

تقرير يحذر من تطبيقات مزيفة لـ ChatGPT على أندرويد



الأحد 18 يونيو 2023 04:35 م

أظهر تقرير حديث أن هناك مشكلة متنامية مع البرامج الضارة على هواتف Android يمكن أن تسبب تلفاً أو تسرق المعلومات من هاتفك، حيث يتظاهر البرنامج الضار بأنه روبوت محادثة AI شائع يسمى ChatGPT يستخدمه كثير من الناس. ولم يتم إطلاق تطبيق ChatGPT لمستخدمي أندرويد بعد، وإذا وجدت أي تطبيق يدعي أنه ChatGPT، يجب عليك الامتناع عن استخدامه لأن هذه التطبيقات قد تكون برامج ضارة خطيرة مصممة لسرقة معلوماتك الشخصية.

اكتشف الباحثون من Palo Alto Networks Unit 42 برامج ضارة بدأت في الظهور بنفس الوقت تقريباً الذي أصدرت فيه OpenAI GPT-3.5 و GPT-4، تستهدف تغييرات البرامج الضارة هذه على وجه التحديد الأشخاص المهتمين باستخدام أداة ChatGPT. هناك نوعان من البرامج الضارة النشطة التي حددها الباحثون أحدهما يسمى Meterpreter Trojan، ويتنكر في شكل تطبيق يسمى "SuperGPT"، في حين تتظاهر البرامج الضارة الأخرى بأنها تطبيق ChatGPT الفعلي، لكنها ترسل رسائل سرّاً إلى أرقام هواتف باهظة الثمن.

وجد الباحثون أيضاً نموذجاً خبيثاً لـ (Android Package Kit (APK)، وهو نوع من الملفات المستخدمة لتنصيب التطبيقات على أجهزة أندرويد تبين أن ملف APK الضار هذا هو نسخة معدلة من تطبيق أصلي.

و بحسب India Today التطبيق الشرعي هو مساعد AI يعتمد على أحدث إصدار من ChatGPT، إذا وقع شخص ما في الحيلة وقام بتنصيب هذا الإصدار الضار، فإنه يسمح للمهاجم بالتحكم في هاتف أندرويد الخاص بهذا الشخص عن بُعد وفقاً.

كذلك اكتشف الباحثون مجموعة أخرى من عينات البرامج الضارة بتنسيق APK تظهر هذه العينات بريئة على السطح، وتعرض صفحة ويب تحتوي على معلومات حول ChatGPT ومع ذلك فإنهم يخفون غرضاً خبيثاً.

ما يجعل عينات البرامج الضارة هذه أكثر خداعاً هو أنها تستخدم شعار OpenAI، المؤسسة التي تقف وراء ChatGPT، كرمز لتطبيقها، يضيف هذا إلى القصة المضللة أن هذه التطبيقات مرتبطة بأداة ChatGPT AI المشروعة.

تتمتع نماذج APK الضارة هذه بالقدرة على إرسال رسائل SMS إلى أرقام عالية التكلفة باهظة الثمن، تكلف أرقام التعريف المميزة أكثر من أرقام الهواتف العادية وتستخدم عادةً للخدمات التي يدفع فيها المستخدمون مقابل المعلومات أو نوع من الخدمة، وفي هذه الحالة يستخدم منشئو البرامج الضارة الأرقام لكسب المال من خلال عمليات الاحتيال والأنشطة الاحتيالية.

لحماية نفسك من الضروي توكي الحذر عند تنزيل التطبيقات على هاتف أندرويد، والإلتزام بالمصادر الموثوقة وكن حذراً من التطبيقات التي قد تتظاهر بأنها ليست كذلك خاصة إذا كانت تدعي أنها مرتبطة بـ ChatGPT.