Report | January 2026

FraudWear

Inside the Cyber Threat of Brand-Impersonating Online Stores

Analysis by CTM360

CTM360®

INDUSTRY	COUNTRY	REGION	DATE
E-Commerce	All	Global	Jan, 2026

OVERVIEW :

CTM360 continues to track the growing threat of brand impersonation scams targeting the **fashion e-commerce ecosystem**. These campaigns exploit consumer trust in established brands and capitalize on online shopping behaviors to facilitate large-scale deception. Fraudsters are increasingly sophisticated in the way they replicate brand identities, leveraging realistic **website designs and digital footprints** that make their operations appear legitimate at first glance.

The sustained growth of this threat highlights the increasing sophistication and persistence of impersonation activity within the digital commerce space. Threat actors constantly adapt to consumer behaviors and platform changes, refining their methods to remain undetected and maximize reach. Beyond the direct impact on individual consumers, these campaigns create significant reputational and operational risks for **affected brands**, eroding trust and undermining confidence in legitimate online retailers.

CTM360 remains actively engaged in identifying, analyzing, and monitoring these threats, continuously tracking new domains, ad campaigns, and associated payment channels.

"FraudWear" refers to a deceptive tactic that creates fake fashion shopping platforms to trick consumers. These sites are crafted to appear professional and appealing, encouraging engagement through seemingly attractive deals. While the look and feel may seem genuine, the purpose of these platforms is to manipulate users and erode confidence in online shopping environments.

Key Findings

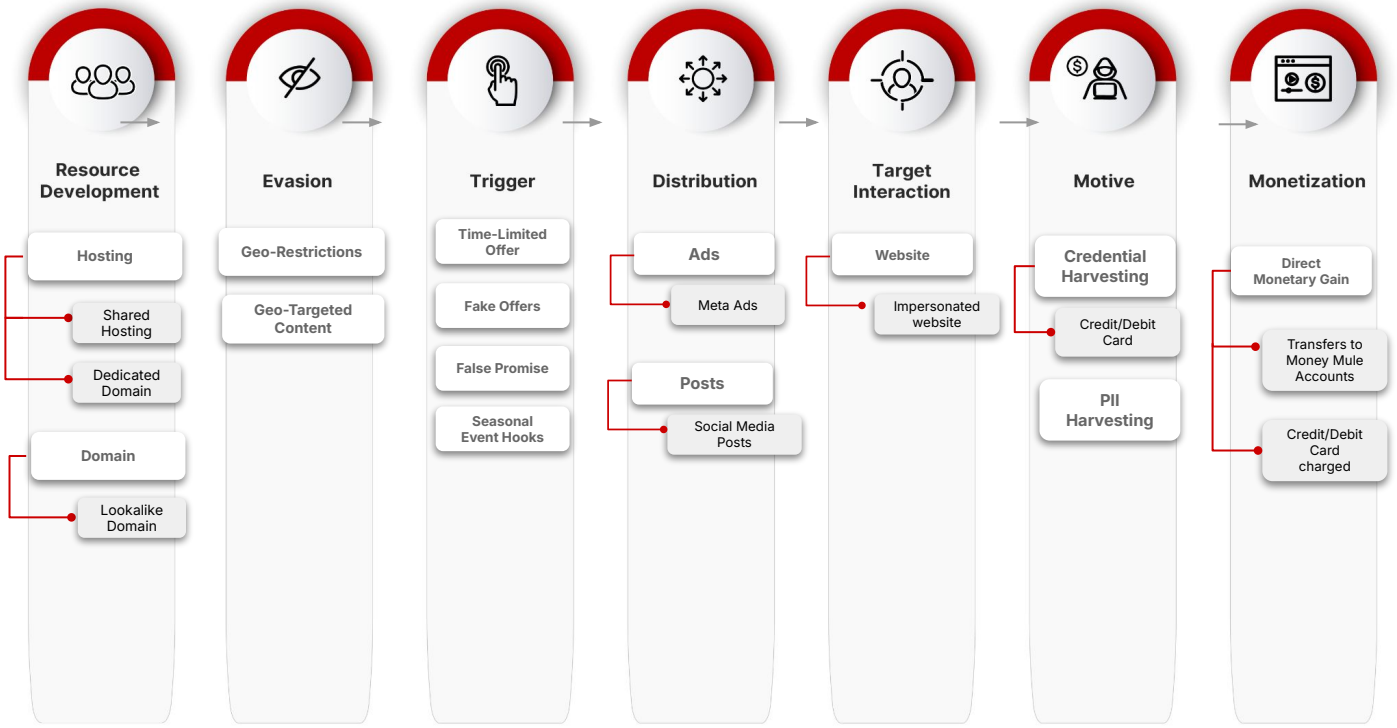
- Over **30k+** malicious fashion e-commerce sites have been identified across **80+ countries,** collectively impersonating **350+ trusted global brands,** including major names like **Nike, Adidas, Puma, and Timberland.**
- These fraudulent sites attract victims by offering deep discounts, exclusive deals, and limited-time promotions on **Apparel and Clothing**, taking advantage of consumer interest in popular brands.
- Victims are led into fraudulent payment flows, resulting in funds sent to money-mule accounts and compromised payment credentials.
- These campaigns are regionally tailored, using local languages, currencies, and social media platforms, and rely heavily on ad-driven exposure via Meta Ads, and social media channels to reach consumers searching for branded fashion items online.

