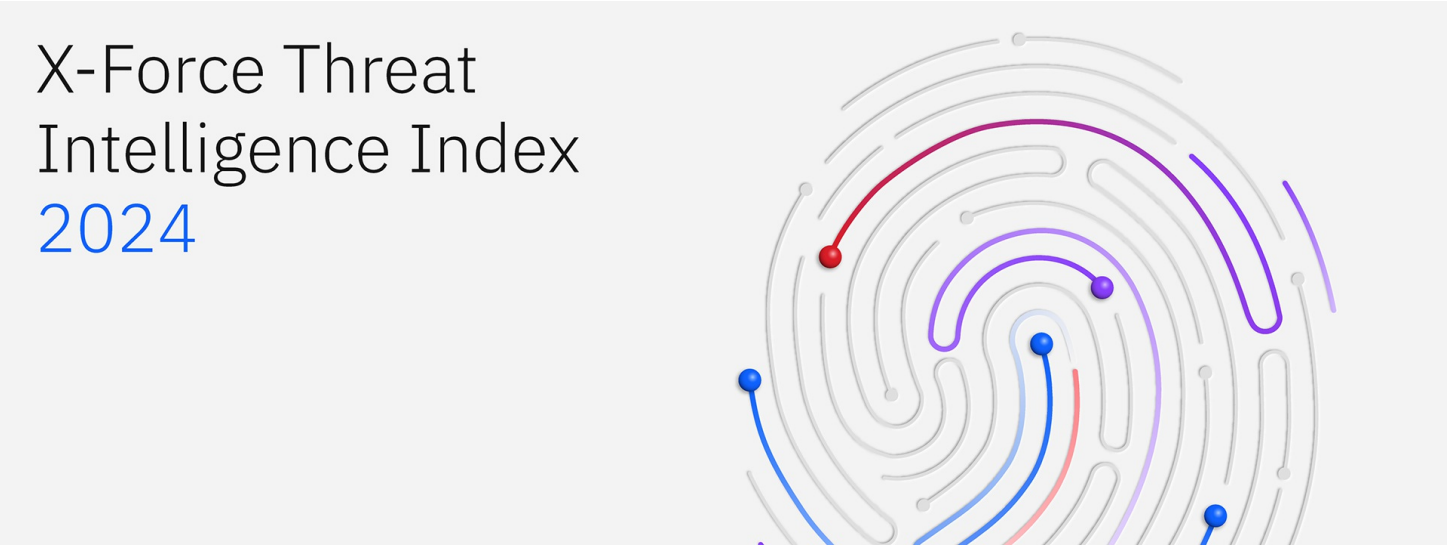
Communiqués de presse

IBM annonce aujourd'hui les résultats de l’édition 2024 de son rapport annuel X-Force Threat Intelligence Index sur le paysage mondial des menaces.



Voici l’extrait des données clés pour la France et l’Europe (le communiqué de presse **ci-dessous** présente les **chiffres au niveau mondial**) :

Données France

- 59 % des attaques observées en France visaient les services aux entreprises[1], qui ont été les principales victimes.
- Les pays d’Europe les plus ciblés sont : le Royaume-Uni (27%), l’Allemagne (15%), le Danemark (14%), le Portugal (11%), **la France (8%)** et l’Italie (8%)

Données Europe (le continent)

- En 2023, l'Europe a été la zone géographique la plus ciblée au niveau mondial, avec près d'une attaque sur trois observée dans le monde dirigée contre cette région (32 %), un nombre record d'attaques jamais signalé par X-Force auparavant dans cette région. Le volume des attaques contre l'Europe en 2023 a dépassé celui de l'Amérique du Nord, de l'Asie-Pacifique, de l’Amérique Latine et de la région Moyen-Orient-Afrique.
- En Europe, X-Force a observé une augmentation de 66 % d'une année sur l'autre des attaques causées par l'utilisation frauduleuse de comptes valides.
- Les maillons les plus faibles pour les organisations européennes ont été les identités et les emails - avec l'utilisation abusive de comptes valides (30 %) et le phishing (30 %), qui constituent les causes les plus

fréquentes d'attaques dans la région.

