ANALYSIS OF CYBER-ATTACKS IN SOME GEOPOLITICALLY EXPOSED COUNTRIES IN EUROPE

Boštjan Špehonja*
GEA College – Faculty of Entrepreneurship,
Slovenia

Ajda Fošner
GEA College – Faculty of Entrepreneurship,
Slovenia
ajda.fosner@gea-college.si

Robert Brumnik
GEA College – Faculty of Entrepreneurship,
Slovenia

Abstract

The goal of the research was to determine, analyse and compare the type and number of cyber-attacks in the chosen countries: Germany, the United Kingdom, Serbia, and Slovenia. In all four countries, we set up honeypots and in Germany, we installed the fifth server for managing and collecting data from honeypots. Each of the four servers had the identical setup of six sensors: secure shell sensor, file transfer protocol sensor, vulnerable website sensor, server message block sensor, point-to-point tunnelling protocol sensor, and sensor for structured query language protocol for working with databases SQL. Data collection lasted for 12 days in February 2021, during which we detected a total of 1.847.395 attacks. The server in the United Kingdom captured 31,53% of the overall traffic, the server in Germany 23,26%, the server in Serbia 22,71%, and the server in Slovenia 22,50% of the overall traffic. After exporting all unique IP addresses from all four servers, we found a significant 12,89% overlap of IP addresses attacking both the Slovenian server and at least one of the other servers. Moreover, we analysed 124 unique samples of malicious code uploaded on the Slovenian server, and all of them were identified before our data capture, confirming that no zero-day vulnerabilities were cached on the Slovenian server.

Key Words

*Corresponding Author

Cybersecurity; cyber-attacks; honeypot; Germany; the United Kingdom; Serbia; Slovenia.

INTRODUCTION

Cybersecurity is essential for building a resilient, green, and digital Europe. One of the key objectives is to achieve strategic autonomy while maintaining an open economy. This includes strengthening the capacity for independent decision-making in cybersecurity to enhance the EU's leadership in the digital domain and its strategic capabilities.

Cyber-attacks and cybercrime are becoming increasingly problematic and appearing in more sophisticated forms across Europe. This trend is expected to continue in the future, as there will be an estimated 22.3 billion Internet of Things devices connected worldwide by 2024 (European Council, n. d.). Given these predictions, both government institutions and the economy are aware of the importance of cybersecurity and defence. Therefore, on March 22, 2021, the EU Council adopted conclusions on the EU's cybersecurity strategy in the digital decade (European Council, 2021).

European Council addresses several areas for action in the coming years, including the establishment of a common cybersecurity unit, the implementation of key internet security standards, support for robust encryption, and the creation of a network of secure operation centres across the EU. Additionally, the European Cybercrime Centre, established under Europol, will assist EU member states in investigating cybercrimes and dismantling criminal networks.

The five most common threats in the past years identified by the European Union Agency for Cybersecurity are: system infection with malware, two different methods of cyberattacks, malicious emails with phishing attempts, attacks through web applications, and unsolicited emails (European Parliament, 2023). Many companies are engaged in security solutions or services to protect users and the information-communication environment from cyber-attacks. These include, for instance, antivirus systems, firewalls, and systems that use artificial intelligence for attack detection. The success of companies in catching attackers depends on how they have set up systems for detecting and collecting attacks. These systems, based on heuristics, artificial intelligence, and known attack patterns, identify new malicious patterns appearing on the internet.

Cyber-attacks can be divided into two categories based on their focus. The first category includes targeted attacks. The goal of such attacks is to infiltrate the precisely chosen target. The second category consists of automated attacks. The entire internet space is limited to 2^{32} IP address spaces, overseen by the non-profit organization ICANN, which distributes these addresses among countries. Malicious attackers create harmful software capable of autonomously and continuously searching for vulnerable systems online, without human interaction. To identify and study such malicious software, we deployed sensors on our own information-

communication and electronic means in multiple European countries. These sensors appeared as different services running on seemingly vulnerable software. The sensors were able to record the type and scope of attacks and, in some cases, the malicious code even automatically exploited the sensors.

