Credential Stuffing Protection

https://campus.barracuda.com/doc/86541241/

The Advanced Bot Protection (ABP) feature can provide protection against credential stuffing, which is described in this article. This feature requires the purchase of an ABP license.

Credential stuffing is used to perform account takeover attacks through automated injection of breached username/password pairs. This method uses stolen email and password logins from other sources to gain unauthorized access to accounts. Attackers leverage large numbers of leaked credentials in an automated fashion against numerous websites, in an attempt to take over user accounts with credential reuse. The attacker acquires these spilled usernames and passwords from a website breach, and uses an account checker (such as SentryMBA) to test the stolen credentials against many websites. Successful logins allow the attacker to take over the account matching the stolen credentials.

The Barracuda ABP system uses a cloud-based database of breached credentials to validate incoming login requests. When a match for the incoming credentials is found, the Barracuda Web Application Firewall is configured to alert the admin and / or block such login requests.

The Barracuda Web Application Firewall does not transmit the complete username or password to the Barracuda ABP cloud for validation. The username/password is hashed, and only the first 16 characters of the hash is transmitted to the cloud for validation.

The **BOT MITIGATION > Bot Mitigation** page allows you to enable Credential Stuffing Protection.

1. On the **BOT MITIGATION > Bot Mitigation** page, click **Edit** in the **Options** column next to the desired Bot Mitigation policy. Next, configure the following values:
    1. **Username** – Specifies the username field in the web page from which the actual username can be extracted by the Barracuda Web Application Firewall.
    2. **Password** – Specifies the password field in the web page from which the actual password can be extracted by the Barracuda Web Application Firewall.
2. Click **Save**.