On Top Home Improvements

Security case study — ontophomeimprovements.com.au

Sector	Home-improvement contractor (AU)
Platform	WordPress
Scope	Database
Attack family	GAnalytics (GAwp) hidden-admin C2 family
Entry vector	WPCode / Code Snippets injection
Verdict	CRITICAL Critical

> **GAnalytics/GAwp malware family — 5 backdoors + casino spam + rogue admin**

The problem

The contractor's site was carrying five separate obfuscated PHP backdoors from the GAnalytics (“GAwp”) malware family, all injected into the database through Code Snippets records. Each one created hidden administrator accounts and quietly transmitted the site's credentials to a network of attacker-controlled servers. On top of that: sixteen published casino spam posts, a confirmed rogue admin, and several typosquatted fake plugins (including one imitating LiteSpeed Cache).

What I did

- Catalogued all five GAwp instances with their injection dates and deterministic hidden-admin username prefixes, and decoded their shared behaviour — hidden admin creation, concealment from the Users list and REST API, and credential exfiltration.
- Located the rogue admin account and the sixteen injected gambling spam posts by ID range.
- Flagged the typosquat and unknown active plugins (an ‘iitespeed-cache’ look-alike, a numeric ‘social-’ plugin in two variants, and others) as backdoor/suspicious.
- Traced the encoded PHP-execution path through the WPCode option and mapped the forensic trace of an already-deleted rogue user.

The result

The client received a complete inventory of a multi-backdoor infection that most scanners would report as a single issue — five distinct C2 backdoors, the spam, the rogue admin, and the fake plugins — with a prioritised remediation roadmap aimed at stopping the ongoing credential exfiltration first, then removing the persistence and closing the entry point.