

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

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

Segurança

CÓDIGO

RLX-MZ-KB-2266

VERSÃO

v2026.10.21

PAÍS · IDIOMA

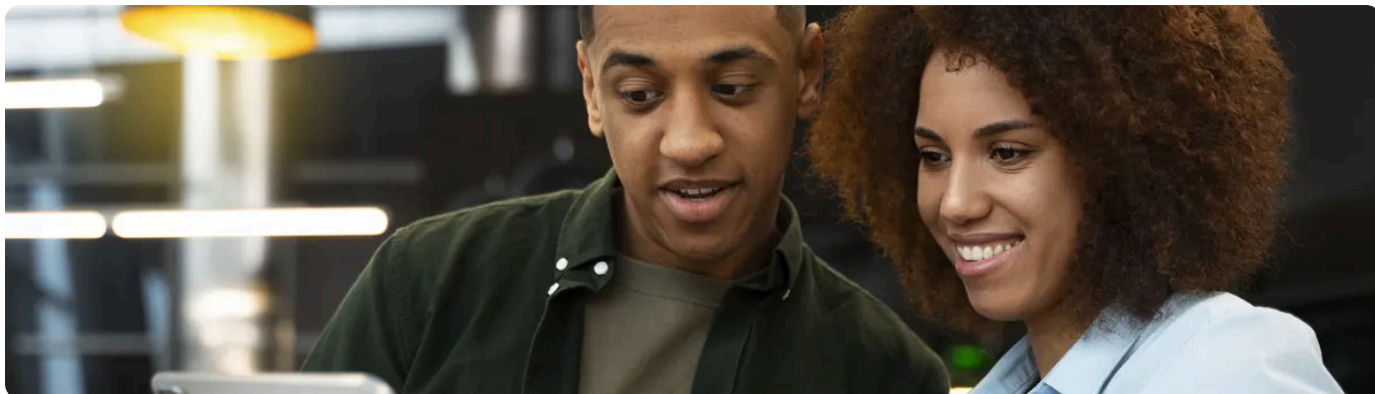
Moçambique · Português

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/2266>



Este artigo é para quem tem um VPS ou um servidor dedicado, com acesso root. **A resposta curta:** uma botnet é um conjunto de máquinas invadidas que alguém comanda à distância; o servidor de **comando e controlo (C2)** é quem dá as ordens. Um aviso destes diz que o seu servidor fala com um C2 conhecido, que corre ele próprio um painel de C2, ou que participa nos ataques da rede. Quer dizer que **alguém está a usar a sua máquina**, quase sempre depois de entrar por uma palavra-passe de SSH fraca, por um serviço aberto à internet ou por uma aplicação desactualizada. O aviso chega do nosso fornecedor de rede ou de uma equipa nacional de resposta a incidentes (CERT), com um prazo curto, muitas vezes de um dia. O root é seu: não entramos no servidor, e a limpeza é sua.

O que o aviso costuma dizer, e o que significa

No aviso	O que significa
Ligações a um IP ou domínio de C2, com a porta	Um programa no seu servidor fala com o controlador: é o bot, à espera de ordens.
Um servidor de C2 a correr no seu IP	Alguém instalou no seu servidor o painel que comanda outros bots, muitas vezes numa porta alta ou atrás de um site.
Participação em ataques ou varrimentos	O bot já está a trabalhar: veja também um ataque DDoS a partir do seu servidor e o seu VPS está a varrer outras redes .
CPU sempre no máximo, com um processo de nome estranho	Mineração de criptomoedas, que costuma vir junto com o bot.

Cortar e limpar, por ordem

1

Encontre o processo que fala com o destino do aviso. Se não aparece logo, pode ligar-se de tempos a tempos: repita o comando, ou deixe o `watch` a correr. `ss -tunap | grep IP_DO_AVISO`

```
lsof -i @IP_DO_AVISO
```

```
watch -n 5 "ss -tunap | grep IP_DO_AVISO"
```

2

Veja o que é. Nomes a imitar processos do sistema, programas a correr de `/tmp` ou com o ficheiro já apagado («(deleted)») são sinais claros: `ps auxf`

```
ls -l /proc/PID/exe
```

```
tr "\0" " " < /proc/PID/cmdline; echo
```

3

Corte o contacto com o C2. Bloqueie a saída para o destino na firewall, antes de mexer no processo: `ufw deny out to IP_DO_AVISO`

ou, com nftables e uma tabela inet filter com a cadeia output:

```
nft add rule inet filter output ip daddr IP_DO_AVISO drop
```

4

Guarde uma cópia e pare o processo. Congele-o, copie o programa para análise e só depois termine-o: `mkdir -p /root/analise`

```
kill -STOP PID
```

```
cp /proc/PID/exe /root/analise/amostra.bin
```

```
kill -9 PID
```

5

Procure o que o faz voltar. Um bot traz quase sempre uma forma de reaparecer: `for u in $(cut -d: -f1 /etc/passwd); do crontab -l -u "$u" 2>/dev/null | sed "s/^/$u: /"; done`

`ls -la /etc/cron.d /etc/cron.hourly /etc/cron.daily`

`systemctl list-units --type=service --state=running`

`ls -la /tmp /var/tmp /dev/shm`

`cat /root/.ssh/authorized_keys` A lista completa está em **o meu VPS foi invadido?**.

6

Descubra por onde entraram. Veja os acessos por SSH e as tentativas falhadas, e o que está aberto à internet: `last -n 30`

`lastb -n 30`

`ss -tulpn`

`docker ps` Um contentor ou um serviço exposto sem palavra-passe é uma porta comum: **usar o Docker num VPS em segurança** e **um n8n ou uma aplicação web vulnerável**.

7

Decida: limpar ou reinstalar. O mais seguro é **reinstalar o sistema** e repor só os dados, de uma cópia de antes da invasão. Depois: **chaves SSH, fail2ban, firewall** e **actualizações automáticas**. Por fim, envie-nos o relatório: **responder a um aviso de abuso**.

Matar o processo não é limpar. Se a porta de entrada e a forma de reaparecer ficam, o bot volta em minutos, e o aviso também. Quem teve root pode ter mexido em programas do sistema para se esconder: nesse caso, só reinstalar dá certeza. A limpeza no sítio é para quem sabe o que está a fazer. 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**.

Guarde num ficheiro os comandos que correu e o que viu, com as horas. É a base do relatório que nos envia, e evita repetir a investigação se o problema voltar. Se perdeu o acesso por SSH, diga-nos no pedido de suporte.

Recebeu um aviso de botnet e precisa de ajuda para ler o registo? Responda no mesmo pedido de suporte.

[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

O meu VPS foi invadido? Verificar 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

Reinstalar ou mudar o sistema operativo do seu VPS

Depois de um ataque, que cópia restaurar? Como escolher uma cópia limpa

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



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