برمجية خبيثة في أندرويد تسرق النسخ الاحتياطية لواتساب

الثلاثاء 20 يونيو 2023 02:18 م

كشفت شركة ESET المتخصصة في مجال الأمن السيبراني عن وجود برمجية خبيثة في أجهزة أندرويد تسرق بيانات حساسة من أجهزة المستخدمين، ومن ذلك النسخ الاحتياطية لتطبيق واتساب

وقالت ESET إن هناك تطبيقين للمحادثة يسميان BingeChat و Chatico يحتويان على برمجية تُسمى GravityRAT تنتمي إلى البرمجيات الخبيثة من نوع حصان طروادة "تروجان" أو "Remote Access Trojan" – تُعرف اختصارًا باسم RAT – وهي تتيح للمخترق التحكم في جهاز الضحية عن بُعد، وفقًا لموقع aitnews .

وأضافت ESET أن تلك البرمجية لها القدرة على استخراج الكثير من المعلومات الحساسة من الأجهزة المخترقة، مثل سجلات المكالمات، وقائمة جهات الاتصال، ورسائل SMS، وموقع الجهاز، ومعلومات الجهاز الأساسية، والملفات ذات الامتدادات المحددة كالصور والمستندات

وما يميز تلك البرمجية قدراتها الإضافية على سرقة النسخ الاحتياطية لتطبيق واتساب، واستقبال الأوامر لحذف الملفات

ولا يوجد التطبيقان السابق الإشارة إليهما على متجر جوجل بلاي، كما لم يجرِ رفعهما على المتجر في أي وقتٍ مضى، وقد انتشرا نظرًا إلى إقدام المستخدمين على تحميلهما من مواقع خارجية

وأوضح الباحثون الأمنيون في ESET أن البرمجية الخبيثة مصممة لاستهداف الضحايا ضمن نطاق جغرافي محدد استنادًا إلى عنوان الجهاز "IP Address"، وأشارت البيانات التي حصلت عليها الشركة إلى أن معظم الضحايا كانوا من الهند

ونسبت شركة ESET الهجوم السيبراني من برمجية GravityRAT إلى مجموعة من المخترقين المحترفين، الذين يُعرفون باسم SpaceCobra، وهم على الأرجح من باكستان، وفقًا للشركة

وأكد الباحثون أن الهجوم بدأ في أغسطس، وأن تطبيق BingeChat المُصاب لا يزال نشطًا حتى الآن

وقد بُني التطبيق المصاب اعتمادًا على تطبيق آخر يُسمى OMEMO، وهو تطبيق محادثة مفتوح المصدر متوفر على أنظمة تشغيل مختلفة

ويُنصح دومًا بتجنب تحميل أي تطبيقات أو ألعاب من خارج متجر جوجل بلاي لضمان عدم إصابة الجهاز بأي برمجيات خبيثة