Threat Advisory: Additional Fake Petstock E-Commerce Sites

22 May 2026

Key Points

- Two additional fraudulent e-commerce sites have been identified that impersonate Petstock.
- The domains are part of the same campaign observed in April 2026[1].
- Login credentials entered into the phishing sites may enable threat actors to log into legitimate Petstock customer accounts.
- Credit card details and personally identifiable information entered during the checkout process are expected to be used for fraudulent purposes.
- WOW Group SOC has requested a Cloudflare banner to warn visitors of the fraudulent nature of the two newly identified websites.

Overview

On 20 April 2026, WOW Group SOC reported on a fraudulent website impersonating Petstock. Two additional fake Petstock e-commerce sites (hosted at hxxps://petstockshop[.]shop and hxxps://petstockhubprime[.]shop) have since been identified. The sites are identical to the previously reported phishing site hosted at hxxps://petstockhub[.]shop. As shown in Figure 1, since at least 21 May 2026, the two phishing sites have been impersonating Petstock's legitimate customer website. As with the previously identified site, the newly identified fraudulent sites purportedly offer generous discounts including up to 70% off and free worldwide shipping. The sites contain fraudulent login and checkout forms designed to capture personal and financial information.

[1] See Threat Advisory: Fake Petstock E-Commerce Site published on 20 April 2026 for details of the fake e-commerce site previously identified.

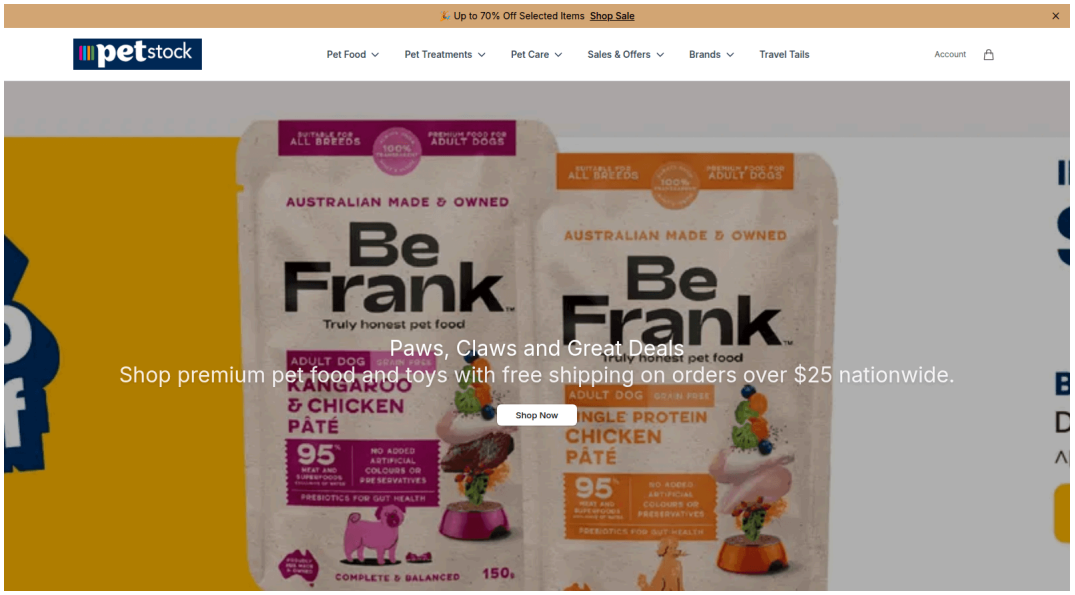

Figure 1 - Fake Petstock shop home page

Threat Detail

The fraudulent domains petstockshop[.]shop and petstockhubprime[.]shop were registered via Dynadot Inc on 30 April 2026 and 15 May 2026 respectively. This is the same registrar as petstockhub[.]shop was registered via on 17 April 2026.

The fake Petstock sites include a login page, shown in Figure 2, as well as a signup page. Any valid Petstock customer credentials entered into the phishing sites could enable unauthorised access into legitimate Petstock customer accounts.

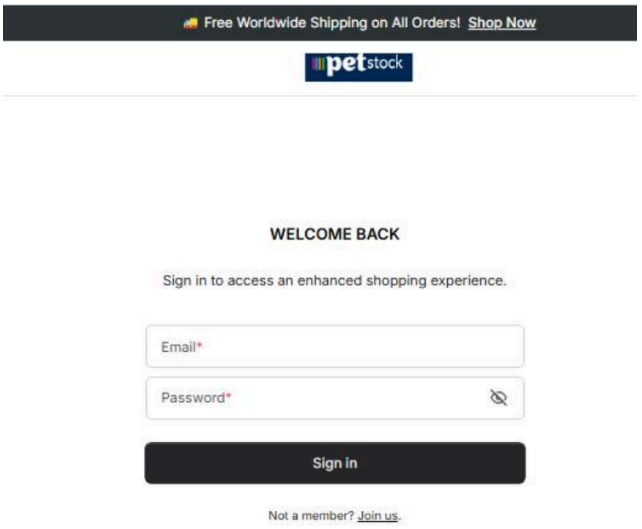

Figure 2 - Fake Petstock shop login page

During the checkout process, the two new sites load an iframe from the domain jigfdrercetv654734[.]shop - a different domain to the domain (kkyq[.]shop) used by the original website. Users enter their credit card details directly into this external iframe instead of the main site. The checkout page establishes a WebSocket connection with this external server while the payment form is open. After submitting payment details, the iframe displays a 3-D Secure[2] verification page to the user.

Both of the domains are Cloudflare-hosted. WOW Group SOC has requested a Cloudflare banner to warn website visitors of the fraudulent nature of both websites.

[2] 3-D Secure (commonly known as 3DS) was introduced by Visa in 2001 to provide an additional layer of security for online payments to help combat credit card fraud. 3DS uses multi-factor authentication (MFA) to help verify that the card is being used by the card owner. It does this by redirecting a customer to their card issuer's 3DS web page after they enter their payment information during the checkout process. The 3DS web page requests the customer to authenticate by:

- Entering a password or answering questions previously set up with their bank
- Entering an OTP sent to their mobile phone
- Biometrics (fingerprint and/or face recognition) using their bank's mobile application.