Les cybercriminels progressent/: la cyber-sécurité doit riposter sans attendre

Publié le 31 mars 2025

Mobeen Tahir
Director, Research

- Les cybercriminels utilisent l'IA et l'ingénierie sociale pour lancer des attaques plus sophistiquées.
- Une détection rapide est essentielle : certaines violations progressent en moins d'une minute.
- Les cyberattaques de grande ampleur impliquent des risques géopolitiques, qu'il s'agisse d'ingérence dans les élections ou d'atteintes à l'intégrité des gouvernements.

J'ai récemment créé un site Web, mais peu après son lancement, j'ai remarqué qu'il n'apparaissait pas dans les recherches Google. Alors que je cherchais une solution, j'ai reçu un e-mail contenant des instructions détaillées sur la marche à suivre. Rien ne semblait suspect, pas même l'adresse de l'expéditeur. Mais lorsque j'ai utilisé l'intelligence artificielle (IA) pour vérifier son authenticité, elle a été signalée comme étant d'origine douteuse.

Il y a quelques années, les e-mails d'hameçonnage comportaient des signaux d'alerte évidents : fautes de grammaire, mise en forme inhabituelle ou liens douteux. Grâce aux outils d'IA dont ils disposent, les cybercriminels sont aujourd'hui beaucoup plus ingénieux. S'ils gagnent en intelligence, alors la cybersécurité doit se montrer encore plus clairvoyante.

Le coût exorbitant d'une violation de données

En 2024, le coût moyen d'une violation de données a considérablement augmenté, pour atteindre près de 5 millions de dollars1. Et il ne s'agit que d'une moyenne, ce qui signifie que de nombreuses violations ont entraîné des pertes nettement plus importantes. Bien que ce nombre soit en hausse depuis plusieurs années, l'augmentation a été particulièrement marquée en 2024, soulignant la manière dont l'adoption généralisée d'outils d'IA avancés rend les cybercriminels plus intelligents et les attaques plus coûteuses que jamais.

« La vitesse des attaques pourrait être multipliée par 100 à mesure que les acteurs malveillants tirent parti de l'IA générative » – Palo Alto Networks

Dans bien des cas, le véritable coût d'une violation de données dépasse les considérations financières : il est inestimable. Que se passe-t-il lorsque la confiance des clients dans la sécurité d'une entreprise est brisée ? L'atteinte à la réputation peut être irréversible. Que se passe-t-il si un hôpital est piraté et que des vies humaines sont en jeu ? Les conséquences ne sauraient être plus graves. C'est pourquoi la cybersécurité est plus qu'une simple priorité, c'est une nécessité absolue. Et le monde prend enfin conscience de cette réalité.

Les cybercriminels deviennent plus intelligents

d'augmentation du nombre d'attaques par hameçonnage vocal (vishing) au S2 2024 par rapport au S1 2024

des attaques étaient exemptes de logiciels malveillants en 2024 (contre 40 % en 2019)

51 secondes

durée de propagation la plus rapide enregistrée pour un acte de cybercriminalité

adversaires répertoriés, dont 26 nouveaux en 2024

Source : Rapport 2025 sur les menaces mondiales de CrowdStrike, mars 2025.

Lorsque les cybercriminels compromettent une cible, leur intention est d'infiltrer l'organisation via un maillon faible et de s'introduire profondément dans le réseau. La durée de propagation d'un acte de cybercriminalité désigne la vitesse à laquelle les cybercriminels prennent le contrôle, passant de l'intrusion initiale aux systèmes critiques, au vol de données, à la désactivation des systèmes de sécurité ou au déploiement de rançongiciels. Certains attaquants y parviennent en moins d'une heure, d'où l'importance d'une détection et d'une réaction rapides. En 2024, certains attaquants ont franchi cette étape en seulement 51 secondes2.

Les attaquants ne se contentent pas d'envoyer des e-mails : les appels indésirables que nous recevons sont souvent plus malveillants qu'il n'y paraît. Les attaques par vishing (hameçonnage vocal) consistent pour les cybercriminels à recourir à des appels téléphoniques pour se faire passer pour des entités de confiance, telles que des banques, des agences gouvernementales ou des fournisseurs de services, afin d'inciter les victimes à révéler des informations sensibles ou à transférer de l'argent. Ces escroqueries ont connu un essor spectaculaire, avec une augmentation de 442 % du vishing au S2 2024 par rapport au S1 20243, ce qui révèle à quel point les criminels exploitent la confiance des individus au téléphone pour contourner les barrières de cybersécurité traditionnelles.

