TrendAI™ Reports Nation-State Activity in H1 2026 APT Activity Roundup

Generative AI is now sharpening nation-state exploits and powering autonomous reconnaissance, mid-year findings show

DALLAS, July 29, 2026 /PRNewswire/ -- TrendAI™, the global AI security leader and enterprise business unit ofTrend Micro Incorporated (TYO: 4704; TSE: 4704), today released its H1 2026 APT Activity Roundup.

The mid-year findings on the H1 2026 threat landscape showed that AI has moved beyond isolated experiments. Nation states used AI in more stages of the intrusion lifecycle than any other prior half TrendAI™ has tracked. Between January and June 2026, TrendAI™ detected the following APT (advanced persistent threat) nation-state activity:

- **China-aligned threat actors** used generative AI to sharpen exploits and iteratively build malware through vibe coding. One AI agent independently ran its own reconnaissance and lateral movement inside a target network.
- **Russia-aligned Pawn Storm** opened the year with an Office zero-day vulnerability and kept pressing Ukraine and its partners across government, defense, and wartime-aid organizations.
- **DPRK-aligned actors** folded commercial AI into their operations and poisoned a widely used software package to reach downstream developers.
- **Iran-aligned Earth Vetala** scanned for a newly disclosed Ivanti vulnerability within days of its release, and other Iran-aligned actors carried out hands-on attacks against internet-exposed operational technology, tampering with fuel-tank gauges at sites in the United States.

Robert McArdle, Director of Cybercrime Research at TrendAI™: "Artificial intelligence has stopped being a side tool for attackers and has become a teammate embedded in the operation itself. We are watching nation-state actors hand reconnaissance and lateral movement to an AI agent, and use generative models to iterate on malware the way a developer ships code. Defenders now have to assume the adversary on the other end of an intrusion may not be a person typing commands, but a system executing a plan."

Key findings include:

- AI now touches more stages of the intrusion lifecycle, from exploit development to autonomous reconnaissance and lateral movement
- Known and zero-day vulnerabilities are weaponized within days of disclosure, and the software supply chain remains a favored entry point
- Operational technology and physical-world targets — including fuel-tank monitoring systems — are back in attackers' crosshairs
- A newer tracking method, ADINT, harvests location and device data from online ad auctions without deploying any malware
- Threat actors increasingly hide command-and-control on trusted cloud platforms, developer tunnels, blockchains, and paste sites
- Malware-as-a-service and shared tooling make attribution harder, even as nation-state motives remain durable through year end

To read a full copy of the report, visit ourwebsite.

About TrendAI™
TrendAI™, the global AI security leader and enterprise business unit of**Trend Micro**, empowers organizations with full AI visibility and consolidated security that inspires confidence, drives innovation, and eliminates risk. Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data. AI Fearlessly.

trendaisecurity.com

SOURCE TrendAI

For further information: For further information: Trend Micro Communications, media_relations@trendmicro.com

---