„DIGITALNI ZATVOR“

NADZOR I REPRESIJA CIVILNOG DRUŠTVA U SRBIJI

REZIME

AMNESTY INTERNATIONAL

Amnesty International je pokret koji broji 10 miliona ljudi, pokreće humanost u svakome i zalaže se za promene kako bismo svi uživali ljudska prava. Naša vizija je svet u kome oni koji su na vlasti drže data obećanja, poštuju međunarodno pravo i pozivaju se na odgovornost. Mi delujemo nezavisno od bilo koje vlade, političke ideologije, ekonomskog interesa ili religije i većinom se finansiramo iz članarina i javnih donacija. Verujemo da solidarnost i empatija sa ljudima širom sveta mogu da učine naša društva boljim.

Prvi put objavio 2024.
Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: EUR 70/8814/2024
Originalni jezik: engleski

amnesty.org

Naslovna fotografija: *Kolaž fotografija Amnesty International-a napravljena korišćenjem fotografija koje smo dobili od Svi Će i Dragana Gmizića*

AMNESTY INTERNATIONAL

REZIME

U februaru 2024. godine, Slaviša Milanov, nezavisni novinar iz Dimitrovgrada u Srbiji koji se bavi temama od lokalnog značaja, priveden je u policijsku stanicu nakon naizgled rutinske saobraćajne kontrole.

Nakon što je pušten, primetio je nešto čudno na svom telefonu, koji je na zahtev policijskih službenika ostavio na prijavnici policijske stanice – podešavanja za podatke i Wi-Fi bila su isključena. Svestan da ovo može biti znak hakovanja, kao i rizika od nadzora kojim su novinari u Srbiji izloženi, Slaviša je kontaktirao Sigurnosnu laboratoriju Amnesty International-a kako bi zatražio analizu svog telefona.

Analiza koju je Amnesty International sproveo dovela je do dva značajna otkrića. Prvo je forenzičkom analizom otkriveno da je korišćen proizvod kompanije Cellebrite za otključavanje uređaja. Cellebrite, koja policijama širom sveta pruža forenzičke alate za ekstrakciju podataka sa uređaja, tvrdi da poseduje stroge politike za sprečavanje zloupotrebe svojih proizvoda. Ipak, ovo otkriće pruža jasne dokaze o targetiranju Slavišinog telefona bez ikakvih zakonom propisanih procedura. Slaviši nije tražena šifra Android uređaja, niti ju je on dao. Vlasti ga nisu obavestile o nameri da pretraže njegov uređaj, niti su navele bilo koju zakonsku osnovu za takvu pretragu. Slaviša i dalje ne zna koji podaci su preuzeti sa njegovog telefona.

Još relevantnije bilo je drugo saznanje do kojeg se analizom došlo. Amnesty International je otkrio tragove do sada nepoznatog špijunskog softvera, pod nazivom 'NoviSpy'. NoviSpy omogućava prikupljanje osetljivih ličnih podataka nakon što se željeni telefon zarazi, kao i daljinsko aktiviranje mikrofona ili kamere. Forenzički dokazi ukazuju na to da je špijunski softver instaliran uz pomoć tehnologije za otključavanje uređaja kompanije Cellebrite dok je srpska policija bila u posedu Slavišinog uređaja. Kombinacija ove dve izuzetno invazivne tehnologije korišćena je za targetiranje uređaja nezavisnog novinara, ostavljajući gotovo ceo njegov digitalni život dostupan srpskim vlastima.

Priča se ne završava sa Slavišom. Dalja istraživanja Amnesty International-a otkrila su šire razmere primene digitalnog nadzora u Srbiji, uključujući upotrebu najmanje tri različita tipa špijunskog softvera, kao i kontinuiranu zloupotrebu visoko sofisticirane digitalne forenzičke tehnologije kompanije Cellebrite.

