Comment l’IA générative redessine les lignes de front de la cybersécurité

Publié le 25 mars 2024

Mobeen Tahir
Director, Research

- L’IA générative confère aux attaquants de nouveaux pouvoirs et rend plus accessible la possibilité pour un individu de devenir un acteur malveillant.
- L’IA générative peut et doit également être utilisée pour renforcer les cyberdéfenses.
- Le besoin de cybersécurité est plus important que jamais, ce qui continue de créer des opportunités d’investissement.

En 2024, les habitants de 55 pays, qui représentent 42 % de la population mondiale, voteront pour élire leurs dirigeants, avec notamment des élections de premier plan pour la présidence des États-Unis ainsi qu’au Parlement européen1. En plus de conduire plusieurs milliards de personnes à voter, ces événements sont susceptibles d’appâter des acteurs malveillants. Ceux-ci disposant désormais d’outils d’intelligence artificielle (IA) générative, ils chercheront à saboter directement le processus électoral en piratant des systèmes, ou à influencer l’opinion publique au moyen de fausses informations ou de deepfakes. Leurs capacités sont plus étendues que jamais.

Comment l’IA générative peut être exploitée par les attaquants

Auparavant, une formation de base à la cybersécurité était suffisante pour permettre aux personnes d’identifier et de se défendre contre les attaques de type hameçonnage. Mauvaise grammaire, noms de domaine suspects et liens douteux étaient généralement simples à repérer.

Aujourd’hui, les outils d’IA générative, tels que WormGPT2, qui sont formés sur les données liées aux logiciels malveillants et développés spécifiquement pour les activités criminelles, aident non seulement à éliminer les indices faciles à détecter dans les courriels d'hameçonnage, mais réduisent également les obstacles à franchir pour devenir un acteur malveillant.

L’IA générative peut aussi contribuer à créer un code malveillant polymorphe, un type de programme qui apprend et évolue pour devenir automatiquement plus intelligent après une tentative infructueuse. Cela signifie que si la cible ne met pas à jour son logiciel de sécurité, le code malveillant reviendra plus fort pour exploiter toute vulnérabilité du système3.

L’IA générative améliore la qualité des deepfakes. D’après le Forum économique mondial, entre le 9 décembre 2023 et le 8 janvier 2024, plus de 100 deepfakes d’interventions vidéo du Premier ministre britannique Rishi Sunak ont été détectés sur Meta, dont beaucoup ont suscité des réponses émotionnelles incluant des termes tels que « la population est indignée ».4

L’IA générative est par ailleurs susceptible d’être utilisée à des fins d’usurpation d’identité. Si une victime est effectivement trompée, et qu’elle divulgue ses informations personnelles sensibles, des documents tels que des passeports et des permis de conduire peuvent être falsifiés.

Comment l’IA générative peut être exploitée par les défenseurs

Il est impératif que l’IA générative soit utilisée comme moyen de défense contre des attaques de plus en plus sophistiquées. L’IA générative peut par exemple contribuer au développement de modules de formation plus avancés, afin de permettre aux utilisateurs de mieux se protéger contre les attaques d’hameçonnage de haute qualité.

Elle peut aussi être utilisée pour analyser de grandes quantités de données, afin d’identifier les modèles, les tendances et les anomalies susceptibles d’indiquer des vulnérabilités dans le système, ainsi que pour permettre aux équipes de cybersécurité de remédier aux défaillances avant qu’un code malveillant polymorphe ne fasse son retour.

L’IA générative peut contribuer à l’amélioration des processus répétitifs ainsi qu’à la rationalisation de tâches non seulement fastidieuses, mais également sujettes aux erreurs humaines, telles que la réponse aux incidents, la recherche de menaces et l’analyse des logiciels malveillants.

La cybersécurité est plus importante que jamais

Les chiffres alarmants ci-dessous rappellent que l'importance de la cybersécurité ne saurait être surestimée.

