Posebno tužilaštvo za visokotehnološki kriminal

Savska 17a, Beograd

KRIVIČNA PRIJAVA

protiv:

N.N. ovlašćenih lica iz Bezbednosno-informativne agencije i policije

zbog postojanja osnova sumnje da su:

tokom 2023. i 2024. godine na nekoliko različitih lokacija u policijskim stanicama i prostorijama BIA

napravili računarski virus u nameri njegovog unošenja u tuđ računar ili računarsku mrežu, uneli računarski virus u tuđ računar ili računarsku mrežu i time prouzrokovali štetu, i kršeći mere zaštite, neovlašćeno se uključili u računar ili računarsku mrežu, ili neovlašćeno pristupili elektronskoj obradi podataka,

- čime je izvršeno krivično delo **Neovlašćeno prikupljanje ličnih podataka iz člana 146 stav 2**, krivično delo **Pravljenje i unošenje računarskih virusa iz člana 300 stav 1 i stav 2** i krivično delo **Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka iz člana 302 stav 1** Krivičnog zakonika i/ili neko drugo krivično delo za koje se gonjenje preduzima po službenoj dužnosti ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 i 94/2024)

O b r a z l o ž e nj e

Dana 16.12.2024. godine nezavisna međunarodna organizacija Amnesty International objavila je izveštaj pod nazivom **"Digitalni zatvor: Prismotra i gušenje civilnog društva u Srbiji"** u kome su izneti dokazi da su policija i pripadnici BIA napravili računarski virus (špijunski softver), koji je u pomenutom izveštaju imenovan NoviSpy, te su isti uneli u najmanje četiri zaštićena računarska sistema (pametna telefona) aktivista, novinara i članova civilnog društva. Za ostvarivanje neovlašćenog pristupa zaštićenim računarskim sistemima pripadnici MUP i BIA zloupotrebili su hardversko - softversko rešenje "Cellebrite UFED".

Dokaz: Izveštaj Amnesty International **"Digitalni zatvor: Prismotra i gušenje civilnog društva u Srbiji"** dostupan na sledećem linku: https://www.amnesty.org/en/documents/eur70/8813/2024/en/

Stručnjaci za digitalnu forenziku su analizom uređaja građana Srbije direktno pogođenih korišćenjem intruzivnih tehnologija, **pouzdano utvrdili** da su policija i BIA rutinski koristili novi tip špijunskog softvera koji Amnesty International naziva NoviSpy, uz zloupotrebu visoko sofisticiranog alata za digitalnu forenziku izraelske kompanije Cellebrite.

Mobilni uređaji pripadnika civilnog društva, novinara i aktivista bili su zaraženi špijunskim softverom prilikom informativnih razgovora, privođenja ili boravka u prostorijama policije i BIA, kada su njihovi uređaji bili oduzimani ili van njihovog domašaja. Nakon što bi telefon uzeli pripadnici policije i BIA, koristili su Cellebrite UFED kako bi prisilno otključali telefon i sa njega preuzeli podatke, a potom direktnim pristupom instalirali špijunski softver NoviSpy. Prema nalazima forenzičara organizacije Amnesty International, NoviSpy može da pravi skrinšotove i sa telefona ih šalje na server BIA, ali i da ostvari dozvole za pristup lokaciji, mikrofonu i kameri.

