks on the U.S. water sector continued. Recent attacks have been attributed to russian cyber groups.

The U.S. is still grappling with the aftermath of the cyberattack on Change Healthcare. New details continue to emerge about the cyber incident that inflicted $872 million in damage on UnitedHealth, the owner of Change Healthcare. It has also been revealed that hackers managed to steal a significant amount of personal data belonging to the company's clients, and its CEO will testify before the U.S. House of Representatives. This is not the only incident involving American healthcare companies in April. Medical conglomerate Kaiser reported a data breach affecting millions of its clients (it has a total of 13.4 million clients). Clearly, these events will lead to changes in approaches to cybersecurity in the healthcare sector and developing relevant standards. The latter may become problematic, among other things due to underfunding of the key American agency responsible for developing such standards, the National Institute of Standards and Technology (NIST).

Ukraine is enhancing qualifications and increasing awareness in cybersecurity at all levels. Among other initiatives, the National Cybersecurity Coordination Center (NCSCC) conducted training on vulnerability management for cybersecurity specialists from oblast military administrations, helping them to improve skills in conducting comprehensive analyses of the cybersecurity status of their institutions and understand the principles and approaches of cybercriminals. The National Academy of the Security Service of Ukraine (SBU) presented an interdepartmental educational platform for representatives of the security and defense sector, where, among other things, courses on protecting critical infrastructure objects and countering crimes using virtual assets will be available. The Government Computer Emergency Response Team Ukraine (CERT-UA) published instructions on using two-factor authentication (2FA) for certain messengers and information systems, while the Cyberpolice started a new Cyber Gate project to improve cyber hygiene among Ukrainians.

In line with the gradual adoption of European and NATO standards in the digital and cyber sphere, Ukraine held its first meeting with European Union (EU) representatives as a candidate country dedicated to digitalization. It included an explanatory session by the European Commission for Ukraine regarding Negotiating Chapter 10 «Digital Transformation and Media.» The Ministry of Defense approved the basic principles of information and cybersecurity in the ministry's information and communication systems by order, which will take into account the best practices of NATO, international standards, and practices in information security and cybersecurity. During the third international meeting of the National Cyber Security Cluster on the topic «Building Partnerships for Cyber Resilience in Southeast Europe,» participants discussed deepening cooperation with the EU and NATO and practical steps Ukraine has taken in cybersecurity. The Secretary of the National Cybersecurity Coordination Center under the NSDC of Ukraine Nataliya Tkachuk, called on EU and NATO countries to jointly counter russia's cyber aggression.

There has been a sharp increase in the activity of Chinese hackers, leading to deeper analysis of their activities by Western governments. New reports are emerging about a cyber espionage campaign against members of the Inter-Parliamentary Alliance on China, revealing that another victim of Chinese hackers is the Chair of the Foreign Affairs parliamentary committee of Belgium. In the context of the American elections, Chinese hackers are using artificial intelligence (AI) to fuel social tension in the U.S. Meanwhile, China is also transforming its cyber forces, having created the Information Support Forces this month. Despite these growing threats, experts point out that the number of Chinese-made devices in U.S. networks has increased over the past year, reaching 300,000, which is 40% higher than last year (185,000).

The EU is taking steps to adapt to a new, more dynamic cyber threat landscape. In particular, the EU is developing a Space Law that will include cybersecurity issues, which is especially relevant against the backdrop of increasing efforts by both state and private companies to explore space (including launching satellite systems into orbit). Additionally, the EU is gradually preparing for the widespread adoption of post-quantum cryptography to prevent new cyber threats. For this purpose, the European Commission issued recommendations to EU members, explicitly pointing out the need for developing relevant roadmaps. Germany plans to create a separate cyber forces branch of the military for faster responses to new threats.

Law enforcement continues successful cyber operations against cybercriminal infrastructure. In April, British police disrupted the operations of LabHost, which provided platform as a service (PaaS). However, the long-term impact of these operations has sparked discussions. Experts at Trellix found that the infrastructure of the supposedly dismantled LockBit group is actively being restored and is starting to operate again.

