DarkOwl Vision UI to Search API Field Map

Base search options:

Searching for tokenized entities in results:

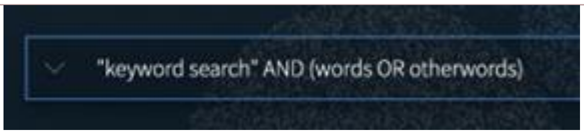
Using filters:

Other functions:

- Additional response options
- Using the Leak Context endpoint with search results from data leaks

Search bar

Any text that goes directly into the search bar in the UI goes directly into the 'q' field. All keywords, Boolean operators, regex, etc.

UI	API
Search Bar	**'q'**
 "keyword search" AND (words OR otherwords)	/api/v1/search?q="keyword search" AND (words OR otherwords)

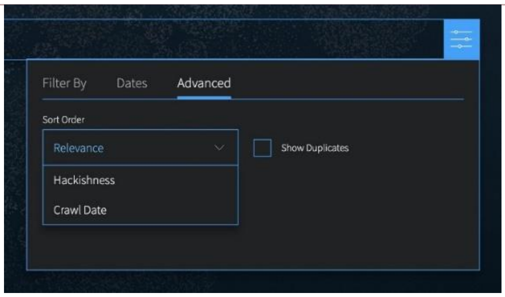
Note: The API examples in this document are shown before URL encoding.

Next page of results

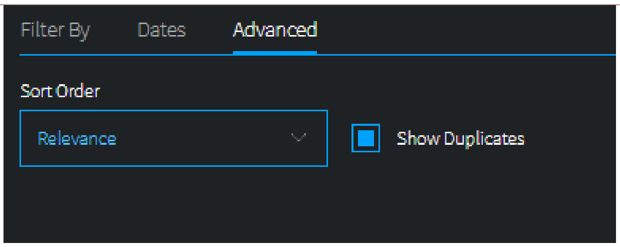
By default, a page in both UI and API are 20 results. To go to the next 'page' via API, do the exact same search but with offset=20 for the second page, offset=40 for the third, and so on.

UI	API
Next/Previous Page	'offset'

Sort options

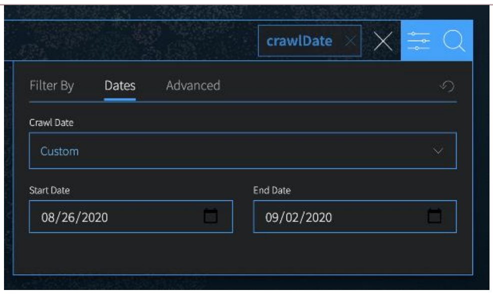
UI	API
Filters -> Advanced -> Sort	'sort'
 Filter By Dates Advanced Sort Order Relevance Hackishness Crawl Date Show Duplicates	/api/v1/search?sort=r (Relevance) /api/v1/search?sort=d (Crawl Date) /api/v1/search?sort=h (Hackishness)

De-duplicate result sets

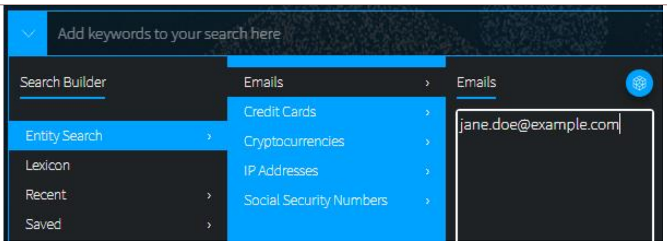
UI	API
Filters -> Advanced -> Show Duplicates Box checked - true; Box unchecked - false	'similar'
 Sort Order: Relevance ☑ Show Duplicates	/api/v1/search?similar=true /api/v1/search?similar=false

Using date parameters

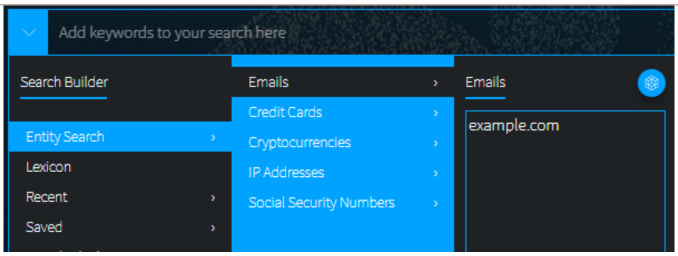
Use 'to' and 'from' together to form a range, or just set 'from' to a period in the past (i.e. 6 hours) to find all documents found in the last 6 hours. Keep in mind that while crawl date in the UI is displayed in local time, the API parameters and crawlDate field returned are in UTC.

