НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

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

May 2023

USAID
FROM THE AMERICAN PEOPLE

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 4

KEY TENDENCIES 5

1. FIRST WORLD CYBER WAR 8

Curtailing russia's ability to support war ambitions in Ukraine should be a task of the Transatlantic Partnership, according to a paper from the Belfer Center 8

Cyber Lessons from Ukraine: Prepare for a Prolonged Conflict,Not a Knockout Blow 8

French City Hall Websites Hit by pro-russian Cyber Attacks 8

Website of French Senate Attacked by russian Hackers 9

russia Attacks Civilian Infrastructure in Cyberspace just as it does on the Ground – CERT-UA 9

For Money and Attention: Killnet Apparently Reorganizes Again 9

CERT-UA Warns of SmokeLoader and RoarBAT Malware Attacks Against Ukraine 9

Kremlin-Linked «Snake» Espionage Malware Eliminated, Justice Department Says 10

Microsoft Releases a Fix for Patched Outlook Issue Exploited by russian Hackers 10

Evolving Cyber Operations and Capabilities – CSIS Report 10

CERT-UA Identifies Possible russian Cyber Espionage Campaign 11

Ireland Considers Cyber Assistance to Ukraine as a Contribution to Collective Security 11

2. CYBERSECURITY SITUATION IN UKRAINE 12

Ukraine became a member of NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) 12

NCSCC deepens cooperation with Recorded Future, a leading cyber security company 12

Cyber security for healthcare and personal data protection discussed at a meeting of the National Cyber Security Cluster 13

The Ukrainian delegation, as a member of the CCDCOE, took part in the Center's Steering Committee for the first time 13

The Ministry of Digital Transformation meets with G7 digitization ministers 14

Meeting on further interaction of key cyber security agencies with the CCDCOE held in the NSDC apparatus of Ukraine 14

New stage of #FraudGoodbye information campaign starts, cyber police remind of important payment security rules 15

Romanian technical cyber security delegation visits State Special Communications Service 15

Nataliya Tkachuk Participates in Black Sea Regional Forum of the George C. Marshall European Center for Security Studies Programs' Graduates 15

NSDC specialists take part in conference on communication and Internet resilience during the war 16

Ministry of Digital Transformation and Palantir sign a memorandum on cooperation in the spheres of defense and reconstruction of Ukraine after the russian invasion 16

Ukraine improving quality of professional training in cyber security and information protection 17

Strengthening cyber defense: government adopts mechanism for holding a Bug Bounty 17

To reduce fraud risks, payment service providers will use enhanced authentication 18

Strengthening the cyber resilience of the financial system: the NCSCC starts Vulnerability Management training for specialists in the banking sector 18

NCSCC holds 2-day training on cyber security and cyber intelligence for security and defense sector specialists 18

With NCSCC assistanceNCSCC, training for Ukrainian cyber security specialists was held at the NATO CCDCOE 19

SSSCIP holds write-up competition based on online cyber security competition 19

Number of cyber attacks on commercial sector increased since start of year – statistics 19

Attackers use legitimate software for destructive attacks on Ukrainian state agencies – analysis 20

SSSCIP conducts second training on cyber protection for category «A» civil servants 20

SBU liquidated powerful proxy center in Poltava used by the russian Federation to conduct special information operations on the Internet 21

Cyber police officers expose Chernivtsi resident in the development and sale of malicious software 21

SBU liquidates network of botnets with an audience of almost 200,000 users working to destabilize Ukraine 21

The National Police and U.S. FBI eliminate service network exchanging criminally obtained cryptocurrency 22

SBU detains two private detectives in Kyiv who sold confidential information from government databases 22

National Police eliminate large-scale fraud scheme: participants embezzled money from the accounts of more than 10,000 citizens 23

Lviv, law enforcement expose criminal organization whose members used phishing to embezzle about 6 million UAH 23

Attackers launched another campaign of attacks using emails with the subject «bills» – analysis 24

ACRONYMS

AFU	Armed Forces of Ukraine
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT-UA	Government Computer Emergency Response Team Ukraine
CISA	Cybersecurity & Infrastructure Security Agency
CMU	Cabinet of Ministers of Ukraine
CRDF Global	Civil Research and Development Fund (U.S.)
CSEU	
CSIS	Center for Strategic and International Studies (U.S.)
CTF	Capture the Flag
DDoS	Distributed Denial-of-Service
DNSC	National Cyber Security Directorate (Romania)
EU	European Union
FBI	Federal Bureau of Investigation
FSB	Federal Security Service (russian Federation)
GPO	Group Policy
GRU	Main Directorate of the General Staff of the Armed Forces of the russian Federation
ICS	Industrial Control System
IP	Internet Protocol
NATO	North Atlantic Treaty Organization
NBU	National Bank of Ukraine
NCSCC	National Coordination Cybersecurity Center
NHS	National Health Service of Ukraine
NSDC	National Security and Defense Council of Ukraine
OKI	
OS	Operating System
OT	Operational Technology
RaaS	Ransomware as a Service
SBU	Security Service of Ukraine
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
TTPs	Tactics, Techniques, and Procedures
UCM	Consultative Mission of the European Union in Ukraine
UN	United Nations
UNICEF	United Nations Children's Fund
VDP	Vulnerability Management
VPN	Virtual Private Network

KEY TENDENCIES

Ukraine is now a full member of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), another step on Ukraine's path to NATO membership. As a full member of the CCDCOE, Ukraine took part in the May 2023 meeting of the Center's Steering Committee. A meeting was also held to discuss practical cooperation that paid special attention to Ukraine's participation in the Center's annual cyber training, Locked Shields. There are plan to use Ukraine's experience in cyber warfare to develop a scenario for Locked Shields-2024. CCDCOE also conducted training for Ukrainian specialists on cyber security for critical information infrastructure. Ukraine's CCDCOE membership came per the initiative of the National Coordination Cybersecurity Center (NCSCC) at the National Security and Defense Council (NSDC).

The European Union (EU) continues to strengthen its policy limiting foreign (non-European) presence in its market. The EU also continues to place increasingly strict requirements on other market players as it seeks to limit the influence of Chinese companies on its 5G networks rollout; for example, Portugal plans to expand international ties with South Korea. New requirements for foreign operators of cloud services are being formed, research spending on cyber security is increasing, and the EU is preparing to launch the European Cyber Shield program.

In Ukraine this month, much attention was paid to the issue of cyber security in the financial sector. The NCSCC started Vulnerability Management training for Ukrainian banking sector specialists. To harmonize Ukrainian legislation with EU legislation regarding payment services and to strengthen its implementation, the National Bank of Ukraine (NBU) established a requirement for payment service providers to apply enhanced authentication of users to reduce fraud risks. The National Police disrupted an extensive criminal network, conducting investigations in 20 regions of the country with more than 500 officers participating. As a result, 56 criminals who sent phishing links to obtain citizen bank card data were exposed. The National Police and the U.S. FBI eliminated a network of services for exchanging criminally obtained cryptocurrency.

The U.S. formed new security priorities regarding the security of critical infrastructure and implemented a policy of zero trust for federal agencies. This includes the Pentagon, which is reforming the security of internal networks, exploring new cyber security solutions, and conducting joint operations of space and cyber security forces. Along with zero trust, the Pentagon is reviewing its own IT development strategy and possible dependence on a small number of suppliers.

Cyber security agencies of the Five Eyes alliance continue to demonstrate a high level of cooperation and coordinated efforts. In May, the alliance published materials on enemy cyber activity, sent joint cyber security teams to European countries (in particular, Latvia), and increased the effectiveness of joint operations.

Malicious hackers continue to regroup and find new tools and tactics. Although the number of ransomware incidents decreased in 2022 and ransomware groups suffered setbacks last year, these groups still pose a threat. New groups are popping up and Ransomware as a Service (RaaS) is getting more and more popular. State-sponsored hackers are increasingly targeting small and medium-sized businesses to leverage for larger attacks. Meanwhile, insurance companies' attempts to avoid paying insurance premiums to victims of cyberattacks, citing policy exclusions for acts of war, have so far been unsuccessful. Merck & Co.'s victory in a legal dispute with insurers over coverage for $1.4 billion in losses from malware is expected to force insurance policies to more clearly confront responsibility for the fallout from nation-state cyberattacks.

There is an increasing focus of hackers on Industrial Control System (ICS) / Operational Technology (OT) systems, with new vulnerabilities appearing and such targets gaining more attention on hacker forums. Increasingly dangerous vulnerabilities have been found in the products of well-known manufacturers of industrial equipment (Rockwell Automation, Siemens, Teltonika, Lacroix) and new viruses targeting ICS (May's Cosmic Energy) appear every month.

While ransomware threats are frequently reported in the media, the larger financial threats from cyberattacks mostly come from business email compromises, accounting for more than 50 percent of all malicious activity. U.S. intelligence and government agencies continue to analyze high-profile cases of devastating attacks such as Colonial Pipeline and Solar Winds and to suggest ways to strengthen cyber security, especially in light of the potential escalation of the U.S.-China standoff, which the U.S. intelligence community predicts will almost certainly lead to attacks on the OKI of the U.S. from Beijing.

The first world cyber war continues: russiarussian crime syndicates are reshaping themselves to ensure greater efficiency. Ukrainian cyber security structures constantly discover and warn of new cyber threats from russia, and successful operations of russian hackers abroad continue (for example, cyber attacks on the websites of some French government institutions). Meanwhile, detection of russian cyber-espionage is becoming more effective: in May, it was established that a long-standing spy company had been using Snake WPS for years to gather intelligence from government agencies in many countries.

Analysts continue to draw conclusions from the cyber component of the russia-Ukraine war. Among the main assessments:

- Many countries underestimate their need for cyber defenses
- Effectively built defenses are truly capable of stopping or deterring enemy cyber activity
- Cyber components of conflicts will not be fleeting; there will be long positional battles among the conflict participants

The goals and objectives of the Transatlantic Partnership include deterring russia's ability to achieve its goals in Ukraine.

1. FIRST WORLD CYBER WAR

CURTAILING RUSSIA'S ABILITY TO SUPPORT WAR AMBITIONS IN UKRAINE SHOULD BE A TASK OF THE TRANSATLANTIC PARTNERSHIP, ACCORDING TO A PAPER FROM THE BELFER CENTER

The Harvard Kennedy School's Belfer Center for Science and International Affairs published the paper «Addressing russian and Chinese Cyber Threats» in May 2023. The paper comprehensively addresses cyber threats to the transatlantic partnership and focuses on two significant challenges faced by democracies: curtailing russia's ability to support war ambitions in Ukraine and defending the transatlantic partners against Chinese cyber warfare threats.

One recommendation to the EU and U.S. is to facilitate creating an international body that institutionalizes big tech cyber support for Ukraine with help of the U.S. Department of State's Bureau of Cyberspace and Digital Policy. Another is that the Ukrainian government should focus immediate action on better coordinating hacktivist groups and emphasize the rejection of counter-attacks.

CYBER LESSONS FROM UKRAINE: PREPARE FOR A PROLONGED CONFLICT, NOT A KNOCKOUT BLOW

The Breaking Defense article, authored by Sydney Freedberg Jr., states that the widespread fear of a «cyber Pearl Harbor» or «cyber 9/11» (i.e., a decisive, paralyzing, lightning-fast cyber attack) has so far proved unfounded.

«The strategic lesson for the U.S., several independent experts said, is that this kind of drawn-out cyber conflict is a more likely model for future wars than the sudden-death visions of a 'cyber Pearl Harbor' or 'cyber 9/11' predicted by U.S. officials for over a decade». Although cyber operations have been and will likely continue to be an important component of future wars, they are unlikely to be decisive in winning wars, nor will they bring significant advantages at the operational level.

FRENCH CITY HALL WEBSITES HIT BY PRO-RUSSIAN CYBER ATTACKS

On May 4, European Pravda, with reference to Le Figaro, reported that, on the previous day, many French city government websites had come under cyberattacks and pro-russian messages had replaced the websites' content. At least 30 cities across the country were affected. Among the attacked websites was that of the town Bry-sur-Marne (department of Val-de-Marne), on which a blank page appeared to users with the following message: «Respect russia! Otherwise, we will continue to fight with you». At the time of publication, it was not known who was behind the attack.

WEBSITE OF FRENCH SENATE ATTACKED BY RUSSIAN HACKERS

On May 5, Ukrinform, with reference to The Guardian, reported that russian hackers had disabled the website of the French Senate. The NoName group claimed responsibility for the attack, saying on Telegram that the reason for the attack was that «France is working with Ukraine on a new aid package that may include weapons».

RUSSIA ATTACKS CIVILIAN INFRASTRUCTURE IN CYBERSPACE JUST AS IT DOES ON THE GROUND – CERT-UA

According to Volodymyr Kondrashov, spokesman for the State Service of Special Communications and Information Protection, the Government Computer Emergency Response Team (CERT-UA) monitors the activities of more than 80 hacker groups, most of which are from the russian Federation, and 90 percent of their members are russian military operatives. He emphasized that the russian government uses the same tactics in cyberspace as it does on the conventional battlefield: it attacks civilian infrastructure.

FOR MONEY AND ATTENTION: KILLNET APPARENTLY REORGANIZES AGAIN

According to the report published by Flashpoint on May 4, KillNet continues to evolve. «Flashpoint has pointed out several times that, for all of its nationalistic antics, Killnet has remained a primarily financially-motivated group that has used the media exposure provided by an eager russian pro-Kremlin media ecosystem to promote its DDoS-for-hire services. Killnet has partnered with several botnet providers and the Deanon Club, a partner threat group, to target narcotics-focused darknet markets».

There is no indication that Killnet has acquired more sophisticated tactics, techniques, and procedures (TTPs). Its reliance on simple tools became an object of ridicule among other cyber underground players. «Killnet remains widely ridiculed on top-tier russian-speaking forums», Flashpoint writes.

CERT-UA WARNS OF SMOKELOADER AND ROARBAT MALWARE ATTACKS AGAINST UKRAINE

As reported by The Hacker News on May 8, there is an ongoing phishing campaign with invoice-themed lures targeting Ukraine, according to CERT-UA. The campaign is an attempt to distribute the SmokeLoader malware in the form of a polyglot file.

The emails are sent using compromised accounts and come with a ZIP archive that, in reality, is a polyglot file containing a decoy document and a JavaScript file.

The JavaScript code is then used to launch an executable that paves for the execution of the SmokeLoader malware. SmokeLoader, first detected in 2011, is a loader whose main objective is to download or load a stealthier or more effective malware onto infected systems.

CERT-UA attributed the activity to a threat actor it calls UAC-0006 and characterized it as a financially motivated operation carried out with the goal of stealing credentials and making unauthorized fund transfers.

KREMLIN-LINKED «SNAKE» ESPIONAGE MALWARE ELIMINATED, JUSTICE DEPARTMENT SAYS

On May 9, U.S. and international authorities announced that they had successfully dismantled a malware implant, dubbed «Snake», used for two decades by Turla, a notorious hacking group affiliated with the russian Federal Security Service (FSB).

«We assess this to be their premier espionage tool», a senior FBI official told reporters, noting it had been deployed against NATO countries and others with the goal of pilfering sensitive U.S. information.

According to John Hultquist, the Head of Mandiant Intelligence Analysis at Google Cloud, the disruption in Turla's activities will be temporary. He stressed that there is a war on and there is never a better time to disrupt the enemy's intelligence apparatus then when they are trying to make better decisions to «get off the back foot».

MICROSOFT RELEASES A FIX FOR PATCHED OUTLOOK ISSUE EXPLOITED BY RUSSIAN HACKERS

On May 10, Microsoft released a new fix for a vulnerability in Outlook that was initially patched in March but was later discovered to be flawed. The vulnerability could have been exploited by russian hackers to carry out targeted attacks against organizations in government, transportation, energy, and military sectors in Europe.

Ukrainian cyber security officials at CERT-UA reported the vulnerability to the Microsoft incident response team, but later Akamai researchers discovered a way around the patch that would allow an attacker to use the vulnerability to coerce an Outlook client to connect to an attacker-controlled server. The issue is a zero-click vulnerability.

EVOLVING CYBER OPERATIONS AND CAPABILITIES – CSIS REPORT

On May 18, experts of the Center for Strategic and International Studies (CSIS) published a report on how Ukraine counters russian cyber threats. The report focuses on the factors that have helped Ukraine effectively counteract russian cyber efforts and highlights several lessons the Western world should draw from this confrontation.

One of the key findings is that Ukraine has successfully applied the concept of cyber resilience. In addition, it is crucial to build strong relationships with allies and partners to share intelligence, technology and tactics. Mobilizing private sector and civil society resources and support may also result in unique advantages.

However, experts caution against relying solely on Ukraine's experience, as there is no guarantee that enemy hackers in other conflicts will be as incompetent and unprepared as in this cyber war. At the same time, the Ukrainian case provoked a wider discussion about the applicability of international law in relation to cyber conflicts.

CERT-UA IDENTIFIES POSSIBLE RUSSIAN CYBER ESPIONAGE CAMPAIGN

On May 22, CERT-UA reported that russian cyber spies had probably managed to compromise the accounts of the Embassy of Tajikistan. The attackers, known as UAC-0063 in Ukraine, used these accounts in a phishing campaign designed to install keyloggers (LOGPIE), backdoors (CHERRYSPY), and file stealers (STILLARCH or DownEx) onto target devices.

«It was established that on April 18, 2023 and April 20, 2023, emails were sent to the agency's email address, probably from the official email account of the Embassy of Tajikistan in Ukraine (probably as a result of hacking of the account): the first letter contained an attachment in the form of a document with a macro, and the second letter – a link to the same document», CERT-UA says. According to CERT-UA, the campaign affected not only targets in Ukraine, but also organizations in Mongolia, Kazakhstan, Kyrgyzstan, Israel and India. Bank Info Security writes that this campaign is similar to the operations conducted by Fancy Bear associated with the russian Main Intelligence Directorate (GRU).

