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

May 2024

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

CONTENT

ACRONYMS 5
KEY TENDESES 6
1. Cybersecurity situation in Ukraine 10
NCSCC enhances cooperation with the EU Advisory Mission 10
With NCSCC support, the first international scientific and practical conference on cyberdiplomacy was held in Kyiv 10
Estonia to provide Ukraine with means to enhance capabilities in cyberspace within the IT Coalition 10
Nataliya Tkachuk participated in the Annual Asian Leadership Conference 11
Serhii Demediuk called for forming a unified conceptual framework for cyber defense at the international level 11
Deputy Minister of Foreign Affairs Anton Demyokhin paid a working visit to the United States of America 11
CERT-UA specialists participated in the RSA 2024 Cybersecurity Conference 12
Ukraine and Poland signed a memorandum on cooperation in digitalization 12
SBU, the FBI, and EU partners uncovered an international network of hackers developing ransomware for attacks on American and European companies 12
Ministry of Defense of Ukraine began cooperating with the Defense Builder Accelerator Program (DBA) 12
Digital Power Summit 2024 held in Ukraine 13
SSSCIP specialists participated in the 12th EU MITRE ATT&CK Community Workshops 13
Cyberpolice officer participates in the Payments and Credit Security Forum 13
SSSCIP initiates experimental project on information protection system compliance 14
Nationwide information campaign on payment security launched in Ukraine: #CyberSecurityFinance 14
CERT-UA prepared analytical report on «russian Cyber Operations H2 2023» 14
CERT-UA warns about increased cyberattacks against accountants 14
CERT-UA warns about targeted attacks using SuperOps RMM remote access program 15
Cyberpolice expose fraudster who scammed a military service member 15
2. THE FIRST WORLD CYBER WAR 16
UK and allies expose leader of russian cybercrime group LockBit 16
Powerful DDoS attack on Monobank 16
In 2024, the russian cyber threat will demonstrate a new level of aggression and maneuverability – U.S. National Cyber Director H. Coker 16
North Atlantic Council statement on russia's recent hybrid activities 16
Kosovo government faces kremlin-supported cyberattacks 17
russian group FlyingYeti attempts to attack Ukrainian citizens 17
Ukrainian and russian hackers exchange attacks on television on May 9 17
kremlin-backed APT28 targets Polish institutions in malware campaign 17
russian hackers gained access to the website of the Polish Press Agency (PAP) and posted a fake article 17

russia increasingly obstructs Ukraine's use of Starlink services 18
File not found: russia is hacking evidence of its war crimes 18
«russian» hackers defaced hundreds of local British news websites 18
russian actors use legitimate services for multi-malware attack 18
BlueDelta from gru targets key networks in Europe in multi-phase espionage campaigns 19

ACRONYMS

AI	Artificial Intelligence
AMOS	Atomic macOS Stealer
APT	Advanced Persistent Threat
C2	Command and Control
CDTO	Chief Digital Transformation Officer
CERT-UA	Government Computer Emergency Response Team Ukraine
CERT.PL	Government Computer Emergency Response Team Polska
CIPS	Comprehensive Information Protection System
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMU	Cabinet of Ministers of Ukraine
CRDF Global	Civil Research and Development Fund (U.S.)
DBA	Defense Builder Accelerator Program
DDoS	Distributed Denial-of-Service
DHS	Department of Homeland Security (U.S.)
EPA	Environmental Protection Agency (U.S.)
EU	European Union
EUAM	European Union Advisory Mission
FBI	Federal Bureau of Investigation (U.S.)
GAO	Government Accountability Office (U.S.)
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
ICC	International Criminal Court
IT	Information Technology
MB	Megabyte
MISP	Malware Information and Threat Sharing Platform
NATO	North Atlantic Treaty Organization
NBU	National Bank of Ukraine
NCSCC	National Cybersecurity Coordination Center
NCSC	National Cyber Security Centre (UK)
NGO	Non-Governmental Organization
NIST	National Institute of Standards and Technology (U.S. Department of Commerce)
NSDC	National Security and Defense Council of Ukraine
ONCD	Office of the National Cyber Director (U.S.)
PAP	Polish Press Agency
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
UN	United Nations

