# قراصنة يستهدفون مستخدمي أندرويد بنسخة خبيثة من تيليجرام

الأحد 15 يناير 2023 05:20 م

اكتشف باحثون في مجال أمن المعلومات أن مجموعة القرصنة (StrongPity APT) تنشر تطبيقًا مزيفًا لخدمة الدردشة (Shagle)، ولكنه، في واقع الأمر، نسخة حصان طروادة تحوي بابًا خلفيًا من تطبيق التراسل الفوري تيليجرام على نظام أندرويد.

يُشار إلى أن (Shagle) هي منصة للدردشة المرئية العشوائية تسمح للغرباء بالتحدث إلى بعضهم عبر قناة اتصالات مشفرة، وتقوم المنصة بالكامل على الويب، ولا يوجد لها تطبيق على الأجهزة المحمولة.

واكتشف الباحثون أن مجموعة (StrongPity) تستخدم منذ عام 2021 موقع ويب مزيفًا ينتحل هوية موقع (Shagle) الفعلي لخداع الضحايا لتنزيل تطبيق أندرويد ضار.

ويُمكِّن هذا التطبيق القراصنة، فور تثبيته، من التجسس على الضحايا المستهدفين، ومن ذلك: مراقبة المكالمات الهاتفية، وجمع الرسائل النصية القصيرة، والاستيلاء على قوائم الاتصال.

ويُنسب إلى مجموعة (StrongPity)، المعروفة أيضًا باسم (Promethium) أو (APT-C-41)، حملات سابقة نشرت فيها نسخة حصان طروادة من تطبيق (Notepad++)، ونسخًا خبيثة من تطبيقي (WinRAR) و(TrueCrypt)، وذلك بغية إصابة الأهداف بالبرامج الضارة.

واكتشف النشاطَ الأحدث لمجموعة التهديدات المستمرة المتقدمة (APT) باحثو شركة أمن المعلومات (ESET) الذين نسبوا الحملة إليها بناءً على أوجه التشابه بين الكود الخاص بالتطبيق الحديث والحمولات السابقة للمجموعة.

وبالإضافة إلى ذلك، قال الباحثون إن تطبيق أندرويد الضار وُقِّع بالشهادة نفسها التي استخدمتها المجموعة لتوقيع تطبيق ينتحل هوية تطبيق الحكومة الإلكترونية السورية على نظام أندرويد في حملة شُنَّت خلال عام 2021.

وأوضح الباحثون أن تطبيق أندرويد الضار الذي نشرته (StrongPity) هو ملف (APK) اسمه (video.apk)، وهو تطبيق: (Telegram V7.5.0)، وقد عُدِّل لانتحال هوية تطبيق (Shagle) للأجهزة المحمولة. ويُنشر تطبيق (APK) الضار مباشرةً من موقع (Shagle) وهمي، ولم يُنشر عن طريق متجر التطبيقات جوجل بلاي.

وتقول (ESET) إن الموقع الوهمي المُستنسَخ ظهر أول مرة عبر الإنترنت في شهر تشرين الثاني/ نوفمبر 2021، لذلك يُحتمل أن يكون ملف (APK) قيد النشر النشط منذئذ. ومع ذلك، فإن أول اكتشاف مؤكد للحملة جاء في شهر تموز/ يوليو 2022.

يُشار إلى أن أحد عيوب استخدام تطبيق تيليجرام كأساس للتطبيق الضار المزيف هو أنه إن كان هاتف الضحية يحوي بالفعل تطبيق تيليجرام المشروع، فإن الباب الخلفي لن يُثبَّت على الجهاز.

وقال الباحثون إن مُعرِّف واجهة برمجة التطبيقات (API ID) المُستخدَم في العينات المُلتقطة مقيدٌ حاليًا بسبب الإفراط في الاستخدام، لذا لن يقبل تطبيق حصان طروادة تسجيل أي مستخدم جديد بعد الآن، ومن ثَمَّ، لن يعمل الباب الخلفي، وتعتقد (ESET) أن هذا يشير إلى أن مجموعة (StrongPity) تمكنت بالفعل من نشر البرامج الضارة على أجهزة الضحايا المستهدفين.

وعند التثبيت، يطلب البرنامج الضار الوصول إلى خدمة إمكانية الوصول (Accessibility Service) ثم يجلب ملفًا مشفرًا ببروتوكول (AES) من خادم الأوامر والتحكم الخاص بالمهاجم. ثم يُستخدم الملف لأداء وظائف ضارة مختلفة، تشمل تخزين بيانات تُخزَّن وتُجمع في دليل التطبيق، ثم تُشفَّر وتُرسل إلى خادم المهاجم مرة أخرى.

ومن خلال إساءة استخدام خدمة إمكانية الوصول، يمكن للبرنامج الضار قراءة محتوى الإشعارات من تطبيقات، مثل: مسنجر، وفايبر، وسكايب، ووي شات، وسناب شات، وإنستاجرام، وتويتر، وجيميل، بالإضافة إلى تطبيقات أخرى.

وفي الأجهزة التي عُدِّلت للوصول فيها إلى صلاحيات المسؤول، يمنح البرنامج الضار نفسه تلقائيًا الإذن لإجراء تغييرات على إعدادات الأمان، والكتابة على نظام الملفات، وإجراء عمليات إعادة التشغيل، وأداء وظائف خطرة أخرى.

يُشار إلى أن مجموعة القرصنة (StrongPity) تنشط منذ عام 2012، وعادةً ما تستخدم الأبواب الخلفية في مُثبِّتات البرامج الشرعية. واستنادًا إلى تقرير (ESET)، فإن المجموعة تستمر في استخدام التكتيك نفسه منذ عشر سنوات.

ويجب على مستخدمي أندرويد توخي الحذر مع ملفات (APK) التي تُنزَّل من خارج متجر جوجل بلاي، والانتباه إلى طلبات الأذونات أثناء تثبيت التطبيقات الجديدة.