heimdall

security research

A DIVISION OF ISH

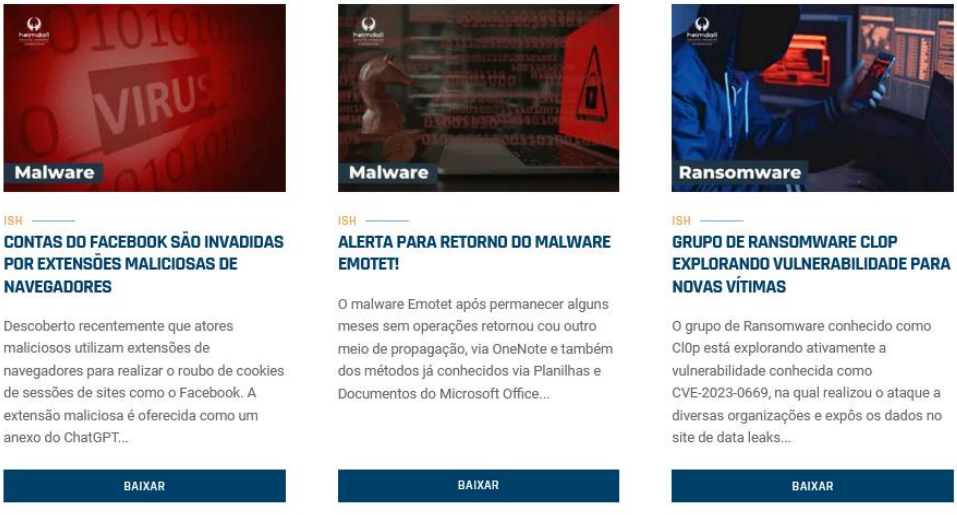
FraudGPT, outra ferramenta de IA para ataques cibernétidos

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



Sumário

Lista de Figuras

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.

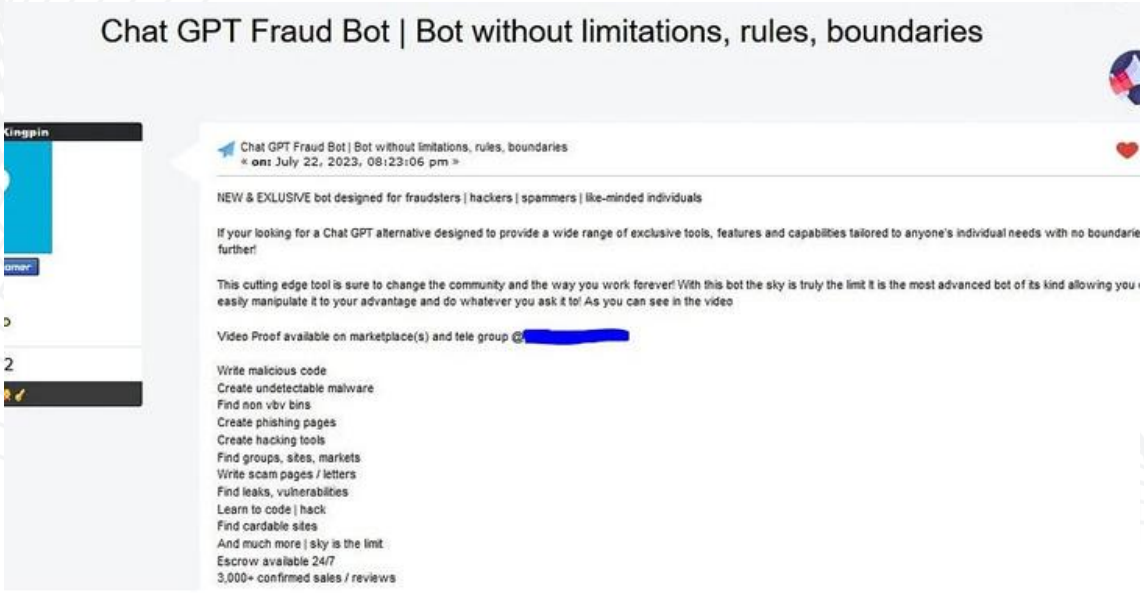


Figura 1 – Anúncio da ferramenta FraudGPT.

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