برمجية خبيثة على أندرويد تحول الأجهزة إلى أدوات تجسس على المستخدمين

الثلاثاء 18 يوليو 2017 06:07 م

كشفت شركة أمن المعلومات تريند مايكرو أن برمجية خبيثة قديمة تستهدف نظام التشغيل أندرويد أصبحت تستخدم حيلًا جديدة لتحويل الأجهزة إلى أدوات تجسس على المستخدمين.

وتسمح البرمجية الخبيثة، التي تُعرف باسم "جوست كونترول" GhostCtrl، للمخترقين بالسيطرة الكاملة على الأجهزة، حتى أنها تسمح لهم بالاطلاع على كافة محتويات الهاتف والتجسس على المستخدمين دون علمهم.

وقال باحثو الشركة اليابانية في منشور على مدونتها إنهم تمكنوا من الكشف عن ثلاثة إصدارات مختلفة من البرمجية. إذ صُمم الإصداران الأوليان لجمع البيانات والتحكم عن بعد بميزات الهاتف المختلفة، أما الإصدار الثالث فهو يجمع بين أفضل إمكانات الإصدارين السابقين، ومن ثم يضيف المزيد. وأسوأ ما في الأمر أن الباحثين يتنبؤون بأن الثغرة سوف تستمر في التطور.

ووفقًا للنتائج التي توصلوا إليها، تعد برمجية "جوست كنترول" امتدادًا لفيروس دودة خبيث يسرق البيانات كان قد انتشر بين المستشفيات وثغرة OmniRAT سيئة السمعة التي برزت في عناوين الأخبار بعدما أن قيل إنها تسمح عن بعد باختراق حواسب ويندوز وماك ولينوكس عن طريق أي جهاز أندرويد، والعكس بالعكس.

وغالبًا ما تُموَّه البرامج الخبيثة لتبدو وكأنها تطبيقات مشروعة مثل واتس اب وغيره من التطبيقات الشهيرة. وحينما تُشغَّل، يتجه التطبيق الرئيسي إلى تثبيت تطبيق أندرويد خبيث بصيغة APK ليعمل بعد ذلك في الخلفية.

وعند هذه النقطة، يمكن للمهاجمين استغلال هذا الباب الخلفي لجعل الأجهزة المصابة تقوم بما يريدون. وحذرت تريند مايكرو من أن الثغرة تسمح بتنفيذ مجموعة واسعة من الأوامر، مما يتيح للقراصنة تحديد واستهداف المحتوى دون موافقة المالك أو معرفته.

وقد نشرت الشركة قائمة من الشيفرات التنفيذية التي تسمح للقراصنة بمراقبة البيانات التي تجمعها حساسات الجهاز في الوقت الحقيقي، وتسمح لهم بحذف وتعديل ونقل الملفات المخزنة، والاتصال وإرسال رسائل نصية إلى جهات الاتصال، وجمع معلومات مثل سجلات المكالمات، وسجلات الرسائل SMS، ومدخلات الموقع وكذلك الإشارات المرجعية للمتصفح.

وبالإضافة إلى كل هذا، لاحظ الباحثون أن لـ "جوست كنترول" أيضًا القدرة على إعادة تعيين كلمات السر عن بعد، وتشغيل أصوات مختلفة على الهاتف، وتشغيل الكاميرا، ومراقبة بلوتوث وأكثر من ذلك. ويعني هذا بالأساس أنه بمجرد أن ينجح المهاجم في إصابة النظام، فإن الجهاز يتحول إلى أداة للتجسس على المستخدم.

ولحل المشكلة، توصي تريند مايكرو المستخدمين بتحديث هواتفهم إلى أحدث إصدار من نظام أندرويد على الفور، وتقييد أذونات المستخدم على أجهزتهم الشخصية، وأخذ نسخ احتياطية عن البيانات الشخصية بانتظام.