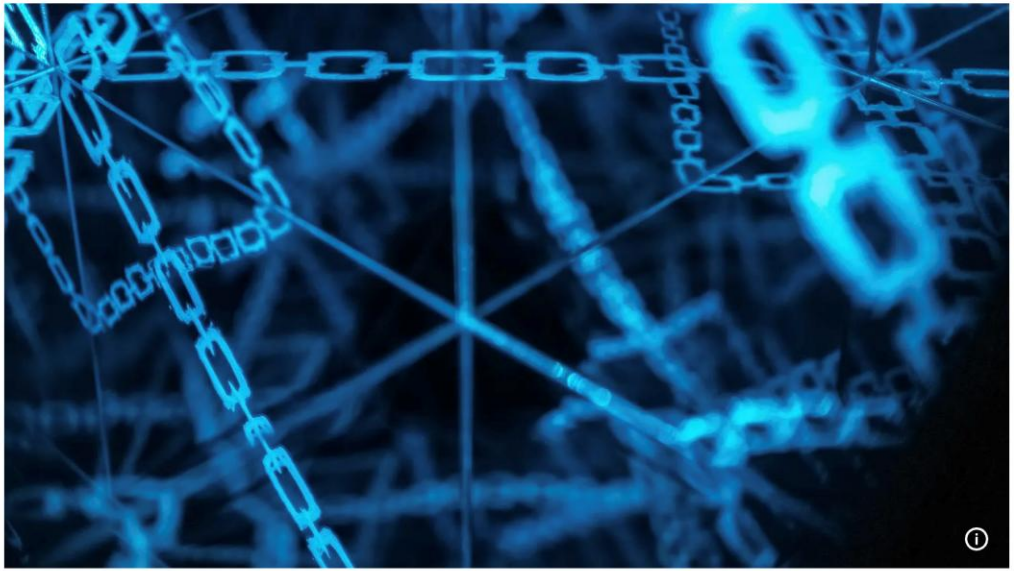
REGIONE PIEMONTE

CSI your digital partner

WEBINAR
SICURI di essere **SICURI?**

Intelligenza Artificiale e Cybersecurity: come difenderci dai nuovi attacchi informatici

Minaccia cyber dell'AI entro mesi, non anni, avvertono le agenzie d'intelligence occidentali



Diritti d'autore Canva

Di Pascale Davies

Pubblicato il 23/06/2026 - 13:26 CEST

In un raro comunicato congiunto, l'alleanza Five Eyes che riunisce le intelligence di Australia, Stati Uniti, Regno Unito, Canada e Nuova Zelanda ha invitato governi e Big Tech a blindare i sistemi informatici prima che sia troppo tardi. Il timore è che i nuovi modelli di IA possano diventare così potenti da diventare un'arma inarrestabile per i cybercriminali.

FONTE: https://it.euronews.com/next/2026/06/23/minaccia-cyber-dellai-entro-mesi-non-anni-avvertono-le-agenzie-dintelligence-occidentali

Nel primo semestre del 2025, in Italia, quasi il 40% dei circa 900 gravi episodi informatici registrati ha coinvolto direttamente strumenti di intelligenza artificiale generativa. Phishing e spear-phishing restano le principali modalità di attacco, ma la loro efficacia è potenziata dall'uso massiccio dei modelli linguistici: oltre l'80% delle e-mail di phishing e il 91% delle campagne di spear-phishing sfruttano oggi LLM, mentre il 52% degli attacchi basati su AI utilizza modelli pubblici per generare contenuti o codice malevolo.

