interweb

Gerado a 16/10/2026 10:32

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Analisar o site à procura de malware no cPanel: o que o Imunify encontra e o que fazer com o resultado

Segurança

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-1696	v2026.10.15	Angola · Português

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

https://www.meu.interweb.ao/knowledgebase/1696

A resposta curta: o cPanel tem uma ferramenta chamada **Imunify360**, no grupo **Segurança**, que analisa os ficheiros da sua conta à procura de código malicioso (malware). Pode mandar analisar quando quiser e ver a lista do que ela marcou. Serve para **descobrir** um problema; o que fazer a seguir é o que decide se o site fica limpo de vez.

Como a usar

1. **No cPanel,** procure o ícone **Imunify360** na secção **Segurança** e abra-o.

2. **Procure a área de análise de malware** (Malware Scanner). Verá a lista de ficheiros que a ferramenta marcou e o estado de cada um, ou a indicação de que não encontrou nada.

3. **Peça uma análise** quando suspeitar de algo, em vez de esperar pela seguinte. O tempo depende de quantos ficheiros a conta tem.

4. **Para cada ficheiro marcado,** veja o caminho, o nome do tipo de ameaça e a data. Apontar isto é o mais útil que pode juntar a um pedido de suporte.

O que cada botão faz, nomeadamente se a ferramenta limpa os ficheiros por si, **depende da versão e da licença instaladas no servidor**. Se um botão de limpeza estiver desativado ou não existir na sua conta, abra um pedido: tratamos nós ou dizemos-lhe o que fazer à mão.

O que fazer com o resultado

O que vê	O que fazer
Nada encontrado, mas o site tem comportamentos estranhos (redireciona, mostra anúncios)	Uma análise automática não apanha tudo. Veja **A análise diz limpo mas o site ainda redireciona**.
Ficheiros de plugins, temas ou do núcleo do WordPress marcados	Muitas vezes a solução é voltar a instalar a versão limpa a partir da fonte oficial, e não limpar à mão.
Um ficheiro marcado numa pasta de imagens ou de envios (`uploads`)	Ficheiros `.php` numa pasta de imagens são quase sempre suspeitos.
Vários ficheiros em várias pastas	Provavelmente há uma porta aberta (palavra-passe roubada, plugin desatualizado). Limpar sem a fechar é inútil.

Depois da limpeza

1. **Mude as palavras-passe:** cPanel, FTP, base de dados, administrador do WordPress. Veja **Alterar a palavra-passe do administrador do WordPress**.

2. **Atualize** o WordPress, os plugins e os temas, e apague os que não usa. Veja **Plugin abandonado ou PHP antigo**.

3. **Ligue a verificação em dois passos** onde puder: **Ativar a autenticação de dois fatores**.

4	**Se tiver de repor uma cópia,** escolha uma anterior à infeção: **Depois de um ataque, que cópia restaurar**.

Não apague às cegas. Antes de remover ficheiros que a ferramenta marcou, faça uma cópia da conta: um falso alarme num ficheiro do seu programa pode partir o site. E uma ferramenta de análise não substitui a prevenção: atualizações, palavras-passe fortes e cópias de segurança.

A análise marcou ficheiros e não sabe o que fazer? Abra um pedido com o domínio e a lista dos caminhos que viu.

Abrir pedido de suporte

VEJA TAMBÉM

A análise diz limpo mas o site ainda redireciona: onde se esconde uma infeção

Depois de um ataque, que cópia restaurar? Escolher uma cópia limpa

Alterar a palavra-passe do administrador do WordPress

ModSecurity e firewalls de aplicações web: o que fazem e o que fazer quando uma o bloqueia

interweb

Versão online deste documento

A Interweb é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020
FUNDADA

37 mil+
CLIENTES

130+
INSCRIÇÕES POR DIA

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-1696 · v2026.10.15 · Gerado a 16/10/2026 10:32