Geradores de sites de IA reaproveitados por adversários para campanhas

Data: 2025-08-21 22:44:53

Autor: Inteligência Against Invaders

Os adversários estão usando os construtores de sites movidos a IA para acelerar o desenvolvimento de infraestrutura prejudicial em um cenário de ameaças em rápida mudança, reduzindo assim as barreiras de entrada para distribuição de malware e phishing de credenciais.

Plataformas como o Loveable, que permitem aos usuários gerar sites totalmente funcionais por meio de avisos de linguagem natural, foram observados em inúmeras campanhas desde o início de 2025.

Essas ferramentas, projetadas para facilitar o uso com hospedagem gratuita sob o adorável[.]domínio do aplicativo, permita que até atores iniciantes implantem sofisticados kits de phishingcarregadores de malware e sites de fraude sem habilidades avançadas de desenvolvimento da Web.

Ameaças emergentes no cibercrime cibernético assistido pela AI

Os pesquisadores do ProofPoint documentaram dezenas de milhares de URLs adoráveis ??maliciosos no tráfego de e -mail mensalmente, direcionando organizações com iscas que representam marcas confiáveis ??como Microsoft, UPS e plataformas de criptomoeda.

Esse abuso destaca uma mudança em que a IA não apenas automatiza a criação do site, mas também incorpora elementos enganosos, como captchas e lógica de back-end para a exfiltração de dados, geralmente roteando credenciais roubadas para canais de telegrama ou permitindo ataques adversários no meio (AITM).

O modelo de Loveable, que oferece até cinco prompts gratuitos diariamente e sem restrições de projetos públicos, inadvertidamente facilitou a rápida escala de campanhas.

Por exemplo, em fevereiro de 2025, um magnata em larga escala Phishing-como um serviço (PHAAS) A operação distribuiu centenas de milhares de e-mails com temas de compartilhamento de arquivos, liderando os destinatários através dos desafios do Captcha para falsificar páginas de autenticação do Microsoft que colheram credenciais, tokens e cookies de sessão de MFA.

As campanhas subsequentes em junho se disfarçaram de departamentos de RH, explorando as narrativas dos benefícios dos funcionários para implantar técnicas semelhantes do AITM.

Além de Phishing, os atores criaram sites para cartão de pagamento e roubo de dados pessoais, como páginas de travessuras de UPS que coletam detalhes por meio da colheita de código SMS e publicam-os no telegrama.

As ameaças focadas em criptomoedas incluem drenadores de carteira disfarçados de plataformas defi como AAVE, onde os URLs redirecionados do sendGrid levam a interfaces que conectam e sifão os ativos do usuário.

A entrega de malware também aumentou, com campanhas de julho usando iscas de língua alemã representando empresas de software, redirecionando por meio de serviços como cookies recarregados para arquivos raros hospedados em Dropbox, contendo executáveis ??trojanizados que descendam os doiloader e implantam o ZGRAT Remote Access Trojans.

Esforços de mitigação

Em resposta a essas descobertas, a Lovable implementou proteções orientadas pela IA, incluindo detecção em tempo real durante o processamento imediato e a varredura automatizada de projetos publicados, resultando na queda de centenas de domínios maliciosos.

A empresa planeja aprimoramentos adicionais, como monitoramento proativo de conta de usuário, para conter o abuso.

No entanto, os experimentos de Proofpoint revelado Os corrimãos iniciais mínimos, permitindo a criação fácil de sites de phishing com linguagem manipulativa contrastando com políticas mais rigorosas em ferramentas como o ChatGPT.

Isso ressalta a necessidade de salvaguardas robustas nas plataformas de IA para evitar a exploração, à medida que os adversários mudam o foco do desenvolvimento manual para a otimização de cadeias de ataque.

As organizações são aconselhadas a adotar a lista de permissão para ferramentas comumente abusadas e monitorar ameaças emergentes geradas pela IA em e-mail e vetores de SMS.

Indicadores de compromisso (IOCs)

Indicador	Descrição	Primeiro visto
hxxps: // ups-flow-harvester[.]adorável[.]app/	Página de destino de representação da UPS	15 de junho de 2025
hxxps: // app-54124296d32502[.]adorável[.]app/	Rediretor de representação da UPS	15 de junho de 2025
hxxps: // captcha-office-redirect[.]adorável[.]app/	URL de phishing de representação da Microsoft	17 de junho de 2025
hxxps: // 33eq8[.]Oquvzop[.]es/cftvqhhpugs@x/	Redirecionamento de magnatas	17 de junho de 2025
hxxps: // aave-reward-notification[.]adorável[.]app/	AAVE PERSONAÇÃO SENVIDGRID Redirect	17 de junho de 2025
hxxps: // recompensa-aave[.]nós/web3/	Página de destino de representação de AAVE	17 de junho de 2025
hxxp: // lexware-invoice-deutsch-popup[.]adorável[.]app/	Alvo de redirecionamento recarregado de biscoitos	22 de julho de 2025
hxxp: // www[.]Dropbox[.]com/scl/fi/i6n7wcxpfi366wn46qngu/de0019902001000re.rar? rlkey =	Baixe URL de adorável	22 de julho de 2025

Indicador	Descrição	Primeiro visto
ec07od5O0p41q02cq7e3kp5iq & st = 7k1wp1oo & dl = 1		
84[.]32[.]41[.]163: 7705	ZGRAT C2	22 de julho de 2025

Encontre esta notícia interessante! Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas!**