SRBIJA

Pejzaž digitalnih pretnji: Građansko društvo i mediji

Internews
Local voices. Global change.

SHARE FOUNDATION

Sadržaj

Polazna osnova

Pod aktuelnim režimom, Srbija doživljava nazadovanje demokratije što nezavisnim medijima sužava mogućnosti da rade bez upliva sa strane i pojačava pritisak na civilno društvo. To nazadovanje uvećava rizik od digitalnih pretnji srpskom civilnom društvu i medijima. Ovaj izveštaj je pripremio *Internews*ov tim za slobodu i otpornost na internetu u okviru tekućeg rada na jačanju sposobnosti organizacija civilnog društva, novinara i drugih branitelja ljudskih prava da otkriju, analiziraju i izgrade otpornost na digitalne napade putem lokalizovane ekspertize za analizu pretnji i reagovanje na incidente. Izveštaj nudi pregled pretnji s kojima se civilno društvo i medijske organizacije suočavaju u Srbiji, kao i smernice za stručnjake za digitalnu bezbednost koji pružaju podršku zajednici. Takođe ima za cilj da industriji sajber bezbednosti predstavi širi kontekst, u slučaju potrebe za analizom bezbednosnih incidenata koji pogađaju srpsko civilno društvo i medije. Izveštaj zaključujemo diskusijom o primeni mitigacionih mera koje bi stručnjaci za digitalnu bezbednost mogli da ponude organizacijama sa kojima rade, kao i civilnom društvu i medijskim organizacijama.

Ovaj izveštaj je napisan u bliskoj saradnji sa SHARE Fondacijom, neprofitnom organizacijom sa sedištem u Srbiji, osnovanom 2012. godine radi unapređenja ljudskih prava i sloboda u onlajn sferi, promocije pozitivnih vrednosti otvorenog i decentralizovanog interneta, kao i slobodnog pristupa informacijama, znanju i tehnologiji. Primarne oblasti aktivnosti SHARE Fondacije su sloboda izražavanja na internetu, privatnost podataka, digitalna bezbednost i otvoren pristup znanju.

Pretnje, trendovi i studije slučaja izdvojeni u ovom izveštaju identifikovani su kroz direktnu podršku za digitalnu bezbednost rizičnih zajednica (koju pružaju *Internews* i SHARE Fondacija), desk istraživanje i razgovore sa pouzdanim članovima zajednice za slobodan internet. Izveštaj objedinjava podatke prikupljene tokom reagovanja na incidente i dokumentuje obrasce napada koji su specifični za Srbiju.

Oktobar 2023

Napisali i uredili: Martijn Grooten, Ashley Fowler, Marc Shaffer, i Skyler Sallick
Lektura, dizajn i prelom: Skyler Sallick

Pejzaž digitalnih pretnji

Politički kontekst, građansko društvo i mediji

Pod aktuelnim predsednikom Aleksandrom Vučićem, Srbija doživljava nazadovanje demokratije i sve brojnije optužbe za kršenje ljudskih prava i slobode štampe. *Freedom House* rangira Srbiju kao „delimično slobodnu", sa ocenom 60 od 100,[1] beležeći nastavak trenda opadanja.[i], [2] Srbija učestvuje u značajnom regionalnom sporu zbog Kosova, koje je 2008. godine jednostrano proglasilo nezavisnost. Kosovo je kao suverenu državu priznala 101 članica Ujedinjenih nacija, dok Srbija ostaje pri stavu da je Autonomna pokrajina Kosovo i Metohija srpska teritorija. Spor sa Kosovom i dalje predstavlja jedno od ključnih pitanja u srpskoj politici, uz povremeno izbijanje nasilja, poslednji put sredinom 2023.[3]

Pod Vučićem, civilno društvo i nezavisne medijske organizacije trpe pojačani pritisak. Novinari čije izveštavanje oponira zvaničnoj liniji vlasti, suočeni su sa čestim strateškim tužbama protiv učešća javnosti (SLAPP), uključujući optužbe za veze sa organizovanim kriminalom.[4] U načelu, domaće i međunarodne nevladine organizacije mogu slobodno da rade, ali su one koje previše otvoreno kritikuju vlasti izložene uznemiravanju i pretnjama.[5]

Pod Vučićem, civilno društvo i nezavisne medijske organizacije trpe pojačani pritisak. Novinari čije izveštavanje oponira zvaničnoj liniji vlasti, suočeni su sa čestim strateškim tužbama protiv učešća javnosti (SLAPP), uključujući optužbe za veze sa organizovanim kriminalom.

U poređenju sa drugim zemljama regiona, značajan broj proreżimskih tabloida objavljuje govor mržnje protiv nezavisnih novinara, često postavljajući njihove fotografije uz optužbe da su neprijatelji države. Zbog pojačanog pritiska vlasti, tržište za nezavisne medije se sužava. Usled toga, mediji su prinuđeni da traže donatore kako bi održali svoje poslovanje.

