CHATGPT ACELERA A DISPUTA ENTRE GANGUES DIGITAIS E TIMES DE CYBER SECURITY PELO DOMÍNIO DA IA

ChatGPT é um modelo de linguagem de Inteligência Artificial (IA) desenvolvido pela OpenAI para processar linguagem natural e responder a perguntas e conversas online. Embora o ChatGPT não armazene dados de usuários, nem tenha acesso a informações pessoais, a menos que lhe sejam providas, gangues digitais podem utilizar técnicas de engenharia social e outras táticas para enganar os usuários e obter informações confidenciais. A história da humanidade prova que todas as ferramentas tecnológicas podem ser usadas para fins negativo

As estratégias das gangues digitais para manipular o Chat GPT são variadas:

Desenvolvimento de malware

O ChatGPT pode ajudar no desenvolvimento de malware. Algumas pesquisas mostram que os autores de malware podem também desenvolver software avançado com o ChatGPT, como um vírus polimórfico, que altera seu código para escapar de detecção.

E-mails de phishing

Um e-mail autêntico do banco do usuário tem pouca probabilidade de ser mal escrito, com erros de gramática, por exemplo. Há uma preocupação legítima de que hackers usarão ChatGPT para escrever e-mails de phishing que pareçam ter sido escritos por um profissional.

Impostura

Em poucos segundos o ChatGPT pode escrever textos com a expressão e o estilo de uma pessoa real. A capacidade do ChatGPT de fazer-se passar por pessoas poderia resultar em fraudes mais convincentes. É um fato o crescente número de esquemas falsos de criptomoedas de Elon Musk que trapaceiam investidores amadores para tirar-lhes milhões. Tais esquemas seriam ainda mais atraentes quando escritos com o estilo de Elon por um chatbot de IA.

Spam

Pessoas que enviam spam costumam dedicar poucos minutos a escrever o texto. Com o ChatGPT, elas podem ampliar seu fluxo de trabalho gerando textos de spam instantaneamente. Embora a maioria dos spams seja inofensiva, alguns podem conter malware ou levar os usuários a websites maliciosos.

Ransomware

Muitos dos criminosos não escrevem seu próprio código. Em vez disso, eles o compram de criadores de ransomware em mercados da Dark Web. É possível que, daqui em diante, essas gangues deixem de depender de terceiros. Alguns pesquisadores descobriram que o ChatGPT pode ser bem-sucedido em escrever código malicioso capaz de criptografar um sistema inteiro em um ataque de ransomware.

Roubo de dados

Os criminosos usam diversas ferramentas e técnicas para roubar dados. A capacidade do ChatGPT de fazer-se passar por outras pessoas, escrever textos sem erros e criar código pode ser usada indevidamente por qualquer pessoa que tenha intenções maliciosas.

BEC (Business email compromise, Comprometimento de e-mail empresarial)

Comprometimento de e-mail empresarial (BEC) é um tipo de ataque de engenharia social no qual um criminoso usa e-mail para enganar alguém da organização, levando a pessoa a compartilhar dados confidenciais da empresa ou enviar dinheiro. Os software de segurança costumam detectar ataques de BEC identificando padrões. Entretanto, um ataque de BEC criado com ChatGPT poderá burlar filtros de segurança.

Para reduzir os riscos de segurança cibernética associados ao ChatGPT é importante seguir algumas práticas de segurança. Isso inclui não fornecer informações pessoais confidenciais ao ChatGPT, não clicar em links suspeitos enviados por meio da plataforma e manter atualizado o software de segurança do dispositivo do usuário.
Embora o ChatGPT possa ser usado de maneira negativa, é um erro estigmatizar essa ferramenta e suas irmãs, plataformas como DALL-E 2, Microsoft Bing e Chatsonic. Vale destacar que há cada vez mais desenvolvimentos de IA ao alcance dos usuários, algo que promete uma diversificação de sistemas nunca vista antes.

Inteligência Artificial para vencer ataques baseados em Inteligência Artificial

Em muitos casos, a melhor estratégia para vencer ameaças cibernéticas construídas com apoio de IA é usar soluções do mesmo naipe para proteger a organização. Estudo da Precedence Research indica que o tamanho do mercado global de Inteligência Artificial em segurança cibernética foi avaliado em USD 17,4 bilhões em 2022 e deve atingir algo em torno de USD 102,78 bilhões até 2032. A razão para isso é clara: as técnicas de IA são muito promissoras nas áreas de análise, detecção e resposta às ameaças.

Hoje, grandes empresas usuárias já estão investindo em IA, mas, por não terem pessoal interno qualificado, nem sempre conseguem colocar em prática seus projetos. Estudo da (ISC) 2 de janeiro de 2023 indica que, em todo o mundo, há uma demanda por mais de 3,4 milhões de profissionais de cibersegurança. Uma parte desse total diz respeito a vagas em aberto na área de projeto, implementação e gestão de soluções de segurança baseadas em IA. A implementação de um sistema de IA exige conhecimento técnico para lidar com

raciocínio complexo de máquina e, a partir de uma abordagem customizada para cada negócio, implementar a solução de cibersegurança IA que contemple a heterogeneidade da organização. A escassez de talentos treinados é um dos maiores desafios para o avanço dos projetos de IA em todos os setores, seguida por falta de financiamento, falta de acesso à tecnologia apropriada e falta de acesso a dados de usuários.

Por mais que a jornada de adoção de soluções de segurança baseadas em AI tenha questões a serem equacionadas, parece haver um consenso em relação ao valor que esta tecnologia aporta ao time de ICT Security. Sua capacidade de aplicar, em escala, técnicas avançadas de análise e baseadas em lógica pode aliviar a carga sobre os gestores de segurança. A meta é ajudar esses profissionais a atuar de forma proativa e preditiva contra ameaças construídas com ajuda de plataformas de AI.

Análise comportamental de usuários

A análise do comportamento de usuários e entidades (UEBA – User Entitity Behavior Analysis), por exemplo, pode ajudar a detectar pessoas internas mal-intencionadas, bem como invasores externos hostis que se infiltram na rede e em seus ativos.

A análise do tráfego da rede é outra área em que a IA pode brilhar. Na economia digital o volume do tráfego da rede costuma ser massivo – por isso, levar a cabo uma análise exaustiva e contínua somente com esforços humanos torna-se impossível. Técnicas avançadas de IA e ML (Machine Learning), como a análise de big data, podem ajudar a detectar malware e ameaças avançadas com alto grau de precisão, inclusive as mutações e variantes.

Seja por meio do Chat GPT, seja através de outras plataformas, a Inteligência Artificial veio para ficar, e intensificou ainda mais a guerra cibernética. Cabe aos gestores das organizações estudarem estratégias para garantir que essa tecnologia produza crescimento, e não as perdas em cascata causadas por ataques automatizados e customizados baseados em IA.