# 21 OSINT Research Tools for Threat Intelligence


Silo
By Authentic8

silo
By Authentic8

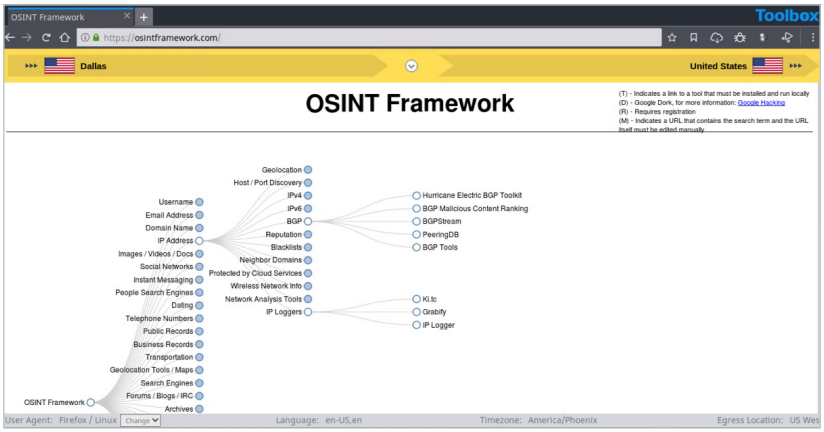
# Introduction

To help you investigate the vast expanses of the open, deep, and dark web, Authentic8 engineers used Silo for Research (Toolbox) to build a list of 21 useful tools that could make your research work easier and more productive.

## Table of Contents

## 1. Find Free OSINT Resources with OSINT Framework

https://osintframework.com/




**What It Is**

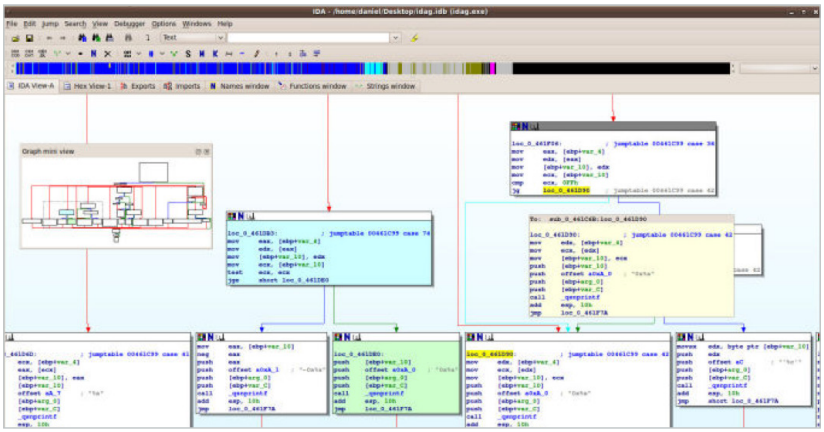
OSINT Framework indexes a multitude of connections to different URLs, recommending where to look next when conducting an investigation. It also provides suggestions on what services can help analysts find specific data that might aid in their research.

**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. The OSINT Framework also offers a list of potential resources where more information related to that particular source can be found.

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

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



**What It Is**

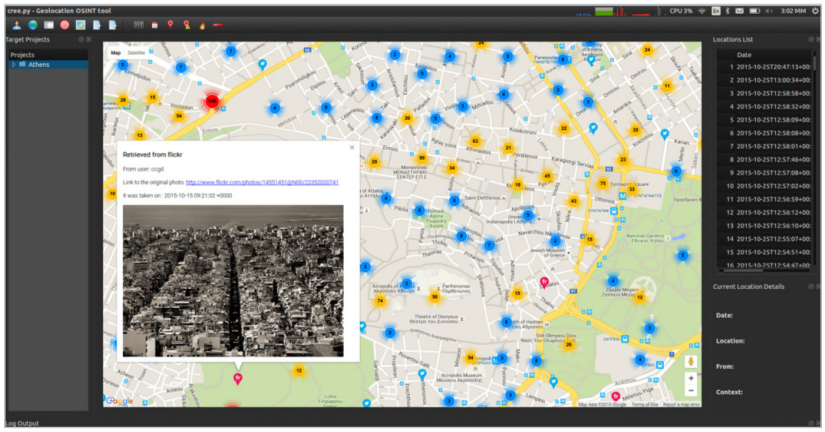
The source code of the software isn't always available. A disassembler like IDA Pro translates machine-executable code into readable assembly language source code, enabling research specialists to analyze programs that are suspected to be contain malware or spyware.

**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. Gather Geolocation Information with Cree.py

https://www.geocreepy.com/



**What It Is**

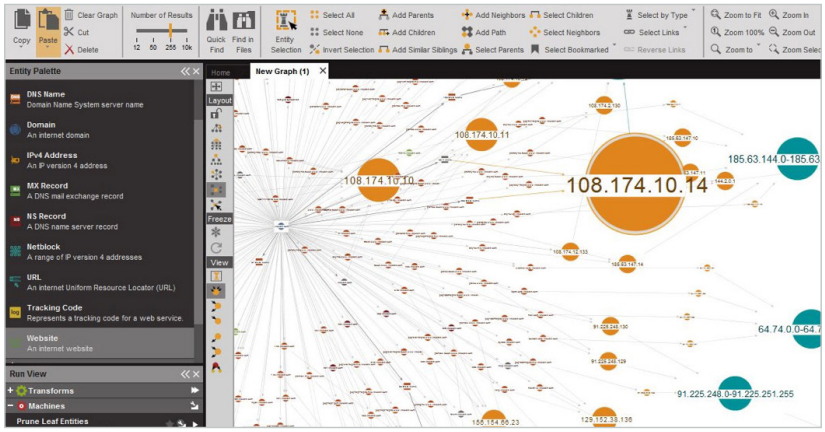
Cree.py is a geospatial visualization tool that centralizes and visualizes geolocated information pulled across multiple online sources.

**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. Mine, Merge, and Map Information with Maltego

https://www.maltego.com




**What It Is**

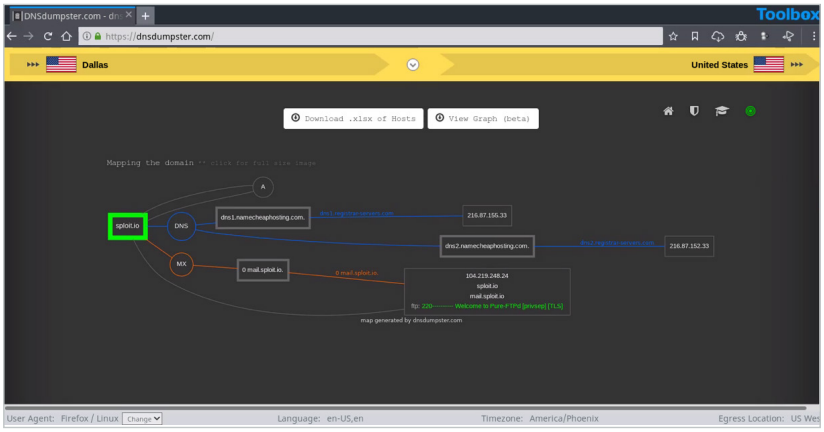
Integrate data from public sources, commercial vendors, and internal sources via the Maltego Transform Hub. All data comes pre-packaged as Transforms, ready to be used in investigations. Maltego takes one artifact and finds more.

**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. ctions as link analysis, bar graphs, timelines, et al.

## 5. Find and Lookup DNS Records with DNSdumpster

https://dnsdumpster.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.

