Trend Micro Predicts 2026 as the Year Cybercrime Becomes Fully Industrialized

DALLAS, Nov. 25, 2025 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today released its annual *Security Predictions Report* for 2026, warning that the coming year will mark the true industrialization of cybercrime. Artificial intelligence (AI) and automation are now enabling threat actors to run entire campaigns autonomously, from reconnaissance to extortion, creating unprecedented speed, scale, and complexity for enterprise defenders.

To read the full report,* The AI-fication of Cyberthreats - Trend Micro Security Predictions for 2026*, please visit:
https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/the-ai-fication-of-cyberthreats-trend-micro-security-predictions-for-2026

Ryan Flores, Lead of Forward-Looking Threat Research at Trend:"2026 will be remembered as the year cybercrime stopped being a service industry and became a fully automated one. We are entering an era where AI agents will discover, exploit, and monetize weaknesses without human input. The challenge for defenders is no longer simply detecting attacks, it's keeping pace with the machine-driven tempo of threats."

The report highlights how generative AI and agentic systems are transforming the economics of cybercrime. Autonomous intrusion campaigns that adapt in real time, polymorphic malware that constantly rewrites its own code, and deepfake-driven social engineering will be standard tools for attackers. The same automation also threatens to flood businesses with synthetic code, poisoned AI models, and flawed modules hidden inside legitimate workflows, blurring the line between innovation and exploitation.

Hybrid cloud environments, software supply chains, and AI infrastructures are expected to be the primary targets in 2026. Poisoned open-source packages, malicious container images, and over-privileged cloud identities will become common attack vectors, while state-sponsored groups will increasingly turn to "harvest-now, decrypt-later" strategies to future-proof espionage against the advance of quantum computing.

Ransomware is evolving into an AI-powered ecosystem capable of managing itself, e.g. identifying victims, exploiting weaknesses, and even negotiating with targets via automated "extortion bots." Trend threat researchers expect these campaigns to become faster, harder to trace, and more persistent, driven by data rather than encryption alone.

Trend advises organizations worldwide to move from reactive defense to proactive resilience by embedding security across every layer of AI adoption, cloud operations, and supply chain management. Organizations that integrate ethical AI use, adaptive defense, and human oversight will be the ones best positioned to succeed in the future.

Trend's 2026 predictions outline a path forward based on visibility, automation with human validation, and a cultural shift that treats security as strategic infrastructure. Those who innovate securely, by balancing speed with governance and intelligence with ethics, will set the standard for trust and resilience in an increasingly autonomous world.

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information between people, governments, and enterprises. Trend leverages security expertise and AI to protect more than 500,000 enterprises and millions of individuals across clouds, networks, endpoints, and devices worldwide. At the core is Trend Vision One™, the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management and security operations, delivering layered protection across on-premises, hybrid, and multi-cloud environments. The unmatched threat intelligence delivered by Trend empowers organizations to proactively defend against hundreds of millions of threats every day. Proactive security starts here. TrendMicro.com

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---