FRAUD STAGES:

CTM360 Fraud Navigator

CTM360 Fraud Navigator, inspired by the MITRE framework, is an analysis of the observed scams showing how the scammers navigate through different stages of the fraud. Fraud Navigator is a tool that categorizes common fraud techniques, providing insights into typical patterns of fraudulent activity. Built on the MITRE model, it identifies seven key stages in a fraud: resource development, Evasion, trigger, distribution, target interaction, motive, and monetization. There are commonly 2 phases in the fraud, represented as Phase 1 (in white) & Phase 2 (in grey).

The Fraud Navigator framework has been mapped below to show how it aligns with each stage of the newly identified fraud variants. This helps highlight how the fraud evolve across both phases.

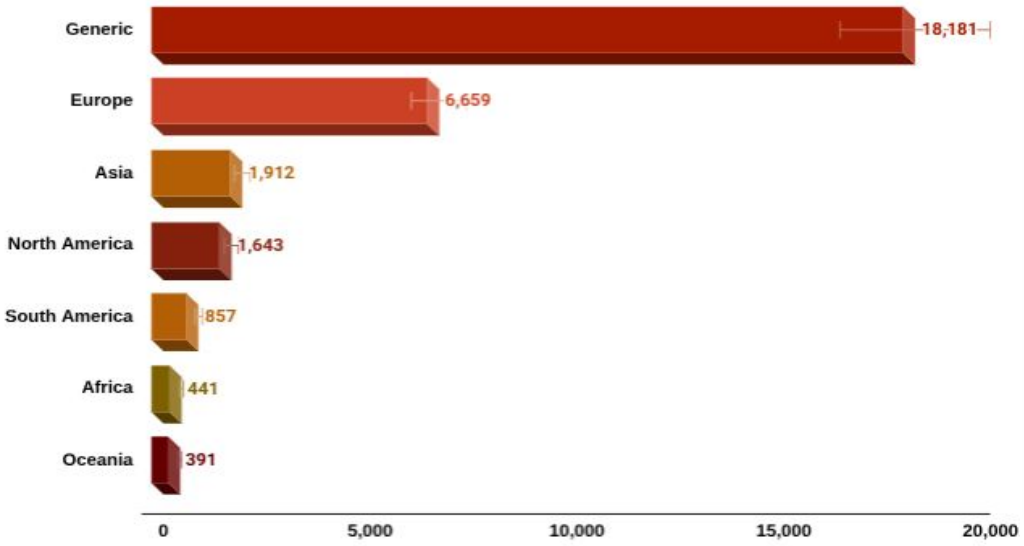


Fraud Navigator Framework - FraudWear Campaign

TARGETED REGIONS DISTRIBUTION

*Displayed below are graphs depicting the number of **FraudWear** scam incidents detected in different regions, highlighting how these campaigns vary in scale and location.*

