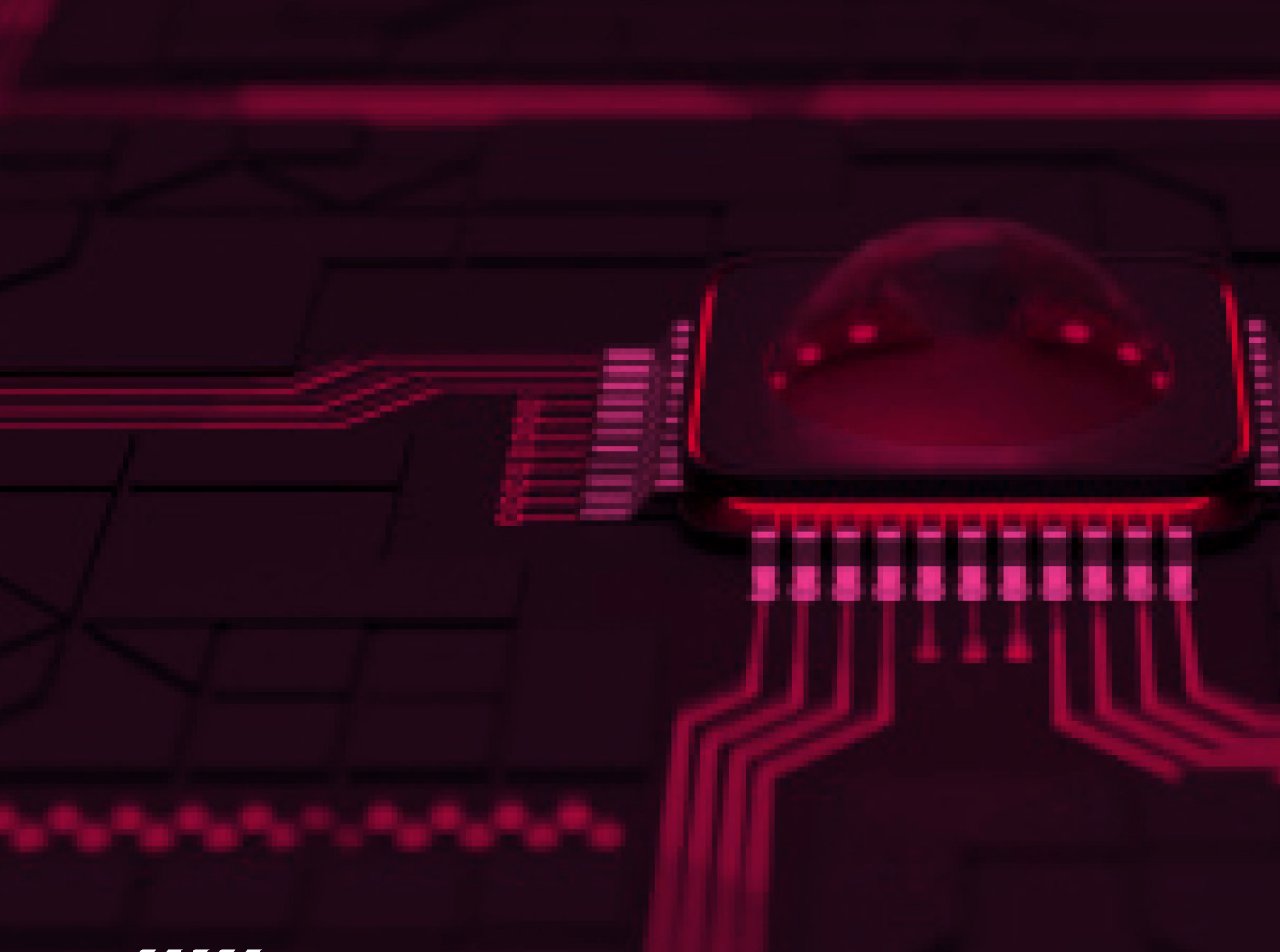


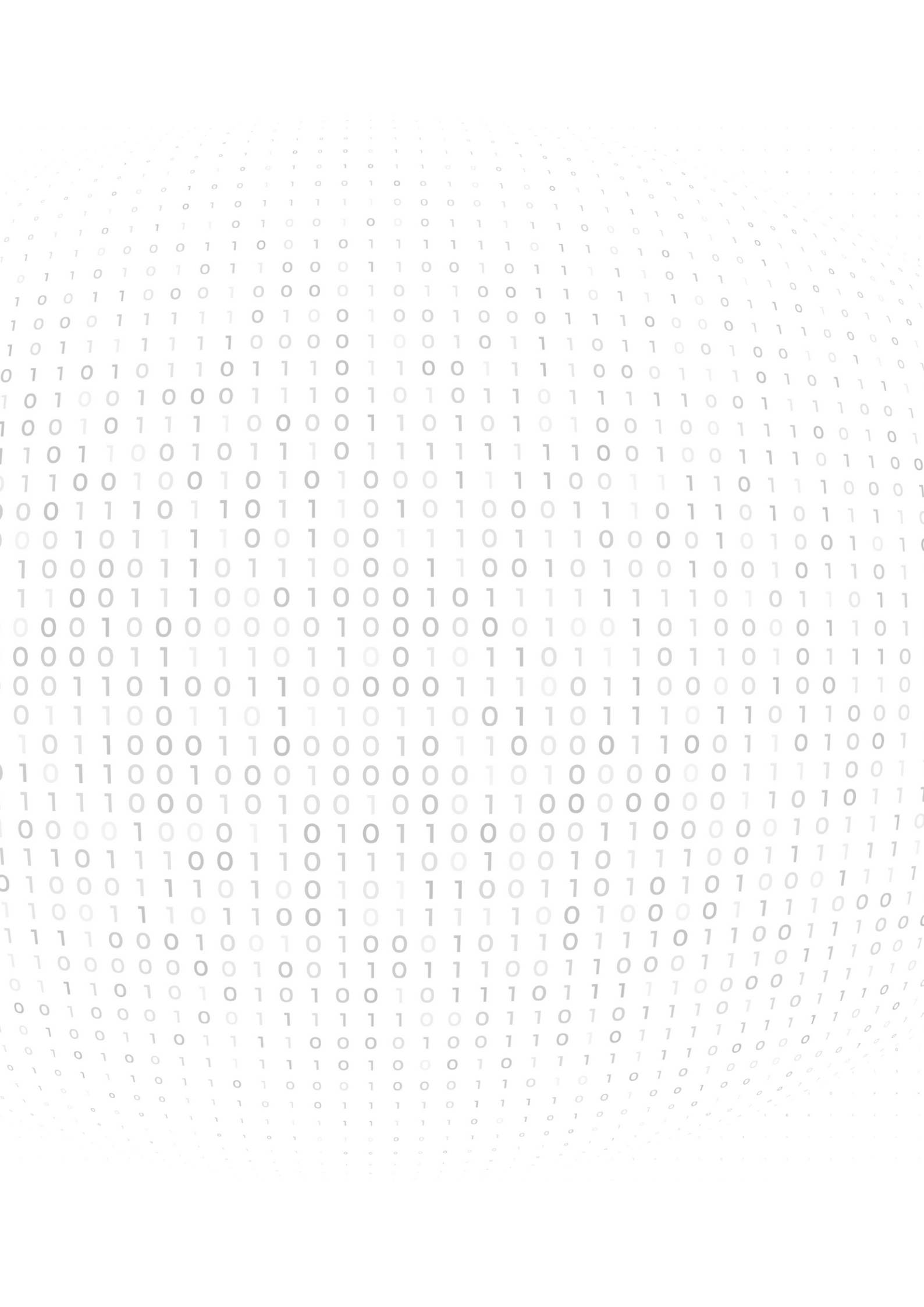
Bosna i Hercegovina

IZVJEŠTAJ O CYBER SIGURNOSNIM PRIJETNJAMA

Oktobar 2023.

CSEC Cyber Security Excellence Centre

BIRN BALKAN INVESTIGATIVE REPORTING NETWORK BOSNIA & HERZEGOVINA



Bosna i Hercegovina

IZVJEŠTAJ O CYBER SIGURNOSNIM PRIJETNJAMA

Oktobar 2023.

Autori:

Predrag Puharić, Aleksandar Đurić,
Jurica Banić i Enes Halilović (CSEC)

Enes Hodžić i Aida Mahmutović
(BIRN BiH)

januar – august 2023.

Centar za izvrsnost u cyber sigurnosti (CSEC)
csec.ba

u saradnji s

Balkanskom istraživačkom mrežom Bosne i Hercegovine (BIRN BiH)
Detektor.ba

Autori:
Predrag Puharić, Aleksandar Đurić, Jurica Banić i Enes Halilović (CSEC)
Enes Hodžić i Aida Mahmutović (BIRN BiH)

januar – august 2023.

Sadržaj

1. Uvod

Centar za izvrsnost u cyber sigurnosti (CSEC), u saradnji s Balkanskom istraživačkom mrežom Bosne i Hercegovine (BIRN BiH), predstavlja drugi izvještaj o cyber sigurnosnim prijetnjama u BiH. Prvi izvještaj ovakve vrste objavljen je u martu 2023. i u njemu su obrađeni podaci prikupljeni u periodu od oktobra do decembra 2022. godine.

U novom izvještaju predstavljamo trendove i cyber sigurnosne prijetnje na osnovu podataka koje je CSEC prikupio od januara do augusta 2023. godine. Oni na praktičan način ilustriraju opasnosti s kojima se suočavaju korisnici interneta u našoj zemlji.

1.1. Uloga CSEC-a

Osnovan kao dio Udruženja Centar za istraživanje politike suprotstavljanja kriminalitetu (CPRC) u Sarajevu, CSEC djeluje kao akademski računarski tim za hitne slučajeve (CERT) s glavnim zadatkom uspostavljanja komunikacijskih kanala za prikupljanje svih detalja o potencijalnim cyber napadima, propustima i drugim vrstama opasnosti kojima su korisnici interneta u BiH izloženi. S obzirom na to da je osnovan tokom 2022. godine, CSEC i dalje radi na razvoju mreže različitih kontakata koji mu mogu pružiti informacije o potencijalnim cyber prijetnjama, kao i na razvoju raznih događaja, kampanja i informativnih kanala za podizanje svijesti zajednice o internetu, kao i uspostavljanju alata i mogućnosti za rano upozoravanje na cyber prijetnje.

Kako je BiH jedina zemlja u regionu koja nema nacionalni CERT, članovi CSEC-a nastoje da ta organizacija bude centralna tačka za prikupljanje svih podataka koji se odnose na internet sigurnost, a koji su ili kreirani u okviru internet zajednice u BiH ili su povezani s tom zajednicom. Proces se odvija kroz uspostavljanje saradnje s nacionalnim CERT-ovima u zemljama regiona i Evropske unije, ali i sa svim vladinim i nevladinim organizacijama u BiH koje su zainteresirane za pružanje informacija o cyber prijetnjama, što bi upravo bio zadatak nacionalnog CERT tima, koji ne postoji u BiH. Osim toga, dodatni proces uključuje i testiranje sistema i korisnika, kao i različite oblike obuka, kako bi se istakla važnost prevencije i odbrane od cyber napada..

2.

Odricanje od odgovornosti

Centar za izvrsnost u cyber sigurnosti (u daljnjem tekstu **CSEC**) osnovan je kao dio Udruženja Centar za istraživanje politike suprotstavljanja kriminalitetu (CPRC) radi jačanja cyber sigurnosti u Bosni i Hercegovini (BiH), uz podršku Vlade Ujedinjenog Kraljevstva. Kao dio CSEC-a, uspostavljen je akademski i održiv tim za odgovor na incidente u cyber sigurnosti (CERT).

