

Microsoft sued individuals who created a service to deceive its AI

"In a complaint filed in the Eastern District of Virginia, we seek actions to stop the activities of cybercriminals who deliberately develop tools specifically designed to bypass the safeguards of generative AI services, including Microsoft, to create offensive and harmful content," the company said.

The service, which operated from July to September 2024, contained detailed instructions on using tools to create illegal content. The perpetrators allegedly used undocumented Microsoft APIs and compromised API keys to access the company's Azure servers, bypassing built-in security controls designed to "prevent the creation of harmful content."

Microsoft also sued seven individuals who allegedly used the service.