Bulletin of "Carol I" National Defence University
10.53477/2284-9378-22-92

HOW THE RUSSIA-UKRAINE WAR MAY CHANGE THE CYBERCRIME ECOSYSTEM

Student Claudia–Alecsandra GABRIAN, Ph.D. Candidate*

According to statistics, in recent years there has been an increase in cyber-attacks and their negative impact on individuals, organizations, and governments. Cyber attackers have acquired the resources and expertise to launch massive attacks against other nations to gain strategic advantages, mainly targeting critical infrastructure and public services. Current geopolitical events, through the action launched by the Russian Federation in Ukraine, demonstrate that cyber security threats are ever greater. States' responses to these challenges must be quick and effective, adapted to this context. Over the past year, Russian cybercrime groups have strengthened their position as threats to the global digital ecosystem, demonstrating adaptability, persistence, and a willingness to exploit computer systems. This paper will analyze how cybercrime groups have been more present in the international space due to this war, as well as the importance given to them due to the types of attacks launched and their division into belligerent support camps.

Keywords: Cyber Attacks; Cyber Crime Groups; Ransomware; Cyberspace; Cyber Security; Resilience.

Cyberspace represents an environment of strategic importance, which is made up not only of the Internet and all the technologies, respectively hardware and software interconnected globally, but also of the actions carried out by their users, which make it possible to generate, process, store or transmit data in electronic format. To protect such systems, a better understanding of cybercrime is a necessary condition in order to develop appropriate responses to prevent and combat these types of threats. This phenomenon of cybercrime has global implications, transcends geographical borders, and can be carried out from anywhere, against any person and any technology. There is no single definition of the term cybercrime, but it describes a variety of illegal crimes or what is considered illicit behavior by individuals/groups that launch attacks on critical IT devices, networks, systems, and infrastructure (Donalds and Osei-Bryson 2019).

In response to these ever-growing and ever-present threats, governments around the world have adopted strategies and enforced them through legal frameworks to establish better computer security, a concrete example being Computer Incident Response Teams (CSIRTs, referred to in usual CERT mode), to improve response. They investigate and prevent these types of illicit cyber activities involving the use of information and communication technologies (ICT). According to Ngafeeson, the classification of cybercrime is one of the three important elements to combat it, and Barn argues that a better understanding of cybercrime is a necessary condition for developing appropriate responses and for correct estimates of economic costs, in particular (Donalds and Osei-Bryson 2019). (Donalds, Osei-Bryson, 2022).

The meaning of the term "hacker" has changed over time, and the activities of hackers are usually seen as illegal actions operating in hidden environments, but this is true when they cause intentional damage to society's information systems. Hackers are the primary agents of cybercrime, and their subculture is complex and encompasses multiple motivations, degrees of idealism, and skill sets. Attackers are individuals or groups of individuals who attempt to exploit vulnerabilities, often for personal or financial gain, and they may work for governments conducting espionage for the new battlefield (Sabillon, et al. 2016).

Hacking becomes illegal once it crosses the threshold of gaining unauthorized access to computer systems. Hackers are classified into several categories such as white hats, which work under ethical hacker laws or as security experts; gray hats, who work as security consultants, and black hats, who are motivated by power, anger, or hatred, and have no qualms about stealing or destroying data from networks. Another

Babeș-Bolyai University, Cluj-Napoca
e-mail: *claudiaalecsandra@yahoo.com*

important category is cyber terrorists who are part of the category of those who use shorthand and cryptology to exchange information and exchange data online to steal information of important value to society, and hackers as government agents are those individuals or groups who work for specific government purposes that may compromise national cyber security. Cyberterrorism is another element that is part of the construct of what is called cybercrime and refers to that class of cyber terrorists who exploit computer vulnerabilities. Attackers are motivated by political ideology, religion, hacktivist tendencies, or personal motives, and cyber theft refers to those cybercriminals who seek financial gain by stealing and selling information in all possible ways (Sabillon, et al. 2016).

