

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **80** ze dne **27.8.2024**

AI pomáhá hackerům. Počet ransomware útoků vzrostl o více než 20 %

Rozšíření generativní umělé inteligence umožňuje i méně zdatným skupinám provádět sofistikované útoky na soukromé i firemní cíle a vede také k nárůstu jejich počtu.

"Z veřejně dostupných údajů vyplývá, že počet útoků ransomwarem v prvním čtvrtletí roku 2024 vzrostl o více než 20 % ve srovnání s prvním čtvrtletím předešlého roku," řekl Ondřej Ševeček, odborník na bezpečnost a etický hacking z Počítačové školy GOPAS.

Podle dat zprávy ESET Threat Report H1 2024 bylo využití nástrojů umělé inteligence během prvního pololetí 2024 patrné u několika různých typů kybernetických hrozeb. Šlo například o hrozby zaměřené na mobilní bankovní služby platformy Android. Nový mobilní malware GoldPickaxe dokonce dokáže krást data pro rozpoznávání obličeje a vytvářet deepfake videa, která útočníci používají k ověření podvodných finančních transakcí.

"S rozvojem automatizace, strojového učení a umělé inteligence se vývoj těchto prostředků zjednodušuje. Útočníci navíc své zbraně mohou již kupovat jednoduše jako službu. Stále lepší automatické překlady také odbourávají jazykové bariéry. Složitost českého jazyka byla dlouho pro útočníky překážkou, ale s rozvojem velkých jazykových modelů i tato bariéra padá," poznamenal Michal Černý ze společnosti Audiopro.

Metoda Prompt Injection

Metoda Prompt Injection je sofistikovaný způsob kybernetického útoku, který využívá schopnosti velkých jazykových modelů AI ke generování obsahu. Tato technika spočívá v začlenění specifických instrukcí nebo kódů do promptů, které jsou zadávány do AI. Tyto prompty jsou formulovány tak, aby byly pro AI zdánlivě neškodné, ale ve skutečnosti obsahují skryté příkazy nebo kód, který může vést k neautorizovanému přístupu k datům nebo spuštění škodlivých operací.

Tato metoda představuje značné riziko, protože může být obtížné odhalit a zablokovat takové manipulativní prompty, zejména pokud jsou dobře maskované. To vyžaduje neustálé monitorování a aktualizaci bezpečnostních protokolů AI, aby bylo možné tyto hrozby identifikovat a neutralizovat.

Dobrá čeština dělá phishing nebezpečnější

Jedním z důsledků rozvoje nástrojů generativní umělé inteligence je také rychlý rozvoj phishingu a metod sociálního inženýrství i ve složitějších a menších jazycích, jako je čeština. Dříve byly phishingové e-maily buď v angličtině nebo v úsměvně nedokonalé češtině. To už dnes neplatí. Spolu se zdokonalením personalizace povede k růstu úspěšných útoků vedených tímto způsobem.

Útočníci využívají AI k vytváření pokročilých phishingových kampaní, které je stále těžší odhalit. AI také umožňuje automatizaci a škálování útoků. Nástroje generativní umělé inteligence umožňují útočníkům lépe a chytřejší zacílit na jednotlivé uživatele s cílem vylákat jejich přístupové údaje nebo je přimět k akci, která poškozuje je samotné nebo společnost, ve které pracují. Útočníci už teď mohou automatizovaně sesbírat informace o jednotlivých zaměstnancích v řádech několika minut, a za stejně dlouhou dobu připravit personalizovaný e-mail, na kterém na první pohled nebude nic podezřelého.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **80** ze dne **27.8.2024**

Rozvoj kybernetické kriminality jako služby

"Řada hackerů nyní přechází na model využívání hackerského nástroje jako služby. Kyberzločinci si tak mohou koupit celou infrastrukturu ransomwaru. Ransomwarové skupiny jsou nyní součástí širšího ekosystému kybernetické kriminality. K dispozici mají široké spektrum zdrojů, se specializací například na počáteční přístup do podnikových IT prostředí, pověření, útoky na soubory cookie pro aplikace SSO (Single Sign-On), a to včetně infrastruktury pro distribuci. Zároveň mají tyto skupiny odborníky zaměřené na rekrutování pomocníků z řad osob, které mají přístup do interního systému," řekl Ondřej Ševeček z Počítačové školy GOPAS.

Slabým článkem jsou tradičně lidé

Nejslabším článkem zabezpečení firem jsou, ať už úmyslně nebo neúmyslně, zaměstnanci. Mohou vědomě vynášet citlivé informace, ale i bez špatného úmyslu klikat na nebezpečné odkazy nebo otevírat zavirované přílohy. Či bez uvážení předávat firemní data nedůvěryhodným zdrojům, v krajním případě i hackerům či šmejdům posílat firemní finanční prostředky. A nejnověji na ně útočí i AI v podobě naprogramovaných chatbotů nebo zcela novým rizikům souvisejícím s ChatGPT.

Podle výsledků simulovaných útoků odolnosti firem pětina zaměstnanců klikne na odkaz ve zprávě, aniž by si prověřila, kam směřuje. Únik nebo poškození dat, falešné platební příkazy nebo phishingové léčky mohou způsobit firmám katastrofální škody. Zacílení na jednotlivce je velmi účinná technika, mnoho zaměstnanců stále kliká na phishingové e-mailové odkazy a stahuje přílohy se škodlivými soubory.

"Riziko pro firemní data a celkovou bezpečnost, které přichází od zaměstnanců, je stále velmi vysoké. A phishingové útoky, které hackeři vedou přes zaměstnance jsou velmi účinné. Firmy mají stále ve vzdělávání svých zaměstnanců zejména v bezpečném chování na internetu rezervy," uzavřel Ondřej Ševeček z Počítačové školy GOPAS.

Zdroj: AVcentrum ČR