

# Statistiques sur les menaces

Période d'analyse : 1er janvier au 31 octobre 2021

Ces statistiques sont basées sur notre outil de sandboxing, **Breach Fighter**. Cet outil analyse **plusieurs millions de fichiers par an**, provenant de toutes les entreprises utilisant les solutions Stormshield à travers le monde.

En raison de la distribution des clients de Stormshield, il s'agit surtout de statistiques européennes.



**1**  
**500**  
COMME PROPORTION DE FICHIERS MALVEILLANTS  
EN 2021

EN 2020 ELLE ÉTAIT DE 1 / 300

## Des pistes d'explications :



Moins de clics des collaborateurs sur des liens de phishing (grâce à la sensibilisation ?)



Moins d'attaques (vraiment ?)

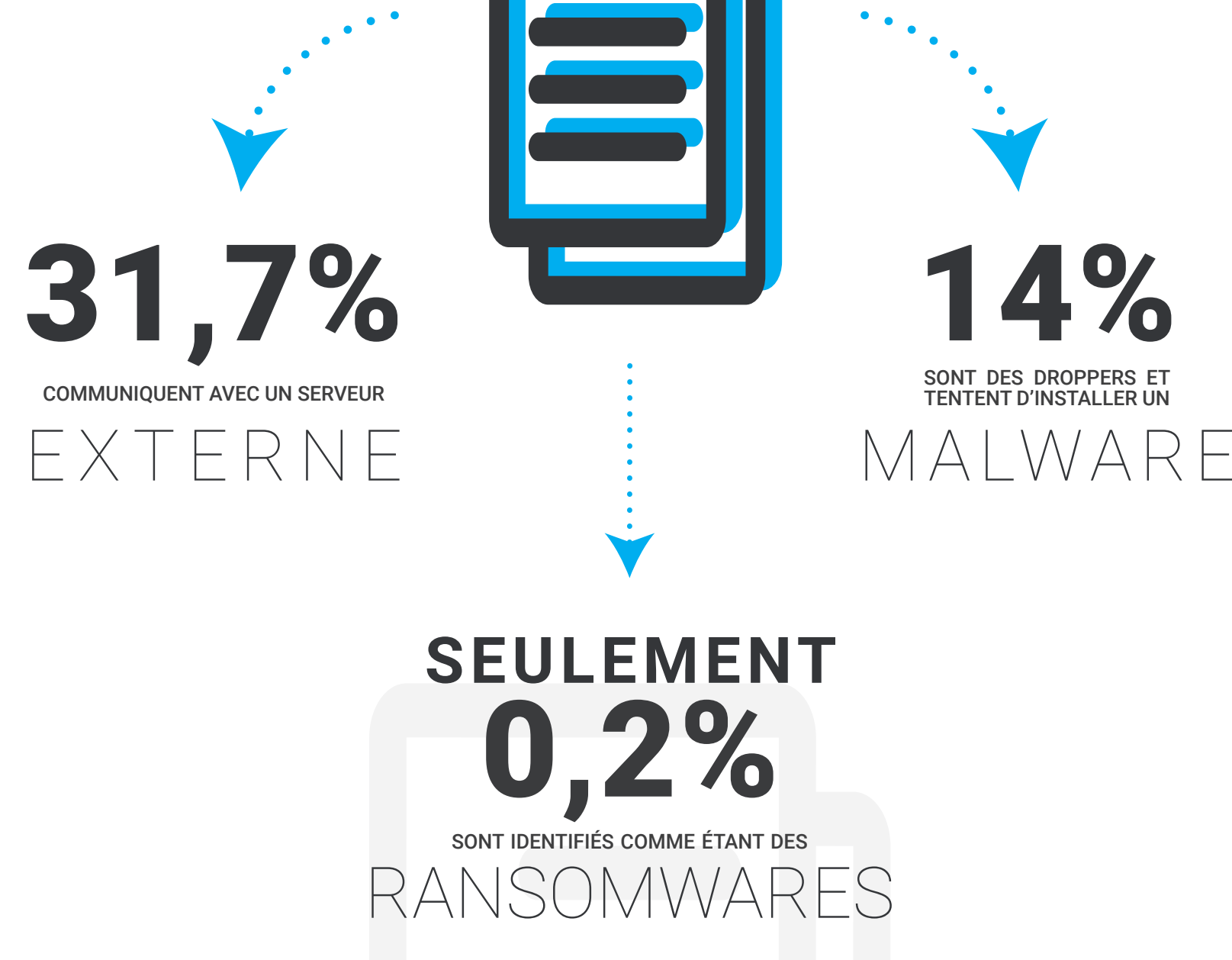


Plus d'attaques ciblées



