НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

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

June 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

AI	Artificial Intelligence
APT	Advanced Persistent Threat
ATP CS	Automated Technological Process Control Systems
CERT-UA	Government Computer Emergency Response Team Ukraine
CISA	Cybersecurity & Infrastructure Security Agency
CRDF Global	Civil Research and Development Fund (U.S.)
DDoS	Distributed Denial-of-Service
EBA	European Business Association
ENISA	European Union Agency for Cybersecurity
EU	European Union
FSB	Federal Security Service (russian Federation)
GDP	Gross Domestic Product
GRU	Main Directorate of the General Staff of the Armed Forces of the russian Federation
IP	Internet Protocol
JSC	Joint Stock Company
MDT	Ministry of Digital Transformation of Ukraine
NATO	North Atlantic Treaty Organization
NCSCC	National Coordination Cybersecurity Center
NSA	National Security Agency (U.S.)
OS	Operating System
OT	Operational Technology
SBU	Security Service of Ukraine
SCADA	Supervisory Control and Data Acquisition
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
TTX	Table Top Exercise
U.S.	United States

KEY TENDENCIES

At the beginning of June, a number of international events related to cyber security took place in Tallinn, Estonia, including the CyCon conference. Participants focused on discussing the theory and practices of cyber conflicts, primarily taking into account the realities of cyber confrontation in the russian-Ukrainian war. In addition, participants noted the need to increase the number of professional diplomats dealing with cyber security issues at the international level. The fifth U.S.-Ukrainian bilateral cyber consultations became part of these events, and the U.S. plans to provide Ukraine with an additional $37 million in cyber security assistance.

Interstate cooperation is deepening with a distinct emphasis on the Asian direction. While joint investigations and the publication of relevant guidelines within the “Five Eyes” alliance demonstrate a constant positive trend for at least the last six months, more and more joint projects are appearing between the U.S. and the European Union (EU) with Asian countries, such as South Korea, Singapore, and Taiwan. In 2024, the latter is expected to become one of the key focuses of the Pentagon’s cyber security assistance.

The EU continues to implement measures that limit China’s influence on the EU’s digital infrastructure and is developing its cyber capabilities. In particular, in mid-June, the European Commission adopted a decision for additional restrictions on the activities of Huawei and ZTE in the EU. At the same time, European legislators are finalizing work on the Law on Cyber Resilience, which should create a number of new opportunities for the EU to improve its own cyber security. Also, the EU continues discussions with partners (in particular, NATO) regarding possible areas of cooperation to build the stability of critical infrastructure facilities.

A key event in June was a cyberattack by the russian malicious group Cl0p using a vulnerability in the popular file sharing program MOVEit. As a result of the cyberattack, several American federal institutions (mainly in the energy sector) and large industrial companies were affected. Currently, cyber security authorities continue to investigate the consequences of the cyberattack and the extent of data loss.

Artificial intelligence (AI) is the center of special attention for both national governments and international discussions. The European Union Agency for Cybersecurity (ENISA) held regular discussions on the possible threats of uncontrolled use of AI for personal data, and the EU in general is preparing to introduce regulatory norms for the use of AI. The U.S., in turn, points to the threat of illegal AI use by authoritarian countries and draws attention to the fact that countries such as China are ready to enter new races of technological development with the West using old methods of not-always-fair competition.

The U.S. is preparing for possible large-scale destructive cyberattacks from China in the event of a "hot" conflict. According to Cybersecurity & Infrastructure Security Agency (CISA) leaders, this may include effective cyberattacks on the operational technology (OT) equipment of American critical infrastructure facilities. The U.S. military is preparing for cyberattacks against existing satellites and practicing defense and attack procedures. This concern is confirmed by research results; Chinese advanced persistent threat (APT) groups that target other countries generate 79 percent of all detected targeted malicious actions.

Energy companies are still one of the most desirable targets for hacking groups. Although viruses that affect OT have not yet gained widespread use, however, the energy sector feels its insecurity in today's cyber threat landscape. As the cyber standoff unfolds against the backdrop of the russian-Ukrainian war, European energy companies invest in their own cybersecurity capabilities, but they feel a lack of security for renewable energy companies.

The strengthening of passive countermeasures against cybercriminals (for example, by Microsoft regarding the use of macros in letters or documents) results in criminals looking for new attack vectors. They already find ways to bypass two-factor authentication and resort to new methods of social engineering (e.g., using fake call centers). They also focus on compromising supplier and contractor accounts for subsequent cyberattacks.

Allies of Ukraine continue to identify and analyze russian cyberattacks against Ukraine and Western countries. In June, Microsoft announced the discovery of a new russian cyber group, Cadet Blizzard, possibly linked to the russian Main Intelligence Directorate (GRU). This group may have been involved in cyberattacks against Ukrainian web resources before the full-scale military invasion in 2022. russian cybercriminals are regrouping (most likely under the control of Special Services) to intensify cyberattacks. In June, it became known that RomCom had resumed its operation and Killnet had restructured. Shuckworm and REvil have not stopped their attacks.