KEY TENDESES

In early May, the U.S. Department of State released its International Cyberspace and Digital Policy Strategy, aiming to curb the digital influence of russia and China in developing countries and make these countries' attempts to interfere in elections less effective. The strategy seeks to engage more developing countries in a «positive vision» of cyberspace that rejects digital repression. As part of this effort, the U.S. will continue years of lobbying among allies and partners to avoid using key communication technologies and software created in autocratic countries like russia and China. Overall, it can be characterized as an attempt by the U.S. to create a coalition against China. In response, China released the report «Threats from the U.S. and Sabotage of Global Cyberspace Security and Development,» exposing the «hegemony and aggressive behavior of the United States in cyberspace».

This month, Ukraine focused on various aspects of international cooperation. At the First International Scientific and Practical Conference on Cyber Diplomacy, Foreign Minister Dmytro Kuleba emphasized that Ukraine is an integral part of the European and Euro-Atlantic security systems, with its experience countering russia and its reputation as an innovator. Deputy Secretary of the National Security and Defense Council (NSDC) Serhii Demediuk called for joint efforts to build strategies for predictably and continuously strengthen collective cyber resilience. Ukrainian representatives participated in several important international events, including the Asian Leadership Conference and RSA Conference 2024. As part of the IT coalition, Estonia will provide resources to strengthen Ukraine's cyber capabilities. Ukraine also began collaborating with Poland in digital technologies and innovations, IT industry development, artificial intelligence (AI), protection of critical information, and state registers.

The U.S. is starting to assess the effectiveness of President Biden's strategic cybersecurity directives. The U.S. Government Accountability Office (GAO) released the results of an assessment by government agencies of Executive Order 14028 "Improving the Nation's Cybersecurity", indicated that 49 out of 55 tasks (90%) were completed. Additionally, the U.S. government adopted an updated National Cybersecurity Strategy Implementation Plan, adding 31 new tasks. At the same time, the Office of the National Cyber Director (ONCD) assessed the effectiveness of the first Implementation Plan: about 90% of the tasks were implemented (33 out of 36 planned initiatives). Notably, the U.S. government has significantly increased oversight of the processes for implementing its strategic decisions, making assessment procedures more regular and public.

The human factor remains one of the key sources of cyber threats to organizations and their information systems, as evidenced by recent studies by Verizon and Proofpoint. Verizon survey respondents indicated that 68% of security breaches occurred due to non-malicious human factors, such as incidents related to insider errors or people falling for social engineering schemes. Proofpoint found similar statistics, with its study covering 1,600 Chief Information Security Officers (CISOs), 74% of whom indicated that human errors are the biggest cyber vulnerability for their organizations. The problem is broader than just training organizational staff and is related to the overall level of cyber awareness. Therefore, in May 2024, the Cybersecurity and Infrastructure Security Agency (CISA) launched its second nationwide cyber awareness program, targeting various audiences, with campaign information disseminated on all major platforms: television, radio, digital advertising, shopping centers, social media, and outdoor advertising.

The Secure by Design approach is gaining more importance in the public policies of leading nations. CISA actively promotes its Secure by Design pledge platform, a voluntary association of companies committed to adhering to Secure by Design principles, with 68 companies participating as of May. The United Kingdom (UK) is also preparing to implement this approach for market participants. According to Ollie Whitehouse, technical director of the UK's National Cyber Security Centre (NCSC), the current "thousands of patches" approach to cybersecurity (where software or technology developers address specific cybersecurity issues in their products) must completely change. Essentially, developer companies should have greater social responsibility towards their clients, especially among organizations with traditionally limited cybersecurity budgets, like non-governmental organizations (NGOs), schools, etc. Government agencies are also involved in enhancing the cybersecurity of socially important organizations: CISA, the U.S. Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI) published a guide for high-risk organizations, in collaboration with international partners.

