Open-Source Intelligence and how to assist law enforcement agencies with ongoing investigations

Eleftherios Athousakis
Μέλος της ΑΛΛΗΛΟΝ
Cyber Security Specialist, ΥΠΕΘΑ
Eleftherios A. | LinkedIn

Summary
This year in mid-August, during **DEFCON 31**[1], one of the most prestigious and well-known cyber conventions held annually in Las Vegas, Nevada I was part of an Open-Source Intelligence (OSINT) Global search party event. The people behind it from **Trace Labs**[2] came in direct contact with the Law Enforcement (LE) agencies in U.S. and provided the participants with information on missing persons and the teams were scanning the internet for information that could help. The adrenaline and the enthusiasm during the 4 hours long event were untold as people from around the globe were volunteering their skills and time to help someone they didn't know and never will. Here's some things about OSINT that could get you started.

What exactly is Open-source intelligence (OSINT)?

Open-source intelligence (OSINT) is the collection, analysis, and evaluation of publicly available information. It can be used by law enforcement agencies to gather intelligence on a variety of criminal activities, including terrorism, illegal trafficking, and organized crime, by armed forces to understand/predict enemy movements and use of locations as well as from investigators employed by companies to gather intelligence on rivals as to their movements, methods, customers, products etc. As you can understand the possible applications of OSINT in today's connected and mostly, in wrongdoing by us, "publicly shared" life are infinite.

OSINT is a valuable tool for analysts and law enforcement because it is a cost-effective way to collect information that can be used to relate cases and solve crimes. It can also be used to gather information that would be difficult or impossible to obtain through other means, such as undercover operations or wiretaps. Let's take a look on the differences between open-source data, information, and intelligence as they are described in the United States Joint Intelligence Joint Publication 2-0 and the NATO OSINT Handbook v1.22 broken down into three core sections:

Open-Source Data (OSD) is raw content that is gathered or collected.
With the understanding of where it came from (its source) and with other data to provide context and meaning, we can perform processing tasks on it to transform the individual bits into something more meaningful information.
Open-Source Information (OSIF) which is processed data that leverages
filtering and validation processes. OSIF is also "exploited," which means that places of interest within the data are identified that the agency may find useful.
Scrutinizing the information, adding analysis, making recommendations,
and publishing the results in a solid report,

[1] DEFCON https://defcon.org/
[2] Trace Labs https://www.tracelabs.org/

is changing information into Open-Source Intelligence (OSINT). And this is our final goal.

Different types of OSINT

There are different types of OSINT that can be used to help law enforcement agencies, such as social media posts, photos, or videos, that people upload in their accounts, and an analyst can search through public records, news articles financial information and cryptocurrencies as well. Here's an indicative list:

Social media OSINT

This involves collecting and analyzing information from social media platforms, such as Facebook, Twitter, and Instagram as well as newer platforms of Snapchat and Tic-Toc. Social media OSINT can be used to identify suspects, track their movements, and gather intelligence on their activities.

Public records OSINT

This involves collecting and analyzing information from public records, such as court records, property records, and business records. Public records OSINT can be used to verify a suspect's identity, obtain their contact information, and learn about their financial history and the amount of information that can be gathered depends on the country's legislation.

News and media OSINT

This involves collecting and analyzing information from news articles, blogs, and other media sources. News and media OSINT can be used to learn about current events, identify potential threats, and track the activities of criminals and terrorist groups.

Geolocation OSINT

This consists of collecting and analyzing information from sources to help you boost geolocation and vehicle tracking intelligence to identify possible routes and installations used by those you are looking for.

Cryptocurrency OSINT

It is extremely valuable to examine the intersection of illicit crypto activity and online publicly available information. Open-source data can uncover a wealth of valuable information to help identify cryptocurrency crimes, resolve identities, and track threat actors as they seek out more anonymous cryptocurrencies or exchanges[3].

Dark web OSINT

This involves collecting and analyzing information from the dark web, which is a hidden part of the internet that is not accessible through traditional search engines. Dark web OSINT can be used to identify suspects who are involved in illegal activities, such as drug, weapons or human trafficking and cybercrime, especially breached data.

Challenges of using OSINT

One of the biggest challenges of using OSINT is the vast amount of information that is available. The internet is constantly expanding, and new information is being created all the time. This can make it difficult to find the information that is relevant to your investigation and to filter out the noise which constitutes the second great challenge.

There is a lot of misinformation and disinformation online, and it can be difficult to distinguish between what is true and what is not. This can make it time-consuming and difficult to find the information that you need and always verify your information to your best ability.

In order to be able to get a clear path you have to have a goal in your mind. Before you start your OSINT investigation, it is important to ask the right questions "What can we find out about the target". What information are you trying to find? Once you have identified your goal, you can begin by creating the framework that will govern your assessments. Afterwards you can start to narrow down your search and

[3] FIVECAST https://www.fivecast.com/blog/the-role-of-osint-in-cryptocurrency-compliance/

focus on the most relevant sources.

Tips to Prevail

Use a variety of sources. Don't rely on just one source of information. Use a variety of sources and cross check your information to get a more complete picture and be critical of the information that you find. Not all of the information that you find online is true. Disinformation is part of the internet nowadays and a lot of information is used to mislead analysts and investigators. Be critical of the information that you find and verify it from multiple sources before using it.

Use OSINT tools and techniques. There are a number of OSINT tools and technologies available that can help you to collect, analyze, and evaluate OSINT data faster than just using a web browser. These tools can help you to save time and to filter out the noise.

Using your knowledge for the greater good

OSINT is a powerful tool that can be used to help law enforcement agencies to solve crimes and keep communities safe. However, it is important to remember that OSINT is not a silver bullet. It is just one tool in the law enforcement toolbox. To be effective, OSINT must be used in conjunction with other investigative methods.

The future of OSINT is bright. As the amount of information available online continues to grow, law enforcement agencies will need to develop new and innovative ways and allowing volunteers to use OSINT to make a difference could be the winning factor. This can possibly end up in training with the law enforcement officers on how to combine the use of OSINT by all parties effectively and developing new tools and technologies to help them collect, analyze, and evaluate information for the common good.

References

NATO OSINT Handbook v1.22 https://archive.org/details/NATOOSINTHandbookV1.2

United States Joint Intelligence Joint Publication 2-0 https://irp.fas.org/doddir/dod/jp2_0.pdf

SANS OSINT Resources https://www.sans.org/osint/