Of course, many online services display cyber-attacks in real time based on such sensors, but these services do not provide results that can be used for research purposes. Therefore, we decided to set up our independent system and use the acquired data for further analysis. We stored all attempted attacks in a database, which formed the basis for analysis. We collected data from our servers in Germany, the United Kingdom, Serbia, and Slovenia. The countries were chosen based on their geopolitical exposure in Europe.

The purpose of this research was to determine, analyse and compare the type and number of cyber-attacks in the chosen countries. We assumed that due to its size and limited geopolitical and economic influence, Slovenia is not the primary target of hacker attacks, resulting in a smaller number of cyber-attacks compared to other countries. Further, we studied the origin of cyber-attacks. We assumed that the sources of cyber-attacks targeting Slovenia are distinct from those targeting Germany, the United Kingdom, and Serbia. We looked for any patterns or trends in the origin of cyber-attacks that would help us understand the goals and tactics of cyber attackers who target Slovenia and other countries under study. Finally, we assumed that a zero-day vulnerability file would not be uploaded to a server in Slovenia. Zero-day vulnerabilities are highly valuable to cyber attackers as they offer the advantage of being unpatched and undetected by security measures. We evaluate the level of security and potential danger of exploiting such vulnerabilities in Slovenia's information-communication infrastructure by looking into the existence or absence of zero-day vulnerability files in the country's server.

H1: The number of cyber-attacks in Slovenia is statistically smaller than the number of cyber-attacks in Germany, the United Kingdom, and Serbia.

H2: The origin of cyber-attacks in Slovenia is different from the origin of cyber-attacks in Germany, the United Kingdom, and Serbia.

H3: A zero-day vulnerability file will not be uploaded to a server in Slovenia.

MATERIALS AND METHODS

For the purpose of our research, we have set up four servers, one in Germany near the city of Nuremberg, one in the United Kingdom near London, one in Serbia in Belgrade, and the last one in Slovenia in Ljubljana. We selected Germany and England because both countries are among the top five EU countries in terms of the number of cyber-attacks in all

international statistics. This is an expected fact, as Germany is considered the economic engine of Europe. The United Kingdom, on the other hand, stands out as the country with the highest number of cyber-attacks in the EU in 2018. This is likely attributed to various factors, including the country's decision to leave the European Union, the impact of the COVID-19 pandemic, and the historically close ties with the United States of America. Serbia was selected as one of the study's countries, which is noteworthy because it isn't a part of the EU but is nonetheless in Europe. Serbia's participation in the study enables a larger and more varied perspective on cyberattacks in the region of Europe. Compared to EU members, Serbia may have different cybersecurity dynamics and problems.

In all four countries, we set up honeypots, virtual systems used as a trap to detect and prevent unauthorized access. Honeypots are security systems designed to detect and prevent unauthorized access or use of a computer system. They capture unauthorized users and hackers within the network in a way that allows them to be identified and prevented from causing further trouble (Lutjevich et al., n. d.).

In Germany, we installed the central software Modern Honey Network, a centralized server for managing and collecting data from our honeypots. To detect attacks, we installed on each server virtual vulnerable software called sensors. These are services that are virtually vulnerable and can be exploited by attackers. The software does not allow the complete takeover of the server but is designed to record attacks and upload files to the servers. Each executed attack on the service is logged in the database. Data collection for the research lasted 12 days and was conducted in February 2021.

All virtual private servers had the same configuration, running the Linux Ubuntu version 18.04 operating system, with the following vulnerable sensors:

- Secure Shell Sensor (SSH),
- File Transfer Protocol Sensor (FTP),
- Vulnerable Website Sensor,
- Server Message Block (SMB) Sensor
- Point-to-Point Tunneling Protocol (PPTP) Sensor,
- Sensor for Structured Query Language protocol for working with databases SQL.

All sensors sent data in real-time to the central server, responsible for collecting all the data and storing it in the database. The central server was located in Germany and did not have any sensors installed. All sensors presented themselves as outdated versions of services with known vulnerabilities. Attackers were able to connect to some sensors, exploit them, and upload malicious software to the server, while other servers were only used to record the number of requests made.

