Šta se krije iza vaše istorije pretrage na internetu?

Ivan Marković <ivan.markovic@security-net.biz>
Novembar, 2024

Sadržaj:

Legenda:

- Uređaj (Kompjuter, Telefon, Tablet)
- Internet ili intranet lokacija
- Grupa posećenih lokacija
- Lokacije povezane sa BOT mrežama
- Lokacije povezane sa vladajućom partijom
- Državne lokacije visokog rizika

Odricanje od odgovornosti

Ovaj rad je isključivo edukativne prirode i namenjen je podizanju svesti o potencijalnim pretnjama u domenu sajber bezbednosti. Autor nema nameru da promoviše, podstiče ili opravdava bilo kakve nezakonite aktivnosti.

Informacije sadržane u radu služe za bolje razumevanje načina na koje funkcionišu pretnje u sajber prostoru, kako bi se pružila osnova za implementaciju mera zaštite i prevencije. Svako korišćenje ovih informacija u svrhe koje nisu u skladu sa zakonom je u potpunosti na odgovornost pojedinca, i autor ni na koji način ne snosi odgovornost za posledice takvih aktivnosti.

Čitaocima se preporučuje da sve aktivnosti u vezi sa sajber bezbednošću sprovode u skladu sa važećim zakonima i etičkim standardima.

:\1> Zašto pričamo o ovoj temi ?

Svakog dana svako od nas generiše ogroman broj poseta raznim lokacijama na internetu, ali i internim lokacijama. Često se dešava da koristimo iste uređaje i za poslovne, i za privatne aktivnosti.

Ako neko pogleda našu istoriju pretrage može da sazna mnogo o nama.

Samim tim postajemo meta malicioznih strana koje na razne načine *prikupljaju podatke sa naših uređaja, i kasnije ih koriste za izvršavanje svojih agendi.

*
* Prikupljanje se uglavnom dešava na par načina:
- direktnim pristupom uređaju
- prisluškivanjem saobraćaja na nekom od mrežnih uređaja
- prisluškivanjem saobraćaja na (kompromitovanim) web lokacijama
- otkupom saobraćaja ili logova
*

Tokom istraživanja koje je prethodilo pisanju ovog teksta fokus se više puta promenio. Uzrok tome je visok stepen nerazumevanja opsega izazova koje stvara more informacija o korisnicima interneta, a i rizicima po poslovanje i funkionisanje vitalnih institucija.

Kako bih probao da pomognem u rešavanju ovog problema, u ovom dokumentu fokus ćemo staviti na primerima vizuelizacije podataka i korelacijom posećenih lokacija.

Ideja je da se ova metoda analize podataka, kao i tipovi rizika, približe istraživačima i novinarima.

U ovu svrhu razvijen je i alat koji automatski generiše dinamične grafikone, a koje možete videti u svom internet pretraživaču. Za detalje slobodni ste da me kontaktirate.

:\2> Kako jednostavno doći do podataka?

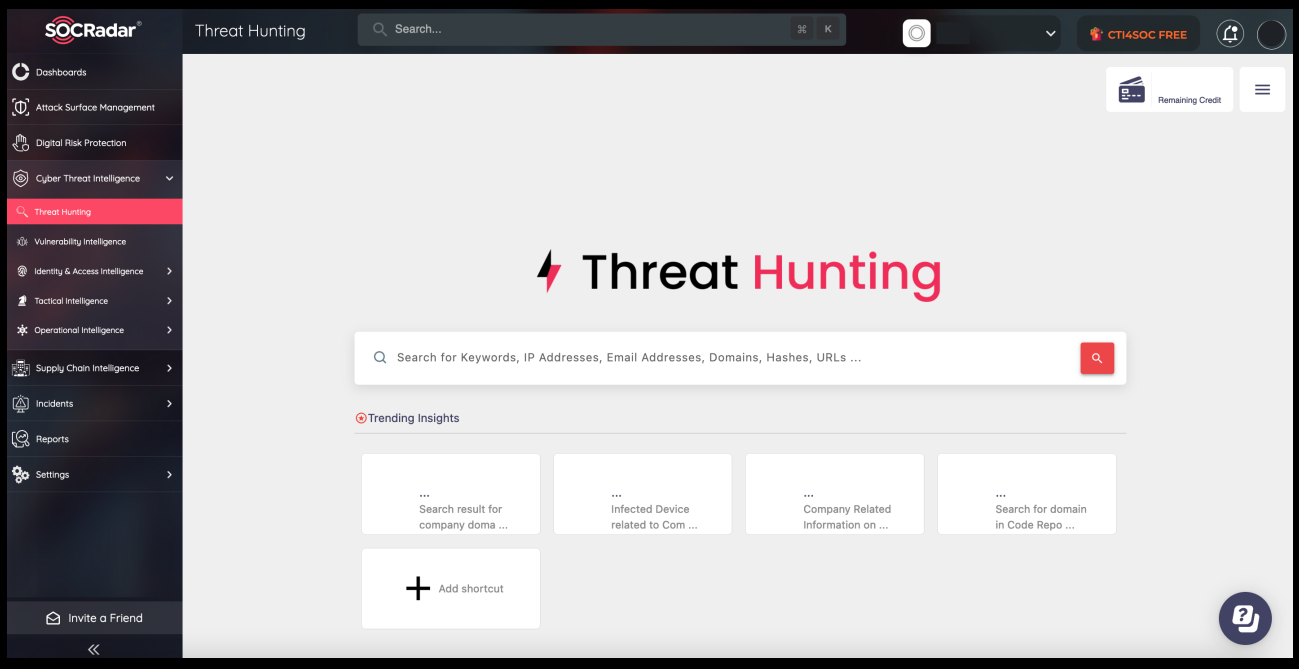
Postoji više načina da dođemo do podataka za analize ali ovde ćemo opisati samo par osnovnih, koje možete koristiti za početak:

1. Možete da eksportujete svoju istoriju pretrage, a i da zamolite i druge ljude da učestvuju u analizi i podele svoje podatke.

   Obevezno obratiti pažnju da u podacima nema URL adresa ili naslova koji otkrivaju lične ili osetljive podatke.

2. Možete koristiti javne izvore podataka o iscurelim pretragama poput socradar.io.

   Ovaj servis pretražuje “deep i dark web” za raznim logovima koji se preprodaju od strane malicioznih strana, i onda pruža uslugu pretrage na osnovu internet lokacije. U besplatnoj verziji, koju koristimo u ovom istraživanju, moguće je dobiti ograničenu listu internet lokacija koje su posećene sa nekog kompromitovanog uređaja.



Ovi logovi su poznati i kao “Stealer Logs”.

:\3> Primer: Operatori bot mreža i državna bezbednost

Nije nepoznata činjenica da postoje organizovane mreže za manipulacije na internetu. Ovakve mreže nazivamo mrežama botova, one koji upravljaju njima operatori, a same osobe ili robote koji vrše interakciju sa svetom, botovima ili slepim sledbenicima.
Više puta su novinari i istraživači *pisali o slučajevima organizovane manipulacije medijima, i mi nećemo ići u detalje posledica koje oni ostavljaju, ali uzećemo neke od poznatih činjenica kao početnu tačku za naše istraživanje.

*
* Linkovi ka detaljnim analizama:
- https://www.cenzolovka.rs/pritisci-i-napadi/castleleaks-novi-podaci-iz-sns-tvrdjave/
- https://www.cins.rs/sns-botovi-imali-pristup-kuriru-i-espresu/
- https://birn.rs/castle-kako-srpska-vlast-manipulise-razumom-a-gradani-za-to-jos-i-placaju/
- https://www.slobodnaevropa.org/a/botovi-srbija-akcija/32499215.html
- https://security-net.biz/shared/bots/sns_grad/
*

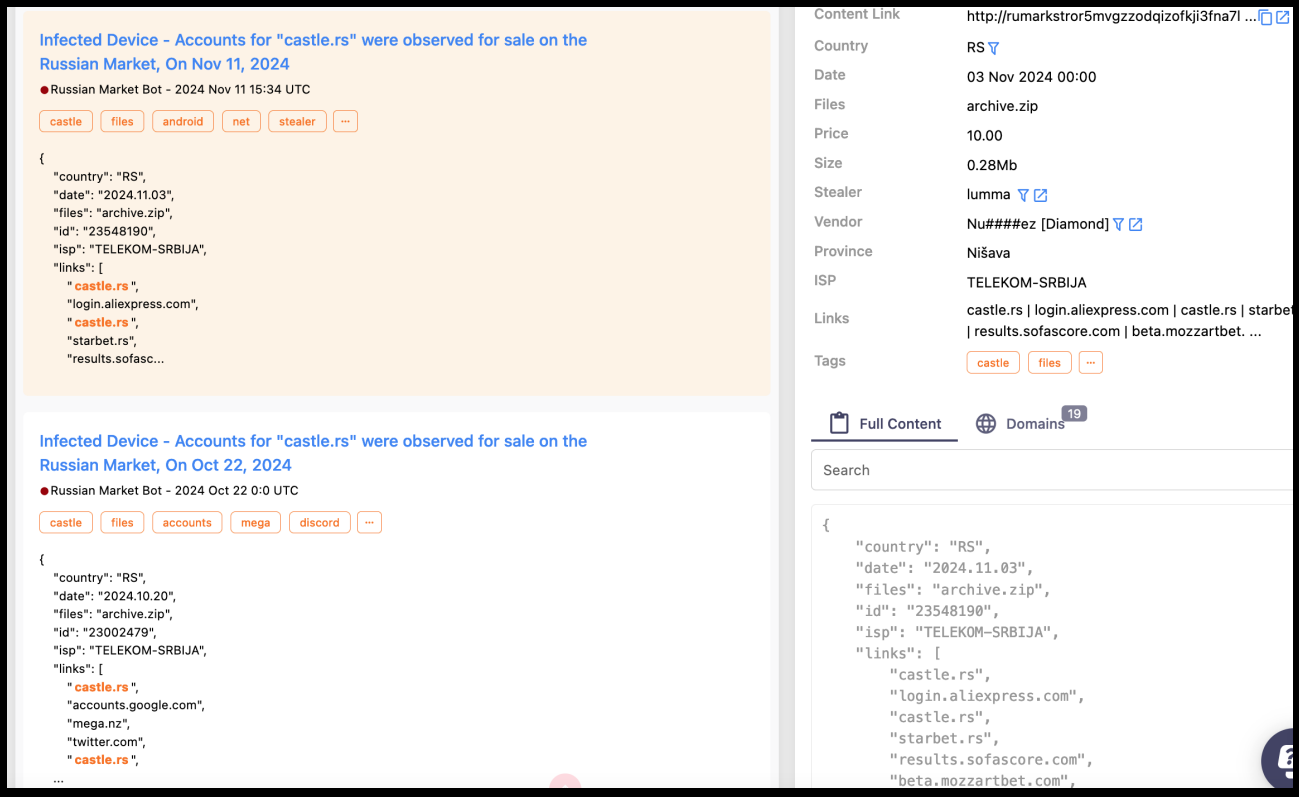
Dakle iz prethodnih analiza možemo videti da su se, u nekom trenutku, operatori i korisnici bot mreža logovali na platforme na domenima castle.rs a prethodno verovatno i na fortress.rs.

Ideja je da probamo da nađemo istoriju pretrage osoba koje su posećivali ove platforme, i da na osnovu tih informacija zaključimo više o namerama, ali i posledicama nemara.