Ovaj izveštaj predstavlja studiju slučaja o tome kako su srpske vlasti koristile tehnologiju nadzora i taktike digitalne represije kao instrumente šire kontrole i represije države usmerene ka civilnom društvu. Srbija predstavlja paradigmatski primer sistema u kome takvi alati mogu postati ključni faktori digitalne represije, a njihova upotreba se verovatno može odraziti i na druge zemlje i kontekste, što se možda već dešava.

Ovaj izveštaj se objavljuje u trenutku kada se državna represija pojačava, a stanje po pitanju slobode izražavanja i otvorenog dijaloga je u zemlji sve nepovoljnija. Srbija je od 2021. godine doživela nekoliko velikih talasa protesta protiv vlasti, a svaki od njih izazvao je sve oštrije reakcije – od kontinuiranih i nasilnih kampanja protiv kritičnih nevladinih organizacija (NVO), medijskih kuća i novinara, do pravne represije usmerene protiv građana koji se mirno organizuju i učestvuju u političkom nezadovoljstvu.

U ovom izveštaju Amnesty International kombinuje opsežne intervjue sa predstavnicima civilnog društva u Srbiji sa visoko tehničkim digitalno-forenzičkim istraživanjem kako bi se razotkrile konkretne prakse nadzora koje srpske vlasti primenjuju. Otkrivajući ove taktike, izveštaj ima za cilj da osnaži napore civilnog društva da utvrdi odgovornost za sprovođenje nezakonitog nadzora, otkloni slojeve tajni i smanji informacione asimetrije. Netransparentnost digitalnog nadzora uz osećaj omnipotentnosti i nekažnjivosti, može podstaći i osnažiti represivni državni aparat da se upusti u ovakve prakse, s devastirajućim uticajem na stanje čitavog društva.

Nalazi izveštaja otkrivaju sveprisutnu rutinsku upotrebu invazivnog špijunskog softvera u Srbiji, uključujući Pegasus kompanije NSO Group, kao i novi domaći špijunski softver za Android uređaje pod nazivom NoviSpy, koji je prvi put otkriven u ovom izveštaju. Bezbednosno-informativna agencija Srbije, poznata u Srbiji kao BIA,

i srpska policija koristile su NoviSpy i mobilne forenzičke alate kompanije Cellebrite kako bi targetirale nezavisne aktiviste iz think-tank organizacija, mirne demonstrante i nezavisne novinare.

Združeni, ovi alati pružaju državi ogromne mogućnosti za prikupljanje podataka kako potajno, u slučaju špijunskog softvera, tako i otvoreno, kroz nezakonitu i nelegitimnu upotrebu Cellebrite tehnologije za ekstrakciju podataka s mobilnih telefona. Vlasti u Srbiji koriste ove alate sistematski protiv mirnih demonstranata koji su već prečesto zbog svog aktivizma podvrgnuti neopravdanoj kriminalizaciji. Ova nezakonita praksa digitalnog nadzora i prikupljanja podataka usmerena protiv civilnog društva krši ljudsko pravo na privatnost i zaštitu ličnih podataka, i duboko utiču na druga prava i slobode, uključujući pravo na slobodu izražavanja, udruživanja i mirnog okupljanja.

Nalazi u ovom izveštaju zasnovani su na detaljnim intervjuima vođenim sa 13 osoba koja su direktno bila predmet špijunskog softvera ili proizvoda za ekstrakciju podataka sa mobilnih uređaja, kao i 28 predstavnika civilnog društva iz cele Srbije, koji su pružili dragocen uvid u sve izazovnije okruženje u kojem deluju. Njihova svedočenja su potkrepljena detaljnom forenzičkom analizom mobilnih uređaja dvadesetak aktivista i novinara koju je sprovela Sigurnosna laboratorija Amnesty International-a. Sigurnosna laboratorija koristila je digitalne forenzičke alate koje je razvio Amnesty International, uključujući *open-source* alat za verifikaciju mobilnih uređaja (MVT) i AndroidQF, kako bi prikupila i analizirala forenzičke dokaze za potrebe ovog izveštaja.

