Matematički fakultet
Univerzitet u Beogradu

Seminarski rad iz predmeta Računarstvo i društvo

OSINT – Lupa u moru

Mentor:
dr Sana Stojanović Đurđević
docent

Student:
Mitar Avramović
broj indeksa: 398/2021

16. maj 2024.

Sadržaj

1 Uvod

1.1 Definicija

Termin Open Source Intelligence (OSINT) se pre svega odnosi na specifičan izvor saznanja. Uopšteno, izvori saznanja se koriste za stvaranje sirovih podataka koji mogu biti procesuirani u šest koraka obrade podataka za stvaranje uvida. Open Source Intelligence se definiše kao **skup podataka stvoren iz javno dostupnih izvora** koji je prikupljen i obrađen za odgovarajuću publiku za potrebe davanja odgovora na specifično pitanje.

1.2 Istorija

Tokom Drugog svetskog rata, Vilijam Donovan je formirao Odeljenje za strateške usluge (OSS), koje će kasnije postati Centralna informativna agencija (CIA). Unutar OSS-a, čitav jedan deo je bio posvećen analizi javno dostupnih informacija u obliku prikupljanih novina kao i radio prenosa širom sveta, držeći se reči svog osnivača "čak i režimski mediji će izdati nacionalne interese u očima neumornog posmatrača".

1.3 Internet

Porastom upotrebe interneta se priroda javnih informacija menja u korenu. Čak i novine su sve više prisutne u digitalnom svetu, sa čestim ažuriranjem. Ovo rezultira bržim i lakšim pristupom novostima. Dodatno, internet pruža još više opcija svakom svom korisniku za iskazivanje vesti, znanja i mišljenja sa minimalnim, gotovo nepostojanim restrikcijama. Ovo je ojačano raznovrsnošću novih javnih izvora poput ličnih sajtova, foruma, blogova, društvenih mreža itd. Takođe, razne kompanije i organizacije koriste priliku da daju informacije i nude usluge poput pretraživača, platformi za društvene mreže, platformi za trgovinu, dejting sajtova itd.

Ove usluge se koriste i ohrabruju korisnike da dele širok spektar ličnih informacija koje se vezuju za online pseudonim, ili u nekim situacijama, lična imena. Trend davanja osetne količine ličnih informacija je relativno nov. To se može videti kao jaka suprotnost incidentu iz 1983. godine u Nemačkoj, kada zbog zahteva za neke lične informacije za potrebe novouvedenog popisa stanovništva su izbili masovni protesti. Iako je do nekih izvora malo teže doći, većina se smatra javno dostupnim. Životni vek jednog izvora se može kretati od svega nekoliko godina do više od jedne decenije.

Ono što nam ostaje kao posledica je da svi ovi izvori informacija nisu dostupni samo ljudima i organizacijama koje se bave obaveštajnim poslom. Iz razno raznih razloga, veliki broj raznih lica i organizacija razvija i koristi alate i tehnike kako bi analizirali javno dostupan sadržaj.

2 Upotrebe OSINT-a

Kao što je navedeno u prvom delu, ovde ćemo se pozabaviti širokim spektrom upotrebe OSINT-a.

Obaveštajne službe: 2015. jedan džihadista ISIL-a kači selfi koji u pozadini sadrži fabriku bombi. 23 sata kasnije, SAD napada i uništava tu istu fabriku.

Novinarstvo: Belingketski kolektiv (koji uključuje istraživače, inspektore i amaterske novinare) predstavlja organizaciju koja prevashodno koristi javne izvore i društvene mreže za svoja istraživanja. Oni su uspeli da povežu ruske obaveštajce sa istragom Leta 17 Malasiya Airlines-a kao i trovanjem porodice Skripal.

Poslodavci: Deloitte-ovo istraživanje iz 2012. godine je pokazalo da je u tom trenutku 13% ljudi pozvanih na intervju kompanija Dax i Mdax bilo procesuirano i odrađene su im pozadinske provere na osnovu njihovog onlajn ponašanja.