FraudWear Scams



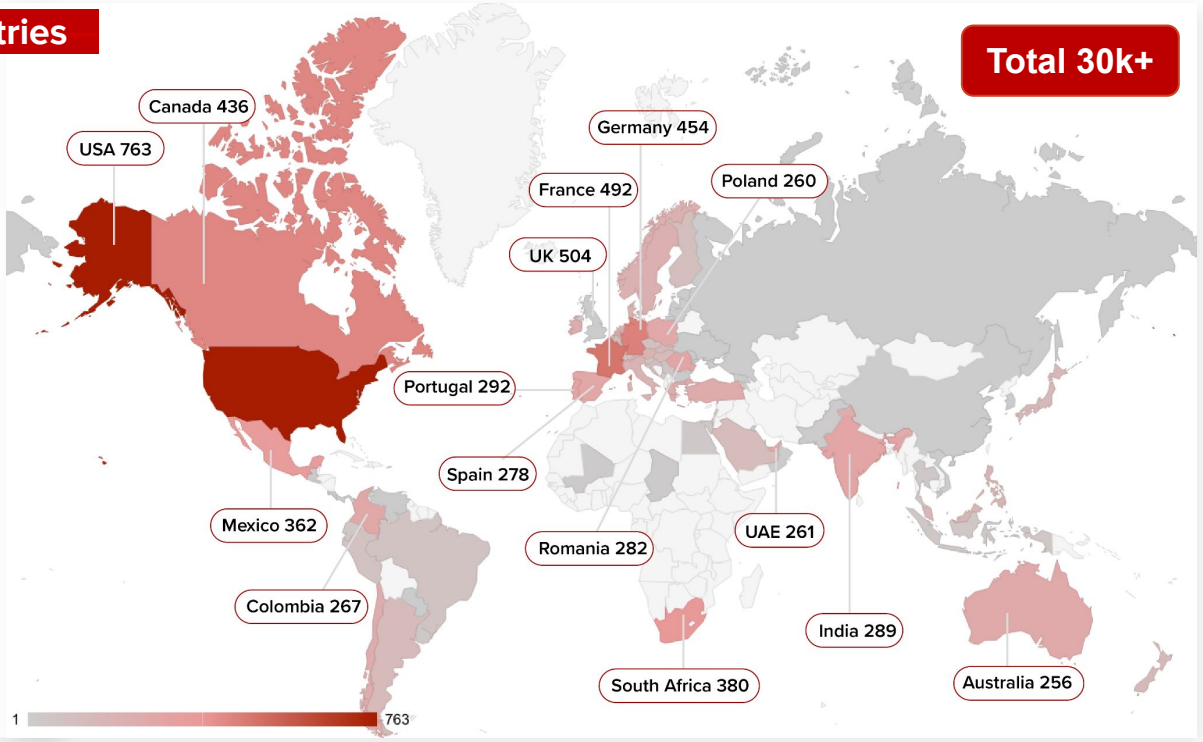
Top Targeted Regions

- Europe
- Asia
- North America

***Note:** The data presented above is approximate, based on current analysis, and is expected to increase over time.*

Targeted Countries

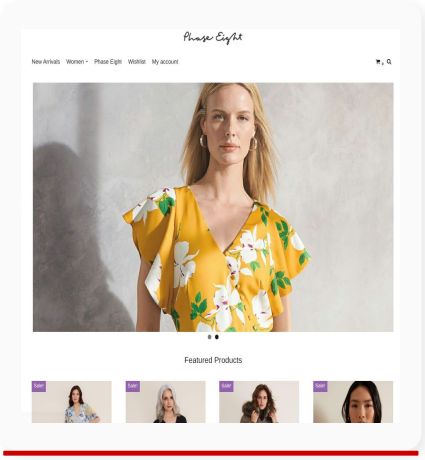
United States
United Kingdom
France
Germany
Canada
South Africa
Mexico
Portugal
India
Romania
Spain
Colombia
United Arab Emirates
Poland
Australia
66 more...

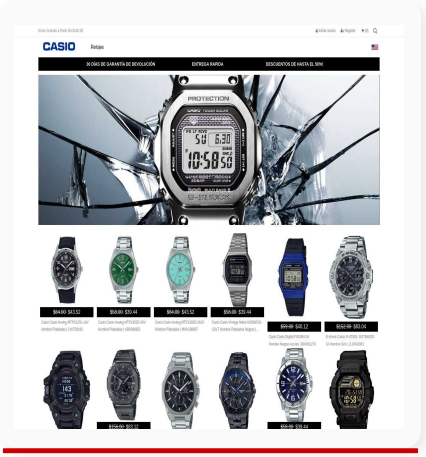


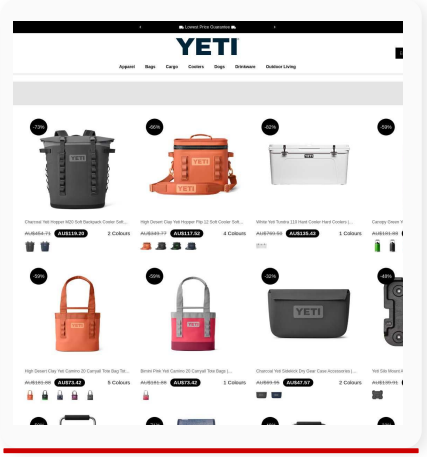
CTM360 Observations

As CTM360 identified the campaign, we observed that this global scam campaign extends beyond well-known brands such as **Adidas and Nike** to include lesser-known or regionally popular brands, such as **Phase Eight, Ganni, and Miu Miu,** and many others. It is not limited to specific age groups or genders and spans a broad range of products, including business, casual, and sportswear, as well as jewelry, and watches.

