НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

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

JANUARY 2024

Prepared with the support of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity.
This publication is made possible by the support of the American people through the United States Agency for International Development (USAID).
The authors' views expressed in this publication do not necessarily reflect the views of USAID or the U.S. Government.

CONTENT

ACRONYMS

AFU	Armed Forces of Ukraine
AI	Artificial Intelligence
CDTO	Chief Digital Transformation Officer
CEO	Chief Executive Officer
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
DKK	Danish Krone
EU	European Union
FSB	Federal Security Service (Russian Federation)
GenAI	Generative Artificial Intelligence
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
HPE	Hewlett Packard Enterprise
IT	Information Technology
NATO	North Atlantic Treaty Organization
NCSCC	National Cybersecurity Coordination Center
NCSC	National Cyber Security Centre (United Kingdom)
NGO	Non-Governmental Organization
NSA	National Security Agency (U.S.)
PSYOP	Psychological Operations
SBU	Security Service of Ukraine
SCPC	State Cyber Protection Center
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
U.S.	United States
UAH	Ukrainian Hryvnia
UAV	Unmanned Aerial Vehicle
UDCG	Ukraine Defense Contact Group
USAID	United States Agency for International Development

KEY TENDENCIES

In January, we focused on the vulnerability of Ivanti Connect Secure, which the Chinese group UNC5221 uses as a tool for cyber espionage. This zero-day vulnerability is so potentially dangerous that the Cybersecurity and Infrastructure Security Agency (CISA) issued an urgent directive that is binding on all federal agencies. The British National Cyber Security Centre (NCSC) also issued its own warning about this threat. The Chinese cyber espionage group's activity fits into the broader context of Western concerns about Chinese activity. For example, the massive collection of vulnerabilities in software used by foreign companies. CISA additionally advises critical infrastructure facility owners in the U.S. to cautiously use Chinese-made unmanned aerial vehicles (UAVs) and issued guidance on preventing data leaks as a result.

The U.S. continues to look for effective ways to protect its own critical infrastructure facilities, especially in the sectors that are currently under the greatest pressure, healthcare, and water supply. In the healthcare sector, the situation is becoming particularly acute as attacks against hospitals have become common, as has the theft of patient personal data. Perpetrators are looking for new tools not only to conduct attacks, force the victims to pay ransoms (the federal government is becoming less and less loyal to this process) and blackmailing not only the attacked organizations but also patients. Even private companies (e.g., Palo Alto Network) are beginning to issue guidelines for healthcare institutions, and government agencies are preparing to impose restrictions on federal funding for healthcare institutions that have not implemented minimum cybersecurity requirements.

Following a series of cyberattacks against water and wastewater systems in December 2023, the organizations responsible for them have become the center of attention for security agencies and lawmakers. In the U.S., there is an ongoing discussion at both the national and local level about the best way to protect more than 50,000 water utilities currently operating in the country. In mid-January, CISA and its partners published the Cyber Incident Response Guide for the Water and Wastewater Sector to help organizations, but the companies' owners say they often lack resources for cyber defense measures. In the meantime, attacks on such organizations continue; for example, Southern Water, a company that provides water services to 2.5 million customers and wastewater services to 4.7 million customers in the southern regions of England, was attacked in January.

While the debate continues over the extent of artificial intelligence's (AI's) impact on cybersecurity, almost all organizations point to it as a game-changer in the cybersecurity landscape. Criminals are preparing to use generative AI (GenAI) to generalize the data they have already stolen and in effect create new attack vectors or ransomware opportunities. Defenders are looking for opportunities to use AI more widely to analyze cyber threats (at the same time, experts point out conceptual problems in this regard, including those related to the datasets the AI is trained on). The NCSC released its own long-term assessment of how AI affects the situation and, in their opinion, AI will increase the volume and impact of cyberattacks over the next two years.

The problems of quantum computing and post-quantum encryption are once again of concern to security agencies. Cybersecurity authorities in Europe are raising awareness regarding the need to pay more attention to this issue and not be distracted by approaches that are questionable in terms of effectiveness, including that NATO adopted its first quantum strategy. The U.S. National Security Agency (NSA) is starting open discussions on the future of quantum computing and how it will affect the security sector, and IBM believes that there will be more cyberattacks in 2024 to steal encrypted data in the hope of gaining access to its content with the advent of quantum computers.

In January, Ukrainian organizations suffered several powerful cyberattacks: one targeting a banking center and another significantly affecting one of the largest data centers in Ukraine. The latter resulted in service disruption in several government organizations and information systems. In general, this correlates with increased russian cyberactivity against Ukrainian information systems. According to the State Service of Special Communications and Information Protection of Ukraine (SSSCIP), the number of cyber incidents last year increased by 62.5%. In response, Ukraine is launching counterattacks (such as the actions of Ukraine's military intelligence against one of russia's IT systems suppliers for industry) and is cooperating more actively with partners, e.g., Denmark announced that it will provide €12 million for Ukraine's cyber defense.

Western researchers study russian actions in cyberspace and provide their own forecasts and recommendations. CSO Online described the structure and methods of the pro-russian hacker group NoName057(16) and claimed that the organization could become a model for future cybercriminals. At the same time, the publication emphasized that so far, the group's actions, which primarily focus on distributed denial of service (DDoS) attacks, do not pose a serious threat to the West. Researcher Monica Kello argues that the public shaming and sanctions used by Western governments today, trying to influence russia's actions in cyberspace, are not effective. In her opinion, the response should be based on russian strategic culture and include transparent investigations into the consequences of russian hacking and leakage operations. It should also use the distrust that prevails in the russian intelligence services and society to intensify feuds in the enemy's operating environment.

Several cybersecurity companies and cybersecurity departments of large companies were attacked in January, including at Microsoft, which fell victim to an attack by the russian state actor Midnight Blizzard. As a result of the attack, the perpetrators gained access to "a very small percentage of Microsoft corporate email accounts, including members of the leadership team and employees in cybersecurity."

In early February, Mandiant's account on the X network fell victim to the perpetrators and was used for a short time to promote deceptive cryptocurrency transactions. The mailboxes of the HP Enterprise tech giant cybersecurity department also fell victim to an attack by hackers who are linked to the kremlin. russian cybersecurity company Kasperski also disclosed details of an attack that affected its employees' phones.

The National Cybersecurity Coordination Centre (NCSCC), the Ministry of Veteran Affairs, and the Civil Research and Development Fund (CRDF Global) are working together to integrate veterans into the cyber workforce by providing them with comprehensive cybersecurity and cyber defense training, and then support them to find employment in the public or private sector. Concurrently, the public sector is building its capacity to protect and respond to cyberattacks. On the one hand, Google will provide 5,000 security keys to protect the accounts of Ukrainian government officials and provide them with the necessary training to use the keys in 2024. On the other hand, the SSSCIP conducts trainings for government agencies' Chief Digital Transformation Officers (CDTO) and category B and C public officials who are responsible for cybersecurity to improve their cooperation with the Government Computer Emergency Response Team Ukraine (CERT-UA).

The NCSCC warned about a high level of cyber threats to communications companies. Major cybersecurity agencies have recorded an increase in cyberattacks on Ukraine's critical infrastructure, a trend that is in line with global developments. Attacks in Ukraine are expected to peak in February 2024. At the same time, the struggle between Ukraine and russia in cyberspace is intensifying and russia is targeting Ukrainian government officials and military personnel through phishing and trying to sow panic among the Ukrainian population. The Defense Intelligence of the Ministry of Defense of Ukraine reported successful attacks on the far-eastern research center for space hydrometeorology, the special communications server of the russian federation's ministry of defense, and the IT infrastructure of IPL Consulting, which specialized in implementing information systems in russian federation industry.

