QUARTERLY ANALYTICAL SUMMARY

Q2/2024

Acronyms

AI	Artificial Intelligence
APT	Advanced Persistent Threat
CEO	Chief Executive Officer
CERT-UA	Government Computer Emergency Response Team Ukraine
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CSIS	Center for Strategic and International Studies (U.S.)
EPA	Environmental Protection Agency (U.S.)
EU	European Union
FBI	Federal Bureau of Investigation (U.S.)
ICC	International Criminal Court
IT	Information Technology
NATO	North Atlantic Treaty Organization
NCSCC	National Cybersecurity Coordination Center
NSDC	National Security and Defense Council of Ukraine
NCSC	National Cyber Security Centre (UK)
NGO	Non-Governmental Organization
NHS	National Health Service
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
ONCD	Office of the National Cyber Director (U.S.)
OT	Operational Technology
PAP	Polish Press Agency
SBU	Security Service of Ukraine
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
U.S.	United States of America
UK	United Kingdom

Global trends

In the second quarter of 2024, there was a sharp increase in the activity of Chinese hackers, which attracted increased attention from Western governments. In May, the U.S. National Intelligence published a report indicating that China remains the biggest cyber threat to the United States, particularly in the context of elections, where Chinese hackers use artificial intelligence (AI) to fuel social tension.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) found that Chinese cybercriminals focused on attacks on critical infrastructure, particularly in the aviation and energy sectors. The main targets were small- and medium-sized businesses that provide essential services. Federal officials also acknowledged that the Chinese campaign Volt Typhoon has fundamentally changed the cyber threat landscape. Volt Typhoon, aimed at destabilization and creating public panic, especially during conflicts, demonstrates a shift from traditional espionage to Beijing's more sinister intentions. The changed approach is accompanied by techniques that other foreign adversaries of the U.S. could use.

Chinese cyber activity is not limited to the United States. Recently, there have been increasing reports of cyber espionage campaigns against members of the Inter-Parliamentary Alliance on China. In particular, Chinese hackers attacked the Chair of the Foreign Affairs Committee of the Belgian Parliament. The Netherlands also detected a large-scale espionage campaign by Chinese hackers who conducted a complex operation to penetrate the country's military networks. In June, Dutch military intelligence reported that the investigation of the incident is ongoing, and the scale of the interference was much larger than initially believed.

Meanwhile, China continues to strengthen its cyber forces, having created the Information Support Forces in April. Despite the growing threat from China, experts note that the number of Chinese-made devices in U.S. networks has increased by 40% over the past year, reaching 300,000 devices compared to 185,000 the previous year.

In the second quarter of 2024, there was a clear trend of increased law enforcement activity in combating ransomware groups and their infrastructure. In April, British police halted the activities of LabHost, which provided Phishing-as-a-Service services used to create initial points of entry into victims' networks.

This publication was made possible through support provided by the U.S. Agency for International Development, under the terms of Award to the Ukrainian Foundation for Security Studies within the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International De velopment or the United States Government.

A whole series of large-scale law enforcement actions took place in May. Law enforcement agencies from 13 countries conducted the Endgame special operation, which destroyed the criminal infrastructure of several malicious groups, including IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee, and Trickbot. Ukrainian law enforcement officers actively participated in this operation, making most of the searches and arrests.

British, American, and Australian law enforcement officers conducted another operation to identify the leader of the LockBit cybercriminal group, who turned out to be russian Dmitry Khoroshev. The U.S. Department of State already announced a $10 million reward for information leading to his capture. Also in May, the Security Service of Ukraine (SBU), the U.S. Federal Bureau of Investigation (FBI), and law enforcement agencies of the United Kingdom (UK) and the European Union (EU) conducted a special operation in eight European countries, exposing more than 30 members of transnational hacker groups.

However, it is currently difficult to say whether these measures will have a long-term effect. Already in May, Trellix experts discovered that the infrastructure belonging to the LockBit group is actively being restored and starting to function again.

