كارثة إسرائيل تتجسس على هواتف سامسونج في مصر والشرق الأوسط عبر تطبيق «AppCloud» غير القابل للحذف

السبت 20 سبتمبر 2025 08:30 م

كشف تحقيق صحفي نشرته وسائل إعلام عربية مؤخرًا عن قيام الاحتلال الإسرائيلي بالتجسس على هواتف سامسونج المنتشرة في مصر ودول الشرق الأوسط، عبر تطبيق «AppCloud» المثبت مسبقًا على أجهزة المستخدمين، والذي لا يمكن حذفه.
التطبيق يقوم بجمع بيانات شخصية للمستخدمين دون إذنهم، بما في ذلك الموقع الجغرافي، سجل المكالمات، الرسائل، وسلوك التصفح.

قبل أيام، أدلى رئيس الوزراء الإسرائيلي السابق بنيامين نتنياهو بتصريح استفزازي أمام وفد من الكونجرس الأمريكي قائلاً: «هل لديك هاتف محمول؟ إذن أنت تحمل قطعة من إسرائيل هنا»، متباهياً بالتكنولوجيا الإسرائيلية في مجال التجسس والأمن السيبراني. التصريح أظهر بوضوح النظرة الاستراتيجية لإسرائيل تجاه استغلال الأجهزة الرقمية لجمع المعلومات.

كيفية التجسس وآلية العمل

يعمل تطبيق «AppCloud» كخدمة سحابية أساسية في هواتف سامسونج، ويُثبت مسبقًا على الجهاز، ما يمنحه وصولًا شبه كامل لبيانات المستخدمين.
التطبيق يجمع بيانات حساسة بشكل مستمر، بما في ذلك:
الموقع الجغرافي لحظة بلحظة.
سجل المكالمات والرسائل النصية.
سجل التصفح والتطبيقات المستخدمة.
كون التطبيق غير قابل للحذف من قبل المستخدم العادي، فإن أي محاولة لحماية الخصوصية الفردية تصبح شبه مستحيلة. هذا يضع مستخدمي الشرق الأوسط أمام خطر مراقبة مستمرة من أجهزة الاستخبارات الإسرائيلية أو شركائها التقنيين.

أثر التجسس على المستخدمين

خبراء الأمن السيبراني حذروا من أن مثل هذا التجسس يهدد:
الخصوصية الفردية، إذ تُجمع البيانات دون موافقة واضحة.
الأمن الرقمي، حيث يمكن استخدام المعلومات لأغراض تجارية أو سياسية.
سلامة البيانات الحساسة، خصوصًا في الأجهزة الرسمية للحكومات أو الشركات.
التعرض لمثل هذه الممارسات يضع المستخدمين في موقف هش، ويجعلهم عرضة للاستغلال من أطراف متعددة.

ردود الفعل الدولية والمحلية

التحقيق الصحفي أثار استنكارًا واسعًا، إذ اعتبره متخصصون في حماية البيانات انتهاكًا صارخًا للخصوصية.
في مصر ودول الشرق الأوسط، تدرس بعض الهيئات الرقابية تعزيز الرقابة على التطبيقات المثبتة مسبقًا.
خبراء الأمن الرقمي أكدوا ضرورة تقييم هواتف الموظفين الحكوميين والمستخدمين الرسميين لضمان حماية المعلومات الحساسة.
عدة تقارير تحذر من أن السماح للتطبيقات المدمجة بالوصول غير المحدود للبيانات يمثل ثغرة خطيرة للأمن الرقمي.

الجانب التقني والتقارير الأمنية

تم اكتشاف التجسس عبر تحقيقات صحفية متعمقة وتحليلات برمجية أظهرت:
قدرة التطبيق على جمع بيانات حساسة بشكل مستمر وسري.
ارتباطه بالخوادم الإسرائيلية، مما يتيح الوصول إلى المعلومات في الخارج.
المقارنة مع برامج تجسس عالمية مماثلة تظهر خطورة هذه الممارسات على الأمن الرقمي للمستخدمين العاديين والحكومات على حد

سواء

التوصيات والتحذيرات

خبراء الأمن الرقمي والخصوصية يوصون بما يلي:

توخي الحذر في استخدام التطبيقات المدمجة وفحص إعدادات الخصوصية بانتظام

مطالبة الشركات والهيئات الحكومية بفحص الأجهزة الرسمية والتأكد من عدم وجود تطبيقات تجسس

تشديد الرقابة على التطبيقات المثبتة مسبقًا، خاصة تلك التي لا يمكن حذفها، لضمان حماية البيانات الشخصية للمستخدمين

وختاما فكشف التجسس عبر تطبيق «AppCloud» يسلط الضوء على هشاشة الخصوصية في العصر الرقمي، ويشكل تحديًا أمنيًا وسياسيًا لدول الشرق الأوسط التصريحات الإسرائيلية تؤكد النظرة الاستراتيجية للتكنولوجيا كأداة لجمع المعلومات والسيطرة، مما يستدعي من الحكومات والمؤسسات اتخاذ إجراءات عاجلة لحماية مواطنيها ومواردها الرقمية

كما أن القضية تمثل تذكيرًا صارخًا بأن الهواتف الذكية ليست مجرد أدوات للتواصل، بل أصبحت بوابة لمراقبة واسعة، وضرورة إدراك المستخدمين والجهات الرسمية لخطورة البيانات الشخصية في العصر