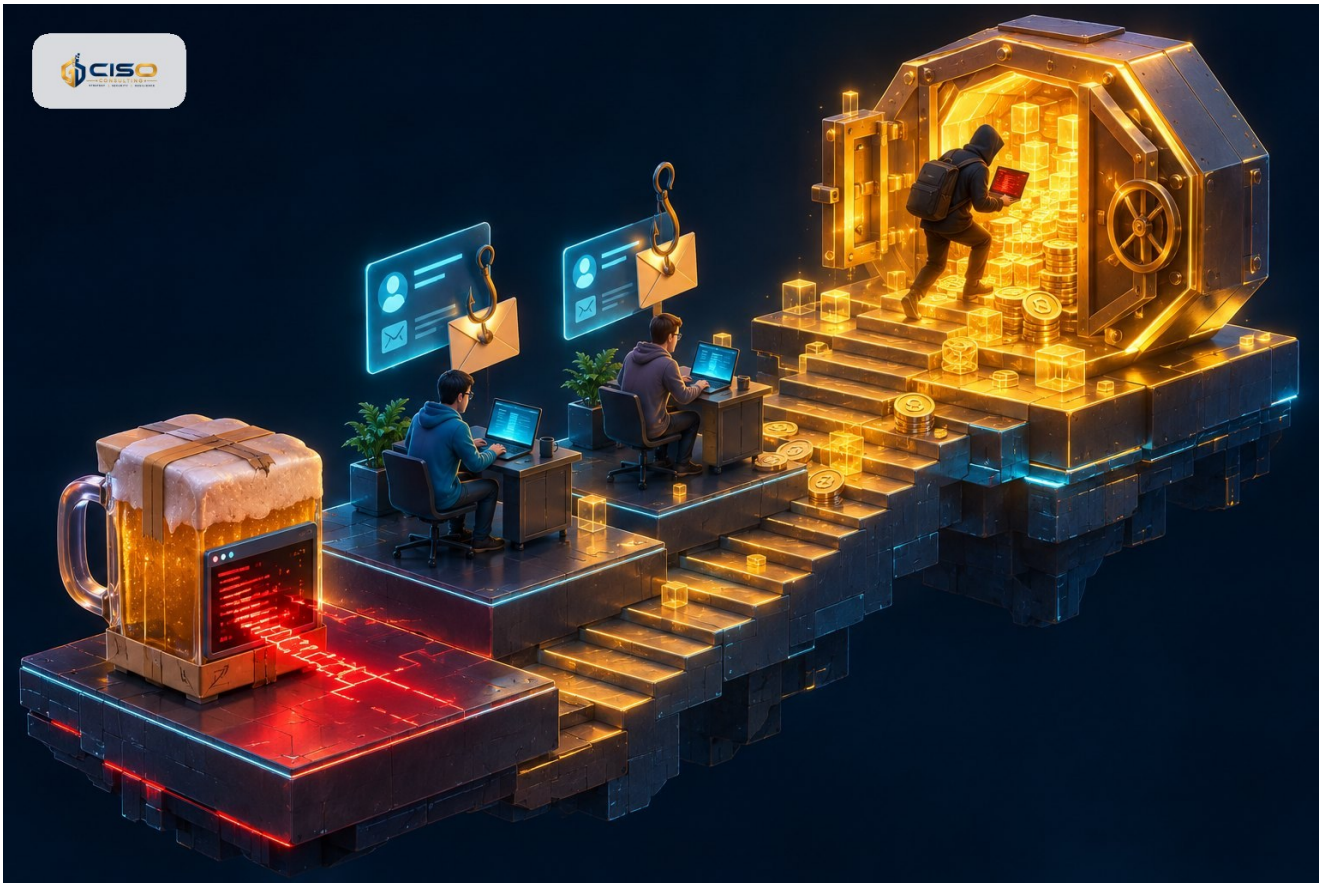
بينانس تكشف حملة متعددة المراحل وراء سرقة بقيمة 6.43 مليار دولار



أفادت بينانس بأن سرقة 6.43 مليار دولار جاءت نتيجة حملة متعددة المراحل لا اختراقاً واحداً، شملت تثبيت Homebrew معدلًا وهندسة اجتماعية بذريعة التوظيف استهدفت مهندسَين.

- أعلنت بينانس سرقة أصول بقيمة 6.43 مليار دولار ووصفتها بأنها رقم قياسي.
- وصفت الشركة الحادثة بأنها حملة متقنة متعددة المراحل وليست اختراقاً منفرداً أو تصيداً بسيطاً.
- استخدم المهاجمون تثبيتاً معدلًا لأداة Homebrew.
- استهدفت الهندسة الاجتماعية بذريعة التوظيف مهندسَين لدى بينانس.

أعلنت بينانس أن سرقة أصول بقيمة 6.43 مليار دولار من منصتها، وهي بحسب وصفها الأكبر في القطاع، كانت المحطة الأخيرة في حملة مدروسة المراحل وليست حادثة منفردة.

ما أعلنته الشركة

بحسب ملخص بيان بينانس المتاح، جمعت الحملة بين تثبيت معدل لأداة **Homebrew** وهندسة اجتماعية قائمة على موضوع التوظيف، واستهدفت مهندسَين اثنين لدى الشركة. وشددت بينانس على أن ما جرى لم يكن اختراقاً منفرداً ولا تصيداً احتيالياً بسيطاً.

ولا يقدم المقتطف المتاح تفاصيل تقنية إضافية، مثل التسلسل الزمني أو كيفية وصول التثبيت المعدل إلى المهندسين أو طريقة تحريك الأصول. لذا ينبغي عدم افتراض تفاصيل تتجاوز ما أعلنته الشركة، ومراجعة المصدر الكامل لمتابعة أي مستجدات.

أهمية الحادثة للجهات المنظمة

يشير النمط المعلن إلى أن العاملين التقنيين ذوي الصلاحيات، والأدوات التي يستخدمونها، قد يكونون مسار هجوم. فالمهندسون الذين يتعاملون مع أنظمة حساسة قد يُستهدفون عبر تواصل وظيفي يبدو مقنعاً وعبر أدوات تطوير تُثبَّت على أجهزتهم. وقد لا تكفي الضوابط التي تركز على التصيد عبر البريد وحده لكشف هذا النوع من الأساليب المتعددة المراحل.

وتحسن الجهات في المملكة التي لديها فرق هندسية داخلية، خصوصاً من تصل إلى أنظمة حرجة أو أصول العملاء، مراجعة حوكمة التواصل الخارجي وتثبيت البرمجيات والوصول ذي الصلاحيات.

ما يجب فعله الآن

1. توعية المهندسين وأصحاب الصلاحيات بأساليب الاستهداف عبر التوظيف، ومنها مقابلات أو مهام وظيفية غير متوقعة تتطلب تثبيت برمجيات.
2. حصر تثبيت أدوات التطوير في مصادر معتمدة ومراجعة استخدام مديري الحزم مثل Homebrew على أجهزة الهندسة.
3. مراجعة صلاحيات المهندسين وتطبيق مبدأ الحد الأدنى من الصلاحيات وفصل المهام للأنظمة القادرة على تحريك الأصول.
4. إدراج سيناريوهات الهندسة الاجتماعية المتعددة المراحل في برامج التوعية وتمارين الاستجابة للحوادث.
5. حث الموظفين على الإبلاغ الفوري لفريق الأمن عن أي تواصل خارجي غير معتاد أو طلب تثبيت غير متوقع.