21 OSINT Research Tools for Threat Intelligence
Introduction

To help investigators make use of the vast expanse of information available on the surface, deep and dark web, Authentic8 experts have curated a list of the most useful tools. With these resources, investigators can simplify their research and improve productivity.

Table of Contents

1. OSINT Framework: Find Free OSINT Resources ................................................................. 3
2. IDA Pro: Perform State-of-the-Art Binary Code Analysis ....................................................... 3
3. Creepy: Gather Geolocation Information ............................................................................... 4
4. Maltego Transform Hub: Mine, Merge and Map Information ................................................... 4
5. DNSdumpster: Find and Look Up DNS Records ................................................................. 5
6. TinEye: Reverse Image Search .............................................................................................. 5
7. Shodan: The Search Engine for the IoT .................................................................................. 6
8. Wayback Machine: Explore Billions of Webpages ................................................................. 6
9. Have I Been Pwned: Find Out if Your Account Has Been Compromised ................................. 7
10. CipherTrace: Follow the Money ............................................................................................. 7
11. Voter Records: Search Anyone’s Public Records ................................................................... 8
12. Whitepages: Find People and Perform Background Checks ................................................ 8
13. Fake Name Generator: Disguise Your Identity ....................................................................... 9
14. CityProtect: Explore Crime Maps .......................................................................................... 9
15. Torch Search Engine: Explore the DarkNet ......................................................................... 10
16. Dark.fail: Go Deeper into the Darknet .................................................................................. 10
17. PhishTank: Use PhishTank to Research Suspected Phishes .................................................. 11
18. HoneyDB: Community-Driven Honeypot Sensor Data Collection ....................................... 11
19. ThreatMiner: IOC Lookup and Contextualization .................................................................. 12
20. VirusTotal: Analyze Suspicious Files and URLs ................................................................. 12
Silo for Research: Secure, Anonymous Online Investigations .................................................. 14
1. OSINT Framework: Find Free OSINT Resources

https://osintframework.com/

**WHAT IT IS**

OSINT Framework indexes a multitude of connections to different URLs, recommending where to look next when conducting an investigation. It also provides suggestions on what services can help analysts find specific data that might aid in their research.

**USE CASE**

When you plug a piece of data (such as an email address, phone number, name, etc.) into the framework, it returns all known online sources that contain information relevant to that data. OSINT Framework also offers a list of potential resources where more information related to that particular source can be found.

2. IDA Pro: Perform State-of-the-Art Binary Code Analysis

https://www.hex-rays.com/products/ida/

**WHAT IT IS**

The source code of the software isn’t always available. A disassembler like IDA Pro translates machine-executable code into readable assembly language source code, enabling research specialists to analyze programs that are suspected to be contain malware or spyware.

**USE CASE**

An incident response team loads a malicious artifact found on a breached server into IDA Pro to further analyze and understand its behavior, potential damage and method of traversal. IDA Pro can also be used as a debugger to aid analysts in reading and examining the hostile code.
3. Creepy: Gather Geolocation Information
https://www.geocreepy.com/

WHAT IT IS
Creepy is a geospatial visualization tool that centralizes and visualizes geolocated information pulled across multiple online sources.

USE CASE
Once the plugin is configured, a user can feed the tool a social media artifact. Creepy draws all available locations on the map, allowing the user to see where the devices were located when the information was posted.

4. Maltego Transform Hub: Mine, Merge and Map Information
https://www.maltego.com

WHAT IT IS
Integrate data from public sources, commercial vendors and internal sources via the Maltego Transform Hub. All data comes pre-packaged as Transforms, ready to be used in investigations. Maltego takes one artifact and finds more.

USE CASE
A user feeds Maltego domain names, IP addresses, domain records, URLs or emails. The service finds connections and relationships within the data and allows users to create graphs in an intuitive point-and-click logic.
5. DNSdumpster: Find and Look Up DNS Records
https://dndumpster.com/

WHAT IT IS
DNSdumpster is a free domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers’ perspective is an important part of the security assessment process.

