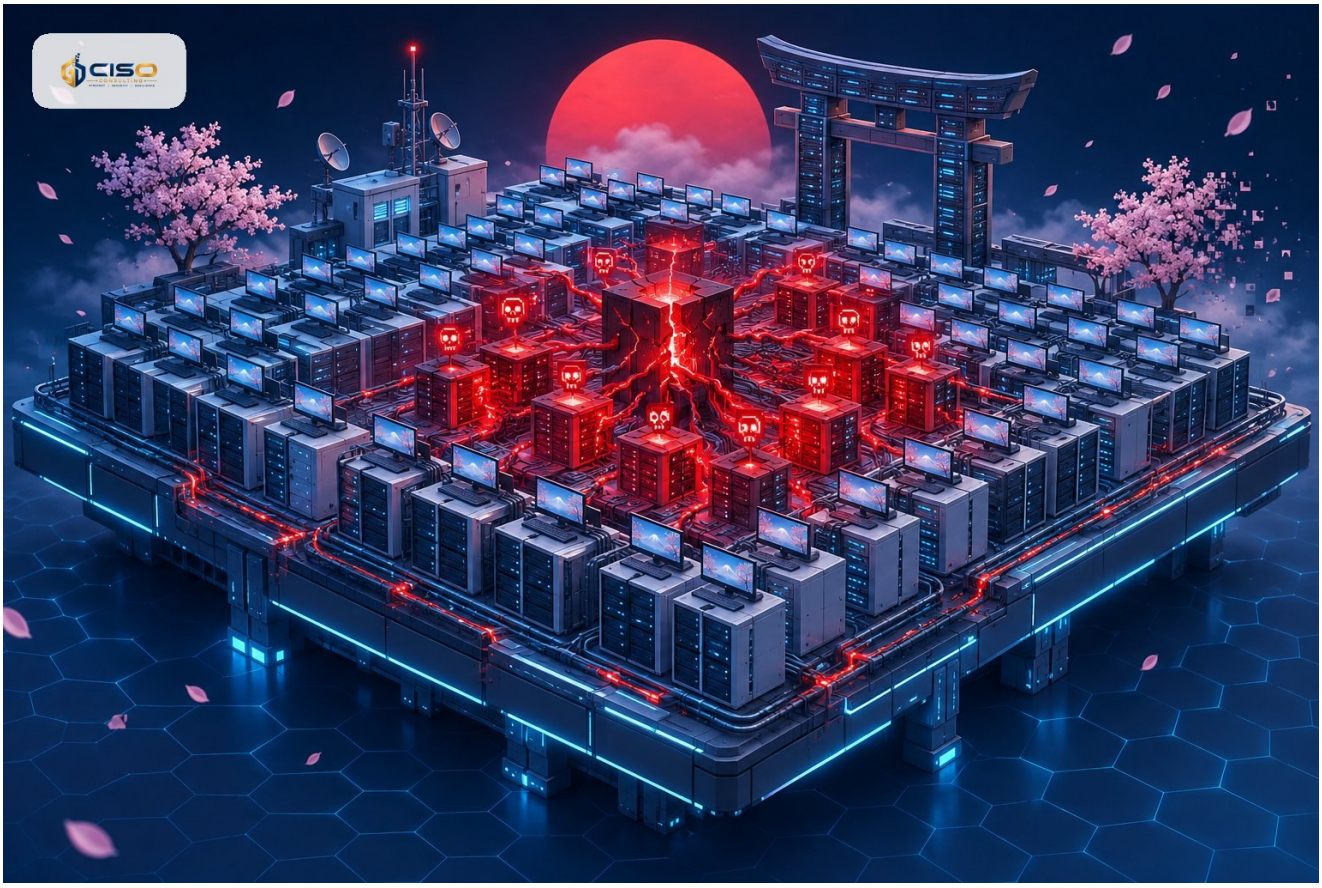
اختراق Onamae Desktop Cloud في اليابان وإصابة ما يصل إلى 26,739 خادمًا لعملاء الخدمة



اخترق مهاجمون البنية التحتية لـ Onamae Desktop Cloud، وهو مزوّد خدمات VPS في اليابان، وثبّتوا برمجيات خبيثة على ما يصل إلى 26,739 خادمًا لعملاء الخدمة، بحسب BleepingComputer.

- يوصف Onamae Desktop Cloud بأنه مزوّد شائع لخدمات VPS في اليابان.
- أُفيد بأن البنية التحتية الخاصة بالمزوّد نفسه تعرضت للاختراق.
- ثُبّتت برمجيات خبيثة على ما يصل إلى 26,739 خادمًا لعملاء الخدمة.
- لا يتضمن المقتطف المتاح تفاصيل عن أسلوب الهجوم أو نوع البرمجية الخبيثة أو الجدول الزمني.

نقلت BleepingComputer أن مهاجمين اخترقوا البنية التحتية لـ Onamae Desktop Cloud، وهو مزوّد شائع لخدمات الخوادم الافتراضية الخاصة (VPS) في اليابان. وبعد ذلك ثبّت المهاجمون برمجيات خبيثة على ما يصل إلى 26,739 خادمًا تخص عملاء الخدمة.

ما المعروف حتى الآن

يؤكد المقتطف المتاح الوقائع الأساسية فقط: اختراق البنية التحتية للمزوّد، وتأثر خوادم العملاء ببرمجيات خبيثة. ولا يوضح كيف دخل المهاجمون، ولا طبيعة البرمجية الخبيثة، ولا موعد الحادثة، ولا ما أبلغ به المزوّد عملاءه. ويُستحسن الرجوع إلى التقرير الكامل وإلى أي إشعار صادر عن المزوّد.

أهمية الخبر للجهات في المملكة

يذكّر الحادث بأن اختراق مزوّد استضافة أو خوادم افتراضية قد يمتد إلى خوادم عملائه، حتى لو كانت إعدادات العميل سليمة. وتتحمل الجهات التي تشغّل أعمالها على خدمات VPS أو سحابية لدى أطراف ثالثة، مباشرة أو عبر مورّديها، مخاطر اعتماد من هذا النوع. ولا يربط المصدر الحادثة بجهات سعودية، لذا فالمطلوب مراجعة هادئة لمدى التعرض لا استجابة طارئة.

المقاربة المقترحة

تحقق مما إذا كانت جهتك أو مورّدوها يستخدمون Onamae Desktop Cloud أو مزوّدين مماثلين، وتأكد من أن حوادث الاختراق على مستوى المزوّد مشمولة في إدارة مخاطر الأطراف الخارجية وخطة الاستجابة للحوادث.

ما يجب فعله الآن

1. تحقق مما إذا كانت جهتك أو مورّدوها الرئيسيون يستخدمون Onamae Desktop Cloud، واطلب منهم تأكيد أي تأثر.
2. حدّث سجل أصول الخوادم الافتراضية وأعباء العمل السحابية المستضافة خارجيًا مع تحديد المالكين وتصنيف البيانات.
3. راجع عقود الأطراف الثالثة ومزوّدي الخدمات السحابية من حيث التزامات الإبلاغ عن الحوادث وحقوق التحقق من الضمانات الأمنية.
4. تأكد من أن خطط الاستجابة للحوادث تغطي حالة اختراق يبدأ من مزوّد الاستضافة.
5. راقب الخوادم المستضافة خارجيًا بحثًا عن عمليات غير متوقعة واتصالات صادرة واستثنائية وتغييرات في الإعدادات.