Threat Logs

https://campus.barracuda.com/doc/73721397/

Viewing and Searching Threat Logs

The Threat Logs page lists files scanned by the Barracuda Content Shield Suite MPC agent that were determined to be suspicious or malicious, or were encrypted. To view the Threat Logs for an account, navigate to the **Accounts** page, click **Manage** for that account, then do the following:

1. Click **Threat Logs** in the left navigation menu.
2. In the search box at the top, enter an endpoint name, a filename, or leave the search box empty to view all threat logs for the account for the selected date range.

Threats identified by the service are logged by:

- **Date**
- **User**
- **Endpoint Name**
- **Path**
- **Filename**
- **Scan Determination** – *Suspicious*, *Malicious* or *Encrypted*. For handling of encrypted or password-protected files, see How to Set Threat Policies.

Sorting and Reporting Threat Log Data

- To download a scan report showing file metadata, threat analysis, and other details about the file, click on the *Report* icon in the **View** column.
- To change the date range of the display, select **Last 7 days, Last 30 days or Last 24 Hours** from the drop-down on the upper right of the page.
- To change the Threat Logs view, select the number of rows to display using the **Rows per page** drop-down at the bottom of the display.
- To export the logs, click **Download CSV**.

Reporting False Positives

If you determine that any files scanned were falsely reported as suspicious or malicious, you can report that file to Barracuda by doing the following:

1. On the **THREAT LOGS** page, click the 3 dots (⋮) in the **More** column.
2. Click on *Report False Positive*.
3. You'll see a pop-up with the file name. Click **Report** to send the file to Barracuda, or click **Cancel.**

Figures

1. 3Dots.png