CSEC ne garantira 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.

Prikazani podaci odnose se na jednu tačku, odnosno jednu IP adresu i mrežu *honeypot*[1] servera u svijetu, dok ukupan broj servera i njihova distribucija ostaju nepoznati. Podaci ne pokazuju broj uspješno izvedenih cyber napada s posljedicama po žrtve, ali pokazuju pojave u cyber prostoru kako bi pomogli podići svijest svih korisnika o opasnostima koje svakodnevno vrebaju na internetu.

Cilj predstavljanja ovih podataka ni na koji način nije stvaranje loše slike o BiH, jer se identične svakodnevne pojave dešavaju u svim dijelovima svijeta gdje postoji internet. U većini slučajeva radi se o automatiziranim skriptama koje skeniraju mrežu u potrazi za žrtvama protiv kojih je "vrijedno" poduzeti korake kako bi kompromitirali svoje sisteme i podatke.

Balkanska istraživačka mreža Bosne i Hercegovine (**BIRN BiH**) obradila je podatke dobijene od CSEC-a u ovom izvještaju i stavila ih u kontekst prvog izvještaja iz marta 2023. godine, ranijih studija BIRN-a BiH i drugih javno dostupnih podataka.

Cijeli izvještaj je namijenjen za javno objavljivanje, pa ga svako može koristiti i pozivati se na njega, ali isključivo u izvornom obliku, bez ikakvih izmjena i uz obavezno navođenje izvora informacija. Upotreba ovog dokumenta suprotno ovim odredbama podrazumijeva povredu autorskih prava.

CSEC i BIRN BiH će jednom godišnje objavljivati izvještaj o prijetnjama cyber sigurnosti. Izvještaj će nastojati da sistematski i kontinuirano prikazuje ranjivosti u domenu kibernetičke sigurnosti BiH, kao i rizike od oštećenja ključne infrastrukture. Kako su edukacija i podizanje svijesti ključni fokus i **CSEC-a i BIRN-a BiH**, ovaj izvještaj će služiti i u obrazovne svrhe i bit će distribuiran civilnom društvu u BiH.

---

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

3.

Sažetak glavnih nalaza u izvještaju

Nedavna otkrića strane kompanije za cyber sigurnost približila su nas otkrivanju osobe odgovorne za prošlogodišnji napad na internet stranicu Parlamentarne skupštine BiH. Ove godine, najčešći cyber napadi u zemlji bili su oni usmjereni na privatne kompanije, kojima to povećava troškove. Žrtve su sve više frustrirane zbog sporog odgovora institucija za provođenje zakona, što ih ostavlja nezaštićenima i ranjivim, a istovremeno utječe na njihove prihode, odnosno dovodi do finansijskih gubitaka. Jedan napad na medij ostavio je njihove čitaoce bez pouzdanog izvora vijesti, dok je drugi *ransomware* napad, koji se koristi za iznude, na veliku gasnu kompaniju kompromitirao podatke kupaca na početku sezone grijanja. Ovi incidenti naglašavaju sistemske greške u zakonodavstvu i raspodjeli resursa.

Spora reakcija organa za provođenje zakona rezultira gubitkom važnih podataka o napadu, što otežava identifikaciju krivca i prikupljanje dokaza. Dok su napadi distribuiranog uskraćivanja usluge (DDoS) smanjeni, mediji su i dalje glavne mete i ovakvi napadi ometaju pristup javnosti novim informacijama koje mogu biti ključne u vremenima krize.

Tokom izvještajnog perioda, CSEC je otkrio 15,4 miliona prijetnji cyber sigurnosti u BiH kroz svoj *DecoyNET Honeypot* sistem. Ove alarmantne brojke, zajedno s najnovijim izvještajima Ureda za reviziju institucija BiH, koji ukazuju na nepostojanje strateškog i pravnog okvira za cyber sigurnost, ilustriraju ranjivost bh. građana, kompanija i institucija na cyber napade koji bi mogli ugroziti ključne sektore. Od objavljivanja posljednjeg izvještaja u martu 2023. godine, ostvaren je samo neznatan napredak u stvaranju sigurnijeg cyber okruženja u BiH.

Razmjera cyber prijetnji	Izvještaj otkriva porast broja cyber napada od 72 posto, na mjesečnom nivou, u odnosu na prethodni period.
Vrste napada	Najviše je bilo napada na infrastrukturu Private Branch Exchange (PBX), s više od 1,7 miliona zabilježenih incidenata. Ovi napadi su također poznati kao "prevara putem telefona". Ovo naglašava potrebu za daljnjim istraživanjem ekonomskog utjecaja takvih napada na mreže i svakodnevne operacije, kao i druge prateće troškove u BiH.
Najveći incidenti	– Medijske organizacije su pretrpjele višestruke DDoS napade i izvijestile su o sporim odgovorima organa za sprovođenje zakona. – Najistaknutija sarajevska gasna kompanija pretrpjela je Ransomware napad, s kojim se borila kroz interne resurse. – Haker iz Banje Luke uhapšen je pod sumnjom da je izvršio cyber napad, zloupotrebu podataka i iznudu.
Distribucija napada po zemljama	Za razliku od prethodnog izvještaja, izvori napada usmjereni na mete u BiH promijenili su se – s Francuskom, SAD-om, Rusijom, Bugarskom i Estonijom kao najčešćim izvorima napada. Ova promjena podržava teoriju da napadači najčešće koriste Virtualne privatne mreže (VPN) da prikriju svoje podatke, zbog čega je znatno teže otkriti stvarni izvor napada.
Vladine mjere	BiH ostaje jedina zemlja na Zapadnom Balkanu bez Tima za odgovor na cyber incidente (CERT) i jasnog pravnog i strateškog okvira za cyber sigurnost. Iako je došlo do ograničenog napretka u radu vlasti, našoj državi još uvijek nedostaje sveobuhvatno rješenje problema. Rješenja koja se sada predlažu, ukoliko budu usvojena, poboljšala bi sposobnost BiH da zaštiti institucije vlasti, sarađuje s međunarodnim organizacijama i poboljša odgovore na prijetnje.

4.

Izvještaj o cyber prijetnjama

Za opći pregled cyber sigurnosnih prijetnji u Bosni i Hercegovini, od januara do augusta 2023. godine, CSEC i BIRN BiH su pregledali i analizirali podatke o prijetnjama prikupljene putem nekoliko servera i uređaja dizajniranih za ovu svrhu. Ovi uređaji, poznatiji kao *honeypot* ili mamci, zapravo su specijalizirani uređaji za prikupljanje informacija iz različitih međunarodnih izvora, ali i uređaji koji su integrirani u samu CSEC infrastrukturu. Svi oni služe za privlačenje potencijalnih napadača i vrijedan su obrazovni alat.

BIRN BiH je, uz podatke CSEC-a, u ovaj izvještaj uključio i vlastite analize i istraživanja iz prethodnog perioda posvećene izvještavanju o prijetnjama cyber sigurnosti u BiH.[2]

Kako bi se zaštitili od ovih prijetnji, CSEC preporučuje organizacijama, institucijama, kompanijama i pojedincima da ispitaju svoje sisteme i koriste indikatore kompromisa za otkrivanje zlonamjernih aktivnosti.

4.1. Sistem prikupljanja podataka

Podaci prikazani u ovom izvještaju prikupljeni su putem ***Tpot servera i DecoyNet Honeypot*** uređaja, odnosno *honeypot* servera i uređaja instaliranih u samoj CSEC infrastrukturi.

Novi izvori podataka koji se koriste za različite analize u ovom izvještaju jesu ***OpenCTI*** i ***Shadowserver***. O njima ćemo više govoriti u narednim poglavljima.

Honeypot predstavlja mehanizam cyber sigurnosti koji koristi "namjerno proizvedenu" metu napada, da cyber kriminalcima skrene pažnju s legitimnih meta. Ovaj uređaj se može modelirati na bilo kojoj digitalnoj imovini, od softverskih aplikacija, servera, do cijele mreže. Namjerno je dizajniran da izgleda kao stvarna meta. Na ovaj način, napadači se uvjeravaju da su pristupili meti, kako bismo ih ohrabrili da provode što više vremena u tom kontroliranom okruženju.

U suštini, *honeypot* predstavlja mamac, ali može poslužiti i kao alat za učenje, koristeći pokušaje napada za procjenu napadačeve tehnike, sposobnosti i sofisticiranosti. *Honeypot* može imitirati stvarne uređaje kao što su mobilni telefoni, serveri ili mrežni sistemi, kako bi otkrio na koji način su oni ugroženi.

2 Ovaj izvještaj uključuje taktike, tehnike i procedure (TTP) te indikatore kompromisa (IOC) povezane sa zlonamjernim aktivnostima.

Obavještajni podaci prikupljeni pomoću *honeypot* uređaja mogu pomoći organizacijama da poboljšaju svoje strategije cyber sigurnosti kao odgovor na prijetnje u stvarnom svijetu i realnom vremenu, identificirajući potencijalne "slijepe tačke" u postojećoj strukturi, kao i sigurnost informacija i mreže.

STRUKTURA MAMACA

- **Tpot (Tpotce)** se sastoji od 23 različita *honeypot* servera, od kojih svaki imitira jedan ili više poznatih i najčešće eksploatiranih servisa, protokola, aplikacija i drugog.
- **DecoyNET Honeypot** je dizajniran za stvaranje mreže uređaja postavljenih u mreži klijenta kako bi se otkrili pokušaji cyber napada prije nego što napadač uspije u potpunosti kompromitirati sistem. To zapravo predstavlja mamac koji koristi 16 servisa koji su najčešće napadnuti ili ciljani pokušajima kompromitiranja.
- **OpenCTI** je platforma otvorenog koda dizajnirana za upravljanje i analizu obavještajnih podataka o cyber prijetnjama. Primarni cilj OpenCTI-a je da nam omogući bolje razumijevanje lepeze cyber prijetnji i razmjenu znanja o cyber prijetnjama.
- **Fondacija Shadowserver**, od svog osnivanja 2004. godine, postala je jedan od vodećih svjetskih resursa za izvještavanje o internet sigurnosti i istraživanje zlonamjernih aktivnosti. Fondacija zapošljava tim s punim radnim vremenom i održava globalnu infrastrukturu koja obuhvata 80 zemalja. **CSEC** je ponosni član ove fondacije od marta 2023. i pruža senzorske podatke iz svoje infrastrukture od juna ove godine.

4.2. Najvažniji događaji od januara do augusta

Tokom posmatranog perioda, dokumentirali smo nekoliko incidenata koji nisu potekli direktno iz mreže uređaja putem kojih CSEC prikuplja podatke, već su isplivali na površinu razmjenom informacija. Ovo ilustrira ključnu ulogu razmjene informacija u zaštiti cyber sigurnosti, činjenicu koju stručnjaci naširoko naglašavaju. U narednom periodu, institucije i drugi sudionici u BiH trebaju aktivno raditi na poboljšanju razmjene podataka.

Ovi slučajevi otkrivaju brojne probleme, kao što su spore reakcije policije, uzrokovane nedostatkom strateških rješenja. Policijske agencije često nemaju dovoljno resursa ili sposobnosti za obavljanje ove funkcije i to je razlog zašto je potrebna specijalizirana institucija kojoj bi napadnuti subjekti mogli prijaviti ovakve incidente.