CIVILNO DRUŠTVO U SRBIJI SUOČAVA SE SA PRETNJAMA ŠPIJUNSKIM SOFTVEROM

Izveštaj pruža detaljan pregled istorijata korišćenja ili nabavke visoko invazivnog špijunskog softvera od strane srpskih vlasti tokom poslednje decenije, uključujući sisteme kompanija Finfisher, NSO Group i Intellexa.

Ono što je veoma važno je činjenica da istraživanje pokazuje da je špijunski softver NoviSpy tajno instaliran na mobilnim uređajima trojice aktivista i jednog nezavisnog novinara tokom informativnih razgovora sa srpskom policijom ili BIA-om. Do zaražavanja je došlo dok su telefoni bili privremeno oduzeti vlasnicima i navodno smešteni u ormariće u policijskim stanicama. Čini se da je ova izuzetno obmanjujuća taktika, tj. tajna instalacija špijunskog softvera na mobilne uređaje tokom informativnih razgovora, široko rasprostranjena. Tehnički dokazi sugerišu da je tokom poslednjih godina na desetine, ako ne i stotine jedinstvenih uređaja targetirano špijunskim softverom NoviSpy. Ukupan obim targetiranja verovatno prevazilazi nezakonito targetiranje civilnog društva.

U oktobru 2024. godine, aktivistica beogradske NVO Krokodil pozvana je u kancelariju BIA da pruži informacije o napadu na ovu organizaciju. Tokom razgovora, njen telefon bio je ostavljen bez nadzora van prostorije za ispitivanje. Naknadna forenzička analiza sprovedena u Sigurnosnoj laboratoriji Amnesty International-a pronašla je dokaze da je upravo tada instaliran špijunski softver NoviSpy za Android uređaje. Iako je manje tehnički napredan od komercijalnih špijunskih softvera kao što je Pegasus, NoviSpy špijunski softver za Android uređaje i dalje srpskim vlastima pruža opsežne mogućnosti nadzora nakon što se instalira na targetirani uređaj. Pored Slaviše i aktivistice iz Krokodila, Amnesty International je pronašao dokaze o instalaciji ili pokušaju instalacije špijunskog softvera NoviSpy na mobilne uređaje još najmanje dvojice aktivista civilnog društva u Srbiji.

U odgovoru na ova saznanja, kompanija NSO Group, koja je razvila Pegasus, nije mogla da potvrdi da li je Srbija njen klijent, ali je navela da „ozbiljno shvataju svoju odgovornost u smislu poštovanja ljudskih prava i da su se snažno obavezali da će izbeći nanošenje, doprinošenje ili direktnu povezanost sa negativnim uticajem na ljudska prava, kao i da će detaljno razmotriti sve kredibilne navode o zloupotrebi proizvoda kompanije NSO Group."

NOVISPY ŠPIJUNSKI SOFTVER POVEZUJE SE SA BEZBEDNOSNO-INFORMACIONOM AGENCIJOM

Analiza nekoliko uzoraka aplikacije špijunskog softvera NoviSpy pronađeni na zaraženim uređajima pokazala je da su svi komunicirali sa serverima u Srbiji, kako bi primali komande i pratili podatke. Zanimljivo je da je jedan od ovih uzoraka špijunskog softvera bio konfigurisan tako da se direktno poveže sa IP adresom koja se direktno dovodi u vezu sa Bezbednosno-informativnom agencijom Srbije. Istraživanje je takođe pokazalo da podaci o konfiguraciji ugrađeni u uzorak špijunskog softvera vode do zaposlenog u BIA-i koji je ranije bio uključen u napore Srbije da nabavi Android špijunski softver od sada već nepostojeće kompanije Hacking Team.

Ovi ozbiljni propusti u operativnoj bezbednosti, kao i činjenica da je u više slučajeva špijunski softver instaliran tokom intervjua sa službenicima BIA-e, omogućavaju Amnesty International-u da sa velikom dozom sigurnosti pripiše ovu upotrebu špijunskih softvera BIA-i i srpskim vlastima.