Ako odemo na veb sajt socradar.io i registrujemo besplatan nalog moći ćemo da ukucamo ove domene u pretragu i da dobijemo pristup veoma ograničenoj listi *podataka, ali dovoljnoj za naš eksperiment.

*
* Ovi podaci su navodno dobijeni sa kompromitovanih uređaja, i
* prodaju se na zlonamernim berzama podataka. U ovoj analizi se
* nećemo baviti integritetom ovih podataka, cilj je približiti
* važnost operativne bezbednosti širokim masama.
*

Podaci koje ćemo dobiti izgledaju slično ovome na slici:



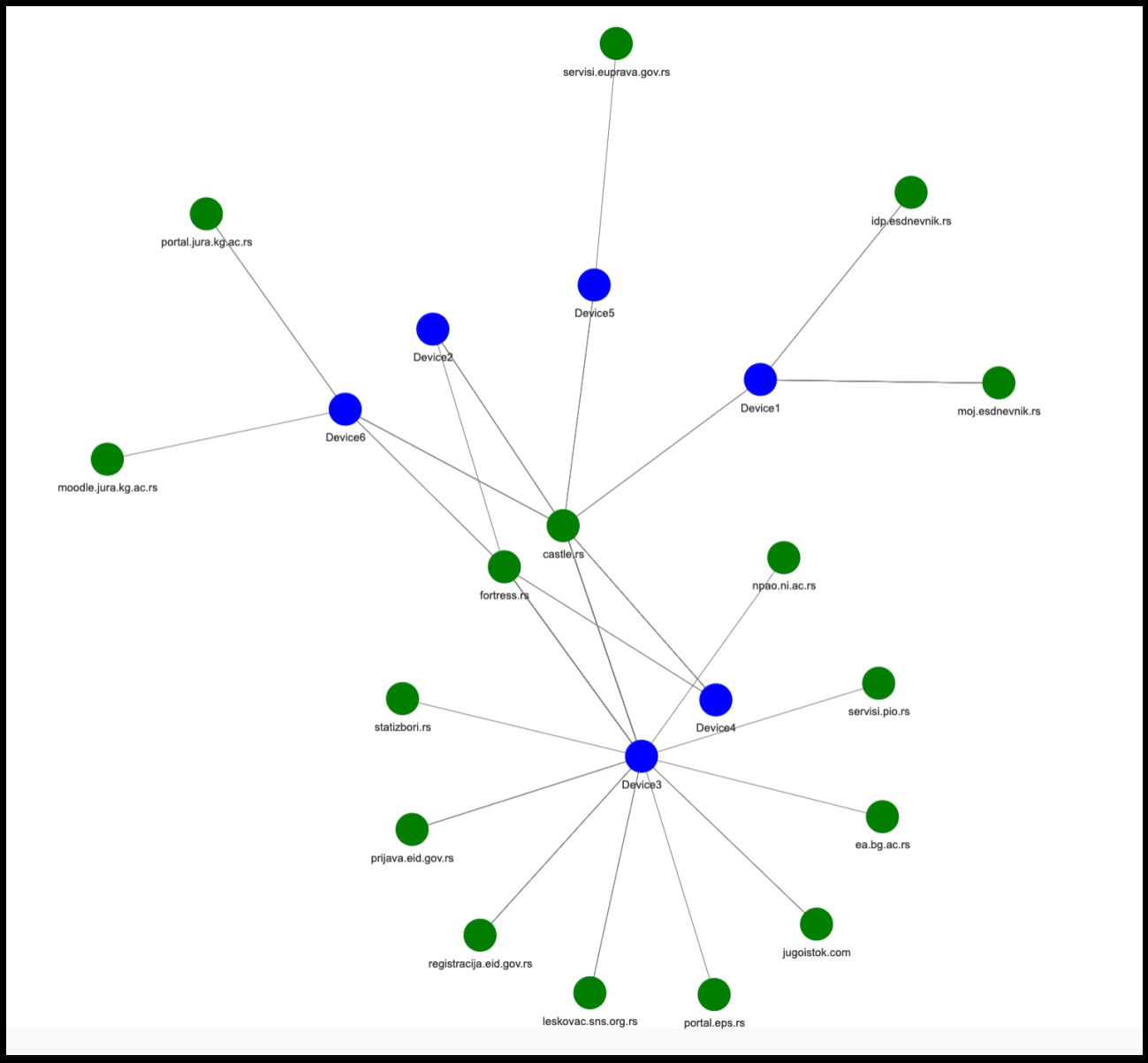
Sada jednostavno možemo da kliknemo levo na “Infected Device” i da onda sa desne strane dobijemo listing posećenih internet lokacija (za koje maliciozna strana poseduje i korisničke podatke).

Iz par pokušaja dobijeni su podaci za 6 kompromitovanih uređaja koji su posetili internet lokaciju castle.rs, i to sa sledećih lokacija:

