O aplicativo de AI chinês Deepseek criou um respingo no mundo da inteligência artificial que não é visto desde que o Openai introduziu o ChatGPT. Toda a atenção chamada pelo modelo de IA, no entanto, poderia representar uma ameaça ao seu sucesso nos Estados Unidos, como descobriram outras empresas de tecnologia nos países que o tio Sam considera “estados adversários”.

Embora o aplicativo quase não esteja fora do portão de partida, foram levantadas perguntas sobre isso como uma ameaça à segurança nacional. Esses são os tipos de perguntas que afundaram as vendas de empresas como Kaspersky e Huawei e ameaçam o popular aplicativo de mídia social Tiktok.

“(T) ele não pode permitir que modelos de PCC (Partido Comunista Chinês), como a DeepSeek, arrisquem nossa segurança nacional e alavancar nossa tecnologia para avançar em suas ambições de IA. Devemos trabalhar para colocar rapidamente controles de exportação mais fortes sobre as tecnologias críticas à infraestrutura de IA da Deepseek ”, disse ao deputado John Moolenaar, R-Mich., Presidente do Comitê Seleto da China, disse à NBC News na segunda-feira.

Deepseek explodiu em cena no fim de semana, quando se tornou o principal download na App App Store da Apple nos Estados Unidos, saltando AI Stalwart Chatgpt. O aplicativo chinês também tem recebido elogios por sua velocidade, eficiência e poderosas habilidades de raciocínio.

Além disso, ele funciona com fichas menos poderosas do que seus concorrentes dos EUA. De acordo com a DeepSeek, esses chips permitem treinar seu modelo por menos de US $ 6 milhões-uma fração do que o Google, Openai e Meta estão gastando para treinar seus modelos com processadores de primeira linha.

Se as reivindicações da Deepseek sobre seu escrutínio de passagem tecnológica, isso poderá afetar drasticamente a indústria da IA. Pode haver menos demanda por chipsets de alta octanagem, os requisitos de energia poderiam ser reduzidos e haveria menos necessidade de mais centers de escala, como aqueles a serem construídos pelo projeto Stargate de US $ 500 bilhões do governo Trump.

“A Deepseek force uma pergunta sobre os custos e investimentos necessários para competir com resultados e inovações da AGI”, disse Jeff Le, ex -vice -secretário de gabinete da Califórnia.

“Esta corrida também está focada no tempo, mas há consequências de energia e infraestrutura, especialmente se houver validação que forçaria outras pessoas a renunciar ao projeto Stargate recentemente anunciado”, disse ele à Technewsworld.

O que você vai ler:

- Riscos de segurança nacional
- Portal para vazamento de dados
- Camuflagem protecionista

Riscos de segurança nacional

Depois, há uma coisa de segurança nacional que tropeçou em empresas como Huawei, Kaspersky e, mais recentemente, Tiktok.

Em 2018, a Huawei era uma fabricante de smartphones e telecomunicações. Ele empurrou temporariamente a Apple para o terceiro lugar no mercado global de smartphones. No entanto, os smartphones da Huawei foram proibidos de serem vendidos nos Estados Unidos devido a preocupações com a segurança nacional, e sua participação de mercado nunca se recuperou.

Em 2024, o Departamento de Indústria e Segurança do Departamento de Comércio dos EUA proibiu o Kaspersky Lab de fornecer direta ou indiretamente o software antivírus e produtos ou serviços de segurança cibernética nos Estados Unidos ou para nós.

A Repartição constatou que as operações contínuas da empresa nos Estados Unidos apresentaram um risco de segurança nacional – devido às capacidades cibernéticas ofensivas do governo russo e à capacidade de influenciar ou direcionar as operações do Kaspersky.

Depois, há Tiktok, que Washington quer das mãos chinesas por medo de que seu proprietário, Bytedance, possa potencialmente coletar e compartilhar dados confidenciais de usuários americanos com o governo chinês.

Deepseek poderia representar uma ameaça maior à segurança nacional do que a Tiktok, manteve Allie Mellen, analista sênior da Forrester, uma empresa nacional de pesquisa de mercado com sede em Cambridge, Massachusetts. Ela apontou que a política de privacidade da Deepseek afirma explicitamente Entrar, solicitar arquivos, feedback, histórico de bate -

papo ou outro conteúdo ”e use -o para fins de treinamento.

“Ele também afirma que pode compartilhar essas informações com agências policiais, autoridades públicas e assim por diante, a seu critério, e que qualquer informação coletada é armazenada na China”, disse ela à Technewsworld.

“Além disso”, continuou ela, “as informações enviadas à Deepseek são mais amplas. Alguns estão enviando gravações de voz, fotos, informações pessoais e dados corporativos e IP na ferramenta. ”

Portal para vazamento de dados

Rich Vibert, CEO da Metomic, uma empresa de software de privacidade e segurança de dados em Londres, afirmou que a probabilidade de o governo dos EUA proibir Deepseek depende se suas capacidades são percebidas como uma ameaça de segurança nacional.

“Se a ferramenta demonstrar um potencial de exploração em larga escala de vulnerabilidades ou potencial para vazar dados sensíveis, é plausível que as agências regulatórias ou de segurança possam atuar para restringir seu uso”, disse ele à Technewsworld.

Tais vulnerabilidades foram relatadas na segunda -feira pela Kela, uma empresa de inteligência de ameaças israelense. “A equipe AI Red da Kela foi capaz de jailbreak o modelo (Deepseek) em uma ampla gama de cenários, permitindo gerar saídas maliciosas, como desenvolvimento de ransomware, fabricação de conteúdo sensível e instruções detalhadas para criar toxinas e dispositivos explosivos” Empresa relatada em um blog.

“À medida que as tecnologias de IA como a Deepseek se tornam cada vez mais avançadas, os riscos de não garantir dados sensíveis crescem exponencialmente”, disse Vibert.

Ele observou que, embora o Deepseek e o Tiktok suscitem preocupações sobre a segurança dos dados, seus riscos são distintos. “As preocupações com Tiktok se concentram na escala da coleta de dados, com medos em torno de onde e como esses dados são armazenados”, explicou ele. “O DeepSeek, no entanto, representa um risco mais direcionado, pois parece ser projetado para identificar e explorar vulnerabilidades em uma escala enorme”.

A Deepseek estende as preocupações de segurança nacional além das questões de privacidade do consumidor de Tiktok, contestaram Gal Ringel, co-fundador e CEO da Mineos, uma plataforma de governança de dados com sede em Tel Aviv, Israel. “Ele se expande para a exposição potencial de informações comerciais proprietárias, segredos comerciais e informações estratégicas corporativas”, disse ele à Technewsworld.

“Assim como o Tiktok levantou bandeiras vermelhas sobre a exposição aos dados pessoais, as ferramentas de AI da Deepseek aplicam as mesmas regras de risco a informações corporativas sensíveis”, disse ele. “As organizações agora devem auditar e rastrear urgentemente seus ativos de IA para impedir a exposição potencial de dados à China”.

“Não se trata apenas de saber quais ferramentas de IA estão sendo usadas”, continuou Ringel. “Trata -se de entender onde os dados da empresa fluem e garantir que as salvaguardas robustas estejam em vigor, para que não acabe inadvertidamente nas mãos erradas”.

“Os paralelos com Tiktok são impressionantes, mas as apostas podem ser ainda maiores ao considerar a exposição potencial de dados comerciais que acabam em mãos adversárias”, acrescentou.

Camuflagem protecionista

As preocupações com a segurança nacional também podem ser usadas para camuflar as políticas protecionistas, a maneira como a Apple foi protegida da Huawei e as roupas de mídia social de hoje estão sendo protegidas do Tiktok.

“Trump é totalmente imprevisível, por isso não sabemos o que vai acontecer em termos de proibição”, disse Greg Sterling, co-fundador da Near Media, uma empresa de pesquisa de mercado em São Francisco.

“Eu acho que é um pouco prematuro especular, mas o armazenamento dos dados dos EUA em servidores chineses com acesso total pelo governo chinês faz com que pelo menos o risco de segurança que Tiktok é”, disse ele à Technewsworld.

“A mesma lógica aplicada aqui se aplicaria teoricamente a qualquer aplicativo chinês”, acrescentou. “Então, o governo deve decidir qual é a política geral. A UE não permitirá que os dados do cidadão da UE sejam para os servidores dos EUA. Os EUA podem assumir uma posição semelhante com os aplicativos chineses e proibir completamente aqueles que representam os riscos mais significativos. ”