372 Dental

Security case study — 372dental.co.uk

Sector	Dental practice (UK)
Platform	WordPress
Scope	File + Database
Attack family	EtherHiding blockchain-C2 kit
Entry vector	Nulled Elementor Pro (pro-elements)
Verdict	CRITICAL Critical

> **Actively compromised — blockchain-hosted self-healing kit**

The problem

The practice's website had been taken over by one of the most advanced persistence kits I've dealt with: an “EtherHiding” operation that stored its payload on the Ethereum blockchain (reached through 0xrpc.io) so it could re-download itself even after a normal cleanup. Real visitors were being bounced to a malicious redirect (myoglocker.com), the homepage carried hidden German “Slotimo” casino spam, and three unauthorised administrator accounts had been added on consecutive days.

What I did

- Reconstructed the entire self-healing chain — a hidden .user.ini auto_prepend directive that forced a dropper to run on every page load, which in turn rebuilt a malicious must-use plugin from a zip hidden in the uploads folder.
- Decoded the blockchain command-and-control layer: 16 “sc_” options, the live RPC endpoint, and a ~260KB encoded payload that re-plants itself across three separate files.
- Identified all three rogue admins and their exact creation order, pinpointing the first foothold, and separated them from the one legitimate agency account.
- Traced the most likely entry point to a nulled (pirated) copy of Elementor Pro and catalogued the attacker's post-access tooling.

The result

I handed over a complete, evidence-backed picture of the compromise and its reinfection engine, with the decisive operational insight that the files and database had to be cleaned in the same pass

— clean either half alone and the other re-plants it within the hour — followed by a full credential-rotation and hardening plan to break the cycle for good.