TELEKOM-BB - Zlatibor: 1
TELEKOM-SRBIJA - Nišava: 4
TELENORDOO-APN - Belgrade: 1

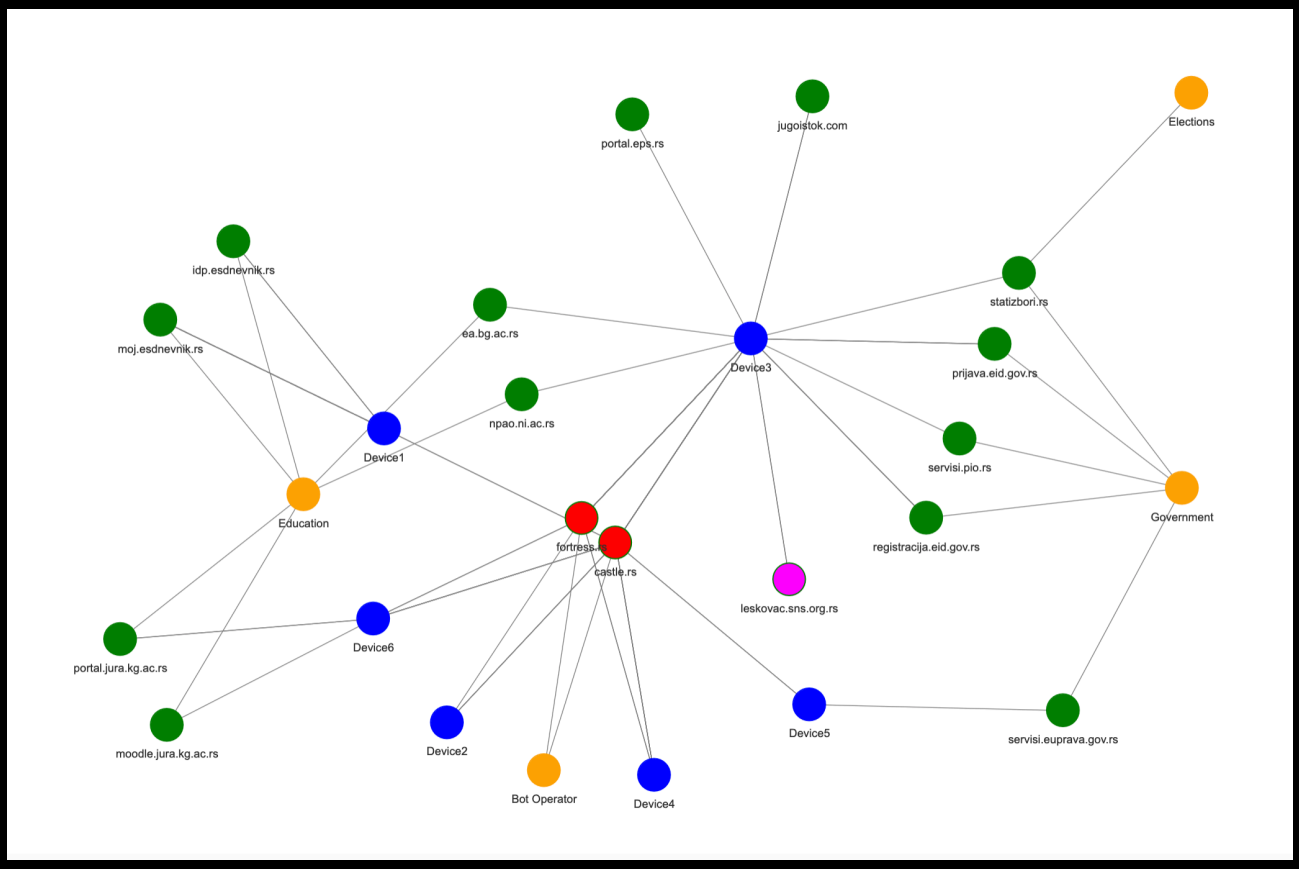
U sledeće koraku napravićemo vizuelizaciju poseta, sa primenjinim filterima kako bi mogli lakše da razumemo podatake.

Recimo da želimo da vidimo koje to državne sajtove posećuju oni ljudi koji posećuju i platforme za upravljanje botovima:



Sa slike možemo da vidimo da se sa istih uređaja sa kojih se pristupa mrežama za upravljanje botovima, pristupa i raznim veb servisima koji su uglavnom dostupni za sve građane. Vidimo da imamo i studente ili profesore koji posećuju platforme za učenje (Moodle).

Za bolji pregled dodaćemo par grupa i nove boje za zanimljive lokacije:



Ono što je posebno zanimljivo je da smo:

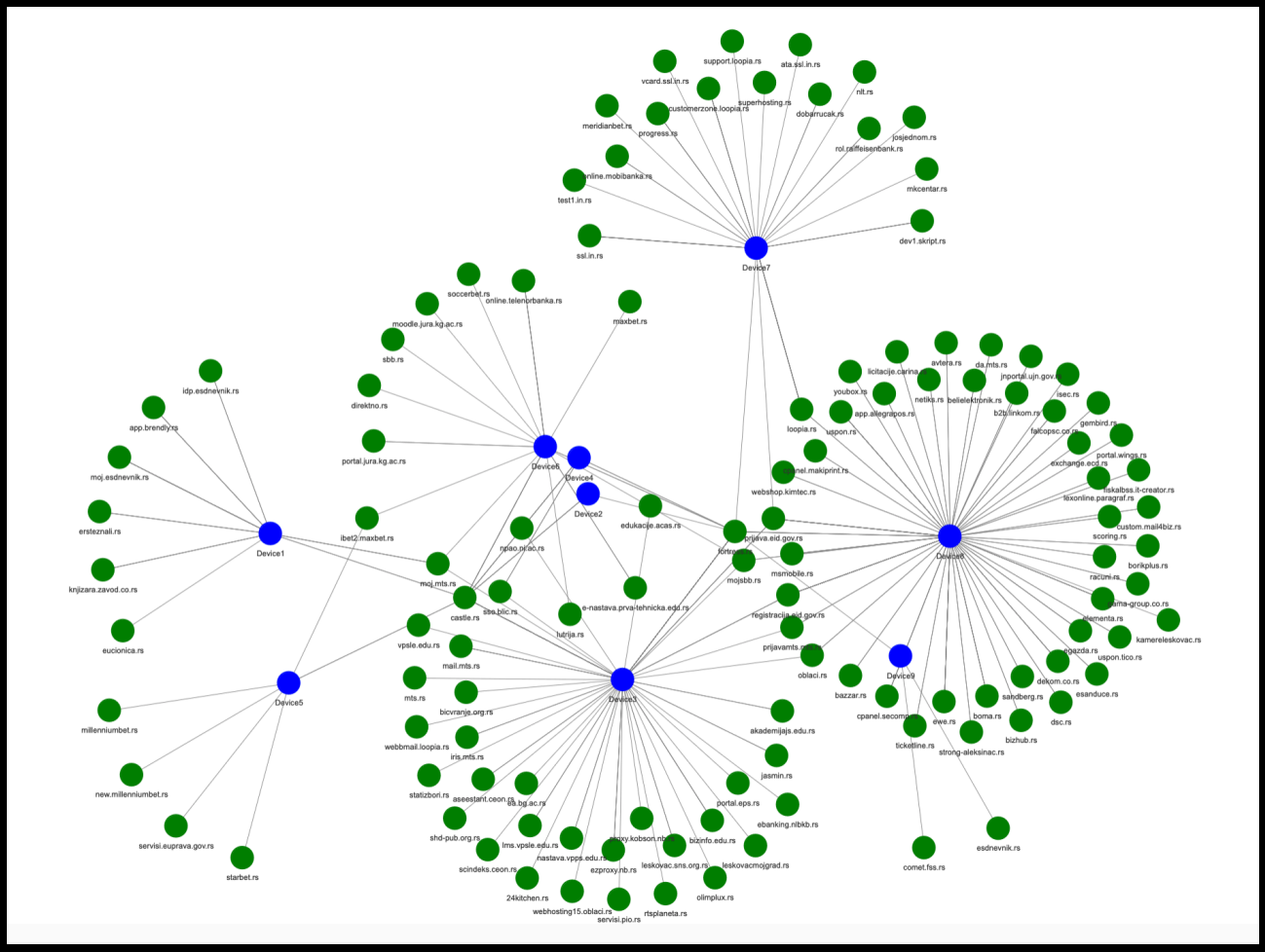
1. Identifikovali drugi domen koji se takođe koristio za upravljanje botovima, fortress.rs.

