2024 cybersecurity threats: AI-powered malware, deepfakes, and ransomware on the rise

TOI Tech Desk / TIMESOFINDIA.COM / Jun 27, 2024, 16:30 IST

In the first half of 2024, sophisticated cyber threats demand vigilance and advanced security measures, including combating new malware, deepfakes, ransomware-as-a-Service tools, and insecure IoT devices. Proactive cybersecurity strategies are crucial for staying safe online.

The cybersecurity provider, Quick Heal warns of a surge in sophisticated cyber threats in the first half of 2024. New malware leverages artificial intelligence (AI) and bypasses traditional defenses, while deepfakes pose significant misinformation risks.

Quick Heal, drawing on data from Seqrite Labs identified these emerging threats:

- Fileless Malware: This insidious malware exploits legitimate system tools for undetected infiltration. Traditional antivirus scans are ineffective.

- Deepfakes: AI-generated fake videos and audio are used to spread disinformation, damage reputations, and commit financial fraud.

- Ransomware-as-a-Service: Easy-to-use ransomware tools empower a wider range of attackers, leading to a rise in data-encrypting ransomware attacks.

- Insecure IoT Devices: The growing number of internet-connected smart devices creates new vulnerabilities for hackers to exploit in launching large-scale attacks.

Quick Heal urges individuals and businesses to adopt a multi-layered approach to cybersecurity. Their Total Security solution uses advanced technologies like AI and behavioural detection to combat these sophisticated threats.

The report emphasises the need for vigilance. As cybercriminals develop ever-more-complex tactics, robust cybersecurity solutions and user awareness are crucial for staying safe online.