الخليج

اقتصاد, تقنية وسيارات

30 يناير 2023 14:59 مساء

«استهداف الهواتف الذكية وأجهزة الحاسوب عبر «الراوتر

«دبي: «الخليج

(DNS Changer) أفاد باحثو كاسبرسكي في يناير 2023 باكتشافهم وظيفة جديدة لأداة تغيير نظام أسماء النطاقات التخريبية. يستطيع مجرمو الإنترنت، بموجب الوظيفة الجديدة المكتشفة، Roaming Mantis المستخدمة في حملة المخترقة في المقاهي والفنادق والمطارات (Wi-Fi) استخدام أجهزة التوجيه (الراوتر) في شبكات الإنترنت اللاسلكية Wroba.o ببرمجية Android والأماكن العامة الأخرى لإصابة المزيد من الهواتف الذكية التي تعمل بنظام أندرويد الخبيثة. وتستهدف التقنية الجديدة في الوقت الراهن المستخدمين في كوريا الجنوبية، ولكن بالإمكان استخدامها قريباً في بلدان أخرى.

حملة تخريبية يقودها مجرمو الإنترنت، رصدتها (Shaoye المعروفة أيضاً باسم) Roaming Mantis وتعد حملة للتحكّم في الأجهزة APK «كاسبرسكي لأول مرة في عام 2018. وتستخدم ملفات خبيثة من نوع «حزمة تطبيق أندرويد وقدرات تعدين العملات الرقمية على iOS المصابة وسرقة المعلومات منها، كما تتمتع بقدرات التصيّد على أجهزة

أجهزة الحاسوب الشخصية. ويدلّ اسم الحملة على انتشارها في الهواتف الذكية التي تتجول بين شبكات «واي فاي»، والتي يُحتمل أن تنقل الإصابة وتنشرها إلى غيرها من الأجهزة.

تمكنها من مهاجمة المستخدمين عبر أجهزة الراوتر DNS Changer وظيفة جديدة لـ

في DNS Changer قد أدخلت حديثاً وظيفة جديدة على Roaming Mantis اكتشف خبراء كاسبرسكي أن وهو البرمجية الخبيثة التي استُخدمت (XLoaderو Moqhaoو Agent.eq المعروف أيضاً بالأسماء) Wroba.o برمجية خبيثة توجّه الجهاز المتصل بجهاز الراوتر المخترَق إلى خادم يقع DNS Changer لأول مرّة في الحملة. ويُعدّ الأصلي. وعندما يصل جهاز الضحية إلى الصفحة المقصودة، DNS تحت سيطرة مجرمي الإنترنت، بدلاً من خادم يُطلب من الضحية المحتملة تنزيل برمجية خبيثة يمكنها التحكّم في الجهاز أو سرقة بيانات اعتماد الدخول إلى حسابات مستخدمه.

في الوقت الحالي، على أجهزة الراوتر Roaming Mantis وينحصر استهداف الجهة التخريبية الكامنة وراء DNS الموجودة في كوريا الجنوبية، والتي تصنعها شركة كورية معروفة مختصة بالأجهزة الشبكية. وتحصل وظيفة الخاص بالراوتر وتتحقق من طرازه لتمييزه عن غيره من الطرز، وضمان اختراق IP الجديدة على عنوان Changer ولاحظت كاسبرسكي في ديسمبر 2022، حدوث .DNS أجهزة الطراز المستهدف فقط عن طريق الكتابة فوق إعدادات خبيثة في كوريا الجنوبية 508 APK عمليات تنزيل لحُزم.

وكشف تحقيق في الصفحات الخبيثة المقصودة عن أن المهاجمين يستهدفون أيضاً مناطق أخرى باستخدام الرسائل ويستخدم هذا الأسلوب الرسائل النصية لنشر الروابط الخبيثة التي توجّه .DNS Changer النصية القصيرة بدلاً من الضحية إلى الموقع المراد لتنزيل البرمجية الخبيثة على الجهاز أو سرقة معلومات المستخدم عبر أحد مواقع التصيّد.

التي غطّت المدة بين (KSN) Kaspersky Security Network ووفقاً لإحصائيات شبكة كاسبرسكي الأمنية (Trojan-Dropper.AndroidOS.Wroba.o) الخبيثة Wroba.o سبتمبر وديسمبر 2022، فقد حدث أعلى معدّل لاكتشاف برمجية في فرنسا (54.4%) واليابان (12.1%) والولايات المتحدة (10.1%).

وأوضح سوغورو إيشيمارو الباحث الأمني الأول لدى كاسبرسكي، أن اتصال هاتف ذكي مصاب بأجهزة راوتر سليمة في شبكات الإنترنت العامة في المقاهي أو الفنادق أو مراكز التسوق أو المطارات، أو حتى المنازل، يسمح لبرمجية الخبيثة باختراق أجهزة الراوتر تلك والتأثير في الأجهزة الأخرى المتصلة بالشبكة. وقال: «يمكن لوظيفة Wroba.o الجديدة إدارة جميع اتصالات الجهاز باستخدام الراوتر المخترق، مثل إعادة التوجيه إلى الأجهزة DNS Changer المضيفة الخبيثة وحتى تعطيل التحديثات في المنتجات الأمنية، لذلك يُعدّ هذا الاكتشاف مهماً للأمن الرقمي لأجهزة أندرويد، نظراً لكونه قادراً على الانتشار الواسع في المناطق المستهدفة».

ويوصي باحثو كاسبرسكي باتباع التدابير التالية لحماية الاتصال بالإنترنت من هذه الإصابة:

أو الاتصال بمقدّم خدمة DNS مراجعة دليل الاستخدام الخاصة بجهاز الراوتر للتحقق من أنه لم يتمّ العبث بإعدادات الإنترنت للحصول على الدعم.

تغيير تسجيل الدخول وكلمة المرور الافتراضيين للراوتر عبر الويب، وتحديث برمجياته الثابتة بانتظام من المصدر

.الرسمي

الامتناع عن تثبيت البرمجيات الثابتة للراوتر من مصادر خارجية، وتجنُب استخدام مستودعات خارجية لأجهزة .أندرويد

عند طلب https التحقُق دائماً من عناوين المتصفح والموقع الإلكتروني للتأكّد من أصالتها، بالبحث عن علامات مثل .إدخال البيانات في صفحة ما

.الحرص على تثبيت حل أمني خاص بالأجهزة المحمولة، لحمايتها من هذه التهديدات وغيرها