2. I pronašli smo da se sa istog uređaja (Device3) pristupalo i domenima za upravljanje botovima (castle.rs, fortress.rs), i internet lokaciji vladajuće partije (leskovac.sns.org.rs).

Dalje možemo uraditi pretragu logova vezanih za domen fortress.rs, i u ovom slučaju imamo sledeće podatake:

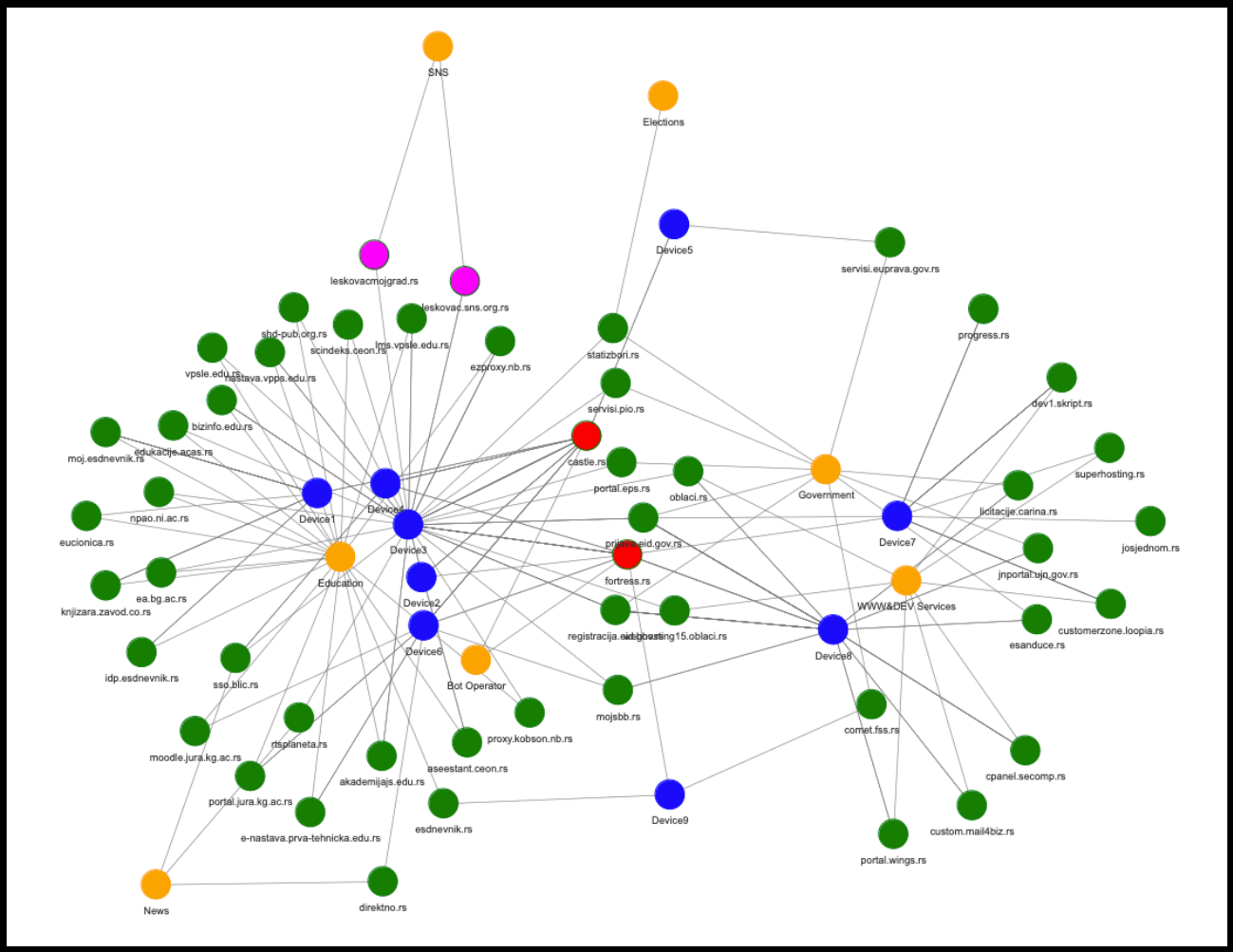
Serbia Broadband - Belgrade: 2
Sat-Trakt D.O.O. - Vojvodina: 1

Sada možemo da ukrstimo ove podatke. Pogledajmo posete samo za .RS domene:



Na osnovu posećenih lokacija lako možemo da zaključimo i koje je zanimanje osobe, ali i gde radi i na kojoj lokaciji.