ZLUPOTREBA DIGITALNIH FORENZIČKIH ALATA KOMPANIJE CELLEBRITE

Ovaj izveštaj takođe otkriva opsežnu i nelegitimnu upotrebu tehnologije za ekstrakciju podataka kompanije Cellebrite u cilju preuzimanja ličnih podataka sa telefona organizatora protesta i novinara. Podaci dobijeni korišćenjem ovakvih alata mogu omogućiti vlastima mapiranje društvenih mreža organizatora protesta, prikupljanje šifrovanih razgovora iz aplikacija kao što su Signal i Telegram, kao i ekstrakciju podataka smeštenih u *cloud*-u. Mogućnost preuzimanja praktično celokupnog digitalnog života pojedinca korišćenjem Cellebrite UFED-a i sličnih mobilnih forenzičkih alata, nosi ogromne rizike po ljudska prava, ako se takvi alati ne podvrgnu strogoj kontroli i nadzoru. Pravni okvir u Srbiji koji se odnose na kontrolu upotrebe ovakvih alata nedovoljan je, a korišćenje Cellebrite forenzičkih proizvoda u Srbiji predstavlja ozbiljan rizik po ljudska prava.

U najmanje dva slučaja koja je Amnesty International dokumentovao, proizvod Cellebrite UFED i povezani *exploit* alati korišćeni su za tajno zaobilaženje sigurnosnih zaštita telefona, omogućavajući srpskim vlastima da zaraze uređaje špijunskim softverom NoviSpy. Ovo tajno zaražavanje, koje se takođe dogodilo tokom razgovora sa policijom ili BIA-om, realizovano je isključivo zahvaljujući mogućnostima koje pruža napredna tehnologija poput Cellebrite UFED za zaobilaženje enkripcije uređaja. Iako su aktivisti već davno izrazili zabrinutost zbog zaražavanja špijunskim softverom tokom policijskih intervjua, Amnesty International smatra da ovaj izveštaj opisuje prva forenzički dokumentovana zaražavanja špijunskim softverom omogućena korišćenjem Cellebrite forenzičke tehnologije za mobilne uređaje.

Ovo istraživanje je takođe otkrilo *„zero-day" exploit* koji omogućava eskalaciju privilegija i koji koristi Cellebrite UFED; tokom ovog istraživanja on je zakrpljen (*pečovan*) što pomaže zaštiti miliona Android uređaja. U saradnji sa istraživačima Google-a koji rade na pitanjima bezbednosti, Amnesty International je identifikovao *exploit* pažljivom analizom forenzičkih logova pronađenih na telefonu jednog organizatora protesta koga su srpske vlasti privele.

REPRESIJA CIVILNOG SEKTORA U SRBIJI

Digitalni nadzor u Srbiji odvija se u kontekstu rastuće represije države i sve nepovoljnijeg stanja slobode izražavanja. Od 2021. godine, zemlja je svedočila brojnim protestima protiv vlasti, pri čemu je svaki od njih naišao na sve oštriju represiju. Nakon masovnih protesta održanih širom zemlje u julu i avgustu 2024. protiv eksploatacije litijuma i sporazuma Srbije sa Evropskom unijom (EU) o pristupu sirovinama, napadi vlasti na civilno društvo značajno su eskalirali. U avgustu, u popularnom režimskom mediju, TV Informer, prikazani su opsežni izveštaji koji sugerišu da oko 40 NVO „finansiranih iz inostranstva" sprovodi „specijalni rat protiv Srbije" po nalogu stranih donatora, opisujući ih kao „strane plaćenike". Klevete izrečene o ovim organizacijama dodatno su podstakli visoki zvaničnici, uključujući predsednika, članove Parlamenta i guvernerku Narodne banke.

