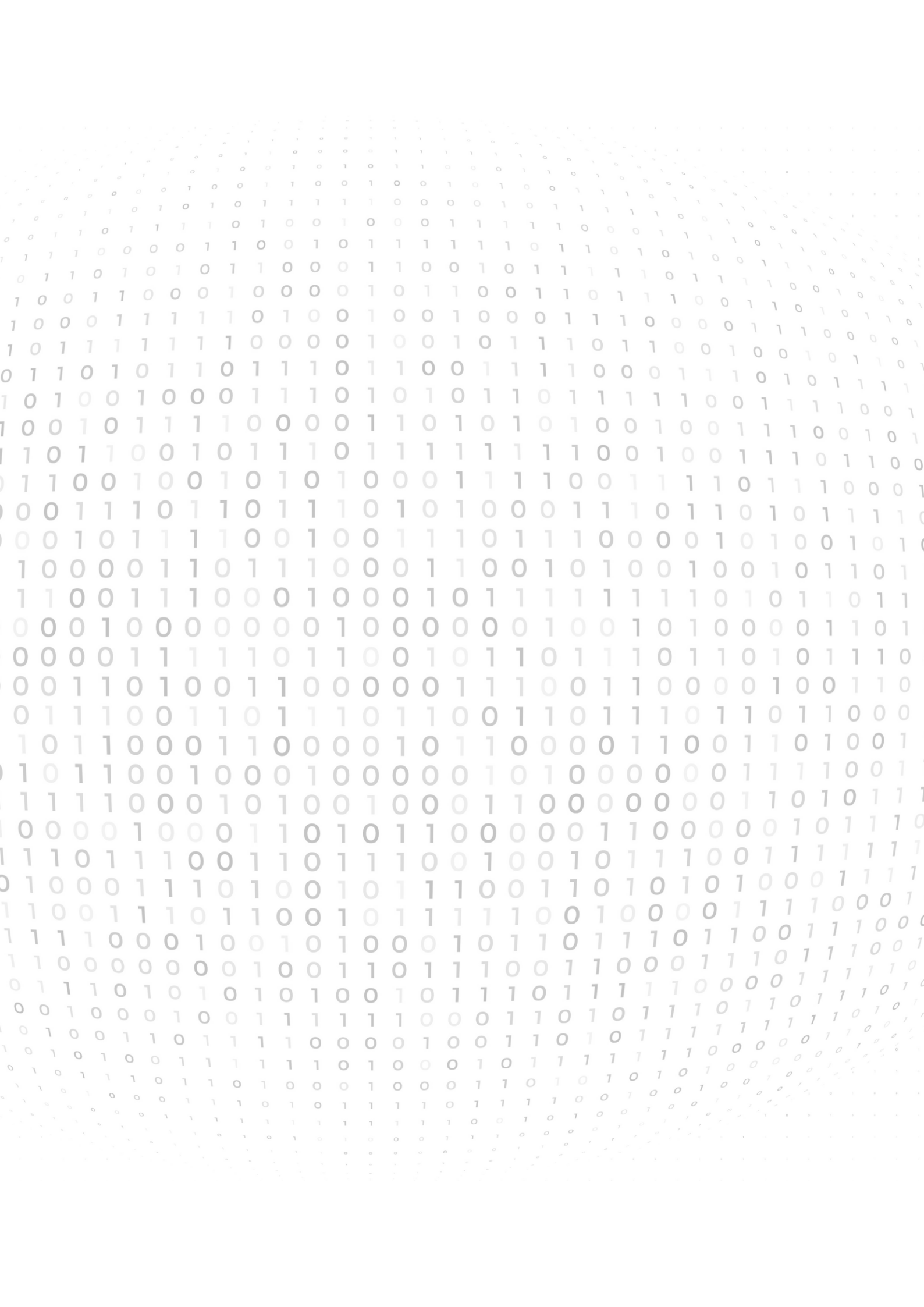
Izvještaj o

CYBER SIGURNOSNIM PRIJETNJAMA

u Bosni i Hercegovini

CSEC Cyber Security Excellence Centre

BIRN BALKAN INVESTIGATIVE REPORTING NETWORK BOSNIA & HERZEGOVINA



Izvještaj o

CYBER SIGURNOSNIM PRIJETNJAMA

u Bosni i Hercegovini

Pišu:
Aida Mahmutović i Enes Hodžić
(BIRN BiH)

Sarajevo
oktobar – decembar 2022.

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

Balkanska istraživačka mreža Bosne i Hercegovine (BIRN BiH)
Detektor.ba

Pišu: Aida Mahmutović i Enes Hodžić (BIRN BiH)

Period oktobar – decembar 2022.

Sadržaj

1. Uvod

1.1. Prva procjena cyber sigurnosnih prijetnji

Centar za izvrsnost u cyber sigurnosti (CSEC), u saradnji sa Balkanskom istraživačkom mrežom Bosne i Hercegovine (BIRN BiH), predstavlja vam prvi izvještaj o cyber sigurnosnim prijetnjama u BiH. Riječ je o prvom izvještaju u kome su obrađeni podaci prikupljeni u periodu od oktobra do decembra 2022. godine, a koji se odnose na cyber sigurnosne prijetnje koje je CSEC zabilježio u ovom periodu u BiH i koji na praktičan način ilustriraju sve cyber opasnosti sa kojima se korisnici internet prostora u našoj zemlji suočavaju.

Osnovan pri Centru za istraživanje politika suprotstavljanja kriminalitetu u Sarajevu, CSEC radi kao akademski računarski tim za hitne slučajeve (CERT), čija je osnovna zadaća uspostavljanje kanala komunikacije za prikupljanje svih detalja o potencijalnim cyber napadima, propustima i drugim vrstama opasnosti kojima su izloženi korisnici interneta u BiH. S obzirom da je formiran tokom 2022. godine, CSEC još uvijek radi na razvoju mreže različitih kontakata koji im mogu obezbijediti informacije o potencijalnim cyber sigurnosnim prijetnjama, ali i razvoju različitih događaja, kampanja i informacionih kanala putem kojih se pokušava podići nivo svijesti internet zajednice i stvoriti mogućnosti raznog upozorenja na cyber prijetnje.

1.2. Uloga CSEC-a

Kako je BiH jedina zemlja regije u kojoj ne postoji nacionalni CERT tim, članovi CSEC-a teže da ova organizacija postane centralna tačka za prikupljanje svih podataka u vezi sa internet sigurnošću, koje su kreirane u internet zajednici BiH ili koje su u vezi sa ovom zajednicom. Taj proces odvija se kroz stvaranje saradnje sa nacionalnim CERT timovima iz zemalja regije i Evropske unije, ali i sa svim vladinim i nevladinim organizacijama u BiH koje su zainteresovane za pružanje informacija o cyber prijetnjama, što bi upravo bio posao nacionalnog CERT-a koji u BiH ne postoji. Također, dodatni proces koji se odvija uz to jeste testiranje sistema i korisnika, te različite vrste obuka kako bi se ukazalo na važnost prevencije i odbrane od cyber napada.

Napadi koji su najčešće zabilježeni u promatranom periodu jesu DDoS napadi i napadi na baze podataka, što je vrlo slično iskustvima koja bilježe CERT timovi zemalja iz okruženja. Ipak, zbog kratkog vremena postojanja CSEC-a i relativno male mreže za prikupljanje podataka, te različitih metodologija prikupljanja podataka, teško je upoređivati rezultate akademskog CERT tima iz BiH sa rezultatima iz regije. No, važnost cyber sigurnosne zaštite najbolje pokazuje zabilježeni broj napada u promatranom periodu, koje je CSEC prikupio kroz vlastite honeypotove, prijavljivanje incidenata i generalno dijeljenje informacija sa drugim CERT timovima.

Iz toga je nastala i potreba za kreiranjem jednog izvještaja koji će pokazati sva dešavanja u cyber sigurnosnom svijetu Bosne i Hercegovini te koliko je važno hitno djelovanje u ovom polju.

2.

Izjava o odricanju od odgovornosti

Centar izvrsnosti za kibernetičku sigurnost (u daljnjem tekstu **CSEC**) osnovan je kao dio Centra za istraživanje kriminalne politike sa namjerom da postane dio Univerziteta u Sarajevu, radi jačanja cyber sigurnosti u Bosni i Hercegovini (BiH), uz podršku Vlade Ujedinjenog Kraljevstva. Kao dio CSEC-a, bit će uspostavljen akademski i održiv tim za odgovor na incidente u cyber bezbjednosti (CSIRT).

