Gerado a 21/10/2026 17:54

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Páginas de phishing no site ou servidor: removê-las, ver por onde entraram e evitar um bloqueio

Segurança

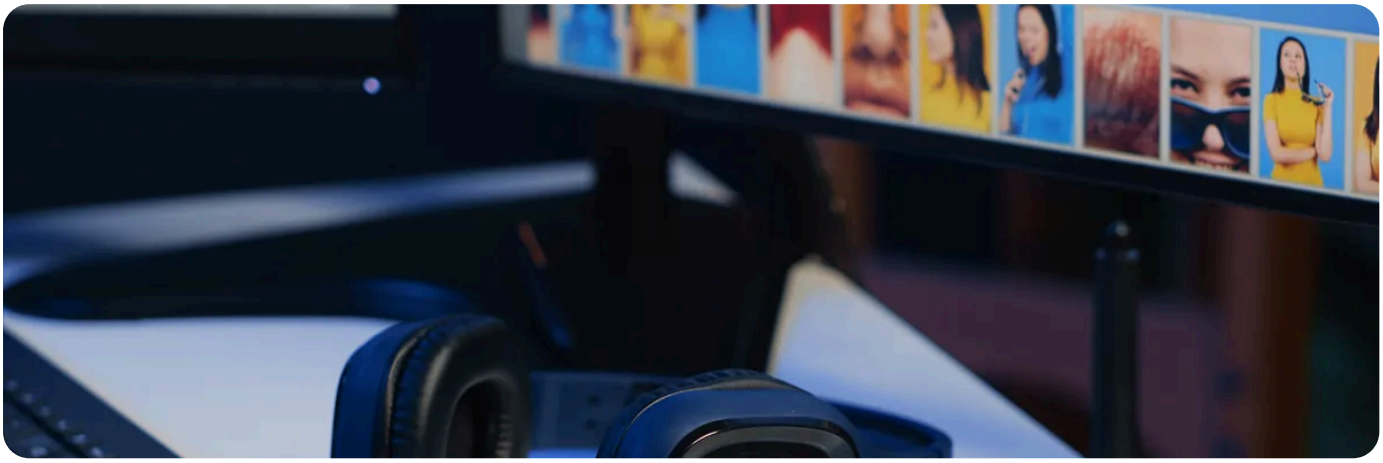
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-MZ-KB-2261	v2026.10.21	Moçambique · Português

MozOut Moçambique
RLX Holdings, S.A. · Grupo RLX Holdings
NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

https://www.meu.mozout.co.mz/knowledgebase/2261

Páginas de phishing no site ou servidor: removê-las, ver por onde entraram e evitar um bloqueio

Segurança · Criado em **21 de outubro de 2026** · 5 min de leitura



A resposta curta: uma página de phishing imita um banco, uma empresa de entregas ou um serviço conhecido para roubar palavras-passe e dados de cartão. Quando aparece no seu site, quase nunca foi o dono que a pôs: alguém entrou por um plugin desactualizado, uma palavra-passe roubada ou um formulário de envio de ficheiros, e deixou lá uma pasta. O aviso chega-nos do nosso fornecedor de rede, de uma equipa nacional de resposta a incidentes (CERT) ou da própria empresa imitada, com **um prazo curto, muitas vezes de um dia**, e nós reencaminhamo-lo por pedido de suporte no Meu MozOut. O trabalho tem três partes: **tirar a página do ar**, **descobrir por onde entraram** e fechar essa porta, e enviar-nos um **relatório curto**. O processo inteiro está em **um aviso de abuso sobre o seu servidor**.

O que procurar, e onde costuma estar

O que procurar	Onde costuma estar
A página do aviso	O endereço (URL) que vem no aviso diz a pasta. Um endereço que acaba em `/wp-content/uploads/xyz/login.php` está em `public_html/wp-content/uploads/xyz/`.
O kit em zip	Ficheiros .zip com nomes de bancos ou de transportadoras, deixados ao lado da página. É o «pacote» que o atacante descomprimiu.
Pastas escondidas	Pastas começadas por ponto, ou dentro de `.well-known`, onde ninguém costuma olhar.
Scripts de envio e de recolha	Ficheiros PHP pequenos que enviam e-mail ou guardam o que as vítimas escrevem, às vezes num ficheiro .txt ao lado.
Portas das traseiras (web shells)	Ficheiros PHP com nomes aleatórios em pastas de imagens ou de cache, muitas vezes com `eval` ou `base64_decode`.
Acessos que não criou	Administradores novos no WordPress, contas FTP, utilizadores ou chaves SSH num VPS.