Meilleur filtrage d'URLs ou davantage de solutions d'anti-phishing déployées

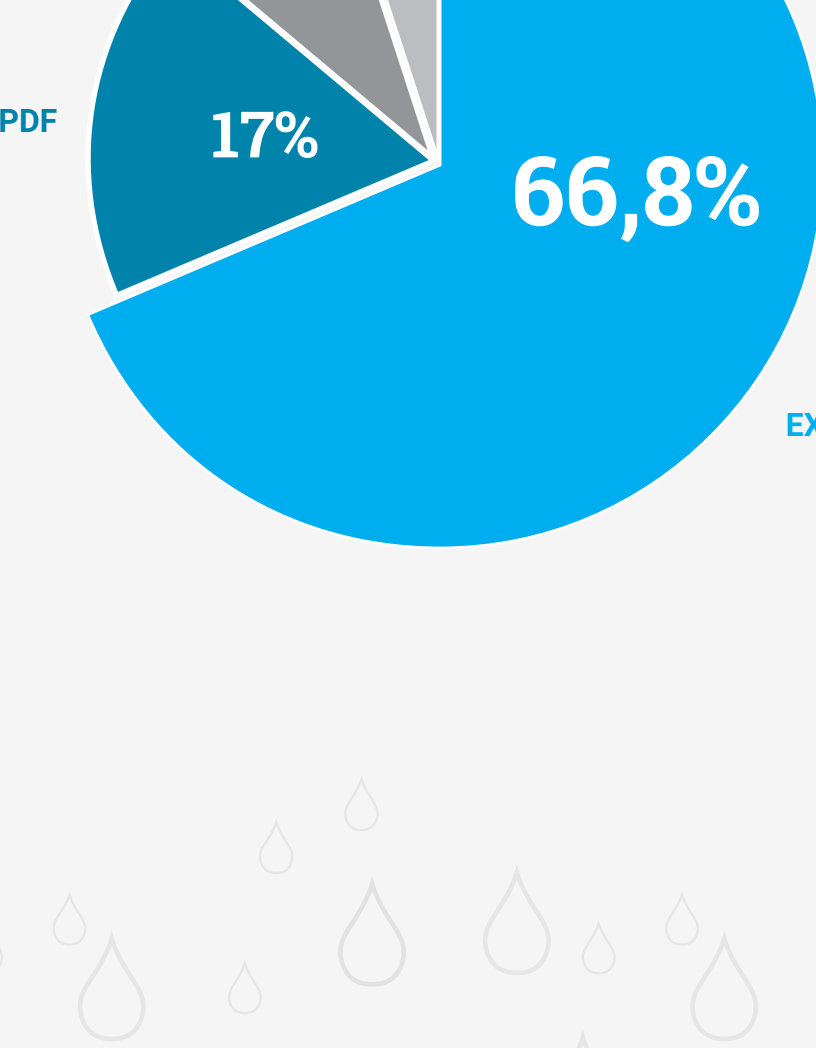
## Dans ces fichiers malveillants



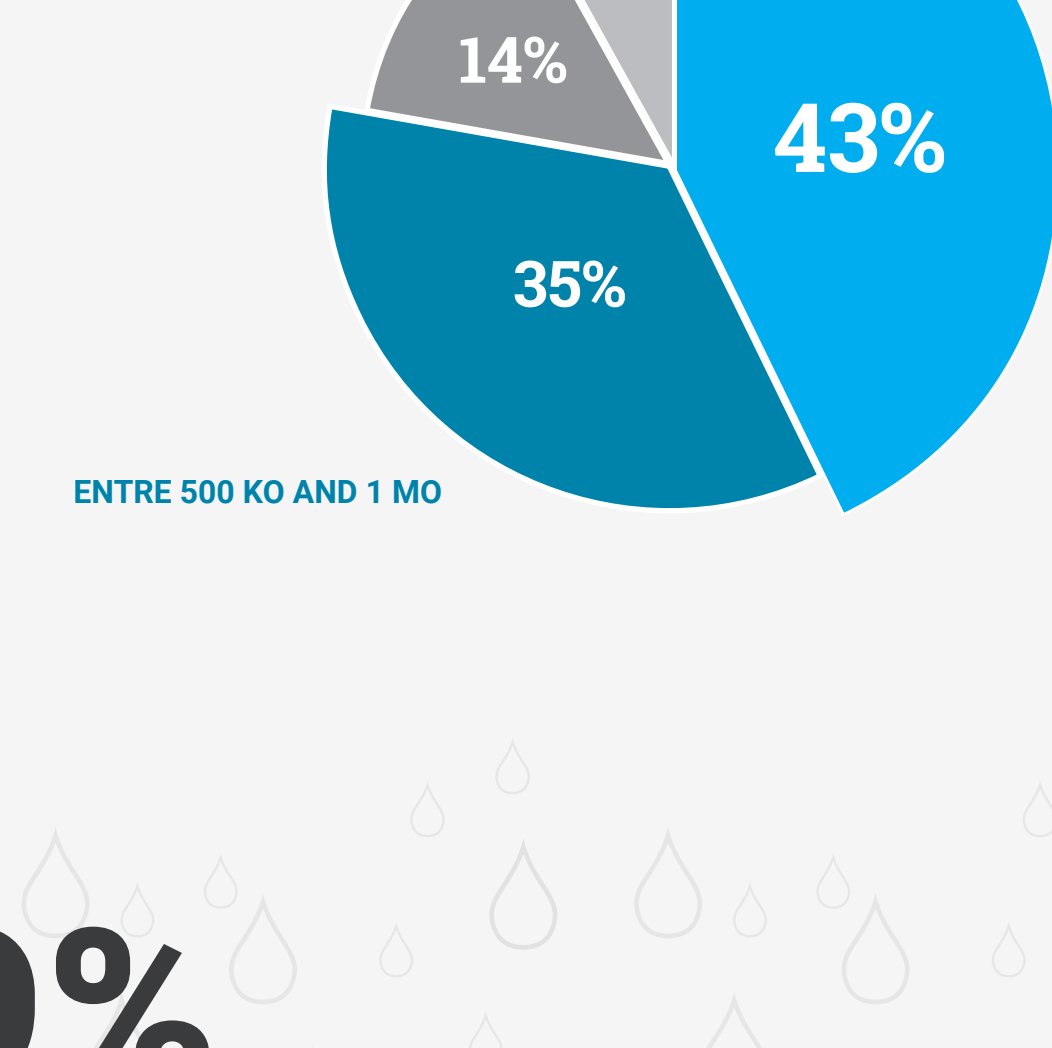
Ce chiffre peut sembler faible, mais il s'explique par le fait que notre solution de sécurité va bloquer les droppers initiaux ou les tentatives de phishing, les ransomwares malveillants seront donc rarement téléchargés.