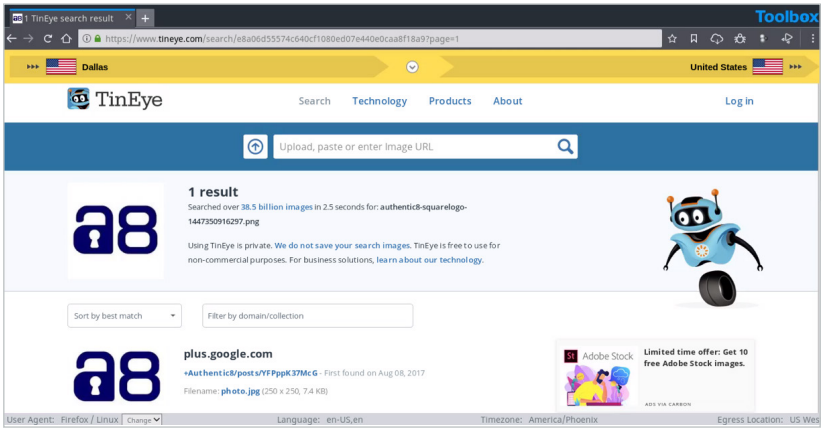
### Use Case

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

---

## 6. TinEye for Reverse Image Search

https://tineye.com/




### What It Is

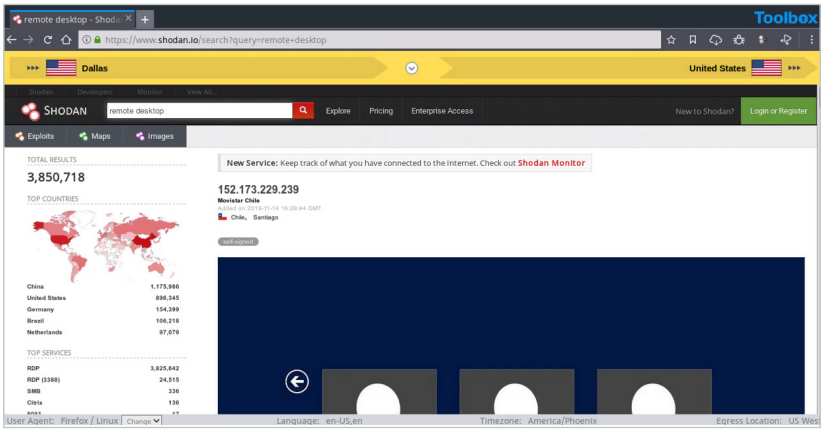
TinEye is an image-focused web crawling database that allows users to search by image and find where that image appears online.

### 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 April 2020, over 39.7 billion images).

## 7. Shodan: The Search Engine for the IoT

https://shodan.io/




### What It Is

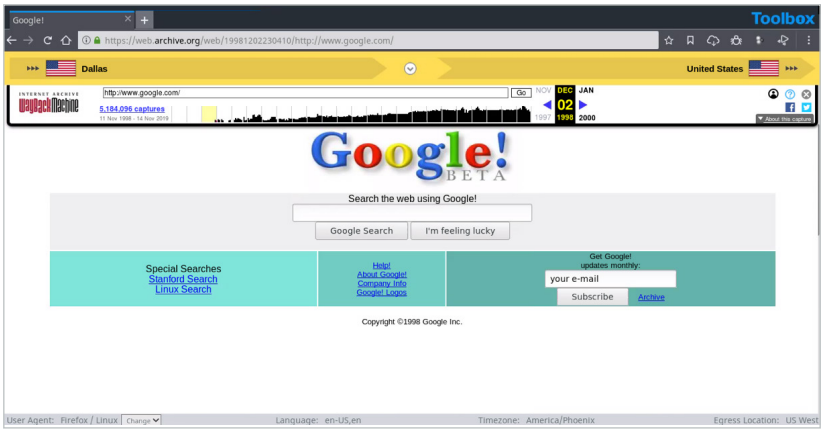
Websites are just one part of the internet. Shodan allows analysts to discover which of their devices are connected to the internet, where they are located, and who is using them.