IRELAND CONSIDERS CYBER ASSISTANCE TO UKRAINE AS A CONTRIBUTION TO COLLECTIVE SECURITY

On May 23, the Irish Times reported that cyber security assistance is provided in «significant volumes» by Ireland to Ukraine during the war with russia. Dublin views this aid as a contribution to collective security.

2. CYBERSECURITY SITUATION IN UKRAINE

UKRAINE BECAME A MEMBER OF NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (CCDCOE)

On May 16, 2023, Ukraine became a full member of NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). An official ceremony to raise the Ukrainian flag as a new CCDCOE member took place at the center in Tallinn, Estonia, to mark the occasion.

Ukraine's accession to the CCDCOE was initiated by the National Coordination Center for Cyber Security (NCSCC) of the National Security and Defense Council of Ukraine (NSDC).

«It is a historic day for our country», said Oleksiy Danilov, Secretary of the NSDC, «and certainly an important step on Ukraine's way towards NATO. CCDCOE membership will allow us to interact more effectively in the international arena in the sphere of cyber security and cyber defense, as well as exchange experience with the Center's member states. After all, today Ukraine is at the forefront of the global cyber war waged against us, European countries and other democratic states by the russian Federation. And we must mobilize all the necessary resources, join forces and means in order to repulse the enemy together once and for all».

Membership in the CCDCOE will enable rapid exchange of information on the detection and countering modern cyber threats. It will also allow Ukraine to practice skills for joint response to cyber attacks, to conduct joint defense and deterrence operations in cyberspace, and to take part in forming strategic approaches and developing new policies on cyber security and cyber defense at the international level. Ukraine will have access to advanced technologies and cutting edge research conducted by CCDCOE.

NCSCC DEEPENS COOPERATION WITH RECORDED FUTURE, A LEADING CYBER SECURITY COMPANY

Christopher Alberg , CEO and co-founder of Recorded Future, met with Serhiy Demediuk, NSDC Deputy Secretary, Nataliya Tkachuk, head of the NSDC Information Security and Cyber Security Service, and Serhiy Prokopenko, head of the NCSCC Department for Ensuring ActivitiesNCSCC. They discussed ways to deepen practical cooperation between the NCSCC and the company. «Today, cyber attacks are a full-fledged component of russia's war against Ukraine», said Serhiy Demediuk. «To win the cyber war, we use all available resources: we constantly interact with leading companies and governments of democratic countries of the world, strengthen information exchange, conduct training, and oppose the aggression of the russian Federation together. After all, only thanks to joint efforts, we can speed up the victory of Ukraine and defeat the common enemy. And we are grateful to the Recorded Future company for their help and highly appreciate their support».

CYBER SECURITY FOR HEALTHCARE AND PERSONAL DATA PROTECTION DISCUSSED AT A MEETING OF THE NATIONAL CYBER SECURITY CLUSTER

Participants of the 19th National Cybersecurity Cluster discussed cyber security in healthcare and medicine. They discussed protecting medical data and countering cyberattacks in the healthcare sector's information systems.

Opening the meeting, Serhii Prokopenko, head of the NCSCC specialized service of the NSDC, noted that hostile attacks by the russian Federation have two goals: to destroy infrastructure and to access personal data of citizens.

«The protection of personal and medical data is very important, especially when our country is at war. russian hackers constantly try to steal the data of Ukrainians for cyber attacks and information campaigns. Therefore, we must pay special attention to cyber security issues at the strategic, organizational and technical levels. After all, anyone in the public and private sectors can become an element of a supply chain attack», said Prokopenko.

More than 200 representatives from 80 organizations participated in the online event. The key speakers of the event represented the Ministry of Health of Ukraine, the National Health Service of Ukraine (NHS), eHealth, Cybersecurity & Infrastructure Security Agency (CISA), and other organizations responsible for digitalization and cyber security of the industry.

THE UKRAINIAN DELEGATION, AS A MEMBER OF THE CCDCOE, TOOK PART IN THE CENTER'S STEERING COMMITTEE FOR THE FIRST TIME

The Ukrainian delegation took part in the meeting of the Steering Committee of the NATO CCDCOE on May 29, 2023 in Tallinn, Estonia. The head of the Ukrainian delegation, NSDC Deputy Secretary Serhii Demedyuk, noted that the raising of the flag of Ukraine at the CCDCOE was an important step for the country on the way to joining NATO.

«Ukraine, which has been forced to defend its independence and fight against a terrorist country on all fronts for more than eight years, has shown a high level of resilience in cyberspace as well. However, russian hackers are a threat not only to our country, but also to the whole world. To make sure international security and fundamental values of the entire democratic world are protected we must unite and together oppose the common enemy», said Demediuk.

The NSDC Deputy Secretary also thanked the Steering Committee members for their support of Ukraine, noting that the CCDCOE demonstrated unity about the country's accession to the Center.

THE MINISTRY OF DIGITAL TRANSFORMATION MEETS WITH G7 DIGITIZATION MINISTERS

The G7 Digital and Tech Ministers' Meeting 2023 was held on April 29-30. The Ukrainian delegation was represented by Valeriya Ionan, Deputy Digital Transformation Minister in charge of European Integration. The meeting took place in preparation for the summit of the G7 countries.

During the meeting, key attention was paid to the principles of governing new technologies. The participants discussed the digitalization of society, cross-border data transfer, the use of artificial intelligence, the provision of sustainable digital infrastructure and challenges in cyber security.

«G7 meetings shape the global agenda», said Valeriya Ionan. «It is a great honor for Ukraine to take part in a conference of this level and to be able to share the experience of building a digital state and resilience. We are grateful to the G7 countries for their unanimous support of Ukraine and their willingness for strategic cooperation».

At the end of the meeting, the G7 ministers issued a joint declaration that defined the directions of cooperation in the digital innovation development. Governments have agreed that technology infrastructure plays a key role in addressing global challenges such as climate change, the effects of the Covid-19 pandemic and the war against Ukraine. The G7 also prioritized overcoming the digital divide and building telecommunications infrastructure.

