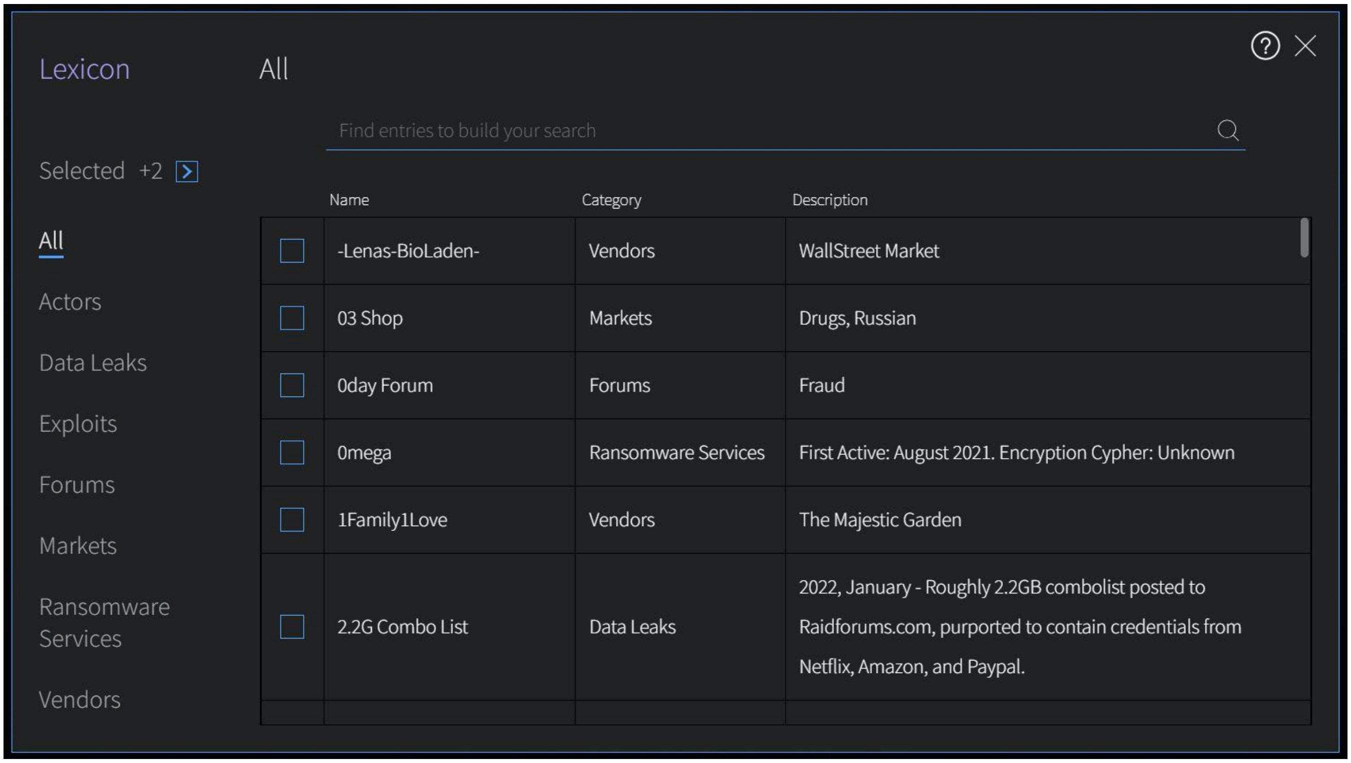
Lexicon Content Guide for DarkOwl Vision

The Basics: How to Use the Lexicon

The DARKINT Search Lexicon includes curated lists of commonly searched keywords, domains, and data leaks, intended to help you find interesting content within our data collection. While not an exhaustive list of items in our data, it's a good place to get started.

To use the Lexicon, pick a topic on the left, or start typing in the Find Entries bar. Selecting the box next to your desired entry(ies) will immediately add the entry(ies) to the search bar. Click the > icon, or anywhere outside of the modal, to go back to the Search Bar.



