تطبيق سبّب تحديثه الضرر بعشرة ملايين مستخدم..وخبراء الأمن السيبراني يحذّرون!

وبدأ خبراء الأمن السيبراني في MalwareBytes في نهاية العام الماضي في تلقي تقارير حول تطبيق Barcode Scanner من LAVABIRD LTD، والذي وقع تحميله أكثر من 10 ملايين مرة.

وأبلغ المستخدمون الذين قاموا بتنزيل التطبيق، أن الإعلانات كانت تفتح على المتصفح الافتراضي على جهاز أندرويد الخاص بهم بشكل مفاجئ من العدم.

وتلقت مؤسسة MalwareBytes بلاغا مفاده أن الجاني المخالف هو تطبيق Android Scanner Barcode.

ووقع حذف التطبيق من متجر "غوغل بلاي" (Play Google) بعد قيام MalwareBytes بإخطار شركة LAVABIRD LTD.

وتم اكتشاف أن التطبيق، الذي يبدو أنه ظل غير ضار لسنوات، تحول إلى آخر "ممتلئ بالبرامج الضارة" بعد التحديث.

وكشف خبراء MalwareBytes عن التهديد في منشور عبر الإنترنت: "في حالة Scanner Barcode، تمت إضافة شيفرة ضارة لم تكن موجودة في الإصدارات السابقة من التطبيق. علاوة على ذلك، استخدمت الشيفرة المضافة التعتيم الشديد لتجنب الكشف".

وفي دراستهم، شارك MalwareBytes أيضا مقطع فيديو قصيرا يظهر الشيفرة المشبوهة أثناء العمل.

وأبلغ المستخدمون بأن التحديث الجديد للتطبيق يشغل الإعلانات غير المرغوب فيها في المتصفح من العدم، ويتجه المتصفح إلى صفحة بريد عشوائي بها إعلان مزعج يحاول حمل المستخدم المستهدف على تنزيل تطبيق ما.

وإذا قمت بتنزيل Scanner Barcode مسبقا، فإن MalwareBytes تنصح بإزالة التطبيق يدويا.

بدلاً من ذلك ، إذا كان لديك ماسح ضوئي للبرامج الضارة على هاتف Android الخاص بك، فيجب أن يكون قادرًا على اكتشاف التهديد.

وأضافت MalwareBytes: "من الصعب معرفة المدة التي قضاها Scanner Barcode في متجر غوغل بلاي كتطبيق شرعي قبل أن يصبح ضارا. واستنادا إلى العدد الكبير من عمليات التثبيت وتعليقات المستخدمين، نشك في وجوده منذ سنوات. إنه لأمر مخيف أنه مع تحديث واحد يمكن أن يتحول أحد التطبيقات إلى ضار أثناء خضوعه لرادار Protect Play Google. مطور التطبيق الذي يمتلك تطبيقا شائعا سيحوله إلى برامج ضارة. هل كان هذا هو المخطط طوال الوقت؟، أن يكون التطبيق في وضع الخمول، في انتظار الإضراب بعد أن يصل إلى الشعبية؟ أعتقد أننا لن نعرف أبدا".

المصدر: إكسبريس