Prema Krivičnom zakoniku, posedovanje, distribucija i upotreba špijunskih softvera, kao vrste računarskih virusa, predstavlja krivično delo. Takođe, svaki neovlašćeni pristup zaštićenim uređajima i podacima je kriminalizovan. Špijunski softver je tip zlonamernog softvera koji ima za cilj da prikupi informacije o osobi ili organizaciji i pošalje ih drugom entitetu na način koji šteti korisniku – na primer, ugrožavanjem njegove privatnosti ili ugrožavanjem bezbednosti njegovog uređaja. Samim tim, nelegalnost upotrebe špijunskih softvera je dvostruka. Najpre, prema važećem Krivičnom zakoniku računarski virusi predstavljaju računarske programe ili skupove naredbi koji deluju na druge programe ili podatke u računaru ili računarskoj mreži. S obzirom na to da špijunski softver deluje na podatke i programe na zaraženim uređajima, on se može klasifikovati kao specifična vrsta računarskog virusa. Međutim, ono što ga čini dodatno opasnim jeste njegova funkcija špijuniranja korisnika. Osim što je nelegalno instalirati špijunski softver na uređaj, njegova upotreba podrazumeva neovlašćeni pristup svim podacima na uređaju, čime se namerno nanosi šteta targetiranim korisnicima, ali i svim drugim osobama čiji se podaci nalaze na tom uređaju. Na taj način direktno se narušava pravo na privatnost i zaštitu podataka o ličnosti.

Izveštaj organizacije Amnesty International daje čvrste dokaze o nezakonitom korišćenju sofisticiranih tehnologija za špijuniranje novinara, aktivista i građana. U nastavku navodimo sledeće događaje:

Novinar Slaviša Milanov

U februaru 2024. godine, Slaviša Milanov, nezavisni novinar iz Dimitrovgrada priveden je u policijsku stanicu nakon naizgled rutinske saobraćajne kontrole. Nakon što je pušten, primetio je da su podešavanja za podatke i Wi-Fi bila isključena na telefonu, koji je na zahtev policijskih službenika ostavio na prijavnici policijske stanice. Svestan da ovo može biti znak neovlašćenog pristupa, kao i rizika od nadzora kojim su novinari u Srbiji izloženi, Milanov je kontaktirao Bezbednosnu laboratoriju Amnesty Internationala 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. Ova kompanija 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 telefona Slaviše Milanova bez ikakvih zakonom propisanih procedura. Milanovu nije tražena lozinka Android uređaja, niti je on lozinku dao. Milanov takođe nije obavešten o nameri da se njegov uređaj istraži, niti je naveden bilo koji zakonski osnov za takvu istragu. Milanov i dalje ne zna koji podaci su preuzeti sa njegovog telefona.

Još relevantnije bilo je drugo saznanje do kojeg se došlo analizom. Amnesty International je otkrio tragove do sada nepoznatog špijunskog softvera, koji je za potrebe izveštaja nazvan “NoviSpy”. NoviSpy omogućava prikupljanje osetljivih ličnih podataka nakon što se ciljani 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 su pripadnici policije bili u posedu uređaja Slaviše Milanova. Kombinacija ove dve izuzetno invazivne tehnologije korišćena je za targetiranje uređaja nezavisnog novinara, ostavljajući gotovo ceo njegov digitalni život dostupan.

Ovi navodi potkrepljeni su sledećim dokazima:

Izvorna tabela data je u izveštaju organizacije Amnesty International **“Digitalni zatvor: Prismotra i gušenje civilnog društva u Srbiji”**, na strani 33:

Lokalno vreme	Događaj
2024-02-21 11:10 (približno)	Telefon Slaviše Milanova ostavljen je bez nadzora tokom razgovora sa organima vlasti Republike Srbije.
2024-02-21 11:56:07	Xiaomi aplikaciji za upravljanje datotekama je odobrena dozvola za instaliranje Android APK paketa.
2024-02-21 11:56:09	Aplikacija za instalaciju Android paketa se otvara da bi se instalirala Android aplikacija.
2024-02-21 12:01:32	Android opcija ACCESS_RESTRICTED_SETTINGS je izmenjena da bi se omogućilo dozvoljavanje aplikacija usluge pristupačnosti za Android. Ovo je neophodno da bi se omogućila funkcionalnost špijunskog softvera NoviSpy.
2024-02-21 12:16:10	Drugi Android paket instaliran preko aplikacije za instalaciju Android paketa.
2024-02-21 12:40:18	Zabeležena komunikacija NoviSpy špijunske aplikacije **com.accesibilityservice** sa špijunskim serverom na IP adresi **195.178.51.251**.
2024-02-21 13:27	Organi vlasti su u ovom trenutku vratili telefon Milanovu.
2024-02-26 09:24	Milanov je uklonio **com.accesibilityservice** NoviSpyAccess špijunsku aplikaciju koristeći bezbednosnu aplikaciju za Android.
2024-02-26 09:26	**com.serv.services** NoviSpyAdmin špijunska aplikacija uklonjena sa telefona.

Prevod na srpski jezik, Tabela 5: Forenzički tragovi špijunske aplikacije NoviSpy na telefonu Slaviše Milanova

Dana 19.03.2024. godine Slaviša Milanov je Posebnom odeljenju za visokotehnološki kriminal Višeg javnog tužilaštva u Beogradu, podneo krivičnu prijavu, zavedenu pod brojem KTN VTK 1097/24. Takođe, Milanov se, preko punomoćnika, 21.03.2024. godine obratio Sektoru unutrašnje kontrole MUP-a.

Aktivista Nikola Ristić

U novembru 2024. godine, Amnesty International je forenzički analizirao telefon aktiviste Nikole Ristića. Ova analiza je potvrdila drugi slučaj osobe čiji je uređaj otključan pomoću Cellebrite alata i zaražen “NoviSpy” softverom dok je bio u posedu službenika policije.

Nikola Ristić je bio jedan od ključnih organizatora protesta u Beogradu nakon tragičnog incidenta u Novom Sadu u novembru, kada je urušena nadstrešnica na gradskoj železničkoj stanici.

Dana 3. novembra, Ristić i njegov kolega su stigli na Trg Republike oko 10:00h, dva sata pre zakazanog protesta. Nedugo zatim, zaustavila su ih četvorica muškaraca koji su se predstavili kao pripadnici BIA-e i zatražili od Ristića da ih prati u policijsku stanicu radi informativnog razgovora. Ristić je isprva odbio, jer službenici nisu imali bilo kakav nalog, ali je zatim pristao da pođe.

U policijskoj stanici, Nikola Ristić je zamoljen da isprazni džepove, a službenici su sve njegove stvari, uključujući telefon, stavili u plastičnu kesu i rekli da će mu ih vratiti nakon razgovora. Čim je pušten, Ristić je posumnjao da je došlo do neovlašćenog pristupa njegovom uređaju nakon čega je kontaktirao Bezbednosnu laboratoriju organizacije Amnesty International.

Forenzički tragovi pokazuju da je telefon Nikole Ristića takođe zaražen špijunskim softverom NoviSpy putem fizičkog pristupa uređaju tokom saslušanja. Analiza je pokazala da je telefon bio povezan sa računarom pomoću Android ADB protokola, a promene su ponovo izvršene na uređaju kako bi se izbeglo otkrivanje, uključujući onemogućavanje ažuriranja bezbednosti uređaja i zaštite Google Play Protect.

Telefon je i dalje bio aktivno zaražen špijunskim softverom NoviSpy u trenutku analize, nedelju dana nakon inicijalne infekcije. Dokazi izvučeni sa uređaja pokazuju da su operateri špijunskog softvera 5. novembra 2024. ponovo konfigurisali infekciju, naređujući softveru NoviSpy da šalje podatke na server svakih 3 minuta (180 sekundi) umesto podrazumevanih 30 sekundi, što ukazuje na to da su operateri aktivno upravljali zaraženim uređajem.

Forenzički tragovi ukazuju na to da je alat Cellebrite ponovo korišćen za eksploataciju telefona pre instalacije špijunskog softvera. Dokazi o upotrebi Cellebrite za ovaj slučaj dokumentovani su u odeljku 5.2.2. pomenutog izveštaja.