### Use Case

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

## 8. Explore Billions of Web Pages with Wayback Machine

https://web.archive.org/




### What It Is

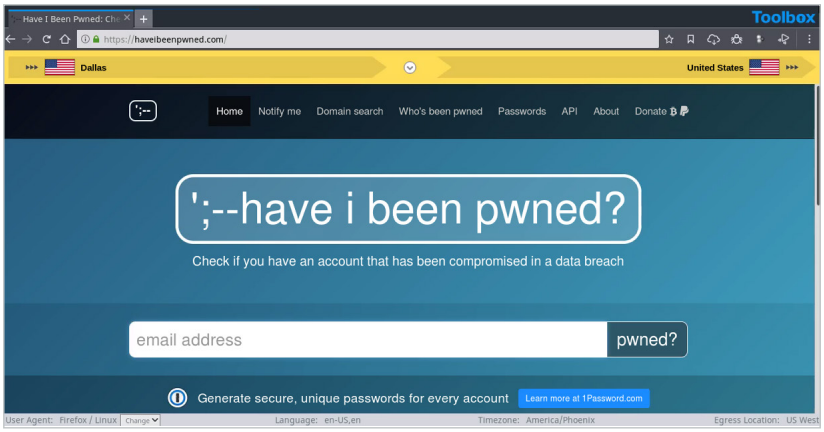
Wayback Machine analyzes websites published across time, allowing researchers to review how the web page looked when it was originally launched or updated, revealing data that may no longer be visible or searchable through regular search engines.

### 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. Find out If Your Account Has Been Compromised Using Have I Been Pwned

https://haveibeenpwned.com/




**What It Is**

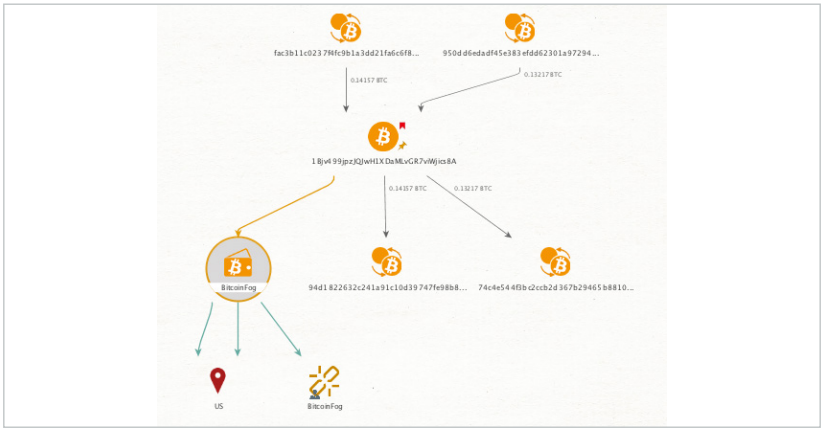
The service exposes the severity of the risks of online attacks, while helping victims of data breaches learn about compromises of their accounts. Users can subscribe to receive breach notifications, and search for pwned accounts and passwords across domains.

**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 what types of data (email addresses, names, passwords, locations, etc.) has been stolen.

## 10. Follow the Money with CipherTrace Maltego Transform

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




**What It Is**

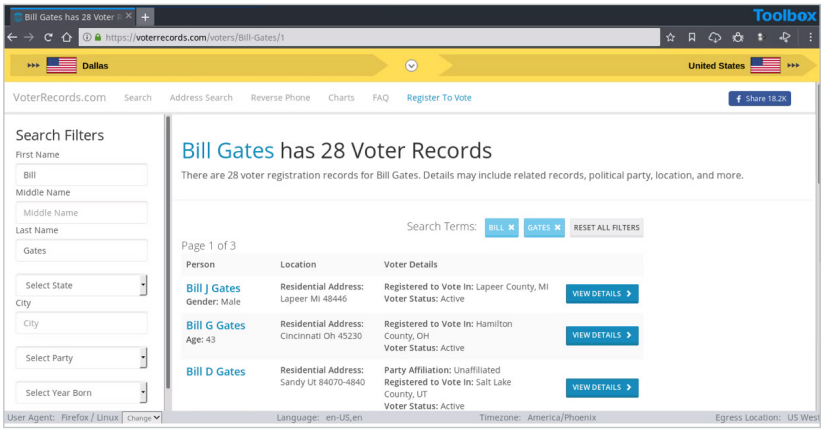
Maltego is a popular security research and forensics tool that uses the Bitcoin blockchain to track funds. Maltego uses identifiers for criminal, mixer, dark market, gambling, ATM, exchange activities. It comes in the form of a Maltego transform plugin.

