Kyberbezpečnost a umělá inteligence: Vývoj hrozeb v roce 2023

15.12.2023 - | PROTEXT

V souvislosti s rychlým technologickým pokrokem a společenskými změnami zaujalo téma „umělé inteligence“ pevné místo v popředí globálních diskusí.

Rozšíření velkých jazykových modelů (LLM) vyvolává větší obavy o narušení bezpečnosti a soukromí. Výzkumníci společnosti Kaspersky ukazují, jak nástroje umělé inteligence pomohly kyberzločincům v jejich škodlivé činnosti v roce 2023, a zároveň představují potenciální obranné aplikace této technologie. Odborníci společnosti také předpovídají budoucí vývoj hrozeb souvisejících s umělou inteligencí, které mohou zahrnovat:

Komplexnější zranitelnosti

Se začleňováním instrukcemi řízených systémů LLM do stále většího počtu produktů určených běžným uživatelům se budou na rozhraní pravděpodobnostní generativní AI a tradičních deterministických technologií objevovat nové komplexní zranitelnosti, čímž se rozšíří pole působnosti útoků, které musí odborníci na kybernetickou bezpečnost zabezpečit. To bude vyžadovat, aby vývojáři prozkoumali nová bezpečnostní opatření, jako je uživatelské povolování akcí iniciovaných agenty LLM.

Všestranný AI asistent pro specialisty na kybernetickou bezpečnost

Pracovníci zabývající se simulací kybernetických útoků a výzkumní pracovníci zapojují generativní AI do inovativních nástrojů kybernetické bezpečnosti, což může vést k vytvoření asistenta využívajícího LLM nebo strojové učení (ML). Takový nástroj by mohl automatizovat úlohy simulovaných útoků a nabízet rady na základě provedených příkazů při penetračních testech.

Neuronové sítě se budou stále častěji využívat k vytváření vizualizací pro podvody

V nadcházejícím roce mohou podvodníci posílit své taktiky pomocí neuronových sítí a využívat nástroje umělé inteligence k vytváření přesvědčivějšího podvodného obsahu. Díky schopnosti snadno vytvářet realistické obrázky a videa představují škodliví aktéři zvýšené riziko eskalace kybernetických hrozeb spojených s podvody a zpronevěrami.

Umělá inteligence se v roce 2024 nestane hnací silou převratných změn v oblasti hrozeb

Navzdory výše uvedeným trendům zůstávají odborníci společnosti Kaspersky skeptičtí ohledně toho, že by umělá inteligence v dohledné době výrazně změnila prostředí hrozeb. Kyberzločinci sice do svých aktivit zapojují generativní umělou inteligenci, totéž však platí o kyberobráncích, kteří budou používat stejné nebo ještě pokročilejší nástroje k testování pro zvýšení bezpečnosti softwaru a sítí, takže je nepravděpodobné, že by AI zásadně změnila podmínky provádění útoků.

Vodoznak pro obsah generovaný umělou inteligencí

K označení nebo identifikaci uměle vytvářeného obsahu budou zapotřebí větší regulace a pravidla pro poskytovatele služeb AI, a rovněž další investice do detekčních technologií. Vývojáři a výzkumní pracovníci se budou podílet na vývoji metod označování syntetických médií vodoznakem pro snadnější identifikaci a určení původu.

„Umělá inteligence je v oblasti kybernetické bezpečnosti dvousečná zbraň. Její adaptivní schopnosti posilují naši obranu a poskytují proaktivní štít proti vyvíjejícím se hrozbám. Stejná dynamika však představuje riziko, protože útočníci využívají umělou inteligenci k vytváření sofistikovanějších útoků. Pro zabezpečení našich digitálních hranic je nejdůležitější najít správnou rovnováhu a zajistit zodpovědné používání AI bez nadměrného sdílení citlivých údajů,“ říká Vladislav Tushkanov, bezpečnostní expert společnosti Kaspersky.

https://www.ceskenoviny.cz/tiskove/zpravy/kyberbezpecnost-a-umela-inteligence-vyvoj-hrozeb-v-roce-2023/2454325