Proliferation of AI-driven Attacks Anticipated in 2024

Trend Micro urges industry-led regulation and innovative defense strategies

DALLAS, Dec. 5, 2023 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today warned of the transformative role of generative AI (GenAI) in the cyber threat landscape and a coming tsunami of sophisticated social engineering tactics and identity theft powered GenAI tools.

To read more about Trend Micro's 2024 cybersecurity predictions, please visit: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/critical-scalability-trend-micro-security-predictions-for-2024

The widespread availability and improved quality of generative AI is expected to disrupt the phishing market in 2024.

Eric Skinner, VP of market strategy at Trend:"Advanced large language models (LLMs), proficient in any language, pose a significant threat as they eliminate the traditional indicators of phishing such as odd formatting or grammatical errors, making them exceedingly difficult to detect. Businesses must transition beyond conventional phishing training and prioritize the adoption of modern security controls. These advanced defenses not only exceed human capabilities in detection but also ensure resilience against these tactics."

The widespread availability and improved quality of generative AI, coupled with the use of Generative Adversarial Networks (GANs), are expected to disrupt the phishing market in 2024. This transformation will enable cost-effective creation of hyper-realistic audio and video content—driving a new wave of business email compromise (BEC), virtual kidnapping, and other scams, Trend predicts.

Given the potentially lucrative gains* that threat actors might achieve through malicious activities, threat actors will be incentivized to develop nefarious GenAI tools for these campaigns or to use legitimate ones with stolen credentials and VPNs to hide their identities.

AI models themselves may also come under attack in 2024. While GenAI and LLM datasets are difficult for threat actors to influence, specialized cloud-based machine learning models are a far more attractive target. The more focused datasets they are trained on will be singled out for data poisoning attacks with various outcomes in mind—from exfiltrating sensitive data to disrupting fraud filters and even connected vehicles. Such attacks already cost less than $100 to carry out.

These trends may, in turn, lead to increased regulatory scrutiny and a push from the cybersecurity sector to take matters into its own hands.

"In the coming year, the cyber industry will begin to outpace the government when it comes to developing cybersecurity-specific AI policy or regulations," said Greg Young, VP of cybersecurity at Trend. "The industry is moving quickly to self-regulate on an opt-in basis."

Elsewhere, Trend's 2024 predictions report highlighted:

A surge in cloud-native worm attacks, targeting vulnerabilities and misconfigurations and using a high degree of automation to impact multiple containers, accounts and services with minimal effort.

Cloud security will be crucial for organizations to address security gaps in cloud environments, highlighting the vulnerability of cloud-native applications to automated attacks. Proactive measures, including robust defense mechanisms and thorough security audits, are essential to mitigate risks.

More supply chain attacks will target not only upstream open-source software components but also inventory identity management tools, such as telco SIMs, which are crucial for fleet and inventory systems. Cybercriminals will also likely exploit vendors' software supply chains through CI/CD systems, with a specific focus on third-party components.

Attacks on private blockchains will increase as a result of vulnerabilities in the implementation of a number of private blockchains. Threat actors could use these rights to modify, override, or erase entries and then demand a ransom. Alternatively, they could try to encrypt the entire blockchain if it's possible to seize control of enough nodes.

**BEC cost victims over $2.7bn in 2022, according to the FBI.*

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of AI-enabled threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

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

---

https://newsroom.trendmicro.com/2023-12-05-Proliferation-of-AI-driven-Attacks-Anticipated-in-2024