CSEC ne garantuje da su podaci u ovom izvještaju potpuni, tačni i ažurni. Ovakvi podaci se mijenjaju iz minute u minutu i ne odnose se na cijeli svijet i/ili geografsko područje Bosne i Hercegovine. Analiza podataka je urađena u saradnji CSEC-a i BIRN-a BiH.

Prikazani podaci odnose se na jednu tačku, odnosno jednu IP adresu te mrežu *honeypot*[1] servera u svijetu, a ukupan broj servera i njihov razmještaj nije poznat.

Podaci ne prikazuju broj uspješno izvedenih cyber napada sa posljedicama po žrtvu, već prikazuju dešavanja u cyber prostoru sa ciljem podizanja svijesti svih korisnika internetskih usluga o opasnostima koje vrebaju svakodnevno.

Cilj prikazivanja ovih podataka ni na koji način nije stvaranje loše slike o BiH, jer su ove pojave istovjetne i svakodnevne u svim dijelovima svijeta gdje postoji internet.

U najvećoj mjeri, riječ je o automatiziranim skriptama koje skeniraju mrežu u potrazi za žrtvama prema kojima "vrijedi" poduzeti korake u kompromitaciji njihovih sistema i podataka.

Balkanska istraživačka mreža Bosne i Hercegovine (u daljem tekstu **BIRN BiH**) obrađivala je u ovom izvještaju podatke dobijene od CSEC-a te ih stavljala u kontekst ranijih istraživanja **BIRN-a BiH** i drugih javno dostupnih podataka.

Cijeli dokument izvještaja je namijenjen za javnu objavu, te se svako smije njime koristiti i na njega pozivati, ali isključivo u izvornom obliku, bez izmjena i uz obavezno navođenje izvora.

Korištenje ovog dokumenta protivno navodima iznad znači povredu autorskih prava.

CSEC i BIRN BiH će Izvještaj o cyber sigurnosnim prijetnjama u BiH objavljivati dva puta godišnje. Izvještaj ima za cilj da sistemski prati i kontinuirano ukazuje na ranjivosti BiH u domenu cyber sigurnosti, kao i na izloženost potencijalnoj šteti koja može ugroziti kritičnu infrastrukturu. S obzirom na to da je jedna od osnovnih dodatnih aktivnosti CSEC-a obrazovanje i podizanje svijesti o važnosti cybersigurnosti, ovaj izvještaj će služiti za edukativne svrhe i civilnom društvu u BiH.

---

1 Honeypot je mehanizam cyber sigurnosti koji koristi namjerno "proizvedenu" metu napada da odmamicyber kriminalce od legitimnih meta. Honeypots također prikupljaju obavještajne podatke o identitetu, metodama i motivacijama protivnika. Vjerovatno najlakši način da se ovo shvati je da se honeypot vidi kao mamac koji ima za cilj privlačenje cyber napada.

3.

Sažetak glavnih nalaza izvještaja

U samo mjesec dana 2022. godine, u Bosni i Hercegovini je registrovano više od 9,2 miliona prijetnji cyber sigurnosti, od kojih su DDoS napadi najčešće zabilježeni. Taj broj napada i najnoviji revizorski izvještaji institucija, koji su pokazali da ne postoji strateški i pravni okvir za cyber sigurnost u BiH, najbolje ilustruje ranjivost građana, kompanija i institucija BiH na cyber napade koji bi mogli ugroziti ključne sektore, kao što su vladavina prava, privreda, energetika, zdravstvo ili obrazovanje.

Razmjere cyber sigurnosnih prijetnji	Od početka rada CSEC-a do trenutka objave ovog izvještaja broj cyber napada koje bilježi ovaj tim u konstantnom je porastu, što govori o važnosti monitoringa cyber sigurnosnog sektora u Bosni i Hercegovini.
Vrste napada	DDoS napadi u promatranom periodu prepoznati su kao najviše zastupljeni cyber napadi. Njihove namjene su raznovrsne, a sam učinak može biti katastrofalan po kritičnu infrastrukturu.
Najveći incidenti	Jedna od cyber sigurnosnih prijetnji koje je CSEC registrirao u posmatranom periodu posebno je zanimljiva jer je stigla sa e-mail adresa jedne od zvaničnih institucija BiH. CERT tim iz Španije primijetio je phishing kampanju sa e-mail adresa jedne od državnih institucija, a nakon reakcije srbijanskog CERT-a i CSEC-a ustanovljeno je odakle prijetnja dolazi i ona je u kratkom roku otklonjena.
Distribucija napada po zemljama	Cyber napadi zabilježeni u BiH najčešće su stizali iz Brazila, Nizozemske, SAD-a, Rusije, Njemačke i Kine. Neočekivano su se u vrhu liste našle Nizozemska i Njemačka, a pretpostavka je da je razlog činjenica da napadači iz nekih drugih zemalja najčešće koriste VPN servere u ove dvije zemlje za izvođenje napada i sakrivanje svojih podataka.
Mjere vlasti u BiH	BiH je posljednja zemlja Zapadnog Balkana bez sveobuhvatnog tima za odgovor na cyber sigurnosne incidente. To cijelu državu, infrastrukturu i građane ostavlja izložene cyber šteti i zloćudnim vanjskim utjecajima. Poseban problem predstavlja i nedostatak odgovarajućih strategija i zakonskih rješenja kojim bi ova oblast bila uređena. U periodu koji razmatra ovaj izvještaj nije bilo značajnijih izmjena zakonskog okvira, niti aktivnosti zakonodavnih vlasti u vezi sa cyber sigurnošću u BiH.

4. Izvještaj o cyber prijetnjama

Da bismo sagledali trenutno stanje cyber prijetnji u Bosni i Hercegovini, za period oktobar – decembar 2022. godine, CSEC i BIRN BiH pratili su eksploataciju ranjivosti jednog honeypot servera i jednog honeypot uređaja, koji su instalirani unutar CSEC infrastrukture na dijelu DMZ (demilitarizirane zone). Akademska jedinica za praćenje, analiziranje i reagovanje na incidente, odnosno CSEC identifikovao je i IP adrese sa kojih su te prijetnje najčešće dolazile.

BIRN BiH je analizirao podatke CSEC-a i vlastite ranije izvještaje u kojima su pojašnjavani fenomeni cyber sigurnosnih prijetnji u Bosni i Hercegovini, kao i njihovi izvori.

Ovaj izvještaj uključuje taktike, tehnike i procedure (TTP), te indikatore kompromisa (IOC) povezane sa zlonamjernim aktivnostima. Kako bi se zaštitili od ovih prijetnji, CSEC preporučuje organizacijama, institucijama, kompanijama i pojedincima da ispitaju svoje TTP sisteme i koriste IOC za otkrivanje zlonamjernih aktivnosti[2].

Ukoliko budu otkrivene bilo kakve aktivnosti poput napada i zloupotreba, institucije i kompanije bi trebale pretpostaviti da je njihov mrežni identitet kompromitovan, te slijediti procedure odgovora na incident.

4.1. Sistem prikupljanja podataka

Podaci koji su predstavljeni u ovom izvještaju prikupljeni su putem **Tpot servera** i **OpenCanary uređaja**, koji predstavljaju honeypot server i uređaj instaliran unutar CSEC infrastrukture na dijelu DMZ mreže.

Honeypot je mehanizam cyber sigurnosti koji koristi ciljano "proizvedenu" metu napada s ciljem skretanja cyber kriminalaca od legitimnih meta. Honeypot se može modelirati prema bilo kojoj digitalnoj imovini, uključujući softverske aplikacije, servere ili samu mrežu, a namjerno je dizajniran da pruža sliku legitimne mete svojim modelom, u smislu strukture, komponenti i sadržaja. Time se potencijalni napadači nastoje ubijediti da su pristupili legitimnoj meti, kako bi ih se ohrabrilo da provedu što je moguće više vremena u tom kontroliranom okruženju.

U svojoj suštini, honeypot predstavlja mamac, ali može poslužiti i kao alat za izviđanje, koristeći pokušaje napada za procjenu napadačeve tehnike, sposobnosti i sofisticiranosti. Honeypot može da imitira stvarne uređaje poput mobilnih telefona, servera ili mrežnih sistema kako bi otkrio na koji način su oni ugroženi.

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

Obavještajne informacije prikupljene honeypot uređajima korisne su u pomaganju organizacijama u evoluiranju i poboljšanju svojih strategija cyber sigurnosti, kao odgovor na prijetnje u stvarnom svijetu i vremenu, identifikaciji potencijalno slijepih tačaka u postojećoj arhitekturi, te informacijskoj i mrežnoj sigurnosti.

