Understanding Advanced Threat Protection Reports

https://campus.barracuda.com/doc/96023051/

The Advanced Threat Protection (ATP) service analyzes inbound email attachments with most file types and publicly accessible direct download links in a separate, secured cloud environment, detecting new threats and determining whether to block such messages. ATP offers protection against advanced malware, zero-day exploits, and targeted attacks, such as phishing, not detected by Email Gateway Defense virus scanning features.

ATP Classifications

When publicly accessible direct download links are scanned, and a file is determined to be suspicious, it is automatically classified as malicious; publicly accessible file links are classified as either malicious or clean.

- **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 Networks 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; each detection layer is designed to progressively eliminate threats at different levels of severity and complexity. Note that files may not necessarily undergo all detection layers.

- Enhanced Antivirus detection scans the file through a comprehensive system of traditional antivirus signatures.
- Behavioral Heuristics analyzes through a heuristics engine utilizing behavioral indicators.
- Dynamic Analysis targets zero-day malware and other advanced threats, which are highly elusive and can remain undetected for days and months. A combination of analysis and de-obfuscation of suspicious code makes this layer fast and highly effective at pre-filtering malware for cloud-based sandboxing.
- Sandboxing executes the file in an isolated environment where its behavior is analyzed and assigned a risk level.