MEETING ON FURTHER INTERACTION OF KEY CYBER SECURITY AGENCIES WITH THE CCDCOE HELD IN THE NSDC APPARATUS OF UKRAINE

On May 23, at the NSDC Apparatus of Ukraine, the NCSCC met with the NATO CCDCOE regarding the interaction of representatives of the key Ukrainian agencies in charge of cyber security. The meeting was chaired by NSDC Deputy Secretary Serhiy Demedyuk. Participants discussed the mechanism for Ukrainian specialists to cooperate with and participate in CCDCOE events.

The head of the NSDC Information and Cyber Security Service, NCSCC Secretary Nataliya Tkachuk, noted that Ukraine can now improve its cooperation in the international arena in cyber security and cyber defense.

«CCDCOE membership will also contribute to strengthening the capabilities of the Ukrainian national cyber security system. Currently, on the basis of the NCSCC, we implement an effective cooperation mechanism with our representative in the CCDCOE for the prompt exchange of information about ways to detect and counteract modern cyber threats and practice the skills of joint response to cyber attacks in the interests of all Ukrainian cyber security agencies, as well as ensure Ukraine's active participation of in the formation of strategic approaches and policies on key issues of cyber security and cyber defense at the international level», said Tkachuk.

The meeting also addressed the participation of key cyber security actors in events organized by the CCDCOE. Particular attention was paid to Ukraine's participation in the Center's annual cyber training, Locked Shields. This year, Ukraine, the U.S., and Estonia, took second place in these competitions. Next year, it is planned to use Ukraine's cyber warfare experience to develop a scenario for Locked Shields-2024.

NEW STAGE OF #FRAUDGOODBYE INFORMATION CAMPAIGN STARTS, CYBER POLICE REMIND OF IMPORTANT PAYMENT SECURITY RULES

The All-Ukrainian information campaign on payment security #FraudGoodbye (#ШахрайГудбай) is designed to improve citizens' awareness and remind them of the basic security rules of cashless payments. For the launch of the new stage of the campaign, a round table was held involving general partners, in particular, the Cyber Police Department.

«Since the beginning of this year, the Cyber Police Department has already received more than 20,000 citizen complaints, more than 75 percent of which are related to fraud on the Internet», said the head of the Cyber Police Department, Yuriy Vykhodets. «We observed similar percentages last year, so countering online fraud remains one of the main areas for the cyber police».

He noted that thanks to the joint initiative of the NSDC NCSCC, the National Center for Operational and Technical Management of Telecommunications Networks, the NBU, and the Cyber Police, a mechanism for filtering and blocking phishing domains was established. Since the beginning of this year, more than 16,000 domain names used by fraudsters to create phishing links have been blocked, and because of this, the number of phishing crimes has decreased by almost 30 percent.

The information campaign will continue until the end of the year in all regions of Ukraine. The NBU together, with its partners, will inform citizens about how to protect themselves from payment fraud.

ROMANIAN TECHNICAL CYBER SECURITY DELEGATION VISITS STATE SPECIAL COMMUNICATIONS SERVICE

The Romanian technical cyber security delegation, headed by the head of the National Cyber Security Directorate of Romania, State Secretary Dan Kimpean, visited the State Service of Special Communication and Information Protection of Ukraine (SSSCIP).

During the meeting with SSSCIP head Yuriy Shchygol and deputy heads of State Special Forces Viktor Zhora and Oleksandr Potii, the Romanian representatives discussed expanding cooperation between the DNSC and the SSSCIP, including cooperation issues related to cyber threats and cyber attacks in the course of the russian-Ukrainian war.

Special attention was paid to the exchange of experience regarding critical infrastructure protection and harmonization of the regulatory framework with EU norms, establishment of cooperation with NATO and EU bodies and guidelines for coordination and interaction with EU bodies. In addition, the Romanian delegation visited the UA30 Cyber Center and spoke with CERT-UA representatives.

NATALIYA TKACHUK PARTICIPATES IN BLACK SEA REGIONAL FORUM OF THE GEORGE C. MARSHALL EUROPEAN CENTER FOR SECURITY STUDIES PROGRAMS' GRADUATES

Natalia Tkachuk, Head of NSDC CISA, took part in the Black Sea Regional Forum of the George C. Marshall European Center for Security Studies Programs' Graduates. Participants discussed identifying and neutralizing obstacles to Ukraine and Moldova's EU accession and countering the russian Federation's hybrid influencerussia.

The Ukrainian side shared its successful experience in countering the russian Federation's informational and cyber aggression russiaduring martial law and building national resilience. During her speech, Natalya Tkachuk emphasized that Ukraine is currently the only country in the world that was able to gain an advantage in resisting cyber attacks and russian information aggression.

«Ukraine's experience is invaluable for European countries. The critical thinking of the Ukrainian people is already at such a high level that we have national immunity from russian propaganda. Thanks to Ukraine, the entire democratic world finally realized that russia was and remains a terrorist country all this time», said Tkachuk.

NSDC SPECIALISTS TAKE PART IN CONFERENCE ON COMMUNICATION AND INTERNET RESILIENCE DURING THE WAR

On May 26, Volodymyr Zverev, CISA Deputy Head and head of NSDC SSSCIP, took part in the conference «Ukraine: communication and Internet resilience during war».

The participants discussed ensuring communication during the war, interaction between interested parties, and the need to restore telecommunications infrastructure.

«Thanks to the effective interaction and timely decision-making of the National Security Council of Ukraine and the NCSCC, our country not only survived, but also gained an advantage in information and cyberspace. The state, critical infrastructure and business acted as a united front, and this became the key and decisive factor in our struggle», said Volodymyr Zverev.

MINISTRY OF DIGITAL TRANSFORMATION AND PALANTIR SIGN A MEMORANDUM ON COOPERATION IN THE SPHERES OF DEFENSE AND RECONSTRUCTION OF UKRAINE AFTER THE RUSSIAN INVASION.

The collaboration involves the use of Palantir technologies, in particular in the assessment of damage to buildings and infrastructure, and the use of software to optimize reconstruction.

