WordPress マルウェア調査 – 実演レポート

Excel/CSV・既存システムの独立検証 ｜ tauridev

本レポートは 合成した検証用サイト に意図的な改ざんを仕込み、調査手順を実演したものです。顧客サイトのデータは使用していません。手法と報告様式をご確認いただくための見本です。

① 想定した感染の状況 ／ ② 実施した調査

「Google検索に外国語ページが大量にインデックスされ、身に覚えのない管理者ユーザーが存在する」という典型的なSEOスパム型改ざんを再現しました。原因の多くはプラグイン等の脆弱性を突いたファイル書き込みです。以下7種類の観点 を、サイトを一切実行せず（PHPを動かさず）テキストとして機械的に走査しました。

検査	観点	結果
T1	テーマ/プラグインへのコード注入（難読化実行）	1件 検出
T2	アップロード領域内のPHP（バックドア位置）	2件 検出
T3	身に覚えのない管理者ユーザー	1件 検出
T4	SEOスパム投稿（外国語ページの大量生成）	3件 検出
T5	.htaccess の不正リダイレクト	1件 検出
T6	コアファイルの改ざん（公式ハッシュ不一致）	1件 検出
T7	隠しPHPファイル	1件 検出

③ 検出結果（除去前）– 合計 10 件

件数は走査結果から機械的に算出しています（申告値ではありません）。各項目に証拠（ファイル:行 / SQL行）を添えます。なお検出したURLは、誤クリック防止のため hxxp[.] 表記に無害化しています。

種別	場所	証拠
T1	wp-content/themes/twentytwentyone/functions.php:5	@eval(base64_decode('REVNTy1JTkVSVDogdGhpcyBpcyBhIHN5bnRoZXRpYyBtYXJrZXIgZm9yIGEgc2Nhbm5lciBkZW1vLCBub3QgcmVhbCBjb2RlLiB
T2	wp-content/uploads/.ico.php:1	PHP file under wp-content/uploads
T2	wp-content/uploads/2024/07/settings.php:1	PHP file under wp-content/uploads
T3	db_dump.sql (SQL 4行)	administrator capability for login mailmag
T4	db_dump.sql (SQL 6行)	spam keyword in title; non-Latin title characters; suspicious guid host spam.example.invalid
T4	db_dump.sql (SQL 7行)	non-Latin title characters; suspicious guid host spam.example.invalid
T4	db_dump.sql (SQL 8行)	spam keyword in title; non-Latin title characters; suspicious guid host spam.example.invalid
T5	.htaccess:14	conditional line 13; external redirect to hxxp://spam[.]example[.]invalid/?
T6	wp-includes/version.php:1	SHA-256 differs from supplied core checksum
T7	wp-content/uploads/.ico.php:1	hidden PHP path component

④ 除去後の再検査 – なぜ「安全」と言えるのか

除去後のサイトを同じ7観点で再走査した結果 → 残存 0 件・エラー 0 件・SAFE

「駆除しました」という言葉ではなく、除去後の再走査が0件であることを安全の根拠とします。安全宣言は必ずこの再検査に紐づけ、7つの検査すべてが0件を返したときにのみ SAFE と表示します（1件でも残れば、または入力が読めなければ SAFE にはなりません）。

⑤ 今後の注意点 ／ この検査の限界（正直な範囲）

・本ツールはレビュー指標であり、感染の不存在を証明するものではありません。eval/assert＋base64、uploads内PHP（大文字拡張子含む）、別名の管理者などは検出しますが、関数名を文字列分割で組み立てる高度な難読化は検出せず、手動レビューに回します。
・実サイトでは走査の前に必ずバックアップを取得し、後に公式チェックサム（WordPress.org の正本）と突合します。
・再感染を防ぐため、原因となった脆弱なプラグイン/テーマの更新と、パスワード・認証情報の再発行をあわせて実施します。
