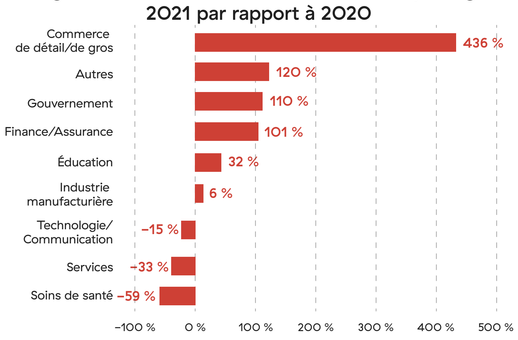
Rapport ThreatLabz 2022 sur l'hameçonnage

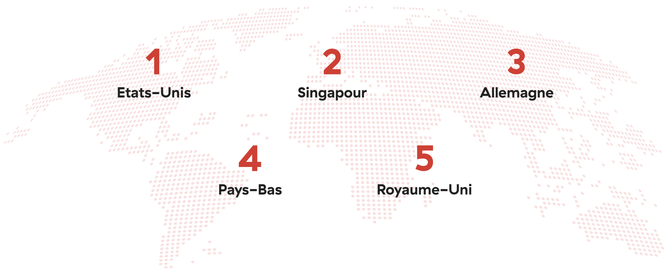
L'hameçonnage a augmenté de 29 % en 2021 par rapport à 2020, selon une étude de ThreatLabz portant sur les données du plus grand cloud de sécurité au monde.

Le commerce de détail et la vente en gros ont connu la plus forte hausse des attaques par hameçonnage, avec une augmentation de 436 %.

Augmentation en % des tentatives d'hameçonnage 2021 par rapport à 2020

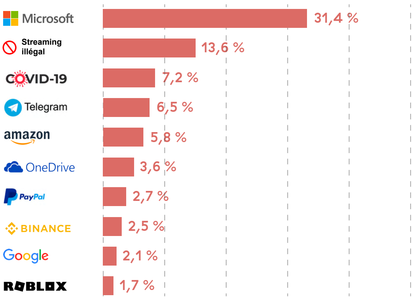


Les pays les plus ciblés sont les États-Unis, Singapour, l'Allemagne, les Pays-Bas et le Royaume-Uni.



Les attaques par hameçonnage imitent les marques populaires et tirent parti d'événements d'actualité.

Principaux thèmes en 2021



L'hameçonnage en tant que service, y compris les kits d'hameçonnage et les cadres open source, permet de mener des attaques avec très peu de compétences techniques. Il s'agit notamment de :

- Fichiers Web PHP/HTML
- Systèmes de distribution du trafic
- Mécanismes d'évitement de la détection
- Méthodes d'exfiltration
- Environnements de contrôle back-end

Protéger votre entreprise contre l'hameçonnage

1. **Comprendre les risques** pour mieux orienter les politiques et la stratégie
2. **Tirer parti des outils automatisés et des informations sur les menaces** pour réduire les incidents d'hameçonnage
3. **Mettre en place des architectures Zero Trust** pour limiter le rayon d'action des attaques réussies
4. **Dispenser une formation en temps utile** pour renforcer la sensibilisation à la sécurité et promouvoir le signalement par les utilisateurs
5. **Simuler des attaques par hameçonnage** pour identifier les lacunes de votre programme

Pour plus de statistiques, de tendances, de prédictions et de conseils, consultez le

Rapport 2022 de ThreatLabz sur l'état de l'hameçonnage.

Zscaler, Inc.
120 Holger Way
San José, California
+1 408 533 0288
www.zscaler.fr