USE RESEARCH TOOLS

Research Tools enables users to safely explore open-source, dark web, and raw data that Mandiant Threat Intelligence has collected for Digital Threat Monitoring (DTM). Providing raw threat and related data in an easy interface, Research Tools helps you find what matters, see what is happening in the cyber realm, and thus better protect your business.

We recommend you use Research Tools as a precursor to creating a Monitor. This will help you create Monitors focused on what matters and reduce false positives.

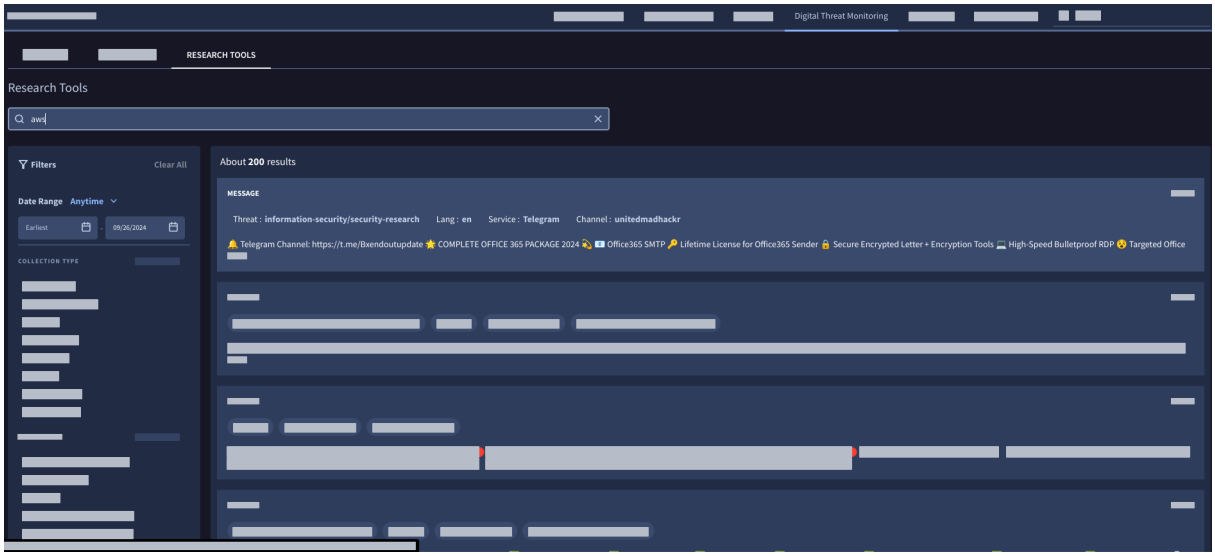
Access Research Tools

1. Sign into Mandiant Advantage.
2. Navigate to DTM (**MANDIANT ADVANTAGE** > **Threat Intelligence** > **Digital Threat Monitoring**).
3. Click **Research Tools**.

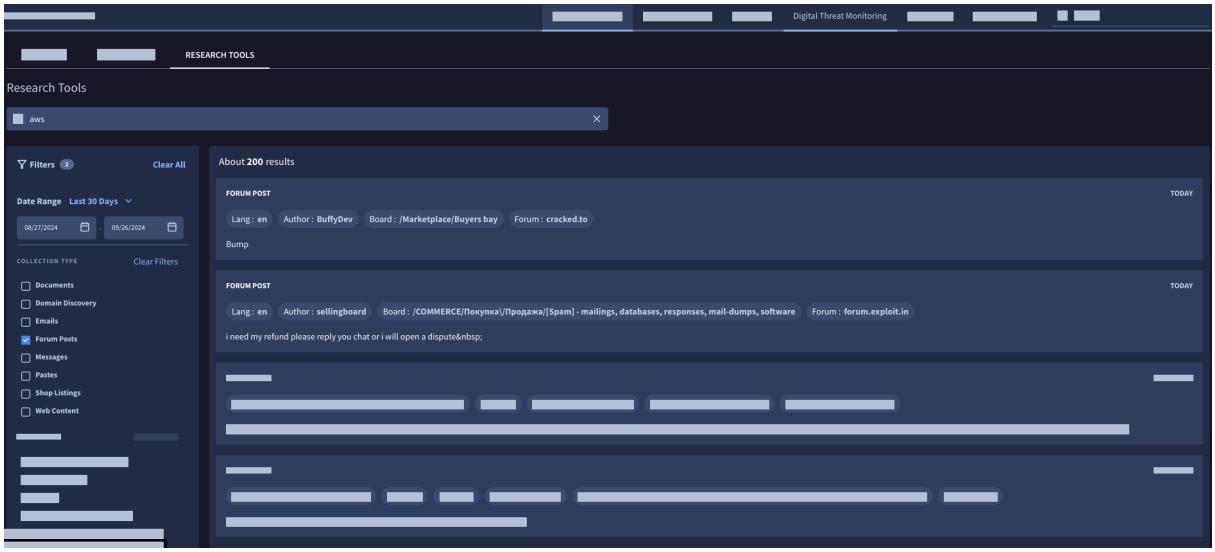
Search using Research Tools

The search bar is intended to meet needs of basic users and advanced users. There are additional filters on the left side of the search to help you refine your search. If you're an advanced user, you can use the **Lucene query syntax (https://www.elastic.co/guide/en/elasticsearch/reference/7.15/query-dsl-query-string-query.html#query-string-syntax)** when creating your query. For Lucene search examples see **Lucene Queries (https://docs.mandiant.com/home/dtm-lucene-queries)**.

