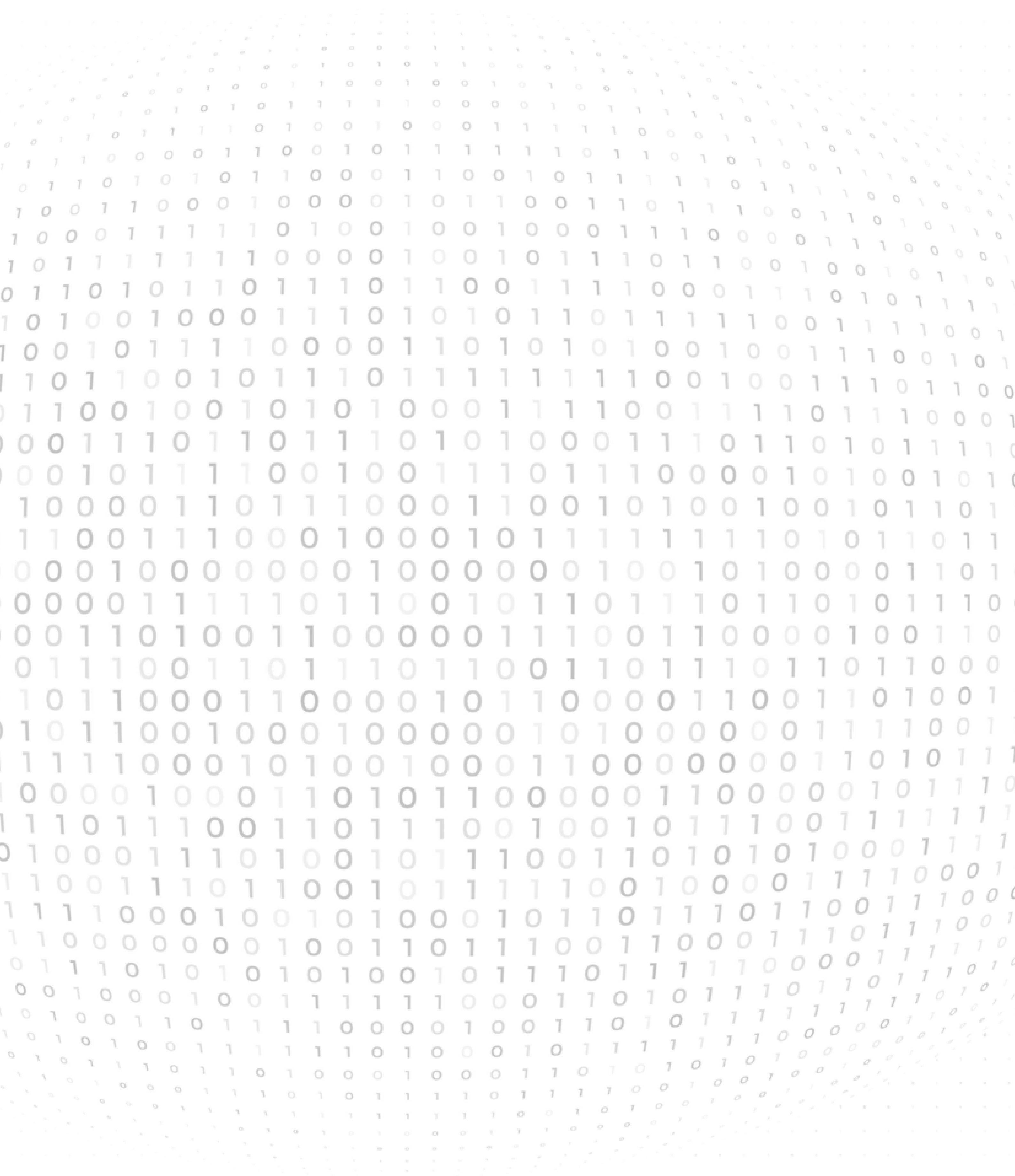
Bosnia and Herzegovina

CYBER SECURITY THREAT ASSESSMENT

October 2023

CSEC
Cyber Security
Excellence Centre

BIRN
BALKAN
INVESTIGATIVE
REPORTING
NETWORK
BOSNIA &
HERZEGOVINA



Bosnia and Herzegovina

CYBER SECURITY THREAT ASSESSMENT

October 2023

Written by:

Enes Hodžić and Aida Mahmutović
(BIRN BiH)

CSEC team

January – August 2023.

Cyber Security Excellence Center in Bosnia and Herzegovina (CSEC)
csec.ba

Balkan Investigative Reporting Network of Bosnia and Herzegovina (BIRN BiH)
Detektor.ba

Written by:
Enes Hodžić and Aida Mahmutović (BIRN BiH)
CSEC team

January – August 2023.

