



heimdall
security research

A DIVISION OF ISH



FraudGPT, outra ferramenta de IA para ataques cibernéticos



Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

[Heimdall Security Research](#)



Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall](#)



ISH —
CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH —
ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH —
GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

Sumário

1	Sobre o FraudGPT	6
2	Referências.....	8

Lista de Figuras

Figura 1 – Anúncio da ferramenta FraudGPT.....	6
Figura 2 – Venda realizada por meio de canal no Telegram pelo ator de ameaça.....	7

1 SOBRE O FRAUDGPT

Atores de ameaças estão anunciando mais uma ferramenta de inteligência artificial (IA) que pode ser utilizada para fins de crimes cibernéticos, conhecida como FraudGPT.

Essa ferramenta anda em conjunto com a outra ferramenta para ataques cibernéticos denominada WormGPT, sendo que neste caso, a FraudGPT está sendo anunciada em vários mercados da Dark Web e em canais do Telegram.

O pesquisador de ameaças Rakesh da Netenrich, afirmou que seria um Bot de IA direcionado exclusivamente para fins ofensivos, como a criação de e-mails de spear phishing, ferramentas de cracking, cargind e outros tipos de ameaças.

A venda da plataforma estaria circulando desde pelo menos 22 de julho de 2023, com um custo de assinatura de US\$200 mensais (ou US\$1.000 por seis meses e US\$1.700 por um ano).

De acordo com o anúncio do ator de ameaça, este afirmou que a ferramenta pode ser usada para escrever códigos maliciosos, criar malwares indetectáveis, encontrar vazamentos e vulnerabilidades e que havia mais de 3.000 vendas e análises confirmadas. Não foi divulgado o modelo de linguagem (LLM) utilizado para desenvolver o sistema.

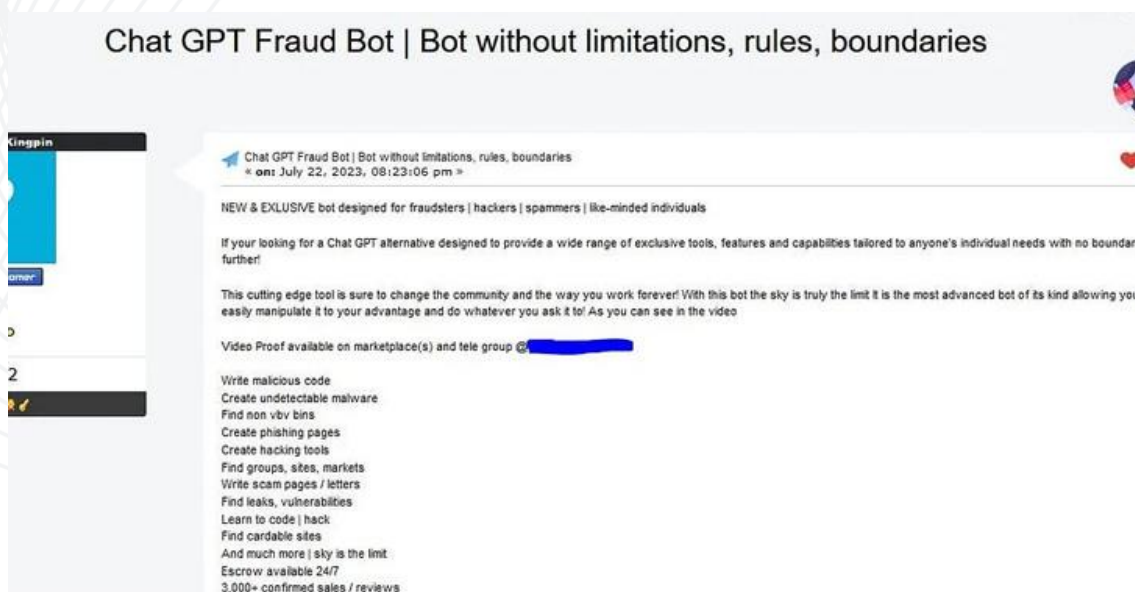


Figura 1 – Anúncio da ferramenta FraudGPT.

Welcome All To,
CanadianKingpin12 Proofs / Voucher Group.

As many of you may already know i have proudly served as a verified vendor for 4+ years on some of the most well known marketplaces across the globe.

Through out that time i have maintained an impressive 90% positive sales rating, With over 3,000 confirmed sales and hundreds of verified reviews from satisfied customers.

However a few months ago i took a much needed break only to return and find my telegram account has been auto deleted 🤖 This unfortionate incident allowed imposters to claim my old username @CanadianSmoker12 as well as take over old group names, bot names, etc. To make an unfortionate situation worse my pgp key expired thus locking me out of my vendor pages that were on vacation mode.

But not to worry because i am already re established on 3 well known marketplaces and starting fresh with a new alias. I'm excited to be back and pick up where i left off providing you with the freshest and highest quality services on the market!

Figura 2 – Venda realizada por meio de canal no Telegram pelo ator de ameaça.

Salientamos que o desenvolvimento destas ferramentas por atores de ameaças estão cada vez maior, aproveitando das ferramentas de IA do tipo OpenAI (ChatGPT) para criar variantes adversárias que são explicitamente projetadas para promover todos os tipos de atividades cibercriminosas sem qualquer tipo de restrição.

2 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- [Relatório](#) da Neterich - FraudGPT



heimdall
security research

A DIVISION OF ISH