The campaign is highly localized, with fraudulent websites tailoring pricing structures, promotional themes, and overall presentation to the targeted brand and country, often referencing local holidays or events. While most activity centers on fake apparel & clothing shops, smaller-scale variants have also been observed offering outdoor equipment, electronics, and household items.







Fake Apparel and Clothing Sites

30,000+ Total URLs identified

- A large number of fraudulent Apparel & Clothing storefronts are hosted on low-cost, frequently abused top-level domains, notably **.shop, .com, and .top**. Many of these domains are deliberately crafted to resemble legitimate brands and often include country names or regional indicators in the domain (e.g., puma-espana.com, ralphlaurenmexico-mx.com) which increases perceived authenticity and helps deceive victims. This naming technique enables rapid deployment and rotation of fake stores, complicating detection and enforcement.

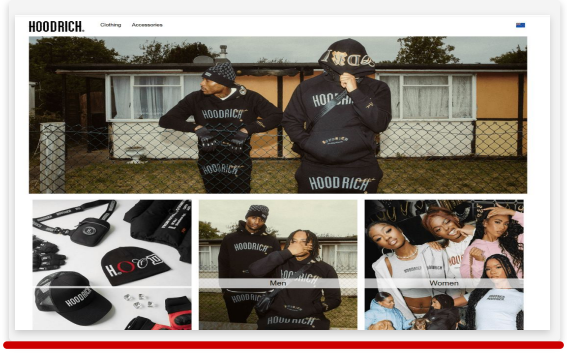
- Out of the **30k+ URLs identified, 8,000+** URLs are currently active and continue to lure individuals into these fraudulent storefronts, threat actors rapidly register and deploy new domains on a daily basis, allowing the scam ecosystem to continuously regenerate. This high turnover rate, coupled with the low cost of domain acquisition, makes the campaign highly scalable, resilient, and increasingly difficult to contain.

- On average, threat actors deploy approximately 50+ new fraudulent e-commerce websites per day, enabling the campaign to rapidly regenerate. This continuous influx of newly registered fake storefronts significantly undermines mitigation efforts, allowing the scam infrastructure to remain persistent, adaptive, and difficult to disrupt at scale

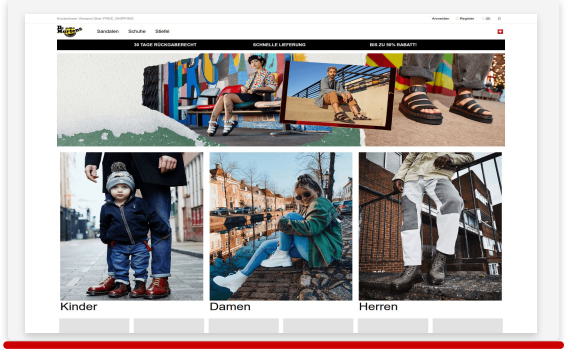
CTM360 Observations

The screenshots below showcase sample templates of **FraudWear** scams across different regions, highlighting how this campaign targets shoppers by impersonating well-known brands, using fake storefronts, ads, and social pages to lure victims with deep discounts and "exclusive" offers.

