

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Um aviso de abuso sobre o seu servidor: o que significa, o prazo e o que precisamos de si

Segurança

CÓDIGO

RLX-MZ-KB-2242

VERSÃO

v2026.10.21

PAÍS · IDIOMA

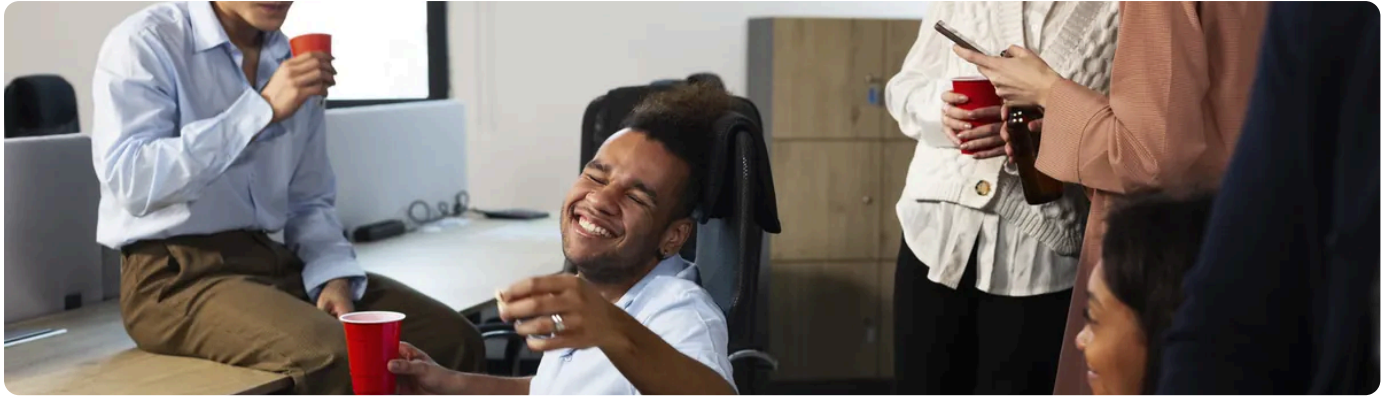
Moçambique · Português

Interweb Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

<https://www.meu.interweb.co.mz/knowledgebase/2242>



A resposta curta: o nosso fornecedor de rede vigia o tráfego. Quando vê um ataque a partir de um servidor nosso, recebe uma queixa de terceiros ou um relatório de uma equipa nacional de resposta a incidentes (CERT), envia-nos um **aviso de abuso** com um identificador, o registo do que viu e **um prazo curto, muitas vezes de um dia**, para resolver e responder. Nós reencaminhamos-lho por **pedido de suporte** no Meu Interweb e pedimos-lhe **um relatório curto**: a causa, o que removeu e o que fez para não se repetir. Este artigo é para quem tem um **VPS ou servidor dedicado**; os avisos sobre sites (phishing, fraude) também valem para quem tem hospedagem.

Que aviso recebeu, e onde ler

O aviso fala de	O que quer dizer	Onde ler
Netscan (varrimento de rede)	O seu servidor abriu muitas ligações a uma gama de endereços, nas mesmas portas, em poucos minutos.	O seu VPS está a varrer outras redes
DDoS a partir do servidor	Sai do seu servidor uma enxurrada de tráfego contra um alvo.	Um ataque DDoS a partir do seu servidor
Redis aberto	O Redis responde a qualquer pessoa na internet e pode ser usado em ataques.	Redis aberto à internet
Resolver DNS aberto	O servidor responde a perguntas de DNS de qualquer pessoa e serve para amplificar ataques.	Um resolver DNS aberto
CLDAP, Portmapper (rpcbind) ou outro serviço UDP	Um serviço UDP aberto que serve para ataques de reflexão.	Serviços UDP abertos à internet
MySQL, MariaDB ou PostgreSQL acessível de fora	A base de dados aceita ligações de qualquer endereço.	Bases de dados acessíveis da internet
n8n vulnerável ou aplicação web com falhas críticas	Uma versão com falhas conhecidas está exposta.	Um n8n ou uma aplicação web vulnerável
Phishing	Páginas a imitar bancos ou empresas de entregas no seu site, ou e-mails de phishing a sair do servidor.	Páginas de phishing no seu site ou servidor
Lista negra de spam (Spamhaus, SpamCop)	O IP do servidor foi listado por enviar spam.	O IP do seu servidor está numa lista negra
Botnet ou comando e controlo (C2)	O servidor faz parte de uma rede de máquinas comandadas por outra pessoa.	Actividade de botnet no seu servidor
Site fraudulento	Uma queixa de que um site da sua conta engana pessoas (falso investimento, loja falsa).	Uma queixa de fraude sobre um site