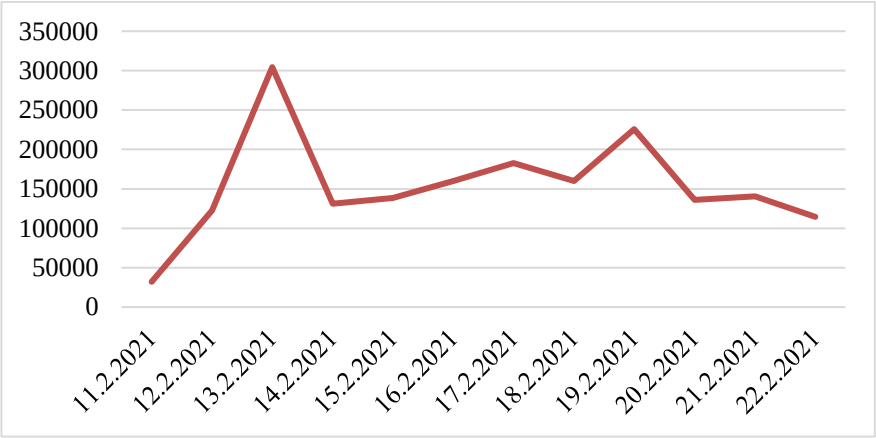
After setting up the sensors on all four servers, we verified whether they corresponded to the desired configuration. For testing the publicly accessible services, we used Nmap (version 14), a powerful and versatile network scanning tool that helps to discover open ports and services on target

systems. To minimize the risk of obtaining inaccurate or incomplete data, we manually checked each sensor before starting the data collection procedure.

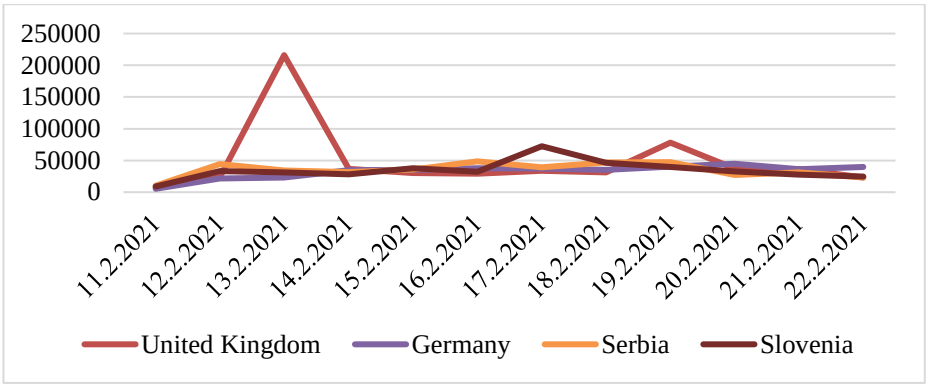
RESULTS

We collected the data for 12 days: from February 11, 2021, at 00:00 to February 22, 2021, at 00:00. During this period, we detected a total of 1.847.395 attacks across all sensors, which served as our primary source of information for conducting the analysis. On average, we observed 1,78 attacks per second. The lowest number of attacks (32.146) occurred on the first day of setup. This relatively low number of intrusion attempts on the first day can be attributed to the fact that servers were newly exposed to the internet. However, the number remains substantial, confirming that the internet is a hazardous space where various cyberattacks constantly occur. On the second day of data collection, we already recorded 122.480 detections on the sensors. The highest number of attacks was observed on the third day, reaching 304.411 incidents. The reason is the notable increase in attack attempts on the server in the United Kingdom. For the remaining days, there were more than 130.000 intrusion attempts per day, with the seventh day and the ninth day showing over 182.000 attacks.