Istovremeno, aktivisti koji su učestvovali ili govorili o protestima protiv litijuma suočavali su se sa hapšenjima i neutemeljenim ali veoma ozbiljnim krivičnim optužbama, uključujući „podsticanje nasilnog rušenja ustavnog poretka", krivično delo za koje je predviđena kazna do osam godina zatvora. Aktivisti i advokati intervjuisani za potrebe ovog izveštaja ispričali su da je policija često navodila objave aktivista na društvenim mrežama, njihove govore ili prosto učešće na protestima kao osnov za ove optužbe. Tokom protesta održanih u avgustu, najmanje 33 osoba je uhapšeno ili zadržano na informativnim razgovorima, tokom kojih su bila podvrgnuta dugotrajnim ispitivanjima, izvršen je pretres stanova, a telefoni i računari su oduzeti radi pretrage. U trenutku objavljivanja ovog izveštaja, niko od njih nije zvanično optužen.

Amnesty International je razgovarao sa devet aktivista koji su bili zadržani ili ispitivani u periodu između jula i novembra 2024. godine, čiji su telefoni i računari privremeno oduzeti od strane policije i podvrgnuti detaljnim pretragama, uključujući ekstrakciju digitalnih podataka kako bi se omogućilo tužiocima da odluče da li će ih formalno optužiti ili ne. Aktivisti sumnjaju da su ove intruzivne istražne mere, koje se čine legitimnim prema srpskom zakonodavstvu, bile pre izgovor za policiju i obaveštajne službe da saznaju više o njihovim društvenim mrežama i budućim planovima, nego namera da se bave krivičnim gonjenjem.

NEADEKVATAN PRAVNI I KONTROLNI OKVIR DIGITALNOG NADZORA U SRBIJI

Zakonodavstvo Srbije predviđa upotrebu posebnih mera, uključujući tajni nadzor komunikacija i definiše specifične okolnosti pod kojima se ovakve mere mogu zakonito primenjivati. Međutim, upotreba modernih tehnologija, uključujući špijunski softver i druge napredne forenzičke alate koji prikupljaju velike količine ličnih

podataka, nije potpuno prepoznata niti dovoljno regulisana zakonom, ostavljajući previše prostora za potencijalnu zloupotrebu ovakvih tehnika, uključujući i u političke svrhe.

Generičke odredbe sadržane u različitim zakonima koje regulišu primenu posebnih mera nisu dovoljno jasne, niti pružaju suštinsku zaštitu od zloupotrebe kada je reč o tehnologijama digitalnog nadzora, koje su znatno invazivniije i manje ciljane od konvencionalnih sredstava tajnog nadzora komunikacija, poput prisluškivanja. Čak ni mehanizam sudskog *ex-ante* nadzora, kao što je sudska odluka koja precizira mere, striktni vremenski okvir i predmet nadzora, ne može pružiti efikasnu zaštitu protiv modernih digitalnih alata za nadzor, uključujući špijunski softver, koji mogu dobiti sveobuhvatan i nekontrolisan pristup podacima, porukama, slikama, fajlovima i metapodacima na uređaju.

Pored toga, u kontekstu često izražavanih zabrinutosti o neprimerenom političkom uticaju vlasti na sudove i tužioce, kao i o stepenu zarobljavanja države u Srbiji, sredstva kontrole i nadzora nad upotrebom posebnih mera, koja na papiru mogu delovati dovoljna, u praksi postaju besmislena ili neefikasna.

Vlada Srbije nije dala komentar na saznanja sadržana u izveštaju, koja su im dostavljena pre njegovog objavljivanja.

EFEKAT ZASTRAŠIVANJA

Digitalni nadzor ne samo da ima devastirajući uticaj na pravo na privatnost, već u velikoj meri utiče i na prava na slobodu izražavanja, udruživanja i mirnog okupljanja. Aktivisti u Srbiji izjavili su za Amnesty International kako je saznanje da su bili targetirani učinilo da se osećaju povređeno, ranjivo i usamljeno, te ih primoralo da preispitaju ili promene svoje ponašanje. Neki su postali oprezniji kada je reč o javnom izražavanju o spornim pitanjima, dok su drugi odlučili da manje istupaju ili u potpunosti prekinu sa aktivizmom.

