Google warns hackers are abusing Gemini to accelerate cyberattacks.

Google says that state-backed hacking groups are using Gemini to accelerate cyberattacks, from target research to vulnerability exploitation.

Google says hacker groups are abusing Gemini to speed up the process of carrying out cyberattacks – and this goes beyond simple phishing emails.

In a new report from Google Threat Intelligence Group, the company stated that state-backed hacking groups have used Gemini at various stages of an attack campaign, from initial target research to post-infiltration operations.

This activity involved multiple attack clusters linked to China, Iran, North Korea, and Russia. Google noted prompts and output that included: target profile collection, social engineering phishing content creation, translation, code support, vulnerability testing, and bug fixing when tools malfunctioned during the intrusion process.

Even if it only supports 'everyday' tasks, processing these steps faster can still change the course of an attack.

According to Google researchers, using AI is more about 'accelerating' the process than creating entirely new tactics. Hackers already perform steps such as reconnaissance, crafting deceptive content, modifying malware, and fixing bugs. Gemini simply helps shorten this loop, especially when attackers need to quickly edit content, support languages, or fix code under high pressure.

The report describes an operation linked to China, in which an actor impersonated a cybersecurity expert and requested Gemini to automate vulnerability analysis and build a targeted test plan in a hypothetical scenario. Google also stated that another actor based in China repeatedly used Gemini for debugging, research, and technical guidance to support their intrusion activities.

The risks aren't limited to phishing.

The biggest change Google highlighted is the pace. As attack groups can repeat the process faster – from target selection to tool refinement – ??defense teams will have less time between initial warning signals and actual damage.

This also means fewer gaps due to manual errors, delays, or repetitive operations – signs that could otherwise be detected in system logs.

Google also warned of another threat that is less similar to traditional phishing: model extraction and knowledge distillation. In this scenario, actors with legitimate API access would send a series of prompts to replicate how a model works and reasons, then use that information to train another model.

Google views this as a commercial and intellectual property risk, but if scaled up, it could have far-reaching consequences. The report cites an example of sending 100,000 prompts to replicate the behavior of handling non-English language tasks.

What should businesses monitor?

Google stated that it has disabled accounts and infrastructure associated with the documented Gemini abuse and added targeted defense mechanisms to Gemini's classification system. The company also emphasized its continued testing and maintenance of security layers.

For cybersecurity teams, the practical message is: assume that AI-powered attacks will happen faster, not necessarily 'smarter'. Watch for signs such as a sudden improvement in the quality of phishing content, an unusually rapid pace of tool development, or unusual API access patterns. Simultaneously, incident response processes need to be optimized so that speed doesn't become the attacker's biggest advantage.

You finished reading the article "**Google warns hackers are abusing Gemini to accelerate cyberattacks.**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com