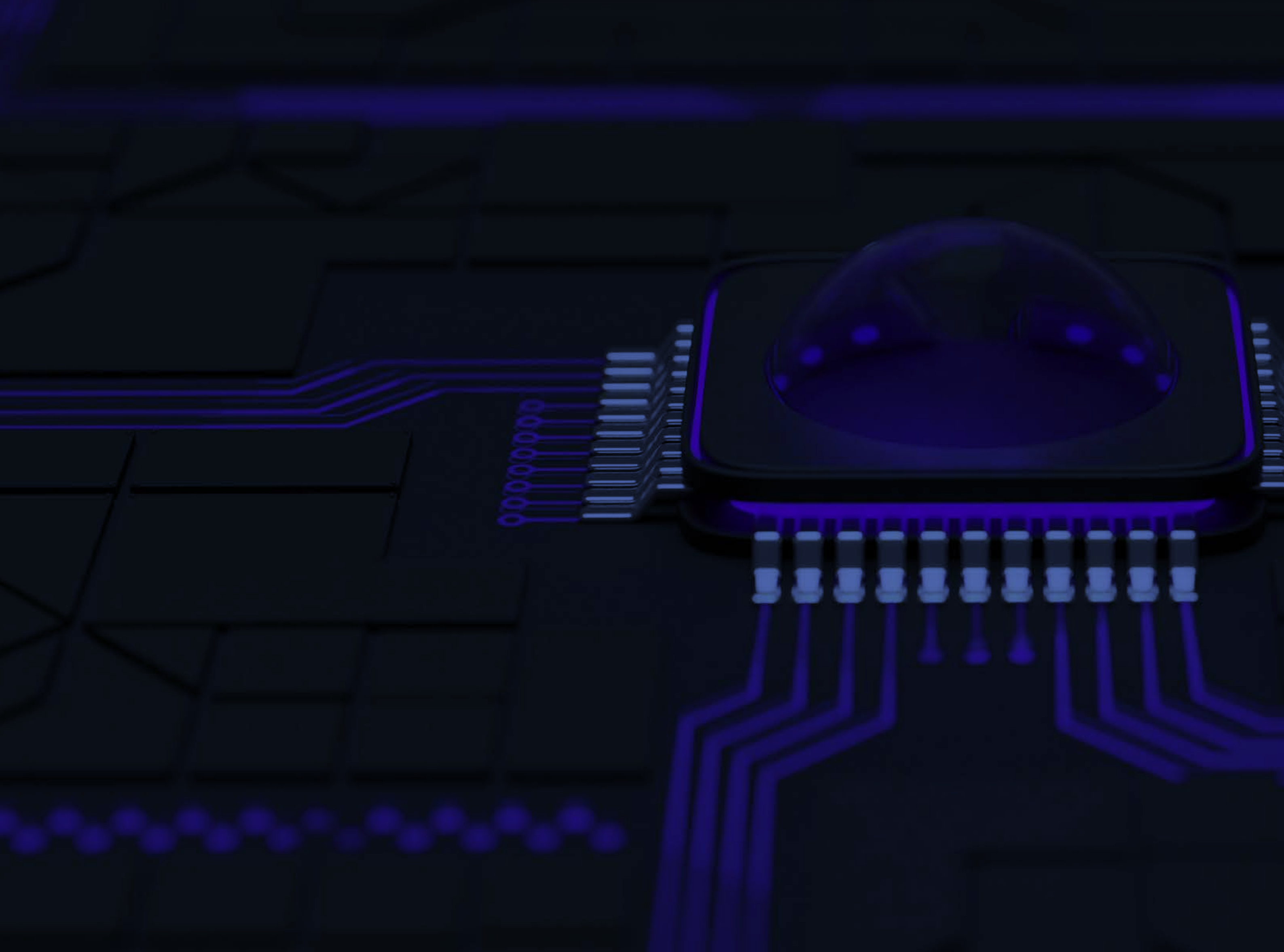


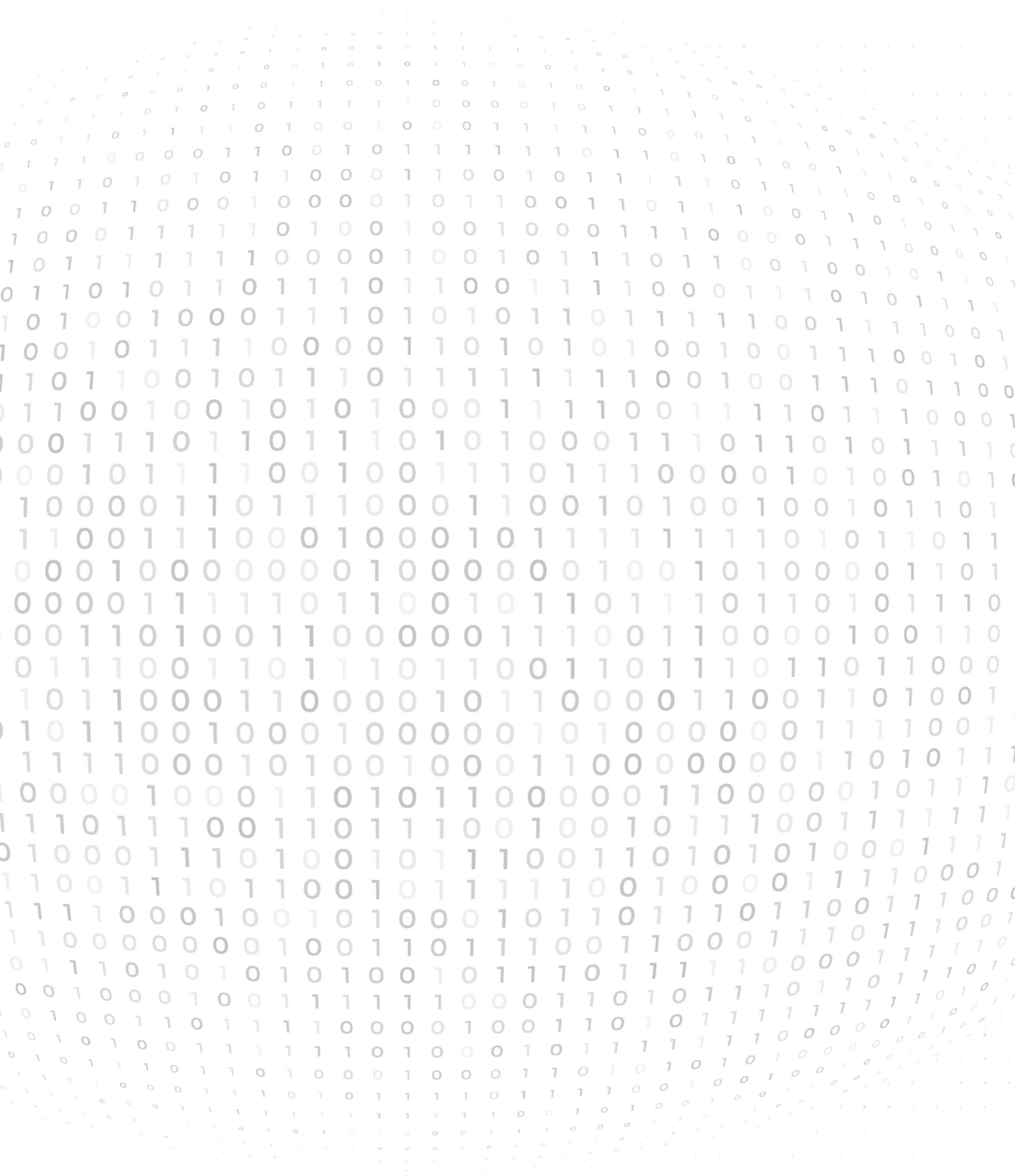
Bosnia and Herzegovina

CYBER SECURITY THREAT ASSESSMENT

March 2023

CSEC
Cyber Security Excellence Centre

BIRN
BALKAN INVESTIGATIVE REPORTING NETWORK
BOSNIA & HERZEGOVINA



Bosnia and Herzegovina

CYBER SECURITY THREAT ASSESSMENT

March 2023

Written by:
Aida Mahmutovic and Enes Hodzic
(BIRN BiH)

Sarajevo
October - December 2022

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: Aida Mahmutovic and Enes Hodzic (BIRN BiH)

October - December 2022

Table of contents

1. Introduction 6
1.1. First Cyber Security Threat Assessment. 6
1.2. The role of CSEC 6
2. Disclaimer 7
3. Summary of main findings of the report 8
4. Report on cyber threats 9
4.1. Data collection system. 9
4.2. Incident highlights in October to December 10
4.3. Attack distribution in BiH. 11
4.4. Cyber attacks detected through Tpot device. 12
4.5. Distribution of attacks by country of origin 13
4.6. DDoS attacks 17
4.7. Cyber attacks in BiH detected through OpenCanary Honeypot device 18
4.8. Cyber security advisor – Usernames and passwords. 19
4.9. Government measures update. 21
5. About Cyber Security Excellence Center in BiH 23
6. About BIRN BiH 24
7. Terminology 25

1.

Introduction

1.1. First Cyber Security Threat Assessment

The Cyber Security Excellence Center, CSEC, in collaboration with the Balkan Investigative Reporting Network of Bosnia and Herzegovina, BIRN BiH, presents you with the first report on cyber-security threats in BiH. It analyses data collected from October to December 2022 pertaining to cyber-security threats recorded by CSEC in BiH in the same period and illustrating, in a practical way, all cyber dangers facing Internet users in our country.

The attacks most frequently recorded during the observation period were DDoS (distributed denial-of-service attacks) and attacks on databases, which is very similar to experiences recorded by CERTs (Computer Emergency Response Teams) in the surrounding countries. Nevertheless, owing to the short lifetime of CSEC and relatively small network for collection of data, as well as different data collection methodologies, it is hard to compare the results of the academic CERT of BiH with the results from the region. However, the importance of cyber-security protection is best illustrated through the recorded number of attacks during the observation period, which CSEC collected through its own "honeypots", incident reports and generally through exchange of information with other CERTs.

As a result, the need arose to create a single report to demonstrate all events in the cyber-security world in Bosnia and Herzegovina and show the importance of immediate action in that field. CSEC will publish a threat assessment twice a year.

1.2. The role of CSEC

Founded as part of the Criminal Policy Research Center in Sarajevo, CSEC operates as an academic Computer Emergency Response Team, CERT, with the main task of establishing communication channels for collecting all details about potential cyber-attacks, oversights and other types of dangers to which Internet users in BiH are exposed. Given that it was established during 2022, CSEC is still working on developing a network of various contacts that can provide it with information about potential cyber-security threats, as well as on developing various events, campaigns and information channels to raise awareness within the Internet community and create possibilities for early warning about cyber threats.

As BiH is the only country in the region that does not have a national CERT, members of CSEC strive to make that organization a central point for gathering all data relating to Internet security, data which has either been created within the Internet community in BiH or is connected with it. The process takes place through establishment of cooperation with national CERTs in the countries of the region and the European Union, but also with all governmental and nongovernmental organizations in BiH that are interested in providing information about cyber threats, which would precisely be the task of a national CERT that is non-existent in BiH. Besides, an additional role is also to test systems and users, as well as provide different forms of trainings to highlight the relevance of prevention and defense from cyber-attacks.

2.

Disclaimer

The Cyber Security Excellence Center (hereinafter referred to as **CSEC**) was founded as part of the Criminal Policy Research Center with the intent of becoming part of Sarajevo University, to strengthen cyber security in Bosnia and Herzegovina (BiH), with United Kingdom government support. As part of CSEC, an academic and sustainable Cyber Security Incident Response Team (CSIRT) will be established.

CSEC does not guarantee that the data in this report is complete, correct and up to date. Such data changes minute by minute and does not refer to the entire world and/or geographic area of Bosnia and Herzegovina. The judgements and analysis in this report are the assessment of CSEC and BIRN BiH.

The data shown refers to one point, one IP address, and the network of Honeypot[1] servers in the world, while the total number of servers and their distribution remains unknown. The data does not show the number of successfully executed cyber attacks with consequences for victims, but it shows occurrences in cyberspace with the aim of raising awareness of all users of dangers lurking on the Internet every day.

The goal of presenting this data is in no way to create a bad image of BiH, because identical day-to-day phenomena happen in all parts of the world where there is Internet.

In most cases, it is about automated scripts that scan the network in search of victims that are “worth” taking steps against to compromise their systems and data.

Balkan Investigative Reporting Network of Bosnia and Herzegovina (hereinafter referred to as **BIRN BiH**) processed the data obtained from CSEC in this report and put it in the context of earlier studies by **BIRN BiH** and other publicly available data.

The entire report is intended for public disclosure, so anyone may use it and call upon it, but exclusively in its original form, not making any changes and mandatorily indicating the source of information.

The use of this document contrary to the above stated provisions implies a copyright infringement.

CSEC and BIRN BiH will publish a cyber security threat report twice a year. The report will strive to systematically and continuously show vulnerabilities within the BiH cyber security domain, as well as the risks of damage to key infrastructure. Considering that education and raising awareness are a key focus of both CSEC and BIRN BiH, this report will also serve for educational purposes and will be distributed to the civil society in BiH.

[1] Honeypot is a cyber security mechanism that uses a purposefully “manufactured” attack target to lure cybercriminals away from legitimate targets. Honeypots also gather intelligence about the identity, methods and motivations of adversaries. Probably the easiest way to understand this is to see honeypot as a decoy aimed at attracting cyber attacks.

3.

Summary of main findings of the report

More than 9.2 million cyber security threats were registered in Bosnia and Herzegovina, in just a one month period between November 17 and December 17, 2022 of which DDoS attacks were the most frequently recorded. That number of attacks and the latest audit reports of institutions, which showed that there is no strategic and legal framework for cyber security in BiH, is the best illustration of the vulnerability of citizens, companies and institutions of BiH to cyber attacks that could threaten key sectors, such as the rule of law, the economy, energy, health or education.

Scale of the Cyber Threat	From the start of CSEC operations to the moment this report was published, the number of cyber attacks recorded by this team has been rising steadily, which shows the importance of monitoring cyber security in Bosnia and Herzegovina.
Attack types	During the observation period, DDoS (distributed denial-of-service) attacks were the most common cyber attacks. Their purpose is varied, while the effects can be catastrophic for critical infrastructure.
Incident Highlights	One of the cyber security threats CSEC detected is particularly interesting as it came from e-mail addresses of one of the official institutions of BiH. A CERT team from Spain noticed a phishing campaign from e-mail addresses of one state institution, but after the Serbian CERT and CSEC intervened, the origin was identified and the threat eliminated in a short time.
Attack distribution by country	Cyber attacks recorded in BiH most often came from Brazil, the Netherlands, USA, Russia, Germany and China. Unexpectedly, the Netherlands and Germany found themselves at the top of the list. Presumably, this is due to the fact that attackers from other states most often use virtual private network (VPN) servers in those countries to conduct attacks and hide their data.
Government Measures	BiH is the last Western Balkans country not to have a full-scale cyber security incidents response team, but also without a clear legal and strategic framework for cyber security. The activities of the institutions of BiH in ensuring the basic assumptions for cyber security were recently analyzed by the Audit Office of the Institutions of BiH, which observed a whole series of irregularities and sent several recommendations to all institutions regarding cyber security in BiH.

4.

Report on cyber threats

To get a picture of cyber threats in Bosnia and Herzegovina, from October to December 2022 CSEC and BIRN BiH monitored how a vulnerability in one honeypot server and one honeypot device, installed within the CSEC infrastructure in the demilitarized zone (DMZ), was exploited. CSEC's academic unit for monitoring, analyzing and reacting to incidents identified the IP addresses from which most of the threats came.

BIRN BiH analyzed CSEC's data and its own earlier reports that explained cyber security threats in Bosnia and Herzegovina and their sources.

This report includes the tactics, techniques and procedures (TTP), as well as the indicators of compromise (IOC) associated with malicious activities. To protect themselves from those threats, CSEC recommends that organizations, institutions, companies and individuals inspect their systems and responses to detect malicious activities.

If any activities such as attacks and misuse are discovered, institutions and companies should assume that their network identity has been compromised and follow the incident response procedures[2].

4.1. Data collection system

The data presented in this report were collected through a **Tpot server** and **OpenCanary device**, i.e. a honeypot server and a device installed within the CSEC infrastructures in the DMZ part of the network.

Honeypot is a cyber security mechanism that uses a purposefully "manufactured" attack target with the aim of diverting cyber criminals from legitimate targets. Honeypot can be modelled on any digital asset, including software applications, servers or a network itself, and it is purposefully designed to look just like a legitimate target in its structure, components and content. This way, attackers are being persuaded that they have accessed a legitimate target to encourage them to spend as much time as possible in that controlled environment.

In essence, Honeypot represents a bait, but it can also serve as a learning tool, using attempted attacks to evaluate the attacker's technique, capability and sophistication. Honeypot may imitate real devices such as mobile phones, servers or network systems to discover in what way they are endangered.

[2] https://www.csec.ba/guidelines

Intelligence gathered by honeypot devices can help organizations improve their cyber security strategies in response to real-world and real-time threats, identifying potential blind sports in the existing architecture, as well as their information and network security.

Tpot (Tpotce) consists of 23 different honeypot servers, each of which pretends to be one or more known and most often exploited services, protocols, applications etc.

OpenCanary is designed to create a network of Canary devices set up in a client's network in order to detect attempted cyber attacks before the attacker manages to fully compromise the system. It actually represents a bait using 16 services that are most frequently attacked or targeted by compromising attempts.

4.2. Incident highlights in October to December[3]

Although we deal with a relatively small sample of collected and analyzed data – given the short period covered by this report – several incidents highlight the importance of monitoring and reacting to cyber security threats which are on the rise in BiH.

The first warning about such threats arrived from Spain, where the national CERT team observed a phishing campaign from e-mail addresses with Bosnia and Herzegovina's **.ba** national domain. Those addresses belonged to an official BiH state institution, so urgent action was required. However, as there is no official national CERT team in Bosnia and Herzegovina, about which BIRN BiH has reported previously[4], Spain's CERT approached Serbia's national CERT. The information later reached CSEC through unofficial channels in Serbia. A quick check determined where the state institution's e-mail server was located, the service provider was contacted and the problem was resolved very quickly. Phishing is widespread and is one of the most common tools attackers use to obtain sensitive personal user data, such as usernames, passwords or credit card information. Some cyber experts say that 97 percent of initial attack vectors, or the ways in which attackers launch their attacks, come through phishing. The attacker's main goal is to access data that might benefit them at the victim's expense, be it through ransom demands or direct exploitation of the data.

BIRN BiH journalists also discovered such threats when state parliamentarians told them that in October 2022, e-mails from the Bosnian State Parliament's official domain were marked suspicious. This means that someone, imitating the parliament's domain administrator, was trying to access data of members of parliament. The General Secretariat of the BiH Council of Ministers confirmed exposure to constant cyber attacks to BIRN BiH, but could not say where the attacks came from or whether they were connected with attacks against institutions in some other regional countries.

[3] The attacks presented in this chapter refer to attacks recorded through CSEC's honeypot systems, but also those about which information has arrived from other sources.

