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

OCTOBER-NOVEMBER 2023

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

CONTENT

ACRONYMS

AI	Artificial Intelligence
C2C	Customer-to-Customer
CERT-UA	Government Computer Emergency Response Team Ukraine
CISA	Cybersecurity & Infrastructure Security Agency
COVID-19	Coronavirus Disease or 2019 Novel Coronavirus
CRDF Global	Civil Research and Development Fund (U.S.)
DHS	U.S. Department of Homeland Security
EDMS	Electronic Document Management System
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUCS	European Cybersecurity Certification Scheme for Cloud Services
FEMA	U.S. Federal Emergency Management Agency
FSB	Federal Security Service (russian federation)
ICC	International Criminal Court
ICS	Industrial Control System
ICT	Information and Communications Technology
IT	Information Technology
MITRE	
NATO	North Atlantic Treaty Organization
NCSCC	National Cybersecurity Coordination Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency (U.S.)
NSDC	National Security and Defense Council of Ukraine
OJSC	Open Joint-Stock Company
OSINT	Open-source Intelligence
OT	Operational Technology
OWA	Outlook on the Web
SBI	State Bureau of Investigation of Ukraine
SBU	Security Service of Ukraine
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
TTX	Table Top Exercise
U.S.	United States
UDCG	Ukraine Defense Contact Group
UK	United Kingdom
USAID	United States Agency for International Development

KEY TENDENCIES

The world continues to formulate a systemic cybersecurity policy on artificial intelligence (AI). At the end of October, US President J. Biden signed a new decree. For its implementations, Cybersecurity & Infrastructure Security Agency (CISA) has already published its own Roadmap on how this key federal cybersecurity agency will take into account AI challenges in its activities, and it has already issued joint recommendations for the safe development of AI systems in cooperation with the UK National Cyber Security Centre (NCSC). The European Union, in turn, plans to conduct the risk assessment posed by AI; the results of this assessment will be used to develop a regulatory framework and policies to reduce risks and strengthen the EU's position in the global technological landscape. This intensification of governmental efforts is driven by the increased use of AI-based technologies: from the development of new software to threats to autonomous maritime transport control systems.

The digital global rivalry between USA and China is ongoing. RAND Corporation in its research indicates that it is the competition between the United States and China for digital infrastructure that will be crucial for military forces and operations in the region. Chinese APT groups are stepping up their cyber-espionage operations, both against government organisations (such as a major campaign against Cambodian government agencies) and the private sector (including a group of semiconductor manufacture companies in East Asia).

The fight against ransomware continues. The United States is currently considering the next step in the fight not only to combat the criminal infrastructure or specific groups, but also to change the behaviour of victims. In particular, this includes strengthening measures to prevent the payment of ransoms in order not to encourage criminals to commit malicious acts. So far, these efforts have been only partially successful, as ransomware groups continue to be quite successful while attacking new targets. In November, one of the major banks in China (ICBC) and the British Library were targeted by the actions of such groups. In the United States, the healthcare sector remains under attack. The lack of attention to cybersecurity in this sector is evidenced by the fact that, according to Sophos, attackers managed to encrypt data in almost three quarters of attacks.

The last quarter of the year is a traditional time for the cybersecurity landscape predictions for the next year. In October-November, there were two of such insights from Proofpoint and Trellix. Despite different emphases, both companies note the growth of threats from AI (its criminal use to organise phishing attacks, voice fraud), phishing attacks against mobile devices, increased attention of criminals to user accounts, and hidden attacks on peripheral devices. These predictions are complemented by the UK's NCSC assessments, which noted that the critical infrastructure objects face a 'continuing and significant threat' amid the rise of state groups, as well as a result of increased overall aggressive cyber activity and new geopolitical challenges.

Generally, more and more companies are noticing an increase in the perpetrators' attention to social engineering. Although 'human attacks' have been a key method in the early stages of cyberattacks, AI has given a new impetus to this activity. AI's ability to create more authentic phishing emails, imitate people's voices and even videos, and the ability to dynamically manage a large number of social media accounts is significantly changing the threat landscape.

The most notable case in the field of threats to critical infrastructure was the successful attack against the control system associated with a hydraulic lift station conducted by the Iranian cyber group Cyber Av3ngers. Although the company stated that there were no threats to users, the fact that an industrial system was attacked represents a steady trend of hackers' attempts to influence the functioning of critical infrastructure. This is particularly worrisome because many industrial control systems are accessible via the Internet. So far, researchers have identified about one hundred thousand such systems, even though stricter security regulations have led to a decrease in this figure compared to 2019. This is compounded by the discovery of new zero-day vulnerabilities in industrial routers. As a countermeasure, security organisations (CISA, NSA) are publishing new open-source OT security guidelines and have also launched the OT Intrusion Detection Signature and Analytics repository to help identify and detect potentially malicious cyber activity in industrial OT environments faster. Despite all these efforts, the US healthcare sector has made little progress in improving its cybersecurity.

In October-November 2023, Ukrainian law enforcement agencies managed to conduct several successful operations against international cybercrime groups. One of the biggest successes was the elimination of a group that caused $80 million in damage through the use of ransomware. These successes are complemented by other operations of the Cyberpolice jointly with Czech colleagues, as well as an operation against a group that has attacked 168 companies since 2020.

