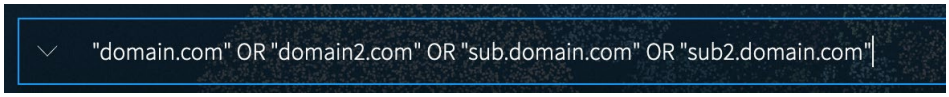
DARKINT Exposure Search Guide

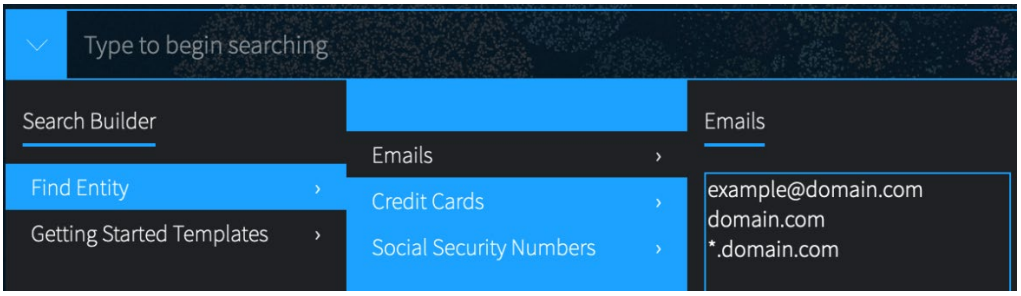
>> General Exposure Search – Domain Mentions

To find mentions of a domain on the dark web, simply enter all relevant organizational domains in the search bar.



>> General Exposure Search – Email Mentions

1. Use the "Search Builder" on the left side of the search bar.
2. Select "Find entity" → "Emails" and enter either a specific email address, or a domain to monitor. (The * is used to capture any subdomains.)



3. Remove *example@domain.com* to return every document we have with at least one email address ending in "domain.com".

>> Recommended Filters

These filters can be used to narrow down to the results used in the calculation of an Exposure Score.

Crawl Date

The Scores formula weighs recent search results more heavily than "all-time" results. To filter to these recent results that are weighed more heavily, use the Crawl Date filter and filter to "Last 90 days".

Hackishness

Hackishness is measured on a scale of 0.0-1.0 (in the UI, represented as a percentage). Higher hackishness values indicate more vulnerable information in the document. A useful trick is to set the hackishness filter to a range of 1-100, to eliminate all 0% hackish documents

Groups/Data Leaks

Scores takes Darknet, Transitory, and Data Leak credentials and domain mentions into account.

- To filter to darknet results only, use the **"Darknet"** option under the **Groups filter.**
- To filter to transitory results only, use the **"Paste Sites"** option under the **Groups filter.**
- To filter to results found only in Data Leaks, select **"Any"** under the **Data Leaks filter.**