NCSCC
NATIONAL CYBERSECURITY
COORDINATION CENTER

USAID
FROM THE AMERICAN PEOPLE

UKRAINIAN FOUNDATION
FOR SECURITY STUDIES

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

June 2024

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

CONTENT

ACRONYMS

AI	Artificial Intelligence
APT	Advanced Persistent Threat
CERT-UA	Government Computer Emergency Response Team Ukraine
CFCS	Center for Cybersecurity (Denmark)
CISA	Cybersecurity and Infrastructure Security Agency
CMU	Cabinet of Ministers of Ukraine
CRDF Global	Civil Research and Development Fund (U.S.)
CSIS	Center for Strategic and International Studies (U.S.)
DDoS	Distributed Denial-of-Service
ENISA	European Union Agency for Cybersecurity
EU	European Union
EuroDig	European Dialogue on Internet Governance
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
HUR	Main Intelligence Directorate of Ukraine
ICC	International Criminal Court
IMEI	International Mobile Equipment Identity
IT	Information Technology
MIVD	Military Intelligence and Security Service (Netherlands)
NATO	North Atlantic Treaty Organization
NCSCC	National Cybersecurity Coordination Center
NICE	National Initiative for Cybersecurity Education
NSDC	National Security and Defense Council of Ukraine
OFAC	Office of Foreign Assets Control (USA)
ONCD	Office of the National Cyber Director (U.S.)
OT	Operational Technology
SBU	Security Service of Ukraine
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
U.S.	United States
UAV	Unmanned Aerial Vehicle
UK	United Kingdom
VPN	Virtual Private Network

KEY TENDESES

The United States is focusing on the educational component, recognizing a significant shortage of cybersecurity specialists across all sectors of the economy (currently, there are about 500,000 unfilled vacancies). The Office of the National Cyber Director (ONCD) is actively promoting the National Cybersecurity Education and Workforce Strategy, engaging in discussions with market participants. In these discussions, there is a growing consensus to conceptually abandon the requirement for higher education when hiring cybersecurity specialists and instead focus solely on proven qualifications. This is expected to help the U.S. Department of Defense, which currently has about 27,000 unfilled cybersecurity positions due to bureaucratic issues.

The operational technology (OT) sector is trying to adapt to the new reality of increased cyber threats to this unique field. The U.S. is concerned about the low cybersecurity standards specifically for OT, which are critical to the economy's essential services. The government is attempting additional regulation, but industrial facility owners point out systemic issues with the regulation process, which is mostly fragmented and inconsistent with sectoral standards. Additionally, industrial company owners highlight the specificity of OT as technological solutions that are difficult and expensive to upgrade. However, these arguments are unlikely to have much effect, as many industrial organizations do not adhere to even the simplest cybersecurity standards (such as changing default passwords), putting critical infrastructure operation at risk.

Ukraine is improving and implementing state policies for cybersecurity and advanced technologies. The Ministry of Digital Transformation presented a White Paper on regulating artificial intelligence (AI) in Ukraine. This step will help companies prepare for legislative regulation in this area and assist the state in integrating into the European Union (EU). The Cabinet of Ministers of Ukraine (CMU) approved the tasks of the National Informatization Program. To automate monitoring of the implementation of Ukraine's Cybersecurity Strategy, the National Cybersecurity Coordination Center (NCSCC) presented a new tool, the CyberTracker. The State Service for Special Communications and Information Protection (SSSCIP) approved requirements for information security auditors on critical infrastructure facilities and the procedure for certifying them, while Ukraine's first Certification Center for Information Technology and Cybersecurity began certifying specialists.

Ukraine is actively integrating into the European and Euro-Atlantic cybersecurity space, as building cyber resilience and countering russian federation threats is a joint task for Ukraine and EU countries. In June, the NCSCC became a partner of the Paris Cyber Summit, and Ukraine participated for the first time in the European Cybersecurity Exercise, Cyber Europe. The Ukrainian innovation platform Brave1, NATO, and the Defense Innovation Unit of the U.S. Department of Defense held the first NATO-Ukraine Defense Innovators Forum, where they discussed prospects for investing in Ukrainian defense tech and plans for cooperation in the defense technology sector.