Prema Međunarodnoj federaciji novinara, Srbija je jedna od najopasnijih zemalja za novinare u Evropi. Fizički napadi na novinare i dalje su uobičajeni i mada aktuelni napori da se situacija popravi delimično imaju uspeha, neprijateljsko okruženje koje je stvorila vlada podriva rad nezavisnih novinara.[6]

Sajber bezbednost u Srbiji

Sajber napadi izazivaju sve veću zabrinutost u Srbiji. Mada je Srbija potpisnica Budimpeštanske konvencije[ii],[7] i ima uspostavljen okvir za borbu protiv sajber kriminala, ovaj problem i dalje preovladava usled nedostatka osoblja u relevantnim vladinim službama i opšteg manjka svesti u široj javnosti.[8]

[i] Freedom House je Srbiju poslednji put kategorisao kao „slobodnu" 2018. sa ocenom 73 od 100 [2].

[ii] Srbija je potpisnica Budimpeštanske konvencije, „okvira koji omogućava stotinama stručnjaka iz država članica da razmenjuju iskustva i stvaraju odnose koji olakšavaju saradnju u određenim slučajevima, uključujući i vanredne situacije, mimo posebnih odredbi predviđenih ovom Konvencijom". [7]

Sajber kriminal motivisan finansijskim interesima cilja na privatne subjekte kao i na samu državu. Srbija je bila primarna meta napredne, finansijski motivisane kampanje koju je 2019. otkrila bezbednosna kompanija ESET.[9] Na početku pandemije kovida-19, javno komunalno preduzeće u Novom Sadu, drugom po veličini gradu u Srbiji, napadnuto je ucenjivačkim softverom. Srećom, otkrivena je greška u mehanizmu za enkripciju, koja je omogućila oporavak 50TB šifrovanih podataka bez plaćanja otkupnine.[10] Za više informacija o tom incidentu pogledajte ovaj izveštaj, dostupan na srpskom jeziku, koji je objavila SHARE Fondacija.[11]

Relativno se malo zna o državno sponzorisanom malveru kojem je Srbija na meti. Međutim, 2021. godine, *PwC* je razotkrio kampanju koja je bila usmerena na vladine i vojne institucije u Srbiji i Republici Srpskoj[iii] u Bosni i Hercegovini.[12] *PwC* je aktera koji stoji iza ove kampanje označila nazivom „Beli Tur", ali nije uspela da poveže sajber kriminalce sa konkretnom zemljom. Ministarstvo unutrašnjih poslova Srbije je 2023. bilo meta nekoliko napada distribuiranog uskraćivanja usluge (DDoS) koji se dovode u vezu sa regionalnim tenzijama, uključujući nasilne sukobe između etničkih Srba na severu Kosova i vlasti etničkih Albanaca.[13]

Srbija je takođe dom sajber kriminalaca koji deluju izvan njenih granica. Tako je 2017. otkriveno da srpski programer i ultranacionalista stoji iza relativno opskurnog „SerbRansom" rensomvera.[14] Naredne, 2018. godine, jedan Srbin je uhapšen zbog sumnje da je bio u vezi sa hakerskom ekipom *Dark Overlord*, jednom od najaktivnijih onlajn kriminalnih grupa u to vreme.[15] Tokom 2022, muškarac sa dvojnim srpsko-mađarskim državljanstvom, priznao je krivicu za kompromitovanje poslovnih mejlova (*business email compromise*, BEC) kada je od žrtava na prevaru uzeto ukupno 3,7 miliona dolara.[16]

Stanje sajber bezbednosti u građanskom društvu i medijima

Sajber napadi počinjeni u Srbiji takođe na meti imaju organizacije civilnog društva i medijsko okruženje. Iako su i ovi napadi često motivisani finansijskim interesima, postoje dokazi o supresivnim provladinim aktivnostima, kao što su napadi botovima koje su orkestrirali prorežimski nalozi, a koji imaju za cilj da poremete sposobnost ovih zajednica da obavljaju svoj posao.

Balkanska istraživačka mreža (BIRN) i SHARE Fondacija verifikovali su 190 slučajeva kršenja digitalnih prava u periodu od avgusta 2019. do novembra 2020. godine, najčešće u obliku „pritisaka zbog izražavanja i aktivnosti na internetu".[17] U pogledu kršenja digitalnih prava, najčešće mete su građani, novinari, onlajn mediji, javne ličnosti, državni zvaničnici i aktivisti.[18] Primer vrste napada na novinare i organizacije civilnog društva može se naći u delu 'Studije slučaja' ovog izveštaja.

Medijske kuće i organizacije civilnog društva obično su na meti digitalnih pretnji – čak i ako većina napada nije direktno usmerena na njih. Žene su suočene s većom pretnjom digitalnih napada, koji su često lične prirode sa fokusom na rod.[19] Primer takvih napada s kojima su suočene novinarke može se naći u delu 'Studije slučaja' ovog izveštaja. Za mnoge organizacije civilnog

[iii] Region Republike Srpske u Bosni i Hercegovini ima većinsko srpsko stanovništvo.

društva i medijske organizacije, neizvesna priroda njihovog finansiranja ograničava primenu digitalnih bezbednosnih mera, neophodnih za zaštitu od nadzora i drugih ciljanih napada.

