Week in OSINT #2018–35

Your regular weekly update is back! With some tools, a blog, some sites and even an infographic!

Sector035 Follow
Sep 2, 2018 · 5 min read

Last week I had a guest author for the first time and I received some very positive feedback! Not only about that, but also about what was in the news letter. I loved it that someone could take over and write this news letter and share their own knowledge about things they are passionate about. So there will be some more guest writers in the future, but I am also asking you to contact me if you have a niche area to cover! There are two guest editions planned at this moment, so I definitely can use some more! But first things first, let's go over this weeks overview:

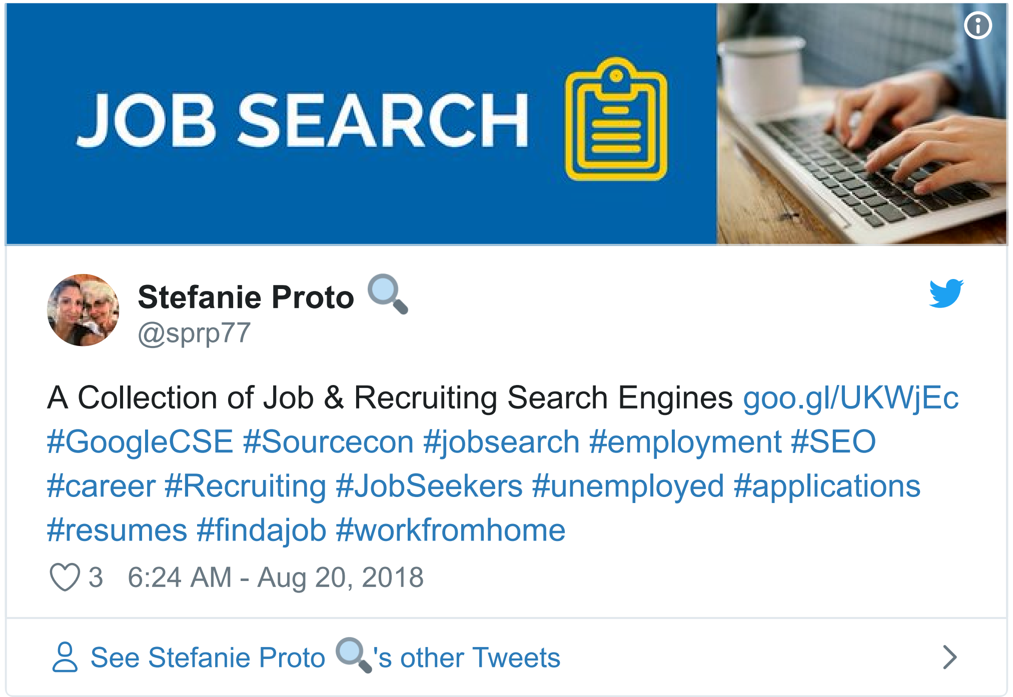
- Job Search Engines
- Dark Web Investigation Tools
- Visualizing the Social Media Universe

- OSINT.link Resource Portal
- POOPAK
- Are All Sources Created Equal?
- Photon
- CYMON
- Mitaka
- Lorand’s Start.me

. . .

Job Search Engines

Some of you would go: Job search engines? Why? As most of you know already, OSINT can be used for a variety of things. One of them is a physical security assessment and what better way to get inside the target company than to respond to a job vacancy. Here is a Google Sheet full of job search engines to use in case you ever need it.



Stefanie Proto 🔍
@sprp77

A Collection of Job & Recruiting Search Engines goo.gl/UKWjEc #GoogleCSE #Sourcecon #jobsearch #employment #SEO #career #Recruiting #JobSeekers #unemployed #applications #resumes #findajob #workfromhome

♡ 3 6:24 AM - Aug 20, 2018

See Stefanie Proto 🔍's other Tweets

Talking about that, Stefanie Proto herself is still looking for a job in the Connecticut area, or remote if possible. Despite her own awesome list of resources, she hasn't been able to find work yet. So whether you have a position as a starting analyst or a seasoned office manager, please get in touch with her.

Link: https://docs.google.com/spreadsheets/d/1cAeOLwsM65pDJus5xIaZf-yfSEh1g6-59yzc00TyR9Y

. . .

Website: Dark Web Investigation Tools

The IACA Dark Web Investigation Support website is set up by the International Anti Crime Academy based in The Netherlands. This academic institute has specialised in open source intelligence and social media intelligence (OSINT and SOCMINT). They provide several search tools to find information in marketplaces, sites and social media platforms that are hosted on the Dark Web.

Link: https://iaca-darkweb-tools.com/

• • •

Infographic: Visualizing the Social Media Universe

This infographic does not just name the most popular social media sites, but also show their size in users. There are more posts on this website regarding social media, for instance the adoption rate of media platforms, what happened on the internet every minute in 2017 and a huge overview of (social) media platforms that were known last year. So if you are hunting for new platforms to explore, then have a look at these pages.

Link: http://www.visualcapitalist.com/social-media-universe/

. . .

Links: OSINT.link Resource Portal

And again there is a huge link collection that popped up lately in my Twitter timeline. I am not sure which tweet pointed me to it, but more important to know is that is run by the Twitter account onlineosint.

From search engines to news sites, from data leaks to government records. Everything is neatly organised, very easy to get to and an awesome new source for websites.

Link: http://osint.link/

Tool: POOPAK

POOPAK is a hidden service crawler for the dark web, running on your own instance. It is built to run in a Docker container and has some very nice features. It extracts things like URL’s, Email addresses, EXIF data, BTC/ETH addresses, makes screenshots, runs security tests and even provides an easy to use GUI. So fire up your VM, clone the repo and go out and explore the dark crevices of the internet!

Link: https://github.com/thelematic/poopak

. . .

Blog: Are All Sources Created Equal?

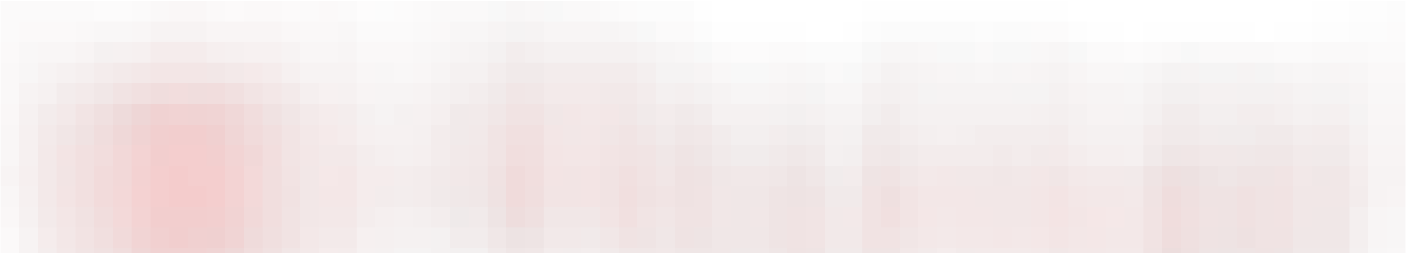
At Capteurs Ouverts they have been thinking about the several sources of information, but especially how reliable the sources and the information itself is. They came up with a proposal to give a score to the information gathered and the sources it came from. More information in the blog post.

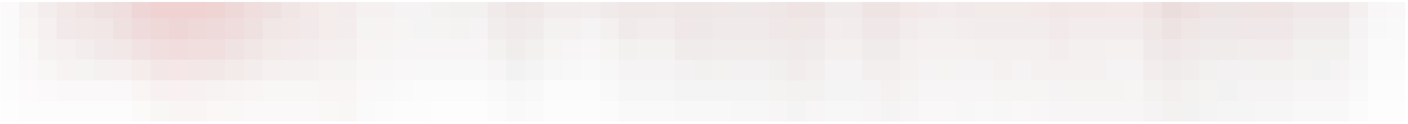
Link: https://capteursouverts.com/en/2018/08/19/are-all-sources-created-equal/

. . .

