Well That Didn't Take Long - FraudGPT: The New ChatGPT Alternative for Cybercrime

August 4, 2023 - Just last week we published an article on artificial intelligence and how it would become a factor in identity theft. At the time, we were unaware of the fact that just a week earlier a service known as FraudGPT had become available on the dark web. But we're aware of it now and unfortunately it has lowered the barriers for entry into cybercrime to a cost that most high school students can afford.

Artificial Intelligence (AI) has revolutionized various aspects of our lives, but it has also opened up new avenues for cybercrime. FraudGPT is an alternative to ChatGPT that is exclusively targeted for offensive criminal purposes. It's been making waves in dark web marketplaces and Telegram channels, posing significant threats to individuals and businesses alike. And because it is now out there in the open, consumers need to know about practical defense measures to safeguard against AI-generated criminal activity.

FraudGPT is an AI bot catering to cybercriminals looking to exploit unsuspecting users. Based on the ChatGPT-3 technology, this sophisticated tool enables its users to engage in a wide range of malicious actions, including:

- Â· Crafting Spear Phishing Emails: FraudGPT can generate highly deceptive and convincing phishing emails, making it challenging for recipients to discern the authenticity of the messages.

- Â· Creating Cracking Tools: The AI-powered bot can develop tools that aid in breaking encryption and accessing protected systems or data.

- Â· Carding: FraudGPT facilitates the generation of stolen credit card information for fraudulent financial transactions.

- Â· Writing Malicious Code: It can produce harmful code and malware to infect systems, compromising data security and integrity.

- Â· Finding Leaks and Vulnerabilities: FraudGPT can detect weaknesses in software and systems, enabling cybercriminals to exploit them for illicit gains.

Sold as a service, it has been available on the dark web and Telegram channels since at least July 22, 2023. The pricing

model offers different subscription options:

- Â· $200 per month

- Â· $1,000 for a six-month subscription

- Â· $1,700 for a one-year subscription

The price range suggests that this AI tool is accessible to both experienced cybercriminals and potentially novice actors seeking to enter the world of cybercrime.

It is already being advertised and sold on various dark web marketplaces and Telegram channels. And reports suggest that over 3,000 confirmed sales and reviews have been made already, indicating a significant demand and adoption within the cybercriminal community.

FraudGPT and ChatGPT share the same underlying AI technology, but they differ significantly in their intended purposes and applications. While ChatGPT, developed by OpenAI, aims to provide helpful and informative responses to users' queries, FraudGPT operates with malicious intent and lacks ethical boundaries. The key differences are:

- Â· Purpose: ChatGPT is designed for general conversation and information sharing, while FraudGPT is exclusively focused on offensive cyber activities.

- Â· Safeguards: ChatGPT is developed with ethical safeguards to ensure responsible AI usage, whereas FraudGPT operates without any restrictions or ethical considerations.

With this in mind, protecting against the threats posed by FraudGPT requires a multi-faceted approach:

- Â· Cybersecurity Awareness: Individuals and organizations must stay informed about emerging cyber threats, including AI-powered tools like FraudGPT.

- Â· Updated Security Measures: Keep software, operating systems, and applications up-to-date with the latest security patches to mitigate vulnerabilities.

- Â· Anti-Phishing Training: Educate users about identifying phishing attempts and encourage them to report suspicious messages.

- Â· AI Detection Tools: Invest in AI-based security solutions that can detect and respond to AI-generated criminal activities.

- Â· Incident Response Planning: Develop a comprehensive incident response plan to handle potential cyberattacks promptly and effectively.

Recognizing potential targets of AI-generated criminal activity involves being vigilant about certain red flags:

- Â· Highly Personalized Phishing: Be cautious of phishing emails that appear exceptionally personalized or contextually relevant.

- Â· Unusual Requests: Be wary of unexpected requests for sensitive information or financial transactions.

- Â· Impersonal Communication: AI-generated messages may lack emotional context and human touch, sounding mechanical or generic.

In consclusion FraudGPT represents a concerning development in the world of cybercrime, leveraging the power of AI to carry out malicious activities. While FraudGPT may be one of the first AI driven tools to be used by cybercriminals, it certainly won't be the last. And it probably won't be the least expensive either. Because of this it becomes imperative for individuals and organizations to be proactive in their cybersecurity measures. By staying informed, implementing robust defenses, and exercising caution, we can better protect ourselves against the threats posed by this new breed of AI-powered cybercrime tools.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS