

L'État des attaques cryptées en 2020

Aucune inspection SSL, Aucune protection contre les menaces

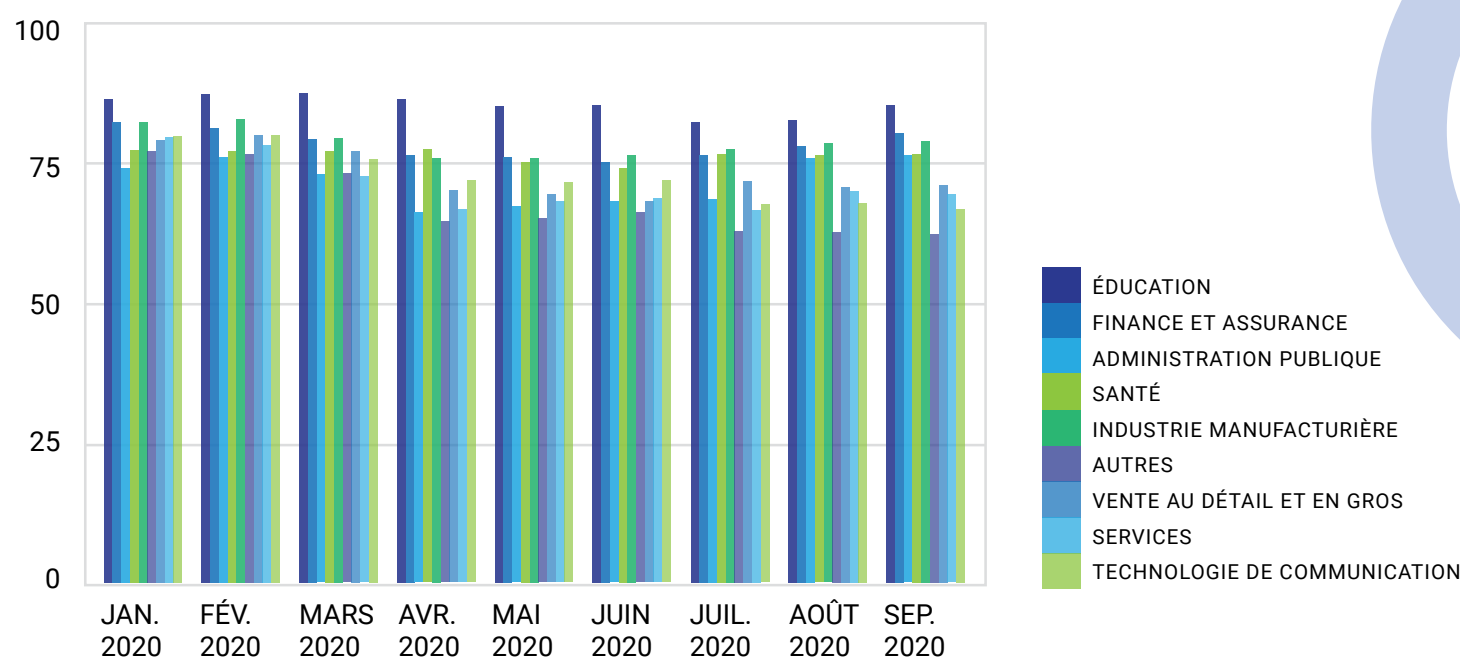
L'équipe ThreatLabZ de Zscaler a analysé les menaces véhiculées à travers le trafic Internet crypté en 2020.

[Lire le rapport](#)

Trafic crypté SSL en expansion

Jusqu'à 80 % du trafic Internet est crypté par le protocole SSL

Pourcentage du trafic crypté dans les secteurs d'activité



260 %

Augmentation du volume des menaces dans le trafic SSL

30 %

Des menaces liées au SSL partent des services de partage de fichiers basés sur le cloud

500 %

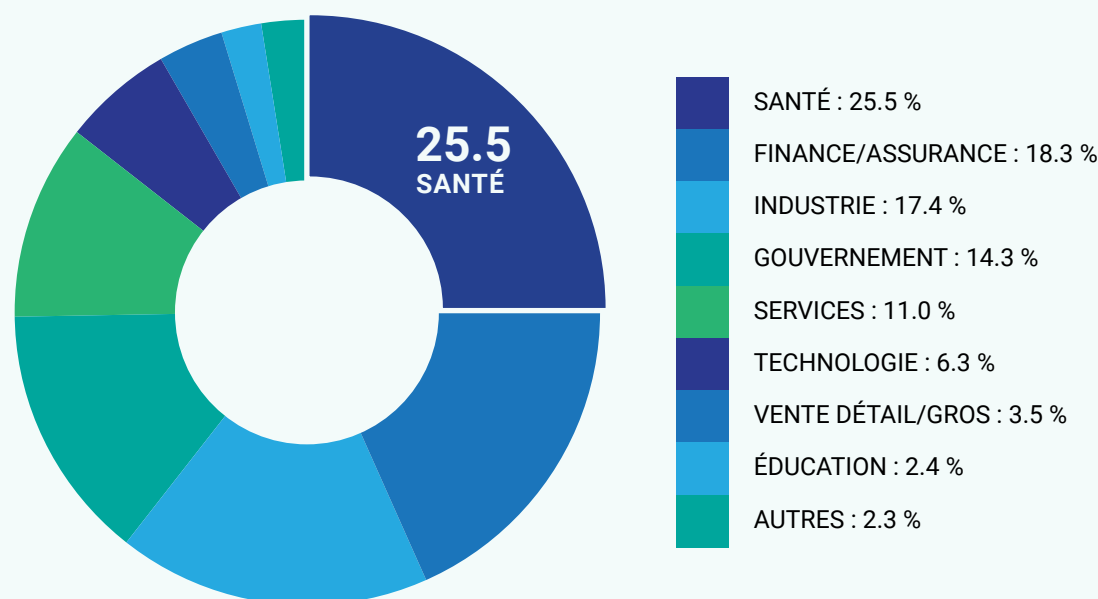
Accroissement des ransomwares à travers le trafic SSL

