Chainalysis: الهجوم كشف بيانات اعتماد جميع المستخدمين ورموز الجلسات الفعّالة



أفادت Chainalysis بأن تحقيقها في هجوم سيبراني وكيلي كشف عن أسماء جميع المستخدمين وأسماء الدخول وتجزئات كلمات المرور والرموز الفعّالة، وأنها أوقفت الوصول إلى Datag Reactor Solutions أثناء التحقيق.

- لا يزال التحقيق في الهجوم السيبراني الوكيلي على أنظمة Chainalysis جارياً.
- شملت البيانات المكشوفة جميع المستخدمين: الأسماء وأسماء الدخول وتجزئات كلمات المرور والرموز الفعّالة.
- أوقفت الشركة الوصول إلى Data Solutionsg Reactor خلال التحقيق.
- تذكر الشركة أنه لا يوجد حتى الآن دليل على الوصول إلى بيانات التحقيقات.

ما الذي أُعلن

ذكرت شركة تحليل البلوكتشين Chainalysis أن تحقيقها المستمر في هجوم سيبراني وكيلي استهدف أنظمتها أظهر أن الكشف يشمل جميع المستخدمين، وتتضمن البيانات المتأثرة الأسماء وأسماء الدخول وتجزئات كلمات المرور والرموز الفعّالة.

وأوقفت الشركة أثناء التحقيق الوصول إلى خدمتين هما Reactor وData Solutions. وأكدت أنه لا يوجد حتى الآن دليل على الوصول إلى أي بيانات تحقيقات. ولا يوضح المصدر تفاصيل إضافية عن الهجوم أو توقيته أو عدد المستخدمين.

أهمية الخبر

تمثل الرموز الفعّالة العنصر الأكثر إلحاحاً، فقد يتيح الرمز الصالح الوصول دون كلمة مرور، ولذلك قد لا يكفي تغيير كلمات المرور وحده لإغلاق الثغرة. كما تشكل تجزئات كلمات المرور خطراً إذا كانت كلمات المرور ضعيفة أو مستخدمة في مواضع أخرى.

على الجهات في المملكة التي تستخدم منتجات Chainalysis، مثل أعمال مكافحة الجرائم المالية أو مراقبة المعاملات، أن تتعامل مع الحادثة بوصفها كشفاً لدى طرف ثالث، وأن تتحقق من وضعها مباشرة مع المزوّد دون انتظار مزيد من التفاصيل المعلنة.

النهج المقترح

الخطوات أدناه احترازية وتندرج ضمن معالجة حوادث الأطراف الثالثة والهوية المعتادة. ويمكن تعديل نطاقها متى أكد المزوّد الحسابات والخدمات المتأثرة في جهتكم.

ما يجب فعله الآن

1. تأكدوا من Chainalysis ما إذا كانت حسابات جهتكم وخدماتها متأثرة.
2. ألغوا الرموز والجلسات ومفاتيح API المرتبطة بخدمات Chainalysis وأعيدوا إصدارها.
3. أعيدوا تعيين كلمات المرور للحسابات المتأثرة ولأي أنظمة أخرى استُخدمت فيها كلمات المرور نفسها.
4. فعّلوا المصادقة متعددة العوامل على بوابات المزوّد وراجعوا سجلات الدخول الأخيرة بحثاً عن أي سلوك غير معتاد.
5. وثّقوا الحادثة في سجل مخاطر الأطراف الثالثة وقيّموا ما إذا كانت هناك التزامات إخطار داخلية.