interweb

Generated on 15/11/2026 01:48

KNOWLEDGE BASE · PUBLIC DOCUMENT

DDoS attack or just a traffic spike: how to tell, and what to do

Abuse Notices & Blocklists

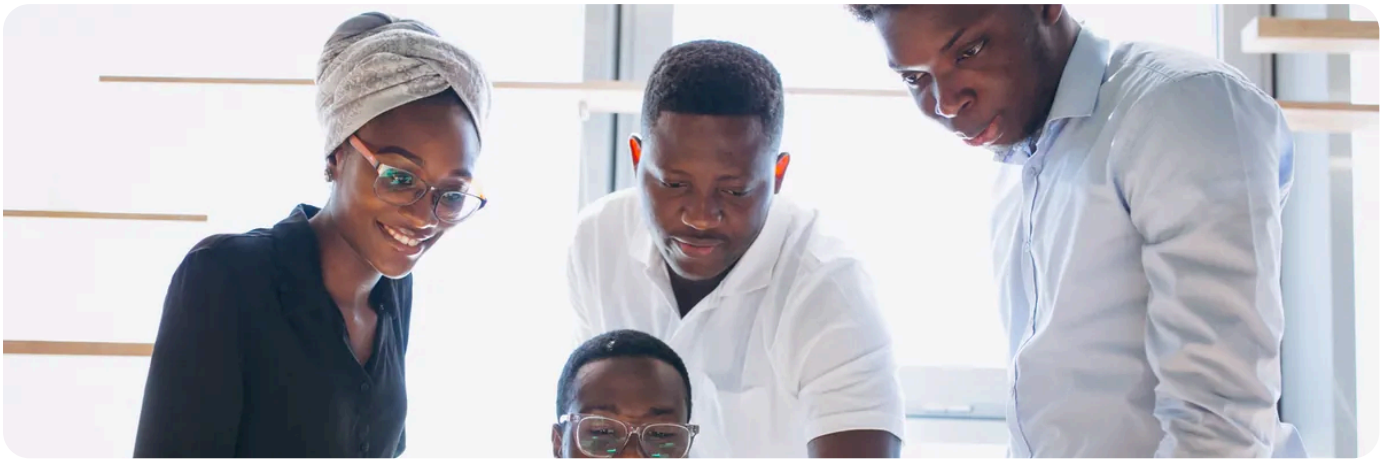
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-1510	v2026.10.18	Mozambique · English

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/1510

DDoS attack or just a traffic spike: how to tell, and what to do

Abuse Notices & Blocklists · Created on **October 10, 2026** · Updated on **October 18, 2026** · 4 min read



The short answer: a **DDoS** (distributed denial of service) attack is a flood of fake requests, from many addresses at once, meant to stop the site answering the real ones. But most of the "attacks" customers report to us are something else: **a campaign that went well**, **bots reading the whole site**, or **a plugin asking for too much**. The difference shows when you look at *who* is asking and *for what*.

The four most common explanations

Cause	What it looks like	What to do
A genuine traffic spike	A rise right after a post, an advert or a press mention. Visitors see different pages and stay a while.	Nothing hostile: it is a good sign. If the site copes badly, see **what actually makes a difference to speed**.
Bots and crawlers	Many requests, from a handful of origins, walking through every page or the internal search.	Limit with `robots.txt` and block the worst. See **AI bots crawling your site**.
A plugin or script asking for too much	Resource use climbs without the visitor count climbing. Typical of `admin-ajax.php` or a scheduled task.	See **admin-ajax eating your resources**.
A real attack	Thousands of requests a minute from many unrelated addresses, nearly all to the same place: the home page, the search, `wp-login.php`, `xmlrpc.php`. The pages asked for do not vary and nobody stays on the site.	See below.

How to confirm, in four steps

1. **Note the start time** and how it began: suddenly, or in a ramp.

2. **Look at the statistics in cPanel** (visitors and raw access). The addresses and pages most requested say a lot. Find them in **visitor statistics**.

3. **Look at the errors the site returns.** A 508 or 503 error means the site reached its account limits or the server is busy: **website errors: 500, 403, 404 and 508**.

4. **Compare with a normal day.** If the activity only changed on one page or one address, it is almost always the site; if it changed everywhere and from all over, it is likelier to be external.

If it is an attack

1. **Talk to us straight away.** Our servers have volumetric attack filtering at network level, and we can see what reaches the server. Tell us the start time and the domain hit. What we do and what remains yours is in **what we do about security, DDoS included**.

2. **If the addresses are few and clear,** block them, as in **blocking an IP address from visiting your site**. In a real attack there are too many for that.

3. **If your site is a likely target,** put it behind a service that filters requests before they reach the server, with an “emergency mode”. Cloudflare is one example, and it is an account of your own. See **when it helps and how to switch it on**. No service promises absolute protection.

Messages demanding money so that the site is not attacked

are, nearly always, only the message: they threaten an attack that has not begun. Do not pay, do not reply, and keep the e-mail. In a very large attack, the network’s usual answer is to cut traffic to the address under attack for a few hours: unpleasant, and the least bad option.

Leaving a protection service’s “attack mode” on for good makes every visitor pass a check before seeing the site. Switch it on during the attack and off afterwards.

NEED A HAND?

Did the site slow down or stop answering, and you suspect an attack? Tell us the time and the domain.

Open a support ticket →

Where to see it in your account

- **Resource Usage** in cPanel: graphs of CPU, memory, I/O and entry processes against your account's limits, with the moments a limit was hit. A flood of requests shows as a sudden climb that touches the ceiling.
- **Errors 508 or 503** when you visit the site: 508 means the account reached its limits, 503 that the server was busy.
- **Visitor statistics and the raw access log**, under Metrics: the addresses and pages most requested at the time.

Take those three to the ticket, with the start time, the domain and, if you can, a screenshot of Resource Usage. With that in hand we can tell much faster whether the cause is the site or something outside it.

SEE ALSO

- What we do about security, DDoS included, and what stays yours →
- Blocking an IP address from visiting your site →
- AI bots crawling your site: robots.txt and how to block them →
- Cloudflare: when it helps, how to switch it on →

interweb

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

Online version of this document

RLX-MZ-KB-1510 · v2026.10.18 · Generated on 15/11/2026 01:48