

Understanding Advanced Threat Protection Reports

<https://campus.barracuda.com/doc/51191630/>

The Advanced Threat Protection (ATP) service scans files for malware, zero-day exploits, and targeted attacks not detected by Email Gateway Defense virus scanning features or intrusion prevention system. ATP analyzes files in a separate, secured cloud environment, and once scanning is complete, determines the risk level for each scan (determination), and then assigns a verdict.

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.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.