OSINT

OPEN-SOURCE INTELLIGENT

DATE: 20-07-2023

COLLECT, ANALYZE, AND SPECIFIED

By HUMNA ABID

TABLE OF CONTENT

WHAT IS OSINT?

OSINT stands for Open-Source Intelligence. It is the practice of gathering and analyzing information from publicly available sources, such as social media, newspapers, and more. OSINT is used to gain insights, assess risks, and gather intelligence about individuals, organizations, events, or any subject of interest. Used by public, private, and Government organizations.

USE CASES

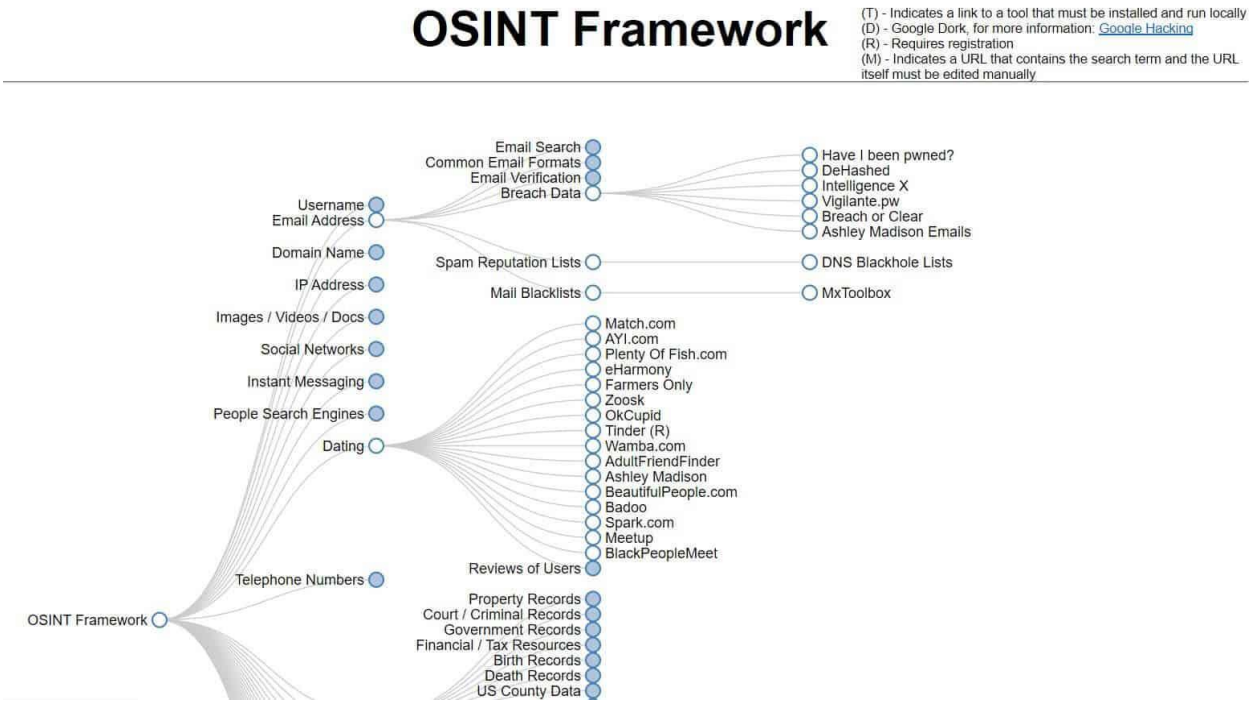
- Cyberoperation
- Social Media Investigation
- Risk Management

HISTORY

- 1939: First use of OSINT predates August, British government requests BBC to launch a civilian OSINT service.
- 1941: U.S. President F.D. Roosevelt creates Foreign Broadcast Monitoring Service (FBMS) to analyze propaganda messages against the United States.
- 1947: FBMS was renamed Foreign Broadcast Intelligence Service (FBIS) and placed under Central Intelligence Agency.
- 1948: Official partnership established between BBC and FBMS for the exchange of information.
- OSINT expands to business, politics, law enforcement intelligence, and academia.
- After 9/11, the U.S. enacts Patriot Act and Homeland Security Act to enhance information sharing and counterterrorism efforts.
- OSINT continues to play a vital role in various fields, including national security and research.

TOOLS USED IN OSINT

- OSINT Framework
- Goole Dorking
- Github Dorking
- Shodan
- SOCMINT (Social Media Intelligence)
    - Linkedin
    - Facebook
    - Twitter
- Instagram
- Spyse (detailed info regarding the domain can be found here)
- threatmap.checkpoint.com (cyber attack visualization)
- yougetsignal.com (web osint osint)
- hackertarget.com/ip-tools (web osint)
- grep.app (search on multiple github repos just using keywords)
- Maltego (using visualization)
- the harvester (email scraper from Domain)
- piple (premium using the domain, very useful information can be found, but it is not a free deal)



STRONGEST SKILLS REQUIRED

1. **Keen Attention to Detail:** Think like an attacker, exploring every angle with an active and attentive mind to uncover crucial information.
2. **Critical Thinking and Problem-Solving:** Excel in analyzing fragmented data, building relationships between pieces, and uncovering insightful conclusions.
3. **Deep and Dark Web Proficiency:** Have a unique advantage in investigating beyond the surface internet, accessing valuable hidden information.
4. **Keeping Abreast of OSINT Tools**: Stay up to date with the latest software and tactics, ensuring efficient and effective investigations.

