Gerado a 21/10/2026 17:22

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

O IP do servidor numa lista negra de spam: descobrir a origem e sair do Spamhaus ou do SpamCop

Segurança

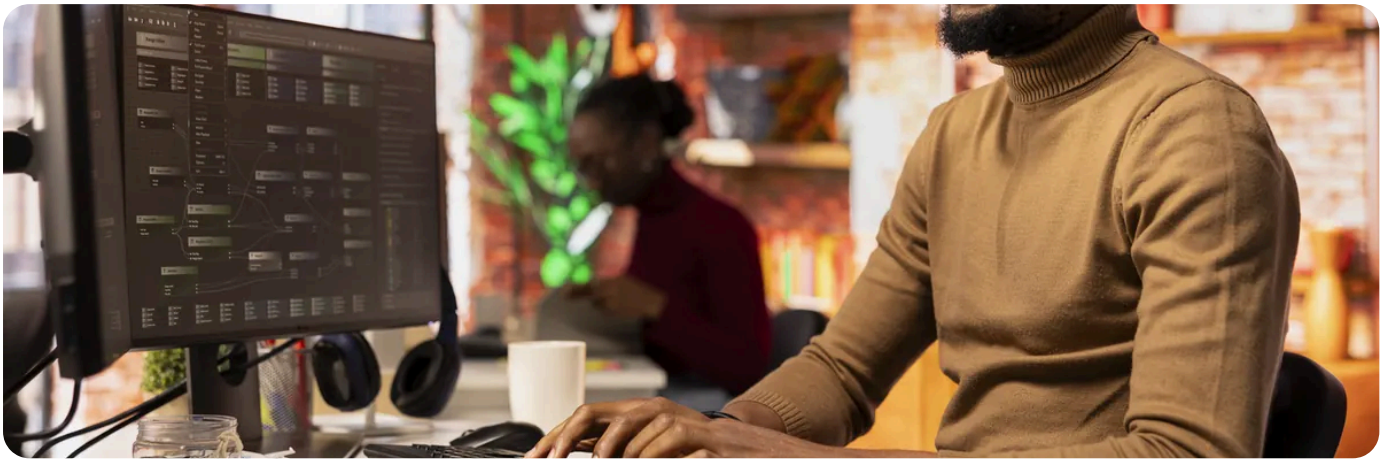
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-6876	v2026.10.21	Angola · Português

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

https://www.my.mozout.com/knowledgebase/6876

O IP do servidor numa lista negra de spam: descobrir a origem e sair do Spamhaus ou do SpamCop

Segurança · Criado em **21 de outubro de 2026** · 4 min de leitura



Este artigo é para quem tem um VPS ou um servidor dedicado, com acesso root. Se tem um plano de hospedagem, comece por **o seu domínio ou IP está numa lista negra**. **A resposta curta:** o IP do seu servidor entrou numa lista negra porque, algures, alguém viu sair spam dele, ou tráfego de uma máquina infectada. O Spamhaus e o SpamCop são das listas mais consultadas: com o IP lá dentro, muitos servidores de correio recusam o que envia. Às vezes o aviso chega também do nosso fornecedor de rede, com um prazo curto, muitas vezes de um dia. A ordem é sempre a mesma: **encontrar a origem, pará-la, e só depois pedir a remoção**.

As listas mais comuns, e o que querem dizer

Lista	O que costuma querer dizer	Como se sai
Spamhaus SBL	O IP foi visto a enviar spam ou ligado a uma operação de spam ou de phishing.	Corrigir a causa e pedir a remoção no centro de remoção do Spamhaus, explicando o que fez.
Spamhaus XBL	Uma máquina infectada, ou um programa a enviar correio directamente, sem passar pelo servidor de correio.	Limpar o servidor e pedir a remoção no mesmo centro. A página da consulta diz o passo para o seu caso.
Spamhaus PBL	Não é um castigo: é uma lista de IPs que não deviam enviar correio directo.	Se tem um servidor de correio a sério, com DNS reverso, a página do Spamhaus explica como pedir a exclusão.
SpamCop	Pessoas que receberam spam do seu IP e o denunciaram.	Sai sozinho quando as denúncias param. A página de consulta do SpamCop diz o que se aplica ao seu IP.
Outras listas	Há muitas, mais pequenas. Algumas cobram por uma «remoção rápida».	Não pague: nas listas sérias a remoção é gratuita.

