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

July 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

AFU	Armed Forces of Ukraine
AI	Artificial Intelligence
APT	Advanced Persistent Threat
C2	Command and Control
CERT-UA	Government Computer Emergency Response Team Ukraine
CISA	Cybersecurity and Infrastructure Security Agency
CMU	Cabinet of Ministers of Ukraine
CRDF Global	Civil Research and Development Fund (U.S.)
CTF	Capture the Flag
DDoS	Distributed Denial-of-Service
DPRK	Democratic People's Republic of Korea
EEPO	Entrepreneurship and Export Promotion Office
EU	European Union
EU4PAR	Support to Comprehensive Reform of Public Administration in Ukraine
FBI	Federal Bureau of Investigation (U.S.)
HOVERLA	USAID Governance and Local Accountability Activity
IDF	Israeli Defense Forces
IT	Information Technology
MDT	Ministry of Digital Transformation and Entrepreneurship of Ukraine
MoD	Ministry of Defense of Ukraine
NATO	North Atlantic Treaty Organization
NCSCC	National Cybersecurity Coordination Center
NSA	National Security Agency (U.S.)
NSDC	National Security and Defense Council of Ukraine
ONCD	Office of the National Cyber Director (U.S.)
SBU	Security Service of Ukraine
SME	Small- and Medium-Sized Enterprise
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
UAH	Ukrainian Hryvnia
UAV	Unmanned Aerial Vehicle
UK	United Kingdom
UN	United Nations
VPN	Virtual Private Network

KEY TENDESES

The key event in July was a cyber incident involving a CrowdStrike product. A supply chain incident occurred due to insufficient testing of a product update, affecting over half of the companies on the Fortune 500 list. The issues impacted hospitals, led to the cancellation of flights worldwide, and affected a total of 8.5 million Windows devices (Apple and Linux devices were not affected). Affected companies (such as Delta Air Lines) and countries (like Malaysia) are now seeking compensation from CrowdStrike, Microsoft, or insurance companies, but the prospects for this remain uncertain. A likely long-term consequence of the incident will be clearer definitions of liability clauses in contracts with cybersecurity cloud organizations and increased government regulation of cloud services. This complements ongoing processes in the European Union (EU), where specific sectors, such as aerospace and defense, are pushing for greater control over service providers, insisting on keeping European users' data within the EU.

The United States is expanding mandatory cybersecurity requirements for federally funded research organizations. The latest memorandum from the Office of the National Cyber Director (ONCD) requires government agencies to accelerate the transition to a Zero Trust architecture by providing a strategy within 120 days and implementing quantum-resistant encryption. This is complemented by initiatives aimed at increasing access to the public sector by cybersecurity professionals, including the removal of job restrictions based on the possession of a formal educational degree.

The United Kingdom (UK) is aligning with European trends to strengthen cybersecurity requirements for both the public and private sectors. The country is preparing to pass a Cybersecurity and Resilience Act, which will focus on protecting critical infrastructure, increasing the powers of regulatory bodies, enhancing reporting requirements, and introducing fines and penalties for organizations that fail to comply with established cybersecurity standards. This move comes in response to the revelation of extremely weak cybersecurity systems in some public institutions, such as the UK Electoral Commission, which had inadequate cybersecurity policies that allowed malicious actors to access the data of 40 million British citizens.

Ukraine continues to strengthen international cooperation in cybersecurity, integrating with Western institutions and sharing its experience in countering russian aggression in cyberspace. An agreement was reached to deepen cooperation during the third round of the Ukraine-EU Cyber Dialogue. During a meeting with the EU's Political and Security Committee ambassadors in Brussels, the Ukrainian delegation shared its experience resisting russian cyber aggression and provided recommendations to partners on enhancing national cybersecurity. Specialists from the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) shared their experience countering cyber threats at the USA-Ukraine Cyber Bridge and the Hack the Capitol conference in the United States. An IT coalition donated network equipment and licenses to Ukraine, which will bolster the capabilities of the data processing and cybersecurity centers of the Ministry of Defense (MoD) and the Armed Forces of Ukraine (AFU).

