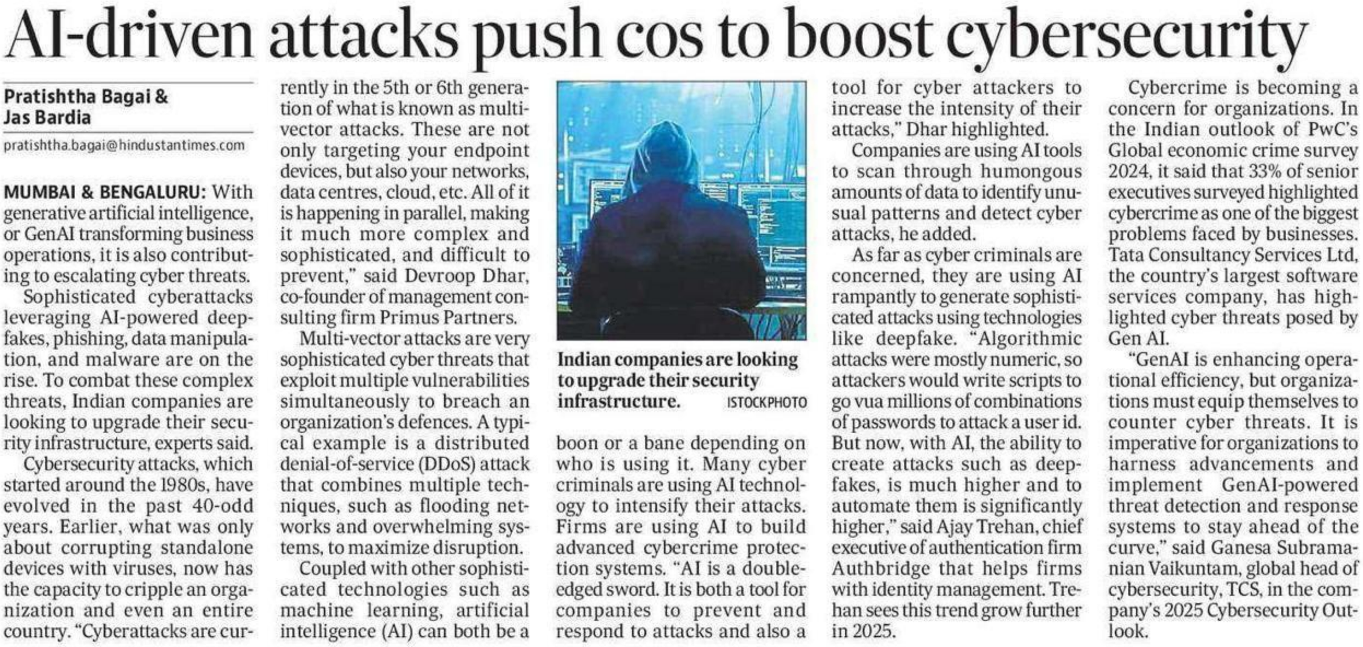
Quote By Devroop Dhar- Co-Founder & Managing Director, Primus Partners

Published in Hindustan Times
Dec 26, 2024

AI-driven attacks push cos to boost cybersecurity

Authored by Pratishtha Bagai & Jas Bardia

Article Content:



AI-driven attacks push cos to boost cybersecurity

Pratishtha Bagai & Jas Bardia
pratishtha.bagai@hindustantimes.com

MUMBAI & BENGALURU: With generative artificial intelligence, or GenAI transforming business operations, it is also contributing to escalating cyber threats.

Sophisticated cyberattacks leveraging AI-powered deepfakes, phishing, data manipulation, and malware are on the rise. To combat these complex threats, Indian companies are looking to upgrade their security infrastructure, experts said.

Cybersecurity attacks, which started around the 1980s, have evolved in the past 40-odd years. Earlier, what was only about corrupting standalone devices with viruses, now has the capacity to cripple an organization and even an entire country. "Cyberattacks are currently in the 5th or 6th generation of what is known as multi-vector attacks. These are not only targeting your endpoint devices, but also your networks, data centres, cloud, etc. All of it is happening in parallel, making it much more complex and sophisticated, and difficult to prevent," said Devroop Dhar, co-founder of management consulting firm Primus Partners.

Multi-vector attacks are very sophisticated cyber threats that exploit multiple vulnerabilities simultaneously to breach an organization's defences. A typical example is a distributed denial-of-service (DDoS) attack that combines multiple techniques, such as flooding networks and overwhelming systems, to maximize disruption.

Coupled with other sophisticated technologies such as machine learning, artificial intelligence (AI) can both be a boon or a bane depending on who is using it. Many cyber criminals are using AI technology to intensify their attacks. Firms are using AI to build advanced cybercrime protection systems. "AI is a double-edged sword. It is both a tool for companies to prevent and respond to attacks and also a tool for cyber attackers to increase the intensity of their attacks," Dhar highlighted.

Indian companies are looking to upgrade their security infrastructure. ISTOCKPHOTO

Companies are using AI tools to scan through humongous amounts of data to identify unusual patterns and detect cyber attacks, he added.

As far as cyber criminals are concerned, they are using AI rampantly to generate sophisticated attacks using technologies like deepfake. "Algorithmic attacks were mostly numeric, so attackers would write scripts to go vua millions of combinations of passwords to attack a user id. But now, with AI, the ability to create attacks such as deepfakes, is much higher and to automate them is significantly higher," said Ajay Trehan, chief executive of authentication firm Authbridge that helps firms with identity management. Trehan sees this trend grow further in 2025.

Cybercrime is becoming a concern for organizations. In the Indian outlook of PwC's Global economic crime survey 2024, it said that 33% of senior executives surveyed highlighted cybercrime as one of the biggest problems faced by businesses. Tata Consultancy Services Ltd, the country's largest software services company, has highlighted cyber threats posed by Gen AI.

"GenAI is enhancing operational efficiency, but organizations must equip themselves to counter cyber threats. It is imperative for organizations to harness advancements and implement GenAI-powered threat detection and response systems to stay ahead of the curve," said Ganesa Subramanian Vaikuntam, global head of cybersecurity, TCS, in the company's 2025 Cybersecurity Outlook.