Tpot (Tpotce) se sastoji od 23 različita honeypot servera, od kojih svaki glumi jednu ili više vrsta poznatih i najčešće eksploatisanih servisa, protokola, aplikacija itd.

OpenCanary je zamišljen za kreiranje mreže Canary uređaja postavljenih u mreži klijenta, kako bi detektirali pokušaje cyber napada, prije nego što napadač u potpunosti uspije kompromitirati sistem. On, zapravo, predstavlja mamac koristeći 16 servisa koji najčešće bivaju napadnuti ili bivaju meta pokušaja kompromitiranja.

4.2. Najveći incidenti u periodu oktobar – decembar[3]

Iako govorimo o relativno malom uzorku, u smislu prikupljenih i analiziranih podataka – s obzirom na vremenski period ovog izvještaja – nekoliko incidenata iz promatranog perioda govore o važnosti praćenja i reagiranja na cyber sigurnosne prijetnje, kojih je u BiH sve više.

Prvo upozorenje o takvim prijetnjama stiglo je iz Španije, čiji nacionalni CERT tim je primijetio phishing kampanju sa email adresa koje nose *.ba* domenu, državnu domenu Bosne i Hercegovine. Ove e-mail adrese su pripadale jednoj od zvaničnih državnih institucija u Bosni i Hercegovini, zbog čega je bila potrebna i hitna reakcija. No, kako u Bosni i Hercegovini ne postoji zvanični nacionalni CERT tim, o čemu je BIRN BiH i ranije pisao[4], španski nacionalni CERT obratio se CERT-u Republike Srbije. Nakon toga, nezvaničnim kanalima iz Srbije ova informacija je stigla do CSEC-a. Brzom provjerom ustanovljeno je gdje se tačno nalazi e-mail server ove državne institucije, te je kontaktiran provider usluga i situacija je vrlo brzo riješena. Phishing kampanje su široko rasprostranjene i one su jedan od najčešćih alata putem kojih napadači nastoje doći do osjetljivih, ličnih podataka korisnika, kao što su korisnička imena, lozinke ili podaci s kreditnih kartica. Pojedini cyber stručnjaci navode da 97 posto inicijalnih vektora napada, odnosno načina na koji napadači započinju svoj napad, dolazi preko phishinga. Osnovni cilj napadača u ovom slučaju jeste da dođu do određenih podataka, koji će im obezbijediti mogućnost da steknu neku vrstu koristi na štetu žrtve, bilo kroz određene zahtjeve za otkupninu ili kroz direktno korištenje podataka.

Ovakve prijetnje otkrili su i novinar BIRN-a BiH, razgovarajući sa državnim parlamentarcima, koji su im pojasnili da su tokom oktobra 2022. godine sumnjivim označeni e-mailovi koji su stizali sa zvanične domene Državnog parlamenta BiH. To, praktično, znači da je neko, imitirajući administratora domene Parlamenta, pokušavao doći do podataka zastupnika u ovoj instituciji. Takvu izloženost konstantnim cyber napadima potvrdili su za BIRN BiH i u Generalnom sekretarijatu Vijeća ministara BiH, kazavši kako ne mogu potvrditi odakle su napadi došli, niti da li su u bilo kakvoj vezi s napadima na institucije nekih drugih zemalja regije.

3 Napadi koji su predstavljeni u ovom poglavlju odnose se na napade zabilježene kroz honeypot sisteme CSEC-a, ali i one o kojima su informacije stigle iz drugih izvora.

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

BIRN BiH je i ranije pisao o problemima sa kojima se suočavaju državne institucije i ustanove u BiH, zbog nepostojanja nacionalnog CERT tima i ključnih dokumenata[5] kojim bi bilo određeno tačno djelovanje u slučaju cyber napada.

> *Jedan od najkonkretnijih primjera zašto je postojanje CERT timova neophodno zabilježen je početkom septembra, kada je zaposlenike Parlamentarne skupštine dočekala obavijest u kojoj je stajalo:* ***"MOLIMO DA NE PALITE RAČUNARE DOK NE DOBIJETE OBAVIJEST."*** *Tada je ustanovljen problem sa pristupom e-mailovima i drugim digitalnim servisima u Parlamentarnoj skupštini i Vijeću ministara BiH, zbog cyber napada, što dovoljno govori o* ***RANJIVOSTI CYBER INFRASTRUKTURE OVE ZEMLJE.*** *Slične prijetnje zabilježene su i u oktobru 2022. godine, kada su sumnjivim označeni e-mailovi koji su stizali sa zvanične domene Državnog parlamenta BiH.*

Problemi sa informacionim tehnologijama u državnim institucijama traju već godinama, pa su tako i u aprilu 2017. godine serveri Vijeća ministara bili blokirani, ali ne zbog cyber napada, nego zbog neslaganja dvije državne službe oko toga ko je nadležan za održavanje klima-uređaja u server sali[6], te sporosti da se problem otkloni i otkazivanja sistema upozoravanja. Zbog toga su serveri bili pregrijani, te su gotovo u potpunosti zaustavili rad državnih institucija na četiri cijela dana. Ovakvi primjeri najbolje ilustruju nepostojanje jasnih strateških, zakonskih i organizacionih okvira u bh. institucijama, kada je riječ o zaštiti informacionih tehnologija i cyber sigurnosti.

Drugi incident zabilježen je direktno kroz honeypot sisteme CSEC-a, nakon što je registrirana neobična aktivnost koja je dolazila sa IP adresa iz opsega jednog od subjekata sa kojim CSEC ostvaruje saradnju od osnivanja. Nakon prikupljenih informacija o vrsti i načinu napada, članovi CSEC-a kontaktirali su IT osoblje ovog subjekta, te je vrlo brzo otkriven kompromitovani izvor napada, koji je potom i uklonjen.

Treći primjer koji ilustruje aktivnosti CSEC-a u prethodnom periodu dogodio se nakon dojave iz Neretva grupe[7], da se iz IP adresnog prostora koji pripada akademskom sektoru jedne od zemalja iz bh. susjedstva širio malware sadržaj. CSEC je potom obavijestio kolege iz nacionalnog CERT-a ove zemlje, te je brzom reakcijom i procedurama otklonjena uočena nedozvoljena aktivnost.

4.3. Distribucija napada u BiH

CSEC je tokom perioda od oktobra do decembra 2022. godine zabilježio veliki broj cyber sigurnosnih incidenata na dva uređaja koji su korišteni kao mamci u njihovoj mreži. Prvi od tih uređaja nosi naziv **Tpot (Tpotce)** i predstavlja uređaj koji se sastoji od 23 različita honeypot servera, od kojih svaki glumi jedan ili više vrsta poznatih i najčešće eksploatisanih servisa, protokola i aplikacija.

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 U bliskoj saradnji s Delegacijom EU-a i specijalnim predstavnikom EU-a u BiH, Misija OSCE-a u BiH je osnovala međunarodnu koordinativnu grupu, Neretva grupa, koja se sastoji od stručnjaka za cybersigurnost. Izvor: https://www.osce.org/files/f/documents/9/7/468372.pdf

Među njima su serveri koji detektiraju pokušaje napada na Android uređaje, različite vrste napada na industrijske kontrolne protokole i *brute force* terminalne napade, DDOS napade, pokušaje kompromitacije različitih servera i servisa, kao i oni koji bilježe *login* podatke u pokušaju napada na određene servise, te detektor prevara putem telefonskih poziva, simulator printera i e-mail servisa.

Svi ovi dijelovi uređaja pomažu kako bi što veći broj i što više vrsta napada mogli biti zabilježeni širom svijeta.

U konkretnom slučaju CSEC-a, ovaj **Tpot** server korišten za prikupljanje podataka dio je mreže **Tpot** servera Deutsche Telekom Securityja, te svjetski trendovi prikupljeni kroz ovu mrežu pokazuju da se širom svijeta, u prosjeku, događa:

- 65.000–115.000 napada u jednoj minuti;
- 3–4,5 miliona napada u jednom satu;
- 55–80 miliona napada tokom 24 sata.

> *Važno je napomenuti da ovi podaci nisu potpuni, niti sveukupni, nego predstavljaju **SAMO PRESJEK SA POSTOJEĆIH Tpot SERVERA U SVIJETU,** a stvarni broj napada se mijenja iz minute u minutu i vjerovatno je taj broj mnogostruko veći.*

4.4. Cyber napadi zabilježeni kroz Tpot uređaj

Broj napada u Bosni i Hercegovini zabilježen kroz ovaj servis mijenja se konstantno, te je i u trenutku pisanja ovog izvještaja broj napada zabilježenih pomoću **Tpot** uređaja u konstantnom porastu, što nam govori o važnosti njihovog praćenja, registriranja i adekvatnog procesuiranja u cyber sigurnosnom okruženju BiH.