Zatim dodamo grupisanje, filtere i boje:



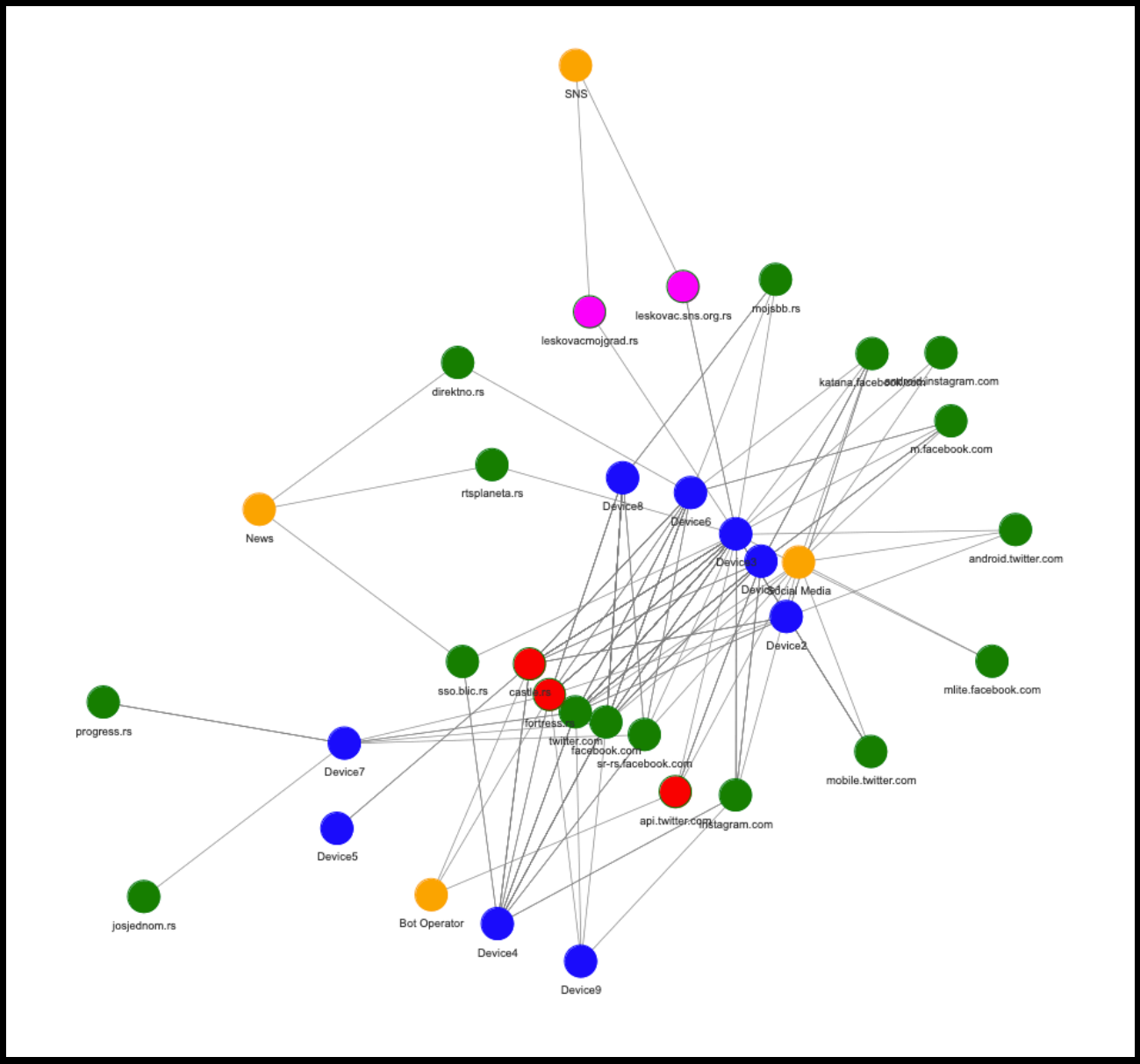
I možemo da primetimo sledeće:

3. Uređaj 3 se koristio i za logovanje na lokacije za upravljanje botovima, i ujedno na lokacije vladajuće partije (leskovac.sns.org.rs, leskovacmojgrad.rs).

4. Uređaj 7 i 8 podsećaju na uređaj nekoga ko se bavi razvojem aplikacija. Takođe ima posete domenima koje imaju samo login stranicu (izvor: WebArchive), od kojih se jedan zove progress.rs a drugi josjednom.rs.

5. Izgleda da imamo i uređaje koji imaju pristup novinarskim portalima (direktno.rs, sso.blic.rs, rtsplaneta.rs). Ovo može možda biti i javni korisnički pristup.

Pre nego što nastavimo dalje, hajde da pogledamo kako izgleda povezanost sa društvenim mrežama:



Kao što smo mogli i da pretpostavimo ovi uređaji su posećivali socijalne mreže, kao i njihove aplikativne interfejse (API).

Pored ovih lokacija uglavnom u logovima se nalaze sajtovi banaka, kladionica, online prodavnica i sajtova za odrasle. Za potrebe istraživanja prikazaćemo samo najrelevantnije lokacije.

