

TrendAI™ Research Reinforces Japan's Urgent Cybersecurity Warning as Incidents Surge in 2026

Japan-headquartered cybersecurity leader shares threat intelligence and practical guidance as AI accelerates the global threat landscape.

DALLAS, Oct. 12, 2026 /PRNewswire/ -- TrendAI™, the global AI security leader and enterprise business unit of Trend Micro Incorporated (TYO: 4704; TSE: 4704), today issued a threat advisory for organizations in Japan after Masaaki Taira, who chairs the Liberal Democratic Party's National Cybersecurity Strategy Headquarters, said that "cyberspace is in a state of emergency." TrendAI™ Forward-Looking Threat Research data shows Japan recorded more publicly disclosed cybersecurity incidents in the first nine months of 2026 than in all of 2025. September alone saw 86 incidents, up about 18% from August and 37% from July.

The party's headquarters met on Oct. 9 in response to a series of cyberattacks on Japanese businesses and called on the government to strengthen public-private cooperation. Breaches at retailers, financial services firms, a car-sharing service and a rail operator have exposed data of millions of customers. The government's National Cybersecurity Office has sent guidance to ministries, local governments and private companies on keeping security protection up to date, using strong passwords and tightening security across supply chains.

The TrendAI™ Incident Response team has also seen a rise in incidents in Japan. In recent engagements, attackers exploited known vulnerabilities in public-facing applications to plant web shells on web servers, giving them a foothold from which they may attempt privilege escalation, lateral movement or access to connected databases. Japanese-language analysis of these cases from TrendAI™, along with hardening guidance, is available [here](#).

"Cyberattacks are increasing globally, and so are the breaches and data leaks as a result. While AI might not be directly involved, its ability to help the attackers find targets and automate their operations makes cyberattacks scalable. Organizations need to shrink their cyber exposure and close the vulnerabilities in order to lower the odds of being victimized," said Ryan Flores, Co-lead, Forward-Looking Threat Research, TrendAI™.

AI is lowering the cost of attacks. TrendAI™ has not established a connection between the recent incidents in Japan and the use of AI by attackers. However, AI does let attackers accelerate reconnaissance, analyze vulnerabilities and produce convincing phishing in languages they do not speak. This weakens protections that languages, such as Japanese, once offered against foreign attackers. Automation also makes smaller organizations, including suppliers, more attractive targets given the increased return on investment for cybercriminals.

"While organizations around the world learn to work with their AI budgets, it's important to remember that AI has zero cost for cybercriminals," said Robert McArdle, Director, Forward-Looking Threat Research, TrendAI™. "There's already a robust economy for stolen accounts, APIs, and tokens, and this is driving the increasingly automated and agentic cybercrime campaigns we see today. The current surge in Japan should not be interpreted as a peak in criminal activity, it should be seen as the new baseline of attacks that will only increase in volume, speed, and relentlessness."

To harden protections, TrendAI™ recommends:

- **Patch internet-facing systems first.** Keep an accurate inventory of public web servers, applications and cloud services, apply security updates promptly, prioritize vulnerabilities known to be actively exploited, and use virtual patching to cover the gap while fixes are tested and deployed.
- **Harden web servers.** Restrict write access to application code, isolate file-upload directories, prevent uploaded content from running as scripts, and monitor for unauthorized changes to application files and configurations.
- **Watch database access.** Monitor sensitive database operations and abnormal access patterns; run applications with minimum-privilege database accounts.
- **Check suppliers.** Ask hosting and cloud providers how they would notify you of an incident, review which third parties hold customer data, and confirm critical services can recover independently of a single provider.
- **Strengthen identity verification.** Review processes that rely solely on uploaded photographs of identity documents and adopt chip-based or other stronger verification consistent with regulatory guidance.
- **Bring AI usage into scope.** Identify AI applications, models, and agents used across the organization, assess their provenance and reputation, review their access to sensitive data and internal systems, and apply appropriate security controls and approval processes.

TrendAI™ threat researchers and incident responders are tracking the activity behind the current wave of incidents in Japan and will publish further findings as the analysis continues. Organizations that want to discuss their exposure can contact their TrendAI™ account team.

In addition, the TrendAI Vision One™ platform is purpose-built to help organizations address their expanding AI security risks due to shadow AI, sensitive data submitted to external services, or AI agents connected to internal systems with excessive

permissions. Vision One operates on a unified model of visibility, observability, actionability, and governance, spanning endpoints, cloud, identity, data, and AI, giving security practitioners the tools to anticipate and stop threats across their attack surface before they impact the business. To help organizations further identify and reduce AI risk, TrendAI is introducing new capabilities to its Vision One AI security suite in December 2026, including **AI Gateway** and **AI Risk Insights solutions with digital asset reputation scoring**. With the addition of these new controls in Vision One, organizations can holistically achieve:

- **Visibility** — Map AI and the sensitive data it touches.
- **Observability** — Continuously score risk and monitor AI interactions across models, applications, agents, MCP servers, and datasets — detecting and responding quickly to potential attacks.
- **Ownership** — Control AI identity, including establishing ownership and managing access.
- **Governance** — Prove AI risk control and continuous compliance to the board and regulators.

Availability: TrendAI™ Vision One AI Risk Insights, including the AI digital asset reputation assessment capability, is scheduled for general availability in January 2027.

About TrendAI™: TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility, governance, and consolidated security to inspire confidence, drive innovation, and eliminate risk. Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data. Global Fortune 500 companies rely on TrendAI™ to stop threats up to 115 days earlier, powered by world-leading threat and attack intelligence.

Through deep ecosystem partnerships with market leaders like NVIDIA, Anthropic, AWS, Google, and Microsoft, TrendAI™ enables teams to securely move at the speed of AI. AI Fearlessly. Learn more at trendaisecurity.com.

SOURCE TrendAI

For further information: media_relations@trendmicro.com

<https://newsroom.trendmicro.com/2026-10-12-TrendAI-TM-Research-Reinforces-Japans-Urgent-Cybersecurity-Warning-as-Incidents-Surge-in-2026>