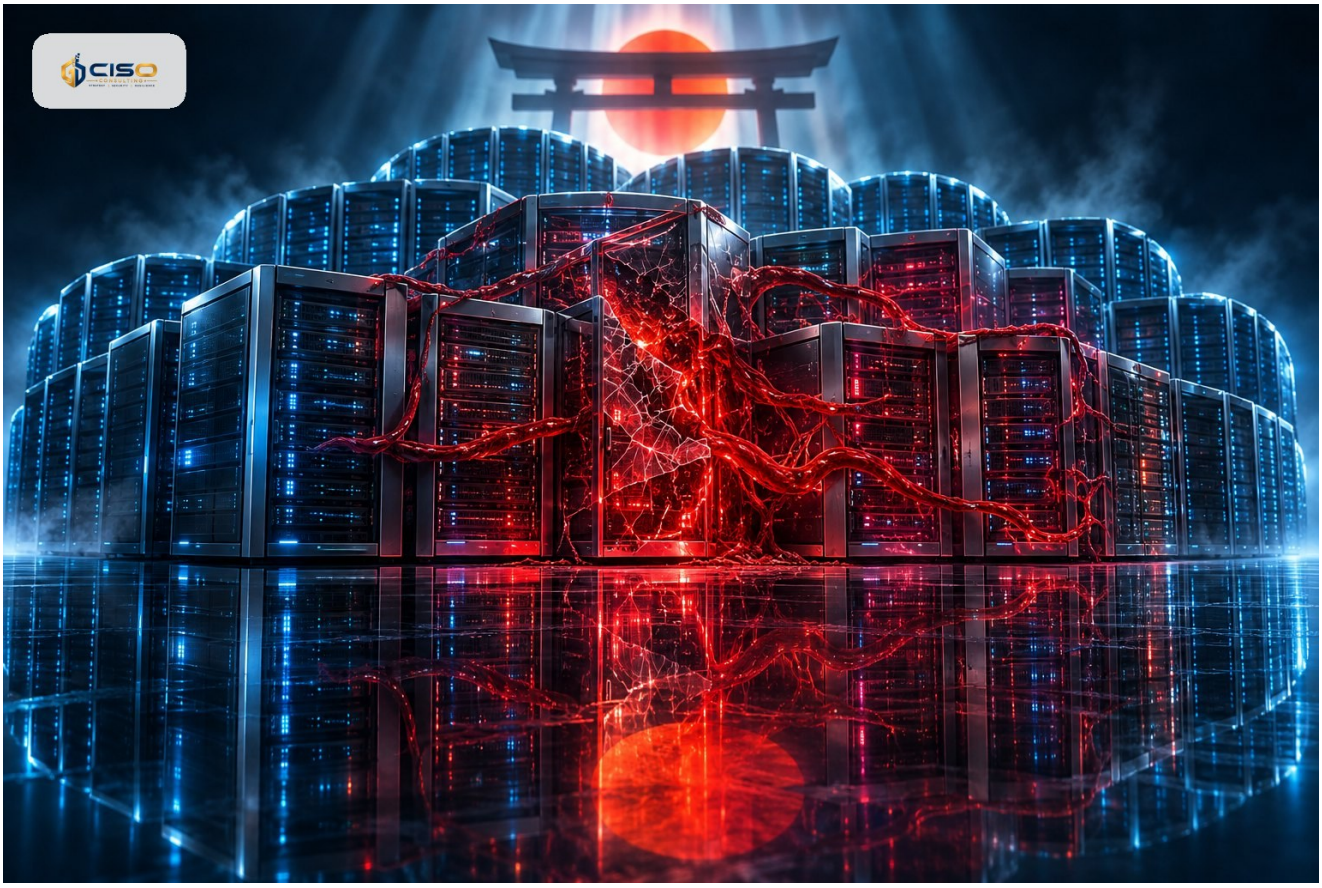
اختراق Onamae Desktop Cloud في اليابان يطال ما يصل إلى 26,739 خادمًا لعملائه



وفق BleepingComputer، اخترق مهاجمون البنية التحتية لمزوّد خدمات VPS الياباني Onamae Desktop Cloud وثبّتوا برمجيات خبيثة على ما يصل إلى 26,739 خادمًا لعملائه.

- تعرّضت البنية التحتية للمزوّد نفسه للاختراق، وليس حسابات عملاء فرادى فقط.
- ثُبّتت برمجيات خبيثة على ما يصل إلى 26,739 خادمًا لدى العملاء.
- يوصف Onamae Desktop Cloud بأنه مزوّد شائع لخدمات VPS في اليابان.
- المقتطف المتاح لا يوضح طريقة الهجوم ولا نوع البرمجية الخبيثة ولا مدى تسرّب البيانات.

ما الذي ورد في التقرير

تفيد BleepingComputer بأن مهاجمين اخترقوا البنية التحتية لـ Onamae Desktop Cloud، وهو مزوّد شائع

لخدمات الخوادم الافتراضية الخاصة (VPS) في اليابان، وثبّتوا برمجيات خبيثة على ما يصل إلى 26,739 خادمًا تخص عملاءه.

المقتطف المتاح من المصدر موجز؛ فهو لا يبيّن كيف حصل المهاجمون على الوصول، ولا ما تفعله البرمجية الخبيثة، ولا ما إذا كانت بيانات العملاء قد اطُّلع عليها. لذلك نقتصر على الوقائع المنشورة دون استنتاجات إضافية.

لماذا يهم المؤسسات الخاضعة للتنظيم

يذكّر الحادث بأن اختراق مزوّد الاستضافة أو VPS قد يصل مباشرة إلى أعباء عمل العملاء. فمنصة المزوّد خارج سيطرة العميل، لكن أثر الحادث يقع على خوادمه وبياناته.

وعلى الجهات في المملكة التي تستخدم استضافة VPS أو خدمات سحابية، محلية كانت أم أجنبية، حتى للأعباء غير الحرجة، أن تعدّ ذلك دافعًا لمراجعة انكشافها على الأطراف الثالثة والخدمات السحابية، لا حادثًا يخص اليابان وحدها.

النهج المقترح

لم يُذكر أي ارتباط بجهات سعودية. والمناسب مراجعة هادئة ومتناسبة: تحديد مزوّدي الاستضافة المستخدمين، ومتابعة ما يصدر عنهم، والتأكد من أن المراقبة لديكم قادرة على كشف أي برمجيات غير متوقعة على الخوادم المستضافة. وتابعوا إشعارات المزوّد الرسمية لمعرفة التفاصيل الفنية متى توفرت.

ما يجب فعله الآن

1. حصر جميع مزوّدي VPS والاستضافة السحابية المستخدمين، بما في ذلك ما تديره وحدات الأعمال.
2. التحقق مما إذا كانت أي أعباء عمل تعمل على Onamae Desktop Cloud، وإن وُجدت فاتباع إرشادات المزوّد الرسمية.
3. التأكد من أن مراقبة الخوادم ونقاط النهاية تشمل نسخ VPS المستضافة وقادرة على رصد البرمجيات غير المتوقعة.
4. مراجعة بنود الإبلاغ عن الحوادث في عقود مزوّدي الاستضافة.
5. التحقق من حداثة النسخ الاحتياطية للأعباء المستضافة وعزلها واختبارها.