

Spionaggio AI: come Stati e aziende rubano segreti nell'era dell'intelligenza artificiale



Lo **spionaggio AI** rappresenta oggi una delle minacce più insidiose all'economia globale. C'è una guerra silenziosa che si combatte ogni giorno nelle server room di Google, nei laboratori di ricerca delle università americane, negli uffici dei CEO delle startup tecnologiche. Non fa rumore, non lascia macerie visibili, eppure costa all'economia statunitense centinaia di miliardi di dollari ogni anno. È il nuovo volto dello spionaggio industriale nell'era dell'intelligenza artificiale, dove la posta in gioco non sono più solo documenti militari classificati, ma l'intera infrastruttura dell'innovazione tecnologica che determinerà il futuro del potere globale.

Il caso Google: anatomia di uno spionaggio AI perfetto

Nel marzo 2024, quando l'FBI ha arrestato Linwei Ding, un ingegnere software cinese di trentotto anni che lavorava per Google, è emersa una storia che racconta perfettamente il modus operandi dello **spionaggio AI** contemporaneo. L'accusa formulata dal Dipartimento di Giustizia degli Stati Uniti era chiara quanto devastante: furto di segreti commerciali legati all'intelligenza artificiale su scala industriale.

Secondo i documenti processuali, tra maggio 2022 e maggio 2023, Ding trasferì dal network aziendale al suo account personale su Google Cloud oltre mille file contenenti

informazioni riservate sulla tecnologia AI di Google. L'imputazione integrativa emessa nell'aprile 2025 ha precisato che il numero totale superava i mille file unici, rispetto ai cinquecento inizialmente contestati. Non si trattava di documenti qualsiasi: erano i mattoni fondamentali dell'architettura AI di Google, compresi dettagli tecnici su chip TPU e GPU, il software che permette a questi chip di comunicare ed eseguire compiti complessi, e il sistema che orchestra migliaia di chip in un supercomputer capace di addestrare modelli AI all'avanguardia.

La sofisticazione del piano rivela quanto sia evoluto lo **spionaggio AI** moderno. Mentre era impiegato da Google dal 2019, Ding si affiliò segretamente a due aziende tecnologiche con sede nella Repubblica Popolare Cinese. A giugno 2022 ricevette l'offerta per diventare Chief Technology Officer di una startup tecnologica cinese in fase iniziale, che gli prometteva uno stipendio mensile di circa quattordicimila ottocento dollari, più bonus annuale e azioni della società. L'uomo creò persino una presentazione PowerPoint citando le politiche nazionali cinesi che incoraggiano lo sviluppo dell'industria AI domestica, e preparò un'altra presentazione per candidarsi a un programma di talenti sponsorizzato dal governo cinese con sede a Shanghai.

Nell'aprile 2025, quando la giustizia americana ha formalizzato sette capi d'accusa per spionaggio economico e altrettanti per furto di segreti commerciali, è emerso chiaramente come i programmi sponsorizzati dalla Repubblica Popolare Cinese incentivino individui impegnati in ricerca e sviluppo all'estero a trasmettere quella conoscenza in patria in cambio di salari, fondi di ricerca, spazio per laboratori o altri incentivi. Nella sua candidatura al programma di talenti, Ding affermò che il prodotto della sua azienda avrebbe aiutato la Cina ad avere capacità infrastrutturali di potenza di calcolo alla pari con il livello internazionale. Se condannato, Ding rischia fino a quindici anni di carcere per

ogni capo d'accusa di spionaggio economico e dieci anni per ogni capo di furto di segreti commerciali.

Questo caso non è isolato. Rappresenta invece la manifestazione più eclatante di un fenomeno sistemico che il direttore dell'FBI Christopher Wray ha definito, nelle sue dichiarazioni ufficiali, come la minaccia più ampia e completa alle idee, all'innovazione e alla sicurezza economica degli Stati Uniti. Come ha affermato Wray durante l'annuncio delle accuse contro Ding, questi casi illustrano fino a che punto le affiliate di aziende con sede nella Repubblica Popolare Cinese siano disposte ad arrivare pur di rubare l'innovazione americana.