4.2.1. Napadi na medije i javne ličnosti

U aprilu 2023. *Nezavisne novine*, dnevni list u Banjoj Luci, izvijestile su o cyber napadu na svoju internet stranicu, koji je ozbiljno ograničio pristup njihovim čitaocima. Prema informacijama prikupljenim za ovaj izvještaj, ovi napadi su trajali skoro deset uzastopnih dana, a bili su praćeni svakodnevnim napadima različitih razmjera.

Sandra Gojković-Arbutina, glavna urednica *Nezavisnih novina*, vjeruje da je napad bio ciljan: "S obzirom na intenzitet i upornost, čini mi se da nismo slučajno izabrani i da nismo bili slučajni uzorak za napad, već, čini mi se, da se radi o ciljanom napadu, sa specifičnom namjerom da se sruše *Nezavisne*. Uprava i ja odbacili smo mogućnost da je to bila slučajnost."

Iako su *Nezavisne* prijavile napad policiji, do trenutka pisanja ovog izvještaja nisu dobili nikakvu povratnu informaciju o izvoru napada. Ova medijska kuća je još 2019. godine podnijela prijavu policiji o sličnim incidentima, ali nije dobila bilo kakve rezultate policijske istrage. Ovaj put su sami dokumentirali značajne detalje napada koji su ukazivali da se radi o upornom napadu distribuiranog uskraćivanja usluge (DDoS) na njihove usluge. Podatke su podijelili za ovaj izvještaj.

Milioni pokušaja za pristup naslovnici njihove web stranice poticali su s različitih lokacija širom svijeta. IT odjel ovih novina sumnja da je riječ o istom napadaču koji koristi različite usluge kako bi prikrio svoju pravu lokaciju i izveo napade. Oni također vjeruju da bi to mogao biti dio specifične kampanje.

"Kada padnemo, kada nismo dostupni, kada je *Nezavisnim* teško pristupiti, kada vam treba nekoliko sekundi da otvorite link, svake sekunde gubimo čitatelje. Za medije, posebno komercijalne, koji nisu finansirani od strane države, ova vrsta napada dovodi do direktne finansijske ugroženosti", napomenula je Gojković-Arbutina.

Drugi mediji, uključujući *Buku* i televizije *BN* i *Face*, također su se suočili sa cyber napadima u aprilu. Iz *Face TV-a* su za **Detektor** potvrdili da su zabilježili do 300 miliona pokušaja pristupa njihovoj stranici u jednom danu. Smatraju da takav napad podriva povjerenje među njihovim gledateljima i pripisuju ga njihovom izvještavanju o političkim promjenama.

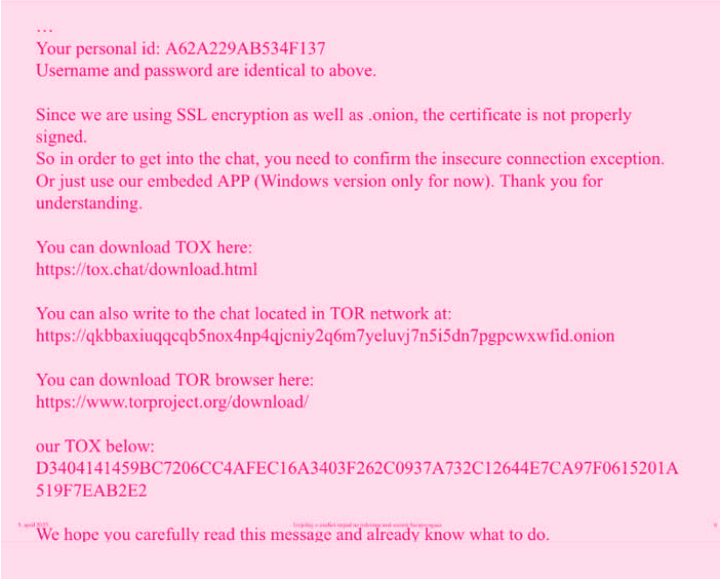
Osim medija, na meti cyber napada našle su se i javne ličnosti. *Nezavisne* su u julu objavile da je haker iz Banje Luke uhapšen zbog sumnje da je izvršio cyber napad na istaknutu advokaticu u Sarajevu. Napadač je ukrao podatke o slučajevima u kojima je advokatica učestvovala, te slao lažne poruke u njeno ime u pokušaju da počini iznudu.

Ovo hapšenje BIRN-u BiH potvrdilo je Ministarstvo unutrašnjih poslova Republike Srpske. Naveli su da je osoba povezana s nekoliko krivičnih djela, uključujući *ransomware* napade, neovlašteni pristup zaštićenim računarima i mrežama, telekomunikacionim mrežama, elektronsku obradu podataka i kompjuterske prevare.

4.2.2. Studija slučaja: "Sarajevogas"

Nakon niza *ransomware* napada koji nisu objavljeni u javnosti, Kantonalno javno komunalno preduzeće "Sarajevogas" pružilo je pozitivan primjer tako što su javno obznanili značajan *ransomware* napad na svoju mrežu, koji se dogodio krajem augusta 2022. godine.

Ishak Alajbegović, glavni inženjer infrastrukture u kompaniji, objašnjava da su u jednoj noći izgubili pristup svim podacima.


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

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

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

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

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

our TOX below:
D3404141459BC7206CC4AFEC16A3403F262C0937A732C12644E7CA97F0615201A519F7EAB2E2

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

"Sve je šifrovano", naveo je on i dodao da je cijela mreža ugrožena, uključujući 40 do 50 virtualnih mašina koje sadrže baze podataka korisnika i druge kritične podatke.

Napadači, koji su se predstavili kao "Donut Leaks", poslali su poruku "Sarajevogasu" u kojoj traže da instaliraju poseban softver za daljnju komunikaciju.

Rukovodstvo "Sarajevogasa" kao javne kompanije odlučilo je incident prijaviti policiji. Bili su iznenađeni dugotrajnom procedurom prijave, zbog koje su čekali nekoliko dana da u potpunosti vrate operativnost svog sistema. Sve vrijeme dok su čekali, morali su da rade u pomoćnom odnosno improviziranom okruženju. Srećom, njihova ranija priprema za potencijalne cyber napade pomogla im je da se oporave, jer su ranije uveli sigurnosne kopije podataka sa četiri nivoa. Ovaj postupak omogućio im je da obnove sve podatke sačuvane prije napada.

"Radili smo u okruženju za podršku, ali nismo mogli čekati jer su svi stajali zbog napada. Ekipe na terenu su čekale, a zbog situacije, bez posla je bilo 300 ljudi. Trebalo mi je desetak sati da prođem čitavu proceduru rješavanja problema, a već sutradan smo imali sve u funkciji i sve što je bilo potrebno za normalan rad", prisjetio se Alajbegović.

Nakon deset dana bez ikakvog odgovora policije, pojasnio je Alajbegović, kompanija je morala donijeti pragmatičnu odluku. Napravili su dokument u kome su naveli da su sačuvali dio dokaza, kao i da nisu imali izbora osim da izbrišu sve druge kompromitirane podatke, kako bi ponovo pokrenuli sistem. Tada su se oslonili na vlastite resurse i podatke koji su ostali nešifrirani u sigurnosnim kopijama, vraćajući na kraju sve bitne procese kompanije u operativno stanje.

Alajbegović ovaj napad smatra vrijednim iskustvom učenja, uprkos izazovima. To im je, kaže, omogućilo da testiraju efikasnost sigurnosnih mjera koje su uspostavili, ali i vlastitu spremnost za suprotstavljanje cyber napadima. Osim toga, napad im je pomogao da identificiraju i nedostatke i dijelove sistema kojima je potrebna dodatna pažnja, u odbrani od cyber napada. Zbog potencijalnih novih napada, nisu za ovaj izvještaj mogli otkriti detalje o tome kako su poboljšali sistem zaštite.

Uz ovo iskustvo, Alajbegović ističe da mnoge kompanije, u javnom i u privatnom sektoru, ne shvataju u potpunosti razmjere prijetnji s kojima se suočavaju, pa tako često i ne ulažu dovoljno u resurse za zaštitu.

"Kasnije, istražujući ovaj napad, saznali smo da je taj isti haker napao i gasnu kompaniju u Grčkoj, samo sedam ili osam dana prije nego što je napao našu. U našem slučaju, vjerovatno su

ušli zbog eksterne kompanije u sistemu, koja je implementirala određena softverska rješenja i stvorila prostor za napad", zaključuje Alajbegović.

Iskustvo ove kompanije relevantno je za sva preduzeća u BiH, posebno za komunalna, zbog čega bi se svi oni trebali pripremiti za napade. Ovaj primjer dodatno naglašava nedostatke unutar sistema, posebno policijskih struktura, kojima nedostaju odgovarajući resursi, obuke, alati i znanje za rješavanje takvih napada, što bi u budućnosti trebao biti jedan od važnijih fokusa za vlasti.

4.2.3. Male zajednice nepripremljene za cyber napade

Cilj ovog izvještaja je i procijeniti odgovore lokalnih vlasti na cyber prijetnje.

Adnan Bjelić, gradonačelnik Srebrenika, kaže da, do sada, u njegovoj lokalnoj zajednici nije bilo zabilježenih cyber napada. Međutim, dodaje kako se takvi problemi mogu pojaviti u budućnosti, kada sve organizacije, pa i one u javnom sektoru, završe proces digitalizacije. Dodaje i da su lokalne zajednice svjesne ovih prijetnji, ali smatra da odgovor treba doći s viših nivoa vlasti, kako bi se donijele odgovarajuće zakonske i strateške mjere i podržale lokalne zajednice.

"Ako lokalne zajednice budu prepuštene same sebi u smislu cyber sigurnosti, mislim da će biti teško. Nemamo ni kadrovsku ni tehničku obuku. Bojim se da nam treba mnogo više pomoći organa vlasti na višim nivoima nego što to možemo i pomisliti", precizira Bjelić.

Srebrenik trenutno radi na digitalizaciji određenih procesa. Bjelić tvrdi da izostanak zabilježenih cyber prijetnji zasad može pripisati njihovom ograničenom prisustvu na digitalnim platformama, ali da se nove opasnosti pojavljuju svaki dan.

"Uz modernizaciju, alati koji osiguravaju sigurnost moraju pratiti ovaj angažman. Dok ne bude uspostavljena sigurnost u elektronskoj industriji, lokalnim zajednicima i svim drugim nivoima, bit će teško da iskoriste sve prednosti te industrije", ističe.

Iako je Grad Srebrenik uspostavio određene zaštitne sisteme, svjesni su kako je neophodno dodatno ojačati kapacitete ovih zaštitnih mjera. Bjelić ističe i potrebu za boljom obukom, kako sami javni funkcioneri ne bi ugrozili gradski sistem administracije. Dodaje da prijetnje koje se u početku čine benignim, imaju mogućnost nanijeti značajnu štetu cijelom sistemu.

Ovo iskustvo i drugi podaci iz izvještaja dovode do zaključka da je u narednom periodu potrebno usvojiti pravni i strateški okvir cyber sigurnosti u BiH, u koji bi bili uključeni različiti modeli rješavanja problema lokalnih zajednica.

4.3. Distribucija napada u BiH

U promatranom periodu CSEC je dokumentirao niz cyber sigurnosnih incidenata, na dva namjenska uređaja koji su zapravo mamci za napadače. Jedan od ovih uređaja, Tpot server,

dio je Deutsche Telecom Security mreže Tpot servera, čiji zbirni podaci svakog sata otkrivaju milione napada širom svijeta.