Za mnoge organizacije civilnog društva i medijske organizacije, neizvesna priroda njihovog finansiranja ograničava primenu digitalnih bezbednosnih mera, neophodnih za zaštitu od nadzora i drugih ciljanih napada.

Poslednjih godina, tehnološke kompanije su preduzele mere za borbu protiv provladinih naloga kojima su na meti opozicione onlajn aktivnosti. Tako je 2020. Tviter uklonio 8.500 provučićevskih naloga i više od 43 miliona tvitova.[20] Kompanija Meta je 2023. izvestila da je sprovela aktivnosti protiv mreže „koordinisanog neautentičnog ponašanja" (*Coordinated Inauthentic Behavior*, CIB) u Srbiji, povezane sa vladajućom Srpskom naprednom strankom.[21] Ta kampanja je trebalo da stvori utisak široke podrške naprednjačkoj stranci i predsedniku Vučiću. Takođe 2023. godine, Projekat za izveštavanje o organizovanom kriminalu i korupciji (*Organized Crime and Corruption Reporting Project*, OCCRP) otkrio je ciljanu kampanju dezinformacija u kojoj je učestvovala izraelska „grupa za dezinformacije", usmerenu na javno blaćenje jednog od Vučićevih političkih rivala.[22]

Srpska Bezbednosno-informativna agencija (BIA) kupila je špijunski softver *FinFisher* i pregovarala o kupovini špijunskog softvera kompanije *Hacking Team*.[23] Ostalo je nejasno da li je BIA zapravo koristila neki od tih špijunskih softvera, kao i protiv koga. Obe vrste špijunskog softvera su korišćene za ciljanje pripadnika civilnog društva i novinara u drugim zemljama.

BIA je takođe poznati klijent kompanije za mobilni nadzor *Circles*, čiji se proizvodi mogu koristiti za presretanje telefonskih poziva i SMS brojeva.[24] Takav softver može da se koristi za ciljanje onih naloga na platformama *WhatsApp* ili *Signal* koji nemaju pristupne kodove za dodatnu zaštitu.

Da bi se zaštitila njihova sposobnost da efikasno rade, potrebno je preduzeti aktivnosti i na individualnom i na društvenom nivou. Treneri za digitalnu bezbednost mogu pomoći u zaštiti ovih ranjivih organizacija podrškom za primenu sledećih mitigacionih taktika.

Istraživači *Citizen Lab*a identifikovali su Srbiju kao verovatnog kupca špijunskog softvera *Predator*, koji je razvila kompanija *Cytrox* iz Severne Makedonije.[25] To je kasnije potvrdio *Google*.[26] I ovde je nejasno ko su bile mete, ali je vlast širila infekcije Predatora preko dva domena lažno predstavljena kao srpski mediji. Upotreba srpskih medijskih sajtova sugeriše da su se bar neke od meta nalazile u Srbiji, jer bi se za mete u inostranstvu verovatno koristili domeni na drugim jezicima.

Bezbednost organizacija civilnog društva i medija u Srbiji je ugrožena. Da bi se zaštitila njihova sposobnost da efikasno rade, potrebno je preduzeti aktivnosti i na individualnom i na društvenom nivou. Treneri za digitalnu bezbednost mogu pomoći u zaštiti ovih ranjivih organizacija podrškom za primenu sledećih mitigacionih taktika.

Mitigacione mere

Bezbednost naloga je važna svakome u Srbiji, ali je od ključnog značaja za pripadnike civilnog društva. **Dvofaktorska autentifikacija je obavezna** – i ublažava rizik zbog upotrebe slabih i/ili istih lozinki. Organizacije ne mogu da kontrolišu lozinke svojih zaposlenih, pa aktiviranje dvofaktorske autentifikacije smanjuje rizik u slučajevima kada zaposleni koriste slabe lozinke. Mada je SMS bolji nego da dvofaktorske autentifikacije uopšte nema, ne bi ga trebalo smatrati sigurnom opcijom, posebno za korisnike u riziku. Aplikacija za autentifikaciju je bolja od SMS-a, dok hardverski token u načelu pruža najveću sigurnost, mada zahteva dodatnu opremu.

Za naloge povezane sa telefonskim brojem na platformama kao što su *Telegram*, *WhatsApp* i *Signal*, dvofaktorska autentifikacija obuhvata **dodavanje pristupnog koda na nalog** pored linkovanja SMS-a koji se koristi za povezivanje naloga sa telefonskim brojem. Kada je ova funkcija omogućena, aplikacija će periodično tražiti od korisnika da unese svoj pristupni kod kako bi se osiguralo da porukama ne pristupa niko drugi osim vlasnika naloga. Ovo sprečava preuzimanje naloga putem presretanja SMS-a, bilo društvenim inženjeringom ili preko servisa kao što je *Circle*s.