Il y a quelques semaines, j'ai vu sur LinkedIn une publication qui montrait un homme entouré de policiers. Il racontait comment il s'était introduit physiquement dans une organisation, franchissant les points de sécurité, accédant aux zones sensibles et tentant sa chance jusqu'à ce qu'il se fasse finalement attraper. Il ne s'agissait pas toutefois d'une véritable attaque, mais d'un test de pénétration, un exercice contrôlé de sécurité visant à détecter les failles avant qu'elles ne soient exploitées par des criminels. Les organisations

effectuent ces tests dans la mesure où les pirates informatiques utilisent des techniques d'ingénierie sociale de plus en plus sophistiquées, manipulant les individus plutôt que les systèmes, afin de contourner la sécurité et d'accéder aux informations. La menace ne cesse de croître, 79 % des attaques en 2024 étant exemptes de logiciels malveillants, contre 40 % en 20194, ce qui prouve que les cybercriminels n'ont pas nécessairement besoin de logiciels malveillants lorsqu'ils peuvent simplement convaincre les individus d'ouvrir la porte.

Les attaques de grande ampleur exposent à des risques géopolitiques

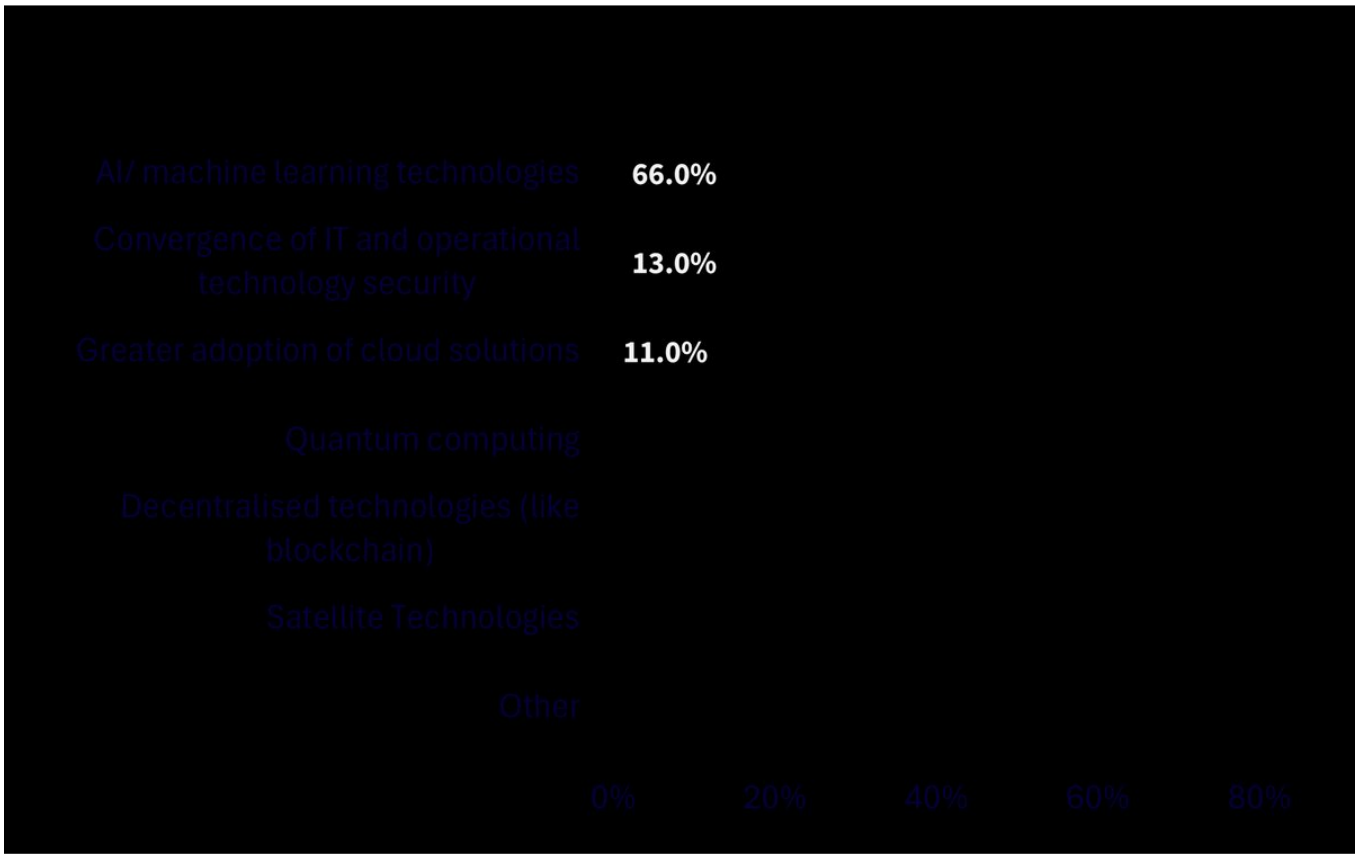
Au début de l'année 2024, les préoccupations concernant les risques de cybersécurité pour cette année à forts enjeux électoraux étaient largement partagées. Alors que de nombreux pays ont organisé leur cycle électoral sans incident cybernétique majeur, l'élection présidentielle en Roumanie au mois de décembre a dû être annulée en raison de soupçons d'ingérence russe. L'avance inattendue du candidat d'extrême droite, Calin Georgescu, au premier tour a donné lieu à des enquêtes révélant une campagne en ligne coordonnée et des cyberattaques soutenant sa candidature, ce qui a conduit les tribunaux à annuler l'élection.

