

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **78** ze dne **11.8.2024**

Kyberzločinci mají také oblíbené nástroje s umělou inteligencí

Umělá inteligence pomáhá v boji s kyberzločinem, ale současně nejrůznější AI služby využívají i útočníci. Jedná se o velmi nebezpečný trend, který mění digitální svět. Chcete vytvořit nějaký obrázek, zjistit více o zajímavém tématu, napsat článek nebo text na sociální síť? Se vším vám dnes pomohou AI nástroje, jako například ChatGPT. Ale podobné chytré nástroje mají k dispozici i kyberzločinci. Mohou tak vytvářet ještě efektivnější útoky a snadněji analyzovat ukradené informace nebo využít AI k vytvoření a vylepšení hrozeb a útočných taktik. Například FraudGPT, XXXGPT nebo WolfGPT jsou ukázkou, jak lze umělou inteligenci zneužít ke škodlivým účelům.

"Tyto nástroje ukazují, že kyberzločinci mohou umělou inteligenci přizpůsobit tak, aby výrazně zvýšili účinnost svých útoků a efektivitu krádeží dat. Je tedy nutné přehodnotit stávající kyberbezpečnostní strategie a zaměřit se na etický rámec, kterým se řídí vývoj a používání umělé inteligence," upozorňuje Pavel Krejčí, Security Engineer ze společnosti Check Point Software Technologies.

FraudGPT

FraudGPT představuje milník v oblasti škodlivého využívání AI technologií, protože se jedná o platformu, kterou si lze předplatit jako jakoukoli jinou službu a umožňuje vytvářet falešné identity, účinné phishingové e-maily, malware nebo využít sociální inženýrství k oklamání uživatelů. Vše navíc na velmi vysoké úrovni. I osoby s minimálními technickými dovednostmi tak mohou provádět komplexní útoky.

XXXGPT

Nástroj XXXGPT s oblibou využívají zločinci pro generování RAT kódů, které umožňují vzdáleně ovládnout zařízení oběti a nepozorovaně krást citlivá data nebo je v tichosti změnit či poškodit. Může také vytvářet spyware, ransomware, keyloggers a speciální kódy pro cílené útoky. Nebo vytvářet a šířit nejrůznější dezinformace či kompromitující materiál určený k vydírání a šikaně.

WolfGPT

WolfGPT je známý svou komplexností a architekturou postavenou na programovacím jazyce Python. Dokáže vytvářet šifrovaný malware a přesvědčivé phishingové kampaně. Navíc umožňuje vytvářet široký arzenál kybernetických zbraní, včetně botnetů, trojanů pro vzdálený přístup, keyloggerů nebo nástrojů pro krádeže dat a kryptoměn. Kyberzločinci jej využívají i pro přípravu škodlivých kódů, zaměřených na pokladny a pro cílené útoky na bankomaty, případně pro praní špinavých peněz a identifikaci slabých míst v podnikových sítích.

Důsledky pro kybernetickou bezpečnost a etický rozměr

Vzestup pokročilých AI modelů, jako jsou FraudGPT, XXXGPT a WolfGPT, vyžaduje nový přístup k bezpečnosti. Konvenční obrana je totiž proti komplexním, adaptivním hrozbám nedostačující. Současně je nutné řešit i etické otázky týkající se odpovědnosti tvůrců AI a jak celkově zabránit zneužití umělé inteligence. Noříme se totiž do éry AI, kdy je dvojí využití těchto technologií stále zřetelnější.

"Zneužívání AI služeb představuje vážnou hrozbu, kterou nelze ignorovat. Je nezbytné, aby vlády, regulační orgány a technologické společnosti spolupracovaly na vývoji a implementaci opatření, která by zneužívání AI technologií omezila," dodává Pavel Krejčí.

Zdroj: AVcentrum ČR