UI	API
Filters -> Dates	'to' and 'from'
 Crawl Date: Custom Start Date: 08/26/2020 End Date: 09/02/2020	/api/v1/search?from=2020-08-26T00:00:00Z&to=2020-09-02T00:00:00Z

Find email addresses in documents

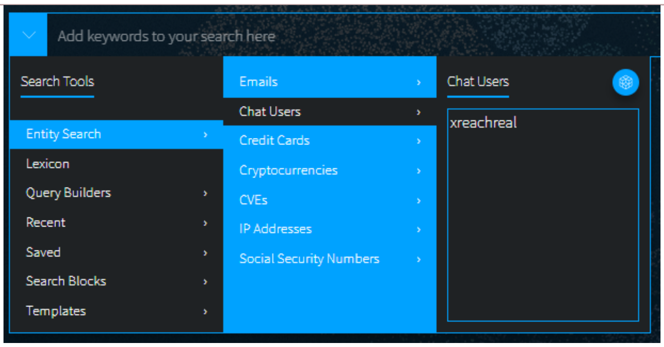
UI	API
Search Builders -> Entity Search -> Emails	'email'
 Add keywords to your search here Search Builder Entity Search Lexicon Recent Saved Emails Credit Cards Cryptocurrencies IP Addresses Social Security Numbers Emails: jane.doe@example.com	/api/v1/search?email=jane.doe@example.com

Finding all email addresses from a domain in documents

UI	API
Search Builders -> Entity Search -> Emails	'emailDomain'
 Add keywords to your search here Search Builder Entity Search Lexicon Recent Saved Emails Credit Cards Cryptocurrencies IP Addresses Social Security Numbers Emails example.com	/api/v1/search?emailDomain=example.com

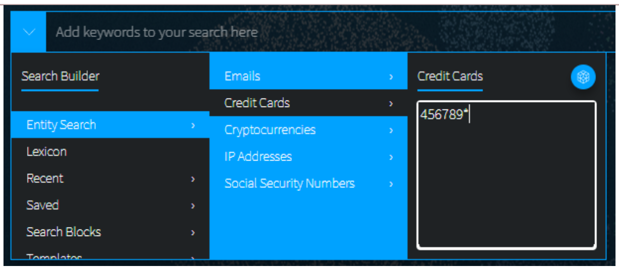
Find chat users in documents

Use the chatUsers parameter to find documents with usernames or user IDs from Telegram or Discord. For Discord usernames, only include the name, not the hashtag or suffix.

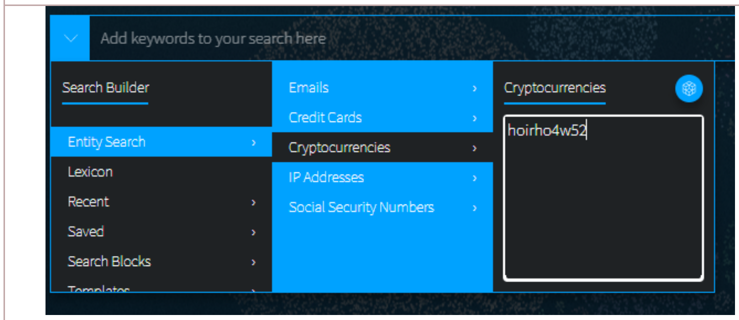
UI	API
Search Builders -> Entity Search -> Chat Users	'chatUser'
 Add keywords to your search here Search Tools Entity Search Lexicon Query Builders Recent Saved Search Blocks Templates Emails Chat Users Credit Cards Cryptocurrencies CVEs IP Addresses Social Security Numbers Chat Users xreachreal	/api/v1/search?chatUser=xreachreal Acceptable input includes either username or user ID