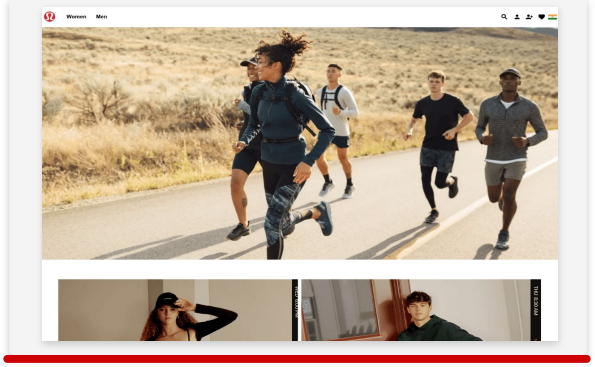
OCEANIA



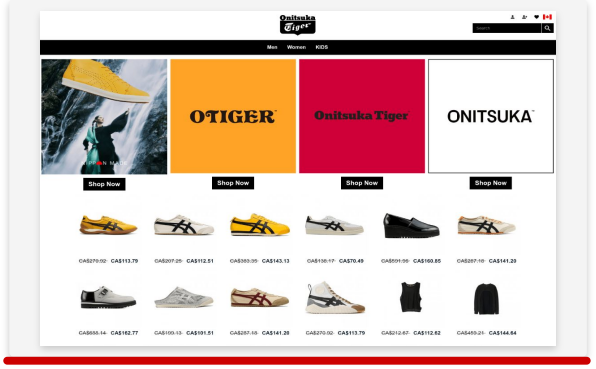
EUROPE



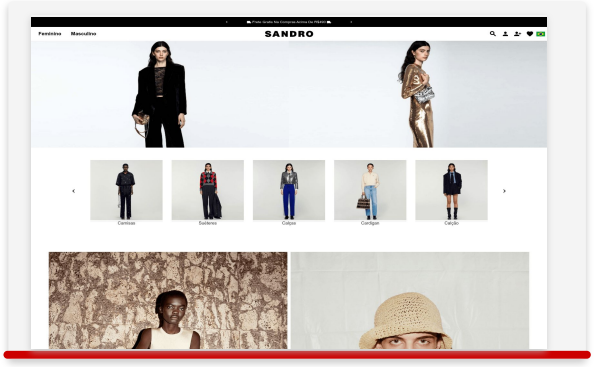
ASIA



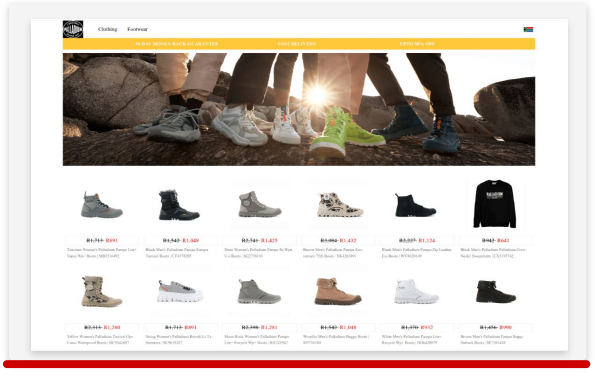
NORTH AMERICA



SOUTH AMERICA



AFRICA

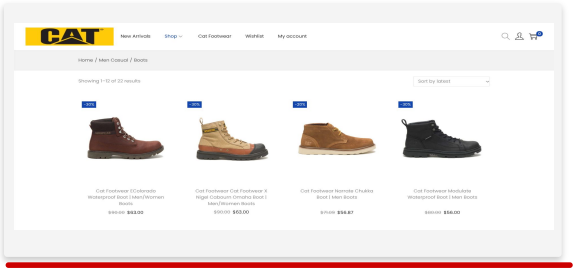


30k+ Fake Apparel and Clothing Sites

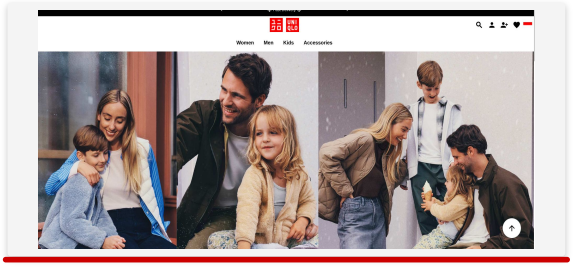
CTM360 Observations

The screenshots below showcase sample templates of **Fake Apparel & Clothing sites** globally, across different brands.