Le même mois, le département du Trésor américain a fait état d'une importante violation de cybersécurité attribuée à des pirates informatiques financés par l'État chinois. Les attaquants ont exploité un fournisseur de logiciels tiers pour accéder à des postes de travail ainsi qu'à des documents non classifiés du Trésor américain. La violation a concerné le vol d'une clé de sécurité, permettant l'accès à distance aux systèmes du département. Bien que le ministère chinois des Affaires étrangères ait démenti ces allégations, l'incident souligne la convergence croissante des risques géopolitiques et de cybersécurité.

Les dirigeants sont préoccupés par les risques liés à l'IA

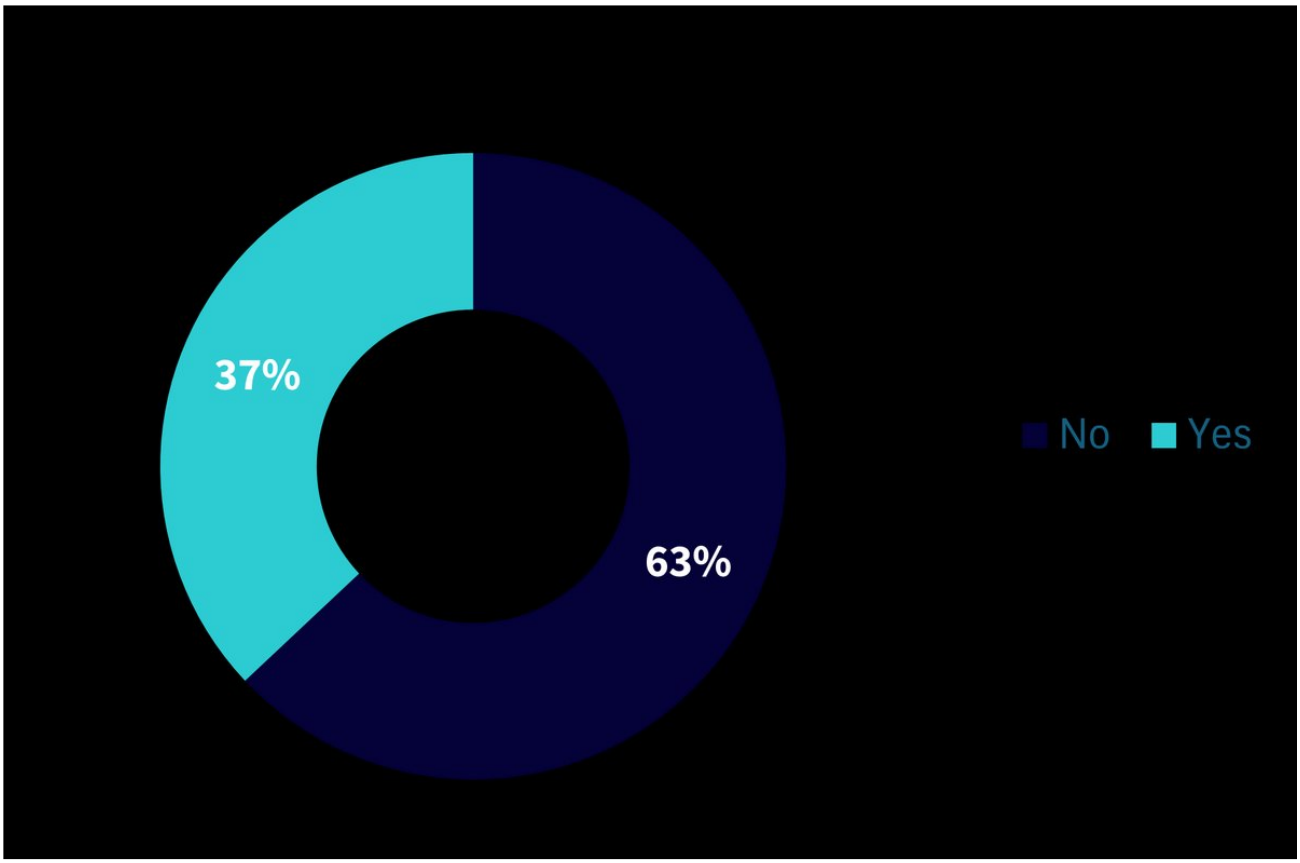
Une récente enquête du Forum économique mondial5 menée auprès des dirigeants a révélé que 66 % d'entre eux estimaient que l'IA et l'apprentissage automatique exerceraient l'impact le plus important sur la cybersécurité au cours des douze prochains mois. Pourtant, 63 % d'entre eux ont admis que leur organisation ne disposait pas de procédures permettant d'évaluer la sécurité des outils d'IA avant leur déploiement, ce qui met en évidence le décalage majeur entre innovation et gestion des risques.

