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

August 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
C2	Command and Control
CCDCOE	The NATO Cooperative Cyber Defence Centre of Excellence
CERT-UA	Government Computer Emergency Response Team Ukraine
CISA	Cybersecurity and Infrastructure Security Agency
CRDF Global	Civil Research and Development Fund (U.S.)
DDoS	Distributed Denial-of-Service
DHS	U.S. Department of Homeland Security
ENISA	European Union Agency for Cybersecurity
EPA	Environmental Protection Agency (U.S.)
EU	European Union
FBI	Federal Bureau of Investigation (U.S.)
GAO	Government Accountability Office (U.S.)
HUR	Main Intelligence Directorate of Ukraine
ICS	Industrial Control System
IP	Internet Protocol
IT	Information Technology
JICA	Japan International Cooperation Agency
KPI	Kyiv Polytechnic Institute
NATO	North Atlantic Treaty Organization
NCSCC	National Cybersecurity Coordination Center
NGO	Non-Governmental Organization
NIS	Network and Information Security
NIST	National Institute of Standards and Technology (U.S. Department of Commerce)
NSA	National Security Agency (U.S.)
NSDC	National Security and Defense Council of Ukraine
ODNI	Office of the Director of National Intelligence (U.S.)
OT	Operational Technology
PESCO	Permanent Structured Cooperation (EU)
RAT	Remote Access Trojan
SBU	Security Service of Ukraine
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
TTPs	Tactics, Techniques, and Procedures
UAE	United Arab Emirates
UAH	Ukrainian Hryvnia
UK	United Kingdom

KEY TENDESES

The key focus in the U.S. in August was the election. Both presidential candidate teams reported attempts to hack their information systems, with Trump's team blaming Iranian hackers. Reports from private companies (such as Microsoft, Google, and Meta) also pointed to increasing Iranian activity related to the elections. On August 19, the Office of the Director of National Intelligence (ODNI), the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint statement addressing heightened Iranian hacking activity targeting U.S. elections. Iran denies involvement in these incidents. In response to Iranian cyber activity, the U.S. Department of State announced a $10 million reward for information on six Iranian hackers involved in the cyberattack on U.S. water supply systems at the end of 2023.

European countries are taking steps to strengthen their cybersecurity, primarily through interstate cooperation and implementing incentives at the European Union (EU) level. For example, Switzerland announced plans to join two security projects under the EU's Permanent Structured Cooperation (PESCO), one of which focuses on cybersecurity, specifically the Cyber Polygon Federation. Simultaneously, the European Union Agency for Cybersecurity (ENISA) launched a new program to support the cybersecurity of EU member states. This program will allow European cybersecurity service providers to offer their services to EU nations and their critical infrastructure according to the Network and Information Security (NIS2) Directive. ENISA plans to allocate €28.3 million to these efforts.

Post-quantum encryption has once again become a key topic in government and expert discussions following the release of NIST standards for three basic algorithms that are resistant to quantum computing. The United Kingdom has already incorporated these standards into its strategic documents. Additionally, a RAND study published in August explores the potential of quantum computing and artificial intelligence to enhance the capacity of the U.S. Department of Homeland Security. Artificial intelligence is moving toward real-world implementation: CISA has appointed a head of AI, and the NSA is launching an AI-driven automated penetration testing platform. Experts are analyzing the impact of AI on cybersecurity operations.

Industrial facilities and the cybersecurity of operational technologies (OT) have become a priority for government agencies. According to a Censys report, nearly half of the 40,000 industrial control systems (ICS) connected to the Internet in the U.S. are vulnerable due to weak security protocols, particularly in building automation systems. Amid cyberattacks on Halliburton and Microchip, researchers highlight coordination issues between IT and OT teams in many organizations (as shown in a Cisco report, this affects nearly half of all companies). A particular concern is the security of water supply systems: the U.S. Government Accountability Office (GAO) has urged the Environmental Protection Agency to conduct an urgent comprehensive risk assessment across the sector and develop a risk-based strategy.

Ukraine continues to expand its international cybersecurity partnerships and strengthen existing ties. Several key events took place in August, including the sixth round of the U.S.-Ukraine Cyber Dialogue, where topics such as modern cyber threats, critical infrastructure protection, cyber sanctions, and cyber diplomacy cooperation were discussed. The National Cybersecurity Coordination Center (NCSCC) held meetings with the Japanese Embassy, and the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) signed a memorandum on cooperation in cybersecurity and cyber defense with Latvia's Ministry of Defense.

