Dvmap .. برمجية خبيثة جديدة تستهدف نظام أندرويد

الخميس 15 يونيو 2017 10:06 م

اكتشف خبراء كاسبرسكي لاب حصان طروادة جديدًا غير اعتيادي ينتشر في متجر جوجل بلاي، وقالوا إن بإمكان حصان طروادة الجديد، والمعروف باسم Dvmap الحصول على صلاحية الوصول إلى الجذر في أجهزة الهواتف المتنقلة بنظام أندرويد، كما يمكنه أيضًا التحكم بالجهاز عن طريق حقن الكود البرمجي الخبيث في مكتبة النظام.

وأوضح الخبراء أنه وفي حال نجح في ذلك، يقوم مباشرة بحذف بيانات الوصول إلى الجذر، مما يساعد على تجنب اكتشافه. يذكر أن حصان طروادة الذي أبلغ عن وجوده لـشركة جوجل، قد تم تنزيله من متجر جوجل بلاي أكثر من 50 ألف مرة منذ شهر آذار/مارس2017. كما أبلغت كاسبرسكي لاب عن اكتشاف حصان طروادة لـشركة جوجل، وتم الآن إزالته من المتجر.

وأشار خبراء شركة أمن المعلومات الروسية إلى أن استخدام تقنية حقن الكود في نظام الضحية يعد تطورًا خطيرًا جديدًا في مشهد البرمجيات الخبيثة المستهدفة للأجهزة المتنقلة. ونظرًا لإمكانية استخدام هذا النهج لتفعيل أنماط برمجية خبيثة حتى في حال حذف بيانات الوصول إلى الجذر، فإن أي حلول أمنية وتطبيقات مصرفية مزودة بخصائص الكشف عن الجذر التي يتم تثبيتها بعد الإصابة لن تتمكن من الكشف عن وجود مثل هذه البرمجية الخبيثة.

وأضاف الخبراء أنه ومع ذلك، فإن تعديل مكتبات النظام هي في الواقع عملية محفوفة بالمخاطر وقد لا تكلل بالنجاح. وتوصل الباحثون أثناء مراقبتهم لبرمجية Dvmap إلى أن هذه الأخيرة تقوم بالإبلاغ عن كل تحرك ونشاط لها إلى خادم التحكم والسيطرة، وذلك على الرغم من عدم ورود أي استجابة أو تعليمات من الخادم المعني. وهذا يشير إلى أن البرمجية الخبيثة ليست جاهزة تمامًا أو قد تم تفعيلها.

وتنتشر برمجية Dvmap الخبيثة على شكل لعبة في متجر جوجل بلاي. ولتخطي إجراءات الفحص والتحقق الأمني المطبقة في المتجر، قام مطورو البرمجية المذكورة بتحميل تطبيق نظامي ونظيف في المتجر بنهاية شهر آذار/مارس 2017. ثم قاموا بتحديث هذا التطبيق بمعلومات خبيثة لفترة قصيرة من الزمن قبل تحميل إصدار آخر نظيف. وفي غضون أربعة أسابيع، كرر أولئك تلك العملية لخمس مرات على الأقل.

وأوضح خبراء كاسبرسكي لاب أن برمجية حصان طروادة Dvmap تقوم بتثبيت نفسها على جهاز الضحية على مرحلتين. وأثناء المرحلة الأولية، تحاول البرمجية الحصول على صلاحية الوصول إلى الجذر على الجهاز. وفي حال نجاحها، تقوم بتثبيت عدد من الأدوات، بعضها مزود بتعليقات وملاحظات مكتوبة باللغة الصينية. ومن إحدى هذه الأنماط تطبيق بعنوان: com.qualcmm.timeservices، وهو يربط حصان طروادة بخادم التحكم والسيطرة الخاص به. ومع ذلك، لوحظ عدم تلقي البرمجية الخبيثة في المقابل لأي أوامر خلال فترة التحقيق.

وفي المرحلة الرئيسية من الإصابة، يقوم حصان طروادة بإطلاق ملف بدء مرحلة الإصابة، ويتحقق من إصدار أندرويد المثبت على الجهاز ويقرر نوع المكتبة التي سيقوم بحقن الكود فيها. وتتمثل الخطوة التالية في استبدال التعليمات الموجودة بتعليمات خبيثة، مما يتسبب في تعطل الجهاز المصاب بالكامل.

وتقوم مكتبات النظام التي تم تحديثها حديثًا بتفعيل نمط البرمجية الخبيثة، التي يمكنها إيقاف خاصية التحقق من التطبيقات VerifyApps. بعد ذلك تقوم البرمجية بتشغيل خاصية إعدادات المصادر المجهولة أو Unknown Sources التي تسمح لها بتثبيت التطبيقات من أي موقع، ليس فقط من متجر جوجل بلاي. وبالتالي، قد تكون هذه المصادرة عبارة عن برمجيات خبيثة أو تطبيقات إعلانية غير مرغوب فيها.

وقال رومان يوناشيك، محلل أول للبرمجيات الخبيثة في كاسبرسكي لاب: "تشكل برمجية حصان طروادة Dvmap تطورًا خطيرًا جديدًا في مشهد البرمجيات الخبيثة المستهدفة للأجهزة بنظام أندرويد، حيث يتم حقن كود البرمجية الخبيثة ذاتيًا إلى مكتبات النظام، مما يجعل من الصعب اكتشافها وإزالتها وبالتالي، هناك أوقات صعبة تنتظر المستخدمين مستقبلًا، خصوصًا أولئك الذين ليس لديهم برامج حماية أمنية فاعلة تمكنهم من تحديد ومنع التهديدات قبل حدوثها نحن نعتقد بأننا قد تمكنا من الكشف عن هذه البرمجية الخبيثة في مرحلة مبكرة جدا ويظهر تحليلنا بأن الأنماط البرمجية الخبيثة تقوم بإبلاغ المهاجمين عن كل تحرك لها، وهناك أيضًا بعض التقنيات التي يمكنها التسلل إلى الأجهزة المصابة لذا، فإن الوقت يشكل عاملًا مهمًا ورئيسيًا في إطار الجهود المبذولة للحيلولة دون وقوع هجوم أوسع وأكثر خطورة".

ويُنصح المستخدمون الذين لديهم مخاوف من احتمال إصابتهم ببرمجية DVmap الخبيثة بإجراء نسخ احتياطي لجميع البيانات الخاصة بهم واختيار نمط إعادة ضبط المصنع للبيانات وبالإضافة لذلك، تنصح كاسبرسكي لاب جميع المستخدمين بتثبيت حل أمني موثوق به، مثل Kaspersky Internet Security للأجهزة بنظام التشغيل أندرويد على أجهزتهم، والتأكد دائمًا من اختيار التطبيقات المصممة فقط عن طريق مطورين ذوي سمعة حسنة في السوق، والحرص على تحديث نظام التشغيل وبرامج التطبيقات المثبتة على أجهزتهم، والامتناع عن تنزيل أي عناصر مشبوهة أو مريبة أو التي لا يمكن التحقق من مصدرها