Hackers promise AI, install malware instead

May 3 2023

Tech titan Meta says it expects hackers and other malicous actors online to begin using generative artificial intelligence to scale up attacks.

Meta on Wednesday warned that hackers are using the promise of generative artificial intelligence like ChatGPT to trick people into installing malicious code on devices.

Over the course of the past month, security analysts with the social-media giant have found malicious software posing as ChatGPT or similar AI tools, chief information security officer Guy Rosen said in a briefing.

"The latest wave of malware campaigns have taken notice of generative AI technology that's been capturing people's imagination and everyone's excitement," Rosen said.

Meta, the parent company of Facebook, Instagram and WhatsApp, often shares what it learns with industry peers and others in the cyber defense community.

Meta has seen "threat actors" hawk internet browser extensions that promise generative AI capabilities but contain malicious software designed to infect devices, according to Rosen.

In general, it is common for hackers to bait their traps with attention-grabbing developments, tricking people into clicking on booby-trapped web links or downloading programs that steal data.

"We've seen this across other topics that are popular, such as crypto scams fueled by the immense interest in digital currency," Rosen said.

"From a bad actor's perspective, ChatGPT is the new crypto."

Meta has found and blocked more than a thousand web addresses that are touted as promising ChatGPT-like tools but are actually traps set by hackers, according to the tech firm's security team.

Meta has yet to see generative AI used as more than bait by hackers, but is bracing for the inevitability that it will be used as a weapon, Rosen said.

"Generative AI holds great promise and bad actors know it, so we should all be very vigilant to stay safe," Rosen said.

At the same time, Meta teams are working on ways to use generative AI to defend against hackers and deceitful online influence campaigns.

"We have teams that are already thinking through how (generative AI) could be abused, and the defenses we need to put in place to counter that," Meta head of security policy Nathaniel Gleicher said in the briefing.

"We're preparing for that."

© 2023 AFP

Citation: Hackers promise AI, install malware instead (2023, May 3) retrieved 9 April 2024 from https://techxplore.com/news/2023-05-hackers-ai-malware.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.