This is the second report on cybersecurity threats in Bosnia and Herzegovina, published by the Cyber Security Excellence Center (CSEC) in collaboration with the Balkan Investigative Reporting Network of Bosnia and Herzegovina (BIRN BiH). It covers the timeframe from January to August 2023, reflecting data collected by CSEC. It offers practical explanation of the threats, risks, and emerging trends in the national cybersecurity landscape, in the hopes of assisting government entities, the private sector, and the general public of BiH as they address these challenges.

Table of contents

1.

Summary of Main Findings

Recent findings from a foreign cybersecurity company have brought us closer to identifying the individual responsible for the attack on the State Parliament website last year. This year, the most frequent cyberattacks in the country have been those targeting private companies, increasing their costs. Victims are increasingly frustrated over the slow response from law enforcement, which leaves them unprotected and vulnerable while also impacting their revenue streams, resulting in financial losses. One attack on a media outlet left their readers without a reliable news source, while another ransomware attack on a gas company compromised customer data at the onset of the heating season. These incidents highlight system failures in legislation and resource allocation.

Slow law enforcement response results in the loss of important data about the attack, making it harder to identify the culprit and gather evidence. While Distributed Denial-of-Service (DDoS) attacks have decreased, media outlets continue to be prime targets, hampering public access to new information which can be crucial during times of crisis.

Throughout the reporting period, CSEC detected **15.4 million cybersecurity threats in BiH** through its DecoyNET Honeypot system, with **attacks increasing at a rate of 72 percent per month**. These alarming figures, couple with the latest institutional audits indicating the absence of a strategic and legal cybersecurity framework, illustrate the vulnerability of Bosnian citizens, companies, and institutions to cyberattacks that could jeopardize key sectors. Since the publication of the last report in March 2023, only marginal progress has been made in the creation of a more secure cyber environment in Bosnia and Herzegovina (BiH).

Scale of the Cyber Threat	The report reveals an increase of nearly 73 percent in cyberattacks per month as compared to the previous period.
Attack Types	Attacks on Private Branch Exchange (PBX) infrastructure were the most numerous in this period, with more than 1.7 million recorded incidents. These attacks are also known as “dial-through fraud.” This underscores the need for further investigation into the economic impact of such attempts on networks and everyday operations, as well as associated costs in Bosnia and Herzegovina.
Incident Highlights	– Media organizations suffered multiple DDoS attacks and reported slow responses from law enforcement. – The most prominent Sarajevo gas company suffered a Ransomware attack, which it dealt with through internal resources. – A hacker from Banja Luka was arrested under suspicion of a cyberattack-related abuse and extortion.
Attack Distribution by Country	In contrast to the previous report, the sources of attacks targeting entities in BiH have shifted, with France, the USA, Russia, Bulgaria, and Estonia now the most common origins. This shift supports the theory that attackers are using virtual private network (VPN) servers to conceal their data, making it harder to trace the attacks back to their point of origin.
Government Measures	BiH remains the only country in the Western Balkans without a cyber security incident response team or a clear legal and strategic framework for cybersecurity. While there has been limited progress in the government’s approach during the reporting period, the country still lacks a comprehensive solution to this problem. The proposed government solutions, if adopted, would improve BiH ability to protect government institutions, collaborate internationally and improve responses to threats.

2.

Report on Cyber Threats

For a general overview of cybersecurity threats in Bosnia and Herzegovina during the period from January to August 2023, CSEC and BIRN BiH examined threat data collected through bait servers and devices designed for this purpose. These bait servers, commonly known as honeypots, are specialized devices that gather information from various international sources, while honeypot devices are integrated into the CSEC infrastructure itself. Both serve to lure potential attackers and are valuable educational tools.[1]

BIRN BiH also analyzed CSEC's data in conjunction with its own previous investigative reporting on cybersecurity threats in BiH and their sources.[2]

To defend against these threats, CSEC advises organizations, institutions, companies, and individuals to inspect their systems and response mechanisms in order to detect any signs of malicious activities. In the event that suspicious activities, such as attacks or unauthorized use, are detected, institutions and companies should operate on the assumption that their network identity has been compromised and should initiate the response procedures.

2.1 Attack Distribution

Between January and August 2023, CSEC documented a series of cybersecurity incidents on two dedicated devices used as bait within their network infrastructure. One of these devices, the Tpot server, is part of Deutsche Telekom Security's network of Tpot servers, the collective data of which reveals millions of attacks occurring worldwide every hour.[3]

When we compare the volume of attacks recorded through the Tpot devices during this reporting period with the data presented in the initial report on cybersecurity threats, we see a significant decline in the number of attacks.

However, it is important to note that this dataset is not comprehensive or aggregate; it merely offers a sectional view gleaned from the existing Tpot servers across the globe. The

[1] For the purposes of this report CSEC used different types of sources, which are: Tpot (Tpotce), DecoyNET Honeypot, OpenCTI and The Shadowserver Foundation.

[2] This report includes the tactics, techniques and procedures (TTP), as well as the indicators of compromise (IOC) associated with malicious activities.

