



**State Service
of Special Communications
and Information
Protection of Ukraine**

WAR IN UKRAINE. PULSE OF CYBER DEFENSE

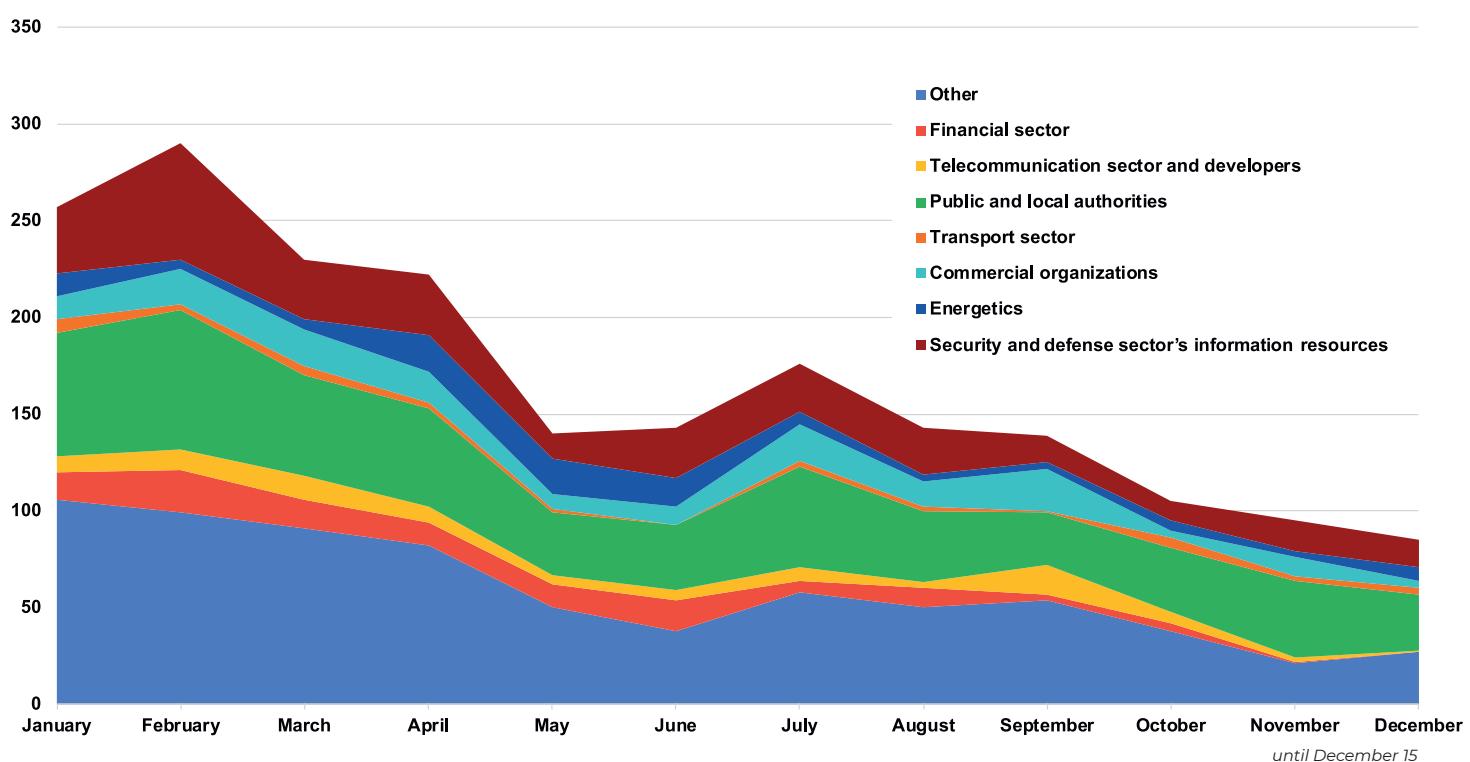


September–December 2022



1.