USE CASE
After a user enters a domain name, DNSdumpster identifies and displays all associated subdomains, helping map an organization’s entire attack surface based on DNS records.

6. TinEye: Reverse Image Search
https://tineye.com/

WHAT IT IS
TinEye is an image-focused web crawling database that allows users to search by image and find where that image appears online.

USE CASE
An investigator uploads an image to TinEye or searches by URL. TinEye constantly crawls the web and adds images to its extensive index (as of August 2021, over 48 billion images).
7. Shodan: The Search Engine for the IoT
https://shodan.io/

WHAT IT IS
Websites are just one part of the internet. Shodan allows analysts to discover which of their devices are connected to the internet, where they are located and who is using them.

USE CASE
Shodan helps researchers monitor all devices within their network that are directly accessible from the internet and therefore vulnerable to attacks.

8. Wayback Machine: Explore Billions of Webpages
https://web.archive.org/

WHAT IT IS
Wayback Machine analyzes websites published across time, allowing researchers to review how the webpage looked when it was originally launched or updated, revealing data that may no longer be visible or searchable through regular search engines.

USE CASE
Suppose a website was seized by the FBI, but the original content is no longer there. Researchers can use Wayback Machine to reveal information that the site may have contained prior to the raid.
9. Have I Been Pwned: Find Out if Your Account Has Been Compromised

https://haveibeenpwned.com/

**WHAT IT IS**

The service exposes the severity of the risks of online attacks, while helping victims of data breaches learn about compromises of their accounts. Users can subscribe to receive breach notifications and search for pwned accounts and passwords across domains.

**USE CASE**

Users can securely enter email addresses and passwords to find out if they have been hacked. The site returns a complete list of breaches where specific accounts have been exposed, and it lists what types of data (email addresses, names, passwords, locations, etc.) have been stolen.

10. CipherTrace: Follow the Money

https://ciphertrace.com/ciphertrace-maltego-transform/

**WHAT IT IS**

Maltego CipherTrace is a popular security research and forensics tool that uses the Bitcoin blockchain to track funds. CipherTrace uses identifiers for criminal, mixer, dark market, gambling, ATM and exchange activities. It comes in the form of a Maltego Transform plugin.

**USE CASE**

Create directed graphs to track an asset's final destination, even when a Bitcoin mixer attempts to launder the funds.
11. Voter Records: Search Anyone’s Public Records
https://voterrecords.com/

WHAT IT IS
Voter Records is a free political research tool that contains more than 70 million voter registration records. Details include related public records, political party affiliations, relatives, location, current and previous addresses and more.

USE CASE
A researcher could gain comprehensive information about any person’s affiliations, location and connections.

12. Whitepages: Find People and Perform Background Checks
https://www.whitepages.com/

WHAT IT IS
Whitepages offers reverse name, address and phone number lookup and returns high-level information on any individual or business.

USE CASE
A useful tool for verifying that the persons a researcher is dealing with are who they say they are. Investigations can locate people and businesses, verify their addresses, look up phone numbers and even perform complete background checks.
13. Fake Name Generator: Disguise Your Identity
https://www.fakenamegenerator.com/

WHAT IT IS
Fake Name Generator produces an entire new false identity for a person, including detailed contact information, a mother’s maiden name, street address, email, credit card numbers, phone number, social security number and more.

USE CASE
A fake identity can be useful for filling out online forms without giving out personal details, using it as a pseudonym on the internet, testing payment options with randomly generated credit card numbers and all other types of research where an analyst doesn’t want to expose his or her real identity.

14. CityProtect: Explore Crime Maps
https://www.cityprotect.com

WHAT IT IS
CityProtect is a crime visualization site. Users provide a location within the U.S., along with some other parameters, and detailed crime reports are delivered. The reports are rendered geospatially.

USE CASE
A user can analyze quantified criminal behavior in a geographic area over time to help build an intelligence-lead brief.
15. Torch Search Engine: Explore the DarkNet

http://xmh57jrzrnw6insl.onion/ (Tor browser is required to open link)

**WHAT IT IS**

Torch, or TorSearch, is a search engine designed to explore the hidden parts of the internet. Torch claims to have over a billion darknet pages indexed and allows users to browse the dark web uncensored and untracked.