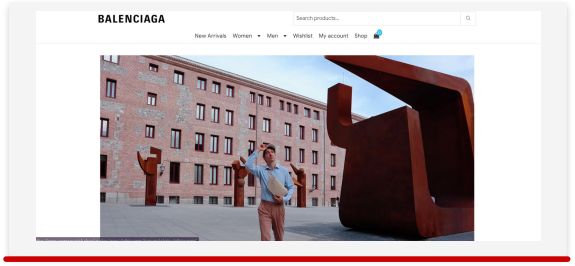
CAT FOOTWEAR



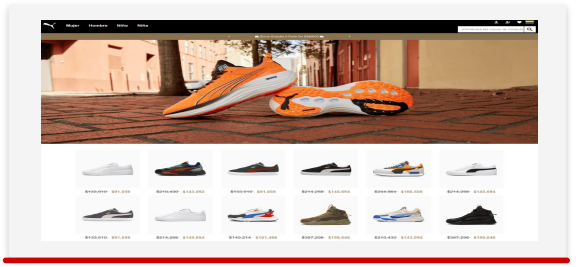
UNIQLO



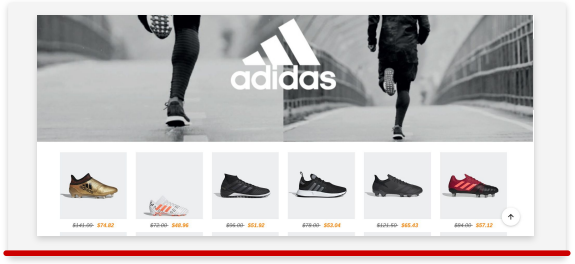
BALENCIAGA



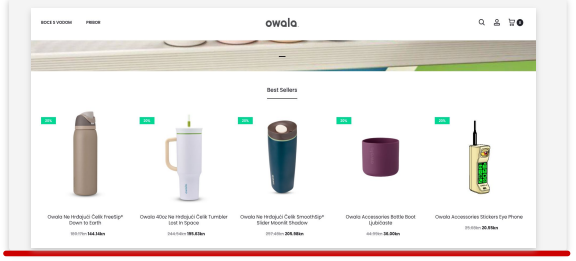
PUMA



ADIDAS



OWALA



The following screenshot represent some of the most globally recognized **Apparel & Clothing** brands targeted by **FraudWear**

350+ Apparel & Clothing Brands

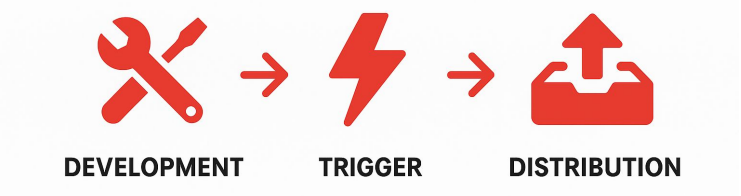
CTM360 Observations

Resource Development

Scammers deploy the scheme by creating and distributing coordinated advertising campaigns across Meta Ads, social media platforms, and other online channels.

These advertisements are designed to quickly attract user attention and drive traffic toward attacker-controlled e-commerce domains. The exploitation of social media platforms allows threat actors to rapidly scale their operations, reach diverse audiences, and rotate domains as campaigns evolve.

This deployment strategy enables sustained exposure while complicating detection and takedown efforts, supporting the continued operation of fraudulent fashion e-commerce campaigns.



Trigger and Distribution

Scammers attract victims through sponsored ads and fake social media profiles, promoting counterfeit stores that impersonate trusted brands. These promotions often promise exclusive deals on Apparel and Clothing shops, creating a sense of temptation to buy.

- **Meta Ads & Social Media Promotions:** Ads typically feature high-quality product imagery, official brand logos, and enticing discounts, all aimed at increasing credibility and driving clicks.

- **Fake E-Commerce Sites:** Clicking the ad redirects users to fraudulent online stores that replicate the structure of genuine shopping platforms. These sites feature fabricated product listings, copied storefront layouts, and misleading testimonials to encourage user interaction and simulate a functional retail environment.