Nakon što je saznao da je bio targetiran, Slavišu je veoma zabrinula činjenica da bi neki od njegovih izvora mogli biti kompromitovani, te je bio primoran da promeni način na koji istražuje za svoje članke i komunicira sa izvorima:

„Više ne smem da koristim telefon ili email; primoran sam da pronađem druge načine komunikacije sa ljudima, uključujući, kontakte uživo. To praktikujem isključivo kada smo na javnim mestima i u većim grupama, što, naravno, nije idealno."

„Goran" je još jedan od aktivista targetiranih pomoću Pegasusa koje je Amnesty International intervjuisao. Napad ga je primorao da u velikoj meri preispita svoj dalji rad.

„To me je navelo da preispitam svoje angažovanje u organizaciji. Pitao sam se da li treba da nastavim da radim, kako to utiče na organizaciju i razmišljao sam o povlačenju. Napad poput ovoga zaista duboko dotiče lični integritet i stav prema radu i natera vas da se zapitate da li ste, uprkos svemu, spremni da nastavite da radite ono što radite. Imao sam stotine pitanja."

„Goran" je ostao u organizaciji, ali je bio primoran da uvede brojne mere bezbednosti kako u svom privatnom životu, tako i u organizaciji.

„Ako vlast može da uradi ono što su uradili meni, to znači da sledeći put mogu da targetiraju nekog drugog. Shvatio sam da su aktivnosti svih organizacija civilnog društva pod stalnim nadzorom vlasti i da moramo biti oprezni."

Za organizacije koje su već pod različitim pritiscima, suočavanje s pitanjima digitalne sigurnosti predstavlja još jedan oblik udaljavanja od njihove osnovne delatnosti, kazao je aktivista Krokodila Amnesty International-u

„Istovremeno suočavanje s velikim brojem različitih napada u velikoj meri nas okupira i na taj način nas suštinski slabi do tačke da nećemo moći da funkcionišemo... To je verovatno cilj."

ODGOVORNOST KOMPANIJA I DRUGIH AKTERA ZA LJUDSKA PRAVA

Države imaju primarnu dužnost da poštuju zakon o ljudskim pravima, ali i kompanije i drugi subjekti imaju odgovornost da poštuju ljudska prava gde god da deluju u svetu, kao i u svim svojim poslovnim aktivnostima. Ključni segment ispunjavanja ove odgovornosti je adekvatna primena dubinske analize ljudskih prava, kako bi se identifikovali, sprečili i ublažili potencijalni rizici po ljudska prava na koje kompanije mogu uticati. Amnesty International je otkrio da je nekoliko kompanija u Srbiji propustilo da ispuni svoje obaveze u tom smislu.

Pored toga, Ministarstvo spoljnih poslova Norveške, koje je doniralo tehnologiju Cellebrite UFED i Kancelarija Ujedinjenih nacija za projektne usluge (UNOPS), koja je bila zadužena za nabavku za koju su korišćena sredstva norveškog granta za potrebe Ministarstva unutrašnjih poslova, nisu sproveli adekvatnu dubinsku analizu kako bi procenili i ublažili potencijalne rizike ove tehnologije po ljudska prava, niti su obezbedili mere zaštite protiv njene zloupotrebe. S obzirom na slabo regulisanu oblast digitalnog nadzora u Srbiji, zabrinutost za nezavisnost pravosuđa i stalna izveštavanja o pretnjama civilnom društvu i nezavisnim novinarima, norveška vlada i UNOPS imali su obavezu da vrše nadzor i sprovedu dubinsku analizu prilikom nabavke visoko invazivne tehnologije i njenog prenosa srpskim institucijama. Ovakvim propustom omogućeno je i doprinelo se kršenju ljudskih prava na privatnost, slobodu izražavanja, udruživanje i mirno okupljanje primenom nezakonitog digitalnog nadzora.