Find credit card numbers in documents

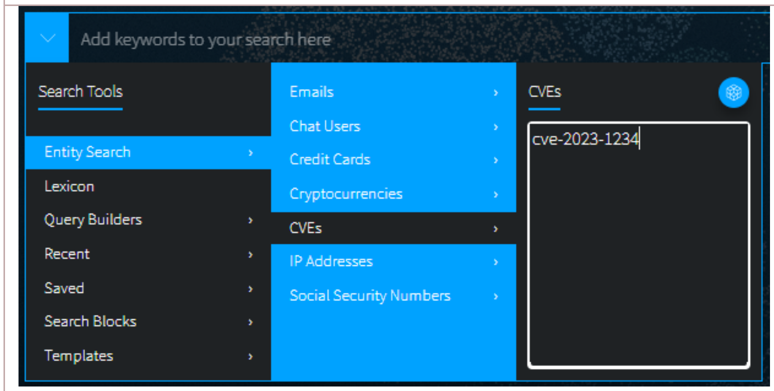
Full credit card number or BIN searching is available in both the UI and API. For full credit card numbers, type the number in the Credit Card search builder. For BIN searching (example below), type the BIN digits and a wildcard character (*) in the Credit Card search builder.

UI	API
Search Builders -> Entity Search -> Credit Cards	'ccn'
 Add keywords to your search here Search Builder Entity Search Lexicon Recent Saved Search Blocks Emails Credit Cards Cryptocurrencies IP Addresses Social Security Numbers Credit Cards 456789*	/api/v1/search?ccn=456789*

Find cryptocurrency addresses in documents

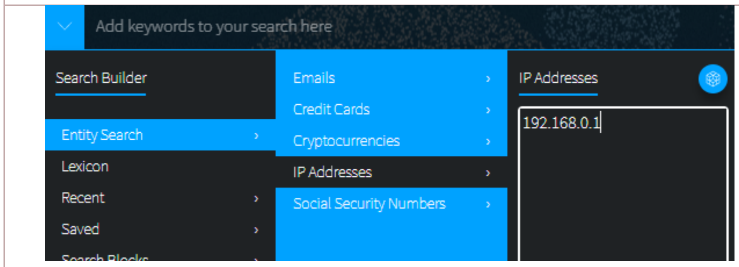
UI	API
Search Builders -> Entity Search -> Cryptocurrencies	'cryptoAddress'
 Add keywords to your search here Search Builder Entity Search Lexicon Recent Saved Search Blocks Templates Emails Credit Cards Cryptocurrencies IP Addresses Social Security Numbers Cryptocurrencies hoirho4w52	/api/v1/search?cryptoAddress=hoirho4w52

Find CVEs in documents

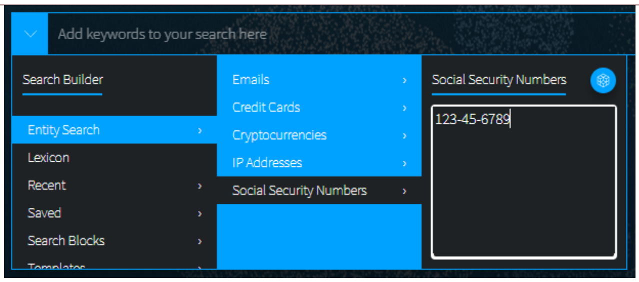
UI	API
Search Builders -> Entity Search -> CVEs	'cve'
 Add keywords to your search here Search Tools Entity Search Lexicon Query Builders Recent Saved Search Blocks Templates Emails Chat Users Credit Cards Cryptocurrencies CVEs IP Addresses Social Security Numbers CVEs cve-2023-1234	/api/v1/search?cve=cve-2023-1234 Acceptable inputs include any of: cve-2023-1234 cve-2023 2023 2023-1234

Find IP addresses in documents

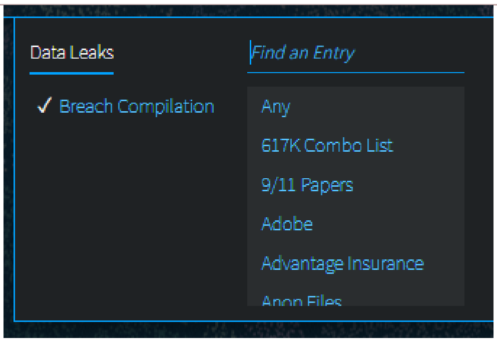
For API, you can use either the 'ipAddress' field or just use the q field.

