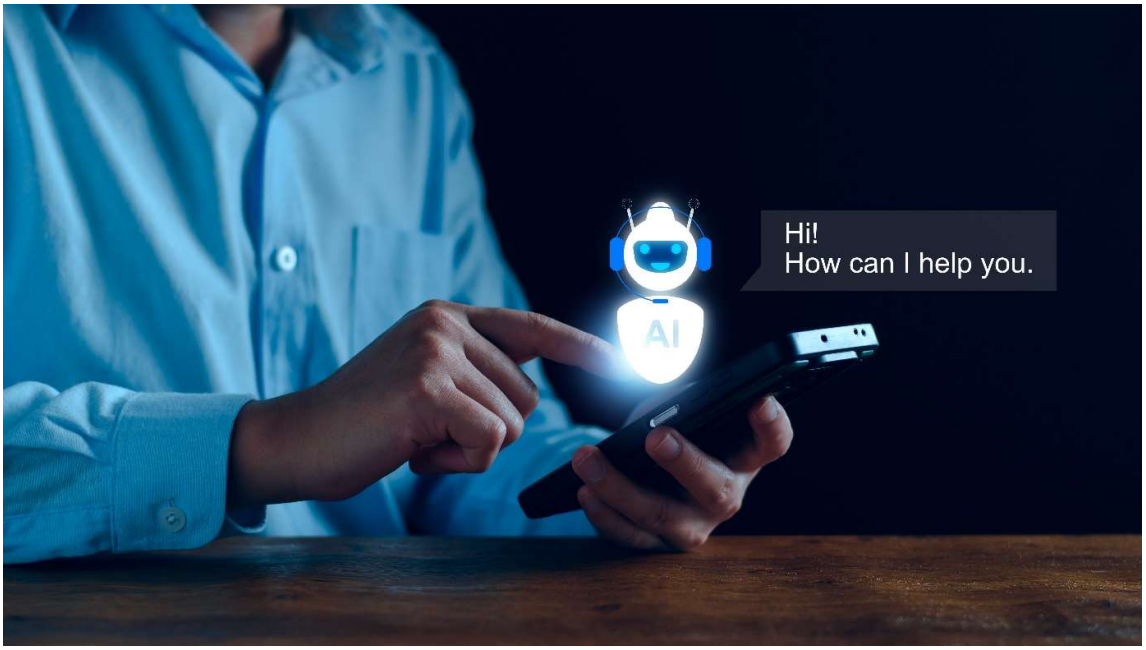
Chat GPT come potenziale aiuto per i criminali informatici

I progressi nel campo dell'intelligenza artificiale, e in particolare nell'area degli LLM (Large Language Models), sono stati all'origine di una serie di sviluppi interessanti, tra cui i chatbot come Chat GPT. Tali strumenti sono in grado di condurre conversazioni simili a quelle umane e di aiutare a svolgere una serie di compiti. Ad esempio, il chatbot è in grado di scrivere un saggio, comporre canzoni oppure scrivere e-mail in pochissimo tempo. In questo modo, i malintenzionati ne approfittano sempre di più.



Phishing e Social Engineering

La capacità di Chat GPT di generare testi simili a quelli umani apre nuove opportunità per i criminali informatici di ingannare. Impersonando persone o istituzioni reali, possono effettuare **attacchi** di **phishing**. Un esempio di ciò è la creazione di **siti Web falsi** o **e-mail autentiche,** in cui le vittime sono indotte con l'inganno a **rivelare le loro credenziali o** informazioni. A tal fine, **viene utilizzato un approccio di Social Engineering**, che risveglia la loro fiducia sfruttando le caratteristiche umane e quindi li invoglia ad agire. Sebbene siano state prese precauzioni di sicurezza con Chat GPT per rilevare intenzioni potenzialmente minacciose, queste possono essere aggirate ponendo una domanda corretta (Prompt-Engineering).

Automazione degli attacchi

Chat GPT può anche essere utilizzato per **automatizzare gli attacchi ai sistemi informatici**. Utilizzando l'intelligenza artificiale, i criminali informatici possono **creare malware personalizzato, identificare vulnerabilità o eseguire attacchi alle reti**.

Creazione di malware, exploit e ransomware

I criminali informatici potrebbero utilizzare Chat GPT per **sviluppare malware** (software dannoso) ed exploit (sequenza di programmi/comandi dannosi per sfruttare vulnerabilità e malfunzionamenti) personalizzati. Grazie alla programmazione del modello linguistico con la conoscenza delle vulnerabilità e dei metodi di attacco, i criminali possono generare automaticamente codice maligno su misura per obiettivi specifici. Questo potrebbe aumentare l'efficacia e la diffusione del malware e renderne più difficile il rilevamento da parte delle soluzioni di sicurezza.

In un **attacco ransomware**, i dati della vittima vengono prima crittografati e poi viene richiesto un riscatto per il loro rilascio. Per pagare il riscatto, gli hacker utilizzano anche l'intelligenza artificiale per creare sistemi di pagamento in criptovaluta. Tuttavia, l'intelligenza artificiale non viene utilizzata solo per questi movimenti finanziari, ma anche per il riciclaggio di denaro. Mediante

conversazioni autentiche sulle attività commerciali, le transazioni vengono ignorate o classificate come poco appariscenti dai sistemi di sorveglianza.

Conclusione

L'uso potenziale della chat GPT come strumento per i cyber-criminali comporta seri rischi. È fondamentale che gli sviluppatori, i produttori e gli utenti di questa tecnologia **riconoscano le proprie responsabilità e adottino misure per prevenire gli abusi**. Gli esperti di sicurezza di **KONVERTO** sottolineano che questi **rischi** possono essere **ridotti al minimo** implementando una **soluzione di sicurezza esaustiva** oltre a modelli di monitoraggio continuo. Allo stesso tempo, dovremmo sfruttare le caratteristiche positive della chat GPT e promuovere un **uso etico e responsabile.**

Cos'è Chat GPT?

Chat GPT (Generative Pre-trained Transformer) è un potente modello di intelligenza artificiale rilasciato da Open AI nel novembre 2022. È stato istruito per rispondere ad un'ampia gamma di domande e quesiti in linguaggio del tutto naturale. Ciò consente all'IA di generare testi, scrivere canzoni, fornire informazioni (talvolta obsolete o travisate) ed aiutare a risolvere i vari problemi. Dall'inizio di maggio lo strumento è nuovamente disponibile in Italia in seguito ad una breve interruzione