Barracuda Active Threat Intelligence

https://campus.barracuda.com/doc/95260599/

Barracuda Active Threat Intelligence (ATI) is a service that provides enhanced capabilities for bot attack detection and prevention, bot classification, configuration management, and visualization for client-side attacks.

It operates as a cloud service and can process millions of events per minute, across geographies. Active Threat Intelligence uses data from the WAF and WAF-as-a-Service as input and augments the information using threat feeds and other intelligence databases. A detailed analysis is carried out on these events individually and as a part of a user session, in order to categorize the clients as humans or bots.

A risk score is then calculated for the clients based on which the local source, i.e., the WAF or WAF-as-a-Service account, can effectively handle bot traffic.

In addition to supporting all the analysis required for Advanced Bot Protection, Active Threat Intelligence is used in client-side protection and the Auto-Configuration Engine.

Active Threat Intelligence tracks any external resources that can be used by the application, such as an external JavaScript or a style sheet. Browser violations reported for such resources can be tracked by administrators for analysis and remediation of the problem. In many cases, the resources may have been modified maliciously, and this can be caught by analyzing the information shown in the ATI dashboard.

ATI uses the metadata and provides configuration recommendations to the administrators through the Auto-Configuration Engine based on the real traffic coming to the applications.

Features of Barracuda Active Threat Intelligence:

- Bot Protection
- Credential Information Lookup
- Auto-Configuration Engine
- Client-side Violation Protection

Active Threat Intelligence infrastructure is made up of multiple layers:

- Augmentation Layer
- Stream Processing Layer
- Session Processors

Augmentation Layer

The Augmentation Layer consumes the raw data, and tags the data with additional information powered by various static threat intelligence databases such as IP reputations and URL reputations. The reputation data is gathered by Barracuda Networks from its own analysis teams as well as from third-party systems. The diverse portfolio of Barracuda Networks provides visibility into a wide range of threat vectors resulting in a much more comprehensive threat intelligence.

Stream Processing Layer

The Stream Processing Layer processes various augmented events in order to detect multiple types of anomalies. These anomalies are primarily in the structure of the traffic. The anomaly detection engine analyzes request metadata using multiple heuristics and machine-learning models. During stream processing, the ATI engines analyze headers, URLs, and other protocol-related parameters to detect unexpected or malicious clients.

Session Processors

Specific session-based models are used to analyze session-related anomalies such as abnormal browsing, application reconnaissance, and fingerprinting.

While processing this traffic, the Threat Intelligence layers create the application's functional profile, which includes the type of traffic the application processes, the normal rates of errors, and the mix of different types of traffic and files. This profile per application is used by the other layers in the system to build specific mitigations to thwart malicious behavior.