In April, infrastructure relying on open-source software faced a global threat related to a sophisticated and well-prepared attempt to compromise the XZ Utils library by unknown criminals. A Microsoft employee incidentally discovered the threat. This incident has once again highlighted concerns about the security of open-source products and the need for changes in approaches to prioritize the security of applications. In this context, CISA revitalized its initiatives regarding summits for open-source software developers and implementing secure-by-design principles.

russian hackers continue to target Ukraine's allies, not only attacking local municipal systems in the U.S. but also deploying new backdoors during attacks in Eastern Europe. Meanwhile, Ukraine actively launches counterattacks. For example, there was a successful operation by the pro-Ukrainian hacker group Blackjack that targeted the infrastructure of russia's Moscollectors.

1. CYBERSECURITY SITUATION IN UKRAINE

UKRAINE IS DEEPENING COOPERATION WITH CYBERSECURITY AGENCIES IN THE EU, NATO, AND ROMANIA

On April 11, a delegation of representatives from Ukraine's key cybersecurity entities, led by NCSCC Secretary Nataliya Tkachuk, visited the European Cybersecurity Competence Center (ECCC), the Euro-Atlantic Resilience Center (EARC), the Project Office of the Council of Europe Convention on Cybercrime (C-PROC), the National Cybersecurity Directorate of Romania (DNSC), and the Polytechnic University of Bucharest. During the meeting with ECCC head Luca Tagliaretti, the delegation discussed prospective areas of cooperation and Ukraine's participation in ECCC's «Digital Europe» and «Horizon Europe» programs. The delegation also presented a letter from NSDC Secretary Oleksandr Lytvynenko expressing intentions for partnership and cooperation between the NCSCC and ECCC.

THE NCSCC SECRETARY URGED EU AND NATO COUNTRIES TO COLLABORATE IN COUNTERING RUSSIA'S CYBER AGGRESSION

On April 12 in Bucharest , Romania, the NCSCC and Civil Research and Development Fund (CRDF Global) held the third international meeting of the National Cybersecurity Cluster on the topic «Building Partnerships for Cyber Resilience in Southeast Europe.» During the event, NCSCC Secretary Nataliya Tkachuk noted that today the russian federation is waging cyber warfare not only against Ukraine, but also against EU and NATO countries. «It is important to have a clear message from our partners that such actions are unacceptable, as well as to ensure public attribution to the russian federation. Otherwise, the sense of impunity will lead to further escalation of covert cyber aggression by the russian federation against countries of the Euro-Atlantic community and their citizens,» said the NCSCC Secretary. Participants discussed several topics, including risks of cyber warfare escalating in Southeast Europe, synergy between the state and business to strengthen collective security, deepening cooperation with the EU and NATO, and practical steps for Ukraine in the field of cybersecurity.

UKRAINE PARTICIPATED IN NATO CCDCOE CYBER DEFENSE TRAINING LOCKED SHIELDS

Ukrainian representatives took part in Locked Shields 2024, the world's largest realistic cyber defense exercise, highlighting the global community's commitment to combating cyber threats. The NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) organized the training for approximately 4,000 experts from over 40 countries. NSDC Deputy Secretary Serhii Demediuk emphasized the importance of Ukrainian experts' participation in Locked Shields cyber exercises to strengthen both national and international cyber resilience. «This year, Ukraine is teaming up with Czechia as a joint team for these exercises. Collaborative skill development, knowledge sharing, and cooperation are key elements in effectively countering modern cyber threats.»

FOR THE FIRST TIME, UKRAINE PARTICIPATED IN AN EXPLANATORY SESSION OF THE EUROPEAN COMMISSION DEDICATED TO DIGITALIZATION

On April 23, European Commission for Ukraine regarding Negotiation Chapter 10 «Digital Transformation and Media» held an explanatory session. This was Ukraine's first meeting as a candidate country with EU representatives dedicated to the digitalization sphere. The EU expressed readiness to continue supporting Ukraine on its path towards European integration reforms, including via the Ukraine Facility mechanism, which outlines comprehensive reform and investment strategies for the next four years. The European Commission also presented over 100 EU legal acts, describing the specifics of each and insights for implementing them. The list of acts includes existing EU legislation being implemented within the Association Agreement with Ukraine, as well as acts that are currently in the project stage but are expected to be adopted by the EU soon and become mandatory for Ukraine, e.g., eIDAS 2, the Artificial Intelligence Act, the Cyber Resilience Act, and the Cyber Solidarity Act.

