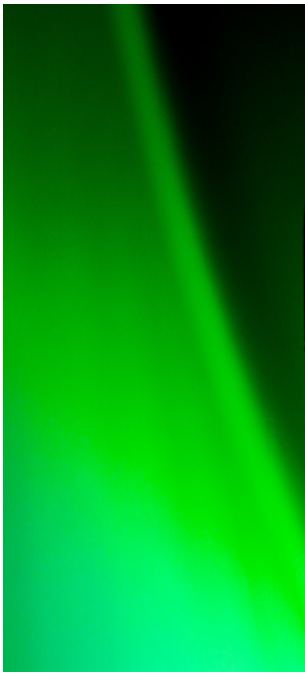
احذر منها... تطبيقات مزيفة على متاجر خارجية تصيب ملايين أجهزة أندرويد



يتمثل أحدث تهديد يواجه مستخدمي هواتف أندرويد فى خداعهم لتثبيت تطبيقات معينة تُسبب مشاكل بمجرد تنزيلها على أجهزتهم، ويُطلق على هذا الهجوم اسم "Kaleidoscope"، وهو هجوم احتيالي بالإعلانات، حيث تتوفر تطبيقات شرعية في متجر جوجل بلاي.

ووفقًا لما ذكره موقع "arena Phone"، فإنه:"توجد نسخ خبيثة لهذه التطبيقات في متاجر تطبيقات تابعة لجهات خارجية، تُساهم في الإعلانات الاحتيالية".

وأطلقت مختبرات Labs Threat IAS على هذا الهجوم اسم Kaleidoscope لأنه يتغير باستمرار لتجنب الكشف.

ووفقًا للبيانات، يتم اختراق "2.5" مليون جهاز جديد كل شهر، ويوجد 20% منها في الهند، وتشمل المناطق الأخرى التي تم اكتشاف Kaleidoscope فيها إندونيسيا والفلبين والبرازيل.

ويؤدي تثبيت التطبيقات الخبيثة عبر واجهات متاجر تطبيقات تابعة لجهات خارجية إلى اتساع نطاق هذا التهديد.

يعمل Kaleidoscope على النحو التالي:

يُثبت مستخدم أندرويد تطبيقًا من متجر بلاي يبدو ويعمل كتطبيق شرعي.

يتم إدراج نسخة مكررة خبيثة من التطبيق في متجر تطبيقات تابع لجهة خارجية؛ تُوجِّه الرسائل ووسائل التواصل الاجتماعي المستخدمين إلى تثبيت الإصدارات الضارة من هذه التطبيقات عبر متاجر تطبيقات خارجية، مع تثبيتها مباشرةً.

يعتقد مالك جهاز أندرويد أنه ثبّت تطبيقًا شرعيًا، ويعتقد المعلنون أن إعلاناتهم تُعرض على تطبيقات شرعية.

بدلًا من ذلك، بمجرد تثبيت الإصدار الخبيث من التطبيق على الهاتف، يعرض إعلانات مزعجة، تتضمن صورًا ومقاطع فيديو بملء الشاشة لا تتطلب أي تفاعل من المستخدم لتشغيلها.

ويمكنك أن ترى مدى إزعاج هذا لأصحاب الأجهزة غير المحظوظين الذين ينتهي بهم الأمر بامتلاك هاتف يمنح أموالًا طائلة لمجرمي الإنترنت ويمنع المستخدمين من عرض شاشاتهم.

وأزالت جوجل التطبيقات المُعلَّمة من متجر Play، وأضافت الشركة أنها ستحمي مستخدمي أندرويد من الإصدارات المعروفة من Kaleidoscope.

ويتسبب هذا النوع من البرامج الإعلانية الخبيثة في ارتفاع درجة حرارة الهاتف، واستنزاف البطارية بسرعة، وبطء الجهاز في العمل مع أداء بطيء.