CERT-UA continues to monitor enemy cyberattacks involving malicious emails. In August, two such attacks were recorded. The first attack used the theme of prisoners of war from the kursk direction, distributing a malicious archive titled "spysok_kursk.zip," which contained spyware programs SPECTR and FIRMACHAGENT. The second attack involved emails allegedly from the Security Service of Ukraine (SBU), with an attached file named "Documents. zip," the download of which launched the ANONVNC malware. To counteract hostile cyber activities, Ukraine is seeking innovative solutions. In particular, the Ministry of Digital Transformation and the State Service of Special Communications and Information Protection held a Cybersecurity Innovations Hackathon, where over 200 participants developed solutions to protect against dangerous cyber products and modernize cybersecurity systems in the energy sector.

With the support of international partners, Ukraine is actively developing its training system in the field of cybersecurity, focusing on practical measures. On the initiative of the NCSCC, the first national cyber range, «Cyber Range UA», was presented at the National Aviation University. Additionally, the «Cybersecurity Laboratory for Automated Control Systems» was opened at the Igor Sikorsky Kyiv Polytechnic Institute. The laboratory's infrastructure simulates the environment of an industrial control system, modeling real-world scenarios in various sectors, such as manufacturing, water supply, and utilities. In August, the INCIDENT RESPONSE DAYS 3.0 cyber competition took place, with 100 students and cybersecurity professionals from the public sector participating.

Global cyber conflict is gaining momentum, involving new participants. The russian-Ukrainian cyberwar remains a central element of this struggle, but the scope of politically motivated hackers' activities is expanding.
International researchers note that russia is shifting the focus of its cyberattacks from Ukrainian organizations to personal mobile devices of military personnel and security sector employees. Alongside the russian-Ukrainian front, activity is also increasing around Taiwan, where cyber groups likely linked to China are ramping up attacks. The U.S. or Israel is suspected of being behind an attack on Iran's Central Bank.

1. CYBERSECURITY SITUATION IN UKRAINE

THE 6TH ROUND OF CYBER DIALOGUE BETWEEN UKRAINE AND THE U.S. TOOK PLACE IN KYIV

Participants discussed the current cyberthreat landscape, critical infrastructure protection, cyber sanctions, and cyber governance. Ukraine and the U.S. considered cooperation in cyber diplomacy, combating cybercrime, innovations in cybersecurity, and the security and competitiveness of Ukrainian IT and telecommunications. They also discussed ways to provide cyber assistance to Ukraine, including the Tallinn Mechanism.

The Deputy Secretary of the National Security and Defense Council of Ukraine (NSDC) Serhii Demediuk noted that russia is one of the biggest threats both to Ukraine and to Western countries. Therefore, enhancing cooperation, especially to exchange analytical intelligence on cyber threats between Ukraine and the U.S., is extremely important for improving situational awareness and effectiveness in joint counteraction to cyber threats. He also emphasized the need to establish a Cyber Resilience Competence Center in Ukraine and expressed gratitude for U.S. support in strengthening Ukraine's cybersecurity.

INITIATED BY THE NCSCC, UKRAINE LAUNCHED ITS FIRST DOMESTIC CYBER RANGE, «CYBER RANGE UA»

On August 23, the National Aviation University hosted the presentation of the first national cyber range, «Cyber Range UA», a virtual environment for emulating infrastructure and cyberattacks. The platform allows dozens of cybersecurity specialists to simultaneously learn to respond to incidents in conditions as close to real life as possible.

The cyber range currently includes 15 scenarios, with plans to continuously expand this number. Initially, the training will be for representatives of government institutions and critical infrastructure and the National Aviation University students. The platform will also be available for private companies and other educational institutions, fostering experience exchange and interaction among different sectors and cybersecurity entities to enhance the national cybersecurity system.

Cyber Range UA is a joint project of the NCSCC under the NSDC of Ukraine, the National Aviation University, and Cyber Unit Technologies. The cyber range was created with the support of CRDF Global in Ukraine and the U.S. Department of State.

