Respect des bonnes pratiques

cybersécurité

MATHIUS Baptiste

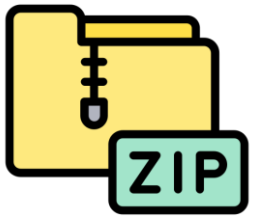
Les formats de fichiers dangereux

- Les fichiers présents en pièce jointes de mail provenant d'une source non fiable

- Certaines extensions sur navigateur, URL douteux, téléchargement sur des sites peu fiables...

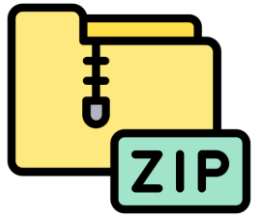
- D'autres fichiers également dangereux :
  - .AVEC
  - Fichiers BAT
  - Fichiers Batch DOS
  - Extensions comme superfilm.avi
  - Chevaux de Troie
  - Webkit exploités avec le jailbreak sur Mac OS

- D'autres fichiers pouvant être suspects, sur PC comme sur Android et IOS



Des fichiers plus dangereux que d'autres

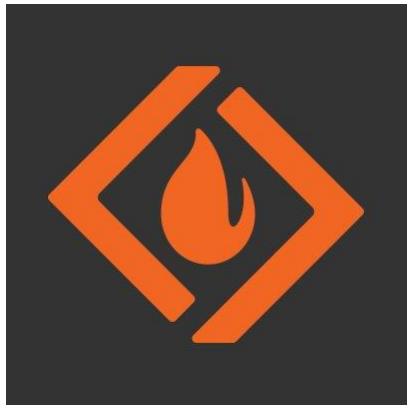
- Fichiers Word, Excel, Powerpoint qui ne proviennent pas d'une source fiable.
- Fichiers .EXE et zip dont nous ne connaissons pas la provenance.



Des sources plus fiables que d’autres

- Voici quelques sources fiables pour tout ce qui est téléchargement de fichiers :

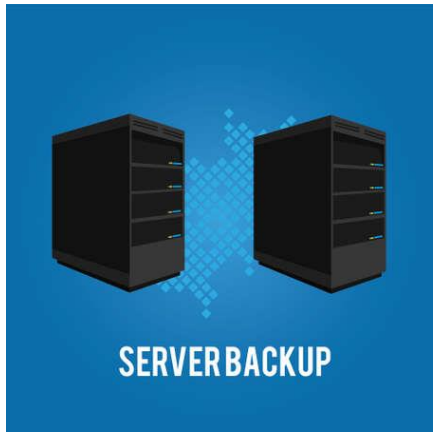
- SourceForge, GitHub ou encore FossHub



Se protéger au mieux des menaces de rançongiciel

- Prevention d’éventuelles menaces :

Sauvegarde miroir (2 serveurs de sauvegardes).
Application de normes de sécurité
Investir auprès d’une entreprise pour la sécurité des e-mails.



Pourquoi ses mesures sont-elles vitales pour l'entreprise ?

- En cas de rançongiciel cela est important car c'est la vie de l'entreprise qui est en péril.

- Au niveau financier, production, achat, vente.
- Perte de temps pour les services auprès des clients.
- Baisse de confiance des clients vis-à-vis de l'entreprise.
- Eventuellement perte de clients importants et réputation entachée.