STATISTICS



Overall statistics of cyber incidents and cyberattacks registered and investigated by the Computer Emergency Response Team for Ukraine (CERT-UA) has reached **2,100** over the year and above **1,500** since the beginning of the full-scale military invasion.

It is not military but civil infrastructure that has been the primary target for russian hackers throughout the year. Cyberattack intensity remains at a certain constant level with minor deviations toward increase or decrease.



2.

KEY INSIGHTS

The primary goals of russia's attacks on Ukrainian cyberspace are the following:

- **espionage** (obtaining intelligence as regards logistics, armaments, plans and operations of the Security and Defense Forces). This is why the adversary tries to remain as discreet as possible, while retaining access to and presence in Ukrainian commercial IT systems and public institutions for as long as possible;
- **PsyOps and fake information** aimed at undermining public confidence in capabilities of the public authorities, the Security and Defense Forces, and spreading panic among the people;
- **Maximum destructive effect**, i.e. attempts to disable critical information infrastructure facilities, deprive citizens of access to public, banking services, etc.

russia-affiliated groups are still unable to achieve their strategic purpose and inflict substantial damage to our infrastructure.

russian and pro-russian hacking groups that have been active in Ukraine during the reporting period

ARMAGEDDON/GAMAREDON/ PRIMITIVE BEAR

rf Federal Security Service, activity tracked by the ID UAC-0010

SANDWORM

rf Main Department of the General Staff of the Armed Forces, activity tracked by the ID UAC-0082

APT28/FANCY BEAR

rf Main Department of the General Staff of the Armed Forces, activity tracked by the ID UAC-0028

APT29/COZY BEAR

rf Foreign Intelligence Service, activity tracked by the ID UAC-0029

UNCT1151/ GHOSTWRITER

belarus Ministry of Defense, activity tracked by the ID UAC-0051

XAKNET, KILLNET, Z-TEAM, CYBERARMYOFRUSSIA_REBORN

pro-russian cyber terrorists, activity tracked by the IDs UAC-0106, UAC-0108, UAC-0109, UAC-0107 respectively



3.

WHAT IS TARGETED BY RUSSIAN HACKERS

As usual, russian cyber operations may serve to reinforce ground operations against Ukraine.

The **public sector** traditionally ranks first by cyberattack quantity, accounting for about one fourth of all the cases investigated by the Computer Emergency Response Team for Ukraine (CERT-UA) both throughout the year and during the reporting period. Both obtaining Ukrainians' personal data and destroying infrastructure of public services poses equally major threat for the country's security, especially at times of war. This is why protection of public information infrastructure is critical.

russian hackers' focus remains on the **energy sector** with regard to consistency of their sectoral targets at the strategic level. We observe an increase in the number of targeted attacks against energy companies, such as power grid operators, regional electricity distributors, customer service companies, and design institutions. Those attacks are complex as regards their preparation and implementation, so they are more difficult to detect and respond to.

Not only the companies managing regional electricity distributors are under the constant eye, but also the companies providing them services, hardware and software. So, the attacks through supply chains remain a source of growing threat. For instance, we detected an attempt to attack an energy sector facility this December. They tried to launch this attack by hacking the company developing and supplying software for the facility in question.

CERT-UA detected an increasing number of attacks on the **commercial sector** early in the second half of the year. The growing quantity of cyber incident reports can be explained by strengthened PPP and acknowledgement of free-of-charge CERT-UA assistance opportunities by private companies.

Besides, russian hackers keep attacking Ukrainian **telecom sector and software developers**. First and foremost, software developers may become an entry point to their clients' infrastructure (supply chain attack). So, the companies providing services to critical infrastructure and public sector should be aware of the threat posed by russian hackers as something that concerns them personally.

Attacks on the **logistics sector** in cyberspace come as a natural next step in supply chain disruption and affecting logistics capacities of critical equipment and means to both civil and military sectors. russia is trying to obtain intelligence on the supply routes and quantity of the armament and assistance provided by our partner countries.

