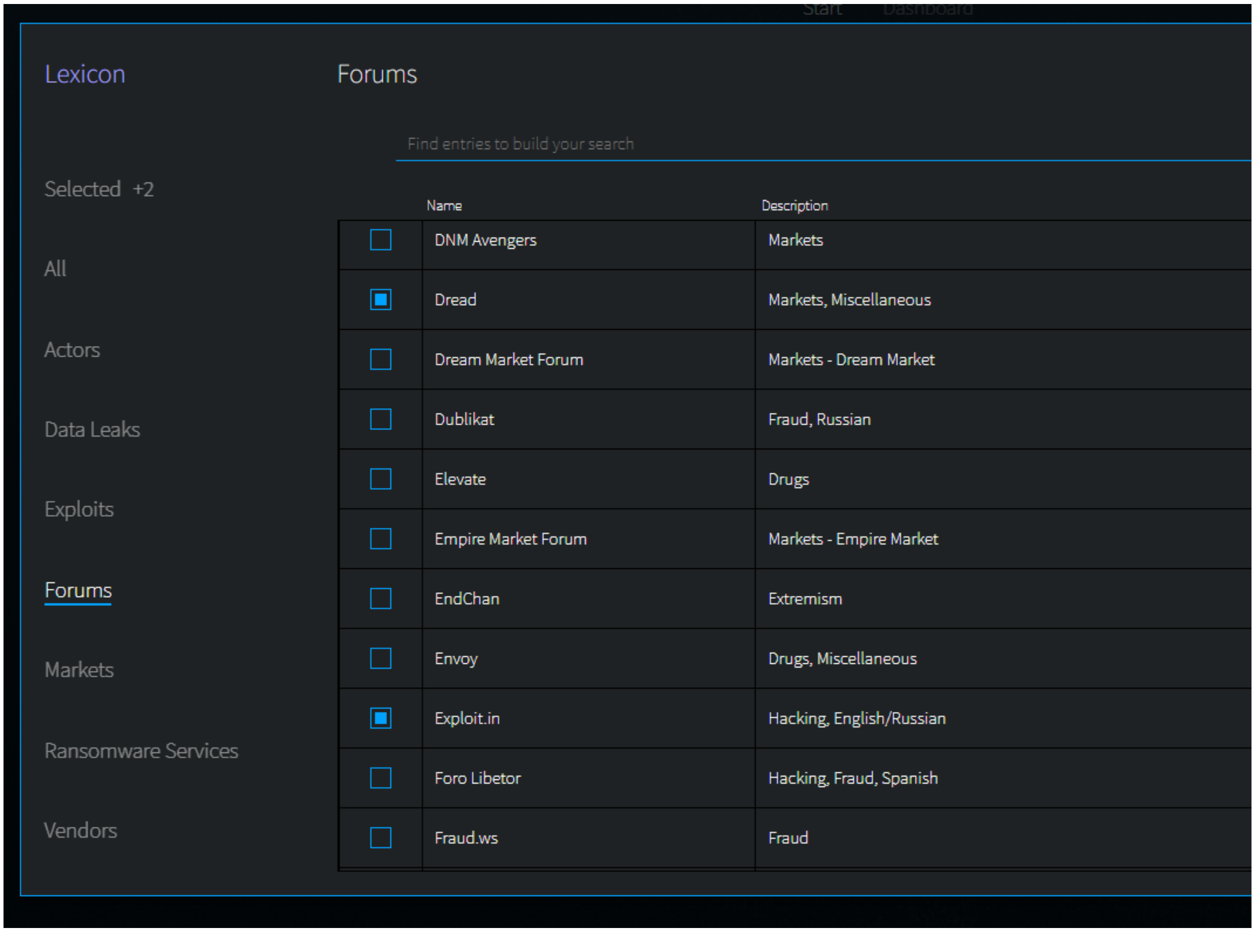
Lexicon Content Guide for DarkOwl Vision

The Basics: How to Use the Lexicon

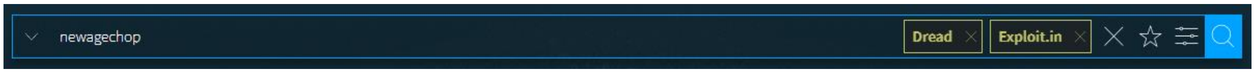
The **DARKINT Search Lexicon** includes curated lists of commonly searched keywords, domains, and data leaks, intended to help you find interesting content within our data collection. While not an exhaustive list of items in our data, it's a good place to get started.

Start searching over *All* content, or pick a topic on the left, then filter or scroll to find entries of interest. Selecting the box next to your desired entry(ies) will add them to the search bar. In the screenshot below, we're selecting Dread and Exploit.in forums. This will filter results to only those two markets.



	Name	Description
□	DNM Avengers	Markets
☑	Dread	Markets, Miscellaneous
□	Dream Market Forum	Markets - Dream Market
□	Dublikat	Fraud, Russian
□	Elevate	Drugs
□	Empire Market Forum	Markets - Empire Market
□	EndChan	Extremism
□	Envoy	Drugs, Miscellaneous
☑	Exploit.in	Hacking, English/Russian
□	Foro Libetor	Hacking, Fraud, Spanish
□	Fraud.ws	Fraud

Click the X to go back to the search bar. You can run the search with just the Lexicon entries, or add more keywords to your search (example shown below).



newagechop

Submit an Entry to the Lexicon

The Lexicon will continue to grow and become more comprehensive as we add more content. So, if you know a prominent threat actor, or have heard of a darknet marketplace that's not in our list – we want to know about it! Submit your entry at darkowl.com/lexicon.

Topics You'll Find in the Lexicon

Actors	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 this list from MITRE. Note: with the Actor and Vendor lexicons, it may be helpful to use additional search terms to reduce false positive results with Actor names that are also common words, such as *(HACK CRACK FULLZ EXFILTRATION DDOS)*.
Data Leaks	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	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	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	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	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	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.
- We focus on data leaks found or posted on the dark web.