AI development and its impact on cybersecurity is increasingly the focus of cybersecurity organizations and researchers. While China and the U.S. seek to invest more in AI research and start high-level dialogues on the issue, cybersecurity specialists are already facing challenges. For example, Unit42 cybersecurity specialists managed to train AI to create effective malware using a relevant database of initial data. The AI-created malware was not only effective but could also be quickly modified by AI, creating numerous variations of the malware core and adapting it for different platforms. Horizon3.ai specialists are already offering new AI-supported services to accelerate prioritizing cyber protection and vulnerability remediation in organizations' cybersecurity. AI is also becoming a subject of cyber espionage; in May, an unidentified advanced persistent threat (APT) group attacked American AI researchers trying to access their data.

In the U.S., debates continue regarding UnitedHealth and the devastating ransomware attack against the IT systems of its subsidiary, Change Healthcare. Following a series of investigations and Senate hearings, it was revealed that the company paid a $22 million ransom. Simultaneously, numerous deficiencies in the organization's cybersecurity policy, weak protection of client personal data, and inadequate staffing policies for cybersecurity top management were identified (i.e., the CISO had no experience in cybersecurity positions). The organization's total losses due to this incident have already exceeded $800 million and are estimated to reach $1 billion. The UnitedHealth case is likely to lead to stricter cybersecurity requirements across the U.S. healthcare sector. A similar situation may arise for the water supply sector; due to a series of successful cyberattacks over the past six months, U.S. Environmental Protection Agency (EPA) inspections revealed that over 70% of water supply systems do not fully comply with the Safe Drinking Water Act and have critical cybersecurity vulnerabilities.

Law enforcement agencies dealt another significant blow to the infrastructure of criminal organizations. In May, law enforcement agencies from 13 countries conducted Operation Endgame, which dismantled the criminal infrastructure of several malicious groups: IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee, and Trickbot. Ukrainian law enforcement actively participated in the operation, conducting most of the arrests and searches. Also in May, British, American, and Australian law enforcement identified the leader of the LockBit cybercrime group as russian federation citizen Dmitry Khoroshev. The U.S. Department of State has already offered a $10 million reward for information leading to his capture.

In terms of countering cyber threats, the Security Service of Ukraine (SBU), FBI, and law enforcement agencies from the UK and the European Union (EU) conducted a special operation in eight European countries, uncovering over 30 members of transnational hacker groups. Government Computer Emergency Response Team Ukraine (CERT-UA) specialists noted increased interest from enemy hackers in the Ukrainian telecommunications sector in the second half of 2023. Attacks on military personnel aimed at accessing, controlling, and collecting intelligence information from specialized situational awareness systems remain a strategic military goal for the enemy. CERT-UA also warned about cybercriminals using the legitimate remote management software SuperOps RMM to gain unauthorized access to Ukrainian organizations' information systems.

In May, there were several mirrored cyberattacks by pro-russian and pro-Ukrainian groups. On May 9, Ukrainian hackers managed to replace the signal from the May 9 parade with footage from the war in Ukraine on some russian TV channels. In a mirrored attack, russian hackers hacked the satellite signal of the Inter TV channel and broadcast the russian parade to Ukrainian viewers. russian hackers are increasingly targeting the information resources of Ukraine's international partners: APT28 targeted Polish institutions, unidentified russian hackers hacked the website of the Polish Press Agency (PAP) and posted a fake article aimed at worsening Ukrainian-Polish relations, and another successful russian hacker attack led to the hacking of hundreds of local British news websites.

1. CYBERSECURITY SITUATION IN UKRAINE

NCSCC ENHANCES COOPERATION WITH THE EU ADVISORY MISSION

On May 20, Oleksandr Lytvynenko, NSDC Secretary, met with Rolf Holmboe, Head of the European Union Advisory Mission (EUAM) to discuss supporting Ukraine's reform process toward EU membership and specific support for the NSDC and Ukraine's security architecture. Developing cybersecurity capabilities is a significant area of EUAM support, with a priority on practical interaction with the National Cybersecurity Coordination Center (NCSCC) to effectively build Ukraine's national cybersecurity system and share experiences with EU countries.

WITH NCSCC SUPPORT, THE FIRST INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE ON CYBERDIPLOMACY WAS HELD IN KYIV

Minister of Foreign Affairs Dmytro Kuleba emphasized in his address that modern Ukraine has already established itself as an innovator and has a chance to take a leading position in global cyberspace. «Undoubtedly, this makes our country an integral part of the European and Euro-Atlantic security systems.» NSDC Deputy Secretary Serhii Demediuk noted that recent official statements by NATO and EU partners attributing cyberattacks to russian hackers indicate the international community's awareness of the crimes committed by the russian federation against their countries and populations. «It is now necessary to jointly build strategies to predictably and continuously strengthen collective cyber resilience, which is an important step in ensuring security at both national and international levels,» he said. During the event, speakers identified cyberdiplomacy as an important tool for maintaining stability in cyberspace, discussed the need to protect it, and examined the role of AI in cyberdiplomacy and its impact on strategic decision-making in international relations. Special attention was paid to countering russian disinformation and information warfare.

ESTONIA TO PROVIDE UKRAINE WITH MEANS TO ENHANCE CAPABILITIES IN CYBERSPACE WITHIN THE IT COALITION

Ukraine's Deputy Minister of Defense Kateryna Chernohorenko met with Deputy Commander of the Cyber Command of the Estonian Defense Forces Mihkel Tikk and Head of the Cyber Policy Department and Coordinator of the IT Coalition from the Estonian Ministry of Defense Laura Oolup in Kyiv to discuss further cooperation on projects within the coalition. During the visit, the Estonian delegation held meetings with cyber experts from the Ministry of Defense of Ukraine and the Armed Forces of Ukraine. The partners particularly noted the professionalism of Ukrainian experts and confirmed their readiness to continue providing expert assistance on cybersecurity issues.

NATALIYA TKACHUK PARTICIPATED IN THE ANNUAL ASIAN LEADERSHIP CONFERENCE

Head of the NSDC Staff Information Security and Cybersecurity Service and NCSCC Secretary Nataliya Tkachuk participated in the Asian Leadership Conference held May 22-23 in Seoul. She spoke about Ukraine's achievements in building a national cybersecurity system, shared unique experiences in countering russian cyberattacks as part of the full-scale military invasion, and emphasized the importance of international support for Ukraine and the need to unite efforts among states to counter cyber threats. «Ukraine and South Korea have much in common: the Koreans lived through the bitter experience of war, which Ukraine is now going through, but managed to rebuild the country, turning it into one of the leaders in the Asian region in advanced technologies and cybersecurity. And this is an inspiring example for us. The same goal is set for our country, and Ukraine already has positive achievements,» emphasized the NCSCC Secretary.

SERHII DEMEDIUK CALLED FOR FORMING A UNIFIED CONCEPTUAL FRAMEWORK FOR CYBER DEFENSE AT THE INTERNATIONAL LEVEL

During a meeting of the National Cybersecurity Cluster on May 30, NSDC Deputy Secretary Serhii Demediuk emphasized that unified terminology of key cybersecurity concepts should be formed at the international level. «We need to form unified terminology of key cybersecurity concepts. russian hackers openly demonstrate their attacks on critical infrastructure facilities of foreign states, interfere in internal political processes. And the world, unfortunately, remains silent. So now we need to initiate processes to form a certain ideology of cyber defense during the war.» NCSCC Secretary Nataliya Tkachuk emphasized the need to build a transparent and effective national regulatory framework, including for conducting cyber operations. The participants also discussed issues of war crimes in cyberspace, including modern legal approaches and gaps, mechanisms for international deterrence and response to military actions in cyberspace, and key needs and solutions in the cybersecurity education and science sector.