UI	API
Search Builders -> Entity Search -> IPs	'ipAddress' or 'q'
 Add keywords to your search here Search Builder Entity Search Lexicon Recent Saved Search Blocks Emails Credit Cards Cryptocurrencies IP Addresses Social Security Numbers IP Addresses 192.168.0.1	/api/v1/search?ip=192.168.0.1 /api/v1/search?q=192.168.0.1

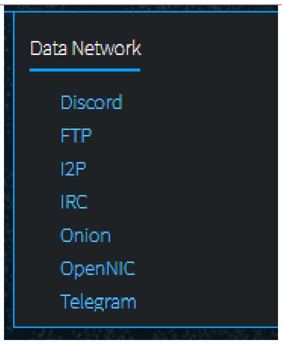
Find social security numbers in documents

UI	API
Search Builders -> Entity Search -> Social Security Numbers	'ssn'
 Add keywords to your search here Search Builder Entity Search Lexicon Recent Saved Search Blocks Templates Emails Credit Cards Cryptocurrencies IP Addresses Social Security Numbers Social Security Numbers 123-45-6789	/api/v1/search?ssn=123-45-6789

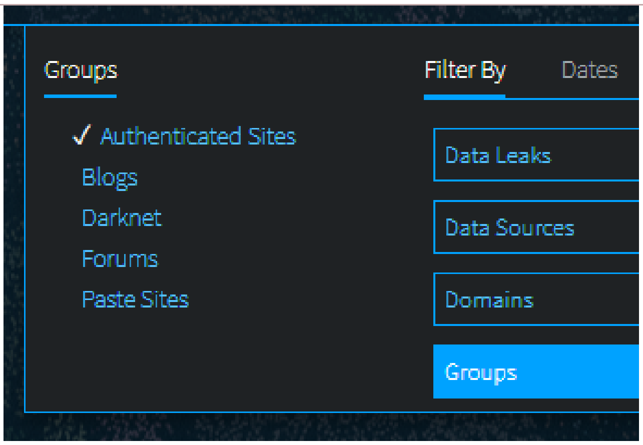
Filter to results from a data leak

UI	API
Filters -> Data Leaks	'leak'
 Data Leaks Find an Entry Any 617K Combo List 9/11 Papers Adobe Advantage Insurance Anon Files ✓ Breach Compilation	/api/v1/search?leak=breachcompilation

Filter to results collection from a data network

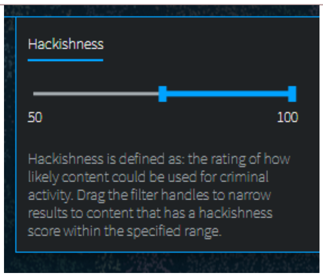
UI	API
Filters -> Data Network	'source'
 Data Network Discord FTP I2P IRC Onion OpenNIC Telegram	/api/v1/search?source=onion Source values are: discord, ftp, i2p, irc, onion.v2, onion.v3, openNIC, telegram, zeronet

Filter to results classified as a particular group or type

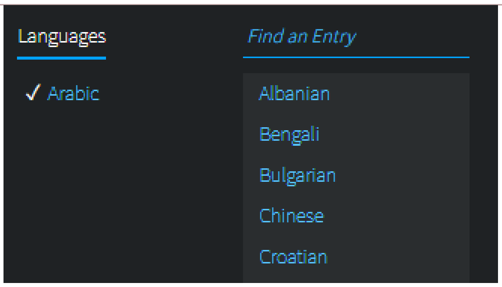
UI	API
Filters -> Groups	'group'
 Groups Filter By Dates ✓ Authenticated Sites Blogs Darknet Forums Paste Sites Data Leaks Data Sources Domains Groups	/api/v1/search?group=authenticated Other group values include: blogs markets chans pastes darknets ransomware forums

Filter to results scored with Hackishness

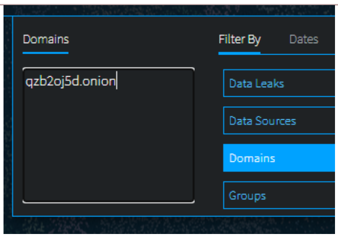
Hackishness in the UI is displayed as a percentage value, but it's really a floating point value between 0 and 1. Hackishness of "50%" in the UI is equivalent to 0.5 in the API. Hackishness is defined as: the rating of how likely content could be used for criminal activity.

