

Joshua David Plumbing

Security case study — joshuadavidplumbing.com.au

Sector	Plumbing services (AU)
Platform	WordPress
Scope	Database + File
Attack family	WPCode DB backdoor + DB trigger + file web-shells
Entry vector	Vulnerable template-import plugin
Verdict	CRITICAL Critical

Confirmed casino-spam/cloaking backdoor → fully cleaned & closed out

The problem

The plumbing company's site was quietly running a casino-spam and Googlebot-cloaking framework: a malicious WPCode snippet disguised as “Completely Disable Comments” that hid spam authors, injected scripts, and showed search engines a different site than real visitors saw. A hidden rogue admin, a Tiny File Manager web-shell tucked inside the theme, and staged web-shell payloads rounded out the picture — and it had been “cleaned” before, only to come back.

What I did

- Ran a full database and file forensic pass, confirming the WPCode backdoor, the cloaking configuration (a list of Google IP ranges), 100 blocks of injected casino spam, and the rogue admin.
- Found the file-side backdoors: a 185KB Tiny File Manager web-shell hidden in the theme and a cluster of staged PHP-exec payloads, and reconstructed the true patient-zero date from file timestamps.
- During verification, uncovered the reinfection mechanism — a malicious MySQL trigger that re-created the rogue admin from a booby-trapped comment — and confirmed it was gone across three successive database exports.
- Built and delivered a custom hardening must-use plugin (rogue-admin auto-block, trigger tripwire, upload/option scanning, alerts) plus a root .htaccess ruleset and install guide.

The result

The engagement closed fully clean: no rogue admin, all malware signatures at zero, file backdoors deleted, and the self-healing trigger eliminated. On top of a verified-clean site, the client walked away with a bespoke security plugin actively guarding against exactly the techniques that had been used against them, and server-side hardening (rotated credentials, least-privilege database user) done by their host.