interweb

Gerado a 15/11/2026 00:29

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

A análise diz que está limpo mas o site continua a redirecionar: onde se esconde a infeção

Sites atacados e malware

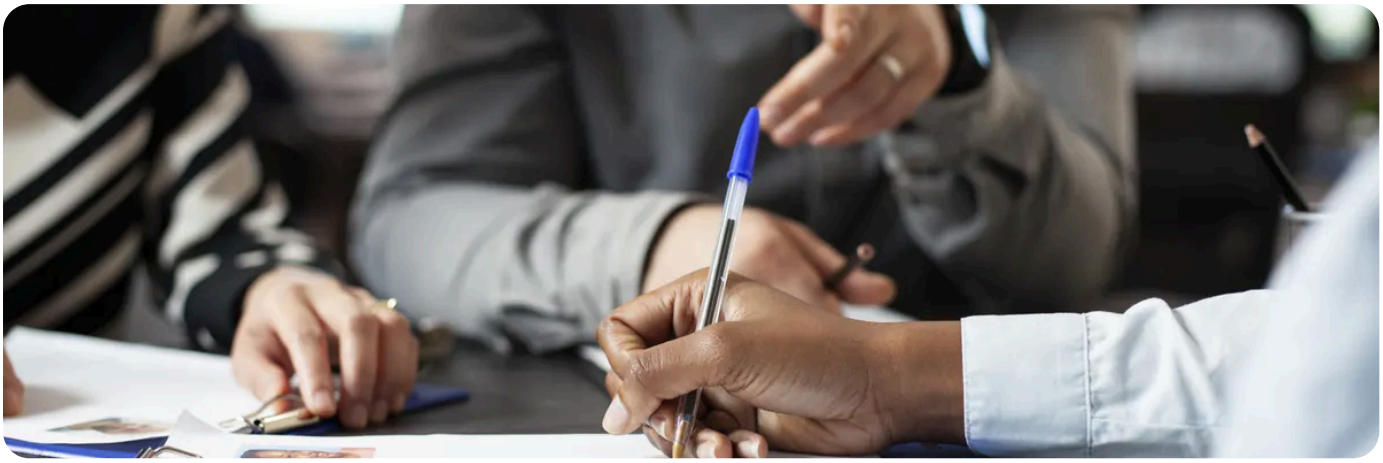
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-1498	v2026.10.10	Angola · Português

Interweb Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/1498

A análise diz que está limpo mas o site continua a redirecionar: onde se esconde a infeção

Sites atacados e malware Criado em **10 de outubro de 2026** 3 min de leitura



A resposta curta: uma análise só vê o que sabe reconhecer. Uma infeção moderna esconde-se **fora dos ficheiros que se olham primeiro** (na base de dados, num `.htaccess`, numa tarefa agendada, num site esquecido da mesma conta) e muitas vezes **só aparece a certos visitantes**: quem vem do Google, quem usa telemóvel, quem não tem sessão iniciada. Por isso o dono, que entra sempre da mesma maneira, nunca vê nada.

Os sítios onde costuma estar

Onde	O que procurar
`.htaccess`	Regras de redirecionamento que não escreveu, sobretudo as que dependem de «de onde vem o visitante» ou do tipo de aparelho. Verifique o da raiz e os das subpastas.
Base de dados	Em WordPress, scripts inseridos nos artigos e nas opções (a tabela `wp_options`), e utilizadores administradores que não criou.
Ficheiros «normais»	Linhas estranhas no início ou no fim de `index.php`, `wp-config.php` ou `footer.php` do tema, com texto ilegível e funções como `eval` ou `base64_decode`.
Pasta `uploads`	Ficheiros `.php` numa pasta onde só devia haver imagens e documentos.
Tarefas agendadas	Em «Cron Jobs» no cPanel, uma tarefa que não criou e que volta a descarregar o código depois de o apagar.
Outros sites da conta	Um WordPress antigo numa subpasta ou num domínio adicional, esquecido e desatualizado, pode reinfetar tudo o resto.

Como procurar, passo a passo

1. **Veja o site como o veria um estranho.** Em janela privada, saia do WordPress, abra o Google, pesquise o nome do seu site e entre pelo resultado, de preferência no telemóvel. Muitas infeções só atuam aí.

2. **Reveja o que o «Imunify Security» do cPanel detetou** e as datas: um ficheiro assinalado tem quase sempre outros por perto. Para o ponto de partida, veja **como saber se o site foi comprometido**.

3. **Ordene os ficheiros por data de modificação** no Gestor de Ficheiros e procure o que mudou sem o ter tocado. É o método mais simples e dos mais eficazes.

4. **Compare com uma instalação limpa.** Descarregue a mesma versão do WordPress, do tema e dos *plugins* de origem oficial e compare com o que está no site: o que existe a mais, ou é diferente, é suspeito.

5. **Substitua em vez de remendar.** Reponha o núcleo do WordPress e os *plugins* com cópias limpas, em vez de procurar linha a linha. Siga a ordem de **limpar um site comprometido**, e mude todas as senhas só *depois* de tapar a entrada.

Se limpar e o problema voltar em horas ou dias, há uma porta de trás.
É um ficheiro escondido que volta a instalar o resto, ou uma conta de administrador criada para esse fim. A limpeza só está feita quando a porta for encontrada e fechada, não quando o aviso desaparece.

Antes de começar, descarregue o estado atual, infetado: é a prova de como entraram. Se acha mais seguro recomeçar, veja a cópia limpa mais recente em **depois de um ataque, que cópia restaurar**.

PRECISA DE AJUDA?

Já limpou e a infeção voltou? Diga-nos o domínio e o que viu: lemos o registo para encontrar a entrada.

Abrir pedido de suporte →

VEJA TAMBÉM

- Como saber se o site foi comprometido →
- Como limpar um site comprometido →

- Retirar o aviso vermelho do Google do seu site
- Depois de um ataque, que cópia restaurar

interweb

Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@interweb.ao · +244 942 011 191 · www.interweb.ao
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-AO-KB-1498 · v2026.10.10 · Gerado a 15/11/2026 00:29

Versão online deste documento