Kada obim napada zabilježenih putem ovog uređaja, tokom ovog izvještajnog perioda, uporedimo s podacima prikazanim u prvom izvještaju o cyber prijetnjama, vidljiv je značajan pad broja napada.

Među Tpot serverima su oni koji otkrivaju pokušaje napada na *Android* uređaje, napade na industrijske kontrolne protokole i *brute force* napade, DDos napade, pokušaje kompromitiranja različitih servera i servisa, kao i one koji prate podatke za prijavu prilikom pokušaja napada na određene servise, te detektor za prevare putem telefonskih poziva, simulator štampača i e-mail servisa.

Svi ovi dijelovi uređaja pomažu u snimanju što većeg broja i vrste napada širom svijeta. U konkretnom slučaju CSEC-a, ovaj Tpot server, koji se koristi za prikupljanje podataka, dio je mreže Tpot servera Deutsche Telekom Securityja, čiji podaci pokazuju da se u prosjeku u svijetu događa sljedeće:

- 35.000 – 65.000 napada u minuti;
- 1,5 – 3 miliona napada na sat;
- 35 – 55 miliona napada u 24 sata.

Upoređujući broj napada zabilježenih tokom posmatranog perioda putem Tpot uređaja s podacima iz prvog izvještaja o prijetnjama po cyber bezbjednost, vidimo značajno smanjenje broja napada. Tačnije, broj je smanjen za skoro 50.000 napada u minuti, u prosjeku. Od oktobra do decembra 2022. godine broj napada je bio:

- 65.000 – 115.000 napada u minuti;
- 3 – 4,5 miliona napada na sat;
- 55 – 80 miliona napada u 24 sata.

No, važno je napomenuti da ovi podaci nisu ni potpuni ni zbirni, već predstavljaju samo presjek s postojećih Tpot servera širom svijeta, dok se stvarni broj napada mijenja iz minute u minutu i vjerovatno je višestruko veći.

4.4. Cyber napadi otkriveni kroz Tpot uređaj

Broj cyber napada u BiH koji se bilježe putem ovog servisa stalno se mijenja, što dodatno naglašava važnost stalnog praćenja, registracije i efikasne obrade podataka iz cyber sigurnosnog okruženja u našoj zemlji.[3]

3 U posljednjih 30 dana posmatranog perioda, dokumentirano je 2.315.855 napada, od kojih je većina bila usmjerena na privatnu telefonsku (PBX) infrastrukturu, njih 1.769.658. Slijede napadi na FTP servere, kao i na MSSQL i MySQL/MariaDb bazu podataka u ukupnom iznosu od 281.267.

Najznačajniji pad zabilježen je kod DDoS napada, koji uključuju mnoštvo uređaja koji "bombardiraju" jednu internet stranicu zahtjevima za pristup, preplavljuju njen server i uzrokuju rušenje. U prosjeku mjesečno bilježimo tri do četiri miliona takvih napada.

U augustu 2023. godine, ovi uređaji su zabilježili 16.802 DDoS napada, što je 80 posto manje u odnosu na prethodni period. Međutim, to ne znači da će DDoS napadi prestati. Umjesto toga, trebali bi da služe kao podsjetnik na potrebu da ostanete na oprezu, jer će nove DDoS kampanje vjerovatno ponovo dostići tri do četiri miliona mjesečnih napada u kratkom vremenskom periodu. Isto važi i za sve vrste cyber napada, za koje također očekujemo da ćemo do kraja godine imati prosječan porast.[4]

Najznačajniji pad broja napada zabilježen u ovom izvještaju odnosi se na pokušaje napadača da kompromitiraju uređaje koji koriste *Android* operativni sistem. U prethodnom izvještaju, unutar mjesec dana bilo je 478 takvih napada. Međutim, trenutni izvještaj otkriva ukupno 538 takvih napada tokom izvještajnog perioda, što pokazuje da nisu ugroženi samo tradicionalni računari, nego i uređaji koji koriste i neke drugačije operativne sisteme.

Iz dostavljenih podataka vidljivo je drastično smanjenje pokušaja napada od juna do augusta 2023. godine, u odnosu na prvih pet mjeseci praćenog perioda, gdje je prosječan broj napada za 30 dana iznosio između sedam i osam miliona pokušaja. Isto vrijedi i za prethodni izvještaj, gdje su podaci u podudarnosti s podacima za period januar – maj 2023.

4.4.1. Napadi prema zemlji porijekla

U promatranom periodu, tim CSEC-a identificirao je Francusku kao novu zemlju koja je postala primarni izvor cyber napada unutar BiH. Nju na ovoj listi slijede SAD, Rusija, Bugarska, Estonija, Vijetnam, Belgija i Njemačka. Posljednje dvije zemlje na listi onih iz kojih su najčešće stizali napadi na mete u BiH jesu Indonezija i Kina.

Preliminarni podaci iz CSEC-a sugeriraju da je značajan udio napada prijeklom iz Francuske i SAD-a. Međutim, ovo je vjerovatno rezultat činjenice da napadači koriste VPN servise kako bi prikrili svoje stvarne lokacije.

U odnosu na prvi izvještaj o cyber prijetnjama u BiH, zemlje iz kojih su napadi najčešće stizali sada su se promijenile. Sada bilježimo nove izvore napada, u zemljama kao što su Francuska, Bugarska, Estonija, Belgija i Indonezija. S druge strane, Brazil, Holandija, Bangladeš, Kostarika i Indija su nestale sa ove liste. Ova pomjeranja ne znače nužno da sada cyber prijetnje potiču od napadača koji su drugačiji od onih iz prvog izvještaja, nego bi takvi podaci mogli ukazivati na to da su napadači, osim metodologije samih napada, promijenili i geografsko porijeklo napada. Ovo može biti i odbrambeni mehanizam, u kojem napadači koriste VPN usluge da prikriju fizičke lokacije.

4 Preostali napadi su bili:
- Pokušaji kontrole računara ili eksploatacije e-mail protokola i Postgres baze podataka – 121.700 napada;
- Pokušaji kompromitovanja Cisco uređaja – 80.301;
- Pokušaji eksploatacije Redis cache servera – 11.481;

Kroz mnoge od ovih napada moguće je primijetiti metode i sposobnosti koje su u skladu s taktikama povezanim s Rusijom i Kinom. To je i u skladu s globalnim iskustvima i podacima, koji sugeriraju da su ove dvije zemlje glavni izvori cyber napada. U svom najnovijem "Izvještaju o digitalnoj odbrani", kompanija Microsoft navodi da napadači koji su povezani s određenim državama, pokreću sve sofisticiranije cyber napade, dizajnirane da izbjegnu otkrivanje i unaprijede strateške ciljeve. Za primjer ističu upotrebu cyber oružja Rusije u sukobu u Ukrajini, uključujući širenje propagande kako bi se utjecalo ne samo na mišljenja građana Ukrajine nego i onih u drugim zemljama.

U ovom izvještaju se navodi: "Izvan Ukrajine, akteri nacionalnih država povećali su aktivnost i počeli su da koriste napredak u automatizaciji, cloud infrastrukturi i tehnologijama za daljinski pristup, kako bi napali širi skup ciljeva."

Izvještaj naglašava da su mjere cyber sigurnosti postale još važnije, jer napadači veoma brzo iskorištavaju ranjivosti, koriste sofisticirane tehnike, ali i primitivnije, nasilne metode, dok prikrivaju svoje operacije putem otvorenog koda ili legitimnog softvera.

Kako su ovi obrasci primijećeni u cijelom svijetu, možemo pretpostaviti da i BiH prati svjetske trendove. Ako postoji veliki broj napada s porijeklom u Francuskoj ili SAD-u, zajedno s manjim obimom napada iz Rusije ili Kine, logično je zaključiti da stvarni napadači manipuliraju svojim IP adresama kako bi prikrili svoje prave lokacije.

COMMONLY USED IP ADRESSES FOR ATTACKS TOWARDS TARGETS IN BiH

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

Važnost praćenja ovakvih slučajeva pokazana je i nedavnom odlukom glavnog tužioca Međunarodnog krivičnog suda u Haagu, kojom je odlučeno da će ovaj sud biti posvećen i istraživanju i procesuiranju cyber kriminala, koji krši postojeće međunarodne zakone, kao što to rade za slučajeve ratnih zločina, o čemu je nedavno izvijestio Wired.

4.4.2. Napadi na PBX infrastrukturu

Za kompanije koje zavise od komunikacije s klijentima ili drugim kompanijama putem interneta, bilo kakvo ugrožavanje njihove internet stranice ili njena nedostupnost može stvoriti značajne troškove i ometanje njihovog rada. Za različite korisnike, cyber napadi mogu dovesti do uskraćivanja pristupa različitim važnim zdravstvenim podacima, ometanja putovanja, pa čak i ometanja aplikacija za mobilno bankarstvo koje su u širokoj upotrebi.

Najčešći cyber napadi koje smo dokumentirali od januara do augusta 2023. godine ciljali su PBX sisteme, odnosno privatne telefonske mreže, koje su veoma važne za interno poslovanje kompanija. Ovi napadi nameću nepredviđeni teret kompanijama.

Naprimjer, napadači mogu iskoristiti mrežu kompanije da upućuju skupe pozive, uzrokujući im tako znatne telefonske troškove. U studiji iz 2021. godine ovi globalni troškovi premašili su 1,2 milijarde dolara. Osim toga, ovi napadi mogu poremetiti internu komunikaciju i u potpunosti ometati poslovanje.

U BiH smo zabilježili 1,7 miliona ovakvih napada samo u posljednjih 30 dana izvještajnog perioda. Iako je riječ o manjem broju nego u prethodnom periodu, napadi na PBX infrastrukturu su najčešće izvedeni u cijeloj zemlji. Zbog toga ovaj dio izvještaja služi kao upozorenje za preduzeća i organizacije koje održavaju komunikacijske mreže.

S obzirom na postojeće ranjivosti u BiH, gotovo je sigurno da brojna preduzeća snose troškove zbog PBX napada. Ovi podaci naglašavaju potrebu za daljnjim istraživanjem ekonomskog utjecaja ovakvih napada na komunikacijske mreže i svakodnevne poslove kompanija, kao i troškove povezane s njima u našoj zemlji.

Globalno gledano, PBX napadi su među vodećim metodama za probijanje mreža. Prema istraživanju Udruženja za kontrolu komunikacijskih prevara (CFCA), ovi napadi su bili među prvih pet vrsta prevara između 2013. i 2017. godine. Osim direktnog porasta troškova zbog neovlaštenog korištenja telefonske mreže, napadači mogu dobiti i evidenciju o pozivima korisnika, što dovodi do kršenja privatnosti i potencijalnog gubitka povjerljivih podataka.

Kao rezultat, kompanije mogu dobiti nove troškove oporavka sistema i popravke ugroženih dijelova mreže.

Drugi aspekt ovih napada je mogućnost prisluškivanja internih komunikacija, čime se omogućava korporativna špijunaža. Procjena je da tokom takvih napada nastaje ogromna šteta, kao i da takvi napadi mogu potrajati duži vremenski period.

Praćenje ovih napada dodatno je kompliciranо jer napadači mogu prikriti digitalne tragove kroz takozvanu "PBX looping" tehniku, u kojoj jednu mrežu koriste za upućivanje poziva preko druge mreže.

4.5. Cyber napadi u BiH otkriveni putem DecoyNET Honeypot uređaja

Uz znatno veći Tpot uređaj, CSEC podatke o cyber sigurnosnim prijetnjama u BiH prikuplja i kroz vlastiti DecoyNET sistem. DecoyNET se sastoji od šest uređaja, čija je glavna svrha otkrivanje cyber napada prije nego što napadači budu u mogućnosti ugroziti cijeli sistem. Iako ima mnogo uži domet od Tpot servera, ovaj sistem veoma je koristan za izradu izvještaja u kojima je moguće porediti različite metode i taktike.

