

Borderless Migration

Security case study — borderlessmigration.com.au

Sector	Migration agency (AU)
Platform	WordPress
Scope	Database + File
Attack family	Code Snippets hidden-admin backdoor + spam-as-a-service plugin
Entry vector	File-manager plugin (leading candidate)
Verdict	CRITICAL Critical

Reinfection after prior clean — two malware families + spam network enrollment

The problem

This migration agency had been cleaned barely a week earlier and was already re-infected — the clearest possible sign the problem ran deeper than the WordPress layer. Inside were two independent malware families: a Code Snippets “Analytics Configuration” backdoor that generated hidden admins on the fly and exfiltrated credentials across dozens of command-and-control domains, and a “Link Factory” plugin that had signed the site up as a “donor” to a remote-controlled spam network.

What I did

- Decoded the Code Snippets backdoor: runtime-granted hidden admins seeded from the site's own secret keys, concealment across user queries, REST, sitemaps and author archives, and credential exfiltration to a rotating list of C2 domains.
- Followed up at the file level and confirmed the “Link Factory” plugin — cryptographically-signed remote routes that create rogue admins, inject casino spam, and plant hidden footer links — plus Indonesian gambling doorway pages wired in through planted sitemap and feed files.
- Explained why deleting the rogue users alone fails: they carry no stored role, so their admin rights are granted at runtime by the snippets.
- Assembled the reinfection evidence (prior-cleanup artifacts, two malware families, root-level tampering) into a clear host-level escalation case.

The result

I gave the client an unambiguous verdict: this was no longer a WordPress-cleanup problem but an account/host-level compromise, and the right move was full credential rotation and a rebuild on properly isolated hosting rather than another surface clean. Two reports (database and file-level) documented every finding and the reasoning behind the escalation.