بسمه تعالی

کشف درب پشتی مخفی در ۳ افزونه Wordpress

تیم امنیت وردپرس به تازگی سه افزونه را به طور کلی از بخش افزونه های وب‌سایت های خود حذف نموده است. دلیل این عمل، کشف درب پشتی در کدهای این افزونه‌ها ذکر شده است. نام این افزونه ها را در جدول زیر مشاهده می فرمایید.در بررسی های صورت گرفته مشخص شده است که کد درب پشتی موجود در هر سه افزونه بسیار مشابه هم می باشد و در نهایت یک کار خاص و واحد را انجام میدهند.

ابتدا خود را به یک آدرس مشخص متصل می کنند و محتوای مورد نظر نفوذگر را در آدرس های سایت آلوده شده تزریق می کنند.کارشناسان امنیت بر این باورند که درب پشتی برای تزریق کدهای مخرب پنهان در صفحات HTML (لینک مخفی) در

نام پلاگین	تعداد نصب	نسخه دارای درب پشتی	توسعه دهنده	تاریخ حذف
Duplicate Page and Post	+۵۰,۰۰۰	۲.۱.۰	Cloud-wp.org	۱۴/۱۱/۲۰۱۷
No Follow All External Links	+۹,۰۰۰	۲.۱.۰	Cloude.wpserv.org	۱۹/۱۱/۲۰۱۷
WP No External Links	+۳۰,۰۰۰	۴.۲.۱	Wpconnect.org	۲۲/۱۱/۲۰۱۷

سایت های آلوده شده برای بهبود رتبه بندی موتور های جست‌جو(SEO) استفاده شده است.

کارشناسان wordfence متعقدند که احتمالا آلوده سازی این افزونه ها توسط یک نفر(یا تیم) انجام شده است و دلایل آن به شرح زیر بیان شده است:

۱- کد درب پشتی افونه اول و سوم به دو دامنه متفاوت که به یک سرور متصل شده اند داده ها را ارسال می کنند.
۲- شرکت فروشنده افزونه های اول و دوم مشابه است.
۳- درخواست خرید از طریق ایمیل که به صاحبان افزونه های دوم و سوم فرستاده می‌شود دارای یک الگوی مشابه است.
۴- تمام افزونه ها توسط کاربرانِ تازه ایجاد شده در wordpress.org قرار داده شده‌اند.
۵- کد درب پشتی هر سه افزونه شباهت ساختاری زیادی داشته است.

این اولین بار نیست که تیم Wordfence اقدام به اجرای یک عملیات بزرگ برای کشف افزونه های قدیمی دارای آسیب پذیری میکند. موارد بسیاری تا الان گزارش شده است که بسیاری از شرکت های فعال در ضمینه SEO و Backlink اقدام به خرید افزونه های قدیمی نموده و از آن‌ها برای تزریق کد های HTML افزایش بازدید استفاده می کنند. پیش از این نیز تیم Wordfence گزارشی درباره فرد بریتانیایی به نام Mason Soiza منتشر نمود که اقدام به خرید و درج درب پشتی در پلاگین های معروفی مانند Captcha ، Display widgets و ۳۰۱ to ۴۰۴ کرده است.