The development of AI and its impact on cybersecurity are becoming increasingly relevant topics for cybersecurity organizations and researchers. This became especially noticeable during the RSA Conference 2024. Researchers from the Center for Strategic and International Studies (CSIS) think tank demonstrated how AI can influence decision-making processes in national security. While China and the U.S. plan significant investments in AI research (China – $50 billion, the U.S. – $39 billion) and begin high-level dialogue on this issue, cybersecurity experts already face new challenges.

For example, Unit42 cybersecurity experts trained AI to create effective malware using a relevant database of source data. The AI-created software turned out to be not only effective but also capable of rapidly modifying, creating numerous variations, and adapting to different platforms. Horizon3.ai experts already offer new AI-supported services to accelerate the prioritization of cyber protection and eliminate vulnerabilities in organizations' cybersecurity.

AI is also becoming an object of cyber espionage. In May, an unknown advanced persistent threat (APT) group attacked American AI researchers, attempting to gain access to their data. In June 2024, CISA conducted the first command-and-control exercises dedicated to AI threats and officially expressed concern about AI's potential impact on increasing cyber threats in the chemical and biological sectors.

At the same time, U.S. government structures are looking for ways to apply AI to enhance security. The U.S. Department of Defense is currently considering the possibilities of using AI for rapid response to cyberattacks.

Trends and forecasts

The Operational Technology (OT) sector is striving to adapt to the new reality of heightened cyber threats facing this unique field. Concerns about low cybersecurity standards, on which critical economic services depend, are increasing. The U.S. government is actively addressing this issue through additional regulation, but industrial facility owners point to systemic problems with the regulatory process, which is largely fragmented and inconsistent regarding sector-specific standards. They also note that OT involves specific technological solutions that are difficult and expensive to modernize.

However, these arguments are unlikely to have a significant impact since many industrial organizations do not even adhere to the simplest cybersecurity standards, such as changing default passwords, which jeopardizes the functioning of critical infrastructure. A similar situation is observed in the water supply sector: following a series of successful cyberattacks over the past six months, the U.S. Environmental Protection Agency (EPA) conducted inspections revealing that over 70% of water supply systems do not comply with the Safe Drinking Water Act and have critical cyber vulnerabilities.

Against this backdrop, active discussions continue regarding the need for a complete ban on ransom payments to ransomware hackers. However, this issue faces opposition from some stakeholders who are concerned that such restrictions could jeopardize their operations in the event of a cyberattack. On the other hand, malicious actors increasingly resort to unconventional pressure tactics, including physical coercion of potential attack victims, as seen in the activities of the UNC3944 group.

The Secure by Design approach is gaining more weight in the public policy of key countries. CISA is actively promoting its Secure by Design Pledge platform, a voluntary initiative that brings together companies committed to following Secure by Design principles. The UK is also preparing to implement this approach for market participants.

Ollie Whitehouse, Chief Technical Officer of the British National Cyber

Security Centre (NCSC), notes that the current "thousands of patches" approach to cybersecurity, where software or technology developers address specific cybersecurity issues in their products on a case-by-case basis, needs to change. This also pertains to the social responsibility of development companies towards their customers, particularly organizations with traditionally limited cybersecurity budgets, such as non-governmental organizations (NGOs) and schools.

An important case illustrating the need for greater security in software development occurred in April when the infrastructure of open-source software, based on using open libraries, faced a global threat due to a complex and well-prepared attempt to compromise the XZ Utils library by unknown criminals. The threat was accidentally discovered by a Microsoft employee. This incident highlighted the issue of security in using open-source products and the need to change approaches in this area towards greater application security.

The human factor remains one of the key sources of cyber threats to organizations and their information systems. This was confirmed in April by Verizon and Proofpoint studies. According to Verizon's survey, 68% of security breaches were caused by non-malicious human factors, i.e., incidents involving insider errors or victims of social engineering. Proofpoint provides similar statistics. This issue has a broader scope than just personnel training and is related to the overall level of cyber awareness. In this regard, CISA launched its second nationwide cyber awareness program in May, covering various target audiences. The campaign will disseminate information across all major platforms and channels: television, radio, digital advertising, shopping malls, social media, and outdoor advertising.