- Les logiciels malveillants ont été le type d’attaque le plus observé, représentant 44% des incidents, et la région a connu le plus grand nombre d'attaques par ransomware au niveau mondial (26%), ce qui a en partie contribué à son ascension dans le classement en 2023.
- Les trois impacts les plus importants pour les organisations basées en Europe sont la collecte d'informations d'identification (28 %), l'extorsion (24 %) et la fuite de données (16 %).
- Au niveau sectoriel, l'industrie manufacturière est passée de la deuxième place en 2022 à l'industrie la plus ciblée en 2023, avec 28 % des incidents.
- Les services aux entreprises et aux consommateurs arrivent en deuxième position avec 25 % des cas tandis que la finance et l'assurance ainsi que l'énergie suivent avec respectivement 16 % et 14 %.
- Lors de l'analyse des attaques par secteur d'activité à l'échelle mondiale, c’est l'Europe qui a connu le pourcentage le plus élevé d'incidents dans le secteur de l'énergie (43 %), ainsi que dans le secteur de la finance et de l'assurance (37 %).

Données Europe (l’Union Européenne)

- Près de 70 % des attaques auxquelles X-Force a répondu contre des organisations européennes ont eu lieu dans des États membres de l'UE.
- Près de 74 % des attaques observées visaient des infrastructures critiques.
- Les logiciels malveillants ont constitué le type d’attaque le plus observé, représentant 40 %. Viennent ensuite l'utilisation d'outils légitimes (26 %) et l'accès aux serveurs (15 %).
- Les ransomwares étaient le principal type de logiciels observés dans près de 26 % des attaques par logiciels malveillants.

Rapport IBM : L'identité numérique fait l'objet d'attaques, ce qui ralentit le temps de récupération des entreprises suite à des violations

- *A l’échelle mondiale, augmentation de 71 % des cyberattaques causées par l'exploitation de l'identité*
- *La barre des 50 % d’adoption atteinte par l’IA va déclencher un problème cyber*
- *Près de 70% des attaques au niveau mondial ont visé les infrastructures critiques en 2023*

CAMBRIDGE, Massachusetts, le 21 février 2024 : IBM a publié aujourd'hui le rapport X-Force Threat Intelligence Index 2024, qui met en évidence une crise mondiale émergente des identités numériques, alors que les cybercriminels redoublent d'efforts pour exploiter les identités des utilisateurs afin de compromettre les entreprises dans le monde entier. Selon IBM X-Force (l’équipe d'IBM Consulting spécialisée dans les services de sécurité offensifs et défensifs), en 2023, les cybercriminels ont vu davantage d'opportunités de se "connecter" aux réseaux d'entreprise par le biais de comptes valides plutôt que de pirater les réseaux, faisant de cette tactique une arme de choix pour les cyberattaquants.

Le rapport X-Force Threat Intelligence Index est basé sur des informations et des observations issues de la surveillance de plus de 150 milliards d'événements de sécurité par jour dans plus de 130 pays. En outre, les données sont recueillies et analysées à partir de plusieurs sources au sein d'IBM, notamment IBM X-Force Threat Intelligence, Incident Response, X-Force Red, IBM Managed Security Services, ainsi que des données fournies par Red Hat Insights et Intezer, qui ont contribué à l'élaboration du rapport 2024.

Voici quelques-uns des points saillants du rapport :

- **Les attaques contre les infrastructures critiques révèlent les difficultés rencontrées par ce secteur**. Dans près de 85 % des attaques contre des secteurs critiques, la compromission aurait pu être atténuée par l'application de correctifs, l'authentification multifactorielle ou le principe du moindre privilège, ce qui montre que ce que le secteur de la cybersécurité a toujours décrit comme la "sécurité de base" est peut-être plus difficile à mettre en œuvre qu'on ne le croit.

- **Les groupes de ransomwares s'orientent vers un modèle économique plus simple .** Les attaques par ransomware contre les entreprises ont chuté de près de 12 % l'année dernière, les grandes entreprises ayant choisi de ne pas payer et de ne pas déchiffrer, préférant reconstruire leur infrastructure. Cette réticence croissante est susceptible d'avoir un impact sur les revenus que les attaquants attendent de l'extorsion basée sur le chiffrement. On observe par ailleurs que les groupes qui se spécialisaient auparavant dans les ransomwares sont en train de se reconvertir en voleurs d'informations.