UI	API
Filters -> Hackishness Range Slider	'hack_min' and 'hack_max'
 Hackishness is defined as: the rating of how likely content could be used for criminal activity. Drag the filter handles to narrow results to content that has a hackishness score within the specified range.	/api/v1/search?hack_min=.15&hack_max=.80

Filter to results in a certain language

UI	API
Filter by -> Language	'lang'
 Languages Find an Entry ✓ Arabic Albanian Bengali Bulgarian Chinese Croatian	/api/v1/search?lang=Arabic Value options located here

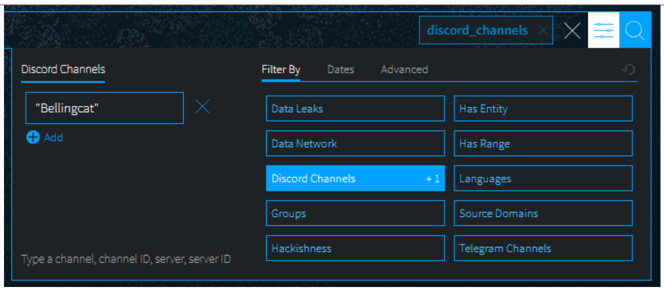
Filter to results that were collected from a particular domain

<table>
<tr><th>UI</th><th>API</th></tr>
<tr><td>Filters -> Domain</td><td>'domain'</td></tr>
<tr><td>

Domains: qzb2oj5d.onion

</td><td>/api/v1/search?domain=qzb2oj5d.onion</td></tr>
</table>

Filter to results from a particular Discord channel or server

Use to filter the result set to Discord content. Acceptable input includes a Discord channel name, channel ID, server name, or server ID.

<table>
<tr><th>UI</th><th>API</th></tr>
<tr><td>Filters -> Discord Channels</td><td>'discordChannel'</td></tr>
<tr><td>

discord_channels

Discord Channels: "Bellingcat"

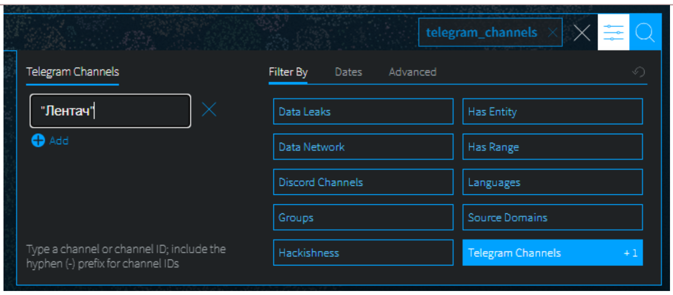
Type a channel, channel ID, server, server ID

</td><td>/api/v1/search?
discordChannel=Bellingcat

Note: do not use quotes in the API</td></tr>
</table>

Filter to results from a particular Telegram channel

Use to filter the result set to Discord content. Acceptable input includes a Telegram channel name or channel ID (including the hyphen - prefix).

<table>
<tr><th>UI</th><th>API</th></tr>
<tr><td>Filters -> Telegram Channels</td><td>'telegramChannel'</td></tr>
<tr><td>

telegram_channels

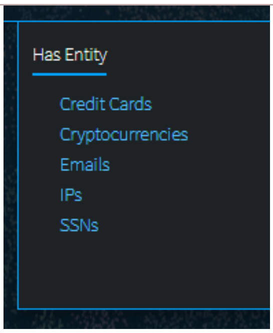
Telegram Channels: "Лентач"

