interweb

Generated on 21/10/2026 17:26

KNOWLEDGE BASE · PUBLIC DOCUMENT

Scanning your site for malware in cPanel: what Imunify finds and what to do with the result

Security

CODE
RLX-MZ-KB-1714

VERSION
v2026.10.18

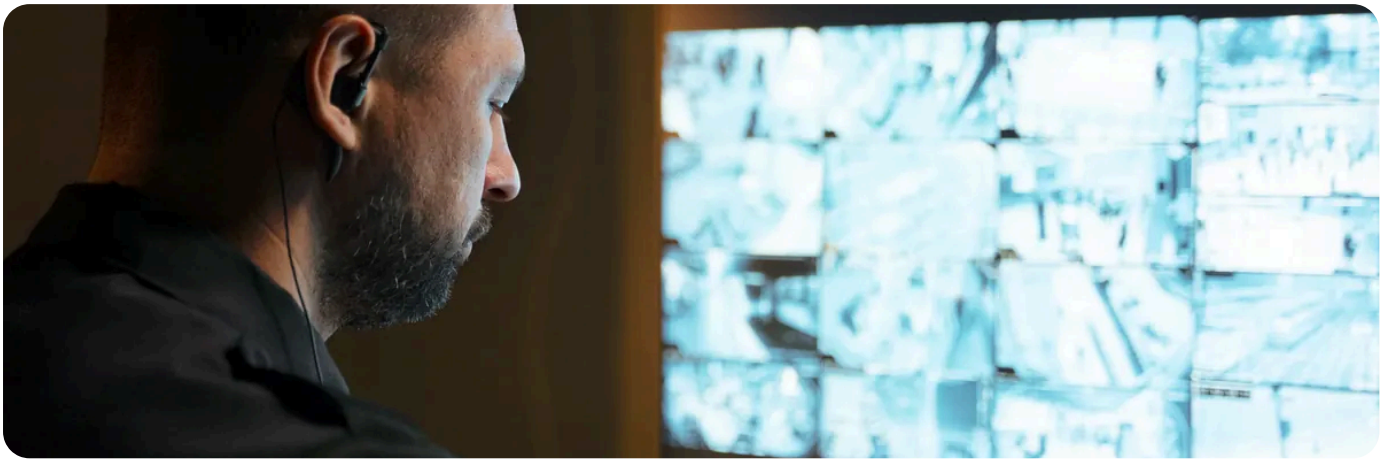
COUNTRY · LANGUAGE
Mozambique · English

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/1714

Scanning your site for malware in cPanel: what Imunify finds and what to do with the result

Security Created on **October 15, 2026** Updated on **October 18, 2026** 3 min read



The short answer: cPanel has a tool called **Imunify360**, in the **Security** group, that scans your account's files for malicious code (malware). You can order a scan whenever you like and see the list of what it flagged. It is for **finding out** there is a problem; what you do next decides whether the site is clean for good.

How to use it

1. **In cPanel,** look for the **Imunify360** icon in the **Security** section and open it.
2. **Find the malware scanning area** (Malware Scanner). You will see the list of files the tool flagged and the state of each, or a note that it found nothing.
3. **Order a scan** when you suspect something, rather than waiting for the next one. How long it takes depends on how many files the account has.
4. **For each flagged file,** note the path, the threat type's name and the date. Writing this down is the most useful thing you can add to a support request.

What each button does, namely whether the tool cleans the files for you, **depends on the version and licence installed on the server**. If a clean-up button is disabled or missing on your account, open a ticket: we will handle it or tell you what to do by hand.

What to do with the result

What you see	What to do
Nothing found, but the site behaves strangely (redirects, shows ads)	An automatic scan does not catch everything. See **The scan says clean but the site still redirects**.

What you see	What to do
Files from plugins, themes or WordPress core flagged	Often the fix is to reinstall the clean version from the official source, rather than cleaning by hand.
A flagged file in an images or uploads folder (`uploads`)	`.php` files in an images folder are almost always suspect.
Several files in several folders	There is probably an open door (stolen password, outdated plugin). Cleaning without closing it is pointless.

After the clean-up

1. **Change the passwords:** cPanel, FTP, database, WordPress administrator. See **Changing the WordPress administrator password**.
2. **Update** WordPress, plugins and themes, and delete the ones you do not use. See **An abandoned plugin or an old PHP version**.
3. **Switch on two-step verification** wherever you can: **How to enable two-factor authentication**.
4. **If you must put a copy back,** choose one from before the infection: **After a hack, which backup do you restore**.

Do not delete blindly.
Before removing files the tool flagged, take a copy of the account: a false alarm on one of your program's files can break the site. And a scanning tool does not replace prevention: updates, strong passwords and backups.

NEED A HAND?

Did the scan flag files and you do not know what to do? Open a ticket with the domain and the list of paths you saw.

Open a support ticket →

Where to see it in your account

- **The scanner.** Look for Imunify360 in the Security section of cPanel. What you see there, including whether a clean-up button is active, is what is available on your account; if it is missing, open a ticket.
- **A clean point to go back to.** Every shared plan makes an automatic daily backup, with restores at no cost. JetBackup (or Backups) in cPanel lists the restore points: choose one from before the first date on your list of flagged files.
- **Signs besides the scan.** Resource Usage can show CPU or process spikes nobody asked for, and the Statistics sidebar shows a sudden jump in files. Neither proves an infection, but both are worth noting in the ticket.
- **On a VPS.** You have full SSH access and look after security yourself, so do not expect the cPanel Security section there.

SEE ALSO

- The scan says clean but the site still redirects: where an infection hides
- After a hack, which backup do you restore? Choosing a clean copy
- Changing the WordPress administrator password
- ModSecurity and web application firewalls: what they do, and what to do when one blocks you

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-1714 · v2026.10.18 · Generated on 21/10/2026 17:26