لائحة اتهام أمريكية: شريك مؤسس لشركة استعادة بيانات متهم بدفع فدى سرًا لعصابات الفدية



وجّهت هيئة محلفين أمريكية اتهامات لشريك مؤسس شركة استعادة بيانات في فلوريدا بدفع مبالغ للمهاجمين سرًا مع ادعائه قدرة شركته على فك التشفير دون فدية. القضية تذكير بأهمية تدقيق مزودي الاستعادة.

- يواجه المتهم ثلاث تهم احتيال عبر وسائل الاتصال، عقوبة كل منها قد تصل إلى السجن 20 عامًا، في مقاطعة رود آيلاند.
- تزعم النيابة أن الشركة ادّعت امتلاك تقنية فك تشفير متطورة وهي غير موجودة، وأنها تفاوضت مع المهاجمين من وراء عملائها.
- في عملية سرية لمكتب التحقيقات الفيدرالي في يونيو 2026، دفع المتهم نحو 6,000 دولار بالبيتكوين مقابل مفتاح، وحاسب الضحية الوهمية بنحو 13,260 دولارًا.
- تفيد النيابة بأن العائدات استُخدمت لشراء عدة عقارات في فلوريدا.

- في يوليو حُكم على مفاوض فدية سابق في DigitalMint بالسجن 70 شهرًا لتسريبه تفاصيل التفاوض إلى مشغّلي ALPHV) BlackCat).

ما الذي تزعمه النيابة

أفادت وزارة العدل الأمريكية بأن هيئة محلفين اتحادية في مقاطعة رود آيلاند وجّهت إلى خوان ريكاردو بالاسيو إسكوبار، الشريك المؤسس لشركة استعادة بيانات في فلوريدا، ثلاث تهم احتيال عبر وسائل الاتصال. وقد أُلقي القبض عليه في لاس فيغاس يوم 22 أكتوبر. وهذه اتهامات لم يصدر بشأنها حكم إدانة.

وتذكر لائحة الاتهام أن الشركة أبلغت ضحايا برامج الفدية بأن لديها تقنية متطورة لفك التشفير تستعيد البيانات دون دفع فدية. وتزعم النيابة أن هذه التقنية غير موجودة، وأنه تفاوض مع المهاجمين دون علم عملائه، ودفع لهم، ثم حاسب العملاء بمبلغ أعلى ليحتفظ بالفارق.

الدليل من العملية السرية

تستند القضية إلى عملية سرية نفذها مكتب التحقيقات الفيدرالي في يونيو 2026، حيث انتحل العملاء صفة شركة تعرضت لهجوم فدية وصفة المهاجم الذي يحتجز بياناتها. ويُزعم أن بالاسيو دفع للمهاجم الوهمي نحو 6,000 دولار بالبيتكوين مقابل مفتاح فك التشفير، ثم حاسب الشركة الوهمية بنحو 13,260 دولارًا، أي أكثر من الضعف.

ويشير المصدر إلى قضية ذات صلة: ففي يوليو حُكم على أنجيلو مارتينو، المفاوض السابق في شركة الاستجابة للحوادث DigitalMint، بالسجن 70 شهرًا لتمريره تفاصيل سرية من المفاوضات، منها حدود وثائق التأمين، إلى مشغّلي ALPHV) BlackCat) الذين استخدموها لرفع مطالب الفدية.

لماذا يهم المؤسسات المنظمة

تتعلق القضيتان بأطراف ثالثة يُوثق بها وقت الأزمة، حين تُتخذ القرارات بسرعة وتحت الضغط. وعلى الجهات التي تعتمد على مختصي استعادة أو تفاوض خارجيين أن تعامل هؤلاء المزودين كموردين عاليي المخاطر، مع شفافية تعاقدية ورقابة على أي تواصل مع المهاجمين.

ما يجب فعله الآن

1. دقّق في أي مزود استعادة بيانات أو تفاوض مع مهاجمي الفدية قبل وقوع الحادث: تحقق من الاعتمادات والمراجع والأساس التقني لادعاءات الاستعادة.
2. اشترط في العقود الإفصاح عن أي تواصل أو دفع للمهاجمين، وإمكانية مطابقة التكاليف مع فواتير المزود.
3. احتفظ بعقد جاهز ومعتمد مسبقًا لخدمات الاستجابة للحوادث لتفادي اتخاذ القرار تحت الضغط مع جهات مجهولة.
4. قيّد الاطلاع على التفاصيل الحساسة، مثل حدود التأمين السيبراني، بمن يحتاجها فقط، وضمّنها في بنود السرية مع الأطراف الثالثة.
5. حافظ على نسخ احتياطية معزولة تُختبر دوريًا وخطة استعادة تقلل الاعتماد على ادعاءات فك التشفير من أطراف خارجية.

6. حدّد خطوات اعتماد داخلية ومراجعة قانونية، بما فيها التنسيق مع الجهات السعودية المختصة، قبل أي قرار يتعلق بدفع الفدية.