Os Invasores Abusam de Ferramentas de IA para Gerar CAPTCHAs Falsos

Data: 2025-09-19 18:45:22

Autor: Inteligência Against Invaders

Os cibercriminosos estão abusando das plataformas de IA para criar e hospedar páginas CAPTCHA

falsas para aprimorar as campanhas de phishing, de acordo com uma nova pesquisa da Trend

Micro.

Os invasores estão explorando a facilidade de implantação, hospedagem gratuita e marca confiável oferecida por essas plataformas para configurar essas páginas em velocidade e escala.

O páginas CAPTCHA falsas Redirecione as vítimas para sites maliciosos hospedados pelos invasores. Essa abordagem aumenta a probabilidade de sucesso dos ataques de phishing, pois a aparente verificação de segurança de rotina faz com que o link malicioso pareça mais legítimo para a vítima e ajude a contornar as ferramentas de segurança.

O uso de plataformas de IA para essas páginas tem sido observado desde janeiro de 2025, aumentando acentuadamente de fevereiro a abril, de acordo com dados da Trend Micro.

Os pesquisadores destacaram o uso de três plataformas baseadas em IA pelos invasores – Lovable, que permite que qualquer pessoa crie e hospede aplicativos com pouco ou nenhum conhecimento de codificação, e Netlify e Vercel, que são plataformas de desenvolvimento nativas de IA.

A Vercel foi vinculada a 52 e-mails de phishing, a Lovable 43 e a Netlify três.

Os pesquisadores observaram que essas ferramentas de IA permitem que os invasores configurem sites CAPTCHA falsos convincentes com habilidades técnicas mínimas.

“No Lovable, os invasores podem usar a codificação vibe para gerar um CAPTCHA falso ou uma página de phishing, enquanto o Netlify e o Vercel simplificam a integração de assistentes de codificação de IA no pipeline de integração contínua/entrega contínua (CI/CD) para produzir páginas CAPTCHA falsas”, explicaram os pesquisadores.

Além disso, a disponibilidade de níveis gratuitos nessas plataformas reduz o custo de entrada para iniciar essas sofisticadas operações de phishing.

“O aumento do phishing CAPTCHA falso destaca como os invasores estão armando plataformas de

criação de sites com inteligência artificial. Embora esses serviços impulsionem a inovação para desenvolvedores legítimos, eles também podem fornecer aos cibercriminosos as ferramentas para lançar ataques de phishing em escala, rapidamente e a um custo mínimo", escreveram os pesquisadores da Trend Micro em um blogue publicado em 19 de setembro.

Como funcionam as campanhas de phishing

As campanhas de phishing geralmente começam com e-mails de spam com mensagens urgentes, como "Redefinição de senha necessária" ou "Notificação de mudança de endereço do USPS".

Clicar no URL incorporado direciona o alvo para uma aparente página de verificação CAPTCHA – isso serve ao duplo propósito de fazer com que o link pareça mais legítimo e ajudar a contornar as ferramentas de detecção, pois os scanners automatizados que rastreiam a página encontram apenas um CAPTCHA.

Depois que o CAPTCHA é concluído, a vítima é redirecionada para a página de phishing real, onde suas credenciais e outros dados confidenciais podem ser roubados.

A Trend Micro forneceu uma série de recomendações para as organizações sobre como mitigar os riscos de campanhas de phishing baseadas em captcha:

- Instrua os funcionários sobre como identificar tentativas de phishing baseadas em captcha, incluindo a verificação de URLs antes de interagir com captchas
- Implementar defesas capazes de analisar cadeias de redirecionamento
- Monitore domínios confiáveis em busca de sinais de abuso rastreando o tráfego para seus subdomínios