U posljednjih trideset dana promatranog perioda, zabilježeno je ukupno **8.733.270 napada**, od čega najveći broj zauzimaju **DDoS napadi sa 3.827.666** zabilježenih napada. Ovaj broj najbolje ilustruje koliko tehnologija ide izvan poimanja prosječnog korisnika tehnologije, gdje se stvari dešavaju mnogo brže u realnom vremenu, te ovakav broj napada nije neočekivana posljedica. Naredni na ovoj listi su **napadi na PBX[8] infrastrukturu, Telnet napad i napadi na web servere**, kojih je u navedenom periodu zabilježeno **3.607.736**.

Ostatak napada odnosi se na sljedeće:

- Pokušaj kontrole nad računarima, te pokušaji eksploatacije e-mail protokola i Postgres baza podataka[9] – **632.462 napada**;
- Pokušaji kompromitiranja FTP[10] servera, te MSSQL i MySQL/MariaDb baza podataka[11] – **612.125 napada**;

8 PBX je akronim od engleskog "Private Branch Exchange", a predstavlja privatnu telefonsku mrežu koja omogućava korisnicima da razgovaraju jedni s drugima.

9 Postgres (PostgeSQL) je vrsta objektno-orijentisanih relacionih sistema za upravljanje bazama podataka. Smatra se jednom od najpouzdanijih baza podataka, a najčešće se koristi za web aplikacije i web baze podataka.

10 FTP (File Transfer Protocol) je standardizirani mrežni protokol koji se koristi za razmjenjivanje podataka između dva ili više računara, preko mreže bazirane na TCP protokolu, kao što je internet.

11 SQL je programski jezik u kojem se pišu upiti za rad s bazama podataka, te se uz njegovu pomoć vrši odabir i izmjena informacija, a MySQL i MSSQL su proizvodi različitih kompanija koji su bazirani na ovom programskom jeziku.

- Pokušaji eksploatacije Android uređaja – **13.853 napada**;
- Pokušaji eksploatacije industrijskih kontrolnih protokola – **6.086 napada**;
- Pokušaji malicioznog prometa prema web aplikacijama – **5.222 napada**;
- Pokušaji kompromitacije Redis[12] data store podataka i CITRIX[13] infrastrukture – **8.520 napada**.

Ovi napadi nam govore koje su preferencije napadača, odnosno koji sistemi su više izloženi napadima i na koje treba obratiti više pažnje u zaštiti. Napad na web server omogućava stvaranje kvalitetnih phishing web stranica, koje bi bile postavljene umjesto pravih i izgledale vrlo uvjerljivo. Također, ako ste kompanija koja ovisi o komunikaciji sa klijentima ili sa drugim kompanijama putem web stranice, svako kompromitiranje vaše stranice ili njena nedostupnost stvara stvarne troškove za vas i onemogućuje poslovanje. Također, ako je riječ o web stranicama i servisima važnim za građane, dobar primjer je pandemija COVID-a. Ako niste mogli pristupiti stranicama na kojima možete dobiti svoje informacije i potvrde o vakcinaciji, tada ne biste mogli putovati niti ostvariti bilo koje drugo pravo. Danas na svojim mobilnim uređajima čuvamo mnogo podataka, ne samo klasične lične, već i finansijske podatke i podatke o našem kretanju. Dodatna opasnost je i kompromitacija aplikacije za mobilno bankarstvo.

4.5. Raspodjela napada prema zemlji porijekla

Pregled najčešćih zemalja iz kojih su dolazili napadi prema Bosni i Hercegovini koje je zabilježio **CSEC** tim pokazuje da se na vrhu ove liste nalazi Brazil kao zemlja iz koje je stiglo ubjedljivo najviše napada. Naredne na listi su Nizozemska i Sjedinjene Američke Države (SAD), a zatim Rusija, Njemačka, Kina i Kostarika. Posljednje na listi deset zemalja iz kojih su napadi najčešće stizali su Vijetnam i Indija.

Prema prvim preliminarnim podacima CSEC-a, najveći broj napada dolazi iz Nizozemske i Njemačke. Pretpostavka je da je osnovni razlog to što napadači najčešće za izvođenje različitih napada koriste VPN [engl. Virtual Private Network – Virtualna privatna mreža], pomoću koje sakrivaju stvarne lokacije izvora napada. Metode i načini napada koji su zabilježeni, kao i skrivanje putem VPN konzistentno je sa napadima koje su zabilježene širom svijeta iz Rusije i Kine.

Ovaj stav podržava i web stranica The Hacker News[14], koja je objavila izvještaj o tome kako kineski i ruski hakeri koriste različite alate, od kojih su najpoznatiji SILKLOADER i BAILLOADER, kako bi sakrili izvorno porijeklo svojih napada i ostali ispred zakona. O tome je pisao i CNN[15], navodeći da su hakeri najvjerovatnije povezani s Kinom mjesecima koristili popularni alat Pulse Secure VPN za napade na razne vladine agencije i finansijske institucije u SAD-u i Evropi, dok je

12 Redis je projekt koji služi za skladištenje podataka, kao i za njihovu pohranu u privremenu memoriju, a posebno je popularan jer omogućava brz protok podataka uz minimalno kašnjenje. Najčešće se koristi za različite web aplikacije, jer omogućava obezbjeđivanje određene informacije na korisnički zahtjev u mikrosekundama, zbog čega ga koriste velike kompanije kao GitHub, Twitter i StackOverflow.

13 CITRIX je američka korporacija koja proizvodi softvere dizajnirane da obezbijede siguran pristup aplikacijama i sadržajima.

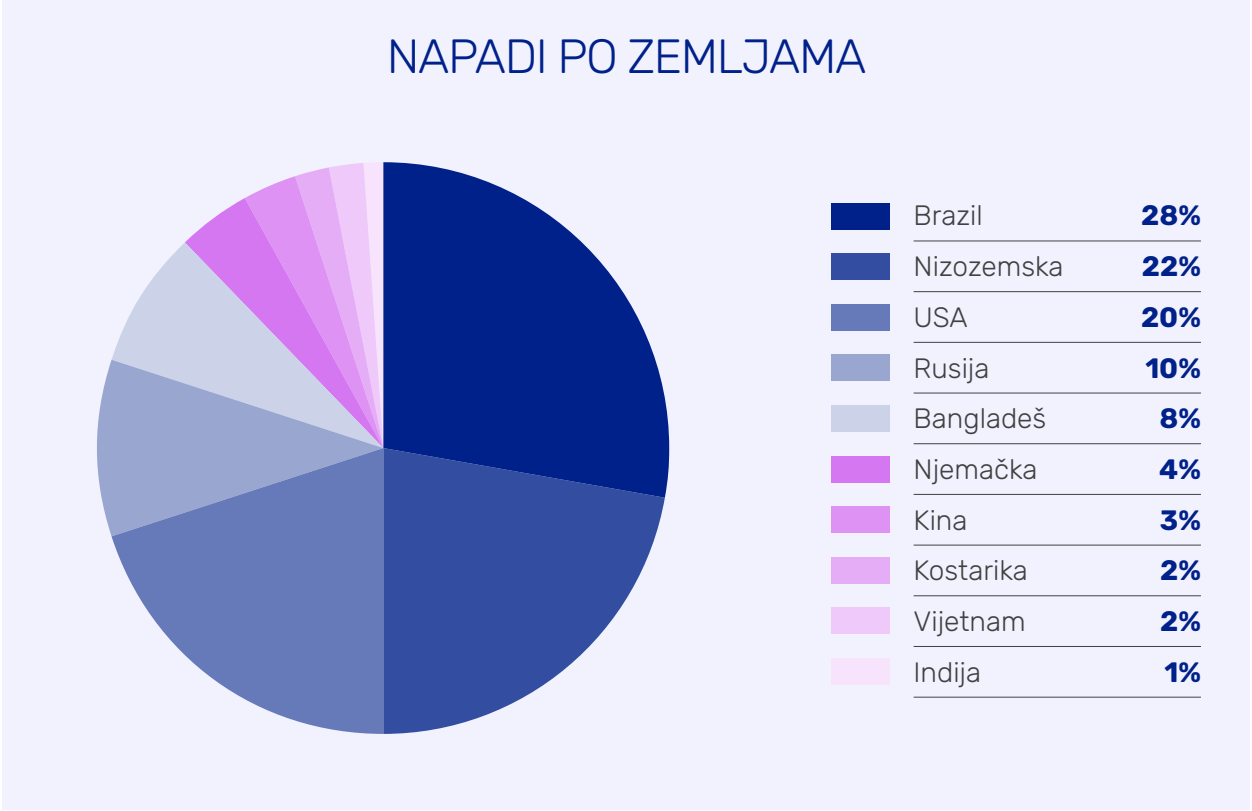
14 https://thehackernews.com/2023/03/chinese-and-russian-hackers-using.html

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

AtlasVPN pisao o podacima[16] koje su prikupili, prema kojima su Rusija i Kina sponzorirale više od 50 cyber napada 2022. godine, a Ukrajina je bila najčešća meta tih napada.

