Loans in Namibia

Security case study — loansinnamibia.com

Sector	Finance / loans (NA)
Platform	WordPress
Scope	Database
Attack family	Fake-plugin dropper set + rogue admin
Entry vector	Elementor stack / file-manager (probable)
Verdict	CRITICAL Critical

> **Active compromise — rogue admin in live use + multi-backdoor plugin set**

The problem

This lending site had a rogue administrator account — named “admlnlx” to be misread as “admin” at a glance — that wasn't just sitting there: it held five live login sessions from several different foreign IP addresses, direct evidence the attacker was actively using it. Backing it up were a fake active backdoor plugin and four dormant “protect-uploads” droppers staged in randomly-named folders, a classic self-healing arrangement built to survive a partial cleanup.

What I did

- Confirmed the rogue admin from the raw user tables — its disguised name, misspelled “wordpress” email, five concurrent foreign-IP sessions, and attacker-created metadata — as the single highest-priority item.
- Identified the fake active plugin and the four dormant redundant droppers from WordPress's own plugin-update transient, matching them to a documented backdoor-dropper family.
- Verified the reassuring part honestly: post content, cron schedule, and core URLs were all clean, so the problem was bounded to the access layer where reinfection originates.
- Was explicit about scope limits — a database-only export can't prove the entry vector — and set out the ranked probable vectors plus exactly what evidence (files + logs) would confirm it.

The result

The client got an unambiguous verdict and a priority-ordered plan: kill the rogue admin and its live sessions first, remove all five backdoor plugins, rotate every credential, then supply files and logs

so the entry point could be confirmed rather than inferred. The honesty about what a DB-only scan can and cannot prove kept the remediation grounded in evidence.