

KNOWLEDGE BASE · PUBLIC DOCUMENT

Botnet or command-and-control activity from your server: cutting it off and cleaning up

Security

CODE

RLX-MZ-KB-2266

VERSION

v2026.10.21

COUNTRY · LANGUAGE

Mozambique · English

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

<https://www.meu.interweb.co.mz/knowledgebase/2266>



This article is for customers with a VPS or a dedicated server, with root access. **The short answer:** a botnet is a set of hijacked machines that someone controls remotely; the **command-and-control (C2)** server is the one giving the orders. A notice like this says your server talks to a known C2, runs a C2 panel itself, or takes part in the network’s attacks. It means **someone else is using your machine**, nearly always after getting in through a weak SSH password, a service open to the internet or an outdated application. The notice comes from our network provider or from a national incident response team (CERT), with a short deadline, often a single day. Root is yours: we do not log in to the server, and the clean-up is yours.

What the notice usually says, and what it means

In the notice	What it means
Connections to a C2 IP or domain, with the port	A program on your server talks to the controller: that is the bot, waiting for orders.
A C2 server running on your IP	Someone installed on your server the panel that commands other bots, often on a high port or behind a website.
Taking part in attacks or scans	The bot is already at work: see also a DDoS attack coming from your server and your VPS is scanning other networks .
CPU always at full, with an oddly named process	Cryptocurrency mining, which often comes along with the bot.

Cutting it off and cleaning up, in order

1

Find the process talking to the destination in the notice. If nothing shows straight away, it may connect only now and then: repeat the command, or leave `watch` running. `ss -tunap | grep NOTICE_IP`

```
lsof -i @NOTICE_IP
```

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

2

See what it is. Names that mimic system processes, programs running from `/tmp`, or whose file is already deleted ("(deleted)") are clear signs:

```
ps auxf
```

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

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

3

Cut off contact with the C2. Block outgoing traffic to the destination in the firewall before touching the process: `ufw deny out to NOTICE_IP`

or, with `nftables` and an `inet` filter table with an output chain:

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

4

Keep a copy and stop the process. Freeze it, copy the program for analysis, and only then end it: `mkdir -p /root/analysis`

```
kill -STOP PID
```

```
cp /proc/PID/exe /root/analysis/sample.bin
```

```
kill -9 PID
```

5

Look for what brings it back. A bot nearly always carries a way to reappear: `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` The full list is in **is my VPS compromised?**.

6

Find the way in. Look at SSH logins and failed attempts, and at what is open to the internet: `last -n 30`
`lastb -n 30`
`ss -tulpn`
`docker ps` A container or a service exposed without a password is a common door: **running Docker on a VPS safely** and **a vulnerable n8n or web application**.

7

Decide: clean up or reinstall. The safest path is to **reinstall the system** and restore only the data, from a copy taken before the break-in. Then: **SSH keys, fail2ban, a firewall** and **automatic updates**. Finally, send us the report: **writing the reply to an abuse notice**.

Killing the process is not cleaning up. If the way in and the way back stay, the bot returns within minutes, and so does the notice. Whoever had root may have altered system programs to hide: then only a reinstall gives certainty. Cleaning in place is for people who know what they are doing. If the traffic continues past the deadline, the server is switched off to protect the network, without deleting any data: **why the server was switched off or locked**.

Keep the commands you ran and what you saw in a file, with the times. It is the basis of the report you send us, and saves repeating the investigation if the problem returns. If you have lost SSH access, tell us in the support ticket.

Got a botnet notice and need help reading the log? Reply in the same support ticket.

[Open a support ticket](#)

SEE ALSO

An abuse notice about your server: what it means, the deadline and what we need from you

Is my VPS compromised? Checking processes, cron jobs, users, SSH keys and temporary folders

Writing the reply to an abuse notice: cause, what you removed and how it will not happen again

Reinstalling or changing your VPS operating system

After a hack, which backup do you restore? Choosing a clean copy

Keeping your VPS or dedicated server secure: the six that matter



Online version of this document

Interweb is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020

FOUNDED

37,000+

CLIENTS

130+

SIGN-UPS A DAY

Interweb Mozambique

RLX Holdings, S.A. • Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 • CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz • +258 84 635 1111 • +258 86 635 1111 • www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed