# GMO Offers Up to $1 Million Reward for Tips on Cloud Desktop Breach After Refusing Extortion




Japan's GMO Internet Group will pay up to $1 million in total for tips leading to the attackers who breached its Onamae.com Desktop Cloud service. The company refused an extortion demand.

- GMO Internet Group is offering up to $1 million in total for tips about the attackers.
- The breach affected its Onamae.com Desktop Cloud service, which hosts Windows desktops used for FX trading.
- The company refused to pay the extortion demand.
- The reward program opened on October 28.
- Payment is made only if a tip helps lead to an arrest or an international wanted notice.

Japan's GMO Internet Group has announced a reward of up to $1 million in total for information that helps identify and catch the attackers who breached its Onamae.com Desktop Cloud service. The company says it refused to pay an extortion demand.

## What the source reports

The service hosts Windows desktops used for FX trading. The reward program opened on October 28. Payment is conditional: a tip qualifies only if it helps lead to an arrest or an international wanted notice. The source excerpt does not give further detail on the intrusion, the data affected, the number of customers or the attackers' identity, so those points should not be assumed.

## Why it matters for regulated institutions

The case involves a hosted desktop environment used for trading, a model that some financial firms and their staff or partners also rely on. It also shows a firm publicly declining an extortion demand and pursuing the attackers through a reward. Institutions in the Kingdom can use the news as a prompt to review how much they depend on hosted desktops and how they would respond to an extortion attempt against a provider or against themselves.

No action is needed in response to this specific incident unless you use the affected service. The steps below are general good practice.

## What to do now

1. Check whether any business unit or third party uses Onamae.com Desktop Cloud, and if so contact the provider for official guidance.
2. Inventory hosted or virtual desktop services used for trading or other critical work, and confirm their owners.
3. Review third-party risk assessments and contract terms for cloud providers, including incident notification duties.
4. Confirm your ransomware and extortion response playbook states who decides on payment, with legal and executive input.
5. Verify that access to hosted desktops requires multi-factor authentication and that logs are retained for investigation.