U ovom izvještajnom periodu, kroz DecoyNET Honeypot uređaj zabilježeno je ukupno 15.478.783 napada, među kojima je najviše bilo zabilježeno pokušaja pristupa MSSQL bazama podataka, njih ukupno 9.908.666.[5]

U prvom izvještaju o cyber prijetnjama iz marta 2023. godine, ukupan broj zabilježenih napada je bio 520.717 za mjesec dana, dok sada vidimo povećanje od skoro dva miliona napada na mjesečnom nivou. Ovo pokazuje da je interesovanje napadača sve veće. Ali to može biti iz različitih razloga, poput činjenice da napadači testiraju različite taktike kako bi razvili sopstvene sisteme napada i prodrli u ciljane sisteme, ali i da je došlo do globalnog povećanja cyber incidenata.

4.6. Cyber napadi otkriveni putem OpenCTI-a

Za razliku od prvog izvještaja, CSEC je također pronašao neke nove načine za prikupljanje informacija o cyber incidentima. Prva metoda je prikupljanje podataka kroz OpenCTI, platformu otvorenog koda dizajniranu za upravljanje i analizu obavještajnih podataka o cyber prijetnjama. Primarni cilj OpenCTI-a je da omogući bolje razumijevanje pejzaža cyber prijetnji i razmjenu znanja o cyber prijetnjama.

5 Osim pokušaja pristupa MSSQL bazama, kroz uređaj su zabilježeni i sljedeći napadi:
- 4.697.318 pokušaja dobijanja daljinskog pristupa računarskim sistemima (VNC);
- 735.705 pokušaja neovlaštenog pristupa MySQL bazama podataka;
- 82.286 pokušaja kompromitovanja protokola za razmjenu podataka (FTP, SMB, SIP, HTTP, HTTPS);
- 77.190 pokušaja neovlaštenog pristupa Redis bazama podataka;
- 9.815 pokušaja kompromitovanja NTP i SNMP protokola za sinhronizaciju vremena na računarima;
- 538 pokušaja kompromitovanja Android uređaja.

4.6.1. Podaci o Bosni i Hercegovini u OpenCTI-u

Bosna i Hercegovina je trenutno, nažalost, navedena samo preko *Alienvault* podataka, o čemu se može pronaći nešto više informacija u nastavku ovog poglavlja. Vjerovatni razlog za malu količinu podataka dolazi iz činjenice da niko iz naše zemlje zvanično ne doprinosi međunarodnoj CERT zajednici, zbog nepostojanja nacionalnog CERT tima. Trenutno, samo CSEC zbraja podatke i priprema procedure za razmjenu podataka, s čime bi trebali početi tokom 2024. godine.

Prema podacima *Alienvaulta*, postoje samo tri izvještaja u vezi s Bosnom i Hercegovinom – dva iz 2020. i jedan iz ove godine – u kojima se ne navode dodatni detalji:

1. **FASTCash 2.0: Sjevernokorejski BeagleBoyz pljačka banke (26. august 2020)**
   Ovo zajedničko savjetovanje rezultat je analitičkih napora između Agencije za kibernetičku sigurnost i sigurnost infrastrukture (CISA), Odjela za trezor (Treasury), Federalnog istražnog biroa (FBI) i Cyber Commanda SAD-a (USCYBERCOM). U suradnji s partnerima iz vlasti SAD-a, CISA, Treasury, FBI i USCYBERCOM identificirali su zlonamjerni softver i indikatore kompromisa (IOC) koje je koristila Vlada Sjeverne Koreje u shemi isplate gotovine na automatiziranom bankomatu (ATM) – koju Vlada SAD-a naziva "FASTCash 2.0: Sjevernokorejski BeagleBoyz pljačka banke".

2. **Ruski APT28 koristi mamce COVID-19 za isporuku Zebrocyja (9. decembra 2020.)**
   U novembru 2020, Intezer je otkrio COVID-19 mamce za krađu identiteta koji su korišteni za isporuku Go verzije Zebrocy malwarea. Zebrocy se uglavnom koristi protiv vlada i komercijalnih organizacija koje se bave vanjskim poslovima. Mamci su se sastojali od dokumenata o Sinopharm International Corporation – farmaceutskoj kompaniji čija je vakcina protiv COVID-19, u trenutku detekcije napada, prolazila kroz fazu tri klinička ispitivanja – i lažno pismo o evakuaciji Generalnog direktorata za civilno zrakoplovstvo. Mamac je isporučen kao dio virtualnog tvrdog diska (VHD) koji zahtijeva od žrtava da koriste *Windows 10* za pristup datotekama.

3. **Dark Pink – Novi APT stiže u Aziju, Pacifik i Evropu (11. januara 2023)**
   Nova grupa naprednih aktera upornih prijetnji (APT) ciljat će na vladine i vojne institucije širom Azije i Evrope u narednih pet godina, prema istraživačima cyber sigurnosti Group-IB, koji su do sada otkrili sedam napada.

Ove informacije naglašavaju značajan nedostatak sveobuhvatnog doprinosa podacima iz BiH, posebno u dijelu o incidentima u sistemu, koji izgleda potpuno prazan. Štaviše, opće je poznato da je došlo do najmanje jednog cyber napada na parlament naše zemlje. Dodatno, primjetan je nedostatak smislenih veza između aktera u Bosni i Hercegovini u vezi sa identificiranim prijetnjama. Većinu *malwarea* otkrivenih u Bosni i Hercegovini koristilo je nekoliko APT grupa, neke od njih su APT28, poznati kao FancyBear ili Sofacy, Hidden Cobra ili Lazarus i Dark Pink. S obzirom na činjenicu da je trenutno mali broj dijeljenih informacija iz oblasti cyber sigurnosti, CSEC jedino može potvrditi da se podaci s njihovih mamaca podudaraju s trendovima iz svjetskih izvještaja.

Neki od zlonamjernih programa identificiranih u Bosni i Hercegovini koje koriste ove APT grupe jesu:

4.6.2. Dark Pink zlonamjerni softver

Dark Pink je naziv koji je Group-IB, u jednom od detaljnih izvještaja o novim cyber prijetnjama, dao novom talasu APT napada koji je pogodio APAC (Azijsko-pacifički) region. Group-IB nije mogao pripisati ovaj val napada niti jednom poznatom napadaču, što pokazuje da je Dark Pink vrlo vjerovatno potpuno nova grupa. Postoje dokazi da su se ovakve vrste napada pojavile sredinom 2021. godine, iako je aktivnost napadača porasla od sredine do kraja 2022. godine, a do sada je registrirano sedam poznatih napada koji su uključivali Dark Pink.

Nevjerovatan uspjeh Dark Pinka se uglavnom pripisuje spear-phishing[6] e-mailovima, koji se koriste za početni upad. Tipični napad uključivao je napadače koji su se maskirali u kandidate za posao i koristili fizički svijet da bi došli do podataka koje je moguće koristiti za napade, poput informacija sa oglasnih ploča u prostorijama kompanija. To im je poslužilo kako bi napisali što uvjerljivije *e-mailove* sa mamcima, takozvane phishing e-mailove.

Takvi e-mailovi sadrže link koji vodi na određeno mjesto na internetu, odakle žrtve nesvjesno preuzimaju specifične datoteke koje sadrže zlonamjerni softver neophodan za kompromitaciju mreže, odnosno za upad u samu mrežu.

Letter-of-Motivation	3/8/2022 4:09 PM	Microsoft Word 9...	954 KB
Letter-of-Motivation.doc	9/10/2021 9:54 AM	Application	1,878 KB

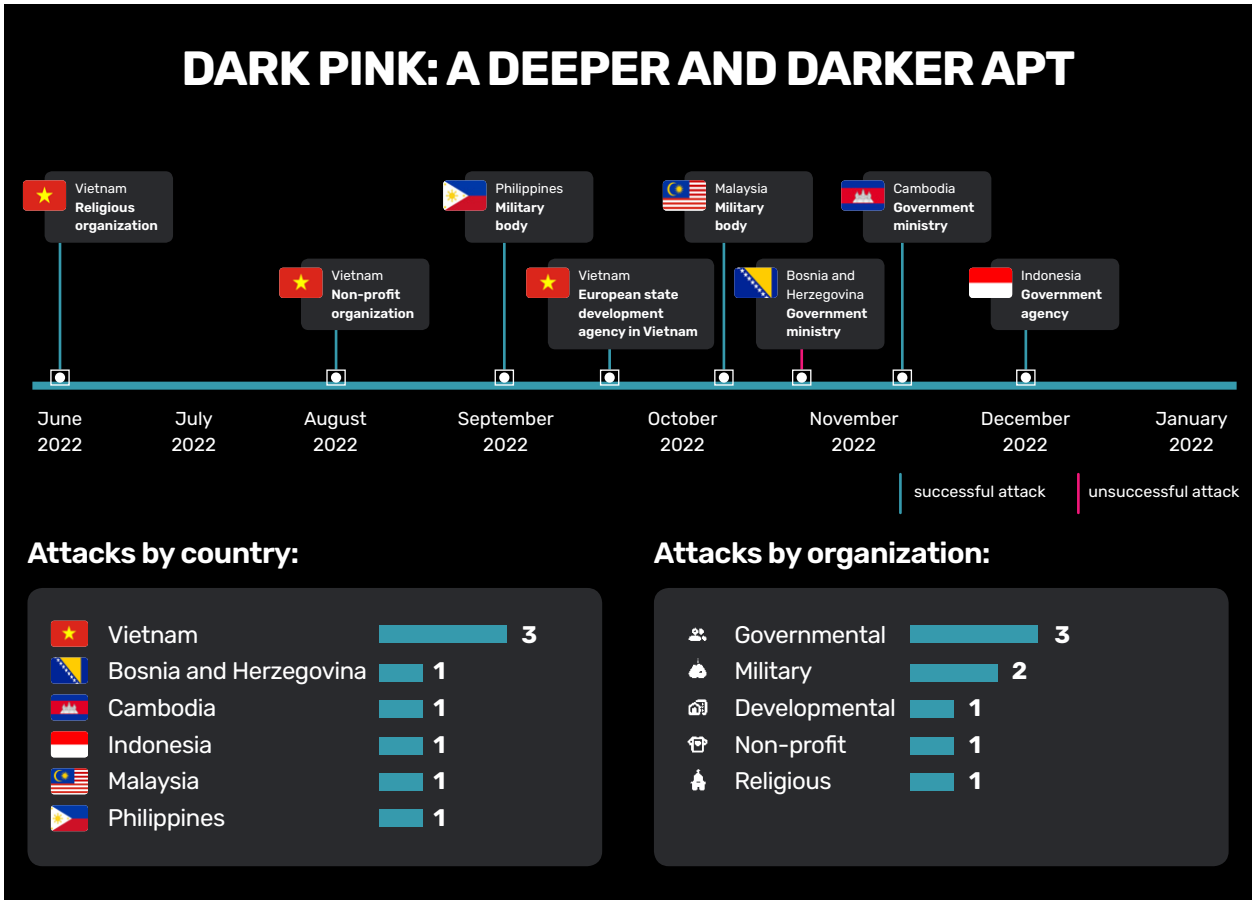
Kada se mreža infiltrira, cilj Dark Pinka je prikupljanje velikog broja informacija o mrežnoj infrastrukturi žrtve. Zlonamjerni softver traži detalje od standardnih uslužnih programa, internet pretraživača, instaliranog softvera uključujući antivirusna rješenja, kao i informacije o povezanim USB uređajima i dijeljenju mreže.

