Как да оправите хакнат WordPress сайт

https://go359.com/bg/haknat-wordpress-site-p1488

Да откриете, че вашият WordPress сайт е хакнат или компрометиран, е изключително стресиращо. Менютата изчезват, акаунтите се променят, сайтът започва да пренасочва към порно или фармацевтични сайтове, изведнъж се появява съдържание на чужди езици, а понякога дори губите достъп до администрацията. И за капак – Chrome може да започне да показва голям червен екран, предупреждавайки посетителите ви, че сайтът ви е заразен. Това определено ще изплаши потенциалните ви клиенти.

Целта не е просто да възстановите сайта, а да го възстановите правилно, без да разпространите заразата.

Тази статия ще ви даде насоки как да подходите, за да възстановите сайта си. Стъпките изискват технически познания и ако нямате или не са ви достатъчно, обърнете се към нас или към друг WordPress специалист.

Стъпка 1: Запазете спокойствие

Знаем, че сте заети и имате много задачи. Всичко ще бъде наред и ще се справите.

Просто има недобросъвестни хора, които предпочитат да печелят пари по лесния начин и/или да подобряват класирането на своите или клиентски сайтове чрез хакове и недобри практики, вместо с реална работа, което създава стойност. Досадно е, но такива са нещата. Има всякакви хора.

Стъпка 2: Експортирайте сайта си (файлове + съдържание)

Преди да блокирате достъпа до сайта, свалете данните си.

Най-сигурният начин е чрез контролния панел на хостинга (cPanel, Plesk или подобен):

- Експортирайте копие на базата данни
- Архивирайте файловете на сайта, като архивирате и изтеглите цялата директория на сайта (обикновено това е public_html, htdocs, www или httpsdocs) в зависимост от контролния панел, който вашия WordPress хостинг ползва.

Ако не можете да използвате контролния панел по някакви причини:

- Използвайте плъгин за архивиране или миграция като UpdraftPlus или All-in-One WP Migration
- Или използвайте вградената опция на WordPress – Tools > Export – за да запазите поне публикациите и страниците си, картинките вероятно ще сочат към сайта.

Ако не сте чиствали WordPress сайт от вируси до сега, може би е добра идея да наемете опитен WordPress специалист. И ние можем да помогнем – просто ни пишете (платена услуга).

Важно: Ако имате няколко сайта в един и същи хостинг акаунт, знайте, че има вероятност и другите сайтове да са заразени, защото файловете от един сайт са достъни от всички други сайтове. Експортирайте и проверете всеки WordPres сайт поотделно.

По възможност направете експортирането по няколко различни начина, за да намалите риска от проблеми при архивите. Примерно ако единия архив е повреден, другите може да не са.

Стъпка 3: Блокирайте достъпа до хакнатия WordPress сайт

След като имате резервно копие файловете и данните, блокирайте достъпа до сайта. Това предотвратява както достъпа на хакерите, така и автоматичните WordPress задачи (WP Cron). Това ще намали шанса хостинга ви да блокира профила ви, защото дори и хакерите да се опитват да няма да стигнат да могат да контролират сайта.
… има обаче хакери, които качват файлове, които не зависят от WordPress и благодарение на двете блокирания по-долу те няма да могат да контролират сайта.

Две нива на бокиране на достъпа:

1. Блокирайте външния достъп чрез .htaccess

Добавете това като първи ред в .htaccess:

deny from all

Това спира всички външни заявки.

2. Спрете вътрешното изпълнение чрез wp-config.php

Отворете wp-config.php и веднага след <?php добавете:

```
if (php_sapi_name() !== 'cli' && !(defined('WP_CLI') && WP_CLI)) {
    header("HTTP/1.1 503 Service Temporarily Unavailable");
    header("Retry-After: 3600");
    die("Down for maintenance, please check back in an hour.");
}
```

Така:

- Уеб заявките получават правилно съобщение 503 + Retry-After, което казва на търсачките, че сайтът е временно в поддръжка.
- CLI сесиите (WP-CLI, PHP CLI) могат да продължат работа безопасно.

Комбинирано, това напълно „замразява“ заразения сайт, докато сте готови да го възстановите.

Стъпка 4: Възстановете сайта от чиста WordPress инсталация

Не преинсталирайте WordPress директно в същия заразен хостинг профил. Ако има вирус или троянски кон измежду файлове, новата ви инсталация ще бъде зарезена или атакувана почти веднага.

Не препоръчваме и да чистите сайта на вашия компютър, защото вируса може да се разпространи на други сайтове, над които работите или да изтрие важна информация от компютъра ви, особено ако сайтовете нямат добра изолация.

Вместо това инсталирайте сайта наново в сигурна среда, като например:

- Отделен (временен) WordPress хостинг, или
- Go359 или специалиирана услуга за staging WordPress сайтове, като qSandbox.com или WPSandbox.net

Оттам:

- Инсталирайте чиста версия на WordPress от wordpress.org
- Инсталирайте теми и плъгини само от оригинални източници (wordpress.org, официалния сайт на разработчика или доверени пазари като ThemeForest или Elegant Themes)

- Не използвайте старите папки на теми и плъгини от хакнатия сайт
- Импортирайте публикациите и страниците си
- Прегледайте съдържанието си за скрити спам връзки или зловреден код или ако има пренасочване.
- Добре е да сканирате файловете за вируси.

След като новият сайт е тестван и изглежда ок, можете да го прехвърлите обратно към основния си хостинг или към друг WordPress хостинг.

Стъпка 5: Защитете новия сайт

Преди отново да пуснете сайта онлайн, подсигурете инсталацията си.

- Обновете WordPress, темите и плъгините
- Сменете всички потребителски пароли и обновете security salts в wp-config.php
- Сменете паролите за хостинг панела и FTP профилите за всеки случай
- Активирайте двуфакторна автентикация (2FA) за администраторите
- Инсталирайте защитен плъгин като Wordfence или Sucuri
- Сканирайте сайта изцяло за остатъчен зловреден код
- Ограничете достъпа до wp-login.php (по IP адрес, ако е възможно)
- Изключете или блокирайте достъпа до XML-RPC файла, ако не е нужен

Многослойна сигурност

Най-добрата защита е защита на няколко слоя. Това означава, че не разчитате само на един инструмент, а изграждате защита на няколко нива:

- DNS защита (напр. Cloudflare блокира лошия трафик още преди да стигне до вашия сайт или сървър)
- Защитна стена (firewall) на хостинг ниво
- Защитна стена на сървъра (server firewall)
- Защитна стрена за уеб приложения (web firewall) (плъгини, като Wordfence, Sucuri и др.)

Представете си го като един катинар входната вратата в двора, катинар или греда на входната врата и също аларма в дома и един 1-2 питбула вътре в дома. Всяко от тези добавя допълнителна защита и затруднява достъпа.

Поддържайте плъгините, темите и WordPress обновен и с резервни копия

Повечето хакове идват от остарял софтуер. Превърнете обновяването в навик:

- Обновявайте редовно WordPress, темите и плъгините, но изчакайте малко 1-2 дни, защото при пускането на нови версии има вероятност за грешки и несъвместимости. Не всеки успява да си тества софтуера качествено.
- Премахвайте неизползвани разширения периодично
- Настройте автоматични резервни копия, съхранявайте ги на външна услуга и извън сървъра (Google Drive, Dropbox, Amazon S3 и др.)

Така, дори нещо да се обърка, ще можете бързо да се върнете към предишна версия.

За възстановяването всеки добър хостинг доставчик може значително да улесни възстановяването с дневни архиви, тестови среди и бърза поддръжка, но понякога и техните архиви могат да имат проблем.

Обновяване на Security Salts в wp-config.php

Освен смяната на паролите, е важно да обновите security salts в wp-config.php. Това са специални ключове, които WordPress използва, за да криптира потребителските сесии и “cookies” – с други думи, те осигуряват достъпа до администраторските профили.

Ако сайтът е бил компрометиран, нападателят може да има активни сесии, които ще останат валидни дори след смяна на паролата – освен ако не обновите salts. След смяната им всички активни логин сесии ще станат невалидни, и потребителите (включително хакерите) ще бъдат принудени да влязат отново с нова парола.

Как да регенерирате WordPress Salts

Има два начина да го направите:

1. Чрез WP-CLI:

Влезте в root директорията на вашия WordPress сайт и изпълнете:

wp config shuffle-salts

Тази команда автоматично ще генерира нови security keys и ще ги запише в wp-config.php.

2. Ръчно, чрез WordPress.org Salt Generator:

Отворете този официален адрес: https://api.wordpress.org/secret-key/1.1/salt/

Там ще видите нов набор от security ключове, например. Не ги копирайте от статията, а от линка по-горе. Всеки път ще генерира нови:

```
define('AUTH_KEY',         '#-.#-f}GjI#FOQxFa]p@,4Rc1QYUX g&D8yV>:k`F+X0SbE6 TiNbl-/gj
define('SECURE_AUTH_KEY',  '*x^dZjtc`;z-h-<6O}C-?O!E9QroKc8-:-i+kBM-nDMN`7ITtZ;2Hgd:
define('LOGGED_IN_KEY',    ']H,Is^,W}FF5pF!s/$c3f*0ARi<+Nd1?^dAM~%LKtd#b/(#k=J0 }Iv
define('NONCE_KEY',        '>`{YYK<S.t]@6;I-O9ml{(rvtRO6H6|823kF<+y+?()HHHd=TG63<V_
define('AUTH_SALT',        '|vL;@j0e]12IPwxD3qOK7muBjf|cZ|T;fEeV1*}v2KtWmMtwIV<fP$,tq;8
define('SECURE_AUTH_SALT', 'qf`4^qem0D`C<dSOI@}|ogSvqHhXQ0W~>O*LsFw`hy9]e#1Y
define('LOGGED_IN_SALT',   '=[h:%Bk,e2Jcgb?b8}b[Gfd|paQM<D7yCW?anVNBB!;25O##|w8;
define('NONCE_SALT',       'toAPX--)~.GTH+D$yD@j/oUks*vd]k;Y,TQ,-|y&{Ajv|t`FUEx!@&ri8@
```

Копирайте тези редове и ги поставете в wp-config.php, заменяйки старите.

Защо това е важно

- Принуждава всички потребители да се впишат наново (прекъсва потенциални сесии на нападатели).
- Изчиства всички сесии, кеширани токени и cookies, свързани с предишните ключове.
- Намалява риска от неоторизиран достъп, дори ако някой има стара парола или cookie.

Отговорност на хостинга и сигурността

В повечето случаи WordPress хостингът не е пряко виновен за хакването/заразяването, освен ако не сте на неправилно конфигуриран сървър, където сайтовете не са изолирани или вие сте си взели сървър, който не е менажиран и някой приятел или съсед ви го е настроил преди години и така си работят нещата с години.

Реалните причини обикновено са:

- Остарели или изоставени плъгини/теми

- Плъгини от непроверени източници нулирани плъгини и теми (nulled plugis/themes)
- Кликване на имейл, който е заразил компютъра и от там е хванал паролата за сайта (малко вероятно но е възможно).
- Слаби пароли или компрометирани акаунти

Ако разработчикът ви е дал изключително ниска цена за разработка на сайта може би е ползвал нулирани плъгини или теми ... за да спести някой лев или евро без да е помислил за проблемите, които ще дойдат от това лошо решение. Другата негативен резултат от ползването на нулирани плъгини и теми е, че създаването и поддържането на плъгини и теми отнема време и ресурси и така разработчика не си получава парите за труда, което афектира биснеса и възможността да поддържа продуктите си.

Стъпка 7: Стартирайте WordPress сайта и следете

След като сайтът е изчистен и защитен:

- Насочете домейна към новата инсталация
- Настройте ежедневни или седмични външни архиви с поне 30-дневно съхранение (например Hetzner Storage Box)
- Проверявайте редовно за подозрителни акаунти или промени по файлове
- Поддържайте всичко актуализирано

Финални мисли

Възстановяването на WordPress сайт от хакване или вируси може да изглежда като катастрофа, но не е краят на сайта ви. Ако останете спокойни, подсигурите данните си, блокирате заразения сайт, възстановите го в безопасна среда и засилите защитата, ще излезете от ситуацията по-опитни, търпеливи и уверени.

Ако всичко това ви се струва твърде сложно. Свържете се с нас. Ще направим всичко възможно да почистим сайта ви и да ви помогнем да го защитите за в бъдеще.

Go359 предлага доста защити от атаки и всеки сайт е изолиран. Ние също блокираме обичайните заявки и така намаляваме риска от заразяване.

П.П. Ако искате можете да разгледате нашата WordPress поддръжка в секцията ни услуги