ET CISO.in
From The Economic Times

2026 will be the year of cognitive threats: Seqrite warns of human-mimicking cyberattacks

A new cybersecurity assessment warns that 2026 may see the rise of AI-driven "cognitive threats" that combine automation with human-like intelligence. These attacks are expected to enable highly personalized phishing, adaptive malware, and direct targeting of AI systems. The analysis stresses the need for organizations to shift from reactive security to intelligence-led resilience to counter increasingly autonomous and deceptive cyber threats.

A recent cybersecurity assessment outlines emerging threat patterns expected to shape the landscape in 2026, highlighting the rise of "cognitive threats" — AI-augmented attacks designed to mimic human behavior with increasing accuracy and autonomy. The report indicates that threat actors are likely to rely more heavily on generative AI to automate reconnaissance, develop convincing social engineering techniques, and maintain persistence while evading conventional detection systems.

Unlike the largely malware-driven attacks seen in 2025, the projected 2026 threat environment is expected to combine automation with adaptive intelligence. These attacks may dynamically adjust tactics in real time, creating a more complex challenge for enterprise security teams.
One of the most significant risks identified is hyper-personalized phishing. Attackers are expected to use generative AI to replicate the communication styles, voices, and visual presence of trusted contacts, increasing the likelihood of successful deception. These techniques may be paired with AI-enabled mobile banking malware capable of automating credential entry, bypassing biometric checks, and executing fraudulent transactions without direct human involvement.

The report also notes that both state-sponsored and organized cybercrime groups are expected to integrate AI across the full attack lifecycle, including vulnerability discovery, payload adaptation, and attribution obfuscation. Such campaigns may allow attackers to modify malware signatures in response to defenses and imitate the behavior of other threat groups to complicate investigation and response.

Beyond traditional targets, AI systems themselves are expected to become a focus of attack. As organizations increasingly deploy AI in areas such as healthcare, finance, manufacturing, and fraud detection, attackers may attempt to manipulate AI models by poisoning training data, introducing logic-based backdoors, or triggering harmful misclassifications. Enterprise AI tools may also be exploited for unauthorized access or data leakage.

The analysis concludes that addressing these emerging risks will require a shift from reactive security models to resilience-focused approaches. Recommended measures include improved predictive intelligence, faster vulnerability remediation, stronger identity controls, protection of AI systems, autonomous detection and response capabilities, assumption-of-breach planning, enhanced threat intelligence sharing, and ongoing user awareness to reduce social engineering risks.

As cyber threats become more adaptive and human-like, the report suggests that security strategies will need to prioritize intelligence, resilience, and speed to keep pace with increasingly autonomous adversaries.