JM Painting Services

Security case study — jmpaintingservice.com

Sector	Painting contractor (US)
Platform	WordPress
Scope	File + Database
Attack family	Security-plugin-evasion backdoor
Entry vector	Exposed credentials / plugin exposure
Verdict	CRITICAL Critical

> **Wordfence-evasion backdoor → cleaned & verified clean**

The problem

JM Painting's site looked fully protected — the Wordfence dashboard even showed an active Premium licence — but that was the malware talking. A rogue plugin called “wordfence-activator” was masquerading as a Wordfence extension while doing three things at once: forging a fake Premium licence, hiding itself from the plugins screen, and poisoning Wordfence's own scan-exclusion list over 205,000 times so it would never be scanned. The site was also hosting an Indonesian gambling doorway page and a publicly-reachable backup file leaking live database credentials.

What I did

- Reverse-engineered the wordfence-activator backdoor and documented all three evasion behaviours, including the exact SQL that appended its own path to the scan-exclusion list on every page load.
- Explained precisely why Wordfence never caught it — the malware was engineered specifically to neutralise Wordfence's detection — which reframed the client's “but we had security” confusion into a clear story.
- Catalogued thirteen findings across critical-to-info severity, including the gambling doorway file, the exposed wp-config backup, a phpinfo disclosure, and exposed staging credentials.
- Re-scanned the post-remediation database and clean wp-content the owner provided to verify the cleanup.

The result

The verification scan came back clean — no malware, backdoors, or injected code in either the database or the file system after remediation. The client got the full lifecycle in one report (what was found, what was done, and proof it worked), plus a plain-English explanation of how a “protected” site had been fully compromised without a single security alert.