Les cybercriminels ne font aucune exception éthique, pas même durant la pandémie du COVID, alors qu'ils continuent sans la moindre discrimination à cibler à travers les canaux cryptés le secteur de la santé avec des menaces avancées.

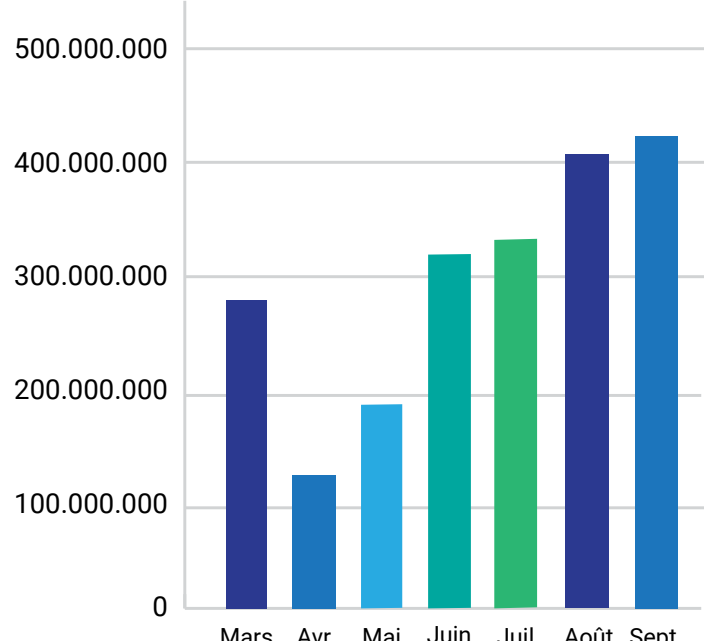
Les cybercriminels tirent profit de la COVID-19

Le secteur de la santé fait les frais des menaces liées au chiffrement SSL

Programmes malveillants bloqués à travers les canaux chiffrés, par industrie



Menaces avancées bloquées sur TLS/SSL par les principaux services de stockage cloud



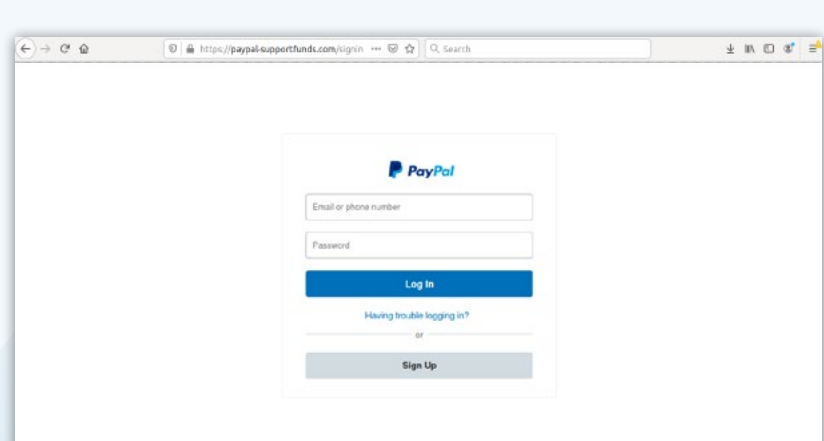
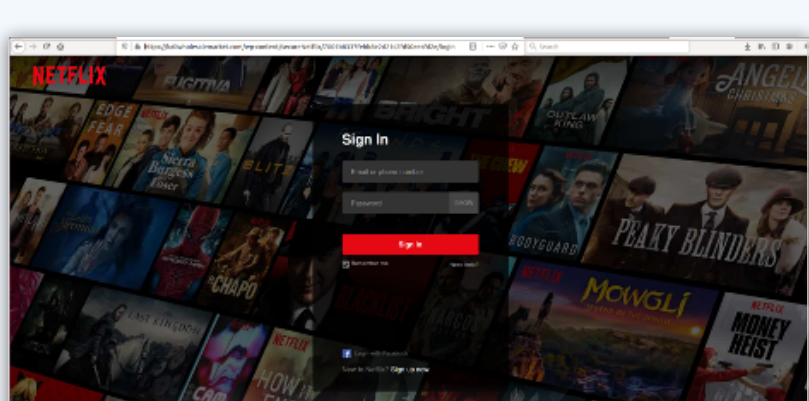
Les hackers abusent des services de partage de fichiers

Croissance constante des attaques visant Google Drive, OneDrive, AWS et Dropbox

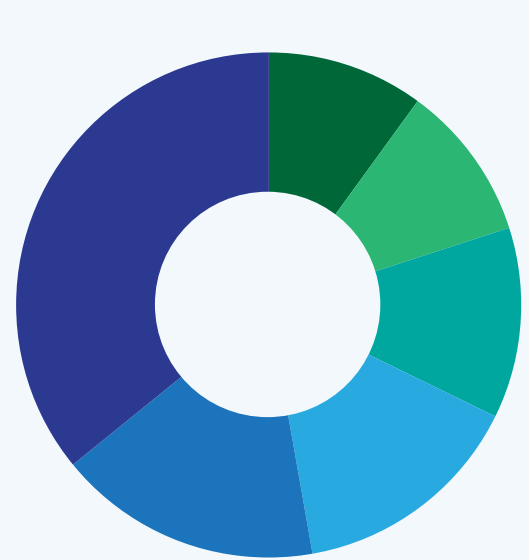
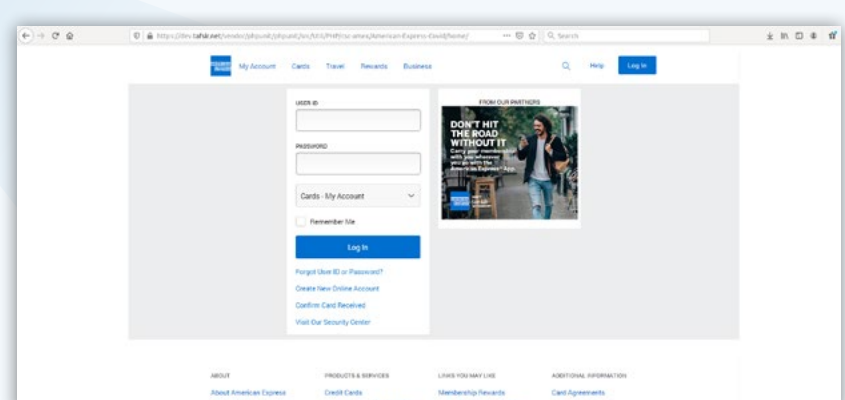
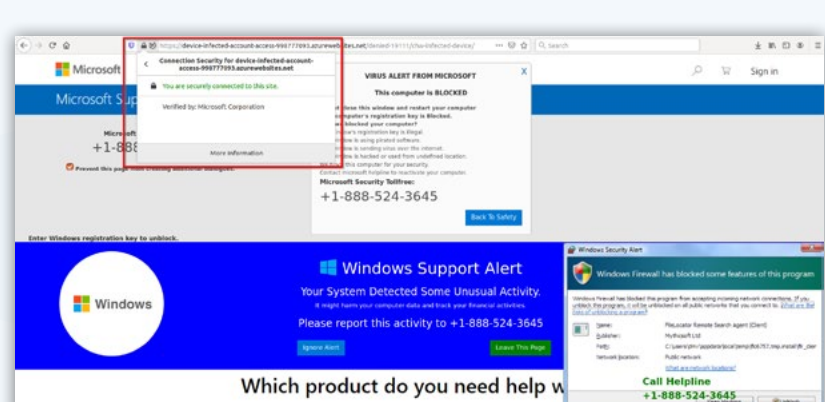


Les erreurs d'orthographe peuvent coûter très cher

Le squat de domaine et les attaques d'homographes dominent le paysage des menaces SSL



Ces images sont des copies illégitimes de légitimes pages Web. Les cybercriminels utilisent les marques populaires pour appâter l'utilisateur peu méfiant avec un faux site Web afin de voler les identifiants de connexion, les PII et les informations financières, puis exécuter des programmes malveillants.



Marques et fonctions d'entreprise les plus fréquemment piratées

Microsoft : 36 %
Support technique : 17 %
PayPal : 15 %
Webmail : 12 %
Google : 10 %
OneDrive : 10 %

ThreatLabZ, l'équipe mondiale de recherche de Zscaler sur les menaces a analysé plus de 6.6 milliards de sessions pour son rapport annuel. Les menaces cachées dans le trafic crypté SSL sont en augmentation, et les équipes de sécurité doivent reconnaître que le trafic crypté ne signifie plus un trafic sûr. À mesure que ce vecteur d'attaque se développe, la nécessité d'inspecter l'ensemble du trafic SSL est de plus en plus importante.

[Lire le rapport](#)



zscaler.com

Research ©2020 ThreatLabZ. Tous droits réservés. Zscaler, Zscaler Internet Access, ZIA, Zscaler Private Access, et ZPA sont soit 1) des marques déposées ou marques de service, soit 2) des marques commerciales ou marques de service de Zscaler, Inc aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs. V11.10.20