

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **36** ze dne **12.5.2023**

Hrozí, že hackeři budou zneužívat AI chatboty k vytváření phishingových e-mailů a malwaru

Společnost Check Point zveřejnila varování, že kyberzločinci již začali používat populární nástroj ChatGPT k vývoji škodlivých kódů a útočných nástrojů. Na hackerských fórech se objevily návody a příklady, jak technologie umělé inteligence od OpenAI využít pro různé podvodné aktivity a vytvoření malwaru. Velmi reálná je také hrozba zneužití ChatGPT k vytváření phishingových e-mailů.

"Umělá inteligence bude zcela jistě jedním z hlavních témat roku 2023. AI technologie pomáhají při ochraně před kybernetickými hrozbami, ale zároveň vidíme velký zájem kyberzločinců například o ChatGPT. Hackeři zkouší tuto dostupnou technologii používat k psaní škodlivého kódu, a i když jsou současné pokusy poměrně jednoduché, je jen otázkou času, než začnou AI nástroje využívat mnohem sofistikovanějším způsobem i profesionální hackerské skupiny," říká Petr Kadrmas ze společnosti Check Point Software Technologies.

Tvorba malwaru pomocí ChatGPT

29. prosince 2022 se na populárním hackerském fóru objevilo vlákno s názvem *"ChatGPT – výhody malwaru"*. Autor vlákna prozradil, že experimentuje s ChatGPT, aby vytvořil malwarové kmeny podle popisu ve výzkumných publikacích. Podařilo se mu například vygenerovat základní nástroj pro krádeže, který v systému vyhledává 12 běžných typů souborů (například dokumenty MS Office, PDF a obrázky). Pokud jsou nalezeny zajímavé soubory, malware je zkopíruje do dočasného adresáře, zazipuje a odešle přes web. Soubory jsou ovšem odesílané v nezašifrované podobě, takže se mohou dostat do rukou i třetím stranám. Další skript by bylo možné snadno upravit tak, aby stáhl a spustil jakýkoli program, včetně běžného malwaru.

Mohlo se sice jednat o technicky orientovaného hackera, který chce jen vyzkoušet možnosti nové technologie, ale ve skutečnosti se zdálo, že příspěvky spíše ukazují technicky méně zdatným kyberzločincům, jak ChatGPT využít k tvorbě malwaru a k útokům.

Tvorba vícevrstvých šifrovacích nástrojů

21. prosince 2022 zveřejnil hacker s přezdívkou USDoD skript v jazyce Python, o kterém zdůraznil, že je to *"první skript, který kdy vytvořil"*. USDoD zároveň potvrdil, že script byl vytvořen s pomocí OpenAI. Je to ukázka, že kyberzločinci, kteří nemají téměř žádné vývojářské zkušenosti, by mohli umělou inteligenci využít k vývoji škodlivých nástrojů a útoky na úrovni profesionálních kyberzločinců jsou zase o krok blíž i amatérům.

Zmíněné kódy lze samozřejmě použít i neškodným způsobem. Zároveň je však možné skript jednoduše upravit, aby zcela bez interakce uživatele zašifroval něčí počítač. Kód lze dokonce změnit i na ransomware, což by mohlo vyvolat paniku, protože ransomwarové útoky už tak patří mezi nejnebezpečnější hrozby současnosti.

Zneužití k cíleným kybernetickým útokům s využitím phishingu

Hackeři by také mohli zneužít chatbota OpenAI ChatGPT a také OpenAI Codex k cíleným kybernetickým útokům. Pomocí chatbota ChatGPT lze totiž relativně snadno vytvořit phishingový e-mail s přiloženým excelovým dokumentem obsahujícím škodlivý kód. A pokud bychom vše propojili s kódem vytvořeným pomocí OpenAI Codexu, bylo by možné vše použít k jednoduchému a přitom efektivnímu útoku.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **36** ze dne **12.5.2023**

Využití ChatGPT pro podvody a obchodování s nelegálním zbožím

Kyberzločinci také ukazují, jak pomocí ChatGPT vytvořit skripty pro darkwebové tržiště a nabídnout platformu pro automatizovaný obchod s nelegálním nebo kradeným zbožím, jako jsou kradené účty nebo platební karty, malware nebo dokonce drogy a munice, přičemž veškeré platby mohou probíhat v kryptoměnách.

Na hackerských fórech také probíhají diskuze, jak využít ChatGPT k vytváření podvodných schémat. Většinou se jedná o generování uměleckých děl pomocí jiné OpenAI technologie (DALLE2) a online prodej pomocí legitimních platforem, jako je Etsy. Jiný hacker zase vysvětluje, jak vygenerovat e-knihu nebo krátkou povídku pomocí ChatGPT a prodat obsah online.

Zatím je příliš brzy, abychom mohli jasně říci, jestli se ChatGPT stane novým oblíbeným nástrojem hackerů. Nicméně kyberzločinci možnosti zneužití aktivně zkoumají, měli bychom proto zpozornět a připravit se na nové nebezpečné výzvy.

Zdroj: SystemOnLine.