How to Use Advanced Threat Protection Reports

https://campus.barracuda.com/doc/54265199/

When the Advanced Thread Protection (ATP) service determines an attachment contains a threat and blocks the message, Barracuda Networks recommends that you review each infected ATP Report before determining whether to deliver the message.

Determine Whether to Deliver Message

1. Log in to Cloud Protection Layer as the administrator, and go to **MESSAGE LOG**.
2. Set message filters and search criteria as needed, and click **Search**.
3. Messages blocked by ATP display as **Not Delivered**.
4. Click on the message, and in the reading pane, click **ATP Reports**.
5. The **Email Delivery Warning** dialog box displays a list of attachments, one or more of which is suspected of being **Infected**. If you want to deliver the email and the associated attachments, first review the report for each attachment.
6. Click **View Report** for the suspicious attachment, and review the report details.
7. Repeat *step 6* for each attachment.
8. Once you review all attachments, and if you determine you want to deliver the email and the associated attachments, review and accept the disclaimer, and click **Deliver** in the **Email Delivery Warning** dialog box.
9. If the message is delivered successfully, the **Delivery Status** changes to **Delivered**. If the mail cannot be delivered, this is reflected as a notice in your browser window and the **Delivery Status** does not change.

ATP Classifications

- **Malicious** – File classified as high risk. File is highly likely to be malware.
- **Suspicious** – File classified as medium risk. File may pose a potential risk.
- **Clean** – File classified as low risk. No malicious indicators were detected.
    Exercise caution even with files marked CLEAN as malware authors are continually finding new ways to evade detection.

Terminology

- **Determination versus Verdict** – When a scan is complete and the risk potential is classified, that scan displays a *Determination*. For example, if the file is determined to have medium risk,

the determination is **Suspicious**. After all scans are complete, a *Verdict* displays based on the determination of all scans.

- **Reclassified** – If a scan determination is **Malicious** or **Suspicious**, but the file is reviewed by the Barracuda Analyst Team and determined to be **Clean**, the *Verdict* displays as **Clean** and **Reclassified by Analyst** displays.

ATP Report Sections

The ATP report is divided into the following sections:

Scan Description

This section provides a short description of the ATP report and how the scan verdict is reached.

Overall Determination

This section displays the scan verdict and reason for this file. The verdict is based on the outcome, or determination, of each scan.

File Metadata

This section lists file-specific details including file extension, file size, meta-data, and when the file was first submitted.

Threat Analysis

This section lists the outcome of each scan:

- Enhanced Antivirus detection scans the file through a comprehensive system of traditional antivirus signatures.
- Behavioral Heuristics analyzes through a heuristics engine utilizing behavioral indicators.
- Sandboxing executes the file in an isolated environment where its behavior is analyzed and assigned a risk level.