Nakon toga, svaki put kada se USB disk ubaci u zaraženi uređaj, pokreće se akcija preuzimanja TeleBotDroppera na disk. Proces počinje s pokretanjem WMI događaja, koji automatski preuzima .ZIP arhivu s Github naloga aktera prijetnji. Arhiva sadrži tri datoteke: Dism.exe, Dism.sys i Dismcore.dll, sa DLL datotekom koja ima zadatak da raspakira originalni izvršni fajl iz datoteke Dism.sys.

BIRN BiH je ranije izvještavao o tome kako već gotovo godinu dana nije poznato ko je izvršio cyber napad na Državni parlament i Vijeće ministara BiH. Jedine informacije koje su otkrile neke detalje bile su sadržane u odgovoru Ministarstva sigurnosti BiH državnim parlamentarcima u kome su naveli da je Tužilaštvo BiH formiralo predmet o napadu i da je pronađena e-mail adresa koja se dovodi u vezu s njim.

6 Prema pojašnjenju Ureda direktora nacionalne obavještajne službe SAD-a, spear phishing je vrsta phishing kampanje koja cilja određenu osobu ili grupu, i često uključuje informacije za koje se znalo da su od interesa za metu, kao što su trenutni događaji ili finansijski dokumenti.

Napad je, kako je navelo Ministarstvo, izvršen na eksternom disku "D" i tom prilikom je kriptovana, odnosno šifrirana kompletna infrastruktura Parlamentarne skupštine, pa uposlenici sedmicama nisu mogli pristupiti mailovima i drugim servisima. To, praktično, znači da je putem jednog e-maila došlo do kompromitacije mreže, a zatim i napada na jedan od eksternih diskova, zbog čega je blokirana cijela infrastruktura Državnog parlamenta.



4.6.3. Cucky Malware

Cucky je prilagođeni kradljivac baziran na .NET-u, radi van mreže, pohranjujući prikupljene informacije u *%TEMP%\backuplog* folder umjesto da komunicira s mrežom. Cucky je dizajniran za izdvajanje podataka kao što su lozinke, historija pregledavanja, vjerodajnice za prijavu i kolačići iz odabranih internet preglednika.

Iako je tačna upotreba ukradenih podataka i dalje nejasna, pretpostavlja se da bi mogli poslužiti u nekoliko namjena. To uključuje dobijanje pristupa klijentima e-pošte zasnovane na webu, provođenje daljnjeg izviđanja infrastrukture kroz internet historiju, sastavljanje liste zaposlenih iz organizacije žrtve, distribuciju priloga prožetih zlonamjernim softverom i utvrđivanje da li je kompromitovana mašina stvarno ili virtualno okruženje.

Funkcionalnost Cuckyja se proteže na veliki broj pretraživača, koji uključuju ali nisu ograničeni na: Chrome, MS Edge, CocCoc, Chromium, Brave, Atom, Uran, Sputnik, Slimjet, Epic Privacy, Amigo, Vivaldy, Kometa, Comodo, Nichrome, Maxthon, Comodo Dragon, Avast Browser i Yandex.

4.6.4. Zebrocy zlonamjerni softver – S0251

Zebrocy je trojanski zlonamjerni softver koji koristi grupa aktera koji se od 2015. nazivaju APT28/Sofacy. Sastoji se od tri glavne komponente: Backdoor, Downloader i Dropper. Komponente Downloader i Dropper olakšavaju procese otkrivanja i preuzimanje primarnog zlonamjernog softvera na sisteme. Backdoor komponenta, u međuvremenu, osigurava postojanost sistema, špijunažu i ekstrakciju podataka.

Iako nije nov, Zebrocy je evoluirao tokom vremena i pokazuje varijante u više programskih jezika kao što su Delphi, C#, Visual C++, VB.net i Golang. Poznato je da napredni napadači povremeno revidiraju svoje *malware* alate koristeći različite jezike i tehnologije.

Zebrocy koristi brojne tehnike društvenog inženjeringa, pozivajući žrtve da otvore priložene datoteke putem tematskih, lažnih e-poruka koje kruže na mjestu distribucije zlonamjernog softvera.[7]

Ovi napadači se prvenstveno bave špijunskim aktivnostima usmjerenim na kritične i strateške elemente državnih institucija i organizacija. Ovi ciljevi se prvenstveno nalaze na Bliskom istoku, Evropi i Sjevernoj Americi.

7 Zlonamjerni softver uglavnom cilja:
- Ministarstva energetike i industrije
- Naučne i inženjerske centre
- Ministarstva vanjskih poslova
- Nacionalne sigurnosne i obavještajne agencije
- Press servise

Nakon faze otkrivanja, Zebrocy prenosi određene tipove datoteka na komandni i kontrolni server radi ekstrakcije podataka.[8]

4.6.5. ECCENTRICBANDWAGON Malware

ECCENTRICBANDWAGON je "trojanac" za daljinski pristup (RAT) prvi put identificiran u augustu 2020. godine. Pripisan je sjevernokorejskim napadačima. Radi kao alat za izviđanje i posjeduje funkcije *keylogginga* odnosno snimanja onoga što korisnik kuca na svojoj tastaturi, kao i snimanja ekrana. Ove mogućnosti *malware* čini vještim u prikupljanju informacija o kompromitiranim sistemima.

Vjeruje se da je grupa HIDDEN COBRA kreator ovog novog "trojanca". Pretpostavlja se da je specifična upotreba ovih daljinskih alata za pokretanje visoko ciljanih napada na različite sektore kao što su finansije, inženjering, vlade i nevladine organizacije.

Svaka varijanta ECCENTRICBANDWAGON-a sastoji se od primarne DLL datoteke koja, kada se jednom pokrene, koristi tri odvojene datoteke za snimke ekrana, sistemske evidencije i ključeve. Neke verzije zlonamjernog softvera šifriraju ove datoteke pomoću algoritma za enkripciju RC4, dok druge imaju jednostavnu funkciju čišćenja dizajniranu da uklone datoteke dnevnika nakon pokretanja ECCENTRICBANDWAGON-a.

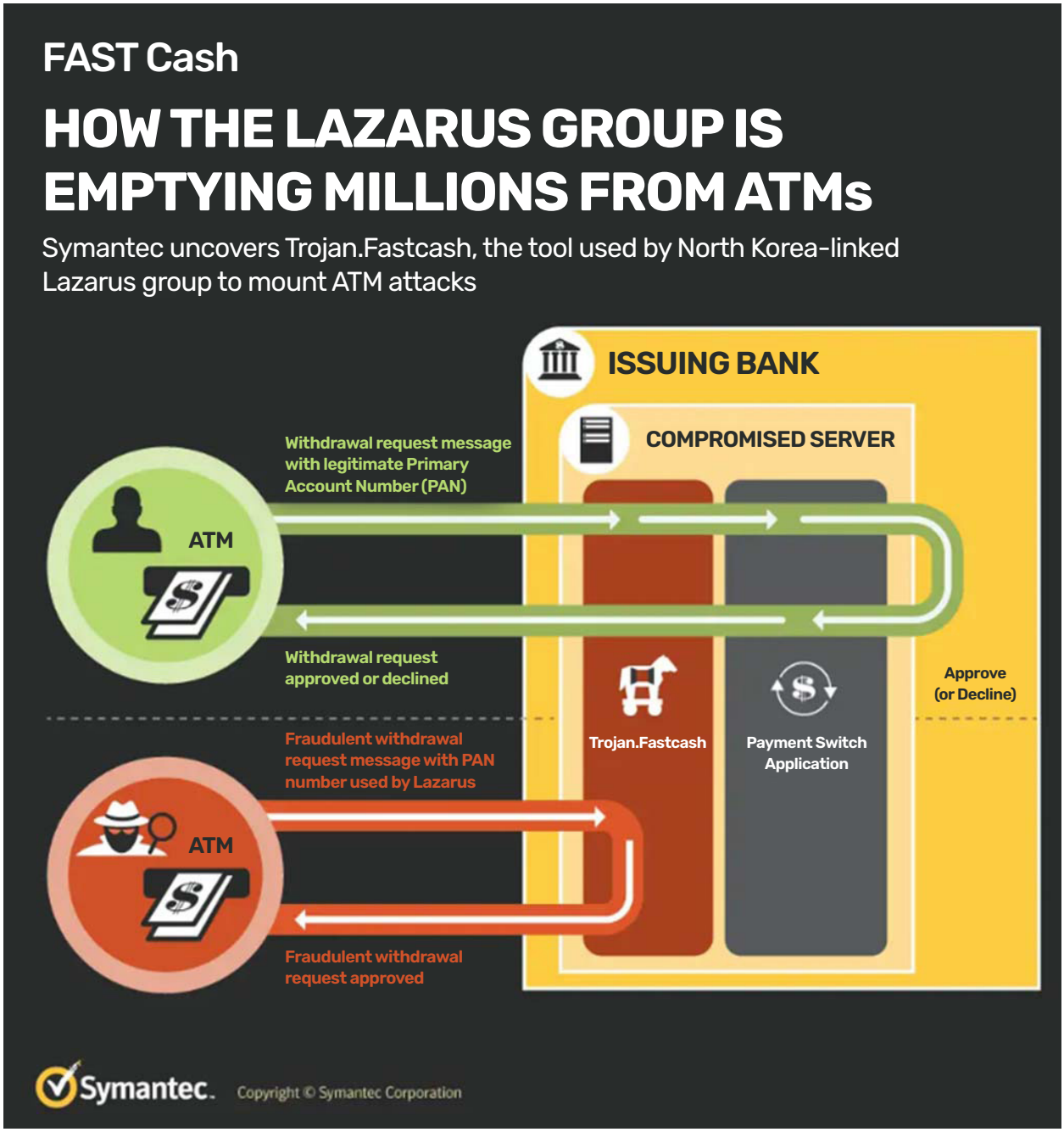
4.6.6. Zlonamjerni softver FASTCash

Hidden Cobra, poznata i kao Lazarus, veoma je aktivna i ozloglašena grupa za cyber napade, poznata po svojoj umiješanosti u cyber kriminal i špijunažu. Grupa, u početku poznata po svojim remetilačkim napadima visokog profila, kao što je napad na Sony Pictures 2014. godine, provodi operacije "FASTCash" najmanje od 2016. godine. Ove operacije ciljaju na krađu novca iz bankomata od banaka u Aziji i Africi.

Posljednjih godina Lazarus je proširio svoje aktivnosti na finansijski motivirane napade. Značajni primjeri uključuju krađu 81 miliona američkih dolara od Centralne banke Bangladeša i WannaCry napad.

Operacija "FASTCash" omogućava Lazarusu da na prevaru podiže gotovinu s bankomata. Metoda uključuje prvo infiltriranje u mreže ciljanih banaka i kompromitaciju servera aplikacija koji upravljaju bankomatima.

8 .doc, .docx, .xls, .xlsx, .ppt, .pptx, .exe, .zip, .rar



Nakon kompromitacije ovih servera, postavlja se ranije nepoznati zlonamjerni softver Trojan. Fastcash. Ovaj zlonamjerni softver presreće lažne Lazarus zahtjeve za podizanje gotovine i šalje lažne odgovore za odobrenje, omogućavajući tako napadačima da podignu gotovinu s bankomata.