To enhance regional cyber resilience, the National Cybersecurity Coordination Center (NCSCC) organized the first Regional Cyber Resilience Forum in Lviv, which gathered around 400 participants. The Ministry of Digital Transformation and Entrepreneurship (MDT) and the Entrepreneurship and Export Promotion Office (EEPO) launched a cyber diagnostics program to help 500 Ukrainian companies assess their digital infrastructure for vulnerabilities. The NCSCC, Ministry of Veterans' Affairs, and Civil Research and Development Fund (CRDF Global) conducted the third round of training for veterans as part of the "Cyber Defenders" reintegration program, providing them with knowledge and skills in cybersecurity and cyber defense for employment in both the public and private sectors. The SSSCIP also held educational events for professionals responsible for cybersecurity in the public sector and critical infrastructure.

This month, cybersecurity companies focused on the activities of the Chinese APT41 group. Zscaler published a technical report detailing the group's operations, Mandiant warned of APT41's attempts to infiltrate the global transportation and technology sectors, and Cisco Talos uncovered a malicious APT41 campaign that compromised a Taiwanese government research institute. Additionally, Western cybersecurity agencies, including the U.S. National Security Agency (NSA) in collaboration with Australian partners, highlighted the activities of APT40, which is linked to Chinese intelligence services.

The first global cyber war is rapidly expanding its scope, evolving into a nearly open and widespread cyber conflict. In this struggle, russian cybercriminals' offensive operations remain a key factor. In June, a breach of the TeamViewer software was attributed to the russian APT29 group. russian hackers intensified attacks on Finnish websites, with the NoName group conducting numerous distributed denial of service (DDoS) attacks, while the hacker coalition High Society is planning attacks on NATO, Europe, Ukraine, and Israel.

Meanwhile, the Western world is actively countering russian cyber activities. In July, the U.S. dismantled a russian artificial intelligence (AI) bot farm, imposed restrictions on using Kaspersky anti-virus software, and sanctioned russian hackers from the CARR group. In Australia, a couple was arrested on suspicion of espionage for russia. Ukrainian military intelligence, along with cyber volunteers, attacked nearly a 100 russian websites, and a new advanced persistent threat (APT) group, CloudSorcerer, was observed attempting to target russian government institutions, using cloud services for command and control (C2) operations and data theft.

Tensions between China and the West are escalating, with both sides accusing each other of destructive activities in cyberspace. Germany accused China of a cyberattack on its national mapping agency in 2021, which accelerated the process of removing Huawei and ZTE equipment from its 5G networks. In response, China accuses Western countries of disinformation campaigns against it, asserting that the controversy surrounding the activities of the Vault Typhoon cyber group is the result of a coordinated operation by the NSA, Federal Bureau of Investigation (FBI), and other U.S. agencies, along with the intelligence services of the Five Eyes alliance.

1. CYBERSECURITY SITUATION IN UKRAINE

EU AND UKRAINE HOLD THIRD ROUND OF CYBER DIALOGUE IN BRUSSELS

The parties agreed to deepen cooperation in cybersecurity amid russia's invasion and Ukraine's EU accession negotiations. Dialogue participants reaffirmed their commitment to the United Nations UN framework on responsible state behavior in cyberspace, discussed changes in the cyber threat landscape, recent legislative developments, enhanced cyber diplomacy, and ways to build cyber resilience. They also agreed to strengthen information sharing on situational awareness and use the EU's cyber sanctions regime under the EU Cyber Diplomacy Toolbox.

The EU emphasized its readiness to continue supporting Ukraine in strengthening its cyber resilience, cooperation, and response to cyber threats, particularly concerning critical infrastructure and networks. The parties discussed the possibility of Ukraine accessing the EU Cybersecurity Reserve and organizing additional training for Ukrainian civil and military institutions. A fourth round of the Cyber Dialogue is scheduled for 2025.

NCSCC ORGANIZED THE FIRST REGIONAL CYBER RESILIENCE FORUM IN LVIV

On July 24-25, the first Regional Cyber Resilience Forum was held in Lviv. The importance of strengthening cybersecurity in Ukraine's regions brought together representatives of government, business, cyber community, technology companies, and leading Ukrainian and international experts. The 2-day forum featured three panel discussions and more than 30 expert presentations and workshops covering a wide range of topics. The event brought together about 400 participants, both in-person and online. The forum also included a regional C2 exercise involving the Lviv Regional Military Administration and city administration, key Ukrainian cybersecurity entities, and critical infrastructure facilities in the region.

The NCSCC and CRDF Global organized the Regional Cyber Resilience Forum with support from the U.S. Department of State and in cooperation with the Security Service of Ukraine (SBU), SSSCIP, Lviv Regional State Administration, and Lviv State University of Life Safety of the State Emergency Service of Ukraine.

IT COALITION DONATED NETWORK EQUIPMENT WORTH OVER €2 MILLION TO UKRAINE

The IT Coalition donated networking equipment and supporting licenses worth more than €2 million to Ukraine, thanks to contributions from Luxembourg and Denmark. This equipment will strengthen the capacity of the MoD and AFU data centers and cyber defense.

Earlier, an IT coalition led by Estonia and Luxembourg handed over laptops, monitors, and other communication equipment worth €900,000 to the AFU. In total, the IT Coalition has already delivered over €5 million worth of assistance to the MoD and Ukrainian Defense Forces as part of contributions from the UK, Denmark, Lithuania, Latvia, Luxembourg, and bilateral assistance from Canada.

UKRAINE SHARES ITS EXPERIENCE IN COUNTERING RUSSIAN CYBER AGGRESSION WITH EU AMBASSADORS

On July 3, NCSCC representatives, led by Head of the Information and Cybersecurity Service of the National Security and Defense Council of Ukraine (NSDC) and NCSCC Secretary Natalia Tkachuk, met with the EU ambassadors of the Political and Security Committee in Brussels. Organized with support from the Permanent Representation of Estonia to the EU, the event was aimed at deepening EU ambassadors' understanding of current challenges and opportunities in the field of cybersecurity in Ukraine. The Ukrainian delegation shared its experience in countering russia's cyber aggression and provided recommendations to partners on how to strengthen national cybersecurity.

Natalia Tkachuk noted that the meeting is an important step in strengthening cooperation between Ukraine and the EU in the field of cybersecurity, emphasizing the need to strengthen Europe's collective cyber defense through using Ukrainian experience

THE MDT AND EEPO LAUNCHED A PROGRAM ON BUSINESS CYBER DIAGNOSTICS WITH USAID SUPPORT

The program will help 500 Ukrainian companies use free digital infrastructure diagnostic services from cybersecurity companies. The program's total fund is $1.5 million. Cyber diagnostics services will help small and medium-sized enterprises (SMEs) check their digital infrastructure for vulnerabilities.

Business representatives will be able to use one of three services free of charge:
- Penetration test
- Application security test
- Information environment vulnerability assessment

In order to receive one of the three free cyber diagnostic services, SMEs need to register in a special section of the Diia.Business portal, select a service, participate in an auction, digitally sign the contract on the portal, and agree with the service provider on the date of cyber diagnostics.

SSSCIP EXPERTS SHARED THEIR EXPERIENCE IN COUNTERING CYBER THREATS AT THE USA-UKRAINE CYBER BRIDGE AND HACK THE CAPITOL CONFERENCE IN THE UNITED STATES

SSSCIP representatives took part in the USA-Ukraine Cyber Bridge and the Hack the Capitol conference in Washington, DC. As part of the USA-Ukraine Cyber Bridge, organized by CYBER RANGES, cybersecurity experts in Washington and Kyiv heard reports from representatives of the Cybersecurity and Infrastructure Protection Agency (CISA) and the international organization MITRE. The participants also took part in panel discussions and practical training based on scenarios developed by Government Computer Emergency Response Team Ukraine (CERT-UA) experts, as well as in the Hack the Capitol conference.

