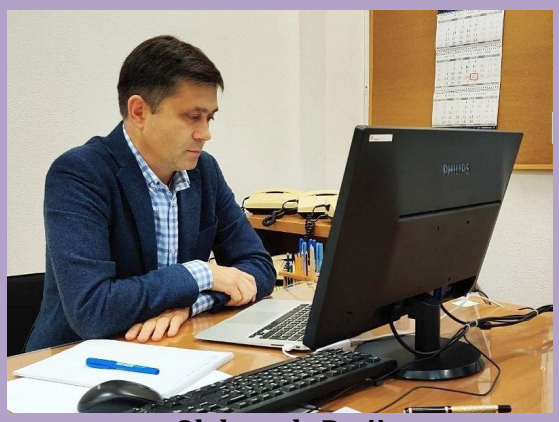
INTERVIEW WITH THE LEADERSHIP OF THE STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE

The State Service of Special Communications and Information Protection of Ukraine (SSSCIP) was established on February 23, 2006. The SSSCIP is a specialized central executive authority for special communication and information security, a defense and security agency being the principal actor in the national cybersecurity system. It coordinates the activities of cybersecurity actors in the field of cyber defence and administers communication.

- Website https://cip.gov.ua/
- Email for official correspondence: info@dsszzi.gov.ua
- Email for the media: press@dsszzi.gov.ua

Yurii Shchyhol
Head of the State Service of Special Communications and Information Protection of Ukraine

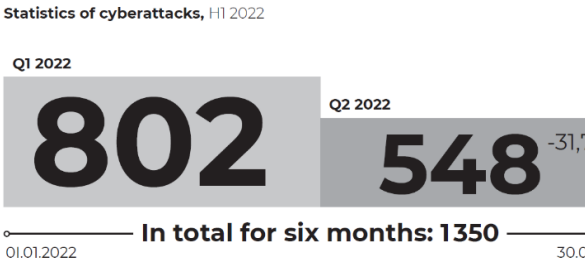


Oleksandr Potii
Deputy Chairman of the State Service of Special Communications and Information Protection of Ukraine

Russian aggression against Ukraine is going on, Russia keeps violating international law by waging unlawful attacks on land, at sea, in the air and in cyberspace.

Russian hackers do not seem to be curtailing their activity. Instead, they are still trying to attack Ukrainian infrastructure and even descending to civilian targets.

The most widespread cyberattack methods are infiltration into information systems and malware distribution. Yet, scammers' attempts to mislead the people have also increased substantially since the beginning of the full-scale invasion. They swindle banking card data under the guise of payments from various Ukrainian and foreign public agencies to withdraw money from those cards



Top sectors targeted by russian hackers

- Government and local authorities
- Security and defense
- Energy sector
- Financial sector
- Commercial sector
- Telecommunication sector and developers
- Transport sector

The most widespread types of cyberattack

- Malicious code
- Intrusion
- Intrusion attempts
- Violation of information properties
- Accessibility disruption
- Dangerous (abusive) content
- Known vulnerability
- Scam

All the cyberattack methods used by Russians are well known, there are no high-complexity or hardly identifiable ones among the latest cyber incidents. Phishing accounts for around 60 to 70% of Russian hacking attacks on Ukraine's public sector, recorded by the CERT-UA

Phishing emails help russian hackers steal user account data and use compromised accounts to distribute spyware or destruction software. Their proficiency in creating phishing emails has reached a high level over the years of regular cyberattacks on Ukrainian infrastructure.

This is why protection of account credentials is becoming an increasingly pressing issue when it comes to public officials and critical infrastructure personnel. This concerns not only Ukraine, but the entire world as well, because information security experts are already detecting intensification of russian hackers' activity all around the world.

Current Russian war against Ukraine has given mature democracies some extra evidence that it is no one but Russia behind aggressive attacks on critical infrastructure all over the world

Attacks on energy infrastructure never stop since the Ukrainian energy system was

disconnected from Russia and synchronized with the EU. Russian security services are not even trying to conceal their illegal interference. Ukrenergo, Ukraine's transmission operator, has reveals the facts of scanning their systems by the russian Federal Guard Service and SC Roscosmos. Russian group Killnet claims to be responsible for the latest overt attacks on Lithuania, a NATO member.

Russian cyber troops show that their actions are tightly coordinated with land and missile assaults. On June 22, Russian troops assaulted Mykolaiv city, the administrative center of a southern region of Ukraine, bordering currently occupied Kherson region. A total of seven missiles hit the city.

Roughly at the same time, Mykolaiv region suffered a cyberattack. Russian security services attacked the email server of the Mykolaiv Region State Administration on the very next day, June.

Because of that, they have gained access to the mailbox of the regional press center. Russian hackers coordinate their targets with attacks on the fuel and energy sector as well. Due to the invasion, Ukraine has found itself cut off from usual fuel supply and petroleum refineries and fuel depots have become permanent targets for missile assaults. To make gas and diesel fuel imports for Ukrainian road transport even more difficult, hackers have attacked online resources of the National Transport Safety Agency of Ukraine.

A well-coordinated DDoS attack by a russian hacking group on the dsbt.gov.ua web addresses and the SHLIAKH system servers was launched on June 28. As this system is used to manage the national border crossing, it has affected road traffic speed at Ukraine's international checkpoints. The traffic has been hindered for six hours.

The response to such attacks should be collective, joint and united. A collective security policy is the only way for all of us to defend ourselves efficiently

This approach is already being implemented at the top level. It is stated in NATO Strategic Concept 2022 https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
and the G7 Leaders' Final Communiqué https://www.consilium.europa.eu/media/57555/2022-06-28-leaders-communique-data.pdf

Sharing threat indicators and joint training exercises of cyber defense specialists working for the public sector are the two primary aspects of the collective cybersecurity system. Deeper integration of Ukraine into the CCDCOE will contribute to setting this system up. In late May, the Ukrainian delegation participated in a meeting of the NATO Cooperative Cyber Defence Centre of Excellence for the first time.

Joining the CCDCOE will be an important step for our country towards the enhanced international cooperation
in cybersecurity and cyber defense, as well as towards NATO membership for Ukraine. Granting the EU candidate status to Ukraine will also facilitate cooperation with relevant European institutions.

New methods of cyber defense are being shaped here in Ukraine through successful resistance to attacks. The key elements of cyber defense are sufficient funding at the national level as well as at private companies managing critical infrastructure, efficient use of these funds, cyber hygiene at all levels, and extensive international cooperation

Despite the ongoing war, Ukrainian Government has granted extra UAH 1.2

billion to the Administration of the State Service of Special Communications and Information Protection. These funds will be allocated for the purpose of further construction of the National Information Resource Backup Center and cyber defense, such as software update and backups of the national critical public information resources.

The SSSCIP stands on the frontline in this cyberwar, defending the national IT infrastructure. The SSSCIP Head Yurii Shchyhol has presented his analysis of the firs lessons learnt in the ongoing cyberwar to the global expert community: https://www.atlanticcouncil.org/blogs/ukrainealert/vladimir-putins-ukraine-invasion-is-the-worlds-first-full-scale-cyberwar/

Conclusion

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.

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 cyber attacks, security monitoring, migration to cloud environments, deployment of state-of-the-art systems to defend your workstations and servers against cyber-attacks, etc.