

OSINT v slovenskom prostredí

Michal Sládeček
doc. RNDr. Martin Stanek, PhD.

30. júna 2020

Čo je OSINT?

- ▶ Metóda zberu informácií
- ▶ Využívanie verejne dostupných zdrojoch
- ▶ Využívaná napr. v informačnej bezpečnosti alebo pri rôznych vyšetrovaniach
- ▶ Začal ako čítanie novinových článkov, vďaka internetu sa stal omnoho dôležitejším

Regionalita OSINTu

- ▶ Otvorené zdroje v každej krajine sú rozdielne
- ▶ Množstvo informácií sa dá nájsť len cez tieto regionálne zdroje

Ciele práce

- ▶ Popísať momentálny stav zdrojov OSINTu na Slovensku
- ▶ Práca sa zaoberala zdrojmi voľne dostupnými na internete
- ▶ Ukázať na príkladoch ako sa tieto zdroje dajú využívať
- ▶ Zautomatizovať časti procesu

Momentálny stav problematiky

- ▶ Medzinárodne je OSINT dobre preskúmaná téma
- ▶ Na Slovensku sa OSINTom zaoberali hlavne žurnalisti
- ▶ Sme prví, kto zhodnotil zdroje OSINTu aj z pohľadu informačnej bezpečnosti

Osobné údaje

- ▶ Popis zdrojov o osobných údajoch
- ▶ Naprogramovanie modulu do programu Sherlock
- ▶ Demonštrácia postupov

Osobné údaje - príklady spracovaných zdrojov

- ▶ Kataster nehnuteľností
- ▶ Register záložných práv
- ▶ Obchodný a živnostenský register
- ▶ Telefónne zoznamy
- ▶ Databázy ŠPZ

Osobné údaje - prezývky na internete

- ▶ Dorobili sme modul pre 24 slovenských webstránok do open-source programu Sherlock
- ▶ Program zisťuje, či je hľadaná prezývka registrovaná na stránkach
- ▶ Vieme tak zisťovať, ktoré stránky cieľ používa

Osobné údaje - prípadová štúdia

- ▶ Na vzorke sme ukázali, ako prebieha hľadanie informácií o osobe.
- ▶ Využili sme mená zo zoznamu absolventov FMFI UK z roku 2000
- ▶ Do práce sme zahrnuli anonymizované výsledky
- ▶ 5 žien a 5 mužov
- ▶ Tri osoby zo zoznamu žijú v zahraničí, preto ich neuvádzame vo výsledkoch

Osobné údaje - výsledky

		Cieľ			
		Nájdená	Adresa	Tel. číslo	Dátum narodenia
Osoba	1	Y	P	P	P
	2	Y	Y	N	Y
	3	N	N	N	N
	4	Y	P	P	P
	5	Y	N	N	N
	6	Y	Y	N	Y
	7	P	P	P	P

Organizácie

- ▶ Popis zdrojov o organizáciach, zmluvách a obstarávaníach
- ▶ Demonštrácia využitia zdrojov na súkromných firmách
- ▶ Demonštrácia použitia zmlúv – nájdenie antivírusových systémov používaných na ministerstvách

Organizácie - príklady zdrojov

- ▶ Obchodný register
- ▶ Register účtovných uzávierok
- ▶ Súdne rozhodnutia
- ▶ Zmluvy a tendre

Organizácie - prípadové štúdie

- ▶ Na siedmich firmách sme vyskúšali všetky zdroje a popísali, koľko informácií sme našli
- ▶ Použili sme elektronické trhovisko na nájdenie používaných bezpečnostných softvérov na ministerstvách.
- ▶ V elektronickom trhovisku sme našli tendre na predĺženie licencie Esetu pre viacero ministerstiev.

Webové stránky

- ▶ Cieľ – nájsť spriaznené webové stránky
- ▶ Nájdenie špecifickej metódy pre SK web a automatizácia
- ▶ Nástroj využíva verejne dostupný zoznam SK webových stránok a niekoľko databáz, ktoré sme vytvorili webcrawlingom

Dezinformačné webové stránky

- ▶ Ukážka databáz a metód na hľadanie administrátorov dezinformačných stránok
- ▶ Popis rôznych využití nástroja *blbec.online*

Red teaming

- ▶ Red teaming – simulácia útoku na organizáciu
- ▶ Prvá fáza útoku býva zvyčajne OSINT
- ▶ Pre túto fázu sme popísali metódu a demonštrovali sme ju na organizácii Univerzity Komenského
- ▶ Našli sme viaceré informácie, ktoré by mohli pomôcť útočníkom
 - ▶ Otvorené služby
 - ▶ Uniknuté heslá zamestnancov
 - ▶ Heslá verejne dostupné na Githube, Pastebine
 - ▶ Umiestnenie niektorých kamier v budovách UK
- ▶ Zanalyzovali sme, v ktorých častiach RT pomohli slovenské zdroje

