Adversarial Patch Generation

Malware

MalPatch

Patch Initialization

①

Patch Injection

②

Malware: 0.957
Benign: 0.043

Malware: 0.021
Benign: 0.979

③

Universal Adversarial Attack

Input → **Apply** → Adversarial Patch → Adversarial Example → **Detected** → Labeled as Benign