Ovi navodi potkrepljeni su sledećim dokazima:

Izvorna tabela iz izveštaja, Amnesty International **“Digitalni zatvor: Prismotra i gušenje civilnog društva u Srbiji”**, strana 34:

Lokalno vreme	**Događaj**
2024-11-02 01:56	Telefon uključen.
2024-11-03 10:00 (približno)	Pripadnici BIA odvode Nikolu Ristića u policijsku stanicu.
2024-11-03 10:48:44	Greška procesa povezana sa eksploatacijom putem Cellebrite UFED; logovi izbrisani.
2024-11-03 11:39:19	Bezbednosno obaveštenje u aplikaciji Podešavanja.
2024-11-03 11:40:29	Instalacija špijunske aplikacije NoviSpy **com.serv.services**
2024-11-03 11:42:05	Instalacija špijunske aplikacije NoviSpy **com.accesibilityservice**
2024-11-03 12:12:39	Huawei aplikacija za upravljanje datotekama omogućava pristup eksternoj memoriji.
2024-11-03 13:30 (približno)	Nikolu Ristića pušta BIA.
2024-11-05 09:08:01	Novi interval NoviSpy aploudovanja (opcija „UIR“) je promenjen sa 30 sekundi na 180 sekundi.

Prevod, Tabela 6: Tragovi instaliranja špijunskog softvera NoviSpy na telefonu Nikole Ristića

Aktivista Ivan Bjelić

Ivan Bjelić, ekološki aktivista i slobodni novinar, redovno je bio pod pojačanim nadzorom policije zbog svog učešća u nenasilnim kampanjama građanske neposlušnosti. Dana 17. decembra 2023. godine, Bjelić je zaustavljen tokom putovanja autobusom ka Beogradu i odveden u zgradu Ministarstva unutrašnjih poslova u Beogradu, gde su ga ispitivali službenici policije i pripadnici BIA. Hapšenje se dogodilo istog dana kada su održani sporni opšti i lokalni izbori, što je izazvalo masovne antivladine proteste. Tokom nekoliko sati provedenih u policijskoj stanici, službenici su Ivanu Bjeliću pokazali formalni nalog na osnovu kog su ga primorali da otkrije svoj PIN kod i otključa telefon, Xiaomi Mi 10T Pro.

Bjelićev uređaj je zadržan dok je on bio ispitivan u drugoj prostoriji. Nakon konstatacije službenika da nisu pronašli ništa inkriminišuće, tj. nikakve dokaze ili naznake da je bio umešan u pokušaje „nasilnog rušenja ustavnog poretka“ ili akte terorizma, zbog čega je bio priveden, Bjelić je pušten.

Amnesty International je forenzički pregledao Bjelićev telefon nakon njegovog puštanja i identifikovao dokaze koji potvrđuju da je korišćen forenzički alat UFED kompanije Cellebrite što je službenicima omogućilo da izvuku sve podatke sa njegovog telefona.

Ovi navodi potkrepljeni su sledećim dokazima:

Izvorna tabela iz izveštaja, Amnesty International **“Digitalni zatvor: Prismotra i gušenje civilnog društva u Srbiji”**, strana 78:

Naziv fajla	**SHA 256 heš vrednost**
falcon	3621ffeb67efa3eccb9c1f20cd671b81b286a02425e582a8a1553e85b012403d
nandread	3936a6ec20405990802f59ea2747a1685886bab4f5949d258e84e4646006a4c1
nandshell	556a409603f56ed6e4a833da37263134ca00469970516634e845dccee080ad3c

Prevod, Tabela 11: Binarni fajlovi pronađeni na telefonu Ivana Bjelića

Amnesty International povezuje “falcon” binarni fajl sa Cellebrite UFED proizvodom (Amnesty International **“Digitalni zatvor: Prismotra i gušenje civilnog društva u Srbiji”**, strana 78).

Forenzički logovi (kernel crash logs) sa Bjelićevog telefona ukazuju na to da je proces “falcon” bio pokrenut.

