علایمی که نشان میدهند سایت شما هک شده است و راه‌های مقابله با آن

چگونه از هک شدن سایت وردپرسی مطلع شویم؟

سایت وردپرسی شما ناگهان رفتارهای عجیبی از خود نشان می‌دهد؟ ترافیک سایت به شدت کاهش پیدا کرده یا قالب سایت تغییر پیدا کرده است؟ محتوای جدیدی روی سایت مشاهده کنید، در حالی‌که قادر نیستید به سایت لاگین کنید؟ برای همه این پرسش‌ها یک پاسخ شفاف و روشن وجود دارد. سایت شما هک شده و قربانی یک حمله هکری شده‌اید. هک شدن یک سایت موضوع پیچیده‌ای نیست و این اتفاق برای هر سایتی ممکن است رخ دهد. به‌طور مثال، سال گذشته تعدادی از سایت‌های دولتی هک شدند و حتی یکی از سایت‌های معروف حوزه فناوری در داخل کشور که در زمینه اخبار دنیای فناوری به فعالیت اشتغال دارد نیز هک شد. اما پرسشی که اکنون مطرح می‌شود این است: چگونه باید از هک شدن سایت خود اطلاع پیدا کنیم و پس از آگاهی یافتن چه کاری باید انجام دهیم؟

با توجه به اینکه **وردپرس** هنوز هم یکی از سامانه‌های مدیریت محتوای قالب در مقایسه با نمونه‌های مشابه به شمار رفته و طیف گسترده‌ای از سایت‌ها، ازجمله سایت‌های داخلی بر مبنای آن ساخته می‌شوند، در نتیجه جای تعجب نیست که مشاهده می‌کنیم هکرها به دنبال آن هستند تا **سایت‌های وردپرسی** را **هک** کنند. در حالی‌که افزونه‌های امنیتی مختلفی برای محافظت از سایت‌های وردپرسی در اختیار وب‌مسترها قرار دارند، اما باید به این نکته توجه داشته باشید که به‌کارگیری ابزارهای امنیتی هیچ‌گاه تضمین کننده این موضوع نیستند که شما تا ابد در امان خواهید بود. در نتیجه لازم است با یکسری نشانه‌هایی که خبر ازهک شدن سایت شما می‌دهند، آشنا باشید.

شماره یک، سایت شما کاملا ناآشنا به نظر می‌رسد

در قالب کار روزانه به عنوان مالک یک سایت یا وبلاگ وردپرسی وارد پانل مدیریتی می‌شود. تصمیم می‌گیرید پست جدیدی ارسال کرده، دیدگاه‌های قرار گرفته از سوی مخاطبان را بررسی کرده، اشتباه‌های تایپی متن‌ها را ویرایش کرده و کارهای این چنینی را انجام دهید. اما زمانی که سایت را مطابق روزهای قبل باز می‌کنید متوجه می‌شوید که سایت مثل روزهای قبل نیست و به نظر می‌رسد مشکلی وجود دارد. یکسری تغییرات بصری روی سایت رخ داده، لوگوی جدید، عکس‌های جدید و شاید محتوای غیرمتعارفی روی سایت شما قرار گرفته است. در صورتی که شما و کارمندان‌تان از تغییرات به وجود آمده بی اطلاع هستند. این نشانه‌ها می‌گویند که شما هک شده‌اید. به‌طور معمول فایل‌های قالب‌بندی نیز جایگزین شده‌اند (ممکن است این فایل‌ها نقطه ضعف امنیتی شما بوده‌اند) و به احتمال زیاد کدهای مخربی به سایت شما اضافه شده‌اند که به شکل محسوسی روی کارآیی سایت شما تاثیر منفی گذاشته‌اند.
زمانی که سایت شما **هک** می‌شود در کنار مواردی که به آن‌ها اشاره شد، نشانه‌های زیر نیز قابل تشخیص هستند:

- محتوایی نامناسب یا نامتعارف در زمان باز کردن سایت به نمایش در می‌آید.
- بخش فوتر سایت با لینک‌های جدیدی که به سایت‌های دیگر اشاره دارند، اشباع شده است.
- کدهایی به سایت شما اضافه شده که تنها از سوی خزنده‌های وب قابل خواندن بوده و روی کارآیی سایت و همچنین سئو سایت شما تاثیر منفی می‌گذارند. کدهایی که در ارتباط با سایت‌های ثالثی هستند که سایت‌های مدنظر

هکرها را فراخوانی کرده و به این شکل باعث کند شدن **سایت وردپرسی** شما می‌شوند.
• **هکر**ها ممکن است برای دسترسی به **سایت وردپرسی** شما فونت‌ها را به سرقت برده باشند.
زمانی که سایت شما از طریق کدهای مخربی هک شده باشد، این موضوع به سرعت از سوی ربات‌های گوگل شناسایی می‌شود. در اغلب موارد گوگل با پیغام خطایی این موضوع را به شما اطلاع می‌دهد.

مطلب پیشنهادی

پاسخ گویی به ابهامات بزرگ
۵ سوال بزرگ کاربران درباره امنیت فضای مجازی و جواب آن‌ها

شماره دو، شما نمی‌توانید به سایت لاگین کرده و به پانل مدیریتی دسترسی داشته باشید

ممکن است سایت شما در ظاهر خوب به نظر برسد، اما اگر به شکل ناگهانی متوجه شدید که دیگر نمی‌توانید به آن لاگین کنید با خود چه فکری می‌کنید؟ این مشکل معمولا دومین نشانه‌ای است که خبر از **هک شدن سایت** می‌دهد. (شکل 1)

در این حالت شما نه از طریق مرورگر وب و نه از طریق نسخه موبایلی **وردپرس** نمی‌توانید به پانل مدیریتی وارد شوید. اگر گذرواژه سایت خود را تغییر نداده‌اید و به شکل درستی همه کاراکترها را وارد کرده‌اید اما بازهم موفق نشده‌اید به سایت خود لاگین کنید، در این صورت به احتمال زیاد سایت شما هک شده است. هکرها در اغلب موارد حساب کاربری مدیریتی را حذف کرده یا به سادگی گذرواژه را تغییر می‌دهند تا مانع از آن شوند که شما دومرتبه به پانل مدیریتی وارد شده و همه چیز را به حالت قبل بازگردانید. درست است که هک مستقیم به ندرت رخ می‌دهد اما احتمال آن همواره وجود دارد. هک مستقیم بیشتر از طریق اسکریپت‌ها، افزونه‌ها یا کدهای مخربی که در قالب تم‌ها یا کدهای تبلیغاتی به اطلاعات شما دست پیدا می‌کنند، رخ می‌دهد.

شماره سه، ترافیک ورودی سایت ناگهان با افت شدید روبرو می‌شود

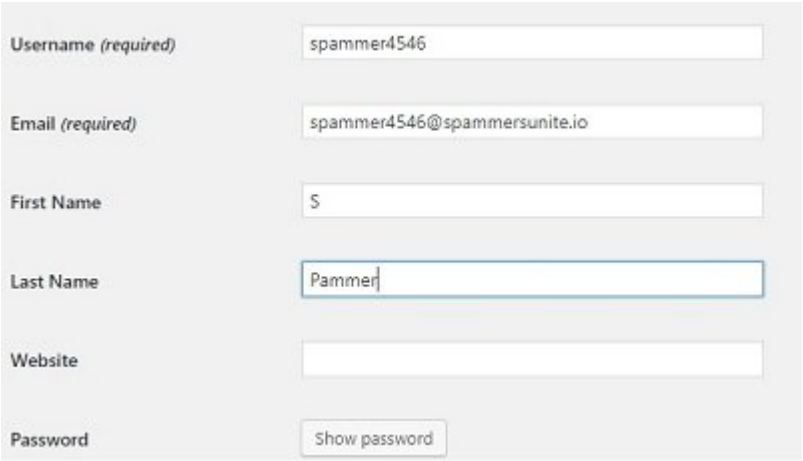
برخی از وب‌مسترها عادت دارند به جای لاگین کردن روزانه از یک برنامه به منظور بررسی تعداد ورودی‌های آی‌پی و بازدیدها استفاده کنند. نرم‌افزارهایی که برای این منظور مورد استفاده قرار می‌گیرند یکسری هشدارهای مشخص را نشان می‌دهد. این سامانه‌ها بیشتر بر تعداد بازدیدکنندگان سایت نظارت دارند. کاهش قابل توجه تعداد بازدیدکنندگان ممکن است به واسطه عدم علاقه کاربران به محتوا یا یک مشکل فنی رخ داده باشد. در چنین شرایطی ترافیک سایت کاهش پیدا می‌کند. اما به این موضوع توجه داشته باشید بدافزارهایی که وب‌سایت‌ها را هدف قرار می‌دهند در برخی موارد سعی می‌کنند بازدیدکنندگان سایت شما را به سمت سایت‌هایی که مدنظر **هکر**ها قرار دارد هدایت کنند. این‌کار از طریق تغییر مسیر به سایت دیگر که به آن Redirect URL گفته می‌شود انجام می‌شود. با توجه به این‌که حمله فوق کمی زمان‌بر است، کاربرانی که در سایت شما ثبت‌نام کرده‌اند، اغلب به سایت‌های مخرب هدایت نمی‌شوند، بلکه بازدیدکنندگانی که گاه‌و بی‌گاه به سایت شما مراجعه می‌کنند به سایت‌های دیگر هدایت می‌شوند. اما استمرار این موضوع باعث می‌شود تا ترافیک سایت شما به مرور کاهش پیدا کرده و همچنین سرعت سایت نیز کم شود.

شماره چهار، ایمیل‌های اسپم برای کاربران ارسال می‌شود

زمانی که بازدیدکنندگان در سایت شما ثبت نام کرده و عضو خبرنامه می‌شوند، آدرس‌های ایمیلی خود را در اختیارتان قرار می‌دهند. در اغلب موارد سایت‌ها به کاربران اجازه می‌دهند گذرواژه‌های خود را ریست کرده یا به بازتعریف مجدد ایمیل‌ها بپردازند. **هکر**ها می‌توانند از این قابلیت سوء استفاده کرده و پس از هک کردن سایت شما و دسترسی به بانک اطلاعاتی سایت ایمیل‌های مربوط به بازدیدکنندگان سایت را به دست آورده و در ادامه ایمیل‌های اسپم را برای بازدیدکنندگان سایت ارسال کنند. ایده‌ای که در پس‌زمینه این حمله قرار دارد مشخص است. **هکر**ها می‌خواهند بازدیدکنندگان سایت شما را متقاعد سازند تا به سراغ سایت‌های مدنظر آن‌ها بروند. پیام‌های ارسال شده برای کاربران ممکن است همراه با محتوای فریب‌دهنده‌ای باشد که اطلاعات شخصی نیز درون آن‌ها قرار گرفته است. تکنیکی که به نام حمله فیشینگ از آن نام برده می‌شود. در این پیام‌ها هکرها به کاربران وعده دریافت جوایز مختلفی را می‌دهند تا به این شکل اطلاعات شخصی کاربران سایت شما را به دست آورند. در اغلب موارد اسپم‌ها همراه با لینک‌های مخربی که پیشنهاد دانلود نرم‌افزارهایی را می‌دهند برای کاربران ارسال می‌شود.

شماره پنج، ساخت حساب‌های کاربری جدید بدون اطلاع شما

در کنار ایمیل‌های اسپم ارسال شده برای کاربران و قالب‌های سایت که بازطراحی شده و تغییر پیدا کرده‌اند، **هکر**هایی که وبلاگ‌ها و **سایت‌های وردپرسی** را هدف قرار می‌دهند، در اغلب موارد حساب‌های کاربری جدیدی را ایجاد می‌کنند. (شکل 2)



هکرها این کار را بدون آنکه سایت شما را به معنای واقعی کلمه هک کنند انجام می‌دهند تا به مزایای متعددی دست پیدا کنند. ساخت حساب‌های کاربری پیشرفته با بالاترین سطح مدیریتی به آن‌ها اجازه می‌دهد تا خود را به عنوان یکی از مدیران سایت شما معرفی کرده و از کاربران اطلاعات شخصی‌شان را دریافت کنند. در نتیجه همیشه ایده خوبی است که اطمینان حاصل کنید، حساب‌های کاربری بدون تایید شما ایجاد نمی‌شوند. با وجود این اگر متوجه

شدید حساب‌هایی بدون اطلاع شما ساخته شده‌اند، باید به وجود یک فرد ناشناس روی سایت خود مشکوک شوید.