Tool: Photon

Photon is a very interesting little web scraper for OSINT work. It doesn't just download a website, but it also goes through the data and extracts email addresses, social media accounts, Amazon buckets, URL's that contain parameters, files, keys and lots more! So whether you need some basic recon on a website for a blackbox assessment, or want to find people for social engineering, maybe give this tool a go!





Link: https://github.com/s0md3v/Photon

. . .

Website: CYMON

Last week I discovered another website full of information regarding malware, botnets and spam. You can search on hashes, IP’s or domains and filter the results to see what is publicly known about any threat that for instance a company is involved in. Via the timeline option on the left you can see all the events that have been indexed there, with all information that is known about it. It’s maybe not a one-stop-shop for threat intel, but just one of those sites that maybe can provide you with the specific info that you need.

Link: https://cymon.io/

. . .

Plugin: Mitaka

Mitaka is a Chrome extension and according to their own description on GitHub it is an OSINT friendly ‘indicator of compromise’ search tool. With a single right click on a piece if information it is possible to run reverse WHOIS look-ups, run queries on Shodan or Censys, find related information at Talos Intelligence or Hybrid-Analysis and so on.

Get to GitHub to check out the code, or directly install the extension from the Google store and start playing!

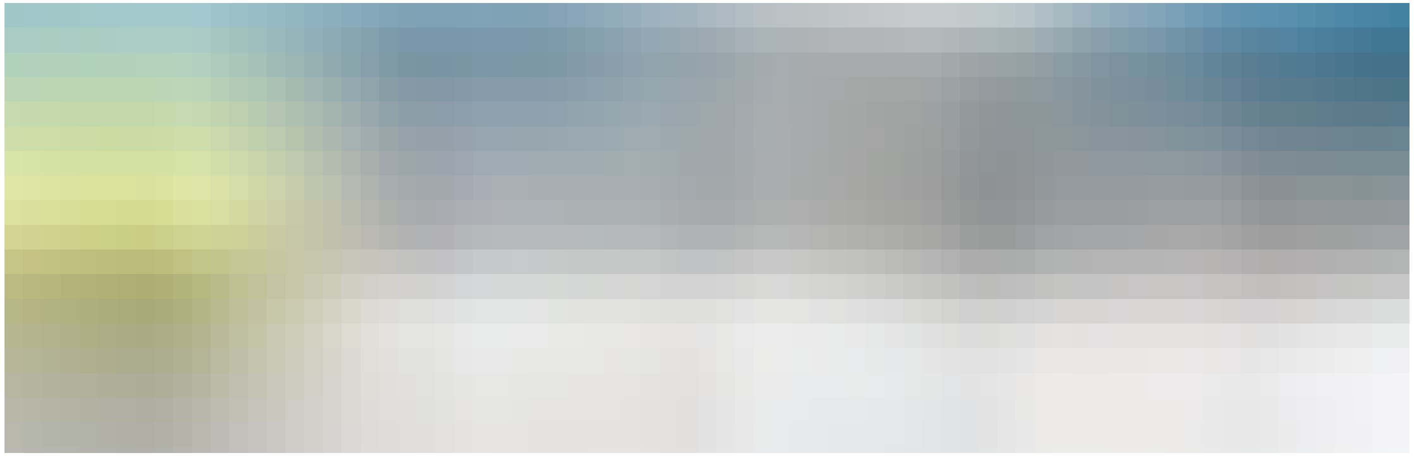
Link: https://github.com/ninoseki/mitaka