U odgovoru na saznanja do kojih se došlo u izveštaju, Ministarstvo spoljnih poslova Norveške navodi da smatra da je „zabrinjavajuća mogućnost da su digitalni forenzički alati, nabavljeni preko projekta koji je finansirala Norveška zloupotrebljeni za targetiranje predstavnika civilnog društva u Srbiji“, i dodaje da „ukoliko bi ovi navodi bili tačni, [to] bi predstavljalo očigledno kršenje principa norveške razvojne pomoći, kao i dogovorene svrhe podrške pružene srpskim vlastima u tom trenutku“. Ministarstvo je dodalo da se očekuje da će UNOPS, koji je bio odgovoran za sve projektne aktivnosti, sprovesti temeljnu istragu navodnih zloupotreba.

Jednako je važna činjenica da je kompanija Cellebrite imala obavezu da sprovede dubinsku analizu u oblasti ljudskih prava kako bi osigurala da njen proizvod niti uzrokuje niti doprinosi negativnim uticajima na ljudska prava. Na svojoj internet stranici, Cellebrite ističe da će „preduzeti sve potrebne mere da zabrani zlonamernim akterima korišćenje ili pristup“ svojim rešenjima kada se tehnologija Cellebrite „koristi na način koji nije u skladu sa međunarodnim pravom, kada se ne poštuju uslovi korišćenja ili se krše korporativne vrednosti ove kompanije.“ Međutim, sve do danas dostupne informacije ukazuju na to da Cellebrite nije preduzela dovoljne i efikasne mere da upotrebi svoj uticaj za rešavanje rizika po ljudska prava u Srbiji. Kako istraživanje Amnesty International-a pokazuje, upotreba proizvoda kompanije Cellebrite imala je negativan uticaj na ljudska prava srpskih aktivista i novinara. U najmanju ruku, kompanija Cellebrite je direktno povezana sa ovim konkretnim kršenjima ljudskih prava.

Prema Vodećim principima o poslovanju i ljudskim pravima Ujedinjenih nacija, kompanija Cellebrite nije ispunila svoju korporativnu odgovornost u smislu ublažavanja ili sprečavanja potencijalne i stvarne štete po branioce ljudskih prava, te su s toga potrebne efikasnije politike i procedure u ovoj oblasti. U situacijama kada je kompanija doprinela stvarnim negativnim efektima, trebalo bi da obezbedi reparaciju pogođenim pojedincima.

Kao odgovor na upit koji je Amnesty International poslao tokom procesa istraživanja, Cellebrite je odgovorio da oni nisu kompanija za nadzor i da ne obezbeđuju niti tehnologiju za sajber nadzor niti špijunske softvere. Navode da je njihov proizvod „digitalna forenzička platforma [koja] oprema agencije koje se bave sprovođenjem zakona tehnologijom potrebnom za zaštitu i spašavanje života, ubrzavanje pravde i zaštitu privatnosti podataka“, te da su njihovi proizvodi „licencirani isključivo za zakonitu upotrebu, zahtevaju nalog ili pristanak kako bi pomogli agencijama za sprovođenje zakona u zakonitim istragama nakon što se zločin dogodi.“

Pre objavljivanja, Amnesty International je podelio nalaze ovog izveštaja sa Cellebrite-om. U odgovoru, Cellebrite je naveo: „Naša digitalna softverska rešenja za istrage ne instaliraju špijunski softver niti vrše nadzor u realnom vremenu kao što to rade špijunski softveri ili bila koja druga vrsta invazionih sajber aktivnosti.