CABINET OF MINISTERS SUPPORTED DRAFT LAW PROHIBITING THE USE OF RUSSIAN SOFTWARE

The government supported a draft law prohibiting the use of sanctioned electronic resources to strengthen cybersecurity. The draft law, elaborated by the SSSCIP at the instruction of the NSDC of Ukraine, strengthens sanctions legislation concerning the list of digital products created by russian companies or any representatives of countries associated with aggressor states or terrorist organizations. The prohibition will also extend to websites and services that pose a threat to national security and are owned or controlled by individuals or organizations subject to sanctions.

MINISTRY OF DEFENSE PRESENTED THE NEW ARMY+ PLATFORM

The Ministry of Defense of Ukraine introduced the Army+ application, which enables submitting electronic reports, reducing paperwork. The application includes 11 types of reports, grouped into four categories: Leave, Assistance, Direction, and Issuance of Direction. Reports can be submitted in a few minutes, with prompts to help fill them out correctly. Reports are sent for signature using a unique military number, Army ID. Army+ also features surveys that allow the government to gather opinions from military personnel on various issues, enabling service members to influence real changes in the Ukrainian Defense Forces. The application is already available on Google Play and in the Apple Store.

THE CYBERSECURITY LABORATORY OF AUTOMATED CONTROL SYSTEMS OPENED AT IHOR SIKORSKY KYIV POLYTECHNIC INSTITUTE

The state-of-the-art laboratory will help 200 current and future operators responsible for critical infrastructure to improve their skills and knowledge to reduce and eliminate vulnerabilities in automated control systems.

The laboratory infrastructure effectively duplicates an ICS environment, modeling real situations in various sectors such as production, water supply, and municipal services. This facilitates practical experiments and expands training opportunities. The initiative was implemented with support from the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity.

THE INNOVATIVE DELTA SYSTEM WAS SUCCESSFULLY IMPLEMENTED ACROSS ALL SECURITY FORCES IN UKRAINE

The DELTA ecosystem of innovative products for combat operations, developed by the Ministry of Defense, has demonstrated high effectiveness on the battlefield and is now operational for all units of Ukraine's security and defense sector. The decision was made at the Commander-in-Chief's headquarters.

Defense Minister Rustem Umerov reported that the DELTA system already helped destroy enemy equipment worth over $15 billion. He also emphasized that, together with partners, including the SSSCIP and SBU, security measures have been modernized to ensure the effective use of DELTA.

The DELTA system, developed by the Ministry of Defense's Innovation Center, underwent an audit and meets modern standards of comprehensive information protection. This year, it passed tests for five different interoperability standards and integrated with the Polish artillery fire control system TOPAZ, handling complex scenarios of data collection on the location of Ukraine's forces and allied units.

NCSCC REPRESENTATIVES MET WITH THE EMBASSY OF JAPAN AND JICA

On August 19, the Deputy Secretary of the NSDC of Ukraine and the Deputy Head of the NCSCC Serhii Demediuk, the Head of the Information Security and Cybersecurity Department of the NSDC of Ukraine, the Secretary of the NCSCC Nataliya Tkachuk and the Head of NCSCC Operations Department Serhii Prokopenko held a working meeting with representatives of the Embassy of Japan in Ukraine and the Japan International Cooperation Agency (JICA). They discussed the results of cooperation in the field of cybersecurity, including large-scale Hackwave cyber exercises conducted last year by the NCSCC in collaboration with JICA.

At the request of the Japanese side, the possibility of conducting training events by Ukrainian specialists for Japanese colleagues was considered, taking into account Ukraine's unique experience in countering cyber aggression in the context of a full-scale military invasion. The parties also outlined further steps to deepen cooperation, including developing the National Cybersecurity System, training, and implementing advanced technologies.

THE SSSCIP AND THE MINISTRY OF DEFENSE OF LATVIA SIGNED A MEMORANDUM OF UNDERSTANDING ON CYBERSECURITY AND CYBER DEFENSE

During a visit of the delegation from the Ministry of Defense of the Republic of Latvia to Ukraine, the SSSCIP and Latvian Ministry of Defense signed a Memorandum of Understanding on exchanging information on cyber incidents, joint exercises and training, implementing joint research projects in cybersecurity and cyber defense, and exchanging experiences and best practices on countering cyber threats.

