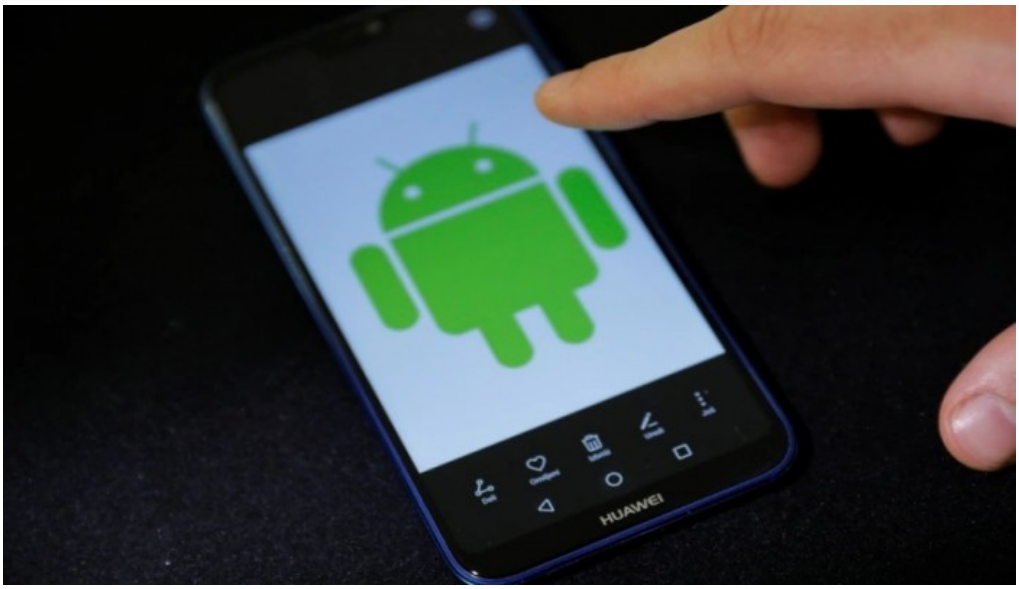
8 تطبيقات يجب على مستخدمي هواتف أندرويد حذفها



السبت 13 مارس 2021 03:18 م

اكتشف المحتالون الإلكترونيون طريقة جديدة لسحب الأموال من تطبيقاتك المصرفية، فقد ذكر بحث جديد أجرته شركة "تشيك بوينت ريسيرش" (Check Point Research) 8 من هذه التطبيقات التي كانت متاحة على متجر غوغل بلاي (Google Play) والتي يمكن أن تشكل تهديدا كبيرا لخصوصيتك.

ويقترح البحث أن "كلاست 82" (Clast82) -وهي أداة "قطارة" (Dropeper)- تقوم بإسقاط البرامج الضارة داخل الأجهزة وكانت تنتشر في 8 تطبيقات مصممة لتقديم برامج ضارة، والجزء الصادم حول هذه التطبيقات هو أن برنامج الحماية "غوغل بلاي بروتيكت" (Google Play Protect) لم يتتبعها من قبل.

تختبئ البرامج الضارة داخل أحد التطبيقات، ولا يتم تنشيطها إلا بعد تثبيت التطبيقات المصابة، وبعد تثبيت أحد التطبيقات المعدية يقوم برنامج القطارة بفك ضغطه بنفسه وتثبيت البرامج الضارة التي يطلق عليها "آلين بوت بانكر" (AlienBot Banker)، وهي متغير يقوم على وجه التحديد بحقن التعليمات البرمجية الضارة في التطبيقات المالية.

لا تصيب هذه البرامج الضارة التطبيقات المصرفية فحسب، ولكنها تتيح أيضا لجهات خارجية الوصول إلى هاتفك المحمول عن بعد.

بعد إصابة هاتفك يمكن للمهاجمين عبر الإنترنت الوصول الكامل عن بعد إلى جهازك، ويمكنهم اختطاف التطبيقات المصرفية وتثبيت أي تطبيق آخر، وتحويل الأموال من حسابات المحفظة المصرفية الخاصة بك، وكذلك اعتراض رموز المصادقة الثنائية.

وقال الباحثون "عند السيطرة على الجهاز تكون لدى المهاجم القدرة على التحكم في وظائف معينة، تماما كما لو كان يمسك بالجهاز ماديا، مثل تثبيت تطبيق جديد على الجهاز، أو حتى التحكم فيه باستخدام برنامج "تيم فيور" (TeamViewer)".

وأصدر الباحثون أسماء التطبيقات الثمانية المعدية التي يمكنها إفراغ حساباتك المصرفية، وهي "كيك في بي إن" (Cake VPN)، و"باسفيك في بي إن" (Pacific VPN)، و"إي في بي إن" (eVPN)، و"بيت بلاير" (BeatPlayer)، و"كيو آر باركود سكانر ماكس" (QR/Barcode Scanner MAX)، و"ميوزيك بلاير" (Music Player)، و"تولتيبناتورلايبراري" (tooltipnatorlibrary)، و"كيو ريكوردر" (QRecorder)، فإذا كانت التطبيقات المذكورة مثبتة على جهازك فقم بإلغائها فورا.