The development of international cooperation remains an important vector of activity for Ukrainian cybersecurity structures. In November 2023, Ukraine (the National Coordination Centre for Cybersecurity (NCCC) of the National Security and Defense Council of Ukraine (NSDC) and the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) signed the Working Arrangement on cooperation with the European Union Agency for Cybersecurity (ENISA). For ENISA, this was the first such agreement with a non-EU partner. The signing of such document is an important element in the formation of a global cyber coalition to counter threats emanating from russia and other states that stand on the same side with the aggressor.

Hostile activity continues as in the reporting period alone, russia's APT29 attacked embassies across Europe, and the UAC-0165 group attempted to interfere with 11 Ukrainian providers; these data are supplemented by another report from the SSSCIP, which indicates that the number of registered cyber incidents in the first half of 2023 more than doubled.

Ukrainian cybersecurity agencies (the SSSCIP and the Security Service of Ukraine (SSU)) have released their own assessments of the current Ukrainian cyber threat landscape and predictions for the near future. These assessments include an increase in the number of sophisticated attacks on supply chains, and companies that develop software for critical infrastructure and the military will be subject to active targeted cyberattacks in the long term. On the other hand, most hostile cyberattacks are already aimed at accessing the electronic document flow of Ukrainian government agencies and technological infrastructure systems. Thus, the SSU and the SSSCIP drew the attention of power companies to the increased cybersecurity threats from russia in the winter. Based on the previous years' experience, the special services point to the likelihood of active attempts of russian hackers to influence the operation of critical information infrastructure facilities, the energy sector, and the provision of vital services.

Ukraine continues to expand its cyber incident response capabilities. In particular, it is expanding the practice of conducting cyber exercises (for example, the NCCC held the HackWave cybersecurity competition and INCIDENT RESPONSE DAYS 2.0, as well as CI-REX. CoBridge — the first sectoral cyber exercise for the transport industry). Additionally, it launches new cyber hygiene tools (for example, the Ministry of Digital Transformation launched a test on the knowledge of security rules in the Cybergram network, and the SSSCIP held an all-Ukrainian online cybersecurity lesson for more than 20 thousand viewers) and stimulates innovations in the cybersecurity sector.

There is an ongoing discussion regarding more radical changes in the activities of Ukrainian security agencies in the field of cybersecurity. For instance, in November 2023, for the first time the Defense Intelligence of Ukraine conducted an offensive cyber operation, which was announced publicly. Nataliia Tkachuk, the Secretary of the NCCC of the NSDC, also emphasised the urgent need to create Ukrainian cyber forces based on Ukraine's experience and successful international cases.

The First World Cyber War continues, and the aggressor does not reduce the intensity of its actions. At the same time, according to Microsoft, in 2023, authoritarian governments (russia, China, Iran, and North Korea) focused on cyber espionage operations in an effort to gain more information about important foreign policy initiatives.

At the same time, attacks on the critical infrastructure are still an important goal of cyber operations. This is evidenced by Mandiant's report on the SandWorm cyberattack on the operational technology (OT) systems of a Ukrainian power company in late 2022. The actor first used OT-level liveing off the land (LotL) techniques to likely trip the victim's substation circuit breakers, causing an unplanned power outage that coincided with massive missile strikes on critical infrastructure across Ukraine. Cyber-attacks against the energy sector around the world by russian criminal groups are a noticeable trend, and such actions are becoming increasingly dangerous. A prominent example is Denmark, where 22 energy companies were subjected to a coordinated cyberattack in May 2023. Sandworm (APT28) is suspected to be behind this attack.

1. CYBERSECURTY SITUATION IN UKRAINE

UKRAINE AND ENISA SIGNED THE WORKING ARRANGEMENT

On 13th November, ENISA and Ukraine (represented by the National Coordination Centre for Cybersecurity (NCCC) of the National Security and Defense Council of Ukraine of Ukraine (NSDC) and the State Service of Special Communications and Information Protection of Ukraine (SSSCIP)) signed the Working Arrangement. The agreement envisages cooperation in several areas: raising awareness and expanding capacities to strengthen cyber resilience; sharing best practices to ensure legislation harmonisation and implementation (including NIS2 in cyber field, and in such sectors as telecommunications and energy); sharing knowledge and information on the cybersecurity threat landscape to increase overall situational awareness, etc. This is the first cooperation arrangement for ENISA with a non-EU partner.

NCCC HELD AN INTERNATIONAL MEETING OF THE NATIONAL CYBERSECURITY CLUSTER IN PRAGUE

On 26th October 2023, the National Coordination Center for Cybersecurity (NCCC) of the National Security and Defense Council of Ukraine (NSDC), together with CRDF Global in Ukraine and with the support of the U.S. Department of State, held an international meeting of the National Cybersecurity Cluster 'Public-Private Partnerships at the International Level and Introduction of Cyber Diplomacy' in Prague.

During the discussion panels the participants discussed several topics, including Ukraine's experience and the world's leading countries in cyberwarfare; development of cyber diplomacy both in Ukraine and the world; public-private partnerships to ensure global resilience in cyberspace.