On June 15, the creation of the “IT coalition as a part of Rammstein” was announced. This initiative will contribute to increasing Ukraine’s capabilities, in particular in matters of cyber defense, and is part of the wider international partner efforts to support Ukraine. The continued support from the U.S. in the digital sphere should also be noted. Meanwhile, Western experts continue to discuss how effective Ukrainian approaches to cyber defense were during the war, draw conclusions, and work out possible changes in their own approaches to cybersecurity.

THE NCSCC HELD A 2-DAY INCIDENT RESPONSE DAYS CYBERSECURITY COMPETITION

The National Coordination Cybersecurity Center (NCSCC) and Civil Research and Development Fund Global in Ukraine (CRDF Global), with U.S. Department of State support, held a 2-day Incident Response Days cyber competition on June 12-13, with more than 100 public sector professionals participating.

Incident Response Days combines cybersecurity competitions with training on cyber operations, cyber incident response, and forensics. Over six hours, participants worked on a unique scenario, investigated incidents, collected artifacts, and analyzed malware.

For the first time, the new-generation Ukrainian cyber training ground developed by the Cyber Unit Technologies company was used during Incident Response Days. Participants were also trained in the safe use of AI technologies, digital forensics, and cyber threat information sharing practices.

NCSCC CONDUCTED THE FIRST TABLETOP EXERCISES AT THE REGIONAL LEVEL IN POLTAVA

On June 29, the NCSCC successfully conducted the first regional tabletop exercise (TTX), attended by representatives of Poltava Oblast Military Administration, key Ukrainian cyber security entities, and critical infrastructure facilities of Poltava Oblast. Participants worked out the interaction mechanism during a response to cyberattacks and communication of cyber incidents.

Based on the TTX results, appropriate decisions will be made to improve coordination and cooperation between the responsible regional bodies and strengthen the capabilities to build up the National Cyber Security System of Ukraine overall.

NCSCC AND CRDF GLOBAL HELD THE 20TH MEETING OF THE NATIONAL CYBER SECURITY CLUSTER IN POLTAVA

On June 29, the 20th meeting of the National Cyber Security Cluster was held in Poltava to discuss cybersecurity in the region's leading industries. About 200 people attended from the public and private sectors, international institutions, and the scientific community, both online and in person.

Cluster participants discussed the current state of cybersecurity in the region's leading industries and main challenges and threats, taking into account russian Federation aggression in cyberspace. Participants proposed a number of initiatives and projects to increase cybersecurity in Ukraine and strengthen cooperation between the state, academic community, and private sector.

CYBER DIALOGUE RESULTS: U.S. WILL ALLOCATE $37 MILLION TO SUPPORT UKRAINE'S CYBER RESILIENCE

The 5th annual Cyber Dialogue of Ukraine and the United States on cyber policy issues took place in Estonia. The U.S. delegation expressed support for Ukraine in the fight against russian aggression and announced that, in cooperation with Congress, it would provide an additional $37 million in cyber aid. The funds will be directed towards strengthening Ukraine's cyber resilience and protecting critical networks and digital infrastructure.

OLEKSIY REZNIKOV ANNOUNCED THE CREATION OF AN INTERNATIONAL IT COALITION

Summarizing the results of his visit to NATO headquarters in Brussels, Minister of Defense of Ukraine Oleksiy Reznikov reported on a number of valuable "victories" for the country on the diplomatic front. In particular, he said that Minister of Defense of the Grand Duchy of Luxembourg Francois Bausch and Minister of Defense of the Republic of Estonia Hanno Pevkur supported the idea of creating an IT coalition. The ministers of defense of friendly countries are ready to take a leadership role in creating the group.

UKRAINE STRENGTHENS INTERNATIONAL COOPERATION IN THE PROTECTION OF NETWORK RESOURCES

Deputy Chairman of the Digital Transformation Committee Serhii Shtepa and Ambassador of the Kingdom of the Netherlands to Ukraine Jennes de Mol held a working meeting to discuss possible measures to protect network resources (IP addresses) used by communications operators (providers) operating in the temporarily occupied territory of Ukraine.

The committee has been working on these issues for a long time and has organized several meetings with telecom industry representatives and government authorities to work out the necessary mechanisms for influencing the situation with IP addresses in the temporarily occupied territories. IP addresses are an important information infrastructure that impact cybersecurity issues in electronic communications.

MINISTRY OF DEFENSE DISCUSSED TOPICAL ISSUES OF BILATERAL COOPERATION WITH U.S. DELEGATION

Deputy Ministers of Defense Volodymyr Gavrylov and Vitaly Deinega met in Kyiv with a delegation from the defense and mining industry in the state of Arizona (USA), led by President of the Defense-Industrial Coalition of Arizona Lindy Smith.