**Não sabe por onde
começar**

O aviso não diz a causa, só o que se viu
de fora.

**O meu VPS foi
invadido?**

O que acontece, do aviso à resposta

1

O fornecedor de rede envia-nos o aviso, com um identificador, a data e a hora **em UTC**, o IP de origem (o seu servidor), os destinos e as portas.

2

Reencaminhamos-lho por pedido de suporte no Meu Interweb, com o registo tal como veio. Confirme que o e-mail da sua conta está certo e que lê os avisos de novos pedidos.

3

Investiga o seu servidor. Num VPS ou servidor dedicado o acesso root é seu: não entramos no servidor, e uma firewall configurada dentro dele só o senhor a muda. Comece por **verificar se o VPS foi invadido**.

4

Envia-nos o relatório curto, no mesmo pedido: a causa e como entrou, o que encontrou e removeu, e o que fez para não se repetir. O modelo está em **responder a um aviso de abuso**.

5

Respondemos ao fornecedor dentro do prazo, com o seu relatório.

6

Primeiro investiga, com o servidor ligado. Se até ao prazo a causa não ficar clara, ou o tráfego continuar, o servidor pode ser desligado para proteger a rede. Os dados ficam intactos. O caminho de volta está em **porque o servidor foi desligado ou bloqueado**.

As horas do aviso estão em UTC

O registo usa a hora UTC; os registos do seu servidor podem estar noutro fuso. Antes de procurar nos ficheiros de registo, veja o fuso do servidor e a hora UTC ao mesmo tempo: `timedatectl`

`date -u` Se o relógio estiver errado, corrija-o primeiro: **acertar o fuso e o relógio do VPS**.

Não ignore o aviso, nem responda só «já está resolvido». Sem a causa e sem o que fez, não temos o que mandar ao fornecedor, e o prazo passa na mesma. Apagar o ficheiro do ataque sem fechar a porta por onde entrou também não chega: o abuso volta e o servidor é desligado outra vez.

Responda cedo, mesmo sem ter tudo. Uma linha no pedido a dizer o que já fez e o que falta ajuda-nos a responder ao fornecedor dentro do prazo. Se perdeu o acesso SSH, diga-o no pedido (**perdi o acesso SSH**).

Recebeu um aviso de abuso e não percebe o registo? Responda no próprio pedido de suporte e explicamos-lhe linha a linha.

[Abrir pedido de suporte](#)

VEJA TAMBÉM

Responder a um aviso de abuso: a causa, o que removeu e como não se vai repetir

Porque o seu servidor foi desligado ou bloqueado depois de um aviso de abuso, e como o religar

O meu VPS foi invadido? Ver processos, cron, utilizadores, chaves SSH e pastas temporárias

O que fazemos pela segurança, DDoS incluído, e o que fica do seu lado

Manter o seu VPS ou servidor dedicado seguro: as seis que contam

Denunciar abuso: como se faz e o que acontece a seguir



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 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@interweb.co.mz • +258 84 635 1111 • +258 86 635 1111 • www.interweb.co.mz

HORÁRIO 2ª. à 6ª. Feira - 08 à 16 Horas
Sábado & Domingo - Fechado