DEPUTY MINISTER OF FOREIGN AFFAIRS ANTON DEMYOKHIN PAID A WORKING VISIT TO THE UNITED STATES OF AMERICA

In May, Deputy Minister of Foreign Affairs for Digital Development, Digital Transformations, and Digitalization Anton Demyokhin paid a working visit to the USA. Speaking at the RSA 2024 cybersecurity conference in San Francisco, he emphasized that Ukraine is at the epicenter of a major war both in the physical and cyber space, which requires maximum coverage on the largest global platforms. He also participated in the United Nations (UN) Global Ministerial Roundtable on strengthening cybersecurity capabilities, and held a number of bilateral and multilateral meetings with foreign partners from the public, private, and NGO sectors. The Ukrainian diplomat also held bilateral meetings with high-ranking officials from Singapore, the USA, and representatives of the UN and Civil Research and Development Fund (CRDF Global).

CERT-UA SPECIALISTS PARTICIPATED IN THE RSA 2024 CYBERSECURITY CONFERENCE

CERT-UA specialist Nazar Tymoshyk shared with the global expert community Ukraine's advanced experience in countering russia's aggression in cyberspace. In a panel discussion on the evolution of cyber threats from russia during the war, speakers discussed new trends and methods used by enemy hackers. He urged conference participants to use Ukraine's experience to identify vulnerabilities in their organizations to similar threats and develop strategies to counter and protect digital resources.

UKRAINE AND POLAND SIGNED A MEMORANDUM ON COOPERATION IN DIGITALIZATION

Deputy Prime Minister for Innovation Development, Education, Science, and Technology – Minister of Digital Transformation Mykhailo Fedorov and Deputy Prime Minister – Minister of Digitalization of Poland Krzysztof Gawkowski signed a memorandum on cooperation in digitalization. The focus of the joint work between Poland and Ukraine is cooperation in digital technologies and innovations, IT industry development, AI, e-government, developing Diia and mObywatel, etc. The Deputy Prime Ministers also discussed support in protecting critical information and state registers.

SBU, THE FBI, AND EU PARTNERS UNCOVERED AN INTERNATIONAL NETWORK OF HACKERS DEVELOPING RANSOMWARE FOR ATTACKS ON AMERICAN AND EUROPEAN COMPANIES

The SBU, FBI, and UK and EU law enforcement agencies conducted a large-scale special operation in eight European countries. As a result of the joint actions, over 30 members of transnational hacker groups involved in developing and distributing malicious software were exposed, including Pikabot, System BC, Bumblebee, Smokeloader, and IcedID. According to international investigation materials, the perpetrators "hacked" networks of well-known companies and then sold access to these networks to other hackers. Among them were russian groups BlackBasta, Revil, and Conti. The investigators documented dozens of extortion cases from Western corporations for a total amount of several tens of millions of dollars. Law enforcement officers in eight EU and North American countries seized over 90 servers and blocked over 1,000 domains used by hackers.

MINISTRY OF DEFENSE OF UKRAINE BEGAN COOPERATING WITH THE DEFENSE BUILDER ACCELERATOR PROGRAM (DBA)

The goal of the cooperation is to jointly assist developers in creating technological solutions for the needs of the Defense Forces and quickly delivering them to the front line. As part of DBA, up to 15 defense startups will create a team management system, formalize the legal and financial structure, and attract investments more effectively over four months. Participants will also have access to testing at the training ground and receive quick feedback on the application of their developments from the battlefield. The program will involve defense technology developers who already have a minimally viable product or prototype in the areas of unmanned aerial vehicles (UAVs), ground and water robotic systems, cybersecurity, sensors, etc.

DIGITAL POWER SUMMIT 2024 HELD IN UKRAINE

During the forum, regional administrations' chief digital transformation officers (CDTOs) and community digital leaders communicated with government representatives, discussing priority projects for 2024 and digital solutions that can be initiated in their communities and regions. Key topics included digital tools in education, healthcare, social and financial sectors, digital economy and digital services, cybersecurity and cyber resilience, human capital development, state programs for this, and Estonia's experience in small towns' digital transformation.