1. CYBERSECURTY SITUATION IN UKRAINE

THE NATIONAL CYBERSECURITY COORDINATION CENTER, THE MINISTRY OF VETERANS AFFAIRS, AND CRDF GLOBAL LAUNCHED CYBER DEFENDERS PROGRAM TO REINTEGRATE UKRAINIAN VETERANS

The NCSCC, Ministry of Veterans Affairs, and CRDF Global launched the Cyber Defenders Reintegration Program to create conditions for veterans to acquire the necessary skills and knowledge to build a successful career in cybersecurity. The initiative provides comprehensive training in cyber defense and cybersecurity areas and support to find employment in the public sector or with Ukrainian cybersecurity institutions.

GOOGLE PROVIDES UKRAINIAN GOVERNMENT OFFICIALS WITH 5,000 SECURITY KEYS FOR ACCOUNT PROTECTION

During a meeting between the Ministry of Digital Transformation and Google in Davos, Switzerland, Google announced that it continues cooperating with Ukraine in cybersecurity. In particular, it will provide 5,000 security keys to protect the accounts of Ukrainian government officials in 2024. In addition, Google plans to provide education and training so the Ukrainian government officials can learn how to use these devices and effectively utilize all the functionality. Google and the Ukrainian government will also work on joint cybersecurity workshops to share best practices and develop new strategies for data protection.

DEPUTY MINISTER OF DEFENSE KATERYNA CHERNOHORENKO URGED NATO MEMBERS TO STRENGTHEN COOPERATION IN DEFENSE INNOVATIONS

Kateryna Chernohorenko participated in a meeting of the Committee on Innovation and Hybrid Threats at NATO Headquarters as part of the NATO-Ukraine Council. The Deputy Minister of Defense briefed the committee on the Ministry's priorities in innovation and cyber defense. She also emphasized the technologies that Ukraine needs to change the 'rules of the game' on the battlefield.

THE NETHERLANDS JOINS THE IT COALITION AND NEW CONTRIBUTIONS FROM THE MEMBER STATES

The Netherlands joined the IT coalition at the meeting of the Ukraine Defense Contact Group (UDCG). The new coalition member has already contributed €10 million. In addition, Denmark allocated DKK 91 million (more than €12 million) to strengthen Ukrainian cybersecurity in the framework of the UDCG IT coalition. The funds will be allocated for Ukrainian Armed Forces and Ministry of Defense cybersecurity projects and are an important contribution to the long-term support of the state's cyber defense.

UKRAINE AND ROMANIA SIGNED A COOPERATION AGREEMENT FOR DIGITALIZATION AND CYBERSECURITY

The Ministry of Digital Transformation of Ukraine and the Ministry of Research, Innovation, and Digitalization of Romania signed an agreement to develop electronic communications and cooperation in digitalization and cyber defense. The agreement will enable exchanging experience between Ukrainian and Romanian specialists and implementing joint projects to develop telecommunications infrastructure, digitalization, and cyber defense. In addition, the agreement will allow Ukraine to participate in European Union (EU) financial assistance programs.

SERVERS AND NETWORKS OF THE AGGRESSOR STATE OF RUSSIA ARE LEGITIMATE TARGETS FOR OUR CYBER SPECIALISTS, ANDRII CHERNIAK

In his commentary to Suspilne on January 31, Andrii Cherniak, Representative of the Defense Intelligence of the Ministry of Defense of Ukraine, said that operations in the cyberspace of the aggressor state of russia continue, resulting in the russian ministry of defense's server being hacked and terminating the functioning of special communications between enemy units. He added that attacks in russian cyberspace would continue. As "such servers and networks are a legitimate target for our cyber specialists and the Security and Defense Forces of Ukraine."

SSSCIP UPDATES THE PROCEDURE AND OPERATION TYPES TO PROTECT INFORMATION FOR GOVERNMENT AGENCIES' OWN USE

The SSSCIP updated the procedure and operation types for protecting information for government agencies' own use. The relevant order is available on the SSSCIP website. As per the updated procedure, SSSCIP authorization is only required for information security assessment operations and operations to detect eavesdropping devices for the agencies' own use. The document unifies technical protection of information by i ntroducing the same operation types both in terms of authorization and in terms of relevant licensing.

