

Falešná aplikace ChatGPT pro komunikaci s UI s novým malwarem krade uživatelům hesla k sociálním sítím a údaje o kreditních kartách

tadesco.org/falesna-aplikace-chatgpt-pro-komunikaci-s-ui-s-novym-malwarem-krade-uzivatelum-hesla-k-socialnim-sitim-a-udaje-o-kreditnich-kartach

Podle nejnovější zprávy zveřejněné ve čtvrtek objevila skupina výzkumníků aktivní malware, který využívá rostoucí popularity ChatGPT s umělou inteligencí.

Bezpečnostní společnost Kaspersky tvrdí, že hackeři šíří malware prostřednictvím skupin na Facebooku tím, že propagují falešnou desktopovou verzi ChatuGPT.

„Tato kampaň zaměřená na ChatGPT je ukázkovým příkladem toho, jak útočníci využívají techniky sociálního inženýrství ke zneužití důvěry, kterou uživatelé vkládají do populárních značek a služeb. Je důležité, aby si uživatelé uvědomili že to, že se služba jeví jako legitimní ještě neznamená, že tomu tak je,“ řekla Darja Ivanová, bezpečnostní analytička společnosti Kaspersky.

Kromě „bota“ jsou uživatelé infikováni trojským koněm Fobo, který krade citlivé informace jakými jsou přihlašovací údaje k účtům na Facebooku, TikToku, Googlu a také firemní a soukromé finanční údaje.

Dle vyšetřování jsou lidé, kteří kliknou na odkaz v příspěvku přesměrováni na webovou stránku, která se téměř identicky podobá webu ChatGPT.

Webová stránka pak vyzývá diváky ke stažení něčeho, co vypadá jako verze ChatGPT pro Windows, ale ve skutečnosti se jedná o archiv se spustitelným souborem.

Když se program nepodařilo nainstalovat, zobrazí se chybové hlášení a instalační procedura se náhle ukončí.

Podle výzkumu se ve skutečnosti do počítače nainstaluje nový trojský kůň s názvem Trojan-PSW.Win64.Fobo. Program se nainstaluje bez vědomí uživatele.

Hlavním cílem tohoto trojského koně je krádež uložených informací o účtu z populárních prohlížečů, včetně prohlížečů Chrome, Edge, Firefox a Brave.

Trojský kůň se v rámci útoku kromě krádeže přihlašovacích údajů pokouší shromáždit i další informace: výši peněz za reklamu a aktuální zůstatek na firemních účtech.

Cílem útoků teroristů je světový trh. Jak uvádí výzkum, falešný „desktopový klient“ ChatGPT se zaměřuje na uživatele v Africe, Asii, Evropě a Americe.

Zdroj: Insider Paper