Izvorna tabela iz izveštaja, Amnesty International **“Digitalni zatvor: Prismotra i gušenje civilnog društva u Srbiji”**, strana 80:

```
2023-12-17 17:56:45.574680: Process falcon (pid: 10050, stack limit = 0x00000000eac9e565)
2023-12-17 17:56:45.574700: CPU: 0 PID: 10050 Comm: falcon Tainted: G S O 4.19.157-perf-
g8779875ad741 #1
2023-12-17 17:56:45.574711: Hardware name: Qualcomm Technologies, Inc. xiaomi apollo (DT)
2023-12-17 17:56:45.574726: pstate: 00400005 (nzcv daif +PAN -UAO)
```

```
2023-12-17 17:56:45.574756: pc : pipe_read+0xac/0x308
2023-12-17 17:56:45.574769: lr : pipe_read+0x4c/0x308
2023-12-17 17:56:45.574778: sp : ffffff802e43bc80
2023-12-17 17:56:45.574787: x29: ffffff802e43bcf0 x28: fffffff4ce02c400
2023-12-17 17:56:45.574800: x27: fffffff4ce02c410 x26: 00000000000003ff
2023-12-17 17:56:45.574813: x25: 0000000000000028 x24: 00000000000003ff
2023-12-17 17:56:45.574826: x23: fffffff506d57620 x22: fffffff506d57600
2023-12-17 17:56:45.574839: x21: fffffff4ce02c400 x20: 0000000000000000
2023-12-17 17:56:45.574852: x19: fffffff4ce02c40c x18: 0000000000000000
2023-12-17 17:56:45.574864: x17: 0000000000000000 x16: 0000000000000000
2023-12-17 17:56:45.574877: x15: 0000000000000000 x14: 0000000000000000
2023-12-17 17:56:45.574890: x13: 0000000000000000 x12: 0000000000000000
2023-12-17 17:56:45.574903: x11: 0000000000000000 x10: 0000000000000000
2023-12-17 17:56:45.574916: x9 : 0000000000000001 x8 : 00000000dead0000
2023-12-17 17:56:45.574930: x7 : ffffffff00000000 x6 : 0000000000000002
2023-12-17 17:56:45.574942: x5 : 0000000000000000 x4 : 00000000000003ff
2023-12-17 17:56:45.574954: x3 : 0000000000000001 x2 : ffffff802e43bda8
2023-12-17 17:56:45.574967: x1 : fffffff4ce02c400 x0 : fffffff506d57600
2023-12-17 17:56:45.574982: Call trace:
2023-12-17 17:56:45.574996: pipe_read+0xac/0x308
2023-12-17 17:56:45.575014: __vfs_read+0xf8/0x140
2023-12-17 17:56:45.575027: vfs_read+0xb8/0x150
2023-12-17 17:56:45.575039: ksys_read+0x6c/0xd0
2023-12-17 17:56:45.575053: __arm64_sys_read+0x18/0x20
2023-12-17 17:56:45.575071: el0_svc_common+0x98/0x160
2023-12-17 17:56:45.575083: el0_svc_handler+0x68/0x80
2023-12-17 17:56:45.575097: el0_svc+0x8/0xc
2023-12-17 17:56:45.575114: Code: aa1c03fb aa1c03e1 b840ce68 f8410f69 (f9400529)
2023-12-17 17:56:45.575127: ---[ end trace 72c08623f6dedcd7 ]---
2023-12-17 17:56:45.575174: Kernel panic - not syncing: Fatal exception
```

Prevod, Tabela 13: Log sa greškom “falcon” binarnog fajla

Aktivista iz Udruženja Krokodil

U oktobru 2024. godine, aktivista nevladine organizacije **Udruženje Krokodil** odlazi po sopstvenom zahtevu na sastanak sa **BIA** kako bi pružio informacije o napadu na kancelariju njihove organizacije. Tokom sastanka, njegov telefon je ostao bez nadzora ispred prostorije za razgovor. Naknadna forenzička analiza telefona koju je sprovela **Bezbednosna laboratorija Amnesty Internationala** pronašla je dokaze da je u tom periodu na uređaj instaliran špijunski softver **NoviSpy**.