Type a channel or channel ID; include the hyphen (-) prefix for channel IDs

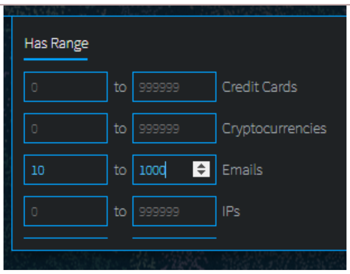
</td><td>/api/v1/search?
telegramChannel=Лентач

Note: do not use quotes in the API</td></tr>
</table>

Filter to results that have particular entities in them

UI	API
Filters -> Has Entity	'has'
 Has Entity Credit Cards Cryptocurrencies Emails IPs SSNs	/api/v1/search?has=email /api/v1/search?has=ssn /api/v1/search?has=ccn /api/v1/search?has=cryptocurrency /api/v1/search?has=cve /api/v1/search?has=ip

Filter to results that have a certain number of entities in them

UI	API
Filters -> Has Range (Credit Cards) Filters -> Has Range (Emails) Filters -> Has Range (SSNs) Filters -> Has Range (IPs) Filters -> Has Range (Cryptocurrencies) Filters -> Has Range (CVEs)	'cccn_min' and 'cccn_max' 'cemail_min' and 'cemail_max' 'cssn_min' and 'cssn_max' 'cip_min' and 'cip_max' 'ccrypto_min' and 'ccrypto_max' 'ccve_min' and 'ccve_max'
Has Range 0 to 999999 Credit Cards 0 to 999999 Cryptocurrencies 10 to 1000 Emails 0 to 999999 IPs	/api/v1/search?cemail_min=10& cemail_max=1000

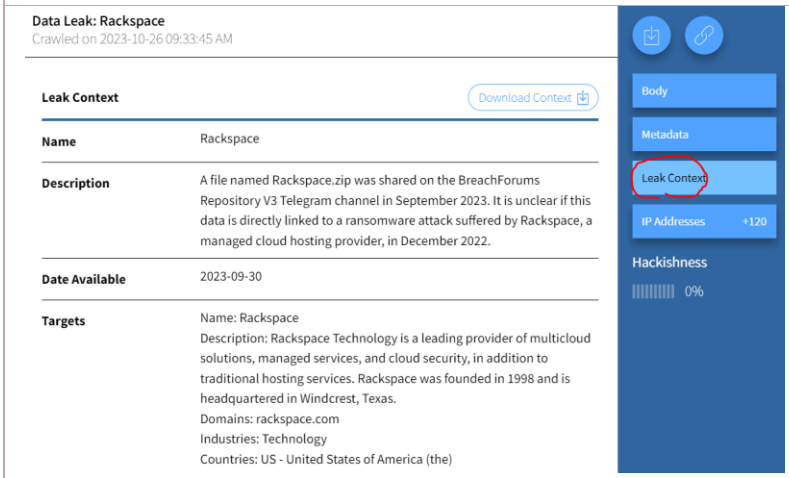
Additional Response Options

The following API parameters can be used according to your preference. The DarkOwl Vision UI uses the following defaults:

- req (false)
- detail (full)
- count (20)
- highlight (true)
- empty (false)

Using the Leak Context endpoint with data leak search results

Enrichment Option: When a search result retrieved from Search API is from a data leak, it will return a leak field which includes name, host, associations, and other leak-specific fields. If part of your API subscription, the leak name can be passed to the Leak Context endpoint in order to retrieve analyst-curated information about the leak itself.

UI	API
Search Result -> Leak Context button	Use leak name value with Leak Context API
 Data Leak: Rackspace Crawled on 2023-10-26 09:33:45 AM Leak Context Name: Rackspace Description: A file named Rackspace.zip was shared on the BreachForums Repository V3 Telegram channel in September 2023. It is unclear if this data is directly linked to a ransomware attack suffered by Rackspace, a managed cloud hosting provider, in December 2022. Date Available: 2023-09-30 Targets: Name: Rackspace Description: Rackspace Technology is a leading provider of multicloud solutions, managed services, and cloud security, in addition to traditional hosting services. Rackspace was founded in 1998 and is headquartered in Windcrest, Texas. Domains: rackspace.com Industries: Technology Countries: US - United States of America (the) Download Context Body Metadata Leak Context IP Addresses +120 Hackishness 0%	/api/v1/context/leak? name=[leaknamevalue]