U izvještaju[17] Agencije za kibernetičku sigurnost i sigurnost infrastrukture (CISA) američke vlade o zlonamjernim cyber aktivnostima ruske vlade, objavljenom u aprilu 2022. (revidiranom[18] u maju 2022.), navodi se da su cyber akteri koje sponzorira ruska država pokazali da mogu kompromitovati IT mreže; razviti mehanizme za održavanje dugoročnog, trajnog pristupa IT mrežama; izdvojiti osjetljive podatke iz IT i mreža operativne tehnologije (OT) i poremetiti funkcije kritične industrijske upravljačke sisteme (ICS)/OT funkcije primjenom destruktivnog zlonamjernog softvera.

Izvještaj[19] kompanije Check Point Research (CPR) ukazuje na porast cyber napada usmjerenih na zemlje NATO-a sa kineskih IP adresa. Upoređujući periode neposredno prije i neposredno nakon ruske invazije na Ukrajinu u februaru 2022., zaključili su da su se takvi cyber napadi na zemlje NATO-a više nego udvostručili (porast od 116 posto), a napadi širom svijeta iz istih izvora porasli su za 72 posto.



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

17 https://www.cisa.gov/uscert/russia

18 https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

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

BIRN BiH je u protekloj godini, kroz dvije mjesečne emisije TV Justice, ukazivao na rastuću zabrinutost zbog ruskog i kineskog utjecaja u Bosni i Hercegovini.

Kina kroz telekomunikacijsku kompaniju Huawei širom svijeta širi i svoj utjecaj[20], zbog čega je dospjela na listu sankcija nekih zemalja. U regionu, pa tako i u BiH, ova kompanija želi biti prva u uspostavljanju 4G i 5G mreža, takozvanih pametnih i sigurnih gradova, ali izaziva i zabrinutost zbog mogućeg manjka transparentnosti i zaštite privatnosti korisnika i građana.

BIRN BiH je istraživao ciljeve, posljedice, ali i načine širenja ove kompanije, te je tom prilikom otkriveno kako je Huawei plaćao ministrima odlaske na putovanja. SAD su Huaweiju 2019. godine uvele sankcije uz obrazloženje da predstavlja sigurnosnu prijetnju zbog veza sa kineskom vladom, kojoj daje pristup podacima drugih zemalja. To izaziva i zabrinutost cyber sigurnosnih profesionalaca, koji upozoravaju da bi korištenje nezaštićene opreme, koja nije provjerena i koja omogućava lak ulazak u ključne sisteme, moglo utjecati na odvijanje normalnog života na različite načine kroz, recimo, upravljanje energetskim ili nekim drugim sektorima. Upozoravaju da bi, na taj način, Kina mogla dobiti pristup različitim vrstama podataka građana, ali i ključnim sektorima, što je već samo po sebi zabrinjavajuće. Iz kompanije Huawei negiraju navode koji ih optužuju za saradnju sa kineskim vlastima.

S druge strane, zemlje zapadne Evrope i NATO izražavaju sve veću zabrinutost od ruskog utjecaja u BiH, a najviše se to očitovalo u predizbornom periodu tokom 2022. godine. Eksperti su za BIRN BiH pojasnili kako je režim ruskog predsjednika Vladimira Putina u posljednjoj deceniji razvio cijeli niz načina na koje može utjecati na izbore u BiH, što je već ranije zabilježeno u nekim drugim zemljama Evrope[21], a zabrinutost raste posebno jer je Balkan označen kao jedna od ključnih tačaka u opasnosti od ruskog utjecaja, nakon invazije na Ukrajinu.

Ova povećana zabrinutost posebno se ističe u svijetu cyber napada[22] koji se, uz širenje dezinformacija i podržavanje secesionističkih politika i ekstremističkih grupa, najčešće spominju u medijskim i stručnim analizama kao mogući načini ruskog štetnog utjecaja.

Stručnjaci sa kojima su razgovarali novinari BIRN-a BiH upozorili su kako se Rusija i ranije miješala u različite demokratske procese, poput izbora, te da koriste postojeće slabosti kako bi doveli do nestabilnosti u različitim zemljama. Uz neke standardne alate, cyber napadi, kao i razna digitalna sredstva u digitalnom okruženju izdvajaju se kao jedna od najvećih opasnosti. Zemlje regije suočile su se u značajnoj mjeri sa cyber napadima iz Rusije, koji su u velikoj mjeri utjecali na funkcioniranje zemalja, a u BiH postoji još i veća zabrinutost zbog nepostojanja ključnog zakonodavstva kojim bi se oblast cyber sigurnosti uredila do zadovoljavajućeg nivoa, kao što su nacionalna strategija cyber sigurnosti, zakon o cyber sigurnosti ili sigurnosti informacija, te zakon o zaštiti kritične infrastrukture koji bi pomogli u uređivanju ove oblasti.

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

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

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

Bilježeći napade **CSEC** je u obrađivanom periodu zabilježio i različite izvore napada, a posebno je zanimljivo porijeklo, odnosno reputacija IP adresa sa kojih su napadi dolazili. Gledano na globalnom planu, najveći broj napada dolazi od *poznatih napadača [engl. known attacker]* što predstavlja IP adrese koje je moguće na bilo koji način locirati, u smislu geografskog lociranja odakle ti napadi potiču.

Pri analiziranju tačnih IP adresa sa kojih su stizali napadi, najveći broj tih adresa lociran je u Nizozemskoj, Sjedinjenim Američkim Državama (SAD) i Njemačkoj. Detaljnija analiza pokazuje da je ***SA SAMO DVIJE, OD DESET NAJČEŠĆE KORIŠTENIH IP ADRESA, STIGLO 2.376.706 NAPADA,*** *što predstavlja gotovo 30 posto ukupnih napada koje je CSEC zabilježio u promatranom periodu.*

Kako smo u prethodnom poglavlju naveli, napadi sa ovih IP adresa u ovolikoj mjeri dolaze, najvjerovatnije, zbog toga što napadači za svoje napade koriste VPN servere stacionirane u tim zemljama. Pretpostavka je da ih najčešće koriste napadači iz Rusije i Kine.

Source IP	Count	Geografski
185.224.128.2	1.345.411	Nizozemska
72.251.235.152	1.031.295	SAD
45.95.147.40	295.367	Nizozemska
67.217.56.210	203.008	SAD
185.250.223.122	123.813	SAD
173.212.233.104	103.868	Njemačka
91.235.137.223	64.956	Nizozemska
212.80.219.230	61.515	Nizozemska
45.93.16.176	57.974	Njemačka
212.80.219.226	57.489	Nizozemska

Naredni na listi napada, prema reputaciji IP adresa, su ***mass scanneri***, koji predstavljaju programe konstruisane za što brže skeniranje portova, odnosno mrežnih mjesta na kojima se nalaze različite vrste aplikacija ili podataka. Današnji ***mass scanneri*** dizajnirani su kako bi mogli omogućiti što je moguće brže skeniranje cijelog interneta, a prema autoru ***mass scannera*** Robertu Grahamu, to može biti učinjeno za manje od šest minuta.

Mass scannere najčešće koriste cyber security profesionalci i "lovci" na greške u određenim sistemima, k ako bi pronašli probleme u određenoj mreži, odnosno kako bi sami pronašli tačke koje potencijalno mogu biti meta cyber napada i kako bi identificirali nedostatke svog sistema, u cilju njegovog jačanja. Ovu metodu nerijetko koriste i napadači, kako bi na najbrži način otkrili nedostatke u mreži ili mrežama, putem kojih bi mogli uputiti cyber napad sa većom mogućnošću ulaska u određenu mrežu. Razlog velikog broja pokušaja cyber napada ovom metodom jeste upravo njena brzina, odnosno mogućnost da se za veoma kratko vrijeme dobiju traženi podaci koji mogu olakšati pristup određenoj mreži i proboj sigurnosnih mjera.

