Untraceable Banknotes

Security case study — untraceablebanknotes.com

Sector	WooCommerce store
Platform	WordPress + WooCommerce
Scope	File + Database
Attack family	Nulled-plugin supply-chain compromise
Entry vector	Nulled Elementor Pro 4.0.0
Verdict	HIGH High

> **Nulled Elementor Pro with injected code + template rerouting**

The problem

This WooCommerce store had no live web-shell and no injected database code — but it was running a pirated (“nulled”) copy of Elementor Pro whose licensing code had been swapped out for attacker-supplied code. That code forged a fake “Agency tier” licence and, more importantly, re-routed Elementor's template downloads to a non-official server over unencrypted HTTP — a built-in channel to fetch and run remote content whenever the operator chose. A cluster of eight automated bot customer accounts had also been created.

What I did

- Isolated the root cause to the nulled Elementor Pro upload — confirmed by every file sharing a single install timestamp — and read the injected code that writes a fake licence and hooks every outbound HTTP request.
- Documented the template-rerouting behaviour (downloads redirected to a third-party host with SSL verification disabled) as the latent backdoor channel.
- Confirmed the genuinely clean areas honestly: uploads, core files, wp-config, htaccess, cron, must-use plugins, and database content all showed no live payload.
- Identified the eight bot customer accounts and the lower-severity exposures (an exposed error log, leftover backup and fingerprinting files).

The result

I gave the client a calibrated High verdict that matched the evidence: not a running web-shell, but untrusted third-party code with a remote-fetch channel that has to be treated as a compromise of

trust. The fix was concrete — remove the nulled plugin and replace it with a genuine licensed copy, rotate credentials and keys, and clear the spam accounts — with the reasoning for the rating spelled out.