Lexicon

All

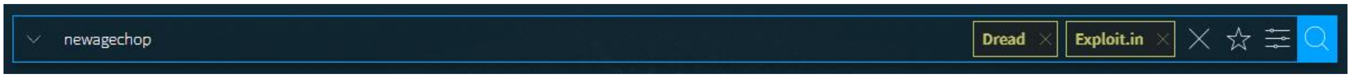
Find entries to build your search

Selected +2

All
Actors
Data Leaks
Exploits
Forums
Markets
Ransomware Services
Vendors

	Name	Category	Description
□	-Lenas-BioLaden-	Vendors	WallStreet Market
□	03 Shop	Markets	Drugs, Russian
□	0day Forum	Forums	Fraud
□	0mega	Ransomware Services	First Active: August 2021. Encryption Cypher: Unknown
□	1Family1Love	Vendors	The Majestic Garden
□	2.2G Combo List	Data Leaks	2022, January - Roughly 2.2GB combolist posted to Raidforums.com, purported to contain credentials from Netflix, Amazon, and Paypal.

In the screenshot below, we've selectied Dread and Exploit.in forums, which will filter results to content from only those two forums. You can run the search with just the Lexicon entries, or add more keywords to your search (example shown below).



newagechop

Dread

Exploit.in

Guidelines for using multiple search components (Filters, Lexicon entries, and free text) in the same search. Generally, using multiple different search components AND together; using multiple of the same search component (but different values) OR together:

- Lexicon Market, Lexicon Exploit in same search—AND
- Lexicon Actor, Lexicon Actor in the same search—OR
- Network (Tor), Network (Discord) in the same search—OR
- Entity Search, Search Bar Free Txt in the same search—AND

Submit an Entry to the Lexicon

The Lexicon continues to grow as we add more content and hear from our customers. If you know of a new threat actor or darknet marketplace that's not in our list – please let us know about it at https://www.darkowl.com/lexicon.

Topics You'll Find in the Lexicon

Section	**Search Component**	**Description**
Actors	Free Text query string	Use the Actor lexicon to find actor names mentioned within search results. Actors are malicious individuals or groups that carry out targeted attacks or campaigns, with motives ranging from political hactivism to cybercrime. Many of the actors in the Lexicon come from from the MITRE attack groups list. Note: with the Actor and Vendor lexicons, it may be helpful to use additional search terms or Search Blocks to reduce false positive results with Actor names that are also common words, such as (HACK CRACK FULLZ EXFILTRATION DDOS).
Data Leaks	Filter: Leak	Use the Data Leaks lexicon to find search results from known breaches or other leak data that are tagged by name in our data. A description of each breach is included.
Exploits	Free Text query string	Use the Exploits lexicon to find exploit names mentioned within search results. Exploits are software tools designed to capitalize on flaws in a computer system, typically for malicious purposes. Examples: trojans, malware, viruses, RATs, ransomware, botnets.
Forums	Filter: Domain	Use the Forums lexicon to find search results from known darknet and deep web forms. Forums are online places where

		people discuss specific topic threads. Some require authentication to access. Forums that are associated with specific markets and/or vendor reviews are indicated.
Markets	Filter: Domain	Use the Markets lexicon to find search results from known darknet market domains and vendor shops. Content includes both small, vendor-owned markets, to big-name marketplaces such as Hydra and Empire. Some marketplaces have previously been taken down by law enforcement, though our data collection may still have historical content.
Ransomware Services	Filter: Domain	Use the Ransomware Services lexicon to find search results from domains administered by ransomware gangs. Each entry includes a description of when the gang was first active, associates and affiliates, and encryption cipher used.
Vendors	Free Text query string	Use the Vendors lexicon to find vendor names mentioned within search results. Vendors are sellers of goods or services on darknet marketplaces or forums. Each vendor in the Lexicon includes markets or forums where the vendor is active.

Actors and Vendors

- Use additional search terms to reduce false positive results with Actor or Vendor names that are also common words.
    - For vendors, use terms such as PROFILE VENDOR SALE COUNTERFEIT.
    - For actors, use terms such as HACK CRACK FULLZ EXFILTRATION DDOS.

Forums and Markets

- Scroll to the middle of the page to find good stuff: markets and forums tend to have a lot of “filler” content, such as a forum mantra that is repeated on every page.
- We’ve labeled each Forum and Market with descriptive categories. Many sites have content in multiple categories; categories have been assigned for the main topics

Data Leaks

- Each data leak has a description of where and when it was found, as well as the types of information contained within it.
- DarkOwl focuses on data leaks found or posted on the dark web.