لائحة اتهام أمريكية: شركة «استرداد بيانات» من برامج الفدية دفعت للمهاجمين سرًا وضاعفت التكلفة على العملاء



تتهم لائحة أمريكية أحد مؤسسي RansomwareHelp بالادعاء باستخدام أدوات فك تشفير متقدمة بينما كان يشتري المفاتيح سرًا من المهاجمين ويرفع السعر. القضية تذكير بأهمية تدقيق موردي التعافي والتفاوض.

- وُجّهت تهمة الاحتيال عبر الاتصالات إلى المؤسس المشارك ومدير التقنية في RansomwareHelp ومقرها فلوريدا، في لائحة صدرت في رود آيلاند.
- أعلنت الشركة امتلاك أدوات فك تشفير خاصة وعدم دفع الفدية، لكن عملية استدراج للـFBI أظهرت بحسب الاتهام أنها كانت تشتري المفتاح من المهاجمين.
- بحسب الاتهام، حاسبت الشركة الضحية الوهمية بمبلغ 16,010 دولارات مقابل اتفاق على نحو 6,000 دولار بالبيتكوين.

- أفادت شركة أمنية بأن الشركة في حالة عام 2024 طلبت وصولاً عن بُعد غير مقيّد وقدمت عرضًا بقيمة 438,880 دولارًا وتفاوضت سرًا مع Lockbit.
- تأتي القضية بعد ملاحقات أمريكية أخرى لشركات أمنية متهمة بالاحتيال على ضحايا الفدية.

وُجّهت في ولاية رود آيلاند تهمة الاحتيال عبر الاتصالات إلى المؤسس المشارك ومدير التقنية في شركة RansomwareHelp الواقعة في فلوريدا. كانت الشركة تطلب من الضحايا عدم دفع الفدية، وتزعم أن أدواتها التشفيرية الخاصة تستعيد البيانات بنسبة نجاح عالية جدًا. أما لائحة الاتهام فتقول إنها كانت تدفع لمجموعات الفدية مقابل مفاتيح فك التشفير ثم تحاسب الضحايا بمبالغ أعلى بكثير.

ما تقوله لائحة الاتهام

في عملية استدراج نفّذها مكتب التحقيقات الفيدرالي، تقمّص العملاء دور الضحية ودور مجموعة الفدية معًا. وبحسب الاتهام طلبت الشركة من المهاجمين الوهميين أقل سعر ممكن لأداة فك التشفير، ثم أبلغت الضحية الوهمية بأن التكلفة 13,260 دولارًا. وكان السعر المتفق عليه مع المهاجمين نحو 6,000 دولار بالبيتكوين، بينما حوسبت الضحية بمبلغ 16,010 دولارات شاملة رسم تشخيص قدره 2,750 دولارًا.

تجربة إحدى الضحايا

روى بول إيمي من شركة Soteria حالة عام 2024 لشركة محاسبة صغيرة أصابها Lockbit. وذكر أن الشركة أصرّت على وصول عن بُعد غير مقيّد عبر AnyDesk، وقدمت عرضًا بقيمة 438,880 دولارًا مع ادعاءات تقنية غير معقولة، ويبدو أنها حذفت مذكرات الفدية من الشبكة. واكتشفت الضحية لاحقًا أن الشركة تفاوض Lockbit منذ أيام دون إبلاغها. ثم لجأت إلى مزود أكثر رسوخًا ودفعت نحو نصف المبلغ المعروض.

السياق الأوسع

تأتي القضية بعد إجراءات أخرى لوزارة العدل الأمريكية ضد مختصين أمنيين متهمين باستغلال ضحايا الفدية، منها قضايا تخص مسؤولين في Cybersteward وMonsterCloud ومفاوضًا حُكم عليه في يوليو. وهذه اتهامات في قضايا لم يُذكر في المصدر صدور حكم فيها بحق Palacio.

الدرس العملي للجهات المنظمة: ينبغي اختيار موردي الاستجابة للحوادث والتفاوض والتعاقد معهم قبل وقوع الأزمة، مع حدود واضحة للصلاحيات وشفافية كاملة بشأن أي دفعة.

ما يجب فعله الآن

1. أهّلوا مسبقًا مزودي الاستجابة للحوادث والتفاوض مع المهاجمين، وتحققوا من المراجع والمؤهلات والوضع القانوني قبل وقوع الحادثة.
2. اشترطوا الشفافية تعاقديًا: إفصاح كتابي عن أي تواصل مع المهاجمين وأي دفعة والمبالغ الفعلية المدفوعة.
3. لا تمنحوا الموردين وصولاً عن بُعد غير مقيّد؛ استخدموا وصولاً محدود المدة ومسجّلاً وبأقل الصلاحيات وتحت إشرافكم.
4. احتفظوا بمذكرات الفدية الأصلية والأدلة بأنفسكم، وأبقوا قناة التواصل مع المهاجمين تحت سيطرتكم.

5. اعتبروا وعود فك التشفير المضمون أو الشامل إشارة تحذير واطلبوا مراجعة تقنية مستقلة.
6. ضمّنوا قرارات التعامل مع الفدية وإشراك الموردين في خطط الاستجابة وإدارة الأزمات، مع الإبلاغ إلى الهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي عند الاقتضاء.