Policija: Početkom 2016. godine, Nemački policijski univerzitet sprovodi trogodišnje istraživanje sa ciljem ustanovljavanja da li je OSINT kao tehnika dovoljno efikasna kako bi se uvela kao odeljenje u okviru nemačke policije. Dolaze do zaključka da može pružiti korisne informacije i već 2019. počinju sa zapošljavanjem službenika.

Javno praćenje: Europol je pokrenuo projekat "Stop Child Abuse" u kom se javnost ispituje da identifikuje detalje slika nađenih na mestima zločina nad decom.

Pronalazak nestalog lica: Nakon nestanka Džima Greja (informatičara i dobitnika Tjuringove nagrade) tokom krstarenja brodom 2007. godine, angažovan je veliki broj civila iz okoline mesta gde je nestao u pretrazi javno dostupnih satelitskih i avionskih slika i snimaka.

Krađa: 2016. Kim Kardašijan je, u svojoj sobi u Parizu, bila opljačkana pod pretnjom pištolja. Iz sobe je iznet nakit u vrednosti od 6 miliona evra. Kada je jedan od počinilaca bio uhvaćen, nakon ispitivanja francuske policije, priznao je da je, zajedno sa saučesnicima, uz pomoć analize objava na Instagramu i drugih javno dostupnih izvora dobio neophodne informacije da izvrši krađu.

3 OSINT metodologija

U ovom poglavlju ćemo definisati osnovne termine OSINT metodologije kao i alate i tehnike.

3.1 OSINT proces

Model koji se koristi za prikupljanje i obradu sirovih podataka u korisne obaveštajne podatke se zove **ciklus obaveštajnih informacija** (intelligence cycle). On predstavlja zatvoren ciklus koji se sastoji od čvorova koji se mogu ponavljati, zavisno od potrebe. Krajnji njegov cilj su operativne informacije koje se predstavljaju odgovornim licima. Deli se na šest etapa (čvorova) koji su: **planiranje, prikupljanje, obrada, analiza, distribucija i obrada povratnih informacija.**

Planiranje: Pre svega, uzimaju se sveukupne potrebe za operativnim informacijama. To radi obično stručno lice, čiji posao i jeste da donese odluku o neophodnim informacijama za dati problem. Jedna OSINT istraga počinje uglavnom sa specifičnim zadatkom ili zahtevom klijenta. Tipični zadaci bi bili: procena opasnosti za pojedince ili događaje, profil ciljeva za pojedince ili događaje, profil ciljnih grupa. Neophodno je izvršiti verifikaciju pruženih identifikatora kao što su imena, onlajn pseudonimi, email adrese ili domena (ako je cilj IT sistem).

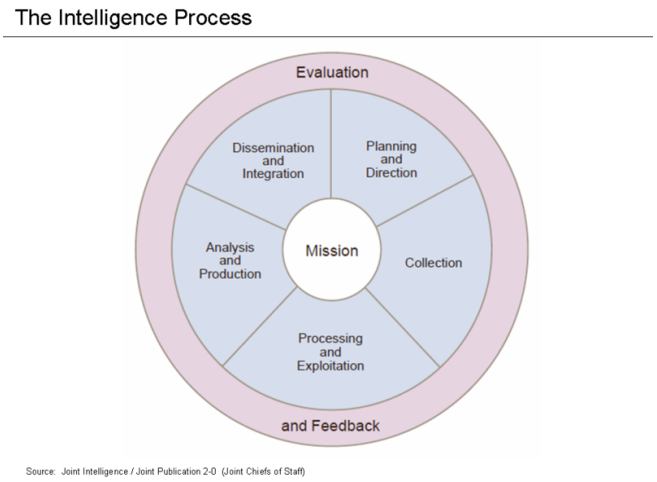
Prikupljanje: Faza u kojoj se prikupljaju podaci. Ideja je da se javni izvori sistematski pretraže koristeći prethodno uspostavljene identifikatore. To se vrši u tri koraka. Prvi korak predstavlja pretragu specijalizovanih pretraživača, veb-sajtova i usluga koje mogu zahtevati naplatu (zato što su dobar vid internet dokumentacije pojedinca ili grupe). Drugi korak je primena određenih OSINT aplikacija, alata I tehnika zavisno od cilja istrage, za efektivniju pretragu, ali i povezivanje online putanja proverenih identifikatora. Treći korak je beleženje svih nalaza.

