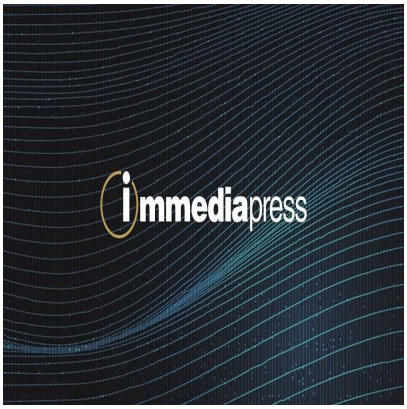

Kaspersky: lâ??AI cancella le impronte digitali, rendendo piÃ¹ difficile attribuire la responsabilitÃ degli attacchi informatici

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Con la progressiva integrazione dellâ??AI generativa nel cybercrime, lâ??attribuzione degli attacchi informatici Ã¨ destinata a diventare sempre piÃ¹ complessa. Il codice generato dallâ??intelligenza artificiale e i contenuti di phishing, infatti, eliminano quelle â??impronte digitaliâ?• 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 allâ??intelligenza artificiale per generare codice, e-mail di phishing e contenuti operativi. A differenza dei materiali scritti dallâ??uomo, i risultati prodotti dallâ??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 sullâ??infrastruttura, sulle sovrapposizioni degli strumenti utilizzati e sugli indicatori comportamentali.

Kaspersky prevede inoltre che lâ??intelligenza artificiale assumerÃ un ruolo sempre piÃ¹ 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 giÃ osservato forme di sviluppo assistito dallâ??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.

â??Prevediamo che lâ??intelligenza artificiale rimarrÃ uno dei fattori chiave nel plasmare il panorama delle minacce nel 2026, poichÃ© stiamo giÃ osservando come stia ridefinendo i flussi di lavoro degli aggressori e accelerando le loro operazioniâ?•,ha commentato Georgy Kucherin, Senior Security Researcher del Kaspersky GReAT. â??Riducendo tempi e costi necessari per sviluppare e adattare strumenti dannosi, lâ??AI consente agli autori delle minacce di iterare piÃ¹ rapidamente e ampliare i propri sforzi. I difensori devono quindi prepararsi a cambiamenti piÃ¹ rapidi nelle tatticheâ?•.

Kaspersky delinea ulteriori tendenze che caratterizzano il panorama delle minacce:

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 5, 2026
Autore
redazione