رصد تطبيقات أندرويد خبيثة نُزِّلت مليوني مرة من جوجل بلاي

الثلاثاء 6 ديسمبر 2022 02:07 م

تسللت مجموعة جديدة من التطبيقات الضارة، والتطبيقات الدعائية، وتطبيقات التصيد الاحتيالي المخصصة لنظام أندرويد، إلى متجر جوجل بلاي، وتمكنت من خداع أكثر من مليوني مستخدم لتثبيتها.

وكانت خدمة مكافحة الفيروسات Dr. Web هي من اكتشفت التطبيقات، وقالت إن التطبيقات تظاهرت بأنها أدوات مساعدة مفيدة ومحسنة لأداء النظام، ولكنها كانت على العكس من ذلك.

وقالت Dr. Web إن واحدًا من التطبيقات التي اكتشفتها هو تطبيق TubeBox، الذي جمع ميلون تنزيل، ويبدو أنه حُذف من متجر التطبيقات حديثًا.
ويَعِدُ TubeBox المستخدمين بمكافآت مالية مقابل مشاهدة مقاطع الفيديو والإعلانات على التطبيق، ولكنه لا يفي بوعوده ألبتة، فهو يعرض أخطاء مختلفة حين محاولة استرداد المكافآت التي جمعها المستخدمون. أما المستخدمون الذين يُكملون حتى خطوة السحب النهائية، فإنهم لا يتلقون الأموال، ويُعتقد أن الأمر لا يعدو كونه خدعة لمحاولة الاحتفاظ بالمستخدمين لأطول مدة ممكنة على التطبيق، ومشاهدة الإعلانات وتحقيق إيرادات للمطورين.
أندرويد جوجل بلاي

وذكرت Dr. Web من تطبيقات أندرويد الدعائية الأخرى التي ظهرت على متجر جوجل بلاي في شهر تشرين الأول/ أكتوبر الماضي، ولكنها أُزيلت منذئذ، تطبيق Bluetooth device auto connect الذي نُزِّل مليون مرة، وتطبيق Bluetooth & Wi-Fi & driver الذي نُزِّل 100 ألف مرة، وتطبيق Volume, Music Equalizer الذي نُزِّل 50 ألف مرة، وتطبيق Fast Cleaner & Cooing Master الذي نُزِّل 500 مرة.

وتتلقى هذه التطبيقات أوامر من Firebase Cloud Messaging، منصة الإشعارات والتراسل العابرة للمنصات والتابعة لشركة جوجل، وتُحمِّل التطبيقات مواقع الويب المحددة في هذه الأوامر، مما يؤدي إلى ظهور إعلانات احتيالية على الأجهزة المصابة.

وفي حالة تطبيق Fast Cleaner & Cooling Master، الذي يمتاز بصغر حجمه، فإنه يمكن للمشغلين عن بُعد تكوين الجهاز المصاب ليعمل بوصفه خادمًا وكيلًا يسمح لجهات التهديد الفاعلة بتوجيه حركة المرور الخاصة بهم عبر الجهاز المصاب.
واكتشفت Dr. Web مجموعة من تطبيقات الاحتيال المتعلقة بالقروض التي تدعي أن لها علاقة مباشرة بالمصارف الروسية ومجموعات الاستثمار، إذ يبلغ معدل تنزيل كل منها 10,000 مرة على متجر جوجل بلاي.

وقد رُوِّج لهذه التطبيقات عبر إعلانات خبيثة في تطبيقات أخرى، تَعِد بأرباح استثمارية مضمونة. وفي الواقع، تأخذ هذه التطبيقات المستخدمين إلى مواقع التصيد حيث تُجمع معلوماتهم الشخصية.

وللحماية من التطبيقات الاحتيالية على متجر جوجل بلاي، يُنصح المستخدمون بالتحقق دائمًا من التعليقات السلبية، وفحص سياسة الخصوصية، بالإضافة إلى زيارة موقع المطور لتقييم مصداقيته. وبصورة عامة، يُنصح الجميع بمحاولة الاحتفاظ بعدد التطبيقات المثبتة على الجهاز عند الحد الأدنى والتحقق دوريًا من تفعيل ميزة الحماية Google Play Protect.