برمجية Keenadu الخبيثة مثبّتة مسبقًا على أكثر من 220 ألف جهاز أندرويد



رصدت كاسبرسكي Keenadu على أكثر من 220 ألف جهاز أندرويد خلال أول عشرة أشهر من 2026، مزروعة في البرمجيات الثابتة عبر سلسلة التوريد. على المؤسسات فحص عينات قبل الشراء بالجملة.

- رُصدت Keenadu على أكثر من 220 ألف جهاز أندرويد في أول عشرة أشهر من 2026.
- مع عائلة Triada تمثل 88% من الأجهزة التي وُجدت عليها برمجيات خبيثة مثبّتة مسبقًا هذا العام، وقد تضاعف العدد الشهري للاكتشافات أكثر من مرتين ونصف خلال عام.
- تستقر البرمجية في قسم النظام، فلا تستطيع مضادات الفيروسات ولا نظام التشغيل إزالتها، وقد لا تنفع إعادة تثبيت النظام.
- بقيت نسخ Keenadu المفحوصة خاملة نحو شهرين ونصف قبل التفعيل، غالبًا لتفادي الاكتشاف.
- استُخدمت في معظم الهجمات المعروفة للاحتيال الإعلاني، لكن تصميمها المعياري يتيح

للمهاجمين دفع وحدات إضافية.

تفيد كاسبرسكي بأن أجهزة أندرويد الجديدة قد تغادر المصنع وفي برمجياتها الثابتة برمجية خبيثة. ووفق الشركة، تضاعف عدد هذه الأجهزة المرصودة شهريًا أكثر من مرتين ونصف خلال العام الماضي.

ما الذي رُصد

وصلت Keenadu إلى أكثر من 220 ألف جهاز في الأشهر العشرة الأولى من 2026. ومع عائلة Triada الأقدم، وُجدت على 88% من الأجهزة التي اكتُشفت عليها برمجيات خبيثة مثبّتة مسبقًا هذا العام. وظهر نحو عشرين متغيرًا مختلفًا من Triada في 2026.

تعتمد Keenadu تصميمًا معياريًا مشابهًا لـ Triada، يتيح للمهاجمين دفع وحدات إضافية وحقنها في التطبيقات المستهدفة. وبقيت نسخ الباب الخلفي التي فحصتها كاسبرسكي خاملة نحو شهرين ونصف قبل أن تأمر خوادم القيادة والتحكم بتفعيلها، وتعتقد الشركة أن الغاية تفادي الاكتشاف. أما معظم الهجمات المعروفة فاستخدمتها في الاحتيال الإعلاني، مثل النقرات الوهمية.

أهمية الأمر للمؤسسات

تصل هذه الإصابات عبر سلسلة التوريد: فقد يثبّت المصنّع البرمجية عمدًا، أو يزوّد مقاول سيئ النية علامة تجارية مشروعة ببرمجيات ثابتة خبيثة، أو يتعرض أحد مكونات عملية البناء للاختراق. وما إن تستقر البرمجية في قسم النظام حتى لا تستطيع مضادات الفيروسات ولا نظام التشغيل إزالتها بحسب كاسبرسكي، وبعضها يبقى حتى بعد إعادة تثبيت النظام.

وبالنسبة للشركات التي تصرف أجهزة لموظفيها، تشمل المخاطر بطء الأجهزة وإعلانات خفية وحسابات مخترقة وسرقة عملات رقمية وتسرب بيانات الشركة، كما يمكن ضم الأجهزة إلى شبكات وكيل أو شبكات DDoS. وتنصح كاسبرسكي بفحص عينات واختبارها تجريبيًا قبل الطلبات الكبيرة، مع التنبيه إلى أن ذلك لا يغني عن برمجيات الحماية، فقد يرسل المورّد عينات سليمة، وقد يُستهدف نظام التحديث نفسه.

ما يجب فعله الآن

1. فحص عينات من الأجهزة واختبارها تجريبيًا قبل أي شراء بالجملة للهواتف أو الأجهزة اللوحية أو غيرها من الأجهزة المتصلة.
2. عدم الاكتفاء باختبار العينات، والإبقاء على برمجيات حماية ومراقبة مستمرة على كل جهاز مصروف.
3. مراجعة موردي الأجهزة وسلسلة توريد برمجياتها الثابتة ضمن تقييم مخاطر الأطراف الثالثة.
4. رصد سلوك الأجهزة المصروفة بحثًا عن بطء أو إعلانات غير متوقعة أو اختراق حسابات أو حركة شبكة غير معتادة.
5. التعامل مع الأجهزة المشتبه بإصابتها ببرمجية مثبّتة مسبقًا على أنها غير قابلة للإصلاح والتخطيط لاستبدالها بدل الاعتماد على إعادة تثبيت النظام.