E-Bezpečí 2024, 9(2): Page 4-5. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=4179

JAK PODVODNÍCI ZNEUŽÍVAJÍ POPULARITU UMĚLÉ INTELIGENCE K ŠÍŘENÍ MALWARU A PHISHINGU

Kamil KOPECKÝ

V poslední době se umělá inteligence, zejména nástroje jako ChatGPT, Gemini či Copilot staly nejen středem zájmu technologických nadšenců, ale také cílem podvodníků, kteří využívají její popularitu k šíření malwaru a phishingu. Tento trend je znepokojivý, protože s rostoucím zájmem o AI se zvyšuje i počet lidí, kteří se nechají nalákat na falešné sliby snadného zisku nebo řešení problémů pomocí těchto pokročilých technologií.

1. Šíření malware prostřednictvím falešných AI nástrojů

Podvodníci často vytvářejí falešné aplikace, které slibují přístup k pokročilým AI nástrojům, ale **ve skutečnosti obsahují malware**. Tyto falešné aplikace se šíří například prostřednictvím reklam na sociálních sítích nebo jako přílohy v e-mailech, které tvrdí, že nabízejí exkluzivní přístup k populárním AI nástrojům. Jakmile uživatel stáhne a spustí takovou aplikaci, jeho zařízení může být infikováno malwarem, který může krást citlivé informace, jako jsou hesla nebo finanční údaje (Dvojklik.cz, 2023; Trend Micro, 2023).

2. Phishingové kampaně a falešné sliby zázračného zbohatnutí

Dalším běžným způsobem, jak podvodníci zneužívají popularitu AI, je **vytváření phishingových kampaní, které lákají oběti na sliby rychlého zbohatnutí pomocí AI**. Phishingové e-maily nebo zprávy na sociálních sítích často obsahují odkazy, které vedou na

falešné stránky, kde uživatelé musí zadat své osobní údaje nebo platební informace. Tyto stránky mohou vypadat velmi přesvědčivě a být navrženy tak, aby kopírovaly důvěryhodné platformy (The Verge, 2023; WeLiveSecurity, 2023).

3. Zneužití sociálních sítí pro propagaci podvodů

Sociální sítě hrají klíčovou roli v šíření těchto podvodů. Podvodníci využívají reklamní systémy a prostřednictvím falešné reklamy často slibují, že **díky AI může každý vydělat miliony**, Ve skutečnosti reklamní bannery vedou na stránky, kde se uživatelé stávají obětí phishingu nebo jsou vybízeni ke stažení malwaru (WeLiveSecurity, 2023).

Jak se chránit před těmito podvody

Aby se lidé vyhnuli těmto nástrahám, je důležité dodržovat několik základních pravidel:

A. Nestahujte software z nedůvěryhodných zdrojů. Pokud vás nějaká aplikace slibující AI funkce zaujme, ověřte si, zda pochází z důvěryhodného zdroje.
B. Pozor na příliš lákavé nabídky. Pokud něco zní příliš dobře, aby to byla pravda, pravděpodobně jde o podvod.
C. Ověřte si, na jaké stránky klikáte. Pokud vám e-mail nebo zpráva na sociální síti nabídne odkaz na „exkluzivní“ obsah, ujistěte se, že odkaz vede na bezpečnou stránku.

Pro E-Bezpečí,
Kamil Kopecký

Použité zdroje:

Dvojklik.cz. ChatGPT jako vějička: Jak útočníci zneužívají známé AI nástroje.

Trend Micro. Beware of Fake AI Tools Masking Very Real Malware Threats.

The Verge. Meta's Warning: ChatGPT Malware is Targeting Business Accounts.

WeLiveSecurity. Beware Fake AI Tools Masking Very Real Malware Threat.