Able2

Security case study — able2.com.au

Sector	Assistive-technology retailer (AU)
Platform	WordPress
Scope	File + Database
Attack family	EtherHiding blockchain-C2 kit
Entry vector	Access-layer / plugin exposure
Verdict	CRITICAL Critical

> **Compromised → cleaned → re-scan PASSED**

The problem

Able2's store was running the same blockchain-C2 spam kit family I later found at 372 Dental: a set of “sc_” options wired to an EtherHiding reinfection engine, nearly a thousand hidden casino spam revisions seeded into the database, and a rogue administrator account that had been created on the very day of the scan — a sign the attacker was still active.

What I did

- Separated real signal from noise — corrected an inflated “cialis” spam count that was actually matching the word “specialist,” and confirmed the true figure of 999 casino revisions with none published live.
- Confirmed the file tree was clear of active shells and that the damage was concentrated in the database access layer.
- Wrote a safe, transactional cleanup query set — removing the four “sc_” options, the casino revisions, and orphaned metadata — with admin removal staged separately after verification.
- Ran an independent re-scan of the cleaned database export to verify the work.

The result

The re-scan passed cleanly: the blockchain-C2 options were gone, the rogue admin was removed, and content, users, and plugins all checked out, with only harmless cosmetic log entries left behind (which actually proved the spam was gone). The client got a verified-clean site plus a hardening list to keep it that way.