La strategia cinese: un Piano sistematico per l'acquisizione tecnologica

Il governo cinese non nasconde le sue ambizioni di dominare il settore dell'intelligenza artificiale. Documenti ufficiali come il tredicesimo piano quinquennale e il programma Made in China 2025 delineano chiaramente quali tecnologie e proprietà intellettuali il paese intende acquisire da fonti straniere. Secondo un rapporto dell'FBI del 2019 intitolato "China: The Risk to Corporate America", la Cina aveva all'epoca fino a cento piani attivi per guidare l'acquisizione straniera nel campo della scienza e della tecnologia, con il tredicesimo piano quinquennale e Made in China 2025 identificati come i due piani più influenti e di vasta portata.

L'approccio cinese allo **spionaggio AI** è multiforme e sofisticato, orchestrato attraverso una combinazione di tattiche che vanno dal cyber spionaggio diretto all'infiltrazione di insider, passando per programmi di talenti sponsorizzati dallo Stato. Questi programmi creano incentivi economici sostanziali per individui impegnati in

ricerca e sviluppo fuori dalla Cina, offrendo loro compensi generosi per trasmettere conoscenze e ricerche alla Repubblica Popolare in cambio di salari competitivi, fondi di ricerca, spazio per laboratori o altri benefici materiali.

I numeri dello **spionaggio AI** e del furto di proprietà intellettuale parlano un linguaggio inequivocabile. Secondo il rapporto dell'FBI e le stime confermate dall'Office of the United States Trade Representative, il costo annuale per l'economia statunitense derivante da contraffazione, software piratato e furto di segreti commerciali legato alla Cina si colloca in un intervallo compreso tra duecentoventicinque e seicento miliardi di dollari. Questa stima include non solo lo **spionaggio AI** diretto, ma l'intero spettro delle violazioni di proprietà intellettuale, dalla pirateria del software alla contraffazione di beni fisici, fino al furto sistematico di segreti commerciali attraverso operazioni di intelligence.

La dimensione e la portata delle operazioni cinesi di **spionaggio AI** sono aumentate drammaticamente negli ultimi anni. Secondo il Global Threat Report 2025 di CrowdStrike, pubblicato nel febbraio 2025, le operazioni di cyber spionaggio cinesi sono aumentate del centocinquanta per cento complessivamente nel 2024 rispetto all'anno precedente. Ancora più allarmante è l'escalation in settori specifici: gli attacchi contro i settori finanziario, dei media, manifatturiero e industriale sono aumentati tra il duecento e il trecento per cento. Questa crescita esponenziale riflette una strategia deliberata e coordinata per acquisire tecnologie critiche e vantaggi competitivi in settori chiave dell'economia globale.

Il Center for Strategic and International Studies ha documentato nel suo database di incidenti cyber significativi come nel febbraio 2025 gli hacker cinesi abbiano condotto campagne continue di cyber spionaggio mirate ai settori governativo, manifatturiero, delle telecomunicazioni e dei media nel Sud-Est asiatico, Hong Kong e Taiwan, impiegando

backdoor sofisticati e incorporandosi in servizi cloud come Dropbox per il comando e controllo, al fine di eludere il rilevamento.

L'espionage aziendale: quando lo spionaggio AI diventa arma competitiva

Lo **spionaggio AI** non coinvolge solo Stati nazionali in competizione geopolitica. Il panorama delle minacce include anche attori aziendali che cercano vantaggi competitivi illegali attraverso il furto di ricerca e sviluppo dei concorrenti. Le startup AI, in particolare, si trovano in una posizione di vulnerabilità critica: spesso mancano delle risorse di sicurezza informatica delle grandi aziende consolidate, ma possiedono tecnologie all'avanguardia che le rendono bersagli estremamente attraenti per operazioni di spionaggio industriale.

Gli esperti di sicurezza informatica hanno documentato come i criminali informatici stiano sfruttando l'intelligenza artificiale generativa per facilitare attacchi su scala industriale. L'AI riduce drasticamente il tempo e lo sforzo che i criminali devono spendere per ingannare i loro obiettivi, rendendo gli schemi fraudolenti significativamente più credibili e difficili da individuare. Nel 2024, secondo quanto emerge dal rapporto annuale dell'FBI Internet Crime Complaint Center, il quarantadue per cento delle organizzazioni ha subito attacchi di phishing, vishing, deepfake e altri attacchi di social engineering che hanno avuto successo nel compromettere sistemi o rubare informazioni sensibili.

La tecnologia AI sta anche abbassando le barriere tecniche per i criminali informatici meno qualificati. Il National Cyber Security Centre del Regno Unito ha previsto che entro il 2025 l'intelligenza artificiale migliorerà significativamente le

tattiche di hacking esistenti, consentendo sia ad attori statali che non statali di condurre operazioni più sofisticate con maggiore facilità e minor costo operativo. Questa democratizzazione delle capacità di hacking esacerba drammaticamente il panorama delle minacce alla sicurezza informatica globale, rendendo lo **spionaggio AI** accessibile a un numero sempre crescente di attori malintenzionati.

Nel giugno 2025, quando la società di sicurezza SentinelOne ha rivelato che oltre settanta organizzazioni in molteplici settori erano state prese di mira da un gruppo di cyber spionaggio collegato alla Cina, è emerso un quadro inquietante della pervasività di queste operazioni. Le vittime includevano un'entità governativa dell'Asia meridionale, un'organizzazione mediatica europea e decine di aziende nei settori manifatturiero, governativo, finanziario, delle telecomunicazioni e della ricerca. Gli attaccanti avevano sfruttato vulnerabilità nelle gateway Check Point solo pochi giorni prima che queste vulnerabilità fossero divulgate pubblicamente, e avevano utilizzato infrastrutture di rete operativa gestite dalla Cina per mascherare le loro attività e mantenere l'accesso persistente ai sistemi compromessi.

CEO e dirigenti nel mirino: l'escalation dello spionaggio AI contro i leader aziendali

I dirigenti aziendali, in particolare quelli coinvolti in settori strategici come l'intelligenza artificiale, la biotecnologia e la tecnologia dei semiconduttori, sono diventati obiettivi prioritari per governi stranieri impegnati in operazioni di **spionaggio AI**. Nel 2024, la House Select Committee on the Chinese Communist Party ha allertato il pubblico su una serie continua di campagne di cyber spionaggio altamente mirate collegate al Partito Comunista Cinese, progettate specificamente per compromettere organizzazioni e

individui coinvolti nella politica commerciale e nella diplomazia tra Stati Uniti e Cina.

In settimane recenti, secondo quanto documentato dalla commissione, sospetti cyber-attaccanti cinesi hanno impersonato il presidente della commissione John Moolenaar in email inviate a controparti fidate, tentando di ingannare i destinatari e indurli ad aprire file e link che avrebbero garantito agli attaccanti l'accesso ai loro sistemi e informazioni durante impegni commerciali in corso ad alto livello tra Stati Uniti e Cina. L'analisi tecnica altamente qualificata della commissione ha confermato che gli autori hanno abusato di software e servizi cloud per nascondere la loro attività, utilizzando strumenti sviluppatori per creare percorsi nascosti che permettevano di sottrarre dati segretamente direttamente ai loro server.

Questi attacchi non si limitano a funzionari governativi. Il gruppo APT-31, anche conosciuto come Zirconium e attivo almeno dal 2013, ha preso di mira sistematicamente funzionari governativi statunitensi, appaltatori della difesa, organizzazioni mediatiche, università, think tank e altre infrastrutture critiche. Secondo il rapporto di ClearanceJobs pubblicato nel gennaio 2025, nel 2024 sette membri del gruppo sono stati incriminati dal Dipartimento di Giustizia. Hanno utilizzato attacchi di phishing e distribuzione di malware per rubare dati sensibili e interrompere servizi critici, impiegando metodologie moderne di tipo living-off-the-land che permettono loro di rimanere non rilevati per lunghi periodi mentre conducono ricognizioni sistematiche dei sistemi compromessi.

I dati personali e professionali dei dirigenti vengono raccolti sistematicamente attraverso social network professionali come LinkedIn e Facebook. Gli operatori di **spionaggio AI** utilizzano queste piattaforme per individuare e valutare dipendenti che lavorano nelle aziende target, impiegando poi reclutatori come intermediari per identificare

quali dipendenti potrebbero essere interessati a lasciare le loro posizioni attuali. Questa tattica permette agli spioni di identificare potenziali insider vulnerabili prima ancora di stabilire un contatto diretto, creando una pipeline sistematica per l'acquisizione di informazioni sensibili.

Nel suo avvertimento pubblico dell'ottobre 2024, Mike Casey, il funzionario capo del controspionaggio degli Stati Uniti, ha parlato di un forte aumento degli spioni stranieri che tentano di infiltrarsi segretamente nelle aziende tecnologiche americane, descrivendo una situazione in cui almeno parte di ciò che alimenta questa preoccupazione deriva da intelligence classificata degli Stati Uniti, presentando una sfida enorme per i funzionari che vogliono persuadere dirigenti di startup senza autorizzazione di sicurezza, e con risorse limitate, ad essere molto attenti nella scelta di investitori e partner.

Guerra economica: la competizione commerciale attraverso lo spionaggio AI

La competizione economica globale si è trasformata in una guerra ibrida dove lo **spionaggio AI** è diventato strumento centrale di politica industriale. Il 2025 sta stabilendo la sicurezza nazionale come principio guida del commercio e degli investimenti internazionali. Mentre il commercio globale è previsto in crescita nel 2025, la globalizzazione rimane sotto minaccia crescente poiché la competizione geopolitica guida la frammentazione dei sistemi finanziari e delle supply chain, complicando drammaticamente le scelte tecnologiche che aziende e governi devono compiere.

La Cina ha segnalato ripetutamente che potrebbe impiegare i suoi strumenti di ritorsione commerciale in modo molto più impattante di quanto abbia fatto finora. Mentre l'escalation tit-for-tat tra Stati Uniti e Cina si intensifica, paesi terzi

e multinazionali si trovano sempre più nel mezzo di questa battaglia economica. L'Europa in particolare sarà colpita sia dagli impatti diretti che indiretti dell'escalation, e l'Unione Europea probabilmente risponderà con le stesse misure in termini di imposizione di restrizioni commerciali.

I governi nel 2025 stanno intensificando le politiche industriali per competere con i rivali geopolitici, proteggere le catene di approvvigionamento strategiche e coltivare settori critici come l'intelligenza artificiale, la tecnologia quantistica e la biotecnologia. La competizione geopolitica e i calcoli sulla sicurezza nazionale spingeranno le politiche industriali in più angoli dell'economia globale nel 2025, includendo non solo le nuove tecnologie strategiche e sensibili, ma anche sempre più le infrastrutture e i servizi della vita quotidiana man mano che questi vengono progressivamente digitalizzati e dipendenti da sistemi di intelligenza artificiale.

Il panorama delle minacce informatiche nel 2025 sarà plasmato da attacchi sempre più sofisticati, con ransomware, social engineering e criminalità informatica potenziata dall'AI che rimangono le principali preoccupazioni. Secondo il Global Cybersecurity Outlook del World Economic Forum, il cyberspazio sta diventando più complesso, con tensioni geopolitiche, rapida adozione di tecnologie emergenti e maggiore dipendenza da catene di approvvigionamento interdipendenti come fattori chiave che contribuiscono alla crescente complessità del panorama della sicurezza globale.

Il costo umano ed economico dello spionaggio AI

Dietro le statistiche impressionanti ci sono storie concrete di aziende distrutte e lavoratori licenziati. Una società con sede in Cina è stata condannata per aver rubato i segreti tecnologici di un'azienda americana di turbine eoliche.

L'azienda vittima ha perso completamente il suo vantaggio competitivo, le vendite sono crollate drammaticamente e la società è stata costretta a licenziare quasi settecento lavoratori. Come ha sottolineato il direttore dell'FBI Christopher Wray, non si tratta solo di un problema di Wall Street o di grandi corporazioni, ma di un problema di Main Street che impatta direttamente posti di lavoro americani, famiglie americane e mezzi di sostentamento di comunità intere.

Il rapporto Internet Crime dell'FBI del 2024, pubblicato nell'aprile 2025, ha registrato perdite record di sedici virgola sei miliardi di dollari derivanti da crimini informatici, rappresentando un aumento del trentatré per cento rispetto ai dodici virgola cinque miliardi di dollari del 2023. La frode abilitata dal cyber è stata responsabile di quasi l'ottantatré per cento del totale delle perdite, evidenziando come i criminali si rivolgano sempre più alla criptovaluta come strumento per frodare investitori, riciclare proventi illeciti e facilitare una vasta gamma di altri schemi criminali.

Gli adulti sopra i sessant'anni hanno riportato sia il maggior numero di denunce che le perdite più elevate, con centoquarantasettemila centoventisei denunce per un totale di quasi quattro virgola novecento miliardi di dollari in perdite. In particolare, settemilacinquecento denunciati di età pari o superiore a sessant'anni hanno perso più di centomila dollari ciascuno, con una perdita media di ottantatremila dollari per vittima. Questi numeri rivelano non solo la portata economica dello **spionaggio AI** e dei crimini informatici correlati, ma anche la profonda vulnerabilità umana che questi attacchi sfruttano sistematicamente.

L'Internet Crime Complaint Center ha ricevuto nell'ultimo anno ottocentocinquantanovemilacinquecentotrentadue denunce, leggermente inferiori rispetto alle ottocentoottantamilaquattrocentodiciotto dell'anno precedente.

Tuttavia, dato che le perdite finanziarie hanno mostrato un aumento così marcato, appare evidente che i criminali informatici stanno dimostrando maggiore efficienza nei loro attacchi, perfezionando le loro tecniche attraverso l'uso di strumenti di intelligenza artificiale che rendono le loro operazioni più scalabili e difficili da contrastare.

La risposta: difesa e resilienza contro lo spionaggio AI

Di fronte a questa minaccia multiforme e in continua evoluzione, la risposta deve essere altrettanto complessa e coordinata. Il governo degli Stati Uniti ha intensificato i suoi sforzi attraverso la Disruptive Technology Strike Force, un'iniziativa congiunta del Dipartimento di Giustizia e del Dipartimento del Commercio progettata per trovare e ritenere responsabili coloro che rubano tecnologie americane avanzate e mettono a rischio la sicurezza nazionale e la prosperità economica.

L'alleanza Five Eyes, che comprende Stati Uniti, Canada, Regno Unito, Australia e Nuova Zelanda, ha lanciato simultaneamente nell'ottobre 2024 nuovi avvisi coordinati su come i servizi di intelligence stranieri e i criminali prendono di mira le aziende tecnologiche occidentali. Ogni paese ha creato portali online con opuscoli dettagliati e bollettini che sollecitano le startup e le aziende tecnologiche a essere estremamente attente nella scelta di investitori e partner, riconoscendo che la minaccia dello **spionaggio AI** richiede una risposta collaborativa internazionale.

Le aziende devono adottare un approccio proattivo e multistrato alla sicurezza. Secondo esperti di sicurezza, alcune delle mitigazioni più efficaci contro le minacce insider e lo **spionaggio AI** non devono necessariamente essere costose in termini di investimento finanziario, ma richiedono un impegno organizzativo sostanziale. Si raccomanda agli

sviluppatori di AI e alle aziende tecnologiche di iniziare facendo un inventario completo e dettagliato dei dati proprietari nei loro sistemi, identificando chi vi ha accesso e implementando controlli rigorosi su come queste informazioni possono essere trasferite o condivise.

La collaborazione con l'FBI e altre agenzie di sicurezza è cruciale per identificare e neutralizzare le minacce prima che possano causare danni irreparabili. L'FBI ha dimostrato la sua capacità di intervenire efficacemente, come nel caso dell'Operazione Level Up lanciata all'inizio del 2024, che ha identificato oltre quattromila trecento vittime di frode sugli investimenti in criptovalute e ha impedito con successo quasi duecentottantasei milioni di dollari in potenziali perdite attraverso interventi tempestivi e sforzi investigativi coordinati.

Il direttore generale dell'MI5 del Regno Unito, Ken McCallum, ha un messaggio inequivocabile per le aziende che operano all'avanguardia della tecnologia: se si opera all'avanguardia della tecnologia in questo decennio, si potrebbe non essere interessati alla geopolitica, ma la geopolitica è profondamente interessata a voi. Sarebbe profondamente sconsiderato, non solo con i segreti nazionali ma con la stessa vitalità della propria azienda e il capitale degli azionisti, non pensare seriamente a cosa questo significhi in termini di protezione e sicurezza.

Conclusione: la nuova frontiera dello spionaggio AI

Lo **spionaggio AI** rappresenta una delle sfide più complesse e consequenziali dell'era moderna. Non si tratta più semplicemente di proteggere documenti classificati o installazioni militari, ma di salvaguardare l'intera catena dell'innovazione tecnologica, dalla ricerca di base nelle università fino alla commercializzazione dei prodotti che

definiranno il futuro dell'economia globale. La competizione per la supremazia nell'intelligenza artificiale è fondamentalmente una competizione per il futuro stesso del potere economico e militare globale, con implicazioni che si estenderanno per decenni.

Mentre Stati come la Cina investono massicciamente in programmi sistematici di acquisizione tecnologica attraverso lo **spionaggio AI**, e aziende concorrenti ricorrono a metodi sempre più sofisticati per rubare ricerca e sviluppo, la necessità di una difesa coordinata e multistrato diventa non solo importante ma esistenziale. CEO e dirigenti devono comprendere profondamente che non sono semplicemente leader aziendali responsabili del successo commerciale delle loro organizzazioni, ma custodi di asset strategici nazionali le cui decisioni su sicurezza informatica, gestione del personale e protezione della proprietà intellettuale hanno implicazioni che vanno drammaticamente oltre i bilanci trimestrali e i rapporti agli azionisti.

La guerra per l'intelligenza artificiale si combatte oggi, in questo momento, in silenzio ma con intensità crescente, nelle reti aziendali e nei laboratori di ricerca di tutto il mondo. Chi vincerà questa battaglia silenziosa ma cruciale determinerà chi guiderà l'economia globale e plasmerà gli equilibri geopolitici nei prossimi decenni. E mentre la tecnologia avanza a velocità esponenziale, anche le tattiche dello **spionaggio AI** si evolvono con essa, diventando sempre più sofisticate, difficili da rilevare e potenzialmente devastanti nelle loro conseguenze. L'unica certezza che possiamo avere guardando al futuro è che questa guerra per il controllo dell'intelligenza artificiale è appena iniziata, e le sue conseguenze definiranno il ventunesimo secolo.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/spionaggio-ai/>