1.2 مليون جهاز أندرويد مُصاب بالبرمجية الخبيثة Hummer

الجمعة 1 يوليو 2016 05:07 م

اكتشف باحثون في مجال الأمن تابعين لمُختبرات أبحاث أمن الهواتف المحمولة Cheetah Mobile Security Research Lab ما يعتقدون بأنه أكبر عائلة برمجيات خبيثة من نوع حصان طروادة المعروفة باسم "هامر" Hummer والتي أصابت حوالي 1.2 مليون جهاز يعمل بنظام أندرويد في مُختلف أنحاء العالم.

وتعمل البرمجية هامر على تثبيت برامج ضارة وتطبيقات وألعاب غير مرغوب بها على أجهزة الضحايا، إلى جانب قيامها بإظهار الإعلانات المُنبثقة على الهواتف.

ويحصل مُطوري البرمجية على 0.50 دولار في كل مرة تقوم فيها هامر بتثبيت تطبيق جديد على الأجهزة المُصابة، مما يسمح لصانعيها بجني حوالي 500 ألف دولار يوميًا.

وتم اكتشاف برمجية هامر للمرة الأولى من قبل مختبر بحوث أمن الأجهزة المحمولة Cheetah في عام 2014، إلا أنها بقيت خامدة لعدة شهور.

ونشر الباحثين في مجال الأمن تدوينة تشرح جميع التفاصيل حول كيفية قيام برمجية هامر باصابة مئات الآلاف من الهواتف في صيف العام الماضي، وذلك قبل ان تنتشر بشكل كامل في عام 2016.

وعلى الرغم من انخفاض عدد الهواتف المُصابة، إلا أن البرمجية ما تزال تعمل على أكثر من مليون هاتف ذكي، الأمر الذي يجعلها أكثر برمجيات حصان طروادة انتشارًا في العالم.

وتحصل البرمجية Hummer بعد إصابتها للجهاز على صلاحية الجذر أو امتيازات المسؤول، مما يسمح لها بإظهار الإعلانات المنبثقة وتثبيت التطبيقات والألعاب الغير مرغوب بها إلى جانب التطبيقات الإباحية.

ويؤدي هذا إلى استهلاك كميات كبيرة من البيانات وتحميل المُستخدم المصاب فواتير استخدام بيانات إضافية، حيث أشار الباحثين إلى تمكن البرمجية من الوصول إلى الشبكة أكثر من 10 آلاف مرة خلال عدة ساعات، وقيامها بتحميل أكثر من 200 ملف تطبيقي APK، واستهلاك ما يقارب من 2 جيجابايت من بيانات الإنترنت.

ويعتبر من الصعوبة بمكان إزالة أو إلغاء البرمجية الخبيثة، ويعود ذلك إلى حصولها على صلاحيات وامتيازات كبيرة على الأجهزة المصابة، حيث لا يُمكن إلغاء تثبيتها عبر ادوات مكافحة الفيروسات التقليدية، كما أنه لا يُمكن حذفها من خلال خيار استعادة ضبط المصنع.

واكتشف الباحثون بعد تحليل عينات قيام برمجية هامر بنشر نفسها عن طريق استخدام مجموعة متنوعة من أسماء النطاقات ونقاط العدوى الموجودة ضمن مخازن تطبيقات الطرف الثالث.

حيث يتم خداع المُستخدمين وجعلهم يقومون بتحميل البرمجية الخبيثة إلى هواتفهم عن طريق تحميل نُسخ مُقلدة من التطبيقات الشائعة مثل يوتيوب.

وتعتبر الهند أكثر البلدان المتضررة بعدد أجهزة مصابة يبلغ حوالي 154,248 جهاز، تتبعها اندونيسيا بعدد أجهزة يبلغ 92,889، ومن ثم تركيا بعدد أجهزة 63,906، وتتبعها الصين بعدد أجهزة مصابة يبلغ حوالي 63,285، ومن ثم المكسيك بعدد أجهزة 59,192.