Open-source intelligence (OSINT)

Open-source intelligence (OSINT) is the collection and analysis of public data to produce useful intelligence. This process could not require any existing technical knowledge since it exists several publicly available tools. The only thing needed, that can be trained, is the capacity to link data to create information.

It was mainly developed by the US Department of Defense in response to the September 11 attacks. Since then, it has become popular and is widely used not only by the US intelligence services.

Nowadays, many intelligence services are using OSINT for getting actionable intelligence. Some police services are also using it for solving their investigations and individuals for either good or bad reasons.

Each one of us can make its own research using tools and methodology.

Process: each case is different so actions may differ although steps remain the same.

The main steps are:

- Collect the maximum amount of data
- Identify targets and exploitable vulnerabilities
- Perform a physical intrusion

Generally, by working in a company, the targets are companies and people. At the beginning, not much information is available, and it could be a bit tricky. The key is to not look for anything particular but to gather as much data as possible.

There are many ways of retrieving data in OSINT and the scope of what is possible to get can be disarming. Fortunately, it exists some charts for knowing what to look for and frameworks gathering several tools.

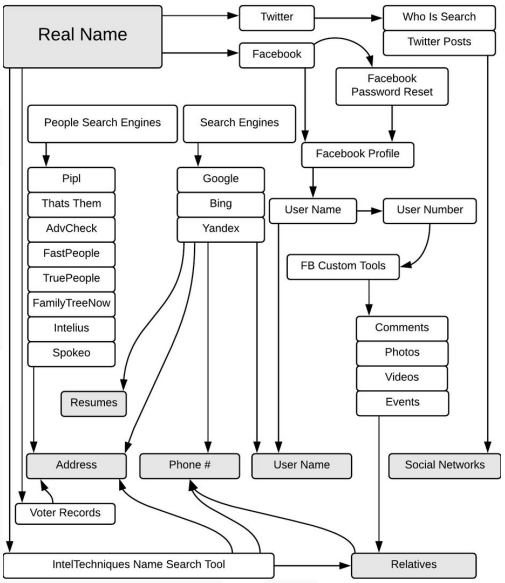


Figure 1 – OSINT chart

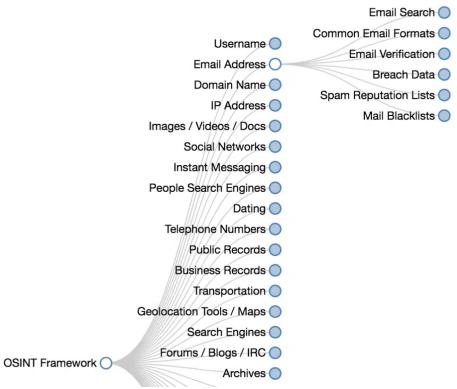


Figure 2 – OSINT framework

For companies, it could be interesting to know who the employees are, what are their role in company, if they talk about their professional and/or personal life on Internet, etc.

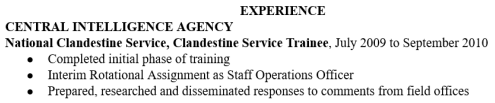
Many different types of data can be useful. A lot of personal information is

publicly available to all of us on social networks, for example your name, your job, your relationships, your location, etc. (Facebook, Instagram, Twitter, LinkedIn, Google). Even nonpublic information can be retrieved for some of them, and it is possible to know who your colleagues are and what you posted. It is also possible to guess the missing information based on the few available with some tools. For instance, just with an email address it is possible to know what account you have (social networks, daring sites).

A lot of tool exists for collecting as many information as possible, like email address, phone number, photo, postal address, etc. Sometimes, it can be scary considering the amount of intrusion it is in your life such as videos from publicly available and non-protected camera. Here is a screenshot of a video flow from inside an office in Spain but there are many more on factories and homes.

Figure 3 – Office video

The scope of a research about non-sufficient protected files is not restricted to video and for example a simple web request is enough to find confidential data. Google documents are not necessarily protected against public research and therefore anyone could possibly have access to your files. Here is an extract from a resume obtained by a complex web request (Google Dorks).



