التجسس على الهاتف.. إشارات تحذيرية لا ينبغي تجاهلها



تتشابه كثير من علامات اختراق الهاتف مع أعراض الأجهزة القديمة العادية، ما يجعل التمييز بينهما أمراً دقيقاً يستوجب اليقظة الدائمة.

تطبيقات مزيفة تنتحل برامج موثوقة وتسرق بياناتك بصمت

يعدّ ظهور تطبيق غير مألوف على الهاتف من أبرز مؤشرات اختراق الهاتف، غير أن بعض البرمجيات الخبيثة تبدو مطابقة لتطبيقات موجودة، برمجية RatHat المستهدفة لأندرويد تنتحل شكل تطبيقات شائعة كجوجل كروم، وتنتشر عبر رسائل نصية ومواقع تنزيل مزيفة تحاكي متجر جوجل بلاي.

تطبيقات مزيفة تنتحل برامج موثوقة

وحين يمنحها المستخدم صلاحيات المدير، تثبّت وكيل ذكاء اصطناعي يعمل في الخلفية يسرق كلمات المرور، ورموز التحقق بخطوتين (2FA)، والرسائل، وإن طلب الهاتف تثبيت تطبيق موجود أصلًا كنسخة ثانية من جوجل كروم، فهذا مؤشر محتمل على وجودها.

وتُزيل ميزة حماية جوجل بلاي التطبيقات الضارة آليًا في أغلب الأحيان، إلّا أن RatHat أعصى على الإزالة، ولا يُقضى عليها إلّا بإعادة ضبط المصنع.

ويُنصح على آيفون بالتحقق من ملفات تعريف الإعداد ضمن قسم (Management Device & VPN) في الإعدادات، وحذف أي ملف مجهول المصدر، مع مراعاة أن حذفه يمسح جميع الإعدادات والتطبيقات والبيانات المرتبطة به.

تنبيهات دخول لم تطلبها وإعلانات خارج المتصفح

يستوجب استقبال رمز تحقق بخطوتين دون محاولة تسجيل دخول التحقق فوراً من أمان الحساب، فقد يعني ذلك حصول شخص ما على كلمة المرور ومحاولته الولوج من جهازه.

ويكشف موقع BGR أن هجوم Pixnapping على أندرويد يستخدم تطبيقاً خبيثاً يُعيد بناء محتوى الشاشة بكسل واحد في كلّ مرة، وأثبتت الأبحاث قدرته على التقاط رمز التحقق في 14 ثانية فحسب.

وتوصي لجنة التجارة الفيدرالية الأمريكية بالتوقف عن تسجيل الدخول إلى الحسابات من الجهاز المشتبه به، وتغيير كلمات المرور من جهاز آخر، والتحقق مع مزود الخدمة من عدم إعداد إعادة توجيه الرسائل القصيرة على الرقم، وهو ما توصي به آبل خصوصاً عند تأمين الحساب.

وتُدرج لجنة التجارة الفيدرالية كذلك كثرة النوافذ الإعلانية المنبثقة ضمن دلائل البرمجيات الخبيثة، والإعلانات التي تظهر دون فتح أي متصفح تُعدّ إنذاراً أشد خطورة.

ورصد باحثو شركة Bitdefender برمجية Mimosa Midnight مثبّتة مسبقاً في آلاف الهواتف الاقتصادية التي تعمل بشرائح MediaTek وتُباع تحت علامات كـCubot وDoogee، إلى جانب مقلّدات سلسلة S Galaxy من سامسونج.

وتختبئ داخل برنامج النظام وتثبّت تطبيقات خدمات صغيرة لعرض إعلانات، بل تُحوّل الهاتف إلى وسيط لتوجيه حركة إنترنت أشخاص آخرين، ولا تُزيلها إعادة ضبط المصنع، ما يعني الاستغناء عن الجهاز كلياً.

سخونة الهاتف واستنزاف البطارية

يُشير سخون الهاتف أثناء خموله أو نفاد بطاريته بصورة مفاجئة إلى احتمال تشغيل برنامج خبيث في الخلفية، إذ يستهلك كل نشاط خبيث طاقة معالجة وبطارية، وتبقي RatHat وكيلاً يعمل باستمرار في الخلفية لمراقبة ما يفعله المستخدم.

ينبغي أولاً استبعاد الأسباب العادية؛ فقد يستهلك الهاتف طاقة أكبر لفترة وجيزة عقب تحديث برمجي، أو لأيام متعددة مع هاتف جديد حتى تستقر أداؤه وعمر بطاريته.

وإن لم ينطبق شيء من ذلك، تُشير إعدادات البطارية على معظم الأجهزة إلى أي تطبيقات بعينها تستهلك أكبر قدر من الطاقة ومدى تكرار استخدامها المكثف.

ارتفاع مفاجئ في استهلاك البيانات

يُشكّل الارتفاع المفاجئ في استهلاك بيانات الهاتف إنذاراً محتملاً باختراق الهاتف، إذ يستلزم أي سرقة للمعلومات نقلها إلى الخارج، حيث ترسل RatHat كل ما تسرقه عبر خادم وسيط إلى المخترقين، فيما تستنزف Mimosa Midnight البيانات حين تُحوّل الهاتف إلى وسيط لتوجيه حركة الإنترنت.