In June, a ransomware attack targeted Synnovis, a clinical research company and a key partner of the United Kingdom (UK) National Health Service. The attackers, suspected to be affiliated with the russian group Qilin, demanded a $50 million ransom. However, active law enforcement response led to a reduction in their activity. The healthcare sector remains one of hackers' favorite targets, especially using ransomware like Knight, due to weak protection systems and a large volume of personal data. Amidst this, there is an ongoing active discussion about the necessity of completely banning ransom payments to criminals. However, some stakeholders express concern over the potential impact of such restrictions on their operations in the event of cyberattacks. In turn, criminals increasingly employ unconventional pressure methods, including physical impact on potential victims, as seen in the case of the UNC3944 group.

AI is becoming a constant element of security discussions. In May, it was a key topic at the RSA Conference 2024, and in June, Ukraine's Cybersecurity and Infrastructure Security Agency (CISA) conducted the first command-and-control exercises on AI threats. Researchers from the U.S. Center for Strategic and International Studies (CSIS) demonstrate how AI can influence decision-making in national security. CISA is also concerned about how AI might increase cyber threats in the chemical and biological sectors. Simultaneously, U.S. government agencies are exploring ways to use AI for greater security; for example, the U.S. Department of Defense is currently working on how to use AI for cyberattack response capabilities.

The increased activity of russian hackers against Ukraine's partner countries cannot be ignored. In June alone, they carried out several significant attacks. Notably, they attacked the website of a Spanish company that repairs Leopard tanks for Ukraine. They also interfered with satellite broadcasts, causing disruptions and even broadcasting russian military videos on a children's channel. russian hackers are constantly seeking new tools to access their victims, such as attacking TeamViewer. There is growing concern over russian hackers' willingness and readiness to interfere in election processes in the U.S. and Europe. Meanwhile, pro-Ukrainian hackers are delivering significant retaliatory blows. Several russian energy companies, IT firms, and government institutions have been affected by the Decoy Dog trojan. Supermarket operations across russia were disrupted, and the Sticky Werewolf group attacked a russian pharmaceutical company and a research institute specializing in microbiology and vaccine development. Additionally, there was a large-scale attack on major russian banks, making their services unavailable to some users.

1. CYBERSECURITY SITUATION IN UKRAINE

NCSCC BECAME A PARTNER FOR PARIS CYBER SUMMIT

The NCSCC became a partner of the Paris Cyber Summit, which took place June 3-5 in France. Participants discussed the latest achievements and challenges in the field of cybersecurity, particularly the impact of AI on cyber policy. The participants included government officials from European countries, industry experts, and business representatives.

UKRAINE PARTICIPATED IN THE EUROPEAN CYBER EXERCISES CYBER EUROPE FOR THE FIRST TIME

The main theme of the exercises was preparedness for large-scale cyberattacks on the EU's energy infrastructure. The 2-day intensive program, prepared by the European Union Agency for Cybersecurity (ENISA), brought together over 1,000 top specialists from the public and private sectors of 30 countries.

NCSCC and CISA representatives participated as observers. As a result of the visit to Athens, Greece, an agreement was reached on deepening cooperation with ENISA, including Ukraine's involvement in scenario development, planning, and participation in Cyber Europe 2026.

NCSCC PRESENTED CYBERTRACKER, A NEW TOOL FOR MONITORING UKRAINE'S CYBERSECURITY STRATEGY

On June 13, the NCSCC, Ministry of Digital Transformation, and SSSCIP conducted a training for specialists from relevant ministries, regional military administrations, and cybersecurity entities responsible for monitoring and reporting on the implementation of Ukraine's Cybersecurity Strategy. The event focused on automating the monitoring using the new CyberTracker portal. The portal will allow analyzing the impact of the strategy's activities, informing the public and international partners about the progress, and simplifying the reporting procedure on the strategy's implementation. The portal was developed with the support of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity.

