HC3: Analyst Note

August 9, 2022 TLP: White Report: 202208091700

OSINT How-To

Executive Summary

Open-Source Intelligence (OSINT) is the act of obtaining intelligence from publicly available resources. It has been around for a long time and was even used as a collection method in World War II. With the advancement of technology and more specifically the internet OSINT has become a valuable tool for many security and intelligence organizations. It can produce effective results with a reasonably low cost. Resources being utilized can come from many places including newspapers, court filings, and of course the internet. Activity on the internet can be more active or passive in nature and investigators should be aware of the wealth of information that exist on the deep and dark web. These layers are estimated to be about 95% of the information available on the internet. Social Media Intelligence is also an important branch of OSINT that has risen over the years which has the potential to reveal information such as a user's geolocation. Tools used to leverage OSINT can be free to use or a paid service and many of them don't require any technical knowledge.

What is Open-Source Intelligence?

Open-source intelligence is the data and information that is available to the public. Its not just the information that we can access online from a search engine. It can come from many sources and it's a valuable tool for security professionals and intelligence organizations, but it's also important to be aware that threat actors leverage OSINT for their own benefit as well. Information available to the public isn't necessarily just free information either it can consist of proprietary or subscription-based information that is available such as a news journal. It could also be information and data that is only available upon request.

Other OSINT Sources

- Newspapers
- Magazine articles
- Academic papers
- Other research
- Books
- Social Media
- Court filings
- Arrest Records
- Public trading data
- Public surveys
- Location data
- Breached data information
- Public indicators (IPs, domains, or hashes)
- Certificate/Domain registration data
- Application/system vulnerability data

How to Collect OSINT

When collecting OSINT it's always good to start off with formulating a strategy and having a framework of what your goals are before you start your collection. This will also aid in documenting activity during your investigation along with following or creating your organizations standard operating procedure (SOP) beforehand. There is a seemingly unlimited amount of publicly available information and its important to not just find information that is relevant, but to find information that can answer the questions you are looking for. You should define what your goal is and what you need to accomplish that. This will help you decide what tools you need to use and if you need to be passive, semi-passive, or active in your collection.

Passive: Passive collection is the most common type of OSINT and the intent behind it is to only target publicly available information.

Semi-Passive: Semi-passive is more technical in nature. Through this form of collection an investigator will be sending traffic to a server to gather information.

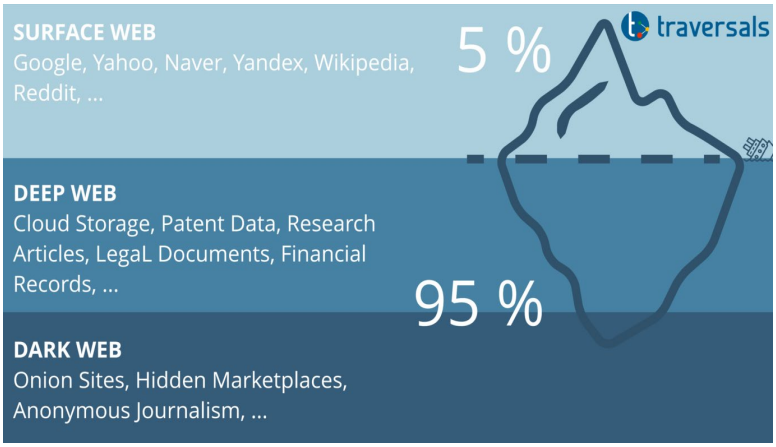
Active: In active collection you would be directly engaging with a system or even a person. This can increase the likely hood of being noticed due to the nature of harvesting data around scanning for vulnerabilities or looking for open ports, which is normally considered malicious.

Performing OSINT can reveal a lot of information about something or someone, but investigators should also take the time to protect their own identity and reduce their digital fingerprint. Investigators should take the time to educate themselves on the best way to hide their identify as doing so is very important to avoid being flagged during any reconnaissance or research. Lastly, prior to starting any OSINT investigations you should contact your legal department or OSINT authority figure. You'll want to make sure that your actions are within company standards.