SSSCIP SPECIALISTS PARTICIPATED IN THE 12TH EU MITRE ATT&CK COMMUNITY WORKSHOPS

State Service of Special Communications and Information Protection (SSSCIP) specialists participated in the 12th EU MITRE ATT&CK Community Workshops, held on May 17. Ukrainian cyber defenders performed online on the same stage with experts from the European Commission, MITRE Corporation, Belgium's Cybersecurity Center, and Luxembourg's Cyber Threat Response Center. These centers have founded and actively developed the Malware Information and Threat Sharing platform (MISP), which is the de facto standard for sharing cyberattack indicators both in Ukraine and the EU. Participation in this conference also provided an opportunity for the SSSCIP to share experiences with other cybersecurity specialists worldwide, learn about the latest trends in cyber threats and countermeasures, and improve their skills in using MITRE ATT&CK for Ukraine's cyber defense.

CYBERPOLICE OFFICER PARTICIPATES IN THE PAYMENTS AND CREDIT SECURITY FORUM

During his speech at the Payments and Credit Security Forum, Colonel Oleksandr Ulyanenkov, a specialist from the Cyberpolice Department, highlighted the importance of developing information exchange mechanisms between banking and payment institutions for effectively combating fraud. «Implementing new technological solutions demonstrates a commitment to innovation and continuous improvement in combating cybercrime,» he said. At the forum, delegates from 39 organizations discussed the interaction between banking and payment institutions based on an updated information exchange system between the Cyber Police Department, banking organizations, and EMA.

SSSCIP INITIATES EXPERIMENTAL PROJECT ON INFORMATION PROTECTION SYSTEM COMPLIANCE

The Cabinet of Ministers of Ukraine (CMU) adopted the resolution «On the implementation of an experimental project on the declaration of compliance for comprehensive information protection systems in information, electronic communication, and information-communication systems, created using security profiles.» The SSSCIP will coordinate the project, which aims to modernize the processes of implementing a comprehensive information protection system (CIPS) using the best global security standards, particularly NIST 800-53 (USA). After the experiment, the SSSCIP will report the results to the Government and propose amendments to legislative and other regulatory acts to enhance the protection of state information resources and adapt systems to new cyber threats. The project is set to last up to two years.

NATIONWIDE INFORMATION CAMPAIGN ON PAYMENT SECURITY LAUNCHED IN UKRAINE: #CYBERSECURITYFINANCE

Starting May 30, the National Bank of Ukraine (NBU) and SSSCIP launched a nationwide information campaign on payment security, #CyberSecurityFinance. The campaign aims to improve citizens' awareness of payment security and develop skills for protecting financial data in the virtual space. The information campaign will run until the end of September 2024 in all regions of Ukraine. As part of the campaign, the NBU created a special webpage, «Cybersecurity of Finance», providing detailed information about the campaign and rules for behavior in the virtual space.

CERT-UA PREPARED ANALYTICAL REPORT ON «RUSSIAN CYBER OPERATIONS H2 2023»

CERT-UA specialists prepared the analytical report «russian Cyber Operations H2 2023» based on a comprehensive analysis of cyber threats detected during the second half of 2023, revealing new trends in the behavior of hostile hackers. Among the trends in the second half of 2023 is the increased interest of hostile hackers in the Ukrainian telecommunications sector, which can be considered an escalation in attempts to maintain initiative and presence in Ukrainian information infrastructure facilities.

Read more in the analytical report «russian Cyber Operations H2 2023» in UA and EN

CERT-UA WARNS ABOUT INCREASED CYBERATTACKS AGAINST ACCOUNTANTS

CERT-UA warned about a significant increase in cyberattacks related to the activities of the financially motivated group UAC-0006. Since May 20, specialists have recorded two large-scale campaigns distributing the malicious software SMOKELOADER. Currently, the UAC-0006 botnet comprises several hundred infected computers. There is a high probability that the attackers will soon activate fraudulent schemes using remote banking services.

CERT-UA WARNS ABOUT TARGETED ATTACKS USING SUPEROPS RMM REMOTE ACCESS PROGRAM

CERT-UA warned about cybercriminals using the legitimate SuperOps RMM remote management program to gain unauthorized access to the information systems of Ukrainian organizations. Cyberattacks were recorded and analyzed, where victims received emails with a link to Dropbox containing an executable file (.SCR) approximately 33 MB in size. Running this file on the victim's computer results in downloading, decoding, and executing malicious Python code, which in turn launches the legitimate SuperOps RMM program, thus providing the attackers with unauthorized remote access to the victim's computer. The cyberattacks have been carried out since February-March 2024 and have a fairly wide geographical scope. The described cluster of cyber threats is tracked under the identifier UAC-0188.