MINISTRY OF DIGITAL TRANSFORMATION PRESENTED A WHITE PAPER ON AI REGULATION IN UKRAINE

The document will help companies understand how to prepare for future legislation in the AI field and create products that are safe for citizens, which will enable Ukrainian companies to become more competitive and enter international markets. For the government, it is an opportunity to integrate into the EU by synchronizing its AI legislation with European standards.

The tools the government will provide to companies include general and sectoral recommendations for different areas and aspects of AI use, from education and journalism to personal data processing. Besides recommendations, plans include creating voluntary codes of conduct, a legal assistance platform for businesses, a regulatory sandbox for testing high-tech products for compliance with future requirements, and more.

BRAVE1, NATO, AND THE DEFENSE INNOVATION UNIT HELD THE FIRST NATO-UKRAINE DEFENSE INNOVATORS FORUM

The NATO-Ukraine Defense Innovators Forum was the first joint event in the field of defense technologies organized by NATO, the U.S. Department of Defense's Defense Innovation Unit, the Brave1 cluster, the NATO-Ukraine Council, and the Ministry of National Defense of Poland. The forum brought together about 400 participants in defense technologies and innovations from over 15 countries.

The forum included panel discussions, a hackathon, and meetings to expand contacts between developers and investors. Key topics included developing defense innovations in Ukraine and NATO allies, challenges faced by developers on both sides, prospects for investment in Ukrainian defense tech, and plans for cooperation in the defense technology sector.

NATALIYA TKACHUK: BUILDING CYBER RESILIENCE AND REPELLING THE AGGRESSOR IS A SHARED TASK WITH EU COUNTRIES

NCSCC Secretary Nataliya Tkachuk participated in the European Dialogue on Internet Governance (EuroDig), which started on June 17 in Vilnius. The main theme of the event was «Balancing Innovation and Regulation.» During the panel discussion «One for All, All for One: The Role of Cooperation in Enhancing Cyber Resilience in Europe» participants discussed various aspects of cooperation to enhance European cyber resilience.

The NCSCC Secretary shared examples of Ukraine's international cooperation and public-private partnership cases. She emphasized that russia will continue its cyber aggression against both Ukraine and EU countries. Therefore, building cyber resilience and repelling the aggressor is a shared task for Ukraine and EU countries.

ANDRIY SYBIHA MET WITH DEPUTY SECRETARY FOR INFORMATION AND COMMUNICATIONS TECHNOLOGY OF THE PHILIPPINES JEFFREY IAN DY

On June 7, during the working visit of First Deputy Minister of Foreign Affairs of Ukraine Andriy Sybiha to the Republic of the Philippines, he met with the Deputy Secretary for Information and Communications Technology of the Philippines, Jeffrey Ian Dy. The parties discussed common challenges in cybersecurity and e-governance.

The Ukrainian side shared its achievements in using digital technologies in governance and service delivery to citizens, including the Diia platform, Prozorro, electronic banking services, and distance education. In the fight against cybercrime, Ukraine proposed signing a memorandum on information exchange between relevant agencies. The parties also discussed cooperation within multilateral cooperation mechanisms.

SSSCIP TOOK PART IN THE NICE CONFERENCE & EXPO

During his speech at the international NICE Conference & Expo in Dallas, Texas (USA), SSSCIP Deputy Head Oleksandr Potii noted that quality professional standards and an effective certification process for cybersecurity specialists are among the main preconditions for developing strong human resource potential in Ukraine.

The event was dedicated to building human resource potential in cybersecurity. During one of the specialized discussions at the event, Oleksandr Potii also shared Ukraine's experience in enhancing cyber resilience in areas where the SSSCIP is making efforts.

CYBERSECURITY AND COUNTERING RUSSIAN DISINFORMATION IN SPORTS: THE NATIONAL CYBERSECURITY CLUSTER HELD IN KYIV

On June 27, the 28th National Cybersecurity Cluster was held in Kyiv, «Red Card to Cyber Threats and Fakes: Challenges and Solutions for Youth and Sports.» The NCSCC organized the event in cooperation with the Ministry of Youth and Sports and CRDF Global in Ukraine, with support from the U.S. Department of State. Over 100 people attended, including representatives from the public and private sectors, sports associations, international organizations, and the public.