OSINT and the Internet

The internet is a great resource for conducting OSINT and its typically the first one to go to with how easy it is to access the vast amount of information available. It's also important to understand the full scope of how to search for information outside of the everyday engines such as Google, Yahoo, and Bing. Advance searches such as Google Dorks, sometimes just referred to as dorking, is a search string that lets you find information that isn't always readily available on a website. In essence, you are revealing hidden information on public websites. It can often show old and forgotten documents and site pages that are still live and accessible. Though this sensitive information can be accessed. While there is nothing illegal about Google Dorking, accessing certain information especially from government sites is, so it is important to be careful when leveraging this. It is more recommended to use this function to test your own security.

While using OSINT online it is also important to know the layers of the internet and what data is accessible on each one. Standard search engines only reveal a small portion of the information that is out there. The three most common layers are the surface web, deep web, and the dark web.



Source: Traversals

HC3: Analyst Note

August 9, 2022 TLP: White Report: 202208091700

Majority of the information online exist in the deep and dark web. The surface web is the information being accessed through mainstream search engines. Accessing the dark web requires the use of a tor browser, which not only grants access to these additional layers, but it is designed to help keep the user anonymous and prevent traffic analysis. Simply just browsing the dark web is relatively safe. However, it is always recommended to keep your privacy if doing research outside of the surface internet. Some of the best practices include:

Use a VPN

When using a VPN your data is encrypted before going to your Internet Service Provider (ISP) and it can also change your virtual location by hiding your IP address.

Create a fake profile

Websites like the fake name generator can help can create a fake identity by providing a name, street address, emails, social security, and even credit card numbers. This is helpful if you wanted to sign up for a chat room or forum. This is another area where you should contact your company's authority figure over OSINT to make sure you are operating within their policies.

OSINT and Social Media

Social Media Intelligence (SOCMINT) is a branch of open-source intelligence, but the information being collected is obtained from social media websites. Platforms like Facebook, Snapchat, and LinkedIn can provide a wealth of information on a target for security professionals and threat actors alike, especially for those looking to craft a convincing spear phishing email. Social media is also a great way to gauge interest on a topic.

The data obtained from SOCMINT is usually broken down into two separate categories:

- Content posted by the person: profile pictures, images, and other multimedia files
- Secondary metadata such as birthdates, geolocation, friends, workplace, and political views

OSINT Common Tools

There are plenty of tools available for anyone performing OSINT. They can range from simple to requiring more technical knowledge to use. Many websites have already collected and compiled OSINT tools, which is great so users to have them available in one place. Usually, these websites will also categorize the tools so it's easier for you to determine which tool you need to accomplish an objective. Some of the resources out there are free and some of them have a cost to use it. Below are some of the most popular OSINT tools and what they are used for.

OSINT Technique's website is a great resource that contains all types of OSINT tools in one place.

Maltego takes the data you put it (IPs, emails, domain names, or URLs) and it will help find relationships in that data. It also creates a graph to help connect these relationships.

Creepy can pull geolocation information through social media and it can help you see where the device was when something was posted to the internet. You can also create a map of the data and filter it out.

Shodan is frequently referred to as the search engine for the Internet of Things. It can help you find devices that are connected to the internet and it can also reveal if a port is open on that device.

Google Dorking can help you perform advance searches that allow you to find more information on a website.

OSINT Framework is a great tool to help investigations make connections in their data. It also gives them ideas on where to look and where to look next after finding a piece of information.

WHOIS is a domain tool that can help you identify who owns a domain and how to get in contact with them. This data can help identify other connections in your framework.

TinEye is a reverse image search and just as the description implies it can help you find where an image originated online.

Whitepages allows you to search for background information on people by inputting their name, phone number, or street address.

Spiderfoot is a reconnaissance tool that can query information from the data you put in (domain name, IP address, email, etc.). It can provide you with OSINT on data leaks or other sensitive information that could aid you in your search.

