FlixOnline يستخدم واتساب لإصابة المستخدمين

الجمعة 9 أبريل 2021 06:14 م

تم اكتشاف برمجية ضارة جديدة لنظام التشغيل أندرويد مخفية ضمن تطبيق يسمى FlixOnline متاح عبر متجر Google Play.
وتنتشر البرمجية الضارة عن طريق الردود التلقائية الضارة على رسائل واتساب المرسلة إلى المستخدم، ويتم تلقي البرمجية الضارة من خادم تحكم وأوامر عن بُعد.
ويقول باحثو الأمن من Check Point: إن التهديد الجديد والمبتكر يمكن أن يرسل المزيد من المحتوى الضار عبر الردود الآلية على رسائل واتساب الواردة.
ويمكن للقراصنة استخدام البرمجية الضارة لتوزيع هجمات التصيد الاحتيالي أو نشر برمجيات ضارة إضافية أو نشر معلومات خطأ أو سرقة بيانات تسجيل الدخول والبيانات من حسابات واتساب والمحادثات.
ويتنكر تطبيق FlixOnline كخدمة تتيح للمستخدمين عرض محتوى Netflix من جميع أنحاء العالم عبر الأجهزة المحمولة.
وبدلاً من القيام بما يعد به، تراقب البرمجية الضارة إشعارات واتساب لإرسال ردود تلقائية وتلقي المحتوى من خوادم التحكم الخاصة بها.
وتوفر رسالة البرمجية الضارة التي يتم إرسالها إلى الضحايا عبر الردود التلقائية للمستخدمين شهرين من محتوى Netflix المتميز المجاني دون أي تكلفة في أي مكان في العالم.
ويقول باحثو Check Point: عند تنزيل تطبيق FlixOnline وتثبيته عبر أجهزة أندرويد، فإنه يبدأ خدمة تطلب أذونات التراكب وتجاهل تحسين البطارية والإشعارات.
وبعد الحصول على هذه الأذونات، تكون البرمجية الضارة قادرة على إنشاء نوافذ جديدة فوق التطبيقات الأخرى، التي عادةً ما تكون شاشات تسجيل دخول مزيفة للتطبيقات الأخرى لسرقة بيانات تسجيل الدخول.
ويؤدي تجاهل تحسينات البطارية إلى منع البرمجية الضارة من التوقف عن طريق روتين تحسين البطارية داخل الجهاز حتى في حالة الخمول.
ويسمح الوصول إلى الإشعارات للبرمجية الضارة بالوصول إلى جميع الإشعارات المتعلقة برسائل الجهاز ورفض الرسائل والرد عليها تلقائيًا عبر الجهاز.
وباستخدام هذه الأذونات، تمتلك البرمجية الضارة كل ما تحتاجه لتوزيع البيانات الضارة والرد على رسائل واتساب الواردة.
وتشير Check Point إلى أنها أخطرت جوجل بشكل مسؤول بشأن البرمجية وأبحاثها، وأزالت جوجل التطبيق من متجرها، لكنه كان متاحًا لمدة شهرين وتم تنزيله نحو 500 مرة.