Participants discussed the importance of protecting the sports sector from cyber threats, especially in the context of increasing digitalization, and the importance of countering russian information operations in the sports context. Special attention was paid to popularizing cybersecurity among young people and engaging them in relevant educational programs.

CYBER POLICE MET WITH UKRAINIAN SCHOOLCHILDREN

Police officers in Chernihiv, Kirovohrad, Volyn, Zakarpattiya, and Zaporizhzhia oblasts informed students about common online threats, including various forms of cyberbullying, and explained the importance of cyber hygiene as an effective way to protect against these negative phenomena. Officers told the children about cyberbullying and warned them about other forms of online threats, including cyber grooming. Additionally, the police officers promoted the Brama project and the importance of adhering to cyber hygiene and protecting personal data, especially under martial law.

THE GOVERNMENT APPROVED THE TASKS OF THE NATIONAL INFORMATIZATION PROGRAM

This will allow the development of modern information infrastructure, implementing digital technologies, and strengthening of cybersecurity. Specifically, the National Informatization Program's tasks include implementing digital anti-corruption tools; creating modern information infrastructure; ensuring the effective functioning of the justice information system; and informatization in the fields of healthcare, education, and science.

Overall, the global task of the National Informatization Program is to continue digital transformation processes in the country and create a digital state. One of the key areas of the National Informatization Program is implementing measures of the State Anti-Corruption Program for 2023–2025.

SSSCIP PRESENTED NEW TECHNICAL SOLUTIONS TO PROTECT STATE INSTITUTIONS FROM DDOS ATTACKS

The SSSCIP presented new technical solutions to protect government institutions from distributed denial-of-service (DDoS) attacks to state representatives. SSSCIP representatives demonstrated the capabilities of the software and service support provided by Radware and Akamai Technologies, which are deployed in the State Cyber Protection Center. These solutions ensure effective detection and blocking of various types of cyber threats and extended traffic monitoring and analysis.

THE FIRST INFORMATION TECHNOLOGY AND CYBERSECURITY QUALIFICATION CENTER IN UKRAINE HAS STARTED CERTIFYING SPECIALISTS

On June 20, the SSSCIP opened the first Information Technology and Cybersecurity Qualification Center. Its goal is to implement a modern system of professional certification for cybersecurity specialists, which will align the knowledge, skills, and competencies of cybersecurity professionals with current market needs in Ukraine.

Specialists can now confirm their skills and competencies at the Qualification Center for two new professional standards in cybersecurity: Information Systems Security Developer and Network and Systems Security Administrator. The Qualification Center's future plans include expanding the accreditation list to nine more qualifications, including Information Security Management System Auditor and Cybersecurity Incident Response Specialist.

SSSCIP APPROVED REQUIREMENTS FOR INFORMATION SECURITY AUDITORS AT CRITICAL INFRASTRUCTURE FACILITIES

The SSSCIP approved requirements for information security auditors at critical infrastructure facilities and the procedure for certifying (or recertifying) them. This order was developed in accordance with CMU Resolution dated 24.03.2023 #257 «Some issues of conducting an independent information security audit at critical infrastructure facilities,» which establishes a set of requirements for individuals who plan to obtain the right to conduct information security audits at critical infrastructure facilities. Full text: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-30-04-2024-228-pro-zatverdzhennya-vimog-do-auditoriv-informaciinoyi-bezpeki-na-ob-yektakh-kritichnoyi-infrastrukturi-ta-poryadku-yikh-atestaciyi-pereatestaciyi.

SBU UNCOVERED BOT FARMS THAT HELPED RUSSIA SPREAD KREMLIN FAKES AND HACK UKRAINIAN SOLDIERS' PHONES

The Security Service of Ukraine (SBU) neutralized two bot farms operating in Zhytomyr and Dnipro. The individuals involved helped russian special services hack the phones of Ukrainian defenders and spread Kremlin propaganda.