**Use Case**

Create directed graphs to track an asset's final destination, even when a Bitcoin mixer attempts to launder the funds.

## 11. Search Anyone's Public Records Though Voter Records

https://voterrecords.com/




### What It Is

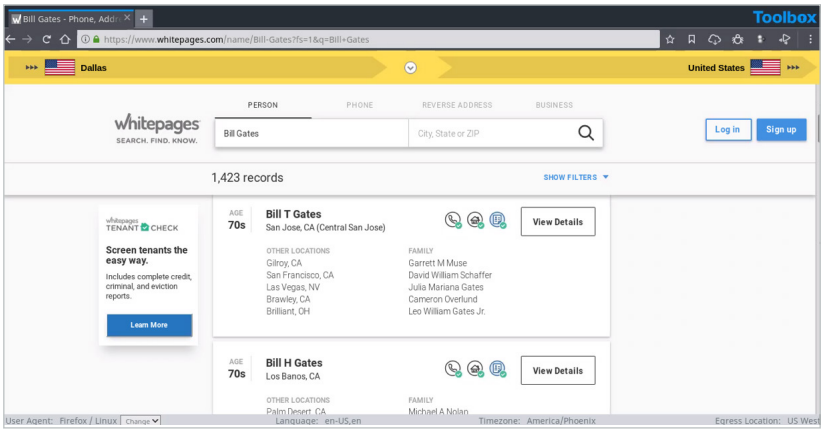
Voter Records is a free political research tool that contains more than 70 million voter registration records. Details include related public records, political party affiliations, relatives, location, current and previous addresses, and more.

### Use Case

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

## 12. Find People and Perform Background Checks with Whitepages

https://www.whitepages.com/




### What It Is

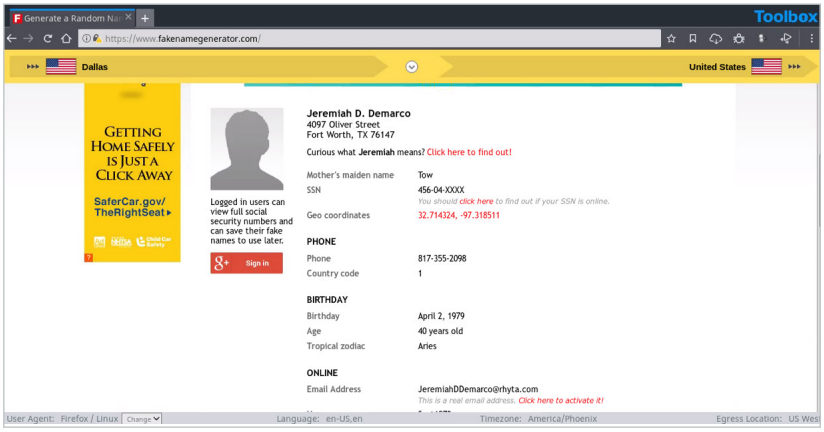
Whitepages offers to perform reverse name, address and phone number look up and returns high-level information on any individual or business.

### 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. Disguise Your Identity with Fake Name Generator

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.