NCSCC HELD THE CYBER COMPETITION INCIDENT RESPONSE DAYS 3.0

The NCSCC under the NSDC of Ukraine supported by CRDF Global in Ukraine held the 2-day cyber competition INCIDENT RESPONSE DAYS 3.0 on August 22-23. Around 100 students and cybersecurity professionals from the public sector participated, forming 21 teams.

The goal of the competition was to enhance the skills and professional capabilities of specialists by performing tasks close to real cyber incidents. Participants investigated incidents, collected artifacts, and analyzed malicious software while working on a unique scenario at the national cyber range «Cyber Range UA».

AT THE CYBERSECURITY INNOVATIONS HACKATHON, SOLUTIONS WERE CREATED FOR DETECTING CYBER THREATS AND MONITORING CRITICAL INFRASTRUCTURE

The Cybersecurity Innovations Hackathon brought together over 200 participants who, over eight days, developed innovative solutions for protecting against dangerous cyber products and modernizing cybersecurity systems in the energy sector. The event involved developers, cybersecurity experts, and startup representatives. The teams worked on projects in three areas:

- Cybersecurity technologies based on AI, machine learning, Big Data, industrial system protection, and special projects
- Solutions for protecting and improving industrial process control systems in the energy sector
- Developing a real project for a client from the hackathon partner

The teams A42, CyberForce, and Fix It were the hackathon winners. They will receive mentoring support from the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity for applying for grant programs and 6-month residency in the first innovation park UNIT.City.

HUR REVEALS CYBER OPERATION THAT PARALYZED NUCLEAR WEAPONS DEVELOPER IN RUSSIA

Cyber specialists from HUR, in collaboration with the hacker group VO Team, successfully attacked a nuclear weapons development enterprise in Snezhinsk (Chelyabinsk Oblast). The attack disabled the servers and network equipment of the sole provider Vega, leaving strategic enterprises in the city, including a nuclear munitions developer VNIITF, without communication and internet for almost a week.

The cyber operation resulted in obtaining employees' personal data and documents from the sanctioned factory, which will aid in identifying sanction circumvention mechanisms and individuals involved. Local sources reported a possible disruption of russia's state defense orders.

CYBER POLICE IN CHERNIHIV OBLAST SHUT DOWN FRAUDULENT CALL CENTERS

Criminals posed as bank employees and used special programs to gain access to citizens' bank accounts. They created a bot in a messenger app to lure victims and force them to disclose their bank card details. Using the confidential information obtained, the criminals unlawfully accessed online banking and transferred funds to their accounts.

The total damage from these actions amounted to over UAH 5.4 million. An investigation is ongoing, and the perpetrators face up to eight years in prison.

IN KHARKIV OBLAST, MEMBERS OF A CRIMINAL GROUP WHO APPROPRIATED INTERNET USER ACCOUNTS WILL BE TRIED

Cyberpolice uncovered three members of an organized criminal group involved in stealing Instagram account credentials. In March 2024, operatives determined that the criminals used brute force methods with special software to guess passwords. After hacking the accounts, the perpetrators sold the obtained data on the dark web.

Law enforcement has completed the investigation and submitted an indictment to the court for unauthorized interference with electronic communication systems and the sale of restricted information. The criminals face up to 15 years in prison.

CERT-UA RECORDED CYBERATTACKS USING EMAILS ABOUT PRISONERS OF WAR FROM THE KURSK DIRECTION

On August 19, the government team CERT-UA recorded cyberattacks using emails themed around prisoners of war from the Kursk direction. The attackers sent emails containing images of supposed prisoners of war and links to download the archive "spysok_kursk.zip." The archive contains a file with a CHM extension and the name "spysok vp, shcho vybyvayut. kursk."

Opening this file leads to the download of components of the well-known spyware SPECTR and a new program, FIRMACHAGENT, which is designed to upload stolen data to a control server.

The attack was carried out by the group UAC-0020 (Vermin), associated with the security agencies of the temporary occupied Luhansk.

CERT-UA RECORDED MASS DISTRIBUTION OF MALICIOUS EMAILS SUPPOSEDLY FROM THE SBU

On August 12, CERT-UA recorded the mass distribution of malicious emails supposedly from the SBU. The emails contained links to a file “Documents.zip,” the download of which triggers the malicious program ANONVNC.