Cyber vulnerabilities are exploited through cyber-attacks, and as technology evolves, new risks and threats emerge that will lead to more advanced hacking Techniques, Tactics, and Procedures (TTPs). In this case, advanced persistent threats (APTs) are known, which refer to when an adversary possesses sophisticated levels of expertise and sufficient resources to achieve their objectives using multiple attack vectors, through target selection, target reconnaissance, command and control, data mining, information dissemination, and information exploitation. Cybercriminals' targets are critical infrastructure, healthcare, public health, information technology (IT), financial services, and energy sectors (Sabillon, et al. 2016).

From the category of cyber-attacks, the following are mentioned: identity theft, which involves stealing someone's identity, whereby the attacker claims this role to obtain financial benefits. Phishing represents a category of fraudulent processes that steal confidential information from users using spam email. Distributed Denial-of-Service (DDoS) refers to those attacks that use a network of several or even thousands of zombie computers that attack a specific target to overload it for failure. Malware attacks are malicious software that is installed through various viruses, and worms, and ransomware is a category of malware that locks users' data to receive payment for unlocking the data (Sabillon, et al. 2016).

Cybercrime is constantly on the rise as these attackers advance through new technologies such as artificial intelligence (AI). From the point of view of obtaining financial goods, the most representative forms of cybercrime are economic espionage, intellectual property theft, financial crime, and ransomware. In terms of state support for cybercriminals, some states are permissive and use the information obtained by them for domestic purposes, for example, in Russia, where there is a close link between the state and organized crime that protects the most advanced cyber criminals. In Russia, cybercrime groups are allowed to pursue their financial motivations, and they are protected by the law, but in exchange for this protection, they must use their skills to support the interests of the government (Smith and Lostri 2022).

Cybercrime groups

Cyberspace has become an important area of warfare, taking place primarily on the Internet, where nations can fight without pooling troops and capabilities. This allows countries with a small military presence to be as powerful as other nations in cyberspace by penetrating other nations' computer systems and networks. These attackers have the resources and expertise to launch massive Internet attacks against other nations, to cause damage or disrupt services, such as shutting down a power grid, but also to gain strategic advantages. The presence of cybercrime groups is more prominent and they seek to cooperate with cybercriminals who have essential skills that these groups can use or need to carry out certain operations, and these people can be coders and hackers.

Information technology has transformed the way certain groups are structured and organized, and criminals can collaborate on hacking activities using pseudonyms, and the risk of revealing their identities and locations to other group members is relatively low. One of the main challenges is the identification of organized cybercrime groups as the extent to which these groups operate exclusively, predominantly, and/or partially online (UNODC 2021). A nation can constantly attack another nation's infrastructure, steal its military secrets and collect information on technology to bridge industrial and military gaps, and the implications of disclosing personal data and access to sensitive data can give attackers the ability to blackmail even government personnel (Neethu 2020).

The current geopolitical events, through the action launched by the Russian Federation in

Ukraine, have transformed the world and people have been put in front of the war in Europe. Seizing this opportunity and pursuing political, economic, and military interests, cyber security threats have become bigger and bigger, and cyber security challenges are evolving and will continue to do so. The security of people and cyber networks has acquired a political significance concerning the state, society, nation, and economy, and the targeting in particular of critical infrastructures intersects with financial, transport, energy, and national security infrastructures (Surdu 2018, 365-372).

Ransomware attacks and CONTI grouping

Over the past year, Russian crime groups have solidified their position as threats to the global digital ecosystem, demonstrating adaptability, persistence, and willingness to exploit computer systems. A ransomware attack involves malicious software that deploys malware to encrypt and exfiltrate data, which it then holds for ransom, often demanding payment in cryptocurrency. Moreover, attackers exfiltrate sensitive data before deploying ransomware to prevent victims from backing out of negotiations. According to statistics, ransomware actors have shifted from a high-volume opportunistic approach to a more selective methodology in choosing victims. Attacks on medical systems have increased, due to perceived weaker security controls and the greater propensity of these victims to pay the ransom due to the criticality of their services. Additionally, since late 2019, ransomware groups have adopted new extortion tactics to maximize revenue and create an additional incentive for victims to pay. In one such tactic, known as "double extortion," ransomware operators exfiltrate massive amounts of a victim's data by encrypting it and then threatening to publish the stolen data if ransom demands are not met (Financial Crimes Enforcement Network 2021).