In Zhytomyr, a woman was caught registering virtual numbers and anonymous accounts on Telegram for russian special services. She sold over 600 mobile numbers used to hack Ukrainian soldiers' phones through phishing emails.

In Dnipro, a man who registered nearly 15,000 fake accounts on social networks and messenger apps was detained. He sold them on darknet forums, where the main buyers were representatives of russia. Investigations are ongoing for both cases.

POLICE SHUT DOWN BOT FARM GENERATING PROFITS IN RUBLES FOR A 23-YEAR-OLD ODESA RESIDENT

The suspect is accused of unauthorized interference in the operation of electronic communication networks, committed in conspiracy with others. He faces up to five years in prison. From November 2022 to July 2023, the man illegally interfered with the operation of a Ukrainian mobile operator by changing the IMEI of SIM cards and renting them out to online virtual number services.

The perpetrator ensured the bot farm's operation and collaborated with russian platforms, receiving payment in rubles. Clients used anonymous numbers to create fake accounts, send phishing emails, and spread propaganda.

LAW ENFORCEMENT IN LVIV UNCOVERED TWO BROTHERS CREATING PHISHING SITES FOR SALE

As established by law enforcement, the suspects created phishing sites and malware designed for unauthorized interference with information (automated) systems, allowing access to citizens' personal data. The perpetrators were charged with committing a criminal offense, facing up to three years in prison.

POLICE UNCOVERED ACCOMPLICE OF RUSSIAN HACKERS WHO ATTACKED LEADING COMPANIES IN THE NETHERLANDS AND BELGIUM

Cyber police and National Police investigators identified a Kyiv resident who disguised a ransomware virus as safe files on behalf of a russian hacker group, which used the hidden program to interfere with the computer networks of a foreign company.

One russian hacker group used the Kyiv resident's services, paying him in cryptocurrency to disguise the Conti ransomware. At the end of 2021, the group infected a company's computer networks in the Netherlands and Belgium with the hidden malware, rendering them unusable. The hackers demanded a ransom for decrypting the computers.

During the investigation, cyber police established the individual's involvement with russian hacker groups LockBit and Conti. He faces up to 15 years in prison.

CERT-UA AND THE CYBER SECURITY CENTER OF THE UKRAINIAN ARMED FORCES, IDENTIFIED AND INVESTIGATED THE ACTIVITY OF THE UAC-0020 (VERMIN) GROUP TARGETING UKRAINE'S DEFENSE FORCES

Employees of law enforcement agencies from temporarily occupied Luhansk carry out the Vermin group's activity, the latest recorded in March 2022. This time, they used SPECTR malware to steal documents, files, passwords, and other information. The legitimate synchronization functionality of the SyncThing software was also used.

The Government Computer Emergency Response Team Ukraine (CERT-UA) tracked this group's activity under the identifier UAC-0020. More details about the malicious activity and threat indicators of UAC-0020 can be found in the CERT-UA article.

HACKERS ATTACKING GOVERNMENT AND DEFENSE SECTOR EMPLOYEES THROUGH SIGNAL

CERT-UA warned about targeted cyberattacks against government officials, military personnel, and representatives of Ukraine's defense enterprises. The attackers use the DarkCrystal RAT malware, distributing it via the popular messenger Signal.

To increase the credibility of such messages, a compromised account of someone from the victim's contact list or shared groups may be used. CERT-UA tracks this activity under the identifier UAC-0200. More details can be found in the CERT-UA article.

2. THE FIRST WORLD CYBER WAR

DENMARK RAISES THREAT LEVEL OF POTENTIAL DESTRUCTIVE CYBERATTACKS TO 3 ON A 5-LEVEL SCALE

On June 4, the Danish Center for Cybersecurity (CFCS) raised its threat level assessment of potential destructive cyberattacks against Denmark from «low» to «medium» due to the increasing threats from russia. According to the CFCS, a «medium» level, or three on the 5-level scale, indicates the presence of one or more actors who have the intent and capability to carry out attacks or malicious activities, but there are no signs or specific plans for such activities.