UKRAINE SIGNED THE BLETCHLEY DECLARATION ON ARTIFICIAL INTELLIGENCE SAFETY

On 2nd November, Ukraine signed the Bletchley Declaration on Artificial Intelligence Safety at the AI Safety Summit attended by representatives of 29 governments, including the US, Australia, and the EU. One of the main goals of the declaration is the countries' collective agreement to develop and implement risk-oriented AI regulation policies that would prevent negative consequences. At the same time, the summit emphasised that AI is a useful technology for economic growth and sustainable development.

DEFENCE INTELLIGENCE OF UKRAINE CONDUCTED THE FIRST OFFENSIVE CYBER OPERATION

On 23rd November, the Defense Intelligence of the Ministry of Defence of Ukraine reported a successful special operation in cyberspace against the 'federal air transport agency' ('rosaviatsia'). The operation resulted in the acquisition of a large volume of classified official documents of rosaviatsiia. As the result of hacking, among the obtained data there was a list of daily reports of 'rosaviatsiia' for the entire russian federation for more than a year and a half. This is the first time that the Ukrainian security service has reported an offensive operation in cyberspace.

THE NCCC WITH THE SUPPORT OF JAPANESE INTERNATIONAL COOPERATION AGENCY (JICA) HELD AN INTEGRATED FOUR-DAY CYBER TRAINING — HACKWAVE 2023

On 26-29th September, the NCCC, with the support of the Japan International Cooperation Agency (JICA) and CRDF Global in Ukraine, held an integrated four-day cyber training Hackwave 2023 for representatives of the public sector and critical infrastructure objects. The main goal of Hackwave 2023 was to comprehensively improve the specialists' knowledge and skills in detecting and responding to cyberattacks, as well as assessing their readiness for cyberattacks.

This was the first cyber training in Ukraine where teams of cybersecurity, management, and communication specialists competed simultaneously.

UKRAINE CALLED FOR SYSTEMATIC DOCUMENTATION OF RUSSIAN WAR CRIMES USING ELECTRONIC EVIDENCE AT IGF 2023

In October 2023, Nataliia Tkachuk, the Secretary of the NCCC, during her participation in the International Internet Governance Forum (IGF 2023), stressed that in addition to defeating the enemy and rebuilding Ukraine, an important task is to bring to justice all russian war criminals responsible for the crimes committed in Ukraine: 'Since the beginning of the aggression of the russian federation, the law enforcement agencies of Ukraine have registered more than 100,000 war crimes. This is an unprecedented number that requires the involvement of all of civil society and the international community in documenting them, the OSINT techniques and the use of electronic evidence are an important tool'.
The IGF is held under the auspices of the United Nations. This year it brought together more than 5000 participants from 175 countries.

THE MINISTRY OF DEFENCE OFFICIALS MEET WITH MILITARY ATTACHES IN KYIV AS PART OF IT COALITION

Rustem Umerov, the Minister of Defence, chaired a meeting with military attaches within the IT Coalition in Kyiv. The event was attended by representatives of more than 30 countries participating in the Ukraine Defence Contact Group. The Minister of Defence of Ukraine emphasised that the war would be won by technology. The meeting participants were also informed on the priority needs that Ukraine expects to receive from the IT Coalition members.

SERHII DEMEDIUK, THE DEPUTY SECRETARY OF THE NSDC: WE NEED TO CREATE A UNIFIED SYSTEM FOR CYBER INCIDENTS INVESTIGATING

On 31st October, Serhii Demediuk, the Deputy Secretary of the NSDC, at an event at the Security Service of Ukraine Academy stated that Ukraine is in dire need of a unified system for investigating cyber incidents. This is due to the fact that although Ukraine has learnt how to effectively examine digital evidence, the process of collecting and documenting it remains a problem. This, in turn, complicates the process of investigating the malicious activities of russian hackers, as well as war crimes of the russian federation.

NATALIIA TKACHUK, THE SECRETARY OF THE NCCC: UKRAINE SHOULD CREATE CYBER FORCES AND ADOPT THE RELEVANT CONCEPT OF THE UKRAINIAN CYBER FORCES

On 10th November, during an interagency event on 'Ensuring the State's Cyber Defence' Nataliia Tkachuk, the Secretary of the NCCC, stressed the need to create Ukrainian cyber forces as soon as possible, based on Ukraine's experience and successful international cases. The first step in this direction should be the development and approval of the Concept of the Ukrainian Cyber Forces.

KATERYNA CHERNOHORENKO, THE DEPUTY MINISTER OF DEFENCE, MEETS WITH DELEGATION OF THE UNITED STATES INSTITUTE OF PEACE

Kateryna Chernohorenko, the Deputy Minister of Defence of Ukraine for Digital Development, Digital Transformation and Digitalisation, met with a delegation from the United States Institute of Peace (USIP) led by Vice President and US Ambassador to Ukraine (2006-2009) Mr William Taylor. The parties discussed the effectiveness of military assistance to Ukraine from partner countries, the establishment of cooperation in the technology sector, the prospects for creating a coalition of cooperation in the engineering sector, and the digitalisation of services for war veterans.

THE NCCC EXPERTS HELD A WORKING MEETING WITH REPRESENTATIVES OF THE EMBASSY OF THE KINGDOM OF DENMARK IN UKRAINE

On 3rd November 2023, Serhii Prokopenko, Head of the NCCC Support Department, met with representatives of the Embassy of the Kingdom of Denmark in Ukraine. They discussed ways to deepen practical cooperation in countering cyberattacks, information exchange, and further partnership in educational projects.