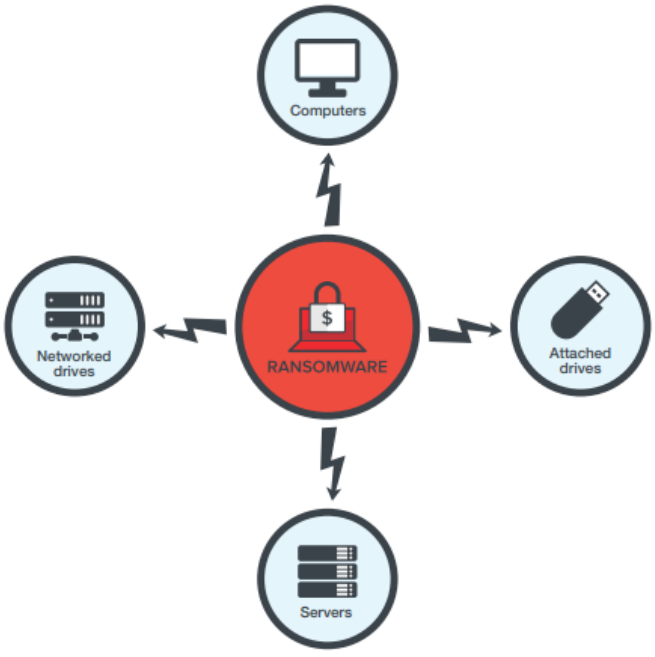

Figure no.1 Ransomware attack mode (TrendMicro 2021)

The second half of 2021 was rich in ransomware attacks, they were not only very active, but also increasingly aggressive. If the number of detections per active customer per country is considered, then we get a slightly different distribution. The following table shows the percentage of customers with at least one malware detection per country in 2021, and here it is noted that the Republic of Moldova has been the target of malware attacks since 2021. This raises several other questions about whether the Republic of Moldova was targeted by several cyber-attacks before the war in Ukraine started, which indicates that most of the time, analyzing the evolution of cyber-attacks, as well as their targets and their change, mainly determines a thorough analysis of the goal pursued by these types of attacks, as well as why the Republic of Moldova represented a target for them.

Ransomware is one of the most profitable cyber-attacks at the moment; it will continue to expand to macOS, and Linux, as well as new environments such as virtual cloud systems and IoT, in general, anything that is connected to an access network is a potential target (Acronis 2021). Most ransomware attacks come from Russia or its allies, and so most ransomware will try to see if a computer is running a common language spoken in Russia or one of its close allies, and if the answer is favorable, the ransomware will abandon the attack. Some attackers recommend enabling Russian as a second language on your computer, if possible, in order to prevent more ransomware from infiltrating. Russia has thus become a cyber-safe country, or as they are also called „havens" for ransomware criminals, and today many ransomware clusters are located in or around Russia (Grimes 2021). During the reporting period, the frequency and complexity of ransomware attacks increased by more than 150% and thus became one of the biggest threats

facing organizations today, regardless of the sector they belong to. Cryptocurrency remains the most common payment method for these actors, with Monero being the preferred one due to the increased anonymity and unknown nature of transactions (ENISA 2021).

Conti is a Ransomware-as-a-Service (RaaS) that was first spotted in December 2019, as with other ransomware families, actors using Conti steal files and sensitive information from compromised networks and threaten to publish these data if the ransom is not paid (MITRE ATT&CK 2021). The Cyber Security and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed increased use of Conti ransomware in more than 400 attacks on US and international organizations. In typical Conti ransomware attacks, malicious cyber actors steal files, encrypt servers and demand a ransom payment (CISA 2021).

