Report on Future of Malware

Nishankumar Kannan

Amity University Rajasthan

Malware with AI refers to malicious software that incorporates artificial intelligence (AI) and machine learning (ML) techniques to evade detection, adapt to new environments, and improve its ability to cause harm. AI-powered malware can be particularly dangerous because it can learn and evolve over time, making it more difficult to detect and remove.

Some examples of AI-powered malware include:

- **Malware.AI**: A detection name produced by the Artificial Intelligence module in Malwarebytes 4 and Malwarebytes business products. These generic malware detections are due to the new automated signature system called BytesTotal and DDS engine that are based on Machine Learning technology with 100% autonomous learning.
- **DeepLocker**: A stealthy AI-powered malware that can infect millions of systems without being detected. It uses AI to recognize specific targets and avoid detection until the precise moment it attacks.
- **AI-enabled malware**: A type of malware that utilizes machine learning and AI to find vulnerable systems, evade detection from security products, and enhance social engineering techniques.

The use of AI in malware can make it more difficult to detect and remove, as it can adapt to new environments and evade detection. Additionally, AI-powered malware can be more targeted and sophisticated, making it more likely to cause significant harm.

However, it's worth noting that AI can also be used to improve malware detection and removal. For example, AI-powered security tools can analyse behaviour patterns and identify potential threats more effectively than traditional signature-based detection methods.

In summary, malware with AI is a growing threat that can be particularly dangerous due to its ability to adapt and evolve over time. It's essential to stay informed about the latest AI-powered malware threats and to use AI-powered security tools to stay protected.