Treće i četvrto mjesto na listi napada prema ovoj vrsti analize zauzimaju napadi čiji izvori su skriveni, a koji se odvijaju preko ***TOR exit nodea*** ili drugih različitih anonimizatora. TOR exit node, u tom slučaju, predstavlja server putem kojeg je moguće pristupiti anonimnoj mreži čime su korisnici, u ovom slučaju napadači, zaštićeni od analize saobraćaja. Drugi ***anonimizatori*** mogu biti bilo koji programi kojima se aktivnosti na mreži pokušavaju sakriti ili učiniti nemogućim za praćenje, te je obično riječ o nekim proxy serverima, preko kojih se napadači povezuju sa internetom, sakrivajući pritom svoje podatke.

Posljednje mjesto na ovoj listi zauzimaju ***botovi***, odnosno ***crawleri*** koji predstavljaju različite tražilice dizajnirane da bilježe sadržaj širom interneta, sa osnovnim ciljem da dobiju informacije sa svake stranice na internetu, kako bi ove informacije mogle biti korištene u nekom narednom periodu.

4.6. DDoS napadi

Gotovo 44 posto napada koje je **CSEC** zabilježio u prethodnom periodu predstavljaju **DDoS napadi**, sa više od 3,8 miliona napada u posljednjih 30 dana promatranog perioda. DDoS je akronim za Distributed Denial of Service, odnosno napade čiji je cilj onemogućavanje korisnika da koriste određeni servis na koji je ovakav napad usmjeren.

DDoS napadi se najčešće koriste za napad na neku internet stranicu, a u praksi to znači da se "bombarduje" određeni servis sa izrazito velikim brojem posebno napravljenih zahtjeva, sve dok ne "zatrpa" zahtjevima do te mjere da posjetitelji više ne mogu otvoriti određenu web stranicu ili neku drugu vrstu servisa. Ovi napadi su problematični jer se danas najčešće izvode putem *botneta*, odnosno mreže računara zaraženih određenim virusom koje je moguće kontrolisati i iskoristiti na način da svi ti računari pošalju veliki broj zahtjeva na određenu IP adresu, zbog čega je otkrivanje napadača jako kompleksan proces.

U BiH se u proteklim godinama ova vrsta napada koristila za onesposobljavanje internet stranica medija, posebno nakon što objave istraživanje o političkoj korupciji.

U izvještaju CERT tima Evropske unije za 2020. godinu[23] DDoS napadi su zabilježeni kao jedni od najčešćih napada koji se koriste kao metoda iznude novca ili druge vrste koristi. U tom izvještaju zabilježeno je nekoliko kampanja DDoS iznuda, u nekoliko sektora uključujući bankarstvo, finansije i nekretnine. Najčešće se ovakve vrste napada izvode na način da napadači traže određenu korist, kako ne bi pokrenuli DDoS napade, a najaktivniji napadači u ovom polju bili su oni skriveni iza naziva D4BC, Lizard Squad, Stealth Ravens, Armada Collective i Fancy Bear, koji je prepoznat kao imitacija ruske špijunske prijetnje, a koja se u posljednje vrijeme najvjerovatnije koristi za zastrašivanje žrtava. Postoji nekoliko napada koji su izvedeni na ovaj način, a jedan od najpoznatijih je napad na berzu Novog Zelanda, koja bila zatvorena četiri dana zaredom zbog DDoS napada. Zahtjevi za otkupninu zbog ovih napada najčešće su izraženi u kriptovaluti bitcoin.

Medijski portali u Bosni i Hercegovini česte su žrtve DDoS napada, što nerijetko dovodi do potpune obustave njihovog rada, čime je potencijalno ugroženo i njihovo poslovanje. Redakcije portala Žurnal.info, *6yka.com* i *Klix.ba* često su se borile sa ovakvim napadima, kada je potpuno onemogućen pristup njihovim stranicama. To njihovo poslovanje otežava na nekoliko nivoa, te osim onemogućenog pristupa stranici, ove redakcije bivaju primorane izdvajati dodatne resurse kako bi se odbranili od ove vrste cyber napada.

Semir Hambo, glavni i odgovorni urednik portala *Klix.ba*, potvrđuje kako se medij za koji on radi samostalno bori sa ovakvim problemima, što im oduzima brojne resurse.

> *"Klix.ba ima DDoS napade gotovo na svakodnevnoj osnovi. Ti napadi uglavnom ne otežavaju rad u nekoj većoj mjeri, ali itekako troše vrijeme i resurse. Naravno,* ***TI NAPADI NEKADA BUDU IZRAŽENIJI I JAČI I TADA USPORE NAŠ RAD.*** *Protiv DDoS napada se borimo sami koliko može naš IT tim i do sada smo se uspijevali zaštititi, međutim to svakako ima posljedice jer usporava rad i stalna je prijetnja da ćete biti onemogućeni u vašem radu, jer vam opterećuju sistem", pojašnjava Hambo, dodavši da je u sistemu odbrane važno imati jasan plan djelovanja u slučaju napada i preveniranu strategiju.*

Ove metode napada korištene su i u Ukrajini, samo dan prije početka ruske invazije na ovu zemlju, kada su ukrajinske banke i institucije pogođene masovnim DDoS napadima.

4.7. Cyber napadi u BiH zabilježeni kroz OpenCanary Honeypot uređaj

Druga vrsta uređaja kojima **CSEC** bilježi napade jesu mreža **Canary uređaja**, koji su postavljeni u mreži kako bi detektirali pokušaje cyber napada prije nego što napadač u potpunosti uspije kompromitirati sistem. **OpenCanary**, zapravo, predstavlja mamac od 16 servisa koje napadači najčešće pokušavaju napasti i kompromitirati. Ovaj uređaj ima manji opseg u odnosu na **Tpot**

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

servere, zbog čega je broj zabilježenih napada mnogo manji, ali predstavlja značajnu pomoć u komparativnoj analizi napada, jer omogućavaju uvid u precizno specificirane napade.

Preko ovog uređaja, u periodu od 18. novembra do 17. decembra 2022. godine, zabilježeno je **520.717 napada**, od čega najveći broj napada zauzimaju pokušaji kontrole nad računarima, sa **335.319 napada.**

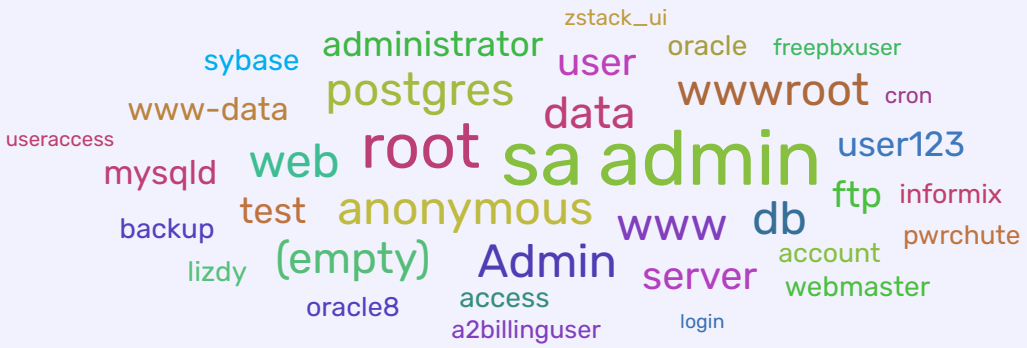
Ostali napadi zabilježeni su u sljedećem obimu:

- MSSQL land MySQL – 159.157 napada; Ovi napadi uključuju pokušaje neovlaštenog pristupa različitim bazama podataka čiji je rad zasnovan na MSSQL i MySQL sistemima. Tokom ovakvih napada, hakeri pokušavaju da iskoriste podatke koje potom uništavaju ili manipulišu sa ciljem da manipulišu uređajem koji napadaju.
- FTP, SMB, SIP, HTTP and HTTPS – 8.745 napada; Ovi napadi zapravo pokušavaju kompromitovati različite protokole za razmjenu podataka, preko kojih korisnici pristupaju internetu ili različitim bazama podataka. I ovdje napadači imaju za cilj pristupiti podacima koji se razmjenjuju putem ovih protokola, kako bi u konačnici kontrolirali različite podatke koje kasnije mogu zloupotrijebiti.
- Redis – 862 napada; Redis je, kao i MSSQL i MySQL sistem, servis za upravljanje bazom podataka, stoga je cilj napadača isti kao i kod prethodno navedenih baza podataka.
- Pokušaji kompromitovanja Android uređaja – 478 napada; U ovom slučaju napadači pokušavaju da uđu u uređaje koji koriste operativni sistem Android, najčešće mobilne uređaje i pametne telefone. U tom slučaju, ako je napad uspješan, napadač može u potpunosti kontrolirati takve uređaje, kopirati podatke s njih, pratiti kretanje, pokrenuti razne procese ili jednostavno uništiti uređaj.
- NTP i SNMP – 642 napada; NTP je protokol koji koriste milioni računara za sinhronizaciju vremena na njima, a napadom na ovaj protokol napadači mogu saznati koliko je računara povezano na određenu mrežu i koji su to računari. Nakon toga, napadom na neke druge protokole, kao što je SNMP, koji je odgovoran za upravljanje i praćenje uređaja povezanih na internet, mogu doći do samih uređaja i podataka koji im omogućavaju napad na druge podatke i baze podataka na tim računarima. SNMP su protokoli koje koriste milioni računara za sinhronizaciju svojih satova.

4.8. Cyber security savjetnik - Korisnička imena i lozinke

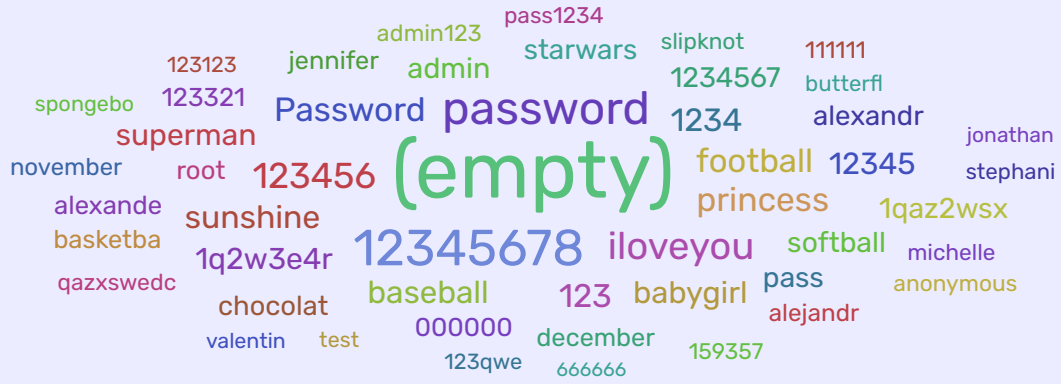
Jedna od najčešćih tehnika koje napadači koriste pri pokušaju kompromitiranja različitih uređaja na mreži, jeste zapravo korištenje predefiniranih korisničkih imena i lozinki, koje su dio standardnih instalacija. Tačnije, oni koriste različita korisnička imena i lozinke,kakvi se dodjeljuju po automatizmu različitim uređajima, kakvi su recimo mrežni routeri, kako bi zatim pristupili određenoj tački unutar mreže i crpili podatke. Nerijetko i sami korisnici ili administratori određenih mrežnih sistema biraju ovakve korisničke podatke, čime dovode u opasnost i sebe, ali i cijeli sistem.

NAJČEŠĆE KORIŠTENA KORISNIČKA IMENA



Naprimjer, modem odnosno router koji građani dobiju kada instaliraju internet priključak za svoj stan često ima unaprijed određene podatke za pristup što kućnu mrežu čini ranjivom. Sve je više kućnih uređaja koji koriste WiFi konekcije pa je i broj uređaja koji se mogu napasti veći. Kompleksnije mreže poput onih u institucijama ili velikim kompanijama imaju puno više uređaja ali tačka putem koje pristupaju internetu i dalje ih čini ranjivima.

NAJČEŠĆE KORIŠTENE LOZINKE



Kako bi se izbjegle kompromitacije sistema, važno je prilikom korištenja uređaja čim je prije moguće blokirati predefinisana korisnička imena i što je moguće kompleksnije lozinke, koje će umnogome otežati napadačima da potencijalno pristupe uređajima koje pokušavamo zaštititi ovim podacima.

Na fotografijama iznad mogli ste pogledati pregled najčešćih korisničkih imena i lozinki koje korisnike mogu dovesti u opasnost, jer izborom ovakvih korisničkih podataka olakšavaju napadačima pokušaj pristupa određenim uređajima.

Vrijeme koje je potrebno hakeru da grubo unese vašu lozinku u 2022. godini					
Broj karaktera	**Samo brojevi**	**Mala slova**	**Velika i mala slova**	**Brojevi, velika i mala slova**	**Brojevi, velika i mala slova, simboli**
4	Odmah	Odmah	Odmah	Odmah	Odmah
5	Odmah	Odmah	Odmah	Odmah	Odmah
6	Odmah	Odmah	Odmah	Odmah	Odmah
7	Odmah	Odmah	2 sekunde	7 sekundi	31 sekunda
8	Odmah	Odmah	2 minute	7 minuta	39 minuta
9	Odmah	10 sekundi	1 sat	7 sati	2 dana
10	Odmah	4 minute	3 dana	3 sedmice	5 mjeseci
11	Odmah	2 sata	5 mjeseci	3 godine	34 godine
12	2 sekunde	2 dana	24 godine	200 godina	3 hiljade godina
13	19 sekundi	2 mjeseca	1 hiljadu godina	12 hiljada godina	202 hiljade godina
14	3 minute	4 godine	64 hiljade godina	750 hiljada godina	16 miliona godina
15	32 minute	100 godina	3 miliona godina	46 miliona godina	1 milijardu godina
16	5 sati	3 hiljade godina	173 miliona godina	3 milijarde godina	92 milijarde godina
17	2 dana	69 hiljada godina	9 milijardi godina	179 milijardi godina	7 triliona godina
18	3 sedmice	2 miliona godina	467 milijardi godina	11 triliona godina	438 triliona godina

4.9. Ažuriranje vladinih mjera

BIRN BiH je ranije analizirao[24] nedostatak sistemskog pristupa polju cyber sigurnosti u Bosni i Hercegovini, te nedostatak ključnih dokumenata koji bi obezbijedili veću sigurnost na ovom polju. BiH je i dalje jedina država Zapadnog Balkana koja nema državnu strategiju za cyber sigurnost, a nedostaje i cijeli niz dokumenata koje je potrebno uskladiti sa zakonodavstvom EU, u približavanju zemlje EU, kao i državno tijelo za cyber sigurnost.

Dokument koji su razvili DCAF i BIRN BiH s osvrtom na cyber sigurnost i ljudska prava[25] naglašava da je pravni i administrativni sistem u Bosni i Hercegovini komplikovan i direktno utiče na to da država kaska u prepoznavanju cyber sigurnosti.

U skladu sa naporima BiH u procesu pridruživanja EU, država će morati provesti mjere koje će osigurati visok nivo sigurnosti njenih digitalnih mreža i infomacijskih sistema. Obavezna je izmijeniti svoje nacionalno zakonodavstvo i provedbu prema Sporazumu o stabilizaciji i pridruživanju potpisanom sa Evropskim zajednicama 2008. godine, što je u direktnoj vezi sa provođenjem Konvencije Vijeća Evrope o cyber kriminalu (Konvencija iz Budimpešte) i Opšte uredbe EU-a o zaštiti podataka (GDPR).

Do sada je usvojeno nekoliko dokumenata, među kojima su Budimpeštanska konvencija o cyber kriminalu, strategije za uspostavu nacionalnog CERT-a te prevenciju i borbu protiv terorizma, kao i analiza (ne)usklađenosti pravnih propisa u domenu cyber sigurnosti u BiH. Ono što je prijeko potrebno za razvoj cyber sigurnosti u BiH jeste usvajanje Strategije o kibernetičkoj sigurnosti, zatim zakona o organizaciji i nadležnostima državnih organa za borbu protiv cyber kriminala te informacionoj sigurnosti, kao i rad na jačanju kadrovskih kapaciteta u informacionoj i komunikacijskoj struci.

U periodu koji razmatra ovaj izvještaj nije bilo značajnijih izmjena zakonskog okvira, niti aktivnosti zakonodavnih vlasti u vezi sa cyber sigurnošću u BiH.

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

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

5.

O Cyber Security Excellence Centru u BiH

BiH se nalazi u nepovoljnom položaju, s obzirom na to da je posljednja zemlja Zapadnog Balkana bez funkcionalnog sveobuhvatnog državnog CSIRT-a. Ovo ostavlja BiH, njene vlasti, ekonomiju i građane izloženim cyber šteti u mjeri koja može ugroziti potencijalne dobrobiti digitalizacije za ekonomiju i društvo, a zemlju učiniti izloženijom zloćudnim vanjskim utjecajima u cyber domeni.