To secure systems against Conti ransomware, CISA, the FBI and the National Security Agency (NSA) recommend implementing mitigation measures that include requiring multi-factor authentication (MFA), implementing network segmentation, and keeping operating systems and software up to date (CISA 2021).

Conti actors often gain initial access to networks through spear phishing campaigns that use personalized emails containing malicious attachments or malicious links. CISA and the FBI observed that the Conti group used Router Scan, a penetration testing tool, to maliciously scan routers, cameras, and network-attached storage devices with web interfaces (CISA 2021).

Conti actors are known to exploit legitimate remote and desktop monitoring and management software. CISA and the FBI observed that Conti actors used different Cobalt Strike server IP addresses unique to different victims, and after the actors had stollen and encrypted the victim's sensitive data, they used a double extortion technique where they asked the victim to pay a ransom to release the encrypted data and threatened the victim with the public release of data if the ransom was not paid (CISA 2021).

As of February 28, 2022, Conti actors remained active and Conti ransomware attacks against US and international organizations were reported to have increased to over 1,000, with notable attack vectors including Cobalt Strike (CISA 2021). In May, this group shut down its operating platform and a decentralized hierarchy took place, and the US Department of Defense offered rewards of up to $10 million for any information that could lead to the identification of important individuals that are part of this grouping.

After they attacked the government of Costa Rica and a national security alert was put in place, this group voluntarily ceased on May 19, 2022, while an reorganization process was taking place in order to ensure the smooth transition of

Rank	Country	Percentage of clients with malware detections in Q3 2021, normalized
1	Taiwan	63.6%
2	Singapore	57.4%
3	China	55.5%
4	Brazil	55.2%
5	Republic of Moldova	50.5%
6	Russia	49.5%
7	Greece	43.3%
8	Bulgaria	41.3%
9	South Korea	40.6%
10	Israel	39.7%
11	Turkey	39.4%

Figure no. 2 Malware detections in countries (TrendMicro 2021)

members of the ransomware group. The takedown followed the group's public allegiance to Russia in its invasion of Ukraine, dealing a huge blow to its operations in Ukraine and causing the leak of thousands of private data. Conti's affiliation with Russia had other consequences, chief among them being its inability to extract ransom payments from victims due to economic sanctions imposed by the West (The Hacker News 2022a).

After Conti publicly supported Russia's invasion of Ukraine, a cybersecurity researcher identified the malware's source code and internal chats between affiliates and made them public. Conti and Hive are currently positioned as two of the biggest players on the ransomware scene. The Conti leaks were about exposing interesting inside information between Conti operatives, such as various jobs, roles within the organization, and their process for hiring new affiliates. Based on the chat logs that were analyzed between Conti and the victims, the following techniques are observed: Conti's communication style is relatively professional, marked by seemingly scripted introductions and an emotionless tone. Actors stay on message, explaining to the victim that they are infected and emphasizing the consequences for the victim if they fail to pay the ransom and try to convince them to pay as quickly as possible (Mckay 2022).

The latest known data on this grouping suggests that former members of the Conti cybercrime group were involved in five different attack campaigns targeting Ukraine from April to August 2022. According to the Google Threat Analysis Group (TAG), they identified those ongoing cyber activities targeting the Eastern European nation against the background of the Russian-Ukrainian war. UAC-0098 is far from the only Conti-affiliated hacking group to target Ukraine since the start of the war, targeting Ukrainian organizations and European non-governmental organizations (NGOs) (The Hacker News 2022c).

UAC-0098 is an initial access broker known for using the IcedID banking trojan to give ransomware groups access to compromised systems on enterprise networks (Gatlan 2022). A concrete example in this sense is given by Ukraine's Computer Emergency Response Team which detected a cyber-attack on Ukraine's critical infrastructure, which it attributed to UAC-0098, but this is not the only example of a massive cyber-attack that targeted Ukraine and the country's security systems (CyberSecurity Help 2022).

Changing the cybercrime ecosystem

Since this war is still ongoing, its impact on cyberspace and cybercriminal groups is considerable, as members of these cybercriminal groups reorganize their attack strategies and operate more in social media, to attract supporters. The call they make is mostly for both camps, and the Australian University of Adelaide discovered millions of fake tweets from an army of pro-Ukraine bots spreading disinformation and anti-Russian propaganda. The hashtag #IStandWithUkraine was posted by bots at a rate of 38,000 tweets per hour, and after that, the number of tweets increased to 50,000 per hour. The researchers note that the peak of activity of pro-Ukraine bots occurred between 6:00 PM and 9:00 PM in US time zones (Gaskin 2022).

Hackers being divided into two camps, pro-Ukrainian and pro-Russian, try in the virtual environment to obtain or transmit as much information as possible that could influence citizens in a certain way. A relevant piece of information on this topic is mainly related to the hacker group called Anonymous, who since the beginning of the war have shown their support for Ukraine, and thus have massively attacked the central operating systems of various institutions and state systems of Russia, a concrete example being the Central Bank of Russia. Instead, among the targets of pro-Russian hackers, there are also countries besides Ukraine that are targeted, for example, Poland. Most of the time, these attacks target the transportation industry and critical infrastructures.

In recent months, the joint efforts of defense and security institutions in several countries have made it possible to arrest prominent hackers from groups such as LockBit and Killnet, who were prosecuted for attacks against several institutions and organizations. Major cyber-attacks also targeted the intelligence services of countries such as Estonia, Poland, Romania, Bulgaria, and Moldova. For example, the pro-Russian group Killnet has claimed responsibility for several cyber-attacks, including an attack on the website and services of the US federal electronic tax

payment system. The Hive cluster also attacked more than 1,300 companies worldwide. It targeted a wide range of enterprises and critical infrastructure sectors, including government facilities, communications, critical manufacturing, information technology, healthcare, and public health (The Hacker News 2022b).

Once the war began, the cybercrime ecosystem shifted to targeting Ukraine in particular, creating a Ukrainian IT army estimated at around 215,000 volunteer affiliates targeting Russian state-sponsored media outlets. The military has executed cyber-attacks on approximately 8,000 Russian assets, successfully targeting the defense industry and countering disinformation campaigns by state-sponsored institutions. Ukrainian President Volodymyr Zelensky noted that Ukraine's IT army had successfully prevented more than 1,300 Russian cyber-attacks in the last eight months of the Russian invasion. For example, after Russia destroyed a major data center in the country, Ukraine moved to the cloud, allowing it to build public ledgers and make payments to war-affected citizens (Dark Reading 2022).

So far, cybercrime groups change this ecosystem by targeting Ukraine and the countries that support it, changing the way these groups have attacked in the past and the likely targets they would have had before this war. The fact that the mobilization of the population in social media is used to attract hundreds of thousands of people to hacktivism, does nothing but prove that this war is also found in cyberspace, it goes beyond the normal borders of territory and has global valence. Forecasts regarding these types of cyber-attacks take into account their scale and how these groups will act, as well as how the potential countries targeted by them will implement strategies to prevent major cyber-attacks, especially on critical infrastructures.

Conclusions

In the conclusions of the article, the following aspects can be mentioned that are justifiable for the researched subject; thus, it is found that cyber-attacks are increasingly complex, and the war in Ukraine is a source of motivation to support or not the belligerents by the cybercrime groups, hence the division of these groups into camps. Ransomware groups have been active since 2020, and in the Russian Federation, it is recognized that cybercrime groups receive support, which then acts in the interest of the state.

The CONTI group is relevant to analyzing how the current war may alter the cybercrime ecosystem because this relatively new group, which has supported and acted against states that do not support Russia's action, has been split only after several cyberattacks have been launched, and will then be resumed under a different identity, but essentially pursuing the same goal. In Russia, offensive operations are aided by advanced technology such as Artificial Intelligence (AI) and automation to provide command and control, and thus cyberspace can be seen as a much more advantageous area in hybrid warfare for these groups to exploit.

