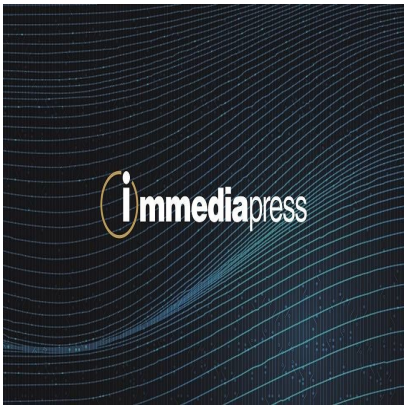

Kaspersky: truffa che sfrutta le funzionalitÃ di collaborazione di OpenAI

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Kaspersky ha individuato una nuova tattica fraudolenta che sfrutta la piattaforma OpenAI. Gli aggressori abusano delle funzionalitÃ di creazione delle organizzazioni e di invito dei team di OpenAI per inviare e-mail di spam da indirizzi OpenAI legittimi, inducendo potenzialmente gli utenti a cliccare su link fraudolenti o a chiamare numeri di telefono falsi.

La campagna di spam inizia con la registrazione di un account sulla piattaforma OpenAI da parte degli aggressori. Durante la procedura di registrazione, agli utenti viene richiesto di inserire il nome di unâ??organizzazione, che puÃ² essere composto da qualsiasi combinazione di simboli. I truffatori sfruttano questa caratteristica inserendo testi ingannevoli, link o numeri di telefono falsi direttamente nel campo riservato al nome dellâ??azienda.

Una volta creata lâ??â??aziendaâ?•, OpenAI offre la possibilitÃ di â??invitare il proprio teamâ?•, consentendo lâ??inserimento degli indirizzi e-mail delle vittime.

Quando gli inviti vengono inviati, questi provengono da un indirizzo OpenAI, risultando quindi apparentemente del tutto legittimi dal punto di vista tecnico. Kaspersky ha rilevato diversi tipi di messaggi contenenti minacce inviati con questa modalitÃ .

Si tratta, ad esempio, di e-mail false che promuovono offerte fraudolente, come servizi per adulti. Un altro tipo di attacco rilevato Ã¨ il vishing, ovvero false notifiche che affermano che un abbonamento Ã¨ stato rinnovato per una somma ingente: gli aggressori istruiscono i destinatari a chiamare un numero di

telefono fornito per â??annullareâ?• lâ??addebito o intraprendere altre azioni che portano a ulteriori compromissioni. Potrebbero inoltre esistere altre minacce via e-mail che si diffondono attraverso la piattaforma OpenAI.

Il testo che gli aggressori vogliono che le vittime leggano (evidenziato in grassetto nel modello di e-mail) risulta strutturalmente incoerente rispetto al resto del modello, originariamente progettato per invitare collaboratori a un progetto. Tuttavia, gli aggressori hanno scommesso sul fatto che le vittime non avrebbero prestato attenzione a questa discrepanza.

â??Questo caso evidenzia una vulnerabilitÃ nel modo in cui le funzionalitÃ della piattaforma possono essere utilizzate come arma per attacchi di social engineering tramite e-mail. Incorporando elementi ingannevoli in campi apparentemente innocui come i nomi delle aziende, i truffatori tentano di aggirare i tradizionali filtri e-mail e sfruttare la fiducia degli utenti nei servizi affidabili. Invitiamo tutti gli utenti a verificare attentamente gli inviti ed evitare di cliccare sui link incorporati senza prima averli esaminati con attenzione. Raccomandiamo inoltre ai brand di valutare se i loro servizi o piattaforme online possano essere oggetto di abuso da parte degli aggressoriâ?•, ha commentato Anna Lazaricheva, Senior Spam Analyst di Kaspersky.

Per proteggersi da queste truffe, 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
Gennaio 20, 2026
Autore
redazione