Američka vlada je navela značajne incidente koji su uključivali ovu operaciju. U 2017. godini gotovina je istovremeno podizana s bankomata u više od 30 različitih zemalja. Još jedan veliki događaj u 2018. godini doveo je do podizanja novca s bankomata u 23 različite zemlje. Procjene sugeriraju da je operacija Lazarus FASTCash do danas ukrala desetine miliona dolara.

4.6.7. ELECTRICFISH Malware

ELECTRICFISH je nedavno identificirana vrsta zlonamjernog softvera povezana sa sjevernokorejskim cyber napadima. Otkriće ELECTRICFISH-a došlo je kao dio operacije praćenja Hidden Cobre, grupe za koju se sumnja da je sponzorirana od države i koju podržava Vlada Sjeverne Koreje.

Također prepoznata kao Lazarus grupa, Hidden Cobra je povezana s nizom napada usmjerenih na finansijske institucije, kritične industrijske sektore i entitete s vrijednom intelektualnom svojinom širom svijeta.

Opis ELECTRICFISH proizlazi iz jedne zlonamjerne 32-bitne *Windows* izvršne datoteke. Nakon analize ovog uzorka metodom reverznog inženjeringa, otkriveno je da zlonamjerni softver sadrži prilagođeni protokol koji omogućava tok prometa između izvorne i odredišne IP adrese. Ova funkcija značajno povećava njen potencijal za kršenje podataka i infiltraciju.

4.6.8. Zlonamjerni softver VIVACIOUSGIFT

VIVACIOUSGIFT je zlonamjerni softver koji se prvenstveno koristi kao mrežni proxy alat, a sastoji se od jedne 32-bitne EXE datoteke s ugrađenim tvrdo kodiranim nizovima. Nakon izvršenja, dekodira ove nizove da bi dobio kombinaciju izvornog i proxy IP/porta. Zlonamjerni softver se zatim povezuje s komandnim i kontrolnim serverom kako bi primio skup nizova za inicijalizaciju.

Nakon uspješnog povezivanja i inicijalizacije, VIVACIOUSGIFT se povezuje na specificiranu odredišnu IP adresu i pokreće svoju proxy funkcionalnost. Ova karakteristika se posebno koristi za krađu finansijskih informacija i za kreiranje proxy servera za aktivnosti napadača.

4.6.9. Zlonamjerni softver CROWDEDFLOUNDER

CROWDEDFLOUNDER je sofisticirani komad zlonamjernog softvera koji je obično upakovan u 32-bitnu *Windows PE* datoteku koja koristi *Themidu* za pakovanje. Kada se pokrene, raspakira i izvršava binarnu datoteku "trojanca" za daljinski pristup (RAT) direktno u memoriji. Ova aplikacija može prihvatiti argumente tokom izvršavanja i može se instalirati kao servis s argumentima komandne linije.

Posebno, CROWDEDFLOUNDER može raditi kao proxy, aktivno osluškujući dolazne veze, a istovremeno prima komande. Nadalje, sposoban je uspostaviti udaljene veze s drugim serverom za primanje komandi. Ove višestruke mogućnosti čine CROWDEDFLOUNDER svestranim alatom za cyber napade, nudeći i daljinski pristup i funkcije kontrole komandi.

4.6.10. Zlonamjerni softver HOPLIGHT

Kampanja zlonamjernog softvera HOPLIGHT uključuje paket od 27 zlonamjernih datoteka, prvenstveno uključujući prijenosne izvršne datoteke (PE) specifične za *Windows* i određene datoteke s podacima. Ova kolekcija obuhvata raznovrstan spektar zlonamjernog softvera,

uključujući backdoor “trojance”, droppere, kradljivce informacija, sakupljače akreditiva i “trojance”/alate za daljinski pristup (RAT).

Prema izvještajima, šesnaest od ovih datoteka omogućava operaterima HIDDEN COBRA, sjevernokorejskoj grupi, da zamagljuju promet između kompromitirane mašine i komandnih i kontrolnih servera. Ovi proxyji mogu generirati fiktivne TLS sesije rukovanja koristeći potpisani javni SSL certifikat, poboljšavajući tajne operacije napadača.

Čini se da je teret datoteka koje koriste napadači zaštićen lozinkom ili kodiran određenim ključem, dajući dodatni sloj sigurnosti njihovim operacijama. Pored toga, čini se da jedna datoteka uspostavlja izlazne veze sa unaprijed određenim IP adresama, dok istovremeno ispušta četiri fajla na kompromitirani sistem. Ove ispuštene datoteke sadrže IP adrese i SSL certifikate koji pomažu da se produbi uporište napadača na zaraženim sistemima.

4.6.11. O OpenCTI-u

OpenCTI je platforma otvorenog koda dizajnirana za upravljanje i analizu obavještajnih podataka o cyber prijetnjama. Primarni cilj OpenCTI-a je da nam omogući bolje razumijevanje sveukupnih cyber prijetnji i razmjenu znanja o cyber prijetnjama.

OpenCTI platforma pruža alate za uvoz i skladištenje raznih podataka koji se odnose na cyber prijetnje, za obogaćivanje ovih podataka i za stvaranje smislenih korelacija kako bi se formirala potpunija slika prijetnji.

OpenCTI može uvesti informacije iz niza eksternih izvora sa različitim formatima, uključujući standard strukturiranih informacija o prijetnjama (STIX2). Platforma podržava unos sirovih podataka i pretvara ih u jedinstveni format koji se može lako obraditi i analizirati. Platforma nam također omogućava izvoz stečenih informacija i znanja na strukturiran, koristan način, pomažući nam u dijeljenju ili arhiviranju njihovih obavještajnih nalaza.

Platforma omogućava efikasno upravljanje informacijama u vezi sa cyber prijetnjama, pružajući analitičarima strukturirano okruženje za istraživanje različitih entiteta, kao što su akteri prijetnji, skupovi upada, *malware* i obrasci napada. Platforma nudi organiziran sistem za skladištenje, preuzimanje i ažuriranje relevantnih obavještajnih podataka o prijetnjama. Ovaj efikasan sistem upravljanja poboljšava efikasnost reagiranja na incidente i operacija otkrivanja prijetnji.

Jedna od najmoćnijih mogućnosti OpenCTI-a je povezivanje podataka iz različitih izvora kako bi se formiralo konkretno razumijevanje pejzaža cyber prijetnji. Platforma može pronaći veze između odvojenih incidenata, prepoznati zajedničke taktike, tehnike i procedure (TTP) i pratiti obrasce u ponašanju aktera prijetnji. Ova funkcija vodi do obogaćenih obavještajnih podataka, pružajući detaljniju sliku potencijalnih prijetnji i ranjivosti.

OpenCTI potiče razmjenu obavještajnih podataka unutar i između organizacija na siguran i kontroliran način. Platforma je dizajnirana da promovira zajednički rad, omogućavajući više analitičara da rade zajedno na istim podacima i dijele svoje uvide. Podržava razmjenu u široj

zajednici obavještajnih podataka o cyber prijetnjama, omogućavajući strategiju kolektivne odbrane od zajedničkih cyber prijetnji.

CSEC-ova OpenCTI platforma uvozi mnogo različitih *feedova* iz različitih dostupnih konektora koji omogućavaju bolje razumijevanje i vidljivost cyber prijetnji na globalnom i regionalnom nivou. Kao što smo ranije pisali u ovom izvještaju, trenutno je Bosna i Hercegovina navedena samo u AlienVaultovim podacima.

OpenCTI-ev AlienVault konektor pruža mogućnost uvoza podataka o prijetnji sa AlienVaultovog OTX-a (Open Threat Exchange) u OpenCTI platformu.

AlienVault OTX je jedna od najvećih zajednica otvorenih obavještajnih podataka o prijetnjama koja omogućava saradnju u odbrani s djelotvornom obavještajnom informacijom o prijetnjama koju pokreće zajednica.

Jedna od glavnih karakteristika OTX-a je njegovo pružanje podataka o prijetnjama koje stvara njegova zajednica. Platforma svakodnevno unosi veliku količinu podataka o pokazateljima kompromisa (IOC). Ovi indikatori uključuju stvari kao što su IP adrese, URL-ovi ili *hashovi* datoteka povezanih s poznatim prijetnjama, i oni su kritični resurs za identifikaciju i odgovor na cyber prijetnje.

OTX omogućava saradnju između korisnika, što daje članovima zajednice da rade zajedno na istraživanju prijetnji, validaciji indikatora i razvoju strategija odgovora. Saradnja može dovesti do efikasnijeg i efektivnijeg odgovora na prijetnje, jer omogućava razmjenu znanja i resursa.

OpenCTI je dizajniran da centralizira sve podatke o prijetnjama u jedan sistem upravljanja znanjem. Povezivanjem na AlienVaultov OTX, on obogaćuje svoju bazu podataka s više vanjskih informacija o prijetnjama u realnom vremenu, omogućavajući CSEC-u da izvrši bolje otkrivanje i prevenciju prijetnji.

4.7. Cyber napadi otkriveni putem Shadowservera

Uz OpenCTI, novi način prikupljanja podataka za CSEC došao je zahvaljujući saradnji sa The Shadowserver Foundation, jednim od vodećih svjetskih resursa za izvještavanje o sigurnosti na internetu i istraživanje zlonamjernih aktivnosti.

Trenutno je 70 milijardi SSL certifikata indeksirano i pretraživo u klasterima podataka i analiza Fondacije, 201 nacionalni CERT koristi svoje dnevne izvještaje koji pokrivaju 175 zemalja i teritorija, uključujući podatke o Bosni i Hercegovini koje prikuplja CSEC.

Shadowserver metodologija podrazumijeva da senzori Shadowservera svakodnevno skeniraju cijeli IPv4 Internet[9] kroz infrastrukturu. Velika mreža *honeypotova* prikuplja podatke o prijetnjama. Svi otkriveni zlonamjerni softveri se analiziraju u *sandbox* okruženju, a uzorci

9 Internet protokol četvrte generacije.

zlonamjernog softvera se čuvaju svakih 90 dana. Dnevni izvještaji se šalju provjerenim pretplatnicima, uključujući policiju.

Shadowserver svaki dan skenira cijeli IPv4 Internet u potrazi za više od 100 različitih mrežnih protokola, a također izvodi IPv6[10] skeniranje na osnovu IPv6 popisa pogodaka za odabrane protokole. Omogućava identifikaciju pogrešno konfiguriranih ili ranjivih uređaja, nepotrebno izložene napadne površine ili jednostavno samo popisivanje stanovništva.

Mreže *honeypotova* koriste se za promatranje hostova koji izvode različite napade na strani servera, kao što su eksploatacije usmjerene na eksterno izložene usluge ili brutalno prisiljavanje akreditiva[11] na IoT (Internet of things[12]) uređajima kako bi se dobio pristup putem protokola za udaljeni pristup kao što su SSH, telnet, VNC, RDP i FTP. Također se mogu koristiti za posmatranje aktivnosti skeniranja mreže i pokušaja DDoS-a pojačanja.

Ono što je zanimljivo za Shadowserver uređaje jesu informacije koje se mogu pronaći u svakoj zemlji u kojoj postoji partner ove fondacije. Govoreći o BiH, ova fondacija napominje da u BiH postoji 29.179 jedinstvenih IP-ova, 770.624 širokopojasne fiksne pretplate i da je broj korisnika interneta 2,3 miliona. Prema njihovim podacima, prosečna brzina interneta u našoj zemlji je 48,51 Mbps.