A SAFE CYBERSPACE SHOULD BE BUILT ON JOINT RESPONSE TO CYBER THREATS, YURII MYRONENKO

At the international conference "Cyber Resilience in Today's World: Ukraine's Experience", SSSCIP Chair Yurii Myronenko said that CERT-UA detected and investigated 1,462 cyber incidents in the second half of 2023. Most of those deliberate attacks targeted ministries, other public authorities, and critical infrastructure. He said the ongoing war has also demonstrated that unlike its kinetic component, cyberspace-based aggression is of a global nature. Everyone is interconnected by a single virtual space, so attacks against Ukraine often affect other countries too.

SSSCIP HELD A WORKSHOP ON CYBER INCIDENT RESPONSE FOR SPECIALISTS FROM PUBLIC AGENCIES AND CRITICAL INFRASTRUCTURE FACILITIES

With partner support, the SSSCIP conducted the 1-day in-person Cyber Incident Response workshop for public agencies' and critical infrastructure facilities' CDTOs and category B and C public officials who are responsible for cybersecurity. About 80 participants attended the event. The workshop goal was to increase coordination between CERT-UA and cybersecurity specialists of relevant institutions and enterprises.

RUSSIAN GROUP APT28 CONDUCTS PHISHING ATTACKS AGAINST UKRAINIAN MILITARY PERSONNEL

The russian federation is intensifying its cyber espionage efforts and continuing its attempts to gain access to Ukrainian military situational awareness and troop control systems by stealing service members' credentials against the background of a lack of success on the battlefield. The hacker group APT28, associated with the main intelligence directorate of the general staff of the armed forces of the russian federation (GRU), distributes phishing html pages of the ukr[.]net mail service. The espionage campaign, which contains several phishing variants, is also aimed at gaining access to mailboxes of service members and units of the Defense Forces of Ukraine.

NCSCC WARNED ABOUT THE GROWING LEVEL OF CYBER THREATS

In connection with a series of cyberattacks on mobile operators, Internet providers, and data processing centers, the NCSCC warned about a high level of cyber threats for communication sector companies. The main entities for ensuring cybersecurity also recorded the growth of harmful and destructive cyberactivity in relation to Ukrainian critical infrastructure. The peak of cyberattacks is expected in February 2024. In addition to infrastructure damage, russian special services try to use any incident in their information operations.

THE SECURITY SERVICE OF UKRAINE (SBU) DETAINED A RUSSIAN INFORMANT WHO WAS SPYING ON THE WARPLANES OF THE ARMED FORCES OF UKRAINE (AFU) IN KIROVOHRAD OBLAST

SBU cyber specialists detained another russian special services informant who was collecting intelligence about the AFU Air Force in Kirovohrad Oblast. The attacker sent the information to special Telegram channels that were created by the russian federation special services to collect intelligence information about Ukrainian defenders. To mask his criminal activities, the informant periodically changed his profile nickname in the messenger and used a proxy server for anonymization. The perpetrator faces up to eight years in prison.

THE SBU WARNED ABOUT A PHISHING E-MAIL NEWSLETTER PURPORTEDLY ON ITS BEHALF AND URGED NOT TO DOWNLOAD MALICIOUS FILES

The SBU recorded phishing e-mails allegedly sent on its behalf targeted mainly at government employees. At first glance, the letters seem plausible, but in fact they have nothing to do with the SBU. The emails contain malicious files and attachments that, when run, download malware to the user's computer to collect sensitive data. Such fake mailings can be used by russian special services for espionage and information gathering.