Como resolver, por ordem

1. **Tire a página do ar, sem destruir a prova.** No cPanel, no Gestor de Ficheiros, comprima a pasta para um zip **fora** de `public_html` (ou descarregue-o) e só depois apague a pasta. Num VPS, com o caminho certo do seu site: `mkdir -p /root/analise` `tar czf /root/analise/phishing.tar.gz /var/www/CAMINHO/DA/PASTA` `rm -rf /var/www/CAMINHO/DA/PASTA` Confirme o caminho duas vezes antes do `rm -rf`: apaga sem perguntar.

2. **Procure as outras cópias.** Quem entra deixa quase sempre mais do que uma. Num plano de hospedagem, corra a análise do Imunify: **analisar o site à procura de malware no cPanel**. Num VPS, liste os PHP alterados nos últimos dias e os que usam funções típicas de código escondido: `find /var/www -type f -name "*.php" -mtime -14 -ls` `grep -rlE "eval\(|base64_decode\(" /var/www --include=*.php` Reveja a lista um a um: há plugins legítimos que usam estas funções.

3. **Descubra por onde entraram.** No registo de acessos, procure o primeiro pedido à pasta da página e, depois, o que o mesmo IP fez antes. No cPanel, o registo está em **Métricas > Acesso em bruto**. Num VPS: `grep "NOME_DA_PASTA" /var/log/nginx/access.log /var/log/apache2/access.log` `grep "IP_DO_ATACANTE" /var/log/nginx/access.log | head -50` Um envio (POST) para um plugin ou para o `wp-login.php` pouco antes de a pasta aparecer costuma ser a porta de entrada.

4. **Feche a porta.** Actualize o CMS, os temas e os plugins, retire os abandonados (**um plugin abandonado ou um PHP antigo**), mude todas as palavras-passe (cPanel, FTP, base de dados, administradores do site) e apague os acessos que não reconhece. Num VPS, faça também a verificação de **o meu VPS foi invadido?**.

5. **Veja se saiu e-mail de phishing do servidor.** Num plano de hospedagem, use o **Track Delivery**. Num VPS, veja a fila de correio com `mailq`. Se saiu, o IP pode acabar numa lista negra: **o IP do servidor numa lista negra de spam**.

6. **Responda no pedido de suporte** com o relatório: a causa e como entraram, o que encontrou e removeu, e o que fez para não se repetir. Há um modelo em **responder a um aviso de abuso**.

7. **Se o navegador ou o Google mostram o site como «enganador»,** depois de limpo peça a revisão no Google Search Console, no relatório de problemas de segurança.

Apagar a pasta e responder «removido» não chega.

Se a porta por onde entraram continua aberta, a página volta, e com ela um aviso novo. Se o prazo passa sem solução, o serviço de hospedagem pode ser suspenso (**serviço suspenso por outro motivo**) ou o servidor desligado, e o nosso fornecedor de rede pode bloquear o IP: **porque o servidor foi desligado ou bloqueado**. Num servidor muito mexido, o mais seguro é reinstalar e repor uma cópia limpa: **que cópia restaurar depois de um ataque**.

Guarde o zip da pasta até o caso fechar,

fora da pasta pública. Mostra o que lá estava e as datas dos ficheiros, e ajuda a escrever o relatório. Não abra a página falsa num navegador com as suas sessões abertas.

PRECISA DE AJUDA?

Recebeu um aviso de phishing e precisa de ajuda para o ler? Responda no mesmo pedido de suporte com o que já encontrou.

Abrir pedido de suporte →

VEJA TAMBÉM

- Um aviso de abuso sobre o seu servidor: o que significa, o prazo e o que precisamos de si →
- Responder a um aviso de abuso: a causa, o que removeu e como não se vai repetir →
- Analisar o site à procura de malware no cPanel: o que o Imunify encontra e o que fazer com o resultado →
- Como resolver um site infectado por malware →
- Depois de um ataque, que cópia restaurar? Como escolher uma cópia limpa →
- Como reconhecer um e-mail ou mensagem de phishing, e o que fazer se clicou →

MozOut Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT	401 191 607
NUEL	105 045 974
CAE	62022
SEDE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Moçambique
CONTACTOS	info@mozout.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.mozout.co.mz
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-MZ-KB-2261 · v2026.10.21 · Gerado a 21/10/2026 17:54