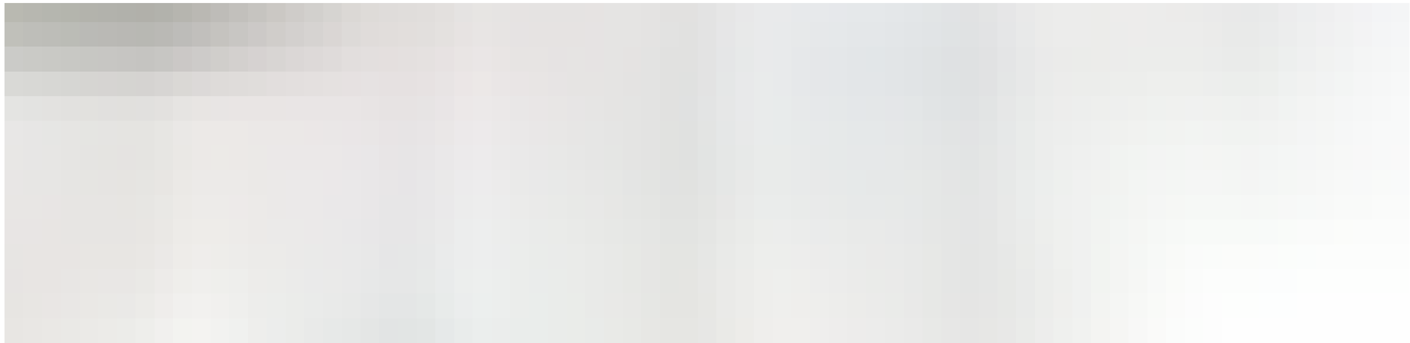
Install:
https://chrome.google.com/webstore/detail/mitaka/bfjbejmeoibbdpfdbmbacmefcbannnbg

. . .

Links: Lorand's Start.me

Last week Lorand Bodo decided to share his set of links that deal with radicalisation and terrorism. A huge set of incredibly interesting and useful links! So this will take some time to go through…





Link: https://start.me/p/OmExgb/terrorism-radicalisation-research-dashboard

· · ·

And that was it! A nicely filled news letter again, trying to satisfy everybody that reads this. You have ideas, interesting links, or want to be a guest writer for once? Get in touch with me via sector035 on Twitter!

Have a good week and have a good search!

Osint Verification

133 claps 1

Sector035

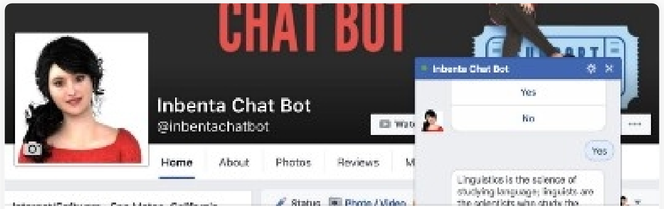
Follow

Just a shadowy nerd... Busy with InfoSec, geolocation and OSINT

Week in OSINT

Follow

Your weekly dose of OSINT websites, tools and aimed at anyone working in the field of analysts, researchers and pentesters.



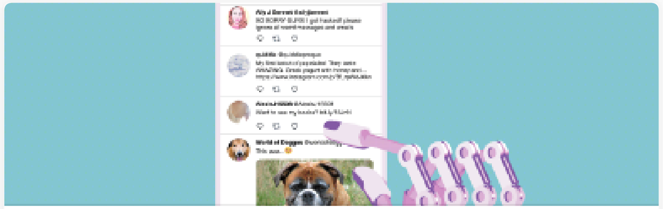
Related reads ★

Incident Report Guessing: Chatbots, the BA Hack and...

Prof Bill Buchanan OBE

Sep 8, 2018 · 4 min read ★

27



Related reads ★

Hackers Are So Fed Up With Twitter Bots They're Hunting Them Down...

The Intercept

Mar 16, 2018 · 10 min read

623

Related reads

Discovering Hidden Email Gateways with OSINT Techniques

Gabor Szathmari

Oct 9, 2018 · 7 min read

279

Responses

Write a response...

Show all responses