THE SBU EXPOSED RUSSIAN PSYCHOLOGICAL OPERATIONS (PSYOP) TRYING TO SOW PANIC AMONG UKRAINIANS THROUGH EMAIL MAILINGS

The SBU warned about the distribution of large-scale mailings to the e-mail addresses of Ukrainians, including state authorities and private company representatives. It was carried out from a large number of electronic mailboxes that were previously hacked by russian hackers. The mailing bears all the signs of an intentional informational and psychological operation. The letters offer cooperation with the russian special services for a reward. Thus, the enemy is once again trying to destabilize the situation inside

THE SBU DETAINED A HACKER WHO WAS PREPARING CYBERATTACKS ON UKRAINIAN GOVERNMENT WEBSITES AND DIRECTED RUSSIAN MISSILES AT KHARKIV

In Kharkiv, SBU cyber specialists exposed a member of the russian hacker group 'russian federation people's cyber army', controlled by the russian federal security service (fsb). The attacker adjusted enemy fire on the city and carried out fsb tasks to prepare a series of DDoS attacks on the websites of Ukrainian state-owned enterprises and government agencies. He sent information to the fsb through a popular messenger as screenshots of electronic maps with the potential targets' coordinates. The perpetrator is currently in custody and faces up to 12 years in prison.

THE NUMBER OF CYBER INCIDENTS ROSE 62.5% IN 2023: STATE CYBER PROTECTION CENTER (SCPC) CYBER INCIDENT RESPONSE OPERATIONS CENTER REPORT

The SCPC Cyber Incident Response Operations Center published a report on the performance of the vulnerability detection and cyber incident and cyberattack response system in 2023.

Throughout 2023, the system's resources were used to process about 18 billion events, collected through monitoring, analysis, and transmission of telemetry information on cyber incidents and cyberattacks. Security analysts directly detected and processed 1,105 cyber incidents, which is 62.5% more than in 2022.
Full report: scpc.gov.ua/uk/articles/334

HACKERS SEND MESSAGES CONTAINING MALWARE TO AFU OFFICERS PRETENDING TO RECRUIT FOR THE 3RD SEPARATE ASSAULT BRIGADE AND THE ISRAEL DEFENSE FORCES

CERT-UA took action against a series of cyberattacks involving malware containing messages sent to AFU officers through the Signal messaging service about recruiting for the AFU's 3rd Separate Assault Brigade and the Israel Defense Forces. The suspicious activity was revealed and reported to CERT-UA by specialists by Trendmicro, an American-Japanese company, in late December 2023. See the technical details of the attack in the CERT-UA message: cert.gov.ua/article/6276988

100 GIGABYTES OF SECRETS WORTH $1.5 BILLION – THE DEFENSE INTELLIGENCE OF UKRAINE RECEIVED AN ARRAY OF SECRET DATA ON THE OCCUPIERS' MILITARY-INDUSTRIAL COMPLEX

The Defense Intelligence of the Ministry of Defense of Ukraine announced that it received 100 gigabytes of classified data from the russian enterprise Special Technological Center LTD. The russian company, which has been under sanctions since 2016, produces military equipment and machinery used by the russian army in the war against Ukraine. The array of information transferred to the Defense Intelligence of Ukraine includes documentation for 194 nomenclature items. According to preliminary estimates, the value of the data obtained may be as high as $1.5 billion. This is a significant blow to terrorist moscow: the archive is already being used to strengthen Ukraine's defense capabilities and weaken the aggressor state.

CYBERPOLICE AND NATIONAL POLICE INVESTIGATORS EXPOSED A HACKER WHO CAUSED HUNDREDS OF MILLIONS IN LOSSES TO A LEADING WORLD COMPANY

A resident of Mykolaiv infected the server of a well-known American company with a miner virus. In the course of an international police operation, law enforcement officers conducted searches and stopped the hacker's activity. In more than two years of criminal activity, the man withdrew almost $2 million in cryptocurrency to controlled electronic wallets, which is equivalent to more than UAH 75 million. The investigation continues to establish possible accomplices of the perpetrator and his involvement in pro-russian hacker groups.

