هجمات منظمة تستهدف مستخدمي وورد برس

حذرت شركتا "هوست غاتور" و"كلاود فلير" الأميركيتان المتخصصتان باستضافة المواقع الإلكترونية من حملة كبيرة منظمة يشنها قراصنة إنترنت ضد مستخدمي خدمة "وورد برس" لإنشاء المدونات، بهدف سرقة كلمات المرور والنفاذ إلى خوادم المستخدمين.

ويقول المحللون إن الهجمات تستهدف تحديدا مستخدمي اسم الحساب "أدمن" (Admin) الذي يضعه موقع وورد برس بشكل افتراضي للمستخدمين، ويشددون على ضرورة أن يتأكد المستخدم من أن اسم حسابه الحالي على وورد برس ليس "أدمن" وأنه يستخدم كلمة مرور قوية جدا.

ويشير تحليل شركة "هوست غاتور" إلى أن الهجوم منظم جدا وشديد التوزيع، كما أنها تعتقد بأن نحو تسعين ألف عنوان إنترنت (addresses IP) معرضة حاليا لخطر الاختراق، في حين عبر مؤسس شركة كلاود فلير، ماثيو برنس، عن اعتقاده بأن القراصنة المهاجمين يسيطرون على نحو مائة ألف "بوت" وهو عبارة عن برنامج ينفذ مهام مؤتمتة عبر الإنترنت، مما يشير إلى أن الهجوم يستهدف عمليا كل موقع يعتمد خدمة "وورد برس" على الشبكة.

ويسعى المهاجمون إلى الوصول إلى كلمات المرور لتحقيق هدف أكبر، وهو السيطرة على الخادم الذي يستخدمه أصحاب مواقع مدونات وورد برس، ويعتقد فريق شركة "كلاود فلير" -وفق موقع تك كرنتش المختص

بأخبار التكنولوجيا- أن المهاجمين يستخدمون حاليا شبكات من حواسيب منزلية بهدف بناء شبكة أوسع من الخوادم المرتبطة ببرامج "بوتنت" التي تتيح للأجهزة التواصل بينها لتأدية مهام معينة تحضيرا لهجوم مستقبلي أوسع.

ويرى موقع تك كرنتش أن الهجمات الحالية تشبه هجمات سابقة شنت عام 2012 على مواقع وورد برس أيضا، لكن تلك الهجمات استهدفت البحث عن إصدارات قديمة من برنامج "تيم ثمب" لتعديل قياس الصور والمستخدم بشكل افتراضي في العديد من قوالب وورد برس.

وينصح الموقع المستخدمين الذي يملكون مدونات يستضيفها موقع "وورد برس.كوم" تفعيل خيار المصادقة المزدوج لإضافة طبقة إضافية من الحماية، وكذلك اختيار كلمة مرور قوية، وتحميل عدد من إضافات وورد برس (Plugins) التي تحد من عدد مرات محاولات الولوج إلى المدونة من نفس عنوان الإنترنت أو الشبكة (IP address).