1. Enter your search term or terms and press `Enter`. In the following screen, `aws` is used as a term in the search bar:

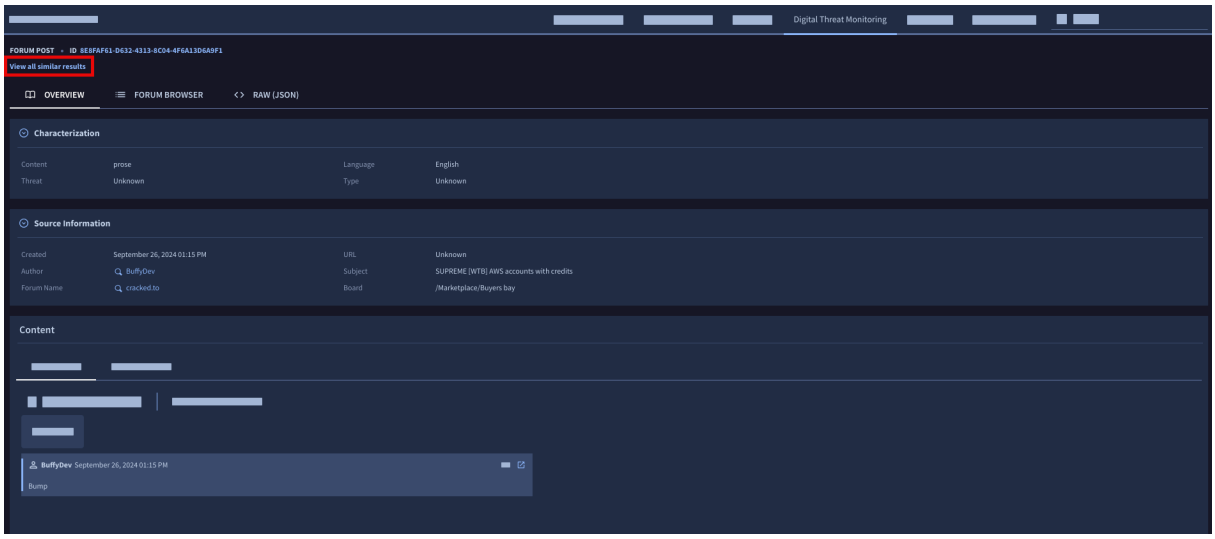


   As you can see in this enhanced view, results are explored and important contextual information is captured at a glance for your review.
2. Optional: Select one or more **Collection Type** to filter your results. Filters automatically apply as you select them.
3. Optional: Change the date range by clicking on the calendar icon. The results are automatically filtered when you select the date range. For example, see the following screen where the **Forum Post** is selected with a **Date Range** for **Last 30 Days**.



4. Click one of the results. It launches in a new page, allowing you to see an overview of the content found and with other tabs **Forum Browser** and **<>Raw (JSON)**.

> If you select **Form Post** for the **Collection Type**, you get an additional **Forum Browser** tab as shown in the following screen.

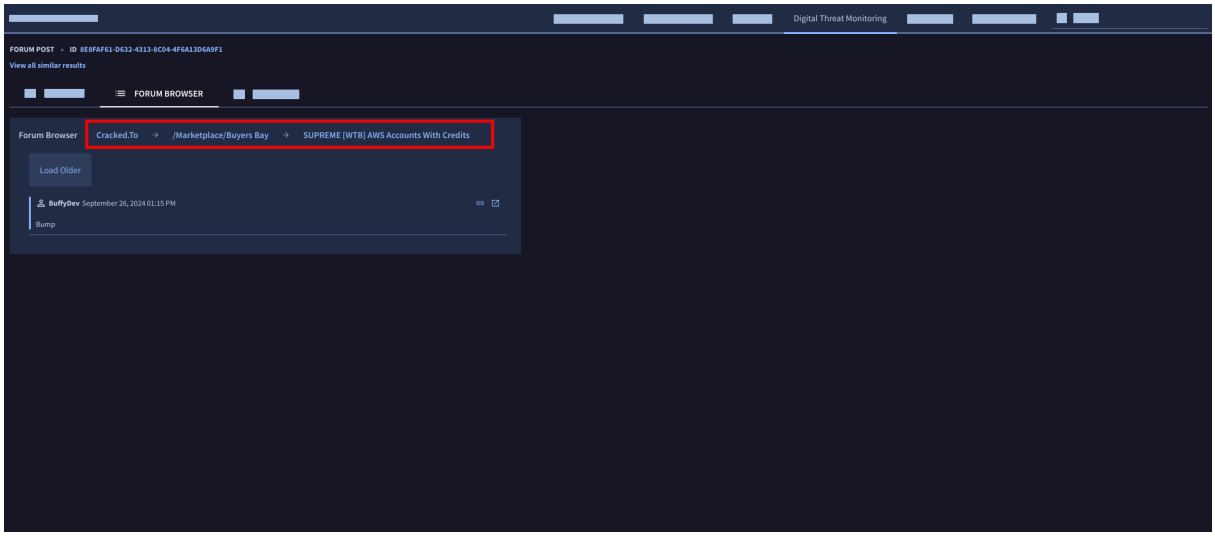


5. Optional: To look at similar content, click **View all similar results**. This step creates a new Research Tools query.

> This functionality is not supported for Domain Discovery and Shop Listings Collection Types.

6. Select **Forum Browser** to browse all the threads in the **Forum Post** with breadcrumbs for further navigation and digging.

> HTML and JAVA scripts are deleted to avoid any malicious content and navigation within a secure environment.



7. Click one of the breadcrumb links to get the summary of that board.