THE 18TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

Cyber Attacks in the Context of Russian-Ukrainian War

Luca Iamandi[1], Ionel Vladimir Vîrgolici[2], Alina Melania Ioniță[3], Alexandru Drăgănescu[4]

Abstract: Geopolitics studies are becoming more and more important in the current context, because the conditions that influence the evolution of a state are determined by its relations with the states around or in the region, as well as the area of economic, political, cultural, ethno-confessional and military relations- strategic. From this point of view, in the past, there were some archaic ideas that became the subject of various schools of political, geographical and humanistic research, as well as modern investigations of geopolitics, geostrategy and geointelligence. Moreover, it is important to identify how the inherent risks of hybrid warfare can be combated, including knowledge and understanding of the notions and concepts that underlie it, as well as the institutions capable of countering it and ensuring security. The use of information technology has become essential for the proper functioning of society. Despite all the risks involved, the world continues to make use of computer systems, thus triggering an increase in cybercrime, which has become an important piece of the criminal puzzle. In response, states are encouraged to take steps to modernize the legal framework necessary to sanction people who use computer systems to commit illegal acts. It is also important that people engaged in the fight against cybercrime receive the appropriate education.

Keywords: Cyber-attacks; Information; War; Security; Ransomware

1. Aspects of Cyber-Attacks in the Context of Russian-Ukrainian War

It has been shown that since the spatial and political relations in an area became interconnected as the scientific concept began to develop. These archaic ideas have survived in different fields of study such as political, geographical, or humanistic, manifesting themselves especially in geopolitics, geostrategy and the rest of similar scientific applications, this knowledge adapting to new regional and global challenges. With the hybrid war, many NATO member states had the obligation to fight on multiple fronts, including the security, knowledge and understanding of this combat corridor, without taking care of the alliance to risk losing this ideological war. More recently, the most profound geopolitical research focuses on the studies of the evolutions of some nations in the geopolitical context, in the case of relations in the more distant geographical space, but also the area of economic, political, cultural, ethno-confessional and military-strategic relations, which. they are conditioned by cooperation.

The third quarter of 2022 marked a change in terms of cyber-attacks in Europe. Analyzing a year of cyber incidents and attacks in Europe, the report highlights a transition from using the conflict in Ukraine

[1] Professor, PhD, Danubius University of Galati, Romania, Address: Blvd Galati, No 3, Galati, Romania, E-mail: luca_iamandi@yahoo.com.
[2] Ministry of Finance, Romania, Address: B-dul Libertății nr. 16, District 5, Bucharest, Romania, Corresponding author: vladimir.virgolici@gmail.com.
[3] Ministry of Finance, Romania, Address: B-dul Libertății nr. 16, District 5, Bucharest, Romania, E-mail: alina.ionita@mfinante.gov.ro.
[4] Regional Transport Police Department, Romania, Address: Str. Gării no.1, District Galati, County Galati, Romania, E-mail: draganescu_alexandru@yahoo.com.

to deliberately launch cyber-attacks with Russia, to creating a high-intensity hybrid cyber war targeting Poland, the Baltic states and Nordics, as well as to several key sectors of society, including aviation, energy, healthcare, banking and public services. As part of its strategy to expand its influence in the region, Russia uses destruction campaigns, cyberbullying, as well as DDoS attacks to temporarily disable servers and affect various services.

Over the past year, the geography of cyber attacks related to the conflict in Ukraine has changed. At the beginning of the conflict, most incidents were concentrated mostly in Ukraine (50.4% compared to 28.6% in the third quarter of 2022). However, in the last six months, European countries have seen a high rate of incidents (46.5% of global attacks vs. 9.8% in the first half of 2022). In the summer of 2022, European countries reported almost as many incidents as Ukraine (85 vs 86), and in the first quarter of 2023, many incidents (80.9%) occurred within the European Union. In addition, countries such as Montenegro and Moldova, which have applied for European integration, have recorded a high number of incidents in the last two years (2.7%, compared to 0.7% in the third and fourth quarters of 2022). Poland experienced the highest number of conflict-related cyber incidents, 114 in 2022, while the Baltic and Nordic countries were also targeted by war hacktivists. Germany also had a relatively high number of reported incidents (58), while France, the UK, Italy and Spain reported a low number of incidents.

At the same time, the beginning of last year led to a change in the destination for which ransomware attacks were designed. Thus, on 24.01.2022, against the background of the escalation of tensions between Russia and Ukraine, the instruments specific to the hybrid war begin to make their presence felt. A group of hackers has carried out a ransomware-type cyber attack on the servers used by the railway system in Belarus, making it difficult for trains to run. Their main purpose was to disrupt the movement of trains, thus managing to slow down the railway transport, towards the border with Ukraine, of Russian weapons, carried out on the territory of Belarus.

In response to the conflict in Ukraine, some European Union countries have imposed measures that prohibit the use or purchase of computer security products made in Russia or by Russian companies. This is due to fears that the Russian Federation could use such solutions to launch cyber attacks. For example, BSI, Germany's Cyber Security Authority, has issued a warning about the increased risk of critical infrastructure companies being the target of a cyber attack from the Russian Federation.