DUTCH INTELLIGENCE SAYS CHINESE CYBER ESPIONAGE WAS MORE EXTENSIVE THAN INITIALLY BELIEVED

On June 11, the Dutch Military Intelligence and Security Service (MIVD) stated that it continues to investigate the incident of Chinese cyber espionage against the Netherlands. Currently, the MIVD believes that the campaign was more extensive than initially thought, targeting Western governments and defense companies in general. The MIVD said that the state-supported Chinese hacker group behind the hacking of the Dutch Ministry of Defense in 2023 attacked at least 20,000 victims worldwide over several months.

ICC PROBES CYBERATTACKS IN UKRAINE AS POSSIBLE WAR CRIMES

On June 15, it was revealed that International Criminal Court (ICC) prosecutors are investigating alleged russian cyberattacks on Ukrainian civilian infrastructure as possible war crimes. The investigation is examining attacks on infrastructure that endangered lives by disrupting electricity and water supplies, interrupting connections to emergency services, or disabling mobile data services that transmit air raid warnings.

RUSSIAN ENERGY COMPANIES, IT FIRMS, AND STATE INSTITUTIONS HIT BY DECOY DOG TROJAN

On June 4, The Hacker News reported that russian companies and institutions had suffered cyberattacks that delivered a version of the Decoy Dog malware for Windows. The cybersecurity company Positive Technologies is tracking an activity cluster called Operation Lahat, attributing it to the advanced persistent threat (APT) group HellHounds, which compromises chosen organizations and embeds itself in their networks, remaining unnoticed for years. There is evidence that the perpetrator has been targeting russian companies since at least 2021, with the malware's development starting as early as November 2019.

UKRAINIAN CYBER ACTIVISTS ATTACKED RUSSIAN COMPANIES SUPPORTING THE WAR

Activists from the BO_Team cyber community and specialists from the Ukrainian Ministry of Defense Main Intelligence Directorate (HUR) continue to attack targets in the aggressor state, causing significant damage. They destroy important data and equipment, paralyze enterprises' operations, and create chaos and bad moods in russia.

In June, they reported destroying over 100 terabytes of data of OrbitSoft, a software developer that fulfilled contracts for the russian occupation army. They also destroyed all data on eight servers of Orient Systems, which developed and supplied navigation equipment. This company cooperated with russian manufacturers of military equipment, including unmanned aerial vehicles (UAVs). In addition, all data on 19 servers of internet providers Linktelecom NN and Access Telecom in Nizhny Novgorod were destroyed. All of these providers' subscribers received letters reminding them of the inevitable retribution for the war against Ukraine.

RUSSIAN HACKERS ATTACKED SPANISH COMPANY REPAIRING LEOPARD TANKS FOR UKRAINECOY DOG TROJAN

On June 5, the Spanish company Santa Barbara Systems, part of General Dynamics, which repairs Leopard tanks for supply to Ukraine, suffered a cyberattack on its website. The hacker group NoName, known for its activities against countries supporting Ukraine, claimed responsibility for the attack in a message on Telegram.

CYBERATTACK DISRUPTED SUPERMARKET OPERATIONS ACROSS RUSSIA

In early June, a popular russian retail chain with over 1,000 stores across the country suffered a cyberattack that disrupted its operations for several days. The supermarket chain Verny confirmed the breach on June 3, adding that it was still working on fully restoring operations. Unknown attackers hacked into the company's website and mobile app. Reports indicate that Verny supermarkets were unable to process bank cards or accept and deliver online orders due to the attack.

BELARUSIAN HACKERS ATTACKED UKRAINE'S MINISTRY OF DEFENSE IN NEW ESPIONAGE CAMPAIGN

On June 4, the cybersecurity firm Cyble reported that state-sponsored Belarusian hackers attacked Ukraine's Ministry of Defense and a military base as part of a new espionage operation. Researchers attributed the attacks to the Ghostwriter group, linked to Belarus and known for its attacks on Ukraine, Lithuania, Latvia, and Poland. During the latest campaign observed by Cyble researchers in April, hackers sent phishing emails to their targets with attachments containing drone images and a malicious Microsoft Excel spreadsheet.