THE DEFENSE INTELLIGENCE OF THE UKRAINIAN MINISTRY OF DEFENSE REPORTED DETAILS OF A SUCCESSFUL OPERATION OF UKRAINIAN CYBER VOLUNTEERS

The Defense Intelligence of the Ministry of Defense of Ukraine reported about a successful cyberattack on the russian federal state unitary enterprise main military construction directorate for special objects. The successful operation was carried out by specialists from the Ukrainian Blackjack organization. The cyber volunteers expertly penetrated the russian state company's database and obtained 1.2 terabytes of valuable data, including technical documentation for more than 500 objects of the russian federation ministry of defense. As part of the cyber operation, all the specified data were deleted from the russian company's servers, which temporarily paralyzed the construction of new facilities.

THE DEFENSE INTELLIGENCE OF THE MINISTRY OF DEFENSE OF UKRAINE REPORTED A CYBERATTACK ON THE SPECIAL COMMUNICATIONS SERVER OF THE RUSSIA'S MINISTRY OF DEFENSE

The Defense Intelligence of the Ministry of Defense of Ukraine reported that a cyberattack on January 30 took down the server of the russian federation's ministry of defense that was used for special communications. As a result of the cyberattack, the exchange of information between units of the russian defense ministry that used the moscow-based server was terminated. The software on the attacked server was approved by russia's fsb as compliant with state information security standards. The software was installed at various of russian public sector strategic facilities, including military facilities.

RUSSIAN HACKERS WERE INSIDE UKRAINIAN TELECOMMUNICATIONS GIANT KYIVSTAR FOR MONTHS

On January 4, Illia Vitiuk, head of the SBU Information Security State Interests Counterintelligence Protection Department, disclosed some details of the cyberattack against mobile operator Kyivstar. According to him, the hacker attack caused "disastrous" destruction and aimed to land a psychological blow and gather intelligence. The attack wiped "almost everything", including thousands of virtual servers and computers, he said, describing it as probably the first example of a destructive cyberattack that "completely destroyed the core of a telecoms operator." According to his information, hackers were in the system since at least May 2023.

UKRAINIAN MONOBANK WAS HIT WITH A MASSIVE DDOS ATTACK

On January 21, Oleh Horokhovskyi, co-founder and CEO of Monobank, confirmed the attack on Monobank and claimed it included 580 million requests. He also reported that Monobank appears to be one of the most attacked IT targets in Ukraine. The attack did not disrupt the online banking services and was the second after a similar DDoS attack in the previous week.

HACKERS ATTACKED PARKOVYI DATA CENTER: THE SHLIAKH SYSTEM, NAFTOGAZ, UKRPOSHTA, UKRAINIAN RAILWAYS WERE AFFECTED

On January 25, Naftogaz, the State Service for Transport Safety, Ukrposhta, and Ukrainian Railway reported technical failures in the operation of their websites and electronic services. There were also problems with the website of the state russian-speaking TV channel FreeDom, which stopped being updated. It turned out the cause was a cyberattack on the Parkovyi Data Center. Naftogaz services were restored only on January 28, it announced.

USAID PROVIDED ASSISTANCE TO IMPROVE THE CYBERSECURITY OF UKRAINE'S ENERGY SYSTEMS

On January 26, USAID presented the results of its assistance to Ukrenergo National Power Company to strengthen the cybersecurity of services that ensure the power system operates. The assistance includes several measures to increase the level of cyber defense and the availability of important services and information flows for the uninterrupted operation of the transmission system operator. In particular, USAID purchased equipment and software to strengthen the system's resilience and readiness to counter cyber challenges in accordance with international standards.

THE COORDINATION HEADQUARTERS FOR THE TREATMENT OF PRISONERS OF WAR HIT BY CYBERATTACK

On January 29, the Coordination Headquarters for the Treatment of Prisoners of War reported that IT specialists restored all its services, which had been subjected to a DDoS attack the previous day, and they were operating normally and available online. The hacker group behind the incident was not identified, but the headquarters points to moscow linking the attack to the recent crash of a russian transport plane that was supposedly carrying Ukrainian prisoners of war.