[3] 35,000 – 65,000 attacks per minute; 1.5 – 3 million attacks per hour; 35 – 55 million attacks per 24 hours.

actual number of cyberattacks is changing by the minute and is likely significantly higher than what these observations suggest.

2.2 Cyberattacks in BiH Detected by Tpot Device

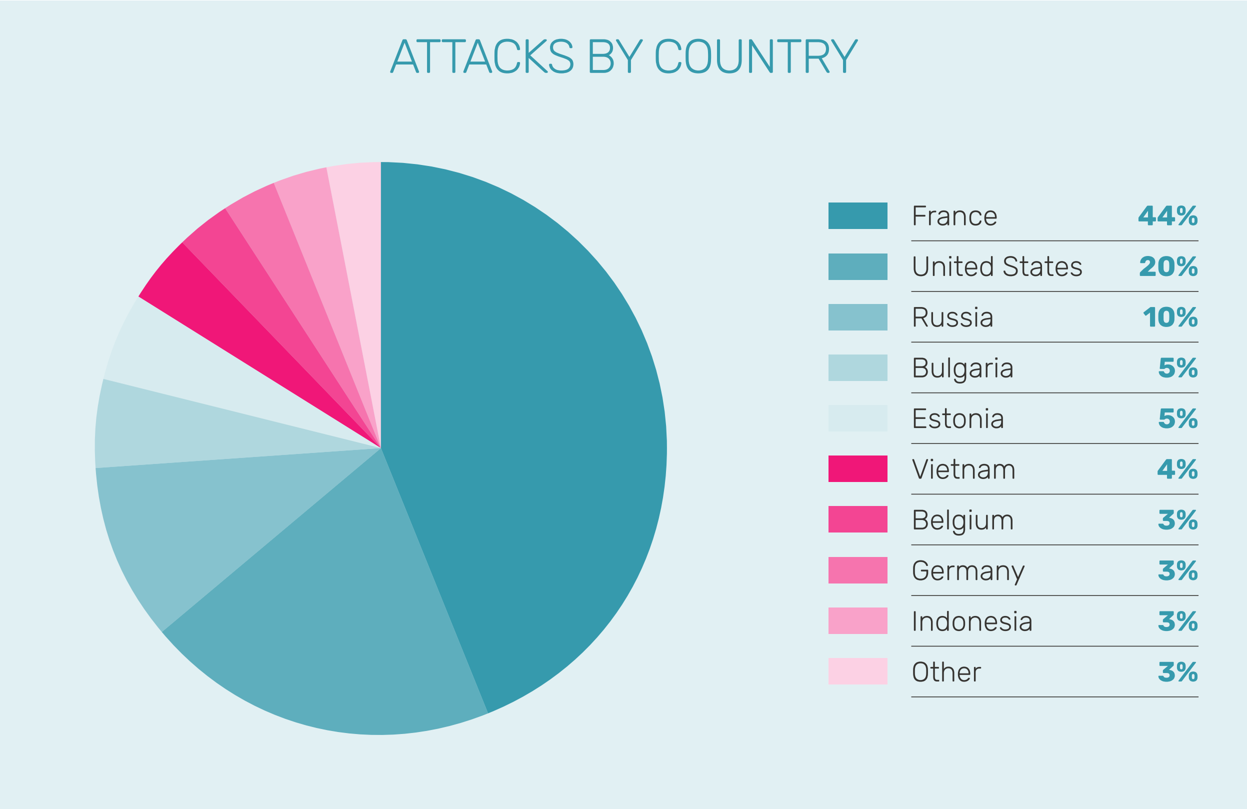
The number of cyberattacks in Bosnia and Herzegovina recorded through this service is changing constantly, with a consistent upward trend observed at the time of writing. This underscores the importance of continuous monitoring, registration, and effective processing in the cyber security environment in BiH. In the last 30 days of the observation period, 2.3 million attacks were documented, with the majority targeting the on PBX (Private Branch Exchange) infrastructure.[4]

The most notable decline was recorded in DDoS attacks, which involve a multitude of devices bombarding a single website with access requests, overwhelming its server, and causing it to crash. On average we are recording three to four million such attacks monthly. In August 2023, the devices recorded 16,802 attacks, marking an 80 percent decrease compared to the previous period. However, this does not indicate that DDoS attacks will stop. Instead, it should serve as a reminder of the need to remain vigilant, as new DDoS campaigns are likely to reach three to four million again in a short period of time. The same applies to all varieties of cyberattacks, in which we also expect to see an average increase by the end of year. This is a trend that has been noted in past observations by CSEC, where attackers adapt their strategies, frequently changing their tactics and methods to enhance the chances of successful attacks.

2.2.1 Distribution of attacks by country of origin and IP address

The CSEC team has identified France as the primary source of cyberattacks, followed by the US, Russia, Bulgaria, Estonia, Vietnam, Belgium, and Germany. Bringing up the rear among the top ten countries from which attacks most frequently originate are Indonesia and China.