Encontrar a origem e sair da lista

1. **Confirme a lista e o motivo.** Consulte o IP na página do Spamhaus (check.spamhaus.org) e na do SpamCop. Anote a lista, a data e o motivo: é a pista para o resto.

2. **Veja a fila de correio.** Uma fila enorme, com destinatários que não conhece, é spam a sair pelo servidor de correio: `mailq | tail -n 1`
`postqueue -p | head -50 # Postfix`
`exim -bpc # Exim (servidores com cPanel/WHM)`

3. **Descubra quem envia.** Uma conta de e-mail com a palavra-passe roubada aparece no registo com o nome de utilizador; um script de um site aparece com a pasta de onde corre: `grep "sasl_username" /var/log/mail.log | tail -50 # Postfix (Debian/Ubuntu)`
`grep "sasl_username" /var/log/maillog | tail -50 # AlmaLinux/Rocky`
`grep "cwd=" /var/log/exim_mainlog | sort | uniq -c | sort -rn | head` Se for uma conta pirateada, veja **a sua conta de e-mail foi pirateada**.

4. **Procure ligações directas à porta 25.** Se aparece um processo que não é o seu servidor de correio (Postfix, Exim), é malware a enviar spam por conta própria: `ss -tnp state established '( dport = :25 )'` Nesse caso, siga **actividade de botnet no seu servidor**.

5. **Pare a origem.** Mude a palavra-passe da conta, desligue o formulário ou o script abusado, retire o malware. Depois limpe da fila só o spam, mensagem a mensagem, com `postsuper -d ID_DA_MENSAGEM`. O `postsuper -d ALL` apaga também o correio legítimo que está à espera.

6. **Evite a recaída.** Se o servidor não precisa de enviar correio directamente, feche a saída pela porta 25 e envie o que precisar por um **smarthost**: `ufw deny out 25/tcp` Se tem mesmo um servidor de correio, confirme o **DNS reverso (PTR)** e o **SPF, DKIM e DMARC**.

7. **Peça a remoção e responda-nos.** No Spamhaus, use o centro de remoção e explique em poucas linhas o que encontrou e o que corrigiu. No pedido de suporte, envie o relatório: **responder a um aviso de abuso**.

! **Pedir a remoção antes de parar a origem é tempo perdido.**
O spam continua, o IP volta à lista, e as listas tratam pior quem reincide. Se o envio continua depois de um aviso, o servidor pode ser desligado para proteger a rede: **porque o servidor foi desligado ou bloqueado**.

Se o IP já estava na lista antes de começar a usar o servidor,
abra um pedido de suporte com o resultado da consulta: um servidor novo, sem correio a sair, explica-se assim no pedido de remoção.

PRECISA DE AJUDA?

O seu IP está numa lista e não encontra a origem? Envie-nos o nome da lista, o que a consulta mostra e a saída dos comandos acima.

Abrir pedido de suporte →

VEJA TAMBÉM

- O seu domínio ou IP está numa lista negra: como verificar e como sair
- 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
- Retransmissão SMTP por um smarthost: enviar correio de um VPS ou de uma aplicação
- PTR e DNS reverso: porque o seu e-mail depende disso
- O meu VPS foi invadido? Verificar processos, cron, utilizadores, chaves SSH e pastas temporárias

MozOut 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@mozout.com · +244 942 011 191 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-AO-KB-6876 · v2026.10.21 · Gerado a 21/10/2026 17:22