CSEC će nastojati da premosti ovaj nedostatak, uz plan da u roku od dvije godine bude u službi posljednjeg cyber sigurnosnog utočišta u BiH, sa zadatkom aktivnog i učinkovitog odgovora na cyber sigurnosne incidente. Akademsko porijeklo CSEC-a pruža priliku za kombinovanje stručnosti i iskustva, izgradnju veza s privatnim sektorom i u konačnici podršku razvojne snage u cyber sigurnosti u BiH.

Finalna misija CSEC-a je “pozicionirati se kao neutralna, ‘go-to’ tačka za sistemski odgovor na cyber incidente u BiH, u cilju podrške razvoju i poboljšanju cyber sigurnosti u BiH”. CSEC, također, planira ojačati komunikaciju između zainteresiranih strana u svijetu cyber sigurnosti i drugih CSIRT timova u regiji. Vizija CSEC-a je “siguran i zaštićen cyber prostor u BiH za sve”.

6.

O BIRN-u BiH

BIRN BiH je medijska, nevladina organizacija sa sjedištem u Sarajevu specijalizirana za praćenje i izvještavanje sa suđenja za ratne zločine, korupciju i terorizam. Novinari BIRN-a BiH godinama su vodeći izvori za javnost iz oblasti tranzicijske pravde, vladavine prava i ekstremizma.

Od svog formiranja 2005. godine, BIRN BiH informiše javnost o procesuiranju ratnih zločina pri državnom i lokalnim sudovima u BiH, ali pred međunarodnim sudovima. Na stranici *Detektor.ba*[26] pohranjene su desetine hiljada izvještaja sa ročišta, izjava svjedoka zločina, preživjelih žrtava i članova porodica nestalih. BIRN BiH je 2015. započeo projekat posvećen praćenju i izvještavanju o slučajevima organiziranog kriminala, korupcije i terorizma. Od tada je objavljeno niz analiza, istraživanja i dokumentarnih emisija o korupcijskim aferama, neprocesuiranim krivičnim djelima i odlascima na strana ratišta, a za koje su međunarodne organizacije nagrađivale tim BIRN-a BiH[27].

Novinarke i novinari BIRN-a BiH također ukazuju na širenje ekstremističkih i desničarskih grupa u regionu, otkrivajući trendove koji se prelijevaju i u BiH, te upozoravajući na negativne posljedice. Uz gostovanja u medijima, objavu oko 25.000 tekstova, BIRN BiH producira i mjesečnu emisiju pod nazivom TV Justice – kojih je do januara 2023. godine objavljeno 145 epizoda. U planu je i dodatno razvijanje TV produkcije emisijom o dezinformacijama i digitalnoj sigurnosti.

Kroz različite projekte, BIRN je javnosti omogućio uvid u nekoliko baza podataka – bazu terorizma, mržnje, službenih automobila, masovnih grobnica i bazu sudski utvrđenih činjenica koja je namijenjena u edukativne svrhe. Samostalnim radom, te kroz različite saradnje, BIRN BiH je do sada objavio deset publikacija dostupnih ovdje[28].

Redakcija BIRN-a BiH raste iz godine u godinu[29], a s njom uz podršku donatora i novi projekti posvećeni tranzicionoj pravdi, vladavini prava, ekstremizmu i borbi za ljudska prava.

26 https://detektor.ba/nagrade/
27 https://detektor.ba/nagrade/
28 https://detektor.ba/birn-publikacije/
29 https://detektor.ba/impresum

7.

Pojmovi

U cilju boljeg razumijevanja problematike cyber sigurnosti, odnosno incidenata i napada prema kompjuterskim i informacijskim sistemima koji dolaze iz cyber prostora, kao i pojmova koji će biti korišteni u ovom konkretnom dokumentu, u nastavku ćemo definisati i objasniti ključne pojmove i skraćenice.

Drugi specifični pojmovi i skraćenice pojašnjeni su unutar dokumenta, u sklopu odgovarajućih cjelina koje se njima bave.

Pojam	Kratki opis
Brute force	Brute Force napad podrazumijeva pokušaj pristupa sistemu žrtve neprekidnim unosom različitih kombinacija slova, brojeva i simbola sa ciljem identifikacije korisničkog imena i lozinke.
CERT	[engl. Computer Emergency Response Team] – Računarski tim za hitne slučajeve
CIRT	[engl. Computer Incident Response Team] – Tim za odgovore na računarske incidente
CSIRT	[engl. Computer Security Incident Response Team] – Tim za odgovore na računarske sigurnosne incidente
Cyber prostor	Prostor unutar kojeg se odvija komunikacija između informacijskih sistema. Obuhvata ne samo internet, već pored međusobno povezanog hardvera, softvera i IKT sistema obuhvata i ljude i društvenu interakciju u okviru ovih povezanih elemenata.
Cyber sigurnost	Obuhvata aktivnosti i mjere kojima se postiže povjerljivost, cjelovitost i dostupnost podataka i sistema u cyber prostoru.
Cyber napad	Podrazumijeva zlonamjeran utjecaj na informacijske sisteme, računarske mreže i ostale elektroničke resurse, koji se odvija u cyber prostoru s ciljem ugrožavanja povjerljivosti, cjelovitosti i dostupnosti podataka koji se na tim sistemima, mrežama i resursima stvaraju, obrađuju, pohranjuju i koji se putem njih prenose.
Cyber događaj	Svaka pojava u računarskoj mreži ili informacijskom sistemu koju je moguće uočiti.

Demilitarizirana zona	Demilitarizovana zona (eng. Demilitarized zone) – posebna zona (segment mreže) u okviru segmentirane računarske mreže, koja treba omogućiti komunikaciju i razmjenu informacija sa vanjskom mrežom u skladu sa jasno definisanim i primijenjenim pravilima pristupa, ali isto tako obezbjeđuje kontrolisan pristup segmentu lokalne (unutrašnje) mreže. Implementacijom pravilno konfigurisane demilitarizovane zone postiže se bolji nivo bezbjednosti računarskih resursa.
DoS i DDoS	Napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema [engl. denial-of-service attack – DoS] je pokušaj napadača da onemogući pristup serveru ili servisima namijenjenim korisnicima. Takav distribuirani napad naziva se DDoS napad, te ima isti cilj kao DoS napad. DDoS napadi postižu veću efikasnost koristeći istovremeno više kompromitovanih računarskih sistema kao izvore napada.
ENISA	Agencija Evropske unije za cyber sigurnost
IKT sistem	Informaciono-komunikacioni sistem
IP adresa	[engl. Internet Protocol adress] je jedinstveni broj koji se dodjeljuje svakom uređaju (npr. računaru ili mobitelu) na računarskoj mreži koja za komuniciranje koristi internetski protokol, tj. protokol za komunikaciju između izvora i korisnika preko internet mreže.
Kritična infrastruktura	Kritična infrastruktura je opšti izraz za fizičke i računarske sisteme koji su ključni za funkcionisanje vlade i privrede. Osim napada na pojedince, sve češći su napadi na kritične infrastrukture.
Malware	Malware [engl. Malicious Software] predstavlja svaki softver koji je napisan u zlonamjerne svrhe, odnosno čiji je cilj nanošenje štete računarskim sistemima ili mrežama.
Phishing	Podrazumijeva cyber napad koji se vrši uz pomoć elektronske pošte, društvenih mreža, telefonskog poziva ili SMS-a, kojim se zahtijeva da se posjeti link ili otvori dokument. Ovaj tip napada se koristi da bi korisnik bio prevaren, u cilju dobijanja njegovih podataka za prijavu, kao što su korisničko ime i lozinka. Još se naziva i mrežna krađa identiteta.
Prijetnja	Potencijalni izvor neželjenog događaja.
Računarsko-sigurnosni incident	Jedan ili više računarsko-sigurnosnih događaja koji su narušili odnosno narušavaju sigurnost informacijskog sistema ili računarske mreže, te ugrožavaju povjerljivost, cjelovitost i dostupnost informacija koje se korištenjem informacijskog sistema ili računarske mreže kreiraju, obrađuju, pohranjuju ili prenose.
SOC	[engl. Security Operations Center] je Sigurnosno-operativni centar čija je funkcija nadziranje, sprečavanje, otkrivanje, istraživanje i odgovaranje na cyber prijetnje 24 sata dnevno.
VPN	[engl. Virtual Private Network] Virtualna privatna mreža

CSEC
Cyber Security
Excellence Centre

BIRN
BALKAN
INVESTIGATIVE
REPORTING
NETWORK
BOSNIA &
HERZEGOVINA