# TTP Detail – T1588.007

## TTP Information

Name: Artificial Intelligence

Description: Adversaries may obtain access to generative artificial intelligence tools, such as large language models (LLMs), to aid various techniques during targeting. These tools may be used to inform, bolster, and enable a variety of malicious tasks, including conducting [Reconnaissance](https://attack.mitre.org/tactics/TA0043), creating basic scripts, assisting social engineering, and even developing payloads.(Citation: MSFT-AI)

For example, by utilizing a publicly available LLM an adversary is essentially outsourcing or automating certain tasks to the tool. Using AI, the adversary may draft and generate content in a variety of written languages to be used in [Phishing](https://attack.mitre.org/techniques/T1566)/[Phishing for Information](https://attack.mitre.org/techniques/T1598) campaigns. The same publicly available tool may further enable vulnerability or other offensive research supporting [Develop Capabilities](https://attack.mitre.org/techniques/T1587). AI tools may also automate technical tasks by generating, refining, or otherwise enhancing (e.g., [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027)) malicious scripts and payloads.(Citation: OpenAI-CTI) Finally, AI-generated text, images, audio, and video may be used for fraud, [Impersonation](https://attack.mitre.org/techniques/T1656), and other malicious activities.(Citation: Google-Vishing24)(Citation: IC3-AI24)(Citation: WSJ-Vishing-AI24)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: resource-development