UNIFIED CYBERSECURITY STANDARDS: THE MINISTRY OF DEFENSE STRENGTHENS THE PROTECTION OF INFORMATION SYSTEMS IN ACCORDANCE WITH NATO STANDARDS

The Ministry of Defense has issued an order approving the basic principles of information security and cybersecurity in information and communication systems. It establishes unified basic requirements (top-level policy) for information protection and cybersecurity in the Ministry of Defense systems. This means that all systems, services, applications, and digital tools of the Ministry of Defense will have unified, clearly defined rules regarding cybersecurity. They will incorporate the best NATO approaches, international standards, and practices in information and cybersecurity.

NCSCC REPRESENTATIVES MET WITH A REPUBLIC OF KENYA DELEGATION

NCSCC representatives briefed the delegation on the center's activities and potential areas of cooperation with Kenya. In particular, they emphasized the potential for exchanging experiences and information in cybersecurity, conducting training events, and enhancing efforts to counter the spread of russian disinformation about Ukraine in African countries. The Kenyan delegation expressed interest in Ukraine's assistance for countering cyber threats and the spread of russian disinformation, including through joint training events and expertise provided by Ukrainian experts.

THE NCSCC CONDUCTED «VULNERABILITY MANAGEMENT» TRAINING FOR CYBERSECURITY SPECIALISTS FROM OBLAST MILITARY ADMINISTRATIONS

With support from the U.S. State Department and CRDF Global, the NCSCC conducted a «Vulnerability Management» (VDP) training for cybersecurity experts from oblast military administrations. Representatives from all regions of Ukraine participated in the event. The training enhanced the professionals' practical knowledge in conducting comprehensive analyses of the cybersecurity status of their institutions and improved their understanding of the principles and approaches used by malicious actors in cyberattacks.

ARMУ+ HAS A SPECIFIC ARCHITECTURE THAT ALLOWS DATA TO BE PROTECTED AS SECURELУ AS POSSIBLE – KATERУNA CHERNOHORENKO

Deputy Minister of Defense Kateryna Chernohorenko explained that the main task facing the developer team is to ensure the reliable protection of military's personnel personal data and official information, even if the process requires more time. "The mobile application itself serves as a kind of preventive measure against leaks because it has a specific architecture that allows for protecting personal data aggregation. We are already involving top experts in the design and development phase of the application. We are separately working on a comprehensive system to ensure that the application is protected at the proper level. Data security is our top priority. And we are willing to partially sacrifice release deadlines for the sake of security," said the Deputy Minister of Defense.

NATALIУA TKACHUK HIGHLIGHTED THE IMPORTANCE AND URGENCУ OF REFINING SECTORAL AND INTERAGENCУ COLLABORATION IN RESPONDING TO CУBERATTACKS

Nataliya Tkachuk, Head of Information Security and Cybersecurity Department NSDC of Ukraine, participated in command-post table top exercises (TTXs) aimed at refining the response mechanism to situations caused by cyber and hybrid threats in the energy sector. During her opening remarks, she noted that the NCSCC had introduced the practice of conducting command-post TTX in Ukraine and enshrined it in Ukraine's Cybersecurity Strategy. TTXs allow for identifying weaknesses in the response mechanism to cyber threats and addressing existing gaps. «Sectoral TTXs, particularly in the energy sector, play a crucial role. Against the backdrop of heightened cyber aggression from the russian federation, which has even begun coordinating cyberattacks with missile strikes on critical infrastructure objects, such exercises become more than relevant and necessary,» – Tkachuk said.

