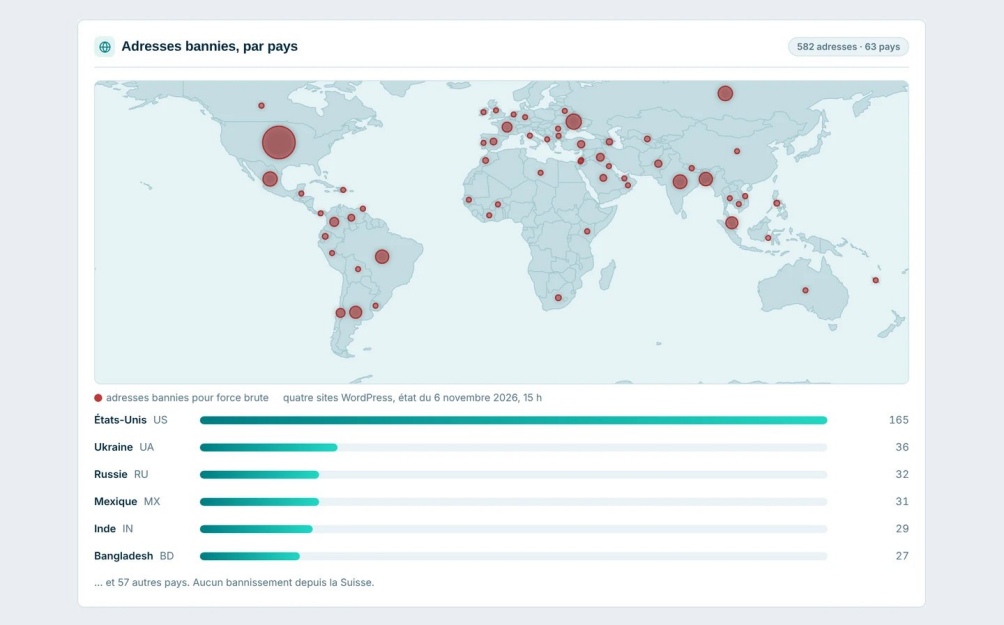
SÉCURITÉ WEB

Sechzehn Tage nach PHP2Shell: was K-Shield auf sieben Websites gesehen hat

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



Quelle: https://www.karbonic.net/journal-kshield-seize-jours.html

Am 21. Oktober veröffentlichte PHP die Korrekturen für PHP2Shell. An diesem Tag haben wir K-Shield auf alle Websites ausgeweitet, die wir betreuen. Sechzehn Tage später zeigen wir, was es gefunden hat: tägliche Angriffe und Schadcode, der lange zuvor installiert worden war.

Die Zahlen

Sieben WordPress-Websites: KMU, eine Gemeinde, ein Pressetitel, Vereine. Alle in der Schweiz gehostet. Keine ist ein offensichtliches Ziel.

- **Mindestens 15’900 feindliche Anfragen blockiert**, bevor sie WordPress erreichten.
- **1’745 gescheiterte Anmeldeversuche.**
- **589 wegen Brute-Force gesperrte Adressen** aus **63 Ländern**.
- **8 Hintertüren entfernt**, auf **3 von 7 Websites**. Die älteste stammte von Juni 2022.

Jeden Tag angegriffen

Die Presse-Website musste in sechzehn Tagen 5’792 blockierte Anfragen verkraften, die der Gemeinde 4’323. Das ist kein Hintergrundrauschen: Es sind Roboter, die bekannte Schwachstellen ausprobieren, Seite für Seite.

Brute-Force hat sein Gesicht verändert. Eine Adresse probiert nicht mehr hundert Passwörter aus: Sie probiert eines und gibt dann ab. Am 5. und 6. November nahm derselbe Adressblock auf zwei Websites dasselbe Administratorkonto ins Visier; auf einer davon wurden 101 Adressen dieses Blocks innerhalb von 24 Stunden gesperrt. Die anvisierten Konten sind echte Konten, er-

raten anhand des Firmennamens oder der E-Mail-Adresse.

Die Schweiz taucht unter den Herkunftsländern nicht auf. Eine Adresse oder ein Land bezeichnet keinen Täter; sie sagen, von wo aus die Maschine arbeitet.

Drei von sieben Websites hatten bereits einen Untermieter

Drei Websites beherbergten Schadcode, der lange vor unserer Ankunft installiert worden war. K-Shield hat alles entfernt und eine Kopie für die Analyse aufbewahrt.

| Website | Was gefunden wurde | Vorhanden seit | Wie es versteckt war | | --- | --- | --- | --- | | Industrielles KMU | 4 Hintertüren, 6 in WordPress eingeschleuste Loader, 88 veränderte Kerndateien, 1’056 gefälschte Spam-Seiten | spätestens November 2024 | Glaubwürdige Dateinamen, gefälschte Daten, verschlüsselter Inhalt. Die Spam-Seiten wurden nur Google ausgeliefert. | | Pressetitel | 2 Hintertüren | März 2025 | Zwei gefälschte WordPress-Dateien, echte Namen am falschen Ort. | | Lokales Geschäft | 2 Hintertüren | Juni 2022 | Die eine getarnt als Erweiterung «Hello Dolly» im Bilderordner, die andere als drei Zeilen im Theme. |

Zwei weitere PHP-Dateien in den Bilderordnern, eine davon seit 2017, wurden vorsorglich isoliert. Ein Bilderordner enthält kein Programm.

Was die Firewall nicht sah

Auf der Presse-Website lief Wordfence während der sieben Monate, in denen die beiden Dateien vorhanden waren. Es blockierte Angriffe. Es sah nicht, was bereits installiert war.

Das ist kein Vorwurf. Diese Dateien tragen keine bekannte Virensignatur. K-Shield hat sie auf andere Weise gefunden:

- **Es vergleicht jede Datei mit dem offiziellen Original.** Eine Datei, die in der veröffentlichten Version von WordPress oder der Erweiterung fehlt, ist verdächtig, unabhängig von ihrem Inhalt.
- **Es lehnt jedes Programm in den Bilderordnern ab.**
- **Es geht von einer verdächtigen Datei zu denen zurück, die sie laden.** Die sechs in WordPress eingeschleusten Loader wurden so gefunden und dann durch die Originale ersetzt.

Keine dieser Websites zeigte für ihre Inhaberin oder ihren Inhaber ein sichtbares Symptom.

Lesen Sie die Spuren

Jede Blockierung trägt einen Code, ein Datum, die Adresse, das Land und das anvisierte Konto. Jede entfernte Datei behält ihren Fingerabdruck und ihre Kopie. Man kann eine Woche später nachlesen, wer zugeschlagen hat, von wo aus, gegen welches Konto, und was K-Shield getan hat.

Die Karte am Anfang dieser Seite stammt von K-Shield und wird mit diesen Spuren gespeist: eine Blase pro Land, ihre Grösse folgt der Anzahl gesperrter Adressen. Sperren laufen ab; am 6. November um 15 Uhr waren auf den vier Websites noch 582 übrig.

Woher diese Zahlen stammen

Sie stammen aus der K-Shield-Konsole, die den Zustand jeder Website mehrmals täglich erhält. Es sind Mindestwerte:

- **Blockierte Anfragen:** Summe, Tag für Tag, des höchsten 24-Stunden-Zählers jeder Website. Dieser Zähler stoppt bei 500; er hat diese Obergrenze an 12 Website-Tagen erreicht.
- **Gesperrte Adressen:** seit der Inbetriebnahme der automatischen Sperrung Anfang November, auf 4 Websites. Eine Adresse, die auf zwei Websites gesperrt wurde, zählt doppelt.
- **Umfang:** 7 Websites, die zwischen Ende September und dem 6. November unter Überwachung kamen. Drei davon sind erst seit wenigen Tagen dabei.

Unsere eigenen Fehlalarme haben wir nicht als Erkennungen gezählt. Es gab welche; jeder wurde im Produkt behoben.

Für Ihre Website

Ein PHP-Update schliesst die Tür. Es sagt nicht, wer bereits drin ist. Wir beginnen damit, anzusehen, was auf Ihrer Website tatsächlich läuft, und überwachen sie anschliessend.

Den Sicherheitsstand meiner Website klären · PHP2Shell: die Lücke schliessen und das Weitere überwachen