[4] https://detektor.ba/2022/11/14/bih-ranjiva-na-cyber-napade-zbog-nedostatka-kljucnih-dokumenata/

BIRN BiH previously reported on problems facing state institutions in BiH due to the lack of a national CERT team and a lack of key documents[5] that would spell out what to do in the case of a cyberattack.

> *A concrete example of the need for CERT teams came in September, when parliament employees were greeted by a notice saying: **“PLEASE DO NOT TURN ON YOUR COMPUTERS UNTIL YOU RECEIVE A NOTIFICATION”.** At the time, a problem with accessing e-mails and other digital services in the Parliamentary Assembly and Council of Ministers of BiH due to cyber attacks had been detected, underlining the **VULNERABILITY OF THE COUNTRY’S CYBER INFRASTRUCTURE.***

Problems with IT in state institutions have existed for years, so in April 2017 the Council of Ministers’ servers were blocked[6], not due to cyber attacks, but to disagreement between two state services over who was in charge of maintaining air conditioners in the server room. The servers then overheated, choking the operation of state institutions for four days. Such examples best illustrate the lack of any clear strategic, legal and organizational framework in Bosnian institutions to protect IT and cyber security.

Another incident was noticed directly through CSEC’s honeypot systems, when an unusual activity was detected, coming from IP addresses on the domain of one of the groups with which CSEC had cooperated since its establishment. CSEC members collected information on the type and method of attack, contacted the relevant IT staff and the compromised source of attack was discovered quickly and removed.

A third example of CSEC’s activities came after a tip from the OSCE-led Neretva Grupa[7] of cyber security experts who reported that malware content was being distributed from the IP address space belonging to the academic sector of one of Bosnia’s neighbors. CSEC informed its colleagues in the national CERT of that country, so through a quick reaction and following set procedures, the unauthorized activity was eliminated.

4.3. Attack distribution in BiH

From October to December 2022, CSEC recorded a number of cyber security incidents on two devices, which were used as baits on their network. The first device is the **Tpot (Tpotce)** – see above. Among the Tpot’s servers are ones detecting attempted attacks on Android devices, attacks on industrial control protocols and brute force terminal attacks, DDos attacks, attempts to compromise various servers and services, as well as those keeping track of login data during attempted attacks on certain services, and a phone call fraud detector, simulator of a printer and e-mail service.

[5] https://detektor.ba/2022/11/14/bih-ranjiva-na-cyber-napade-zbog-nedostatka-kljucnih-dokumenata/

[6] https://detektor.ba/2017/04/25/serveri-vijeca-ministara-nisu-radili-jer-se-ne-zna-ko-odrzava-klime/

[7] In close cooperation with the EU Delegation and Special Representative of EU in BiH, the OSCE Mission to BiH established an international coordination group, called Neretva Grupa, consisting of cyber security experts. Source: https://www.osce.org/files/f/documents/9/7/468372.pdf

All these device parts help record as many attacks and types of attacks as possible worldwide. In the concrete case of CSEC, this **Tpot** server, which is used to collect data, is part of a network of **Tpot** servers of Deutsche Telekom Security, whose data show that on average, the following happens worldwide:

- 65,000 – 115,000 attacks per minute;
- 3 – 4.5 million attacks per hour;
- 55 – 80 million attacks per 24 hours.

> *It is important to note that this data is neither complete nor aggregative, but it only represents* ***A SECTIONAL VIEW FROM THE EXISTING Tpot SERVERS WORLDWIDE,*** *while the actual number of attacks is changing by the minute and is probably many times greater.*

4.4. Cyber attacks detected through Tpot device

The number of attacks in Bosnia and Herzegovina recorded through this service is changing constantly, and at the time of writing, is rising consistently, indicating the importance of monitoring, registering and adequately processing them in the cyber security environment in BiH.

In the last 30 days of the observation period, **8,733,270 attacks** were recorded, the largest number being **DDoS attacks – 3,827,666**. Next came **attacks on PBX**[8] **(private telephone network) infrastructure, Telnet**[9] **attacks and attacks on Web servers,** together totaling **3,607,736**.

The remaining attacks were:

- Attempts to control computers, or exploit e-mail protocols and Postgres database[10] – **632,462 attacks**;
- Attempts to compromise FTP[11] servers, as well as MSSQL and MySQL/MariaDb database[12] – **612,125**;
- Attempts to exploit Android devices – **13,853**;
- Attempts to exploit industrial control protocols – **6,086**;

[8] PBX is the acronym for Private Branch Exchange and represents a private telephone network that enables users to communicate with each other.

[9] Telnet is a network protocol used to virtually access a computer and to provide a two-way, collaborative and text-based communication channel between two machines.

[10] Postgres (PostgeSQL) is a type of object-oriented relational database management systems. It is considered one of the most reliable databases and is most often used for web applications and web databases.

[11] FTP (File Transfer Protocol) is a standardized network protocol used for exchanging data between two or more computers via a TCP protocol-based network, such as the Internet.

[12] SQL is a program language used for writing queries for work with databases, and information is selected and changed with its help, while MySQL and MSSQL are products of different companies that are based on this program language.

- Attempted malicious traffic towards Web applications – **5,222**;
- Attempts to compromise Redis[13] data store data and CITRIX[14] infrastructure – **8,520**.

These attacks tell us what the attacker's preferences are, that is, which systems are more exposed to attacks and which should be paid more attention to when it comes to protection. An attack on a web server makes it possible to create high-quality phishing websites, which would take the place of the real ones and look very convincing. Also, if you are a company that depends on communication with clients or with other companies through a website, any compromise of your site or your site being unavailable creates real costs for you and makes it impossible for business to take place. Also, if we are talking about websites and services important for citizens, a good example is the COVID pandemic. If you could not access the pages where you can get your information and vaccination certificates, then you could not travel or exercise any other right. Today, we keep a lot of data on our mobile devices, not only personal data, but also financial data and data about our movements. Compromise of a mobile banking application is also an additional danger.

4.5. Distribution of attacks by country of origin

The **CSEC** team's records show Brazil was the number one source of attacks, followed by the Netherlands, United States of America, Russia, Bangladesh, Germany, China and Costa Rica. The last on the list of ten countries from which the attacks most often came are Vietnam and India.

The initial preliminary CSEC data showed most attacks came from the Netherlands and Germany, but CSEC assesses this is mainly due to attackers using a VPN (Virtual Private Network) to hide their actual locations and make it look as if they came from elsewhere. Many of these attacks are consistent with the methods and capabilities seen from Russia and China.

