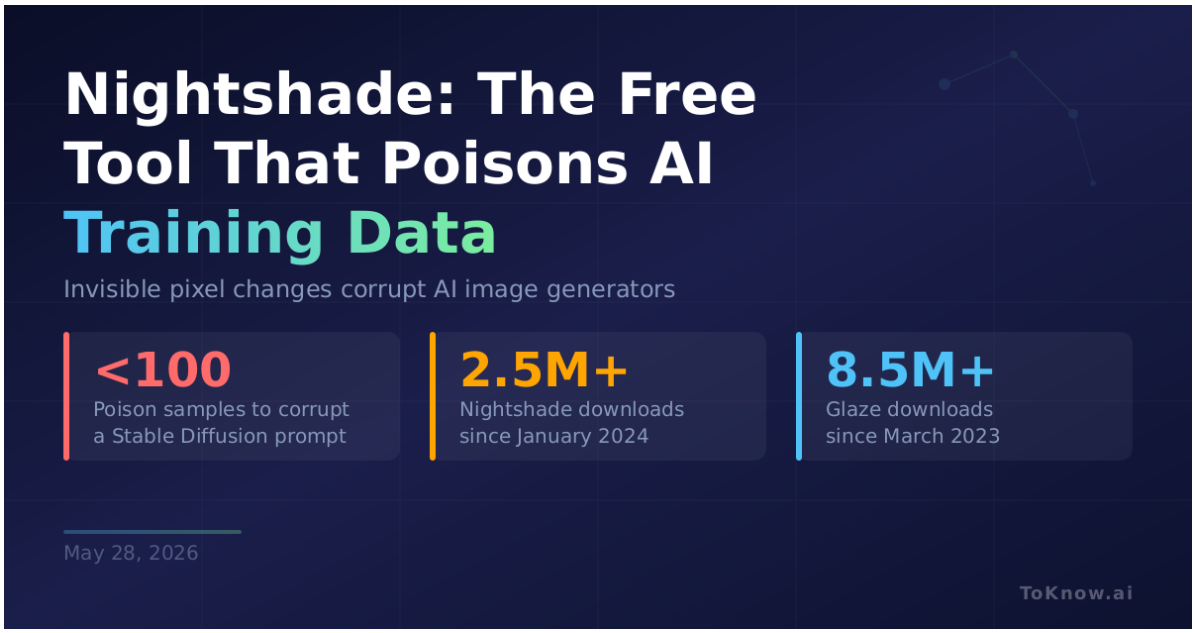
Nightshade: The Free Tool That Lets Artists Poison AI Training Data

Kabui, Charles

2026-05-28

Read at ToKnow.ai



University of Chicago's SAND Lab built Nightshade, a free tool that adds invisible pixel-level changes to artwork before artists post it online. If an AI company scrapes those images for training, the changes teach the model wrong associations: a "dog" prompt produces cats, a "handbag" prompt produces toasters. The technique can corrupt a Stable Diffusion model with fewer than 100 poison samples, and the effects bleed through to related concepts, so

poisoning "fantasy art" also disrupts "dragon" and "castle." The changes survive cropping, compression, screenshots, and resampling. The tool runs completely offline and sends no data back. Version 1.1, released April 2026, fixed Apple Silicon GPU issues and Windows driver bugs. Nightshade has been downloaded over 2.5 million times since January 2024, and its companion tool Glaze (which protects against style mimicry rather than poisoning training data) has passed 8.5 million downloads.

Legal routes like copyright lawsuits and opt-out registries take years and remain largely unenforceable. Nightshade gives individual creators an immediate, technical defense. An illustrator can process their portfolio through both Glaze and Nightshade before uploading, adding mimicry protection and a training-data deterrent in one step. The tool is funded by NSF and DARPA, not venture capital, so there is no business model that depends on eventually charging artists. Lead developer Shawn Shan was named MIT Technology Review's Innovator of the Year for 2024.

Nightshade shifts the economics: as more artists poison their images, the cost of training on unconsented data rises, making it cheaper to license images than to filter out corrupted ones. The bottleneck to protecting creators is no longer technical. It is adoption.

Sources:

- Nightshade Official Site (University of Chicago SAND Lab)
- Nightshade: Prompt-Specific Poisoning Attacks on Text-to-Image Generative Models (arXiv)
- Shawn Shan, MIT Technology Review Innovator of the Year 2024
- This New Data Poisoning Tool Lets Artists Fight Back Against Generative AI (MIT Technology Review)