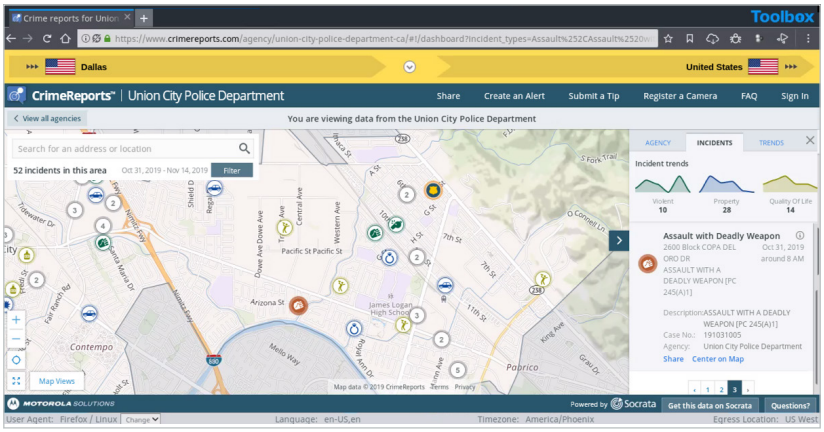
### Use Case

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. Explore Crime Maps with CityProtect

https://www.cityprotect.com




### What It Is

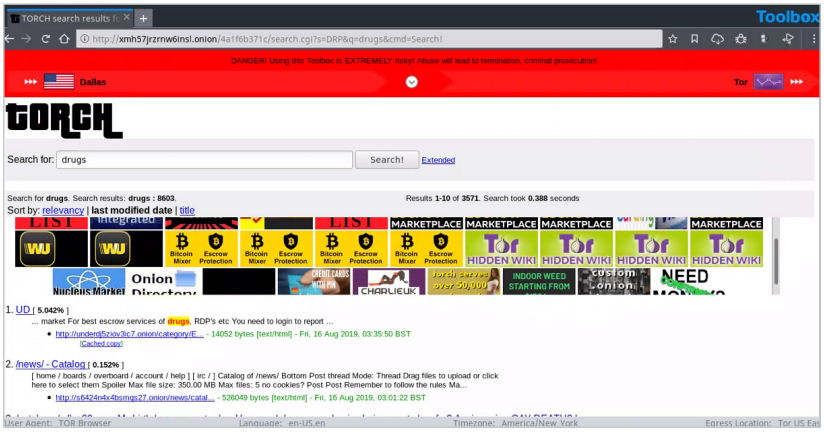
CityProtect is a crime visualization site. Users provide a location within the US, along with some other parameters, and detailed crime reports are delivered. The reports are rendered geospatially.

### Use Case

A user can analyze quantified criminal behavior in a geographic area over time to help build an intelligence-led brief.

## 15. Explore the Dark Net with Torch Search Engine

http://xmh57jrzrnw6insl.onion/




### 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 dark net pages indexed, and allows users to browse the dark web uncensored and untracked.

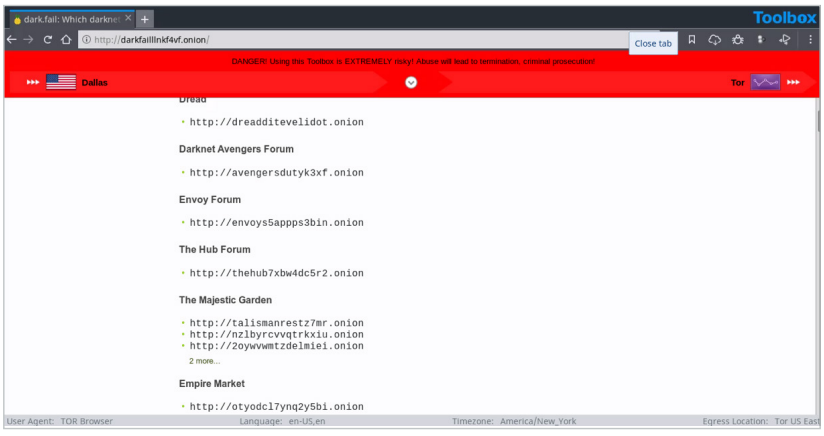
### Use Case

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. Go Deeper into the Dark Web with Dark.fail

http://darkfailllnkf4vf.onion/




### What It Is

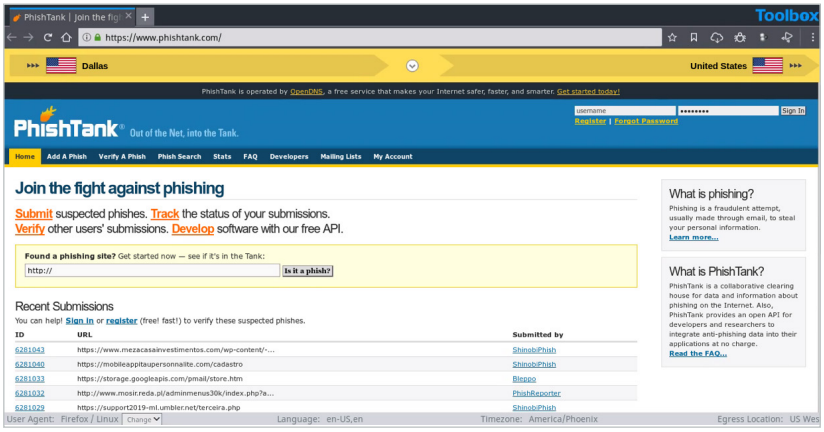
Dark.fail has been crowned the new hidden wiki. It indexes every major darknet site and keeps track of all domains linked to a particular hidden service.

### 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. Use PhishTank to Research Suspected Phishes

https://www.phishtank.com/




### What It Is

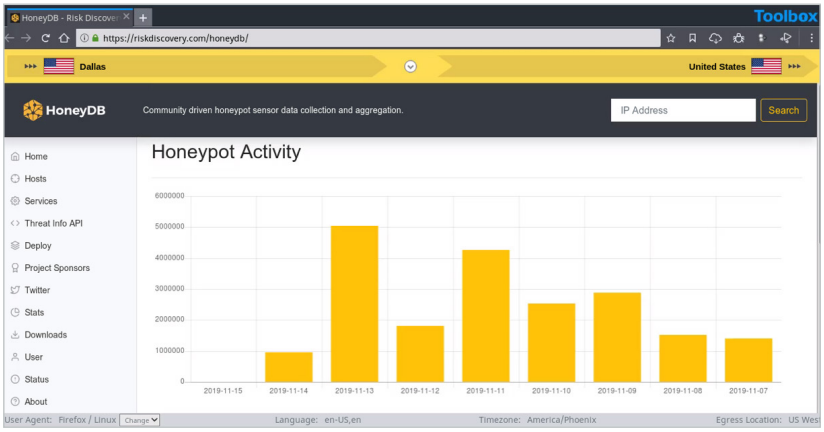
PhishTank is a free community site where anyone can submit, verify, track and share phishing data. PhishTank also provides an open API for developers and researchers to integrate anti-phishing data into their applications.

### Use Case

Users submit suspicious URLs via email, and PhishTank identifies, verifies, tracks, confirms, and publishes phishing site on its web page.

## 18. HoneyDB: A Community-driven Honeypot Sensor Data Collection Service

https://riskdiscovery.com/honeydb/




### What It Is

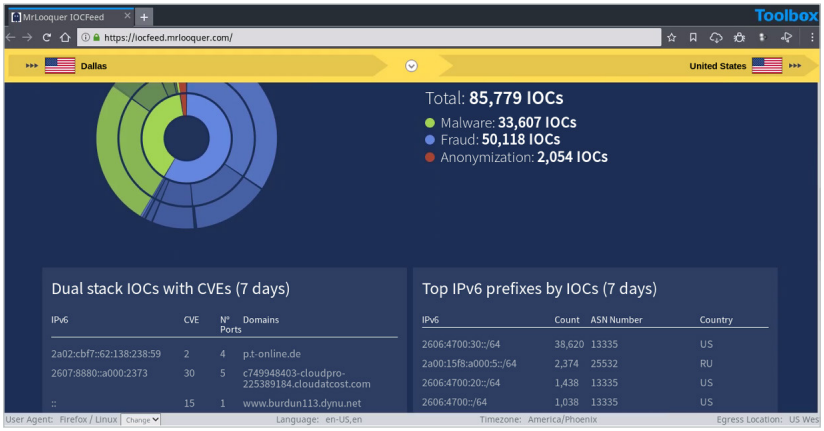
HoneyDB has multiple honeypots throughout the internet waiting to be attacked. The service logs complete details of an attack, including IP address, and the binary that was used to execute it, and lists them in the HoneyDB database.  HoneyDB enables users to run a reverse search on IOCs and correlates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

