مكتب التحقيقات الفيدرالي ينسب سرقة أصول رقمية تتجاوز 6 مليارات دولار إلى مجموعة TraderTraitor الكورية الشمالية



نسب مكتب التحقيقات الفيدرالي رسميًا سرقة أصول رقمية تتجاوز 6 مليارات دولار إلى TraderTraitor، المجموعة المرتبطة بكوريا الشمالية، بمشاركة الخدمة السرية الأمريكية ومصلحة الضرائب.

- نسب مكتب التحقيقات الفيدرالي رسميًا سرقة أصول رقمية تتجاوز 6 مليارات دولار إلى TraderTraitor.
- المجموعة مرتبطة بكوريا الشمالية وتُتتبَّع أيضًا بأسماء Jade Sleet Pressure Chollima وPUKCHONG وSlow Pisces وUNC4899.
- شاركت الخدمة السرية الأمريكية ومصلحة الضرائب (IRS-CI) مكتب التحقيقات في الإعلان.
- يربط عنوان الخبر النشاط بأكبر عملية سرقة بقيمة 6.43 مليار دولار تتعلق بمنصة Binance.

نسب مكتب التحقيقات الفيدرالي الأمريكي رسميًا سرقة أصول رقمية تتجاوز 6 مليارات دولار إلى TraderTraitor، وهي مجموعة قرصنة متقدمة مرتبطة بكوريا الشمالية. وشاركت في البيان الخدمة السرية الأمريكية ووحدة التحقيقات الجنائية في مصلحة الضرائب (IRS-CI). ويصف عنوان المصدر القضية بأنها أكبر عملية سرقة بقيمة 6.43 مليار دولار مرتبطة بمنصة Binance.

ما هو معروف

تُتتبَّع المجموعة بأسماء عدة لدى الجهات المتخصصة: Jade Sleet وPressure Chollima وPUKCHONG وSlow Pisces وUNC4899. وعلى فرق الأمن التي تصادف هذه الأسماء في مصادر استخبارات التهديدات أن تعدّها إشارة إلى مجموعة الجهات الفاعلة نفسها التي تُعرف باسم TraderTraitor.

لا يتضمن المقتطف المتاح لنا الأساليب التقنية أو الجدول الزمني أو مؤشرات الاختراق المحددة، ولذلك لا نستنتج كيفية تنفيذ عمليات السرقة.

الأهمية للمؤسسات في المملكة

يشكّل الإسناد الرسمي بهذا الحجم مرجعًا مفيدًا للمؤسسات التي تحتفظ بأصول رقمية أو تتداولها أو تموّلها، ولكل جهة يتعامل موظفوها أو شركاؤها مع هذه المنصات. وهو دعوة لمراجعة التعرض للسرقة المالية المدعومة من دول، والتأكد من أن تغطية استخبارات التهديدات تشمل أسماء هذه المجموعة. ولا يلزم إجراء يتجاوز المراجعة الدورية ما لم تكن لدى مؤسستكم تعاملات بالأصول الرقمية.

ما يجب فعله الآن

1. إضافة TraderTraitor وأسماءها البديلة (Jade Sleet وPressure Chollima وPUKCHONG وSlow Pisces وUNC4899) إلى قوائم المراقبة في استخبارات التهديدات.
2. التأكد مما إذا كانت لدى مؤسستكم أو شركائها تعاملات مع الأصول الرقمية أو منصات العملات المشفرة.
3. مراجعة ضوابط الصلاحيات المميزة والموافقات المرتبطة بمسارات الأصول الرقمية والتحويلات عالية القيمة.
4. التحقق من أن خطط الاستجابة للحوادث تغطي السرقة المالية واسعة النطاق من جهات مدعومة من دول.