+110 %
Augmentation des cas spécifiques aux environnements cloud

75 %
des attaques n’utilisaient pas de logiciel malveillant en 2023

2 min et 7 s
Durée de propagation la plus rapide enregistrée pour un acte de cybercriminalité

4,45 millions
Coût moyen global d’une violation de données en 2023

Sources : CrowdStrike, « 2024 Global Threat Report », IBM, Cost of a Data Breach Report 2023

La plupart des personnes qui possèdent un smartphone ou un ordinateur portable utilisent généralement des dizaines d'applications logicielles basées dans le cloud. Les criminels ont conscience de ce plus large périmètre d'attaque et s'en prennent de plus en plus à leurs victimes via le cloud. On observe également une augmentation alarmante de la proportion d'attaques sophistiquées n'utilisant pas de logiciel malveillant : 75 % en 2023 contre 40 % en 20195. Ceci indique que les attaquants s'orientent vers des moyens plus rapides et plus efficaces pour infiltrer les organisations qu'ils ciblent, en utilisant par exemple des procédés tels que l'ingénierie sociale plutôt que de compter systématiquement sur l'implantation d'un logiciel malveillant dans le système de leur victime. Il s'agit là d'un rappel important : la formation à la cybersécurité doit apprendre aux utilisateurs à non seulement se défendre contre les attaques d'hameçonnage, mais aussi à se protéger contre les tromperies physiques.

La durée de propagation d'un acte de cybercriminalité correspond au temps nécessaire à un attaquant pour se déplacer latéralement au sein d'une organisation. L'attaquant accède à d'autres utilisateurs après avoir initialement nui à la première victime. La durée moyenne de propagation d'un acte de cybercriminalité est passée de 84 minutes en 2022 à 62 minutes en 2023, la durée la plus rapide enregistrée s'étant élevée à un peu plus de 2 minutes seulement6. Enfin, le coût moyen des violations de données pour les organisations s'est élevé à 4,45 millions de dollars en 2023. Cela signifie que les attaquants deviennent plus rapides, qu'ils utilisent un large éventail d'outils, et qu'ils causent de sérieux préjudices à leurs victimes.

Fort heureusement, les organisations prennent graduellement conscience de cette réalité. Selon IBM, 84 % des dirigeants prévoient de privilégier en 2024 les solutions de cybersécurité d'IA générative par rapport aux solutions de cybersécurité traditionnelles7.

Ce que cela signifie pour les investisseurs

La cybersécurité a figuré parmi les thèmes les plus performants en 2023. L'indice WisdomTree Team8 Cybersecurity UCITS a enregistré un rendement de 66,5 % en 2023, allant jusqu'à l'emporter sur l'indice NASDAQ CTA Artificial Intelligence, qui a enregistré un rendement de 55,9 %.8 Il est évidemment impossible de prédire si nous connaîtrons des chiffres similaires en 2024. Pour autant, si la performance du marché pour les stratégies thématiques est fonction de forts courants positifs dans les technologies sous-jacentes, parallèlement à une appréciation plus large de ces tendances, tout porte à demeurer enthousiaste concernant l'IA générative et son impact sur la cybersécurité.

1 Crowdstrike « 2024 Global Threat Report »

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 Crowdstrike « 2024 Global Threat Report »

6 Crowdstrike « 2024 Global Threat Report »

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

8 Source : Bloomberg, sur la base des indices de rendements totaux nets.

Important Risks Related to this Article

INFORMATIONS IMPORTANTES

Communications commerciales publiées dans l¼Espace économique européen (« EEE ») Ce document est publié et approuvé par WisdomTree Ireland Limited, une société autorisée et réglementée par la Central Bank of Ireland.

Communications commerciales émises dans des juridictions en dehors de l¼EEE Ce document est publié et approuvé par WisdomTree UK Limited, une société autorisée et réglementée par la Financial Conduct Authority du Royaume-Uni.

WisdomTree Ireland Limited et WisdomTree UK Limited sont toutes les deux désignées comme « WisdomTree » (le cas échéant). Notre Politique sur les conflits d¼intérêts et notre Inventaire sont disponibles sur demande.