The parties discussed current issues of bilateral cooperation and long-term prospects for cooperation in the defense sphere. The deputy heads of the defense department outlined the urgent needs of the Armed Forces of Ukraine to increase their capabilities and effectively repel the russian Federation's armed aggression.

The American delegation expressed its readiness to support Ukraine and confirmed its solidarity with the Ukrainian people.

STATE SPECIAL COMMUNICATIONS SERVICE IS DEVELOPING COOPERATION WITH THE EU

The State Service of Special Communications and Information Protection (SSCIP) held an official meeting with the European delegation headed by Margaritis Schinas, Vice President of the European Commission for the Promotion of the European Way of Life. The participants discussed the results of current cooperation, the challenges facing the entire democratic community in cyberspace, providing citizens with television and radio broadcasting in the liberated territories, protecting critical infrastructure facilities, and the Drone Army project.

CISCO WILL HELP UKRAINE WITH DIGITALIZATION AND EDUCATION

The Ministry of Digital Transformation (MDT) and Cisco signed a memorandum of cooperation on innovation and digitalization. The document was signed by the Deputy Prime Minister for Innovation, Development of Education, Science and Technology – Minister of Digital Transformation Mykhailo Fedorov and Cisco Vice President for Country Digital Acceleration Chris Reeves.

The memorandum brings Ukraine into the Cisco Country Digital Acceleration program. The parties will work together on educational projects, in particular on developing the Action. Education platform, and digital initiatives for cyber protection. In addition, the MDT will work with Cisco on developing and implementing Ukraine's innovative strategy.

REPRESENTATIVES OF THE ESTONIAN PARLIAMENT VISITED THE STATE SPECIAL COMMUNICATIONS SERVICE

An Estonian delegation visited the SSSCIP, including Ambassador Extraordinary and Plenipotentiary of the Republic of Estonia to Ukraine Kaimo Kuusk, Defense Attaché Eero Kinnunen, and representatives of the Riigikogu (Estonian Parliament).

The SSSCIP told the guests about its key activities, including cyber protection, government and civil communications, providing television and radio signal broadcasting, and creating the Drone Army. They also discussed the challenges Ukraine faces due to russia's large-scale aggression, which continues in particular in cyberspace.

The Estonian side noted that Ukraine's experience is quite useful for others, both in countering cyber threats and in other issues related to strengthening defense capabilities.

UKRAINIAN STATE BORDER GUARD SERVICE TEAM WON A CYBER COMPETITION

On June 13, the dotXYZ team of the State Border Service of Ukraine won first place during the Incident Response Days cyber competition, organized by the NCSCC and CRDF Global in Ukraine. The key task of the event was to improve the qualification and practical skills of cybersecurity specialists, performing tasks approximating real incidents as close as possible.

The Military Institute of Telecommunications and Informatization team csd33 won second place and the National Guard's "The Guard" team took third place.

TO PROTECT CRITICAL INFRASTRUCTURE, IT IS IMPORTANT TO CORRECTLY ASSESS HOW AN ATTACK ON ONE CRITICAL INFRASTRUCTURE OBJECT CAN AFFECT THE OPERATION OF OTHERS - O. POTII

Speaking at the Paris Cyber Summit, SSSCIP Deputy Head Oleksandr Potii emphasized the importance of correctly assessing the consequences of attacks on critical infrastructure. He emphasized that it is extremely important to deepen cooperation on combating cyber threats to protect critical infrastructure. After all, for many countries, cyberspace is one of the key sources of threats, particularly from russia. To counter these threats, countries should unite, strengthen data exchange, and jointly develop rules for safe behavior in cyberspace and tools for bringing the aggressor to justice.

NCSCC IS EXPANDING ITS ANALYTICAL CAPABILITIES

The NCSCC received access to modern analytical platforms from the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. This will allow the NCSCC to improve the quality of cybersecurity analyses and its ability to forecast potential cyber threats.

Using modern tools will help the NCSCC to expand the capabilities of its own information system in order to more effectively collect information about cyber incidents, provide an analytical assessment of the state of cybersecurity for government and critical infrastructure objects, help them respond effectively to cyber incidents and prevent cyber threats, and ensure the coordination of responding to critical-level cyber incidents.

SSSCIP RECEIVED EQUIPMENT NEEDED BY THE NATIONAL TELECOMMUNICATIONS NETWORK

Thanks to support from the EU4DigitalUA project, financed by the EU, the SSSCIP received modern equipment that will further improve the National Telecommunications Network and strengthen its stability during the war against and numerous missile and drone attacks on Ukrainian infrastructure.