- **Le retour sur investissement des attaques contre l'IA générative n'est pas - encore - au rendez-vous.** L'analyse de X-Force prévoit que lorsqu'une technologie d'IA générative approchera les 50 % d’adoption, ou lorsque le marché se consolidera à trois technologies ou moins, cela pourrait déclencher des cyberattaques à grande échelle contre ces plateformes.

« Même si les « principes fondamentaux de la sécurité » ne suscitent pas autant d'intérêt que les « attaques conçues par l'IA », il n'en reste pas moins que le plus gros problème de sécurité des entreprises se résume aux éléments fondamentaux et connus, et non aux éléments nouveaux et inconnus », a déclaré **Charles Henderson, Global Managing Partner, IBM Consulting, and Head of IBM X-Force***. « L'usurpation de l'identité numérique est utilisée contre les entreprises à maintes reprises : c'est un problème qui va s'aggraver à mesure que les attaquants investissent dans l'IA pour optimiser ce vecteur. »*

Une crise mondiale de l'identité sur le point de s'aggraver

L'exploitation de comptes valides est devenue la voie privilégiée pour les cybercriminels, avec des milliards d'informations d'identification compromises accessibles sur le Dark Web aujourd'hui. En 2023, X-Force a constaté que les attaquants investissaient de plus en plus dans des opérations visant à obtenir l'identité des utilisateurs, avec une augmentation de 266 % des logiciels malveillants de vol d'informations, conçus pour voler des informations personnelles identifiables telles que les e-mails, les identifiants de réseaux sociaux et des applications de messagerie, les coordonnées bancaires, les données des portefeuilles de crypto-monnaie et bien plus encore.

Cette "entrée facile" pour les attaquants est plus difficile à détecter, ce qui entraîne une réponse coûteuse de la part des entreprises. Selon X-Force, les incidents majeurs causés par des attaquants utilisant des comptes valides ont été associés à des mesures de réponse plus complexes de près de 200 % de la part des équipes de sécurité par rapport à un incident moyen - les défenseurs devant faire la distinction entre l'activité légitime et l'activité malveillante des utilisateurs sur le réseau. En fait, le rapport 2023 d'IBM sur le coût d'une violation de données a révélé que les violations causées par le vol ou la compromission d'informations d'identification nécessitaient environ 11 mois pour être détectées et récupérées - le cycle de réponse le plus long de tous les vecteurs d'infection.

Ce vaste accès à l'activité en ligne des utilisateurs a été mis en évidence par le démantèlement, en avril 2023, par le FBI et les forces de l'ordre européennes, d'un forum mondial de cybercriminalité qui avait recueilli les données de connexion de plus de 80 millions de comptes d'utilisateurs. Les menaces basées sur l'identité numérique continueront probablement à se développer à mesure que les attaquants exploiteront l'IA générative pour optimiser leurs attaques. Dès 2023, X-Force a observé plus de 800 000 messages sur l'IA et GPT dans les forums du Dark Web, ce qui confirme que ces innovations ont attiré l'attention et l'intérêt des cybercriminels.

Les adversaires « se connectent » aux réseaux d'infrastructures critiques

Au niveau mondial, près de 70 % des attaques auxquelles X-Force a répondu visaient des entreprises ayant des infrastructures critiques, un constat alarmant qui montre que les cybercriminels misent sur le besoin de

disponibilité de leur infrastructure de ces cibles de grande valeur pour atteindre leurs objectifs.

Près de 85 % des attaques auxquelles X-Force a répondu dans ce secteur ont été causées par l'exploitation d'applications publiques, d'emails de phishing et l'utilisation de comptes valides. Ce dernier point représente un risque accru pour le secteur, la DHS CISA (l'agence fédérale de cybersécurité et de sécurité des infrastructures) ayant déclaré que la majorité des attaques réussies contre des agences gouvernementales, des organisations ayant des infrastructures critiques et des organismes gouvernementaux au niveau de l'État en 2022 impliquaient l'utilisation de comptes valides. Cela souligne la nécessité pour ces organisations de soumettre fréquemment leurs environnements à des tests de résistance afin de détecter les risques potentiels et d'élaborer des plans de réponse aux incidents.