„Cenimo Amnesty International što ističe navodnu zloupotrebu naše tehnologije. Ozbiljno shvatamo sve navode o potencijalnoj zloupotrebi naše tehnologije od strane korisnika na načine koji bi bili u suprotnosti sa eksplicitnim i impliciranim uslovima navedenim u našem ugovoru sa krajnjim korisnikom.“

„Istražujemo tvrdnje iznesene u ovom izveštaju. Ako budu potvrđene, spremni smo da uvedemo odgovarajuće sankcije, uključujući prekid veze Cellebrite-a sa svim relevantnim agencijama.“

ZAKLJUČAK I PREPORUKE

Nalazi ovog izveštaja su emblematični i prikazuju kakao represivni državni aparat kombinuje različite prakse nadzora za postizanje svojih ciljeva. Izveštaj takođe ukazuje na nove taktike nadzora, uključujući široku upotrebu invazivnih digitalno-forenzičkih alata za prikupljanje podataka od mirnih protestanata koji nisu optuženi za bilo kakvo krivično delo. S obzirom da jačanje bezbednosti čini *zero-click* i druge napade špijunskim softverima na daljinu preskupim ili neizvodljivim, vlasti će se sve više oslanjati na zaražavanje uređaja špijunskim softverom putem fizičkog pristupa tim uređajima. Neke države su čak predložile posebne propise kojima bi se dozvolile tajne provale u kuće zarad zaražavanja uređaja ciljanim špijunskim softverima.

Srbija mora da se obaveže da će odmah prestati sa upotrebom visoko invazivnog špijunskog softvera i sprovesti hitnu, nezavisnu i nepristrasnu istragu o svim dokumentovanim i prijavljenim slučajevima nezakonitog digitalnog nadzora. Potrebno je i da preduzme konkretne korake kako bi osigurala da se digitalne tehnologije ne zloupotrebljavaju za kršenje ljudskih prava, što podrazumeva uspostavljanje i striktno sprovođenje pravnog okvira koji pruža smislenu proceduralnu zaštitu, efikasne sisteme kontrole i nadzora kroz sudsko preispitivanje, kao i delotvorne mehanizme za reparaciju žrtvama.

Cellebrite i druge kompanije za digitalnu forenziku koje razvijaju i obezbeđuju visoko invazivne tehnologije policiji i bezbednosnim agencijama u obavezi su da sprovedu suštinske i dubinske analize kako bi osigurali da njihovi proizvodi ne doprinose kršenju ljudskih prava. Cellebrite bi trebalo da istraži kako je njena tehnologija korišćena u Srbiji kako bi procenila moguće negativne uticaje na ljudska prava i da deluje u skladu sa svojom obavezom da „preduzme sve potrebne mere“, uključujući neobnavljanje svojih licenci, kako bi zabranila zlonamernim akterima korišćenje ili pristup svojim rešenjima na način koji nije u skladu sa međunarodnim pravom.

Celokupan spisak preporuka dat je na kraju izveštaja.

AMNESTY INTERNATIONAL JE GLOBALNI POKRET ZA LJUDSKA PRAVA. KADA SE NEPRAVDA DESI JEDNOJ OSOBI TO SE TIČE SVIH NAS.

CONTACT US

info@amnesty.org

+44 (0)20 7413 5500

JOIN THE CONVERSATION

www.facebook.com/AmnestyGlobal

@Amnesty

„DIGITALNI ZATVOR“

NADZOR I REPRESIJA CIVILNOG DRUŠTVA U SRBIJI

REZIME

Ovaj izveštaj dokumentuje kako su vlasti u Srbiji koristile tehnologiju nadzora i taktike digitalne represije kao instrument šire kontrole države i represije usmerene na civilno društvo. Nalazi izveštaja otkrivaju sveprisutnu i rutinsku upotrebu invazivnog špijunskog softvera, uključujući i Pegasus špijunski softver kompanije NSO Group, zajedno sa novim domaćim sistemom špijunskog softvera NoviSpy za Android uređaje, koji je prvi put otkriven u ovom izveštaju. Izveštaj ističe široko rasprostranjenu zloupotrebu mobilnog forenzičkog alata UFED kompanije Cellebrite usmerenu protiv aktivista za zaštitu životne sredine i vođa protesta u Srbiji.

INDEX: EUR 70/8814/2024
DECEMBER 2024
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL