بينانس: مقابلة عمل وهمية وراء سرقة أصول رقمية بقيمة 6.34 مليار دولار



يفيد تقرير بينانس بأن مهاجمين مرتبطين بكوريا الشمالية استخدموا مسؤول توظيف وهميا ومهمة برمجية خبيثة للوصول إلى بنية المحافظ وسرقة نحو 6.34 مليار دولار.

- بدأ الهجوم في سبتمبر عندما تواصل شخص ينتحل صفة مدير مشروع مع مهندس برمجيات عبر منصة توظيف مشروعة.
- مهمة برمجية من مستودع شيفرة عبر الإنترنت ثبّتت برمجية خبيثة غير معروفة سابقا لم ترصدها أدوات حماية الأجهزة.
- بحلول 20 أكتوبر استخدم المهاجمون جهاز المهندس وأداة ذكاء اصطناعي داخلية لاختراق موظفين آخرين والحصول على بيانات اعتماد ورمز نشر للحاويات.
- في 29 أكتوبر وصلوا إلى خدمة توقيع المحافظ، وأتاح إساءة استخدام EIP-7702 في إيثريوم استمرار السرقة بعد تعليق السحب.

- جرى تجميد أو اعتراض نحو 2.85 مليار دولار، وتم تعويض 98% من الرموز المتضررة بحلول 31 أكتوبر.

نشرت بينانس تقرير حادثة يوضح أن سرقة أصول رقمية بقيمة نحو 6.34 مليار دولار في 29 أكتوبر بدأت بمقابلة عمل وهمية. وكان مكتب التحقيقات الفيدرالي قد نسب الهجوم إلى المجموعة الكورية الشمالية المعروفة باسم TraderTraitor، وتُتتبع أيضا باسم Lazarus Group وJade Sleet وAPT38.

كيف جرى الهجوم

في سبتمبر تواصل شخص ينتحل صفة مدير مشروع في شركة وهمية مع مهندس برمجيات عبر منصة توظيف مشروعة، وكان ملفه الشخصي يشير إلى عمله في بينانس. أُجريت بعدها مقابلتان: مكالمة فيديو مع من ادّعى أنه من الموارد البشرية، ثم مقابلة عبر تطبيق دردشة مع من ادّعى أنه الرئيس التنفيذي، طُلب خلالها تنزيل مهمة برمجية من مستودع شيفرة عبر الإنترنت.

ثبّتت الشيفرة برمجية خبيثة مخصصة لم ترصدها أدوات حماية الأجهزة بحسب بينانس. وعلى نظام macOS استُبدل مكوّن مشروع من أداة تطوير بنسخة خبيثة تتلقى أوامر من خادم يتحكم به المهاجمون، وعمل المهاجمون على إخفاء آثارهم.

وبحلول 20 أكتوبر استخدموا جهاز المهندس وأداة ذكاء اصطناعي داخلية لاختراق موظفين اثنين يعملان على بنية المحافظ، وحصلوا على بيانات اعتماد ورمز نشر للحاويات. وفي 29 أكتوبر استُخدمت هذه البيانات لنشر سكربت خبيث والوصول إلى خدمة توقيع المحافظ.

الاستجابة والسياق

تقول بينانس إنها أعادت بناء الأنظمة المتأثرة واستبدلت الأجهزة المخترقة وألغت بيانات الاعتماد المسروقة، وإن شركات أمنية مستقلة تراجع نتائجها. ويشبه الأسلوب حملات كورية شمالية موثقة مثل Contagious Interview وOperation Dream Job، رغم أن بينانس لم تربط الحادثة بأي منهما.

ما يجب فعله الآن

1. توعية المطورين والمهندس��ن وأصحاب الصلاحيات المرتفعة بأساليب منتحلي صفة مسؤولي التوظيف، واشتراط تشغيل أي اختبار برمجي من جهة خارجية في بيئة معزولة وليس على أجهزة المؤسسة.
2. تقييد تطبيقات الدردشة الشخصية وتنزيل الشيفرات من المستودعات على الأجهزة التي تصل إلى أنظمة الإنتاج أو التوقيع.
3. مراجعة تغطية كشف التهديدات على أجهزة macOS وأجهزة المطورين، بما في ذلك التنبيه عند استبدال ملفات الأدوات التنفيذية أو تعديلها.
4. تقييد الوصول إلى رموز نشر الحاويات وخدمات التوقيع ومراقبته، وتدوير بيانات الاعتماد سريعا عند الاشتباه في جهاز.
5. تقييم ما يمكن لأدوات الذكاء الاصطناعي الداخلية الوصول إليه، وفصل المهام والموافقات حول أنظمة العمليات عالية القيمة.

6. إضافة سيناريو اختراق عبر توظيف وهمي إلى تمارين الاستجابة للحوادث.