Obrada: Ova faza je vrlo dinamične prirode, gde se ona može modifikovati da služi bilo kom vidu obrade. To uključuje prevođenje, dekripciju i transformaciju podataka u koristan i razumljiv sadržaj.

Analiza: Ova faza često ume da utopi prethodnu. Ona predstavlja pretvaranje sirovih informacija u obaveštajne podatke. To uključuje integraciju, procenu i analizu sirovih informacija sa ciljem dolaženja do očekivanog rezultata. Ova faza je ključna, jer se ovde zapravo mogu ostvariti ključne veze između podataka koji mogu ukazati na nešto.

Distribucija: Distribucija se vrši klijentu ili svim neophodnim licima. Takođe, distribucija se može izvršiti u fizičkom ili elektronskom formatu zavisno od potreba, ali pre svega poverljivosti nalaza.

Obrada povratnih informacija: Ova faza često biva preskočena, ali predstavlja sveukupnu ocenu kvaliteta i značaja nađenih i obrađenih informacija. Njihov rezultat biva upoređen sa "situacijom na terenu".



3.2 Podaci, informacije i obaveštajni podaci

U prethodnom delu se nismo pozabavili distinkcijom između ova tri pojma, što ćemo sada učiniti.

Podaci predstavljaju skup činjenica bez ikakvog objašnjenja ili analize i njih dobijamo tokom faze prikupljanja. Na osnovu svog formata se mogu klasifikovati u tri klase: struktuirani podaci (SQL baze), polustruktuirani podaci (JSON, XML i HTML dokumenti) i nestruktuirani podaci.

Informacije predstavljaju rezultat faze obrade. Dobijaju se obradom prikupljenih podataka. Zavisno od prirode podataka, obrada uključuje prevođenje, dešifrovanje ili izmenu formata, dodatno filtriranje, povezivanje, klasifikovanje, klasterovanje, itd.

Obaveštajni podaci su proizvod pokušaja rešavanja polaznog pitanja dobijenim informacijama.

Ugrubo govoreći, u OSINT istrazi, podaci se mogu klasifikovati u **sedam kategorija**:

Pojedinac: Nalazi se tiču svih relevantnih informacija o jednoj osobi (ime i prezime, adresa, finansijsko stanje, onlajn pseudonim, email adresa, društvene mreže)

Grupa ljudi: Obično u policijskim istragama, fokus se stavlja na grupu ljudi, njihove odnose i interakcije.

Organizacija: Za razliku od grupe, organizacije karakteriše uglavnom uniforman cilj i postojanje hijerarhije. Primeri su kompanije, institucije čak i države. Ovde od značaja mogu biti razni biznis dogovori, strateški planovi, zapošljeni i mušterije.

Računarski sistemi: Sve informacije jednog IT sistema, poput domena, postojećih poddomena, korišćeni softver itd.

Događaj: Posmatranjem ponašanja ljudi na internetu, možemo ustanoviti neki događaj koji se treba desiti onlajn ili uživo.

Lokacije: Fizičke adrese ili koordinate.

Objekti: Sve što ne spada u ostale klase. Slike, videi npr.

3.3 Alati i tehnike

Čak i ako postavimo precizno pitanje i zadamo krajnje rešivi zadatak u prvoj fazi našeg istraživanja, odgovor će zahtevati prikupljanje, obradu i analizu ogromne količine javno dostupnih podataka. Iz ovog razloga se moramo osloniti na neki vid automatizacije (posebno u fazi prikupljanja) kroz korišćenje specifičnih tehnika i alata.

Pre svega, moramo primetiti da se alati poprilično brzo menjaju. Postoje dva razloga zašto i oba su skorijeg datuma. Prvi je povlačenje nekoliko bitnih alata od strane njihovih vlasnika poput Bazzell-ovog skupa interaktivnih popularnih onlajn alata u junu 2019. godine kao i nestanak meta-pretraživača searx.me. Drugi razlog je dinamična priroda društvenih mreža. Facebook i Instagram aktivno podrivaju korišćenje alata i tehnika vezanih za OSINT. Stoga blokiraju odgovarajuće veb usluge, redovno menjaju svoj izvorni kod i ograničavaju kapacitete koje koristi OSINT zajednica. Na primer, Instagram uključuje specijalno kodiranje znakova u izvorni kod svoje veb stranice kako bi otežao direktno izvlačenje URL-ova.

Uprkos svim ovim teškoćama, postoje različiti pristupi za pregled alata i tehnika. OSINT Framework je najrazvijeniji resurs. Njegov cilj je laka identifikacija OSINT alata pogodnih za pretragu na

osnovu specifičnih identifikatora. Organizovan je kao struktura stabla sa identifikatorima kao korenima i kandidatskim alatima kao listovima.

3.4 Veb pretraživači

Postoje 4 tipa pretraživača: klasični pretraživači (crawler-based search engines), direktorijumi koje uređuju ljudi (human-powered directories), hibridni pretraživači (hybrid search engines) i meta pretraživači (meta search engines).

Za razliku od jednostavnih tekstualnih pretraga, specifično formulisanje upita za pretragu može značajno poboljšati rezultate. Stoga se unos u korisnički interfejs obogaćuje proširenim parametrima pretrage kombinovanim sa Bool-ovim izrazima. Prošireni parametri pretrage su specijalni karakteri i komande koje značajno proširuju mogućnosti tekstualne pretrage. Primeri uključuju upotrebu navodnika za zahtev za tačnim podudaranjem, termin intext: za pretragu unutar tela ili dokumenta, termin inurl: za termin u URL-u. Njihova upotreba proizvodi rafinirane rezultate. Ova tehnika je prvi put primenjena u Google pretraživaču i stoga je poznata kao Google Hacking ili Dorking.

S obzirom na identifikatore kao što su korisnička imena, brojevi telefona ili e-mail adrese kao unose, rezultati opisanih veb pretraživača mogu biti ograničeni. Ovo takođe važi za analizu drugog potencijalno relevantnog sadržaja kao što su slike ili lokacije. Specijalizovani pretraživači su u stanju da adresiraju takve vrste unosa. Ovi uključuju pretragu slika (Google Images), kao i pretrage korisničkih imena (WhatsMyName), e-mail adresa (ThatsThem), lokacija (Google Earth) ili brojeva telefona (Whocalld).

Drugi manje poznati, ali takođe zanimljivi specijalizovani pretraživači: dokumentovanih imena (Names Directory), vesti (Google News), naučnih radova (Sci-Hub), sigurnosnih ranjivosti (Common Vulnerabilities and Exposures), resursa povezanih na internet (Shodan).

3.5 Društvene mreže

Obećavajući izvori informacija o pojedincima ili grupama ljudi su društvene mreže kao što su Facebook, Instagram, LinkedIn, Twitter, Pinterest, YouTube, pa čak i PayPal, gde ljudi dele lične informacije i komuniciraju sa porodicom, prijateljima, kolegama ili čak nepoznatim osobama.

Detaljna analiza je podržana automatskim alatima za preuzimanje prilagođenim odgovarajućoj društvenoj mreži, na primer InstaLooter i Instaloader, fokusiranim na Instagram ili TweetBeaver i exportdata fokusiranim na Twitter.

