

Bruno Castro (VisionWare): “O malware g...

lidermagazine.sapo.pt/bruno-castro-visionware-o-malware-gerado-por-ia-e-significativamente-mais-perigoso

24 de maio de 2023

[Home](#) › [Artigos](#) › [Leading Tech](#) › [Notícias](#) › Bruno Castro (VisionWare): “O malware gerado por IA é significativamente mais perigoso”

Artigos

Bruno Castro (VisionWare): “O malware gerado por IA é significativamente mais perigoso”



24 Maio, 2023 | 2 minutos de leitura

O Future of Life Institute (FLI) tornou-se o centro das atenções, quando em março último lançou um alerta global: *“Pause Giant AI Experiments. We call on all AI labs to immediately pause for at least six months the training of AI systems more powerful than GPT-4”*.

A Carta Aberta, em jeito de Manifesto, pede uma pausa de seis meses no desenvolvimento dos Grandes Modelos de Linguagem (LLMs), nomeadamente o Chat GPT.

Está-se a ir rápido de mais. Será?

Bruno Castro é CEO da VisionWare, empresa 100% portuguesa, especializada em segurança de informação. O responsável ressalta a necessidade de a defesa digital das empresas obrigar a uma maturidade de cibersegurança. Na sua perspetiva, com a pandemia, instalou-se uma nova crise cibernética: a transformação digital ocorreu rapidamente, e a segurança ficou para trás.

Para a revista Líder, colocamos o desafio:

Como podem estes seis meses de interrupção prevenir um ataque da máquina sobre o Homem? Faz sentido parar? O que pode significar o futuro do ChatGPT e dos Grandes Modelos de Linguagem (LLMs)? O que é realmente urgente?

“Considero a Inteligência Artificial um dos campos de desenvolvimento tecnológico mais importantes da atualidade. Embora tornando as nossas vidas muito mais fáceis e ágeis, a tecnologia que possuímos hoje, e continuamos a melhorar, pode ter consequências terríveis para o futuro da cibersegurança – daí a existência do malware ChatGPT. Falo sobre os riscos da utilização do ChatGPT e que um programa melhorado como este pode ser perigoso nas mãos erradas.

Muitas redes na darkweb já levaram à utilização do chatbot para eliminar malware e facilitar ataques de ransomware. Estas preocupações são ainda mais prementes, quando os gigantes da indústria estão dispostos a investir fortemente em tecnologia de IA.

O malware gerado por IA é significativamente mais perigoso do que o malware tradicional já que: é mais fácil de criar; é acessível a todos; é capaz de produzir resultados automaticamente; e pode ser manuseado com maior facilidade. Parece que vivemos tempos muito desafiantes no campo da (inovação da) segurança cibernética, quando a nossa aliada Inteligência Artificial acaba por se revelar a principal inimiga de quem nos protege”

Este artigo foi publicado na edição de primavera da revista *Líder*.

Subscreva a Líder [AQUI](#).