THE NCSCC, MINISTRY OF VETERANS' AFFAIRS, AND CRDF GLOBAL TRAINED VETERANS FOR THE THIRD TIME AS PART OF THE CYBER DEFENDERS REINTEGRATION PROGRAM

As part of the Cyber Defenders program, veterans spent five months acquiring knowledge and skills in cyber defense and cyber security for further employment in Ukraine's public and private sectors. The training culminated in a capture-the-flag (CTF) cybersecurity competition and graduation ceremony.

The project's goal is to provide free comprehensive support to female and male veterans on their way to new career opportunities in cybersecurity. The curriculum included theoretical and practical classes, intensive English language training, professional career counseling, and psychosocial support.

Over the course of the Cyber Defenders project, more than 100 female and male veterans successfully completed the training and significantly improved their theoretical knowledge and practical skills in cybersecurity. As a result, they are more competitive in the labor market, both in the public and private sectors.

THE SSSCIP HELD A SEMINAR FOR CIVIL SERVANTS RESPONSIBLE FOR CYBERSECURITY IN GOVERNMENT AGENCIES AND CRITICAL INFRASTRUCTURE FACILITIES

The SSSCIP held a workshop for senior government officials and specialists responsible for cybersecurity in government agencies and critical infrastructure facilities. Organized jointly with the National Agency on Civil Service, the Higher School of Public Administration, and with the support of the project Support to Comprehensive Reform of Public Administration in Ukraine (EU4PAR 2), the event attracted 50 representatives from 35 government agencies. Participants deepened their knowledge of assessing the security of information and communication systems and registers of information and communication systems and critical information infrastructure and gained skills in finding and identifying vulnerabilities and implementing BugBounty programs. This is the fourth cybersecurity seminar this year, with 400 people already trained.

THE SSSCIP CONDUCTED CYBERSECURITY TRAINING FOR THE MOD AND OTHER GOVERNMENT AGENCIES

In May and June, the SSSCIP conducted cybersecurity training for category B and C civil servants of the Secretariat of the Cabinet of Ministers of Ukraine (CMU), MoD, Supreme Court, and the State Labor Service. About 200 specialists took part. CERT-UA experts taught the participants how to recognize the signs of cyber-attacks, prevent them, and neutralize their consequences. The exercise is aimed at strengthening Ukraine's cyber defense.

FOR THE FIRST TIME IN UKRAINE, CYBERSECURITY OF THE DELTA SYSTEM WAS TESTED ACCORDING TO NATO STANDARDS

The DELTA combat system successfully passed an information security audit, confirming that its integrated information security system meets the established requirements. A leading international consulting company carried out the independent audit, and the cybersecurity diagnostics lasted a month and a half.

The audit analyzed 162 information security measures used in the DELTA system. Built on modern technologies, the system meets the requirements for cyber defense according to NATO standards. The next step is for the Defense Forces to put the DELTA system into operation. It is expected that the system will be widely deployed in combat units, providing a technological advantage over the enemy.

UKRAINIAN INTELLIGENCE AND CYBER VOLUNTEERS ATTACKED ALMOST 100 RUSSIAN WEB RESOURCES

On July 15, a volunteer hacker community and cyber specialists from the Defense Intelligence of Ukraine carried out a large-scale cyberattack on about 100 web resources in russia to destroy the internal information of companies serving clients from the russian public sector involved in the war against Ukraine. In particular, MITgroup, Perm Plant of Promotional Equipment, United Crane Technologies, and RUMOS-LADA were affected.

As a result of the cyberattack, the appearance of the affected web resources was changed: instead of the usual sections, only a pig's head and a 404-error code appeared on the sites.