The fact that Russia is trying to isolate the Russian Internet from the global one is an example to justify arming Russia from within, to practice its cyber activities to target adversary countries. This increased its geopolitical influence and helped amplify its power as a strong player on the international stage. Geopolitics is an essential and indispensable tool for understanding and analyzing new cyber challenges, but the main factor in this equation is politics while geopolitics is the one that interacts and determines the purpose of cyber-attacks.

The international system may remain one in which the desires of member countries are consistent with the defense and integrity of cyberspace and the security of information systems and critical infrastructure, but the area of hybrid threats will be a more exploited and potential one for state or non-state actors, which will likely put pressure on the economy, politics, critical infrastructures, citizens, etc.

BIBLIOGRAPHY

Acronis. 2021. *Acronis Cyberthreats Report 2022 unveils cyberthreat predictions.* https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/.

CISA. 2021. *AA21-265A-Conti Ransomware TLP White.* https://www.scribd.com/document/529330620/AA21-265A-Conti-Ransomware-TLP-WHITE.

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

Dark Reading. 2022. "Ukraine's 'IT Army' Stops 1,300 Cyberattacks in 8 Months of War." https://www.darkreading.com/endpoint/ukraine-it-army-stops-1300-cyberattacks-war.

Donalds, Charlette, and Kweku-Muata Osei-Bryson. 2019. "Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach." *Computers in Human Behavior* 92: 403-418. doi:https://doi.org/10.1016/j.chb.2018.11.039.

ENISA. 2021. *Enisa Threat Landscape 2021.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

Financial Crimes Enforcement Network. 2021. "Financial Trend Analysis." https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.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-public-opinion-in-russia-ukraine-conflict.

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

Grimes, Roger A. 2021. *Ransomware Protection Playbook.* John Wiley & Sons Inc.

Mckay, Kendall. 2022. "Conti and Hive ransomware operations: Leveraging victim chats for insights." https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf?1651576098.

MITRE ATT&CK. 2021. *Conti.* https://attack.mitre.org/software/S0575/.

Neethu, N. 2020. "Role of International Organizations in Prevention of Cyber-Crimes: An Analysis." Nalsar University of Law, Hyderabad, 5-17. https://www.researchgate.net/profile/Neethu-N-2/publication/350525198_Role_of_International_Organisations_in_Prevention_of_Cyber-Cri.

Sabillon, Regner, Victor Cavaller, Jeimy Cano, and Jordi Serra-Ruiz. 2016. "Cybercriminals, Cyberattacks and Cybercrime." *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF).* 1-9. doi: https://doi.org/10.1109/icccf.2016.7740434.

Smith, Zhanna Malekos, and Eugenia Lostri. 2022. *The Hidden Costs of Cybercrime.* McAfee report. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

Surdu, Ileana-Cinziana. 2018. "Cybersecurity. Risks, Threats, and Trends of Manifestation in Romania." *International Conference RCIC'18.* 365-372. https://www.afahc.ro/ro/rcic/2018/rcic'18/volum_2018/365-372%20Surdu.pdf.

The Hacker News. 2022a. *Conti Ransomware Operation Shut down after Splitting into Smaller Groups.* https://thehackernews.com/2022/05/conti-ransomware-gang-shut-down-after.html.

—. 2022b. *Hive Ransomware Attackers Extorted $100 Million from over 1,300 Companies Worldwide.* https://thehackernews.com/2022/11/hive-ransomware-attackers-extorted-100.html.

—. 2022c. *Some Members of Conti Group Targeting Ukraine in Financially Motivated Attacks.* https://thehackernews.com/2022/09/some-members-of-conti-group-targeting.html.

TrendMicro. 2021. "Toward a New Momentum: Trend Micro Security Predictions for 2022." https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2022.

UNODC. 2021. "Digest of Cyber Organized Crime." https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05344_eBook.pdf.