Graph 1: The number of all attacks per day

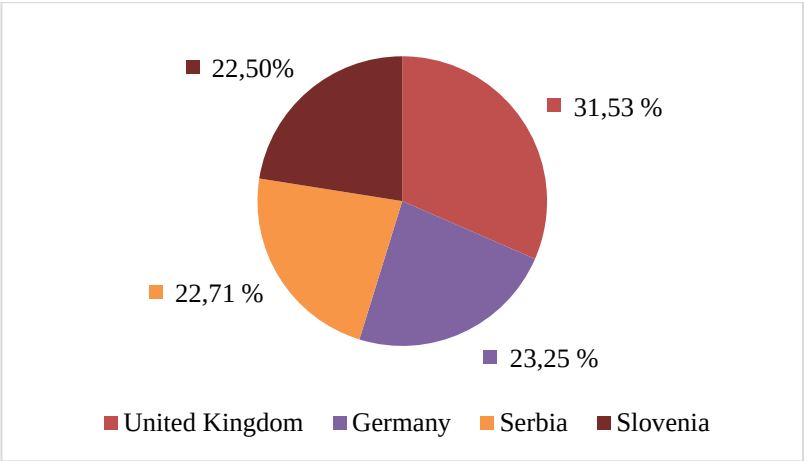


Graph 2: The number of all attacks per day per country



Graph 2 shows the number of all attacks distributed by days and countries. Summing up all the attacks for each country, we observed 582.562 intrusion attempts in the United Kingdom, 429.562 in Germany, 419.631 in Serbia, and 415.640 in Slovenia. The highest number of attacks was recorded in the United Kingdom, which was an expected result considering the other EU statistics regarding the number of cyberattacks. On the other hand, the lowest number of attacks was recorded in Slovenia with the highest number on February 17, 2021, with a total of 72,421 incidents.

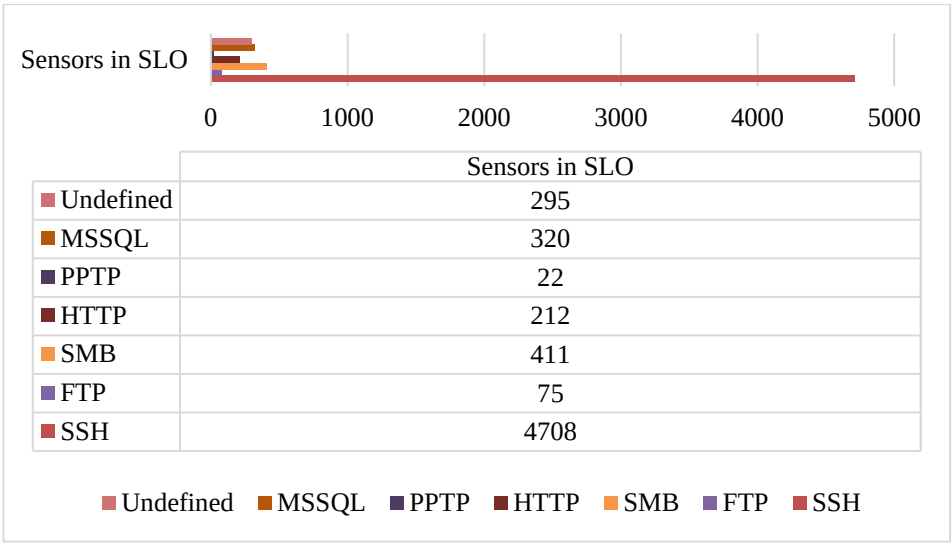
Graph 3: The percentage of attacks on individual servers



Further, we counted the number of unique IP addresses that attack individual countries during the observed period. In Serbia, we detected 13.644 unique IP addresses, in the United Kingdom 10.533 unique IP addresses, in Slovenia 10.104 unique IP addresses, and in Germany only 8,845 unique IP addresses. From this data, it can be concluded that each IP address in Germany sent an average of 48,56 requests, in Slovenia 41,13, in Serbia 30,75, and the United Kingdom 55,30. This means that attackers targeting the server in the United Kingdom are the most aggressive, sending the highest number of requests to the service during their attacks.

We compared IP addresses between the sensors on the Slovenian server and the sensors in other countries. During the observed period, we detected a total of 33.022 unique IP addresses on the German, United Kingdom, and Serbian servers. From February 11, 2021, to March 7, 2021[1], we identified 13,830 IP addresses on the Slovenian server. Therefore, we compared a total of 46.852 addresses. Graph 4 illustrates the number of individual IP addresses that were recorded on both the Slovenian server and on servers in other observed countries. The sensor for SSH has the highest number, with 4.708 IP addresses attacking Slovenian cyberspace and also being active elsewhere in Europe. It is followed by the SMB server with 411 IP addresses and the database sensor with 320 IP addresses. The FTP sensor had the lowest number of connections with 75, followed by PPTP with 22. In total, there were 6.043 detected addresses, representing 12,89% of all addresses, that attacked both Slovenian server and servers in other observed countries, which is higher than expected.