[4] Others include: Together with PBX attacks are Telnet attacks and attacks on Web servers, together totaling – 1,7 mil. Next came attacks on FTP servers, as well as MSSQL and MySQL/MariaDb databases totaling 281,267. The remaining attacks were: Attempts to control computers, or exploit e-mail protocols and Postgres database - 121,700; Attempts to compromise Cisco devices - 80,301; DDoS attacks - 16,802; Attempts to exploit Redis cache server - 11,481.



Initial preliminary data from CSEC suggests that a significant proportion of attacks are originating in France and Bulgaria. However, this is likely the result of attackers utilizing Virtual Private Networks (VPNs) to conceal their actual locations, making it appear as though the attacks are originating from elsewhere.

The distribution of attacks by country has changed since the timeframe covered in the previous report. We now observe new sources of attacks, including France, Bulgaria, Estonia, Belgium, and Indonesia, whereas Brazil, the Netherlands, Bangladesh, Costa Rica, and India have dropped off the list. This shift doesn't necessarily imply that cyber threats now emanate from different actors compared to those in the initial report. It could also substantiate the claim that attackers, in addition to altering their attack methodologies, are changing the geographic origins of their attacks. This may be a defensive maneuver, with attackers using VPN services to mask the origins of their attacks and their physical locations.

Many of these attacks exhibit methods and capabilities consistent with the tactics often associated with Russia and China. This aligns with global experiences and data suggesting that these two countries are major sources of cyberattacks. In its latest digital defense report, Microsoft states that nation-state actors are launching increasingly sophisticated cyberattacks designed to evade detection and advance their strategic objectives. For instance, they highlight the use of cyber weapons by Russia in the conflict in Ukraine, including the dissemination of propaganda to influence not only the opinions of Ukrainian citizens but also those in other countries.

As stated in the report, “Outside Ukraine, nation state actors have increased activity and begun to use advances in automation, cloud infrastructure, and remote access technologies to attack a broader set of targets.”

The report emphasizes that cybersecurity measures have become even more critical, as attackers are quick to exploit vulnerabilities, employing both sophisticated techniques and more primitive, forceful methods while obfuscating their operations through open-source or legitimate software.

Given that these patterns are observed worldwide, we can assume that Bosnia and Herzegovina is following global trends. If there is a high volume of attacks appearing to originate from France or the USA, coupled with a lower volume from Russia or China, it is logical to conclude that the actual attackers are manipulating their IP addresses to obscure their true locations.

COMMONLY USED IP ADRESSES FOR ATTACKS TOWARDS TARGETS IN BiH

Source IP	Count	Geographically
5.196.203.176	700.928	France
66.85.155.162	203.375	USA
35.205.96.143	47.369	Belgium
79.124.56.106	43.594	Bulgaria
79.124.58.138	37.764	Bulgaria
62.122.184.102	34.305	Russia
89.163.242.10	34.276	Germany
185.73.125.94	33.156	Estonia
94.232.44.32	28.949	Russia
62.122.184.101	28.129	Russia

The importance of tracking these attacks is emphasized by the decision of the Chief Prosecutor of the International Criminal Court in The Hague, who has committed the court to investigating and prosecuting cybercrimes that violate existing international laws, as they do for war crimes cases committed in the physical real, as Wired reported recently.

2.2.2 Attacks on PBX Infrastructure

For businesses that depend on web-based communication with clients or other companies, any compromise of their website or its unavailability can create substantial costs and disrupt operations. For users, cyberattacks can result in the denial of access to critical health data, impede travel, and even disrupt the mobile banking applications widely used for everyday financial activities.

The most prevalent cyberattacks documented from January to August 2023 target PBX systems, or private telephone networks, which are critical for internal business communication. These attacks impose financial burdens on companies. For example, attackers can exploit a company's network to place costly calls, incurring substantial telephone expenses. In a 2021 study, these global costs exceeded 1.2 billion dollars. Moreover, these attacks can disrupt internal communication, hampering business operations.

In Bosnia and Herzegovina alone, we logged 1.7 million such attacks in just 30 days. Despite a decrease in the number of attempts compared to the previous period, attacks on PBX systems are the most common attacks in the country.

Hence, this section serves as a warning for businesses and organizations that maintain communication networks. Given the existing vulnerabilities in Bosnia and Herzegovina, it is almost certain that numerous businesses are incurring expenses due to PBX attacks.

This data underscores the need for further investigation into the economic impact of such attempts on networks and everyday operations, as well as associated costs in Bosnia and Herzegovina.

Globally, PBX attacks are among the leading methods for breaching networks. According to a survey by the Communications Fraud Control Association (CFCA), these attacks were among the top five fraud types between 2013 and 2017.

Beyond the direct cost escalation caused by unauthorized network usage for calls, attackers can obtain customer call records, leading to privacy breaches and potential loss of sensitive data. Resulting expenses may include the cost of cleaning and repairing compromised networks.