At the end of 2022, Law No. 354/2022 entered into force, requiring public and local institutions to ban the use of antivirus products of Russian origin, such as Kaspersky. The establishment of prohibitions by Law no. 354/2022 on the protection of information systems of public authorities and institutions in the context of the invasion launched by the Russian Federation against Ukraine is substantiated by the launching of the war against Ukraine by the Russian Federation and the interference of its interests in the activity of some companies that develop and provide programs intended for computer security.

The legislation provides that non-compliance with the restrictions is a misdemeanor and can be punished with a fine between 50.000 and 200.000 lei.

In the context of the hybrid war, where China wants to hold global supremacy, the Tiktok application was created that allows users to upload their own videos to be viewed by other users. Considering the aforementioned, during the meeting of the Cyber Security Operative Council, which took place in accordance with the legal provisions of Law no. 58/2023 on Romania's cyber security and defense, on 18.05.2023, it was decided that all employees in the public system should only use the TikTok application on the devices they own from work. Thus, employees in public institutions are advised not to install and access the application of Chinese origin on their work phones, due to the security risks it involves.

The decision of the Romanian authorities comes some time after the United States, Great Britain and other European Union member countries banned the installation and use of the TikTok application on service devices. The European Parliament and the European Commission decided in March 2023 to ban the application.

The reasons behind such a decision relate to the security of using the TikTok app, an app owned by a Chinese company called ByteDance that has ties to the Chinese government. Amid concerns about Beijing's interest in collecting data on users who use TikTok, the app is under scrutiny by governments and regulators in several Western countries.

The danger that the TikTok application generates is that it collects a large amount of information about the user's device, namely: device model number, device MAC address, SIM card serial and IMEI, Wifi SSID, phone number, GPS coordinates, Device IP, device operating system, patterns and keystroke cadence.

The application keeps Track active and when it is disabled it can remotely debug the application, it can run new processes automatically, it has full access to the Clipboard (creates security risks because a significant number of Password Manager applications exploit the clipboard), makes an age and gender profile of the user, collects information about other services and applications installed on the device, monitors all data entered.

Global cyber reports since the beginning of the conflict have revealed a 61% percentage, committed by pro-Russian hacktivist groups. Among them, Anonymous Russia, KillNet and Russian Hackers Team became evident in the war, reflecting the optimization efforts of the Ukrainian IT army. These newly established groups are better organized, and the resource they need is usually a botnet-as-a-service2, such as the Passion Botnet, with the aim of harassing Western countries that support Ukraine.

These groups see themselves as independent, civil hacktivists rather than cybercriminals. They come with different nationalities and diverse technical skills. Data shows that they have focused on DDoS attacks over data breaches, theft, espionage, influencer campaigns and other types of intrusions such as phishing, ransomware and information theft. These attacks aim to increase anxiety to deter support for Ukraine without major operational impact. In contrast, data erasure attacks would cripple the adversary's systems, and long-term espionage would undermine their integrity.

Russian authorities systematically resort to the use of cyber attacks to harass their enemies, without investing in a real war.

2. Ransomware - the Computer Tool most used in Hybrid Warfare

Ransomware is a type of computer threat that prevents access to or encrypts data stored on a compromised device. To regain control of the device or encrypted data, the affected person is required to pay a certain amount of money as a reward. There are over-the-air programs that can facilitate the removal of an infection, but they are generally ineffective against crypto-extortion threats, because without the file decryption key, their recovery becomes virtually impossible.

Prestige Ransomware first appeared on the global external threat landscape in October 2022. The ransomware is called "Prestige ranusomeware" in its note left on victim devices. The ransom note does not list any specific amount of money expected by the hackers and simply provides an email that the victim can contact and inquire about a decryption tool.

The researchers noted that the attacker had already gained access to privileged credentials from a previous compromise for the targeted networks to deploy the ransomware. So far, this campaign has found no tangible link to a known threat actor attempting to deploy ransomware on Ukrainian enterprise networks. Or, to any of the existing ransomware groups that may be related to previous recent attacks by Russian-linked threat actors.

Despite using similar deployment techniques, the campaign is different from recent destructive attacks using AprilAxe (ArguePatch)/CaddyWiper or Foxblade (HermeticWiper) that affected several critical infrastructure organizations in Ukraine.

The Prestige campaign could mark a significant shift in how the Russian military calculates its rampant assault, helping to increase the risk to groups providing or transporting any kind of humanitarian or military assistance into Ukraine. On a large scale, it poses an increased risk to all organizations in Eastern Europe that are seen by Russia as supporters of this conflict.

In the context of the war in Ukraine, Microsoft company identified a ransomware cyber attack campaign called Iridium, which was associated with Prestige.

Iridium is a Russian threat actor tracked by Microsoft, publicly overlapped with Sandworm, which has been consistently active in the Ukraine war and has been linked to destructive attacks since the start of the war. This attribution assessment is based on forensic artifacts as well as overlaps in victimology, craft, capabilities, and infrastructure with known Iridium activity.

