Credential stuffing is an attack in which cybercriminals use bots to attempt automated login attempts on popular sites using stolen usernames and passwords. When successful, the validated credential pair is used by the cybercriminals to commit account takeovers or sold on the dark web. It can cost as little as $0.30 to set up a botnet for use in carding attacks, and it is cheap and easy to run. Credential stuffing attacks fly under the radar, exceeding the limit of requests from an IP address, and because the number of requests from a single source is small and doesn’t exceed the limit of requests from an IP address, it is difficult to detect with volumetric detection. The validated credential pair is used by the cybercriminals to commit account takeovers or sold on the dark web. Credential stuffing attacks are on the rise, and businesses are negatively impacted by bad bots in multiple ways: increased demand, damage to brand reputation, and make goods, refunds, and fines. Is your organization prepared for credential stuffing attacks? Learn more at www.humansecurity.com.