Another aspect of these attacks is the potential for eavesdropping on internal communications, enabling corporate espionage. Assessing the extent of damage in such attacks is difficult and may take a longer period of time.

Tracing these attackers is further complicated by their ability to obfuscate digital traces through so-called "PBX-looping," a technique where one network is used to place calls through another network.

The most significant decline in attack numbers recorded in this report pertains to attempts to compromise devices running the Android operating system. In the previous report, within one month, there were 478 such attacks. However, the current report reveals a total of 538 such attacks over the reporting period, demonstrating that attackers have shifted their focus toward other types of devices.

2.3. Cyberattacks in BiH Detected by DecoyNET Honeypot

In addition to the considerably larger Tpot device, CSEC also gathers data on cybersecurity threats in BiH through its own DecoyNET system. DecoyNET comprises six devices with the primary purpose of detecting cyberattacks before attackers can compromise entire systems.

While this system has much narrower range than the Tpot server, it is very helpful for making comparisons over specific timeframes. During this reporting period, a total of 15,478,783 attacks were recorded on this system, with the largest portion, totaling 9,908,666 attacks, were attempts to access the MSSQL database.

Additionally, the system documented the following attacks:

- 4,697,318 attempts to gain remote access over computer machines (VNC);
- 735,704 attempts to gain unauthorized access to the MySQL database;
- 77,190 attempts to gain unauthorized access to Redis database;
- 82,286 attempts to compromise data exchange protocols (FTP, SMB, SIP, HTTP, and HTTPS);
- 9,815 attempts to compromise NTP and SNMP protocols for synchronizing time on computers;
- 538 attempts to compromise Android devices.

In the first Threat report published in March 2023, the total number of attacks recorded was 520,717, while now we see an increase of almost two million attacks on a monthly basis. This shows that the interest of attackers is increasing, but this can be due to various reasons, from the fact that attackers are testing different tactics to develop their own attack systems and penetrate target systems, to simply the fact that there has been a global increase in incidents.

2.4 New Measurement Tools for CSEC

Since the publication of the initial report, CSEC has introduced new methods for gathering information on cybersecurity incidents. The first approach involves data collection through OpenCTI, an open-source platform designed to manage and analyze cyber threat intelligence. OpenCTI’s primary objective is to enhance our understanding of the cyber threat landscape and facilitate the sharing of knowledge regarding cyber threats.

AlienVault, a collaborative initiative to exchange global data on cyberattack attempts, is currently the only cybersecurity company providing data on BiH. This is likely a result of the absence of official contributions from within the country to the international computer security incident response team community, which is why BiH should have a national CERT team that could communicate with other relevant authorities throughout the world and ensure the exchange of information. At present, CSEC aggregates data and is in the process of establishing procedures for data sharing, with plans to begin in early 2024. According to AlienVault data, there are only three reports associated with BiH, two dating back to 2020 and one from this year, which is connected to Dark Pink in January.

According to Group IB, a cybersecurity company, a new group of advanced persistent threat (APT) actors has emerged, targeting government and military institutions across Asia and Europe. They have identified seven such attacks, including one in Bosnia and Herzegovina, and anticipate more incidents in the coming five years.

This information highlights a notable absence of comprehensive data contribution, particularly within the incidents section of the system, which appears to be completely devoid of information. Furthermore, it is widely acknowledged that at least one cyberattack has targeted the Bosnian Parliament. Group IB's Threat Intelligence Team has now linked this breach to a specific group, called Dark Pink, although Bosnian authorities still lack official information about the identity of the attackers, which is an additional reason why BiH should have a CERT team and other capabilities for defense and detection of such threats.

Moreover, there is a conspicuous lack of meaningful connections among the actors within Bosnia and Herzegovina concerning the identified threats. Most of the malware detected in Bosnia and Herzegovina has been associated with a few APT groups, including APT28 (known as FancyBear or Sofacy), Hidden Cobra (Lazarus), and Dark Pink.

With the introduction of OpenCTI, CSEC has expanded its data collection capabilities through collaboration with The Shadowserver Foundation, a leading global resource for reporting on internet security and investigating malicious activities. Currently, the Foundation indexes and makes searchable approximately 70 billion SSL certificates within its data and analysis clusters. It provides daily reports used by 201 National CSIRTs, covering 175 countries and territories, including data collected by CSEC for Bosnia and Herzegovina. On average, the Foundation sinkholes between four and five million IP addresses daily, representing over 400 different malware family variants.

One remarkable aspect of Shadowserver devices is the wealth of information available for each country where a partner of the Foundation is present. The Foundation notes that in BiH, there are 29,179 unique IP addresses, 770,624 broadband fixed subscriptions, and an estimated 2.3 million internet users. According to their data, the average internet speed in our country stands at 48.51 Mbps, which is well above the world average.

3.