THE MINISTRY OF DIGITAL TRANSFORMATION AND IFES SIGN A MEMORANDUM OF COOPERATION

The Ministry of Digital Transformation and the International Foundation for Electoral Systems (IFES) have signed a memorandum of cooperation. This will help to strengthen cybersecurity, promote the digital development of our country, and enable the introduction of innovative technologies to improve Ukraine's electoral processes and bring them in line with international standards.

MORE THAN 20 THOUSAND VIEWERS JOINED THE NATIONWIDE ONLINE LESSON ON CYBERSECURITY

On 31st October, the SSSCIP with the support of the Institute of Special Communications and Information Protection of Igor Sikorsky Kyiv Polytechnic Institute held an all-Ukrainian online lesson 'I. Security. Cyberspace'. The main topics included how to protect yourself from hackers, Internet scammers, cyberbullying, and cyber grooming, distinguishing between harmful and unethical content, etc.

THE SSSCIP STARTED THE COOPERATION WITH THE INFORMATION TECHNOLOGY AND CYBER SECURITY SERVICE OF THE REPUBLIC OF MOLDOVA (STISC)

The Administration of the SSSCIP and the Information Technology and Cyber Security Service of the Republic of Moldova (STISC) signed a Memorandum of Understanding on Cybersecurity. The areas of cooperation covered by the Memorandum include:

- contributing to the establishment of bilateral information exchange channels between the Computer Emergency Response Team of Ukraine (CERT-UA) and the CERT-GOV-MD Cybersecurity Centre to identify and respond to threats in cyberspace;
- exchange of information on cyber incidents, cyberattacks, and cyberthreats;
- exchange of experience and best practices in cyber defence, etc.

THE NATIONAL COORDINATION CENTRE FOR CYBERSECURITY (NCCC) HELD TWO-DAY CYBERSECURITY COMPETITIONS INCIDENT RESPONSE DAYS 2.0

On 16th-17th October 2023, the NCCC, and the CRDF Global in Ukraine held two-day cyber competitions INCIDENT RESPONSE DAYS 2.0, with the participation of more than one hundred subject-matter state experts organised into 22 teams. The event combined cybersecurity competitions and cyber operations trainings, cyber incident response and forensics. The participants were working under a unique scenario, investigating incidents, collecting artefacts, and analysing a malware for 6 hours. A total of 100 specialists took part in the training. The participants also worked on communication between the representatives of cybersecurity actors and state authorities.

SECTORAL CYBER EXERCISES FOR THE TRANSPORT SECTOR CIREX.COBRIDGE HELD IN UKRAINE

On the 20th October, the SSSCIP and the USAID Cybersecurity for Critical Infrastructure in Ukraine Project conducted CIREX.CoBridge exercises in the TTX format (tabletop exercises) that focused on critical infrastructure protection from physical attacks and cyberattacks. The event was attended by representatives of central authorities and critical infrastructure for the transport sector, civil protection agencies, law enforcement bodies. The trainings are designed based on the guidelines by the Cybersecurity and Infrastructure Security Agency (CISA).

NATALIIA TKACHUK, THE SECRETARY OF THE NCCC: TO IMPROVE THE NATIONAL CYBERSECURITY SYSTEM, NATO AND EU STANDARDS SHOULD BE IMPLEMENTED

On 23rd November 2023, during an event for the representatives of the main cybersecurity actors in Ukraine on 'Achieving cyber security and resilience posture by improved inter agency cooperation', Nataliia Tkachuk, the NCCC, stressed the need to study and implement NATO and EU standards and policies in Ukraine.
During the workshop, relevant public sector experts were introduced to the most important security and cyber resilience norms at the European and Euro-Atlantic levels. The mechanisms by which the relevant legal norms and technical solutions can be transferred to the Ukrainian context to ensure Ukraine's cyber resilience were discussed.

THE NATIONAL COORDINATION CENTRE FOR CYBERSECURITY (NCCC) REPRESENTATIVE TAKES PART IN GCMC CYBER DIPLOMACY EXERCISE

On 25th-29th September 2023, Serhii Prokopenko, Head of the NCCC) Support Department, took part in the George C. Marshall European Centre for Security Studies cyber diplomacy exercise, which was held jointly with the U.S. Department of State. The event was attended by nearly 30 participants from Europe and the United States. The exercise focused on key aspects of developing cybersecurity capabilities, the role of cyber diplomacy in international security, and national responses to cyberattack approaches.

THE SSSCIP AND THE NCCC HELD A WORKSHOP ON THE IMPLEMENTATION OF THE CYBERSECURITY STRATEGY OF UKRAINE

On 9th-10th October, the SSSCIP together with the NCCC held a workshop on the implementation of the Cybersecurity Strategy of Ukraine. In accordance with the goals and objectives of the event, the participants discussed the mechanisms, aspects, roles, and peculiarities of annual planning of the Strategy implementation actions and focused on the importance of reporting on the results of their implementation.