Ovi navodi potkrepljeni su sledećim dokazima:

Izvodi iz NoviSpy aplikacije, izveštaj Amnesty International **“Digitalni zatvor: Prismotra i gušenje civilnog društva u Srbiji”,** strane 30-31:

Lokalno vreme	**Događaj**
2024-10-01 10:17 (približno)	Počinje policijski razgovor. Telefon ostavljen bez nadzora.
2024-10-01 10:20:45	Telefon je uključen.
2024-10-01 10:24:03	USB kabl povezan.
2024-10-01 10:24:23	Android režim za programere je uključen.
2024-10-01 10:25:54	Google Play Protect zaštita je isključena preko ADB (Android Debug Bridge).
2024-10-01 10:25:55	Instalacija špijunske aplikacije **com.serv.services.**
2024-10-01 10:27:04	Instalacija špijunske aplikacije **com.accesibilityservice.**
2024-10-01 10:27:05	**com.accesibilityservice** je omogućen kao usluga pristupačnosti preko ADB.
2024-10-01 10:31:17	Android režim za programere je isključen.
2024-10-01 10:31:17	Automatska bezbednosna ažuriranja sistema su onemogućena.
2024-10-01 10:38	Sačuvani kontakti preuzeti sa telefona.
2024-10-01 10:39:51	Telefon isključen sa USB kabla.
2024-10-01 11:40 (približno)	Završen policijski razgovor sa aktivistom.
2024-10-01 12:32	Aktivista identifikuje notifikaciju o izvezenim kontaktima i pravi snimak ekrana.

Prevod, Tabela 3: Forenzički tragovi pokazuju instalaciju spajvera

Snimak ekrana notifikacije o izvezenim kontaktima aktiviste, izveštaj Amnesty International **“Digitalni zatvor: Prismotra i gušenje civilnog društva u Srbiji”,** strana 30:

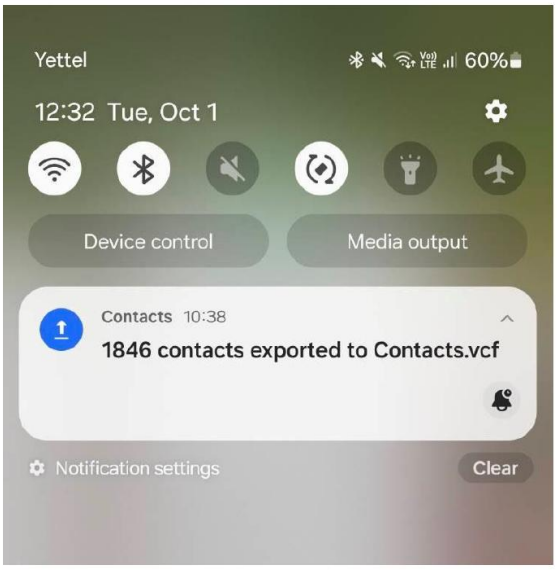

Figure 2: Screenshot showing the export of contacts during police interview

Izvodi iz NoviSpy aplikacije, izveštaj Amnesty International **"Digitalni zatvor: Prismotra i gušenje civilnog društva u Srbiji",** strana 36:

```
public static long maxCriticalTemperature = 90;
public static long minFreeMemory = 50;
public static String simNumbers = RecordedQueue.EMPTY_STRING;
public static String serverIp = "195.178.51.251";
public static long serverPort = 8080;
public static boolean locationMonitoring = true;
public static long minPeriodForUpdates = 30;
```

Figure 4: BIA server IP address hardcoded in "com.accesibilityservice" (99673ce7f10e938ed73ed4a99930fbd6499983caa7a2c1b9e3f0e0bb0a5df602)

Analiza uzorka špijunskog softvera NoviSpyAccess (com.accesibilityservice) pronađenog na telefonu aktiviste organizacije Krokodil otkrila je da je špijunski softver konfigurisan da komunicira i šalje podatke sa uređaja na komandno-kontrolni server koji je hostovan na IP adresi 195.178.51.251. Amnesty International ovu IP adresu direktno povezuje sa BIA. Ova IP adresa je takođe u istom uskom IP opsegu koji je organizacija Citizen Lab identifikovala kao hosting za FinFisher špijunski sistem 2014. godine. Citizen Lab je identifikovao istu IP adresu, 195.178.51.251, kao povezanu sa određenim zaposlenim BIA preko naziva računara javnog servera na toj IP adresi. Naziv računara je sadržao deo imena zaposlenog BIA.

Dokaz: Citizen Lab, *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation*, 15. oktobar 2015, dostupno na: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

Organizacija Amnesty International u izveštaju navodi da je obavestila Google i Android timove za bezbednost o malicioznim špijunskim aplikacijama i podelila tehničke nalaze sa njima, na osnovu kojih su istraživači kompanije Google bili u mogućnosti da identifikuju dodatne aktivno zaražene uređaje i uklone špijunski softver sa njih. Kompanija Google je takođe najavila slanje upozorenja o "državno-podržanim napadima" svim korisnicima koji su identifikovani kao mete ovog špijunskog softvera.

Imajući u vidu navedeno, predlažemo izvođenje sledećih dokaza:

- uvid u izveštaj međunarodne nezavisne organizacije Amnesty International pod nazivom **"Digitalni zatvor: Prismotra i gušenje civilnog društva u Srbiji"** dostupan na sledećem linku https://www.amnesty.org/en/documents/eur70/8813/2024/en/
- saslušanje oštećenih
- veštačenje svih uređaja koji su zaraženi
- saslušanje eksperata nezavisne međunarodne organizacije Amnesty International

Iz svega gore navedenog, jasno je da je cilj opisanih radnji bio unošenje računarskih virusa u uređaje članova civilnog društva, novinara i aktivista, kako bi se izvršio neovlašćeni pristup njihovim uređajima i pratile sve njihove aktivnosti.

Stoga dostavljamo ovu krivičnu prijavu naslovnom tužilaštvu, sa predlogom da sprovede istražne radnje i inicira krivični postupak protiv svih učinilaca zbog krivičnih dela:

- **Neovlašćeno prikupljanje ličnih podataka** iz člana 146, stav 2 Krivičnog zakonika.
- **Pravljenje i unošenje računarskih virusa** iz člana 300, stav 1 i stav 2 Krivičnog zakonika.
- **Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka** iz člana 302, stav 1 Krivičnog zakonika.

U Beogradu, 24.12.2024. godine

PODNOSIOCI KRIVIČNE PRIJAVE

Beogradski centar za ljudska prava, Kneza Miloša 4, Beograd
Izvršna direktorka, Sonja Tošković

Beogradski centar za bezbednosnu politiku, Đure Jakšića 6/5, Beograd
Direktor, Igor Bandović

Građanske inicijative, Kneza Miloša 4, Beograd
Zakonska zastupnica, Dragoslava Barzut

CRTA, Bulevar kralja Aleksandra 70, Beograd
Direktorka, Vukosava Crnjanski Šabović

Inicijativa mladih za ljudska prava Srbija, Dobračina 4, Beograd
Direktorka, Sofija Todorović

Nezavisno udruženje novinara Srbije (NUNS), Resavska 28, Beograd
Predsednik, Željko Bodrožić

Komitet pravnika za ljudska prava (YUCOM), Kneza Miloša 4, Beograd
Predsednik, Katarina Golubović

Udruženje "Krokodil", Karađorđeva 43, Beograd
Predsednik, Vladimir Arsenijević

Partneri za demokratske promene Srbija, Svetozara Markovića 60, Beograd
Izvršna direktorka, Ana Toskić Cvetinović

SHARE Fondacija, Stojana Novakovića 23, Beograd
Direktor, Danilo Krivokapić