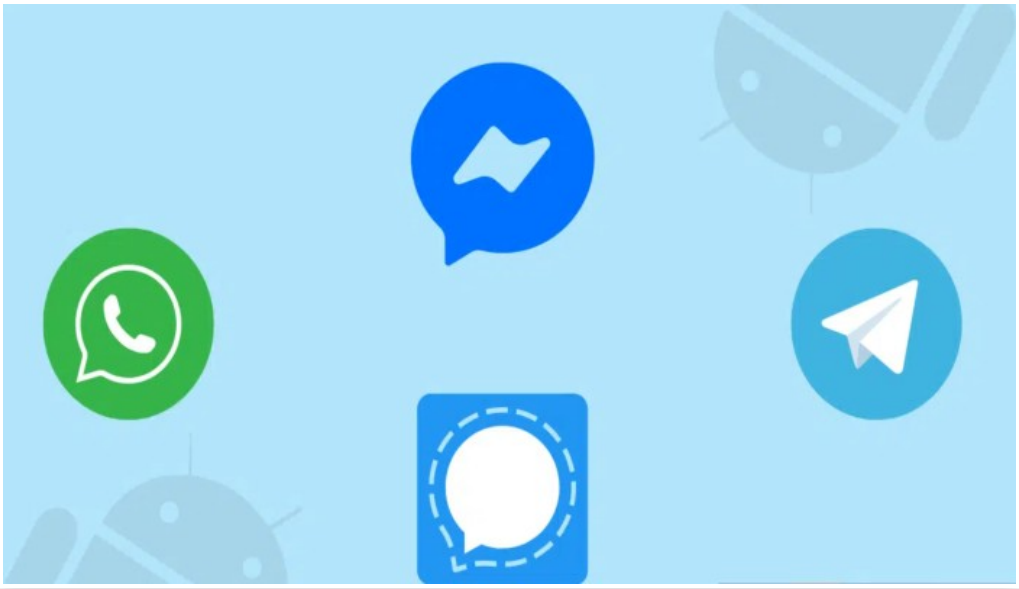
قراصنة يسرقون بيانات مستخدمي واتساب وتيليجرام بتطبيق دردشة وهمي



الثلاثاء 1 أغسطس 2023 04:36 م

اكتشف باحثو شركة أمنية أن مجموعة للقرصنة تستخدم تطبيقًا مزيفًا يُسمّى (سيف شات) SafeChat لإصابة الأجهزة العاملة بنظام التشغيل أندرويد ببرامج تجسس تسرق سجلات المكالمات، والرسائل النصية، ومواقع GPS من الهواتف.

ويُشتبه في أن برامج التجسس المستخدمة هي إحدى أنواع برنامج Coverlm الذي يسرق البيانات من تطبيقات الاتصالات، مثل: تيليجرام، وسيجنال، وواتساب، وفايبر، وفيسبوك مسنجر.

ويقول باحثو شركة CYFIRMA إن مجموعة قراصنة (التهديد المتقدم والمستمر) APT الهندية Bahamut تقف وراء الحملة، وقد نفّذوا هجماتهم الأخيرة بدرجة أساسية من خلال رسائل التصيد الاحتيالي في واتساب التي ترسل الحمولات الضارة مباشرة إلى الضحية.

ويسلط باحثو الشركة الأمنية الضوء أيضًا على العديد من أوجه التشابه في التكتيكات والتقنيات والإجراءات مع مجموعة تهديد أخرى ترعاها الدولة الهندية، وهي: DoNot APT أو APT-C-35، التي سبق أن غزت متجر (جوجل بلاي) بتطبيقات الدردشة المزيفة التي تعمل كبرامج تجسس.

وفي أواخر العام الماضي، ذكرت شركة أمن المعلومات (إسيت) ESET أن مجموعة Bahamut كانت تستخدم تطبيقات مزيفة للشبكات الافتراضية الخاصة VPN لنظام أندرويد تضمنت وظائف برامج التجسس الواسعة النطاق.

وفي أحدث حملة رصدتها CYFIRMA، وجدت الشركة أن مجموعة القرصنة تستهدف أفرادًا في جنوب آسيا.

ومع أن CYFIRMA لم تتعمق في تفاصيل جانب الهندسة الاجتماعية للهجوم، فمن الشائع إقناع الضحايا بتثبيت تطبيق دردشة بحجة نقل المحادثات إلى منصة أكثر أمانًا.

وأفاد المحللون أن SafeChat يتميز بواجهة خادعة تجعله يبدو وكأنه تطبيق دردشة حقيقي وهو أيضًا يأخذ الضحية من خلال عملية تسجيل تبدو مشروعة تضيف نوعًا من المصداقية، وتعمل كغطاء ممتاز لبرامج التجسس.

ومن بين الخطوات الحاسمة في إصابة الضحايا الحصول على أذونات لاستخدام خدمات إمكانية الوصول، التي يُساء استخدامها لاحقًا لمنح برامج التجسس مزيدًا من الأذونات تلقائيًا.

وتتيح هذه الأذونات الإضافية لبرامج التجسس الوصول إلى قائمة جهات اتصال للضحية، والرسائل النصية، وسجلات المكالمات، وذواكر التخزين الخارجية، والحصول على بيانات موقع GPS الدقيقة من الجهاز المصاب.

ويطلب التطبيق أيضًا من المستخدم الموافقة على استبعاده من نظام تحسين البطارية في أندرويد، الذي يُستخدم لإنهاء العمليات في الخلفية عندما لا يتفاعل المستخدم بنشاط مع التطبيق.

وتختتم CYFIRMA التقرير بالقول إن التطبيق يحتوي على أدلة كافية لربط مجموعة Bahamut بالعمل نيابة عن حكومة ولاية معينة في الهند.