مطلب پیشنهادی

اشتباهات رایج کاربران
۷ اشتباه امنیتی مرگ‌بار که احتمالا شما هم مرتکب می‌شوید

چگونه می‌توانیم مانع هک شدن سایت‌های وردپرسی شویم؟

تا این بخش از مقاله پنج نشانه‌ای را که خبر از هک شدن **سایت‌های وردپرسی** می‌دهند، به شما معرفی کردیم. اما برای مقابله با یک حمله **هکری** چه کاری می‌توانید انجام دهید؟ اگر نسخه‌های پشتیبان منظمی را تهیه کرده باشید، کار زیادی پیش رو نداشته و بازیابی محتوای سایت نیز به سادگی امکان‌پذیر است. در مرحله اول باید با مدیر هاست سایت خود تماس گرفته و در خصوص بازیابی گذرواژه و نام کاربری از او سوال کنید. در حالت کلی آن‌ها کل سایت شما را در قالب فرآیند حذف دسترسی هکرها و کدهای مخرب پاک می‌کنند. زمانی‌که این‌کار انجام شد، شما می‌توانید دومرتبه **وردپرس** را نصب کرده و داده‌های خود را بازگردانید. در مدت زمانی که مشغول انجام این‌کار هستید، باید پلاگین‌ها و قالب‌های سایت خود را بررسی کنید. در این بررسی باید کدهای غیر معمولی که ممکن است فرآیند هک کردن را تکرار کنند، شناسایی کرده و آن‌ها را ویرایش کنید. همچنین باید به فکر ساخت حساب‌های مدیریتی جدیدی باشید. ممکن است **هکرها** برای مدتی گذرواژه‌ها و نام‌های کاربری سطح مدیریتی را نگه دارند. پس بهتر است این حساب‌ها را پاک کنید.

مطلب پیشنهادی

بهبود ترافیک سایت
۵ افزونه جادویی وردپرس برای افزایش تعداد مخاطبان سایت

چگونه می‌توانیم از هک شدن سایت خود ممانعت به عمل آوریم؟

درست است که همواره احتمال هک شدن سایت‌ها وجود دارد اما با رعایت یکسری اصول این شانس را به دست می‌آورید تا به سادگی قربانی یک حمله **هکری** نشوید. برای این منظور پیشنهاد ما این است که اقدامات زیر را انجام دهید:

• باید نام کاربری پیش‌فرض Admin را تغییر داده و از یک گذرواژه قدرتمند استفاده کنید. این موضوع مختص به سایت‌ها نبوده و شما در ارتباط با هر وسیله هوشمندی که از آن استفاده می‌کنید باید نام کاربری و گذرواژه پیش‌فرض را تغییر دهید.

• فقط از پلاگین‌هایی که می‌شناسید و به آن‌ها اعتماد دارید استفاده کنید. پیش از به‌کارگیری پلاگین‌ها به دقت آن‌ها را بررسی کرده و سعی کنید از مخزن **وردپرس** در این زمینه استفاده کنید.

• سعی کنید از قالب‌های دزدی (قالب‌هایی که پولی هستند اما برخی از سایت‌ها مدعی می‌شوند به رایگان در اختیار شما قرار می‌دهند) استفاده نکرده و فقط قالب‌ها را از منابع معتبر دریافت کنید. فراموش نکنید قالب‌های به سرقت رفته‌ای که روی سایت خود نصب می‌کنید به احتمال زیاد روی سئو سایت شما تاثیر منفی می‌گذارند.

• همیشه **وردپرس**، پلاگین‌ها و قالب‌های خود را به‌روز نگه دارید.

• یک رویه پشتیبان‌گیری منظم را در دستور کار خود قرار دهید.

• یک پلاگین ورود رمزگذاری شده را نصب کنید تا فرآیند هک کردن سایت شما به سادگی امکان‌پذیر نباشد.

• سعی کنید عبارت Powered by WordPress را پنهان کنید. فایل footer.php به‌طور پیش‌فرض یکسری اطلاعات اولیه را که **هکرها** به دنبال آن‌ها هستند، در اختیارشان قرار می‌دهد.

در نهایت فراموش نکنید که همواره ترافیک سایت خود را از طریق پانل هاستینگ یا ابزارهایی از قبیل گوگل آنالیتیکس مورد بررسی قرار دهید. این‌کار به شما کمک می‌کند تا تغییرات و همچنین لینک‌های خارجی غیرمعمول قرار گرفته روی سایت خود را ردیابی کرده و بررسی کنید.

منبع:

makeuseof
wpglobalsupport
makeuseof

تاریخ انتشار:
29 اسفند 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/13942/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D8%B2-%D9%87%DA%A9-%D8%B4%D8%AF%D9%86-

%D8%B3%D8%A7%DB%8C%D8%AA-
%D9%88%D8%B1%D8%AF%D9%BE%D8%B1%D8%B3%DB%8C-
%D9%85%D8%B7%D9%84%D8%B9-%D8%B4%D9%88%DB%8C%D9%85%D8%9F