«It is a great honor for us to continue developing a partnership with such a top company», said Mykhailo Fedorov, Deputy Prime Minister for Innovation, Development of Education, Science and Technology - Minister of Digital Transformation of Ukraine. «Palantir contributes to Ukraine's victory by providing technological tools and analytics. We are looking forward to the beginning of a new stage of cooperation on Ukraine's recovery. Since the start of the full-scale invasion, cooperation with Palantir has also been of great importance for the economy and building a new image of Ukraine abroad - bold and digital».

Palantir is a world leader in software development and cloud solutions provider. Its products are used by the U.S. Department of Defense and major investment banks.

The company will expand its partnership with Ukraine to achieve common goals:

- Strengthening of digital capabilities for the provision of electronic government services, defense and reconstruction of Ukraine;
- Supporting and coordinating Ukraine's reconstruction based on digital technologies;
- Undertaking joint efforts in digitization, digital innovations and Ukraine's integration into the international market;
- Exchanging data and experience in the implementation of world-leading technologies with the support of the Armed Forces of Ukraine (AFU).

UKRAINE IMPROVING QUALITY OF PROFESSIONAL TRAINING IN CYBER SECURITY AND INFORMATION PROTECTION

The SSSCIP and the National Agency for Quality Assurance of Higher Education signed a Memorandum of Cooperation on May 5.

To conduct an unbiased and reliable inspection of the quality of training of relevant specialists in educational institutions, SSSCIP representatives will be involved as experts of the National Agency for Quality Assurance of Higher Education. Recently, a number of universities have begun to launch educational programs with the prefix «cyber security» and nonexistent professional qualifications in diplomas. Such prefixes attract applicants but often make it impossible to train professionals needed in the real sector and who have the right to occupy relevant positions according to Ukrainian classification of professions. This was especially relevant to those wishing to join the civil service, special cyber defense units, banks, etc.

The situation is being corrected. A new national framework of professional qualifications for cyber security and information protection has been formed. Professions have been harmonized with international standards. Six of the most relevant professional standards have already been developed, covering 14 positions of different levels in cyber security and information protection.

STRENGTHENING CYBER DEFENSE: GOVERNMENT ADOPTS MECHANISM FOR HOLDING A BUG BOUNTY

The Cabinet of Ministers of Ukraine (CMU) adopted a resolution developed by the SSSCIP introducing the procedure for searching for and identifying potential vulnerabilities in electronic systems. This will make it possible to launch a full-fledged national Bug Bounty program to test information systems for vulnerabilities, identify risks in time and improve the systems' security.

The Bug Bounty procedure is widely used around the world. In Ukraine, however, conducting a Bug Bounty for government systems was unacceptable. Modern tools for verification and protection are currently being implemented.

The launch Bug Bounty programs will make it possible to:

- Increase the level of cyber protection of information systems;
- Prevent unauthorized access to information systems;
- Increase the cyber resilience of information systems to incidents.

TO REDUCE FRAUD RISKS, PAYMENT SERVICE PROVIDERS WILL USE ENHANCED AUTHENTICATION

To reduce fraud risks, the NBU established a requirement for payment service providers to apply enhanced user authentication. This decision implements the Law «On Payment Services» and harmonizes Ukrainian legislation regarding payment services with EU legislation. Payment service providers are required to apply enhanced user authentication when:

- They obtain remote access to accounts;
- Initiate a remote payment transaction;
- Any other actions in case of suspected fraud or other illegal actions (or the existence of such a risk).

Based on the results of the user's enhanced authentication procedure, the payment service provider must create a unique authentication code that allows linking a transaction for a certain amount and a specific recipient. This code must be accepted by the payment service provider each time the user accesses the account, initiates a remote payment transaction, etc.

The norms are found in the May 3 NBU Board Resolution #58 «On approval of the Regulation on authentication and the use of enhanced authentication in the payment market». Its requirements apply to all payment service providers.

STRENGTHENING THE CYBER RESILIENCE OF THE FINANCIAL SYSTEM: THE NCSCC STARTS VULNERABILITY MANAGEMENT TRAINING FOR SPECIALISTS IN THE BANKING SECTOR

On May 15, the NCSCC and the NBU Cyber Protection Center, with the support of the Civil Research and Development Fund (CRDF Global) in Ukraine, started Vulnerability Management (VDP) training for the banking sector. More than 30 specialized technical specialists from about 30 banks and the NBU participated in the 11th program in the Vulnerability Management series.

«The Vulnerability Management program is held for the second time for the Ukrainian banking sector because during the russian Federation's full-scale invasion russiainto Ukraine, our banking sector is constantly targeted by russian hackers», said Nataliya Tkachuk, head of the NSDC CISA, opening the event. «The best Ukrainian trainers will provide specialists with theoretical and practical knowledge in five cyber security areas. The participants will be able to enhance their qualifications and improve their skills to ensure the cyber security of information systems».

The 6-week VDP training course will teach cyber security specialists about current challenges and threats in protecting the banking system's critical infrastructure.

NCSCC HOLDS 2-DAY TRAINING ON CYBER SECURITY AND CYBER INTELLIGENCE FOR SECURITY AND DEFENSE SECTOR SPECIALISTS

On May 15-16, the NCSCC, with the support of CRDF Global in Ukraine and the U.S. Department of State, held a 2-day training on cyber security and cyber intelligence for security and defense sector specialists, «Tools, services, and threat intelligence in cyber security».

More than 20 AFU and Ministry of Defense representatives took part in the event. The training was conducted by Internet 2.0 cyber security experts based on the recently signed memorandum of cooperation.

Training participants mastered the latest technologies in cyber security, including threat detection and response, vulnerability scanning and traffic analysis, intelligence gathering and document analysis. Specialists also tested their new skills by completing several tasks.

WITH NCSCC ASSISTANCENCSCC, TRAINING FOR UKRAINIAN CYBER SECURITY SPECIALISTS WAS HELD AT THE NATO CCDCOE

The NATO CCDCOE organized a training for Ukrainian cyber security specialists in Tallinn this week, «Critical Information Infrastructure». The event was held with NCSCC support NCSCCand assistance from the Consultative Mission of the European Union in Ukraine (UCM).