Fizički uređaji, kao što su laptopovi i mobilni telefoni, treba da budu ažurirani primenom bezbednosnih zakrpa za operativne sisteme kao i drugog softvera čim postanu dostupni. **Softver treba nabavljati samo od ovlašćenih izvora**. U mnogim slučajevima, to podrazumeva plaćanje. NVO ne treba da se stide da o tome razgovaraju sa donatorima ili da traže besplatne alternative kao što je softver otvorenog koda i programi koji obezbeđuju softver besplatno ili po sniženim cenama za kvalifikovane NVO.

Iako nije poznato da li je civilno društvo u Srbiji na meti naprednog špijunskog softvera kao što je Predator, oni koji se smatraju metom visoke vrednosti treba da znaju da takav špijunski softver obično koristi tzv. ranjivosti nultog dana i zaraze nultim klikom. To znači da ova vrsta naprednog špijunskog softvera može da zarazi potpuno ažuriran uređaj, a da korisnik nije ni kliknuo na link ili otvorio prilog. Pošto u tom slučaju nema načina da se spreči zaraza, svako ko je izložen riziku od takvog špijunskog softvera treba to da ima na umu.

Potencijalnim metama se savetuje da **koriste poruke koje nestaju** u čet aplikacijama, gde se poruke automatski brišu nakon određenog vremenskog perioda, jer to može ograničiti štetu u slučaju kompromitovanja naloga. Potencijalnu štetu ograničava i **korišćenje različitih uređaja za rad i privatne potrebe**, ili čak **zasebnog uređaja za rad visokog rizika**, ali to podrazumeva dodatne troškove i manju ugodnost.

Pored ažuriranja telefona, **redovno restartovanje *iPhone*a** – idealno jednom dnevno – i korišćenje *Apple*ovog režima zaključavanja, takođe smanjuje verovatnoću da dođe do napada, koji bi verovatno bili uspešni.

Mnogo se manje zna o špijunskom softveru koji cilja Android uređaje, mada to ne znači da su korisnici Androida manje izloženi riziku. Skuplji Android uređaji, uključujući *Google*ove *Pixel* uređaje, sigurniji su i obično dobijaju popravke za ranjivosti brže od jeftinijih Android uređaja. Redovno restartovanje uređaja će verovatno ublažiti štetu, jer se špijunski softver obično uklanja

sa uređaja posle restarta.[iv] Rutovanje Android uređaja takođe može da ukloni dokaze o ranijoj zarazi, što bi neki korisnici možda hteli da izbegnu.

Studije slučaja

Suspenzija naloga Evroprajda na Instagramu

Beograd Prajd, događaj koji se održava u glavnom gradu Srbije kao proslava lokalne LGBTQ+ zajednice i njenih saveznika, prvi put je održan 2001. Tada je dočekan nasiljem sportskih huligana i aktivista ekstremne desnice.[27] Događaj je ponovo održan tek 2010. i opet su iste grupe reagovale nasiljem, što je dovelo do okršaja između ultradesničarskih ekstremista koji su pokušavali da ometaju događaj i više hiljada policajaca.[28]

Pretnje nasiljem dovele su do odluke Vlade Srbije da zabrani održavanje Prajda, ali je ta zabrana 2013. proglašena neustavnom. Izuzev 2020. (zbog pandemije kovida-19) događaj se od 2014. održava svake godine.

Beograd Prajd je 2022. godine bio domaćin Evroprajda, godišnje evropske manifestacije koja proslavlja LGBTQ+ zajednice čitave Evrope.[29] Uprkos većoj vidljivosti međunarodnog događaja, iste grupe koje su se protivile Prajdu od 2001, pokušale su još jednom da poremete okupljanje. Uznemiravanje se prenelo na onlajn prostor preko društvenih medija. Tokom priprema za događaj, Instagram je zasut prijavama protiv naloga Evroprajda zbog navodnog kršenja uslova korišćenja platforme. Iako je teško proveriti, to je verovatno dovelo do „prikrivene zabrane" (*shadow banning*) naloga Evroprajda na Instagramu, a zatim i privremene suspenzije manje od mesec dana pre događaja. Prikrivena zabrana je značila da nalog Evroprajda i dalje može da deli nove objave i storije, ali mu je domet bio značajno ograničen. Kasnija suspenzija učinila je nalog nedostupnim.

U pomoć je priskočila SHARE fondacija, neprofitna organizacija sa sedištem u Srbiji koja radi na unapređenju ljudskih prava i sloboda na mreži i promoviše pozitivne vrednosti otvorenog i decentralizovanog interneta, u koordinaciji sa službom za pomoć organizacije *Access Now*. Iako je *Meta* na kraju ukinula suspenziju, to je značajno uticalo na mogućnost da događaj privuče interesovanje javnosti putem društvenih medija.