Incident Highlights from January to August

During the observed period, we documented several incidents that didn't originate directly from the network of honeypots through which CSEC collects data but surfaced through the exchange of information. This illustrates the crucial role of information sharing in cybersecurity protection, a fact widely emphasized by experts. In the coming period, institutions and other stakeholders in BiH should actively work towards improvements with regard to this issue.

These cases reveal numerous problems, through the slow reactions of the police, which are caused by the lack of adequate strategic solutions. Police agencies often do not have enough resources or the capabilities to perform this function and this is the reason why a specialized institution is needed to which the attacked entities could report such incidents.

3.1 Attacks on the Media and Public Figures

In April 2023, Nezavisne Novine, a daily newspaper in Banja Luka, reported a cyberattack on their website that severely limited access for their readers. According to information gathered for this report, these attacks endured with intensity for nearly ten consecutive days, accompanied by daily attacks of varying scales.

Sandra Gojković-Arbutina, the editor-in-chief of Nezavisne Novine, commented on the situation: "Given the intensity and persistence, it seems to me that we were not chosen randomly and that we were not a random sample for the attack, but it seems to me that it is a targeted attack with the specific intention to crash Nezavisne. The management and I have rejected the possibility that it was a coincidence."

Although Nezavisne reported the attack to the police, at the time of writing this report, they had not received any feedback regarding the source of the attack. Back in 2019, this media company had filed a report with the police concerning similar incidents but didn't receive any results from the police investigation. This time, they documented significant details of the attack themselves, providing data for this report, which indicated that it was a persistent Distributed Denial of Service (DDoS) attack on their services. Millions of attempts to access their website's front page originated from various locations worldwide. The outlet's IT department suspects it's the same attacker utilizing different services to obscure their true location and conduct these attacks. They also believe it might be part of a specific campaign.

“When we go down, when we’re not available, when Nezavisne is difficult to access, when it takes you a few seconds to open a link, we lose readers every second. For media outlets, especially commercial ones, which are not state funded, this type of attack leads to direct financial endangerment,” Gojković-Arbutina remarked.

Other media outlets, including Buka, BN TV, and Face TV, also faced cyberattacks in April. Face TV informed Detektor that they recorded up to 300 million attempts to access their site in a single day. They believe that such an attack undermines trust among their viewers and attribute it to their coverage of political changes.

In addition to the media, public figures have also been targeted by cyberattacks. In July, Nezavisne reported that a hacker from Banja Luka was arrested on suspicion of carrying out a cyberattack against a prominent lawyer in Sarajevo. The attacker stole data related to various cases in which the lawyer was involved, sent false messages on her behalf to numerous individuals, and attempted extortion.

The Ministry of Internal Affairs of Republika Srpska confirmed this arrest to BIRN BiH. They stated that the individual is linked to several criminal acts, including ransomware attacks, unauthorized access to protected computers and networks, telecommunications networks, electronic data processing, and computer fraud. Numerous items pertinent to the commission of these crimes were seized from the suspect.

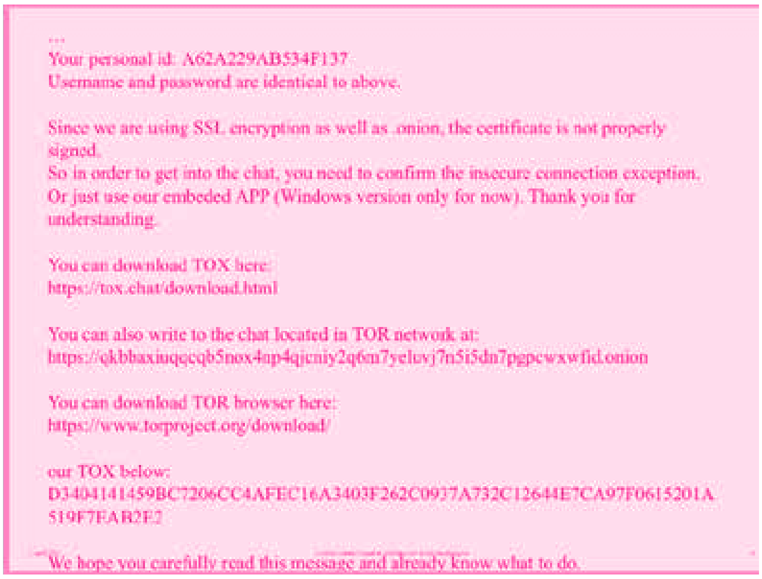
3.2 Case Study: Sarajevogas

Following a series of ransomware attacks which were not made public, the Sarajevogas Cantonal Public Utility Company set a positive example by publicly disclosing a significant ransomware attack on its network in late August 2022.

Ishak Alajbegović, the chief infrastructure engineer within the company, explains that they lost access to all their data in a single night.

“Everything was encrypted,” he stated, elaborating that the entire network was compromised, encompassing 40 to 50 virtual machines containing customer databases and other critical data.

The assailants, identifying themselves as “Donut Leaks,” sent a communication to Sarajevogas, requesting that they install specific software for further communication.



```
...
Your personal id: A62A229AB534F137
Username and password are identical to above.

Since we are using SSL encryption as well as .onion, the certificate is not properly
signed.
So in order to get into the chat, you need to confirm the insecure connection exception.
Or just use our embeded APP (Windows version only for now). Thank you for
understanding.

You can download TOX here:
https://tox.chat/download.html

You can also write to the chat located in TOR network at:
https://qkbbaxiuqqcqb5nox4np4qjcniy2q6m7yeluvj7n5i5dn7pgpcwxwfid.onion

You can download TOR browser here:
https://www.torproject.org/download/

our TOX below:
D3404141459BC7206CC4AFEC16A3403F262C0937A732C12644E7CA97F0615201A
519F7FAB2F2

We hope you carefully read this message and already know what to do.
```

Given their status as a public company, the management of Sarajevogas decided to report the incident to the police. They were surprised by the lengthy application procedure, which left them waiting for several days to fully restore their operational system. Consequently, they had to operate within an auxiliary environment during that time. Fortunately, their earlier preparation for potential cyberattacks helped them to recover, as they had implemented four layers of data backups. This foresight enabled them to restore all data saved prior to the attack.

“I had a supportive environment, but we couldn’t wait ten days, two days, because everyone was standing by that day. The teams in the field were waiting, and 300 people were unemployed because of the situation. It took me about ten hours to go through the entire procedure to solve the problem, and by the next day, we had everything functional and everything we needed for normal operations,” Alajbegović recalled.

However, after ten days without any response from the police, Alajbegović explained that the company had to make a pragmatic decision. They drafted a memorandum, stating that they had preserved a portion of the evidence and had no option but to erase all other compromised data in order to restart the system. They then relied on their backup data that remained unencrypted, ultimately restoring all essential processes within the company.

Alajbegović regards this attack as a valuable learning experience, despite the challenges. It allowed them to test the efficacy of their established security measures and their readiness to counter cyber threats. Additionally, it helped identify areas needing further development in their cybersecurity defenses. Due to future security concerns, certain details are not being disclosed regarding these insights. Nevertheless, Alajbegović emphasizes that many entities, both in the public and private sectors, do not fully comprehend the extent of the threats they face, and as such, they often fail to sufficiently invest in cyber protection resources.

“Investigating it later, that same hacker also attacked a gas company in Greece, just seven or eight days before he attacked our company. In our case, they probably got in because of an external company in our system, which implemented certain software measures and left space for an attack,” concludes Alajbegović.

The experience of this company is relevant for every company in Bosnia and Herzegovina, especially for utility companies, which is why all of them should prepare for attacks. The example further highlights the deficiencies within the system, notably the police, who lack adequate resources, trainings, tools and knowledge to address such attacks, which should be another focus for authorities.

3.3 Small Communities Unprepared for Cyberattacks

This report aims to assess the responses of local authorities to cyber threats.

Adnan Bjelić, the mayor of Srebrenik, reported that, thus far, there have been no documented cyberattacks within the local community under his administration. However, he acknowledged that such problems may arise in the future, when all organizations, including those in the public sector, are forced to digitalize. He added that local communities are aware of these threats, but he believes that a response should come from higher levels of government, in order to enact appropriate legal and strategic measures and to support local communities.

“If local communities are left to fend for themselves in terms of cybersecurity, I think it will be difficult. We have neither the staff nor the technical training. I’m afraid we need a lot more help from higher authorities at the upper levels than we might even think,” Bjelic elaborated.

Under Bjelić’s leadership, the city administration is currently working towards the digitalization of certain processes. He contends that the absence of recorded cyber threats thus far is attributable to their limited engagement digital platforms, but that new dangers are emerging every day.

“With modernization, tools that ensure security must accompany this engagement. Until there’s security in the electronic industry, it will be hard for local communities and any other level to be able to utilize all the benefits of that industry,” he noted.

While the City of Srebrenik has established certain protective systems, they recognize the necessity of bolstering these safeguards. Furthermore, Bjelić stressed the need for increased training, so that public officials themselves do not jeopardize the city administration system. As he pointed out, threats that initially appear benign have the potential to inflict substantial damage to the entire system.

From all of the above, we conclude that in the coming period, it is necessary to adopt the legal and strategic framework on cyber security in Bosnia and Herzegovina, and to include models for solving the problems of local communities. In addition, it would be desirable to develop a platform for cooperation between different municipalities, which, through cooperation and joint financing, could significantly improve their capacities for combating cyber security incidents.

4.

Update on Government Measures

This report highlights the limited legislative efforts in the realm of cybersecurity, evident in the fact that Bosnia and Herzegovina remains the only country in the Western Balkans without a national cybersecurity strategy. The country also lacks the necessary legislation and other regulatory documents required for alignment with EU cybersecurity standards, a crucial step in the process of EU integration.