CERT-UA WARNS OF PHISHING ATTACKS AIMED AT STEALING UKR.NET MAIL ACCOUNTS

CERT-UA detected attacks by the UAC-0102 hacker group in July aimed at hijacking the accounts on the UKR.NET mail service of government officials, military personnel, and employees of Ukrainian enterprises and organizations. The attackers sent emails with archives containing an HTML file. After opening the file, users were redirected to a phishing site imitating an UKR.NET webpage, where their logins and passwords were transferred to the criminals, and a document was downloaded to the computer to distract attention. More information: https://cert.gov.ua/article/6280183

A SURGE IN THE ACTIVITY OF BELARUSIAN HACKERS IS RECORDED

CERT-UA detected a surge in activity by the Belarusian UAC-0057 hacker group on July 12-18. The attackers distributed documents with macros to launch the PICASSOLOADER malware, which installed the Cobalt Strike Beacon backdoor. The subject of the decoy files concerned financial and economic indicators, taxation, and local government reforms, including the USAID Governance and Local Accountability Activity (HOVERLA). More information: https://cert.gov.ua/article/6280159

HACKERS USE MALICIOUS MACRO IN WORD DOCUMENT TO ATTACK UKRAINIAN RESEARCH INSTITUTION

CERT-UA investigated a cyberattack by the UAC-0063 group on a Ukrainian research institution that took place on July 8. The attackers gained access to an employee's email account and sent a malicious macro in a Word document, which led to the installation of HATVIBE and CHERRYSPY malware. These programs gave the hackers unauthorized access to the computers. The investigation revealed that attacks using similar tools could also have been carried out against the Ministry of Defense of the Republic of Armenia.

There are reasons to associate this criminal activity with the APT28 (UAC-0001) group, which is affiliated with russia's military intelligence. For more information on the technical side and threat indicators, please visit the CERT-UA website.

CERT-UA DETECTS NEW CYBERATTACKS ON UKRAINIAN DEFENSE COMPANIES USING UAV PROCUREMENT THEME

Hackers posing as government employees send emails with a ZIP file containing a PDF document with a link. By clicking on the link, the user downloads the GLUEEGG malware, which installs a legitimate remote access tool called ATERA, which gives the attackers control over the victim's computer.

Hostile activity is tracked by the UAC-0180 identifier. This group is actively attacking employees of defense companies and the Ukrainian Defense Forces, constantly updating their arsenal of various malware, but their malicious activity is not limited to Ukraine. More information: https://cert.gov.ua/article/6280099

UKRAINE TO TRY CRIMINAL GROUP THAT EMBEZZLED OVER UAH 6 MILLION FROM COMPANY ACCOUNTS AND KIDNAPPED ITS ACCOMPLICE

Ukraine exposed a criminal group that stole funds from the bank accounts of leading Ukrainian industrial enterprises. The criminals used malware to gain remote access to the financial transactions of the companies, causing losses of over UAH 6 million (about $150,000). As a result of a conflict within the group, two members kidnapped their accomplice, demanding his share of the "income." The police detained the criminals, who now face up to 12 years in prison with confiscation of property.

CYBERPOLICE EXPOSE A GROUP THAT DEFRAUDED DOZENS OF PEOPLE THROUGH THE “FRIEND ASKS FOR A LOAN” SCHEME

Cyberpolice in Prykarpattia exposed a group of fraudsters that hacked social media accounts and sent messages on behalf of the owners asking to borrow money. The scheme was organized by three residents of Zaporizhzhia Oblast and one resident of Prykarpattia, who operated August 2023-January 2024. The group defrauded 50 people, receiving funds to controlled bank accounts. The defendants face up to 15 years in prison.