2. THE FIRST WORLD CYBER WAR

HOW RUSSIA'S NONAME057(16) COULD BE A NEW MODEL FOR HACKING GROUPS

CSO Online's reported on the pro-russian hacktivist group NoName057(16) and its evolution from "a little-known hacker group" to an organized group of volunteer cyber guerrillas. The group, which has carried out a significant number of DDoS attacks, successfully built an online community with financial compensation for volunteers. NoName057(16) initially targeted Ukrainian websites but expanded its focus to include all countries that support Ukraine. The group's operation methods include disinformation, intimidation, and creating chaos. In particular, it relies on the crowdsourced DDoSia botnet and rewards volunteers with cryptocurrency.

Despite its evolving capabilities, the author doubts whether NoName057(16) poses a serious security threat to the West, emphasizing that its impact is currently low. The group's unique approach to integrating financial compensation for volunteers creates a new niche in the hacker community raising questions about its future development, potential imitators, and its role after the russian-Ukrainian war.

'TRIANGULATION' BACKDOOR INFECTED DOZENS OF IPHONES BELONGING TO KASPERSKY EMPLOYEES

As reported by Ars Technica, a recent investigation by Kaspersky revealed details of an advanced and complicated attack called Operation Triangulation that targeted the iPhone, which the company itself experienced. For four years, the attackers exploited an unknown hardware feature, supposedly for debugging or testing purposes, allowing them to achieve an unprecedented level of access. The attackers sent iMessages exploiting four zero-day vulnerabilities to install spyware on iPhone, Mac, iPod, iPad, Apple TV, and Apple Watch. The campaign's unique characteristics make attribution difficult, and the attackers remain unknown. Kaspersky researchers identified and reported more than 30 zero-day vulnerabilities across a variety of products but called this attack chain as the most sophisticated they have seen.

REVENGE FOR KYIVSTAR: UKRAINIAN HACKERS LEFT PART OF MOSCOW WITHOUT INTERNET

On January 9, law enforcement sources reported that hackers from Blackjack group had hacked the moscow-based Internet provider M9com and demolished its servers. As a result, some moscow residents were left without internet and TV. According to the source, the hackers said this a "training attack" before a bigger one, which would be serious revenge for Kyivstar.

UKRAINIAN HACKERS SUCCESSFULLY ATTACKED THE PAYMENT WEBSITE OF ONE OF RUSSIA'S REGIONAL ENERGY COMPANIES

On January 13, hackers from Ukraine's IT army successfully attacked the payment center of Permenergo of russia's Perm Krai. They claimed to have shut down the website and payment gateways. Internal operations of Permenergo may have been disrupted.

BANGLADESH ELECTION APP CRASHES AMID SUSPECTED CYBERATTACK, UKRAINE AND GERMANY BLAMED

The russian state cybersecurity company Solar report indicates that China and North Korea are the key sources of offensive cyber campaigns against russia in 2023. The report identifies China-related activities as aggressive cyber espionage campaigns targeting russian organisations, while North Korean actors focus on gathering information on developments in missile technology. Commentators note that these actions raise questions about diplomatic relations between the russian federation and these countries, considering russia's efforts to strengthen ties with China and North Korea. Despite their alleged cyber activity, moscow seems to be tolerating these actions, probably because of the help these countries are giving russia in the war against Ukraine. The report says that diplomatic relations do not necessarily extend to cyberspace, emphasising the complex dynamics in the geopolitical landscape.

CHINA COLLECTS DATA ON VULNERABILITIES IN SOFTWARE USED BY FOREIGN COMPANIES

On January 18, Newsweek published an overview of the implications of the Regulations on the Management of Network Product Security Vulnerabilities in China, which were published in July 2021 by the Chinese cyberspace control authority. According to the document, Chinese companies must report loopholes in software or products they use within 48 hours of discovery. In many cases, the same software is used by foreign companies, and therefore the Chinese government is collecting a significant database of such vulnerabilities. The procedure specifies that notification to the government must take place before measures are taken to eliminate the vulnerability or inform the public about it.