Predsednik Srbije Vučić je krajem avgusta saopštio da održavanje Evroprajda neće biti dozvoljeno, pozivajući se na političke prilike i strah od nereda.[30] Na kraju je zabrana ukinuta, a događaj je održan u septembru 2022. kako je prvobitno planirano, sa oko 10.000 učesnika.[31] Kompanije kao što je *Meta*, u čijem su vlasništvu društvene mreže kao što je *Instagram*, dobijaju ogromne količine prijava korisnika za kršenje uslova koji važe na platformi. Građansko društvo je često na meti takvih kršenja, poput doksovanja ili pretnji, a posledice mogu biti ozbiljne. Protiv civilnog društva takođe se redovno podnose lažne prijave. Neadekvatno rešavanje prijava koje su podneli korisnici može imati ozbiljne posledice, kakve su doživeli organizatori Evroprajda

[iv] Ovo je slučaj sa svim poznatim špijunskim softverima za iPhone, a verovatno i sa špijunskim softverom za Android, posebno onaj koji „rutuje" uređaj.

2022. *Meta* i druge društvene mreže treba da budu veoma oprezne pre nego što moderiraju sadržaje organizacija civilnog društva, posebno u kontekstu događaja visokog profila.

Hakovanje naloga na Fejsbuku radi objave CSAM

Minja Marđonović je feministička aktivistkinja iz Srbije, čiji se aktivizam uglavnom javlja u digitalnom prostoru. Kao i mnogi digitalni aktivisti, ona se u velikoj meri oslanja na platforme društvenih medija kao što su *Facebook* i *Instagram*.

U septembru 2022. srpski provladin tabloid Informer objavio je intervju sa muškarcem koji je nedavno odslužio kaznu od 15 godina zatvora zbog više krivičnih dela silovanja i fizičkih napada na žene. Sagovornik je otvoreno govorio o osećanju oslobođenosti nakon izvršenja napada i davao „instrukcije" ženama kako da se ponašaju tokom napada. Minja je bila jedna od mnogih u Srbiji koje je ovaj intervju razbesneo.[32]

Nekoliko dana nakon što je podelila svoju frustraciju na društvenim mrežama i u onlajn kolumni za časopis *ELLE*, Minja je dobila fišing mejl kome je na meti bio njen nalog na Fejsbuku. Fišing napad je bio uspešan, a Minjin Fejsbuk i povezani Instagram nalog su hakovani. To je, nažalost, vrlo uobičajeno za ljude koji se bave aktivističkim radom. Međutim, usledilo je nešto krajnje neuobičajeno.

Napadač sa pristupom Minjinim nalozima objavio je materijale seksualnog zlostavljanja dece (*Child Sexual Abuse Material*, CSAM, koji se često naziva „dečja pornografija") na njenim Fejsbuk i Instagram nalozima. Kompanija Meta, u čijem su vlasništvu obe društvene mreže, koristi softver za otkrivanje CSAM-a. Kada se takav sadržaj otkrije, kao što je ovde bio slučaj, nalog se automatski gasi.

Ne samo da je to ostavilo Minju bez mogućnosti da istupa u ime žena, sada je samoj Minji bila potrebna podrška. Pored tehničke pomoći potrebne da povrati svoje naloge, bila joj je potrebna i psihološka podrška. U intervjuu za lokalni sajt *Zoomer*, Minja je govorila o neprospavanim noćima nakon incidenta, ali i o podršci drugih žena koje su joj pomogle da se oseća manje usamljeno.[33]

Mada neuobičajeno, hakovanje naloga praćeno objavljivanjem sadržaja koji automatski dovodi do gašenja naloga, kao što je CSAM ili teroristički materijal, ipak se dešava. Platforme društvenih medija, kao i zajednica za digitalnu bezbednost, treba da budu svesni ove pretnje i da obezbede solidne procedure za sprečavanje takvih napada, kao i adekvatne reakcije.

Oporavak hakovanih naloga na društvenim medijima može biti frustrirajuće težak i, u slučaju civilnog društva, često podrazumeva lične veze i spoljne organizacije koje su „partneri od poverenja" većih platformi. Mnogo je teže kada algoritam označi nalog zbog objave CSAM-a.

Na kraju, uz pomoć lokalnih organizacija kao što je SHARE Fondacija, neprofitna organizacija iz Srbije koja radi na unapređenju ljudskih prava i sloboda na mreži i promociji pozitivnih vrednosti otvorenog i decentralizovanog interneta, kao i slobodnog pristupa informacijama, znanju i tehnologiji, Minja je povratila svoje naloge. Nastavlja da se bavi onlajn aktivizmom.

Dopunska literatura

Kako pokazuje ovaj izveštaj, organizacije civilnog društva i novinari se često suočavaju sa jedinstvenim, naprednim pretnjama, dok im nedostaju resursi da ih otkriju, analiziraju i spreče. Dubinsko razumevanje pretnji s kojima su suočeni civilno društvo i mediji, omogućava specijalistima za digitalnu bezbednost da prilagode svoje reakcije i pruže bolju podršku organizacijama s kojima rade, što rezultira u prilagođenim mitigacionim merama koje su efikasnije, a pripadnicima civilnog društva i medijskim organizacijama lakše za implementaciju. Za više informacija o pretnjama s kojima se suočavaju civilno društvo i novinari, *Internews* je sa partnerima sastavio izveštaj „Globalni trendovi u digitalnim pretnjama: Civilno društvo i mediji", kao i posebne izveštaje o digitalnim pretnjama za Jermeniju, Brazil, Meksiko i Ukrajinu. Ovi resursi se mogu naći na veb stranici *Internews*a Tehnološki resursi.