This view is supported by The Hacker News website[15], which published a report on how Chinese and Russian hackers use various tools, the most famous of which are SILKLOADER and BAILLOADER, to hide the original origin of their attacks and stay ahead of the law. CNN also wrote about it[16], stating that hackers most likely connected to China used the popular tool Pulse Secure VPN for months to attack various government agencies and financial institutions in the US and Europe, while AtlasVPN wrote[17] about the data they collected, according to which Russia and China sponsored more than 50 cyber attacks in 2022, and that Ukraine was the most frequent target of those attacks.

[13] Redis is a project that serves to warehouse data, as well as to store it in temporary memory, and it is particularly popular, as it enables a fast flow of data with minimal delays. It is most often used for various web applications, as it provides for information on user request in microseconds, for which reason it is used by big companies like GitHub, Twitter and StackOverflow.

[14] CITRIX is an American corporation manufacturing software designed to ensure a secure access to applications and content.

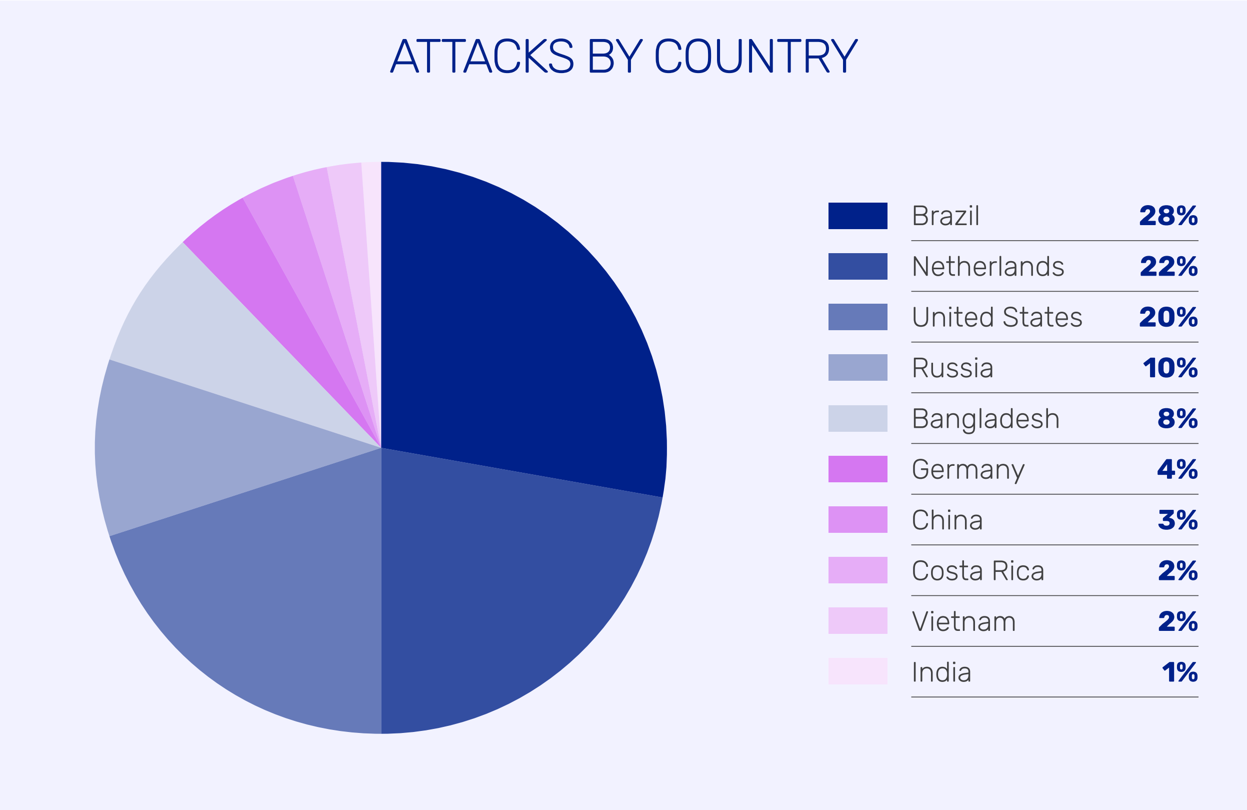
[15] https://thehackernews.com/2023/03/chinese-and-russian-hackers-using.html

[16] https://edition.cnn.com/2021/04/20/politics/fireeye-pulse-secure-vpn-exploit/index.html

[17] https://atlasvpn.com/blog/russia-and-china-sponsored-hackers-threaten-the-world-with-cyberattacks

A report[18] of the U.S. government's Cyber security and Infrastructure Security Agency (CISA) on malicious cyber activities by the Russian government, published in April 2022 (revised[19] in May 2022), states that Russian state-sponsored cyber actors have shown they can compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; extract sensitive data from IT and operational technology networks (OT); and disrupt critical industrial control systems (ICS)/OT functions by deploying destructive malware.

A report[20] by Check Point Research (CPR) suggests a rise in cyber attacks aimed at NATO countries from Chinese IP addresses. CPR, comparing the periods just before and just after the Russian invasion of Ukraine in February 2022, concluded that such cyber attacks on NATO countries more than doubled (a 116 percent rise) and worldwide attacks from the same sources rose 72 percent.



In the past year BIRN BiH, in two of its monthly TV Justice programmes, pointed to growing concern over Russian and Chinese influence in Bosnia and Herzegovina.

Through its telecommunications company Huawei, China is extending its influence around the world, which is why it has been sanctioned in some countries[21]. In the Western Balkans region, including in BiH, the company wants to be the first to establish 4G and 5G networks, and so-called smart and secure cities, but this is also raising concerns about its lack of transparency and privacy protection for users and the general public. BIRN BiH has researched the company's goals, but also

[18] https://www.cisa.gov/russia

[19] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

[20] https://blog.checkpoint.com/2022/03/21/cyber-attacks-from-chinese-ips-on-nato-countries-surge-by-116/

[21] https://detektor.ba/2022/01/07/epizoda-133-netransparentni-rast-i-uslovi-sirenja-huaweija-u-bih-i-srbiji/

the way it is expanding, finding out that Huawei paid for trips abroad for government ministers. In 2019 the USA imposed sanctions against Huawei, saying it was a security threat due to its ties with the Chinese government, to which Washington said it was giving access to other countries' data. This also raises concerns among cyber security professionals who warn that using unprotected equipment, which has not been checked and which enables easy access to key systems, might pose serious risks in key areas such as energy. They warn that, in such a way, China might gain access to various types of citizens' data, but also to key sectors, a major cause of concern. Huawei denies allegations that it works with Chinese authorities.

Western European countries and NATO have also expressed growing concern about Russian influence in BiH, most evident in the run-up to the 2022 elections. Experts have said to BIRN BiH that over the past decade, Russian President Vladimir Putin's regime has developed a number of ways to influence the elections in BiH, as it has in other European countries[22]. Western countries fear the Balkans is at particular risk of Russian influence, especially after the invasion of Ukraine.

Cyber attacks are often named by the media and expert analyses as a potential method of harmful Russian influence[23], in addition to spreading disinformation and supporting secessionist policies and extremist groups. Security experts interviewed by BIRN BiH journalists warn that Russia has interfered with different democratic processes, like elections, before, and that it is using existing societal weaknesses to foment instability in different countries. Cyber attacks stand out as one of the greatest dangers. The experts have said that the region has faced significant cyber attacks from Russia, and BiH is particularly vulnerable as it lacks key legislation such as a national cyber security strategy, a law on cyber security or information security, and a law on protecting critical infrastructure.

During the observation period, **CSEC** detected different sources of attacks, and the origin of IP addresses from which the attacks came was particularly interesting. Globally, most attacks come from known attackers, meaning IP addresses whose geographical location could be identified.

An analysis of IP addresses from which the attacks came shows that ***MOST ARE IN THE NETHERLANDS, THE UNITED STATES OF AMERICA AND GERMANY.*** *A detailed analysis found that* ***2,376,706 ATTACKS*** *came from only two of the most frequently used IPs - nearly 30 percent of the total. [See table below]*

As noted, the reason so many attacks come from those IP addresses is probably because attackers use VPN servers stationed in those countries. Experts assume the attackers are mainly from Russia and China.

[22] https://detektor.ba/2022/09/09/epizoda-141-kako-rusija-moze-uticati-na-izbore-u-bih/

[23] https://detektor.ba/2022/09/09/epizoda-141-kako-rusija-moze-uticati-na-izbore-u-bih/

Source IP	Count	Geographically
185.224.128.2	1.345.411	Netherlands
72.251.235.152	1.031.295	USA
45.95.147.40	295.367	Netherlands
67.217.56.210	203.008	USA
185.250.223.122	123.813	USA
173.212.233.104	103.868	Germany
91.235.137.223	64.956	Netherlands
212.80.219.230	61.515	Netherlands
45.93.16.176	57.974	Germany
212.80.219.226	57.489	Netherlands

Next on the list of attacks, according to origin of IP addresses, are mass scanners, or programs designed for rapid scanning of ports and websites on which different types of applications or data are stored. Contemporary mass scanners are designed scan the entire Internet as fast as possible and, according to Robert Graham who created mass scanners that can be done in less than six minutes.

Mass scanners are most often used by cyber security professionals and bug "hunters" in certain systems in order to identify problems in a particular network, or to personally find points that can potentially be targeted by cyber attacks and identify the shortcomings of their own system in order to strengthen it. This method is often used by attackers too, in order to detect deficiencies in a network as rapidly as possible, through which they could launch a successful cyberattack. The reason so many attempted cyber attacks use this method is precisely its speed and ability to get the desired data in a very short time to break through security measures and gain access to a network.

Attacks with hidden sources are ranked third and fourth most common, and they are carried out through devices called anonymizers such as the TOR exit node, which is a server through which it is possible to access an anonymous network, protecting its users, the attackers, from traffic analysis. Other anonymizers may be any program that tries to hide online activity or make it untraceable, and those are usually some proxy servers through which attackers connect to the Internet, hiding their data.

The last on the list are bots, or crawlers, which include different search engines designed to record content across the Internet with the main goal of obtaining information from every page on the Internet for future use.

4.6. DDoS attacks

Nearly 44 percent of attacks recorded by **CSEC** over the three-month period were **DDoS attacks**, more than 3.8 million of them alone in the last 30 days of observation.

DDoS attacks are most often used to attack an Internet page, which means in practice that a particular service is flooded with a huge number of specially designed requests until visitors can no longer access the site or service. These attacks are most frequently carried out through a botnet, i.e. a network of computers infected with a certain virus, which can be controlled and exploited to submit many requests to a particular IP address, making the identification of attackers very complex.

Such attacks have been used to disable the Internet pages of BiH media, especially after they publish investigations about political corruption.

A report by the European Union's CERT for 2020[24] found that DDoS attacks were frequently used to extort money – usually in the form of bitcoin cryptocurrency - or other benefits. It noted several DDos extortion campaigns, in sectors including banking, finance and real estate. Usually an attacker would demand money or other benefits in return for not launching DDoS attacks. The most active attackers were hidden behind the names D4BC, Lizard Squad, Stealth Ravens, Armada Collective and Fancy Bear; the latter was recognized as an imitation of a Russian spying threat that has recently been suspected of intimidating victims. In a well-known recent case, a DDos attack shut down the New Zealand stock market for four days in a row.

DDoS attacks often target BiH media portals, shutting them down and potentially jeopardizing their operations. The editorial offices of Internet portals Žurnal.info, 6yka.com and Klix.ba have struggled with attacks which completely disabled access to their websites. That hampers their operations at several levels. Access to their websites was blocked and editorial teams were also forced to allocate additional resources to defending themselves from this type of cyberattack.

Klix.ba editor-in-chief Semir Hambo confirmed that the media outlet has to deal with such problems on its own, which eats up its resources.

> *"Klix.ba faces DDoS attacks almost daily. Those attacks generally do not hinder our work to a large extent, but they do waste time and resources. Of course,* ***THOSE ATTACKS ARE SOMETIMES MORE PRONOUNCED AND STRONGER, SLOWING DOWN OUR WORK.*** *Our IT team counters the DDoS attacks on its own as much as they can, and so far we have managed to protect ourselves, but it has surely left consequences," he said. "We face a constant threat of being unable to work because they burden our system." Hambo said it was important to have a clear action plan in case of an attack, as well as a prevention strategy.*

[24] https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf

These attack methods were also deployed in Ukraine one day before the start of Russia's invasion, when Ukrainian banks and institutions were struck by massive DDoS attacks.

4.7. Cyber attacks in BiH detected through OpenCanary Honeypot device

Another type of device with which **CSEC** records attacks is a network of **Canary devices**, which are set up in a network to detect attempted cyber attacks before the attacker manages to compromise the system completely. **OpenCanary**, in fact, is a bait using 16 servers which attackers most often try to attack and compromise. This device has a smaller range than **Tpot servers**, so the number of recorded attacks is smaller, but it helps significantly in comparing attacks, because it gives an insight into precisely specified attacks.

From November 18 to December 17, 2022, this device recorded **520,717 attacks**, mostly (335,319) attempts to control computers.

