Account Protection Dashboard

https://campus.barracuda.com/doc/98212526/

Account takeover occurs when an attacker manages to gain unauthorized access to a legitimate account. The unauthorized access is later used to carry out nefarious activities such as to initiate a fraudulent payment, authorize a wire transfer, or steal sensitive data. Account takeover attacks include the following:

- Credential Stuffing
- Credential Spraying
- Privileged Account Protection

Barracuda Active Threat Intelligence (ATI) provides a mitigation technique for account takeover frauds. For every login, a risk score is generated to identify risky users. With every successful login, a profile is created with network details, location history, device information, and other attributes based on which the risk score is computed. The WAF administrator can use the risk score to take necessary remedial action to prevent further access.

The Account Protection graph displays the total number of login attempts made to the application, and the total number of successful and failed logins. You can drill down to the account level to view the success and failure graph, and drill down even further to the user level to view the profile created for the user, which includes ISP details, geolocation, user agent, header value, and network details.

The Account Protection dashboard displays the following information:

Login Attempts

The **Login Attempts** section provides information about the total number of login attempts made to the application by clients for the selected time scale. The data is generated only when **User Account Profiling** is set to **Yes** for the application/service. You can hover over the graph to see the total number of attempts and the succeeded and failed attempts for a specific time. To see the graph for particular data (**Total Attempts**, **Succeeded** or **Failed**), deselect all other labels apart from the label whose graph you want to see. Click on the label(s) to deselect.

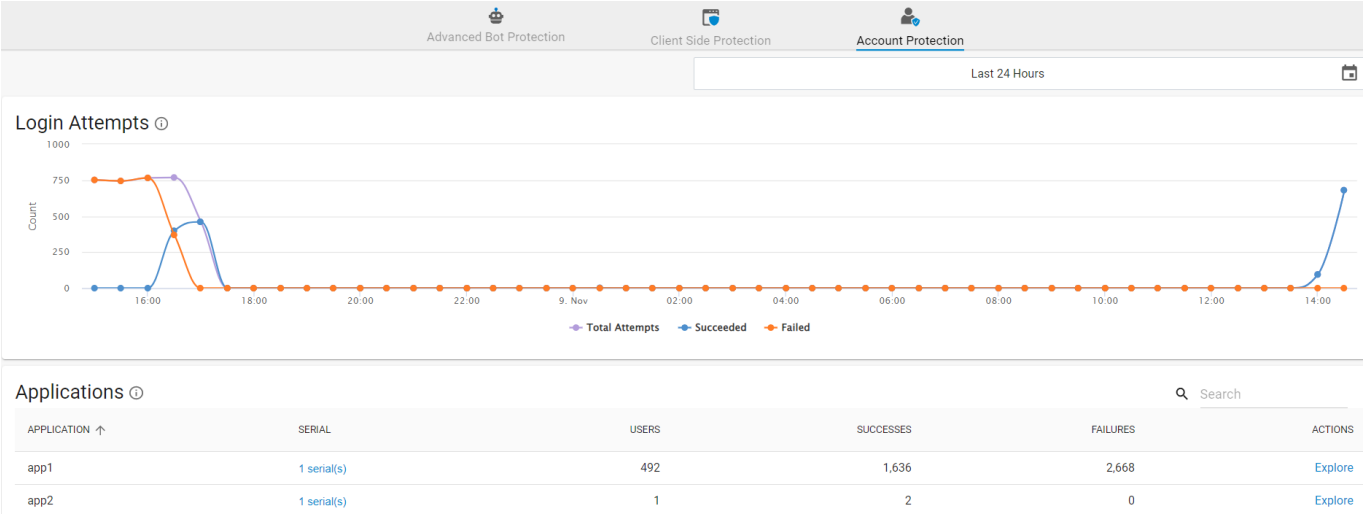
- **Total Attempts**: Displays the total number of login attempts.
- **Succeeded**: Displays the total number of successful login attempts.
- **Failed**: Displays the total number of failed login attempts.

Applications

The **Applications** section provides the details of the application(s) for which account profiling is enabled.

- **Application**: Name of the application.

- **Serial**: Displays the serial number(s) of the appliance(s) the application is configured on.
- **Users**: Total number of users that have accessed the application.
- **Successes**: Total number of successful attempts to the application.
- **Failures**: Total number of failed attempts to the application.
- **Actions**: Click **Explore** to view detailed data about account access and users who accessed the application.



Applications

Search

APPLICATION	SERIAL	USERS	SUCCESSES	FAILURES	ACTIONS
app1	1 serial(s)	492	1,636	2,668	Explore
app2	1 serial(s)	1	2	0	Explore

Figures