Istorija Srbije

Republika Srbija (**Република Србија**) je unitarna parlamentarna republika koja se nalazi u Panonskom basenu i na Balkanskom poluostrvu. Graniči se sa Mađarskom, Rumunijom, Bugarskom, Severnom Makedonijom, Hrvatskom, Bosnom i Hercegovinom i Crnom Gorom. Po završetku Prvog svetskog rata, Srbija je sa ostalim južnoslovenskim narodima formirala Jugoslaviju, najpre pod nazivom Kraljevina Srba, Hrvata i Slovenaca. Nakon oslobođenja od okupacije sila Osovine u Drugom svetskom ratu, Jugoslavija je reorganizovana u saveznu republiku pod komunističkom vlašću. Tokom 1980-ih i 1990-ih, Jugoslavija se raspala, što je dovelo do jugoslovenskih ratova između bivših konstitutivnih republika. Crna Gora je ostala u zajednici sa Srbijom nakon raspada Jugoslavije, sve do mirnog razlaza 2006, kada je Srbija po prvi put od 1918. postala samostalna država.[34] Od 19. veka, kada je Srbija stekla nezavisnost od Otomanskog carstva, Srbija do danas održava bliske odnose sa Rusijom.[35]

Srbija je klasifikovana kao privreda sa višim srednjim dohotkom[36] i članica je Ujedinjenih nacija,[37] Saveta Evrope,[38] Organizacije za evropsku bezbednost i saradnju,[39] Partnerstva za mir,[40] Centralnoevropskog ugovora o slobodnoj trgovini,[41] a trenutno je u procesu pristupanja Svetskoj trgovinskoj organizaciji.[42] Srbija je 2009. podnela zahtev za članstvo u Evropskoj uniji, a njena kandidatura je prihvaćena 2012. Srbija i EU su započele pristupne pregovore 2014. U martu 2021, 538 poslanika u Evropskom parlamentu glasalo je za izveštaj u kojem se navodi da Srbija treba da normalizuje odnose sa Kosovom da bi postala članica EU, kao i da unapredi „pravosuđe, slobodu izražavanja i borbu protiv korupcije i organizovanog kriminala".[43]

Zahvalnost

Od 2021. godine, *Internews* je ostvario saradnju sa sedam *Threat Labs* organizacija (lokalne organizacije sa tehničkim kapacitetima i odgovarajućim alatima za analizu sumnjivih uzoraka fišinga i malvera, koje dele informacije u zajednici o trendovima napada, novim pretnjama i kontramerama) kako bi odgovorile na incidente koji utiču na digitalnu bezbednost civilnog društva i medijskih organizacija širom sveta. Podaci prikupljeni kroz program reagovanja na incidente pomogli su u oblikovanju mitigacionih mera i pristupa u reakcijama za zajednice u riziku, te obezbedili potrebne informacije za ovaj izveštaj.

Internews izražava svoju zahvalnost *Threat Labs* zajednici, koja je radila sa nama na ovom projektu. Njeni pripadnici su posvećeni pružanju pomoći onima kojima je to potrebno, kao i brizi da njihovi partneri u civilnom društvu i medijskim organizacijama mogu da obavljaju svoj važan posao bezbedno i efikasno. Ukupno, ovaj projekat je podržao *Threat Labs* u reagovanju na preko 200 incidenata digitalne bezbednosti i objavljivanju preko 60 obrazovnih resursa na njihovim veb stranicama i platformama društvenih medija.

Posebno zahvaljujemo SHARE Fondaciji na pružanju informacija za dokumentovanje i deljenje ovih studija slučaja, kao i na reviziji i vrednim komentarima za ovaj izveštaj. Izveštaj ne bi bio moguć bez Bojana Perkova i tima SHARE Fondacije.

Beleške

[1] „Sloboda u svetu 2023: Srbija", *Freedom House*, pristupljeno 11.11. 2023. https://freedomhouse.org/country/serbia/freedom-world/2023 [na engleskom jeziku]

[2] „Sloboda u svetu 2019: Srbija", *Freedom House*, pristupljeno 11.11. 2023.

https://freedomhouse.org/country/serbia/freedom-world/2019 [na engleskom jeziku]

[3] Gec, Jovana, „Srbija će tražiti sastanak sa šefom NATO i sednicu Saveta bezbednosti UN o tenzijama na Kosovu", *Associated Press*, 6. juli 2023. https://apnews.com/article/serbia-kosovo-tensions-un-vucic-nato-542321f116c5cd368b0a98f53c9fc904 [na engleskom jeziku]

[4] Mong, Attila, „'Vrlo opasna situacija': Srpski novinari optuženi za veze sa organizovanim kriminalom", Komitet za zaštitu novinara, 30. juni 2021. https://cpj.org/2021/06/serbian-journalists-accused-organized-crime [na engleskom jeziku]

[5] Mong, „' Vrlo opasna situacija': Srpski novinari optuženi za veze sa organizovanim kriminalom".