## Statistiques de Breach Fighter

### FORMAT DES FICHIERS

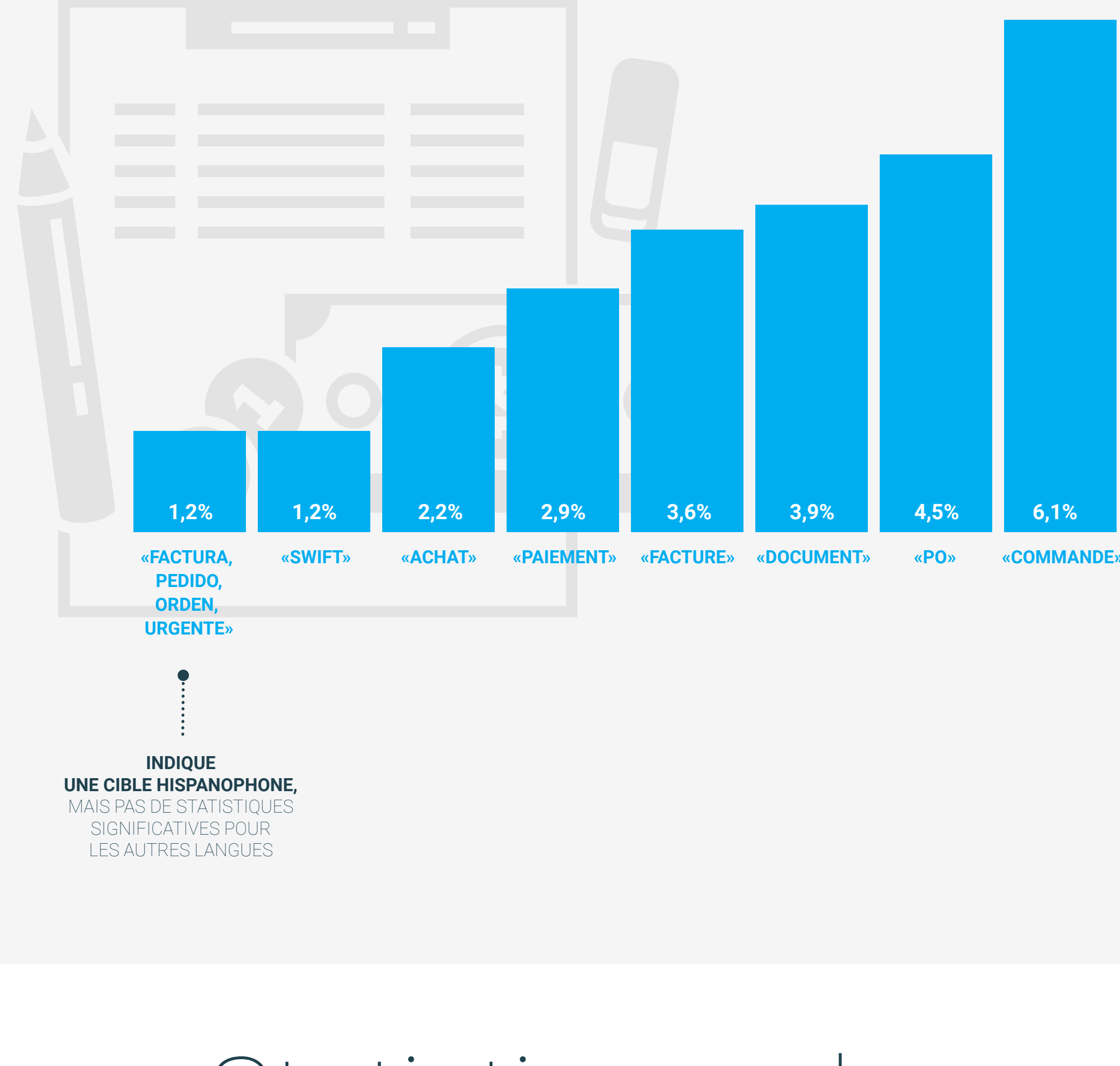