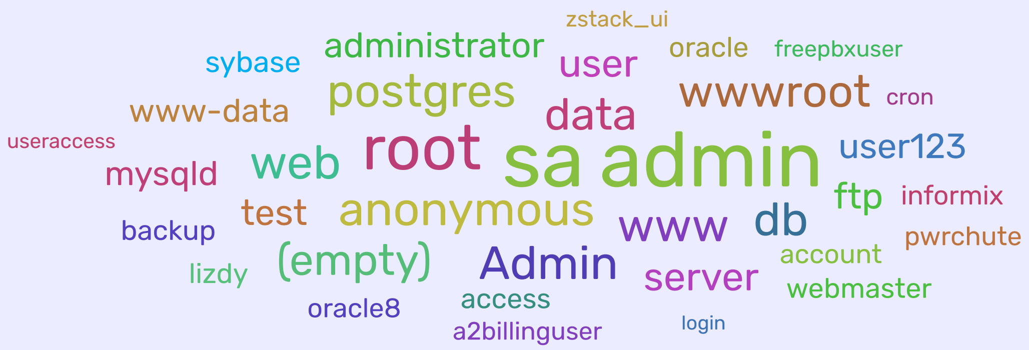
Other recorded attacks include the following:

- MSSQL and MySQL – 159,157 attacks; These attacks include attempts to gain unauthorized access to various databases whose work is based on MSSQL and MySQL systems. During such attacks, hackers try to exploit data, which they then destroy or change with the aim of manipulating the device they are attacking.
- FTP, SMB, SIP, HTTP and HTTPS – 8,745 attacks; These attacks actually try to compromise different data exchange protocols, through which users access the Internet or different databases. Here too, attackers aim to access the data exchanged via these protocols, in order to ultimately control various data that they can misuse later.
- Redis – 862 attacks; Redis, like MSSQL and MySQL system, is a database management service, therefore the goal of the attacker is the same as with the previously mentioned databases.
- Attempts to compromise Android devices – 478 attacks; In this case, attackers try to get into devices running the Android operating system, most often mobile devices and smartphones. In this case, if the attack is successful, the attacker can fully control such devices, copy data from it, monitor movement, start various processes or simply destroy the device.
- NTP and SNMP – 642 attacks; NTP is a protocol used by millions of computers to synchronize the time on them, and by attacking this protocol, attackers can find out how many computers are connected to a certain network and which computers they are. After that, by attacking some other protocols, such as SNMP, which is responsible for the management and monitoring of devices connected to the Internet, they can get to the devices themselves and data that allows them to attack other data and databases on these computers. SNMP are also protocols used by millions of computers to synchronize their clocks.

4.8. Cyber security advisor - Usernames and passwords

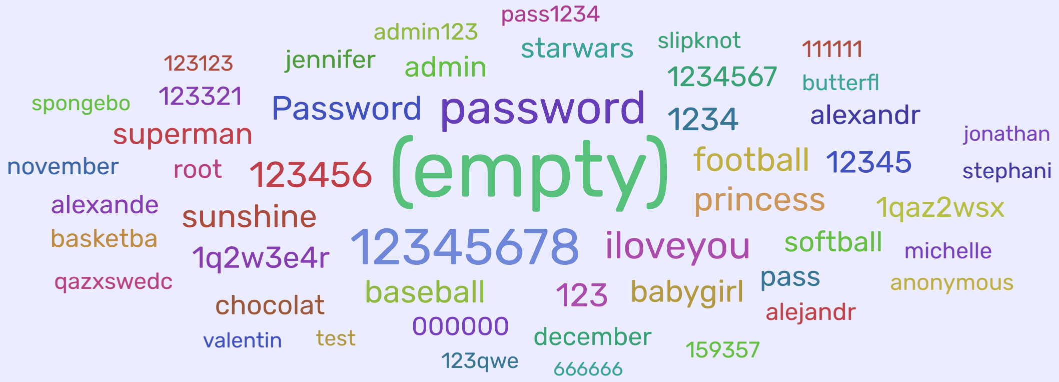
Attackers often try to compromise devices online using predefined usernames and passwords, which are part of standard installations. One example is the pre-set modem or router logon passwords customers get when they want to set up an Internet connection at home. These can make a home network vulnerable. Users or administrators of certain network systems themselves often choose such user data, bringing them and the entire system in danger.

MOST FREQUENTLY USED USERNAMES



As the number of home devices using WiFi connections grows, so does the number of devices susceptible to attack. More complex networks, in institutions or big companies, have many more devices, but the point through which they access the Internet still makes them vulnerable.

MOST FREQUENTLY USED PASSWORDS



Changing predefined usernames and using more complex passwords as soon as possible will make it much harder for attackers to access the devices.

Time it takes a hacker to brute force your password in 2022					
Numbers of Characters	**Numbers Only**	**Lowercase Letters**	**Uper and Lowercase Letters**	**Numbers, Uper and Lowercase Letters**	**Numbers, Uper and Lowercase Letters, Symbols**
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

4.9. Government measures update

BIRN BiH previously analyzed the lack of a systematic approach to cyber security in Bosnia an Herzegovina[25]. As noted above, BiH remains the only Western Balkans country not to have a national cyber security strategy, and it also lacks a state-level body for cyber security as well as documents that need to be harmonized with EU legislation in the EU accession process.

A document developed by DCAF (the Geneva Centre for Security Sector Governance) and BIRN BiH about cyber security and human rights[26] emphasized that Bosnia and Herzegovina's complicated legal and administrative system directly affects its lagging behind in recognizing cyber security as a key issue.

As part of the EU accession process, BiH will have to take steps to ensure its digital networks and information systems are secure. It must revise its national legislation and implementation as laid out in the Stabilization and Association Agreement signed with the European Community in 2008, which is directly connected with implementing the Council of Europe's Convention on Cybercrime (Budapest Convention) and the EU's General Data Protection Regulation (GDPR).

Several documents have so far been adopted, including the Budapest Convention on Cybercrime, strategies for establishing a national CERT, and for preventing and fighting terrorism, as well as an analysis of (non)compliance of laws regulating cyber security in BiH. The country must adopt a cyber security strategy, a law on organization and competencies of state bodies for countering cybercrime and information security, and must strengthen its workforce in information and communications.

In the observation period, BiH legislative authorities made no significant changes to the legal framework covering cyber security.