CYBERPOLICE EXPOSE FRAUDSTER WHO SCAMMED A MILITARY SERVICE MEMBER

A cybercriminal gained access to a military service member's bank account and embezzled his money. The suspect has been charged and faces a prison sentence of 5-8 years. The investigation is ongoing and the police are also identifying other potential victims.

2. THE FIRST WORLD CYBER WAR

UK AND ALLIES EXPOSE LEADER OF RUSSIAN CYBERCRIME GROUP LOCKBIT

On May 7, the UK, U.S., and Australia exposed and imposed sanctions on Dmitry Khorshev, the russian leader of the cybercrime group LockBit. His assets will be frozen, and he will be banned from travel. Additionally, a $10 million reward has been announced for information leading to his arrest.

POWERFUL DDOS ATTACK ON MONOBANK

On May 1, the Monobank app experienced access issues. The next day, co-founder Oleh Gorokhovsky reported that the bank had suffered a powerful distributed denial of service (DDoS) attack.

IN 2024, THE RUSSIAN CYBER THREAT WILL DEMONSTRATE A NEW LEVEL OF AGGRESSION AND MANEUVERABILITY – U.S. NATIONAL CYBER DIRECTOR H. COKER

On May 14, U.S. National Cyber Director Harry Coker emphasized the importance of digital solidarity in cybersecurity as threats grow more serious, speaking at CYBERUK 2024. He cited Ukraine as an example, successfully resisting russian cyberattacks on its critical infrastructure since 2022. However, in 2024, russian cyber threats show new levels of aggression and maneuverability, making network and communication security critical for Ukraine's success on the battlefield.

NORTH ATLANTIC COUNCIL STATEMENT ON RUSSIA'S RECENT HYBRID ACTIVITIES

In early May, NATO and the EU raised alarms about russian hackers and hybrid activities affecting at least seven European countries. The actions included sabotage, violence, cyber interference, disinformation campaigns, and other hybrid operations in Czechia, Estonia, Germany, Latvia, Lithuania, Poland, and the UK. On May 2, NATO issued a statement affirming that russia's actions will not deter Alliance members from supporting Ukraine. «We condemn russia's behavior,» the statement said, adding, «We will act individually and collectively to counter these actions and continue to coordinate our efforts closely.»

KOSOVO GOVERNMENT FACES KREMLIN-SUPPORTED CYBERATTACKS

Recently, russian hackers attacked government websites in Kosovo. As of May 10, several websites were temporarily unavailable due to a widespread denial-of-service incident. «The attack was carried out by russian hackers in retaliation for our support of Ukraine with military equipment,» a government spokesperson told local media.

RUSSIAN GROUP FLYINGYETI ATTEMPTS TO ATTACK UKRAINIAN CITIZENS

On May 31, the security team of Cloudflare reported that it had thwarted a large-scale attack by the russian group FlyingYeti against Ukrainian users. Traditionally targeting Ukraine's defense forces, this time the group's focus was on citizens relying on social welfare payments. The phishing attack, planned since January 2024, involved a phishing site on GitHub and Cloudflare Worker resources.

UKRAINIAN AND RUSSIAN HACKERS EXCHANGE ATTACKS ON TELEVISION ON MAY 9

On May 9, during Victory Day celebrations, which is one of the biggest propaganda holidays in the russian federation, russian outlets reported that unknown hackers had breached the broadcast of the provider Ufanet in Bashkortostan and Orenburg, Omsk, and Irkutsk regions, showing footage related to the war in Ukraine instead of the parade on red square. In response, russians hacked the satellite broadcast of the StarLightMedia and Inter channels in Ukraine, streaming the moscow parade on red square.