### TAILLE DES FICHIERS



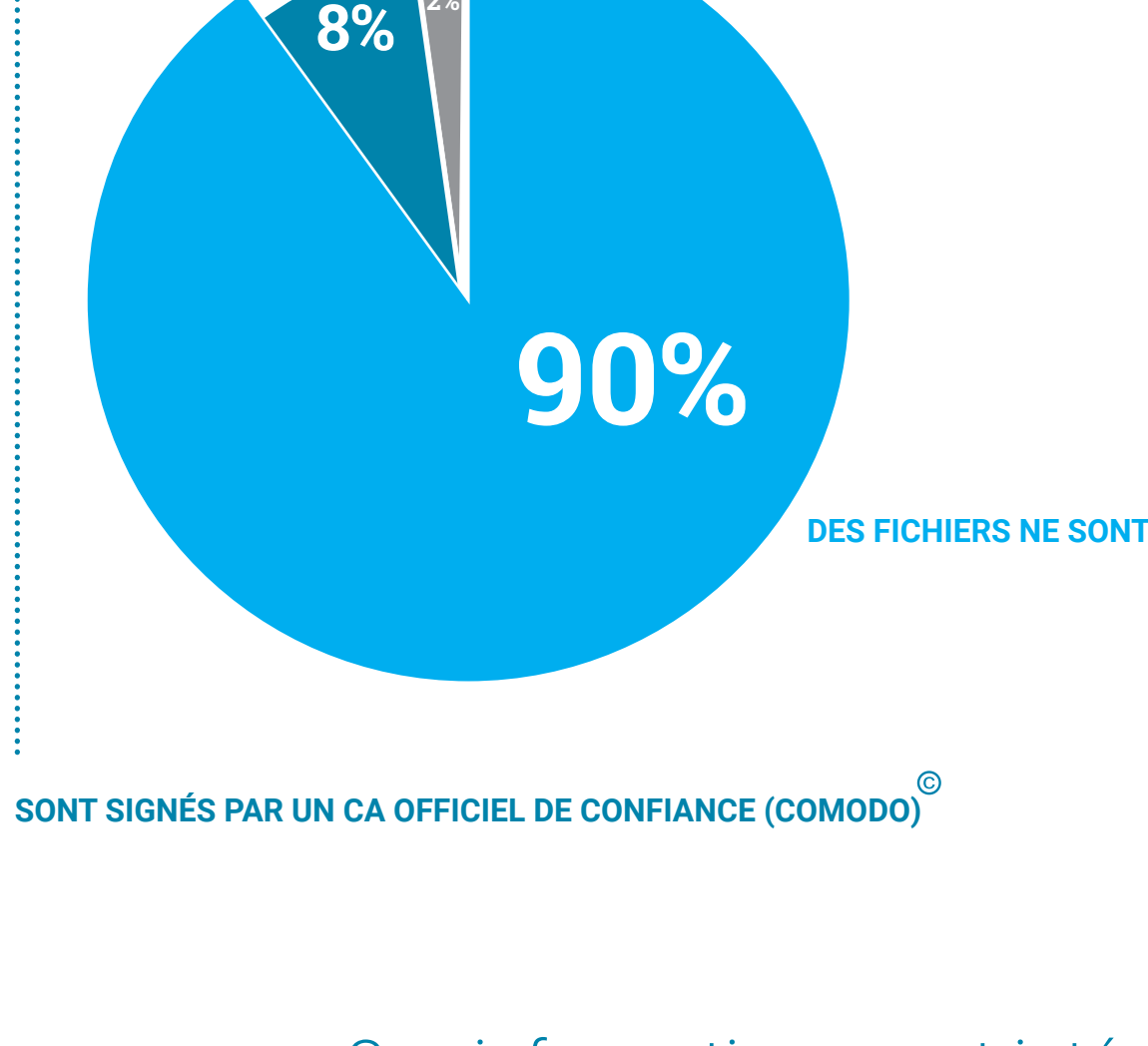
**79%**  
DES DROPPERS SONT DES FICHIERS .XLS OU .DOC