SSSCIP APPROVED RECOMMENDATIONS FOR CYBER PROTECTION OF AUTOMATED TECHNOLOGICAL PROCESS CONTROL SYSTEMS

The SSSCIP approved methodological recommendations for ensuring the cyber protection of automated technological process control systems (ATP CS). They define:

- Requirements for cyber protection of ATP CS, in particular supervisory control and data acquisition (SCADA) systems and the procedure for implementing and confirming compliance.
- General system of designing, implementing, supporting, and continuously improving cyber protection of ATP management systems.
- Minimum levels of standard cyber protection target profiles for critical infrastructure objects of level I (catastrophic consequences) and level II (critical consequences) and negative impacts on the ability to provide basic services in case of destruction, damage, or malfunction of the critical infrastructure object.

SSSCIP TO EXPAND COOPERATION WITHIN TECHNICAL ASSISTANCE PROJECTS

A delegation consisting of DAI Inc. Vice President for U.S. Government Programs James Watson, Vice President for Grants and Contracts Baigal Darambazar, Senior Portfolio Director in Eastern Europe Mark McCord, and Director of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity Petro Matiyashek paid an official visit to the SSSCIP.

SSSCIP representatives and the delegation discussed the state of existing projects and promising areas of cooperation. Thanks to USAID support, the SSSCIP received a lot of equipment that helped ensure the stability of state telecommunications systems and continue their development.

GOVERNMENT AND BUSINESS MUST WORK AS PARTNERS TO PROTECT CRITICAL INFRASTRUCTURE

SSSCIP head Yuriy Shchyhol met with members of the European Business Association (EBA) to discuss the urgent issues of strengthening the protection of Ukraine's critical infrastructure, the SSSCIP's role in coordinating this process, and the importance of business involvement.

Shchyhol noted that most countries have spent 5-7 years building a system to protect critical infrastructure facilities in peacetime. Ukraine, on the other hand, has to do it in a shorter timeframe and in difficult war conditions, when russia's occupying forces deliberately destroy critical infrastructure, such as energy facilities, logistics, communications, etc. Therefore, the synergy of all participants in building a reliable critical infrastructure protection system is extremely important.

CYBER POLICE SIGNED A MEMORANDUM OF COOPERATION WITH THE ASSOCIATION OF UKRAINIAN CITIES

Conferences, trainings, seminars, and exercises are planned as part of the partnership, in particular, to improve citizen awareness of cyber hygiene issues.

Head of the Cyber Police Department Yuriy Vykhodets discussed with the representatives of the All-Ukrainian Association of Ukrainian Cities implementing effective measures to counter cybercrime, prepare relevant methodological recommendations and implement joint practical measures in the event of cyberattacks, the illegal use of information in cyberspace, computer security violations and their prevention, and ensuring mutual exchange of information. In addition, the partners plan preventive work among the population.

THE SSSCIP CONDUCTED CIREX CYBER TRAINING. CYBER. RANSOMWARE

On June 20-21, in Lviv, with the support of the EU4DigitalUA project, the SSSCIP held CIREX cyber security training. The event was attended by representatives of local self-government, regional military and state administrations, and regional SSSCIP divisions. The participants discussed problematic issues related to cyber protection and countering cyber threats and worked out response mechanisms to ransomware attacks.

THE SBU EXPOSED A KYIV IT COMPANY THAT TRIED TO "LEAK" INFORMATION FROM THE ELECTRONIC SYSTEMS OF THE FRONT-LINE MILITARY ADMINISTRATION TO RUSSIANS

The Security Service of Ukraine (SBU) prevented the transfer of defense information circulating in one of Ukraine's regional military-civilian administrations to the russian Federation. The leak was possible through the electronic document management system.

The enemy was most interested in information about the consequences of russia's airstrikes on the region's energy infrastructure. The russian Federation also wanted to know the exact coordinates of the electrical substations where repair and restoration was completed or still underway after the shelling. This would help the enemy to plan and launch repeated air attacks on them.

THE SBU LIQUIDATED A BOTNET IN VINNYTSIA THAT CREATED UP TO 500 FAKE ACCOUNTS EVERY DAY TO SPREAD KREMLIN NARRATIVES

The SBU blocked a powerful botnet in Vinnytsia that worked for russia. As a result of comprehensive measures, three of its organizers were detained.

Perpetrators daily registered up to 500 anonymous accounts in various social networks, including those banned in Ukraine. Ready-made "bots" were used for mass distribution of pro-Kremlin narratives, in particular regarding the situation at the front and the socio-political situation in Ukraine. They also justified armed aggression against Ukraine and called to support racists, including in the international arena.

ATTACKERS USED THE EMBLEM OF THE NATIONAL DEFENSE UNIVERSITY OF UKRAINE - ANALYSIS

The Government Computer Emergency Response Team Ukraine (CERT-UA) discovered and investigated a cyberattack by the group UAC-0057 (GhostWriter). A PowerPoint file "daewdfq342r.ppt" containing a macro and a thumbnail image with the emblem of the National Defense University of Ukraine was detected.

The dates of compiling the programs and creating (modifying) the PowerPoint file indicate that the attack was initiated no later than June 9, 2023. The malware management servers are located in the russian Federation, but the domain names are "hidden" behind Cloudflare.

SCAMMERS TRY TO GAIN ACCESS TO UKR.NET USER MAILBOXES BY SENDING PHISHING EMAILS PURPORTEDLY ON BEHALF OF TECHNICAL SUPPORT

CERT-UA warns of fraudulent activity against users of the ukr.net service. Attackers pretend to be ukr.net technical support and send emails with the subject "Suspicious activity @UKR.NET noticed" and a file attachment called "Security Alert.pdf" in an attempt to gain access to the victim's email inbox.

CERT-UA specialists analyzed the network infrastructure used to carry out similar cyberattacks from 2021 and found at least 118 related domain names registered by Internet Domain Service BS Corp.

THANKS TO COOPERATION WITH RECORDED FUTURE, CERT-UA DISCOVERED THE ESPIONAGE CAMPAIGN OF THE APT28 GROUP (BLUEDELTA) AGAINST UKRAINIAN ORGANIZATIONS

CERT-UA reported on a detected cyber threat from the hacker group APT28 (also known as Pawn Storm, Fancy Bear, BlueDelta). It established that the espionage campaign was attempted using exploits for Roundcube (webmail software) and by sending emails with current news about the situation in Ukraine.

The prompt exchange of information with Recorded Future specialists helped to reveal the cyberthreat attempts.

CYBER POLICE EXPOSED AN ORGANIZED CRIMINAL GROUP THAT EMBEZZLED MORE THAN 2 MILLION UAH ($54,000) WITH THE HELP OF PHISHING

Criminals used phishing links to obtain bank card data of citizens and later appropriated money from their accounts. Law enforcement officials brought charges against the six individuals involved, who may face up to 12 years in prison.

The organizers created a site and community in the Telegram messenger, where instructions and phishing links were provided for participants in the fraudulent scheme. Then they compromised clients' bank cards and used payment systems to "withdraw" the victims' money to controlled accounts.

CYBER POLICE EXPOSED AN ORGANIZED CRIMINAL GROUP USING A NETWORK OF PHISHING BOTS

Criminals created phishing bots in the Telegram messenger under the guise of bots of the Ukrainian energy company DTEK. Having collected the necessary user data, the perpetrators had unauthorized access to the victims' accounts. Later, they used the "hacked" accounts to send out fraudulent advertisements to embezzle citizens' money. According to preliminary data, the attackers made unauthorized interventions in more than 15,000 accounts, and about 3,000 people suffered from fraud under the guise of investing money. Law enforcement officers are working to identify the victims and the amount of damage.

CYBER POLICE EXPOSED THE ORGANIZERS OF A FRAUDULENT CALL CENTER THAT APPROPRIATED CRYPTOCURRENCY ASSETS OF FOREIGN CITIZENS

Criminals scammed Canadians by offering them profits from trading on stock exchanges. The perpetrators asked people to install a program that would allegedly help "withdraw" money, but instead they gained remote access to the victims' computers and appropriated money from their accounts. In cooperation with Canadian law enforcement officers, Ukraine's cyber police are working to identify the victims and the amount of damage caused. According to operational data, representatives of the Ukrainian diaspora are among the defrauded.

SBU EXPOSED 11 MORE INTERNET AGITATORS WHO WERE SPREADING KREMLIN PROPAGANDA IN UKRAINE

The SBU neutralized the subversive activities of 11 more pro-russian Internet agitators in several regions of Ukraine:

- In Kyiv, a resident of the capital created and personally administered several groups on Facebook, Telegram, and Viber and called for "union with russia."
- In Mykolaiv, a cleric of the local Ukrainian Orthodox Church publicly called on the religious community to support the russian occupiers in the war against Ukraine.
- In Dnipropetrovsk Oblast, subversive activities were blocked of two enemy agitators who praised the higher military and political leadership of the russian Federation and discredited Ukrainian defenders in various social networks.
- In Kirovohrad Oblast, a network was neutralized of russian Federation Internet propagandists agitating local residents to join the ranks of the occupying groups of the aggressor country.
- In Vinnytsia, two local residents on the banned Odnoklassniki social network glorified the "feats" of terrorists and suggested erecting monuments to Ramzan Kadyrov, head of the Chechen Republic in the russian Federation.
- Investigations are ongoing to establish all the circumstances of the crimes and bring the culprits to justice.

MDT IS PUT IN CHARGE OF ELECTRONIC COMMUNICATIONS

The government adopted a resolution according assigning powers to the SSSCIP over electronic communications and the radio frequency spectrum until the end of August 2023. From September 1, these functions will be transferred to the MDT. The transfer of powers is part reforming the SSSCIP.

1. FIRST WORLD CYBER WAR

U.S. DEPARTMENT OF DEFENSE PROVIDES STARLINK SERVICES TO UKRAINE

The United States is providing funding for Starlink communications in Ukraine, as reported by C4ISRNet on June 1. Given the sensitive nature of these services, the Department of Defense refrains from disclosing details regarding the cost, duration, and coverage. Throughout the conflict, Starlink has proven instrumental in delivering crucial and reliable connectivity to Ukraine.

RUSSIA ACCUSES THE U.S. OF HACKING THOUSANDS OF APPLE DEVICES TO SPY ON DIPLOMATS

SOURCE 2 **SOURCE 3** **SOURCE 4**

On June 1, the russian Federation's Federal Security Service (FSB) announced that the United States had employed previously unidentified malware to infiltrate iOS devices owned by russian diplomats.

A report by russian cybersecurity firm Kaspersky highlighted iOS malware of unknown origin, suggesting a potential connection between the two attacks due to shared indications of compromise. The malware targeted not only russian users but also foreign numbers and wireless subscribers using SIM cards registered with diplomatic missions and embassies in russia.

According to russian intelligence, the investigation uncovered Apple's collaboration with the U.S. National Security Agency (NSA). However, no technical details were provided regarding the malware and its purported victims.

Apple refuted the accusations, affirming that it "has never collaborated with any government to implant a backdoor in any Apple product and never will."

RUSSIA WANTS OFFICIALS TO USE 2 MILLION PHONES WITH RUSSIAN AURORA OS

On June 2, The Record reported that Rostelecom intends to offer government officials mobile phones powered by the Aurora operating system (OS), a russian alternative to Western software. "As stated on the website," The Record elaborates, "Aurora grants customers complete control over data processing and adheres to russian government security protocols." The shift towards enhanced self-sufficiency serves a dual purpose: first, it addresses security concerns; and secondly, it aims to safeguard national IT capabilities amidst international sanctions imposed in response to russia's invasion of Ukraine.

KREMLIN: HACKED RUSSIAN RADIO STATIONS BROADCAST FAKE PUTIN ADDRESS

On June 5, certain russian radio stations close to the Ukrainian border aired a fabricated radio address purportedly delivered by russian Federation President Vladimir Putin. In the broadcast, the fictional Putin claimed that Ukrainian forces had extensively breached the russian border, prompting russia to impose martial law and initiate general mobilization, while urging residents in border regions to evacuate. Reuters reported that the false message was transmitted in Rostov, Belgorod, and Voronezh oblasts. Official russian media rushed to refute this. “All of these reports are entirely false,” stated russian government spokesperson Dmitry Peskov.

KILLNET REBOOT

SOURCE 2

In a June 6 Radware blog post, the company outlines the transformations occurring within the hacktivist group Killnet, which is led by an individual known as Killmilk on behalf of russian intelligence and security agencies. Radware characterizes the reboot as a transition towards a more proficient and disciplined organization. While Killnet previously presented itself as a grassroots movement, it is now undergoing a process of professionalization.

Subsequently, on June 14, hacker groups Killnet, Anonymous Sudan, and REvil issued threats regarding an imminent and “devastating” assault on the entire European financial system. The assault was slated to commence within the next 48 hours, starting with the SWIFT international communication system. Their stated objective was to obstruct European governments’ capability to provide weaponry to Ukraine. Given the historical connections of all three groups with the GRU, it is plausible that these attacks were endorsed by the russian government.

ROMCOM REVIVES: ATTACKS UKRAINIAN POLITICIANS AND U.S. MEDICAL FACILITIES ASSISTING REFUGEES FROM UKRAINE

On June 7, Blackberry published a report revealing that the threat actor RomCom has been actively monitoring geopolitical developments surrounding the war in Ukraine. The report highlights RomCom’s attacks on various targets, including the military, food supply chains, and IT companies. Blackberry’s Threat Research and Intelligence team recently observed RomCom’s latest campaign, which involved targeting Ukrainian politicians with close affiliations to Western nations. Additionally, the group attacked an American medical company that offers humanitarian aid and medical assistance to Ukrainian refugees residing in the United States.

This report constitutes the initial segment of a comprehensive study that delves into the intricacies of the most recent RomCom malware campaign. The subsequent section of the study focuses on RomCom’s behavioral patterns and detection techniques.

TRUSTWAVE EXPERT DISCUSSION: RESILIENCE OF UKRAINE'S DEFENSE AGAINST RUSSIAN CYBERATTACKS CAME AS A PLEASANT SURPRISE TO MANY

In June 7 discussion, former Texas Congressman William Thornberry and Trustwave Government Solutions President Bill Rucker focused on the cyber aspect of the russia n-Ukrainian war. Both participants acknowledged that russian cyber activities leading up to the invasion were in line with most experts' expectations.