KREMLIN-BACKED APT28 TARGETS POLISH INSTITUTIONS IN MALWARE CAMPAIGN

On May 8, the Government Computer Emergency Response Team Polska (CERT.PL) reported observing a large-scale malware campaign targeting Polish government institutions. Based on technical indicators and similarities to previously described attacks (e.g., on Ukrainian organizations), the campaign can be linked to APT28, which is associated with the Main Directorate of the General Staff of the Armed Forces of the russian federation (gru). The aim of the attack was information gathering.

RUSSIAN HACKERS GAINED ACCESS TO THE WEBSITE OF THE POLISH PRESS AGENCY (PAP) AND POSTED A FAKE ARTICLE

On May 28, an article appeared on the PAP website claiming that Polish citizens would be mobilized to fight in Ukraine. The article stated that Tusk planned to announce a partial military mobilization on July 1: «200,000 Polish citizens, both former military and regular civilians, will be called up for mandatory military service. All conscripts will be sent to Ukraine,» the article said. PAP removed the article a few minutes after it was published, adding that «the source of the text is not the Polish Press Agency.» The article then reappeared and was again removed. On May 31, the Polish government stated that the appearance of this material was likely a russian cyberattack.

RUSSIA INCREASINGLY OBSTRUCTS UKRAINE'S USE OF STARLINK SERVICES

According to the New York Times, russia is using advanced technology to interfere with Elon Musk's Starlink satellite internet service, leading to new service disruptions on the northern front line. Starlink has been critical for the Ukrainian military since the early days of the war with russia, allowing service members to communicate quickly, share information about sudden advances, and exchange messages. The degradation of the Starlink service poses a serious threat to Ukraine, which has often managed to outsmart the russian army using advanced communications and other technologies but has held the line against new russian advances.

FILE NOT FOUND: RUSSIA IS HACKING EVIDENCE OF ITS WAR CRIMES

According to War on the Rocks, as the war in Ukraine continues, russian president vladimir putin is using cyber warfare to rewrite the history of the conflict and avoid post-war justice. russian hackers are attacking Ukrainian databases and International Criminal Court (ICC) databases to modify or delete evidence of war crimes. This tactic is aimed at helping russian criminals avoid prosecution, reflecting russia's broader strategy of using cyberattacks to cover up its atrocities. Digital manipulation of war crime evidence, including potential use of deepfakes, complicates the pursuit of justice. To counter this, enhanced cybersecurity measures, improved preservation of evidence by social media companies, and proactive prevention of cyber intrusions are critical to ensuring accountability and integrity in war crime tribunals.

«RUSSIAN» HACKERS DEFACED HUNDREDS OF LOCAL BRITISH NEWS WEBSITES

On May 11, a group claiming to be «first-class russian hackers» defaced hundreds of local and regional British newspaper websites. The group posted an emergency news item titled «FIRST-CLASS ATTACK BY RUSSIAN HACKERS» on the sites of publications owned by Newsquest Media Group. The fact that so many Newsquest titles were affected suggests that a central or shared content management system may have been hacked, but there is currently no evidence that the hackers were actually russian.

RUSSIAN ACTORS USE LEGITIMATE SERVICES FOR MULTI-MALWARE ATTACK

According to Recorded Future, russian-speaking actors abused legitimate internet services like GitHub and FileZilla in a new cyber campaign to deploy multiple variants of malware. Among other things, this involved deploying the Atomic macOS Stealer (AMOS), the current version of which can infect both Intel and ARM-based Macs. This campaign is unique partly due to the number of different malware families involved and the attackers' reliance on legitimate internet services and shared command and control (C2) infrastructure.

BLUEDELTA FROM GRU TARGETS KEY NETWORKS IN EUROPE IN MULTI-PHASE ESPIONAGE CAMPAIGNS

Insikt Group has been tracking the development of BlueDelta's gru operational infrastructure, which targets networks across Europe using Headlace malware for information theft and credential-harvesting web pages. BlueDelta deployed Headlace infrastructure in three separate phases April-December 2023, using phishing and compromised internet services and leveraging on-site binaries to obtain information. Credential-harvesting pages targeted Ukraine's Ministry of Defense, European transport infrastructure, and an Azerbaijani think tank, reflecting a broader russian strategy to influence regional and military dynamics.