مكتب التحقيقات الفدرالي ينسب سرقة بينانس البالغة 6.3 مليار دولار إلى مجموعة TraderTraitor الكورية الشمالية



نسب مكتب التحقيقات الفدرالي سرقة نحو 6.3 مليار دولار من بينانس إلى مجموعة TraderTraitor الكورية الشمالية، وطلب من مزودي الأصول الافتراضية حظر 628 عنوانًا مرتبطًا بالعملية.

- نسب المكتب السرقة التي وقعت في أو نحو 29 أكتوبر 2026 إلى TraderTraitor، المعروفة أيضًا بـ APT38g Jade Sleetg Lazarus Group.
- أرجعت بينانس الاختراق إلى حاسوب محمول لمهندس DevOps جرى اختراقه، ما أتاح الوصول إلى حاوية خدمة وتنفيذ عمليات سحب غير مصرح بها.
- سُرق نحو 6.36 مليار دولار عبر عشر سلاسل كتل، وتم نقل معظمها خلال 20 دقيقة.
- نشر المكتب 628 عنوانًا (608 إيثريوم و19 بيتكوين وواحد سولانا) وطلب من المنصات ومزودي الأصول الافتراضية حظر المعاملات المرتبطة بها.

- تقول بينانس إنها غطت نحو 95% من المبلغ المتأثر وإن الخسائر لن تُحمَّل للمستخدمين.

نسب مكتب التحقيقات الفدرالي رسميًا سرقة نحو 6.3 مليار دولار من بينانس إلى TraderTraitor، وهي مجموعة كورية شمالية مدعومة من الدولة وتُعرف أيضًا بأسماء Lazarus Group وJade Sleet وAPT38. وحدد المكتب موعد السرقة في أو نحو 29 أكتوبر 2026. وكانت شركتا TRM Labs وChainalysis المتخصصتان في استخبارات سلاسل الكتل قد أشارتا سابقًا إلى المجموعة نفسها.

ما الذي حدث

كانت بينانس قد أرجعت الاختراق إلى حاسوب محمول يخص مهندس DevOps جرى اختراقه. أتاح ذلك للمهاجمين الوصول إلى حاوية خدمة وتقديم عمليات سحب غير مصرح بها. وخرج نحو 6.36 مليار دولار عبر عشر سلاسل كتل، وتمت معظم التحويلات خلال 20 دقيقة.

رصد المكتب تحويل الأصول المسروقة أساسًا إلى إيثريوم، ويتوقع غسلها لاحقًا عبر منصات التمويل اللامركزي (DeFi) وخدمات المبادلة الفورية. وطلب المكتب مع جهاز الخدمة السرية الأمريكي وإدارة التحقيقات الجنائية في مصلحة الضرائب من المنصات ومشغلي سلاسل الكتل ومزودي خدمات الأصول الافتراضية حظر المعاملات المرتبطة بعناوين الغسل، ونشر قائمة تضم 628 عنوانًا.

نمط مألوف

يذكر المصدر عمليات سرقة كورية شمالية سابقة بدأت أيضًا من موظفين أو مطورين لديهم وصول إلى البنية التحتية للأصول المشفرة. ومن الأساليب المستخدمة: منتحلو صفة مسؤولي توظيف ضمن حملة 'Operation DreamJob'، وشيفرة Python خبيثة متنكرة في اختبار ما قبل التوظيف، وعملية هندسة اجتماعية استمرت ستة أشهر وشملت لقاءات حضورية مع مساهمين في Drift.

استجابة بينانس

ذكرت بينانس أنها تستعد لاستئناف المرحلة الأولى من السحب في 1 نوفمبر بين 06:00 و09:00 بالتوقيت العالمي. وتفيد بأنها غطت نحو 95% من المبلغ المتأثر، وأن الباقي رموز أقل سيولة ما زالت تشتريها. وتؤكد أن خدمات الإيداع لم تتأثر وأنها ستتحمل الخسارة.

والدرس للمؤسسات الخاضعة للتنظيم أن أجهزة المهندسين أصحاب الصلاحيات العالية مسار رئيسي إلى الأنظمة الحساسة، وأن المهاجمين يستهدفون الأشخاص بقدر ما يستهدفون البرمجيات.

ما يجب فعله الآن

1. تعزيز حماية ومراقبة أجهزة مهندسي DevOps وأصحاب الصلاحيات العالية، بما يشمل ضوابط على تشغيل الشيفرات غير المراجَعة.
2. تقييد ما يمكن لحاويات الخدمة تنفيذه، وفرض موافقات إضافية أو حدود على عمليات السحب والدفع.
3. في حال العمل في الأصول الافتراضية، إضافة العناوين التي نشرها المكتب إلى قوائم الفحص والحظر.
4. توعية المطورين وفرق المالية بأساليب منتحلي صفة مسؤولي التوظيف واختبارات البرمجة غير المطلوبة

والهندسة الاجتماعية الحضورية في الفعاليات.

5. مراجعة خطط الاستجابة للحوادث ومكافحة الاحتيال لضمان سرعة كشف التحويلات السريعة عالية القيمة.