**USE CASE**

Torch promises peace of mind to researchers who venture into the dark web to explore .onion sites. It also doesn't censor results — so investigators can find all types of information and join discussion forums to find out more about current malware, stolen data for sale or groups who might be planning a cyberattack.

16. Dark.fail: Go Deeper into the Darknet

https://dark.fail/

**WHAT IT IS**

Dark.fail has been crowned the new hidden wiki. It indexes every major darknet site and keeps track of all domains linked to a particular hidden service.

**USE CASE**

Tor admins rely on Dark.fail to disseminate links in the wake of takedowns of sites like DeepDotWeb. Researchers can use Dark.fail when exploring sites that correlate with the hidden service.
17. PhishTank: Use PhishTank to Research Suspected Phishes
https://www.phishtank.com/

**WHAT IT IS**
PhishTank is a free community site where anyone can submit, verify, track and share phishing data. PhishTank also provides an open API for developers and researchers to integrate anti-phishing data into their applications.

**USE CASE**
Users submit suspicious URLs via email, and PhishTank identifies, verifies, tracks, confirms and publishes phishing site on its webpage.

18. HoneyDB: Community-Driven Honeypot Sensor Data Collection
https://riskdiscovery.com/honeydb/

**WHAT IT IS**
HoneyDB has multiple honeypots throughout the internet waiting to be attacked. The service logs complete details of an attack (including IP address) and the binary that was used to execute it, then lists them in its database. HoneyDB enables users to run a reverse search on IOCs and correlates it back to campaigns happening on its honeypots.

**USE CASE**
A campaign that uses a unique exploit to commit a wide-spread attack on every system possible would most likely infect one or more of the honeypots. A user then accesses detailed information on the attack to gather information about its intentions and perpetrators.
19. ThreatMiner: IOC Lookup and Contextualization

https://www.threatminer.org

WHAT IT IS
ThreatMiner is a threat intelligence portal designed to enable an analyst to research indicators of compromise (IOCs) under a single interface. That interface allows for not only looking up IOCs but also providing the analyst with contextual information. With this context, the IOC is not just a data point but a useful piece of information and potentially intelligence.

USE CASE
Identify and enrich indicators of compromise to have a better understanding of attack origins.

20. VirusTotal: Analyze Suspicious Files and URLs

https://www.virustotal.com/

WHAT IT IS
VirusTotal inspects items with over 70 antivirus scanners and URL/domain blacklisting services. Scanning reports produced by VirusTotal are shared with the public to raise the global IT security level and awareness about potentially harmful content.

USE CASE
Users can select a file from their computer using their browser and send it to VirusTotal. Results are shared with the submitter, and also between the examining partners, who use this data to improve their own systems.
21. ExploitDB: The Most Comprehensive Exploit Collection

https://www.exploit-db.com/

WHAT IT IS
The Exploit Database is an archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. Exploits are collected throughout the internet and through user submissions, then archived for community use.

USE CASE
The Exploit Database is a repository for publicly available exploits, making it a valuable resource for those who need actionable data at their fingertips.
Silo for Research: Secure, Anonymous Online Investigations

https://www.authentic8.com/products/silo-for-research

WHAT IT IS
Silo for Research is a purpose-built solution for conducting online research without exposing analysts’ digital fingerprint. Safely pursue investigations across the surface, deep or dark web from a cloud-based browsing interface while controlling how you appear online.

USE CASE
Blend in with the crowd and avoid tipping off your suspect. Manipulate your location, time zone, language and keyboard settings, device type, browser and much more. Keep investigative browsing completely segregated from your device to prevent infection, tracking or identification that could spoil your investigation or make you a target.

Silo for Research is an integrated solution for conducting secure and anonymous web research, evidence collection and data analysis from the surface, deep and dark web. It’s built on Authentic8’s patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

© Authentic8, Inc. All rights reserved. 09092021