[25] https://detektor.ba/2022/11/14/bih-ranjiva-na-cyber-napade-zbog-nedostatka-kljucnih-dokumenata/

[26] https://detektor.ba/wp-content/uploads/2022/12/Cyber-sigurnost-FINAL-WEB-pages-1.pdf

CYBERSECURITY IN BiH:

Adopted documents

- Budapest Convention on Cybercrime,
- Strategy for Establishment of BiH CERT,
- Strategy for the Prevention of and Fight against Terrorism 2015-2020,
- Information Security Management Policy in BiH Institutions for the period 2017-2022,
- Decision designating CERT for institutions of BiH,
- Analyses on (non)compliance of legal regulations in cybersecurity field in BiH.

Required documents

- Strategy on cybersecurity in BiH,
- Law on organization and competencies of state bodies for countering cybercrime,
- Law on information security, a
- Rulebook on systematization of jobs and internal organization of Security Ministry,
- Lack of information and communication professionals

5.

About Cyber Security Excellence Center in BiH

BiH finds itself in a disadvantaged position as the last Western Balkans country with no functioning all-encompassing state-level CSIRT. This leaves BiH, its government, economy and citizens exposed to cyber harm to an extent that may jeopardize the potential benefits of digitalization for the economy and society, and leaves the country more exposed to malign external influences in the cyber domain.

CSEC will try to bridge this gap, and in two years will develop into BiH's last cyber security resort, aiming to provide an active and effective response to cyber security incidents. The CSEC's academic origin provides the opportunity to combine expertise and experience, building links with the private sector and ultimately supporting cyber security workforce development in BiH.

The ultimate mission of CSEC is to "position itself as a neutral, 'go-to' point for systematic response to cyber incidents in BiH in order to support the development of and improvement of cyber security in BiH". CSEC, also, plans to strengthen communication between cyber security stakeholders and other CSIRT teams in the region. The vision of CSEC is "a safe and secure cyberspace in BiH for all".

6.

About BIRN BiH

BIRN BiH is a media non-governmental organization based in Sarajevo, specializing in monitoring and reporting on trials for war crimes, corruption and terrorism. BIRN BiH journalists have been leading sources for the public in the areas of transitional justice, rule of law and extremism for years.

Since its establishment in 2005, BIRN BiH has been informing the public about the prosecution of war crimes by state and local courts in BiH, and also at international courts. Tens of thousands of reports of hearings, statements by witnesses to crimes, surviving victims and family members of the missing are stored on the Detektor.ba[27] website. In 2015, BIRN BiH started a project dedicated to monitoring and reporting on cases of organized crime, corruption and terrorism. Since then, a number of analyses, researches and documentaries have been published on corruption affairs, unprocessed criminal acts and trips to foreign battlefields, for which international organizations awarded BIRN's team[28].

BIRN BiH journalists also shed light on the spread of extremist and right-wing groups in the region, revealing trends that spill over into BiH and warning of the negative consequences. In addition to guest appearances and the publication of around 25,000 articles, BIRN BiH also produces a monthly show, called TV Justice - of which 145 episodes have been published by January 2023. There are plans to further develop the TV production with a show about disinformation and digital security.

Through various projects, BIRN gave public access to several databases – on terrorism, hatred, official cars, mass graves and on established court facts intended for educational purposes. Working independently and through various collaborations, BIRN BiH has so far published ten publications, available here[29].

The editorial office of BIRN BiH grows year by year[30], and with it, with the support of donors, new projects dedicated to transitional justice, the rule of law, extremism and the fight for human rights.

[27] https://detektor.ba/nagrade/

[28] https://detektor.ba/nagrade/

[29] https://detektor.ba/birn-publikacije/

[30] https://detektor.ba/impresum

7.

Terminology

With a view to better understanding the cyber security issues, including incidents and attacks against computer and information systems, which come from cyberspace, as well as the terms which that were used in this concrete document, in what follows we shall define and explain the key terms and abbreviations.

Other specific terms and abbreviations are explained within the document.

Term	Brief description
Brute force	Brute Force attack implies an attempt to access the victim's system through continuous input of various letter, number and symbol combinations with the aim of identifying the username and password.
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
Cyberspace	The space within which communication between information systems takes place. It covers not only the Internet, but, in addition to an interlinked hardware, software and ICT system, it also covers people and social interactions within the frame of those linked elements.
Cyber security	Covers activities and measures to achieve confidentiality, integrity and availability of data and systems in cyberspace.
Cyber attack	Implies malicious influence on information systems, computer networks and other electronic resources, which takes place in cyberspace with the aim of jeopardizing confidentiality, integrity and availability of data that are created, processed and stored in those systems, networks and resources, and transferred through them.
Cyber event	Any occurrence in a computer network or information system that can be observed.
Demilitarized Zone	A demilitarized zone is a part of an entire network within a segmented computer network, whose role is to ensure communication and exchange of information within strictly defined and applied rules of access. At the same time, it ensures controlled access to a part of the internal network. Through development of a demilitarized zone it is easier to increase the security levels of computer resources.

DoS and DDoS	A denial-of-service attack, or DoS, is when an attacker tries to disable or obstruct an Information and Communications Technology system so that a user cannot access a server or services intended for them. A distributed denial-of-service attack, or DDoS, has the same goal but is more efficient as it simultaneously uses many compromised computer systems as the sources of the attack.
ENISA	European Union Agency for Cyber security
ICT system	Information and Communications Technology System
IP address	An Internet Protocol address is a unique number attributed to each device (e.g. computer or mobile phone) on a computer network that communicates through the Internet Protocol, i.e. the protocol for communication between sources and users via the Internet network.
Critical infrastructure	Critical infrastructure is a general term for physical and computer systems that are essential for a government or economy to function. Like attacks targeting individuals, attacks on critical infrastructure have also grown more frequent.
Malware	Malware (Malicious Software) is any software created for malevolent purpose, or the goal of which is to cause damage to computer systems or networks.
Phishing	Means a cyberattack carried out with via electronic mail, social networks, phone calls or text messages, asking the recipient to click on a link or open a document. This type of attack is used to cheat users with the aim of obtaining their login information, such as username and password. It is also called online identity theft.
Threat	Potential source of an unwanted event.
Computer-security incident	One or more computer-security occurrences that weaken the security of the information system or computer network, and jeopardize the confidentiality, integrity and availability of information that is created, processed, stored or transmitted using the information system or computer network.
SOC	The function of a Security Operations Center is to supervise, prevent, discover, investigate and respond to cyber threats 24 hours a day.
VPN	Virtual Private Network.

CSEC
Cyber Security
Excellence Centre

BIRN
BALKAN
INVESTIGATIVE
REPORTING
NETWORK

BOSNIA &
HERZEGOVINA