### NOMS DES FICHIERS

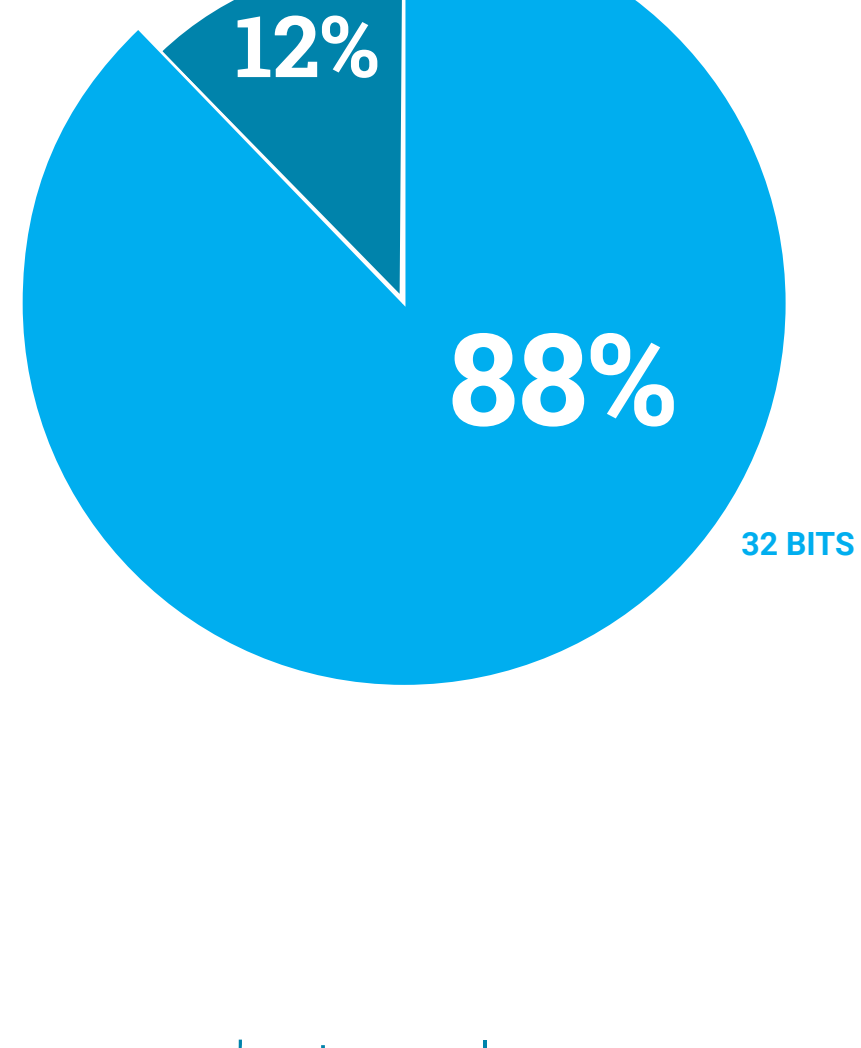


## Statistiques des ransomwares

### INFORMATIONS SUR LES SIGNATURES (AUTHENTICODE)

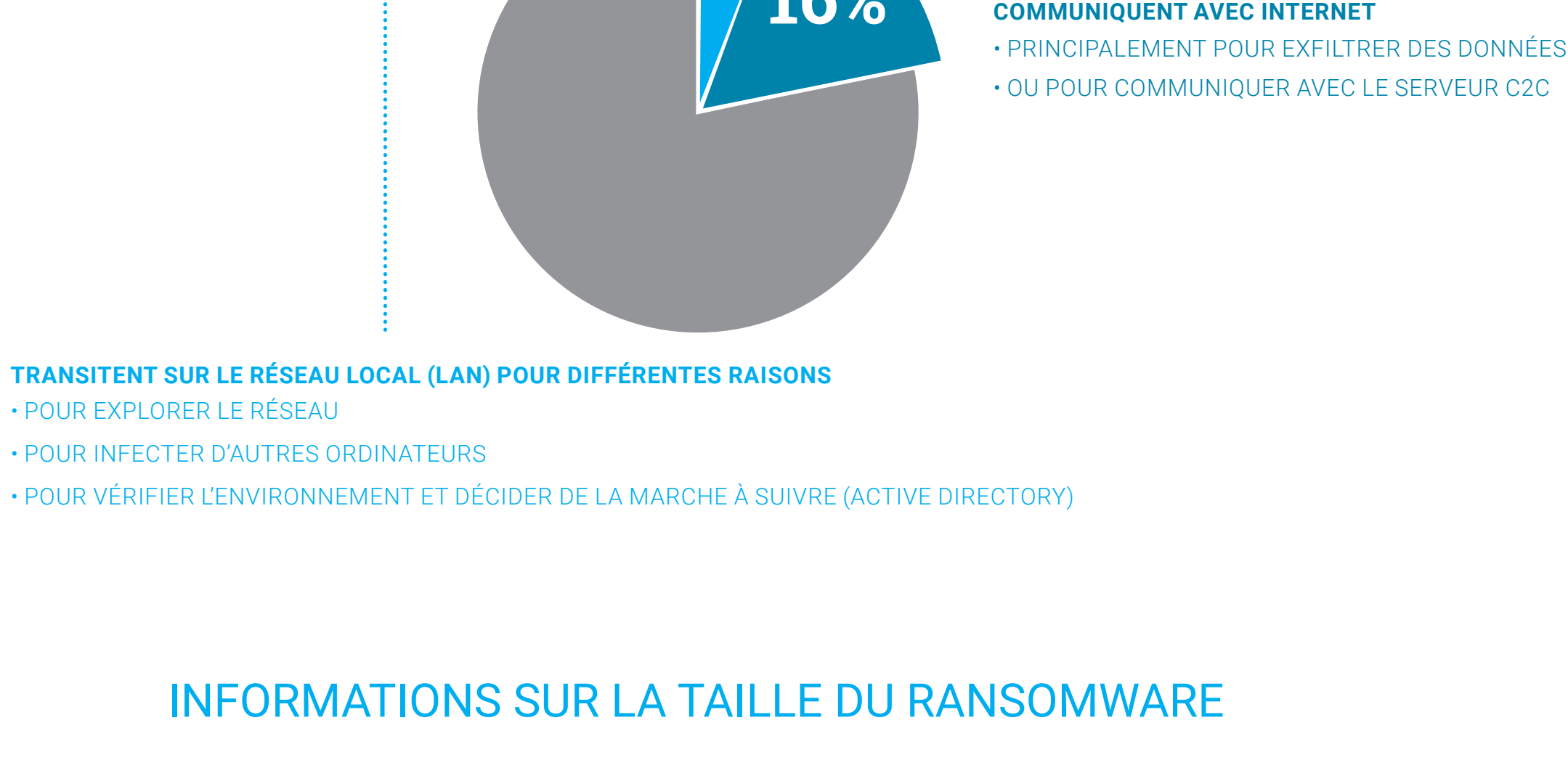


### INFORMATIONS SUR LE CODAGE

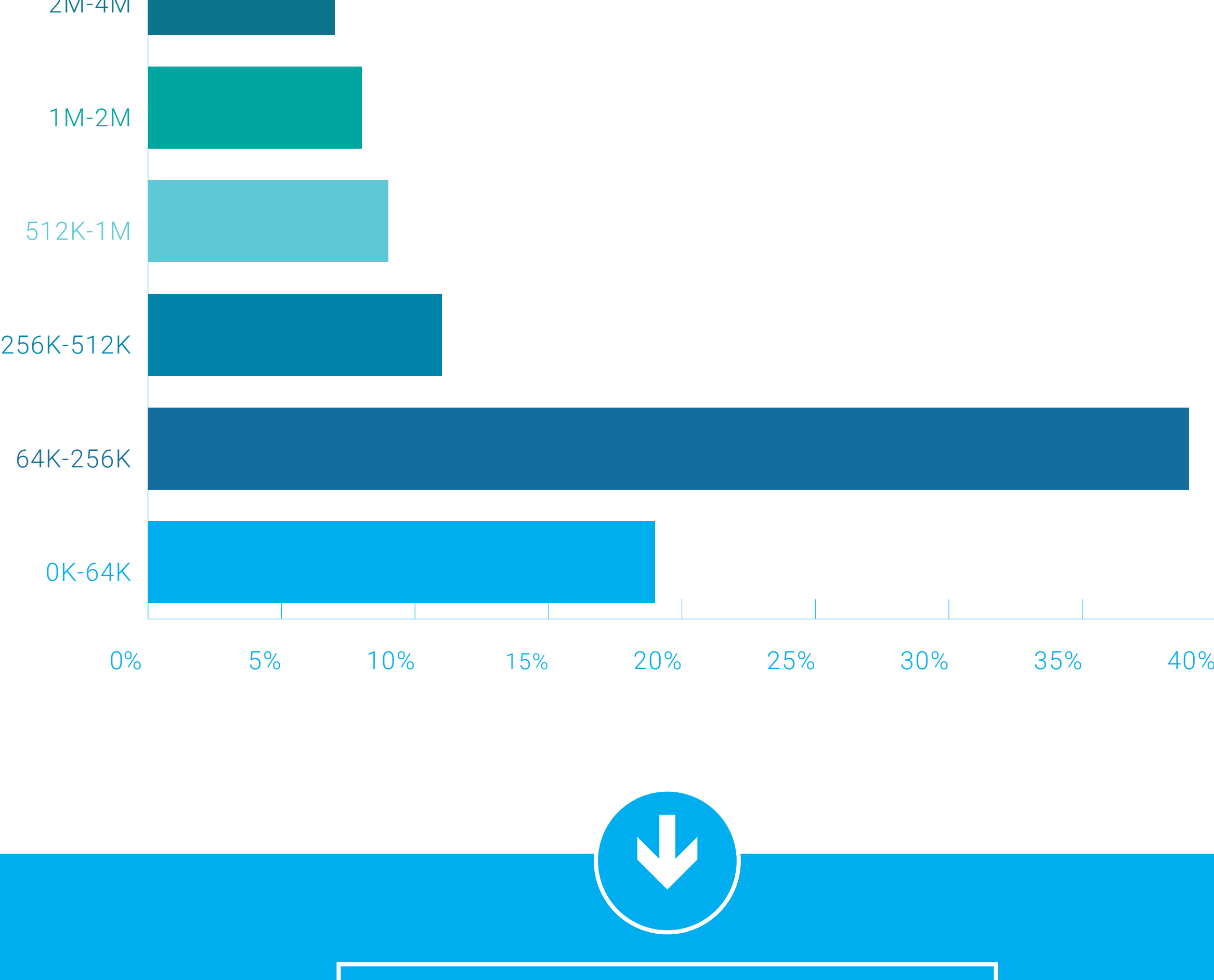


Ces informations sont intéressantes car ce n'est pas la première fois que Comodo est utilisé pour des activités malveillantes. La question du niveau de confiance que l'on peut lui accorder se pose donc. La plupart de ces certificats ont été révoqués par l'autorité, mais pas tous...

### INFORMATIONS SUR LES RÉSEAUX



### INFORMATIONS SUR LA TAILLE DU RANSOMWARE



### AUTHENTICODE

**Authenticode** est un moyen de signer un programme en utilisant une PKI où l'autorité racine est une société de confiance tierce. Ainsi, le programme devient digne de confiance aux yeux des logiciels de sécurité et des systèmes d'exploitation. Par conséquent, ils peuvent plus facilement contourner les protections.



STORMSHIELD

Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin d'assurer la cybersécurité de leurs infrastructures critiques, de leurs données sensibles et de leurs environnements opérationnels. Les technologies Stormshield, certifiées et qualifiées au plus haut niveau européen, répondent aux enjeux de l'IT et de l'OT afin de protéger leurs activités. Notre mission : cyber-séréniser nos clients pour qu'ils puissent se concentrer sur leur cœur de métier, si cruciale pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations. Choisir Stormshield, c'est privilégier une cybersécurité européenne de confiance. Pour en savoir plus : [www.stormshield.com](http://www.stormshield.com)

Powered by **STORMSHIELD** Customer Security Lab