THE MINISTRY OF DIGITAL TRANSFORMATION OF UKRAINE TOGETHER WITH THE USAID CYBERSECURITY FOR CRITICAL INFRASTRUCTURE IN UKRAINE ACTIVITY LAUNCHED A NEW EDUCATIONAL SERIES ON CYBERSECURITY ON DIIA.EDUCATION

The Ministry of Digital Transformation of Ukraine, together with the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, and with the participation of experts from the Kyiv-Mohyla Academy, have created an educational series to help people learn cyber hygiene and protect themselves from cyber threats. The series focuses on the motives of cybercriminals, the responsibility of citizens for their gadgets, passwords, software security, the psychology of cyber fraud and viruses.

GOOGLE AND PARTNERS LAUNCH TRAINING COURSE 'CYBERSECURITY BASICS FOR ENTREPRENEURS

The training course is useful for owners, managers and employees of small and medium-sized businesses who want to protect their business from cyber threats. It consists of 5 training sessions and covers the following topics:

- recognising cyberattacks;
- creating a system to protect your business from cyber threats;
- methods for employees to comply with cyber hygiene;
- development of strategies and tactics to improve business security;
- experience of Ukrainian entrepreneurs in building an effective cybersecurity system.

APT29 TARGETED EMBASSIES ACROSS EUROPE – THE NCCC REPORT

On 14th November the NCCC published a report on the cyberespionage group APT29 activity. The APT29 under investigation operation concerns their operation against embassies across Europe, including Italy, Greece, Romania, Azerbaijan. The main grouping tool is the recently discovered vulnerability with the indicator CVE-2023-38831 concerning the WinRAR software. APT29 uses seemingly innocuous decoys that give attackers access to victims' systems.

NUMBER OF RUSSIAN CYBERATTACKS USING SMOKELOADER HAS INCREASED – THE NATIONAL COORDINATION CENTRE FOR CYBERSECURITY (NCCC) RESEARCH

On 24th October, the NCCC published its research on russian cyber activity using Smokeloader malware. According to the NCCC, since May 2023, Ukrainian financial and government organisations have been attacked by russian hackers using Smokeloader, a software whose functionality includes methods of anti-analysis, data theft, and remote control of the victim's computer. Attackers use financial topics to create campaigns to lure and deceive victims.

THE SSSCIP PREDICTS AN INCREASE IN THE NUMBER OF SOPHISTICATED ATTACKS ON SUPPLY CHAINS

On 30th October, the SSSCIP published a new analytical report on russian cyber operations. The SSSCIP specialists anticipate an increase in high-complexity supply chain attacks. Companies engaged in software development for critical infrastructure and the military are going to suffer from active targeted cyberattacks in the long run. The attackers are likely to use more complex attacks and tools, including the development and deployment of highly complex malware that is more widespread and able to attack multiple operating systems. It is also emphasised that russia is attracting an increasing number of new people for attacks in cyberspace, in particular, young people. Another important conclusion is that hackers associated with the military intelligence of the russian federation emphasize the complexity of the attacks, not the number.

THE NUMBER OF REGISTERED CYBER INCIDENTS IN THE FIRST HALF OF 2023 INCREASED MORE THAN TWICE – THE SSSCIP

On 13th October the SSSCIP updated statistical information on the dynamics of cyber incidents. The Computer Emergency Response Team of Ukraine (CERT-UA) which operates under the SSSCIP registered 762 cyber incidents (excluding SOC incidents) in the first half of 2023. That is, enemy hackers tried to attack Ukrainian information and communication systems four to five times a day on average. For comparison, during the second half of 2022 were registered 342 (not including SOC incidents) cyber incidents, one or two per day on average.

ANOTHER INSTANCE OF MALWARE DISTRIBUTION: HACKERS DISGUISE THEMSELVES AS THE SSU

The government CERT-UA has detected mass emails allegedly on behalf of the SSU. Those emails contain an attached RAR archive 'Електронна вимога СБУ України.rar' ('Electronic request from the SSU'). This activity is tracked by UAC-0050. Earlier, similar dangerous emails from the UAC-0050 group were disguised as those from the Pecherskyi Court and Ukrtelecom.

THE MAJORITY OF HOSTILE CYBERATTACKS ARE AIMED AT ACCESSING THE ELECTRONIC DOCUMENT FLOW OF UKRAINIAN GOVERNMENT AGENCIES AND TECHNOLOGICAL INFRASTRUCTURE SYSTEMS – THE SSU DATA

On 3rd October, the SSU held a practical seminar for 70 representatives of various government agencies. On the event they released the results of their own analysis of the russian hacker groups malicious behaviour. Thus, according to the SSU data, the majority of hostile cyberattacks are aimed at finding unauthorised access to the electronic document flow of Ukrainian government agencies and technological infrastructure systems. Usually, such 'entry points' for russian hackers are publicly available services, primarily e-mail.

THE SSU AND THE SSSCIP URGED ENERGY COMPANIES TO ENHANCE CYBERSECURITY MEASURES FOR WINTER

On 10th November, the Security Service of Ukraine (SSU) and the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) drew the attention of energy companies to the increased cybersecurity threats from russia in winter. Based on experience of the past years, the authorities indicate the likelihood of active attempts by russian hackers to influence the critical information infrastructure facilities operation in the energy sector and providing vital services provision by them. To prepare better for a difficult period, it is suggested to use the materials of the Mandiant company report on a destructive cyberattack directed at one of the Ukrainian regional energy companies in 2022, as well as the Computer Emergency Response Team of Ukraine (CERT-UA) under the SSSCIP recommendations.