As reported earlier, a new Prestige ransomware was detected by Microsoft in Ukraine and Poland in October. This malware targeted Ukrainian and Polish companies involved in the logistics sector. Based on the results of the analysis conducted, we can assert with a high degree of certainty that russian government-backed hackers were behind these attacks.



There is no doubt that russian cyber terrorism is not limited to Ukraine, as the same groups threaten virtually the entire civilized world. That is why design and implementation of a new contributory

system of cyberspace security for the whole civilized world is a priority task for today.

4.

HOW RUSSIAN HACKERS ATTACK

Usually, distribution of malware that steals data or destroys information systems is the most widespread tactics used by russian military hackers in Ukraine. Such attacks make up over a quarter of their total number and may be part of more complex and powerful operations.

Exploiting vulnerabilities of public resources to infiltrate into organizations' internal networks is another highly popular attack method in 2022. Negligence and incomplete implementation of security policies on such resources also plays into the hand of cyber criminals.

In addition to data recon and infrastructure destruction, russia uses hacking services to conduct PsyOps. The November attack on the Ministry of Finance is an example of such attacks. The hackers gained access to email. Even though they failed to obtain the Ministry's sensitive data, the very fact of hacking was used to attempt an information pressure on the society.

russian hackers are still trying to exploit high degree of public trust for the defense and security sector structures by sending bulk emails containing malware.

More specifically, russian hackers disguised themselves as the following institutions in the reporting period:

State Emergency Service, by sending emails titled "How to identify a drone bomber." By doing so, they tried to spread the DolphinCape malware that collects information about an affected computer, launch of EXE/DLL files, listing files and uploading them, as well as capturing and exfiltrating screenshots.

SSSCIP, by disseminating an alleged RAR archive containing documents "TIP instruments covered by an expert opinion as regards their compliance with the Technical Information Protection requirements". Opening this file triggered malware (specifically data stealing malware) download.

UAF General Staff Press Office, by disseminating links to a fake "Order." Following the link would open a page with a notification of the need of software (PDF Reader) update. Clicking the "DOWNLOAD" button would result in the RomCom malware download.

CERT-UA, by sending messages titled "Attention! Malware (CERT-UA)" that contained an attached archive "ESETscanner.rar" with an ESET Online Scanner.exe file in it. Executing this file would result in the device being infected with malware.



5.

CONCLUSIONS ON PROTECTION

Responsible attitude towards cybersecurity and following cyber hygiene rules are basic prerequisites to resilience in cyberspace not only for the public sector and critical infrastructure, but for each individual citizen.

russian hackers are experienced in social engineering, possess accurate data on the ‘hot topics’ in our country and skillfully use all this to wage new attacks. We should continuously work on enhancing our defenses against such attacks.

As reported earlier, the SSSCIP has been carrying out response actions to increase protection of the infrastructure and user accounts at the compromised public sector and critical infrastructure facilities that asked for help since the beginning of the full-scale invasion of Ukraine.

In order to enhance cyber resilience of public information resources, the SSSCIP taught a training course for public officials of A and B categories on cyber defense, compliance with the relevant legal requirements and other aspects of their systems’ cyber resilience enhancement in wartime, in October and December 2022. “The role of governmental agencies in ensuring cyber defense is no less important than ours as a regulatory authority. The Ukrainian legislation on cyber defense and information protection is swiftly adapting to the requirements of time. We are introducing the world’s best practices. However, handling all of this requires appropriate skills, so there should be a constant dialogue between the regulatory authority and implementing actors. This is why we initiated these

training courses,” says the SSSCIP Deputy Head Oleksandr Potii.

All the institutions, whose operation is critical for the country, safety, citizens’ lives and health, should have a responsible attitude to compliance with the cyber defense and information protection legislation, ensure that their staff is duly trained, and keep an eye for ongoing threats at least on CERT-UA and the SSSCIP official resources (websites and social media).