During the reporting period, there were some strides toward establishing a Computer Emergency Response Team (CERT) for state institutions.

Specifically, in May 2023, the BiH Council of Ministers approved the systematization of positions within the Security Ministry, thereby laying the groundwork for the formation of a CERT team. Amendments to the rulebook governing the internal organization of the ministry were also adopted, facilitating the establishment of the CERT team for BiH bodies and institutions, in compliance with EU recommendations. This marked the revival of a process that had been stalled for six years, as the Council of Ministers had previously, in 2017, adopted a decision regarding the appointment of a CERT team for BiH institutions within the ministry.

Representatives of the Security Ministry told BIRN BiH that “the new rulebook established a new organizational unit, CERT for BiH institutions, with a total of five systematized positions, with job descriptions designed in accordance with ENISA’s recommendations and best practices.”

However, the practical implementation of the CERT team is contingent upon several more political decisions. The state government has initiated proceedings to partially fill the new positions within the team, yet budget constraints continue to prevent the full staffing of the team.

“Several meetings were held with international partners who expressed their willingness to help establish CERT for the institutions of BiH, which will certainly be used,” the Security Ministry added. Additionally, they have plans to join CERT teams affiliated with international associations, organizations, and networks to facilitate information exchange.

The State Parliament adopted several resolutions in May of this year that should lead to improvements in cybersecurity. It is imperative to capitalize on this momentum by expeditiously implementing these resolutions and concurrently enacting the requisite laws and strategies such as the Law on cyber security in BiH, the comprehensive Strategic framework on cyber security in BiH, the development Policy of the electronic communications sector in BiH, and the Law on critical infrastructure.As the data from the Shadowserver Foundation revealed, the country has been subject to cyberattacks carried out by sophisticated threat actors, including those from North Korea and Russian groups, which often target critical institutions and key infrastructure. For this reason, the absence of an active CERT team, an issue that CSEC is attempting to address, underscores the urgency of adopting a range of pending documents to improve cybersecurity standards in BiH.

5.

The Cyber Security Excellence Center and BIRN BiH

In light of the lack of a fully operational state-level CSIRT in BiH, a group of cybersecurity enthusiasts from the academic community joined forces to establish CSEC, in an effort to bridge the existing gap and act as the last line of defense in the country's cybersecurity landscape. Leveraging its academic roots, CSEC seeks to harness expertise and experience while fostering connections with the private sector, with the overarching goal of supporting a skilled cybersecurity taskforce.

As CSEC was founded in 2022, it is in the process of building an extensive network of contacts capable of supplying information on potential cybersecurity threats. Additionally, it is working on organizing various events, campaigns, and information dissemination channels to enhance awareness among the online community and create avenues for early warning about cyber threats. CSEC;s ultimate mission is to position itself as a neutral and reliable hub for a systematic response to cyber incidents in BiH contributing to the development and enhancement of the country's cybersecurity.

CSEC also aims to strengthen communication channels between cybersecurity stakeholders and other CSIRT teams within the region. Its vision is to foster a secure and resilient cyberspace in BiH for all citizens.

BIRN BiH is a non-governmental media organization based in Sarajevo, specializing in monitoring and reporting on trials related to war crimes, corruption, terrorism, foreign malign influences, digital threats, and disinformation. It operates the Detektor online portal and shares its stories with other media outlets free of charge. BIRN BiH currently broadcasts two television shows per month and develops databases.

CSEC does not guarantee the completeness, accuracy, or currency of the data presented in this report. Cyber threat data continuously evolves and is not representative of the entire global landscape or the entire geographic area of BiH. The data reflects activity at a single point or IP address within the global Honeypot server network, and the overall number and distribution of these servers remain unknown. The data does not reveal the number of successful cyberattacks with consequences for victims but rather highlights occurrences in cyberspace to raise awareness among all users regarding the persistent threats on the internet.

In presenting this data, the goal is not to tarnish the image of BiH, as similar phenomena occur daily worldwide wherever the internet is accessible. In most cases, automated scripts scan networks in search of potential targets for compromising their systems and data.

BIRN BiH has processed the data obtained from CSEC for this report, placing it in the context of the initial report from March 2023, earlier studies by BIRN BiH, and other publicly available data.

This entire report is intended for public dissemination, allowing anyone to use it and refer to it. However, it must be utilized in its original form without alterations and with the mandatory attribution of the information source. Any use of this document in contravention of these provisions constitutes a copyright infringement. The report will systematically and continuously highlight vulnerabilities within the BiH cybersecurity domain, as well as the risks posed to critical infrastructure. Education and raising awareness are central priorities for both CSEC and BIRN BiH, making this report a valuable educational resource for civil society in BiH.

CSEC
Cyber Security
Excellence Centre

BIRN
BALKAN
INVESTIGATIVE
REPORTING
NETWORK

BOSNIA &
HERZEGOVINA