Specialists from the NSDC, Security Service of Ukraine (SBU) Cyber Security Situation Center, SSSCIP, and the National Police Cyber Security Department took part in the training.

There was also a working meeting of the Ukrainian delegation and representatives with CCDCOE director Mart Noorma to discuss further cooperation on cyber security.

SSSCIP HOLDS WRITE-UP COMPETITION BASED ON ONLINE CYBER SECURITY COMPETITION

On April 28-29, the SSSCIP held a write-up contest based on the results of the all-Ukrainian online cyber security competition UA30CTF. The Knotty Kitten team was the winner. Teams can publish their write-ups on any platform.

A write-up is a free-form narrative in which contestants share information about how they successfully completed specific tasks during the Capture the Flag (CTF).

NUMBER OF CYBER ATTACKS ON COMMERCIAL SECTOR INCREASED SINCE START OF YEAR – STATISTICS

Since the beginning of 2023, the SSSCIP CERT-UA has manually processed more than 700 cyber incidents and cyber attacks, 151 of which occurred in April.

According to CERT-UA, central and local government organizations remain the focus of hostile hackers. However, during March-April, experts also recorded an increase in the number of cyber attacks on commercial organizations, growing almost twice compared to January-February 2023.

Phishing remains a favorite tactic of russian hackers. Their phishing campaigns are well-planned and massive in nature. This type of attack threatens not only employees of targeted organizations (civil servants, employees of critical infrastructure enterprises), but also every citizen. With the help of phishing, the russian special services try to collect all possible information about Ukrainians, focusing on personal data.

ATTACKERS USE LEGITIMATE SOFTWARE FOR DESTRUCTIVE ATTACKS ON UKRAINIAN STATE AGENCIES – ANALYSIS

CERT-UA investigated a cyber attack allegedly associated with the Sandworm group. The attackers used legitimate software to disable server equipment, automated user workstations, and data storage systems, among other things.

Having gained unauthorized access to the target's information and communication system, RoarBat - BAT script was used to disable computers running the Windows operating system (OS). The script recursively searches for files based on a specified list of extensions for their subsequent archiving using the legitimate WinRAR program with the «-df» option. This option involves deleting the source file and subsequently deleting the archives. The script in question was run by a scheduled task, which, according to preliminary information, was created and centrally distributed by means of Group Policy (GPO).

Computers running the Linux OS were decommissioned using a BASH script, which, among other things, ensured the use of the standard «dd» utility to overwrite files with zero bytes.

CERT-UA notes that the malicious plan in this and similar attacks is facilitated by the lack of multi-factor authentication when making remote virtual private network (VPN) connections; lack of network segmentation; and filtering of incoming, outgoing, and inter-segment information flows. General information about the attack and indicators of cyber threats are available at: cert.gov.ua/article/4501891

SSSCIP CONDUCTS SECOND TRAINING ON CYBER PROTECTION FOR CATEGORY «A» CIVIL SERVANTS

To enhance the knowledge of public sector representatives about cyber protection and to provide practical skills that will help institutions be effective in building and managing cyber defenses, the SSSCIP held a second educational course for category «A» civil servants.

The program targets managers who need to become cyber security change leaders in their institutions. Leading Ukrainian experts shared their knowledge with the employees, including representatives of Ukraine's cyber security entities: SSSCIP, SBU, Cyber Police, NSDC NCSCC, CERT-UA, the State Cyber Protection Center, and cyber security specialists from businesses involved in public-private partnerships.

«The entire world joins forces today to counter russian aggression in cyberspace», said the SSSCIP Deputy Head Oleksandr Potii. «It is equally important that we join forces within the country: share knowledge and expertise, cooperate when countering cyber threats. Educational programs of this kind help the country's cyber security and cyber defense experts to spread best practices when the country needs it the most, and build bridges for cooperation in ensuring the state's cyber defense».

SBU LIQUIDATED POWERFUL PROXY CENTER IN POLTAVA USED BY THE RUSSIAN FEDERATION TO CONDUCT SPECIAL INFORMATION OPERATIONS ON THE INTERNET

SBU cyber specialists worked with the Economic Security Bureau to block a powerful proxy center in Poltava used by russia for subversive activities against Ukraine. The organizers of illegal activities who were detained turned out to be two residents of Poltava and Kharkiv Oblasts.

The perpetrators set up an illicit proxy center that worked as a VPN service. It allowed subscribers from any country to impersonate Ukrainian mobile Internet users. A subscription costs almost UAH 2,500 (~$68) per month. According to operational information, those involved received hundreds of orders every day, and money was received through prohibited payment systems.

Among the regular customers were russian Federation citizens russiawho, through the proxy center's services, tried to hide their internet protocol (IP) addresses to access popular social networks. The servers were in russia, which allowed russian special services to gain remote access to Ukrainian Internet space and to spread Kremlin narratives and fake information about the situation at the front, allegedly on behalf of Ukrainian citizens.

Investigative actions are ongoing to establish all the circumstances of the crime and bring the culprits to justice.

CYBER POLICE OFFICERS EXPOSE CHERNIVTSI RESIDENT IN THE DEVELOPMENT AND SALE OF MALICIOUS SOFTWARE

The perpetrator developed a program for remote data management on victims' servers. He sold his product on forums and hackers employed it to carry out attacks on various companies and institutions. The suspect may face up to five years in prison.

The man developed an Obfuscated Web Backdoor type program to encrypt software code and modified malware to remotely control web resources. The perpetrator's product hid the malicious software on the affected resource, imperceptible to the owner.

At the same time, the perpetrator used another program that artificially increased the rating and search output of the web page, bypassing the rules for using and promoting web resources of search engines.

SBU LIQUIDATES NETWORK OF BOTNETS WITH AN AUDIENCE OF ALMOST 200,000 USERS WORKING TO DESTABILIZE UKRAINE

SBU cyber specialists exposed an interregional network of botnets that spread disinformation to destabilize the socio-political situation in Ukraine. The attackers tried to discredit the activities of Ukraine's top military and political leadership. They also spread false information about terrorist attacks in Ukrainian cities and the mining of public places.