2. THE FIRST WORLD CYBER WAR

RUSSIAN CYBER SPIES ARE OFFICIALLY ACCUSED OF HACKING TEAMVIEWER

On July 1, Security Week reported that TeamViewer confirmed that a recent hacking attack on the company's systems was carried out by the Russian cyber-espionage group APT29, also known as Midnight Blizzard. This group is noted for powerful attacks on important organizations such as Microsoft. Initially, it was reported that the hack did not affect the product environment, TeamViewer's connectivity platform, or customer data. However, on July 4, the company reported that APT29 was able to copy employee directory data, including names, corporate contact information, and encrypted passwords for the company's internal IT environment. At the same time, TeamViewer noted that the hack appears to have been localized.

RUSSIA BANS ITS MILITARY FROM USING CELL PHONES ON THE CONTACT LINE

On July 24, the russian parliament passed a law toughening penalties for military personnel for personal use of Internet devices. The law classifies the possession of devices that allow military personnel to store or send video, photos, or geolocation data online as a crime punishable by up to 15 days in prison. The law also prohibits transmitting any information that could be used to identify russian troops and their location.

RUSSIAN HACKERS INTENSIFY ATTACKS ON FINNISH WEBSITES

In early July, numerous Finnish websites fell victim to DDoS attacks, which, according to the Cybersecurity Center, were carried out by the russian hacker group NoName. The cyberattacks targeted, in particular, the Ministry of Finance, the Tax Service, Osuuspankki Bank, and Helsinki Network Services.

APPLE REMOVES VPN APPS FROM RUSSIAN APP STORE UNDER GOVERNMENT PRESSURE

On July 4, Apple removed numerous virtual private network (VPN) apps from its App Store in Russia at the request of Roskomnadzor. The removal affected mobile apps from 25 VPN service providers, including Hidemy.name VPN, Le VPN, NordVPN, PIA VPN, Planet VPN, Proton VPN, and Red Shield VPN, according to Interfax and Media-Zona. It is worth noting that NordVPN closed all its russian servers in March 2019. Red Shield VPN criticized Apple's actions, noting, "Apple's actions, motivated by a desire to preserve revenue from the russian market, actively support the authoritarian regime. This is not only reckless, but also a crime against civil society."

CHINA DENIES ALLEGATIONS OF VOLT TYPHOON ACTIVITY AND ACCUSES THE FIVE EYES ALLIANCE OF A DISINFORMATION CAMPAIGN

On July 19, a joint report was released, "Lie to Me: A Secret Disinformation Campaign Targeting China", prepared by a number of Chinese cybersecurity organizations, including the National Computer Virus Emergency Response Center, the National Computer Virus Protection Technology Engineering Laboratory, and the security service provider 360 Digital Security Group. The report claims that all the information that has been disseminated about the Vault Typhoon group in recent months is the result of a disinformation campaign organized by the NSA, FBI, and other U.S. government agencies, including the Departments of Justice, Defense, Homeland Security, and Energy, with the participation of the Five Eyes' intelligence services.

IDF COLONEL REPORTS REPELLING 3 BILLION CYBERATTACKS SINCE FALL 2023

A commander of the Israeli Defense Forces (IDF), Colonel Rachel Dembinsky, said that the IDF has experienced about 3 billion cyberattacks since last fall. Dembinsky noted that many of these attacks targeted critical military functions, including the exchange of information between ground forces. Many of the cyberattacks are linked to politically-motivated hacker groups trying to join the fight against Israel in the war.

NORTH KOREAN CYBER GROUP CONDUCTS GLOBAL ESPIONAGE CAMPAIGN TO ADVANCE NORTH KOREAN REGIME'S MILITARY AND NUCLEAR PROGRAMS

On July 25, the FBI and its partners released a cybersecurity advisory highlighting cyber espionage activities associated with the 3rd Bureau of the Democratic People's Republic of Korea's (DPRK) General Intelligence Directorate, based in Pyongyang and Sinuiju. The Third Bureau includes the DPRK's state-sponsored cyber group, such as Andariel, Onyx Sleet, DarkSeoul, Silent Chollima, and Stonefly/Clasiopa. The group targets defense, aerospace, nuclear, and engineering organizations to obtain confidential and sensitive technical information and intellectual property. The members of the 3rd Bureau finance their activities through ransomware targeting US healthcare institutions.

GERMANY ACCUSES CHINA OF CYBERATTACK ON MAPPING AGENCY IN 2021

On July 31, Germany accused China of involvement in a 2021 cyberattack on the federal mapping agency, summoning Beijing's ambassador to Berlin to file a formal complaint. The purpose of the attack was espionage. The hackers managed to compromise endpoint devices of individuals and companies. Germany's Federal Agency for Cartography and Geodesy (BKG) plays an important role for organizations involved in critical infrastructure.

NEW APT CLOUDSORCERER GROUP TARGETS RUSSIAN GOVERNMENT AGENCIES

A previously undocumented APT group dubbed CloudSorcerer has been spotted attacking russian government agencies by exploiting cloud services for command and control (C2) and data theft.

Kaspersky, which detected this activity in May 2024, said the mechanism developed by the attackers is similar to CloudWizard, but has differences in the malware source code. The attacks use an innovative data collection program and a number of evasion tactics to hide their tracks.

U.S. DEPARTMENT OF JUSTICE DISMANTLES RUSSIAN AI-BASED BOT FARM

On July 9, the U.S. Department of Justice reported that russian state-run news network RT developed and federal security services operated an artificial intelligence-enhanced bot farm to spread disinformation to incite discord in the United States and other countries. The Department of Justice announced the seizure of two domain names and a search of 968 social media accounts in connection with the operation. FBI Director Christopher Wray noted that this is the first time the United States has disrupted an AI-enhanced bot farm.

KASPERSKY LEAVES THE US MARKET AFTER BEING BANNED BY THE DEPARTMENT OF COMMERCE

russian security vendor Kaspersky has announced its withdrawal from the US market almost a month after the US Department of Commerce announced a ban on the sale of its software due to national security risks. It is also expected that up to 50 employees of the company will be laid off in the United States as a result.

U.S. IMPOSES SANCTIONS AGAINST RUSSIAN HACKERS OF CARR GROUP

The U.S. Treasury Department has announced sanctions against two leaders of the Cyber Army of russia Reborn (CARR) cybercrime group, which has been attacking critical infrastructure around the world.

CYBERATTACK ON EVOLVE BANK EXPOSES DATA OF 7.6 MILLION CUSTOMERS

On July 9, Evolve Bank and Trust notified the Maine Attorney General of a cyberattack that affected at least 7.6 million of its customers earlier this year. The attack was carried out by Lockbit, a russian ransomware group. The full extent of the attack is not yet known as the investigation is ongoing. The statement did not specify what types of data were compromised, but the bank had previously confirmed that names, social security numbers, bank account details and contact information of personal banking customers were accessed.

AUSTRALIAN DEFENSE FORCE PRIVATE AND HER HUSBAND ACCUSED OF SPYING FOR RUSSIA

The federal law enforcement agency alleges that the couple conspired to obtain confidential information after the woman traveled to russia for an extended vacation in 2023. According to law enforcement, she instructed her husband, who remained in Australia, to log into her official work account, access certain information, and send it to her personal email account while she was abroad.

THE LARGEST HACKER ALLIANCE PLANS TO ATTACK NATO, EUROPE, UKRAINE AND ISRAEL

On July 23, CyberNews reported that the High Society hacker coalition, which consists of about 20 cyber groups, including pro-russian groups such as the russian Cyber Army and UserSec, is joining with another hacker group, the October 7th Alliance, to form a new coalition called the Holy League. The hacktivists claim that the coalition has 70 active hacker groups, although the list of cyber groups published on the Holy League's communication channel includes 55 members. All communication on the channel is carried out in English and russian. The alliance stated that its activities are a response to the arrest of NoName members by the Spanish government.