THE SSSCIP, CRITICAL INFRASTRUCTURE FACILITIES, AND STATE AGENCIES DEVELOPED CУBERSECURITУ PROTECTION PLANS FOR INSTITUTIONS

The SSSCIP held the third 1-day in-person seminar, «Cyber Incident Response» for representatives of government agencies and critical infrastructure facilities, with support from the National Agency of Ukraine for Civil Service, the National University of Public Administration, and the EU-funded project «Support to Comprehensive Reform of Public Administration in Ukraine» (EU4PAR 2). Representatives from 21 organizations worked on developing and updating cybersecurity protection plans. Specifically, they formulated a minimum set of tasks that should be implemented or planned for implementation at critical infrastructure sites. SSSCIP and CERT-UA experts supervised the entire process.

MEDICAL INSTITUTION REPRESENTATIVES LEARNED HOW TO COMBAT RANSOMWARE CУBERATTACKS

SSSCIP experts conducted a TTX, CIREX.Cyber.Ransomware, to improve skills in countering hacker attacks that use ransomware programs. Over 30 representatives from medical institutions participated, along with specialists from key entities in the national cybersecurity system. SSSCIP developed the training using CISA's advanced methodologies, adapted to the Ukrainian threat landscape by SSSCIP and Ministry of Health experts.

UKRAINE LAUNCHED AN INTERDEPARTMENTAL EDUCATIONAL PLATFORM FOR THE SECURITY AND DEFENSE SECTOR

The SBU National Academy presented an interdepartmental educational platform with 12 certification programs for representatives of the security and defense sector in Ukraine and international partners. Through this interdepartmental educational platform, security and defense sector professionals will be able to do short-term trainings at the SBU Academy in areas such as counterterrorism, operational search activities, protection of critical infrastructure objects, operational psychology, protection of state secrets, crisis negotiation, combating crimes involving virtual assets, and more. The programs are flexible and can accommodate the individual needs of security and defense sector units.

IN KHMELNYTSKYI, CYBER POLICE CONDUCTED TRAINING ON DIGITAL SECURITY FOR GOVERNMENT AUTHORITIES AND LOCAL SELF-GOVERNMENTS

Khmelnytskyi cyber police experts conducted the training for officials as part of a 2-day seminar «Building a Network of Digital Leaders,» organized by the United Nations Development Programme (UNDP) in Ukraine with support from the Swedish government. Government authorities, local self-governments, local training centers, and invited experts learned about the most common cybercrimes and the most important cyber hygiene rules, and were briefed on the Brama («Gate») cyber police project, which specializes in combating disinformation and illegal content in information space.

SSSCIP EXPERTS CONDUCTED A TRAINING FOR FACILITATORS OF COMMAND AND STAFF EXERCISES

SSSCIP experts conducted a training for TTX facilitators with representatives of sectoral bodies that protect critical infrastructure. Nearly two dozen representatives from central executive authorities participated in the 3-day training, with support from the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The training provided invited ministry representatives with the necessary knowledge to facilitate TTX and other types of exercises.

THE MINISTRY OF FOREIGN AFFAIRS ANNOUNCED A SCIENTIFIC-PRACTICAL CONFERENCE ON CYBER DIPLOMACY

On April 5, Deputy Minister of Foreign Affairs for Digital Development, Digital Transformation, and Digitalization Anton Demiohin participated in the inaugural meeting of the organizing committee for the international «Cyber Diplomacy Forum.» In his welcoming remarks, Deputy Minister Demiohin noted that «given the participants' scientific and educational potential, the Forum is intended to become a leading platform for cooperation and innovation development in the field of cyber diplomacy, as well as a foundation for ensuring peace, stability, and resilience in the digital age.» The first event will be the «First Scientific and Practical Conference on Cyber Diplomacy,» scheduled for May 15-16, 2024, in Kyiv. Its goal is to explore the potential of cyber diplomacy and its role in shaping the future of international relations.

THE SBU IDENTIFIED HACKERS FROM THE RUSSIAN GROUP RESPONSIBLE FOR ATTACKING KYIVSTAR

SBU cyber experts and investigators are gathering evidence against hackers from the Main Intelligence Directorate of the General Staff of the Armed Forces of the russian Federation (GRU), who carried out an attack on Kyivstar, one of the national mobile network operators. After conducting all necessary analyses and pressing chargers, Ukraine will forward the investigation materials to the International Criminal Court (ICC) in The Hague.
Currently, the SBU has determined that the hacker group SandWorm, which is a regular subdivision of the GRU, executed the attack on Kyivstar. The SBU is examining the affected systems and the damage the hackers inflicted. Additionally, the security service sent requests for additional information to international partners.