To spread the fake information, anonymous accounts were created on Facebook, Instagram and Twitter social networks with a total audience of almost 200,000 users. The involved parties installed hardware and software complexes for "growing" bots in their own homes or offices.

As a result of a multi-stage special operation in different regions of Ukraine, nine bot farms were neutralized and their organizers were exposed.

An investigation is ongoing to establish all the circumstances of the crime and bring the guilty to justice.

THE NATIONAL POLICE AND U.S. FBI ELIMINATE SERVICE NETWORK EXCHANGING CRIMINALLY OBTAINED CRYPTOCURRENCY

The services enabled cybercriminals to legalize assets obtained as ransoms from encryption virus attacks. The network was destroyed in an international police operation.

The National Police Cyber Police Department and Main Investigative Department and the Office of the Prosecutor General of Ukraine, in cooperation with the U.S. FBI conducted a multi-level international operation to eliminate nine virtual asset exchange services.

The web resources offered users anonymous exchange of cryptocurrencies, which facilitated the legalization and laundering of money obtained illegally. Hackers channeled assets through malware attacks and online fraud through the exchanges. Exchange services were advertised on closed hacker forums.

As a result of the operation, law enforcement officers blocked the network's infrastructure on servers in the U.S. , in European countries, and in Ukraine and their domain names have been removed. Police are working to identify all those involved in the criminal activity.

SBU DETAINS TWO PRIVATE DETECTIVES IN KYIV WHO SOLD CONFIDENTIAL INFORMATION FROM GOVERNMENT DATABASES

SBU cyber specialists neutralized the criminal activities of a private detective agency in Kyiv that was selling information from closed government databases. The illegal activity was organized by a former investigator of one of the capital's district police departments, who refused to undergo certification for police service and resigned from law enforcement in 2015. Later, he and his acquaintance opened a private detective agency.

Under the guise of a legal business, they collected confidential information about other citizens for their clients, including data stored in government registers. They used their old connections among officials and law enforcement agencies without their knowledge. The cost of a person's file ranged from $800 to $2,600. The amount depended on the volume of personal data and the urgency of the order.

For example, in addition to citizens' passport data, the expanded questionnaires included information about phone numbers, vehicle license plates, border crossings, and administrative offenses.

Investigations are ongoing to bring justice for all persons involved. Information on the possible sale of confidential information to the russian Federation is also being checked.

NATIONAL POLICE ELIMINATE LARGE-SCALE FRAUD SCHEME: PARTICIPANTS EMBEZZLED MONEY FROM THE ACCOUNTS OF MORE THAN 10,000 CITIZENS

A special operation involving over 500 National Police employees was carried out in 20 Ukrainian regions to stop an extensive criminal network and carry out investigations. As a result, 56 people were exposed who had sent out phishing links to obtain data on citizens' bank cards. Those involved gained access to accounts from which they appropriated about 15 million UAH (over $405,000).

The criminals gathered on closed thematic channels and forums. During the investigation, police identified 11 online communities. The community administrators posted announcements about part-time work and those willing to get involved had to create and send out phishing links similar to links sent by official resources to obtain bank card data. Phishing was disguised in various ways, including offers to arrange cash payments for the sale of various goods, mostly household appliances.

According to preliminary data, more than 10,000 citizens were affected by the illegal activities. At this time, it is known that the perpetrators embezzled at least 15 million UAH (over $405,000), and the total amount of damages will be established during the investigation.

Police officers identified 56 persons involved in the fraud and searched their homes in 20 oblasts. The investigation is being conducted under Part 3, 4 of Art. 190 (Fraud) of the Criminal Code of Ukraine. Materials are being prepared to press charges against the suspected criminals.

LVIV, LAW ENFORCEMENT EXPOSE CRIMINAL ORGANIZATION WHOSE MEMBERS USED PHISHING TO EMBEZZLE ABOUT 6 MILLION UAH

Criminals sent phishing links under the guise of registering for social benefits and gained access to the accounts of more than 1,500 people, then appropriated their money. The alleged perpetrators were caught, detained, and charged.

Criminals sent phishing links through social networks and messengers inviting them to receive financial assistance from the President of Ukraine, the United Nations (UN), United Nations Children's Fund (UNICEF), and other organizations. The interface of the fraudulent sites was similar to official government resources and banking sites.

According to preliminary data, the group members gained access to the online banking of about 1,500 people. The total damage is 6 million UAH (over $162,000).

The investigators charged the suspects with fraud, creating and participating in a criminal organization - part 4 of Art. 190, Part 1, Art. 2 255. Three members of the group were also charged with unauthorized interference in the work of information (automated), electronic communication, information and communication systems, electronic communication networks - Part 5 of Art. 361 of the Criminal Code of Ukraine.

ATTACKERS LAUNCHED ANOTHER CAMPAIGN OF ATTACKS USING EMAILS WITH THE SUBJECT «BILLS» – ANALYSIS

CERT-UA discovered and investigated another email campaign with the subject «bills" by the hacker group UAC-0006. Attackers send emails with an attachment in the form of a ZIP or RAR archive containing the SmokeLoader malware. Legitimate compromised email accounts were used for mailing.

CERT-UA notes a number of changes in UAC-0006 tactics, techniques and procedures:

- Using several damage chains;
- The distributed SmokeLoader sample contains 26 botnet management server URLs (the vast majority of domains are unregistered);
- Detecting the Cobalt Strike Beacon malware may indicate an expansion of the list of tools the group uses.

To register domain names and host botnet management servers, attackers use russian domain name registrars and providers: @reg.ru, @nic.ru, @iqhost.ru, @macloud.ru, @cloudx.ru, which contribute to the implementation of the malicious plan.

As CERT-UA reminds, Windows Script Host (wscript.exe, cscript.exe) is used to run the JavaScript loader that delivers and runs SmokeLoader; therefore, to reduce the attack surface, it is recommended to limit the possibility of using this technology on computers. General information about the attack and indicators of cyber threats are available at cert.gov.ua/article/4555802