

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

O seu VPS está a varrer outras redes: encontrar o processo de um aviso de netscan e pará-lo

Segurança

CÓDIGO

RLX-MZ-KB-2250

VERSÃO

v2026.10.21

PAÍS · IDIOMA

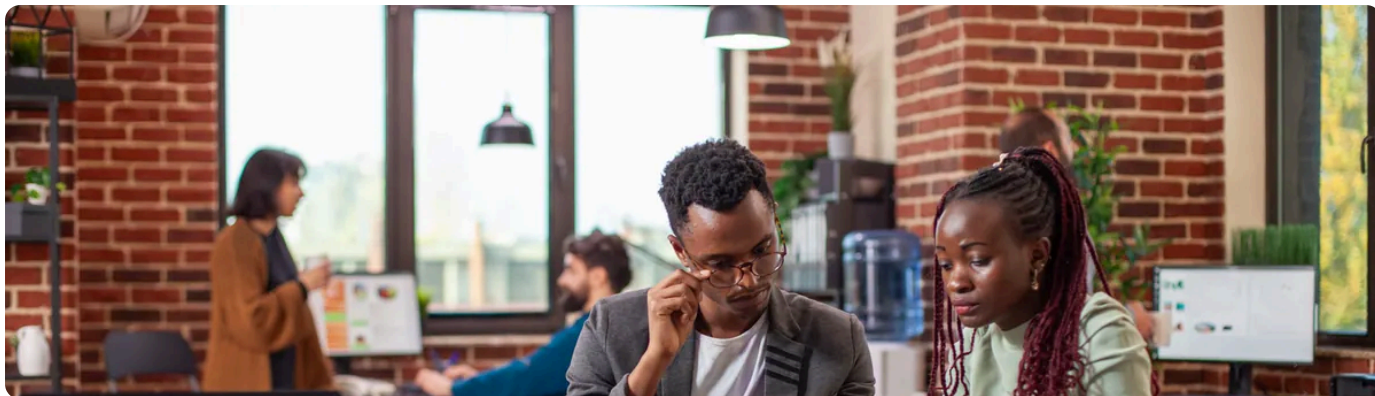
Moçambique · Português

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/2250>



A resposta curta: um aviso de **netscan** quer dizer que o seu servidor abriu, em poucos minutos, ligações a muitos endereços de uma gama, sempre nas mesmas portas (por exemplo 22, 80 e 443, ou 6379). Quase sempre é um **programa malicioso** que entrou no servidor e anda à procura de novas vítimas; às vezes é uma ferramenta de varrimento que alguém correu contra redes que não são suas, o que também é abuso. Este artigo é para quem tem um **VPS ou servidor dedicado**: encontra-se o processo pelas ligações, pára-se, e procura-se por onde entrou.

O que as portas do aviso lhe dizem

Portas de destino no registo	O que o programa anda a fazer
22 (SSH)	A tentar adivinhar senhas de SSH noutros servidores. É muitas vezes assim que o seu também foi apanhado.
80 e 443 (web)	À procura de sites e aplicações com falhas conhecidas.
6379 (Redis)	À procura de Redis abertos. Se o seu Redis está aberto, foi provavelmente por aí que entrou: Redis aberto à internet .
Muitos destinos seguidos (uma gama inteira)	Um varrimento: o programa percorre endereço a endereço.
IP de origem	É o IP do seu servidor. Se tem vários, o aviso diz qual.

Encontrar o processo e pará-lo

1

Anote as portas e a hora (UTC) do aviso, e entre por SSH como root. Se o varrimento ainda decorre, vê-se agora; se já parou, vá directo ao passo 5.

2

Liste as ligações de saída pendentes: um varrimento deixa muitas ligações em `SYN-SENT` (tentativas que ninguém atendeu). Os comandos do bloco abaixo mostram-nas e contam-nas por processo.

3

Identifique o programa: com o número do processo (PID), veja o ficheiro com `ls -l /proc/PID/exe` e a linha de comando com `/proc/PID/cmdline`. Se `iftop` ou `nethogs` estiverem instalados, mostram o tráfego por ligação ou por processo; podem não estar.

4

Congele, copie e só depois mate o processo (segundo bloco). `kill -STOP` pára-o sem o apagar da memória, para poder copiar o programa para análise.

5

Descubra o que o volta a arrancar: quase sempre há uma tarefa cron, um serviço systemd ou uma chave SSH a trazê-lo de volta. Siga **verificar processos, cron, utilizadores e chaves**.

6

Feche a porta por onde entrou (Redis aberto, senha fraca no SSH, aplicação desactualizada), confirme com `ss -tnp state syn-sent` que o varrimento parou, e envie o relatório: **responder a um aviso de abuso**.

Encontrar o processo pelas ligações

Troque PID pelo número que o primeiro comando mostrar no fim de cada linha. Estes comandos só lêem: `ss -tnp state syn-sent`

```
ss -tnp state syn-sent | awk 'NR>1 {print $NF}' | sort | uniq -c | sort -rn | head  
ss -tunap | grep ':6379'
```

```
ls -l /proc/PID/exe  
tr '\0' ' ' < /proc/PID/cmdline; echo  
systemctl status PID
```

Congelar, copiar e parar

Copie o programa antes de o matar: depois de morto, pode já não haver ficheiro no disco. `kill -`

`STOP PID`

```
mkdir -p /root/analise
```

```
cp /proc/PID/exe /root/analise/amostra-PID
```

```
sha256sum /root/analise/amostra-PID
```

```
kill -9 PID
```

Cortar a saída enquanto limpa

Com o **ufw**, bloqueia-se a saída para uma porta; se usa nftables directamente, o terceiro comando mostra as regras que tem. Confirme antes que nenhuma aplicação sua precisa de sair por essa porta:

```
ufw deny out 6379/tcp
```

```
ufw status numbered
```

```
nft list ruleset
```

Matar o processo não chega. Se não retirar o que o arranca (cron, serviço, chave) e não fechar a entrada, o varrimento volta, às vezes minutos depois, e o servidor é desligado. E não bloqueie a saída para as portas 80 e 443 de forma permanente: o próprio servidor precisa delas para se actualizar e para as suas aplicações.

A firewall do servidor ajuda enquanto investiga: bloquear a saída para a porta que o programa varre (o exemplo do bloco é a 6379) corta o abuso sem afectar o resto. Retire a regra quando tiver limpo, se precisar dessa porta. **Num servidor invadido, o mais seguro é reinstalar o sistema e repor uma cópia limpa (reinstalar o sistema do VPS e que cópia restaurar).** A limpeza no sítio é para quem sabe o que está a fazer: um atacante com acesso root pode deixar portas de volta que não se vêem à primeira.

Recebeu um aviso de netscan e não encontra o processo? Envie-nos o resultado de `ss -tunap` no pedido de suporte do aviso.

[Abrir pedido de suporte](#)

VEJA TAMBÉM

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

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

Redis aberto à internet: feche-o com bind, modo protegido, senha e firewall

Configurar a firewall ufw no Ubuntu sem ficar de fora do servidor

Instalar o fail2ban num VPS para travar quem tenta adivinhar a palavra-passe do SSH

Portas e firewall num VPS: porque a aplicação não é alcançável



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