UAC-0165 INTERVENED IN THE WORK OF 11 UKRAINIAN TELECOMMUNICATION PROVIDERS – THE CERT-UA RESEARCH

On 16th November, the CERT-UA published the results of its new research of the russian hackers' activity. The analysis is about activity of an organised cybercriminal group tracked by the identifier UAC-0165. This group interfered with information and communication systems of at least 11 service providers through the period from 11th May until 29th September 2023. This resulted in disruptions of services provided to the customers, in particular.

THE CERT-UA DETECTED AT LEAST FOUR WAVES OF CYBERATTACKS AGAINST ACCOUNTANTS IN EARLY OCTOBER

The government CERT-UA detected at least four waves of cyberattacks carried out by the UAC-0006 group using the SmokeLoader malware in the period from 2nd to 6th October 2023. The typical plot of the UAC-0006 group involves infecting accounting officers' computing devices, through which financial activities are managed, as well as stealing authentication data and creating unauthorised transactions.

THE SSU HAS BLOCKED 76 BOT FARMS WITH AN AUDIENCE OF 3 MILLION FAKE ACCOUNTS SINCE THE FULL-SCALE WAR STARTED

Illia Vitiuk, the head of the Security Service of Ukraine (SSU) Cyber Security Department, told UNITED24 Media in November, that during 2022-2023, the SSU blocked the activities of 76 bot farms that had operated on our country and developed pro-russian narratives. Also, the SSU had neutralised almost 4000 cyber-attacks during 10 months of 2023.

THE CYBERPOLICE AND THE NATIONAL POLICE INVESTIGATORS EXPOSED HACKERS WHO ATTACKED LEADING GLOBAL COMPANIES

The perpetrators have carried out attacks on the world's leading companies' servers using encryption viruses developed by them since 2018. Law enforcement officers conducted more than 30 searches and stopped the group's activities among the international police operation. It was turned out that criminals encrypted more than 1000 global enterprises servers over several years of criminal activity and caused losses in the amount of more than UAH 3 billion in terms of national currency.

THE CYBERPOLICE STOPPED THE RANSOMWARE GROUP ACTIVITY TOGETHER WITH LAW ENFORCEMENT OFFICERS OF 10 COUNTRIES

The information about the large transnational criminal group activity termination that had used ransomware to attack 168 international companies in Europe and America since 2020 was released on 20th October. Currently, it is not known about the extent of the damage caused by the group, however some members were located in Ukraine, while ransomware developer and other group members operated from France.

THE PRYKARPATTIA CYBERPOLICE EXPOSED A GROUP OF FRAUDSTERS OPERATING UNDER THE SCHEME 'A FRIEND ASKS FOR A LOAN'

The perpetrators hacked citizens' e-mails to which social media accounts were linked by selecting passwords. In this way, they gained access to the profiles and sent messages on behalf of the real owners to their friends asking them to borrow money. At the moment, 20 victims defrauded by fraudsters are identified. The total amount of damages is about UAH 150 000.

MICROSOFT WILL PROVIDE FREE CLOUD SERVICES TO UKRAINIAN GOVERNMENT AGENCIES FOR ANOTHER YEAR

On 29th November, the Ministry of Digital Transformation of Ukraine reported that the government agencies of Ukraine will be able to use Microsoft cloud products free of charge for another year: until 31st December 2024. This is a part of Microsoft's corporation support policy for Ukraine.

THE MINISTRY OF DIGITAL TRANSFORMATION OF UKRAINE LAUNCHED CYBERGRAM – A TEST ON ONLINE SAFETY RULES KNOWLEDGE

On 15th November, the Ministry of Digital Transformation with the support of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity launched Cybergram – the test on five basic user competencies:

- devices protection and secure connection to the Internet;
- personal data and privacy protection, Internet security;
- protection of customer's personal rights against fraud and abuse;
- health and well-being protection;
- environmental protection.
- The test is available for all Diia.Education platform users.

GOOGLE LAUNCHED A MEDIA CAMPAIGN ‘ONLINE SAFETY TIPS’ IN UKRAINE

Google together with the Ministry of Digital Transformation of Ukraine and with the SSSCIP support launched a media campaign ‘Online Safety Tips’ in social media. The goal is to help Ukrainians to be cyber-aware and avoid online threats. The media campaign includes four videos that talk about tools to support cyber security. These include multi-factor authentication, software, phishing, and password managers.

UKRAINE HAS NOT RESTRICTED HUAWEI EQUIPMENT IN ACCESS TO INFRASTRUCTURE PROJECTS YET

According to Yehor Dubynskyi, the Deputy Minister of Digital Transformation: Ukraine has not excluded Chinese telecoms suppliers Huawei and ZTE from providing equipment to rebuild its infrastructure damaged by russia’s attacks on its territory. The case is Ukraine has no reliable proof of possible security risks associated with the Chinese supplier.

