Marnetic

Security case study — marnetic.com

Sector	E-commerce / dropshipping
Platform	Shopify
Scope	Theme file audit + live remediation
Attack family	Pirated Shopify theme supply-chain risk
Entry vector	Nulled Booster Theme
Verdict	HIGH High

> **Pirated Booster Theme phone-home (dormant) + owner-email leak; Google-Ads bad-link fixed**

The problem

Marnetic's Shopify storefront was running a pirated copy of the Booster Theme whose site-wide script was coded to POST the shop's domain, owner email, and role to a look-alike of the real vendor's domain — a phone-home channel that was commented out (dormant) but live in every layout, along with the owner's email leaking on every page. Separately, Google Ads had flagged a product landing page for a bad link.

What I did

- Audited the full theme and confirmed a supply-chain risk rather than an active skimmer — no Magecart, no card-harvesting — while documenting the dormant phone-home code and the owner-email leak across all seven layouts.
- For the Google Ads flag, traced the bad link to sixteen product-description images hot-linked from a flagged dropship-supplier CDN, not to the theme.
- Fixed it safely without ever downloading from the flagged domain: found the store already had a clean duplicate of the product, set the dirty product to draft, and swapped the clean twin onto the ad's URL — verified live afterwards.
- Left the client a clear next step to request the Google Ads review and sweep for any other hot-linked supplier images.

The result

The client got a clear-eyed verdict — the theme was a trust and supply-chain risk to replace, not an active card skimmer — and, on the advertising side, a live-verified fix that put a clean product page behind the flagged ad URL so the campaign could recover, all done without touching the flagged supplier domain.