Generated on 21/10/2026 16:04

KNOWLEDGE BASE · PUBLIC DOCUMENT

A DDoS attack coming from your server: finding the outgoing flood and stopping it

Security

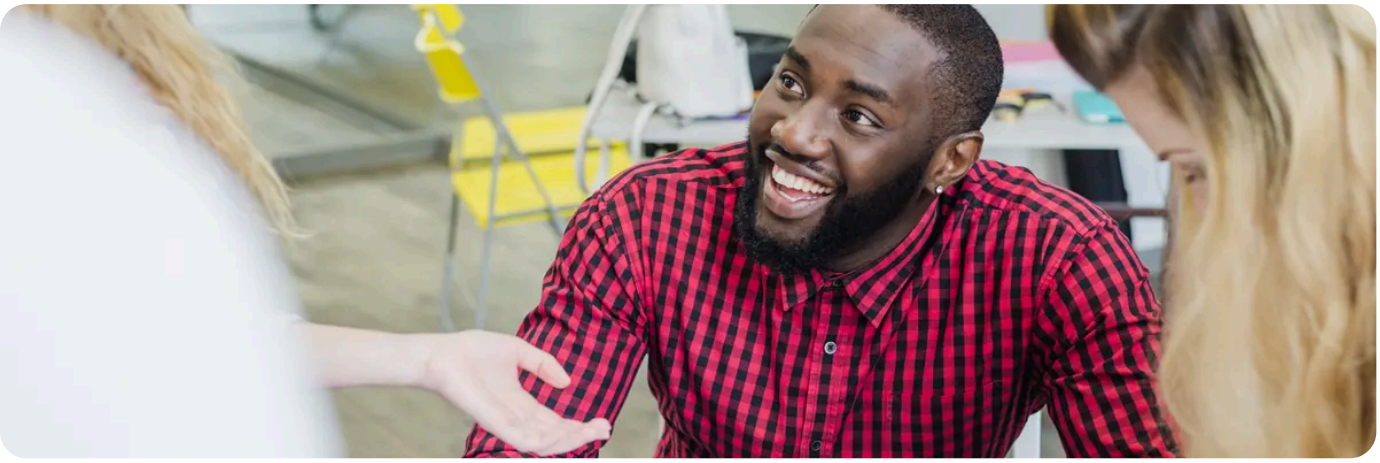
CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-6888	v2026.10.21	International · English

MozOut International
RLX Holdings (Pty) Ltd. · Group RLX Holdings
Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/6888

A DDoS attack coming from your server: finding the outgoing flood and stopping it

Security Created on **October 21, 2026** 4 min read



This article is for customers with a VPS or a dedicated server, with root access. **The short answer:** the notice says a flood of packets or connections left your server's IP towards another address. Our network provider sees that traffic on the network and sends us the notice, with a short deadline, often a single day. There are three usual causes: a **bot** installed on the server, a **service open** to the internet being used for reflection (your server answers forged requests and the answers land on the victim), or a **program of yours** running out of control. While the traffic continues, the server may be switched off and the IP blocked, so the first step is to cut the outgoing flow.

What you see, and what it usually is

What you see	What it usually is
Lots of traffic to a single destination, from a process you do not recognise	A bot following orders: **botnet activity reported from your server**.
UDP replies leaving ports 53, 389, 111, 123 or 11211	Reflection: an open service (DNS, CLDAP, Portmapper, NTP, Memcached). See **the open DNS resolver** and **CLDAP, Portmapper and other UDP services**.
Mass HTTP requests to one site, from a script or a testing tool	A load test or a faulty script. Testing a site that is not yours, without permission, is an attack.
Connections to many different destinations, always on the same port	A scan, not a DDoS: **your VPS is scanning other networks**.

Finding the traffic and stopping it

1. **See where the traffic goes.** `iftop` and `nethogs` may not be installed. The interface name (here `eth0`) may differ: check it with `ip -br link`. `apt install iftop nethogs # Debian/Ubuntu`
`dnf install iftop nethogs # AlmaLinux/Rocky, with EPEL`
`iftop -n -i eth0`
`nethogs eth0`

2. **See which process is sending.** `ss -s`
`ss -tunap | grep -v 127.0.0.1 | head -50`
`lsof -i -n -P | grep -i udp`
`top` A process with high CPU and many connections to the same destination is the suspect.

3. **If it is reflection, see which service answers to the outside.** `ss -ulpn`
`rpcinfo -p` A service you do not use can be switched off right away, for example Portmapper: `systemctl disable --now rpcbind rpcbind.socket` First make sure nothing legitimate depends on it (NFS, for instance, needs it).

4. **Cut the outgoing traffic to the target.** In the server's firewall, which only you can change: `ufw deny out to TARGET_IP`
`# or, with nftables and an inet filter table with an output chain:`
`nft add rule inet filter output ip daddr TARGET_IP drop`

5. **Stop the source.** If it is a bot, keep a copy and end the process, as in **cutting off a botnet**. If it is a service, close it or limit it to your own network. If it is your own program, stop it and fix it.

6. **Check that it stopped.** Watch `iftop` for a few minutes: outgoing traffic should be back to what is normal for your server.

7. **Close the door and reply to us.** Find out how the bot got in (**is my VPS compromised?**), update the system (**automatic updates**), set up the **firewall** and send the report: **writing the reply to an abuse notice**.

Blocking the target hides the symptom, it does not fix the cause.
A bot gets a new target and the next notice arrives with a different destination. And 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**. On a compromised server, the safest path is to reinstall and restore a clean copy.

If the attack is AGAINST your server, you need a different article:
DDoS attack or just a traffic spike. What stays on our side and what is yours is in **what we do about security**.

NEED A HAND?

Got a DDoS notice and cannot find the traffic? Reply in the same support ticket with the output of the commands above.

Open a support ticket →

SEE ALSO

- An abuse notice about your server: what it means, the deadline and what we need from you
- Botnet or command-and-control activity from your server: cutting it off and cleaning up
- CLDAP, Portmapper and other open UDP services: reflection attacks and how to close them
- An open DNS resolver on your VPS: why it is used in attacks and how to turn off recursion
- Writing the reply to an abuse notice: cause, what you removed and how it will not happen again
- DDoS attack or just a traffic spike: how to tell, and what to do

mozout

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

TAX NO. (SARS)	943 907 6234
REGISTRATION NO. (CIPC)	2025/667953/07
REGISTERED OFFICE	1111 Olive Street Saint Louis 63101, Missouri, United States
CONTACT	info@mozout.com · +27 78 823 3325 · www.mozout.com
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-INT-KB-6888 · v2026.10.21 · Generated on 21/10/2026 16:04