

Shahi (Shopify theme audit)

Security case study — storefront: pylomoshop.com

Sector	E-commerce (Shopify theme package)
Platform	Shopify
Scope	Theme file audit
Attack family	Shopify CDN-hosted cloaking injection
Entry vector	Admin app / Files / collaborator (recommended follow-up)
Verdict	CRITICAL Critical

Externally-hosted cloaking script injected site-wide

The problem

This Shopify theme package (191 files) carried a confirmed malicious injection: an obfuscated, cloaking JavaScript payload loaded on every storefront page — but the script wasn't hosted in this store's own files at all. It was pulled at runtime from a completely different, unrelated Shopify store's file bucket on Shopify's own trusted CDN, meaning whoever controlled that other account could change its behaviour at any time without ever touching this theme's code.

What I did

- Traced the injection from the main layout through a deliberately innocuous-looking render snippet and proved the script was hosted on a foreign store's CDN bucket by comparing Shopify file-ID paths.
- Decoded both obfuscated payloads: one fingerprints visitors for headless/automated-browser and GTmetrix signatures, the other rewrites how scripts, iframes, images and links load — including logic that specifically disables Shopify's own theme-preview scripts.
- Distinguished the real threat from noise: a second obfuscated eval block in the theme's own assets decoded to a benign DOM cleanup, which I flagged as bad practice, not malware.
- Reviewed the third-party app integrations and confirmed them legitimate, keeping the finding focused.

The result

I classified this as an active, ongoing compromise and gave a clear removal path — strip the injected script and its render calls, then audit the Shopify Admin app list, Files section, and

staff/collaborator accounts for the source — because a script hosted on someone else's account is a living backdoor, not a one-time edit. The cloaking analysis showed exactly why the store could look clean to a speed test yet misbehave for real shoppers.