Pored toga, postoji broj aplikacija, ekstenzija za pregledače ili veb usluga specijalizovanih za različite društvene mreže koje nude ekstrakciju određenih informacija ili pripremu za manipulaciju URL-ovima (npr. ekstrakcija Facebook userID-a Facebook UserID LookUp) ili samostalne informacije (npr. prikazivanje promena biografije na Twitter-u Twitter Biography Changes). Izazovi se javljaju jer neke društvene mreže omogućavaju primenu jakih privatnih podešavanja na profilu što sprečava detaljan pregled. Iako ovo isključuje značajnu količinu informacija, to ne sprečava nužno curenje informacija. Na primer, moguće je identifikovati javne objave koje nisu direktno prikazane na stranici privatnog profila (OSINT Curious). Druga opcija je analiza povezanih naloga koji mogu biti javni i otkrivati informacije o cilju.

Alati i tehnike za pretragu na društvenim mrežama se stalno razvijaju. Kao što je ranije pomenuto, ovo je uzrokovano čestim promenama samih društvenih mreža kako bi se sprečila eksploatacija informacija na načine koji nisu prvobitno predviđeni. Značajan primer je nestanak Facebook-ove graf pretrage. Prvobitno uvedena za opštu upotrebu, nudila je moćan pristup za dobijanje informacija. Ovo se promenilo 2014. godine, a funkcionalnost graf pretrage bila je dostupna samo pomoću modifikacija URL-ova. Na kraju, svi alati i tehnike koje su se oslanjale na graf pretragu prestali su da rade sredinom 2019. godine.

4 Odgovor društva

Cilj svake OSINT istrage je da se prikupe informacije o cilju. Međutim, ovo može biti u suprotnosti sa interesima cilja. Iz perspektive istog, otkrivanje informacija može biti nepoželjno jer narušava privatnost, ili čak štetno ako se rezultati iskoriste protiv cilja u kriminalnom aktu. Ovo postavlja pitanje da li postoje mere za sprečavanje eksploatacije podataka.

4.1 Protivmere

Suočeni sa neželjenim otkrivanjem ličnih podataka, validno je pitanje šta svako može učiniti da smanji površinu napada. Odgovor leži u principu da se podaci čuvaju privatno i da se deli što manje informacija. Što je manje javno dostupnih podataka o pojedincu, to je manji rizik od otkrivanja tokom OSINT istrage. Takođe postoje neke dobre prakse vremenom ustanovljene.

Prva preporuka je detaljan pregled aktivnosti na društvenim mrežama i aktivno smanjenje količine deljenih informacija. Najefikasnija strategija bi bila potpuno izbegavanje učešća na društvenim mrežama i zatvaranje svih postojećih naloga. Međutim, interakcije na društvenim mrežama su neophodne u svakodnevnom životu. Preporučuje se prilagođavanje podešavanja privatnosti svih profila. Ovo može uključivati korišćenje pseudonima umesto pravog imena. Pored toga, čak i sa strogim podešavanjima privatnosti, pametno je tretirati sve deljene informacije kao javno dostupne i izbegavati izlaganje sadržaja neprikladnog za široku publiku ili kompromitujućeg u pogrešnim rukama.

Pored pregleda aktivnosti na društvenim mrežama, još jedan savet je izbegavanje objavljivanja ličnih informacija kao što su kućna adresa, broj telefona ili email adresa. U slučaju da je objavljivanje neophodno zbog poslovnih razloga, izvodljiv pristup je postavljanje odvojenih kontakt informacija.

4.2 Pravni okvir

GDPR: 2016.Evropska unija je uvela Opštu uredbu o zaštiti podataka (GDPR). Ova uredba uvodi mere zaštite ličnih podataka fizičkih lica. Na primer, zahteva obaveštenje ako se prikupljaju lični podaci i saglasnost za obradu ličnih podataka. Fokusirajući se na OSINT istrage pojedinaca, primena ove uredbe bi ozbiljno ograničila bilo koje prikupljanje ili obradu podataka.