This program allows attackers to gain hidden unauthorized access to the victim’s computer. CERT-UA detected over 100 affected computers, including state bodies and local government authorities.

2. THE FIRST WORLD CYBER WAR

RUSSIA IS CHANGING ITS CYBER OPERATIONS STRATEGY: SHIFTING FROM INFRASTRUCTURE ATTACKS TO SUPPORTING ACTIONS ON THE BATTLEFIELD

Recent reports indicate that russia has changed its approach to offensive cyber activities in Ukraine. russian cyber units have begun focusing on targets related to Ukrainian military objects, trying to compromise devices used by Ukrainian soldiers; gain access to command systems and integral components of military operations; and even use publicly available webcams to gather intelligence data, such as the location of Ukrainian military assets. More than two years into russia's full-scale invasion, russia's cyber operations focus appears to be shifting away from attacking more strategic civilian targets, such as telecommunications and energy, as was the case at the beginning of the conflict. This change seems to reflect moscow's new priorities in the conflict as it continues to occupy Ukrainian territory and might indicate that the potential of cyber weaponry has not been fully realized.

APT41 LIKELY COMPROMISED A TAIWANESE GOVERNMENT-AFFILIATED RESEARCH INSTITUTE USING SHADOWPAD AND COBALT STRIKE

On August 15, Cisco Talos researchers reported that the Chinese hacker group APT41 hacked a Taiwanese government research institute working on confidential technologies. The attack began in July 2023 and used malware such as ShadowPad and Cobalt Strike. According to the report, the institute specializes in computational technologies, a strategic sector for Taiwan, which is a global leader in the semiconductor industry.

Cisco Talos attributes the attack to APT41, a hacker group that the U.S. Department of Justice charged in 2020 for using ransomware and other tools in attacks on over 100 companies and governments worldwide.

RUSSIA'S KURSK OBLAST HIT BY A 'MASSIVE' DDOS ATTACK AMID UKRAINE'S OFFENSIVE

On August 8, russia's kursk oblast suffered a major distributed denial-of-service (DDoS) attack amid a sudden Ukrainian military offensive. Hackers targeted the government, business websites, and critical infrastructure, causing temporary disruptions. The attack involved over 100,000 requests per second, with most IP addresses traced to Germany and the UK. Despite the scale, the attack did not compromise e-government infrastructure or user data. This incident is considered one of the largest cyberattacks on the region since the war began, although no group has claimed responsibility.

APT28 TARGETS DIPLOMATS WITH HEADLACE MALWARE THROUGH PHISHING BAIT ABOUT CAR SALES

A new campaign, using car sales ads as phishing bait to deliver a modular Windows backdoor called HeadLace is attributed to a threat actor associated with russia. “The campaign likely targeted diplomats and began as early as March 2024,” reads an August 2 report from Palo Alto Networks Unit 42. With medium to high confidence, Palo Alto attributed it to russian APT28, also known as BlueDelta, Fancy Bear, Fighting Ursa, Forest Blizzard, FROZENLAKE, Iron Twilight, ITG05, Pawn Storm, Sednit, Sofacy, and TA422.

RESEARCHERS BELIEVE CHINESE-LINKED HACKERS MAY BE BEHIND CYBERATTACKS ON RUSSIAN STATE BODIES

As reported by The Record on August 13, hackers likely linked to Chinese threat actors APT31 and APT27 attacked russian government institutions and technology companies as part of a recent cyberattack campaign called EastWind. The attack, discovered by Kaspersky, was carried out using the GrewApacha remote access Trojan (RAT), the PlugY backdoor, and an updated version of the CloudSorcerer malware. The attackers used phishing emails to deploy the tools, which are associated with known Chinese cyber espionage groups. While Kaspersky did not definitively attribute the attacks to APT31 or APT27, the tools used strongly suggest the involvement of these groups.

CHINA-BACKED EARTH BAKU EXPANDS CYBERATTACKS TO EUROPE, THE MIDDLE EAST, AND AFRICA

On August 14, The Hacker News reported that, starting in late 2022, the China-backed threat actor known as Earth Baku expanded its targets beyond the Indo-Pacific region to include Europe, the Middle East, and Africa. Among the new target countries are Italy, Germany, the United Arab Emirates (UAE), and Qatar, with likely attacks also detected in Georgia and Romania. Governments, media outlets, telecommunications, technology, healthcare, and education sectors are among those affected by the intrusions.