There were only a few significant cyber incidents in the second quarter of 2024, but they underscored serious problems in healthcare cybersecurity. In the U.S., the consequences of an attack on UnitedHealth took nearly three months to resolve, and in June, the British company Synnovis, which conducts clinical research and is a key partner of the National Health Service (NHS), became a victim. russian hackers allegedly attacked this medical facility, demanding a ransom of $50 million. British law enforcement agencies are still investigating this incident, which is likely to lead to changes in the UK's cybersecurity policy in the healthcare sector. Overall, the healthcare sector remains one of the favorite targets for hackers, as medical institutions often have weak security systems and store large amounts of personal data. Local medical institutions are particularly vulnerable, often having limited resources to ensure an adequate level of cybersecurity.

The United States of America

In the second quarter of 2024, the U.S. experienced a significant cyber incident involving an attack on Change Healthcare, which is being compared in scale to the Colonial Pipeline attack. Hackers stole a substantial amount of personal data from the company's clients, leading to the CEO testifying before the U.S. House of Representatives. Investigations and Senate hearings revealed that the company paid a ransom of $22 million. Numerous flaws in cybersecurity policies were also identified, including weak protection of personal data and an inappropriate cybersecurity leadership, as the Chief Information Security Officer (CISO) lacked cybersecurity experience. The total losses for the organization have already exceeded $800 million and are estimated to potentially reach $1 billion. This incident is likely to lead to stricter cybersecurity requirements across the entire U.S. healthcare sector and developing relevant standards, which may be complicated by the underfunding of the National Institute of Standards and Technology (NIST), the agency responsible for developing these standards.

The U.S. continues to rotate cybersecurity specialists and expand its cybersecurity efforts. Amid a White House request for a $13-billion cybersecurity component in the 2025 budget, a new cybersecurity director was appointed at the National Security Agency (NSA), and the Pentagon created a cyber policy department. The NSA and CISA continue to issue security advisories, particularly regarding implementation of Zero Trust. Meanwhile, the number of incidents is increasing. In April, there was a wave of cyberattacks on municipal resources, city IT systems, and the U.S. water sector, where efforts by russian cyber groups were detected.

This logically leads to increased government focus on the educational aspect due to a significant shortage of cybersecurity specialists across all economic sectors (about 500,000 unfilled vacancies). The Office of the National Cyber Director (ONCD) is actively promoting implementation of the National Cyber Education and Workforce Strategy, holding discussions with market participants. There are increasing calls to waive the higher education requirement for hiring cybersecurity professionals in favor of validated qualifications, which should also assist the Department of Defense, currently facing about 27,000 unfilled cyber vacancies due to bureaucratic issues.

European Union

The European Union is actively adapting to a new, more dynamic landscape of cyber threats. One of the key measures is developing the Space Act, which will include provisions on cybersecurity. This is particularly relevant amid the increasing efforts by state and private companies to explore space, including deploying satellite systems into orbit.

The EU is also preparing to implement post-quantum cryptography to prevent new cyber threats. The European Commission already issued recommendations for member states, highlighting the need to develop corresponding roadmaps for this transition.

Germany plans to create a separate branch of the military – cyber forces – to respond more swiftly to new threats and strengthen its cyber defense.

Cybersecurity in Ukraine

In the second quarter of 2024, Ukraine focused on various aspects of international cooperation and integration into the EU and NATO. During the first scientific-practical international conference on cyber diplomacy, held in Kyiv with the support of the National Cybersecurity Coordination Center (NCSCC), Foreign Minister Dmytro Kuleba emphasized that Ukraine is an integral part of European and Euro-Atlantic security systems, thanks to its experience in countering russia and its reputation as an innovator. Deputy Secretary of the National Security and Defense Council of Ukraine (NSDC) Serhiy Demedyuk called for the joint development of strategies to predictably and continuously strengthen collective cyber resilience.

Ukraine held its first meeting with EU representatives as a candidate country, focusing on digitalization issues, particularly on Chapter 10 “Digital Transformation and Media.” The Ministry of Defense approved the Fundamentals of Information Security and Cybersecurity in Information and Communication Systems, incorporating NATO’s best practices and international standards. The third international meeting of the National Cybersecurity Cluster discussed deepening cooperation with the EU and NATO and practical steps Ukraine is taking in the field of cybersecurity.