Graph 4: The number of IP addresses that were detected on the Slovenian server and at least one other server



	Sensors in SLO
Undefined	295
MSSQL	320
PPTP	22
HTTP	212
SMB	411
FTP	75
SSH	4708

Moreover, the overall analysis revealed that we detected 72 patterns of malicious code on both the Slovenian server and at least one other server. Additionally, 52 patterns were found exclusively on the Slovenian server. With these statistics, we cannot confirm the second hypothesis that Slovenian server would be attacked from different sources than servers in other parts of Europe. The highest level of matching was observed with the server in Germany, which experienced an increased number of attacks on the first and on second day of data collection. A total of 55 matching patterns were detected on both servers. On the server in the United Kingdom, we

[1] We extended the observation on Slovenian server.

detected 31 identical patterns, and on the server in Serbia, 37 identical patterns.

During data analysis, we worked with the hashed value of the files in the form of MD5[2]. We analysed all the hashed values on the website Virustotal, an online service where you can upload files, URLs, or search through an existing database of known patterns of malicious code. In the case of the server in Slovenia, after examining all the patterns, we found that all MD5 values were already entered into online services before we started capturing the traffic. With this, we confirmed the third hypothesis, which states that a zero-day vulnerability file will not be uploaded to a server in Slovenia.

DISCUSSION

Cyber-attacks refer to malicious actions carried out by individuals or organisations to breach, exploit, or interfere with computer systems, networks, or electrical equipment. A cyberattack may steal, alter, or destroy a specified target by hacking into a private network or otherwise susceptible system. These attacks may be carried out for a variety of reasons, such as monetary gain, political objectives, espionage, or just to disrupt services. As of today, cyberattacks have become increasingly sophisticated and dangerous. Moreover, in the digital era, cyber-attacks are a major worry because they can result in data breaches, the theft of sensitive information, financial losses, and damage to vital infrastructure.

To achieve the goal of our study, we have set up four servers, in Germany, the United Kingdom, Serbia, and Slovenia. We installed six sensors on each of the four servers: secure shell sensor, file transfer protocol sensor, vulnerable website sensor, server message block sensor, point-to-point tunnelling protocol sensor, sensor for structured query language protocol for working with databases SQL. All sensors presented themselves as outdated versions of services with known vulnerabilities. Attackers were able to connect to some sensors, exploit them, and upload malicious software to the server, while other servers were only used to record the number of requests made.

Data collection on the sensors was conducted for 12 days, during which we detected a total of 1.847.395 attacks, attempted attacks, connections, and queries. This data served as the basis for our analysis. The server in the United Kingdom captured 31,53% of the overall traffic, the server in Germany 23,26%, the server in Serbia 22,71%, and the server in Slovenia captured 22,50% of the overall traffic. These findings confirmed our first hypothesis that the number of cyber-attacks in Slovenia is smaller than the number of cyber-attacks in Germany, the United Kingdom, and Serbia. Moreover, we exported all unique IP addresses from the captured data that were associated with attacks on the sensor in Slovenia. We then used a web

[2] A128-bit cryptographic hash function that is commonly used to produce a fixed-size representation of data.

service's API to determine the country of origin for each IP address. We found only 11 IP addresses associated with Slovenia, some of them were listed on blacklists, indicating that their malicious activities were detected by other sensors. One of the IP addresses was linked to a legitimate web service, suggesting that an intrusion had occurred on a server that was being exploited for further attacks.

In the second hypothesis, we claimed that the server in Slovenia would be targeted by different sources compared to other parts of Europe. However, after exporting all unique IP addresses from all four servers, we found a significant 12,89% overlap of IP addresses attacking both the Slovenian server and at least one of the other servers. This indicates that 6.043 sources attacked both the Slovenian server and another server. Let us point out that the servers were not connected in a way that would allow the attacker to discover the locations of the other servers. This further confirms that the internet is a global space, and Slovenia is not exempt from cyber threats.

