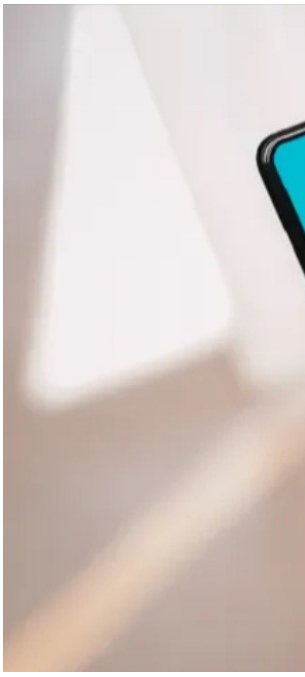
"حصان طروادة" يهدد مستخدمي أندرويد



حذر الخبراء مستخدمي "أندرويد" من تطبيقات تحمل برامج ضارة لسرقة الحسابات المصرفية والتي تستهدف بشكل خاص مالكي هواتف "غالكسي" من "سامسونغ".

وتخفي التطبيقات التي تم تنزيلها من متجر "غوغل بلاي"، خطأ ضارا يسمى Anatsa، وهو فيروس "حصان طروادة المصرفي".

ويشير مصطلح "حصان طروادة" إلى فيروس قادر على تنفيذ إجراءات نيابة عن الضحية، دون علمه، بما في ذلك سحب الأموال من حسابه المصرفي.

وقال الخبراء في شركة الأمن السيبراني Fabric Threat، إن: "التطبيقات تشكل تهديدا خطيرا لمستخدمي "أندرويد"، وبشكل أكثر تحديدا، أولئك الذين يستخدمون هواتف "غالكسي" من "سامسونغ".

وأوضحت الشركة في بيان: "كان الجانب الفريد من هذا البرنامج هو شفرته الخبيثة التي تستهدف أجهزة

سامسونغ على وجه التحديد. وتم تصميم خدمة إمكانية الوصول الخبيثة للتفاعل مع عناصر واجهة المستخدم لأجهزة سامسونغ، ما يعني أن مستخدمي سامسونغ فقط هم الذين تأثروا في هذه المرحلة من الحملة. ويشير هذا إلى أن الجهات الفاعلة في مجال التهديد قامت في البداية بتطوير واختبار التعليمات البرمجية الخاصة بها حصريا لأجهزة سامسونغ".

وتمت إزالة التطبيقات الآن من متجر "غوغل"، لكن فريق الأمن السيبراني قال إنه: "حتى إذا قمت بتنزيل التطبيقات، فقد تظل معرضا للخطر، وحث مستخدمي أندرويد على التحقق من أجهزتهم الآن وحذف تلك التطبيقات".

وقال متحدث باسم "غوغل": "تمت إزالة جميع التطبيقات المحددة في التقرير من غوغل بلاي".

وتتم حماية مستخدمي أندرويد تلقائيا من الإصدارات المعروفة من هذه البرامج الضارة بواسطة "Google Play Protect"، والذي يتم تشغيله افتراضيا على أجهزة "أندرويد" المزودة بخدمات "غوغل بلاي".

وأضاف المتحدث باسم "غوغل": "يمكن لـ Google Play Protect تحذير المستخدمين أو حظر التطبيقات المعروف بأنها تظهر سلوكا ضارا، حتى عندما تأتي هذه التطبيقات من مصادر خارج غوغل بلاي".

وفي الواقع تم رصد تطبيقات حصان طروادة Anatsa منذ نوفمبر عام 2023. وقال الخبراء: "على مدى الأشهر الأربعة الماضية، لاحظنا خمس موجات هجوم متميزة من هذه الحملة، تركز كل منها على مناطق جغرافية مختلفة".

ولا يتوقع الخبراء أن يختفي الفيروس الضار في أي وقت قريب، وقالوا: "بناء على هذا النمط، نتوقع استمرار هذه الحملة، مع ظهور أدوات جديدة في المتجر الرسمي والتوسع في مناطق مستهدفة إضافية".

وينصح المستخدمون بحماية هواتفهم من خلال توخي الحذر بشأن الأذونات التي يسمحون بها على أجهزتهم، وحذف التطبيقات التي لا يتم استخدامها إلا إذا كانوا يثقون في المطور.