2. THE FIRST WORLD CYBER WAR

THE INTERNATIONAL COMMITTEE OF THE RED CROSS PUBLISHED 8 RULES FOR HACKTIVISTS WAGING HYBRID WARFARE

At the beginning of October, two representatives of the International Committee of the Red Cross (ICRC) issued recommendations for hacktivists, published as an essay in the European Journal of International Law. They represent an extension of existing international norms of armed conflict into cyberspace in order to preserve norms that will protect non-combatants not only from attacks on infrastructure, but also from online incitement to violence. Certain specific classes of targets are explicitly prohibited, including medical and humanitarian objects.
Some groups of hacktivists responded with mockery. The IT Army of Ukraine informed the BBC that it was not certain whether it would follow the rules. In particular, the IT Army seems to view the rules as an absolute ban on collateral damage, which is not always avoidable. The group already avoids attacks on hospitals and similar facilities, but it has carried out DDoS attacks on civilian infrastructure such as banks and travel booking services.
Hacktivists on the other side of the war dismissed the ICRC as irrelevant. The russian network Killnet asked: 'Why should we listen to the Red Cross?'. Anonymous Sudan, which despite its name is an auxiliary group of russian hacktivists, categorically rejected the ICRC's rules, saying that the restrictions are 'unsustainable and that their violation for the sake of the group's cause is inevitable'.

AUTHORITARIAN GOVERNMENTS FOCUSED ON CYBER ESPIONAGE OPERATIONS IN 2023 – NEW MICROSOFT REPORT

On 5th October, Microsoft Corporation released its report on malicious cyber activity in 2023, assessing the actions of government actors and their priorities. The main focus is on the actions of russia, China, Iran, and North Korea. The authors of the report conclude that in 2023, all authoritarian governments have focused on cyber espionage operations seeking to gather more information about their important foreign policy initiatives. russian security services redirected their cyberattacks towards espionage in support of the war against Ukraine, while simultaneously continuing destructive cyberattacks in Ukraine and broader espionage efforts.

UKRAINE, ISRAEL, SOUTH KOREA TOP LIST OF MOST-TARGETED COUNTRIES FOR CYBERATTACKS

More than 120 countries faced cyberattacks over the last year, with Ukraine, Israel, South Korea, and Taiwan topping the list of the most targeted countries, according to a new report from Microsoft, published on 6th October.
These attacks were mainly carried out by four countries: russia, China, Iran, and North Korea. Smaller sections are dedicated to hackers based in the Palestinian Territories and mercenary hackers hired by other nations.
Microsoft's Digital Defence Report 2023 revealed changes in attack strategies, noting a shift from destruction and financial gain campaigns (such as ransomware) to campaigns that focus primarily on information theft, covertly monitor communication or information manipulation. Although russia continues to launch cyberattacks on Ukraine but it has also stepped up its espionage activity, while China continuing its unmatched espionage and data theft campaigns while expanding its arsenal to include the potential for destructive attacks.

2023 STATE OF THE THREAT: A YEAR IN REVIEW BY THE SECUREWORKS

At the beginning of October, Secureworks company released its 2023 State of the Threat report, revealing that ransomware remains the main threat faced by organisations: 'The number of attacks has returned to historical norms, then exceeded them after last year's brief slowdown following the invasion of Ukraine. The average dwell time between gaining initial access and delivery of ransomware payload has been significantly reduced to an average of just 24 hours.'
The report also examines the motives behind state-sponsored cyber operations: 'russia focuses on the war in Ukraine, North Korea — on currency theft, Iran — on opposition suppression, and China — on cyber espionage. However, regional focuses are starting to shift in some cases, especially from China, that closely monitors the impact of the war in Ukraine on other European countries.'

CYBERCRIMINALS USE THE RUSSIAN SERVICE KOPEECHKA FOR MASSIVE WORK WITH ACCOUNTS ON SOCIAL MEDIA

On 27th October, the cybersecurity company Trustwave published its research on how cybercriminals use the services of the russian platform Kopeechka to mass creation of accounts on popular social media. Such accounts are used for social engineering, advertising phishing sites, etc.

THE USA SANCTIONS A RUSSIAN ACCUSED OF LAUNDERING VIRTUAL CURRENCY FOR RANSOMWARE AFFILIATE

On 3rd November, a russian citizen Kateryna Zhdanova was sanctioned by the US Treasury Department for allegedly laundering virtual currency on behalf of the russian elites and cybercriminals, including an affiliate of Ryuk ransomware.
Kateryna Zhdanova is accused of laundering more than USD 2.3 million in 2021 for a Ryuk ransomware affiliate through the Garantex cryptocurrency exchange, which was itself designated by OFAC in 2022. According to OFAC, more than USD 100 million in transactions associated with darknet markets and criminals were conducted on the exchange before it was sanctioned.

RUSSIAN 'INFLUENCE-FOR-HIRE' FIRMS SPREAD PROPAGANDA IN LATIN AMERICA– THE U.S. DEPARTMENT OF STATE

On 8th November, the U.S. Department of State has uncovered a russia-funded disinformation campaign across Latin America aimed at undermining support for Ukraine and discrediting the USA and NATO. The campaign is conducted by three local companies: the Social Design Agency (SDA), the Institute for Internet Development, and Structura, which the Department of State describes as 'influence-for-hire' firms with deep technical capability.

russia operates a vast ecosystem of proxy websites, individuals, and organisations that appear to be independent news sources to promote its propaganda in Latin America. A scattered network of Spanish and Portuguese-speaking journalists and media outlets allow russia to integrate pro-russian content into Latin American media while concealing their russian connections. russia also interferes in elections in Africa to keep Moscow-friendly regimes in power.