RUSSIAN HACKTIVISTS PROMISE MASS ATTACKS AGAINST EU ELECTIONS

On June 7, The Register reported that the russian hacktivist group NoName57(16), along with seven other groups, threatened to attack European internet infrastructure at the start of the EU elections as revenge for European Parliament sanctions and so-called «russophobia.» While specific plans were not detailed, DDoS attacks are expected, a common tactic used by NoName and allied groups such as KillNet and Anonymous russia.

Dutch political parties reported DDoS attacks before polling stations closed on June 6, and HackNet claimed responsibility. Mandiant's chief analyst John Hultquist advised not to overstate the importance of these attacks, emphasizing that their goal is to create doubts about election security rather than cause significant harm.

WAR VIDEOS ON CHILDREN'S CHANNEL: RUSSIA INTERFERES WITH EUROPEAN BROADCASTS

On June 7, Ekonomichna Pravda, citing Bloomberg, reported that since mid-March, at least three satellites of the French operator Eutelsat SA had suffered significant interference from russia. Disruptions on these TV channels lasted until the end of May. In two cases, on March 28 and April 17, the interference replaced the program of Walt Disney Co.'s BabyTV children's entertainment channel with russian military videos. As a result, the Dutch cable operator Ziggo removed BabyTV from its viewing offer.

STICKY WEREWOLF EXPANDS CYBERATTACK TARGETS IN RUSSIA AND BELARUS

On June 6, cybersecurity researchers from Morphisec disclosed details of a threat known as Sticky Werewolf, linked to cyberattacks on organizations in russia and Belarus. Phishing attacks targeted a pharmaceutical company, a russian microbiology and vaccine development research institute, and the aviation sector, expanding beyond their initial focus on state organizations, according to the Morphisec report.

SWITZERLAND NOTES INCREASED CYBERATTACKS AHEAD OF UKRAINE PEACE SUMMIT

On June 11, Swiss President Viola Amherd stated at a press conference that cyberattacks on her country had increased in recent weeks but provided no further details. Foreign Minister Ignazio Cassis said there is a clear «interest» in disrupting the Peace Summit. Officials did not attribute the incidents to any specific country, but russia is likely a suspect, as it was not invited and has repeatedly called the summit «senseless and harmful,» based on the peace proposals of Ukrainian President Volodymyr Zelenskyy.

EU POLITICAL PARTIES TARGETED BY DDOS ATTACKS AS ELECTIONS BEGIN – CLOUDFLARE

On the day before and day of the European Parliament elections in the Netherlands, Cloudflare observed DDoS attacks targeting several internet resources related to elections or politics. On June 6, several websites of political parties in the Netherlands suffered cyberattacks, which the pro-russian hacker group HackNeT claimed responsibility for.

FRENCH DIPLOMATIC ENTITIES TARGETED IN CYBERATTACKS LINKED TO RUSSIA

According to the French information security agency ANSSI, state-sponsored actors linked to russia conducted targeted cyberattacks on French diplomatic entities. These attacks are attributed to a group known as Midnight Blizzard (formerly Nobelium), also tracked as APT29, BlueBravo, Cloaked Ursa, Cozy Bear, and The Dukes. ANSSI differentiates them from another cluster, Dark Halo, responsible for the SolarWinds attack in 2020.

Nobelium is known for using compromised legitimate email accounts for phishing campaigns against diplomatic entities. This type of attack is also tracked under the name Diplomatic Orbiter. In May 2023, European embassies in Kyiv, including the French embassy, suffered phishing attacks with emails titled «Diplomatic Car for Sale.» Another attack on the French embassy in Romania was unsuccessful.

