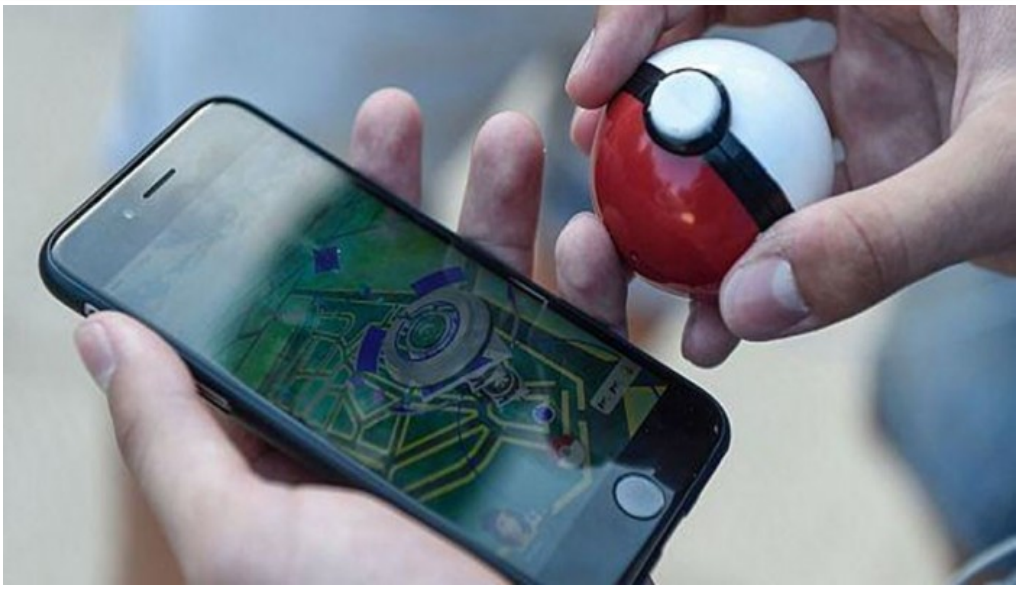
فيروس باسم "بوكيمون غو" يخترق نصف مليون هاتف أندرويد



الاثنين 19 سبتمبر 2016 06:09 م

اكتشف خبراء "كاسبرسكي لاب" مؤخراً تطبيقاً خبيثاً جديداً على متجر "Google Play" يعرف باسم "Guide for Pokémon Go"، لديه قدرة السطو على صلاحية الوصول الى جذر نظام أندرويد المشغل لأجهزة الهواتف الذكية، واستخدام ذلك لتثبيت التطبيقات وإزالتها، وعرض الإعلانات غير المرغوب فيها.

وقد تم تحميل التطبيق لأكثر من 500 ألف مرة، وسُجل ما لا يقل عن 6000 إصابة ناجحة، وبدورها أبلغت كاسبرسكي لاب شركة Google بشأن برمجية حصان طروادة الخبيثة، ومن ثم تمت إزالة التطبيق من المتجر.

وقد نتج عن ظاهرة لعبة "Pokémon Go" العديد من التطبيقات المتشابهة للعبة؛ بسبب الاهتمام المتزايد من جانب مجرمي الإنترنت.

وكشفت نتائج تحليلات كاسبرسكي لاب لتطبيق "Guide for Pokémon Go" عن وجود شيفرة خبيثة تقوم بتحميل برمجية التجذير الخبيثة، وهو ما يضمن الوصول إلى نواة نظام التشغيل أندرويد لأغراض تثبيت وإزالة التطبيق بالإضافة إلى عرض الإعلانات.

وتتضمن برمجية حصان طروادة الخبيثة هذه بعض المزايا المثيرة للاهتمام من شأنها أن تساعد على تخطي برامج الكشف. على سبيل المثال، لا يتم تفعيل هذه البرمجية لحظة قيام الضحية بتشغيل التطبيق، وبدلاً من ذلك، تنتظر حتى يقوم المستخدم بتثبيت تطبيق آخر أو إزالته، وبعد ذلك تقوم بالتحقق لمعرفة إن كان هذا التطبيق يعمل على جهاز حقيقي أو افتراضي.

وفي حال كان التطبيق يعمل على جهاز حقيقي، تنتظر برمجية حصان طروادة ساعتين إضافيتين قبل أن تباشر نشاطها الخبيث، ولن تكون الإصابة مضمونة حتى بعد انقضاء تلك المهلة.