[6] „Srbija: Nezavisno novinarstvo suočeno s najvećom krizom poslednjih godina", Nezavisna federacija novinara, 26. april 2023. https://www.ifj.org/media-centre/news/detail/category/press-releases/article/serbia-independent-journalism-faces-biggest-crisis-in-years [na engleskom jeziku]

[7] „Budimpeštanska konvencija (ETS br. 185) i njeni protokoli", Savet Evrope, pristupljeno 11.11. 2023. https://www.coe.int/en/web/cybercrime/the-budapest-convention [na engleskom jeziku]

[8] Stošić, Lazar i Janković, Aleksandra, „Sajber kriminal u Republici Srbiji: prevalenca, stanje i perspektive", *Kultura polisa* 19, br. 4 (2022): 83. DOI:10.51738/Kpolisa2022.19.4r.82sj [na engleskom jeziku]

[9] Hromcová, Zuzana, „Na Balkanu, firme su na udaru iz dvostrukog oružja", *ESET Research*, 14. avgust 2019. https://www.welivesecurity.com/2019/08/14/balkans-businesses-double-barreled-weapon/ [na engleskom jeziku]

[10] Abrams, Lawrence, „*PwndLocker* rensomver provaljen: Dostupna dekripcija", *Bleeping Computer*, 5. mart 2020. https://www.bleepingcomputer.com/news/security/pwndlocker-ransomware-gets-pwned-decryption-now-available/ [na engleskom jeziku]

[11] „Kako je Novi Sad otet i zaključan", *SHARE Fondacija*, 11. juni 2021. https://www.sharefoundation.info/sr/kako-je-novi-sad-otet-i-zakljucan/

[12] Simpson, Jack, „Preteći akter in-Tur-Est", *PwC, Cyber Threat Intelligence*, 27. januar 2022. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/threat-actor-of-in-tur-est.html [na engleskom jeziku]

[13] Martin, Alexander, „Srpska vlada prijavila 'masivan DDoS napad' usred povišenih tenzija na Balkanu", *The Record*, 8. januar 2023. https://therecord.media/serbian-government-reports-massive-ddos-attack-amid-heightened-tensions-in-balkans [na engleskom jeziku]

[14] Cimpanu, Catalin, „Ultranacionalista programer iza *SerbRansom* rensomvera", *Bleeping Computer*, 11. februar 11, 2017. https://www.bleepingcomputer.com/news/security/ultranationalist-developer-behind-serbransom-ransomware/ [na engleskom jeziku]

[15] Cimpanu, Catalin, „Osumnjičeni član hakerske grupe *TheDarkOverlord* uhapšen u Srbiji", *Bleeping Computer*, 16. maj 2018. https://www.bleepingcomputer.com/news/security/suspected-member-of-thedarkoverlord-hacking-group-arrested-in-serbia/ [na engleskom jeziku]

[16] Vail, Emma, „Stanovnik Srbije priznao krivicu u multimillionskoj prevari", *The Record*, 8. februar 2022. https://therecord.media/serbian-resident-pleads-guilty-to-multi-million-dollar-bec-scheme [na engleskom jeziku]

[17] Perkov et al., „Digitalna prava u regionu tokom političkih i društvenih nemira", juni 2021, str. 53, https://www.sharefoundation.info/wp-content/uploads/Digital-Rights-Falter-Amid-Political-and-Social-Unrest-Report1.pdf [na engleskom jeziku]

[18] Perkov et al., „Digitalna prava u regionu tokom političkih i društvenih nemira", str. 53.

[19] Šajkaš, Marija, „Dvostruki rizik za novinarke u Srbiji dok napadači ciljaju njihov rad i rod", Komitet za zaštitu novinara, 12. oktobar 2017. https://cpj.org/2017/10/two-fold-risk-for-serbias-women-journalists-as-att/ [na engleskom jeziku]

[20] Bush, Daniel, „'Bori se kao lav za Srbiju': Analiza operacija uticaja povezanih sa vlašću u Srbiji", *Stanford Freeman Spogli Institute for International Studies*, 2. april 2020. https://fsi.stanford.edu/publication/april-2020-serbia-takedown [na engleskom jeziku]

[21] Nimmo, Ben, Margarita Franklin, David Agranovich, Lindsey Hudley i Mike Torrey, „Q4 2022 Kvartalni izveštaj o neprijateljskim pretnjama", *Meta*, Februar 2023. https://about.fb.com/wp-content/uploads/2023/02/Meta-Quarterly-Adversarial-Threat-Report-Q4-2022.pdf [na engleskom jeziku]