SANDWORM DISRUPTS POWER IN UKRAINE USING A NOVEL ATTACK AGAINST OPERATIONAL TECHNOLOGY

On 9th November, Mandiant released the results of its study of a cyberattack by the SandWorm group on the operational technology systems (OT) on a Ukrainian energy organisation at the end of 2022. Mandiant Threat Intelligence found out that this incident was a multi-event cyberattack that leveraged a novel technique for impacting industrial control systems (ICS) / operational technology (OT). The actor first used OT-level living off the land (LotL) techniques to likely trip the victim's substation circuit breakers, causing an unplanned power outage that coincided with mass missile strikes on critical infrastructure across Ukraine.

'This attack represents the latest evolution in russia's cyber physical attack capability, which has been increasingly visible since russia's invasion of Ukraine. The techniques leveraged during the incident suggest a growing maturity of russia's offensive OT arsenal, including an ability to recognise novel OT threat vectors, develop new capabilities, and leverage different types of OT infrastructure to execute attacks', - as stated in the report.

A COORDINATED CYBERATTACK WAS CARRIED OUT AGAINST DENMARK'S ENERGY ORGANISATIONS WITH RUSSIAN INVOLVEMENT

On 14th November, the information about a large coordinated attack on energy facilities in Denmark that took place in May this year was spread. During the attack, hackers managed to compromise 22 energy organisations. As part of the attacks, hackers used multiple vulnerabilities in Zyxel firewalls for initial access, code execution and gaining full control over the affected systems. The first wave of attacks occurred on 11th May, the second wave on 22nd May, and the third wave on 24th May. At least in one of the attacks, there was observed activity associated with Sandworm (APT28).

NETFLIX IMPACTED BY ANONYMOUS SUDAN DDOS ATTACK

DDoS attacks remain a typical technique of russian hacktivists. Recently, Anonymous Sudan, a KillNet affiliate, created obstacles for Netflix in several countries, nominally to block LGBTQ content, but likely just to draw attention. Richard Wallace, the Cyber Security Threat Intelligence Analyst at Vercara, explained: 'In addition to the Netflix attack, Anonymous Sudan also took responsibility for the Hulu attacks on the same day' (29th September, 2013).
Earlier this year, Anonymous Sudan threatened to attack US-based organisations in response to ongoing military and financial support for Ukraine. This is not the first time Vercara has observed Killnet attack sites it deems immoral: in the past they have attacked OnlyFans, as well as dark web sites selling drugs. Anonymous Sudan uses any pretext to legitimise its DDoS attacks against Western and European countries in order to get free publicity, continue recruiting and get funding for further activities.

UKRAINE INVESTIGATES WAR CRIMES IN CYBERSPACE

On 18th November, Andrii Kostin, the Prosecutor General of Ukraine, told Politico, that the Ukrainian government has collected evidence of around 109,000 alleged russian war crimes. Among them, four investigations have been launched into cyberwarfare crime charges. Kostin said the inclusion of cybercrimes and crimes against the environment for the International Criminal Court (ICC) evidence is a new initiative by Ukraine during this war, stressing that 'every crime has victims'.

RUSSIAN HACKERS CLAIM ATTACK ON UKRAINE FIGHTER JET SUPPLIER

On 19th November, the Telegraph reported that the well-known LockBit ransomware group, which operates with russia's approval and is actually a russian private company, claims to have hacked the networks of Sabena Engineering Belgian company, which is engaged in the supply of F-16 to Ukraine. The Telegraph reports that LockBit has threatened to publish the confidential data on 26th November, unless it is paid. Sabena says, it continues to investigate the incident and remains confident this incident poses no threat to flight safety.

NONAME057(16) GETS BUSY RECRUITING ONLINE HACKTIVIST ARMY

On 30th November, Australian Cyber Security Magazine reported that the pro-russian hacktivist group NoName057(16) is actively recruiting an online army to ramp up its cyberattacks on the websites of private entities and government agencies in countries it believes display a bias against russia.
Calling prospective online recruits 'patriots and fighters for justice', NoName057(16) says just like bona fide armies, members will have ranks and merit awards depending on their time of service and achievements. On 25th November, the group said recruits would be paid in an electronic currency called dCoin 'according to their contribution to the attacks', adding that the higher the volunteer's rank and the more cyberattacks the recruit made, the more they would be paid.

MUSTANG PANDA HACKERS TARGET PHILIPPINES GOVERNMENT AMID SOUTH CHINA SEA TENSIONS

The China-linked Mustang Panda actor has been linked to a cyberattack targeting a Philippines government entity amid rising tensions between the two countries over the disputed South China Sea. Palo Alto Networks Unit 42 attributed the adversarial collective to three campaigns in August 2023, primarily singling out organisations in the South Pacific. 'The campaigns leveraged legitimate software including Solid PDF Creator and SmadavProtect (an Indonesian-based antivirus solution) to sideload malicious files', the company said.