تحذير جديد سيفاجئ الملايين من مستخدمي "واتسآب"!

وسُلّط الضوء على عملية الاحتيال الجديدة لأول مرة من قبل خبير أمني كتب في مجلة فوربس. وحذر باحثا الأمن لويس ماركيز كاربينتيرو وإرنستو كاناليس بيرينا، من إمكانية حظر أي شخص من حسابه في غضون 36 ساعة.

ويمكن تنفيذ الهجوم حيث يمكن لأي شخص فعليا تثبيت "واتس آب" على جهازه وإدخال رقم هاتف محمول خاص بشخص آخر أثناء عملية إنشاء الحساب الأولي. وإذا قام شخص ما بذلك، فستتلقى نصوصا ومكالمات من "واتس آب" تعطيك رمزا مهما مكونا من ستة أرقام، مطلوبا لإكمال عملية الإعداد.

وما لم يتمكن أحد المتطفلين من إقناعك بإرسال هذا الرمز، فإن احتمالية تمكنه من تخمين ذلك شبه مستحيل. إذن ما سيحدث هو أن المهاجم سيحاول الدخول عبر هذا الرمز المهم، ويستمر في الفشل.

وتكمن المشكلة في أنه بعد عدد من المحاولات الفاشلة، سيوقف "واتس آب" مؤقتا عند إنشاء هذه الرموز.

وسيُعلم تطبيق الدردشة شخصا ما يحاول - ويفشل - إعداد "واتس آب"، أنه يتعين عليه "إعادة إرسال الرسائل القصيرة/الاتصال بي في غضون 12 ساعة".

وبعد انتهاء فترة الـ 12 ساعة هذه، يحتاج المهاجم إلى اتباع الطريقة نفسها كما كان من قبل، مرتين للتأكد من أن "واتس آب" يحظر إنشاء رموز إعداد جديدة. وخلال فترة الـ 12 ساعة الثانية، بينما لا يتم إنشاء رموز إعداد جديدة، يمكن للمهاجم إنشاء عنوان بريد إلكتروني مزيف والاتصال بدعم "واتس آب".

ويمكن للمخادع الشرير تقديم رقم هاتف الهدف، ويقول إن حسابه فُقد أو سُرق ويطلب إلغاء تنشيطه.

ويمكن لـ "واتس آب" بعد ذلك قفل الحساب، دون التحقق من أن الشخص الذي يتصل به عبر البريد الإلكتروني هو الشخص نفسه الذي لديه رقم الهاتف المقدم. وإذا انتظر المهاجم حتى تبدأ الدورة الثانية التي تبلغ مدتها 12 ساعة، فعندئذ في الوقت الذي يبدأ فيه المشارك الثالث في "واتس آب"، يبدو أنه ينهار.

وبدلا من إخبارك أنه يمكن إنشاء رموز إعداد جديدة في غضون 12 ساعة، يطلب "واتس آب" من المستخدم المحاولة مرة أخرى في أقل من ثانية واحدة.

وإذا تقدم الهجوم إلى هذه النقطة، وأرسل المهاجم رسالة إلى دعم "واتس آب" قبل الضحية، فسيواجه الهدف صداعا كبيرا في محاولة استرداد حسابه. وقال الباحثون في هذه المرحلة إن الوقت فات، وبدلا من التعامل مع نظام مساعدة آلي، سيتعين على الضحية محاولة تعقب شخص ما للتحدث معه شخصيا.

وفي حديثه عن التهديد، قال جيك مور من ESET: "هذا اختراق آخر مثير للقلق، يمكن أن يؤثر على ملايين المستخدمين الذين من المحتمل أن يتم استهدافهم بهذا الهجوم. ومع اعتماد الكثير من الأشخاص على "واتس آب" كأداة الاتصال الأساسية الخاصة بهم للعمل الاجتماعي، فمن المثير للقلق مدى سهولة حدوث ذلك".

وقال متحدث باسم "واتس آب" "إن توفير عنوان بريد إلكتروني مع عملية التحقق المكونة من خطوتين يساعد فريق خدمة العملاء لدينا في مساعدة الأشخاص في حالة مواجهة هذه المشكلة غير المحتملة في أي وقت. الظروف التي حددها هذا الباحث تنتهك شروط الخدمة الخاصة بنا ونحن نشجع أي شخص يحتاج إلى

المساعدة لإرسال بريد إلكتروني إلى فريق الدعم لدينا حتى نتمكن من التحقيق".

المصدر: إكسبريس