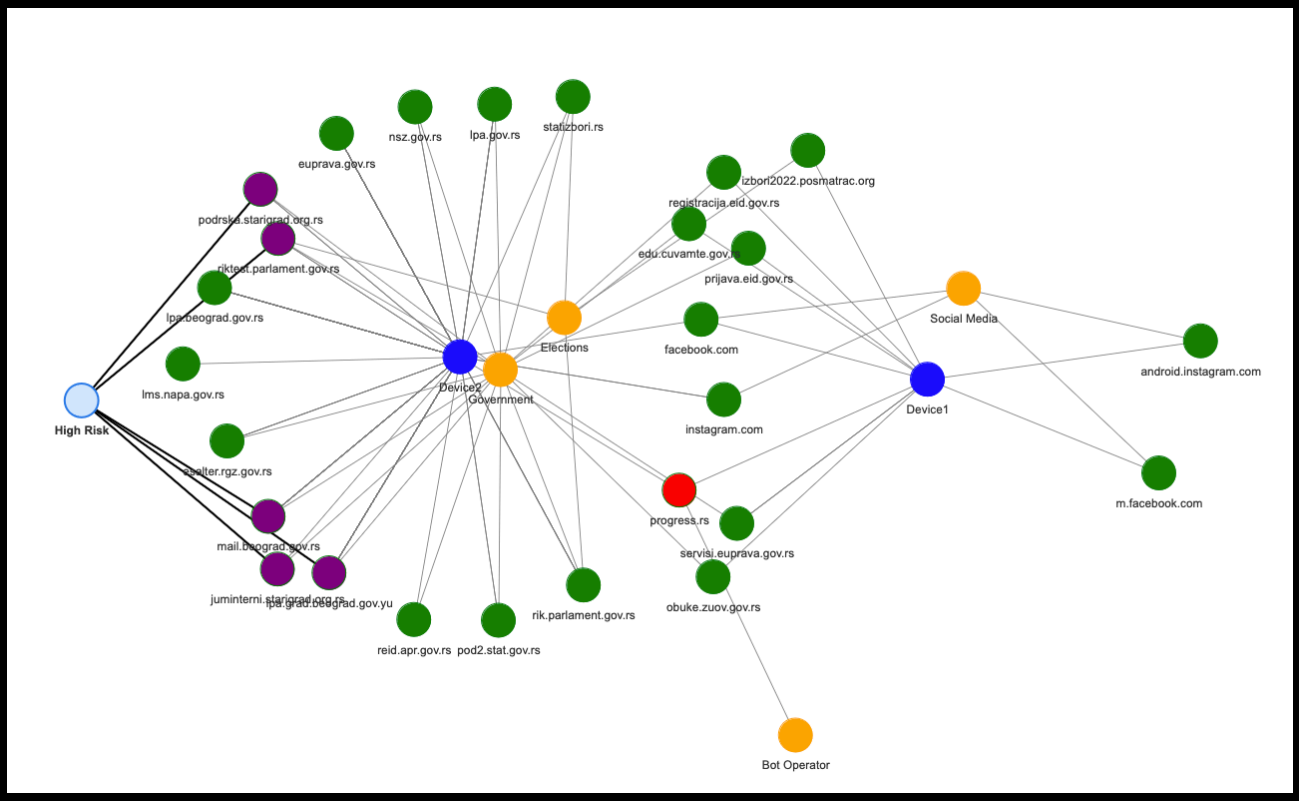
Takođe, u ovom istraživanju nećemo koristiti druge izvore i korelaciju IP adresa i potpunih URL adresa (ali se preporučuje kao sledeći korak).

Kako kroz javne logove vidimo povezanost vladajuće partije sa mrežama botova (a koja u svom imenu ima reč “progress”), i uz to se pojavljuje i lokacija “ progress . rs ”, kao sledeći korak logično je proveriti i da li postoje drugi uređaji koji su posećivali istu lokaciju.

Sa socradar.io dobijamo dva rezultata:

L2VPN Negotin - Belgrade: 1
TELEKOM SRBIJA a.d. - Central Serbia: 1

I to grafički prikazano izgleda ovako:

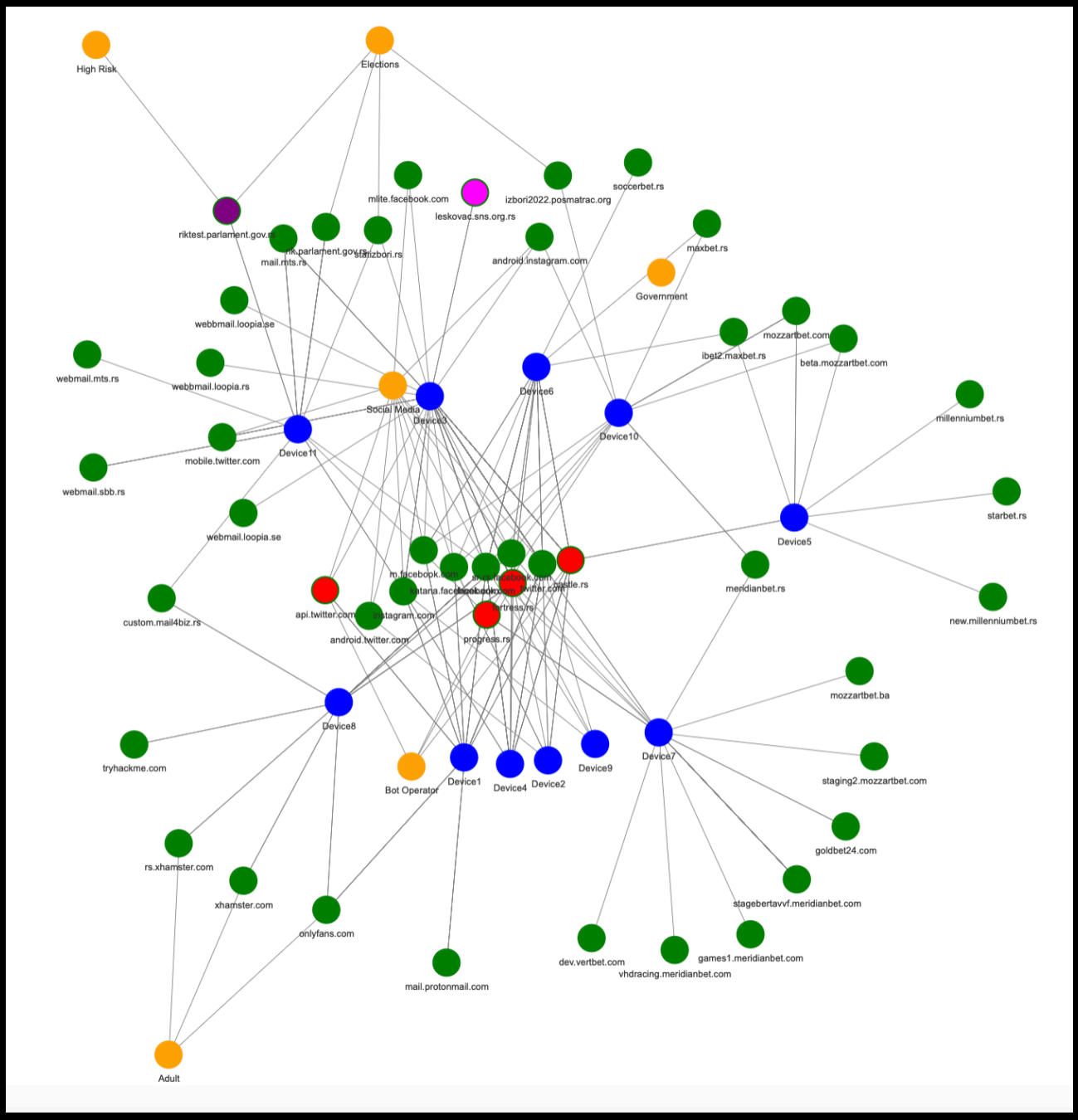


Rezultati nam pokazuju da se sa uređaja koji pristupa domenu progress.rs, pristupa i između ostalog lokacijama vezanim za interne servise državnih službenika:

rik.parlament.gov.rs
mail.beograd.gov.rs
juminterni.starigrad.org.rs
podrska.starigrad.org.rs

riktest.parlament.gov.rs
lpa.grad.beograd.gov.yu

Pogledajmo i kombinovani grafik sa svim uređajima i malo drugačijim filterima:



Ako treba da sumiramo gde nas je odvela analiza:

Uređaji (kompjuteri, telefoni, tableti) koje koriste osobe koje posećuju lokacije za upravljanje mrežama botova, najverovatnije koriste se i u internim državnim sistemima (tragovi/dokazi: test domeni, gov.yu adrese, domen progress.rs).

Ovakav način upotrebe državnih resursa je suprotan svakom etičkom standardu, a pored svega ugrožava državnu bezbednost i izborni proces (tragovi/dokazi: RIK, izbori2022.posmatrac.org, statizbori.rs).

Iz priloženih logova možemo da vidimo da je osoba čiji su podaci o posetama ukradeni koristi vitalne državne resurse.

Na forumu Bezbedan Balkan možete naći više detalja vezanih za mogući incident vezan za riktest.parlament.gov.rs lokaciju, a koji samo potvrđuju da je ove logove pametno dalje detaljno istražiti, i da možda mogu da otkriju uzrok mnogih incidenata.

Link ka detaljima: https://bezbedanbalkan.net/thread-924.html.

:\4> Kako se zaštiti?

Ovde je pravo i prvo pitanje od čega se zaštiti kada vidite da oni koji treba da štite zloupotrebljavaju svoje pozicije, i kada možemo da pretpostavimo da se našoj istoriji pretrage može pristupiti i sa strane sa koje to ne očekujemo. Ali hajde da krenemo od početka:

_ Državne institucije:

Tehničke mere nisu dovoljne. Potrebno je uvesti odgovorno upravljanje po najvećim industrijskim i etičkim standardima, i redovne obuke za sve kadrove.

_ Privatne kompanije:

Uložite vreme u tehničke zajednice u okruženju. Konferencije na kojima se uglavnom reklamiraju proizvođači samo dodaju nove rizike na vaše liste. Postoji mnogo mladih ljudi koji jedva čekaju da počnu da rešavaju probleme sa kojima se suočavate.

_ Građani:

1. Ne koristite tuđe uređaje (čak ni kablove, eksterne punjače ili baterije)
2. Ne delite svoje uređaje sa drugima
3. Kada uređaj nosite u servis, enkriptujte ili obrišite podatke, i obavezno kada preuzmete uređaj još jednom ga vratite na fabričko podešavanje
4. Svaki uređaj mora imati šifru ili pin
5. Za svaki internet nalog potrebno je imati drugu šifru, i po mogućstvu email adresu (ili korisničko ime)
6. Šifre čuvajte u enkriptovanom obliku
7. Ne čuvajte šifre u internet pretraživačima
8. Obavezno instalirajte “antivirus” program
9. Ne koristite piratski softver
10. Ne kačite se na besplatne bežične mreže
11. Pravite redovno eksterne kopije važnih podataka
12. Razdvojite poslovne i privatne aktivnosti (uređaji, korisnička imena, internet pretraživači, VPN)
13. Koristite Signal za komunikaciju
14. Ako vam neko pošalje e-mail, SMS ili vas nazove i želi nešto od Vas uglavnom hitno i tiče se novca, a Vi pre toga niste bili obavešteni o tome, verovatno je prevara koja može da dovede do krađe Vaše istorije pretrage (na primer “Phishing”)
15. Svaki incident prijavite CERT-u

Ako mislite da ste premali da biste napravili razliku, pokušajte da spavate sa komarcem.

- Dalai Lama XIV