

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

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

Segurança

CÓDIGO

RLX-MZ-KB-2248

VERSÃO

v2026.10.21

PAÍS · IDIOMA

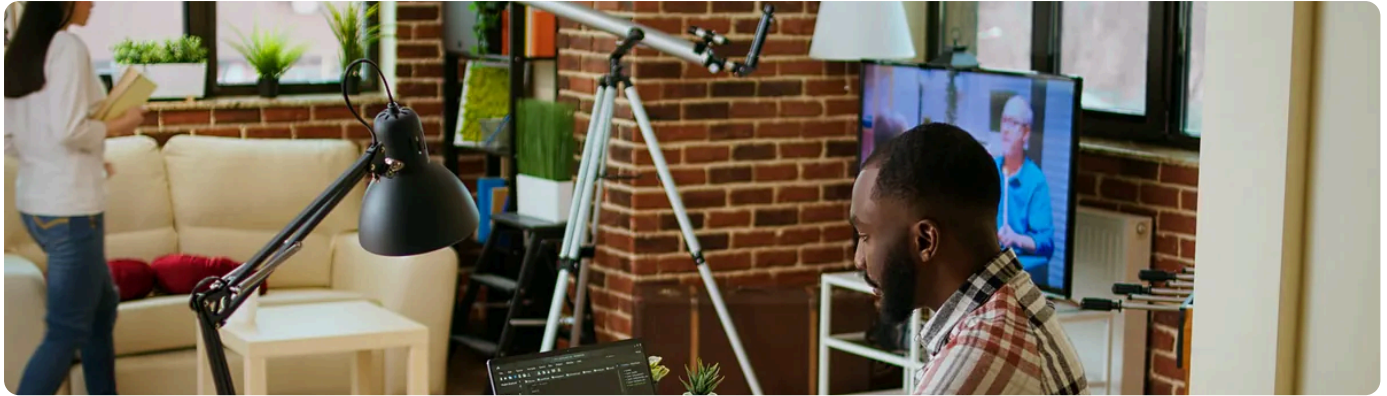
Moçambique · Português

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/2248>



A resposta curta: este artigo é para quem tem um **VPS ou servidor dedicado** com acesso root. Depois de um aviso de abuso, ou se o servidor se porta de forma estranha (CPU sempre alta, ligações que não reconhece), há **oito sítios a ver**: os processos, as ligações de rede, as tarefas cron, os serviços, os utilizadores, os registos de entrada, as chaves SSH e as pastas temporárias. Os comandos abaixo **só lêem**: não mudam nada. Antes de apagar o que encontrar, **faça uma cópia para análise**.

Onde procurar, e o que é suspeito

O que ver	Comando	O que é suspeito
Processos	<code>ps auxf</code> , <code>top</code> ou <code>htop</code>	Nomes aleatórios, nomes que imitam processos do sistema, programas a correr de <code>/tmp</code> ou <code>/dev/shm</code> , CPU sempre no máximo.
Ligações de rede	<code>ss -tunap</code> ou <code>lsof -i</code>	Muitas ligações de saída para endereços que não conhece, ou um programa à escuta numa porta que não abriu.
Tarefas cron	<code>crontab -l</code> de cada utilizador, <code>/etc/cron*</code>	Linhas que descarregam e correm qualquer coisa (<code>curl</code> ou <code>wget</code> com <code> sh</code>), texto em base64.
Serviços e temporizadores	<code>systemctl list-units --type=service</code> , <code>systemctl list-timers</code>	Serviços com nomes que não reconhece, ou que arrancam um ficheiro de uma pasta temporária.
Utilizadores	<code>/etc/passwd</code>	Utilizadores novos com shell, ou outro utilizador além do root com UID 0.
Entradas	<code>last</code> e <code>lastb</code>	Entradas de IPs que não são seus; muitas tentativas falhadas (adivinhar a senha).
Chaves SSH	<code>~/.ssh/authorized_keys</code> do root e de cada utilizador	Chaves que não reconhece: dão entrada sem senha.
Pastas temporárias	<code>/tmp</code> , <code>/var/tmp</code> , <code>/dev/shm</code>	Ficheiros executáveis, ficheiros escondidos (começados por ponto), pastas com nomes estranhos.

A verificação, passo a passo

1

Entre por SSH como root, ou com um utilizador com sudo, e anote a hora a que começa. Se perdeu o acesso, veja **perdi o acesso SSH** e digamos no pedido de suporte.

2

Corra os comandos de leitura do bloco abaixo, um a um, e guarde o que mostram (num ficheiro ou numa nota). Compare com o que sabe que instalou.

3

Para cada coisa suspeita, descubra de onde vem: o caminho do programa de um processo vê-se com `ls -l /proc/PID/exe` (troque PID pelo número do processo). Os registos ajudam a datar a entrada: **onde estão os registos num VPS.**

4

Antes de apagar, copie para análise (segundo bloco abaixo). A cópia e o seu resumo SHA-256 servem para o relatório e para perceber o que aconteceu.

5

Decida: reinstalar ou limpar no sítio. Se encontrou outro utilizador com UID 0 além do root, chaves que não são suas ou programas escondidos no sistema, reinstale. Se for limpar, retire as entradas do cron, os serviços, as chaves e os utilizadores estranhos, e só depois pare os processos.

6

Feche a porta de entrada: mude todas as senhas, passe a usar **chaves SSH**, actualize o sistema e as aplicações, e feche na firewall o que não precisa de estar aberto. Depois escreva o relatório: **responder a um aviso de abuso**.

Os comandos de leitura

Correm como root (ou com `sudo` à frente). Nenhum muda nada no servidor: `ps auxf`

```
ss -tunap
```

```
for u in $(cut -d: -f1 /etc/passwd); do crontab -l -u "$u" 2>/dev/null | sed "s/^/$u: /"; done
```

```
ls -la /etc/cron* /var/spool/cron 2>/dev/null
```

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

```
systemctl list-timers
```

```
awk -F: '$3 == 0' /etc/passwd
```

```
last -a | head -30
```

```
lastb -a | head -30
```

```
cat /root/.ssh/authorized_keys
```

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

Copiar antes de apagar

Guarde uma cópia de cada ficheiro suspeito numa pasta só sua, com o resumo SHA-256, antes de o apagar. Não a deixe numa pasta pública do site: `mkdir -p /root/analise`

```
cp -a /caminho/do/ficheiro-suspeito /root/analise/
```

```
sha256sum /root/analise/*
```

Um atacante com root pode esconder-se dos próprios comandos. Se o sistema foi alterado, `ps` e `ss` podem mentir, e um servidor que «parece limpo» pode não estar. **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. Nunca corra os ficheiros suspeitos para «ver o que fazem».

Muitas linhas em `lastb` não querem dizer que entraram: são tentativas falhadas, comuns em qualquer servidor com o SSH aberto. Reduzem-se com **o `fail2ban`** e com a entrada por chave. O que conta é `last` : as entradas que deram certo.

Encontrou alguma coisa e não sabe se é sua ou de um atacante? Envie-nos o resultado dos comandos no pedido de suporte.

[Abrir pedido de suporte](#)

VEJA TAMBÉM

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

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

Onde estão os registos num VPS Linux: `journalctl` e `/var/log`

Como criar uma chave SSH e entrar no VPS sem palavra-passe

Reinstalar ou mudar o sistema operativo do seu VPS

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



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