Leverage the power of prompt engineering and various AI tools to enhance the efficiency and effectiveness of my investigations (**WEBINT or Web Intelligent used for developing and Research**).

5. **Sentiment Analysis:** AI-powered sentiment analysis allows me to gauge the emotions and attitudes expressed in online content. This can be particularly valuable in understanding public perceptions, identifying potential risks, or detecting deceptive information.
6. **Image and Video Analysis:** AI tools can perform reverse image searches and analyze visual content, aiding in the identification of individuals, locations, or objects relevant to my investigations.
7. **Automation of Repetitive Tasks:** I use AI to automate repetitive and time-consuming tasks, such as data scraping or processing, which allows me to focus on higher-level analysis and decision-making.

DATA SOURCES

SURFACE WEB

There are many of data available for the surface web some are discussed below:

1. **Google Search:** The most widely used search engine for general OSINT research.
2. **Google Advanced Search Operators:** Allows for more specific and targeted searches.
3. **Bing Search:** Microsoft's search engine, is useful for cross-referencing with Google.
4. **Social Media Platforms:** Websites like Twitter, Facebook, LinkedIn, and Instagram for gathering information from public profiles and posts.
5. **Wayback Machine:** Archives web pages, useful for accessing historical versions of websites.

DEEP WEB

There are many deep web data sources available:

1. Google patent database for patents worldwide. This information is really interesting when it comes to Competitor Intelligence.
2. Google academic database for research articles. This information is also interesting for Competitor Intelligence.
3. EU Sanction Lists which is useful for running Vendor Risk Management.
4. HaveIBeenPwned which enables Data Leakage Detection and also background checks.
5. Zabasearch is a free US people and public information search engine.

DARK WEB

To access the dark web a user must use dedicated software to access it, such as TOR or I2P. Also, BitTorrent file-sharing protocol is designed to operate anonymously and maintain user privacy.

- **Ashley Madison —** Ashley Madison is a popular dating site for extramarital affairs on the dark web.
- **Hidden Wikileaks:** This is used to share leaked confidential information and documents from governments, organizations, and individuals to promote transparency and accountability.

- Dark Web search engines like DuckDuckGo (http://bznjtqphs2lp4xdd.onion/)
- Candle (http://gjobqjj7wyczbqie.onion/)
- anemia.fi (surface web engine to search on the dark web)
- tor. wiki

SOME SAFETY OF USING THE DARK WEB

1. Don't Reveal Your Real Identity

Here are some measures to take to prevent revealing your identity:

- **Create a dummy email** or use an encrypted email service like Proton Mail for any Dark Web communication.
- **Turn off your device's location services** to prevent inadvertent disclosure of your whereabouts.
- **Cover your camera and microphone** to protect against potential unauthorized access and surveillance.
- **Opt for cryptocurrency payments**, as they're anonymous and make it difficult to trace transactions back to you.
- **Be cautious when interacting with other users**, as social engineering techniques can be used to extract information about your identity.
- **Avoid sharing any personal details**, such as your name, age, address, or workplace, in online discussions or private messages.
- **Use unique usernames** and strong, distinct passwords for each Dark Web site or service you access to prevent cross-referencing and profiling.

2. **Use a Different Operating System(whonix)**
3. **Disable JavaScript**
4. **Open Downloads Offline**

MORE AREAS

The above experience of investigation shared is based on Passive OSINT collection. There are two more Areas where we investigate.

- **Active Collection of OSINT:** Active OSINT collection contacts the target to gather real-time or more accurate data such as conducting interviews, posting queries on forums, or using specialized tools for data extraction.
- **Tools:** scanning a target website, Online forum, or Social Media platform
- **Semi-Passive Collection of OSINT:** It is between active and passive. Monitoring and observing online sources without direct interaction, like tracking social media posts, website changes, or public events.
- **Tools:** Social media monitoring tools, website change detection tools, and event tracking platforms.

LIMITATIONS

These investigations are not only based on US or Canada. Our research has also yielded a wealth of valuable information pertinent to the United Kingdom and various European countries.

SUMMARY

- OSINT (Open-Source Intelligence) gathers and analyzes public data from sources like social media, newspapers, and websites.
- It serves diverse sectors, including cybersecurity, social media investigations, and risk management.
- OSINT's history dates to pre-World War II, and it has expanded globally beyond the US and Canada.
- Strong skills like attention to detail and critical thinking are vital for OSINT experts.
- AI tools, such as sentiment analysis and image recognition, enhance investigation efficiency.
- Data sources cover surface, deep, and dark web domains.
- Safety measures are crucial when exploring the dark web.
- Active and semi-passive approaches complement traditional passive OSINT.

- OSINT empowers informed decision-making with comprehensive global intelligence.

REFERENCES

- Ransomware Attacks on Critical Infrastructure Sectors (dhs.gov)
- 202208091700_OSINT How-To Analyst Note_TLPWHITE (hhs.gov)
- What Is Open Source Intelligence and How to Conduct OSINT Investigations - Maltego
- Surface Web is Only the Tip of the Iceberg - Traversals
- How to Access the Dark Web Safely: A 2023 Beginner's Guide (wizcase.com)