U.S. BANS SALE OF KASPERSKY ANTI-VIRUS SOFTWARE OVER RUSSIA TIES

On June 21, The Washington Post reported that the Biden administration banned Kaspersky Lab from distributing anti-virus software and cybersecurity products in the U.S., citing a national security threat. Commerce Secretary Gina Raimondo stated that this decision was made after thorough investigation and reflects concerns that russia could use Kaspersky to access Americans' personal information and weaponize it. Kaspersky denied these claims, attributing the ban to geopolitical tensions. The ban goes into effect on September 29, giving users time to find alternatives but leaving them with cybersecurity risks if they continue using Kaspersky products. This move extends previous restrictions and reflects growing U.S. scrutiny of foreign-owned tech companies over data privacy and security issues.

A day after the Commerce Department banned the russian company, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) imposed sanctions on a dozen individuals holding executive and senior management positions at Kaspersky Lab.

RUSSIAN HACKERS ATTACKED TEAMVIEWER

On June 27, the remote desktop software producer TeamViewer announced that it had detected a «breach» in its corporate IT network. It was later revealed that Cozy Bear (also known as APT29 and Midnight Blizzard) were suspected in the attack, which was organized through an employee's account. TeamViewer assures its users that the incident only affected its corporate IT network, which is separate from the production environment and the TeamViewer connection platform.

UKRAINE'S IT ARMY DISRUPTS KEY RUSSIAN ONLINE SERVICES

On June 21, Ukrainian hackers carried out a large-scale attack on major russian banks such as Sberbank and VTB, making their services unavailable to some users. Ukrainian cyber specialists conducted a massive operation against russia's payment system Mir and other financial, communication, and electronic platforms of the aggressor country, according to the Ministry of Digital Transformation on social media.

EXCOBALT CYBER GANG TARGETS RUSSIAN SECTORS WITH NEW GORED BACKDOOR

On June 22, The Hacker News reported that russian organizations have become targets of the cybercriminal gang ExCobalt, which uses a previously unknown Golang-based backdoor called GoRed. According to cybersecurity company Sekoia, ExCobalt has been targeting russian sectors with this new backdoor since early 2023. GoRed is used to maintain long-term access to compromised systems and execute commands remotely, demonstrating the gang's evolving tactics and focus on high-value targets within russia.

CITIZEN OF RUSSIA ACCUSED OF CYBERATTACKS ON UKRAINE BEFORE THE 2022 FULL-SCALE INVASION

On June 27, a 22-year-old russian citizen was indicted in the U.S. for allegedly participating in organizing cyberattacks against Ukraine and its allies in the days leading up to russia's full-scale military invasion of Ukraine in early 2022. The defendant, Amin Stigal, is believed to be associated with the Main Directorate of the General Staff of the Armed Forces of the russian federation (GRU). He remains at large. If convicted, he faces a maximum sentence of five years in prison.

CRIMEA WARNS OF INTERNET DISRUPTIONS DUE TO DDOS ATTACKS ON LOCAL TELECOM OPERATORS

On June 27, local authorities in Crimea warned of internet disruptions due to DDoS attacks targeting telecommunications providers. «Massive» DDoS attacks were launched against Crimean telecom companies on June 26 and continued for at least two days. In Sevastopol, the attacks primarily targeted the local internet provider Miranda Media, which is connected to the russian national telecom operator Rostelecom.

HOW ISOLATED IS THE RUSSIAN INTERNET? CONSEQUENCES OF THE WAR IN UKRAINE

Digital sovereignty is a global concept that involves control over the internet and its infrastructure, and russia has taken significant steps to achieve this over the past two decades. Despite attempts to disconnect from the global internet, russia's internet, unlike China's, remains decentralized and difficult to fully isolate. The increase in isolation cases, combined with sanctions and internal censorship following the full-scale invasion of Ukraine, has weakened russia's internet resilience.

Many tech companies have ceased operations in russia, further degrading its internet reliability. Long-standing censorship in russia has intensified, blocking many social networks and news sites, banning virtual private network (VPN) services, and leading to the exit of international hosting companies. This mutual isolation is compounded by EU sanctions against russian media and reciprocal geoblocking efforts by russia and Western countries.