According to their analysis, russia used all available means to launch cyberattacks against Ukraine as part of a broader strategy. russia has allocated significant resources to sustain these attacks, evident from the prolonged duration of large-scale distributed denial-of-service (DDoS) attacks lasting up to 30 days. Interestingly, there has been a significant decline in credit card data theft, leading Trustwave to speculate that russian cybercriminals have been redirected towards targeting Ukraine.

However, the experts expressed surprise at Ukraine's preparedness and adaptability in defending against these attacks. They cautioned against complacency, emphasizing that it would be dangerous to assume that the cyber component has not had a substantial impact beyond Ukraine itself, so leaders should not develop a false sense of security based.

ASYLUM AMBUSCADE: MALWARE OR CYBER ESPIONAGE?

ESET's We Live Security blog reported on June 8 that the Belarusian threat group known as Asylum Ambuscade, active since at least 2020, is conducting an "unusual mix of cybercrime and cyberespionage." In 2022, it gained attention for its attacks on European governments supporting Ukrainian refugees. Key findings:

- Asylum Ambuscade primarily targets bank customers and cryptocurrency traders across various regions, including North America and Europe.
- Asylum Ambuscade engages in espionage activities against government agencies in Europe and Central Asia.
- The group predominantly employs scripting languages like AutoHotkey, JavaScript, Lua, Python, and VBS for its implant development.

UKRAINIAN HACKERS BREACH A SERVICE PROVIDER FOR RUSSIAN BANKS

SOURCE 2

On June 9, Bleeping Computer quoted Ekonomichna Pravda as saying that Ukrainian hackers Cyber.Anarchy.Squad had successfully breached several russian websites and displayed banners in support of the Ukrainian Armed Forces' counteroffensive. One of the affected sites was that of Infotel JSC, a Moscow-based provider responsible for facilitating interactions between the Central Bank of russia and other legal entities within the country, such as banks, online stores, and credit companies. Both the provider and independent sources have confirmed this information, as stated by Bleeping Computer.

IN RUSSIA, DDOS ATTACKS SURGED BY 58% YEAR-ON-YEAR - THE GEOGRAPHY ALSO EXPANDED

The IT Army of Ukraine reported on June 9 that there has been a significant increase in the number of DDoS attacks in russia during the first quarter of 2023. The number of attacks has risen by 58 percent, reaching 384,800 compared to 226,100 attacks during the same period last year.

Analysts from MTS Red observed a further surge in DDoS attacks, with an 81 percent increase in April compared to March, and a 69 percent increase in part of May.

Among the regions affected, the Northwestern District emerged as the most targeted area, with St. Petersburg being the leading city where 87 percent of all DDoS attacks were recorded. The Central Federal District ranked second, followed by the Volga Federal District.

PRO-RUSSIAN HACKERS ATTACK THE LARGEST PORT IN EUROPE

On June 14, the media reported that the pro-russian hacker group NoName launched DDoS attacks on the websites of the Dutch ports of Groningen, Amsterdam, Rotterdam, and Den Helder.

Consequently, the ports' websites were inaccessible on June 10-11 and for several hours on June 13. The administration of the Port of Rotterdam stated that the cyberattack originated from IP addresses in russia and Serbia, but no further harm was caused aside from the temporary unavailability of the websites.

RUSSIAN HACKERS ATTACK THE WEBSITES OF SUSPILNE

On June 14, the websites of Suspilne fell victim to a cyberattack orchestrated by the russian hacker group Solntsepyok. While certain sites experienced temporary disruptions, all of Suspilne's news platforms, including suspilne.media, remained fully operational without any interruptions.

TRENDS OF THE UKRAINIAN IT ARMY'S CAMPAIGN IN RUSSIA

On June 15, Lawfare released a study focused on the Ukrainian IT army, shedding light on its unique perspective regarding the decisions and actions taken on the offensive side of cyber warfare, as most of the available information primarily stems from the defense side. Author Kyle Fendorf emphasizes that Ukraine's IT army provides valuable insights into using cyberspace in warfare.

In his conclusions, Fendorf highlights the IT army's limited technical capabilities and inclination to surpass international norms by targeting civilian entities. Notably, 90 percent of the attacks were relatively straightforward DDoS attacks, which, despite their simplicity, can inflict significant damage. The IT army's sabotage operations showcase its more advanced abilities; however, its annual count of successful sabotage attacks has never surpassed seven.

The 93 attacks targeting the financial sector, along with the weekly attacks on russian media, exhibit a disregard for the norm of exclusively targeting military entities, as asserted by the United States. Nevertheless, the IT army has its own limitations. Following an attack on the education sector, it has since refrained from further assaults in that area. Additionally, it has shown reluctance to target the healthcare sector. Thus, despite willingness to do more than most Western countries, the IT army has left a few sectors untouched.

