تعطيل شبكة BadBox 3.0 للاحتيال الإعلاني: مخاطر الأجهزة غير المعتمدة العاملة بنظام أندرويد



أعلنت Human Security تعطيل BadBox 3.0، أكبر شبكة احتيال إعلاني من حيث حجم طلبات المزايدة. تصيب الشبكة أجهزة أندرويد رخيصة لعرض إعلانات خفية وتمرير حركة أطراف خارجية عبرها كوكلاء سكنيين.

- بلغت BadBox 3.0 ذروتها بنحو 40 مليار طلب مزايدة يوميًا، وأكثر من 4% من حركة CTV التي رصدتها منصة Human.
- تستهدف الشبكة أجهزة Android Open Source Project رخيصة وغير معتمدة تحمل أبوابًا خلفية تُنزّل وحدات احتيال ووكلاء.
- سُجّلت الأجهزة المصابة في إحدى عشرة شبكة وكلاء سكنية، منها PXYEDGE.
- رصدت Human Security عدة روابط بين الشبكة والشركة الصينية المصنّعة TXCZ.
- يُرجَّح أن عدد الإصابات الفعلي أعلى بكثير من 367 ألف طلب سُجّلت خلال شهر على نسخة مرآة

لمستودع واحد.

أعلنت شركة Human Security أنها عطّلت BadBox 3.0، التي تصفها بأنها أكبر شبكة احتيال إعلاني من حيث حجم طلبات المزايدة. وهي الإصدار الثالث من عملية تستهدف أجهزة أندرويد منخفضة التكلفة. وكانت BadBox 2.0 قد رُصدت أول مرة على أكثر من مليون جهاز، ثم بلغت أكثر من 10 ملايين.

ما الذي تفعله الشبكة

تعمل الشبكة على أجهزة Android Open Source Project غير معتمدة أُصيبت بأبواب خلفية. تُنزّل هذه الأبواب وحدات احتيال تعرض إعلانات الفيديو داخل نافذة مخفية، فتبدو طلبات المزايدة كأنها صادرة من تطبيقات معروفة ينتحل المشغّلون صفتها. لا يرى مالك الجهاز شيئًا، بينما يدفع المعلنون مقابل مساحات إعلانية لم يشاهدها مستخدم حقيقي.

كما سُجّلت الأجهزة نفسها في إحدى عشرة شبكة وكلاء سكنية، منها PXYEDGE، وهي نسخة أُعيدت تسميتها من IpMoYu. ولأن جزءًا كبيرًا من الحركة جاء من عناوين وكلاء سكنية، بدت كأنها مشاهدة منزلية عادية. وبلغت الشبكة في ذروتها نحو 40 مليار طلب مزايدة يوميًا.

الإسناد وحجم الشبكة

وجدت Human Security روابط عدة بالشركة الصينية المصنّعة TXCZ، منها فحص الوحدات لخصائص بناء تخصها، ونطاق تابع لها يقدّم مسارات التحميل وإعدادات الإعلانات. وقد تعطلت بعض نطاقات القيادة والتحكم عندما أزالت Google شبكة XCPE التي ضمّت أكثر من 1.3 مليون جهاز فك ترميز يعمل بأندرويد.

لم تحدد Human الحجم الإجمالي. فقد خدمت نسخة مرآة لمستودع واحد أكثر من 367 ألف طلب خلال شهر، لكن الشركة تؤكد أن ذلك يخص مستودعًا واحدًا وقناة توصيل احتياطية، وأن الإصابات الفعلية أعلى بكثير.

الصلة بالمنظمات

لا يذكر المصدر المملكة العربية السعودية. ومع ذلك فقد تُسجَّل الأجهزة المتصلة رخيصة الثمن في المكاتب وقاعات الاجتماعات واللوحات الرقمية كوكلاء، فتمرّ حركة أطراف خارجية عبر شبكة المنشأة. وتبقى ضوابط الشراء والشبكة هي الدفاع العملي.

ما يجب فعله الآن

1. احصروا الأجهزة العاملة بأندرويد على شبكتكم، مثل أجهزة فك الترميز ومشغلات اللوحات الرقمية وعصي البث، وحددوا النماذج غير المعتمدة أو مجهولة المصدر.
2. اعزلوا هذه الأجهزة في شريحة شبكة منفصلة دون وصول إلى الأنظمة الداخلية.
3. راقبوا حركة الخروج من هذه الشرائح بحثًا عن اتصالات غير معتادة أو سلوك وكيل سكني، واحجبوا ما لا حاجة إليه.
4. أضيفوا فحوص الاعتماد وسلسلة التوريد إلى شراء الأجهزة المتصلة منخفضة التكلفة.
5. أزيلوا الأجهزة التي تظهر عليها مؤشرات أبواب خلفية مثبتة مسبقًا أو استبدلوها، وأدرجوها في سجلات

مخاطر الأطراف الثالثة والأصول.