Prema njihovoj statistici uređaja na takozvanom Internetu stvari, moguće je pronaći razne druge podatke, poput onih o proizvođačima opreme koji su najzastupljeniji u Bosni i Hercegovini, kao i vrste i modele opreme pomoću kojih se mogu pratiti izvore cyber napada. Broj ovakvih uređaja u BiH, prema podacima Shadowservera, iznosi 29.179.

10 Internet protokol šeste generacije.

11 Akreditivi su sredstvo dokazivanja (prepoznavanja) elektronskog identiteta (npr. korisničko ime/lozinka, token na mobilnom telefonu, digitalni certifikat i sl.). Akreditiv služi kao sredstvo prijave na elektronsku uslugu.

12 Internet of things je naziv za sve uređaje koji koriste konekciju na internet, najčešće se misli na kućne uređaje poput "pametnih" televizora, kamera i slično, koji koriste pristup internetu i mogu se napasti.

5.

Napredak na ažuriranju vladinih mjera

Od našeg prvog izvještaja napravljeni su ograničeni napori vlasti da donesu potrebna zakonska i strateška rješenja za cyber sigurnost. BiH i dalje ostaje jedina zemlja Zapadnog Balkana bez nacionalne strategije za cyber sigurnost, ali i regulacionih dokumenata za usklađivanje sa standardima Evropske unije, što je jedan od preduslova u procesu EU integracija.

Tokom izvještajnog perioda ipak se dogodio mali napredak prema uspostavljanju Tima za odgovor na računarske incidente (CERT) za državne institucije. U maju 2023. godine Vijeće ministara usvojilo je odluku o sistematizaciji radnih mjesta u Ministarstvu sigurnosti, čime su stvorene pretpostavke za formiranje nacionalnog CERT tima, u skladu s preporukama EU. Ovo je zapravo oživljavanje procesa koji je u zastoju već šest godina. Jedan od prethodnih saziva Vijeća ministara još 2017. godine donio je odluku o uspostavljanju CERT tima za institucije BiH kao dio Ministarstva sigurnosti.

Predstavnici Ministarstva sigurnosti su za BIRN BiH kazali da je "novim pravilnikom ustanovljena nova organizaciona jedinica, CERT tim za institucije BiH, sa ukupno pet sistematiziranih radnih mjesta, sa opisima poslova dizajniranim u skladu s preporukama i najboljim praksama ENISA-e".

Međutim, praktična implementacija CERT tima i dalje ovisi o nekoliko političkih odluka. Ministarstvo je pokrenulo postupak djelimičnog popunjavanja novoosnovanog tima, ali ih budžetska ograničenja i dalje sprečavaju da ga popune u potpunosti.

"Održano je nekoliko sastanaka s međunarodnim partnerima koji su izrazili spremnost da pomognu u uspostavljanju CERT tima za institucije BiH, koji će se sigurno koristiti", dodaju iz Ministarstva sigurnosti, u kojem planiraju i pridruživanje međunarodnim organizacijama koje će olakšati razmjenu informacija.

Osim ovog, Parlamentarna skupština je u maju ove godine usvojila nekoliko inicijativa. One bi trebale voditi do poboljšanja stanja u cyber sigurnosti. Važno je iskoristiti ovaj pozitivni zamah, kroz brzo donošenje odluka na osnovu ovih zaključaka, ali i istovremeno hitno usvajiti potrebna zakonska i strateška rješenja, kao što je Zakon o cyber sigurnosti u BiH, sveobuhvatan Strateški okvir za cyber sigurnost, Politika razvoja sektora elektronskih komunikacija u BiH te Zakon o kritičnoj infrastrukturi.

Fondacija Shadowserver otkrila je da je BiH bila izložena cyber napadima od sofisticiranih napadača, uključujući sjevernokorejske i ruske grupe, koje često ciljaju ključne institucije i infrastrukturu. To su samo dodatni razlozi zašto je potrebno hitno uspostaviti rad nacionalnog CERT tima, čiji nedostatak sada pokušava nadomjestiti CSEC, kao i usvojiti niz dokumenata koji su na čekanju a koji su neophodni za poboljšanje standarda cyber sigurnosti u BiH.

6.

O Centru za izvrsnost u cyber sigurnosti i BIRN-u BiH

BiH se nalazi u nepovoljnom položaju kao posljednja zemlja Zapadnog Balkana bez funkcionalnog sveobuhvatnog CERT-a na državnom nivou. Ovo ostavlja BiH, njene institucije, ekonomiju i građane izložene cyber šteti u mjeri koja može ugroziti potencijalne koristi digitalizacije za privredu i društvo, a zemlju čini izloženijom zlоćudnim vanjskim utjecajima u cyber domenu.

CSEC će pokušati premostiti ovaj jaz, te će se za dvije godine razviti u posljednje sredstvo cyber sigurnosti u BiH, s ciljem pružanja aktivnog i efikasnog odgovora na incidente cyber sigurnosti. Akademsko porijeklo CSEC-a pruža priliku za kombiniranje stručnosti i iskustva, izgradnju veza s privatnim sektorom i na kraju podržavajući razvoj radne snage za cyber sigurnost u BiH.

Konačna misija CSEC-a je da se “pozicionira kao neutralna, ‘odlazna’ tačka za sistematski odgovor na cyber incidente u BiH kako bi se podržao razvoj i unapređenje cyber sigurnosti u BiH”. CSEC također planira da ojača komunikaciju između aktera u oblasti cyber sigurnosti i drugih CERT timova u regionu. Vizija CSEC-a je “siguran i siguran cyber prostor u BiH za sve”.

7.

O BIRN-u BiH

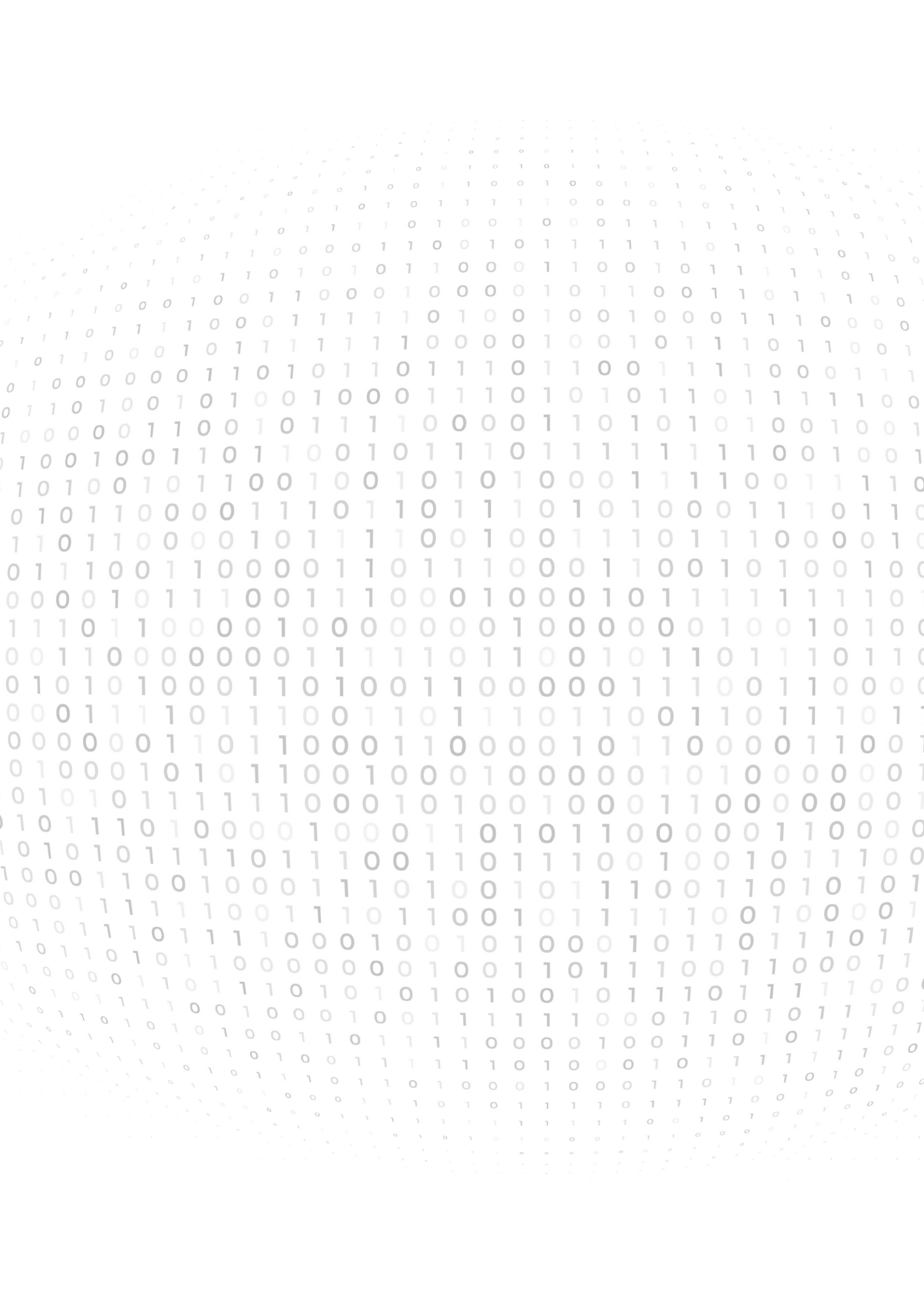
BIRN BiH je medijska nevladina organizacija sa sjedištem u Sarajevu, specijalizirana za praćenje i izvještavanje o suđenjima za ratne zločine, korupciju i terorizam. Novinari BIRN-a BiH godinama su vodeći izvori javnosti u oblastima tranzicijske pravde, vladavine prava i ekstremizma.

BIRN BiH od svog osnivanja 2005. godine informiše javnost o procesuiranju ratnih zločina pred državnim i lokalnim sudovima u BiH, ali i pred međunarodnim sudovima. Na stranici Detektor.ba pohranjene su desetine hiljada izvještaja sa saslušanja, izjava svjedoka zločina, preživjelih žrtava i članova porodica nestalih. BIRN BiH je 2015. godine započeo projekat posvećen praćenju i izvještavanju o slučajevima organiziranog kriminala, korupcije i terorizma. Od tada je objavljen niz analiza, istraživanja i dokumentarnih filmova o aferama korupcije, neprocesuiranim krivičnim djelima i putovanjima na strana ratišta, za što su međunarodne organizacije nagradile BIRN-ov tim.

Novinari BIRN-a BiH rasvijetlili su i širenje ekstremističkih i desničarskih grupa u regionu, otkrivajući trendove koji se prelijevaju u BiH i upozoravajući na negativne posljedice. Osim gostovanja u drugim medijima i objavljivanja gotovo 26.000 tekstova, BIRN BiH proizvodi i dvije mjesečne emisije – *TV Justice*, koja do septembra 2023. ima 153 epizode, i *Detektor Magazin*, koji do objavljivanja ovog izvještaja broji devet epizoda.

BIRN BiH je kroz različite projekte omogućio javni pristup nekoliko baza podataka – o terorizmu, mržnji, službenim automobilima, masovnim grobnicama i o utvrđenim sudskim činjenicama koje ulaze u obrazovni sistem. Radeći samostalno i kroz različite saradnje, BIRN BiH je do sada objavio deset publikacija dostupnih ovdje.

Redakcija BIRN-a BiH raste iz godine u godinu, a sa njom, uz podršku donatora, rastu i novi projekti posvećeni tranzicijskoj pravdi, vladavini prava, ekstremizmu i borbi za ljudska prava.



CSEC
Cyber Security
Excellence Centre

BIRN
BALKAN
INVESTIGATIVE
REPORTING
NETWORK
BOSNIA &
HERZEGOVINA