Réservé aux clients professionnels uniquement. La performance passée ne constitue pas une indication fiable des performances futures. Toute donnée de performance historique incluse dans ce document peut avoir été obtenue par calcul a posteriori (« back testing »). Le back testing est le processus qui consiste à évaluer une stratégie d¼investissement en l¼appliquant à des données historiques afin de simuler la performance que cette stratégie aurait produite. La performance ainsi obtenue est purement hypothétique et n¼est fournie dans ce document qu¼à des fins d¼information. Les données obtenues par calcul a posteriori ne représentent pas une performance réelle et ne doivent pas être considérées comme indicatives d¼une performance réelle ou future. La valeur de tout investissement peut être aectée par des fluctuations de taux de change. Toute décision d¼investissement doit être fondée sur les informations figurant dans le prospectus approprié et sur des conseils indépendants en matière d¼investissement, fiscaux et juridiques. Ces produits peuvent ne pas être disponibles sur votre marché ou ne pas vous convenir. Le contenu de ce document ne constitue ni un conseil en investissement, ni une ore de vente ni une sollicitation d¼ore d¼achat d¼un produit ou d¼investissement.

Un investissement dans des produits cotés en bourse (ETP) dépend de la performance de l¼indice sous-jacent, moins les coûts, mais ne doit pas égaler exactement cette performance. Les ETP présentent de nombreux risques, notamment les risques de marché généraux liés à l¼indice sous-jacent concerné, les risques de crédit sur le fournisseur des swaps sur indice utilisés dans les ETP, les risques de change, les risques de taux d¼intérêt, les risques d¼inflation, les risques de liquidité, et les risques juridiques et réglementaires.

Ce document n¼est pas et ne doit en aucun cas être interprété comme, une publicité ou une ore publique de vente d¼actions aux États-Unis ou dans toute province ou tout territoire des États-Unis, où ni les émetteurs ni leurs produits ne sont agréés ou inscrits, où la distribution des produits n¼est pas autorisée et où aucun prospectus des émetteurs n¼a été déposé auprès d¼une quelconque commission des valeurs mobilières ou autorité de règlementation. L¼introduction, la transmission et la distribution (directes ou indirectes) de ce document ou des informations qu¼il contient sont interdites aux États-Unis. Ni les émetteurs ni aucun titre

émis par eux n¼a été ni ne sera enregistré en vertu de la Loi américaine de 1933 sur les valeurs mobilières (United States Securities Act of 1933) ou de la Loi américaine de 1940 sur les sociétés d¼investissement (Investment Company Act of 1940) et aucun d¼eux n¼a été ni ne sera qualifié en vertu des dispositions légales applicables de tout État relatives aux valeurs mobilières.

Ce document peut contenir des commentaires indépendants sur le marché rédigés par WisdomTree sur la base des informations publiques disponibles. Bien que WisdomTree s¼eorce d¼assurer l¼exactitude du contenu de ce document, WisdomTree ne peut en garantir l¼exactitude. Les fournisseurs de données tiers sollicités pour obtenir les informations contenues dans le présent document ne donnent aucune garantie ou représentation de quelque sorte en rapport avec ces données. Lorsque WisdomTree exprime ses propres opinions concernant le produit ou l¼activité du marché, ces opinions sont susceptibles de changer. WisdomTree, ses ailiés et leurs dirigeants, directeurs, partenaires ou employés respectifs déclinent toute responsabilité pour toute perte directe ou indirecte découlant de l¼utilisation de ce document ou de son contenu.

Ce document peut contenir des déclarations prospectives, y compris notre opinion ou nos attentes actuelles concernant la performance de certains secteurs et/ou catégories d¼actions. Les déclarations prospectives sont sujettes à certains risques, incertitudes et hypothèses. Il n¼existe aucune garantie quant à l¼exactitude de ces déclarations et les résultats réels peuvent diérer sensiblement des résultats prévus dans ces déclarations. WisdomTree recommande fortement de prendre ces déclarations prospectives avec la plus grande précaution.

WisdomTree Issuer ICAV

Les produits pris en considération dans le présent document sont émis par WisdomTree Issuer ICAV (l¼« Émetteur WT »). L¼Émetteur WT est une société d¼investissement à compartiments multiples, à capital variable et à responsabilité séparée entre ses fonds, structurée sous forme de Véhicule de gestion collective d¼actifs de droit irlandais en vertu de la législation irlandaise et agréée par la Central Bank of Ireland (« CBI »). L¼Émetteur WT est structuré sous forme d¼Organisme de placement collectif en valeurs mobilières (« OPCVM ») en vertu de la législation irlandaise et procèdera à l¼émission d¼une catégorie d¼actions distincte (« Actions ») représentative de chaque fonds. Les investisseurs sont invités à lire le prospectus de l¼Émetteur WT (« Prospectus WT ») avant d¼investir, et à consulter la section du Prospectus WT intitulée « Risk Factors » pour plus de détails sur les risques associés à un investissement dans les Actions.

