

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Um ataque DDoS a partir do seu servidor: encontrar o tráfego de saída e pará-lo

Segurança

CÓDIGO

RLX-MZ-KB-2268

VERSÃO

v2026.10.21

PAÍS · IDIOMA

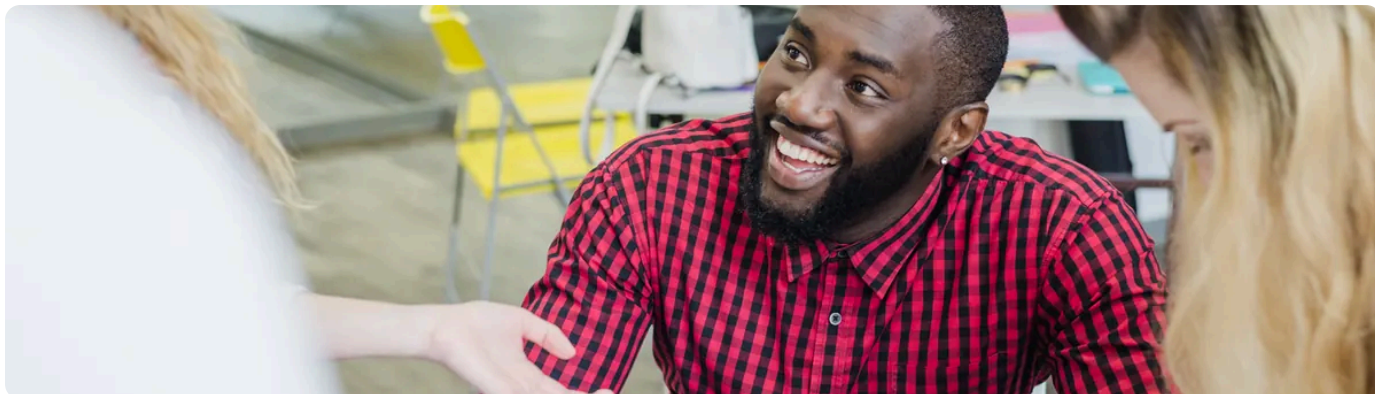
Moçambique · Português

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/2268>



Este artigo é para quem tem um VPS ou um servidor dedicado, com acesso root. **A resposta curta:** o aviso diz que do IP do seu servidor saiu uma enxurrada de pacotes ou de ligações contra outro endereço. O nosso fornecedor de rede vê esse tráfego na rede e manda-nos o aviso, com um prazo curto, muitas vezes de um dia. Há três causas habituais: um **bot** instalado no servidor, um **serviço aberto** à internet usado para reflexão (o seu servidor responde a pedidos falsificados e as respostas caem em cima da vítima), ou um **programa seu** descontrolado. Enquanto o tráfego continua, o servidor pode ser desligado e o IP bloqueado, por isso o primeiro passo é cortar a saída.

O que vê, e o que costuma ser

O que vê	O que costuma ser
Muito tráfego para um só destino, a partir de um processo que não reconhece	Um bot a cumprir ordens: actividade de botnet no seu servidor .
Respostas UDP a sair das portas 53, 389, 111, 123 ou 11211	Reflexão: um serviço aberto (DNS, CLDAP, Portmapper, NTP, Memcached). Veja o resolver DNS aberto e CLDAP, Portmapper e outros serviços UDP .
Pedidos HTTP em massa para um site, a partir de um script ou de uma ferramenta de testes	Um teste de carga ou um script com defeito. Testar um site que não é seu, sem autorização, é um ataque.
Ligações a muitos destinos diferentes, sempre na mesma porta	Varrimento, não DDoS: o seu VPS está a varrer outras redes .

Encontrar o tráfego e pará-lo

1

Veja para onde vai o tráfego. O `iftop` e o `nethogs` podem não estar instalados. O nome da interface (aqui `eth0`) pode ser outro: veja-o com `ip -br link`. `apt install iftop nethogs` # Debian/Ubuntu
`dnf install iftop nethogs` # AlmaLinux/Rocky, com o EPEL
`iftop -n -i eth0`
`nethogs eth0`

2

Veja que processo envia. `ss -s`
`ss -tunap | grep -v 127.0.0.1 | head -50`
`lsof -i -n -P | grep -i udp`
`top` Um processo com muita CPU e muitas ligações para o mesmo destino é o candidato.

3

Se for reflexão, veja que serviço responde para fora. `ss -ulpn`
`rpcinfo -p` Um serviço que não usa pode ser desligado já, por exemplo o Portmapper: `systemctl disable --now rpcbind rpcbind.socket`
Antes, confirme que nada legítimo o usa (o NFS, por exemplo, precisa dele).

4

Corte a saída para o alvo. Na firewall do servidor, que só o cliente pode mudar: `ufw deny out to IP_DO_ALVO`
ou, com `nftables` e uma tabela `inet filter` com a cadeia `output`:
`nft add rule inet filter output ip daddr IP_DO_ALVO drop`

5

Pare a origem. Se é um bot, guarde uma cópia e termine o processo, como em **cortar uma botnet**. Se é um serviço, feche-o ou limite-o à sua rede. Se é um programa seu, pare-o e corrija-o.

6

Confirme que parou. Volte ao `iftop` durante alguns minutos: o tráfego de saída deve voltar ao que é normal para o seu servidor.

7

Feche a porta e responda-nos. Descubra como o bot entrou (**o meu VPS foi invadido?**), atualize o sistema (**atualizações automáticas**), configure a **firewall** e envie o relatório: **responder a um aviso de abuso**.

Bloquear o alvo esconde o sintoma, não resolve a causa. Um bot recebe um alvo novo e o aviso seguinte chega com outro destino. E se o tráfego continua depois do prazo, o servidor é desligado para proteger a rede, sem apagar dados: **porque o servidor foi desligado ou bloqueado**. Num servidor invadido, o mais seguro é reinstalar e repor uma cópia limpa.

Se o ataque é CONTRA o seu servidor, o artigo é outro: ataque DDoS ou apenas um pico de visitas. E o que fica do nosso lado e do seu está em **o que fazemos pela segurança**.

Recebeu um aviso de DDoS e não encontra o tráfego? Responda no mesmo pedido de suporte com a saída dos comandos acima.

[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

Actividade de botnet ou de comando e controlo no seu servidor: cortá-la e limpar

CLDAP, Portmapper e outros serviços UDP abertos à internet: ataques de reflexão e como fechá-los

Um resolver DNS aberto no seu VPS: porque é usado em ataques e como desligar a recursão

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

Ataque DDoS ou apenas um pico de visitas: como distinguir, e o que fazer



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