SHUCKWORM: INSIDE RUSSIA'S RELENTLESS CYBER CAMPAIGN AGAINST UKRAINE

According to Symantec's June 15 report, the Shuckworm spyware group, also known as Gamaredon and Armageddon, actively continues to conduct multiple cyberattacks against Ukraine. Its recent targets have included security services, military organizations, and government agencies. The attackers have persistently sought to infiltrate these entities and extract sensitive information, including reports on Ukrainian military casualties, enemy combat operations, air strikes, arsenal inventories, military training, and other related data. Ukrainian authorities have publicly attributed the group's actions to the FSB. The blog provides detailed insights into the strategies and operations of this group.

CYBERPEACE INSTITUTE PRESENTS TIMELINE OF CYBER ACTORS EMERGING IN THE RUSSO-UKRAINIAN WAR

On June 30, the CyberPeace Institute unveiled a comprehensive timeline outlining the emergence of different cyber actors, both pro-russian and pro-Ukrainian, during the First World Cyberwar. The timeline provides insights into the specific moments when these cyber actors entered the cyber conflict and categorizes them based on their affiliations, such as state groups, cybercriminal networks, or individual hackers.

RUSSIAN "SILICON VALLEY" SUFFERS A CYBERATTACK

Ukrainian hackers successfully breached the systems of the Skolkovo Foundation, an organization established by former russian president Dmitry Medvedev to rival Silicon Valley in the United States. Skolkovo confirmed that the hackers achieved restricted access to specific information systems, including the organization's file service hosted on physical servers.

A group of Ukrainian hacktivists took credit for the attack and shared screenshots of the infiltrated systems on Telegram. Nevertheless, the impact of the attack was largely symbolic, as Skolkovo managed to restore all services within a single day.

SWISS FINANCIAL CENTER DISABLED BY RUSSIAN HACKERS

SOURCE 2

The pro-russian hacker group that targeted Switzerland's critical infrastructure on June 12 also attacked the Geneva Financial Center (GFC), the country's primary banking institution. The cybercrime group, No-Name, publicly claimed responsibility for the attack on the morning of June 15 through its Telegram channel. The GFC is a prominent organization in the Swiss financial sector, accounting for 13 percent of Geneva's GDP.

SANS analyst Lee Neely suggests that the motive behind these attacks is likely linked to Switzerland's shift from a position of neutrality to providing aid to Ukraine.

SWISS INTELLIGENCE WARNS OF CYBER CONSEQUENCES AS THE WEST DEPORTS SPIES

SOURCE 2

In its annual country security report published on June 26, the Swiss Federal Intelligence Service cautions that there will be a rise in cyberattacks aimed at espionage, particularly targeting critical infrastructure operators, due to Western endeavors to disrupt russian intelligence networks in Europe.

Intelligence agencies globally will need to enhance their capabilities to gather data both domestically and internationally. Entities that handle substantial volumes of sensitive data, including financial service providers, government agencies, critical infrastructure operators, and technology companies, face a higher vulnerability to cyber espionage.

2. MISCELLANEOUS

HACKER'S CONFESSION EXPOSES INDIA'S SECRETIVE HACKING INDUSTRY

In a June 1 publication, the New Yorker sheds light on how the revelations of an Indian hacker have exposed the thriving industry of cyberattacks for hire in India. The article highlights that this business is far more extensive than previously acknowledged by experts.

UK GOVERNMENT TO SET A DEADLINE FOR REMOVAL OF CHINESE CCTV CAMERAS SOURCE 2

This proposal is part of the amendments to the law on public procurement, which were published on June 6, 2023. The proposed amendments feature a clause that mandates the "exclusion of physical surveillance equipment produced by companies subject to the National Intelligence Law of the People's Republic of China from the procurement chain." Following the bill's passage, expected during the week of June 11-16, the UK Secretary of State must inform Parliament about the schedule for removing the implicated equipment within six months.

WINNING THE MIND GAME: ROLE OF THE RANSOMWARE NEGOTIATOR

The Hacker News publication on June 7 presented exclusive insights from a real-life ransomware negotiator, who reveals personal accounts of online hostage situations and the strategies employed to resolve them.

EU PLANS TO BAN COMPANIES FROM MANUFACTURING SENSITIVE EQUIPMENT IN CHINA

On June 20, the EU revealed its intentions to prohibit European companies from manufacturing sensitive technologies, including supercomputers, artificial intelligence, and advanced microchips, in certain countries such as China.

Under the European Economic Security Strategy, introduced by Commission President Ursula von der Leyen, Brussels aims to exert greater influence over the investment and trade activities of European companies worldwide. While China is not explicitly named, it is evident that Beijing is the primary focus of this initiative.