WisdomTree Artificial Intelligence UCITS ETF

Nasdaq® et l¼indice Nasdaq CTA Artificial intelligence Index sont des marques déposées de Nasdaq, Inc. (qui, avec ses entités ailiées, sont désignées conjointement « les Sociétés ») et font l¼objet d¼une licence concédée à WisdomTree Management Limited. Les Sociétés ne se sont pas prononcées quant à la légalité ou la pertinence du Fonds WisdomTree Artificial Intelligence UCITS ETF (le « Fonds »). Les Actions du Fonds ne sont ni émises, approuvées, vendues ou promues par les Sociétés. LES SOCIÉTÉS NE

FOURNISSENT AUCUNE GARANTIE ET DÉCLINENT TOUTE RESPONSABILITÉ CONCERNANT LE FONDS.

Notice to Investors in Switzerland – Qualified Investors

Le présent document constitue un document promotionnel relatif au(x) produit(s) financier(s) y mentionné(s).

Le prospectus et le Document d¼informations clés aux Investisseurs (DICI) sont disponibles sur le site Internet de WisdomTree : **https:** //www.wisdomtree.eu/fr-ch/resource-library/prospectus-and-regulatory-reports

Certains des compartiments figurant sur le présent document pourraient ne pas avoir été enregistrés auprès de l¼Autorité fédérale suisse de surveillance des marchés financiers (« FINMA »). En Suisse, les compartiments en question, qui n¼ont pas été enregistrés auprès de la FINMA, seront exclusivement distribués à des investisseurs qualifiés, au sens établi par la Loi fédérale suisse sur les placements collectifs de capitaux ou son ordonnance d¼application (chacune pouvant être amendée, le cas échéant). Le représentant et agent payeur des compartiments en Suisse est Société Générale Paris,

Zurich Branch, Talacker 50, PO Box 5070, 8021 Zurich, Suisse. Le prospectus, les documents d¼informations clés pour l¼investisseur (DICI), les statuts ainsi que les rapports annuels et semestriels des compartiments sont disponibles gratuitement auprès du représentant et agent payeur. Concernant la distribution en Suisse, le lieu d¼exécution et la juridiction compétente correspondront au siège du représentant et agent payeur.

À l¼intention des investisseurs en France

Les informations présentées dans le présent document sont préparées à la seule intention des investisseurs professionnels (au sens de la directive MiFID) qui investissent pour leur propre compte. Par ailleurs, ce document ne saurait aucunement être distribué auprès du public. La distribution du Prospectus et l¼ore, la vente ou remise d¼Actions dans d¼autres juridictions peuvent être restreintes ou interdites par la loi. WT Issuer est un OPCVM régi par la législation irlandaise et agréé par la Financial Regulatory (autorité de réglementation financière) en tant qu¼OPCVM conforme à la réglementation européenne, mais n¼est pas tenu néanmoins de respecter les mêmes règles que celles qui s¼appliquent pour un produit similaire agréé en France. Le Fonds a été enregistré à des fins de commercialisation en France par la Financial Markets Authority (Autorité des marchés financiers) et peut être distribué auprès des investisseurs situés en France. Des copies de tous les documents (c¼-à d. le Prospectus, le Document d¼informations clés pour l¼investisseur, tout supplément ou addenda y aérent, les derniers rapports annuels ainsi que l¼Acte et les statuts constitutifs) sont disponibles en France, gratuitement auprès de l¼agent centralisateur français, Societe Generale au 29, Boulevard Haussmann, 75009, Paris, France. Toute souscription d¼Actions du Fonds s¼eectuera selon les conditions prévues dans le prospectus et tout supplément ou addenda y aérent.

For Investors in Monaco

Ce document est destiné spécifiquement et uniquement aux banques dûment enregistrées et / ou les sociétés de gestion de portefeuille autorisées à Monaco. Ce document ne doit pas être envoyée au public à Monaco.