THE CYBER POLICE AND THE CENTER FOR COUNTERING DISINFORMATION SIGNED A MEMORANDUM OF COOPERATION

On April 2, Chief of the Cyber Police Department Yuriy Vyhodets and Head of the Center for Countering Disinformation Andriy Kovalenko signed a memorandum of cooperation, emphasizing the importance of coordinating actions between government agencies and exchanging experiences in countering disinformation. This includes conducting joint trainings, conferences, and educational programs to enhance cyber and media literacy among Ukrainians. The leaders also discussed current areas of collaboration and the pressing challenges in information security posed to Ukraine by russia's full-scale aggression.

THE CYBER POLICE LAUNCHED THE NEW PROJECT «CYBER GATE» TO IMPROVE THE LEVEL OF CYBER HYGIENE AMONG UKRAINIANS

On April 4, law enforcement officials presented the online platform Cyber Gate, which provides internet users with the tools and knowledge necessary for safely navigating the digital space. The Advisory Mission of the European Union in Ukraine created the project at the initiative of the Department of Cyber Police of the National Police of Ukraine, in partnership with the public organization MINZMIN. The International Renaissance Foundation and the Representation of the European Union in Ukraine are supporting the project's implementation. Cyber Gate is designed for various kinds of users, including students, educators, and entrepreneurs. The resource contains practical recommendations and tools for protection against cyber threats, fakes, and disinformation. Thanks to the project, citizens will be able to receive useful information and easily learn the nuances of safely using online platforms, including social media.

CERT-UA PUBLISHED INSTRUCTIONS FOR SETTING UP 2FA IN POPULAR MESSENGERS

CERT-UA developed instructions for setting up 2FA for certain messengers and information systems, including Telegram, Signal, WhatsApp, Viber, Ukr.net, Google, and Facebook. Using these settings is particularly important in situations where public email services are used as the primary «corporate» means of electronic correspondence.

SSSCIP HEAD MET WITH AMERICAN CHAMBER OF COMMERCE LEADERSHIP

SSSCIP Head Yuriy Mironenko and his team held a working meeting with Vice President of the American Chamber of Commerce in Ukraine (AmCham) Tetiana Prokopchuk, member of the AmCham Board of Directors Serhiy Martynchyk, and members of the AmCham Security and Defense Committee. During the dialogue, the parties discussed a number of relevant issues, including legislative initiatives that businesses may be involved in developing, cybersecurity and critical infrastructure protection issues, and regulating the cloud services sector.

CERT-UA WARNED OF A CYBER THREAT TO THE ARMED FORCES OF UKRAINE (AFU)

CERT-UA reported increased activity from the UAC-0184 group, which is attempting to gain access to military personnel's computers to steal documents and messenger data. The perpetrators are using popular messaging apps, social networks, and other platforms for introductions and communication with the aim of spreading malware. Their methods include:

- tempting lure messages, such as opening executive proceedings/criminal cases; combat action videos; requests for acquaintance, etc.
- files (archives) asking for help in opening/processing them

The attackers employ various malicious programs, including for data theft and extracting from a computer, particularly messages and contact information from the Signal messenger, which is quite popular among military personnel.

RUSSIAN HACKERS USE SOCIAL ENGINEERING FOR CYBERATTACKS ON THE AFU

CERT-UA warned of a new cyber threat targeting AFU military personnel. Attackers are distributing malicious files via the Signal messenger, disguising them as documents required for positions in the United Nations (UN) Department of Peace Operations. CERT-UA is tracking this hostile hacker group under the identifier UAC-0149. It is particularly active against individual service members, employing deception and various offers.