Illustration 1 : Selon vous, lequel des éléments suivants exercera l'impact le plus important sur la cybersécurité au cours des douze prochains mois ?



Source : Rapport mondial sur la cybersécurité 2025 du Forum économique mondial.

Illustration 2 : Votre organisation a-t-elle mis en place une procédure permettant d'évaluer la sécurité des outils d'IA avant leur déploiement ?



Source : Rapport mondial sur la cybersécurité 2025 du Forum économique mondial.

L'ETF regroupe un portefeuille d'entreprises de cybersécurité pure play, qui cible celles qui connaissent une forte croissance de leurs revenus et qui couvrent plusieurs thèmes liés à la cybersécurité. Pour les investisseurs à la recherche d'une exposition intelligente à ce thème crucial, cet ETF peut contribuer à accroître le potentiel de croissance de leur portefeuille.

La cybersécurité doit garder une longueur d'avance

La cybersécurité doit constamment innover, en tirant parti d'une technologie de pointe pour garder une longueur d'avance sur l'évolution des menaces. C'est précisément cette compétition incessante entre défenseurs et attaquants qui fait de la cybersécurité un domaine aussi passionnant et dynamique. Les nouvelles récentes concernant l'informatique quantique suggèrent que l'ère quantique pourrait être plus proche que ce que l'on pensait. Or l'ordinateur quantique du futur pourrait facilement briser les systèmes de chiffrement les plus complexes. Cette évolution redéfinirait la cybersécurité telle que nous la connaissons. Qu'il s'agisse de l'informatique quantique, de l'IA ou de la blockchain, chaque percée engendre de nouvelles vulnérabilités. Il est donc nécessaire d'adopter une démarche proactive plutôt que réactive pour assurer la sécurité. En effet, si l'on attend que l'attaque se produise, il se peut qu'il soit déjà trop tard.

1 IBM, 2025.
2 Source : Rapport 2025 sur les menaces mondiales de CrowdStrike, mars 2025.
3 Source : Rapport 2025 sur les menaces mondiales de CrowdStrike, mars 2025.

4 Source : Rapport 2025 sur les menaces mondiales de CrowdStrike, mars 2025.
5 Source : Rapport mondial sur la cybersécurité 2025 du Forum économique mondial.

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 Banque Centrale d¼Irlande (« BCI »). L¼Émetteur WT est structuré sous forme d¼Organisme de placement collectif en valeurs mobilières (« OPCVM ») en vertu de la législation irlandaise et procédera à l¼émission d¼une catégorie d¼actions distincte (« Actions ») représentative de chaque fonds.

Le Fonds est décrit dans un Document d¼informations clés (DIC) ou Document d¼informations clés pour l¼investisseur (DICI) à l¼intention des investisseurs britanniques, et dans le prospectus de l¼Émetteur WT (« Prospectus WT »). Un exemplaire du Prospectus WT et du DIC / DICI est mis à disposition, pour l¼Espace Économique Européen (l¼«EEE »)/le Royaume-Uni uniquement, en anglais, sur le site www.wisdomtree.eu. Lorsque les réglementations nationales l¼exigent, le DIC sera également disponible dans la langue locale de l¼État membre de l¼EEE concerné. Les investisseurs sont invités à lire le 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.

La synthèse des droits de l'investisseur associés à un placement dans le fonds est disponible en anglais sur le site Internet de WisdomTree Europe. WisdomTree Management Limited peut décider de

résilier les accords portant sur la commercialisation de ses organismes de placement collectif. Dans ces circonstances, les actionnaires sujets de l¼État membre de l¼EEE concerné seront informés de cette décision et se verront orir la possibilité de racheter leur participation dans le fonds, sans frais ni retenues durant une période minimum de 30 jours ouvrables à compter de la date de notification en question.

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