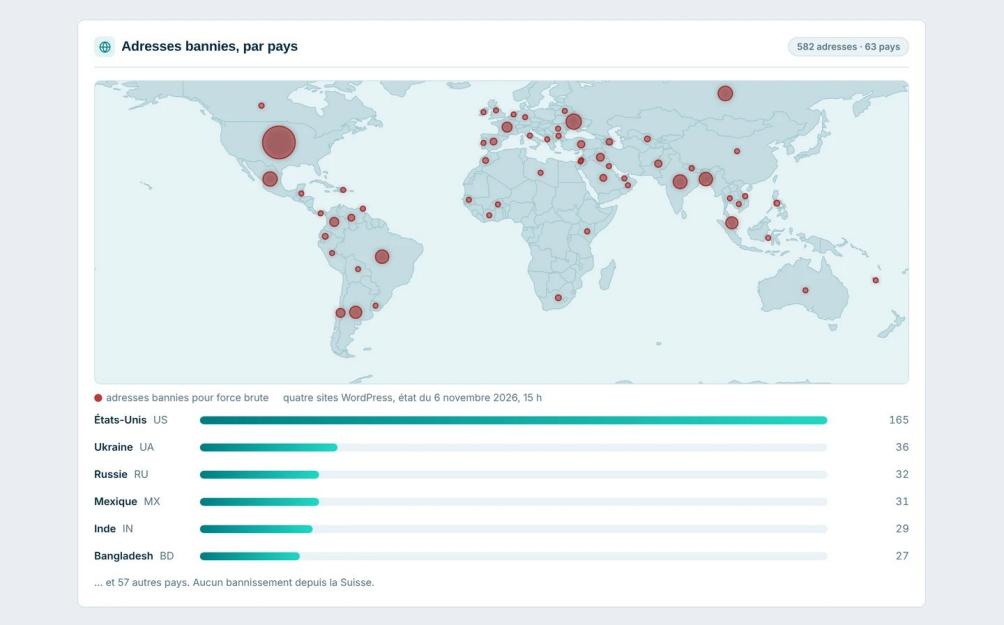
SÉCURITÉ WEB

Sixteen days after PHP2Shell: what K-Shield saw on seven sites

Depuis le 21 octobre : 15 900 requêtes hostiles bloquées, 589 adresses bannies venues de 63 pays, et 8 portes dérobées retirées su

Publié le 6 novembre 2026 — Imprimé le 27 novembre 2026



On 21 October, PHP released the fixes for PHP2Shell. That day, we extended K-Shield to all the sites we manage. Sixteen days later, here is what it found: attacks every day, and malicious code installed long before.

The figures

Seven WordPress sites: SMEs, a municipality, a press title, associations. All hosted in Switzerland. None is an obvious target.

- **At least 15,900 hostile requests blocked**, before they reached WordPress.
- **1,745 failed login attempts.**
- **589 addresses banned** for brute force, from **63 countries**.
- **8 backdoors removed**, on **3 sites out of 7**. The oldest dated from June 2022.

Attacked every day

The press site took 5,792 blocked requests in sixteen days, the municipality's 4,323. This is not background noise: these are robots trying known flaws, page after page.

Brute force has changed its face. An address no longer tries a hundred passwords: it tries one, then hands over. On 5 and 6 November, the same block of addresses targeted the same administrator account on two sites; on one of them, 101 addresses from this block were banned within 24 hours. The accounts targeted are real accounts, guessed from the company name or the email address.

Switzerland does not appear among the countries of origin. An address or a country does not identify an author; they say where the machine is operating from.

Three sites out of seven already had a tenant

Three sites were hosting malicious code installed long before we arrived. K-Shield removed everything, keeping a copy for analysis.

| Site | What was found | Present since | How it was hidden | | --- | --- | --- | --- | | Industrial SME | 4 backdoors, 6 loaders injected into WordPress, 88 modified core files, 1,056 fake spam pages | November 2024 at the latest | Credible file names, falsified dates, encrypted content. The spam pages were served only to Google. | | Press title | 2 backdoors | March 2025 | Two fake WordPress files, real names placed in the wrong location. | | Local shop | 2 backdoors | June 2022 | One disguised as a "Hello Dolly" plugin in the images folder, the other as three lines in the theme. |

Two other PHP files placed in image folders, one of them since 2017, were isolated as a precaution. An image folder does not contain a program.

What the firewall did not see

On the press site, Wordfence was running throughout the seven months the two files were present. It was blocking attacks. It did not see what was already installed.

This is not a criticism. These files carry no known virus signature. K-Shield found them in other ways:

- **It compares every file with the official original.** A file that is absent from the published version of WordPress or of the plugin is suspect, whatever its content.
- **It refuses any program in image folders.**
- **It works back from a suspect file to the files that load it.** The six loaders injected into WordPress were found this way, then replaced with the originals.

None of these sites showed any symptom visible to its owner.

Read the traces

Each block carries a code, a date, the address, the country and the account targeted. Each file removed keeps its fingerprint and its copy. A week later you can reread who struck, from where, against which account, and what K-Shield did.

The map at the top of this page is K-Shield's, fed by these traces: one bubble per country, its size following the number of banned addresses. Bans expire; on 6 November at 3 pm, 582 remained across the four sites.

Where these figures come from

They come from the K-Shield console, which receives the state of each site several times a day. They are minimums:

- **Requests blocked:** sum, day by day, of each site's highest 24-hour counter. This counter stops at 500; it hit that ceiling on 12 site-days.
- **Addresses banned:** since automatic banning went live in early November, on 4 sites. An address banned on two sites counts twice.
- **Scope:** 7 sites, brought under monitoring between late September and 6 November. Three of them have only been in for a few days.

We did not count our own false alarms as detections. There were some; each was corrected in the product.

For your site

Updating PHP closes the door. It does not tell you who is already inside. We start by looking at what is really running on your site, then we monitor it.

Review the security of my site · PHP2Shell: fixing the flaw and monitoring what follows