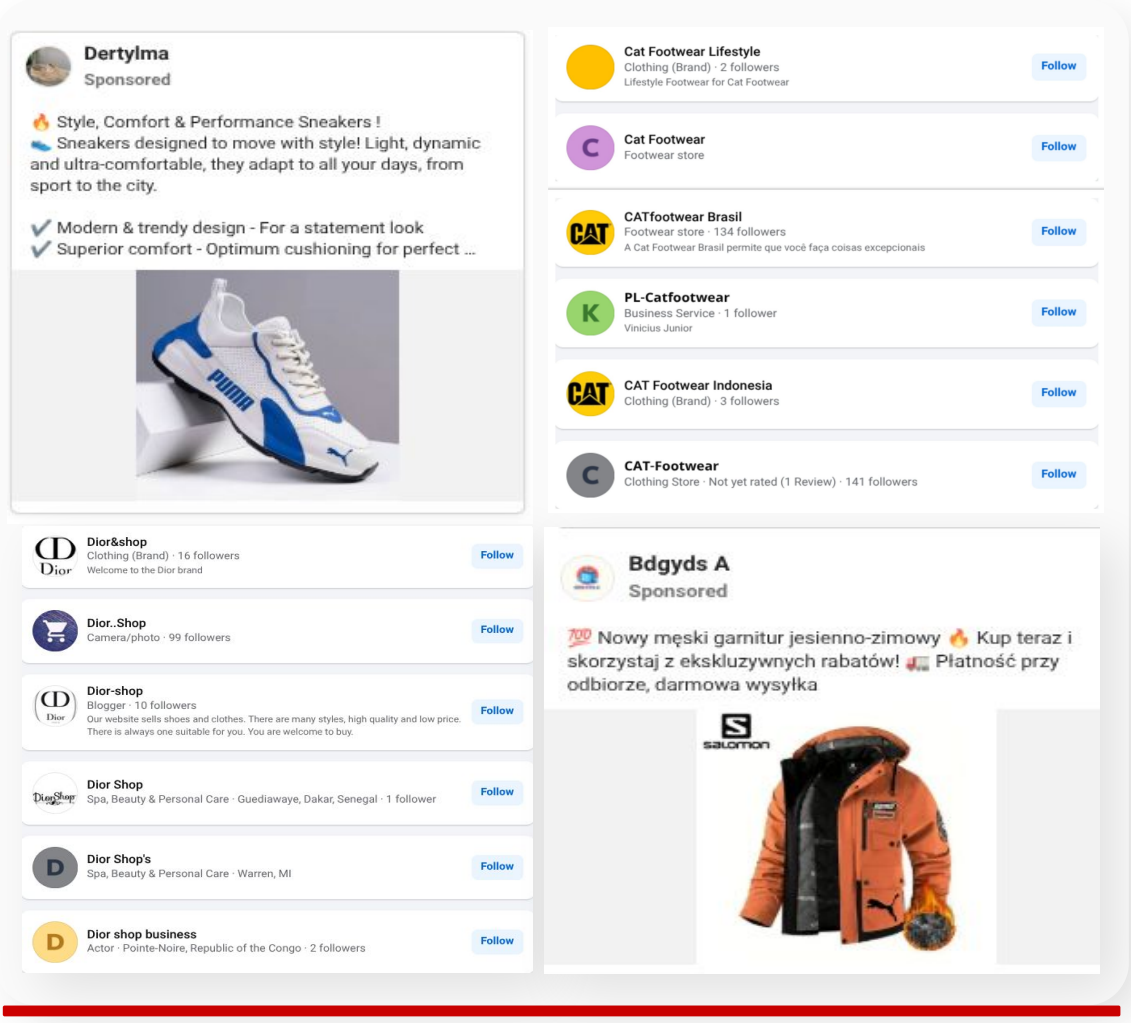
CTM360 Observations

Target Interaction

Bogus Profiles & Fake Ads

The scam mimics legitimate Apparel and Clothing shops' activity through fake ads, profiles, and storefronts, tricking users into engaging and ultimately resulting in financial loss.

- **Deceptive Ads:** Fake ads are widely circulated on Meta Ads, using brand logos, product images, and fake storefronts to attract users with heavily discounted or "exclusive" offers.
- **Bogus Brand Impersonation:** Scammers create fake profiles impersonating real brands or social media shop affiliates to build credibility and trick users into engaging with the fraudulent websites.



Samples of sponsored ads and Bogus profiles

CTM360 Observations

Motive

Financial Gain: Scammers target many known brands in as many countries as possible to maximize their profits.

They set up convincing fake shops offering unrealistic discounts, “exclusive” offers. Victims make payments believing they are purchasing legitimate products, but no items are ever delivered, resulting in direct financial loss.

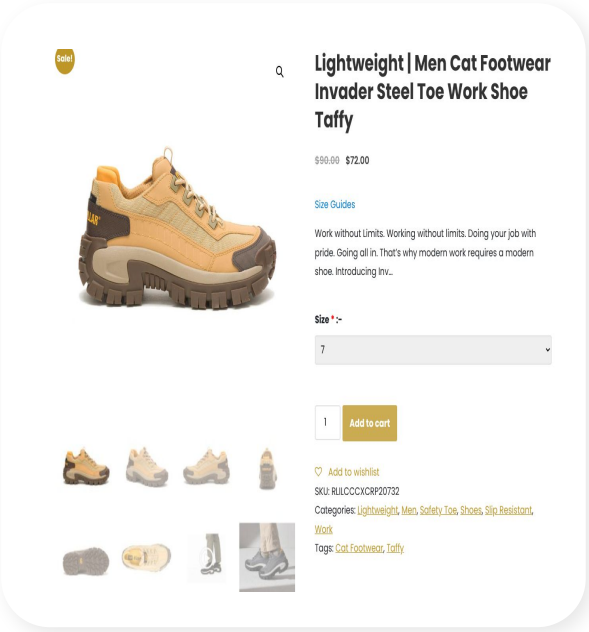
In many cases, scammers also:

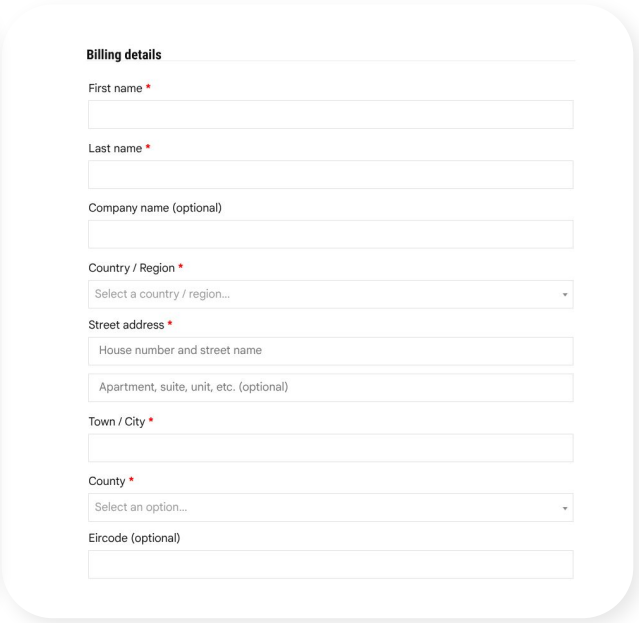
- Operate at scale across hundreds of domains
- Rebrand and relaunch new websites to replace those taken down
- Use money-mule accounts to quickly withdraw or launder funds

Harvesting Credentials & Sensitive Information: Before any payment is processed, scammers collect user information directly on their fake websites, this includes:

- Personal details (name, email, phone number)
- Account credentials
- Delivery information
- Financial or contact data entered during checkout

This stolen information might get used for dark-web resale, future phishing campaigns, social-engineering attacks, or identity theft and credit-fraud attempts.





CTM360 Observations

Monetization

Payment on Fake Shops: Payment on fake shops begins when victims are enticed by heavily discounted “brand products” displayed on fraudulent e-commerce sites. Believing the offer to be legitimate, the victim proceeds to checkout and makes a payment, but ultimately receives nothing in return, resulting in a direct financial loss.

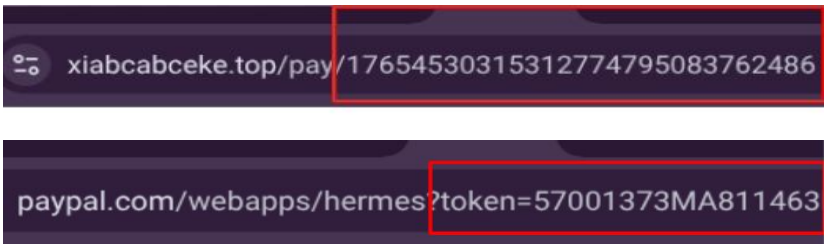
To execute this monetization flow, scammers commonly rely on inexpensive, low-cost TLD domains that can be rapidly acquired and discarded. (such as .**xyz and .cyou**) for **domain randomization.** After the victim clicks **“Place Order”**, the fake shop silently redirects them to a uniquely generated external domain containing a long randomized path ID. This path ID makes each redirect URL unique, obscures tracking and investigation, links the victim’s session to the scammer’s PayPal payment token, and helps the scam remain functional even if some redirect paths are taken down.

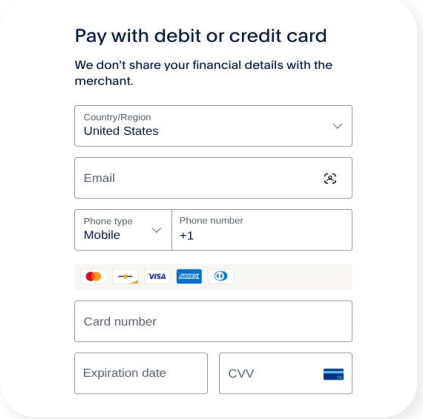
- These redirect domains are cheap, disposable, and frequently rotated.
- Each victim receives a unique redirect path.
- If one domain is taken down, others continue operating.

This redirector then forwards the victim to an authentic PayPal checkout page tied to the **scammer’s payment token**. The scam leverages the credibility of PayPal to create a false sense of security:

- The PayPal page is real, but the token belongs to a scammer, money mule, or compromised merchant account.
- PayPal URLs do not reveal the recipient, increasing victim trust.

This redirection technique is widely observed across fake e-commerce stores offering unrealistic “too good to be true” prices.





ABOUT US

CTM360 provides a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and unlimited managed takedowns), security ratings, third party risk management, email intelligence (dmarc) and cyber threat intelligence.

CONTACT US:

+973 77 360 360

info@ctm360.com

www.ctm360.com

21st Floor, East Tower Bahrain Financial Harbour, Kingdom of Bahrain