EXPERIENCE

CENTRAL INTELLIGENCE AGENCY

National Clandestine Service, Clandestine Service Trainee, July 2009 to September 2010

- Completed initial phase of training
- Interim Rotational Assignment as Staff Operations Officer
- Prepared, researched and disseminated responses to comments from field offices

Figure 4 - Resume extract

Although this person no longer works at the CIA, it is a former employee and could possibly have sensible information for an enemy country.

Protection: it is easy to get public information about anyone, but it is also easy to protect oneself.

It is important to check the amount of your personal data is publicly available online. Of course, everyone like to share its own life on social media, for instance its holidays or the workplace. However, regarding the previous examples it could be dangerous as a malicious person could take advantage of that information. An attacker can use this information do phishing against you or your relatives, sell it to companies for making money, steal your identity or even break into your house.

The basic rule is to not share everything in your life publicly. For example, if you go on holidays and you make a post on a social media about it, that means you are not at your home, and it could possibly be burglarized.

Figure 5 – Brest Tower

If you were on holydays, you probably going to take photos and here is one of a French monument. With a special web browser (Yandex), you can make an inverse image request and determine the location of a photo. Sometimes, you can only guess the city and then you have to navigate on a web mapping platform such as Google Maps.

Another good advice would be to create and use different email addresses: one for administrative purposes like bank or tax and another one for a more personal use. So, when you receive an email in the address not designed for that you can directly know that is a scam.

One fraud that becomes more and more spread is whaling. The objective is to impersonate the CEO of a company and call someone important in that company, for instance an accountant. Then, the attacker would ask to make a transaction very quickly, in less than an hour, because claiming else a very big client would be loss. It does not fail all the time, but it happens more frequently that we could think. If the company is small enough and the bank account is emptied, then company will not have any other choice than to declare bankruptcy and all employees will lose their job.

Moral: although OSINT is (almost) legal, it is not necessarily a moral thing.

As said previously, it is possible to get private or even confidential documents with a complex web request. Those documents are available to all of us if we know how to access it. However, even if the login access is not broken you are potentially browsing on a private company intranet and doing so is illegal.

Some time ago in France, a phishing campaign was widely spread and faked a police summoning. A lot of people received it, they were accused of sexual crimes and the email claimed the victims had to pay a fine if they did not want to be arrested. The police will never send you an email if you were accused of anything, they would at least send a registered letter or directly talk with you.


BRIGADE DE PROTECTION DES MINEURS
REPUBLIQUE FRANÇAISE
Liberté – Egalité – Fraternité
MINISTÈRE DE L'INTÉRIEUR
Gendarmerie Nationale
Gendarmerie nationale
CONVOCATION
ARNAQUE !

Figure 6 – Phishing scam

The goal for the attacker is it to get money from people not questioning the validity of that email. No matter if the victims pay or not, it is not neutral receive a such email. You think you will be accused of a serious crime and maybe end in prison; it could devastate someone's life.

Thus, OSINT is a powerful tool to get intelligence on people, companies, and

governments. It is possible to gain a significant advantage with it by knowing some information others do not know. Of course, it is not without risks because it is in the edge of being illegal and occasionally cause severe damage to people.

[1] 'OSINT Chart'. *Medium*, https://miro.medium.com/max/1050/1*4WMnGFT_Z0UJ3QN3vDLrhw.png. Accessed 12 July 2022.

[2] Nordine, Justin. 'OSINT Framework'. *OSINT Framework*, https://osintframework.com. Accessed 12 July 2022.

[3] 'Office Video'. *Insecam*, http://insecam.org/en/view/1006526/. Accessed 12 July 2022.

[4] WILLIAMS, LYNNAE. 'Resume Extract'. Google Docs, https://docs.google.com/document/d/1WCzVD65qqfQgV9Sx73h1BykFU9kciKLYa-nwSkdIwEo/edit. Accessed 12 July 2022.

[5] 'Brest Tower'. *Office de Tourisme de Brest Métropole*, https://www.brest-metropole-tourisme.fr/sortir-bouger/agenda/evenements/visites-flash-brest-cote-panoramas-56057. Accessed 12 July 2022.

[6] 'Phishing Scam'. *Wiclic*, https://www.wiclic.fr/arnaque-fausse-convocation-gendarmerie-pedophilie-pedopornographie/. Accessed 12 July 2022.