بينانس تربط سرقة أصول رقمية بقيمة 6.3 مليار دولار بجهاز محمول مخترق لمهندس DevOps



أفادت بينانس بأن اختراق جهاز مهندس DevOps أتاح سحوبات غير مصرح بها بنحو 6.3 مليار دولار. ونسبت شركات تحليل البلوكتشين الهجوم إلى TraderTraitor الكورية الشمالية، فيما لم تسمّ بينانس جهة محددة.

- ربطت بينانس سرقة نحو 6.3 مليار دولار بجهاز محمول مخترق لمهندس DevOps وبالوصول إلى حاوية خدمة.
- تقول الشركة إن الهجوم كان معقداً وليس إجراءً واحداً، ولم تجد حتى الآن دليلًا على تسرب مفتاح خاص لمحفظة.
- تنسب TRM وChainalysis الهجوم إلى TraderTraitor المعروفة أيضاً باسم Lazarus Group وAPT38.
- جرى تجميد نحو 2.7 مليار دولار، بينما يظل نحو 2.4 مليار دولار تحت سيطرة المهاجمين.

- علّقت بينانس الإيداع والسحب وألغت صلاحيات العنوان المتأثر، وتعهدت بتغطية جميع الخسائر.

ربطت بينانس سرقة نحو 6.3 مليار دولار من العملات المشفرة بجهاز محمول مخترق يعود لمهندس DevOps. وبحسب المنصة، أتاح هذا الوصول للمهاجمين تقديم معاملات سحب غير مصرح بها بعد وصولهم إلى حاوية خدمة، ولم تعثر حتى الآن على دليل على تسرب مفتاح خاص لمحفظة.

ما أعلنته بينانس

أكد الرئيس التنفيذي المشارك ريتشارد تينغ أن المهاجم لم يكتفِ باستخدام صلاحيات مهندس واحد، وأن العملية لم تكن إجراءً واحداً بل مسار هجوم أكثر تعقيداً. وأضافت بينانس أنها اكتشفت نقاط اختراق إضافية وما زالت تجمع الحقائق. وقد علّقت الإيداع والسحب لإجراء فحوص أمنية، وألغت صلاحيات العنوان المتأثر، وتعمل مع شركاء استخبارات البلوكتشين والجهات الأمنية. وتقول إنها ستغطي جميع الخسائر من صندوق SAFU وأموال الشركة، وستنشر إثبات احتياطيات محدثاً بعد اكتمال المعالجة.

الإسناد والاسترداد

لم تسمِّ بينانس جهة تهديد. أما TRM فنسبت الهجوم إلى TraderTraitor، وهي وحدة قرصنة تدعمها كوريا الشمالية وتُعرف أيضاً باسم Lazarus Group وAPT38، وقالت Chainalysis إنها تؤكد ذلك بدرجة ثقة عالية. وتفيد TRM بأن نحو 6.36 مليار دولار خرجت من محافظ على عشر سلاسل بلوكتشين، معظمها خلال نحو 20 دقيقة، ما يجعلها أكبر سرقة عملات مشفرة مسجلة.

جمّدت جهات مصدِّرة للعملات المستقرة ومجلس أمني لإحدى الشبكات نحو 2.7 مليار دولار. وتذكر TRM أن المهاجم باع USDT لصناع السوق واقترض ETH مقابل USDT، ويحتفظ الآن بأصول تقارب 2.4 مليار دولار لا تستطيع أي جهة إصدار تجميدها.

لماذا يهم ذلك

نقطة الدخول المعلنة كانت جهاز مهندس لا خللًا في المنصة الأساسية. وعلى المؤسسات المنظمة مراجعة كيفية اتصال أجهزة المطورين والمشرفين ببيئات الإنتاج.

ما يجب فعله الآن

1. مراجعة كيفية وصول أجهزة المطورين وفرق DevOps إلى حاويات الإنتاج وخدماته، وحصر هذا الوصول في الضروري فقط.
2. تطبيق حماية نقاط النهاية وتشفير القرص الكامل وفحوص امتثال الأجهزة على كل أجهزة الهندسة ذات الصلاحيات العالية.
3. اشتراط موافقة أطراف متعددة وضوابط مستقلة للمعاملات عالية القيمة حتى لا يستطيع جهاز مخترق واحد اعتمادها.
4. تدقيق بيانات اعتماد الحاويات والخدمات وتدوير الأسرار ومراقبة أي نشاط سحب أو تحويل غير معتاد.
5. اختبار خطط الاستجابة للحوادث وإجراءات التصعيد والتجميد، بما يشمل قنوات التواصل مع الجهات الأمنية والشركاء.