

غوغل تحذر من تطبيق أندرويد شائع يستهدف أموال المستخدمين



تعبيرية

وكالات - الإمارات 71
تاريخ الخبر: 2022-11-24

حذرت غوغل (Google) هذا الأسبوع من استهداف المستخدمين بتهديد جديد قد يداهم أرصدهم المصرفية.

وتم تحذير مستخدمي أندرويد (Android) من أن هواتفهم قد تكون هدفا للمتسللين في حالة استخدامهم لتطبيق مشهور، تم حظره مؤخرًا من قبل غوغل، ويستخدم تكتيكًا متسترًا لتثبيت برنامج شاركبوت (Sharkbot) الضار، فإذا قمت بتنزيله من متجر غوغل بلاي (Play) فيجب حذفه الآن.

وفقًا لفريق الأمان في تطبيق بتفيندر (Bitdefender) -وهو برنامج مضاد للفيروسات مطور

من طرف شركة سوفتوين والتي مقرها رومانيا- فإن التطبيق المسمى إكس- فايل مانجر (X-File Manager) قادر على تجنب قواعد غوغل الصارمة من خلال عدم عرض أي شيء يثير الشبهات عند الظهور على "غوغل بلاي".

في الواقع، كان التطبيق يعمل كما هو معلن عنه، ولم يعلم أي شخص عن المشاكل التي قد يتسبب بها.

حيث إنه بمجرد التثبيت على الجهاز، تظهر رسالة منبثقة على الشاشة تحذر من أن التطبيق يحتاج إلى تحديث حيوي. وبدلاً من أن تأتي هذه الترقية عبر "غوغل بلاي" الرسمي، يتم نقل مالكي الهواتف إلى مواقع ويب تابعة لجهات خارجية حيث يتم بعد ذلك إدخال البرامج الضارة مباشرة على الجهاز.

باستخدام هذا التكتيك المسمى القطار "دروبر" (Dropper) من غير المرجح أن تكتشف غوغل التطبيق الخطير أو تزيله من متجرها.

وقد شرح بتفيندر المزيد عن هذا التهديد "عند تنزيل تطبيق على غوغل بلاي من المحتمل أن يكتشف غوغل وجود برمجية خبيثة في التطبيق، لذلك يلجأ المجرمون إلى المزيد من الأساليب المخادعة. إحدى الطرق هي استخدام تطبيق، يكون شرعياً مع بعض الميزات المعلن عنها، وبعدها يقوم التطبيق بإغراء المستخدمين بالمزيد من الميزات كالقطار التي تضيف المزيد من البرامج الضارة الخبيثة على دفعات".

ويعتقد أن إكس- فايل مانجر تم تنزيله أكثر من 10 آلاف مرة، مع وجود غالبية عمليات التثبيت في المملكة المتحدة.

وإذا كنت تعتقد أنك قد تكون أحد الأشخاص غير المحظوظين الذين تم خداعهم ، فيجب عليك إزالة التطبيق دون تأخير لأن هاتفك قد يكون مصاباً بـ "شارك بوت" وهذا قد يعني أن حسابك المصرفي في خطر.

هذا البرنامج الضار "الشريز" قادر تمامًا على سرقة التفاصيل المصرفية عن طريق تركيب نوافذ تسجيل دخول مزيفة، واعتراض البيانات بما في ذلك رسائل "إس إم إس" (SMS). وبمجرد أن تصبح هذه البيانات في أيدي المتسللين، يمكن استخدامها لسرقة الأموال وإجراء المعاملات دون إذن المالك.

وأضاف بتفيندر "هناك سمة شائعة لاحظناها الأشهر القليلة الماضية وهي التطبيقات الضارة القادمة مباشرة من متجر غوغل بلاي" ويقول أيضا "إذا جاء شيء ما من متجر رسمي، فقد يميل الناس إلى الاعتقاد بأنه آمن. وقد أظهر بحثنا أن هذا غير صحيح، عدة مرات".

وكدليل، وقبل تنزيل أي تطبيقات، من الجيد التحقق من التعليقات والبحث عن التعليقات السلبية.

وبمجرد التثبيت، كن حذرًا بشأن تحديث التطبيق خاصةً إذا بدأ التطبيق في توجيهك إلى مواقع الويب التي ليس لها ارتباط بمتجر غوغل بلاي.



UAE71NEWS