References

Nordine, Justin. "OSINT Framework". Osintframework. https://osintframework.com/

OSINT Techniques. https://www.osinttechniques.com/osint-tools.html

CrowdStrike. "Open Source Intelligence". Feb 25, 2022. https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/

Maor, Etay. "How Attackers Use Open Source Intelligence Against Enterprises" TechTarget. Aug 18, 2021. https://www.techtarget.com/searchsecurity/post/How-attackers-use-open-source-intelligence-against-enterprises

Bule, Guise. "A Guide to Open Source Intelligence". ITSEC. https://itsec.group/blog-post-osint-guide-part-1.html

The Recorded Future Team. "What is Open Source Intelligence and How is It Used". RecordedFuture. Feb 19, 2022. https://www.recordedfuture.com/open-source-intelligence-definition

Kolb, Dirk. "Surface Web is Only the Tip of the Iceberg". Traversals. Aug 4, 2020. https://traversals.com/blog/surface-web/

TechTarget Contributor. "Tor Browser". TechTarget. April 2021. https://www.techtarget.com/whatis/definition/TOR-third-generation-onion-routing

Olech, Julia. “The Good Peoples Guide to the Dark Web (How to Stay Safe in 4 Easy Steps)”. WizCase. Jan 05, 2022. https://www.wizcase.com/blog/how-to-safely-use-the-dark-web/

A8 Team. “21 OSINT research tools for threat intelligence investigators” Authentic8. Sep 29, 2021. https://www.authentic8.com/blog/21-osint-research-tools-threat-intelligence-investigations

A8 Team. “OSINT 2021 Guide: tools and techniques for threat intelligence”. Authentic8. Oct 22, 2021. https://www.authentic8.com/blog/OSINT-2021-guide-tools-and-techniques?UTM=googlepaid&gclid=EAIaIQobChMIqIOMxNWC-QIV5MmUCR0iGwbEEAAYASAAEgKDL_D_BwE

Kolb, Dirk. “5 Ways to Protect your OSINT Investigations” July 08, 2020. https://traversals.com/blog/osint-investigations/

Zelleke, Liku. “The 8 Best OSINT Tools”. Comparitech. Jun 06, 2022. https://www.comparitech.com/net-admin/osint-tools/

Kadar, Tamas. “Top 10 OSINT (Open Source Intelligence) Software & Tools [2022]”. Seon. https://seon.io/resources/the-best-tools-for-osint/

Bisson, David. “10 Open-Source Intelligence Tools (That Actually Work With Your Existing Security Software)”. Securityintelligence. Sep 14, 2021. https://securityintelligence.com/articles/10-open-source-intelligence-tools-existing-security-software/

J. Pastor-Galindo, P. Nespoli, F. Gómez Mármol and G. Martínez Pérez, "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends," in *IEEE Access*, vol. 8, pp. 10282-10304, 2020, doi: 10.1109/ACCESS.2020.2965257. https://ieeexplore.ieee.org/abstract/document/8954668

Hassan, Nihad. “A Guide to Social Media Intelligence Gathering (SOCMINT)”. Secjuice. Jun 21, 2020. https://www.secjuice.com/social-media-intelligence-socmint/

Chan, Joei. “What is Social Media Intelligence (and How Can I Use It?)”. linkfluence. https://www.linkfluence.com/blog/social-media-intelligence

Jones, Tegan. “What is Google Dorking and How to Use It”. Gizmodo. Jan 19, 2021. https://www.gizmodo.com.au/2021/01/what-is-google-dorking-and-how-to-use-it/

Maltego Team. “Everything about Open Source Intelligence and OSINT Investigators (2021)”. Maltego. Oct 31, 2021. https://www.maltego.com/blog/what-is-open-source-intelligence-and-how-to-conduct-osint-investigations/#open-sourceintelligence-techniques-how-to-use-osint-for-your-work

The Recorded Future Team. “What is Open Source Intelligence and How Is It Used?”. RecordedFuture. Feb 19, 2022. https://www.recordedfuture.com/open-source-intelligence-definition

Hassan, Nihad. “An Introduction to Open Source Intelligence (OSINT) Gathering”. Secjuice. Aug 12, 2018. https://www.secjuice.com/introduction-to-open-source-intelligence-osint/

HC3: Analyst Note
August 9, 2022 TLP: White Report: 202208091700

Contact Information
If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback