GMO تعرض مكافأة تصل إلى مليون دولار للإبلاغ عن مهاجمي خدمة سطح المكتب السحابي بعد رفضها دفع الفدية



تعرض مجموعة GMO Internet اليابانية مكافآت تصل إلى مليون دولار إجمالًا لمن يدلي بمعلومات تقود إلى مهاجمي خدمة Onamae.com Desktop Cloud، بعد رفضها دفع مبلغ الابتزاز.

- تعرض GMO Internet Group مكافآت تصل إلى مليون دولار إجمالًا مقابل معلومات عن المهاجمين.
- طال الاختراق خدمة Onamae.com Desktop Cloud التي تستضيف أجهزة Windows المكتبية المستخدمة في تداول العملات الأجنبية.
- رفضت الشركة دفع مبلغ الابتزاز المطلوب.
- بدأ برنامج المكافآت في 28 أكتوبر.
- لا تُصرف المكافأة إلا إذا أسهمت المعلومات في القبض على المهاجمين أو في إصدار نشرة

> دولية بالبحث عنهم.

أعلنت مجموعة GMO Internet اليابانية عن مكافآت تصل إلى مليون دولار إجمالًا لقاء معلومات تساعد في تحديد المهاجمين الذين اخترقوا خدمة Onamae.com Desktop Cloud والقبض عليهم. وتفيد الشركة بأنها رفضت دفع مبلغ الابتزاز المطلوب.

ما ورد في المصدر

تستضيف الخدمة أجهزة Windows مكتبية تُستخدم في تداول العملات الأجنبية. وقد بدأ برنامج المكافآت في 28 أكتوبر. والصرف مشروط، إذ لا تُعدّ المعلومات مؤهلة إلا إذا أسهمت في القبض على المهاجمين أو في إصدار نشرة دولية بالبحث عنهم. ولا يتضمن المقتطف المتاح تفاصيل إضافية عن الاختراق أو البيانات المتأثرة أو عدد العملاء أو هوية المهاجمين، لذا لا ينبغي افتراضها.

أهمية الخبر للجهات المنظمة

تتعلق الحادثة ببيئة سطح مكتب مستضافة تُستخدم في التداول، وهو نموذج قد تعتمد عليه بعض المؤسسات المالية وموظفوها أو شركاؤها. كما تُظهر الحادثة جهة ترفض علناً الاستجابة لطلب فدية وتلاحق المهاجمين عبر مكافأة. ويمكن للمؤسسات في المملكة اعتبار الخبر مناسبة لمراجعة مدى اعتمادها على أجهزة سطح المكتب المستضافة، وكيفية استجابتها لمحاولة ابتزاز تستهدف مزوداً لها أو تستهدفها مباشرة.

لا يلزم اتخاذ إجراء بسبب هذه الحادثة تحديداً ما لم تكن الخدمة المتأثرة قيد الاستخدام لديكم. والخطوات أدناه ممارسات عامة سليمة.

ما يجب فعله الآن

1. تحققوا مما إذا كانت أي وحدة أعمال أو جهة خارجية تستخدم Onamae.com Desktop Cloud، وإن وُجد فتواصلوا مع المزود للحصول على إرشادات رسمية.
2. احصروا خدمات سطح المكتب المستضافة أو الافتراضية المستخدمة في التداول أو الأعمال الحرجة، وأكدوا مالكيها.
3. راجعوا تقييمات مخاطر الأطراف الثالثة وشروط العقود مع مزودي الخدمات السحابية، بما فيها التزامات الإبلاغ عن الحوادث.
4. تأكدوا أن خطة الاستجابة للفدية والابتزاز تحدد من يقرر بشأن الدفع، بمشاركة الجانبين القانوني والتنفيذي.
5. تحققوا من اشتراط المصادقة متعددة العوامل للوصول إلى أجهزة سطح المكتب المستضافة ومن الاحتفاظ بالسجلات للتحقيق.