[22] Sharife, Khadija, Milica Vojinović i Gur Meggido, „Procureli izveštaj osvetljava izvor misterioznog medijskog napada na političkog rivala srpskog predsednika", *Organized Crime and Corruption Reporting Project*, 24. mart 2023. https://www.occrp.org/en/storykillers/israeli-disinformation-expert-linked-to-faked-bank-accounts-in-serbian-smear-campaign [na engleskom jeziku]

[23] Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto i Sarah McKune, „Ne obraćajte pažnju na server iza proksija: Mapiranje stalne proliferacije *FinFishera*", *The Citizen Lab*, 15. oktobar 2015. https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/ [na engleskom jeziku]; „Hacking Team: 'Italijanski posao' srpskih službi bezbednosti", *SHARE Lab*, 13. juli 2015. https://labs.rs/sr/501/

[24] Marczak, Bill, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis i Ron Deibert, „Trčanje u krug: Otkrivanje klijenata firme za sajber špijunažu *Circles*", *The Citizen Lab*, 1. decembar 2020. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/ [na engleskom jeziku]

[25] Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan i Ron Deibert, „*Pegasus* vs. *Predator*: Dvostruko zaraženi *iPhone* disidenta otkriva plaćenički špijunski softver *Cytrox*", *The Citizen Lab*, 16. decembar 2021. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/ [na engleskom jeziku]

[26] Lecigne, Clement i Christian Resell, „Zaštita korisnika Androida od napada 'nultog dana'", *Google*, Grupa za analizu pretnji, 19. maj 2022. https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/ [na engleskom jeziku]

[27] „Istorija Prajda u Srbiji", *Belgrade Pride 2022 EuroPride*, pristupljeno 11.11.2023. https://europride2022.com/history [na engleskom jeziku]

[28] „Brojna hapšenja u Beogradu posle anti-gej nereda", *BBC*, 10. oktobar 2010. https://www.bbc.com/news/world-europe-11507253 [na engleskom jeziku]

[29] „Vreme je za Evroprajd 2022", *Belgrade Pride 2022 EuroPride*, pristupljeno 11.11.2023. https://europride2022.com/ [na engleskom jeziku]

[30] „Srbija: Vlasti moraju da ukinu 'sramnu' zabranu Evroprajd šetnje", *Amnesty International*, 16. septembar 2022. https://www.amnesty.org/en/latest/news/2022/09/serbia-authorities-must-repeal-shameful-ban-on-euro-pride-walk/ [na engleskom jeziku]

[31] N1 Beograd, „Organizatori: Gotovo 10.000 ljudi u šetnji i borbi za ravnopravnost", *N1 SRB*, 17. septembar 2022. https://n1info.rs/vesti/organizatori-gotovo-10-000-ljudi-u-setnji-i-borbi-za-ravnopravnost/

[32] Kalan, Dariusz, „Kako je intervju sa silovateljem pokrenuo feminstkinje u Srbiji", *Al Jazeera*, 31. mart 2023. https://www.aljazeera.com/features/2023/3/31/how-an-interview-with-a-rapist-fired-up-serbias-feminists [na engleskom jeziku]

[33] Marinović, Nemanja, „Minja Marđonović – Doživela sam digitalno ubistvo", *Zoomer*, 27. novembar 2022. http://zoomer.rs/minja-mardjonovic-dozivela-sam-digitalno-ubistvo/

[34] „Srbija, profil zemlje", *BBC*, poslednja izmena 30. juna 2023. https://www.bbc.com/news/world-europe-17907947 [na engleskom jeziku]

[35] McBride, James, „Uticaj Rusije na Balkanu", *Council on Foreign Relations*, poslednja izmena 2. decembra 2022. https://www.cfr.org/backgrounder/russias-influence-balkans [na engleskom jeziku]

[36] „Srednji prihod", *World Bank Data*, pristupljeno 11.11.2023. https://data.worldbank.org/country/XP [na engleskom jeziku]

[37] „Države članice", *Ujedinjene nacije*, pristupljeno 11.11.2023. https://www.un.org/en/about-us/member-states [na engleskom jeziku]

[38] „46 država članica", *Savet Evrope*, pristupljeno 11.11.2023. https://www.coe.int/en/web/portal/46-members-states [na engleskom jeziku]

[39] „Države učesnice", *OSCE*, pristupljeno 11.11.2023. https://www.osce.org/participating-states [na engleskom jeziku]

[40] „Potpisnici okvirnog dokumenta Partnerstva za mir", Organizacija severnoatlantskog sporazuma, poslednja izmena 27. marta 2020. https://www.nato.int/cps/en/natolive/topics_82584.htm [na engleskom jeziku]

[41] „O nama", Centralnoevropski ugovor o slobodnoj trgovini, pristupljeno 11.11.2023. https://cefta.int/about/ [na engleskom jeziku]

[42] „Članice i posmatrači", Svetska trgovinska organizacija, pristupljeno 11.11.2023. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm [na engleskom jeziku]

[43] „Evropski parlament usvojio izveštaj o napretku Srbije", *Euractiv*, 26. mart 2021. https://www.euractiv.com/section/politics/short_news/european-parliament-adopts-serbias-eu-progress-report/ [na engleskom jeziku]