

La cybersecurity nell'era dell'AI generativa: una 'chiacchierata' tra LLAMA2 e ChatGPT per la creazione automatizzata di exploit – Simon Pietro Romano



Alla Cyber Crime Conference 2024, il professor Simon Pietro Romano, esperto di network security presso l'Università Federico II, ha offerto una prospettiva unica sull'intersezione tra intelligenza artificiale generativa e cyber security.

Guarda il video completo dell'intervento:

[embedded content]

Introduzione alla Cybersecurity nell'Era dell'AI Generativa

La sua presentazione, intitolata "LA CYBERSECURITY NELL'ERA DELL'AI GENERATIVA: UNA 'CHIACCHIERATA' TRA LLAMA2 E CHATGPT PER LA CREAZIONE AUTOMATIZZATA DI EXPLOIT", ha esplorato il potenziale uso dell'AI per automatizzare la creazione di codice d'attacco, riguardando specificamente gli exploit.

LLaMA-2 e ChatGPT per l'Automazione della Creazione di Exploit

Il cuore della presentazione del prof. Romano ha riguardato l'utilizzo di due specifici Large Language Models: LLaMA-2,

sviluppato da Meta (Facebook Research) e ChatGPT di OpenAI. Durante l'intervento ha dimostrato come questi modelli possano interagire per generare automaticamente codice di attacco, ovvero exploit, senza che un umano debba formulare direttamente le richieste a ChatGPT. Questo scenario rappresenta un salto qualitativo nel modo in cui l'intelligenza artificiale può essere applicata nel campo della sicurezza informatica, proponendo un modello in cui un'Intelligenza Artificiale può commissionare a un'altra Intelligenza Artificiale la creazione di codice malevolo.

Processo Tradizionale vs Utilizzo dell'AI nella Generazione di Exploit

Il professore ha illustrato come l'attività di generazione di exploit richieda solitamente competenze avanzate in programmazione, conoscenza dei sistemi operativi e delle reti, oltre a un'approfondita comprensione dei linguaggi di programmazione di basso livello come il C. Tradizionalmente, queste attività sono state prerogative degli esseri umani, in particolare degli ingegneri informatici con un'ampia gamma di conoscenze tecniche. Tuttavia, il progetto di Romano cerca di dimostrare che queste competenze possono essere in parte replicate e gestite attraverso l'utilizzo di AI, riducendo così la necessità di intervento umano diretto.

Durante la conferenza, Romano ha discusso il processo di exploit software, che comprende l'identificazione di vulnerabilità nel software e la creazione di codice che può essere utilizzato per attaccare un sistema. La vulnerabilità rappresenta un punto debole che, una volta individuato, può essere sfruttato per scrivere codice aggiuntivo che consegna il payload dell'attacco al nodo target. Questo processo è stato tipicamente eseguito manualmente da esperti del settore, ma con l'introduzione dell'AI nel workflow si possono automatizzare significativamente questi passaggi.

Questioni Etiche nell'Uso dell'AI: Una Riflessione Necessaria

La presentazione ha anche evidenziato come l'uso di AI per generare exploit sollevi questioni etiche significative, dato che semplifica la creazione di attacchi informatici abbassando notevolmente le capacità di barriera utili a contrastare l'accesso degli attaccanti. Romano ha chiarito che il suo obiettivo non è promuovere attività malevole, ma piuttosto aumentare la consapevolezza e preparare meglio i difensori nel campo della cyber security.

Dialogo Innovativo tra LLaMA-2 e ChatGPT, la "Question Generation" per la Produzione di Codice

Uno degli aspetti più interessanti della presentazione è stato il dialogo tra LLaMA-2 e ChatGPT, dove LLaMA-2 funge da iniziatore della conversazione, chiedendo a ChatGPT di generare codice di exploit. Questo approccio utilizza la "Question Generation" come metodo per stimolare la produzione di codice, riflettendo le potenzialità dei moderni AI Models nel comprendere e manipolare contesti tecnici complessi.

Impatto dell'AI Generativa sulla Cybersecurity

In conclusione, Simon Pietro Romano alla Cyber Crime Conference 2024 ha gettato luce su come l'intelligenza artificiale generativa stia iniziando a giocare un ruolo cruciale nella cyber security, non solo nel rafforzare le difese, ma anche nella potenziale creazione di nuove sfide e minacce. L'approccio innovativo del professor Romano ha offerto una nuova prospettiva su come gli AI Models possono essere utilizzati in scenari di sicurezza e pone questioni fondamentali riguardo l'etica e la responsabilità nell'uso

dell'intelligenza artificiale.

Il programma completo della Cyber Crime Conference 2024 è disponibile al seguente link:
<https://www.ictsecuritymagazine.com/eventi/cybercrimeconference2024#programma>

Iscriviti alla nostra newsletter per rimanere aggiornate sulle nostre iniziative:
<https://www.ictsecuritymagazine.com/newsletter/>

Condividi sui Social Network:
<https://www.ictsecuritymagazine.com/cybersecurity-video/la-cybersecurity-nellera-dellai-generativa-una-chiacchierata-tra-llama2-e-chatgpt-per-la-creazione-automatizzata-di-exploit-simon-pietro-romano/>