Searching in DarkOwl Vision

- Using the Search Bar
- Search Techniques
- Filters, Dates, Advanced Search Options

Using the Search Bar

1. The search bar works like most search engines; simply type words, phrases, numbers, or characters. The Search Bar treats words individually, unless you specify otherwise.
   - If you type multiple words, the default search operator is an OR boolean search; i.e. typing Jane Doe will send the query as Jane OR Doe.
   - More information: Searching with Booleans.
   - Using quotations (“Jane Doe”) will send the query as one phrase, Jane Doe.
2. Use the left drop-down menu to open Search Builders, tools to help you create queries.
   - Find Entity > the best way to search for Emails, Credit Cards, SSNs
   - Getting Started Templates > pre-populated templates to get started quickly
   - Lexicon > curated lists of commonly searched items
   - Once you’ve started searching, Recent Searches and Saved Searches will also appear in this menu, for easy access.
3. Use the right Filter menu to create targeted queries. More information: Filters, Dates, Advanced Search Options.

Search Techniques

Searching with Booleans AND, OR, AND NOT

Use Boolean AND, OR, AND NOT to specify inclusions, alternate terms, or exclusions.

- Admin AND Password AND Hack – will return pages that include all three terms.
- Admin OR Password – will return pages that include either Admin or Password in them.
- Admin AND NOT Password – will return pages that include Admin without the word Password.
- Admin -Password – will return pages that include Admin without the word Password.

Using Subqueries ( )

Group together phrases, to form subqueries. Use parentheses ( ) to indicate each clause.

- (quick OR brown) AND fox – will return pages with (quick AND fox) OR (brown AND fox)

Proximity Searches

Find two words within a certain distance of each other. Use quotations around two terms, and then specify a maximum distance that the words can appear in relation to each other.

- “Jane Doe”~2 – will return pages with Jane and Doe no farther than 2 terms apart
Pattern Matching / Regular Expressions

The free text search bar supports Lucene-based regular expressions, which should be wrapped by forward slashes. Please note these queries may time out, particularly when searching for a high volume of unknown characters.

Using Bitcoin as an example, the search to type in the search bar would be as follows, with some notes on the formatting below: /\[13\][a-km-zA-HJ-NP-Z1-9]{25,34}/

- [13] is requesting the match needs to start with either the character ’1’ or ’3’.
- [a-km-zA-HJ-NP-Z1-9]{25,34} is asking for a pattern of any alphanumeric character besides lowercase L, uppercase I, uppercase O, and the number 0 (to prevent ambiguity) and must be anywhere from 25 to 34 characters long.

Using Metadata Fields in a Search

Keyword searching will match against the Body (content) of a result. However, you can also search using the following Metadata fields:

- url:
- title:
- httpHeaders:
- domain:
- contentType:
- ip:

Excluding Items from a Search

Use AND NOT or a hyphen (-) to exclude words or metadata fields from your search.

- AND NOT drugs (or -drugs)
- -httpHeaders:nginx

Filters, Dates, and Advanced Search Options

Refine your search with various filter and date options. Click on the icon to get started.

DataLeaks

Filter to content from known breaches or other leak data, tagged by name in DarkOwl Vision. Type or scroll to find the desired Data Leak. **Click once to include, click twice to exclude.**

Data Sources

Filter to content from a particular DarkOwl data collection source. Options include: Alternate DNS, FTP, I2P, IRC, Onion, Pastebin, Telegram, Zeronet. **Click once to include, click twice to exclude.**

Domains

Filter to content from a particular domain, or exclude a particular domain by typing a hyphen in front of the domain. Type only the domain portion (i.e. without the www prefix).

- arch3rsecgjqcmjb.onion
- -pastebin.com
Groups
Groups are combined filters that narrow your search to specific categories; **click to include:**

- **Authenticated Sites:** Filter to content from sites requiring credentials or other challenges.
- **Blogs:** Filter to content from sites tagged as blogs.
- **Darknet:** Filter to content from the Tor, I2P, and Zeronet darknets.
- **Forums:** Filter to content from sites tagged as forums.
- **Paste Sites:** Filter to content from a curated set of paste sites selected by our analysts.

Hackishness
Hackishness assigns a rating to every piece of content collected, indicating the likelihood to which the information could be used for criminal activity. The lower bound of hackishness is .01 (1%) and the upper bound is 1.0 (100%). **Use the slider** to select a desired hackishness threshold.

Has Entity (Credit Cards, Email, Social Security Numbers)
Filter to content that have at least one selected Entity. **Click next to the Entity name to select.**

Has Range (Credit Cards, Email, Social Security Numbers)
Filter to content that have a certain number of selected Entities. This filter is helpful in finding “dumps,” as many threat actors will post multiple instances of PII on a singular site or document. **Type values next to a selected Entity:** Enter a lower bound (minimum 1), upper bound (maximum 999999), or use both fields to form a range (50 to 1000).

Language
Filter to content in a particular language. Languages are detected by DarkOwl Vision at the time of ingestion, using natural language processing. **Click once to include.**

Dates
Use the drop-down to quickly select a time range for search results.

To custom-select a range, use the crawlDate field in the search bar:

- **crawlDate:**[2020-02-05T00:00:00Z TO 2020-02-12T00:00:00Z]

Advanced Options (Sort By, Show Similar)
Use Advanced Options to select a Sort option, or to show all results (including duplicates).

- Sort by **Relevance** (default), By **Hackishness**, By **Crawl Date**
- Show duplicates (default is off)