MASSIVE CYBERATTACK DISRUPTS THE CENTRAL BANK OF IRAN, PARALYZING ITS COMPUTER SYSTEM

On August 14, the Jerusalem Post reported that the Central Bank of Iran and other major banks were disrupted by a massive cyberattack. Current estimates suggest the attack is one of the largest cyberattacks on Iran’s infrastructure. It remains unclear who is responsible for the attack, but it is widely speculated that it was carried out by the U.S. and/or Israel.

NEW PHISHING CAMPAIGN TARGETS RUSSIAN DISSIDENTS WORLDWIDE

According to research from Citizen Lab and Access Now, hackers linked to russian intelligence, particularly the group Cold River and a new group called Coldwastrel, are targeting kremlin critics worldwide with phishing emails. The campaign, which began around 2022, targets russian opposition members in exile, U.S. and EU non-government organization (NGO) employees, and media organizations. The phishing emails often impersonate trusted acquaintances to trick victims into revealing login credentials. Some of the individuals targeted, including the former U.S. ambassador to Ukraine, have fallen victim to these attacks.

WHY EVERYONE IS SUDDENLY TALKING ABOUT IRAN HACKING ELECTIONS

As Foreign Policy wrote on August 21, with the U.S. presidential elections approaching, Iran has ramped up its efforts to interfere with voting through online disinformation, influence operations, and cyberattacks targeting both Donald Trump's and Kamala Harris's campaigns. U.S. agencies, including the FBI and CISA, have warned about this activity, noting that Iran views these elections as particularly significant to its national security interests. Iran's hacking efforts are part of a broader strategy that involves targeting U.S. officials, potentially in retaliation for the 2020 killing of Iranian General Qasem Soleimani.

Iran's activities are considered more aggressive this election cycle, possibly due to the ongoing Middle East conflict involving Israel. While russia and China are still considered the most sophisticated threats, Iran's actions demonstrate its willingness to exploit vulnerabilities in U.S. election security. U.S. officials claim they are better prepared than in previous elections to counter these threats, warning against overreacting, which could unintentionally undermine public trust in the election process.

TELEGRAM CEO'S ARREST SPARKS CYBERATTACKS ON FRENCH WEBSITES

The arrest of Telegram CEO Pavel Durov in France on August 25 triggered a wave of cyberattacks by hackers protesting his detention. French authorities arrested Durov over Telegram's lack of moderation and cooperation with law enforcement, which allegedly facilitated crimes such as drug trafficking and fraud. In response, hacktivist groups launched a series of DDoS attacks on French websites, including government, media, and healthcare agencies. The attacks under the banner "opDurov" were primarily conducted by pro-russian groups like the russian Cyber Army and UserSec, along with other international hacktivists. The targeted websites experienced outages, though many were restored by the following Monday.

RUSSIA-BACKED ATTACKERS AND COMMERCIAL SURVEILLANCE VENDORS REPEATEDLY USE THE SAME EXPLOITS – GOOGLE REPORT

According to a blog post by Google's Threat Analysis Group, russian state-backed group APT29 (also known as Cozy Bear) and commercial surveillance vendors Intellexa and NSO Group have been repeatedly using the same exploits. Researchers uncovered a spying campaign against websites run by the Mongolian government. This campaign was notable because it marked the first time researchers observed russian APT29 members using the same exploits sold by commercial surveillance vendors.

THE UNITED STATES RELEASED WELL-KNOWN RUSSIAN HACKERS AS PART OF A DIPLOMATIC PRISONER EXCHANGE

On August 2, The Hacker News reported the release of two high-profile russian hackers, Roman Seleznev and Vladislav Klyushin, as part of an international prisoner exchange between Belarus, Germany, Norway, russia, Slovenia, and the United States.

Seleznev, also known by the aliases Track2, Bulba, and nCux, was sentenced in 2017 to 27 years in prison for credit card fraud, which caused nearly $170 million in damages to small businesses and financial institutions in the U.S. He later received an additional 14-year sentence for participating in a $50 million cyber fraud scheme. The second hacker, Vladislav Klyushin, owner of the firm M-13, was sentenced in September 2022 for stealing confidential financial information from U.S. companies, leading to insider trading that amounted to $93 million. Both hackers have returned to russia.