Ukrainian representatives participated in several important international events. Natalia Tkachuk, head of the Information Security and Cybersecurity Service of the NSDC of Ukraine and NCSCC Secretary, spoke at the Asian Leadership Conference about Ukraine’s achievements in building a national cybersecurity system. At the RSA Conference 2024 in San Francisco, Ukrainian representatives shared the country's advanced experiences with the global expert community. Under a signed memorandum, Ukraine and Poland agreed to cooperate in digital technology and innovation, IT industry development, AI, e-governance, and developing platforms like Diia and mObywatel.

In June, the NCSCC became a partner of the Paris Cyber Summit and Ukraine participated in the European cyber exercises Cyber Europe for the first time.

Ukraine is actively improving and implementing state policies in cybersecurity and new technologies. The Ministry of Digital Transformation presented a White Paper on AI regulation to help companies prepare for the legislative framework in this area and integrate Ukraine into the EU. The Cabinet of Ministers of Ukraine approved the tasks of the National Informatization Program. To automate monitoring implementation of the Cybersecurity Strategy of Ukraine, the NCSCC presented a new tool, CyberTracker. The State Service of Special Communications and Information Protection (SSSCIP) approved requirements for information security auditors at critical infrastructure facilities and their certification process. The first Qualification Center for Information Technology and Cybersecurity in Ukraine began certifying specialists in this field. Ukraine is enhancing the qualifications of state cybersecurity specialists at all levels through regular training.

The Government Computer Emergency Response Team Ukraine (CERT-UA) continues to monitor cybersecurity trends. In the second half of 2024, it recorded increased interest from hostile hackers in Ukraine's telecommunications sector. Attacks on the military, aimed at gaining access, control, and theft of intelligence information from specialized situational awareness systems, remain a strategic military target of the enemy. The most active groups attacking Ukraine are those not currently associated with the official special services of the aggressor country, although they operate in the interests of the russian government.

The First World Cyber War

russian hackers continue to attack Ukraine's allies, conducting cyberattacks on local municipal systems in the U.S. and implementing new backdoors during attacks in Eastern Europe. The APT28 group targeted Polish institutions, and unidentified russian hackers hacked the website of the Polish Press Agency (PAP), posting a fake article aimed at worsening Ukrainian-Polish relations. Another successful attack led to the hacking of 100 local British news websites.

In June, russian hackers attacked the website of a Spanish company that repairs Leopard tanks for Ukraine and interfered with satellite broadcasts, causing interruptions and even showing russian military videos on children's TV channels. They are also actively looking for new tools to access victims, such as attacking the company TeamViewer. Of particular concern is their readiness to interfere in elections in the U.S. and Europe.

In May, there was a series of mirror cyberattacks by pro-russian and pro-Ukrainian groups. On May 9, Ukrainian hackers managed to replace the parade signal on some russian TV channels with footage from the war in Ukraine. In response, russian hackers hacked the satellite signal of the Inter TV channel and broadcast a russian parade to Ukrainian viewers.

The pro-Ukrainian hacker group Blackjack successfully carried out an operation against the infrastructure of the russian moscollector. In June, russian energy companies, IT companies, and government institutions fell victim to the Decoy Dog trojan, causing disruptions in the operation of supermarkets across the country. The Sticky Werewolf group attacked a russian pharmaceutical company and a research institute involved in microbiology and vaccine development. A large-scale attack was also carried out on major russian banks, making their services unavailable to some users.

In June, it became known that International Criminal Court (ICC) prosecutors are investigating possible russian cyberattacks on Ukrainian civilian infrastructure as potential war crimes. The investigation covers attacks that endangered civilian lives, disrupted electricity and water supplies, interrupted communication with emergency services, or disabled mobile data services that transmit air raid warnings. The SBU is also collecting evidence on hackers who attacked the Kyivstar mobile operator at the end of 2023 and will submit the materials to the ICC.

In parallel, russian hackers are attacking Ukrainian and ICC databases, attempting to modify or delete evidence of war crimes to rewrite history and avoid post-war justice.