L'IA générative - La prochaine grande frontière à sécuriser

Pour que les cybercriminels obtiennent un retour sur investissement de leurs campagnes d'attaques, les technologies qu'ils ciblent doivent être omniprésentes dans la plupart des organisations du monde entier. Tout comme les technologies largement utilisées dans le passé ont favorisé les activités cybercriminelles - comme on l'a observé avec les ransomwares et la domination du marché de Windows Server, les escroqueries de type Business Email Compromise (compromission des email professionnels) et la domination de Microsoft 365 ou encore le cryptojacking (minage de cryptomonnaie malveillant) et la consolidation du marché de l'infrastructure en mode as-a-service, ce schéma s'étendra très probablement à l'IA.

X-Force estime qu'une fois la domination du marché de l'IA générative établie - lorsqu'une seule technologie approchera les 50 % d'adoption ou lorsque le marché se consolidera à trois technologies ou moins - l'IA pourrait devenir une réelle surface d'attaque, mobilisant des investissements supplémentaires dans de nouveaux outils de la part des cybercriminels. Bien que l'IA générative soit actuellement en phase de pré-mise sur le marché, il est primordial que les entreprises sécurisent leurs modèles d'IA avant que les cybercriminels n'étendent leur activité. Les entreprises doivent également reconnaître que leur infrastructure sous-jacente existante est une passerelle vers leurs modèles d'IA qui ne nécessite pas de nouvelles tactiques de la part des attaquants pour les cibler - ce qui démontre la nécessité d'une approche holistique de la sécurité à l'ère de l'IA générative, comme le souligne le framework d'IBM pour la sécurisation de l'IA générative.

Autres conclusions du rapport :

- **Où sont passés tous les phishings ?** : bien qu'elles restent l'un des principaux vecteurs d'infection, les attaques par phishing ont vu leur volume diminuer de 44 % par rapport à 2022. Mais comme l'IA est sur le point de permettre d'optimiser cette attaque et que les recherches de X-Force indiquent que l'IA peut accélérer les attaques de près de deux jours, ce vecteur d'infection restera un choix privilégié pour les

cybercriminels.

- **Tout le monde est vulnérable** : RedHat Insights a constaté que 92 % des clients ont au moins un CVE[2] avec des vulnérabilités connues non résolues dans leur environnement au moment de l'analyse, tandis que 80 % des dix principales vulnérabilités détectées dans les systèmes en 2023 ont reçu un score de gravité CVSS[3] "élevé" ou "critique".

- **Le "Kerberoasting" rapporte** : X-Force a observé une augmentation de 100 % des attaques de "kerberoasting", dans lesquelles les attaquants tentent d'usurper l'identité d'utilisateurs pour élever leurs privilèges en abusant des tickets Microsoft Active Directory.

- **Mauvaises configurations de sécurité** : les missions de tests d'intrusion d'X-Force Red indiquent que les mauvaises configurations de sécurité représentent 30 % du total des risques identifiés, et ont révélé plus de 140 façons dont les attaquants peuvent exploiter les défauts de configuration.

Sources supplémentaires

- Pour télécharger une copie du **rapport X-Force Threat Intelligence Index 2024**, veuillez cliquer ici.
- Pour en savoir plus sur les principales conclusions du rapport, vous pouvez consulter le blog **d'IBM Security Intelligence**.
- Vous pouvez vous inscrire ici au webinaire **IBM X-Force Threat Intelligence 2024,** qui se tiendra le **21 mars à 15h00.**
- Contactez ici **l'équipe IBM X-Force** pour une analyse personnalisée des résultats.

Contacts Presse :

IBM
Gaëlle Dussutour
Tél. : + 33 (0)6 74 98 26 92
dusga@fr.ibm.com

Weber Shandwick pour IBM

Louise Weber

Tél. : + 33 (0)6 89 59 12 54

ibmfrance@webershandwick.com

---

[1] Les services aux entreprises comprennent des entreprises telles que les services informatiques et technologiques, les relations publiques, la publicité et la communication.

[2] *CVE ou Common Vulnerabilities and Exposures (Vulnérabilités et expositions communes) : dictionnaire des informations publiques relatives aux vulnérabilités de sécurité.*

[3] *CVSS ou Common Vulnerability Scoring System : système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables.*