It should be reminded that pursuant to the legislation (Article 9 of the Law of Ukraine “On Information Protection within Information and Communication Systems”) a system owner is the one responsible for information protection in the system.

We ask leaders of companies, institutions and organization, regardless of their ownership, to take personal control over the issues related to implementation of the aforementioned urgent measures.



6.

PROGRESS OF INTERNATIONAL COOPERATION IN CYBER DEFENSE

Ukraine is tightening cooperation with the U.S., the EU and other partners to build a collective cyber defense system against Russia's aggression in cyberspace.

The global cybersecurity has worsened significantly due to Russia's aggression. Not only Ukrainian critical infrastructure, but the infrastructure of our partner countries is being attacked by Russian hackers. And those attacks involve not only hacking groups associated with the Russian government, but also ordinary cyber terrorists and politically motivated hackers who launch numerous attacks, coordinated through various Telegram channels.

The SSSCIP is becoming a center of global expertise in resisting Russian hackers' attacks, and we are strengthening cooperation with our partners month by month.

For instance, the SSSCIP continues active cooperation with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). A wide range of issues was discussed at the recent meeting with the CCDCOE delegation led by its Director, Dr. Mart Noorma, from collaboration between the Centre and the SSSCIP units to prospective strategy of partner countries' cyber defense based on Ukrainian experience.

A delegation of the National Cyber Security Directorate of Romania (DNSC) visited the SSSCIP. During the meeting with the SSSCIP Deputy Heads Viktor Zhora and Oleksand Potii, the parties

discussed expansion of cooperation between the DNSC and the SSSCIP, including cooperation issues related to cyber threats and cyberattacks in the context of the ongoing Russo-Ukrainian war.

Members of the Internet 2.0 Inc. from Australia specializing in cybersecurity and cyber defense solutions, also visited the SSSCIP to share their experience and discuss joint initiatives, in particular, the introduction of a cyber security course for veterans.

The SSSCIP representatives took part in a number of global cybersecurity events, where practical steps for protection from Russia's cyber aggression and tightening cooperation among the partners were developed. Those events include the second round of the Cybersecurity Dialogue, Singapore International Cyber Week (SICW), the Second International Counter Ransomware Initiative Summit, 2022 Trust Services Forum, the Conference "Building societal resilience by raising public awareness of cyber threats and enhancing the role of cyber education," held by the Polish 2022 OSCE Chairmanship-in-Office, etc.



In addition, we'd like to remind that the SSSCIP State Cybersecurity Centre and the Computer Emergency Response Team of Ukraine (CERT-UA), jointly with the teams of the best Ukrainian cybersecurity companies and the world's major producers of solutions provide comprehensive assistance in establishing multiple-tiered cyber defense systems of the IT infrastructure for institutions and organizations, irrespective of ownership.

The analytical document is prepared by the experts and analysts from the State Service of Special Communications and Information Protection of Ukraine.

If you want to receive regular updates, please subscribe to our analytical mailing at:

<http://eepurl.com/hZS6Xj>



All of us must stay resilient to external challenges, continue providing services to people and ensure the functioning of the business and the economy in whole. Please, send your requests to our official e-mail address

cert@cert.gov.ua

and we will provide you with targeted assistance in defense against cyberattacks, security monitoring, migration to cloud environments, deployment of state-of-the-art systems to defend your workstations and servers against cyberattacks, etc.

Follow the State Service of Special Communications and Information Protection of Ukraine:

www.cip.gov.ua

www.facebook.com/dsszzi

www.instagram.com/dsszzi

www.t.me/dsszzi_official

www.twitter.com/dsszzi

Prepared with the support of the European Union and 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) and the support of the European Union. The authors' views expressed in this publication do not necessarily reflect the views of USAID, the U.S. Government or the EU.



State Service
of Special Communications
and Information
Protection of Ukraine

WAR IN UKRAINE. PULSE OF CYBER DEFENSE
September–December 2022