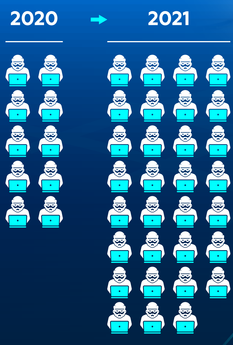
INFOGRAPHIE

L'ÉTAT DES

attaques chiffrées

Le fait que les données soient chiffrées ne signifie pas qu'elles sont en sécurité.

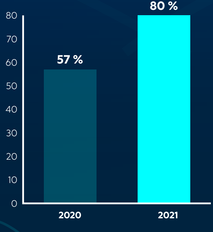
Selon une étude récente de ThreatLabz, les programmes malveillants chiffrés ont augmenté de façon spectaculaire d'une année sur l'autre :



Zscaler a bloqué **314 %** plus d'attaques sur des canaux chiffrés en 2021 qu'en 2020

Plus de **80 %** des attaques se produisent désormais sur des canaux chiffrés, contre 57 % auparavant

Pourcentage des attaques sur des canaux chiffrés

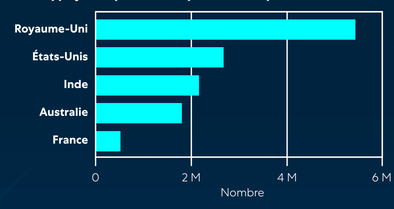


2 344 %
d'augmentation des attaques contre l'industrie technologique

841 %
d'augmentation des attaques contre le commerce de détail et la vente en gros

Les attaques ont touché plus de **200** pays et territoires, ciblant en particulier les centres technologiques

Les cinq pays les plus ciblés par les attaques chiffrées



Attaques chiffrées les plus courantes

- Programmes malveillants
- Hameçonnage
- Cryptominage
- Adspyware
- Botnets
- Attaques de navigateur

Bloquer les attaques chiffrées avec Zero Trust

Empêcher l'intrusion
Protéger les utilisateurs, les serveurs, les charges de travail et l'IoT/OT en minimisant la surface d'attaque et en inspectant l'ensemble du trafic

Empêcher le mouvement latéral
Empêcher les hackers de se déplacer sur votre réseau à la recherche de cibles à forte valeur ajoutée

Empêcher le vol de données
Inspecter toutes les données liées à Internet pour prévenir la perte de données sur Internet et l'exploitation d'appareils non gérés.

Une architecture cloud Zero Trust basée sur un proxy vous permet d'inspecter l'ensemble du trafic, rapidement et à grande échelle. Découvrez plus de statistiques sur les menaces chiffrées et la manière de se protéger : **Téléchargez le rapport.**

Lire le rapport →

zscaler™