OPEN-SOURCE INTELLIGENCE

Syomin K.A.

Belarusian State University of Informatics and Radioelectronics
Minsk, Belarus

Liakh Y.V. – senior teacher

The article deals with the term of Open source intelligence, the role of it in our life, as well as with the main OSINT tools, special commands and examples.

Open source intelligence (OSINT) is information collected from public sources such as those available on the Internet, although the term isn't strictly limited to the internet, but rather means all publicly available sources like mass media, newspaper, radio, magazines, TV [2].

With the development of the Internet, the need for newspapers and radio has decreased dramatically. Now the main front of intelligence has gone to the Internet. Modern people spend a lot of time on the Internet without thinking about what data about themselves they leave on the network. We leave our personal data such as cookies, browser fingerprints, our photo with metadata, queries to the search engine.

All information collected about you is sold to advertising companies. They need it in order to find the kind of advertising that you are sure to be interested in information security and forensic experts use various tools to quickly find and filter the information they need.

And the first tool which everyone has is a Google search engine. To be more precise, it is Google Dorks. A Google dork query, sometimes just referred to as a dork, is a search string that uses advanced search operators to find information that is not readily available on a website. Google dorking, also known as Google hacking, can return information that is difficult to locate through simple search queries [3].

There are some special commands which can help you to find anything:

inurl:followed by a particular string returns results with that sequence of characters in the URL.

intitle:followed by a particular string returns results with that sequence of characters in the title.

site:returns files located on a particular website or domain.

filetype:followed by a file extension returns files of the specified type, such as DOC, PDF, XLS

lang: search only on “lang” site.

More interesting commands and query examples you can find on Google Hacking Database [1]. The Google Hacking Database (GHDB) is a compendium of Google hacking search terms that have been found to reveal sensitive data exposed by vulnerable servers and web applications.

Shodan is a search engine for Internet-connected devices. Web search engines, such as Google and Bing, are great for finding websites. Shodan gathers information about all devices directly connected to the Internet. If a device is directly hooked up to the Internet then Shodan queries it for various publicly-available information. The types of devices that are indexed can vary tremendously: ranging from small desktops up to nuclear power plants.

Maltego is a type of software used for open-source intelligence and forensics, developed by Paterva. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining. Among its data sources are DNS records, whois records, search engines, online social networks, various APIs and various meta data. It is used by security researchers and private investigators.

Also, you can use different online-services to find people by their phone number, usernames, real name, last name like spokeo.com, thatsthem.com, beenverified.com, fastpeoplesearch.com, privacystar.com, getcontact.com, everycaller.com. People search websites allow to opt out, but after people remove themselves from listings, new search services appear with their records in them. The reason for that is the same dataset is bought and used by different services.

To conclude, it’s hard to stay private in the post-privacy world and control what information is floating in this digital ocean. While you can’t control everything that’s out there about you, it’s important to be at least aware about it. It goes without saying, that in the digital age, information plays a key role, so those who know how to find it will always be one step ahead. Turn around, maybe someone's watching you already.

References:

1. Google Hacking Database [Electronic resource]. – Mode of access: https://www.exploit-db.com/google-hacking-database. – Date of access: 15.04.2020.

2. Open-source intelligence [Electronic resource]. – Mode of access: https://en.wikipedia.org/wiki/Open-source_intelligence. – Date of access: 16.04.2020.

3. OSINT: How to find information on anyone [Electronic resource]. – Mode of access: https://medium.com/the-first-digit/osint-how-to-find-information-on-anyone-5029a3c7fd56. – Date of access: 16.04.2020.