

Analyse des tendances des menaces dans le secteur du commerce



La digitalisation continue des organisations commerciales après la pandémie de COVID-19 a stimulé leur croissance, mais a également généré des risques de sécurité dans leur périmètre et pour leurs clients.

Attaques contre les organisations commerciales



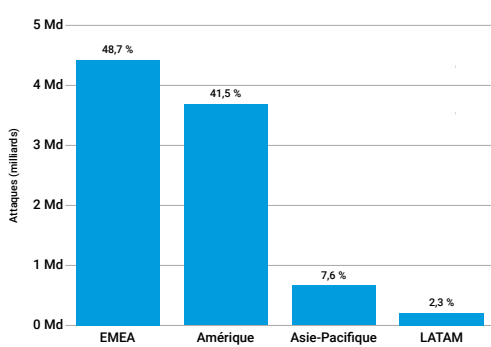
+ de 14 milliards

d'attaques d'applications Web et d'API contre le secteur du commerce

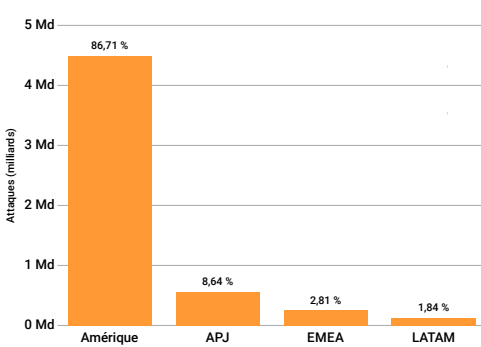
314 %

d'augmentation des attaques par inclusion de fichiers locaux (LFI) entre le 3ème trimestre 2021 et le 3ème trimestre 2022

Les **vecteurs d'attaque émergents**, tels que la falsification de requêtes côté serveur (SSRF) et l'injection de modèles côté serveur (SSTI), représentent une **menace importante** pour le secteur du commerce et d'autres segments de marché, en raison de leur impact potentiel et des dommages qu'ils provoquent, menant à l'**exfiltration de données** et à l'**exécution de code à distance**.



La région Europe, Moyen-Orient et Afrique (EMEA) a dépassé l'Amérique du Nord en matière d'attaques d'applications Web et d'API contre le commerce de détail



L'Amérique du Nord est la première région touchée par les attaques d'applications Web et d'API dans le secteur des hôtels et des voyages, suivie par la zone Asie-Pacifique et Japon

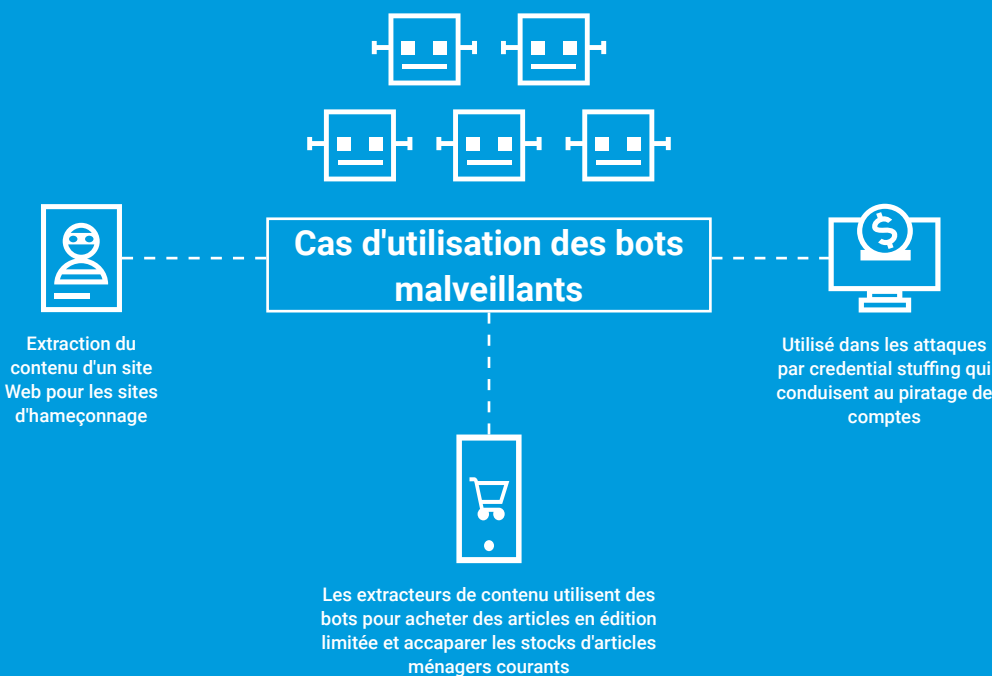
Les agressions contre les clients commerciaux se poursuivent

30,2 %

des campagnes d'hameçonnage imitaient des marques commerciales au 1er trimestre 2023

> 5 000 milliards

de requêtes de bots malveillants entre janvier 2022 et mars 2023



Pour en savoir plus sur les tendances en matière d'attaque dans le secteur du commerce, lisez notre rapport complet.

Télécharger le rapport complet