Ďalšie možnosti výskumu

- ▶ Množstvo zdrojov by mohlo byť lepšie popísaných pomocou OCR
- ▶ Podobný výskum sa dá robiť pre iné krajiny
- ▶ Výskum ukazuje len momentálny stav – zdroje zvyknú pribúdať a ubúdať a preto je dôležité výskum pravidelne aktualizovať
- ▶ Niektoré oblasti sme nepreskúmali do hĺbky, napr. špecificky slovenské sociálne siete

Záver

- ▶ Popísali sme momentálny stav OSINTu v Slovenskej Republike
- ▶ Navrhli sme postupy na hľadanie niekoľkých typov informácií
- ▶ Vybrané postupy sme zautomatizovali

Odpoveď č.1

- ▶ Vedeli by ste zhodnotiť užitočnosť údajov v otvorených štátnych datasetoch (<http://data.gov.sk/dataset>) pre účely datasetov na tejto stránke
- ▶ Na stránke sa nachádzajú špecifické datasety ktoré obsahujú osobné údaje o niektorých ľuďoch
- ▶ Ťažko sa vytvára komplexný obraz stránky, datasety nie sú zoradené logicky ale len podľa toho, ktorý úrad ich zverejňuje

Odpoveď č.1 pokračovanie

- ▶ Mnoho datasetov sa týka rôznych vydaných oprávnení a zoznamov ľudí – napr. veterinári, exekútori, notári, oprávnenia na predaj húb
- ▶ Jediný spôsob ako využiť tieto datasety je všetky ich stiahnuť a prehľadať ich na meno danej osoby.

Odpoveď č.2

- Je ťažké uveriť, že administrátori rôznych dezinformačných stránok stále zverejňujú príspevky v natoľko krátkych časových intervaloch. Čo to podľa autora môže hovoriť o prevádzkovateľoch daných stránok?

Báječný lekár Zdieľal link 04.04.2020 12:59:35
♥ 23 Reakcií 💬 5 Komentáre ➦ 5 Zdieľania

Recepty a rady pre všetkých Zdieľal link 21.04.2020 14:46:31
♥ 0 Reakcií 💬 0 Komentáre ➦ 0 Zdieľania

Báječné zdravie Zdieľal link 21.04.2020 14:46:39
♥ 0 Reakcií 💬 0 Komentáre ➦ 0 Zdieľania

Sme Slováci Zdieľal link 21.04.2020 14:46:42
♥ 4 Reakcií 💬 1 Komentáre ➦ 2 Zdieľania

Báječná vareška Zdieľal link 21.04.2020 14:46:46
♥ 14 Reakcií 💬 5 Komentáre ➦ 0 Zdieľania

Báječné ženy Zdieľal link 21.04.2020 14:47:13
♥ 19 Reakcií 💬 5 Komentáre ➦ 1 Zdieľania

Báječný lekár Zdieľal link 21.04.2020 14:47:16
♥ 7 Reakcií 💬 0 Komentáre ➦ 1 Zdieľania

Odpoveď č.2

- Je ťažké uveriť, že administrátori rôznych dezinformačných stránok stále zverejňujú príspevky v natoľko krátkych časových intervaloch. Čo to podľa autora môže hovoriť o prevádzkovateľoch daných stránok?



Báječný lekár Zdieľal link 04.04.2020 12:59:35
♥ 23 Reakcií 💬 5 Komentáre ➦ 5 Zdieľania

Recepty a rady pre všetkých Zdieľal link 21.04.2020 14:46:31
♥ 0 Reakcií 💬 0 Komentáre ➦ 0 Zdieľania

Báječné zdravie Zdieľal link 21.04.2020 14:46:39
♥ 0 Reakcií 💬 0 Komentáre ➦ 0 Zdieľania

Sme Slováci Zdieľal link 21.04.2020 14:46:42
♥ 4 Reakcií 💬 1 Komentáre ➦ 2 Zdieľania

Báječná vareška Zdieľal link 21.04.2020 14:46:46
♥ 14 Reakcií 💬 5 Komentáre ➦ 0 Zdieľania

Báječné ženy Zdieľal link 21.04.2020 14:47:13
♥ 19 Reakcií 💬 5 Komentáre ➦ 1 Zdieľania

Báječný lekár Zdieľal link 21.04.2020 14:47:16
♥ 7 Reakcií 💬 0 Komentáre ➦ 1 Zdieľania

Odpoveď č.2

- ▶ Krátke časové intervaly zdieľaní sa dajú vysvetliť viacerými hypotézami
- ▶ Môže ísť o automatizovaných botov, ktorí zdieľajú tieto príspevky
- ▶ Administrátor stránky môže mať otvorených viacero tabov a použiť len copy paste
- ▶ Napoly manuálne, napol automatizované riešenie (makro)
- ▶ Nevieme vyvrátiť ani jednu z týchto hypotéz.