One of the sensors allowed attackers to exploit the server and upload malicious files. Each file's fingerprint was calculated and used for further research. We hypothesized that no "zero-day" vulnerability files would be uploaded to the server in Slovenia. These files contain vulnerabilities unknown to software and hardware manufacturers, making system administrators believe they are safe because they have installed all security patches and updates. Analysing 124 unique samples of malicious code uploaded during the data capture, we discovered three different types of malware. The majority of the files distributed ransomware WannaCry. Some samples were related to the worm Conficker, which exploits vulnerabilities in Windows operating systems, while others were associated with the Trojan horse that opens backdoors on infected systems, allowing attackers to gain access. We checked all samples against online databases of malicious software to determine when they were first detected. All our samples were identified before our data capture, confirming that no zero-day vulnerabilities were confirmed on the Slovenian server.

Throughout the data capture, we experienced several cyberattacks. Notably, the server in London experienced a massive attack on the third day of data capture. We initially believed that an attack had occurred on the web server sensor, but further investigation disproved this assumption. The administrator of an unknown website linked its domain to our server's IP address, which was detected by the sensors. The traffic from the website was temporary and ceased shortly after. On the thirteenth day of data capture, we encountered system slowdowns and bottlenecks due to resource limitations on the servers. Capturing such data is highly resource-intensive for the server, as log files and the database quickly fill up, leading to disk space shortages.

Our research has merely confirmed the fact that the increasing reliance on technology, interconnected systems, and the rapid expansion of the internet has provided cybercriminals with more opportunities to exploit vulnerabilities and launch various types of cyberattacks. There is no doubt that the current cyberattacks are sophisticated and complex. As cloud

services become increasingly popular, concerns about the security of data stored in the cloud have grown. Cyber attackers are incorporating artificial intelligence and machine learning into their tools and techniques making attacks more automated, adaptive and difficult to detect. Ransomware attacks have become particularly prevalent and lucrative for cybercriminals, cybercriminals have shifted focus to target the supply chain of organizations. With the proliferation of IoT devices, security vulnerabilities have emerged, making them attractive targets for cyberattacks. Let us also mention Dark Web and Cybercrime-as-a-Service.

Despite these efforts, cyberattacks are likely to continue to be a challenging problem in the future. To stay one step ahead of cybercriminals and safeguard the digital ecosystem, it will be necessary to maintain constant awareness, collaboration, and innovation.

CONCLUSION

The goal of this study was to examine and track cyber-attacks coming from various geographical locations to develop a thorough picture of the global cybersecurity landscape. We intended to gather information on cyber incidents from various geographic regions and multiple ports of entry on the internet by setting up servers in Germany, the United Kingdom, Serbia, and Slovenia. Using this strategy, we were able to examine the patterns and trends of cyberattacks coming from various regions. We were also able to discover potential cybersecurity weaknesses in particular areas and comprehend the strategies, methods, and procedures used by threat actors from various locations thanks to the distributed server arrangement. Thanks to this insightful information we can create stronger and more focused cybersecurity strategies and defences.

Additionally, having servers in these four countries enables us to cooperate with regional law enforcement and cybersecurity specialists to share knowledge, exchange threat intelligence, and together strive to reduce and effectively respond to cyber threats. Due to the fact that cyber dangers are not confined by national boundaries and frequently call for a coordinated worldwide response, international cooperation is essential in the fight against cybercrime.

In conclusion, our research using the four servers installed in Germany, the United Kingdom, Serbia, and Slovenia aimed to provide a thorough analysis of cyber threats and attacks from various origins, strengthen global collaboration in cybersecurity efforts, and improve the overall security posture in the digital environment.

REFERENCES

European Council. (22. 3. 2021). Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy. https://www.consilium.europa.eu/en/press/press-

releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy
European Council. (n. d.). Cybersecurity: how the EU tackles cyber threats. https://www.consilium.europa.eu/en/policies/cybersecurity
European Parliament. (21. 3. 2023). Cybersecurity: main and emerging threats. https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_en.pdf
Lutjevich, B., Clark, C., & Cobb, M. (n. d.). What is a honeypot? https://www.techtarget.com/searchsecurity/definition/honey-pot
Špehonja, B. (2021). Analiza kibernetskih napadov v geopolitično izpostavljenih državah na območju Evrope v primerjavi s Slovenijo [Master's thesis, GEA College – Faculty of Entrepreneurship]. ReVIS. http://revis.openscience.si/IzpisGradiva.php?id=8357&lang=slv&prip=rul:14889991:d3