# Epic Flooring Solutions

Security case study — epicflooringsolutions.com

| | |
|---|---|
| **Sector** | Flooring contractor (Norfolk, VA) |
| **Platform** | WordPress (Managed) |
| **Scope** | Database |
| **Attack family** | Hidden-admin self-heal kit + fake plugins |
| **Entry vector** | Server-level (multi-wave over 4 months) |
| **Verdict** | CRITICAL Critical |

> **Self-healing backdoor kit → cleaned & verified clean**

## The problem

Epic Flooring's managed WordPress site had a self-healing backdoor kit that had been escalating over four months: a hidden administrator account concealed by a WPCode snippet, a beacon cron firing every 60 seconds to phone home, fake “EasyPost” and SEO plugins side-loaded from the uploads folder, an admin-menu hider, a second rogue admin added months later, and Wordfence quietly switched off.

## What I did

- Identified patient zero (the first hidden admin), the concealment snippet created seconds after it, the persistence cron, and the second-wave rogue admin.
- Distinguished the genuinely malicious every-60-seconds heartbeat cron from ordinary WordPress scheduler hashes — and, on verification, corrected my own first-pass report where two legitimate Action Scheduler hashes had been over-flagged.
- Verified the cleaned export and a 12,587-file wp-content snapshot: rogue admins fully removed, snippet store emptied, fake plugins gone from disk and config, Wordfence reactivated, no web-shells or PHP in uploads.
- Flagged the four-month multi-wave pattern as a server-level entry-vector signal, not a one-off.

## The result

The site came back verified clean — both rogue admins and their metadata gone, the fake plugins removed, casino spam pages cleared and their URLs now returning 404s. Just as important, I held

myself to the same evidence standard I hold the malware to, publicly correcting a false-positive in my first report so the client's remediation stayed focused on what was actually malicious.