Ricardo Taylor

Security case study — ricardoctaylor.com

Sector	Author / WooCommerce book store
Platform	WordPress + WooCommerce
Scope	Database + File
Attack family	WPCode DB backdoor + casino doorway network
Entry vector	Nulled migration plugin
Verdict	CRITICAL Critical

> **WPCode backdoor + 275+ casino doorway posts → eradicated over 3 rounds**

The problem

This author's WooCommerce store had been converted into a casino-spam doorway farm: a WPCode backdoor — password-protected, with commands to create admins and phone home to an external command-and-control server — sat behind more than 275 multilingual doorway posts totalling thousands of casino spam hits, plus comment and form-submission spam and a fake plugin storing obfuscated payloads inside fake image files.

What I did

- Documented the WPCode backdoor in full — its stored password, its command set, its cloaking and self-hiding behaviour, and its C2 endpoint.
- Quantified the spam footprint (275+ doorway posts, ~5,776 casino hits) and traced the file-side fake plugin and its payload store.
- Tracked the cleanup across three database exports — catching that after round two the backdoor still survived as a dormant published record even though its active options were gone — and confirmed full removal in round three.
- Flagged the still-active nulled migration plugin as the reinfection risk and gave targeted housekeeping steps for the SEO spam residue.

The result

By round three every indicator was at zero: the backdoor post deleted, the snippet store emptied, zero casino spam in content, and no rogue admins — only the two legitimate owners. The store

was returned to a verified-clean state with a short, specific list of hardening actions to prevent the nulled-plugin door from being used again.