Države: Navešćemo samo primer Nemačke koja se kroz odluku Saveznog suda Nemačke još 2008. obračunala sa svim OSINT pretragama, legalizujući ih, smatrajući javno dostupne informacije legalnim za čitanje svim čitaocima. Sa uvođenjem GDPR-a 2016. godine, obrada ličnih podataka je dodatno regulisana. Ovo se takođe primenjuje u slučaju da istragu sprovode organi za sprovođenje zakona sa direktivom EU 2016/680 koja posebno adresira zaštitu fizičkih lica u vezi sa obradom ličnih podataka od strane nadležnih organa u svrhe sprečavanja, istrage, otkrivanja ili gonjenja krivičnih dela ili izvršenja krivičnih sankcija. Pored toga, prikupljanje javnih informacija od strane vlasti predmet je kontroverznih rasprava. Dok su ciljne pretrage pokrivene opštim ovlašćenjima, korišćenje široko baziranih OSINT pretraga (npr. Big Data) je sporno.

Uslovi korišćenja usluga: Implicirano je da se podaci prikupljeni sa društvenih mreža mogu smatrati javnim. Međutim, pristup najčešćim društvenim mrežama kao što su Facebook ili Instagram je ograničen registracionim procesom. To znači da samo registrovani članovi te društvene mreže imaju pravo pristupa. Iako je ova registracija besplatna, zahteva ulazak u ugovor sa društvenom mrežom. Tako, korisnik mora da pristane na uslove korišćenja te društvene mreže. U nekim slučajevima, primena OSINT alata i tehnika krši ovaj ugovor. Na primer, zabranjeno je pristupanje Facebook-u ili Instagram-u na automatizovan način prema njihovim uslovima korišćenja ili stvaranje Facebook naloga koristeći lažno ime.

4.3 Etička pitanja

U pogledu etičke perspektive, takođe je potrebno diskutovati da li etička upotreba informacija zavisi od toga da li su te informacije namerno učinjene javnim. Na primer, u PayPal-u je moguće pretražiti listu korisnika PayPal-a samo pružanjem nekoliko karaktera imena. Često odgovarajući profili uključuju dodatne informacije kao što je trenutni grad prebivališta. Većina ljudi je dala svoje ime verujući da će samo ograničeni broj ljudi imati pristup tim informacijama. Shodno tome, većina korisnika nije svesna da se neki od njihovih podataka može smatrati javno dostupnim.

Podaci o proboju često se objavljuju, bilo da se naglasi zahtev za uzimanje podataka ili se dokaže uspešan napad. S obzirom na to da su takvi podaci javno dostupni i veoma vredni, OSINT istraživači se pitaju da li se oni mogu iskoristiti za istragu. Po ovom pitanju, mišljenja se razlikuju. Za neke je upotreba neetička jer podaci nikada nisu bili namenjeni za javnost i dobijeni su putem kriminalnih dela. Za druge, nije bitno kako su dobijeni, i oni dopunjuju svoju zbirku podataka.

5 Zaključak

Osnovne mere za zaštitu privatnih informacija od izloženosti OSINT istragama su dostupne, ali nisu uvek vrlo praktične. U celini, upotreba javnih podataka je (u većini slučajeva) zakonita, omogućavajući OSINT istrage fokusirane na računarske sisteme, objekte ili lokacije. Situacija za OSINT istrage o pojedincima je drugačija jer takve istrage zavise od prikupljanja i obrade ličnih podataka. Takvi tipovi podataka podležu ograničenjima na evropskom nivou, što čini pravni status OSINT-a fokusiranog na fizička lica, barem od strane nevladinih entiteta, neizvesnim i predmetom daljih pojašnjenja. Sa etičkog stanovišta, može se primetiti da nije sve što je tehnički moguće i moralno opravdano.

6 Literatura

(1) https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf

(2) https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/

(3) https://www.bellingcat.com/

(4) https://www.europol.europa.eu/stopchldabuse

(5) https://www.sfgate.com/news/article/Vast-search-off-coast-for-data-wizard-2620302.php

(6) https://www.bbc.com/news/world-europe-37538453

(7) Gibson H, in Open Source Intelligence Investigation – From Strategy to Implementation, ed. by B. Akhgar, P.S. Bayerl, F. Sampson (Springer, 2016), 69 – 93

(8) https://osintframework.com/

(9) https://en.wikipedia.org/wiki/Intelligence_cycle

(10) https://en.wikipedia.org/wiki/Open-source_intelligence