تهديد خطير يعرّض هواتف أندرويد للخطر

وضع أصحاب الهواتف الذكية التي تعمل بنظام أندرويد، مرة أخرى، في حالة تأهب قصوى بعد اكتشاف برنامج تجسس للهواتف الذكية عرض البيانات الشخصية لمئات الآلاف من المستخدمين للخطر، مثل سجلات المكالمات والتسجيلات والرسائل النصية والصور وسجل التصفح والمواقع الجغرافية الدقيقة، وفقا لتقرير صادر عن TechCrunch.

واكتشف موقع TechCrunch المشكلة الأمنية كجزء من تحقيق أوسع في برامج التجسس الخاصة بالمستهلكين، حيث يمكن لهذه التطبيقات، التي يتم تسويقها على أنها مخصصة لتتبع أو مراقبة الأطفال، تزويد الهواتف الذكية التي تعمل بنظام التشغيل أندرويد ببرامج أخرى ضارة تسمى Stalkerware.

ووفقا للتقرير فإن برامج Stalkerware الضارة، والتي تأتي مصممة ليتم تشغيلها خلسة في خلفية الهواتف الذكية، تعمل على تسجيل كل ما يفعله المستخدم على الهاتف لقدرتها على تتبع الأشخاص ومراقبتهم دون موافقتهم.

ورفض موقع "TechCrunch"، ذكر اسم التطبيقات المحملة بالبرامج الخبيثة، وقائلا: "لا يمكننا تسمية برنامج التجسس أو مطوره لأنه سيسهل على الجهات السيئة استغلال المشكلة والوصول إلى البيانات الغير آمنة".

وتقوم برامج Stalkerware الخبيثة، بالتجسس على المستخدم بهدوء بمجرد تثبيتها على جهاز الضحية، بسحب المحتويات المحفوظة على الهاتف باستمرار مما يسمح لمشغلها بتتبع مكان الشخص والأشخاص الذين يتواصلون معهم، دون أن يدرك المستخدم أن هاتفه تعرض للاختراق، لأن هذه التطبيقات مصممة لتختفي من الشاشات الرئيسية لتجنب الاكتشاف أو الحذف.

وتترك البرمجيات الخبيثة بيانات مئات الآلاف من الأشخاص معرضة للخطر، حيث تقوم برامج stalkerware بسحب سجلات المكالمات والرسائل النصية والصور وسجل التصفح والمواقع الجغرافية الدقيقة وتسجيلات المكالمات من هاتف الضحية.

ويرسلها الجهاز في إدخالها يتم التي البيانات تسجل التي الضارة البرامج من نوع هو Stalkerware إلى جهة خارجية يتم توفيرها عند تثبيته. يعمل Stalkerware دون علم الضحية بأنه يقوم بجمع معلوماتها ؛ على هذا النحو ، يعد خرقا للخصوصية ويعتبر برنامجا غير مرغوب فيه.

يمكن لـ Stalkerware تتبع أنواع مختلفة من المعلومات. على سبيل المثال ، يمكنه مراقبة رسائل SMS الخاصة بالضحية ، بينما يقوم الآخر بنقل معلومات الهدف إلى من قرر التجسس عليها. على هذا النحو ، يتغير تصميم كل Stalkerware بناء على ما تم تصميمه لتتبعه.