



Kaspersky: l'AI cancella le impronte digitali, rendendo più difficile attribuire la responsabilità degli attacchi informatici

Descrizione

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

Con la progressiva integrazione dell'AI generativa nel cybercrime, l'attribuzione degli attacchi informatici è destinata a diventare sempre più complessa. Il codice generato dall'intelligenza artificiale e i contenuti di phishing, infatti, eliminano quelle impronte digitali umane su cui gli analisti hanno tradizionalmente fatto affidamento.

Gli esperti del Global Research and Analysis Team (GReAT) di Kaspersky segnalano che gli aggressori ricorrono con crescente frequenza all'intelligenza artificiale per generare codice, e-mail di phishing e contenuti operativi. A differenza dei materiali scritti dall'uomo, i risultati prodotti dall'AI tendono a essere neutri e standardizzati, privi di errori linguistici distintivi o di specifici pattern di codifica che in passato supportavano le valutazioni di attribuzione. Di conseguenza, gli analisti della sicurezza dovranno fare maggiore affidamento sull'infrastruttura, sulle sovrapposizioni degli strumenti utilizzati e sugli indicatori comportamentali.

Kaspersky prevede inoltre che l'intelligenza artificiale assumerà un ruolo sempre più rilevante nello sviluppo completo di impianti dannosi. I modelli linguistici di grandi dimensioni sono in grado di generare parti sostanziali di malware, dalla struttura iniziale ai moduli funzionali. I ricercatori hanno già osservato forme di sviluppo assistito dall'AI in campagne legate al gruppo FunkSec, che ha distribuito malware basato su Rust capace di sottrarre dati, crittografare informazioni e manipolare processi. Nella campagna RevengeHotels del 2025, gli autori delle minacce hanno utilizzato modelli linguistici di grandi dimensioni per generare parti del codice di infezione e del downloader.

«Prevediamo che l'intelligenza artificiale rimarrà uno dei fattori chiave nel plasmare il panorama delle minacce nel 2026, poiché stiamo già osservando come stia ridefinendo i flussi di lavoro degli aggressori e accelerando le loro operazioni», ha commentato Georgy Kucherin, Senior Security Researcher del Kaspersky GReAT. «Riducendo tempi e costi necessari per sviluppare e adattare strumenti dannosi, l'AI consente agli autori delle minacce di iterare più rapidamente e ampliare i propri sforzi. I difensori devono quindi prepararsi a cambiamenti più rapidi nelle tattiche».

Kaspersky delinea ulteriori tendenze che caratterizzano il panorama delle minacce:

Contatti:

Kaspersky

kaspersky@noesis.net

COMUNICATO STAMPA «CONTENUTO PROMOZIONALE

Responsabilità editoriale di Kaspersky

»

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione

Marzo 5, 2026

Autore

redazione