NOVO Semanário
Original e Livre

NOVO Semanário, edição impressa, 28 de janeiro de 2023

Empresas de cibersegurança preparam defesa contra o ChatGPT

A nova ferramenta tecnológica pode ser usada para escrever uma música, mas também para ataques de *phishing* a uma escala industrial. "O que me preocupa mais é que seja utilizado o mesmo tipo de tecnologia para criar novas ferramentas de ataque", refere a VisionWare, empresa que já está a participar num projecto europeu para utilizar *machine learning* na sua defesa

Rodolfo Alexandre Reis
reis@medianove.com

Pode servir para escrever uma música ou ter a capacidade de gerar praticamente qualquer tipo de texto com base no pedido do utilizador, mas, nas mãos erradas, o ChatGPT pode permitir aos *hackers* gerar *emails* de *phishing* persuasivos e personalizados a uma escala industrial. "Estamos a assistir a um salto tecnológico grande. Agora, não sei se é possível, neste momento, prever o que pode acontecer", refere, em declarações ao NOVO Economia, Filipe Custódio, *partner* da VisionWare, empresa portuguesa especializada em cibersegurança.

Para o responsável, ter uma ferramenta com acesso a grande parte do conhecimento do mundo significa que um maior número de pessoas rapidamente vão conseguir fazer co-relações e relações entre ataques passados e novos. "Vai servir quer os atacantes, quer os defensores. A questão é saber quem vai aproveitar em primeiro lugar", afirma o especialista.

A empresa tecnológica Kaspersky – reconhecida criadora de antivírus – está a analisar as formas como o ChatGPT poderá ser utilizado nas mãos do público em geral e como o programa vai alterar as regras do mundo da cibersegurança.

Filipe Custódio considera que é impossível prever aquilo em que esta ferramenta se vai tornar. "O ChatGPT é apenas a demonstração de uma tecnologia. Preocupa-me pouco que *hackers* utilizem o ChatGPT para modificar novos tipos de ataque, porque não é previsível que isso aconteça. O que me preocupa mais é que seja utilizado o mesmo tipo de tecnologia para criar novas ferramentas de ataque", explica. E dá o exemplo de um *hacker* que consiga fazer automaticamente aquilo que hoje se faz manualmente, ou seja, andar sistematicamente à procura de falhas nas defesas da vítima, para depois conseguir inventar novas formas de atacar.

"Não consigo dizer se esta ferramenta vai ser boa ou má. Vamos ter de ver nos próximos tempos que ferramentas vão ser feitas com base nesta tecnologia, quer para ataque, quer para defesa", salienta o responsável.

De acordo com a Kaspersky, muitos utilizadores já descobriram que o ChatGPT é capaz de gerar códigos, mas, indefinidamente, isso inclui códigos de *malware*. A criação de um simples *infostealer* (*software* utilizado para roubar informações) será possível sem serem necessárias quaisquer habilitações de programação. No entanto, a maioria dos utilizadores não têm muito a temer. Se o código escrito por um *bot* for realmente utilizado, as soluções de segurança irão detectá-lo e neutralizá-lo tão rapidamente como hoje fazem com todo o *malware* criado por humanos.

Filipe Custódio, *partner* da VisionWare

> "Não consigo dizer se esta ferramenta vai ser boa ou má. Vamos ter de ver nos próximos tempos que ferramentas vão ser feitas com base nesta tecnologia, quer para ataque, quer para defesa"

No entanto, e apesar deste cenário apresentado pela tecnológica russa, Filipe Custódio acredita que em breve irá existir uma mudança tecnológica nos ataques. "Ou seja, vão começar a surgir ataques mais violentos e difíceis de parar com base nesta tecnologia", realça.

Para a Kaspersky, alguns analistas estão preocupados com a possibilidade de o ChatGPT poder vir mesmo a criar um *malware* único para cada vítima em particular, mas salientam que essas amostras ainda exibiriam um comportamento malicioso que, muito provavelmente, será detectado por um programa de segurança.

Apesar disso, o responsável da VisionWare aconselha todas as empresas portuguesas a iniciarem uma preparação para enfrentar esta nova ferramenta, de forma que possam proteger as suas informações, dando o exemplo daquilo que já está a ser aplicado na VisionWare.

"No caso da VisionWare estamos a participar num projecto europeu que visa a utilização do *machine learning* na defesa, ou seja, para tentar identificar este tipo de ataques mais avançados e conseguir dinamicamente lançar defesas antes de os ataques terem sucesso", conclui.