UKRAINE'S MILITARY INTELLIGENCE CONDUCTED AN OFFENSIVE OPERATION AGAINST A RUSSIAN COMPANY SPECIALIZING IN INFORMATION SYSTEMS IN RUSSIAN INDUSTRY

On January 26, the official website of Georgian President Salome Zourabichvili was cyber-attacked by a group of russian hackers. An image of a skull appeared on the page with the inscription "hacked by Cozy Bear, Glory to Russia." In addition, the website of the opposition Georgian TV company Formula was hacked; the page was unavailable for several hours before it was restored.

MICROSOFT FELL VICTIM TO AN ATTACK BY RUSSIAN STATE ACTOR MIDNIGHT BLIZZARD

On January 19, Microsoft announced that on January 12, 2024, it had detected a national-state attack on its corporate systems and identified the threat actor as Midnight Blizzard, the russian group also known as Nobelium. According to the corporation, beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of the senior leadership team and employees in cybersecurity, legal, and other functions. Some emails and attached documents were also exfiltrated.

The investigation indicates the attackers were initially looking for information related to Midnight Blizzard itself. The company emphasizes that the attack was not the result of a vulnerability in Microsoft products or services. Meanwhile, later (on January 27) the company admitted that the hacked corporate account used in the attack did not even have multi-factor authentication. The company also published guidance for responders on nation-state attacks based on its experience.

UKRAINIAN HACKERS BREAK INTO RUSSIAN RESEARCH CENTER FOR SPACE HYDRO-METEOROLOGY

On January 23, the Ukrainian hacker group BO Team hacked a major russian space hydrometeorology research center, Planeta. This was a significant attack on the direct consumers of Planeta, such as the ministry of defense and the general staff of the russian federation, the russian ministry of emergency services, and the northern fleet.

It is reported that Ukrainian hackers gained initial access to two of Planeta's servers and then attacked all of its devices and services. As a result, an unprecedented amount of information was destroyed for this kind of campaign, a total of about 2 petabytes (approximately 2 million gigabytes) of data.

RUSSIAN THREAT GROUP COLDRIVER EXPANDS THE RANGE OF TOOLS IT USES AGAINST WESTERN OFFICIALS

On January 18, Google Threat Analysis Group published a report stating that the russian group COLDRIVER continues to collect credentials through phishing attacks that target Ukraine, NATO countries, academic institutions, and non-governmental organizations (NGOs). To gain the trust of its targets, COLDRIVER often uses accounts that impersonate another person, such as an expert in a particular field or someone who is somehow connected to the target of the phishing attack. The fake account is then used to establish a relationship with the target, which increases the likelihood of the phishing campaign succeeding, and eventually sends a phishing link or a document containing a link. In addition to credential phishing, the group recently has been delivering malware via PDF documents.

TECH GIANT HP ENTERPRISE HACKED BY RUSSIAN HACKERS

On January 25, The Hacker News reported that kremlin-linked hackers are suspected of infiltrating Hewlett Packard Enterprise's (HPE) cloud email environment to exfiltrate mailbox data. According to the company's filing with U.S. regulators, beginning in May 2023, the threat actor accessed and exfiltrated data from a small percentage of HPE mailboxes belonging to individuals involved in cybersecurity, go-to market, business segments, and other functions. The intrusion was attributed to the russian state-sponsored group known as APT29, and which is also tracked under the monikers BlueBravo, Cloaked Ursa, Cozy Bear, Midnight Blizzard (formerly Nobelium), and The Dukes.

RUSSIAN HACKERS ATTACKED THE GEORGIAN PRESIDENT'S WEBSITE

On January 26, the official website of Georgian President Salome Zourabichvili was cyber-attacked by a group of russian hackers. An image of a skull appeared on the page with the inscription "hacked by Cozy Bear, Glory to Russia." In addition, the website of the opposition Georgian TV company Formula was hacked; the page was unavailable for several hours before it was restored.