### 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. MrLooquer IOCFeed – A Threat Feed Focused on Dual Stack Systems

https://iocfeed.mrlooquer.com/




### What It Is

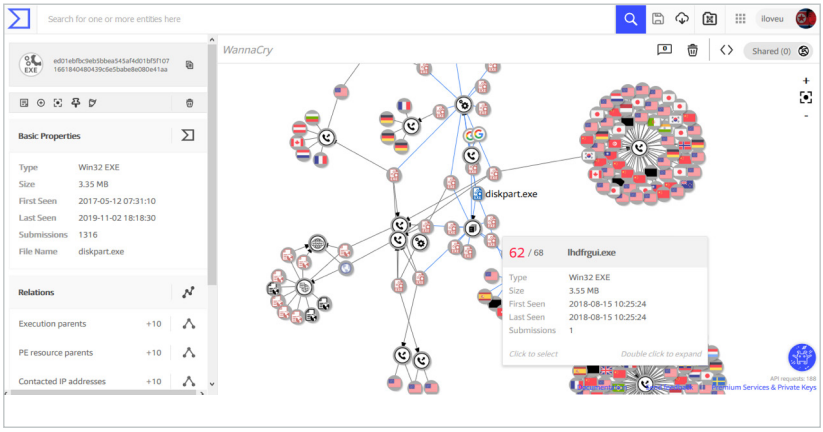
MrLooquer IOCFeed serves as an IOC reverse search engine. It collects a variety of IOC artifacts, like malware, phishing, or common vulnerability exposures used, and shows users which domains they came from.

### Use Case

Users can enter their own IOCs to find out where attacks could be coming from.

## 20. Analyze Suspicious Files and URLs with VirusTotal

https://www.virustotal.com/




### What It Is

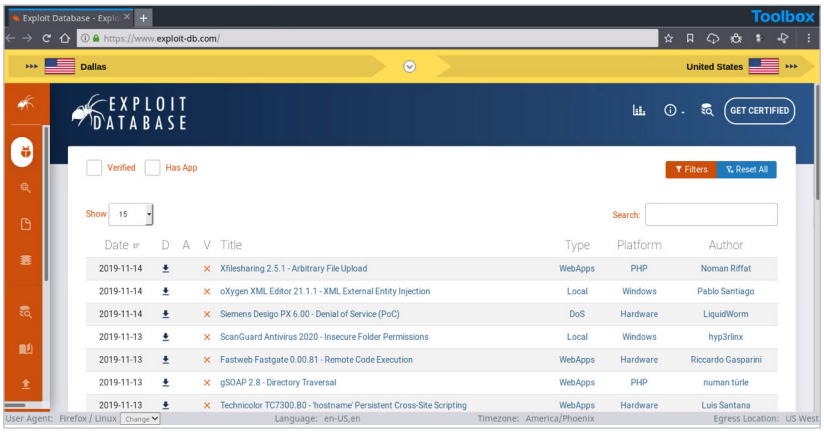
VirusTotal inspects items with over 70 antivirus scanners and URL/domain blacklisting services. Scanning reports produced by VirusTotal are shared with the public to raise the global IT security level and awareness about potentially harmful content.

### 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. Tap into the Most Comprehensive Collection of Exploits on Exploit DB

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, and 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 (Toolbox)** is a secure and anonymous web browsing solution that enables users to conduct research, collect evidence and analyze data across the open, deep and dark web.

Silo for Research is 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.

Research teams can accomplish their goals without introducing risk to the organization or revealing intent. All web activity is logged and encrypted so compliance teams can be sure that the tools are used appropriately.

By Authentic8

**CONNECT WITH US**

+1 877-659-6535
www.Authentic8.com

**PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST**

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.