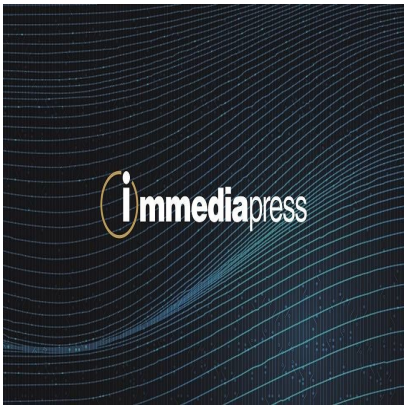

Kaspersky scopre infostealer che imitano Claude Code, OpenClaw e altri strumenti di sviluppo AI

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

A marzo 2026, Kaspersky Threat Research ha identificato una nuova campagna malevola rivolta agli sviluppatori alla ricerca delle istruzioni di installazione di Claude Code, un agente di sviluppo creato da Anthropic. Quando si cerca â??Claude Code downloadâ?•, nella parte superiore dei risultati di ricerca compaiono annunci pubblicitari sponsorizzati. Uno di questi annunci reindirizza gli utenti a una pagina web dannosa che imita fedelmente la documentazione ufficiale di installazione di Claude Code.

Di conseguenza, gli utenti vengono indotti con lâ??inganno a installare malware in grado di raccogliere informazioni sensibili, tra cui credenziali, dati di portafogli crittografici, sessioni del browser e altri file riservati. Campagne dannose simili imitano anche altri strumenti di IA popolari, tra cui OpenClaw.

Esempio di annuncio fraudolento

La pagina con la documentazione falsa Ã¨ visivamente identica a quella legittima ed Ã¨ ospitata sulla piattaforma di creazione e hosting di siti web Squarespace. PoichÃ© la pagina riproduce fedelmente le istruzioni originali, gli utenti potrebbero non notare la differenza durante la copia e lâ??esecuzione dei comandi di installazione.

Pagina fraudulenta di Claude

Tuttavia, invece di installare lo strumento di sviluppo, i comandi inviano malware al sistema della vittima. A seconda del sistema operativo, i comandi dannosi distribuiscono diversi infostealer:

I ricercatori di Kaspersky hanno inoltre identificato campagne dannose che prendono di mira altri popolari strumenti di intelligenza artificiale, tra cui OpenClaw e Doubao. Utilizzando lo stesso approccio, gli aggressori hanno registrato piÃ¹ domini e distribuito file contenenti il programma di furto di informazioni Amatera, mascherandoli come download legittimi per questi strumenti.

â??La campagna presenta rischi significativi perchÃ© strumenti di sviluppo dellâ??IA come Claude Code e OpenClaw sono ampiamente utilizzati non solo da hobbisti e appassionati di automazione, ma anche da sviluppatori professionisti che lavorano in grandi organizzazioni. Se infettate, le vittime potrebbero inconsapevolmente esporre il codice sorgente di progetti attivi, dati aziendali riservati, credenziali di autenticazione e account privati. Questo rende tali campagne particolarmente pericolose per le aziende i cui sviluppatori si affidano a strumenti di codifica assistiti dallâ??IAâ?•, ha commentato Vladimir Gursky, Cybersecurity Expert di Kaspersky.

A dicembre 2025 Kaspersky ha rilevato che alcuni hacker hanno diffuso un infostealer per macOS utilizzando Google Ads. Unâ??interfaccia di chat appositamente generata, progettata per assomigliare a un tutorial di ChatGPT, fingeva di guidare gli utenti nellâ??installazione del browser Atlas. Le istruzioni dannose sembravano essere ospitate su un sito legittimo associato a OpenAI, aiutando gli hacker a guadagnarsi la fiducia degli utenti.

Per proteggersi da queste minacce, Kaspersky consiglia di:

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione

Marzo 12, 2026
Autore
redazione