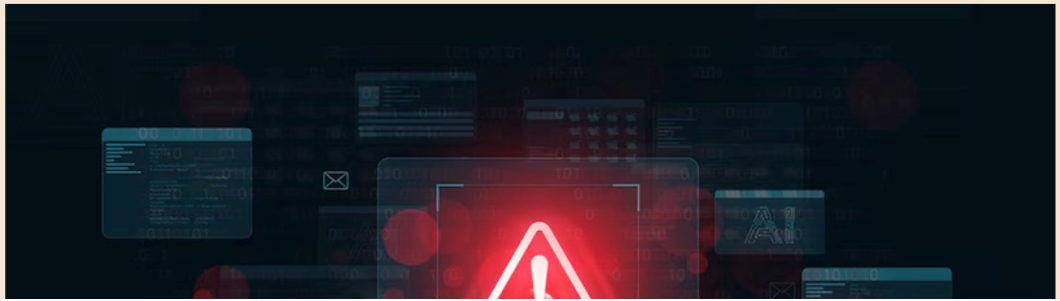
Servizio | La fotografia

Quasi il 40% degli attacchi cyber in Italia coinvolge strumenti di AI

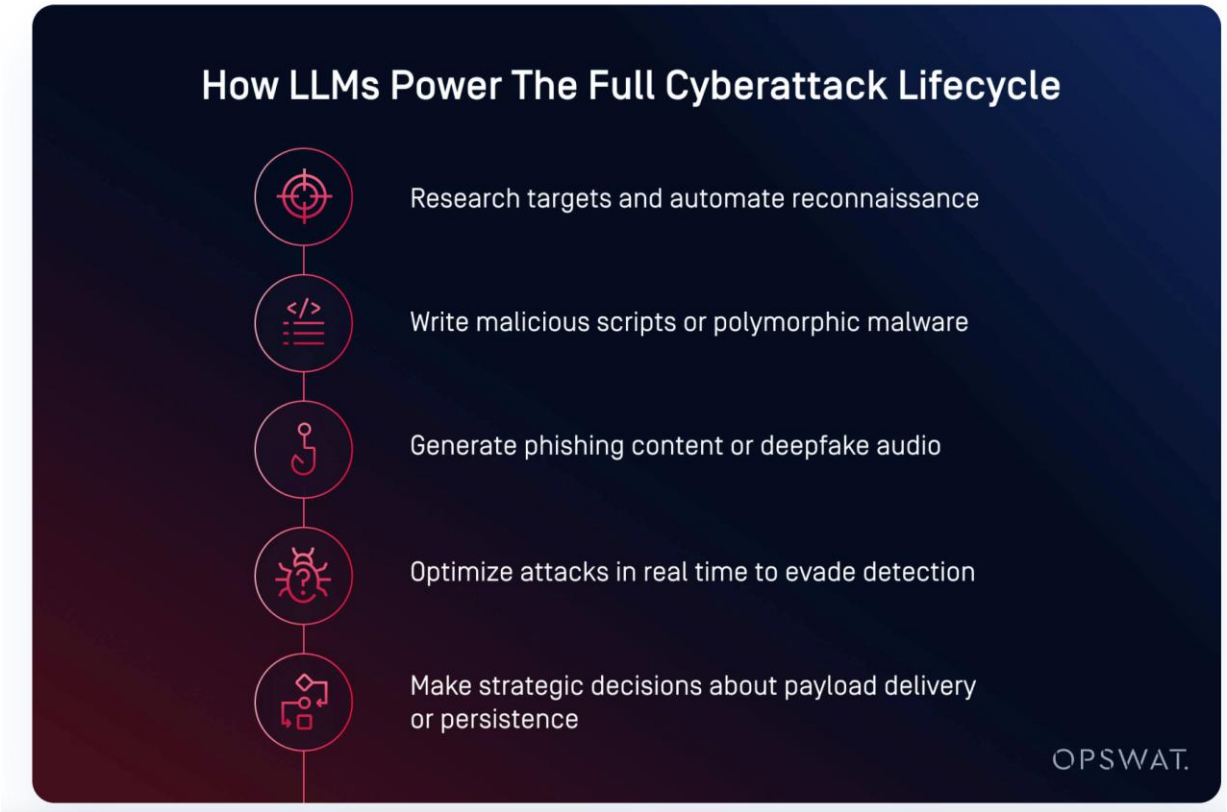
Secondo il Report AI Threat Landscape 2025, phishing e spear-phishing restano le principali modalità di attacco, ma la loro efficacia è potenziata dall'uso massiccio dei modelli linguistici: oltre l'80% delle e-mail di phishing e il 91% delle campagne di spear-phishing sfruttano oggi LLM, mentre il 52% degli attacchi basati su AI utilizza modelli pubblici per generare contenuti o codice malevolo

di Redazione Roma

16 ottobre 2025



FONTE : https://www.ilsole24ore.com/art/quasi-40percento-attacchi-cyber-italia-coinvolge-strumenti-ai-AHTOYdCD#google_vignette



AI Hacking: come gli hacker utilizzano l'intelligenza artificiale nei cyberattacchi

FONTE https://italian.opswat.com/blog/ai-hacking-how-hackers-use-artificial-intelligence-in-cyberattacks

Agentic Crime-as-a-Service e i tre casi che ridisegnano il mercato del cybercrime

A cura di: Redazione 2 Giugno 2026

Da GTG-5004 a GTG-1002, i tre casi documentati da Anthropic, OpenAI e Google fra agosto e novembre 2025 mostrano un sottobosco criminale che non vende più strumenti ma manodopera algoritmica.

«Per anni il sottobosco del cybercrime ha venduto strumenti. Oggi vende manodopera: un agente AI, erogato via API, che esegue ricognizione, sfruttamento, esfiltrazione, estorsione. »

FONTE: https://www.ictsecuritymagazine.com/notizie/agentic-crime-as-a-service/

Il Governo Usa blocca il lancio dei modelli AI avanzati di Anthropic, a Bruxelles scatta l'allarme

Per motivi di "sicurezza nazionale", Washington ordina il blocco per i cittadini stranieri e l'azienda si adegua. La misura sottolinea ancora una volta la dipendenza europea dalla tecnologia americana

di Pierangelo Soldavini

25 giugno 2026

Smartphone con il logo dell'azienda statunitense di intelligenza artificiale Anthropic PBC sullo schermo, davanti a un sito web. In primo piano la parte centro-sinistra del display del telefono. Alamy Stock Photo

Washington ha ordinato, in base alle normative sul controllo delle esportazioni, che l'accesso a questi modelli sia interrotto per "qualsiasi cittadino straniero, all'interno o all'esterno degli Usa", inclusi i "dipendenti stranieri" di Anthropic, in base a quanto riferito dalla startup dell'IA.

FONTE: ilsole24ore.com/art/il-governo-usa-blocca-lancio-modelli-avanzati-anthropic-bruxelles-scatta-l-allarme-AIQ25vpD