IBM joins Project Glasswing as frontier AI attacks push community response

Today's top story, from reporter Sascha Brodsky:

IBM is expanding its AI cybersecurity efforts as executives warn that advanced AI models are dramatically accelerating the speed at which threat actors can identify and exploit software vulnerabilities, shrinking attack timelines from weeks to hours.

The company announced this week that it joined Project Glasswing, a security initiative involving Anthropic and other technology firms aimed at protecting critical software infrastructure. IBM also introduced new AI-driven security tools designed to automate vulnerability detection and response.

"The time to exploit published vulnerabilities a year ago was 23 days on average," Mark Hughes, Global Managing Partner of Cybersecurity Services at IBM, told IBM Think in an interview. "Now, using some of these frontier models, that's gone down to nine hours. So this is real."

Project Glasswing brings together AI companies, software vendors and cybersecurity firms to identify vulnerabilities in widely used software before attackers can exploit them. Participants coordinate fixes, share research and help distribute security patches across open-source projects.

"Through this work, we've been hardening our own products, contributing fixes back to open source, and sharing findings and best practices with other participants," Jamie Thomas, Chief Client Innovation Officer and Enterprise Security Executive at IBM, wrote in a blog post. "This reflects a broader, sustained approach to building resilience against rapidly evolving AI-driven threats."

Pressure on security teams has intensified as generative AI systems have become increasingly capable of analyzing software code and mapping attack paths.

"The fundamental change is that the frontier model AI capabilities allow security vulnerabilities to be discovered, chained together and exploit paths developed," Hughes said. "The window for these models to discover and work out how to exploit vulnerabilities has massively shortened."

Another piece of the strategy involves IBM Autonomous Security, a platform that uses AI agents to automate parts of threat detection and response.

"It won't be simply a question of waiting for a patch to appear," Hughes said. "A lot of the response here is about making sure the existing security controls now operate much more effectively and much faster than they have done before."