الخليج

اقتصاد, تقنية وسيارات

20 يونيو 2022 11:32 صباحا

سلالة من البرمجيات الخبيثة تضرب «أندرويد» وتستهدف الخدمات المصرفية

دبي: «الخليج»

اكتشفت مختبرات «إف 5» مؤخراً سلالة جديدة متطورة لبرمجية خبيثة تستهدف أجهزة أندرويد أُطلق عليها اسم «مالي بوت» MaliBot، وذلك أثناء تعقب برمجية خبيثة أخرى لاختراق حسابات الخدمات المصرفية عبر الإنترنت تدعى «فلو بوت» FluBot.

وتستهدف برمجية «مالي بوت» الخبيثة في الوقت الراهن عملاء الخدمات المصرفية عبر الإنترنت في كل من إسبانيا وإيطاليا، لكن مختبرات «إف 5» تدعو مستخدمي أجهزة أندرويد في سائر أنحاء العالم إلى توخي الحذر من انتشار برمجية «مالي بوت» الخبيثة نظراً لقدراتها المتطورة التي تشمل سرقة كلمات المرور وملفات تعريف الارتباط (الكوكيز)، إضافة إلى سلوكيات وخصائص جاء من أبرزها:

وأسماء تطبيقات أخرى «The CryptoApp»و «Mining X» ـ انتحال أسماء تطبيقات تعدين العملات المشفرة مثل لحمل المستخدمين على تثبيتها في أجهزتهم. «Chrome»و «MySocialSecurity» مثل

ـ سرقة البيانات المالية وكلمات المرور ومحافظ العملات الرقمية والبيانات الشخصية للمستخدمين، واستهداف مؤسسات مالية في إيطاليا وإسبانيا.
ـ القدرة على تجاوز أو سرقة رموز مصادقة الدخول بعوامل متعددة (أو عدة خطوات).
ـ التحكم عن بُعد بأجهزة أندرويد باستخدام خادم للحوسبة الافتراضية عبر الشبكة.
لعرض صفحات إنترنت مألوفة وحث المستخدمين على تعبئة WebView ـ استغلال مكوّن مدمج بنظام أندرويد يدعى بيانات دخول حساباتهم لغرض سرقتها.
بنظام أندرويد لتمرير أوامر دون معرفة المستخدم، من قبيل نسخ Accessibility «ـ استغلال ميزة «إمكانية الوصول كلمات المرور ورموز المصادقة وتسريبها للمهاجمين.
هجمات أوسع
في ضوء ذلك تتوقع مختبرات «إف 5» ازدياد عدد الدول المستهدفة بهذه البرمجية بمرور الوقت واحتمال استخدامها لشن هجمات أوسع تتجاوز عمليات سرقة كلمات المرور والعملات الرقمية. ونوّهت مختبرات «إف 5» بأن أي تطبيق في نظام أندرويد يتحمل مسؤولية تعريض المستخدمين لخطر سرقة كلمات المرور WebView يستخدم مكوّن وملفات تعريف الارتباط.
تجنب الوقوع ضحية الاحتيال
وقال محمد أبو خاطر، نائب الرئيس لمنطقة الشرق الأوسط وإفريقيا لدى «إف 5»: «يعتبر هذا البحث الذي أجرته مختبرات «إف 5» بمثابة تذكير لكل من مطوري التطبيقات والمستخدمين بضرورة البقاء في حالة يقظة تجاه البرمجيات الخبيثة وتجنب الوقوع ضحية الاحتيال المصرفي عبر الأجهزة المتحركة».
وأضاف: «يجب على المستخدمين اتباع أفضل ممارسات الأمان والتأكد بأن أجهزتهم العاملة بنظام أندرويد لا تسمح إلا بتثبيت تطبيقات من متاجر معتمدة، مثل متجر جوجل بلاي للتطبيقات. وكذلك فإننا لا نشجع على تثبيت أي تطبيقات من مواقع الإنترنت مباشرة، خاصة عند ورود رابط لمواقع الإنترنت تلك عبر رسائل نصية أو بريد إلكتروني. ويجب على المستخدمين فهم خطر منح صلاحيات قوية للتطبيقات، مثل منح صلاحية استخدام ميزة 'إمكانية الوصول' لأي تطبيق يقومون بتثبيته. كما يتعين على المطورين الانتباه إلى حقيقة أن البرمجيات الخبيثة المتطورة أصبحت قادرة على تجاوز آليات المصادقة ثنائية العوامل وبأنها تقوم ببناء طبقات أمنية إضافية في التطبيقات، لا سيما تلك التي تمنح إمكانية النفاذ إلى الحسابات المالية».