Coralie Saramago

Security case study — coralie-saramago.com

Sector	Personal / portfolio site
Platform	WordPress
Scope	Database
Attack family	Self-healing backdoor kit (“sw_”)
Entry vector	Nulled Elementor Pro (pro-elements)
Verdict	CRITICAL Critical

> **Self-heal kit cleaned, then reinfected; escalated to server level; finally cleared**

The problem

Coralie's site was carrying a self-healing backdoor kit — a fake “security patch” plugin, a rogue admin, a malicious six-hour self-heal cron, and quarantined web-shells — all tagged with the same “sw_” marker. The site had been brute-forced against valid usernames with no two-factor protection, and a nulled copy of Elementor Pro sat underneath it all as the likely way in.

What I did

- Documented round one in full and confirmed the site content itself was clean (the hundreds of casino URLs were only bot-probe logs, not injected pages).
- On the export labelled “clean,” proved it was actually a fresh reinfection — a brand-new rogue super-admin with an active session and a new web-shell dropped into four directories — and flagged that the nulled Elementor Pro had never been replaced.
- Escalated: a reinfection after a clean means the entry point is likely server- or hosting-level, so I recommended removing the nulled plugin plus a server-level investigation and rebuild on isolated hosting.
- Verified the final export as cleared at the database layer and confirmed with the owner which alarming-looking account was legitimately his.

The result

Across three rounds the site went from actively self-healing to verified clear at the database layer, with the reinfection caught rather than missed and the root cause (a nulled plugin on shared

hosting) named plainly. The client received scan, re-scan, and clearance reports plus a hardening checklist, and a clear recommendation to stop reusing pirated plugins.