In che modo l'IA generativa sta ridisegnando le trincee della sicurezza informatica

Pubblicato il 25 marzo 2024

Mobeen Tahir
Director, Macroeconomics and Thematic Research

Principali insegnamenti

- L'IA generativa dà agli attaccanti nuovi poteri e abbassa l'asticella per coloro che desiderano compiere atti dolosi
- L'IA generativa può e deve essere impiegata anche per rafforzare le difese informatiche
- La necessità di sicurezza informatica è più sentita che mai e questo continua a creare opportunità di investimento
- Prodotti correlati WisdomTree Artificial Intelligence UCITS ETF – USD Acc, WisdomTree Cybersecurity UCITS ETF – USD Acc Scopri di più

Nel 2024, gli abitanti di 55 paesi, che rappresentano il 42% della popolazione mondiale, voteranno per eleggere i loro leader. Tra le varie elezioni, vi sono quelle di alto profilo per la presidenza degli Stati Uniti e del Parlamento dell'Unione europea[1]. Oltre ad attirare alle urne miliardi di persone, questi eventi potrebbero richiamare l'attenzione dei malintenzionati. Con gli strumenti di intelligenza artificiale (IA) generativa a loro disposizione, questi cercano di sabotare direttamente il processo elettorale violando i sistemi o di influenzare l'opinione pubblica usando disinformazione o deepfake, con capacità più grandi che mai.

In che modo l'IA generativa sta trasformando il campo di battaglia della sicurezza informatica e cosa potrebbe significare per gli investitori, che tentano di prevedere il futuro di questo tema d'investimento?

In che modo l'IA generativa può aiutare gli attaccanti

Storicamente, una formazione di base in materia di sicurezza informatica era sufficiente per consentire alle persone di identificare e difendersi dagli attacchi di phishing. Una grammatica scorretta, domini sospetti e link discutibili erano generalmente facili da individuare. Tuttavia, gli strumenti di IA generativa, come WormGPT[2], addestrati su dati relativi a malware e sviluppati specificamente per le attività criminali, possono non solo eliminare gli indizi facili da individuare nelle e-mail di phishing, ma anche abbassare l'asticella per coloro che desiderano compiere atti dolosi.

L'IA generativa può inoltre favorire il codice malware polimorfico, un tipo di programma che apprende e si evolve per diventare automaticamente più intelligente dopo un tentativo fallito. In altre parole, se l'obiettivo

non aggiorna il proprio software di sicurezza, il codice malware tornerà più forte per sfruttare qualsiasi vulnerabilità del sistema[3].

L'IA generativa sta inoltre migliorando la qualità dei deepfake. Secondo il Forum economico mondiale, tra il 9 dicembre 2023 e l'8 gennaio 2024 su Meta sono stati identificati oltre 100 video deepfake che mostravano annunci del primo ministro britannico Rishi Sunak, molti dei quali suscitavano reazioni emotive utilizzando un linguaggio del tipo "la gente è indignata"[4].

L'IA generativa può inoltre essere utilizzata per il furto di identità. Se una vittima viene ingannata e rivela i propri dati personali sensibili, è possibile falsificare documenti come passaporti e patenti di guida.

In che modo l'IA generativa può aiutare i difensori

Impiegare l'IA generativa anche per difendersi da attacchi sempre più sofisticati è una necessità imprescindibile. Ad esempio, questa può aiutare a sviluppare moduli di formazione più avanzati per consentire agli utenti di difendersi meglio da attacchi di phishing di alta qualità.

L'IA generativa può inoltre essere utilizzata per analizzare grandi quantità di dati al fine di identificare modelli, tendenze e anomalie che possono rivelare vulnerabilità nel sistema e aiutare i team di sicurezza informatica a colmare le lacune prima che un codice malware polimorfico faccia il suo ritorno.

Inoltre, può essere utilizzata per automatizzare processi ripetitivi, snellendo attività che non solo sono noiose, ma anche soggette a errori umani, come la risposta agli incidenti, il rilevamento delle minacce e l'analisi dei malware.

La sicurezza informatica è più importante che mai

Le cifre riportate di seguito costituiscono un promemoria allarmante sul fatto che l'importanza della sicurezza informatica non può essere sopravvalutata.

110%
Aumento dei casi che sfruttano il cloud su base annua nel 2023

75%
degli attacchi non conteneva malware nel 2023

2’07”
Tempo più breve mai registrato per l’evasione di un attacco informatico

4,45 mln di USD
Costo medio globale di una violazione dei dati nel 2023

Fonti: “2024 Global Threat Report”, CrowdStrike; “Cost of a Data Breach Report 2023”, IBM.

La maggior parte delle persone che possiedono uno smartphone o un computer portatile utilizza decine di applicazioni software basate sul cloud. I criminali riconoscono questa più ampia superficie di attacco e colpiscono sempre più spesso le loro vittime attraverso il cloud. Si registra inoltre un allarmante aumento degli attacchi sofisticati senza malware: 75% nel 2023 rispetto al 40% del 2019[5]. Questo suggerisce che gli attaccanti stanno passando a mezzi più rapidi ed efficaci per infiltrarsi nelle organizzazioni target, utilizzando strumenti come l'ingegneria sociale invece di affidarsi sempre sull'inserimento di un malware nel sistema della vittima. Si tratta di un importante promemoria di come la formazione in materia di sicurezza informatica non debba limitarsi a insegnare agli utenti come difendersi dagli attacchi di phishing, ma anche come rimanere in guardia contro gli inganni fisici.

Il tempo di evasione di un attacco informatico rappresenta il tempo necessario a un attaccante per spostarsi lateralmente all'interno di un'organizzazione. Significa ottenere l'accesso ad altri utenti dopo aver compromesso la prima vittima. Il tempo medio di evasione di un attacco informatico è sceso da 84 minuti nel 2022 a 62 minuti nel 2023, con il tempo più breve mai registrato pari a poco più di 2 minuti[6]. Infine, nel 2023 il costo medio delle violazioni dei dati per le organizzazioni è stato di 4,45 milioni di dollari. Questo significa che gli attaccanti sono sempre più veloci, utilizzano un'ampia gamma di strumenti e causano gravi danni alle loro vittime.

Fortunatamente, le organizzazioni stanno prendendo coscienza di questa realtà. Secondo IBM, nel 2024 l'84% dei dirigenti prevede di dare priorità alle soluzioni di sicurezza informatica basate sull'IA generativa rispetto a quelle tradizionali[7].

Cosa significa per gli investitori

La sicurezza informatica è stata uno dei temi con la migliore performance nel 2023. Il WisdomTree Team8 Cybersecurity UCITS Index ha registrato un rendimento del 66,5% nel 2023 e ha persino battuto il NASDAQ CTA Artificial Intelligence Index, che ha ottenuto un rendimento del 55,9%[8]. È ovviamente impossibile prevedere se nel 2024 assisteremo nuovamente a numeri simili. Ma se la performance di mercato delle strategie tematiche è frutto di forti correnti positive nelle tecnologie sottostanti, combinate con un più ampio apprezzamento di tali tendenze, c'è sicuramente molto di cui essere entusiasti in merito all'IA generativa e al suo impatto sulla sicurezza informatica.

[1] “2024 Global Threat Report”, CrowdStrike.

[2] https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/

[3] https://www.sangfor.com/blog/cybersecurity/what-is-generative-ai-cybersecurity

[4] https://www.weforum.org/agenda/2024/02/4-ways-to-future-proof-against-deepfakes-in-2024-and-beyond/

[5] “2024 Global Threat Report”, CrowdStrike.

[6] “2024 Global Threat Report”, CrowdStrike.

[7] https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ceo-generative-ai/cyber-security

[8] Fonte: Bloomberg, sulla base di indici di tipo “net total return”.

Important Risks Related to this Article

INFORMAZIONI IMPORTANTI

Comunicazioni di marketing emesse all'interno dello Spazio economico europeo ("SEE"): Il presente documento è stato emesso e approvato da WisdomTree Ireland Limited, società autorizzata e regolamentata dalla Central Bank of Ireland.

Comunicazioni di marketing emesse in giurisdizioni non appartenenti al SEE: Il presente documento è stato emesso e approvato da WisdomTree UK Limited, società autorizzata e regolamentata dalla Financial Conduct Authority del Regno Unito.

Per fare riferimento a WisdomTree Ireland Limited e a WisdomTree UK Limited si utilizza per entrambe la denominazione "WisdomTree" (come applicabile). La nostra politica sui conflitti d'interesse e il nostro inventario sono disponibili su richiesta.

Solo per clienti professionali. I rendimenti ottenuti nel passato non sono un'indicazione affidabile dei rendimenti futuri. I rendimenti storici ricompresi nel presente documento potrebbero essere basati sul back test, ossia la procedura di valutazione di una strategia d'investimento, che viene applicata ai dati storici per simulare quali sarebbero stati i rendimenti di tale strategia. I rendimenti basati su back test sono puramente ipotetici e vengono forniti nel presente documento a soli fini informativi. I dati basati sul back test non rappresentano rendimenti effettivi e non devono intendersi come un'indicazione di rendimenti effettivi o futuri. Il valore di un investimento potrebbe essere oggetto di oscillazioni dei tassi di cambio. Qualsiasi decisione d'investimento deve essere basata sulle informazioni contenute nel Prospetto informativo di riferimento e deve essere presa dopo aver richiesto il parere di un consulente d'investimento, fiscale e legale indipendente. I suddetti prodotti potrebbero non essere disponibili nel Suo mercato o adatti alle Sue esigenze. Il contenuto del presente documento non costituisce una consulenza in materia di investimenti, né un'offerta di vendita o una sollecitazione di un'offerta di acquisto di un prodotto o di sottoscrizione di un investimento.

Un investimento in exchange-traded product ("ETP") dipende dalla performance dell'indice sottostante, sottratti i costi, ma difficilmente replicherà la performance dell'indice con assoluta precisione. I prodotti ETP comportano numerosi rischi inclusi, tra gli altri, rischi generali di mercato correlati all'indice sottostante di riferimento, rischi di credito riferiti al provider degli swap sull'indice utilizzati nell'ETP, rischi di cambio, rischi da tasso d'interesse, rischi d'inflazione, rischi di liquidità, rischi legali e normativi.

Le informazioni contenute nel presente documento non sono, e in nessun caso devono essere interpretate come, un annuncio pubblicitario o un altro strumento di promozione di un'offerta pubblica di azioni negli Stati Uniti o in qualsiasi provincia o territorio degli stessi, laddove nessuno degli emittenti o dei relativi prodotti sia autorizzato o registrato per la distribuzione e laddove nessun prospetto di uno qualsiasi degli emittenti sia stato depositato presso una commissione di vigilanza o autorità di regolamentazione. Nessun documento, o informazione contenuta nel presente documento, deve essere estrapolato, trasmesso o distribuito (direttamente o indirettamente) negli Stati Uniti. Nessuno degli Emittenti né alcun titolo da essi

emesso sono stati o saranno registrati ai sensi dello United States Securities Act del 1933 o dell'Investment Company Act del 1940 o qualificati ai sensi di qualsiasi legge statale sui titoli applicabile.

Il presente documento può contenere commenti indipendenti sul mercato redatti da WisdomTree sulla base delle informazioni disponibili al pubblico. Benché WisdomTree si adoperi per garantire l'esattezza del contenuto del presente documento, WisdomTree non garantisce né assicura la sua esattezza o correttezza. Qualsiasi terzo fornitore di dati di cui ci si avvalga per reperire le informazioni contenute nel presente documento non rilascia alcuna garanzia o dichiarazione di sorta in relazione ai suddetti dati. Laddove WisdomTree abbia espresso dei pareri relativamente al prodotto o all'attività di mercato, si ricorda che tali pareri possono cambiare. Né WisdomTree, né alcuna consociata, né alcuno dei rispettivi funzionari, amministratori, partner o dipendenti, accetta alcuna responsabilità per qualsiasi perdita, diretta o indiretta, derivante dall'utilizzo del presente documento o del suo contenuto.

Il presente documento può contenere dichiarazioni previsionali, comprese dichiarazioni riguardanti le nostre convinzioni o le nostre attuali aspettative in relazione alla performance di determinate classi di attività e/o settori. Le dichiarazioni previsionali sono soggette a determinati rischi, incertezze e ipotesi. Non vi è alcuna garanzia che tali dichiarazioni siano esatte, e i risultati effettivi possano discostarsi significativamente da quelli previsti in dette dichiarazioni. WisdomTree raccomanda vivamente di non fare indebito affidamento sulle summenzionate dichiarazioni previsionali.

WisdomTree Issuer ICAV

I prodotti illustrati nel presente documento sono emessi da WisdomTree Issuer ICAV (l'"Emittente WT"). L'Emittente WT è una società d'investimento multicomparto a capitale variabile e con separazione delle passività tra comparti, costituita ai sensi del diritto irlandese come un veicolo di gestione patrimoniale collettiva irlandese e autorizzata dalla Central Bank of Ireland ("CBI"). L'Emittente WT è costituito come Organismo d'Investimento Collettivo in Valori Mobiliari ("OICVM") ai sensi del diritto irlandese ed emetterà una classe distinta di azioni (le "Azioni") per ciascun comparto. Si consiglia ai potenziali investitori di leggere il prospetto informativo dell'Emittente WT (il "Prospetto WT") prima di effettuare qualsiasi investimento e di riferirsi al capitolo intitolato "Fattori di rischio", per avere ulteriori informazioni in merito ai rischi associati all'investimento nelle Azioni.

WisdomTree Artificial Intelligence UCITS ETF

Nasdaq® e Nasdaq CTA Artificial Intelligence Index sono marchi commerciali registrati di Nasdaq, Inc. (denominata congiuntamente alle sue affiliate come “Società”) e sono concessi in licenza d'uso a WisdomTree Management Limited. La Società non garantisce la legittimità o adeguatezza di WisdomTree Artificial Intelligence UCITS ETF (il “Fondo”). Le azioni del Fondo non sono emesse, sostenute, vendute o promosse dalla Società. LA SOCIETÀ NON FORNISCE GARANZIE E DECLINA QUALSIVOGLIA RESPONSABILITÀ CON RIFERIMENTO AL FONDO.

Per gli Investitori in Svizzera – Invesitori Qualificati

Questo documento costituisce una pubblicità dei prodotti finanziari qui menzionati.

Il prospetto e i documenti di informazioni chiave per gli investitori (KIID) sono disponibili sul sito Web di WisdomTree: **https:** //www.wisdomtree.eu/it-ch/resource-library/prospectus-and-regulatory-reports.

Alcuni comparti di cui al presente documento potrebbero non essere stati registrati presso l'Autorità federale di vigilanza sui mercati finanziari ("FINMA"). In Svizzera, i comparti che non sono stati registrati presso la FINMA saranno distribuiti esclusivamente a investitori qualificati, definiti nella legge svizzera sugli investimenti collettivi di capitale (LICo) ovvero nella sua ordinanza di attuazione (e singolarmente modificate di volta in volta). Il rappresentante e agente per i pagamenti dei comparti in Svizzera è Société Générale Paris, Filiale di Zurigo, Talacker 50, PO Box 5070, 8021 Zurigo, Svizzera. Il prospetto, il documento contenente le informazioni chiave per gli investitori (KIID), lo statuto e le relazioni annuali e semestrali dei comparti sono disponibili gratuitamente presso il rappresentante e agente per i pagamenti svizzero. Con riferimento alla distribuzione in Svizzera, il luogo di giurisdizione e prestazione del servizio è la sede del rappresentante e agente per i pagamenti.

Per investitori francesi

Le informazioni riportate nel presente documento sono destinate esclusivamente agli investitori professionali (secondo quanto definito dalla MiFID) che investono per proprio conto e ne è vietata la distribuzione al pubblico. La distribuzione del Prospetto e l'offerta, la vendita e la consegna di Azioni in altre giurisdizioni possono essere soggette a restrizioni di legge. L'Emittente è un OICVM di diritto irlandese, approvato dall'Autorità di Vigilanza Finanziaria come OICVM conforme alle normative europee, sebbene potrebbe non essere tenuto ad adempiere alle stesse disposizioni vigenti per un prodotto simile approvato in Francia. Il Fondo è stato registrato per la commercializzazione in Francia dall'Autorità dei Mercati Finanziari (Autorité des Marchés Financiers) e può essere distribuito agli investitori in Francia. Le copie di tutti i documenti (ovvero il Prospetto, il Documento contenente le informazioni chiave per gli investitori, eventuali supplementi o appendici, le ultime relazioni annuali, l'Atto costitutivo e lo Statuto) sono disponibili, gratuitamente, presso l'agente centralizzatore francese, Societe Generale con sede in 29, boulevard Haussmann – 75009 Parigi, Francia. La sottoscrizione delle Azioni del Fondo sarà effettuata conformemente alle condizioni indicate nel Prospetto e in eventuali integrazioni o appendici.

Per Investitori Maltese

Questo documento non costituisce o forma parte di qualsiasi offerta od invito alla pubblica sottoscrizione o acquisto di quote nel Fondo, non potrà essere interpretato come tale e nessuna persona al di fuori di quella al quale questo documento stato

indirizzato od inviato sarà considerata come potenziale sottoscrittore di quote nel Fondo. Le quote del fondo non verranno commercializzate in alcun modo al pubblico a Malta senza la precedente autorizzazione dell'Autorità Finanziaria Maltese.