SCAMMERS STEAL WHATSAPP ACCOUNTS BY USING FAKE PETITIONS ASKING TO CONFER THE TITLE OF «HERO OF UKRAINE» ON FALLEN DEFENDERS

CERT-UA warned about a new scam to steal Ukrainians' WhatsApp accounts. Scammers send messages via WhatsApp, urging users to vote for an electronic petition to posthumously confer the title of «Hero of Ukraine» on Ukrainian Armed Forces service members. The messages contain links to a fake website mimicking the official «Electronic Petitions» webpage. CERT-UA has been tracking this activity since April 2024 under the identifier UAC-0195. As of April 20, CERT-UA had identified 18 domain names associated with this scam and had submitted corresponding requests to block them.

THE SBU DETAINED PRO-RUSSIAN HACKERS IN KYIV WHO CREATED FAKE ACCOUNTS OF UKRAINIAN SPECIAL SERVICE OFFICIALS

The SBU shut down bot farms in Kyiv that conducted information sabotage in favor of russian intelligence. During comprehensive actions, two organizers were detained who spread disinformation about the war in Ukraine and attempted to artificially discredit the AFU. They created fake accounts on social media and messenger apps, including ones impersonating the SBU Head and Chief of the Main Intelligence Directorate of the Ministry of Defense (HUR). They also registered fake profiles of Ukrainians from different regions on social media. Overall, the bot farm's capabilities allowed the organizers to generate over 1,000 fake accounts per day. The criminals coordinated their actions with russian intelligence representatives, from whom they received instructions for subversive activities. The suspects are in custody, facing up to 7 years in prison.

2. THE FIRST WORLD CYBER WAR

INSIDE RUSSIA'S SHADOW TRADE IN WEAPON PARTS FUELED BY CRYPTOCURRENCY

On April 1, The Wall Street Journal described how the stablecoin Tether became «indispensable» for russia's military industry. While the U.S. Treasury Department imposed sanctions, aiming to limit moscow's ability to manufacture weapons and develop its military industry, the kremlin managed to circumvent the sanctions using cryptocurrency and paid China millions in cryptocurrency for producing high-tech weapon components.

HACKERS STOLE THE RUSSIAN PRISONER DATABASE TO RETALIATE FOR NAVALNY'S DEATH

On April 1, CNN reported that hackers gained control of the russian penitentiary system's website and published a photo of Navalny and his widow Yulia at a rally with the message «Long live Alexei Navalny!». They also claimed to have stolen a database containing information on hundreds of thousands of russian prisoners, including data on those incarcerated at the penal colony where Navalny died on February 16. It was reported that it took the russian authorities several days to regain control of their computer network. The hackers, among whom, according to CNN, were representatives of various nationalities, say they released this information, including contact information for prisoners' relatives, «in the hope that someone could contact them and help understand what happened to Navalny.»

RESEARCHERS DISCOVERED A NEW RANSOMWARE GANG THAT TARGETS RUSSIAN BUSINESSES, MULYAKA

A previously unknown ransomware gang is targeting russian companies using malicious software based on leaked source code from the Conti hacker group. Dubbed Mulyaka by researchers at the moscow-based cybersecurity company F.A.C.C.T., the gang has left minimal traces of its attacks but is believed to have been active since at least December 2023. Their sophisticated methods make this group worthy of attention. In one registered incident in January, Mulyaka attacked a business by encrypting its Windows systems and VMware ESXi virtual infrastructure using its victim's own virtual private network (VPN) service. The malicious software was disguised as ordinary corporate anti-virus software, allowing it to bypass security protocols and encrypt network files. The geopolitical context in russia creates an optimal environment for such cybercriminal activity. F.A.C.C.T. speculates that the current political situation fosters impunity, negligence in business cybersecurity, and many potential victims, making it attractive to financially motivated hacker groups.

UKRAINE AWARDED FOREIGN IT PROFESSIONALS FOR THEIR ASSISTANCE IN CYBER DEFENSE AGAINST RUSSIA

On April 4, the BBC published an article about foreign IT volunteers who are assisting Ukraine in countering russia's aggression. Author Joe Tidy expresses doubts about the ethics of awarding such cyber experts with distinctions from the AFU, including the Air Assault Forces of Ukraine, as he believes it blurs the distinction between combatants and non-combatants in cyberspace. Ukraine awarded cyber experts from the One Fist group who helped Ukraine obtain data from cameras in occupied Crimea to catalog russian tanks and equipment being transported across the Kerch Strait bridge, as well as stole 100 gigabytes of data from a russian weapons manufacturer.

CLAROTY ANALYZED THE PRO-UKRAINIAN GROUP BLACKJACK'S CYBERATTACK ON THE PHYSICAL INFRASTRUCTURE OF RUSSIA'S MOSCOLLECTOR

On April 15, the industrial and corporate Internet of Things (IoT) cybersecurity firm Claroty conducted an analysis of the malware Fuxnet, designed for attacking Industrial Control Systems (ICS) – the same malware pro-Ukrainian hackers recently used to target the infrastructure of the russian organization Moscollector. According to Claroty's assessment, the group failed to fully achieve the results they claimed. Instead of compromising 87,000 sensors, including those associated with airports, metro systems, and gas pipelines, the hackers managed to disrupt 500 sensor gateways. While this number is lower than claimed, it is still significant because Moscollector will need to spend time physically replacing them, especially considering that these sensors are distributed throughout moscow.

ACCORDING TO MICROSOFT, RUSSIA HAS SIGNIFICANTLY INTENSIFIED ITS INFLUENCE OPERATIONS AGAINST THE U.S. OVER THE PAST TWO MONTHS

In an April 17 report on hostile activity by foreign entities against the American electoral process, Microsoft highlighted that russia has significantly increased its activity to promote anti-Ukrainian narratives in the USA. The main group Microsoft tracked in this regard is Storm-1516, which employs standard techniques used by Russian/Soviet intelligence agencies, conducting information insertion through unreliable sources that then spread through a network of websites, from where these messages are disseminated by legitimate users (russian migrants, officials, and simply interested individuals).

RUSSIAN HACKERS MANAGED TO INFLUENCE THE WATER SUPPLY SYSTEM OF THE SMALL TEXAS TOWN OF MULSHOU

On April 22, details were revealed about cyberattacks on water supply systems in several small American towns, mostly in Texas. The russian group CyberArmyofrussia_Reborn targeted water supply systems in small towns with 2,000-5,000 residents. In one instance, the attack was successful – hackers caused the water supply system to overflow before the attack was halted, and company specialists switched its operation to manual mode. These attacks are a logical continuation of a series of attacks on similar targets that the USA faced in fourth quarter of 2023. The cybersecurity company Mandiant released a report accusing the russian advanced persistent threat (APT) group Sandworm of these attacks.

THE LAPTOP OF THE CHAIR OF THE BELGIAN PARLIAMENTARY COMMITTEE ON FOREIGN AFFAIRS WAS HACKED BY CHINESE HACKERS

On April 25, Els Van Hoof, Chair of the Belgian parliamentary committee on foreign affairs, announced that her laptop had been hacked by Chinese hackers back in 2021. According to her, 400 members of the Inter-Parliamentary Alliance on China (IPAC), a group uniting a network of politicians critical of China (of which Els Van Hoof is a member), were targeted in this cyberattack.

HOW UKRAINIAN HACKER-VOLUNTEERS CREATED A «COORDINATED MACHINE» AROUND LOW-LEVEL ATTACKS

The Record recounts the story of creating and the role of the Ukrainian IT army in cyber resistance against russia. The article notes that the Ministry of Digital Transformation created the IT army to combat russia in cyberspace, using tactics such as website defacement and disruption. Questions remain regarding the group's ties to the Ukrainian government: despite being created by the Ukrainian government's directive, both the IT army and officials claim that their cooperation ended once it was established. However, the nature of the IT army's work leads some global cyber analysts to speculate about potential unofficial cooperation between the group and Ukrainian defense and intelligence sectors.

RUSSIAN APT USES NEW BACKDOOR KAPEKA DURING ATTACKS IN EASTERN EUROPE

The previously undocumented «flexible» backdoor Kapeka has been «sporadically» observed during cyberattacks targeting Eastern Europe, including Estonia and Ukraine, at least since mid-2022, according to the Finnish cybersecurity firm WithSecure, which attributed the malicious software to the russia-linked group Sandworm (also known as APT44 or Seashell Blizzard). Microsoft tracks the same malware under the name KnuckleTouch.