As a mode of operation, in carrying out its tasks, IRIDIUM carries out the targeting of high-privileged credentials, such as the Domain Administrator, by having an already existing access or by obtaining a credential through the previous compromise and using it to launch its ransomware domain. In most cases, the attacker already had existing access to high-privilege credentials or had gained unauthorized access by compromising such prior credentials. This gave the attacker an access path to deploy the ransomware code and ensure it remains on the system. According to the data, risks in Ukraine are constantly changing, with ransomware attacks and destructive crypto-implementation present. To reduce exposure, organizations must improve their security methods and investigate this constant threat. Thus, in the following chapter we presented a series of measures that must be taken to stop or prevent this type of cyber attack.

3. Recommendations

Organizations should act to protect themselves from destructive malwares, which pose a direct threat to their regular operations and critical data and assets. They should increase vigilance and assess their capabilities, including planning, preparedness, detection, and response to these incidents, particularly enterprise-scale distributed propagation methods. To improve their cyber resilience, organizations should consider addressing network architecture, core security, continuous monitoring, and incident response practices.

Destructive malware can use popular communication tools to spread, including worms, instant messages, and infected email attachments, providing a silent and efficient way to gain access. They can attack a wide range of systems and spread to multiple hosts and endpoints on a given network. Organizations should carefully scan their environment for any atypical activity, particularly with enterprise applications, patch management systems, remote monitoring software, asset management consoles, anti-virus systems, systems assigned to system and network administrators, centralized backup

servers and file shares. These can serve as entry points to spread malware and compromise additional resources, allowing isolation or degradation of critical data and application availability.

In addition, consideration must be given to devices such as centralized storage drives, network devices, and other resources, which could be acted upon by actors presenting the threat by manipulating routes, modifying binaries, and removing configuration attributes and/or firmware, which could significantly affect the availability of critical network resources.

Conclusions

Regarding the private environment to protect your systems and ensure the security of remote employees, it is essential to adopt a "zero trust" system. Create a business continuity plan to keep your organization safe in the event of an unforeseen situation. Pay close attention to any information source you or your employees' access, as certain web pages contain advertisements or links to malicious applications. Ensure that all employees identify and report all possible IT threats, including phishing and ransomware attacks, to the IT security team. Considering the solution of password management and multi-step authentication, also implement antivirus, endpoint detection and response and ad-block solutions in your systems and networks. To prevent the spread of a virus, fix any identified vulnerabilities in a timely manner and back up your company data in isolated or separate data centers. Also review the business relationships you have and, in case of identified risks, temporarily block connections from and to countries such as Ukraine and Russia.

References

Treaties, books, monographs, jurisprudence collections

Allen, John; Breedlove, Philip, M.; Lindley-French, Julian; Zambellas, George (2017). *Future war NATO from hybrid war to hyperwar via cyber war*, Globsec NATO adaption initiative, https://www.globsec.org/wp-content/ uploads/2017/10/GNAI-Future-War-NATO-JLF-et-al.pdf.

Amerson, Kimberly; Spencer, B. (2016). Meredith III, The Future Operating Environment 2050: Chaos, Complexity and Competition. *Small Wars Journal*.

Wolfgang, Ischinger, MSC Chairman, *Conferința de securitate de la München/ The Munich Security Conference*, 15-17 February 2019, https://www.securityconference. de/en/activities/munich-security-conference/munich-securityconference/msc-2019/overview/.

Standish, Reid (2018-01-18). Inside a European Center to Combat Russia's Hybrid Warfare. *Foreign Policy*. Retrieved 2018-01-31. [...] hybrid warfare: the blending of diplomacy, politics, media, cyberspace, and military force to destabilize and undermine an opponent's government.

CyberSecurity Help (2022). *Former Conti Hackers Adapt Their Techniques to Use against Ukraine*. https://www.cybersecurity-help.cz/blog/2878.html.

ENISA (2021). *Enisa Threat Landscape* 2021. https://www.enisa.europa.eu/publications/enisa-threatlandscape-2021.

Gatlan, Sergiu (2022). *Google Says Former Conti Ransomware Members Now Attack Ukraine*. BleepingComputer. https://www.bleepingcomputer.com/news/security/google-says-former-contiransomware-members-now-attack-ukraine/.

International Conference RCIC'18. 365-372. https://www.afahc.ro/ro/rcic/2018/rcic'18/ volum_2018/365-372%20Surdu.pdf.

UNODC. (2021). Digest of Cyber Organized Crime. https://www.unodc.org/documents/organizedcrime/tools_and_publications/21-05344_eBook.pdf.

Gaskin, Lee (2022). *Bots Manipulate Public Opinion in Russia-Ukraine Conflict*. The University of Adelaide. https://www.adelaide.edu.au/newsroom/news/list/2022/09/08/bots-manipulate-publicopinion-in-russia-ukraine-conflict.